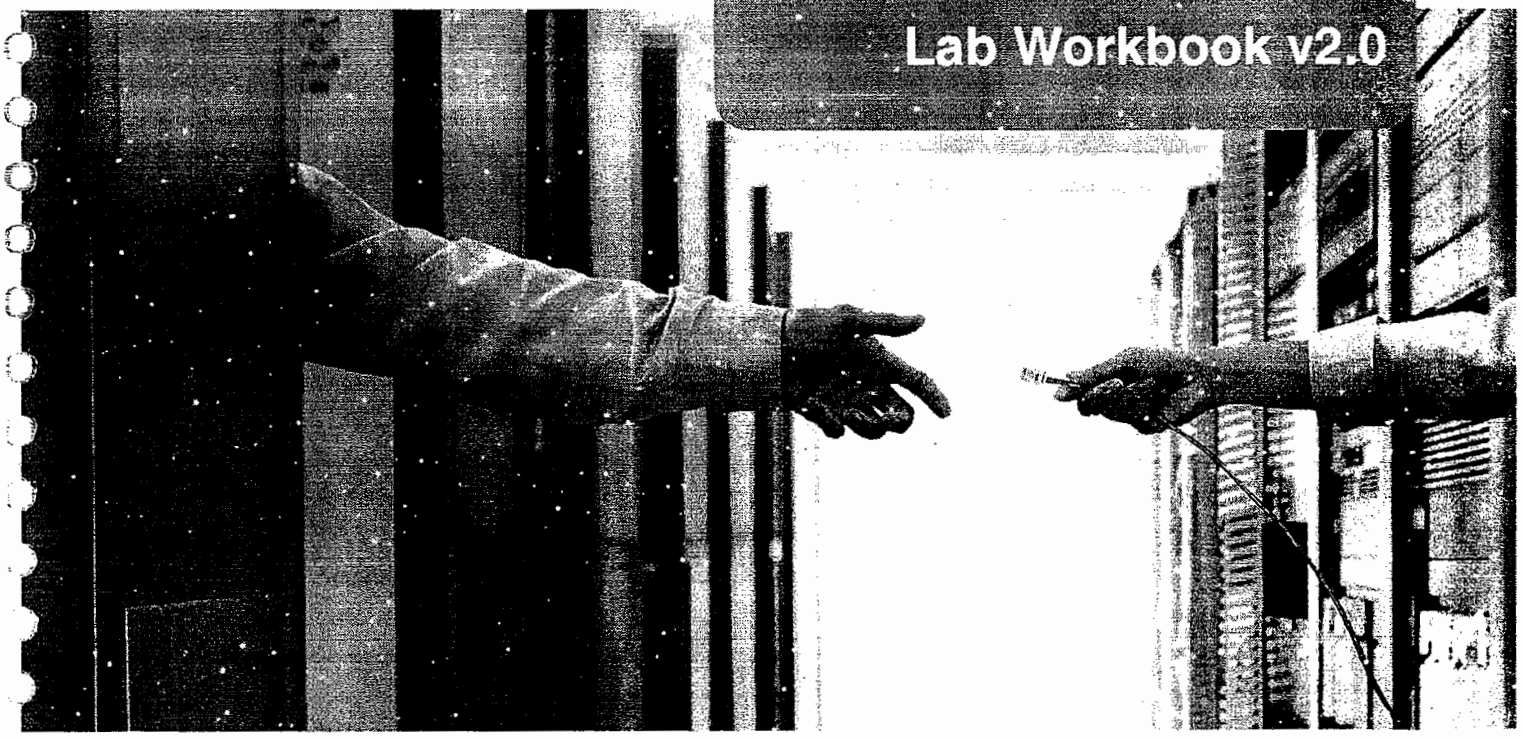
RS = 85/=

NETMETRIC SOLUTIONS

CCNA

Routing & Switching

Lab Workbook v2.0



www.netmetric-solutions.com

Table of Contents

Workbook Introduction 5
Legal Information 6
1. OSI Reference Model 7
1.1 Application Layer (Layer 7) 7
1.2 Presentation Layer (Layer 6) 8
1.3 Session Layer (Layer 5) 8
1.4 Transport Layer (Layer 4) 8
1.5 Network Layer (Layer 3) 9
1.6 Data-Link Layer (Layer 2) 9
1.7 Physical Layer (Layer 1) 10
2. TCP/IP 11
2.1 Comparing OSI and TCP/IP Models 11
2.2 Process/Application Layer 11
2.3 The Internet Layer Protocols 12
3. IP Addressing 14
3.1 IPv4 Address 15
3.2 IP Address Types 16
3.3 Subnet Mask 17
3.4 Subnetting 18
3.5 FLSM Example1 19
3.6 FLSM Example2 20
3.7 FLSM Example3 20
3.8 VLSM (Variable Length Subnet Mask) 21
4. Intro to Routers 23
4.1 Router Classification 23
4.2 External ports of a Router 24
4.3 Internal Components of a Router 25
4.4 Router Start-Up Sequence 27
4.5 Modes of Routers 28
4.6 Accessing the Router 28
4.7 Basic Commands 31
4.8 Basic configurations and verifications 33
5. WAN Connections 38
5.1 Dedicated Line 38
5.2 Circuit Switched 38

5.3 Packet Switched 39
5.4 Leased Line 39
6. WAN Protocols 42
6.1 WAN Encapsulation Protocols 42
6.2 PPP Authentication Protocols 42
6.3 LAB – Basic IP Configuration 45
6.4 Troubleshooting Connectivity 47
6.5 Basic Configuration with 3 Routers 47
7. Frame Relay 49
7.1 Frame Relay Virtual Connection Types 49
7.2 Frame Relay Encapsulations 49
7.3 DLCI (Data Link Connection Identifier) 50
7.4 LMI (Local Management Interface) 50
7.5 Frame Relay Virtual Connection Status Types 50
7.6 Frame Relay Network Connections 50
7.7 VC Advantages 51
7.8 LAB – Basic FR Implementation 51
8. Routing 53
8.1 What is Routing? 53
8.2 Types of Routing? 53
8.3 Autonomous System Number 55
8.4 Routing Protocol Classification 55
8.5 LAB – Static Routing 56
8.6 LAB – Static Routing with 3 Routers 60
8.7 LAB – Default Routing 63
9. RIP v1 (Routing Information Protocol) 66
9.1 What is RIP? 66
9.2 RIP Timers 66
9.3 About RIP Version 2 66
9.4 Advantages of RIP 67
9.5 Disadvantages of RIP 67
9.6 Configuring RIP v1 and v2 67
9.7 LAB – Dynamic Routing using RIP v2 68
10. EIGRP (Enhanced Interior Gateway Routing Protocol) 71
10.1 EIGRP Overview 71
10.2 Dynamic Routing using EIGRP 74

11. OSPF (Open Shortest Path First) 79
11.1 OSPF Overview 79
11.2 OSPF – The seven stage process 80
11.3 OSPF tables 81
11.4 Link-State Data Structure: Network Hierarchy 81
11.5 Issues of maintaing a large OSPF network 82
11.6 OSPF Networking Hierarchy 83
11.7 OSPF Benefits & Drawbacks 83
11.8 LAB – Dynamic Routing using OSPF in Single Area 84
12. ACL (Access Control List) 93
12.1 ACL Overview 93
12.2 Rules of Access List 93
12.3 Wild Card Mask 93
12.4 Standard Access List 94
12.5 Extended Access List 94
12.6 Named Access List 95
12.7 LAB: Implementing Standard Access List 96
12.8 LAB: Restricting Telnet Access to the Router to specified networks or hosts 100
12.9 LAB: Implementing Extended Access List 102
12.10 LAB: Implementing the Standard ACL 105
12.11 LAB: Implementing the Extended ACL 106
13. NAT (Network Address Translation) 108
13.1 NAT Overview 108
13.2 NAT Terminology 109
13.3 Types of NAT 109
13.4 LAB: Implementing Static NAT 111
13.5 LAB: Implement Dynamic NAT 115
13.6 LAB: Implement PAT (Dynamic NAT Overload) 116
13.7 LAB: Implement PAT (Dynamic NAT Overload) 117
14. Basic Switching 119
14.1 Difference between Hub and Switch 119
15. Virtual LAN 127
15.1 Overview 127
15.2 Static VLAN 128
15.3 Dynamic VLAN 129
15.4 Types of Links/Ports 130
15.5 VLAN Identification Methods (Frame Tagging) 130

15.6 LAB: Implementing VLAN 132
15.7 LAB: Creating Basic VLAN Configuration on Switches 135
15.8 LAB: VLAN Trunking 136
16. VLAN Trunking Protocol 145
16.1 Overview 145
16.2 VTP Modes 145
16.3 Benefits of VTP 145
16.4 VTP Configuration in Config Mode 145
16.5 VTP Configuration in Database Mode 146
16.6 LAB: VTP 146
16.7 LAB: Inter VLAN-Routing using Router 152
17. Spanning Tree Protocol (STP) 155
17.1 Overview 155
17.2 STP Terminology 155
17.3 STP Port States 156
17.4 Switch Port States 156
17.5 Typical costs of different networks 156
17.6 LAB: Verifying Spanning Tree Behaviour 157
18. IP Version 6 161
18.1 Overview 161
18.2 Classful Addressing 161
18.3 Techniques to reduce address shortage in IPv4 161
18.4 Features of IPv6 162
18.5 128 bit IPv6 address 162
18.6 IPv6 Address Types 162
18.7 Assigning the IPv6 address 163
18.8 LAB: Basic IPv6 Address Configuration 163
19. Password Recovery on Cisco Routers 165
19.1 Summary 165
19.2 Backup and Restore IOS/Configs 166
19.3 LAB: Restoring the IOS from TFTP into IOS 169

Workbook Introduction

Welcome to Netmetric's CCNA Routing & Switching workbook. Cisco Certified Network Associate (CCNA) is a foundation Cisco certification. This workbook from Netmetric Solutions is designed inline with Cisco's blueprint emphasizing on the core R&S technologies.

This workbook is used alongside CCNA course offered by Netmetric Solutions and upon completion a network professional demonstrates the skills required to install, configure, operate, and troubleshoot medium-size routed and switched networks. A team of technical experts has worked on this workbook lead by Sikandar Shaik – CCIE#35012 (R&S and Service Provider), who is the senior member of our R&S team. Other members who contributed to this workbook are Siddiq Ahmed and Irfan Ahmed.

This workbook consists of 19 modules, each of which is dedicated to a specific technology focusing on the technologies from the blueprint. These modules have practical labs with no unnecessary repetition of tasks from lab to lab. Each lab consists of several tasks. The task portion contains a single or multiple configuration tasks necessary to complete the lab. It is then followed by the configuration solutions for the tasks. Your instructor will provide in-depth explanations of what is being achieved in that particular task.

Thank you for choosing us towards your CCNA Preparation. We are sure you will not be disappointed

Legal Information

Licensing:
This product is individually licensed and copyright of Netmetric Infosolutions Pvt Ltd. Do not Duplicate or redistribute in any form. Violators will be prosecuted. All Rights Reserved.

Trademarks:
Cisco, Cisco IOS, Cisco Systems, CCIE, CCNP, CCNA and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this workbook are the property of their respective owners

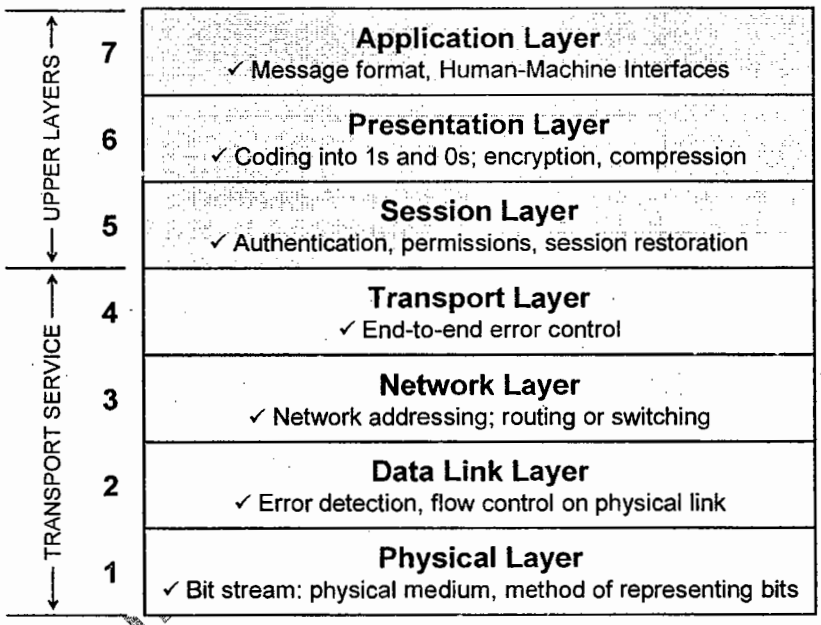
Associations:
This product and contents of the workbook are not associated with, sponsored by, endorsed by or affiliated with Cisco Systems, Inc.

Disclaimer:
All information found here and on Netmetric Solutions website is summary in nature, provided without guarantees of any kind, subject to change without notice and intended for general information only. This publication, CCNA Routing & Switching Workbook, is designed to assist candidates in the preparation for Cisco Systems' CCNA Routing & Switching Exam. While every effort has been made to ensure that all material is as complete and accurate as possible, the enclosed material is presented on an "as is" basis. Neither the authors nor Netmetric Infosolutions Pvt Ltd. assume any liability or responsibility to any person or entity with respect to loss or damages incurred from the information contained in this workbook. This workbook was developed by Netmetric Infosolutions Pvt Ltd. and is an original work of the aforementioned authors. Any similarities between material presented in this workbook and actual CCIE lab material is completely coincidental.

Cisco® Non-Disclosure Agreement Compliance:
This product is compliant with Cisco® Non-Disclosure Agreement (NDA). Netmetric's practice labs, topology, scenarios, topics and solutions are based on the combined practical knowledge of Routing & Switching professionals involved in the creation of this workbook

1. OSI Reference Model

- OSI was developed by the International Organization for Standardization (ISO) and introduced around 1980.
- It is a layered architecture (consists of seven layers), which defines and explains how the communication happens in between two or more network devices within the organization or Internet.
- Each layer defines a set of functions in data communication.



1.1 Application Layer (Layer 7)

- Application Layer is responsible for providing an interface for the users to interact with application services or Networking Services.
- Ex: Web browser etc.
- Identification of Services is done using Port Numbers.
- Port is a logical communication Channel
- Port number is a 16-bit identifier.
  - Total Ports 0 – 65535
  - Reserved Ports 1 – 1023
  - Unreserved Ports 1024 – 65535

Service	Port #
HTTP	80
FTP	21
SMTP	25
Telnet	23
TFTP	69

1.2 Presentation Layer (Layer 6)

- Presentation Layer is responsible for defining a standard format for the data.
- It deals with data presentation.
- The major functions described at this layer are:
  - Encoding – Decoding
    - Ex: ASCII, EBCDIC (Text)
    - JPEG, GIF, TIFF (Graphics)
    - MIDI, WAV (Voice)
    - MPEG, DAT, AVI (Video)
  - Encryption – Decryption
    - Ex: DES, 3-DES, AES
  - Compression – Decompression
    - Ex: Predictor, Stacker, MPPC

1.3 Session Layer (Layer 5)

- Session Layer is responsible for establishing, maintaining and terminating the sessions.
- It deals with sessions or interactions between the applications.
- Session ID is used to identify a session or interaction
  - Ex: RPC, SQL, NFS

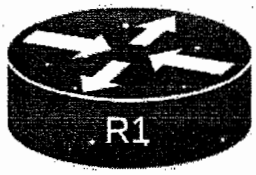
1.4 Transport Layer (Layer 4)

- Transport Layer is responsible for end-to-end transportation of data between the applications
- The major functions described at the Transport Layer are:
  - Identifying Service
  - Multiplexing & De-multiplexing
  - Segmentation
  - Sequencing & Reassembling
  - Error Correction
  - Flow Control

- Identifying a Service: Services are identified at this layer with the help of port **numbers.** The major protocols which takes care of data transportation at Transport layer are...TCP, UDP

TCP	UDP
Transmission Control Protocol	User Datagram Protocol
Connection Oriented	Connection Less
Reliable communication (With ACK)	Unreliable communication (No ACK)
Slower data transportation	Faster data transportation
Protocol number is 6	Protocol number is 17
Ex. HTTP, FTP, SMTP	Ex. DNS, DHCP, TFTP

1.5 Network Layer (Layer 3)



- Network Layer is responsible for end-to end transportation of data across multiple networks.
- Logical addressing & path determination (Routing) are described at this layer.
- The protocols works at Network layer are
  - Routed Protocols:
    - Routed protocols act as data carriers and define logical addressing
    - IP, IPX, AppleTalk... Etc
  - Routing Protocols:
    - Routing protocols performs path determination (Routing).
    - RIP, IGRP, EIGRP, OSPF & others
    - Devices works at Network Layer are Router, Multilayer switch etc.

1.6 Data-Link Layer (Layer 2)

- Data-Link Layer is responsible for end-to-end delivery of data between the devices on a LAN network segment.
- Data link layer comprises of two sub-layers.
  - MAC (Media Access Control)
    - It deals with hardware addresses (MAC addresses).
    - MAC addresses are 12 digit Hexa-decimal identifiers used to identify the devices uniquely on the network segment.

        - It also provides ERROR DETECTION using CRC (Cyclic Redundancy Check) and FRAMING (Encapsulation).
        - Ex: Ethernet, Token ring...etc
    - LLC (Logical Link Control)
        - It deals with Layer 3 (Network layer)
        - Devices works at Data-Link layer are Switch, Bridge, NIC card.

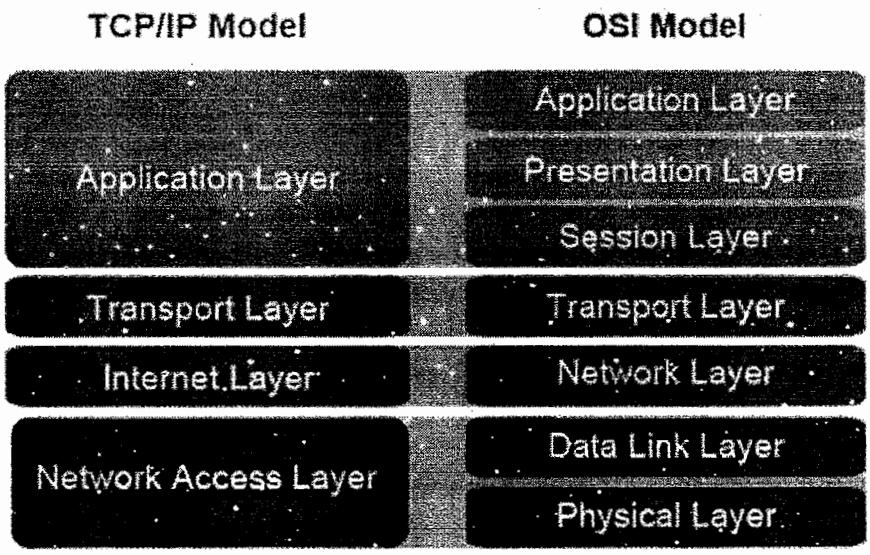
1.7 Physical Layer (Layer 1)

- Physical Layer deals with physical transmission of binary data on the given media (copper, fiber, wireless...).
- It also deals with electrical, mechanical and functional specifications of the devices, media. Etc
- The major functions described at this layer are.
    - Encoding/decoding: It is the process of converting the binary data into signals based on the type of the media.
        - Copper media: Electrical signals of different voltages
        - Fiber media: Light pulses of different wavelengths
        - Wireless media: Radio frequency waves
    - Mode of transmissions of signals: Signal Communication happens in three different modes
        - Simplex
        - Half-duplex
        - Full-duplex
- Devices works at physical layer are Hub, Modems, Repeater, and Transmission Media

2. TCP/IP

- The Transmission Control Protocol/Internet Protocol (TCP/IP) suit was created by the Department of Defense (DoD).
- The DoD model has
  - The Process / Application Layer
  - The Host-to-Host Layer
  - The Internet Layer
  - The Network-access Layer

2.1 Comparing OSI and TCP/IP Models



2.2 Process/Application Layer

- The Process/Application Layer defines protocols for node-to-node application communication and also controls user interface specification.
- Examples for this layer are: Telnet, FTP, TFTP, NFS, SMTP, SNMP, DNS, DHCP etc.
  - Telnet
    - Telnet is used for Terminal Emulation.
    - It allows a user sitting on a remote machine to access the resources of another machine.
  - FTP (File Transfer Protocol)
    - It allows you to transfer files from one machine to another.
    - It also allows access to both directories and files.

        - It uses TCP for data transfer and hence slow but reliable.
    - TFTP (File Transfer Protocol)
        - This is stripped down version of FTP.
        - It has no directory browsing abilities.
        - It can only send and receive files.
        - It uses UDP for data transfer and hence faster but not reliable.
    - SNMP (Simple Network Management Protocol)
        - SNMP enable a central management of Network.
        - Using SNMP an administrator can watch the entire network.
        - SNMP works with TCP/IP.
        - IT uses UDP for transportation of the data.
    - DNS (Domain Name Service)
        - DNS resolves FQDN with IP address.
        - DNS allows you to use a domain name to specify and IP address.
        - It maintains a database for IP address and Hostnames.
    - DHCP (Dynamic Host Configuration Protocol)
        - Dynamically assigns IP address to hosts.

2.3 The Internet Layer Protocols

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

Internet Protocol (IP)

- Provides connectionless, best-effort delivery routing of datagram's.
- IP is not concerned with the content of the datagram's.
- It looks for a way to move the datagram's to their destination.

Internet Control Message Protocol (ICMP)

- ICMP messages are carried in IP datagram's and used to send error and control messages.
- The following are some common events & messages that ICMP relates to:
    - Destination Unreachable
    - Ping
    - Traceroute

Address Resolution Protocol (ARP)

- ARP works at Internet Layer of DoD Model
- It is used to resolve MAC address with the help of a known IP address.

RARP (Reverse ARP)

- This also works at Internet Layer.
- It works exactly opposite of ARP.
- It resolves an IP address with the help of a known MAC address.
- DHCP is the example of an RARP implementation.

3. IP Addressing

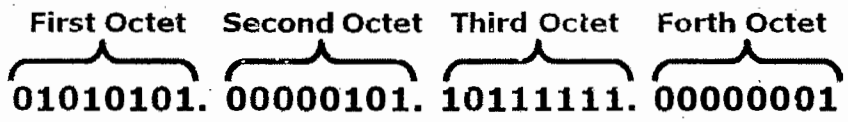
- IP Address is a logical address.
- It is a Network Layer address (Layer 3).
- IP address is given to every device in the network
- It is used to identify the device with in the network.
- Two versions of IP:
  - IPv4 – A 32-bit address
  - IPv6 – A 128-bit address

IP Version 4.0

- **Bit is represent by 0 or 1 (i.e. Binary)**
- **IP address in binary form (32 bits):**

01010101000001011011111100000001

- **32 bits are divided into 4 Octets:**



- **IP address in decimal form:**

85.5.191.1

IP Version 6.0

- 128-bit address is divided along 16-bit boundaries, and each 16-bit block is converted to a 4-digit hexadecimal number and separated by colons (Colon-Hex Notation)
  FD00 : 0DB8 : 7654: 3210 : 2C4C : BA17 : 7124 : 0032

Binary to Decimal Conversion

Taking Example for First Octet :
Total 8 bits, Value will be 0's and 1's
i.e. 2^8 = 256 combination

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
0	0	0	0	0	0	0	0	= 0
0	0	0	0	0	0	0	1	= 1
0	0	0	0	0	0	1	0	= 2
0	0	0	0	0	0	1	1	= 3
0	0	0	0	0	1	0	0	= 4
1	1	1	1	1	1	1	1	= 255

Total IP Address Range
0.0.0.0
to
255.255.255.255

3.1 IPv4 Address

- Total IP Address Range of IPv4 is 0.0.0.0 to 255.255.255.255
- IP Addresses are divided into 5 classes

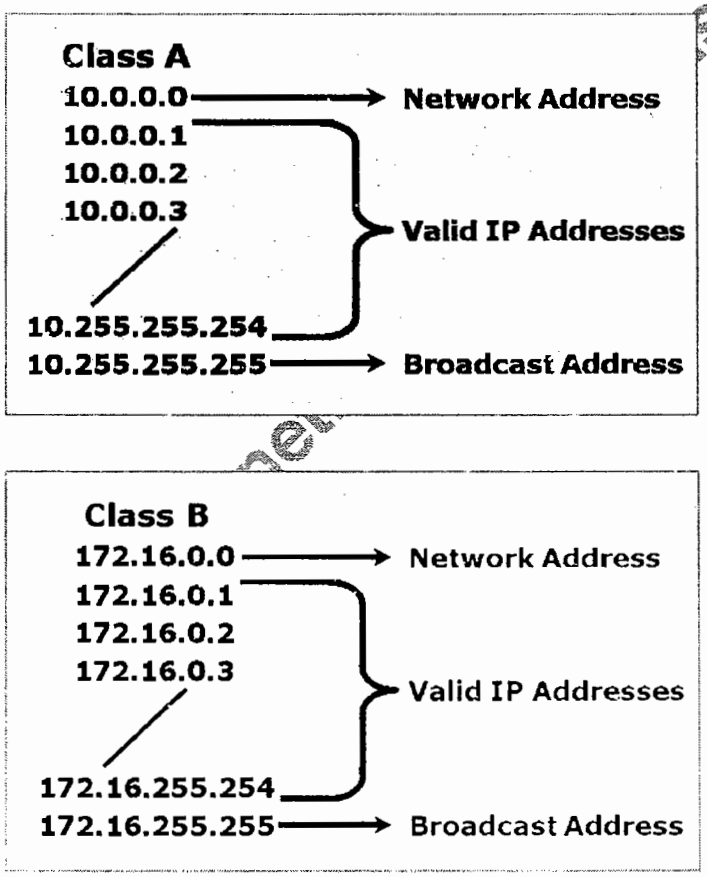
Class	Class Range	Octet Format	Total Network & Hosts
A	0.0.0.0 to 127.255.255.255	**N**.H.H.H	126 Networks & 16777214 Hosts/Network
B	128.0.0.0 to 191.255.255.255	**N.N**.H.H	16384 Networks & 65534 Hosts/Network
C	192.0.0.0 to 223.255.255.255	**N.N.N**.H	2097152 Networks & 254 Hosts/Network
D	224.0.0.0 to 239.255.255.255	Reserved for multicast traffic	
E	240.0.0.0 to 255.255.255.255	Reserved for research and development	

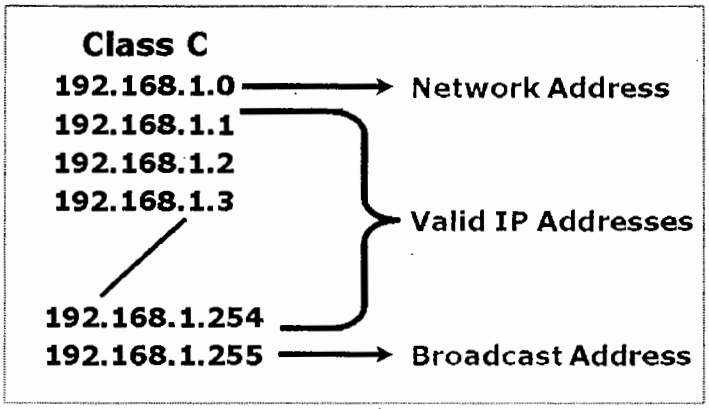
NOTE:

- A host is a specific device in the network
- However a network is a set of devices

3.2 IP Address Types

- Network Address:
  - First IP address of the range
  - It represents the complete network and cannot be assigned to any device
  - This is represented with all bits as **ZERO** in the host portion of the address
- Broadcast Address:
  - The last IP address of the range
  - Used to send the broadcast and cannot be assigned to any device in the network
  - This is represented with all bits as **ONES** in the host portion of the address
- Valid Address:
  - Valid IP Addresses lie between the Network Address and the Broadcast Address.
  - Only Valid IP Addresses are assigned to hosts or any other device in the network





- Private & Public IP addresses:
  - There are certain addresses in each class of IP address that are reserved for Private Networks. These addresses are called private addresses.
  - Range of private IP address
    - Class A – 10.0.0.0 to 10.255.255.255
    - Class B – 172.16.0.0 to 172.31.255.255
    - Class C – 192.168.0.0 to 192.168.255.255

Private IP Address	Public IP Address
Used with LAN or within the company	Used on public network (Internet)
Not recognized on the Internet	Recognized on the Internet
Assigned by the administrator	Assigned by the service provider (IANA)
Unique within the network/company	Globally unique
FREE	Charged by the service provider
Unregistered IP	Registered

- Default Gateway
  - The IP address of the router's ethernet address connecting to the LAN
  - It is an entry and exit point of the network.

3.3 Subnet Mask

- It's an address which is used to identify the network and host portion of an IP address
- Subnet Mask differentiates network portion and host portion of an IP address
- Subnet Mask is been given for network identification of a host Id.
- Represented with all 1's in the network portion and with all 0's in the host portion.

3.4 Subnetting

- Subnetting is the process of dividing a single network into multiple smaller networks.
- Converting host bits into network bits i.e. converting 0's into 1's
- Subnetting helps in minimizing the wastage of IP address
- Subnetting can be performing in two ways.
  - FLSM (Fixed Length Subnet Mask)
  - VLSM (Variable Length Subnet Mask)
- Subnetting can be done based on requirement.
  - Requirement of Hosts? **2^h - 2 >= requirement**
  - Requirement of Networks? **2^n >= requirement**

POWER TABLE

$2^1 = 2$	$2^9 = 512$	$2^{17} = 131072$	$2^{25} = 33554432$
$2^2 = 4$	$2^{10} = 1024$	$2^{18} = 262144$	$2^{26} = 67108864$
$2^3 = 8$	$2^{11} = 2048$	$2^{19} = 524288$	$2^{27} = 134217728$
$2^4 = 16$	$2^{12} = 4096$	$2^{20} = 1048576$	$2^{28} = 268435456$
$2^5 = 32$	$2^{13} = 8192$	$2^{21} = 2097152$	$2^{29} = 536870912$
$2^6 = 64$	$2^{14} = 16384$	$2^{22} = 4194304$	$2^{30} = 1073741824$
$2^7 = 128$	$2^{15} = 32768$	$2^{23} = 8388608$	$2^{31} = 2147483648$
$2^8 = 256$	$2^{16} = 65536$	$2^{24} = 16777216$	$2^{32} = 4294967296$

VALUES IN SUBNET MASK		
Bit	**Value**	**Mask**
1	**128**	**10000000**
2	**192**	**11000000**
3	**224**	**11100000**
4	**240**	**11110000**
5	**248**	**11111000**
6	**252**	**11111100**
7	**254**	**11111110**
8	**255**	**11111111**

3.5 FLSM Example1

- Required hosts are 40, using C-Class address network 192.168.1.0/24
  - $2^h - 2$ >= requirement
  - $2^6 - 2 >= 40$
  - $64 - 2 >= 40$
  - $62 >= 40$
- Host bits required (h) = 6
- Converted network Bits (n) = Total host bits – required host bits
  $= 8 - 6 = 2$
- Converted network Bits (n) = 2
- Total. N. Bits = default N bits + converted N bits = 24 + 2 = /26
- Hosts/Subet $= 2^h - 2 = 2^6 - 2 = 64 - 2$
  $= 62$ Hosts/Subnet
- Subnets = $2^n = 2^2 = 4$ Subnets
- Customized subnet mask = (/26) = 255.255.255.192
- Range: $2^{h=26} = 64$

Network ID	**Broadcast ID**
192.168.1.0/26	192.168.1.63/26
192.168.1.64/26	192.168.1.127/26
192.168.1.128/26	192.168.1.191/26
192.168.1.192/26	192.168.1.255/26

3.6 FLSM Example2

- Required hosts are 500, using B-Class address network 172.16.0.0/16
  - $2^h - 2$ >= requirement
  - $2^9 - 2$ >= 500
  - 512 – 2 >= 510
  - 510 >= 500
- Host bits required (h) = 9
- Converted network Bits (n) = Total. H. Bits -- req. H. Bits
  = 16 – 9 = 7
- Converted network Bits (n) = 7
- Total. N. Bits = default N bits + converted N bits = 16 + 7 = /23
- Hosts/Subet = $2^h - 2 = 2^9 - 2$ = 512 – 2
  = 510 Hosts/Subet
- Subnets = $2^n = 2^7$ = 128 Subnets
- Customized subnet mask = (/23) = 255.255.254.0
- Range: $2^h = 2^9$ = 512

Network ID	Broadcast ID
172.16.0.0/23	172.16.1.255/23
172.16.2.0/23	172.16.3.255/23
172.16.4.0/23	172.16.5.255/23
172.16.6.0/23	172.16.7.255/23
.....	
.....	
.....	
172.16.254.0/23	172.16.255.255/23

3.7 FLSM Example3

- Required hosts are 2000, using A-Class address network 10.0.0.0/8
  - $2^h - 2$ >= requirement
  - $2^{11} - 2$ >= 2000
  - 2048 – 2 >= 2000
  - 2046 >= 2000
- Host bits required (h) = 11
- Converted network Bits (n) = Total. H. Bits – req. H. Bits
  = 24 – 11 = 13
- Converted network Bits (n) = 13
- Total. N. Bits = default N bits + converted N bits = 8 + 13 = /21

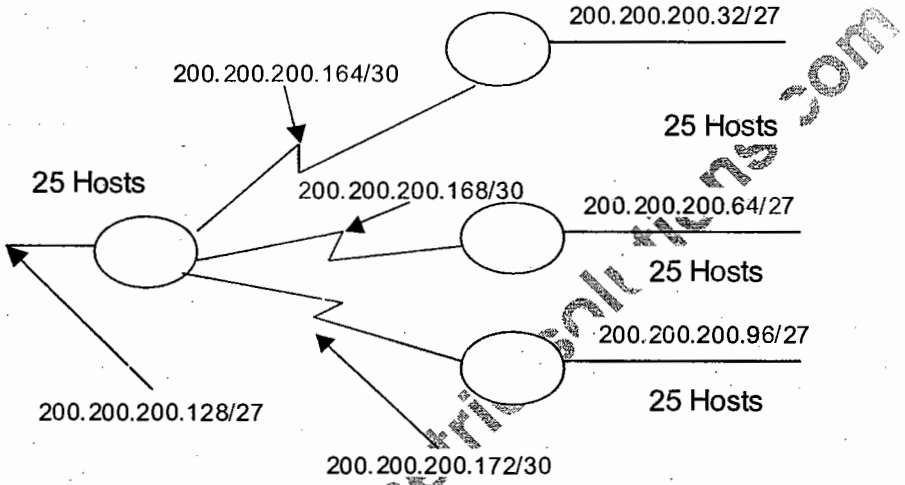
- Hosts/Subet $= 2^h - 2 = 2^{11} - 2 = 2048 - 2$
  $= 2046$ Hosts/Subet
- Subnets $= 2^n = 2^{13} = 8192$ Subnets
- Customized subnet mask = (/21) = 255.255.248.0
- Range:

Network ID	Broadcast ID
10.0.0.0/21	10.0.7.255/21
10.0.8.0/21	10.0.15.255/21
10.0.16.0/21	10.0.23.255/21
....	
....	
10.0.248.0/21	10.0.255.255/21
10.1.0.0/21	10.1.7.255/21
10.1.8.0/21	10.1.15.255/21
10.1.16.0/21	10.1.23.255/21
....	
....	
10.1.248.0/21	10.1.255.255/21
10.2.0.0/21	10.2.7.255/21
10.2.8.0/21	10.2.15.255/21
10.2.16.0/21	10.2.23.255/21
....	
....	
10.2.248.0/21	10.2.255.255/21
....	
....	
10.255.0.0/21	10.0.7.255/21
10.255.8.0/21	10.0.15.255/21
10.255.16.0/21	10.0.23.255/21
....	
....	
10.255.248.0/21	10.255.255.255/21

3.8 VLSM (Variable Length Subnet Mask)

- VLSM is used for proper implementation of IP addresses which allows more than one subnet mask for a given network according to the individual needs

- Logically dividing one network into smaller networks is called as Subnetting or VLSM.
- One subnet can be subnetted for multiple times for efficient use.
- Requires classless Routing Protocols.
- Advantages of VLSM are:
  - Efficient Use of IP addresses
  - Without VLSMs, networks would have to use the same subnet mask throughout the network. But all your networks don't have the same number of hosts' requirement.
- Example of a VLSM Network



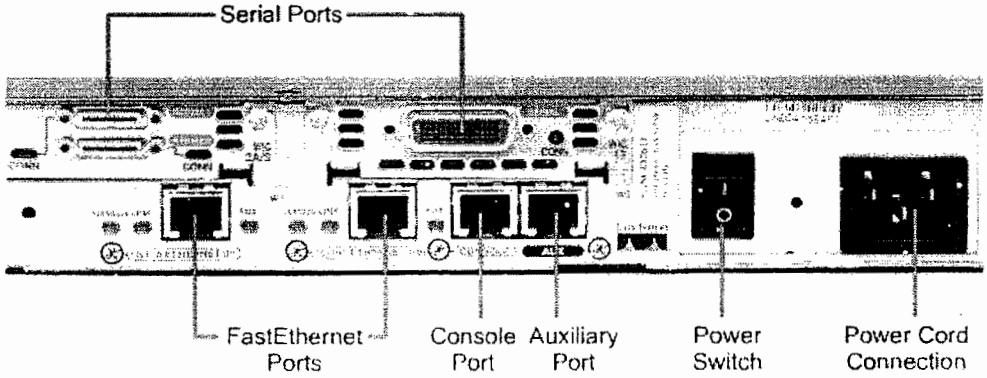
4. Intro to Routers

- Router is a device, which makes communication possible between two or more **different** networks present in same or different geographical locations.
- It is an internetworking device used to connect two or more different networks
- It works on layer 3 (i.e. Network Layer)
- It does two basic things:
  - Select the best path from the routing table.
  - Forward the packet on that path
- Other companies apart from Cisco do manufacture routers:
  - Nortel
  - Netgear
  - Juniper
  - Dlink
  - 3Com

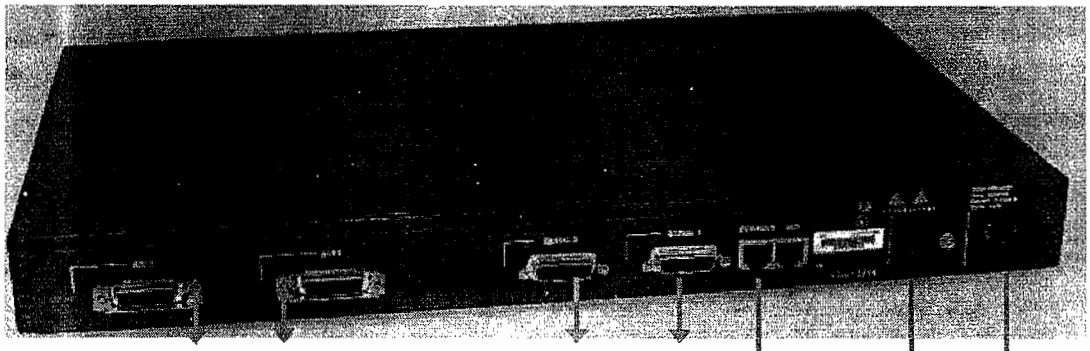
4.1 Router Classification

Fixed Router	Modular Router
Cannot upgrade	Upgradeable
Cannot add or remove interfaces	Can add or remove interfaces
Does not have any slots	Slots are available depending on the router series

Modular router example:

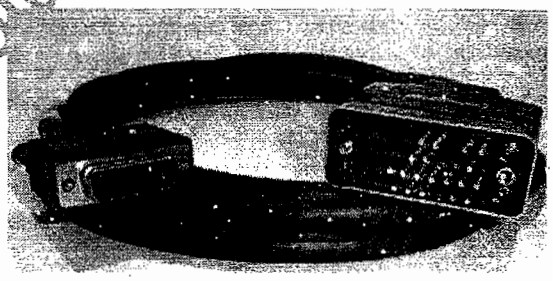


Fixed router example:



4.2 External ports of a Router

- WAN Interfaces
  - Serial interface (s0, s1, s0/0, s0/1, s0/0/0 etc) – 60 pin/26 pin (smart serial)
    - Serial pin configuration is 60-pin configuration female (i.e. 15 pins and 4 rows) and Smart Serial pin configuration is 26 pin configurations female.
    - It is known as WAN Port
    - It is used for connecting to Remote Locations
    - V.35 cable has 60-pin configuration male at one end and on the other end 18-pin configurations male.

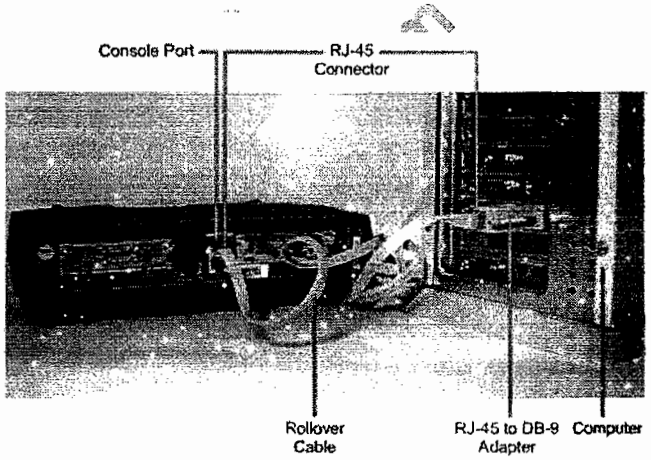


  - ISDN interface (BRI0 etc) – RJ45 (used for ISDN wan connections)
- LAN Interfaces – Ethernet
  - AUI (Attachment Unit Interface) (E0) – 15 pins
    - AUI pin configuration is 15-pin female.
    - It is known as Ethernet Port or LAN port or Default Gateway.
    - It is used for connecting LAN to the Router.
    - Transceiver is used for converting 8 wires to 15 wires i.e., RJ45 to 15 pin converter.
  - 10baseT – RJ45
- Administrative Interfaces
  - Console – RJ45 – Local Administration
    - It is known as Local Administrative Port

- It is generally used for Initial Configuration, Password Recovery and Local Administration of the Router.
- It is RJ45 Port
- **IMP:** It is the most delicate port on the Router. So make less use of the Console Port.

- Auxiliary – RJ45 – Remote Administration
  - It is known as Remote Administrative Port.
  - Used for remote administration
  - Its an RJ-45 port
  - A console or a rollover cable is to be used.

- Console Connectivity
  - Connect a rollover cable to the router console port (RJ-45 connector).
  - Connect the other end of the rollover cable to the RJ-45 to DB-9 converter
  - Attach the female DB-9 converter to a PC Serial Port.
  - Open Emulation Software

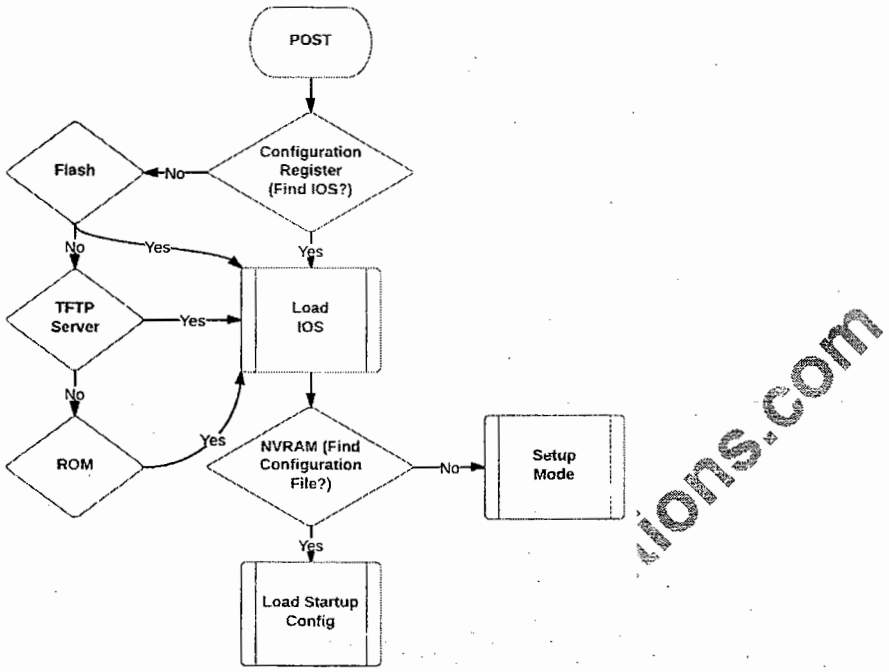


4.3 Internal Components of a Router

- ROM
  - It is an integrated chip on the motherboard which contains the bootstrap program which tells how to load the IOS (Operating System)
  - ROM is used to start and maintain the router.
  - Holds the POST and the bootstrap program, as well as the mini-IOS.
- POST (power-on self-test)
  - Stored in the microcode of the ROM, the POST is used to check the basic functionality of the router hardware and determines which interfaces are present.
- Mini-IOS
  - Also called the RXBOOT or bootloader by Cisco, the mini-IOS is a small IOS in ROM that can be used to bring up an interface & load the Cisco IOS into the flash memory.
  - The mini-IOS can also perform a few other maintenance operations.

- RAM (Random Access Memory)
  - Used to hold the temporary config, recent packet buffers information, ARP cache, routing tables, and also the software/data structures that allow the router to function.
  - Also called as Running-config
  - The IOS is loaded in to the RAM from the Flash at the time of booting.
- Flash memory
  - Stores the Cisco IOS by default.
  - Flash memory is not erased when the router is reloaded.
- NVRAM (NonVolatile RAM)
  - Used to hold the router and switch configuration.
  - NVRAM is not erased when the router or switch is reloaded.
  - It will not store an IOS.
  - The configuration register is stored in NVRAM.
- Configuration register file
  - Used to control how the router boots up. This value can be found as the last line of the *show version* command output
  - By default is set to **0x2102**, which tells the router to load the IOS from flash memory as well as to load the configuration from NVRAM.

4.4 Router Start-Up Sequence



- Performing the POST and Loading the Bootstrap Program
  - The power-on selftest (POST) is a process that occurs on almost every computer when it boots. The POST is used to test the router hardware.
  - After the POST, the bootstrap program is loaded. The bootstrap program locates the Cisco IOS and loads it into RAM.
- Locating and Loading the IOS Software
  - The location of the IOS file is specified by the value of the configuration register setting. The bits in this setting can instruct the device to load the IOS file from the following locations:
    - Flash memory
    - A TFTP server
  - To load the IOS normally from flash, the configuration register setting should be set to 0x2102.
- Locating and Executing the Startup Configuration File or Entering Setup Mode
  - After the IOS is loaded, the bootstrap program searches for the startup configuration file (startup-config) in NVRAM.

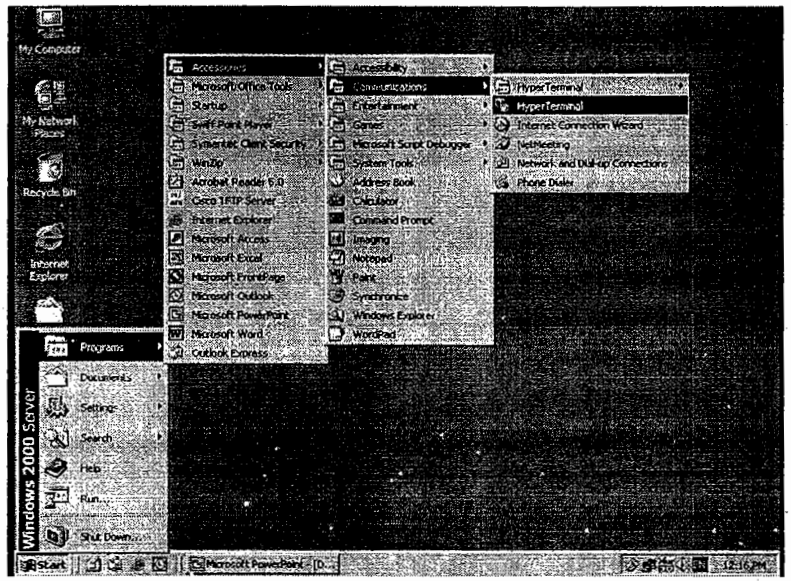
- This file contains the previously saved configuration commands and parameters, including interface addresses, routing information, passwords, other configuration parameters
- If no configuration file is located, the router prompts the user to enter setup mode to begin the configuration process.
- If a startup configuration file is found, a prompt containing a hostname will display. The router has successfully loaded the IOS and the configuration file.

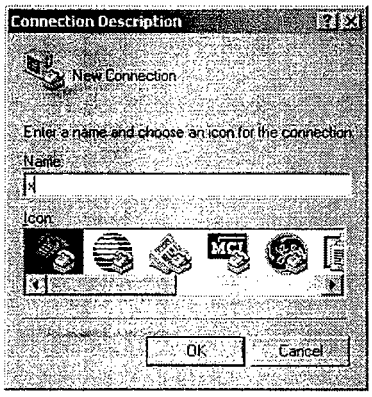
4.5 Modes of Routers

- User Mode
  - Only some basic monitoring
  - Limited to show commands, ping & trace
- Privileged Mode
  - Monitoring and some troubleshooting
  - All show commands, ping, trace, copy, erase
- Global Configuration Mode
  - To make any changes that affect the router like hostname, routing configurations.
  - All Configurations that affect the router globally
- Interface mode
  - Configurations done on the specific interface
- Rommon Mode
  - Reverting Password
- Setup mode
  - The router enters in to setup mode if the NVRAM is blank

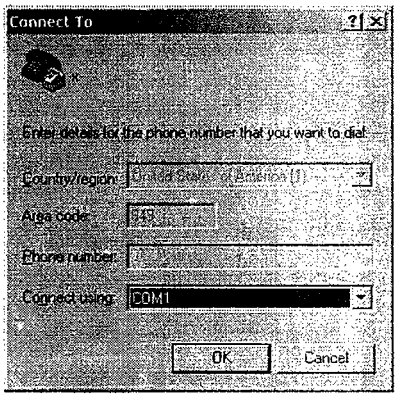
4.6 Accessing the Router

- In Windows
  - Start → Programs → Accessories → Communications → HyperTerminal → HyperTerminal
  - Give the Connection Name & Select Any Icon
  - Select Serial (Com) Port where Router is connected
  - In Port Settings → Click on Restore Defaults
- In Linux
  - # minicom –s (used instead of HyperTerminal in Windows)

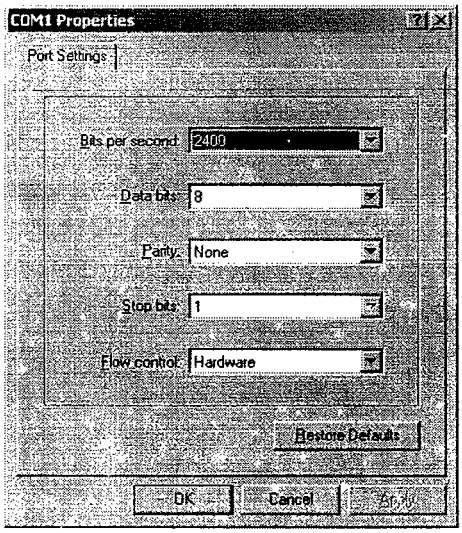




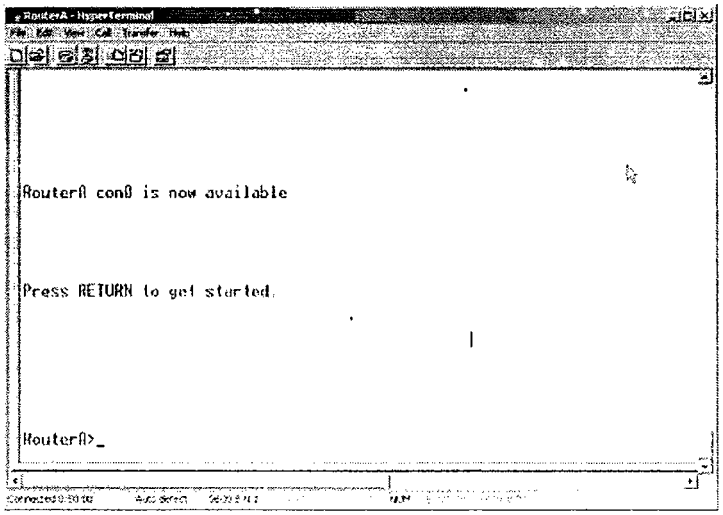
(1) Connection Description



(2) Connect To



(3) COM1 Properties



4.7 Basic Commands

- User mode

```
Router >
Router > enable
```

- Privilege mode

```
Router # show running-config
Router # show startup-config
Router # show flash
Router # show version
Router # show ip interface brief
```

- To enter global configuration mode

```
Router # configure terminal
```

- To change the hostname

```
Router (config) # hostname Netmetric
Netmetric (config) #
```

- Assigning an IP Address

```
Netmetric (config) # interface  <interface type>  <interface no>
Netmetric (config-if) # ip address  <ip address> <subnet mask>
Netmetric (config-if) # no shutdown
```

- Assigning Telnet password

```
Netmetric (config) # line vty 0 4
Netmetric (config-line) # password <password>
Netmetric (config-line) # login
Netmetric (config-line) # exit
Netmetric (config) # exit
```

- Assigning Console password

```
Netmetric (config) # line con 0
Netmetric (config-line) # password <password>
Netmetric (config-line) # login
Netmetric (config-line) # exit
Netmetric (config) # exit
```

- Assigning Auxillary password

```
Netmetric (config) # line aux 0
Netmetric (config-line) # password <password>
Netmetric (config-line) # login
Netmetric (config-line) # exit
Netmetric (config) # exit
```

- Assigning enable password
  - To save the password in encrypted form, use the below command

```
Netmetric (config) # enable secret <password>
```

  - To save the password in clear text, use the below command

```
Netmetric (config) # enable password <password>
```

- To encrypt all passwords

```
Netmetric (config) # service password-encryption
```

- Command to save the configuration (use any one of the 3 commands)

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

- To erase NVRAM configuration

```
Router # erase startup-config
```

4.8 Basic configurations and verifications

- POWER on the router and observe the booting Process (sample output shown below)

```
System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
Cisco 2621 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of
memory

Self-decompressing the image:
################################################################################
[OK]
              Restricted Rights Legend
Use, duplication, or disclosure by the Government is subject to
restrictions as set forth in subparagraph (c) of the Commercial Computer
Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer Software clause
at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706

Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE
(fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang

Cisco 2621 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of
memory
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)
         --- System Configuration Dialog ---
Continue with configuration dialog? [Yes/no]:
% Please answer 'yes' or 'no'.
Continue with configuration dialog? [Yes/no]: no
Press RETURN to get started!
Router>
```

```
Router> show flash
System flash directory:
File  Length    Name/status
  3   5571584   c2600-i-mz.122-28.bin
 [5827403 bytes used, 58188981 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)
```

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE
(fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang
Image text-base: 0x8000808C, data-base: 0x80A1FECC

ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
ROM: C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)

System returned to ROM by reload
System image file is "flash:c2600-i-mz.122-28.bin"

cisco 2621 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of
memory
.
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)
Configuration register is 0x2102
```

```
Router> show ip interface brief

Interface        IP-Address      OK? Method Status                Protocol
FastEthernet0/0  unassigned      YES unset  administratively down down
FastEthernet0/1  unassigned      YES unset  administratively down down
```

```
Router> ping 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/3)
```

```
Router> traceroute 1.1.1.1
Type escape sequence to abort.
Tracing the route to 1.1.1.1
```

- Assigning Telnet password

```
Netmetric> enable
Netmetric# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Netmetric (config)# line vty 0 4
Netmetric (config-line)# password ccna123
Netmetric (config-line)# login
Netmetric (config-line)# exit
```

```
Netmetric # show running-config
Building configuration...

Current configuration: 480 bytes
!
Version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Netmetric
!
!
enable password ccnp123
!
!
```

```
Netmetric # configure terminal
Netmetric (config)# enable secret ccie123
Netmetric (config)# exit
```

```
Netmetric # show running-config
Building configuration...

Current configuration: 480 bytes
!
Version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Netmetric
!
!
enable secret 5 $1$mERr$2ft7pDdq4XzRIT3Dy74gx/
enable password ccnp123
!
!
```

```
Netmetric# erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [Confirm]
[OK]
Erase of nvram: complete
```

```
Netmetric # reload
Proceed with reload? [confirm]

%SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.

System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
cisco 2621 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of
memory

Self decompressing the image :
############################################################################
[OK]
                    Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013
```

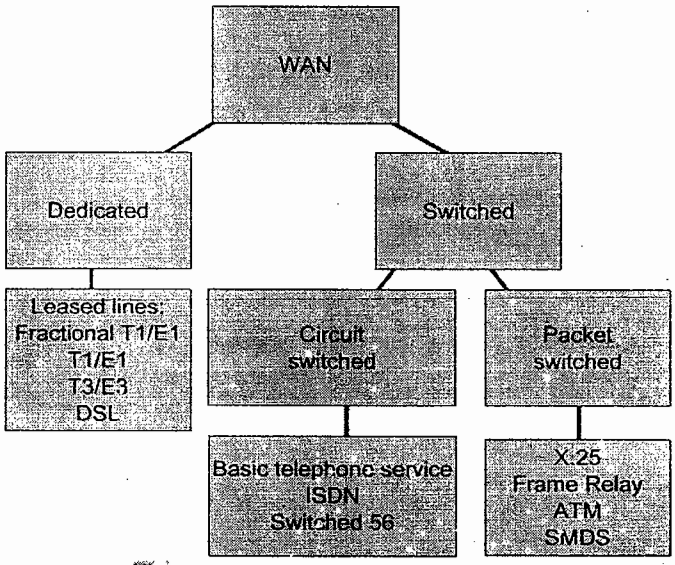
```
           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706

Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE
(fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang

cisco 2621 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of
memory
.
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)


         --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]:
```

NOTE:

- The router enters in to setup mode as the startup-config been erased

5. WAN Connections

- WAN connections are divided into three types
  - Dedicated line
  - Circuit switched
  - Packet switched



5.1 Dedicated Line

- Permanent connection for the destination
- Used for short or long distance
- Bandwidth is fixed
- Availability is 24/7
- Charges are fixed whether used or not.
- Uses analog circuits
- Always same path is used for destination
- Example is Leased Line

5.2 Circuit Switched

- It is also used for short and medium distances.
- Bandwidth is fixed
- Charges depend on usage of line
- Also called as line on demand.
- Usually used for backup line
- Connects at BRI port of router
- ISDN and PSTN are the examples

5.3 Packet Switched

- Used for medium or longer connections
- Bandwidth is shared
- Many virtual connections on one physical connection
- Example is Frame Relay

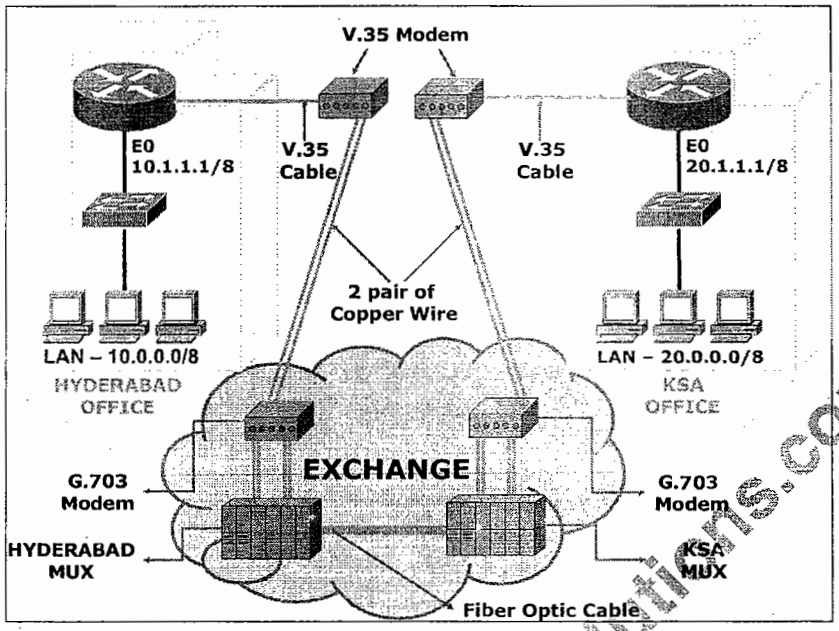
5.4 Leased Line

- A permanent/dedicated physical connection, which is used to connect two different geographical areas.
- Telecommunication companies like BSNL in India provide this connection.
- Leased line provides service 24/7 throughout the year, not like Dial-up Connection which can be connected when required. Leased Lines are obtained depending on the annual rental basis. Moreover, its rent depends on the distance between the sites.
- Leased Line is of three types
    - Short Leased Line
        - Used within the city and cost is also less for it.
    - Medium Leased Line
        - Used to connect sites in two different states like Hyderabad & Chennai.
    - Long Leased Line (iPLC)
        - Also called as IPLC (International Private Lease Circuit) and it is used to connect two different countries. It's the most expensive among all.
- Leased Line provides excellent quality of service with high speed of data transmission.
- It is a private physical connection assures complete security & privacy even with voice.
- Speed of the leased line varies from 64 kbps to 2 Mbps or more. Always Leased Line has fixed bandwidth.

NOTE:

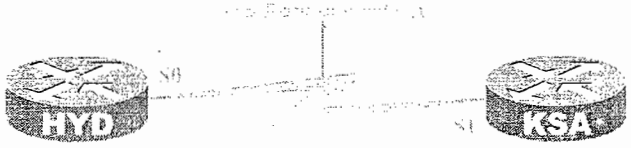
- *Once leased line is setup not only we can send data but also transmission of voice is also possible. In addition to this, both voice and date can be sent simultaneously.*

- Example of leased line

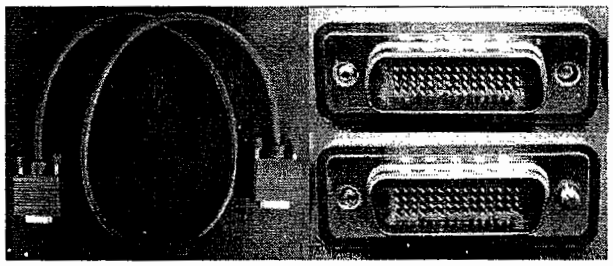


DCE	DTE
Data Communication Equipment	Data Termination Equipment
Generate clocking (i.e., speed)	Accept clocking (i.e., speed)
Example of DCE device(s) in Leased line setup: V.35 & G.703 Modem & Exchange (Modem & MUX)	Example of DTE device(s) in Leased line setup: Router
Example of DCE device in Dial up setup: Dialup Modem	Example of DTE device in Dial up setup: Computer

- Below are the hardware requirements
  - Leased Line Modem
  - V.35 connector & cable
  - G.703 connector & cable
- Leased line modem also called as CSU/DSU (Channel Service Unit and Data Service Unit). It acts as a DCE device, which generates clock rate.
- Lab Setup



- A Back-to-Back cable is used which emulates the copper wire, modems and MUX, the complete exchange setup.
- Without DCE & DTE device communication is not possible.



V.35 Back-to-Back cable

NOTE:

While practicing labs we use V.35 cable for back-to-back connection with router where as in real time V.35 cable terminates at the Lease Line Modem. That's the reason we have to use clock rate command in the labs where as it's not require in the real scenario. CSU/DSU is used to generate the speed.

- In different countries different codes are used for Leased Line with different speeds. In Europe its is identified as E whereas in UK its is identified with letter T
- In Europe, there are five types of lines distinguished according to their speed:
  - E0 (64Kbps),
  - E1 = 32 E0 lines (2Mbps),
  - E1 = 128 E0 lines (8Mbps),
  - E3 = 16 E1 lines (34Mbps),
  - E4 = 64 E1 lines (140Mbps)
- In the United States, the concept is as follows:
  - T1 (1.544 Mbps)
  - T2 = 4 T1 lines (6 Mbps),
  - T3 = 28 T1 lines (45 Mbps),
  - T4 = 168 T1 lines (275 Mbps)

Advantages	Disadvantages
Highly secure	Expensive
High bandwidth	Permanent physical connection
High speed connection	
Superior quality & reliable	

6. WAN Protocols

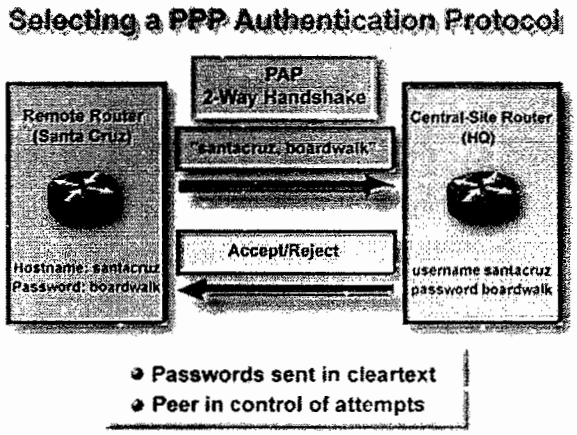
6.1 WAN Encapsulation Protocols

- Leased Lines uses two types of WAN encapsulation protocols:
  - High Data Link Protocol (HDLC)
  - Point to Point Protocol (PPP)

HDLC	PPP
Higher level data link Control protocol	Point to Point protocol
Cisco proprietary layer2 WAN protocol	Standard layer2 WAN protocol
Does not support authentication	Supports authentication
No support for error correction/compresssion	Supports error correction

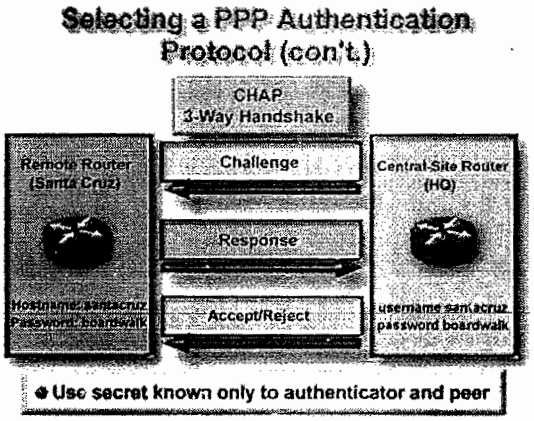
6.2 PPP Authentication Protocols

- PPP supports two authentication protocols
  - PAP (Password Authentication Protocol)
    - PAP provides a simple method for a remote node to establish its identity using a two-way handshake
    - PAP is done only upon initial link establishment
    - PAP is not a strong authentication protocol.
    - Passwords are sent across the link in clear text.



  - CHAP (Challenge Handshake Authentication Protocol)
    - After the PPP link establishment phase is complete, the local router sends a unique "challenge" message to the remote node.
    - The remote node responds with a value (MD5)

- The local router checks the response against its own calculation of the expected hash value.
- If the values match, the authentication is acknowledged. Otherwise, the connection is terminated immediately.



- Configuration of HDLC
- Default is HDLC even if you don't configure this command

```
Router (config)# interface serial 0/0
Router (config-if)# encapsulation hdlc
```

- Configuration of PPP

```
Router # configure terminal
Router (config)# interface serial 0/0
Router (config-if)# encapsulation ppp
```

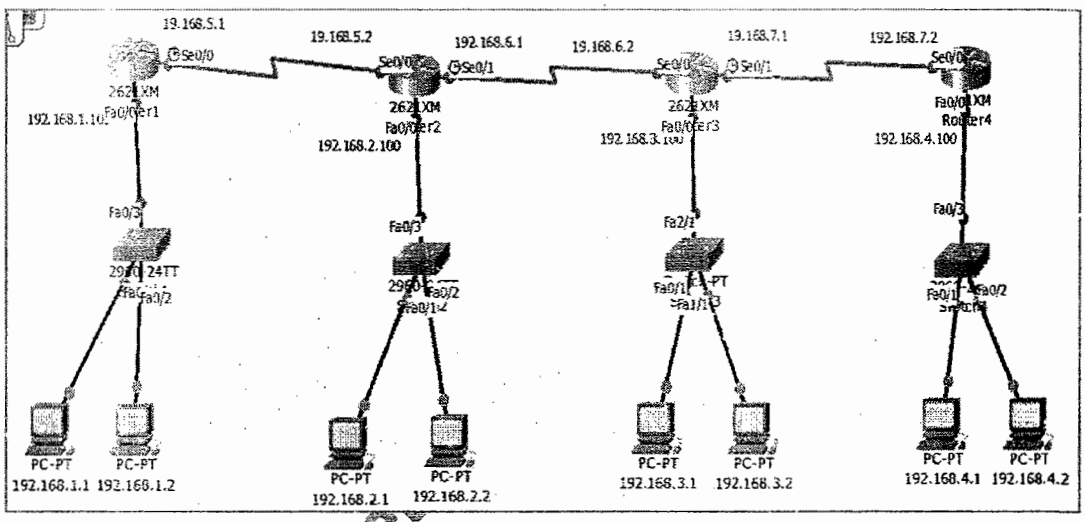
- To enable CHAP authentication

```
Router (config)# interface serial 0/0
Router (config-if)# encapsulation ppp
Router (config-if)# ppp authentication chap
```

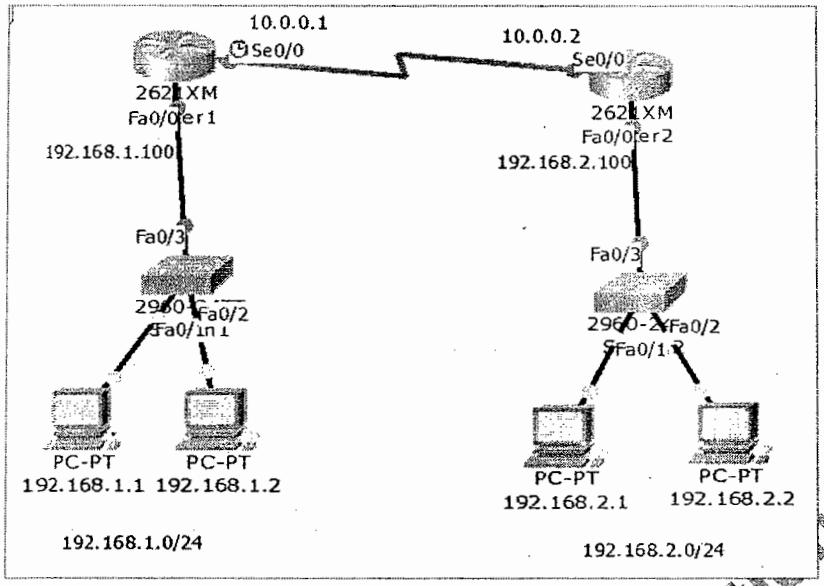
- To enable PAP authentication

