NETMETRIC SOLUTIONS

WWW.NETMETRIC-SOLUTIONS.COM

CISCO CERTIFIED NETWORK ASSOCIATE

CCNA R&S LAB MANUAL

VER 2.0

Sikandar Gouse Moinuddin
CCIE (R&S, SP) # 35012
sikandarbaadshah@gmail.com

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

NETMETRIC SOLUTIONS

SIKANDAR SHAIK CCIE # 35012

Sikandar Shaik

Senior Technical Instructor

Sikandar Shaik has been actively working with data networking as a Network Engineer for over 6 years, and has been working with Cisco routers and switching technology. Sikandar has been teaching and developing content for the CCIE R&S track since 2009. You will find Sikandar in Live Classroom of R&S classes here at Netmetric. Sikandar is responsible for updating, supporting and teaching Netmetric's R&S-related courses. Over the past few years Sikandar has assisted more CCIE R&S engineers in passing the lab than any other Instructor, worldwide!

Core Networking Skills:

Routing : Static Routing, RIPv1, RIPv2, RIPnG, IGRP, EIGRP, OSPF, IS-IS, BGPv4, ODR, GRE, MPLS, IPv6, Traffic Engineering, Policy Based Routing PBR, Route Filtering, Redistribution, Summarization

Security : Zone-Based Firewall, SSL VPN/IPsec VPN/DMVPN/GET VPN, VPN QoS, IPS Tuning, AAA, Firewall Redudancy

Switching : Catalyst CatOS and IOS based Switches, VTP, STP, RSTP, Trunking, VLANs, Layer 3 Switches, Logical Etherchannels

WAN : Leased lines (PPP / HDLC), Channelized lines (E1 / T1 / E3 / T3), Frame Relay, ATM, ISDN

Soft Skills:

Communication Skills: A clear speaker in English and comfortable speaking in front of audience, he can easily facilitate classroom sessions and also address large gathering.

Interpersonal Skills: With positive attitude he has proven ability to deal with difficult situations in a careful and considerate manner.

Learning Skills: Can easily pick up new skills and generally thrive on challenges.

Problem Solving Skills: His analytical skills helps him troubleshoot problems & uncover root causes.

Personal Details:

Education : Bachelors Degree in Computer Science

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

TABLE OF CONTENTS **PAGE NO**

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

IP ADDRESS

- IP Address is Logical Address. It is a Network Layer address (Layer 3).
- IP address is given to every device in the network and it is used to identify the device with in the network.

Two Versions of IP:

IP version 4 is a 32 bit address

IP version 6 is a 128 bit address

IP version 4

- **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:**

First Octet	Second Octet	Third Octet	Forth Octet
01010101.	00000101.	10111111.	00000001

- **IP address in decimal form:**

85.5.191.1

IP version 6 Format

- 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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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

Total IP Address Range
0 . 0 . 0 . 0
to
255.255.255.255

1 1 1 1 1 1 1 1 = 255

IPV4

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 Ranges	Octet Format	No. Networks & Hosts
A	0.0.0.0 - 127.255.255.255	N.H.H.H	126 Networks & 16777214 Hosts per Network
B	128.0.0.0 - 191.255.255.255	N.N.H.H	16384 Networks & 65534 Hosts per Network
C	192.0.0.0 - 223.255.255.255	N.N.N.H	2097152 Networks & 254 Hosts per Network
D	224.0.0.0 - 239.255.255.255	Reserved for multicast traffic	
E	240.0.0.0 - 255.255.255.255	Reserved for Research and development	

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

Host: - a specific device in the network
Network: - set of devices

Network Address

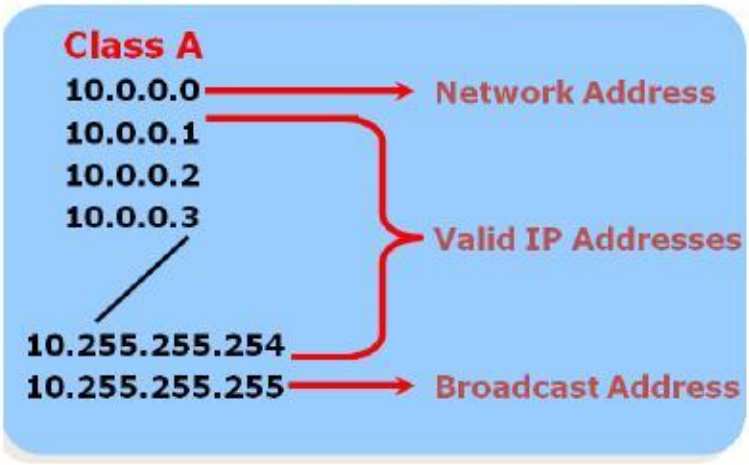
- First IP address of the range
- It represents the complete network and cannot be assigned to any device
- The network address is represented with all bits as **ZERO** in the host portion of the address

Broadcast Address

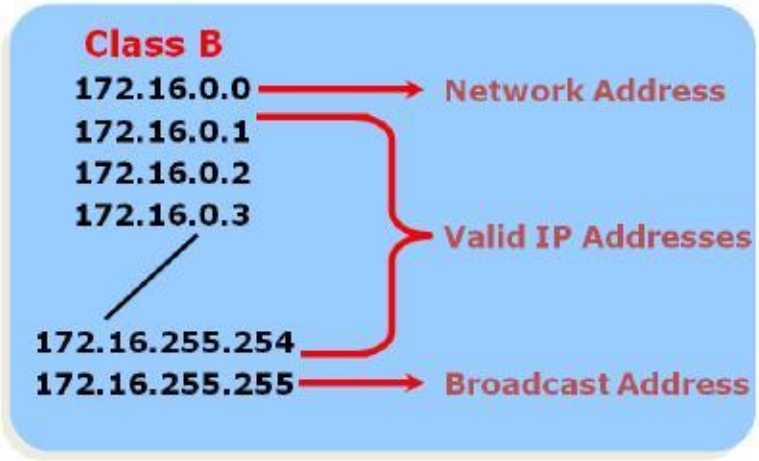
- The last IP address of the range
- Used to send the broadcast with the network and cannot be assigned to any device in the network
- The broadcast address is represented with all bits as **ONES** in the host portion of the address