```
Router (config)# interface serial 0/0
Router (config-if)# encapsulation ppp
Router (config-if)# ppp authentication pap
```

- Rules to assign the IP address to the router
  - All the LAN and WAN should be in different networks (or should not repeat the same network)
  - Router Ethernet IP and the LAN network assigned should be in the same network.
  - Both the interfaces of router facing each other should be in the same network.
  - All the interfaces of routers should be in the different network.
- The below diagram demonstrates the above rules



6.3 LAB – Basic IP Configuration



- On Router1

```
Router> enable
Router# configure terminal
Router (config)# hostname R-1
R-1 (config)# interface fastEthernet 0/0
R-1 (config-if)# ip address 192.168.1.100 255.255.255.0
R-1 (config-if)# no shutdown
R-1 (config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
R-1 (config-if)# exit
R-1 (config)# interface serial 0/0
R-1 (config-if)# ip address 10.0.0.1 255.0.0.0
R-1 (config-if)# no shutdown
R-1 (config-if)# clock rate 64000
```

NOTE:

- *Clock rate is only required in the lab scenario as we are using a **back to back cable** instead of the real exchange where the modems will be installed which will generate the clocking*
- *Here clock rate has to be generated manually using clock rate command*

```
R-1# show ip interface brief

Interface         IP-Address      OK? Method Status                Protocol
FastEthernet0/0   192.168.1.100   YES manual up                    up
FastEthernet0/1   unassigned      YES unset  administratively down down
Serial0/0         10.0.0.1        YES manual down                  down
Serial0/1         unassigned      YES unset  administratively down down
```

- On Router2

```
Router> enable
Router# configure terminal
Router (config)# hostname   R-2
R-2 (config)# interface fastEthernet 0/0
R-2 (config-if)# ip address 192.168.2.100 255.255.255.0
R-2 (config-if)# no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
R-2 (config-if)#exit
R-2 (config)# interface serial 0/0
R-2 (config-if)# ip address 10.0.0.2 255.0.0.0
R-2 (config-if)# no shutdown
R-2 (config-if)# clock rate 64000
```

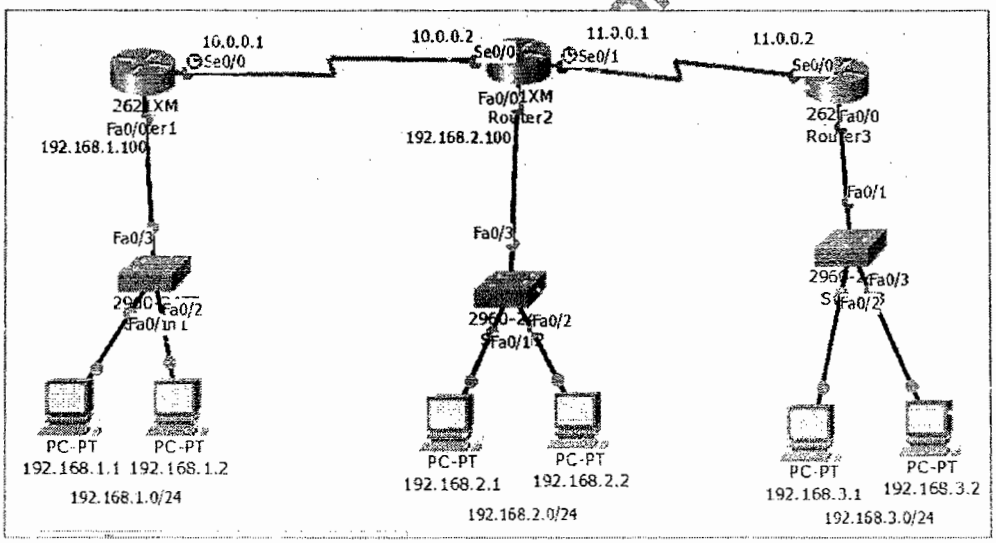
```
R-2# show ip interface brief

Interface         IP-Address      OK? Method Status                Protocol
FastEthernet0/0   192.168.2.100   YES manual up                    up
FastEthernet0/1   unassigned      YES unset  administratively down down
Serial0/0         10.0.0.2        YES manual up                    up
Serial0/1         unassigned      YES unset  administratively down down
```

```
R-1# show ip interface brief

Interface         IP-Address      OK? Method Status                Protocol
FastEthernet0/0   192.168.1.100   YES manual up                    up
FastEthernet0/1   unassigned      YES unset  administratively down down
Serial0/0         10.0.0.1        YES manual up                    up
Serial0/1         unassigned      YES unset  administratively down down
```

6.4 Troubleshooting Connectivity

- Serial is up, line protocol is up
  - Connectivity is fine.
- Serial is administratively down, line protocol is down
  - Local port is in shut down state
  - No Shutdown has to be given on the local router interface
- Serial is down, line protocol is down
  - Remote device turned off
  - Remote port is in shutdown state
  - Interface on the remote router has to be configured
  - Connectivity
- Serial is up, line protocol is down
  - Encapsulation mismatch
  - Clock rate command not given on serial interface (Applicable for the lab scenario)
  - If using PPP, then authentication mismatch

6.5 Basic Configuration with 3 Routers



- For Router1 and Router2 use the above configuration
- On Router3

```
Router> enable
Router# configure terminal
Router (config)# hostname R-3
R-3 (config)# interface fastEthernet 0/0
R-3 (config-if)# ip address 192.168.3.100 255.255.255.0
R-3 (config-if)# no shutdown
R-3 (config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
R-3 (config-if)# exit
R-3 (config)# interface serial 0/0
R-3 (config-if)# ip address 11.0.0.2 255.0.0.0
R-3 (config-if)# no shutdown
R-3 (config-if)# clock rate 64000
```

```
R-3# show ip interface brief

Interface        IP-Address      OK? Method Status                Protocol
FastEthernet0/0  192.168.3.100   YES manual up                    up
FastEthernet0/1  unassigned      YES unset administratively down down
Serial0/0        11.0.0.2        YES manual up                    up
Serial0/1        unassigned      YES unset  administratively down down
```

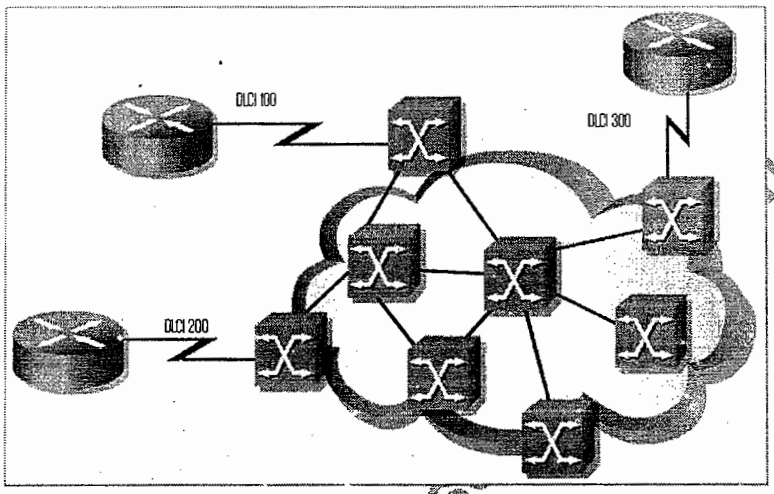
```
R-2# ping 10.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/12/44 ms
```

```
R-2# ping 11.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/20 ms
```

NOTE: *Once the interfaces are up you should be able to ping to the directly connected interfaces of the other routers*

7. Frame Relay

- Frame Relay is a connection oriented, standard NBMA layer 2 WAN protocol
- Connections in Frame Relay are provided by Virtual circuits.
- Virtual circuits are multiple logical connections on same physical connection



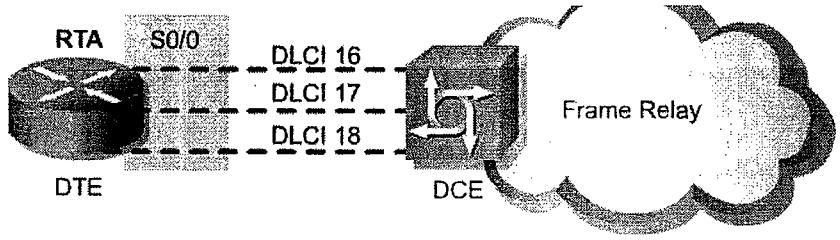
7.1 Frame Relay Virtual Connection Types

- PVC (permanent virtual connection)
  - Similar to the dedicated leased line.
  - Permanent connection is used.
  - When constant data has to be sent to a particular destination.
  - Always use the same path.
- SVC (switched virtual connection)
  - Virtual connection is dynamically built when data has to be sent and torn down after use.
  - It is similar to the circuit switched network like dial on demand.
  - Also called as semi-permanent virtual circuit.
  - For periodic intervals of data with small quantity

7.2 Frame Relay Encapsulations

- There are two types of Frame relay encapsulations
  - Cisco (default and Cisco proprietary)
  - IETF (when different vendor routers are used)

7.3 DLCI (Data Link Connection Identifier)



- Address of Virtual connections
- For every VC there is one DLCI number.
- Locally significant and provided by Frame Relay service provider.
- Inverse ARP (address resolution protocol) is used to map local DLCI to a remote IP.

7.4 LMI (Local Management Interface)

- LMI allows DTE (router) to send status enquiry messages (keep alive) to DCE (frame relay switch) to exchange status information about the virtual circuits devices for checking the connectivity.
- Frame relay LMI types
  - Cisco (Default)
  - ANSI
  - Q933A
- On Cisco router LMI is auto sense able no need to configure

7.5 Frame Relay Virtual Connection Status Types

- Active – Connection is up and operation between two DTE's exist
- Inactive – Connection is functioning between at least between DTE and DCE
- Deleted – The local DTE/DCE connection is not functioning

7.6 Frame Relay Network Connections

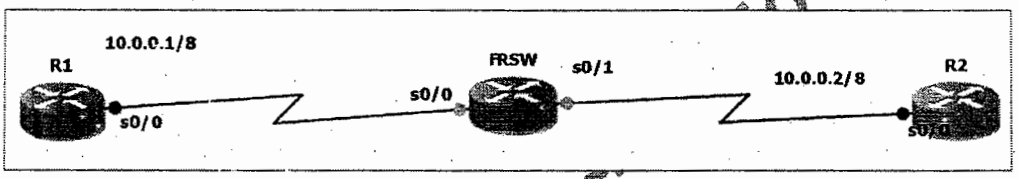
- Point to Point
- Point to Multipoint (NBMA)
- Congestion indicates traffic problem in the path when more packets are transmitted in one direction.
- Congestion notifications
  - FECN (forward explicit congestion notification)
    - Indicates congestion as frame goes from source to destination
    - Used this value inside frame relay frame header in forward direction
    - FCEN =0 indicates no congestion

- BECN (backward explicit congestion notification)
  - Used by the destination (and send to source) to indicate that there is congestion.
  - Used this value inside frame relay frame header in backward direction
  - BCEN =0 indicates no congestion

7.7 VC Advantages

- VC's overcome the scalability problem of leased line by providing the multiple logical circuits over the same physical connection
- Cheaper
- Best quality
- VC's are full duplex

7.8 LAB – Basic FR Implementation



R1
```
interface Serial0/0
no shutdown
ip address 10.0.0.1 255.0.0.0
encapsulation frame-relay
```

R2
```
interface Serial0/0
no shutdown
ip address 10.0.0.2 255.0.0.0
encapsulation frame-relay
```

FRSW
```
enable
configure terminal
frame-relay switching
```

(The above command is to make the router to act as FR SWITCH)

FRSW

```
interface serial0/0
no shutdown
encapsulation frame-relay
frame-relay intf-type dce
frame-relay lmi-type cisco
frame-relay route 100 interface serial0/1 200
!
!
int serial0/1
no shutdown
encapsulation frame-relay
frame-relay intf-type dce
frame-relay lmi-type cisco
frame-relay route 200 interface serial0/0 100
```

- Verification

```
R1#show frame-relay map
Serial0/0 (up): ip 10.0.0.2 dlci 100(0x64,0x1840), dynamic, broadcast,
CISCO, status defined, active
```

```
FRSW#show frame-relay route
Input Intf      Input Dlci      Output Intf     Output Dlci     Status
Serial0/0       100             Serial0/1       200             active
Serial0/1       200             Serial0/0       100             active
```

```
R1#ping 10.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
```

```
R1#sh frame-relay lmi
LMI Statistics for interface Serial0/0 (Frame Relay DTE) LMI TYPE = CISCO
  Invalid Unnumbered info 0              Invalid Prot Disc 0
  Invalid dummy Call Ref 0               Invalid Msg Type 0
  Invalid Status Message 0               Invalid Lock Shift 0
  Invalid Information ID 0               Invalid Report IE Len 0
  Invalid Report Request 0               Invalid Keep IE Len 0
  Num Status Enq. Sent 103               Num Status msgs Rcvd 32
  Num Update Status Rcvd 0               Num Status Timeouts 70
  Last Full Status Req 00:00:02          Last Full Status Rcvd
```

8. Routing

8.1 What is Routing?

- Forwarding of packets from one network to another network choosing the best path from the routing table.
- Routing makes possible for two or more different networks to communicate with each other.
- Routing table consist of only the best routes for every destinations.

8.2 Types of Routing?

- Static Routing
  - The Administrator configures it manually.
  - Mandatory need for the Destination Network ID
  - Used for Small organizations
  - Administrative distance for Static Route is 0 or 1
  - Advantages of static routing
    - There is no overhead on the router CPU
    - There is no bandwidth usage between routers
    - It adds security because the administrator can choose to allow routing access to certain networks only
  - Disadvantages of static routing
    - Used for small network. (It's not feasible in large networks)
    - Each and every network has to be manually configured
    - The administrator must really understand the internetwork and how each router is connected in order to configure routes correctly.
    - Any changes in the internetwork has to be updated in all routers
- Default Routing
  - Default route is used when destination is unknown (Internet)
  - Also can be used at end locations where there is only one exit path for any destination
  - Last preferred route in the routing table
  - Default routes help in reducing the size of your routing table.
  - If the routers do not found an entry for the destination network in a routing table, the router will forward the packet to its default route.
- Dynamic Routing
  - Advantages of dynamic over static
    - There is no need to know the destination networks.
    - Need to advertise the directly connected networks.

- Updates the topology changes dynamically.
- Administrative work is reduced
- Used for large organizations.
- Neighbor routers exchange routing information and build the routing table automatically.
- This is easier than using static or default routing

- Types of Dynamic Routing Protocols
  - Distance Vector Protocol
  - Link State Protocol
  - Hybrid Protocol (Advance Distance Vector Protocol)

Distance Vector Protocol	Link State Protocol	Hybrid Protocol
Works with Bellman Ford algorithm	Works with Dijkstra algorithm	Works with DUAL algorithm
Periodic updates	Incremental updates	Incremental updates
Classfull routing protocols	Classless routing protocol	Classless routing protocol
Full Routing tables are exchanged	Missing routes are exchanged	Missing routes are exchanged
Updates are through broadcast	Updates are through multicast	Updates are through multicast
E.g., RIPv1, RIPv2, IGRP	E.g., OSPF, IS-IS	E.g., EIGRP
-	Link state updates	Advance Distance Vector Protocol

- Classful Protocols
  - Classful routing protocol do not carry the subnet mask information along with updates
  - This means all devices in the network must use the same subnet mask
  - E.g., RIPv1, IGRP
- Classless Protocols
  - Classful routing protocol carry the subnet mask information along with updates
  - This is the reason they support sub networks & default networks
  - E.g., RIPv2, EIGRP, OSPF and IS-IS
- Administrative Distance
  - It is the trustworthiness of the information received by the router.
  - The Number is between 0 and 255

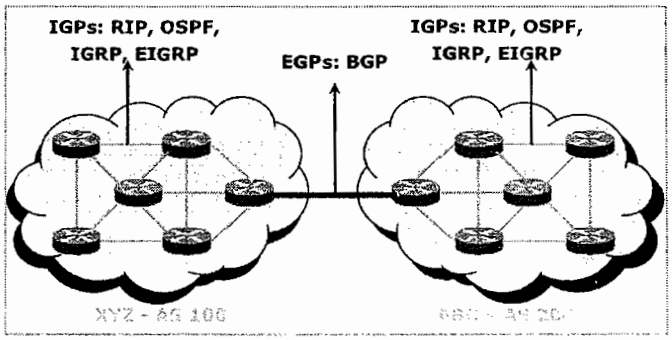
- Least value is more preferred.
- Default administrative distances are as follows:
  - Directly Connected = 0
  - Static Route = 1
  - IGRP = 100
  - OSPF = 110
  - RIP = 120
  - EIGRP = 90/170
  - IS-IS = 115

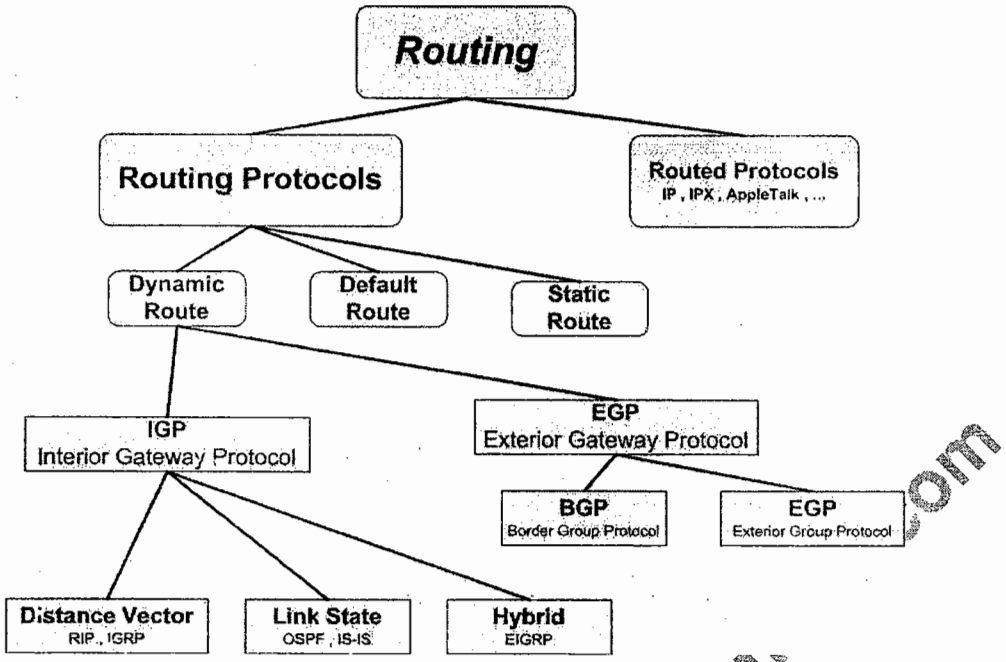
8.3 Autonomous System Number

- An Autonomous System is a collection of networks under a common administrative domain
- A unique number identifying the Routing domain of the routers.
- Ranges from 1- 65535
  - Public from 1 – 64512
  - Private from 64513 – 65535
- Private AS is used within the same service providers
- Public AS is used in between multiple service providers

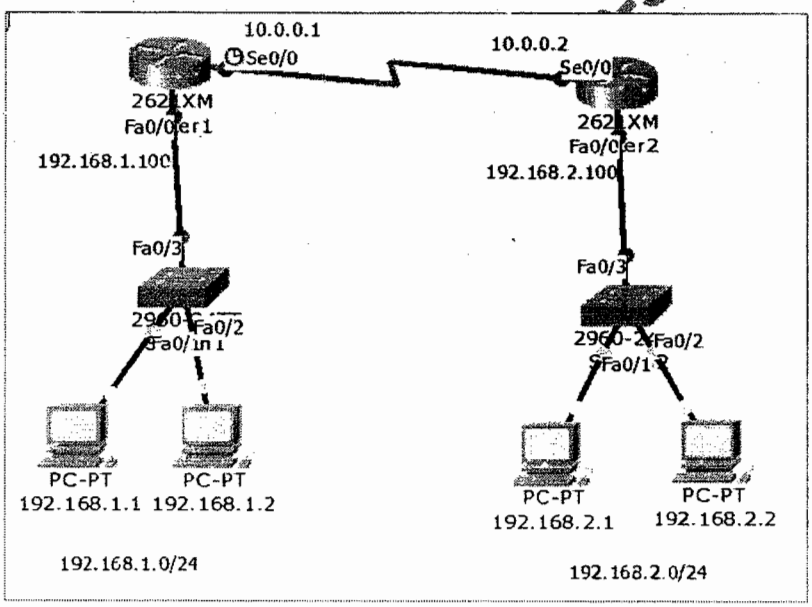
8.4 Routing Protocol Classification

IGP	EGP
Interior Gateway Protocol	Exterior Gateway Protocol
Routing protocols used within the same autonomous system number	Routing protocol used between different autonomous systems
All routers will be routing within the same Autonomous boundary	Routers in different AS need an EGP
E.g., RIP, IGRP, EIGRP, OSPF, IS-IS	E.g., BGP – Border Gateway Protocol





8.5 LAB – Static Routing



- Steps:
  - Pre-requirement for LAB (check previous labs)
  - Design the topology (connectivity)
  - Assign the IP address according to diagram
  - Make sure that interfaces used should be in UP & UP state
- What we do in this lab
  - Static routing
  - Verify routing table & reachability between LAN's using PING & TRACE

```
R-1# show ip route
Gateway of last resort is not set
C    10.0.0.0/8 is directly connected, Serial0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
```

```
R-2# show ip route
Gateway of last resort is not set
C    10.0.0.0/8 is directly connected, Serial0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

NOTE:

- *The above routing table displays only the networks which are directly connected*
- *By default router don't know about the networks which are not directly connected and that the reason there is no reachability between the two LAN's*
- *So to provide reachability we need to implement any of the routing*

```
PC> ipconfig
IP Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100
```

```
PC> ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.1.100: Destination host unreachable.
Reply from 192.168.1.100: Destination host unreachable.
Reply from 192.168.1.100: Destination host unreachable.
Reply from 192.168.1.100: Destination host unreachable.

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- From the above output we can see there is no communication between 192.168.1.1 and 192.168.2.1 and they are on different networks.
- To communicate we need to implement any of the routing (here we use static routing)

```
R-1 (config)# ip route 192.168.2.0 255.255.255.0 10.0.0.2
R-1 (config)# end
```

```
R-1# show ip route

Gateway of last resort is not set
C    10.0.0.0/8 is directly connected, Serial0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
S    192.168.2.0/24 [1/0] via 10.0.0.2
```

```
R-2 (config)# ip route 192.168.1.0 255.255.255.0 10.0.0.1
R-2 (config)# end
```

```
R-2# show ip route

Gateway of last resort is not set
C    10.0.0.0/8 is directly connected, Serial0/0
S    192.168.1.0/24 [1/0] via 10.0.0.1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

```
PC> ipconfig
IP Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100
```

```
PC> ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.1: bytes=32 time=20ms TTL=126
Reply from 192.168.2.1: bytes=32 time=21ms TTL=126
Reply from 192.168.2.1: bytes=32 time=21ms TTL=126
```

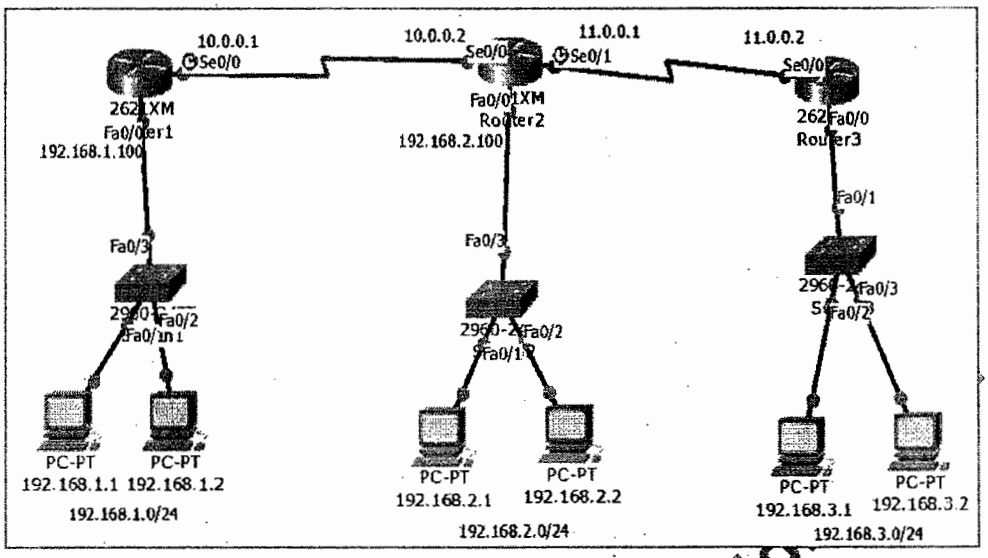
```
PC> ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.2: bytes=32 time=21ms TTL=126
Reply from 192.168.2.2: bytes=32 time=19ms TTL=126
Reply from 192.168.2.2: bytes=32 time=12ms TTL=126
```

```
PC> tracert 192.168.2.1

Tracing route to 192.168.2.1 over a maximum of 30 hops:
  1    44 ms     9 ms     10 ms     192.168.1.100
  2    13 ms     13 ms    12 ms     10.0.0.2
  3    17 ms     22 ms    20 ms     192.168.2.1
```

```
R-1# ping 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/10/31
```

```
R-2# ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/15/
```

8.6 LAB – Static Routing with 3 Routers



- Steps:
  - Pre-requirement for LAB (check previous labs)
  - Design the topology (connectivity)
  - Assign the IP address according to diagram
  - Make sure that interfaces used should be in UP & UP state
- What we do in this lab
  - Static routing
  - Verify routing table & reachability between LAN's using PING & TRACE

```
R-1# show ip route
Gateway of last resort is not set
C    10.0.0.0/8 is directly connected, Serial0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
```

```
R-2# show ip route
Gateway of last resort is not set
C    10.0.0.0/8 is directly connected, Serial0/0
C    11.0.0.0/8 is directly connected, Serial0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

```
R-3# show ip route
Gateway of last resort is not set
C    11.0.0.0/8 is directly connected, Serial0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
```

```
R-1 (config)# ip route 192.168.2.0 255.255.255.0 10.0.0.2
R-1 (config)# ip route 192.168.3.0 255.255.255.0 10.0.0.2
R-1 (config)# ip route 11.0.0.0 255.0.0.0 10.0.0.2
```

```
R-2 (config)# ip route 192.168.1.0 255.255.255.0 10.0.0.1
R-2 (config)# ip route 192.168.3.0 255.255.255.0 11.0.0.2
```

```
R-3 (config)# ip route 192.168.2.0 255.255.255.0 11.0.0.1
R-3 (config)# ip route 192.168.1.0 255.255.255.0 11.0.0.1
R-3 (config)# ip route 10.0.0.0 255.0.0.0 11.0.0.1
```

```
R-1# show ip route
Gateway of last resort is not set
C    10.0.0.0/8 is directly connected, Serial0/0
S    11.0.0.0/8 [1/0] via 10.0.0.2
C    192.168.1.0/24 is directly connected, FastEthernet0/0
S    192.168.2.0/24 [1/0] via 10.0.0.2
S    192.168.3.0/24 [1/0] via 10.0.0.2
```

```
R-2# show ip route
Gateway of last resort is not set
C    10.0.0.0/8 is directly connected, Serial0/0
C    11.0.0.0/8 is directly connected, Serial0/1
S    192.168.1.0/24 [1/0] via 10.0.0.1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
S    192.168.3.0/24 [1/0] via 11.0.0.2
```

```
R-3# show ip route
Gateway of last resort is not set
S    10.0.0.0/8 [1/0] via 11.0.0.1
C    11.0.0.0/8 is directly connected, Serial0/0
S    192.168.1.0/24 [1/0] via 11.0.0.1
S    192.168.2.0/24 [1/0] via 11.0.0.1
C    192.168.3.0/24 is directly connected, FastEthernet0/0
```

```
PC> ipconfig
IP Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100
```

```
PC> ping  192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.1: bytes=32 time=19ms TTL=126
Reply from 192.168.2.1: bytes=32 time=20ms TTL=126
Reply from 192.168.2.1: bytes=32 time=14ms TTL=126
```

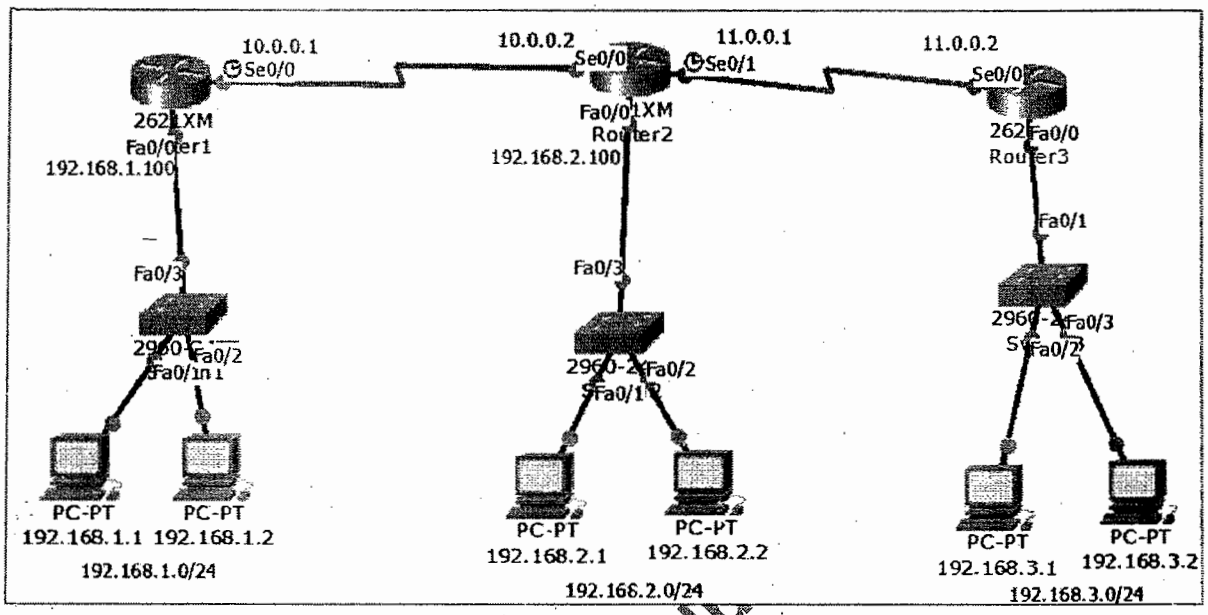
```
PC> ping  192.168.3.1
Pinging 192.168.3.1 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.1: bytes=32 time=27ms TTL=125
Reply from 192.168.3.1: bytes=32 time=22ms TTL=125
Reply from 192.168.3.1: bytes=32 time=25ms TTL=125
```

```
PC> tracert 192.168.3.1
Tracing route to 192.168.3.1 over a maximum of 30 hops:

  1    8 ms     8 ms     8 ms     192.168.1.100
  2   32 ms     9 ms     8 ms     10.0.0.2
  3   12 ms     6 ms    12 ms     11.0.0.2
  4   24 ms    27 ms    25 ms     192.168.3.1
Trace complete.
```

```
R-1# ping  192.168.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/16/31 ms.
```

```
R-3# ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/15/18
```

8.7 LAB – Default Routing



- STEPS: Pre-requirement for LAB (Check Previous Labs)
  - Design the topology (Connectivity)
  - Assign the IP address according to diagram
  - Make sure that interfaces used should be in UP UP state
- What we do in this lab
  - Default route used on R1 and R3, static routing on R2
  - Verify Routing table and reachability between the LAN's (using PING & TRACE commands)


```
R-1# show ip route
Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, Serial0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
```

```
R-2# show ip route
Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, Serial0/0
C    11.0.0.0/8 is directly connected, Serial0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

```
R-3# show ip route
Gateway of last resort is not set

C    11.0.0.0/8 is directly connected, Serial0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
```

```
R-1(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.2
```

```
R-2(config)# ip route 192.168.1.0 255.255.255.0 10.0.0.1
R-2(config)# ip route 192.168.3.0 255.255.255.0 11.0.0.2
```

```
R-3(config)# ip route 0.0.0.0 0.0.0.0 11.0.0.1
```

```
R-1# show ip route
Gateway of last resort is 10.0.0.2 to network 0.0.0.0
C    10.0.0.0/8 is directly connected, Serial0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 10.0.0.2
```

```
R-2# show ip route
Gateway of last resort is not set
C    10.0.0.0/8 is directly connected, Serial0/0
C    11.0.0.0/8 is directly connected, Serial0/1
S    192.168.1.0/24 [1/0] via 10.0.0.1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
S    192.168.3.0/24 [1/0] via 11.0.0.2
```

```
R-3# show ip route
Gateway of last resort is 11.0.0.1 to network 0.0.0.0
C    11.0.0.0/8 is directly connected, Serial0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 11.0.0.1
```

```
PC> ipconfig
IP Address.....................: 192.168.1.1
Subnet Mask....................: 255.255.255.0
Default Gateway................: 192.168.1.100
```

```
PC> ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.2.1: bytes=32 time=19ms TTL=126
Reply from 192.168.2.1: bytes=32 time=20ms TTL=126
Reply from 192.168.2.1: bytes=32 time=14ms TTL=126
```

```
PC> ping 192.168.3.1
Pinging 192.168.3.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.3.1: bytes=32 time=27ms TTL=125
Reply from 192.168.3.1: bytes=32 time=22ms TTL=125
Reply from 192.168.3.1: bytes=32 time=25ms TTL=125
```

```
PC> tracert 192.168.3.1
Tracing route to 192.168.3.1 over a maximum of 30 hops:
  1    8 ms     8 ms     9 ms     192.168.1.100
  2   12 ms     9 ms     6 ms     10.0.0.2
  3   17 ms     6 ms     13 ms    11.0.0.2
  4   14 ms    27 ms     15 ms    192.168.3.1
Trace complete.
```

```
R-1# ping 192.168.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/16/39 ms
```

```
R-1# ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/15/19 ms
```

9. RIP v1 (Routing Information Protocol)

9.1 What is RIP?

- Open Standard Protocol
- Classful routing protocol
- Updates are broadcasted via 255.255.255.255
- Administrative distance is 120
- Metric: Hop count
- Max Hop counts: 15 and Max routers: 16
- Load Balancing of 4 equal paths
- Used for small organizations
- Periodic updates and Exchange entire routing table for every 30 seconds

9.2 RIP Timers

- Update timer: 30 sec
  - Time between consecutive updates
- Invalid timer: 180 sec
  - Time a router waits to hear updates
  - The route is marked unreachable if there is no update during this interval.
- Flush timer: 240 sec
  - Time before the invalid route is removed from the routing table
- Hold down timer 180sec
  - Stabilizes routing information and helps preventing routing loops during periods when the topology is converging on new information.
  - Once a route is marked as unreachable, it must stay in hold-down long enough for all routers in the topology to learn about the unreachable network
- Convergence time is the time taken by the router to use alternate route if the best route is down.