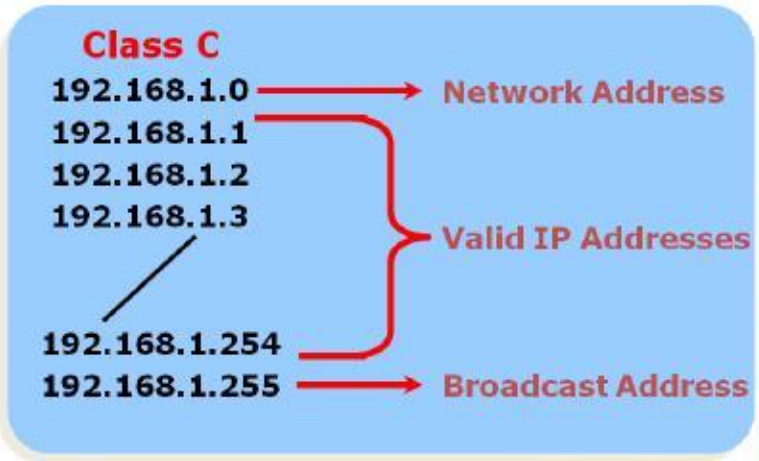
Valid addresses:

- Valid IP Addresses lie between the Network Address and the Broadcast Address.
- Only Valid IP Addresses are assigned to hosts/clients or any other device in the network



sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com





Subnet Mask

It's an address which is used to identify the network and host portion of an Ip address

Class A	N.H.H.H	255.0.0.0
Class B	N.N.H.H	255.255.0.0
Class C	N.N.N.H	255.255.255.0

- Subnet Mask differentiates Network portion and Host Portion
- 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.

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

PRIVATE IP	PUBLIC IP
• Used with the LAN or within the organization • Not recognized on internet • Given by the administrator • Unique within the network or organization • Free • Unregistered IP	• Used on public network (INTERNET) • Recognized on internet • Given by the service provider (from IANA) • Globally unique • Pay to service provider (or IANA) • • Registered

Private IP Address

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:

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**

Default Gateway:-

- The ip address of the router Ethernet address connecting to the LAN
- It is an entry and exit point of the network.

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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.

1. FLSM (Fixed Length Subnet Mask)
2. 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

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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

FLSM: Example – 1

Req = 40 hosts using C-class address network 192.168.1.0/24

$2^h - 2 >= req$

$2^6 - 2 >= 40$

$64 - 2 >= 40$

$62 >= 40$

- Host bits required (h) = 6
- Converted network Bits (n) = Total. H. Bits – req. H. 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/Subet

- Subnets = $2^n = 2^2 = 4$ Subnets

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

- **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

FLSM: Example – 2

Req = 500 hosts using B-class address network 172.16.0.0/16

2^h - 2 >= req

2^9 – 2 >= 500

512 – 2 >= 500

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

- 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

FLSM: Example – 3

Req = 2000 hosts using A-class address network 10.0.0.0/8

$2^h - 2 >= req$

$2^{11} - 2 >= 2000$

$2048 - 2 >= 2000$

$2046 >= 2000$

- 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:

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

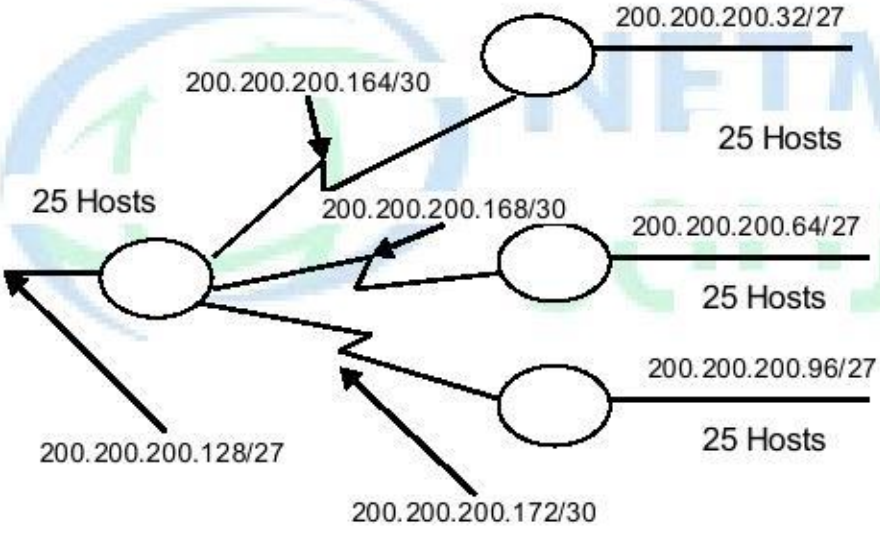
Variable-Length Subnet Mask (VLSM):

- 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

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.

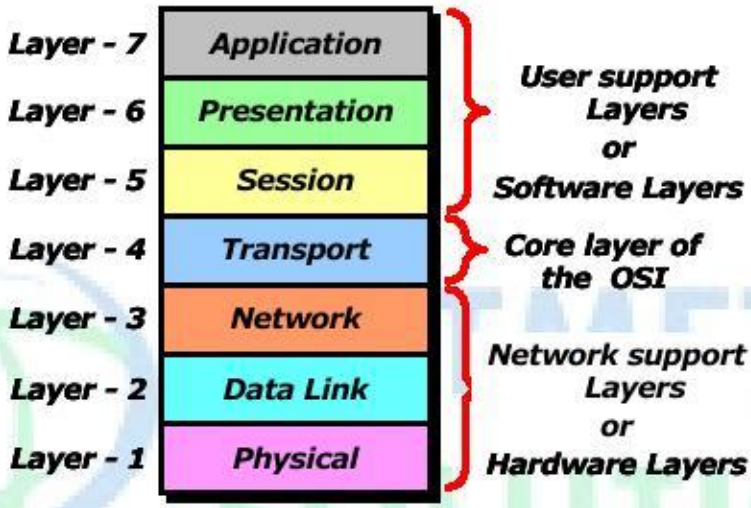
Example of a VLSMs Networks



sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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.



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 No. Ports 0 – 65535
  - Reserved Ports 1 - 1023
  - Unreserved Ports 1024 – 65535

Service	Port No.
HTTP	80
FTP	21
SMTP	25
TELNET	23
TFTP	69

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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

Session Layer (Layer 5)

- It 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

Transport Layer (Layer 4)

- It 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 No's. The major protocols which takes care of Data Transportation at Transport layer are…TCP, UDP

TCP	UDP
• Transmission Control Protocol • Connection Oriented • Reliable communication(with Ack's) • Slower data Transportation • Protocol No is 6	• User Datagram Protocol • Connection Less • Unreliable communication (no Ack's) • Faster data Transportation • Protocol No is 17

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

• Eg: HTTP, FTP, SMTP	• Eg: DNS, DHCP, TFTP

Network Layer (Layer 3)

- It 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 acts as data carriers and defines logical addressing.
- IP, IPX, AppleTalk... Etc

Routing Protocols:

- Routing protocols performs Path determination (Routing).
- RIP, IGRP, EIGRP, OSPF.. Etc
- Devices works at Network Layer are Router, Multilayer switch etc..

Data-link Layer (Layer 2)

- It 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.

1) 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

2) LLC (Logical Link Control)

- It deals with Layer 3 (Network layer)
- Devices works at Data link layer are Switch, Bridge, NIC card.

Physical Layer (Layer 1)

- It 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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

- **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

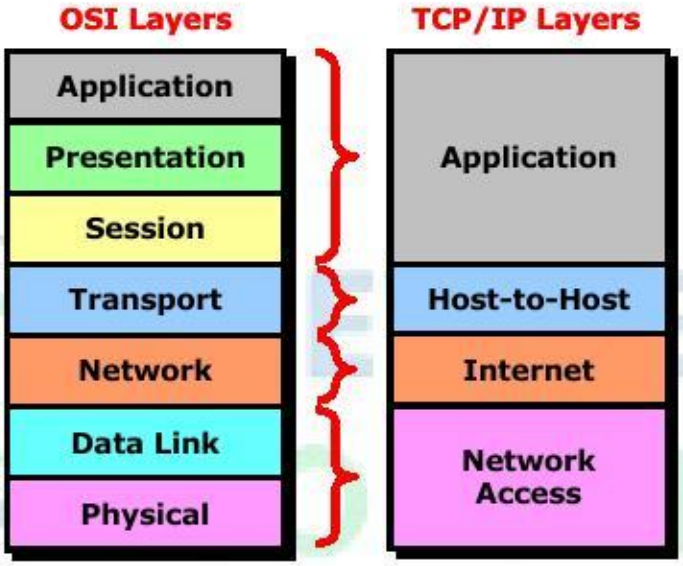
sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

The Transmission Control Protocol/Internet Protocol (TCP/IP) suit was created by the Department of Defense (DoD).

The DoD Model

- The Process / Application Layer
- The Host-to-Host Layer
- The Internet Layer
- The Network-access Layer

Comparing OSI & TCP/IP Model



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.

F T P (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.

T F T P (File Transfer Protocol)

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

- 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.

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.

Host- to – Host layer

TCP	UDP
• Transmission Control Protocol • Connection Oriented • Reliable communication(with Ack's) • Slower data Transportation • Protocol No is 6 • Eg: HTTP, FTP, SMTP	• User Datagram Protocol • Connection Less • Unreliable communication (no Ack's) • Faster data Transportation • Protocol No is 17 • Eg: DNS, DHCP, TFTP

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 and messages that ICMP relates to:

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

- 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.

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

INTRODUCTION TO ROUTERS

What is a Router?

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 Vendors apart from Cisco

Many companies are manufacturing Router:

- Nortel
- Multicom
- Juniper
- Dlink
- Linksys
- 3Com

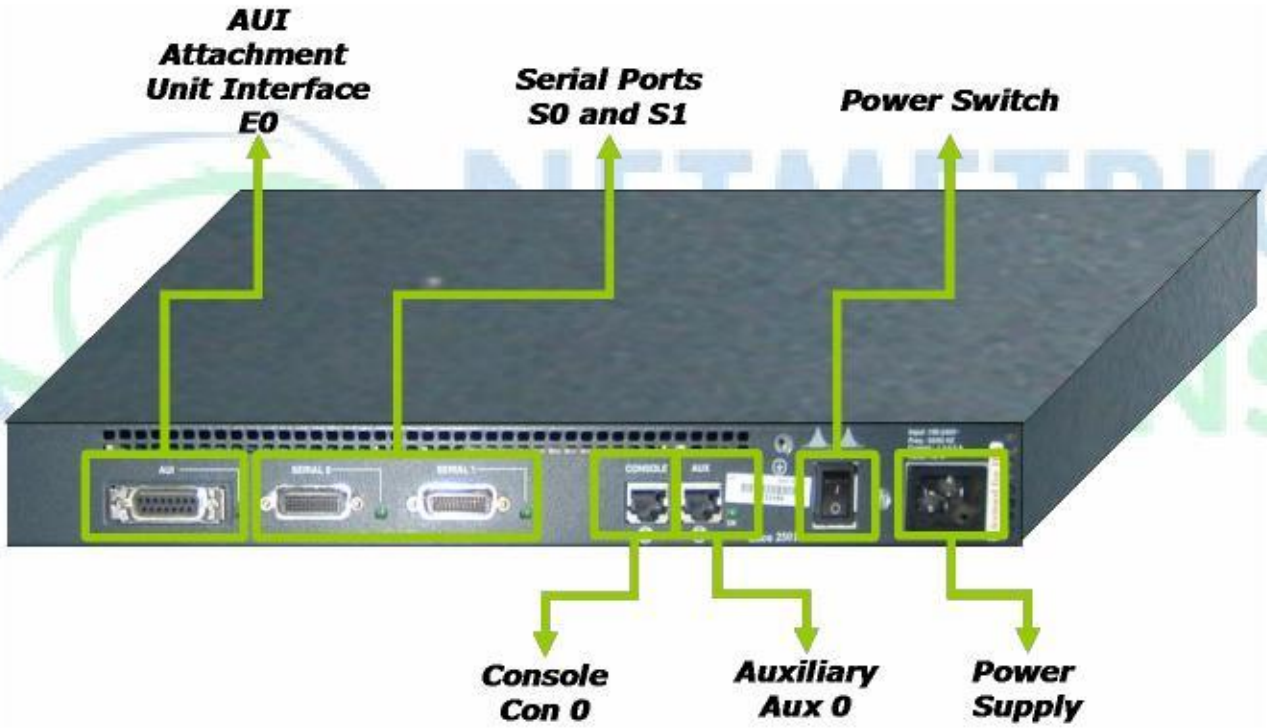
Router Classification

FIXED ROUTER	MODULAR ROUTER
• Fixed router (Non Upgradeable cannot add and remove the Ethernet or serial interfaces) • Doesn't have any slot	• Modular router (Upgradeable can add and remove interfaces as per the requirement) • Number of slots available depend on the series of the router

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

Example Modular Router

Example of Fixed Router



EXTERNAL PORTS OF ROUTER

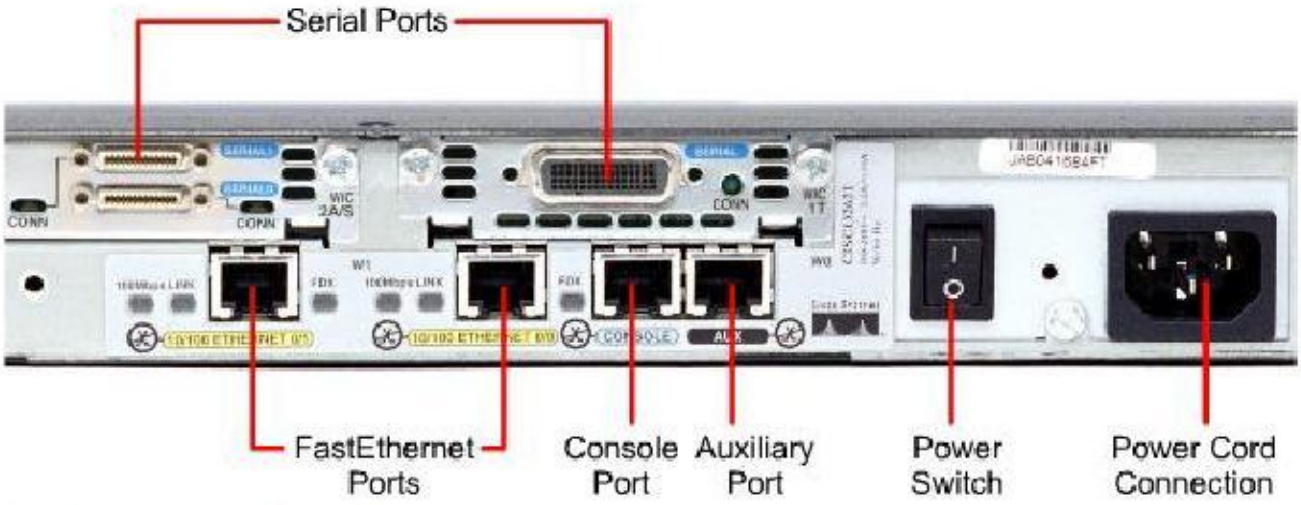
- **WAN interfaces**
  - Serial interface (S0, S1, s0/0, s0/1 , s0/0/0 etc) – 60 pin/26 pin(smart serial)
  - ISDN interface(BRI0 etc) – RJ45 (used for ISDN wan connections)

- **LAN interfaces - Ethernet**
  - AUI (Attachment Unit Interface) (E0)– 15 pin
  - 10baseT – RJ45

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

- **Administration interfaces**
  - Console – RJ45 – Local Administration
  - Auxiliary – RJ45 – Remote Administration

2601 Model Router (Modular Router)

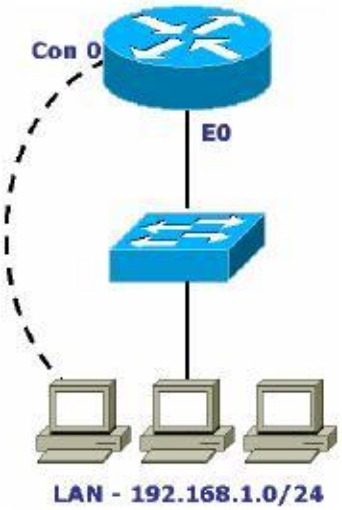


Attachment Unit Interface

- 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.