9.3 About RIP Version 2

- Classless routing protocol
- Supports VLSM
- Supports authentication
- Uses multicast address 224.0.0.9

9.4 Advantages of RIP

- Easy to configure
- No design constraints like OSPF protocol
- No complexity
- Less overhead

9.5 Disadvantages of RIP

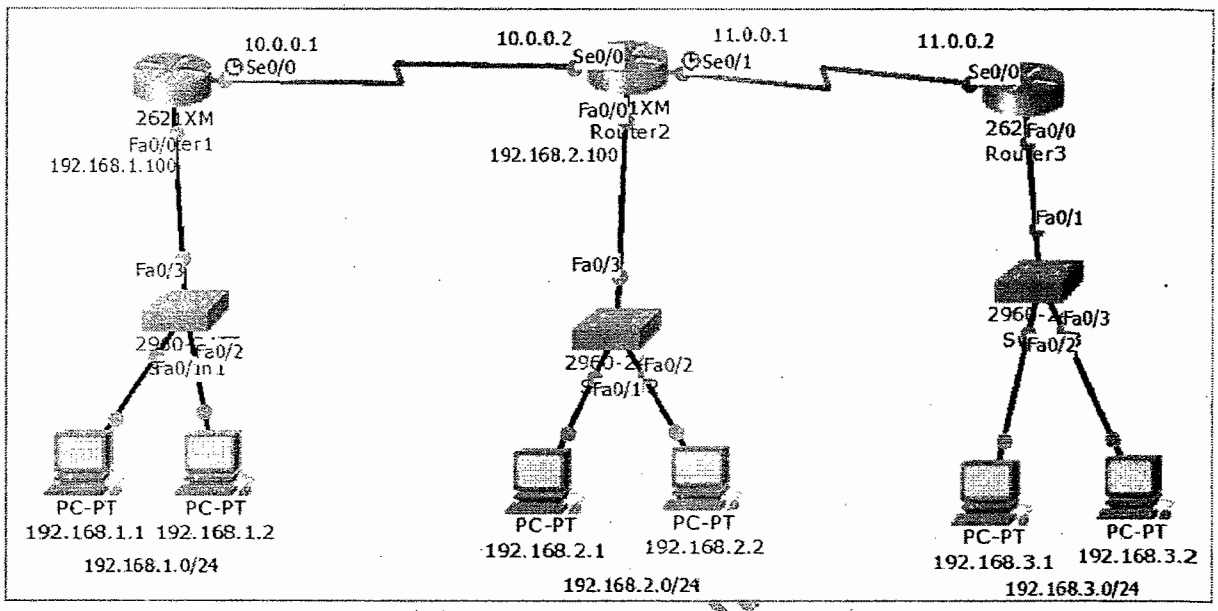
- Bandwidth utilization is very high as broadcast for every 30 second
- Works only on hop count (not consider the Bandwidth)
- Not scalable as hop count is only 15
- Slow convergence

9.6 Configuring RIP v1 and v2

```
Router(config)# router rip
Router(config-router)# network <Network ID>
```

```
Router(config)# router rip
Router(config-router)# network <Network ID>
Router(config-router)# version 2
```

9.7 LAB – Dynamic Routing using RIP v2



- STEPS: Pre-requirement for LAB (check previous labs)
  - Design the topology (connectivity)
  - Assign the IP address according to diagram
  - Ensure that interfaces used should be in UP UP state
- What we do in this lab
  - Dynamic routing using RIPv2
  - Verify Routing table and reachability between the LAN's (Using PING & TRACE commands)


```
R-1# show ip route
Gateway of last resort is not set
C    10.0.0.0/8 is directly connected, Serial0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
```

```
R-2# show ip route
Gateway of last resort is not set
C    10.0.0.0/8 is directly connected, Serial0/0
C    11.0.0.0/8 is directly connected, Serial0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

```
R-3# show ip route
Gateway of last resort is not set
C    11.0.0.0/8 is directly connected, Serial0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
```

```
R-1(config)#router rip
R-1(config-router)#version 2
R-1(config-router)#network 192.168.1.0
R-1(config-router)#network 10.0.0.0
R-1(config-router)#end
```

```
R-2(config)#router rip
R-2(config-router)#version 2
R-2(config-router)#network 192.168.2.0
R-2(config-router)#network 10.0.0.0
R-2(config-router)#network 11.0.0.0
R-2(config-router)#end
```

```
R-3(config)#router rip
R-3(config-router)#version 2
R-3(config-router)#network 192.168.3.0
R-3(config-router)#network 11.0.0.0
R-3(config-router)#end
```

```
R-1# show ip route
Gateway of last resort is not set
C    10.0.0.0/8 is directly connected, Serial0/0
R    11.0.0.0/8 [120/1] via 10.0.0.2, 00:00:03, Serial0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
R    192.168.2.0/24 [120/1] via 10.0.0.2, 00:00:03, Serial0/0
R    192.168.3.0/24 [120/2] via 10.0.0.2, 00:00:03, Serial0/0
```

```
R-2# show ip route
Gateway of last resort is not set
C    10.0.0.0/8 is directly connected, Serial0/0
C    11.0.0.0/8 is directly connected, Serial0/1
R    192.168.1.0/24 [120/1] via 10.0.0.1, 00:00:08, Serial0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
R    192.168.3.0/24 [120/1] via 11.0.0.2, 00:00:16, Serial0/1
```

```
R-3# show ip route
Gateway of last resort is not set
R    10.0.0.0/8 [120/1] via 11.0.0.1, 00:00:26, Serial0/0
C    11.0.0.0/8 is directly connected, Serial0/0
R    192.168.1.0/24 [120/2] via 11.0.0.1, 00:00:26, Serial0/0
R    192.168.2.0/24 [120/1] via 11.0.0.1, 00:00:26, Serial0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
```

```
R-1#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 8 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface              Send  Recv  Triggered RIP  Key-chain
  FastEthernet0/0        2     2
  Serial0/0              2     2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
      10.0.0.0
      192.168.1.0
Passive Interface(s):
Routing Information Sources:
      Gateway         Distance      Last Update
      10.0.0.2              120      00:00:02
Distance: (default is 120)
```

```
R-1# show ip route rip
R    11.0.0.0/8 [120/1] via 10.0.0.2, 00:00:24, Serial0/0
R    192.168.2.0/24 [120/1] via 10.0.0.2, 00:00:24, Serial0/0
R    192.168.3.0/24 [120/2] via 10.0.0.2, 00:00:24, Serial0/0
```

```
PC> ipconfig
IP Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100
```

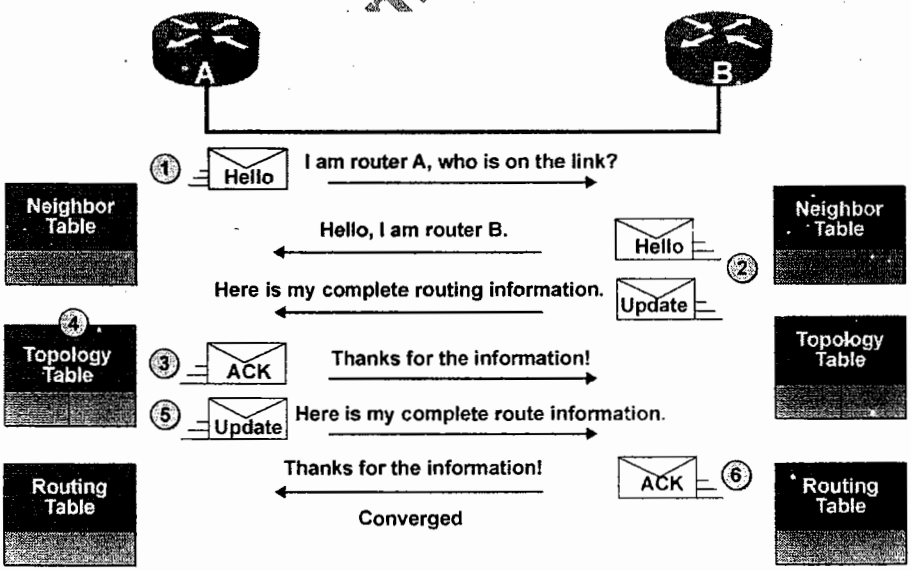
```
PC> ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.2.1: bytes=32 time=19ms TTL=126
Reply from 192.168.2.1: bytes=32 time=20ms TTL=126
Reply from 192.168.2.1: bytes=32 time=14ms TTL=126
```

```
PC>ping 192.168.3.1
Pinging 192.168.3.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.3.1: bytes=32 time=27ms TTL=125
Reply from 192.168.3.1: bytes=32 time=22ms TTL=125
Reply from 192.168.3.1: bytes=32 time=25ms TTL=125
```

10. EIGRP (Enhanced Interior Gateway Routing Protocol)

10.1 EIGRP Overview

- Cisco calls the EIGRP
  - A distance-vector routing protocol (or)
  - Sometimes an Advanced distance-vector (or)
  - Even a hybrid routing protocol
- It is a Cisco proprietary protocol
- Classless routing protocol
- Includes all features of IGRP
- Metric (32 bit): Composite Metric (BW + Delay + load + MTU + reliability)
- Administrative distance is 90
- Updates are through Multicast (224.0.0.10)
- Max Hop count is 255 (100 by default)
- Supports IP, IPX and Apple Talk protocols (Obviously we won't use IPX and AppleTalk, but EIGRP does support them.)
- Hello packets are sent every 5 seconds (dead interval 15 sec)
- Convergence rate is fast
- It uses DUAL (diffusion update algorithm)
- Summarization can be done on every router
- Supports equal and unequal cost load balancing



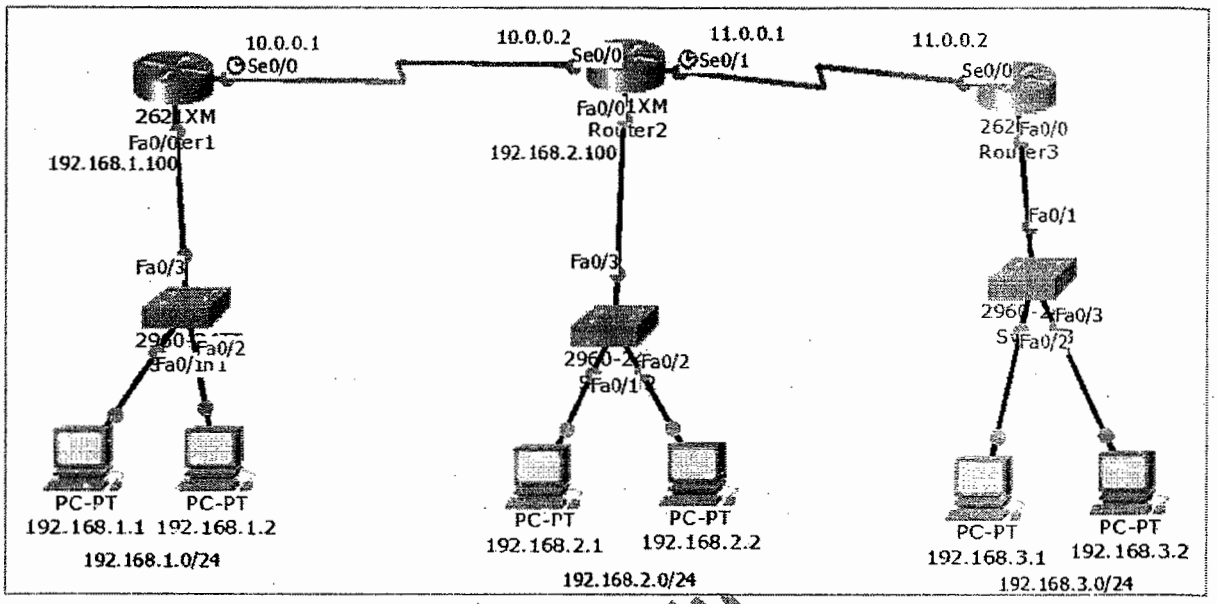
- EIGRP maintains three tables
  - Neighbor table
    - Contains list of directly connected routers
    - When a newly discovered neighbor is learned, the address and interface of the neighbor are recorded, and this information is held in the neighbor table, stored in RAM.
    - `# show ip eigrp neighbor`
  - Topology table
    - List of all the best routes learned from each neighbor
    - `# Show ip eigrp topology`
  - Routing table
    - The best route to the destination
    - `# show ip route`
- The neighbor and topology tables are stored in RAM and maintained through the use of Hello and update packets. Yes, the routing table is also stored in RAM, but that information is gathered only from the topology table.
- Successor
  - Successor is the best route to a remote destination network.
  - A successor route is used by EIGRP to forward traffic to a destination and is stored in the routing table.
- Feasible successor
  - A feasible successor is a second best route to a remote destination network and it is considered a backup route
- EIGRP uses Diffusing Update Algorithm (DUAL) for selecting and maintaining the best path to each remote network. This algorithm allows for the following:
  - Backup route determination if one is available
  - Support of VLSMs
  - Dynamic route recoveries
  - Queries for an alternate route if no route can be found
- EIGRP works only on Cisco devices and it is a disadvantage
- Configuring EIGRP
  - `Router(config)# router eigrp <AS NO>`
  - `Router(config-router)# network <Network ID>`

NOTE:

- *EIGRP uses autonomous system numbers to identify the collection of routers that share route information. Only routers that have the same autonomous system numbers share routes.*
- *AS no should be same on all routers to become neighbors and exchange the routes.*
- *EIGRP routers that belong to different autonomous systems (ASes) don't automatically share routing information and they don't become neighbors.*

- **Maximum Paths and Hop Count**
  - By default, EIGRP can provide equal-cost load balancing of up to four links (actually, all routing protocols do this).
  - However, you can have EIGRP actually load-balance across up to six links (equal or unequal) by using the following command:
    - `R-1(config)# router eigrp 10`
    - `R-1(config-router)# maximum-paths ?`
      `<1-6> Number of paths`
- EIGRP has a maximum hop count of 100, but it can be set up to 255.
  - `R-1(config)# router eigrp 10`
  - `R-1(config-router)# metric maximum-hops ?`
    `<1-255> Hop count`
- `#show ip route` – shows the entire routing table
- `#show ip route eigrp` – shows only EIGRP entries in the routing table
- `#show ip eigrp neighbors` – shows all EIGRP neighbors
- `#show ip eigrp topology` – shows entries in the EIGRP topology table

10.2 Dynamic Routing using EIGRP



- STEPS: Pre-requirement for LAB (check previous labs)
  - Design the topology (connectivity)
  - Assign the IP address according to diagram
  - Make sure that interfaces used should be in UP UP state
- What we do in this lab?
  - Dynamic routing using EIGRP
  - Verify Routing table and reachability between the LAN's (using PING and TRACE commands)


```
R-1# show ip route
Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, Serial0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
```

```
R-2# show ip route
Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, Serial0/0
C    11.0.0.0/8 is directly connected, Serial0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

```
R-3# show ip route
Gateway of last resort is not set

C    11.0.0.0/8 is directly connected, Serial0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
```

```
R-1(config)# router eigrp 100
R-1(config-router)# network 192.168.1.0
R-1(config-router)# network 10.0.0.0
```

```
R-2(config)# router eigrp 100
R-2(config-router)# network 192.168.2.0
R-2(config-router)# network 11.0.0.0
R-2(config-router)# network 10.0.0.0
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.0.0.1 (Serial0/0) is up: new
adjacency
```

```
R-3(config)# router eigrp 100
R-3(config-router)# network 192.168.3.0
R-3(config-router)# network 11.0.0.0
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 11.0.0.1 (Serial0/0) is up: new
adjacency
```

```
R-2# show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address         Interface      Hold Uptime    SRTT   RTO   Q   Seq
                                   (sec)          (ms)       Cnt Num
0   10.0.0.1        Se0/0          10   00:03:44  40     1000  0   6
1   11.0.0.2        Se0/1          12   00:01:10  40     1000  0   7
```

```
R-1# show ip route
Gateway of last resort is not set
C    10.0.0.0/8 is directly connected, Serial0/0
D    11.0.0.0/8 [90/2681856] via 10.0.0.2, 00:05:45, Serial0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
D    192.168.2.0/24 [90/2172416] via 10.0.0.2, 00:05:48, Serial0/0
D    192.168.3.0/24 [90/2684416] via 10.0.0.2, 00:02:49, Serial0/0
```

```
R-1# show ip route eigrp
D    11.0.0.0/8 [90/2681856] via 10.0.0.2, 00:06:05, Serial0/0
D    192.168.2.0/24 [90/2172416] via 10.0.0.2, 00:06:08, Serial0/0
D    192.168.3.0/24 [90/2684416] via 10.0.0.2, 00:03:09, Serial0/0
```

```
R-2# show ip route eigrp
D    192.168.1.0/24 [90/2172416] via 10.0.0.1, 00:07:26, Serial0/0
D    192.168.3.0/24 [90/2172416] via 11.0.0.2, 00:04:52, Serial0/1
```

```
R-3# show ip route eigrp
D    10.0.0.0/8 [90/2681856] via 11.0.0.1, 00:04:32, Serial0/0
D    192.168.1.0/24 [90/2684416] via 11.0.0.1, 00:04:32, Serial0/0
D    192.168.2.0/24 [90/2172416] via 11.0.0.1, 00:04:32, Serial0/0
```

```
R-1# show ip protocols
Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
Redistributing: eigrp 100
  Automatic network summarization is in effect
  Automatic address summarization:
  Maximum path: 4
  Routing for Networks:
     192.168.1.0
     10.0.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.0.0.2        90            18606786
  Distance: internal 90 external 170
```

```
R-1# show ip eigrp topology
IP-EIGRP Topology Table for AS 100

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.1.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 10.0.0.0/8, 1 successors, FD is 2169856
         via Connected, Serial0/0
P 192.168.2.0/24, 1 successors, FD is 2172416
         via 10.0.0.2 (2172416/28160), Serial0/0
P 11.0.0.0/8, 1 successors, FD is 2681856
         via 10.0.0.2 (2681856/2169856), Serial0/0
P 192.168.3.0/24, 1 successors, FD is 2684416
         via 10.0.0.2 (2684416/2172416), Serial0/0
```

```
PC> ipconfig
IP Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100
```

```
PC> ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.2.1: bytes=32 time=10ms TTL=126
Reply from 192.168.2.1: bytes=32 time=10ms TTL=126
Reply from 192.168.2.1: bytes=32 time=14ms TTL=126
```

```
PC> ping 192.168.3.1
Pinging 192.168.3.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.3.1: bytes=32 time=27ms TTL=125
Reply from 192.168.3.1: bytes=32 time=22ms TTL=125
Reply from 192.168.3.1: bytes=32 time=25ms TTL=125
```

```
PC> tracert 192.168.3.1
Tracing route to 192.168.3.1 over a maximum of 30 hops:
  1    5 ms      8 ms      8 ms      192.168.1.100
  2    12 ms     9 ms      8 ms      10.0.0.2
  3    17 ms     6 ms      12 ms     11.0.0.2
  4    24 ms     27 ms     25 ms     192.168.3.1
Trace complete.
```

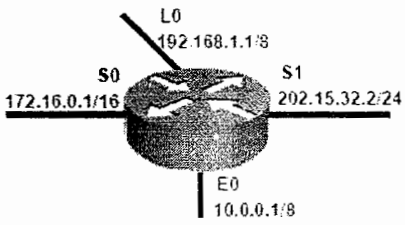
```
R-1# ping  192.168.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/16/31 ms
```

```
R-3# ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/15/18 ms
```

11. OSPF (Open Shortest Path First)

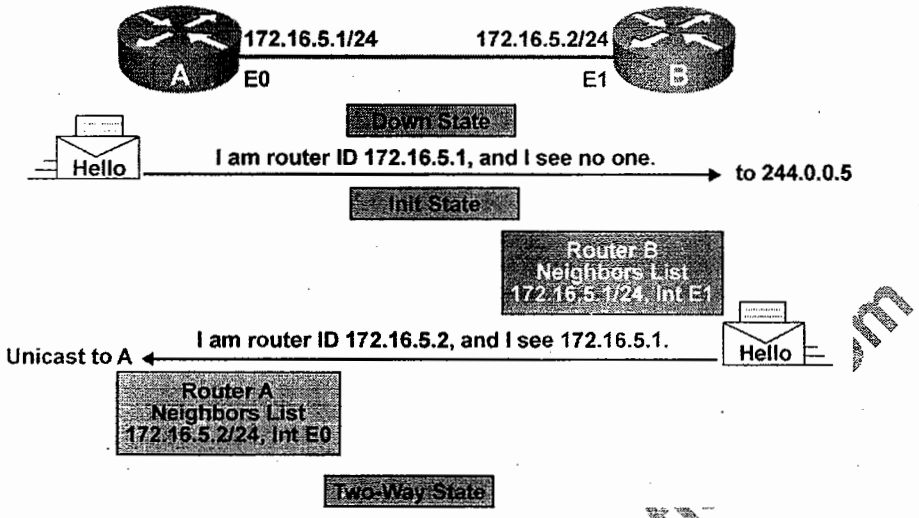
11.1 OSPF Overview

- OSPF stand for Open Shortest path first
- OSPF is an open standard routing protocol that's been implemented by a wide variety of network vendors, including Cisco
- It's a link state protocol
- OSPF works by using the Dijkstra algorithm.
- First a shortest path tree is constructed and then the routing table is populated with the resulting best paths.
- Unlimited hop count
- Metric is cost (cost=10 ^8/B.W.)
- Administrative distance is 110
- It is a classless routing protocol
- It supports VLSM and CIDR
- It supports only equal cost load balancing
- Introduces the concept of Area's to ease management and control traffic
- Provides hierarchical network design with multiple different areas
- Must have one area called as area 0
- All the areas must connect to area 0
- Scales better than Distance Vector Routing protocols.
- Supports authentication
- Updates are sent through multicast address 224.0.0.5
- Faster convergence.
- Sends Hello packet every 10 seconds
- Trigger/Incremental updates
- Router's send only changes in updates and not the entire routing tables in periodic updates
- Router ID
    - The highest IP address of the active physical interface of the router is Router ID.
    - If logical interface is configured, the highest IP address of the logical interface is Router ID

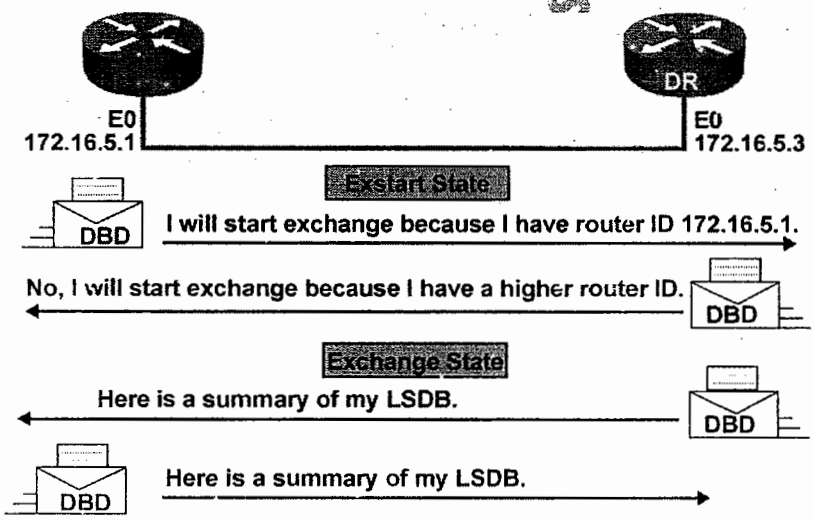


11.2 OSPF – The seven stage process

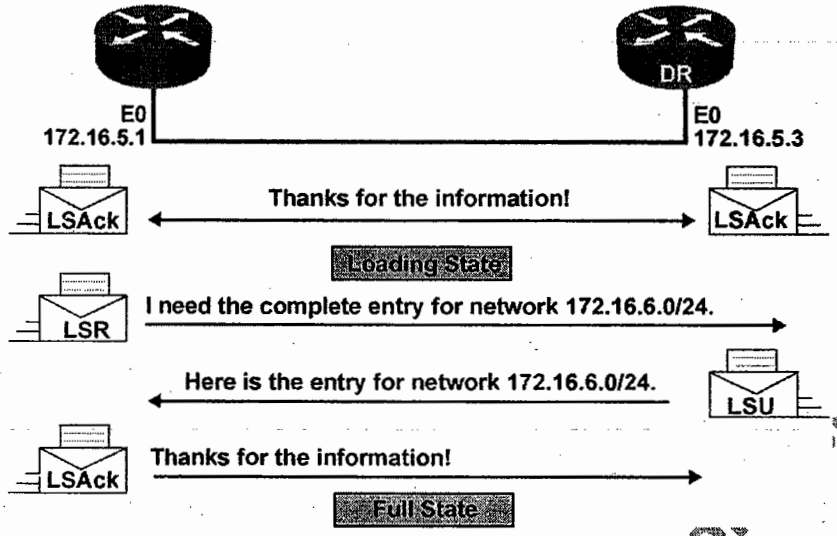
- Establishing Bidirectional Communication



- Discovering the Network Routes



- Adding the link state entries



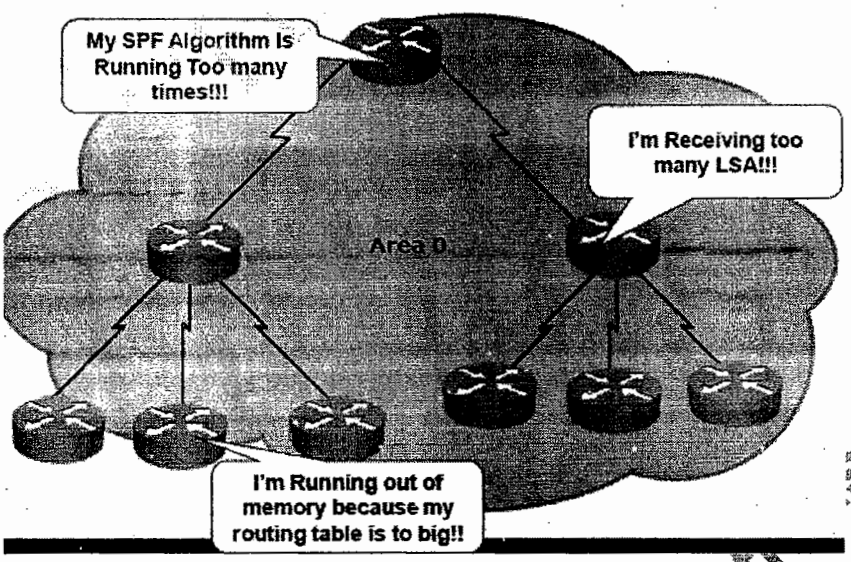
11.3 OSPF tables

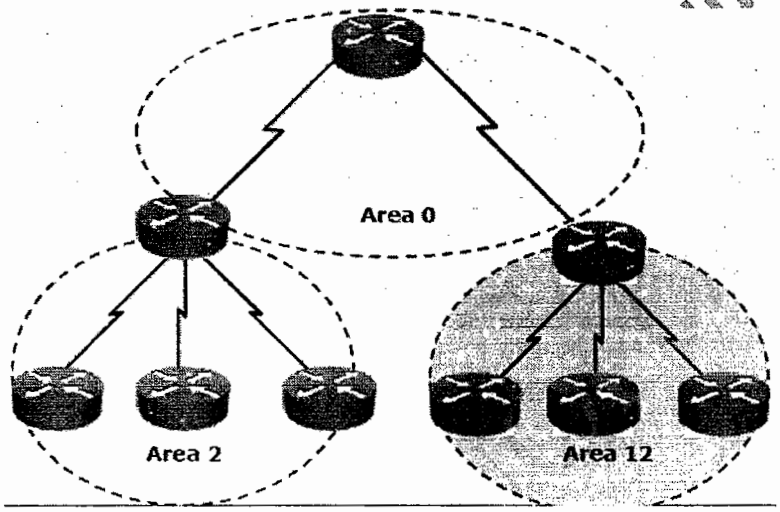
- Neighbor Table
  - Also known as the adjacency database
  - Contains list of directly connected routers (neighbors)
  - `# Show ip ospf neighbor`
- Database Table
  - Typically referred to as LSDB (link state database)
  - Contains information about all the possible routes to the networks with in the area
  - `# show ip ospf database`
- Routing Table
  - Contains list of best paths to each destination
  - `# show ip route`

11.4 Link-State Data Structure: Network Hierarchy

- Link-state routing can have hierarchical network
- This two-level hierarchy consists of the following:
  - Transit area (backbone or area 0)
  - Regular areas (non-backbone areas)

11.5 Issues of maintaing a large OSPF network





- OSPF is supposed to be designed in a hierarchical fashion, which basically means that you can separate the larger internetwork into smaller internetworks called areas.
- The following are reasons for creating OSPF in a hierarchical design:
  - To decrease routing overhead
  - To speed up convergence
  - To confine network instability to single areas of the network
- This does not make configuring OSPF easier, but more elaborate and difficult.

11.6 OSPF Networking Hierarchy

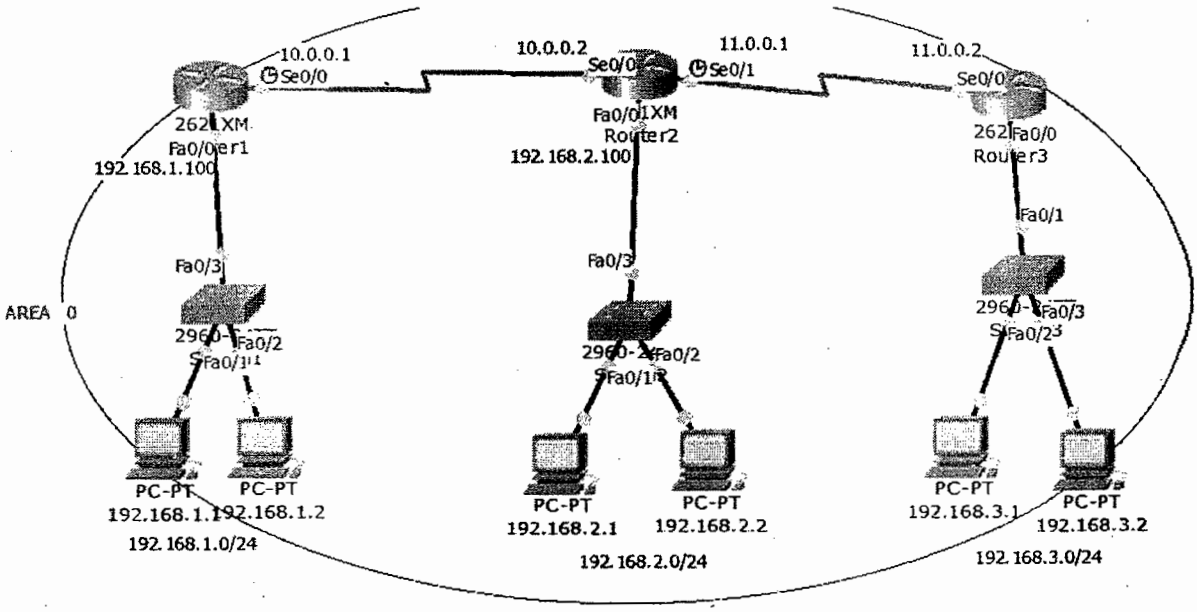
- **OSPF** is a hierarchical routing protocol. It enables better administration and smaller routing tables due to segmentation of entire network into smaller areas. OSPF consists of a backbone (Area 0) network that links all other smaller areas within the hierarchy. The following are the important components of an OSPF network:
- **Areas:** An area consists of routers that have been administratively grouped together. Usually, an area as a collection of contiguous IP subnetted networks. Routers that are totally within an area are called internal routers. All interfaces on internal routers are directly connected to networks within the area. Within an area, all routers have identical topological databases.
- **Area Border Routers:** Routers that belong to more than one area are called area border routers (ABRs). ABRs maintain a separate topological database for each area to which they are connected.
- **Backbone Area:** An OSPF backbone area consists of all routers in area 0, and all area border routers (ABRs). The backbone distributes routing information between different areas.
- **Autonomous System Boundary Routers (ASBRs):** Routers that exchange routing information with routers in other Autonomous Systems are called ASBRs. They advertise externally learned routes throughout the AS.
- **Internal Routers** are routers whose interfaces all belong to the same area. These routers have a single Link State Database.