Console Port

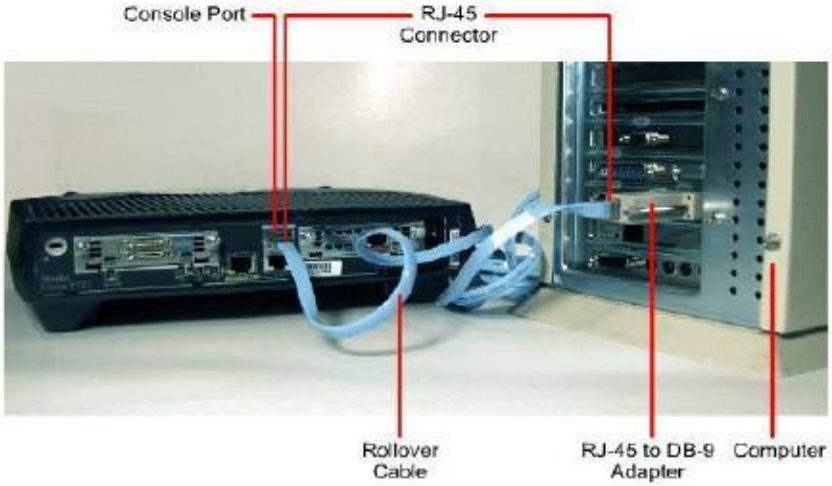
- It is known as Local Administrative Port
- It is generally used for Initial Configuration, Password Recovery and Local Administration of the Router. It is RJ45 Port
- **IMP:** It is the most delicate port on the Router. So make less use of the Console Port.



sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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

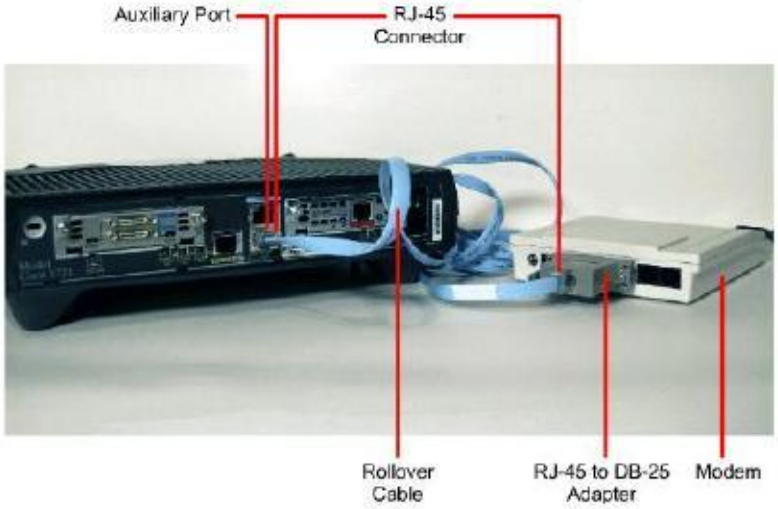


Serial Port

- 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 is having 60 pin configuration male at one end and on the other end 18 pin configurations male.

Auxiliary Port

- 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.



sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

INTERNAL COMPONENTS OF THE ROUTER

ROM:

- Is a chip integrated on the motherboard which contains a Bootstrap program which tells how to load the IOS
- 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 and load a Cisco IOS into 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 and 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.

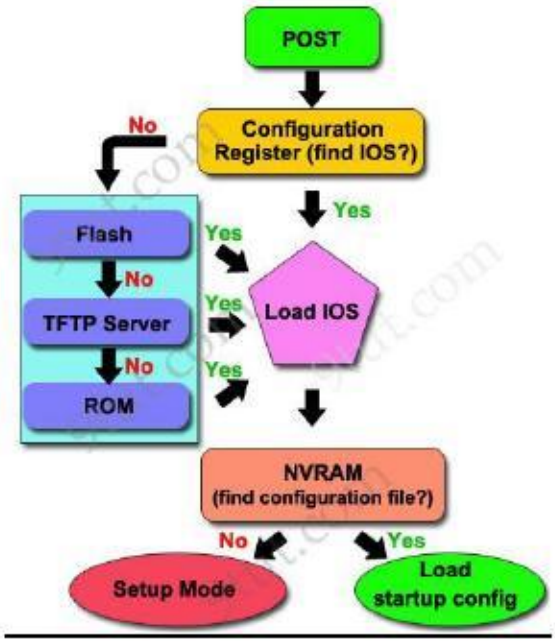
NVRAM (nonvolatile RAM)

- 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.