11.7 OSPF Benefits & Drawbacks

- Benefits
  - Open standard
  - No hop count limitations
  - Loop free
  - Faster convergence
- Drawbacks
  - Consumes more CPU resources
  - Support only equal cost balancing
  - Support only IP protocol don't work on IPX and APPLE Talk

- **Configuring OSPF**
  - `Router(config)# router ospf <process ID >`
  - `Router(config-router)# network <Network ID> <wildcard mask> area <area id>`

11.8 LAB – Dynamic Routing using OSPF in Single Area



- STEPS: Pre-requirement for LAB (check previous labs)
  - Design the topology (connectivity)
  - Assign the IP address according to diagram
  - Make sure that interfaces used should be in UP UP state
- What we do in this lab
  - Dynamic routing using OSPF single area
  - Verify Routing table and reachability between the LAN's (using PING and TRACE commands)

```
R-1# show ip route
Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, Serial0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
```

```
R-2# show ip route
Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, Serial0/0
C    11.0.0.0/8 is directly connected, Serial0/1
```

```
R-3# show ip route
Gateway of last resort is not set

C    11.0.0.0/8 is directly connected, Serial0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
```

```
R-1(config)# router ospf 1
R-1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R-1(config-router)# network 10.0.0.0 0.255.255.255 area 0
```

```
R-2(config)# router ospf 1
R-2(config-router)# network 192.168.2.0 0.0.0.255        area  0
R-2(config-router)# network 11.0.0.0    0.255.255.255    area  0
R-2(config-router)# network 10.0.0.0    0.255.255.255    area  0
06:14:49: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.100 on Serial0/0 from
LOADING to FULL, Loading Done
```

```
R-3(config)#router ospf 1
R-3(config-router)#network 192.168.3.0 0.0.0.255 area 0
R-3(config-router)#network 11.0.0.0 0.255.255.255 area  0
06:15:46: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.2.100 on Serial0/0 from
LOADING to FULL, Loading Done
```

```
R-2# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address      Interface
192.168.1.100     0   FULL/  -        00:00:35    10.0.0.1     Serial0/0
192.168.3.100     0   FULL/  -        00:00:37    11.0.0.2     Serial0/1
```

```
R-1# show ip route
Gateway of last resort is not set
C    10.0.0.0/8 is directly connected, Serial0/0
O    11.0.0.0/8 [110/128] via 10.0.0.2, 00:04:21, Serial0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
O    192.168.2.0/24 [110/65] via 10.0.0.2, 00:04:21, Serial0/0
O    192.168.3.0/24 [110/129] via 10.0.0.2, 00:03:19, Serial0/0
```

```
R-1# show ip route ospf

O    11.0.0.0 [110/128] via 10.0.0.2, 00:04:25, Serial0/0
O    192.168.2.0 [110/65] via 10.0.0.2, 00:04:25, Serial0/0
O    192.168.3.0 [110/129] via 10.0.0.2, 00:03:23, Serial0/0
```

```
R-2# show ip route ospf

O    192.168.1.0 [110/65] via 10.0.0.1, 00:05:09, Serial0/0
O    192.168.3.0 [110/65] via 11.0.0.2, 00:04:14, Serial0/1
```

```
R-2# show ip route ospf

O    192.168.1.0 [110/65] via 10.0.0.1, 00:05:09, Serial0/0
O    192.168.3.0 [110/65] via 11.0.0.2, 00:04:14, Serial0/1
```

```
R-3# show ip route ospf

O    10.0.0.0 [110/128] via 11.0.0.1, 00:04:49, Serial0/0
O    192.168.1.0 [110/129] via 11.0.0.1, 00:04:49, Serial0/0
O    192.168.2.0 [110/65] via 11.0.0.1, 00:04:49, Serial0/0
```

```
R-1# show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.1.100
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.0.0.0 0.0.0.255 area 0
    10.0.0.0 0.255.255.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.0.0.2             110      00:05:46
  Distance: (default is 110)
```

```
R-1#show ip ospf database
            OSPF Router with ID (192.168.1.100) (Process ID 1)
                Router Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum Link count
192.168.1.100   192.168.1.100   468         0x80000003 0x00d1f4 3
192.168.2.100   192.168.2.100   411         0x80000005 0x0054e6 5
192.168.3.100   192.168.3.100   411         0x80000003 0x0010ad 3
```

```
PC> ipconfig
IP Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100
```

```
PC> ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.2.1: bytes=32 time=19ms TTL=126
Reply from 192.168.2.1: bytes=32 time=20ms TTL=126
Reply from 192.168.2.1: bytes=32 time=14ms TTL=126
```

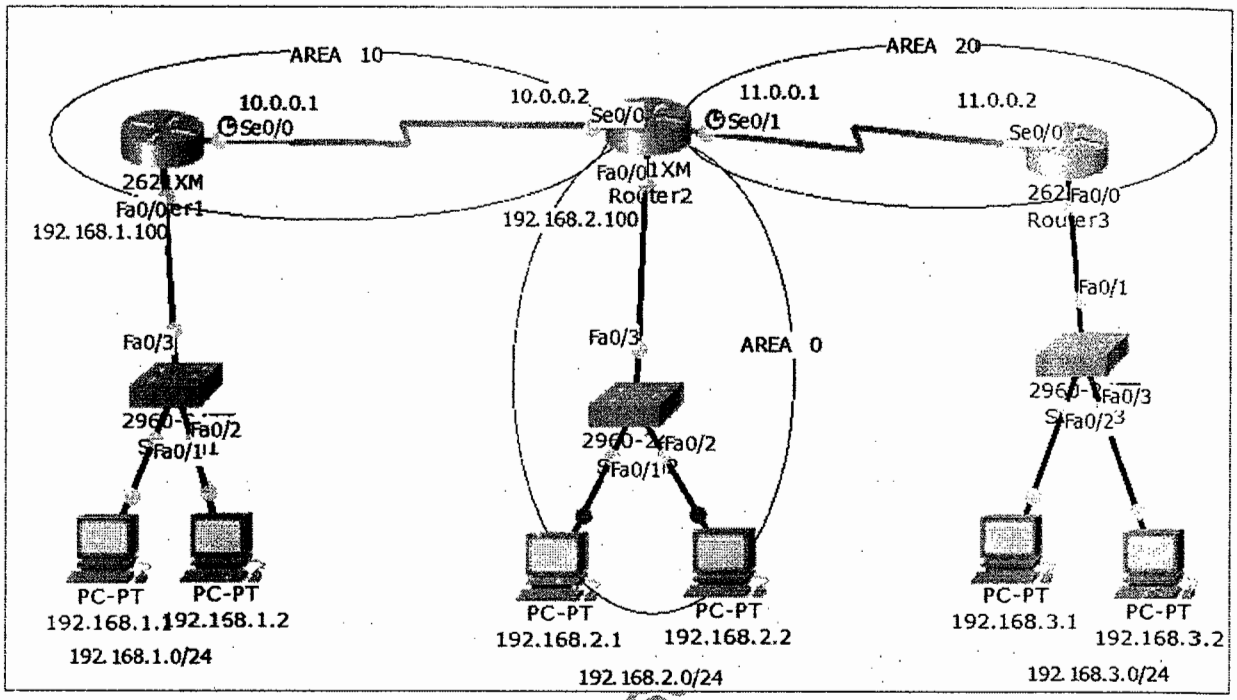
```
PC> ping 192.168.3.1
Pinging 192.168.3.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.3.1: bytes=32 time=27ms TTL=125
Reply from 192.168.3.1: bytes=32 time=22ms TTL=125
Reply from 192.168.3.1: bytes=32 time=25ms TTL=125
```

```
PC> tracert 192.168.3.1
Tracing route to 192.168.3.1 over a maximum of 30 hops:
  1    7 ms      8 ms      8 ms      192.168.1.100
  2    2 ms      9 ms      9 ms      10.0.0.2
  3   17 ms      6 ms     12 ms      11.0.0.2
  4   24 ms     27 ms     25 ms      192.168.3.1
Trace complete.
```

```
R-1# ping 192.168.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/16/31 ms
```

```
R-3# ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/15/18 ms
```

11.9 LAB – Dynamic Routing using OSPF Multiple Area



- STEPS: Pre-requirement for LAB (check previous labs)
  - Design the topology (connectivity)
  - Assign the IP address according to diagram
  - Make sure that interfaces used should be in UP UP state
- What we do in this lab
  - Dynamic routing using OSPF multiple area
  - Verify Routing table and reachability between the LAN's (using PING and TRACE commands)

```
R-1# show ip route
Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, Serial0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
```

```
R-2# show ip route
Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, Serial0/0
C    11.0.0.0/8 is directly connected, Serial0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

```
R-3# show ip route
Gateway of last resort is not set

C    11.0.0.0/8 is directly connected, Serial0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
```

```
R-1(config)# router ospf 1
R-1(config-router)# network 192.168.1.0 0.0.0.255 area 10
R-1(config-router)# network 10.0.0.0 0.255.255.255 area 10
```

```
R-2(config)# router ospf 1
R-2(config-router)# network 192.168.2.0 0.0.0.255        area  0
R-2(config-router)# network 11.0.0.0    0.255.255.255    area  20
R-2(config-router)# network 10.0.0.0    0.255.255.255    area  10
06:14:49: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.100 on Serial0/0 from
LOADING to FULL, Loading Done
```

```
R-3(config)#router ospf 1
R-3(config-router)#network 192.168.3.0 0.0.0.255 area 20
R-3(config-router)#network 11.0.0.0 0.255.255.255 area  20
06:15:46: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.2.100 on Serial0/0 from
LOADING to FULL, Loading Done
```

```
R-2# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address       Interface
192.168.3.100     0   FULL/  -        00:00:39    11.0.0.2      Serial0/1
192.168.1.100     0   FULL/  -        00:00:39    10.0.0.1      Serial0/0
```

```
R-1# show ip route
Gateway of last resort is not set
C    10.0.0.0/8 is directly connected, Serial0/0
O IA 11.0.0.0/8 [110/128] via 10.0.0.2, 00:06:39, Serial0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
O IA 192.168.2.0/24 [110/65] via 10.0.0.2, 00:06:39, Serial0/0
O IA 192.168.3.0/24 [110/129] via 10.0.0.2, 00:06:07, Serial0/0
```

```
R-1# show ip route ospf
O IA 11.0.0.0 [110/128] via 10.0.0.2, 00:06:24, Serial0/0
O IA 192.168.2.0 [110/65] via 10.0.0.2, 00:06:24, Serial0/0
O IA 192.168.3.0 [110/129] via 10.0.0.2, 00:05:53, Serial0/0
```

```
R-1# show ip route ospf
O IA 11.0.0.0 [110/128] via 10.0.0.2, 00:06:24, Serial0/0
O IA 192.168.2.0 [110/65] via 10.0.0.2, 00:06:24, Serial0/0
O IA 192.168.3.0 [110/129] via 10.0.0.2, 00:05:53, Serial0/0
```

```
R-2# show ip route ospf
O    192.168.1.0 [110/65] via 10.0.0.1, 00:08:31, Serial0/0
O    192.168.3.0 [110/65] via 11.0.0.2, 00:08:04, Serial0/1
```

```
R-3# show ip route ospf
O IA 10.0.0.0 [110/128] via 11.0.0.1, 00:08:21, Serial0/0
O IA 192.168.1.0 [110/129] via 11.0.0.1, 00:08:21, Serial0/0
O IA 192.168.2.0 [110/65] via 11.0.0.1, 00:08:21, Serial0/0
```

```
R-1# show ip ospf database
OSPF Router with ID (192.168.1.100) (Process ID 1)
                Router Link States (Area 10)
Link ID         ADV Router      Age         Seq#       Checksum Link count
192.168.1.100   192.168.1.100   902         0x80000003 0x003b8b 3
192.168.2.100   192.168.2.100   902         0x80000002 0x00e758 2

                Summary Net Link States (Area 10)
Link ID         ADV Router      Age         Seq#       Checksum
192.168.2.0     192.168.2.100   905         0x80000001 0x0057cb
11.0.0.0        192.168.2.100   905         0x80000002 0x00063d
192.168.3.0     192.168.2.100   870         0x80000003 0x00ca15
```

```
R-2# show ip ospf database
OSPF Router with ID (192.168.2.100) (Process ID 1)
                Router Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum Link count
192.168.2.100   192.168.2.100   708         0x80000002 0x0070d6 1

                Summary Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
11.0.0.0        192.168.2.100   698         0x80000001 0x00083c
10.0.0.0        192.168.2.100   689         0x80000002 0x001331
192.168.1.0     192.168.2.100   689         0x80000003 0x00e001
192.168.3.0     192.168.2.100   663         0x80000004 0x00c816

                Router Link States (Area 10)
Link ID         ADV Router      Age         Seq#       Checksum Link count
192.168.2.100   192.168.2.100   694         0x80000002 0x00e758 2
192.168.1.100   192.168.1.100   694         0x80000003 0x003b8b 3

                Summary Net Link States (Area 10)
Link ID         ADV Router      Age         Seq#       Checksum
192.168.2.0     192.168.2.100   697         0x80000001 0x0057cb
11.0.0.0        192.168.2.100   697         0x80000002 0x00063d
192.168.3.0     192.168.2.100   662         0x80000003 0x00ca15

                Router Link States (Area 20)
Link ID         ADV Router      Age         Seq#       Checksum Link count
192.168.2.100   192.168.2.100   668         0x80000002 0x000a33 2
192.168.3.100   192.168.3.100   668         0x80000003 0x0010ad 3

                Summary Net Link States (Area 20)
Link ID         ADV Router      Age         Seq#       Checksum
192.168.2.0     192.168.2.100   703         0x80000001 0x0057cb
10.0.0.0        192.168.2.100   689         0x80000002 0x001331
192.168.1.0     192.168.2.100   689         0x80000003 0x00e001
```

```
PC> ipconfig
IP Address.....................: 192.168.1.1
Subnet Mask....................: 255.255.255.0
Default Gateway................: 192.168.1.100
```

```
PC> ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.2.1: bytes=32 time=19ms TTL=126
Reply from 192.168.2.1: bytes=32 time=20ms TTL=126
Reply from 192.168.2.1: bytes=32 time=14ms TTL=126
```

```
PC> ping 192.168.3.1
Pinging 192.168.3.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.3.1: bytes=32 time=27ms TTL=125
Reply from 192.168.3.1: bytes=32 time=22ms TTL=125
Reply from 192.168.3.1: bytes=32 time=25ms TTL=125
```

```
PC> tracert 192.168.3.1

Tracing route to 192.168.3.1 over a maximum of 30 hops:

  1    5 ms     8 ms     8 ms     192.168.1.100
  2   12 ms     9 ms     8 ms     10.0.0.2
  3   17 ms     6 ms    12 ms     11.0.0.2
  4   24 ms    17 ms    25 ms     192.168.3.1

Trace complete.
```

```
R-1# ping 192.168.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/16/31 ms
```

```
R-3# ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/15/18 ms
```

12. ACL (Access Control List)

12.1 ACL Overview

- ACL is a set of rules which allows or deny the specific traffic moving through the router
- It is a Layer 3 security, which controls the flow of traffic from one router to another.
- It is also called as Packet Filtering Firewall.

Standard ACL	Extended ACL
The access-list number range is 1–99	The access-list number range is 100–199
Can block a Network, Host and Subnet	Can block a Network, Host, Subnet and Service
All services are blocked	Selected services can be blocked
Implemented closest to the destination	Implemented closest to the source
Filtering is done based on only source IP address	Filtering is done based on source IP, destination IP, protocol, Port #

12.2 Rules of Access List

- Works in Sequential order (It's always compared with each line of the access list in sequential order—that is, it'll always start with the first line of the access list, then go to line 2, then line 3, and so on)
- All deny statements have to be given First (preferable most cases)
- There should be at least one Permit statement (mandatory)
- An implicit "deny" blocks all traffic by default when there is no match (an invisible statement).
- Can have one access-list per interface per direction i.e., two access-lists per interface, one in inbound direction and one in outbound direction.
- Any time a new entry is added to the access list, it will be placed at the bottom of the list. Using a text editor for access lists is highly suggested.
- You cannot remove one line from an access list. If you try to do this, you will remove the entire list. It is best to copy the access list to a text editor before trying to edit the list. The only exception is when using named access lists.

12.3 Wild Card Mask

- Tells the router which portion of the bits to match or ignore.
- It's the inverse of the subnet mask, hence is also called as Inverse mask.
- A bit value of 0 indicates MUST MATCH (Check Bits)

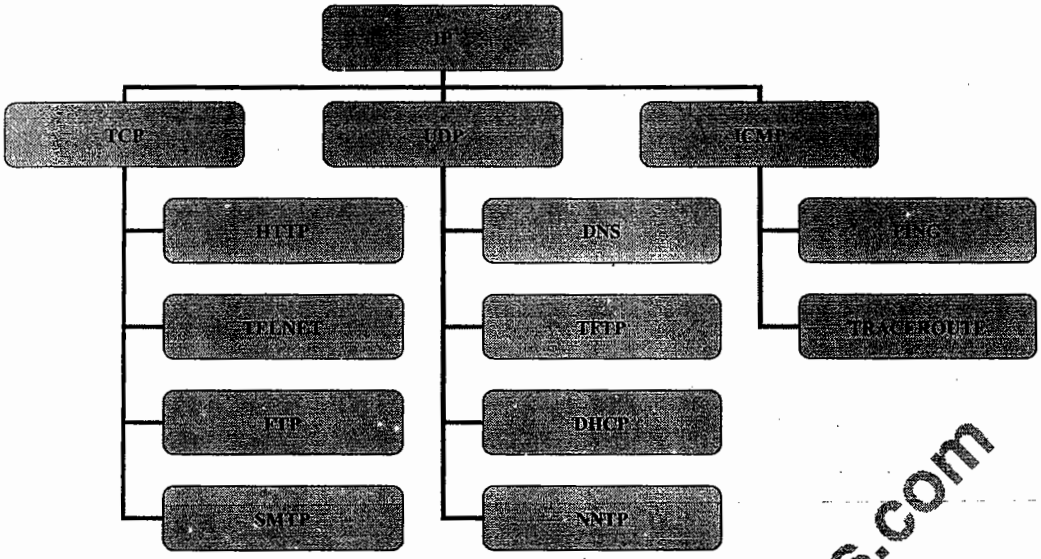
- A bit value of 1 indicates IGNORE (Ignore Bits)
- Wild Card Mask for a Host will be always 0.0.0.0
- A wild card mask can be calculated using formula:
  Global Subnet Mask – Customized Subnet Mask = Wild Card Mask
  - Example1: 255.255.255.255 – 255.255.255.0 = 0.0.0.255
  - Example2: 255.255.255.255 – 255.255.255.240 = 0.0.0.15
  - Example3: 255.255.255.255 – 255.255.255.224 = 0.0.0.31
- Wildcards are used with the host/network address to tell the router a range of available addresses to filter.
- To specify a host, the address would look like this: 172.16.30.5 0.0.0.0

12.4 Standard Access List

- Creation of Standard Access List
  ```
  R1(config)#access-list <acl no> <permit/deny> <source address> <source WCM>
  ```
- Implementation of Standard Access List
  ```
  Router(config)#interface <interface type>  <interface no>
  Router(config-if)#ip access-group  <number>  <out/in>
  ```
- To Verify:
  ```
  Router#show access-list
  Router#show access-list  <no>
  ```

12.5 Extended Access List

- Creation of Extended Access List
  ```
  Router(config)#access-list <acl no> <permit/deny> <protocol> <source address>
  <source wildcard mask> <destination address> <destination wildcard mask>
  <operator> <service>
  ```
- Implementation of Extended Access List
  ```
  Router(config)#interface <interface type> <interface no>
  Router(config-if)#ip access-group <number> <out/in>
  ```
- Operators:
  - eq (equal to)
  - neq (not equal to)
  - lt (less than)
  - gt (greater than)
- If you want to filter by Application layer protocol, you have to choose the appropriate layer4 transport protocol after the permit or deny statement.
- For example, to filter Telnet or FTP you choose TCP since both Telnet and FTP use TCP at the Transport layer.
- If you were to choose IP, you wouldn't be allowed to specify a specific application protocol later



12.6 Named Access List

- Named access lists are just another way to create standard and extended access lists
- Access-lists are identified using Names rather than Numbers
- Names are Case-Sensitive
- No limitation of Numbers here
- Main advantage is editing of ACL is possible. Which means removing a specific statement from the ACL is possible.
- IOS version 11.2 or later allows Named ACL
- Creation of Standard Named Access List

```
Router(config)#ip access-list standard <name>
Router(config-std-nacl)#<permit/deny> <source address> <source wildcard mask>
```

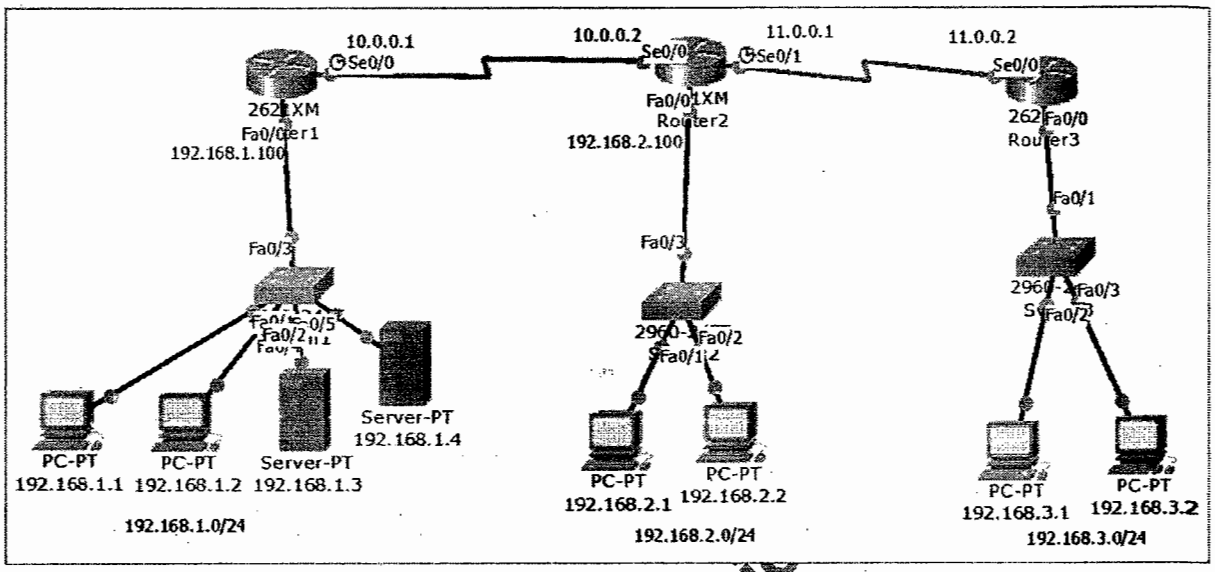
- Creating of Extended Named Access List

```
Router(config)#ip access-list extended <name>
Router(config-ext-nacl)#<permit/deny> <protocol> <source address>
<source wildcard mask> <destination address> <destination wildcard mask>
<operator> <service>
```

- Implementation of Extended Named Access List

```
Router(config)#interface <interface type><interface no>
Router(config-if)#ip access-group <name> <out/in>
```

12.7 LAB: Implementing Standard Access List



- Pre-requirement for LAB (check previous labs)
  - Design the topology (connectivity)
  - Assign the IP address according to diagram
  - Make sure that interfaces used should be in UP UP state
  - Any dynamic routing protocol or static routing
  - Verify routing table & reachability between the LAN's using PING and TRACE commands
- Let's say the Requirement in this LAB is to
  - Deny the host 192.168.1.1 communicating with 192.168.2.0
  - Deny the host 192.168.1.2 communicating with 192.168.2.0
  - Deny the network 192.168.3.0 communicating with 192.168.2.0
  - Permit all the remaining traffic

NOTE:

- *The Above ACL rules should not affect the other communication*
- *Before creating the ACL, make sure that the routing configured is correct and all the three LAN devices are able to communicate with each other using PING command*

```
PC> ipconfig
IP Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100
```

```
PC> ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=17ms TTL=126
Reply from 192.168.2.1: bytes=32 time=20ms TTL=126
Reply from 192.168.2.1: bytes=32 time=16ms TTL=126
Reply from 192.168.2.1: bytes=32 time=17ms TTL=126
```

```
PC> ipconfig
IP Address.....: 192.168.2.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100
```

```
PC> ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=17ms TTL=126
Reply from 192.168.2.1: bytes=32 time=20ms TTL=126
Reply from 192.168.2.1: bytes=32 time=16ms TTL=126
Reply from 192.168.2.1: bytes=32 time=17ms TTL=126
```

```
PC> ipconfig
IP Address.....: 192.168.3.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100
```

```
PC> ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=17ms TTL=126
Reply from 192.168.2.1: bytes=32 time=20ms TTL=126
Reply from 192.168.2.1: bytes=32 time=16ms TTL=126
Reply from 192.168.2.1: bytes=32 time=17ms TTL=126
```

- Creating the ACL rules according to the requirement.

```
R-2(config)#access-list 15 deny 192.168.1.1 0.0.0.0
R-2(config)#access-list 15 deny host 192.168.1.2
R-2(config)#access-list 15 deny 192.168.3.0 0.0.0.255
R-2(config)#access-list 15 permit any
```

- Implementation

```
R-2(config)#access-list 15 deny 192.168.1.1 0.0.0.0
R-2(config)#access-list 15 deny host 192.168.1.2
R-2(config)#access-list 15 deny 192.168.3.0 0.0.0.255
R-2(config)#access-list 15 permit any
```

- Verification

```
R-2# show access-lists
Standard IP access list 15
    deny host 192.168.1.1
    deny host 192.168.1.2
    deny 192.168.3.0 0.0.0.255
    permit any
```

```
PC> ipconfig
IP Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100
```

```
PC> ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 10.0.0.2: Destination host unreachable.
Reply from 10.0.0.2: Destination host unreachable.
Reply from 10.0.0.2: Destination host unreachable.
Reply from 10.0.0.2: Destination host unreachable.
```

```
PC> ping 192.168.3.1
Pinging 192.168.3.1 with 32 bytes of data:
Reply from 192.168.3.1: bytes=32 time=21ms TTL=125
Reply from 192.168.3.1: bytes=32 time=17ms TTL=125
Reply from 192.168.3.1: bytes=32 time=24ms TTL=125
Reply from 192.168.3.1: bytes=32 time=13ms TTL=125
```

```
PC> ipconfig
IP Address.....: 192.168.1.2
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100
```

```
PC> ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 10.0.0.2: Destination host unreachable.
Reply from 10.0.0.2: Destination host unreachable.
Reply from 10.0.0.2: Destination host unreachable.
Reply from 10.0.0.2: Destination host unreachable.
```

```
Server> ipconfig
IP Address.....: 192.168.1.3
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100
```

```
Server> ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=33ms TTL=126
Reply from 192.168.2.1: bytes=32 time=17ms TTL=126
Reply from 192.168.2.1: bytes=32 time=23ms TTL=126
Reply from 192.168.2.1: bytes=32 time=14ms TTL=126
```

```
PC> ipconfig
IP Address.....: 192.168.3.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.3.100
```

```
PC> ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 11.0.0.1: Destination host unreachable.
Reply from 11.0.0.1: Destination host unreachable.
Reply from 11.0.0.1: Destination host unreachable.
Reply from 11.0.0.1: Destination host unreachable.
```

```
PC> ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=16ms TTL=125
Reply from 192.168.1.1: bytes=32 time=29ms TTL=125
Reply from 192.168.1.1: bytes=32 time=16ms TTL=125
Reply from 192.168.1.1: bytes=32 time=21ms TTL=125
```

12.8 LAB: Restricting Telnet Access to the Router to specified networks or hosts

Should you secure your telnet lines on a router?

- You're monitoring your network and notice that someone has telnetted into your core router by using the show users command.
- You use the disconnect command and they are disconnected from the router, but you notice they are back into the router a few minutes later. You are thinking about putting an access list on the router interfaces, but you don't want to add a lot of latency on each interface since your router is already pushing a lot of packets.
- The access-class command illustrated in this lab is the best way to do restrict the users for telnet
- Because it doesn't use an access list that just sits on an interface looking at every packet that is coming and going. This can cause overhead on the packets trying to be routed.
- When you put the access-class command on the VTY lines, only packets trying to telnet into the router will be looked at and compared. This provides nice, easy-to-configure security for your router.

Requirement:

- Continue with the previous lab and use the same diagram only remove the ACL and implementation
- Allow the hosts 192.168.1.1 and 192.168.1.2 to telnet into R1. Any other host should not be allowed.
- Remove the ACL, which was created the previous lab

```
R-2(config)# no access-list 15
R-2(config)# interface fastEthernet 0/0
R-2(config-if)# no ip access-group 15 out
R-2(config-if)# end
```

- Creation of ACL which permits only hosts 192.168.1.1 and 192.168.1.2:

```
R-1(config)#access-list 20 permit host 192.168.1.1
R-1(config)#access-list 20 permit host 192.168.1.2
```

- Implementation:

```
R-1(config)#line vty 0 4
R-1(config-line)#password cisco
R-1(config-line)#login
R-1(config-line)#access-class 20 in
R-1(config-line)#end
```

- Verification

```
PC> ipconfig
IP Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100
```

```
   telnet 192.168.1.100
Trying 192.168.1.100 ...Open
User Access Verification
Password:
```

```
   ipconfig
IP Address.....: 192.168.1.
Subnet Mask.....: 255.255.255.
Default Gateway.....: 192.168.1.
```

```
   telnet 192.168.1.100
Trying 192.168.1.100 ...Open
User Access Verification
Password:
```

```
Server> ipconfig
IP Address.....: 192.168.1.3
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100
```

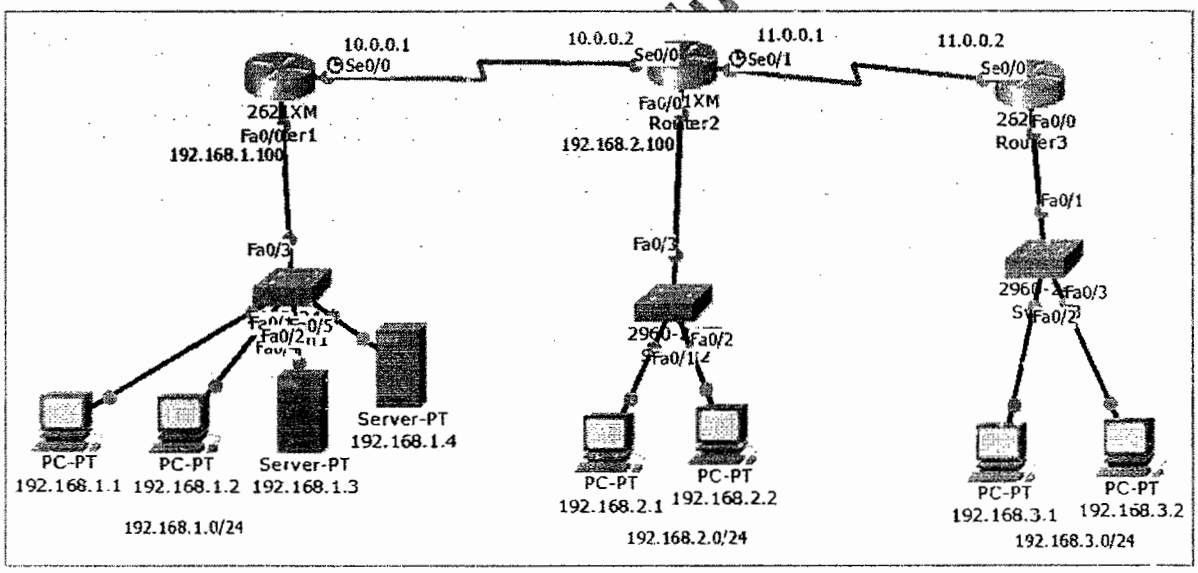
```
Server> telnet 192.168.1.100
Trying 192.168.1.100...
% Connection refused by remote host
SERVER>
```

```
Server> ipconfig
IP Address.....: 192.168.1.4
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100
```

```
Server> telnet 192.168.1.100
Trying 192.168.1.100...
% Connection refused by remote host
SERVER>
```

```
R-2> enable
R-2# telnet 10.0.0.1
Trying 10.0.0.1...
% Connection refused by remote host
```

12.9 LAB: Implementing Extended Access List



- Pre-requirement for LAB (check previous labs)
  - Design the topology (connectivity)
  - Assign the IP address according to diagram
  - Make sure that interfaces used should be in UP UP state
  - Any dynamic routing protocol or static routing
  - Verify Routing table and reachability between the LAN's (using PING and TRACE commands)

- Let's say the Requirement in this LAB is to
  - Deny the users on LAN 192.168.2.0 and should not access 192.168.1.3 **HTTP** service
  - Deny the users on LAN 192.168.3.0 and should not access 192.168.1.4 **FTP** service
  - Deny the users on LAN 192.168.3.1 and should not access 192.168.1.3 **HTTP** service
  - Deny the users on LAN 192.168.2.0 and should not get DNS service from **DNS** server 192.168.1.4
  - Deny ther users from the host between 192.168.3.2 and 192.168.1.2 should **not** be able to send ICMP (ping/trace) messages
  - Remaining hosts and services should be permitted

NOTE: *The Above ACL rules should not affect the other communication*

```
R-1(config)#access-list 145 deny tcp 192.168.2.0 0.0.0.255 host 192.168.1.3 eq www
R-1(config)#access-list 145 deny tcp 192.168.3.0 0.0.0.255 host 192.168.1.4 eq ftp
R-1(config)#access-list 145 deny tcp host 192.168.3.1 host 192.168.1.3 eq www
R-1(config)#access-list 145 deny udp 192.168.2.0 0.0.0.255 host 192.168.1.4 eq ?
<0-65535>   Port number
bootpc      Bootstrap Protocol (BOOTP) client (68)
bootps      Bootstrap Protocol (BOOTP) server (67)
domain      Domain Name Service (DNS, 53)
isakmp      Internet Security Association and Key Management Protocol (500)
            non500-isakmp  Internet Security Association and Key Management
            Protocol (4500)
snmp        Simple Network Management Protocol (161)
tftp        Trivial File Transfer Protocol (69)
```

```
R-1(config)#access-list 145 deny udp 192.168.2.0 0.0.0.255 host 192.168.1.4 eq
domain
R-1(config)#access-list 145 deny icmp host 192.168.3.1 host 192.168.1.1 ?
<0-256>                type-num
echo                   echo
echo-reply             echo-reply
host-unreachable       host-unreachable
net-unreachable        net-unreachable
port-unreachable       port-unreachable
protocol-unreachable   protocol-unreachable
ttl-exceeded           ttl-exceeded
unreachable            unreachable
<cr>
R-1(config)#access-list 145 deny icmp host 192.168.3.2 host 192.168.1.2 echo
R-1(config)#access-list 145 deny icmp host 192.168.3.2 host 192.168.1.2 echo-reply
R-1(config)#access-list 145 permit ip any any
```

- Implementation:

```
R-1(config)# interface fastEthernet 0/0
R-1(config-if)#ip access-group 145 out

OR

R-1(config)#interface serial 0/0
R-1(config-if)#ip access-group 145 in
R-1(config)#access-list 145 permit ip any any
```

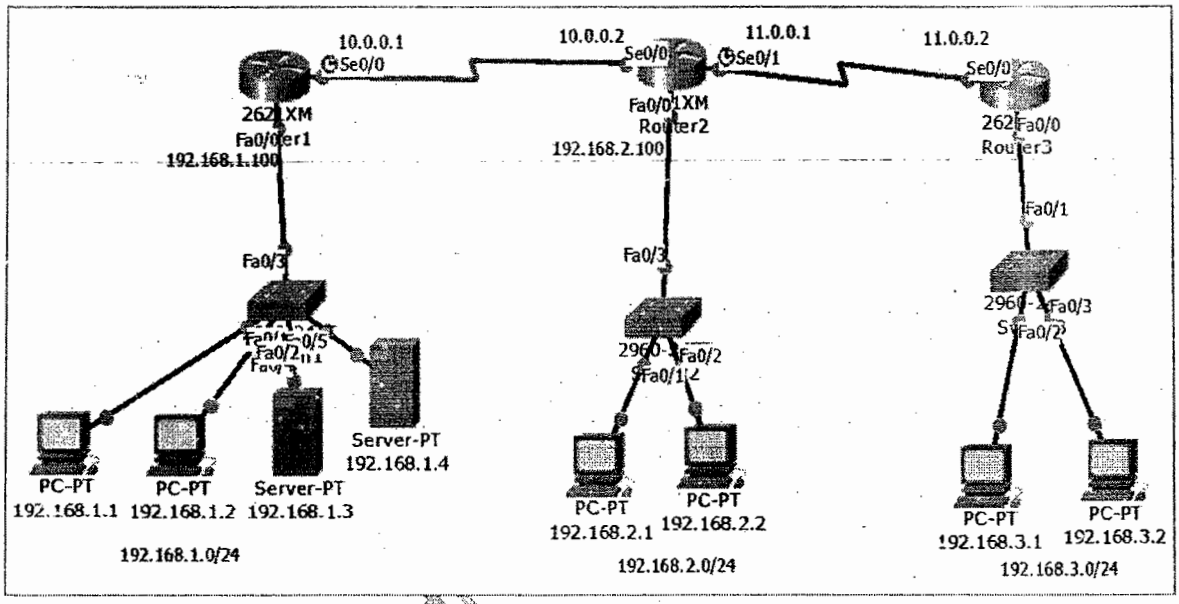
- Verification