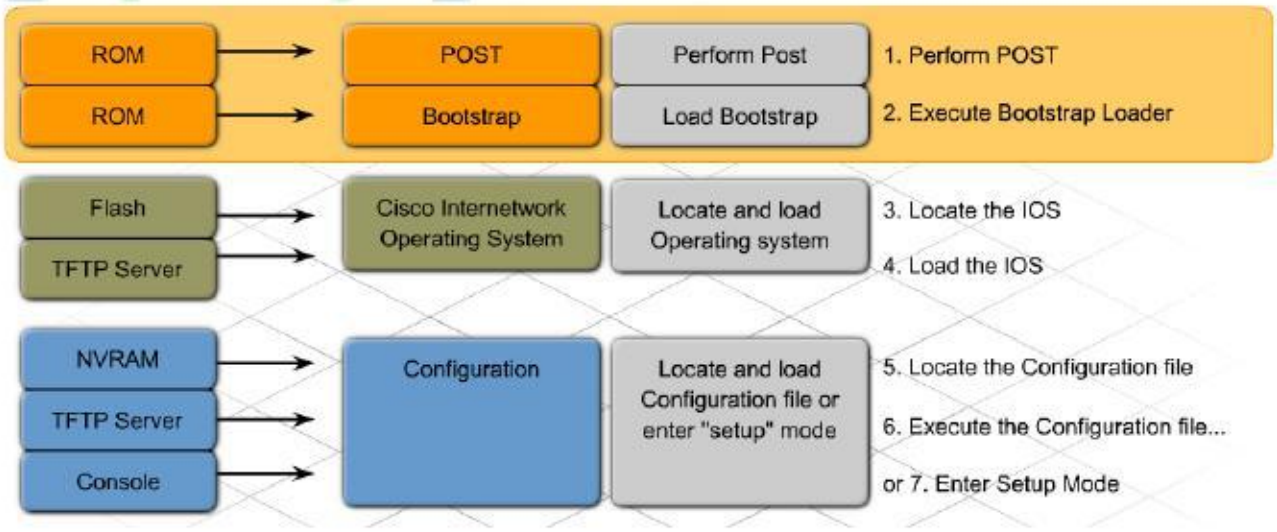
Configuration register file

- 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.

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com



ROUTER START-UP SEQUENCE



1. Performing the POST and Loading the Bootstrap Program

- The power-on self test (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.

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

2. 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.

3. 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.

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

MODES OF ROUTERS

- **User Mode:-**
  - Only some basic monitoring
  - limited 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

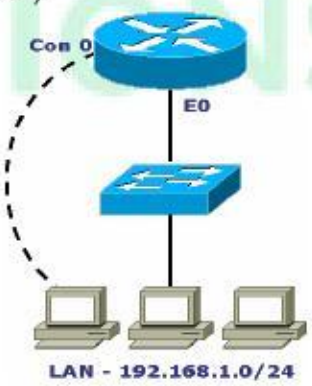
- **Interface mode:-**
  Configurations done on the specific interface

- **Rommon Mode:-** Reverting Password

- **Setup mode**
  - The router enters in to setup mode if the NVRAM is blank

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 on the PC.



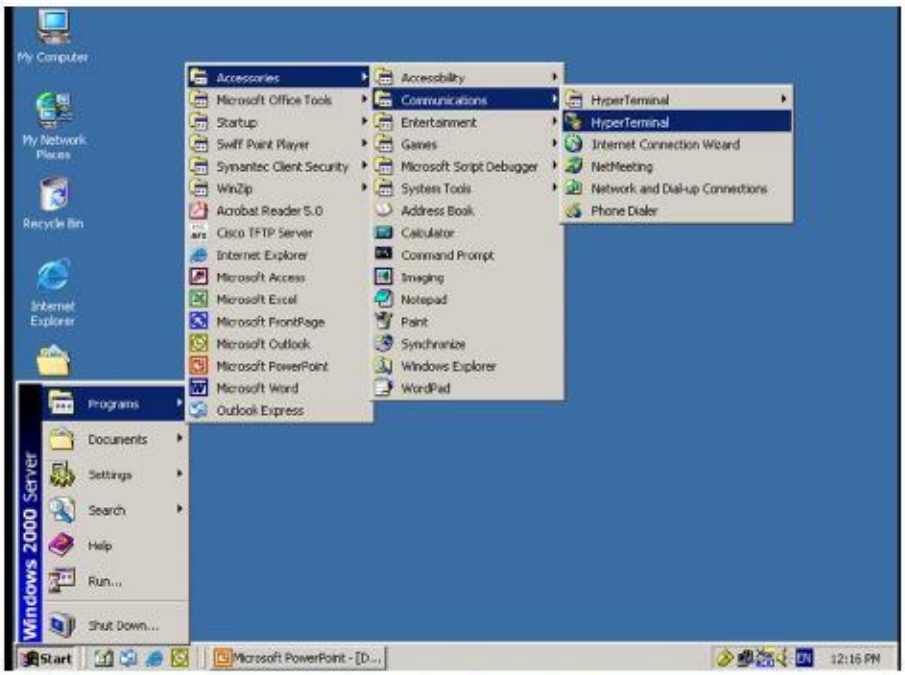
IN WINDOWS

- 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

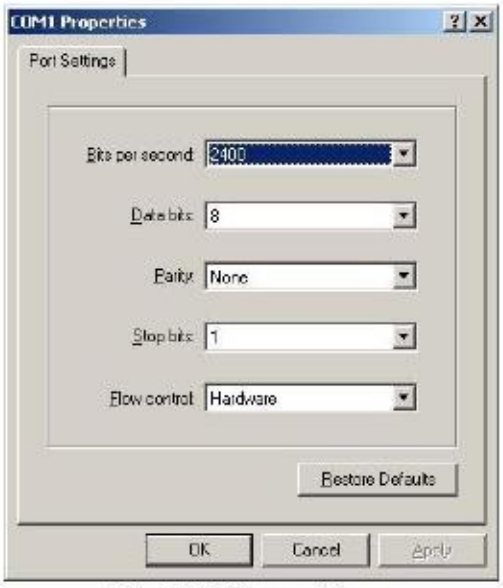
- # minicom –s (used instead of HyperTerminal in Windows)