```
PC> ipconfig
IP Address.....: 192.168.3.2
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.3.100
```

```
PC> ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

```
PC> ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=20ms TTL=
Reply from 192.168.1.1: bytes=32 time=27ms TTL=
Reply from 192.168.1.1: bytes=32 time=13ms TTL=
Reply from 192.168.1.1: bytes=32 time=25ms TTL=
```

12.10 LAB: Implementing the Standard ACL



NOTE: *Refer LAB 12.7 for the specific rules which are used in this lab*

```
R-2(config)#ip access-list standard CCNA
R-2(config-std-nacl)#deny 192.168.1.1  0.0.0.0
R-2(config-std-nacl)#deny host 192.168.1.2
R-2(config-std-nacl)#deny 192.168.3.0  0.0.0.255
R-2(config-std-nacl)#permit any
R-2(config-std-nacl)#exit
```

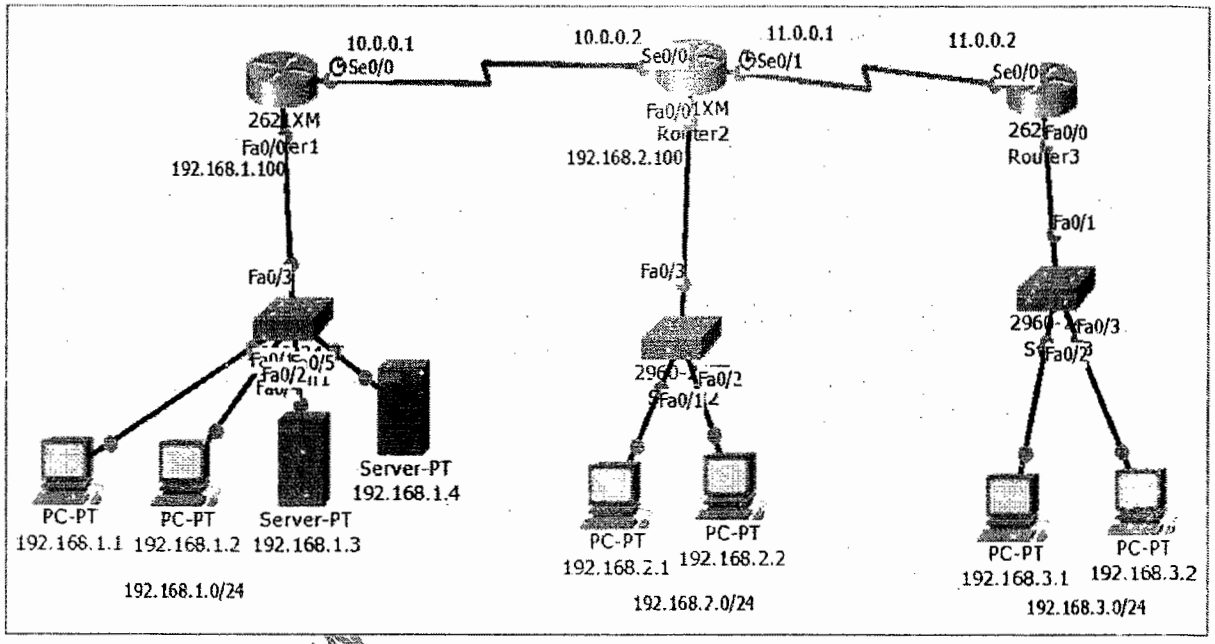
- Implementation:

```
R-2(config)# interface fastEthernet 0/0
R-2(config-if)# ip access-group CCNA out
```

- Verification is same as Lab 12.6

```
R-2# sh access-lists
Standard IP access list CCNA
    deny host 192.168.1.1
    deny host 192.168.1.2
    deny 192.168.3.0 0.0.0.255
    permit any
```

12.11 LAB: Implementing the Extended ACL



NOTE: *Refer LAB 12.8 for the specific rules which are used in this lab*

```
R-1(config)#ip access-list extended CCNP
R-1(config-ext-nacl)#deny tcp 192.168.2.0 0.0.0.255 host 192.168.1.3 eq www
R-1(config-ext-nacl)#deny tcp 192.168.3.0 0.0.0.255 host 192.168.1.4 eq ftp
R-1(config-ext-nacl)#deny tcp host 192.168.3.1 host 192.168.1.3 eq www
R-1(config-ext-nacl)#deny udp 192.168.2.0 0.0.0.255 host 192.168.1.4 eq domain
R-1(config-ext-nacl)#deny icmp host 192.168.3.1 host 192.168.1.1 echo
R-1(config-ext-nacl)#deny icmp host 192.168.3.1 host 192.168.1.1 echo-reply
R-1(config-ext-nacl)#permit ip any any
```

- Implementation:

```
R-1(config)#interface fastEthernet 0/0
R-1(config-if)#ip access-group CCNP out
      (OR)
R-1(config)#interface serial 0/0
R-1(config-if)#ip access-group CCNP in
```

- Verification is same as Lab 12.7

```
R-1# show access-lists
Extended IP access list CCNP
    deny tcp 192.168.2.0 0.0.0.255 host 192.168.1.3 eq www
    deny tcp 192.168.3.0 0.0.0.255 host 192.168.1.4 eq ftp
    deny tcp host 192.168.3.1 host 192.168.1.3 eq www
    deny udp 192.168.2.0 0.0.0.255 host 192.168.1.4 eq domain
    deny icmp host 192.168.3.1 host 192.168.1.1 echo
    deny icmp host 192.168.3.1 host 192.168.1.1 echo-reply
    permit ip any any
```

13. NAT (Network Address Translation)

13.1 NAT Overview

- NAT is the method of "Translation of private IP address into public IP address".
- In order to communicate with Internet we must have registered public IP address.
- Address translation was originally developed to solve two problems:
  - To handle a shortage of IPv4 addresses
  - Hide network addressing schemes
- Small companies typically get their public IP addresses directly from their ISPs, which have a limited number.
- Large companies can sometimes get their public IP addresses from a registration authority, such as the Internet Assigned Numbers Authority (IANA).
- Common devices that can perform address translation include firewalls, routers, and servers. Typically address translation is done at the perimeter of the network by either a firewall (more commonly) or a router.
- There are certain addresses in each class of IP address that are reserved for Private Networks. These addresses are called private addresses.
  - **Class A** 10.0.0.0 to 10.255.255.255
  - **Class B** 172.16.0.0 to 172.31.255.255
  - **Class C** 192.168.0.0 to 192.168.255.255
- Here's a list of situations when it's best to have NAT on your side:
- You need to connect to the Internet and your hosts don't have globally unique IP addresses.
- You change to a new ISP that requires you to renumber your network.
- You need to merge two intranets with duplicate addresses.

Advantages

- Conserves legally registered addresses
- Reduces address overlap occurrence. Increases flexibility when connecting to Internet.
- Eliminates address renumbering as network changes

Disadvantages

- Translation introduces switching path delays
- Loss of end-to-end IP traceability
- Certain applications will not function with NAT enabled

13.2 NAT Terminology

- Inside Local Addresses – Name of inside source address before translation (private IP)
- Inside Global Address – Name of inside host after translation (public IP)
- Outside Local Address – Name of destination host before translation
- Outside Global Address – Name of outside destination host after translation

13.3 Types of NAT

- Static NAT
  - This type of NAT is designed to allow one-to-one mapping between local and global addresses.
  - Keep in mind that the static version requires you to have one real Internet IP address for every host on your network.
  - Syntax:
    ```
    (Config)# IP nat inside source static <private IP> <public IP>
    ```
  - Implementation:
    ```
    (Config)#interface f0/0
    (Config-if)#ip nat inside (interface facing towards LAN)
    (Config)#interface s0/0
    (Config-if)#ip nat outside (interface facing towards ISP)
    ```
- Dynamic NAT
  - This version gives you the ability to map an unregistered IP address to a registered IP address from out of a pool of registered IP addresses.
  - You don't have to statically configure your router to map an inside to an outside address as you would use static NAT, but you do have to have enough real IP addresses for everyone who's going to be sending packets to and receiving them from the Internet.
  - Syntax:
    ```
    (Config)#access-list <ACL-NO> permit <NET.ID> <WCM>
    (Config)#ip nat pool <NAME> <starting Public IP> <end Public IP>
    netmask <mask>
    (Config)#ip nat inside source list <ACL-NO> pool <NAME>
    ```
  - Implementation:
    ```
    (Config)# interface f0/0
    (Config-if)#ip nat inside (interface facing towards LAN)
    (Config)#interface s0/0
    (Config-if)#ip nat outside (interface facing towards ISP)
    ```

- PAT (Dynamic NAT Overload)
  - This is the most popular type of NAT configuration. Understand that overloading really is a form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address—many-to-one—by using different ports.
  - It is also known as Port Address Translation (PAT), and by using PAT (NAT Overload), you get to have thousands of users connect to the Internet using only one real global IP address.
  - NAT Overload is the real reason we haven't run out of valid IP address on the Internet
  - Syntax:

```
(Config)#access-list <ACL-NO> permit <NET.ID> <WCM>
(Config)#ip nat inside pool <NAME> <starting Public IP> <end Public IP>
netmask <mask>
(Config)#ip nat inside source list <ACL-NO> pool <NAME> overload
```

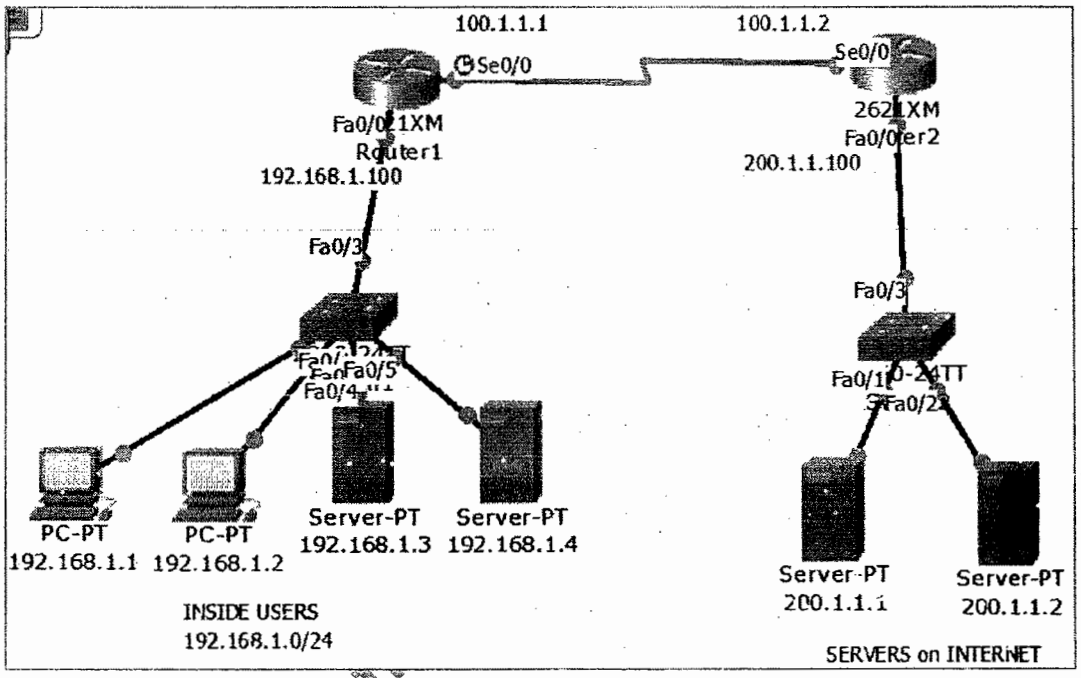
  - Implementation:

```
(Config)# interface f0/0
(Config-if)#ip nat inside (interface facing towards LAN)
(Config)#interface s0/0
(Config-if)#ip nat outside (interface facing towards ISP)
```

13.4 LAB: Implementing Static NAT

- Configure the following translations

PRIVATE IP	PUBLIC IP
192.168.1.1	50.1.1.1
192.168.1.2	50.1.1.2
192.168.1.3	50.1.1.3



- STEPS
  - Configure IP address according to the diagram
  - Configure default route on both routers
  - Configure NAT (static NAT according to the requirement)
- Implementation
  - Verify by generating some traffic from LAN to ouside servers
  - #show ip nat translations

```
R-1# show ip interface brief
Interface          IP-Address      OK? Method Status                Protocol
FastEthernet0/0    192.168.1.100   YES manual up                    up
FastEthernet0/1    unassigned      YES unset  administratively down down
Serial0/0          100.1.1.1       YES manual up                    up
Serial0/1          unassigned      YES unset  administratively down down
```

```
R-1(config)# ip route 0.0.0.0 0.0.0.0 100.1.1.2
```

```
ISP# show ip interface brief
Interface          IP-Address      OK? Method Status                Protocol
FastEthernet0/0    200.1.1.100     YES manual up                    up
FastEthernet0/1    unassigned      YES unset  administratively down down
Serial0/0          100.1.1.2       YES manual up                    up
Serial0/1          unassigned      YES manual administratively down down
```

```
ISP#configure terminal
ISP(config)# ip route 0.0.0.0 0.0.0.0 100.1.1.1
```

- Configure static NAT

```
R-1(config)#ip nat inside source static 192.168.1.1 50.1.1.1
R-1(config)#ip nat inside source static 192.168.1.2 50.1.1.2
R-1(config)#ip nat inside source static 192.168.1.3 50.1.1.3
```

- Implementation

```
R-1(config)#interface fastEthernet 0/0
R-1(config-if)#ip nat inside
R-1(config-if)#exit (interface facing towards LAN)
R-1(config)#interface serial 0/0
R-1(config-if)#ip nat outside (interface facing towards ISP )
```

- Generate Traffic from PC (192.168.1.1 / 192.168.1.2 / 192.168.1.3)

```
PC> ipconfig
IP Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100
```

```
PC> ping 200.1.1.1
Pinging 200.1.1.1 with 32 bytes of data:
Reply from 200.1.1.1: bytes=32 time=12ms TTL=126
Reply from 200.1.1.1: bytes=32 time=12ms TTL=126
Reply from 200.1.1.1: bytes=32 time=10ms TTL=126
Reply from 200.1.1.1: bytes=32 time=20ms TTL=126
```

```
PC> ping 200.1.1.2
Pinging 200.1.1.2 with 32 bytes of data:
Request timed out.
Reply from 200.1.1.2: bytes=32 time=16ms TTL=126
Reply from 200.1.1.2: bytes=32 time=11ms TTL=126
Reply from 200.1.1.2: bytes=32 time=32ms TTL=126
```

```
PC> ipconfig
IP Address.....: 192.168.1.2
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100
```

```
PC> ping 200.1.1.1
Pinging 200.1.1.1 with 32 bytes of data:
Reply from 200.1.1.1: bytes=32 time=25ms TTL=126
Reply from 200.1.1.1: bytes=32 time=11ms TTL=126
Reply from 200.1.1.1: bytes=32 time=21ms TTL=126
Reply from 200.1.1.1: bytes=32 time=22ms TTL=126
```

```
SERVER> ipconfig
IP Address.....: 192.168.1.3
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100
```

```
SERVER> ping 200.1.1.1
Pinging 200.1.1.1 with 32 bytes of data:
Reply from 200.1.1.1: bytes=32 time=24ms TTL=126
Reply from 200.1.1.1: bytes=32 time=16ms TTL=126
Reply from 200.1.1.1: bytes=32 time=10ms TTL=126
Reply from 200.1.1.1: bytes=32 time=20ms TTL=126
```

```
R-1# show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global

icmp 50.1.1.1:21       192.168.1.1:21     200.1.1.2:21       200.1.1.2:21
icmp 50.1.1.1:22       192.168.1.1:22     200.1.1.2:22       200.1.1.2:22
icmp 50.1.1.1:23       192.168.1.1:23     200.1.1.2:23       200.1.1.2:23
icmp 50.1.1.1:24       192.168.1.1:24     200.1.1.2:24       200.1.1.2:24

icmp 50.1.1.2:1        192.168.1.2:1      200.1.1.1:1        200.1.1.1:1
icmp 50.1.1.2:2        192.168.1.2:2      200.1.1.1:2        200.1.1.1:2
icmp 50.1.1.2:3        192.168.1.2:3      200.1.1.1:3        200.1.1.1:3
icmp 50.1.1.2:4        192.168.1.2:4      200.1.1.1:4        200.1.1.1:4

icmp 50.1.1.3:1        192.168.1.3:1      200.1.1.1:1        200.1.1.1:1
icmp 50.1.1.3:2        192.168.1.3:2      200.1.1.1:2        200.1.1.1:2
icmp 50.1.1.3:3        192.168.1.3:3      200.1.1.1:3        200.1.1.1:3
icmp 50.1.1.3:4        192.168.1.3:4      200.1.1.1:4        200.1.1.1:4

---  50.1.1.1          192.168.1.1        ---                ---
---  50.1.1.2          192.168.1.2        ---                ---
---  50.1.1.3          192.168.1.3        ---                ---
```

- To verify generate telnet traffic From PC //192.168.1.1 // 192.168.1.2 // 192.168.1.3

```
PC> telnet 100.1.1.2
Trying 100.1.1.2 ...Open
User Access Verification
Password:
```

```
R-1# show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  50.1.1.1          192.168.1.1        ---                ---
---  50.1.1.2          192.168.1.2        ---                ---
---  50.1.1.3          192.168.1.3        ---                ---
tcp 50.1.1.1:1025      192.168.1.1:1025   100.1.1.2:23       100.1.1.2:23
tcp 50.1.1.2:1025      192.168.1.2:1025   100.1.1.2:23       100.1.1.2:23
tcp 50.1.1.3:1025      192.168.1.3:1025   100.1.1.2:23       100.1.1.2:23
```

13.5 LAB: Implement Dynamic NAT

- Ensure that the inside LAN users (192.168.1.0/24) get translated to public IP with the range of 50.1.1.1 – 50.1.1.200/24
- Continue with the same pre-configurations in the previous lab
- Remove the static NAT configurations.
- Implementation is same as previous lab

```
R-1#clear ip nat translation *
```

NOTE: *Make sure that you clear the translation table before you edit or remove the any NAT configurations*

```
R-1(config)# no ip nat inside source static   192.168.1.1   50.1.1.1
R-1(config)# no ip nat inside source static   192.168.1.2   50.1.1.2
R-1(config)# no ip nat inside source static   192.168.1.3   50.1.1.3
```

- Configure Dynamic NAT

```
R-1(config)#access-list 55 permit 192.168.1.0 0.0.0.255
R-1(config)#ip nat pool CCNA 50.1.1.1 50.1.1.200 netmask 255.255.255.0
R-1(config)#ip nat inside source list 55 pool CCNA
```

- Implementation

```
R-1(config)#interface fastEthernet 0/0
R-1(config-if)#ip nat inside
R-1(config-if)#exit (interface facing towards LAN)
R-1(config)#interface serial 0/0
R-1(config-if)#ip nat outside (Interface facing towards ISP)
```

- Verification: Generate some telnet traffic from inside LAN devices (192.168.1.1 //192.168.1.2 //192.168.1.3 //192.168.1.4//)

```
PC> telnet   100.1.1.2
Trying 100.1.1.2 ...Open
User Access Verification
Password:
ISP>
```

```
R-1# show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 50.1.1.1:1027      192.168.1.1:1027   100.1.1.2:23       100.1.1.2:23
tcp 50.1.1.2:1025      192.168.1.2:1025   100.1.1.2:23       100.1.1.2:23
tcp 50.1.1.3:1025      192.168.1.3:1025   100.1.1.2:23       100.1.1.2:23
tcp 50.1.1.4:1025      192.168.1.4:1025   100.1.1.2:23       100.1.1.2:23
```

13.6 LAB: Implement PAT (Dynamic NAT Overload)

- Ensure that the inside LAN users (192.168.1.0/24) get translated to single public IP (50.1.1.1/29) given by service provider
- Continue with the same pre-configurations in the previous lab
- Remove the static NAT configurations
- Implementation is same as previous lab

```
R-1#clear ip nat translation *
```

NOTE: *Make sure that you clear the translation table before you edit or remove the any NAT configurations*

```
R-1(config)#no ip nat inside source list 55 pool CCNA
R-1(config)#no ip nat pool CCNA 50.1.1.1 50.1.1.200 netmask 255.255.255.0
R-1(config)#no access-list 55
```

- Configure PAT

```
R-1(config)#access-list 55 permit 192.168.1.0 0.0.0.255
R-1(config)#ip nat pool CCNA 50.1.1.1  50.1.1.1 netmask 255.255.255.248
R-1(config)#ip nat inside source list 55 pool CCNA overload
```

- Implementation

```
R-1(config)#interface fastEthernet 0/0
R-1(config-if)#ip nat inside
R-1(config-if)#exit (interface facing towards LAN)
R-1(config)#interface serial 0/0
R-1(config-if)#ip nat outside (Interface facing towards ISP)
```

- Verification: Generate some telnet traffic from inside LAN devices (192.168.1.1 //192.168.1.2 //192.168.1.3 //192.168.1.4//)

```
PC> telnet   100.1.1.2
Trying 100.1.1.2 ...Open
User Access Verification
Password:
ISP>
```

```
R-1# show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 50.1.1.1:1027      192.168.1.1:1027   100.1.1.2:23       100.1.1.2:23
tcp 50.1.1.2:1025      192.168.1.2:1025   100.1.1.2:23       100.1.1.2:23
tcp 50.1.1.3:1025      192.168.1.3:1025   100.1.1.2:23       100.1.1.2:23
tcp 50.1.1.4:1025      192.168.1.4:1025   100.1.1.2:23       100.1.1.2:23
```

13.7 LAB: Implement PAT (Dynamic NAT Overload)

- Ensure that the inside LAN users (192.168.1.0/24) get translated to the public IP used on the outside interface (100.1.1.1) given by service provider.
- Continue with the same pre-configurations in the previous lab
- Remove the PAT configurations.
- Implementation is same as previous lab

```
R-1#clear ip nat translation *
```

NOTE: *Make sure that you clear the translation table before you edit or remove the any NAT configurations*

```
R-1(config)#no ip nat inside source list 55 pool CCNA
R-1(config)#no ip nat pool CCNA 50.1.1.1 50.1.1.200 netmask 255.255.255.0
R-1(config)#no access-list 55
```

- Configure PAT

```
R-1(config)#access-list 55 permit 192.168.1.0 0.0.0.255
R-1(config)#ip nat inside source interface serial 0/0 overload
```

- Implementation

```
R-1(config)#interface fastEthernet 0/0
R-1(config-if)#ip nat inside
R-1(config-if)#exit (interface facing towards LAN)
R-1(config)#interface serial 0/0
R-1(config-if)#ip nat outside (Interface facing towards ISP)
```

- Verification: Generate some telnet traffic from inside LAN devices (192.168.1.1 //192.168.1.2 //192.168.1.3 //192.168.1.4//)

```
PC> telnet   100.1.1.2
Trying 100.1.1.2 ...Open
User Access Verification
Password:
ISP>
```

```
R-1# show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 50.1.1.1:1027      192.168.1.1:1027   100.1.1.2:23       100.1.1.2:23
tcp 50.1.1.2:1025      192.168.1.2:1025   100.1.1.2:23       100.1.1.2:23
tcp 50.1.1.3:1025      192.168.1.3:1025   100.1.1.2:23       100.1.1.2:23
tcp 50.1.1.4:1025      192.168.1.4:1025   100.1.1.2:23       100.1.1.2:23
```

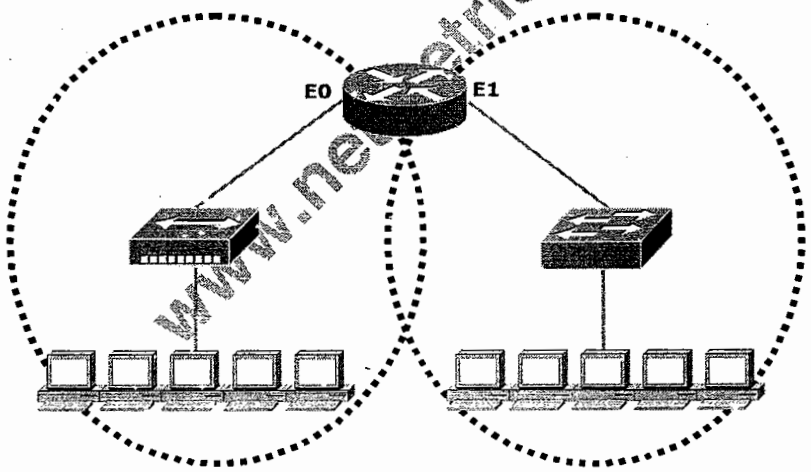
14. Basic Switching

14.1 Difference between Hub and Switch

Hub	Switch
Physical layer device (Layer 1)	Datalink layer device (Layer 2)
Has no intelligence	An Intelligent device
Works with 0's and 1's (Bits)	Works with Physical address (MAC address)
Always do broadcasts	Uses broadcast and unicast
Works with shared bandwidth	Works with fixed bandwidth
Has one broadcast domain	Has one broadcast domain
Has one collision domain	Number of Collision domains depends upon the number of ports
Collisions are identified using access methods called CSMA/CD & CSMA/CA	Maintains a MAC address table

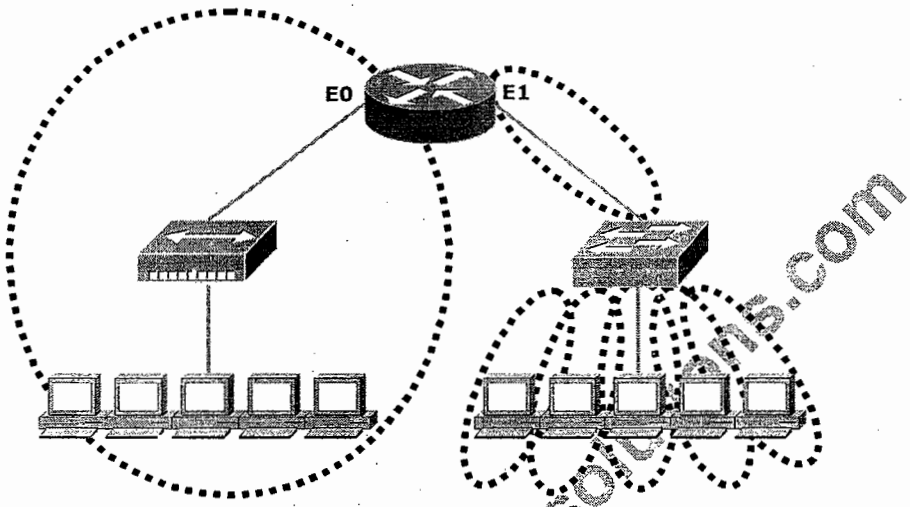
14.2 Broadcast Domain

- Set of devices that receive broadcast frames originating from any device within the set



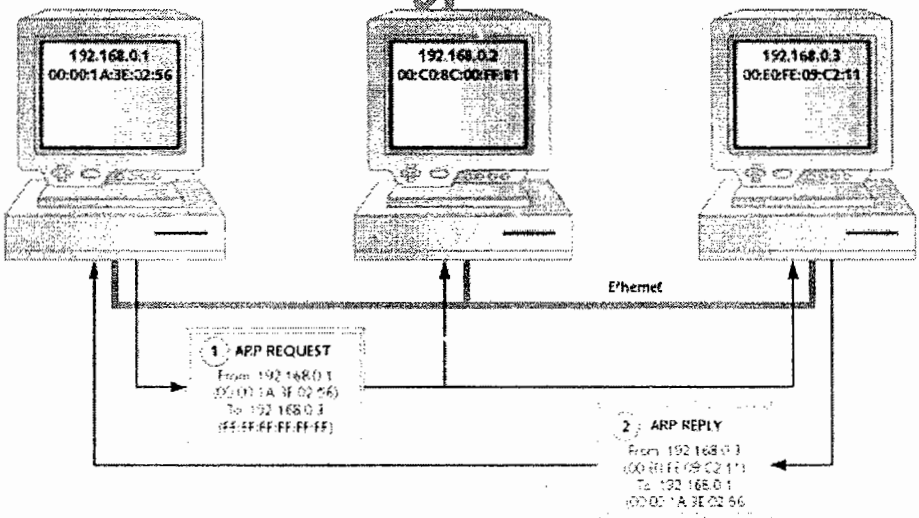
14.3 Collision domain

- In Ethernet, the network area within which frames that have collided are propagated is called a collision domain
- A collision domain is a network segment with two or more devices sharing the same bandwidth



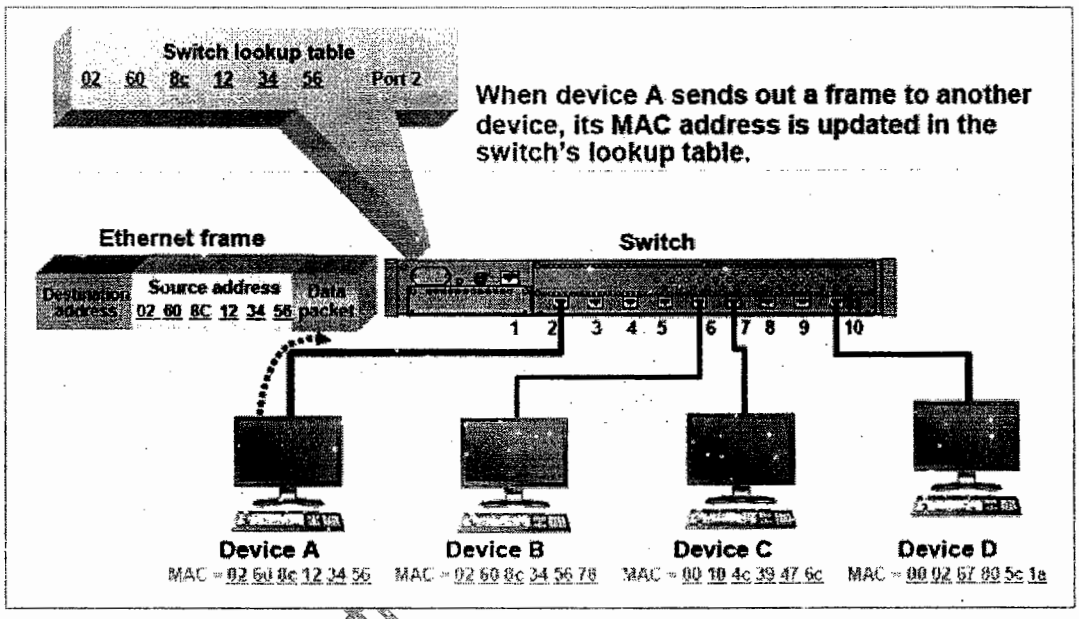
14.4 ARP – Address Resolution Protocol

- ARP helps the switch to resolve the IP address in to respective MAC address.
- It is an inbuilt protocol in TCP/IP

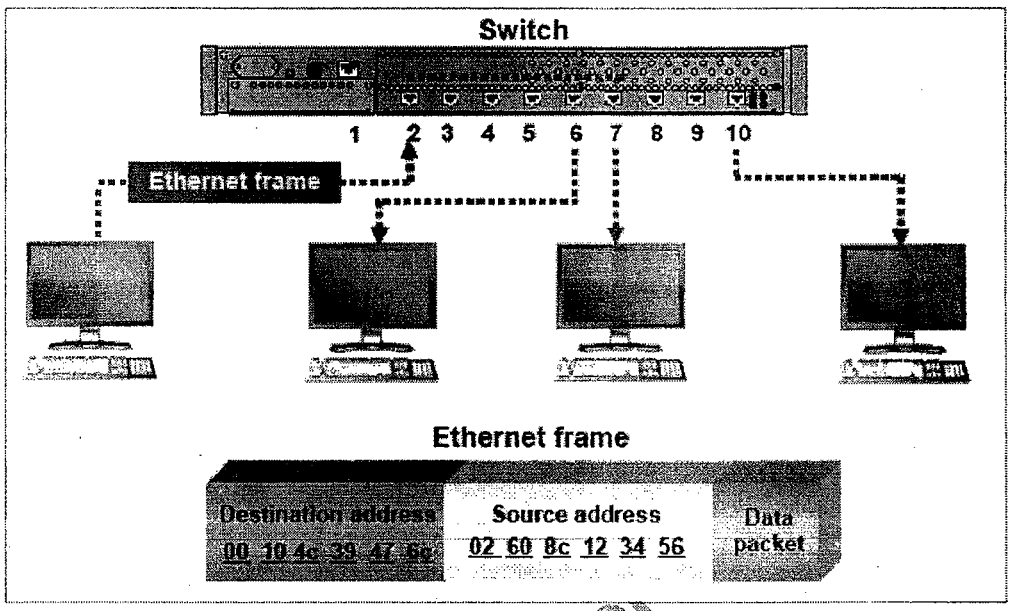


14.5 How do Switches Work?

- After taking a switch out the box, plugging it in, and connecting devices to it, the switch goes through the following processes:
- Learning process:
  - A switch begins learning the local MAC addresses as soon as it is connected to other devices or to a network.
  - This learning capability makes switches easy to use on a network.

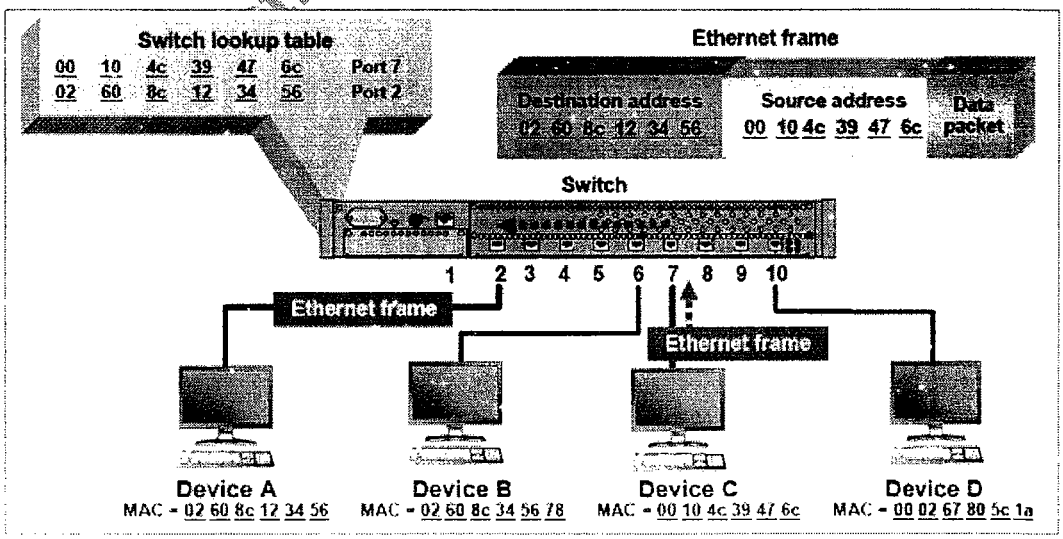


- The switch learning process works like this:
  - As a PC or other networked device sends a frame to another device through the switch, the switch captures the source MAC address of the frame and the interface that received it.
  - The switch confirms or adds the MAC address and the port to the lookup table.
  - A switch also keeps a timer for each of the MAC address entries in its lookup table.
  - By default, many vendors set this time to hold an address entry to 300 seconds (5 minutes) of the traffic inactivity with that Mac-address
  - This can be changed if you want. The timer lets the switch get rid of old entries to keep the lookup process short and fast.
- Learning Flooding:
  - As part of the learning process, a switch will flood the single frame out all of its other ports when it cannot find the destination MAC address in the switch's lookup table.