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com



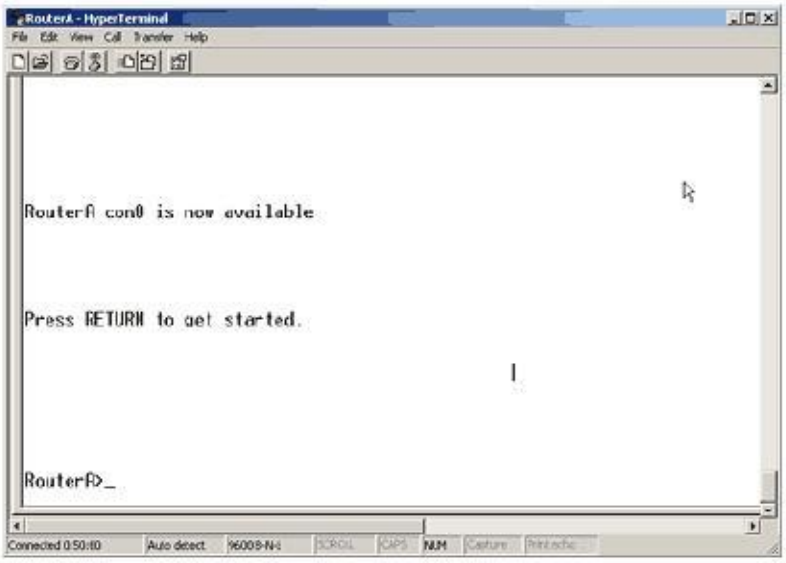
(1) Connection Description

(2) Connect To



(3) COM1 Properties

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com



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

Router # **configure terminal**

(To enter in Global configuration mode)

Global configuration mode:

Router (config) # hostname **Sikandar**

Assigning ip address to Ethernet interface:

Router(config) # interface **<interface type> <interface no>**

Router(config-if) # ip address **<ip address> <subnet mask>** *(Interface Mode)*

Router(config-if) # no shutdown

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

Assigning Telnet password:

Router(config) # line vty 0 4

(To enter into VTY line mode)

Router(config-line) #password **<password>**
Router(config-line) #login
Router(config-line) #exit
Router(config) #exit

Assigning console password:

Router(config) # line con 0

(To enter into Console line mode)

Router(config-line) # password **<password>**
Router(config-line) # login
Router(config-line) # exit
Router(config) # exit

Assigning Auxiliary password:

Router(config) # line aux 0

(To enter into Auxiliary line mode)

Router(config-line) # password **<password>**
Router(config-line) # login
Router(config-line) # exit
Router(config) # exit

Assigning enable password:

Router(config) # enable secret <password>

(The password will be saved in encrypted text)

Router(config) # enable password <password>

(the will be password saved in clear text)

To encrypt all passwords

(config)#service password-encryption

Commands to save the configuration:

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

Router # copy running-config startup-config
(OR)
Router # write memory
(OR)
Router # write

TO erase NVRAM configuration:

Router# **erase startup-config**
(to erase the NVRAM)

LAB: 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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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

.

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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>sh 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

To enter in to privilege mode

Router> **enable**

To enter in to privilege mode

Router# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

TO change the Hostname of the router

Router(config)# **hostname HYDERABAD**

HYDERABAD(config)#

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

TO ASSIGN CONSOLE PASSWORD

HYDERABAD(config)#**line console 0**

HYDERABAD(config-line)#**password** **cisco123**

HYDERABAD(config-line)#**login**

HYDERABAD(config-line)#**end**

HYDERABAD#
%SYS-5-CONFIG_I: Configured from console by console

HYDERABAD# **exit**

HYDERABAD con0 is now available

Press RETURN to get started.

User Access Verification

Password:

(Enter the console password which was configured)

HYDERABAD>
HYDERABAD>**enable**

HYDERABAD# **conf terminal**

Enter configuration commands, one per line. End with CNTL/Z.

HYDERABAD(config)# **line vty 0 4**

HYDERABAD(config-line)# **password** **ccna123**

HYDERABAD(config-line)# **login**

HYDERABAD(config-line)# **exit**

HYDERABAD(config)# **enable password** **ccnp123**
HYDERABAD(config)# **exit**

HYDERABAD# **exit**

HYDERABAD con0 is now available
Press RETURN to get started.

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

User Access Verification

Password:

(Enter the console password which was configured)

HYDERABAD> **enable**
Password:

(enter the enable password which was configured)

HYDERABAD#

HYDERABAD# **sh 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 HYDERABAD
!
!
!
enable password ccnp123
!
!
!
!
==========

HYDERABAD# **configure terminal**

HYDERABAD(config)# **enable secret ccie123**
HYDERABAD(config)# **exit**

HYDERABAD# **show running-config**
Building configuration...

Current configuration : 527 bytes

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

```
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname HYDERABAD
!
!
!
enable secret 5 $1$mERr$2ft7pDdq4XzRIT3Dy74gx/
enable password ccnp123
!
```

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

HYDERABAD# 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
```


sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