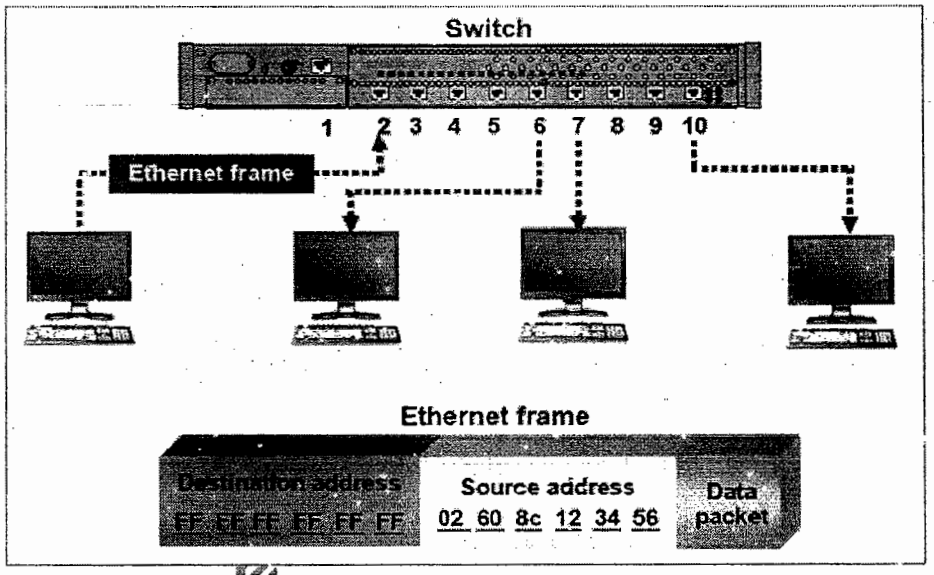
- This flooding process is necessary network overhead. One challenge is that any user at another system attached to the flooding switch that is running a protocol analyzer can see the flooded frame.

- Forwarding and Filtering processes:
  - When a switch has learned the locations of the devices connected to it, the switch is ready to either forward or filter frames based on the destination MAC address of the frame and the contents of the switch lookup table.



  - The switch has already found the port of device A by its MAC address 02 60 8c 12 34 56 and switch port number 2.

- The switch recognizes device C with a MAC address 00 10 4c 39 47 6c when it replies to port 7 on the switch.
- The switch will receive the incoming frame, examine the destination address of the Ethernet frame, and check its lookup table.
- The switch will then make a decision to forward the frame out port 2, and only port 2.
- The switch filters out (or does not send the frame to) other ports on the switch since they do not have the target MAC address in the lookup table. That way, no one else can look at the contents of the frame.



NOTE:

- Switches sends broadcasts (flood) frames out of all the ports if it receives a frame with the destination MAC address is not present in the MAC table of switch (sends with destination address FF:FF:FF:FF)
- If the destination MAC address is present then it will be send only on specific port as per Mac-table
- Update of the Mac-table happens based on the source address of the frames

14.6 Switch Types

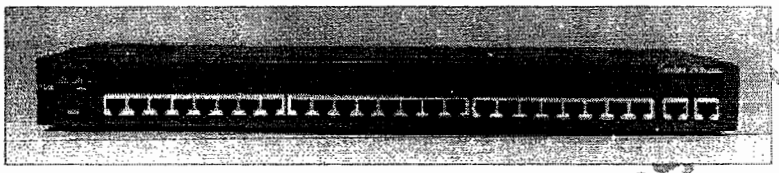
- Unmanageable switches
  - These switches are just plug and play
  - No configurations can be done

- There is no console port.

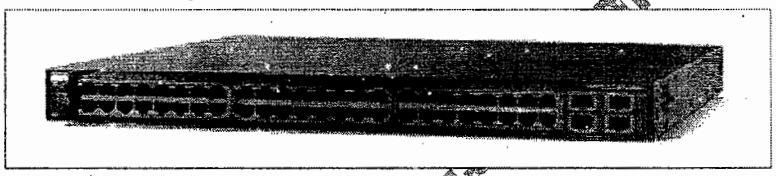
- Manageable switches
  - These switches are also plug and play
  - It has console port and CLI access
  - We can verify and modify configurations and can implement and test some advance switching technologies

14.7 Cisco's Hierarchical Model

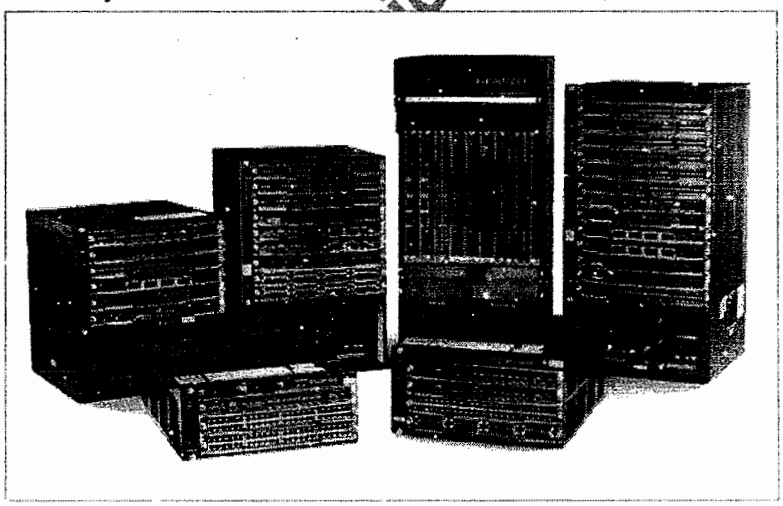
- Cisco divided the Switches into 3 Layers
  - Access Layer Switches - Switches Series: 1900 & 2900



  - Distribution Layer Switches - Switches Series: 3550 , 3560



  - Core Layer Switches - Switches Series : 4500 , 6500



14.8 Switching Modes:

- Store & Forward
  - A Default switching method for distribution layer switches.
  - Latency : High
  - Error Checking : Yes

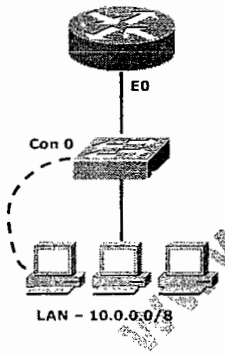
- Fragment Free
  - It is also referred to as Modified Cut-Through
  - A Default Switching method for access layer switches.
  - Latency : Medium
  - Error Checking : On 64 bytes of Frame
- Cut through
  - A Default switching method for the core layer switches
  - Latency : Low
  - Error Checking : No

NOTE:

- *Latency is the total time taken for a Frame to pass through the Switch*
- *Latency depends on the switching mode and the hardware capabilities of the Switc*

14.9 Console Connectivity

- Connect a rollover cable to the Switch console port (RJ-45 connector).
- Connect the other end of the rollover cable to the RJ-45 to DB-9 adapter
- Attach the female DB-9 adapter to a PC Serial Port.
- Open emulation software on the PC.



14.10 Emulation Software

- Windows:
  - Start > Programs > Accessories > Communications > HyperTerminal > HyperTerminal.
  - Give the Connection Name & Select Any Icon
  - Select Serial (Com) Port where Switch is connected
  - In Port Settings > Click on Restore Defaults
- Linux

- # minicom -s

14.11 Initial Configuration of a Switch

- Connect one end of console cable to console port of switch and other end of cable to your computer's COM port.
- Now open hyper terminal and power on the switch.

```
Would you like to enter into initial configuration dialog (yes/no): no

switch>enable
switch#config terminal
```

- To assign telnet Password

```
switch(config)#line vty 0 4
switch(config-line)#password <password>
switch(config-line)#login
```

- To assign Console Password

```
switch(config)#line con 0
switch(config-line)#password <password>
switch(config-line)#login
```

- To assign Enable Password

```
switch(config)#enable secret <password>
          OR
switch(config)#enable password <password>
switch(config)#exit
switch#Show mac-address-table (to see the entries of the MAC table)
switch#Show interface status
```

- To assign IP address to a switch

```
switch(config)#Interface Vlan 1
switch(config-if)#ip address <ip> <mask>
switch(config-if)#no shutdown
```

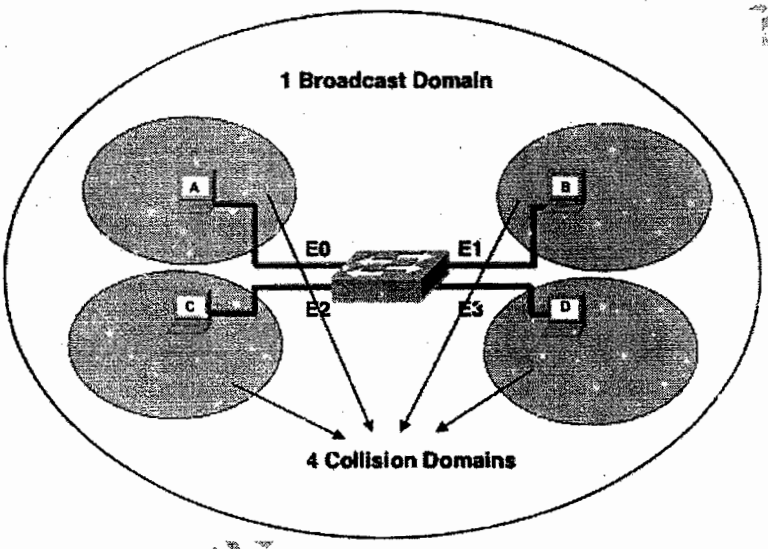
- To assign default gateway to a switch

```
switch(config)#ip default-gateway 192.168.1.100
```

15. Virtual LAN

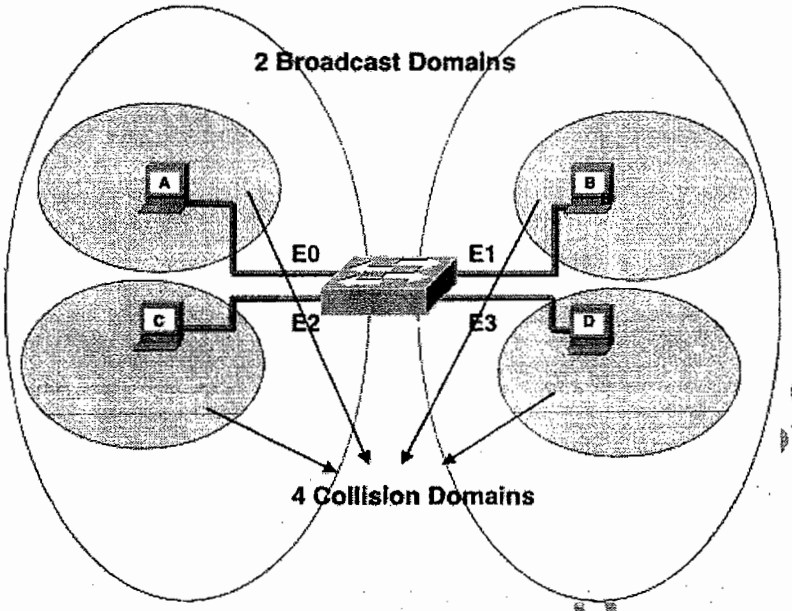
15.1 Overview

- A Layer 2 Security
- Divides a Single Broadcast domain into Multiple Broadcast domains.
- By default all ports of the switch are in VLAN1.
- VLAN1 is known as Administrative VLAN or Management VLAN
- VLAN can be created from 2 – 1001
- Can be Configured on a Manageable switch only
- 2 Types of VLAN Configuration
  - Static VLAN
  - Dynamic VLAN



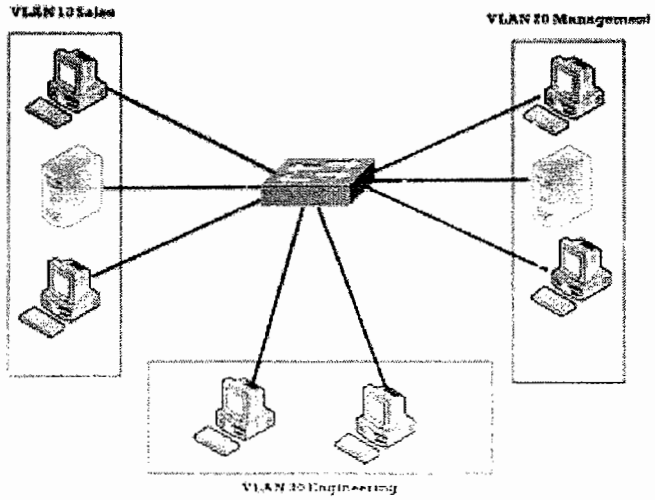
- By default, routers allow broadcasts only within the originating network, but switches forward broadcasts to all segments.
- The reason it's called a flat network is because it's one Broadcast domain, not because its design is physically flat. (Flat Network Structure)
- Network adds, moves, and changes are achieved by configuring a port into the appropriate VLAN.
- A group of users needing high security can be put into a VLAN so that no users outside of the VLAN can communicate with them.
- As a logical grouping of users by function, VLANs can be considered independent from their physical or geographic locations.

- VLANs can enhance network security.
- VLANs increase the number of broadcast domains while decreasing their size.



15.2 Static VLAN

- Static VLAN's are based on port numbers
- Need to manually assign a port on a switch to a VLAN
- Also called Port-Based VLANs
- One port can be a member of only one VLAN



- There are two different ways of creating vlans
- VLAN Creation in config Mode:

```
Switch(config)#vlan <no>
Switch(config-Vlan)#name <name>
Switch(config-Vlan)#Exit
```

  - Assigning ports in Vlan

```
Switch(config)#interface <interface type> <interface no.>
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access Vlan <no>
```

- Static VLAN using Database command:
  - Creation of VLAN

```
Switch#vlan database
Switch(vlan)#vlan  <vlan id>  name <vlan name>
Switch(vlan)#exit
```

  - Assigning port in VLAN:

```
Switch#config terminal
Switch(config)#interface fastethernet <int no>
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan <vlan id>
```

  - Verification

```
Switch#show vlan
```

  - The range command (Assigning multiple ports at same time)
  - The range command, you can use on switches to help you configure multiple ports at the same time

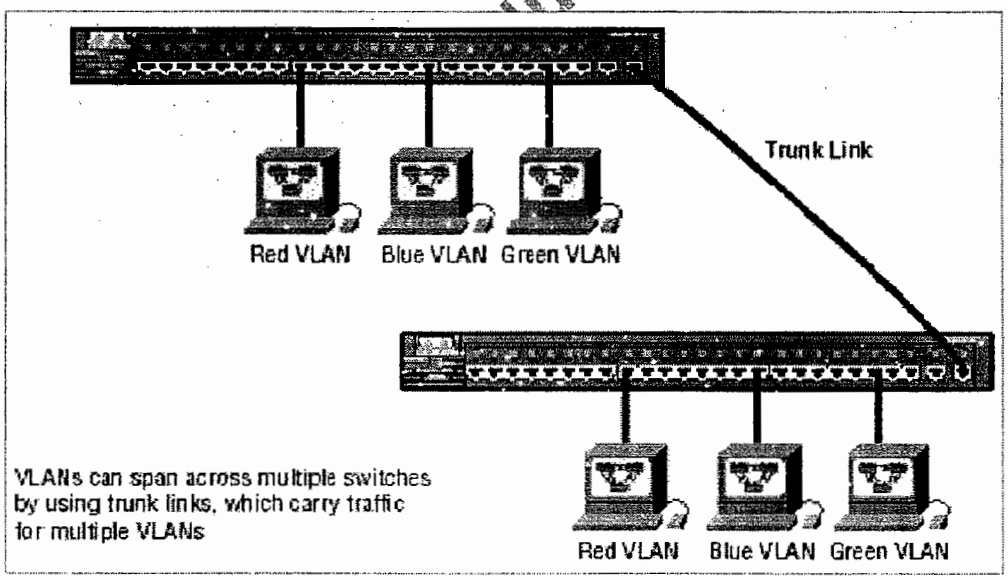
```
Switch(config)#interface range fa0/1-5, fa0/12, fa0/17
```

15.3 Dynamic VLAN

- Dynamic VLAN's are based on the MAC address of a PC
- Switch automatically assigns the port to a VLAN
- Each port can be a member of multiple VLAN's
- For Dynamic VLAN configuration, a software called VMPS (VLAN Membership Policy Server) is needed

15.4 Types of Links/Ports

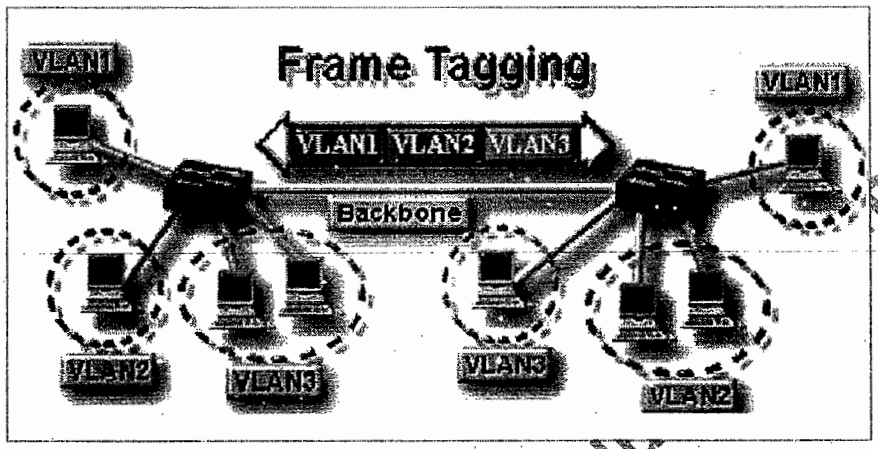
- Access links
  - This type of link is only part of one VLAN, and it's referred to as the native VLAN of the port
  - Any device attached to an access link is unaware of a VLAN membership—the device just assumes it's part of a broadcast domain, but it has no understanding of the physical network
  - Switches remove any VLAN information from the frame before it's sent to an access link device
- Trunk links
  - Trunks can carry multiple VLANs traffic.
  - A trunk link is a 100- or 1000Mbps point-to-point link between two switches, between a switch and router, or between a switch and server. These carry the traffic of multiple VLANs—from1 to 1005 at a time.
  - Trunking allows you to make a single port part of multiple VLANs at the same time.



15.5 VLAN Identification Methods (Frame Tagging)

- Single VLAN can span over multiple switches
- In oder to make sure that same vlan users on different switches communicate with each other there is a method of tagging happens on trunk links
- Tag is added before a frame is send and removed once it is received on trunk link
- Frame tagging happens only on the trunk links

- VLAN identification is what switches use to keep track of all those frames moving through the trunk links
- The below two trunking protocols responsible for frame tagging process
  - Inter-Switch Link (ISL)
  - IEEE 802.1Q

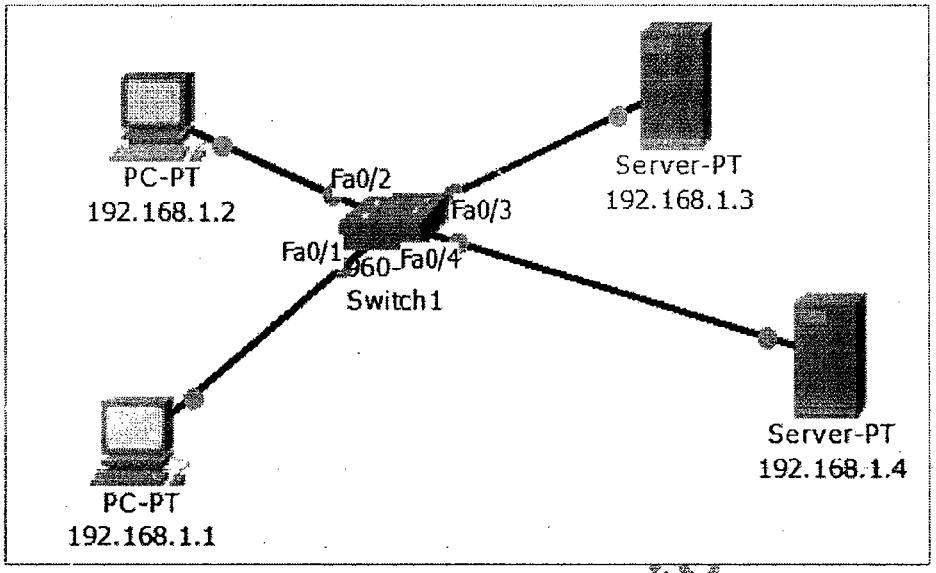


ISL	IEEE 802.1Q
Cisco Proprietary	Open Standard
Works with Ethernet, Token ring, FDDI	Works only on Ethernet
Adds 30 bytes of tag	Only 4 byte tag will be added to the original frame
All VLAN traffic is tagged	Unlike ISL, 802.1q does not encapsulate the frame. It modifies the existing Ethernet frame to include the VLAN ID
Frame is not modified	

- Trunking Configuration

```
Switch(config)#interface <interface type> <interface no.>
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk encapsulation dot1q/ISL
```

15.6 LAB: Implementing VLAN



- Steps
  - Ping between 192.168.1.1 and 192.168.1.3
  - Create VLAN 20
  - Shift port f0/3 , f0/4 in to VLAN 20
  - Ping between 192.168.1.1 and 192.168.1.3

```
Switch# show vlan

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
                                   Gig1/1, Gig1/2
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
```

```
PC> ipconfig
IP Address.....................: 192.168.1.1
Subnet Mask....................: 255.255.255.0
Default Gateway................: 192.168.1.100
```

```
PC> ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=19ms TTL=128
Reply from 192.168.1.2: bytes=32 time=6ms TTL=128
Reply from 192.168.1.2: bytes=32 time=8ms TTL=128
Reply from 192.168.1.2: bytes=32 time=7ms TTL=128
```

```
PC> ping 192.168.1.3
Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=12ms TTL=128
Reply from 192.168.1.3: bytes=32 time=9ms TTL=128
Reply from 192.168.1.3: bytes=32 time=7ms TTL=128
Reply from 192.168.1.3: bytes=32 time=8ms TTL=128
```

```
PC> ping 192.168.1.4
Pinging 192.168.1.4 with 32 bytes of data:
Reply from 192.168.1.4: bytes=32 time=10ms TTL=128
Reply from 192.168.1.4: bytes=32 time=8ms TTL=128
Reply from 192.168.1.4: bytes=32 time=8ms TTL=128
Reply from 192.168.1.4: bytes=32 time=9ms TTL=128
```

- Create Vlan 20 And Shift The Ports 3 And 4 In To Vlan 20

```
Switch(config)#vlan 20
Switch(config-vlan)#name SALES
Switch(config-vlan)#exit

Switch(config)#interface fastEthernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit

Switch(config)#interface fastEthernet 0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
```

```
Switch#show vlan

VLAN Name                 Status    Ports
---- -------------------- --------- -------------------------------
1    default              active    Fa0/1, Fa0/2, 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, Gig1/1, Gig1/2
20   SALES                active    Fa0/3, Fa0/4
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
```

```
PC> ipconfig
IP Address.....................: 192.168.1.1
Subnet Mask....................: 255.255.255.0
Default Gateway................: 192.168.1.100
```

```
PC> ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=19ms TTL=128
Reply from 192.168.1.2: bytes=32 time=6ms TTL=128
Reply from 192.168.1.2: bytes=32 time=8ms TTL=128
Reply from 192.168.1.2: bytes=32 time=7ms TTL=128
```

```
PC> ping 192.168.1.3
Pinging 192.168.1.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

```
PC> ping 192.168.1.4
Pinging 192.168.1.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

15.7 LAB: Creating Basic VLAN Configuration on Switches

```
Switch(config)#vlan 10
Switch(config-vlan)#name sales

Switch(config-vlan)#vlan 20
Switch(config-vlan)#name marketing

Switch(config-vlan)#vlan 30
Switch(config-vlan)#vlan 40

Switch(config-vlan)#end
```

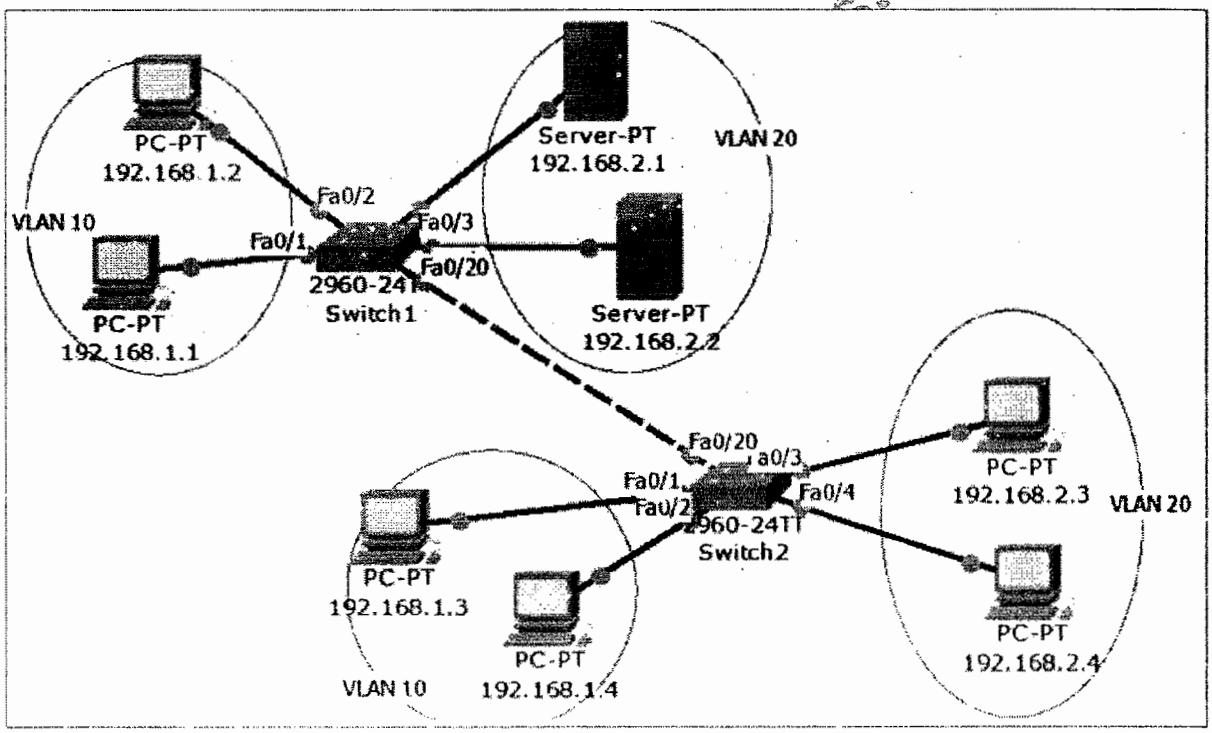
```
Switch#show vlan
VLAN Name                 Status    Ports
---- -------------------- --------- -------------------------------
1    default              active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                    Fa0/9, Fa0/10, 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
                                    Gig1/1, Gig1/2
10   sales                active
20   marketing            active
30   VLAN0030             active
40   VLAN0040             active
```

- Task:
  - Configure port fa0/8 into vlan 10
  - Configure multiple ports (4 – 7 and 10) into vlan 20

```
Switch(config)#interface f0/8
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit

Switch(config)#interface range f0/4 - 7 , f0/10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
```

```
Switch# show vlan

VLAN Name                Status    Ports
---- ------------------- --------- -------------------------------
1    default             active    Fa0/1, Fa0/2, Fa0/3,
                                   Fa0/9, 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
10   sales               active    Fa0/8
20   marketing           active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                   Fa0/10
```

15.8 LAB: VLAN Trunking



- On Switch 1

```
Switch(config)#hostname SW-1
SW-1(config)#interface range f0/1 - 2
SW-1(config-if-range)#switchport mode access
SW-1(config-if-range)#switchport access vlan 10
% Access VLAN does not exist. Creating vlan 10
SW-1(config-if-range)#exit
SW-1(config)#interface range f0/3 - 4
SW-1(config-if-range)#switchport mode access
SW-1(config-if-range)#switchport access vlan 20
SW-1(config-if-range)#end
```

```
SW-1#show vlan

VLAN Name                    Status    Ports
---- --------------------- --------- -------------------------------
1    default                 active    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
                                       Gig1/1, Gig1/2
10   VLAN0010                active    Fa0/1, Fa0/2
20   VLAN0020                active    Fa0/3, Fa0/4
1002 fddi-default            act/unsup
1003 token-ring-default      act/unsup
1004 fddinet-default         act/unsup
1005 trnet-default           act/unsup
```

- On Switch 2

```
Switch(config)#hostname SW-2
SW-2(config)#interface range f0/1 - 2
SW-2(config-if-range)#switchport mode access
SW-2(config-if-range)#switchport access vlan 10
% Access VLAN does not exist. Creating vlan 10
SW-2(config-if-range)#exit
SW-2(config)#interface range f0/3 - 4
SW-2(config-if-range)#switchport mode access
SW-2(config-if-range)#switchport access vlan 20
```

```
SW-2#show vlan

VLAN Name                Status    Ports
---- ------------------- --------- -------------------------------
1    default             active    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
                                   Gig1/1, Gig1/2
10   VLAN0010            active    Fa0/1, Fa0/2
20   VLAN0020            active    Fa0/3, Fa0/4
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
```

```
PC> ipconfig
IP Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100
```

```
PC> ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=19ms TTL=128
Reply from 192.168.1.2: bytes=32 time=6ms TTL=128
Reply from 192.168.1.2: bytes=32 time=8ms TTL=128
Reply from 192.168.1.2: bytes=32 time=7ms TTL=128
```

```
PC> ping 192.168.1.3
Pinging 192.168.1.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

```
PC> ping 192.168.1.4
Pinging 192.168.1.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

```
Server> ipconfig
IP Address.....................: 192.168.2.1
Subnet Mask....................: 255.255.255.0
Default Gateway................: 192.168.2.100
```

```
Server> ping 192.168.2.2
Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=17ms TTL=128
Reply from 192.168.2.2: bytes=32 time=7ms TTL=128
Reply from 192.168.2.2: bytes=32 time=9ms TTL=128
Reply from 192.168.2.2: bytes=32 time=8ms TTL=128
```

```
Server> ping 192.168.2.3
Pinging 192.168.2.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

```
Server> ping 192.168.2.4
Pinging 192.168.2.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

NOTE:

- From the above verification we can see that same vlan users on different switches are not able to communicate
- To communicate, there should be trunking configured on link between the switches

- To configure trunking

```
SW-1(config)#interface fastEthernet 0/20
SW-1(config-if)#switchport mode trunk
SW-1(config-if)#switchport trunk encapsulation dot1q
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/20, changed
state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/20, changed
state to up
SW-2(config)#interface f0/20
SW-2(config-if)#switchport mode trunk
SW-2(config-if)#switchport trunk encapsulation dot1q
% Access VLAN does not exist. Creating vlan 20
SW-2(config-if-range)#end
```

```
SW-1# show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/20      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/20      1-1005

Port        Vlans allowed and active in management domain
Fa0/20      1,10,20

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/20      1,10,20
```

```
SW-2# show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/20      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/20      1-1005

Port        Vlans allowed and active in management domain
Fa0/20      1,10,20

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/20      1,10,20
```

```
PC> ipconfig
IP Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100
```

```
PC> ping 192.168.1.3
Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=17ms TTL=128
Reply from 192.168.1.3: bytes=32 time=13ms TTL=128
Reply from 192.168.1.3: bytes=32 time=12ms TTL=128
Reply from 192.168.1.3: bytes=32 time=10ms TTL=128
```

```
PC> ping 192.168.1.4
Pinging 192.168.1.4 with 32 bytes of data:
Reply from 192.168.1.4: bytes=32 time=25ms TTL=128
Reply from 192.168.1.4: bytes=32 time=14ms TTL=128
Reply from 192.168.1.4: bytes=32 time=12ms TTL=128
Reply from 192.168.1.4: bytes=32 time=13ms TTL=128
```

```
Server> ipconfig
IP Address.....: 192.168.2.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.2.100
```

```
Server> ping 192.168.2.3
Pinging 192.168.2.3 with 32 bytes of data:
Reply from 192.168.2.3: bytes=32 time=13ms TTL=128
Reply from 192.168.2.3: bytes=32 time=12ms TTL=128
Reply from 192.168.2.3: bytes=32 time=13ms TTL=128
Reply from 192.168.2.3: bytes=32 time=13ms TTL=128
```

```
Server> ping 192.168.2.4
Pinging 192.168.2.4 with 32 bytes of data:
Reply from 192.168.2.4: bytes=32 time=26ms TTL=128
Reply from 192.168.2.4: bytes=32 time=12ms TTL=128
Reply from 192.168.2.4: bytes=32 time=12ms TTL=128
Reply from 192.168.2.4: bytes=32 time=13ms TTL=128
```

- TASK:
  - Configure the trunk link such that it only allows Vlan 10, 20, 30, 40
  - Traffic should only be allowed (No other Vlan traffic should be sent)
- On both switches (SW1/SW2)

```
SW-x(config)#interface f0/20
SW-x(config-if)#switchport trunk allowed vlan ?

WORD    VLAN IDs of the allowed VLANs when this port is in trunking mode
add     add VLANs to the current list
all     all VLANs
except  all VLANs except the following
none    no VLANs
remove  remove VLANs from the current list

SW-x(config-if)#switchport trunk allowed vlan 10,20,30,40
```

```
SW-1#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/20      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/20      10,20,30,40

Port        Vlans allowed and active in management domain
Fa0/20      10,20

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/20      10,20
```

```
SW-2#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/20      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/20      10,20,30,40

Port        Vlans allowed and active in management domain
Fa0/20      10,20

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/20      10,20
```

- TASK:
  - Create vlan 50, 60, 70, 80 on both switches
  - Configure the trunk link f0/20 to add vlan 50, 60, 70, 80 to the existing trunk allowed list
- On both switches (SW1/SW2)

```
SW-x(config)#vlan 50
SW-x(config-vlan)#vlan 60
SW-x(config-vlan)#vlan 70
SW-x(config-vlan)#vlan 80
SW-x(config-vlan)#end

SW-x(config-if)#switchport trunk allowed vlan add 50,60,70,80
```

```
SW-1#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/20      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/20      10,20,30,40,50,60,70,80

Port        Vlans allowed and active in management domain
Fa0/20      10,20,50,60

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/20      10,20,50,60
```

```
SW-2#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/20      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/20      10,20,30,40,50,60,70,80

Port        Vlans allowed and active in management domain
Fa0/20      10,20,50,60

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/20      10,20,50,60
```

- TASK: Configure the trunk link f0/20 to remove vlan 70, 80 to the existing trunk allowed list

```
SW-1(config)#interface f0/20
SW-1(config-if)#switchport trunk allowed vlan remove 70,80
```

```
SW-1#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/20      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/20      10,20,30,40,50,60

Port        Vlans allowed and active in management domain
Fa0/20      10,20,50,60

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/20      10,20,50,60
```

```
SW-2#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/20      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/20      10,20,30,40,50,60

Port        Vlans allowed and active in management domain
Fa0/20      10,20,50,60

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/20      10,20,50,60
```

16. VLAN Trunking Protocol

16.1 Overview

- VTP is a Cisco Proprietary protocol
- Used to share the VLAN configurations with multiple switches and to maintain consistency throughout that network.
- Information will be passed only if switches connected with FastEthernet or higher ports.
- VTP allows an administrator to add, delete, and rename VLANs-information that is then propagated to all other switches in the VTP domain.
- For VTP to work, switches should be configured with the same Domain name. Domain names are not case sensitive.

16.2 VTP Modes

- Server Mode
  - Switch configured in server-mode can add, modify and delete VLAN's
  - A default VTP mode for all switches
- Client Mode
  - Switch configured in client-mode cannot add, modify and delete VLAN configurations
  - Doesn't store its VLAN configuration information in the NVRAM. Instead learns it from the server every time it boots up
- Transparent Mode
  - Switch configured in a transparent mode can add, modify and delete VLAN configurations.
  - Changes in one transparent switch will not affect any other switch

16.3 Benefits of VTP

- Consistent VLAN configuration across all switches in the network
- Accurate tracking and monitoring of VLANs
- Dynamic reporting of added VLANs to all switches in the VTP domain
- Plug-and-Play VLAN adding

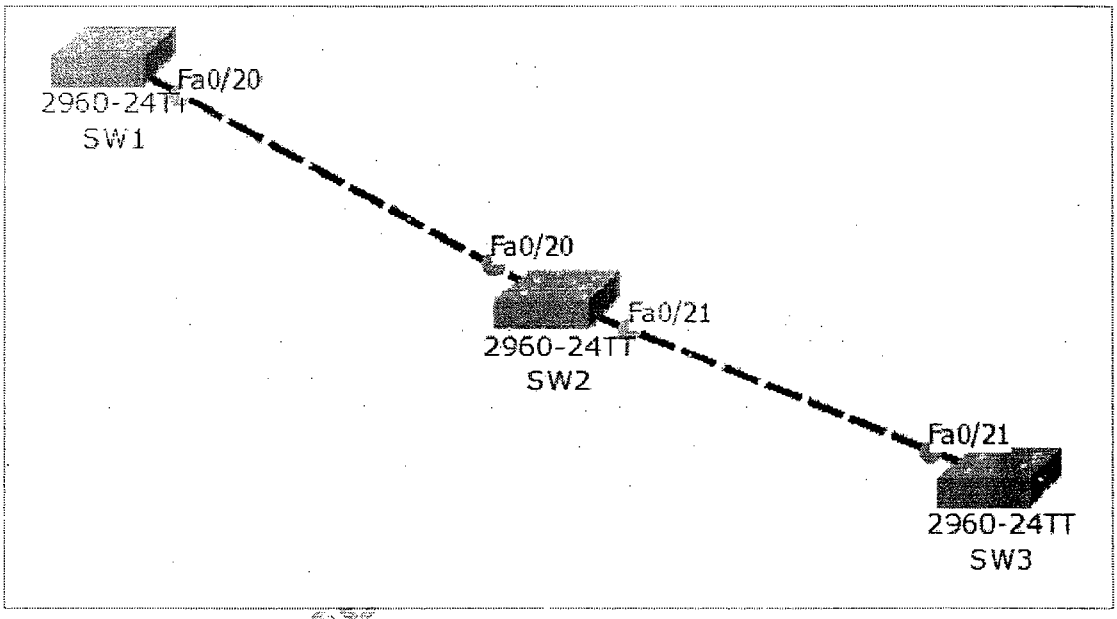
16.4 VTP Configuration in Config Mode

```
Switch(config)# VTP Domain <Name>
Switch(config)# VTP Password <password>
Switch(config)# VTP version 2
Switch(config)# VTP Mode <server/client/transparent>
```

16.5 VTP Configuration in Database Mode

```
Switch# VLAN Database
Switch(VLAN)# VTP Domain <Name>
Switch(VLAN)# VTP Password <password>
Switch(VLAN)# VTP version 2
Switch(VLAN)# VTP Mode <server/client/transparent>
```

16.6 LAB: VTP



- Trunking has to be enabled (vtp advertisements are send only on trunk ports)
- Configure VTP on all switches
- Create vlans on server and verify on client and transparent switch
- Create vlans on transparent switch and verify on client and server

NOTE: *Domain name (case-sensitive) / password / version must match in order for VTP to work*

```
SW1#show vtp status
SW1#show vtp password
VTP Password: cisco123
```

- Task 1:
  - Trunking has to be enabled on SW1 (Server), SW2 (Transparent) & SW3 (Client)
  - VTP advertisements are send only on trunk ports

```
SW-1(config)#interface fastEthernet 0/20
SW-1(config-if)#switchport mode trunk
SW-1(config-if)#switchport trunk encapsulation dot1q
```

```
SW-2(config)#interface range fastEthernet 0/20 - 21
SW-2(config-if)#switchport mode trunk
SW-2(config-if)#switchport trunk encapsulation dot1q
```

```
SW-3(config)#interface fastEthernet 0/21
SW-3(config-if)#switchport mode trunk
SW-3(config-if)#switchport trunk encapsulation dot1q
```

```
SW1# show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/20      on           802.1q         trunking      1
```

- Task 2: Configure VTP on all switches

```
SW-1(config)# vtp domain CCNP
SW-1(config)# vtp password cisco
SW-1(config)# vtp mode server
SW-1(config)# vtp version 2
SW-1(config)# exit
```

```
SW-2(config)# vtp domain CCNP
SW-2(config)# vtp password cisco
SW-2(config)# vtp mode transparent
SW-2(config)# vtp version 2
SW-2(config)# exit
```

```
SW-3(config)# vtp domain CCNP
SW-3(config)# vtp password cisco
SW-3(config)# vtp version 2
SW-3(config)# vtp mode client
SW-3(config)# exit
```

```
SW1# show vtp status
VTP Version                     : 2
Configuration Revision          : 2
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x86 0x22 0x83 0x8E 0x23 0xA8 0x06 0xCC
Configuration last modified by 0.0.0.0 at 3-1-93 00:07:33
Local updater ID is 0.0.0.0 (no valid interface found
```

```
SW-1#show vtp  password
VTP Password: cisco
```

```
SW-3# show vtp status
VTP Version                     : 2
Configuration Revision          : 2
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x86 0x22 0x83 0x8E 0x23 0xA8 0x06 0xCC
Configuration last modified by 0.0.0.0 at 3-1-93 00:07
```

```
SW-2# show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/20      on           802.1q         trunking      1
Fa0/21      on           802.1q         trunking      1
```

```
SW-3# show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/21      on           802.1q         trunking      1
```

- Task 3: Create vlans on server and verify on client and transparent switch

```
SW-1(config)# vlan 10
SW-1(config)# vlan 20
SW-1(config)# vlan 30
SW-1(config)# vlan 40
SW-1(config-vlan)# name sales
SW-1(config)#vlan 50
SW-1(config-vlan)#name marketing
```

```
SW-1# show vlan
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, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig1/1
                                                Gig1/2
10   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active
40   sales                            active
50   marketing                        active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

```
Sw-3# show vlan
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
                                                Fa0/22, Fa0/23, Fa0/24, Gig1/1
                                                Gig1/2
10   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active
40   sales                            active
50   marketing                        active
```

```
SW-2# show vlan
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, Fa0/22
                                       Fa0/23, Fa0/24, Gig1/1, Gig1/2
1002 fddi-default            act/unsup
1003 token-ring-default      act/unsup
1004 fddinet-default         act/unsup
1005 trnet-default           act/unsup
```

NOTE: *You don't see any vlan on the transparent switch as the transparent switch will not synchronize the vlan information*

- Task 4: Create vlans on transparent switch and verify on client and server

```
Sw-2(config)#vlan 100
Sw-2(config-vlan)#vlan 200
Sw-2(config-vlan)#vlan 300
Sw-2(config-vlan)#end
```

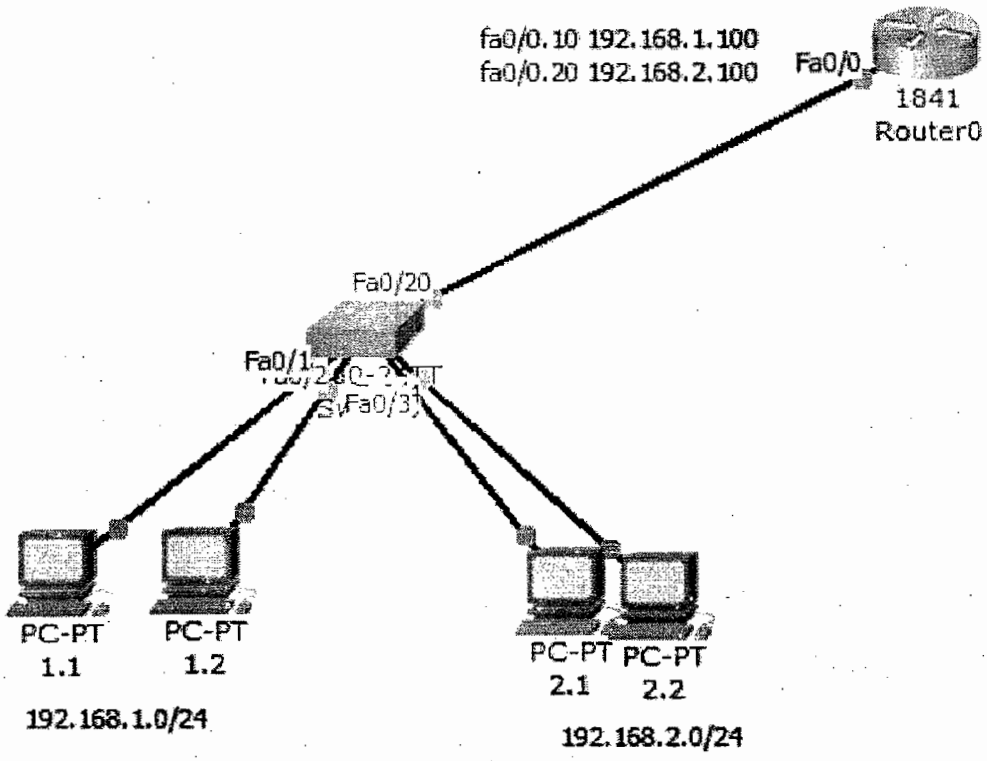
```
SW2# show vlan
VLAN Name                    Status    Ports
---- --------------------- --------- -------------------------------
1    default                 active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                       Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                       Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                       Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                       Fa0/17, Fa0/18, Fa0/19, Fa0/22
                                       Fa0/23, Fa0/24
100  VLAN0100                active
200  VLAN0200                active
300  VLAN0300                active
1002 fddi-default            act/unsup
```

```
Sw1# show vlan
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, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig1/1
                                                Gig1/2
10   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active
40   VLAN0040                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

```
SW3# show vlan

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, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig1/1
                                                Gig1/2
10   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active
40   VLAN0040                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

NOTE: *You don't see any vlan's, which was created on the transparent switch as the transparent switch will not synchronize the vlan information with others*

16.7 LAB: Inter VLAN-Routing using Router



- Steps:
  - Create vlan and shift the ports as per the requirement
  - Configure on switch fa0/20 as trunk port
  - Create sub interfaces on router port fa0/0
  - Verify connectivity between vlans (ping 192.168.1.1 – 192.168.2.1)

- Task 1: Create VLAN and shift the ports

```
Switch(config)#hostname SW-1
SW-1(config)#interface range f0/1 - 2
SW-1(config-if-range)#switchport mode access
SW-1(config-if-range)#switchport access vlan 10
% Access VLAN does not exist. Creating vlan 10
SW-1(config-if-range)#exit
```

```
SW-1(config)#interface range f0/3 - 4
SW-1(config-if-range)#switchport mode access
SW-1(config-if-range)#switchport access vlan 20
SW-1(config-if-range)#end
```

```
SW-1# show vlan
VLAN Name                         Status    Ports
---- ---------------------------- --------- -------------------------------
1    default                      active    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
                                            Gig1/1, Gig1/2
10   VLAN0010                     active    Fa0/1, Fa0/2
20   VLAN0020                     active    Fa0/3, Fa0/4
1002 fddi-default                 act/unsup
1003 token-ring-default           act/unsup
1004 fddinet-default              act/unsup
1005 trnet-default                act/unsup
```

- Task 2: Configure on switch fa0/20 as trunk port

```
SW-1(config)#interface fastEthernet 0/20 (interface facing Router)
SW-1(config-if)#switchport mode trunk
SW-1(config-if)#switchport trunk encapsulation dot1q
```

- Task 3: Creating sub-interfaces on router

```
R-1(config)#interface fa0/0
R-1(config-if)#no shutdown
R-1(config-if)#exit
R-1(config)#interface fa0/0.10
R-1(config-sub-if)#encapsulation dot1Q  10
It should be the exact vlan no (vlan 10)
R-1(config-sub-if)#ip address 192.168.1.100 255.255.255.0
R-1(config-sub-if)#exit
R-1(config)#interface fa0/0.20
R-1(config-sub-if)# encapsulation dot1Q  20
It should be the exact vlan no (vlan 20)
R-1(config-sub-if)#ip address 192.168.2.100 255.255.255.0
```

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status    Protocol
FastEthernet0/0        unassigned      YES unset  up        up
FastEthernet0/0.10     192.168.1.100   YES manual up        up
FastEthernet0/0.20     192.168.2.100   YES manual up        up
```

- Task 2: Configure on switch fa0/20 as trunk port

```
PC> ipconfig
IP Address.....................: 192.168.1.1
Subnet Mask....................: 255.255.255.0
Default Gateway................: 192.168.1.100
```

```
PC> ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.2.1: bytes=32 time=62ms TTL=127
Reply from 192.168.2.1: bytes=32 time=125ms TTL=127
Reply from 192.168.2.1: bytes=32 time=109ms TTL=127
```

```
C> tracert 192.168.2.1
Tracing route to 192.168.2.1 over a maximum of 30 hops:
  1    47 ms     63 ms     62 ms     192.168.1.100
  2    109 ms    125 ms    78 ms     192.168.2.1
```

17. Spanning Tree Protocol (STP)

17.1 Overview

- STP uses Spanning Tree algorithm to avoid switching loops in layer-2 devices (bridges or switches).
- STP works when multiple switches are used with redundant links avoiding broadcast storms, multiple frame copies & database instability.
- First Developed By DEC
- STP is a open standard (IEEE 802.1D)
- STP is enabled by default on all Cisco Catalyst switches

17.2 STP Terminology

- BPDU
  - All switches exchange information through what is called as Bridge Protocol Data Units (BPDUs)
  - BPDUs contain a lot of information to help the switches determine the topology and any loops that result from that topology.
  - BPDUs are sent every 2 sec
- Bridge ID
  - Each switch has a unique identifier called a Bridge ID or Switch ID
  - Bridge ID = Priority + MAC address of the switch
  - When a switch advertises a BPDU, they place their switch id in these BPDUs.
- Root Bridge
  - The bridge with the Best (Lowest) ID.
  - Out of all the switches in the network, one is elected as a root bridge that becomes the focal point in the network.
- Non-Root bridge
  - All Switches other than the Root Bridge are Non-Root Bridges
- Root port
  - The link which is directly connected to the root bridg (or) it is the shortest path to the Root bridge
  - Every Non-root Bridge looks the best way to go Root-bridge
  - For every non-root bridge there is only one root port
  - Root port with the least cost (Speed) connecting to the root bridge
  - The bridge with the Best (Lowest) Switch ID.
  - Lowest Physical Port Number.

- Designated port
  - A designated port will always in Forward Mode
- Non Designated port
  - All the Port or ports, which are blocked by STP to avoid switching loops
  - A Non Designated port Will Always in Blocked Mode

17.3 STP Port States

- Blocking : 20 Sec or No Limits
- Listening : 15 Sec
- Learning : 15 Sec
- Forwarding : No Limits
- Disable : No Limits

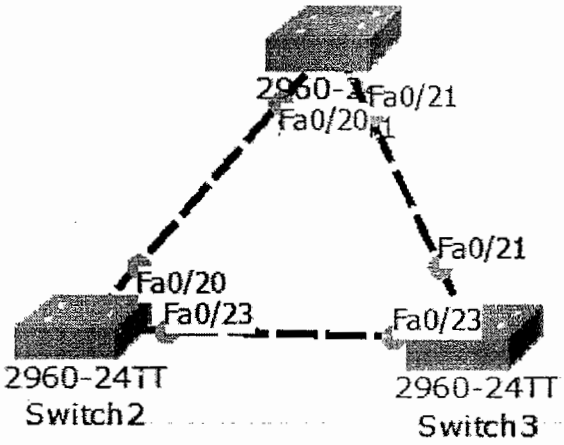
17.4 Switch Port States

- Blocking: Won't forward frames; listens to BPDUs. All ports are in blocking state by default when the switch is powered up.
- Listening: Listens to BPDUs to make sure no loops occur on the network before passing data frames.
- Learning: Learns MAC addresses and builds a filter table but does not forward frames.
- Forwarding: Sends and receives all data on the bridged port.

17.5 Typical costs of different networks

Speed New	IEEE Cost	Original IEEE Cost
10 Gbps	2	1
1 Gbps	4	1
100 Mbps	19	10
10 Mbps	100	100

17.6 LAB: Verifying Spanning Tree Behaviour




```
SW-1# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     000C.CF2D.0388
              Cost        19
              Port        20(FastEthernet0/20)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0060.2F3B.4E61
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20
Interface   Role Sts Cost      Prio.Nbr Type
----------- ---- --- --------- -------- --------------------------------
Fa0/21      Desg FWD 19        128.21   P2p
Fa0/20      Root FWD 19        128.20   P2p
```

```
SW-2# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     000C.CF2D.0388
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000C.CF2D.0388
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20
Interface    Role Sts Cost      Prio.Nbr Type
------------ ---- --- --------- -------- --------------------------------
Fa0/20       Desg FWD 19        128.20   P2p
Fa0/23       Desg FWD 19        128.23   P2p
```

```
SW-3# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     000C.CF2D.0388
              Cost        19
              Port        23(FastEthernet0/23)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00E0.B0E9.E389
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20
Interface    Role Sts Cost      Prio.Nbr Type
------------ ---- --- --------- -------- --------------------------------
Fa0/21       Altn BLK 19        128.21   P2p
Fa0/23       Root FWD 19        128.23   P2p
```

```
SW-2(config)#interface f0/20
SW-2(config-if)#shutdown
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to
administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/20, changed
state to down
```

```
SW-3#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     000C.CF2D.0388
              Cost        19
              Port        23(FastEthernet0/23)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00E0.B0E9.E389
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20
Interface    Role Sts Cost      Prio.Nbr Type
-----------  ---- --- --------- -------- --------------------------------
Fa0/21       Desg LRN 19        128.21   P2p
Fa0/23       Root FWD 19        128.23   P2p
```

```
SW-3#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     000C.CF2D.0388
              Cost        19
              Port        23(FastEthernet0/23)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00E0.B0E9.E389
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20
Interface    Role Sts Cost      Prio.Nbr Type
-----------  ---- --- --------- -------- --------------------------------
Fa0/21       Desg FWD 19        128.21   P2p
Fa0/23       Root FWD 19        128.23   P2p
```

```
SW-2(config-if)# no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to up
```

```
SW-3#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     000C.CF2D.0388
              Cost        19
              Port        23(FastEthernet0/23)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00E0.B0E9.E389
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20
Interface   Role Sts Cost      Prio.Nbr Type
----------- ---- --- --------- -------- --------------------------------
Fa0/21      Altn BLK 19        128.21   P2p
Fa0/23      Root FWD 19        128.23   P2p
```

18. IP Version 6

18.1 Overview

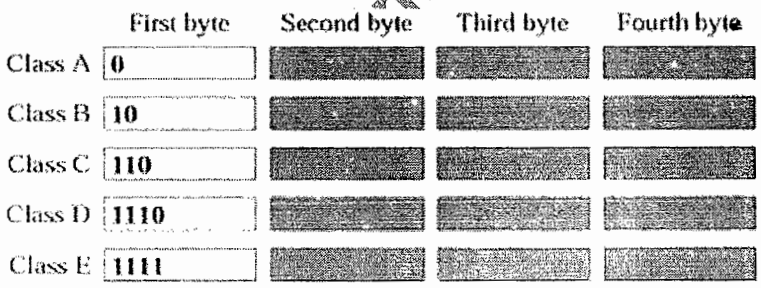
- **Internet -** world's largest public data network, doubling in size every nine months
- IPv4, defines a 32-bit address - 2^{32} (4,294,967,296) IPv4 addresses available
- The first problem is concerned with the eventual depletion of the IP address space.
- Traditional model of classful addressing does not allow the address space to be used to its maximum potential.

18.2 Classful Addressing

- When IP was first standardized in Sep 1981, each system attached to the IP based Internet had to be assigned a unique 32-bit address
- The 32-bit IP addressing scheme involves a two level addressing hierarchy

Network Number/Prefix	Host Number

- Divided into 5 classes
- Class A 8 bits N/W id and 24 bits host id and so on B,C.
- Wastage of IP addresses by assigning blocks of addresses which fall along octet boundaries



18.3 Techniques to reduce address shortage in IPv4

- Subnetting
- Classless Inter Domain Routing (CIDR)
- Network Address Translation (NAT)

18.4 Features of IPv6

- Larger Address Space
- Aggregation-based address hierarchy
- Efficient backbone routing
- Efficient and Extensible IP datagram
- Stateless Address Autoconfiguration
- Security (IPsec mandatory)
- Mobility

18.5 128 bit IPv6 address

3FFE:085B:1F1F:0000:0000:0000:00A9:1234

8 groups of 16-bit hexadecimal numbers separated by ":"

Leading zeros can be removed

3FFE:85B:1F1F::A9:1234

:: = all zeros in one or more group of 16-bit hexadecimal numbers

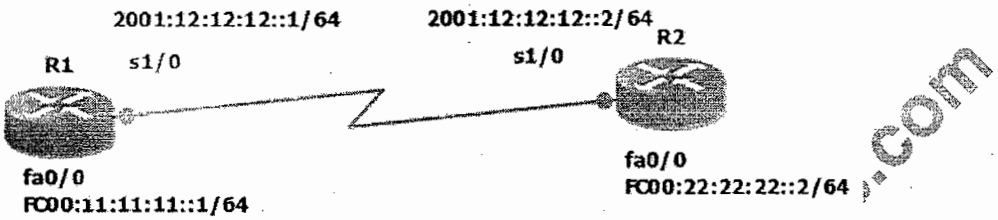
18.6 IPv6 Address Types

- Unicast
  - Global unicast
    - Like public IP (routable), 2000:: and 2001::
  - Site local (unique local)
    - Like private ip (routable)
    - Any address whichever starts with FC or FD in the first two numbers
  - Link local
    - Default IPV6 address on every ipv6 enabled interface
    - (non routable) FE80::
- Multicast
  - Starts with FF00::
- Anycast
  - Similar to multicast, identify multiple interfaces but sends to only one whichever it finds first.
  - The above (site local and Global unicast addresses can be used as anycast.

18.7 Assigning the IPv6 address

- Static
- Auto-configuration
  - Statefull (via DHCP)
  - Stateless (device gets IP IPv6 add by including the MAC add)

18.8 LAB: Basic IPv6 Address Configuration



- Task 1: Configure IPv6 address on R1 according to the above diagram

```
interface fa0/0
ipv6 address fc00:11:11:11::1/64
no shutdown
!
interface s1/0
ipv6 address 2001:12:12:12::1/64
no shutdown
clock rate 64000
```

```
R1# show ipv6 int brief
FastEthernet0/0 [up/up]
    FE80::2D0:FFFF:FED3:1701
    FC00:11:11:11::1
FastEthernet0/1 [administratively down/down]
S1/0 [down/down]
    FE80::207:ECFF:FEC3:501
    2001:12:12:12::1
```

- Task 2: Configure IPv6 address on R2 according to the above diagram

```
interface fa0/0
ipv6 address fc00:22:22:22::1/64
no shutdown
!
interface s1/0
ipv6 address 2001:12:12:12::2/64
no shutdown
clock rate 64000
```

```
R2# show ipv6 int brief
FastEthernet0/0 [up/up]
    FE80::204:9AFF:FEE7:BC01
    FC00:22:22:22::2
FastEthernet0/1 [administratively down/down]
S1/0 [up/up]
    FE80::290:CFF:FEA0:7801
    2001:12:12:12::2
```

19. Password Recovery on Cisco Routers

19.1 Summary

- Console connection
- open hyperterminal window
- power on the router
- press **CTRL+ SHIFT + BREAK** to enter in to Rommon mode
- Modular routers
    - Rommon1> confreg 0x2142
    - Rommon2> reset
- Fixed routers
    - > o/r 0x2142
    - > i

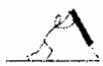
NOTE:

- *Now the router boots without any passwords and enters in to setup mode*
- *Skip setup mode with NO command.*

```
Router>enable
Router#copy startup-config running-config
(very imp if u dont want to loose the configs in the NVRAM)
Router#config  terminal
```

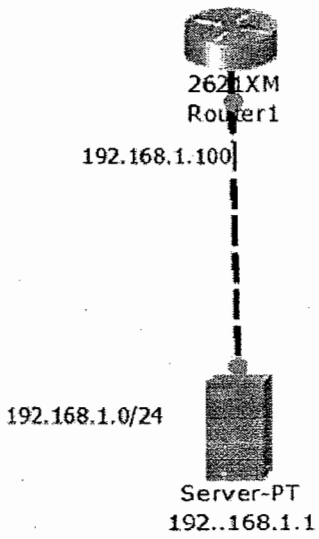
- Change the passwords (Overwrite with the new passwords)

```
Router (config)# config-register 0x2102
Router (config)# end
Router#write
Router#reload
```

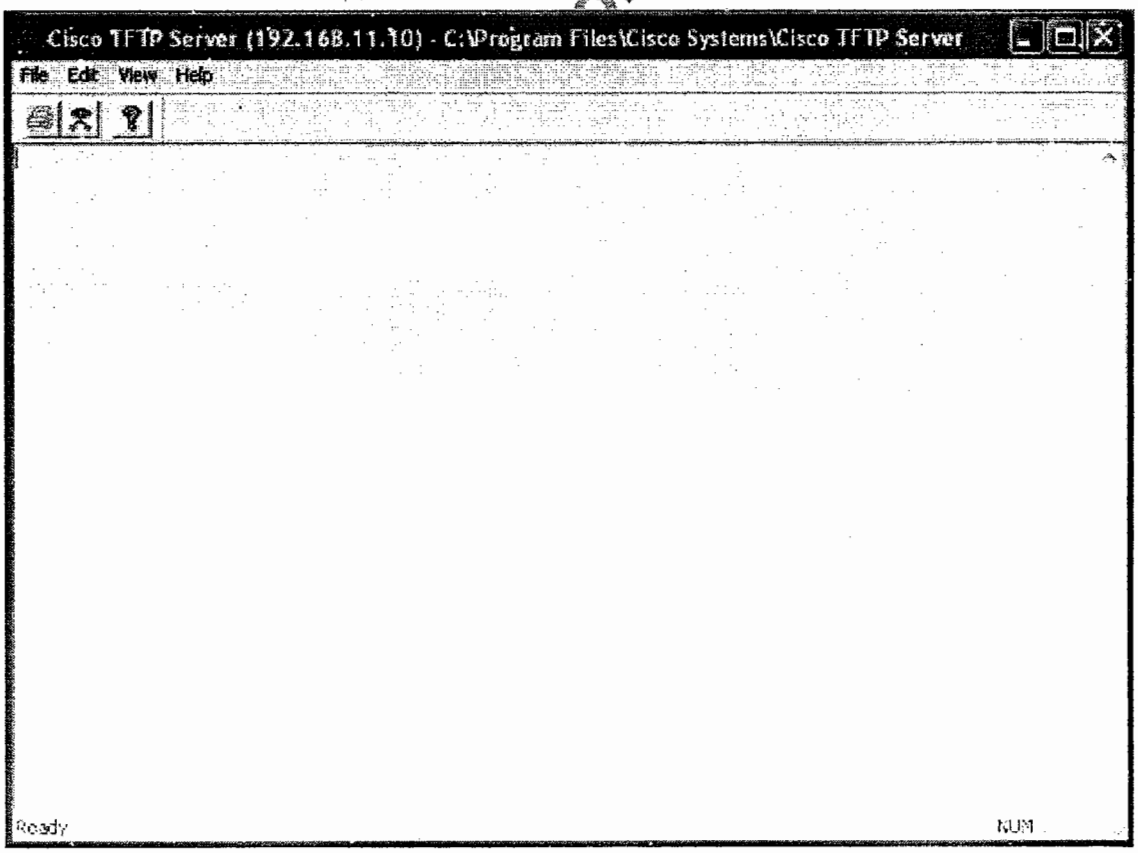


NOTE: *After reloading check for configurations that should be the same and you are able to login with new passwords.*

19.2 Backup and Restore IOS/Configs



- Install TFTP application and ensure you can launch it on PC (it is open and minimized)



```
R-1#show ip interface brief
Interface          IP-Address      OK? Method Status          Protocol
FastEthernet0/0    192.168.1.100   YES manual up              up
```

```
R-1# ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/7/17 ms
```

```
R-1# show flash
System flash directory:
File  Length   Name/status
  3   5571584  c2600-i-mz.122-28.bin
 [5827403 bytes used, 58188981 available, 64016384 total]
63488K bytes of prccessor board System flash (Read/Write)
```

- Backup of IOS: **#copy flash tftp**

```
R-1#copy flash tftp
Source filename []?  c2600-i-mz.122-28.bin
Address or name of remote host []? 192.168.1.1
Destination filename [c2600-i-mz.122-28.bin]?
Writing c2600-i-mz.122-
28.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 5571584 bytes]

5571584 bytes copied in 0.433 secs (12867000 bytes/sec)
```

- Restore or Upgrade IOS: **#copy tftp flash**

```
R-1#copy tftp flash:
Address or name of remote host []? 192.168.1.1
Source filename []? c2600-i-mz.122-28.bin
Destination filename [c2600-i-mz.122-28.bin]?

%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
Erase flash: before copying? [confirm]
Erasing the flash filesystem will remove all files! Continue? [confirm]
Erasing device...
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
...erased
Erase of flash: complete
Accessing tftp://192.168.1.1/c2600-i-mz.122-28.bin...
Loading c2600-i-mz.122-28.bin from 192.168.1.1:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 5571584 bytes]

5571584 bytes copied in 0.41 secs (3113699 bytes/sec)
```

- Configuration backup: **#copy tftp running-config**

```
R-1# copy startup-config tftp:
Address or name of remote host []? 192.168.1.1
Destination filename [R-1-confg]?
Writing startup-config...!!
[OK - 537 bytes]
537 bytes copied in 0.006 secs (89000 bytes/sec)
```

- Restore Congfiguration from TFTP

```
ROUTER# copy tftp running-config
Address or name of remote host []?   192.168.1.1
Source filename []?  R-1-confg
Destination filename [running-config]?

Accessing tftp://192.168.1.1/R-1-confg...
Loading R-1-confg from 192.168.1.1: !
[OK - 537 bytes]

537 bytes copied in 0.002 secs (268500 bytes/sec)

R-1#
%SYS-5-CONFIG_I: Configured from console by console
```

- Detailed instructions for configuring an IP address to the router and TFTP which has no IOS in flash for it to load IOS from PC
- By default router goes in to Rommon mode if there is no IOS in the flash (booting from ROM)

```
tftpdnld
IP_address = 192.168.1.100
ip_subnet_mask = 255.255.255.0
default_gateway = 192.168.1.100

tftp_server = 192.168.1.1
tftp_file =  <filename>

tftpdnld
reset
```

19.3 LAB: Restoring the IOS from TFTP into IOS

- TASK: Delete the existing IOS from Flash

```
R-1#show flash:
System flash directory:
File  Length   Name/status
4     5571584  c2600-i-mz.122-28.bin
[5571584 bytes used, 58444800 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)
```

```
R-1#delete flash:c2600-i-mz.122-28.bin
Delete filename [c2600-i-mz.122-28.bin]?
Delete flash:/c2600-i-mz.122-28.bin? [confirm]
```

```
R-1#reload
Proceed with reload? [confirm]
%SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload
Command.

System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
cisco 2621 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of
memory
Boot process failed...
The system is unable to boot automatically.  The BOOT
environment variable needs to be set to a bootable image.
rommon 1 >
```

- TASK: Configure steps to download IOS from TFTP

```
rommon 1 > tftpdnld

Missing or illegal ip address for variable IP_ADDRESS Illegal IP address.

usage: tftpdnld
Use this command for disaster recovery only to recover an image via TFTP.
Monitor variables are used to set up parameters for the transfer.
(Syntax: "VARIABLE_NAME=value" and use "set" to show current variables.)
"ctrl-c" or "break" stops the transfer before flash erase begins.

The following variables are REQUIRED to be set for tftpdnld:
IP_ADDRESS: The IP address for this unit
IP_SUBNET_MASK: The subnet mask for this unit
DEFAULT_GATEWAY: The default gateway for this unit
TFTP_SERVER: The IP address of the server to fetch from
TFTP_FILE: The filename to fetch

The following variables are OPTIONAL:
TFTP_VERBOSE: Print setting. 0=quiet, 1=progress(default), 2=verbose
TFTP_RETRY_COUNT: Retry count for ARP and TFTP (default=7)
TFTP_TIMEOUT: Overall timeout of operation in seconds (default=7200)
TFTP_CHECKSUM: Perform checksum test on image, 0=no, 1=yes (default=1)
FE_SPEED_MODE: 0=10/hdx, 1=10/fdx, 2=100/hdx, 3=100/fdx, 4=Auto(deflt)
```

```
rommon 2 > IP_ADDRESS=192.168.1.100
rommon 3 > IP_SUBNET_MASK=255.255.255.0
rommon 4 > DEFAULT_GATEWAY=192.168.1.100
rommon 5 > TFTP_SERVER=192.168.1.1
rommon 6 > TFTP_FILE=c2600-i-mz.122-28.bin
rommon 7 > tftpdnld

IP_ADDRESS: 192.168.1.100
IP_SUBNET_MASK: 255.255.255.0
DEFAULT_GATEWAY: 192.168.1.100
TFTP_SERVER: 192.168.1.1
TFTP_FILE: c2600-i-mz.122-28.bin
Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!

Do you wish to continue? y/n: [n]:  y
.Receiving c2600-i-mz.122-28.bin from 192.168.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
File reception completed.
Copying file c2600-i-mz.122-28.bin to flash.

Erasing flash at 0x60000000
Erasing flash at 0x60080000
program flash location 0x60530000
program flash location 0x60540000
program flash location 0x60550000
```

```
rommon 8 > reset
System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
cisco 2621 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of
memory

Self decompressing the image :
################################################################################
# [OK]

             Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706

Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE
(fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang

cisco 2621 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of
memory
.
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

Press RETURN to get started!

ROUTER>
```