```
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]:
```

==========

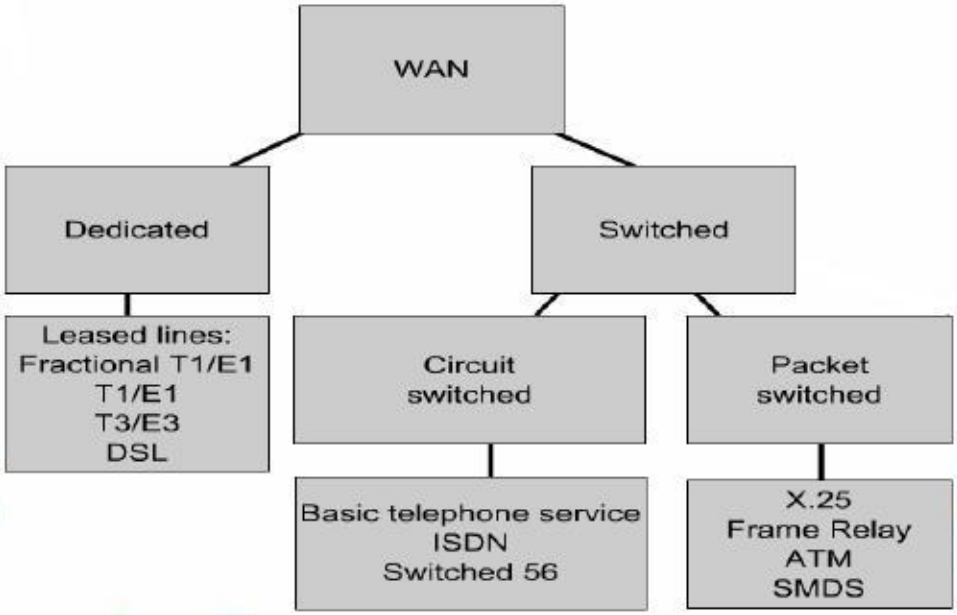
NOTE: The router enters in to setup mode as the startup-config been erased

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

WAN CONNECTIONS

WAN connections are divided into three types

1) Dedicated line
2) Circuit switched
3) Packet switched



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

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

Packet switched:-

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

Example: - Frame Relay

Leased line: -

- A permanent/dedicated physical connection which is used to connect
- two different geographical areas. This connection is provided by telecommunication companies like BSNL in India.
- 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 1) SHORT LEASED LINE 2) MEDIUM LEASED LINE 3) LONG LEASE LINE (IPLC)
Short leased line which is used with in the city and cost is also less for it.
Medium leased line is used to connect sites in two different states like Hyderabad and Chennai.
Long Leased Line also called as IPLC. It stands for International private lease circuit uses to connect two different countries. It's the most expensive among all.

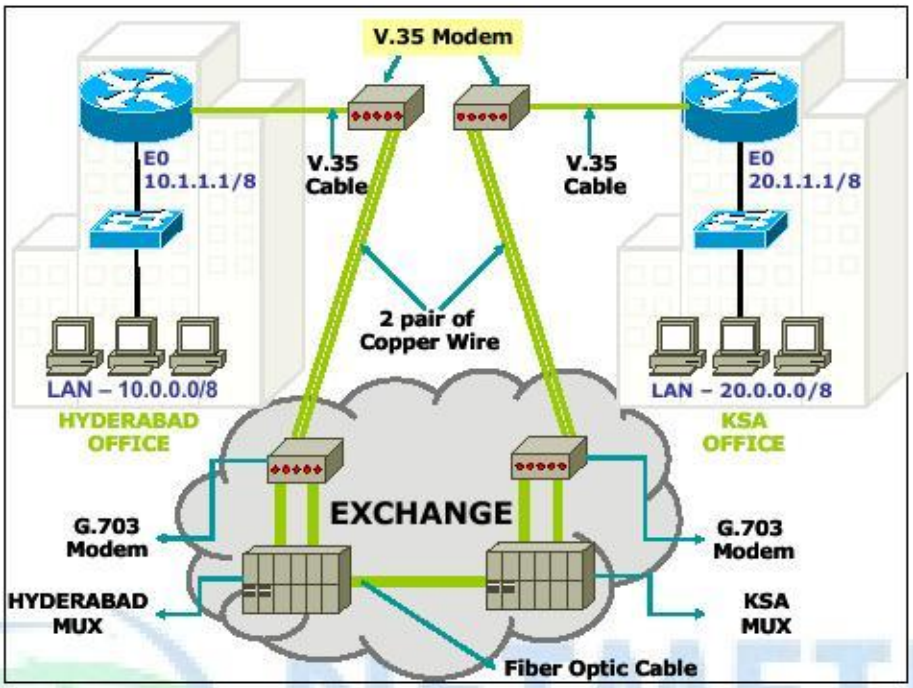
- Leased Line provides excellent quality of service with high speed of data transmission.
- As it's a private physical connection assures complete security and privacy even with voice.
- Speed of the leased line varies from 64 kbps to 2 Mbps or more. Always Leased Line has fixed bandwidth.

Note:-

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

Example of Leased Line



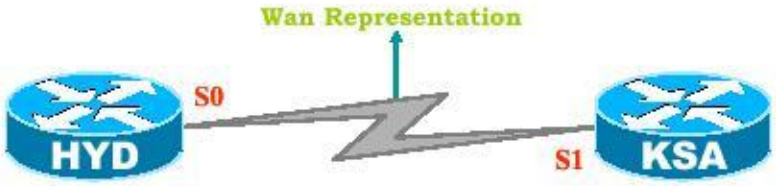
DCE	DTE
• Data Communication Equipment • Generate clocking (i.e. Speed). • Example of DCE device in Leased line setup : V.35 & G.703 Modem & Exchange (Modem & MUX) • Example of DCE device in Dial up setup : Dialup Modem	• Data Termination Equipment • Accept clocking (i.e. Speed). • Example of DTE device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

Coming to the hardware requirements

1) **Leased Line Modem**
2) **V.35 connector & cable**
3) **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.

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com



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:

1. *T1* (1.544 Mbps)
2. *T2* = 4 T1 lines (6 Mbps),
3. *T3* = 28 T1 lines (45 Mbps),
4. *T4* = 168 T1 lines (275 Mbps)

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

ADVANTAGES	DISADVANTAGES
○ COMPLETE SECURE ○ HIGH BANDWIDTH ○ HIGH SPEED CONNECTION ○ SUPERIOR QUALITY ○ RELIABLE	○ EXPENSIVE ○ PERMANENT PHYSICAL CONNECTION

WAN Protocols

Leased Lines uses two types of WAN encapsulation protocols:

1) High Data Link Protocol (HDLC)
2) Point to Point Protocol (PPP)

HDLC	PPP
• Higher level data link Control protocol • Cisco Proprietary Layer 2 WAN Protocol • Doesn't support Authentication • Doesn't support Compression and error correction	• Point to Point Protocol • Standard Layer 2 WAN Protocol • Supports Authentication • Support error correction

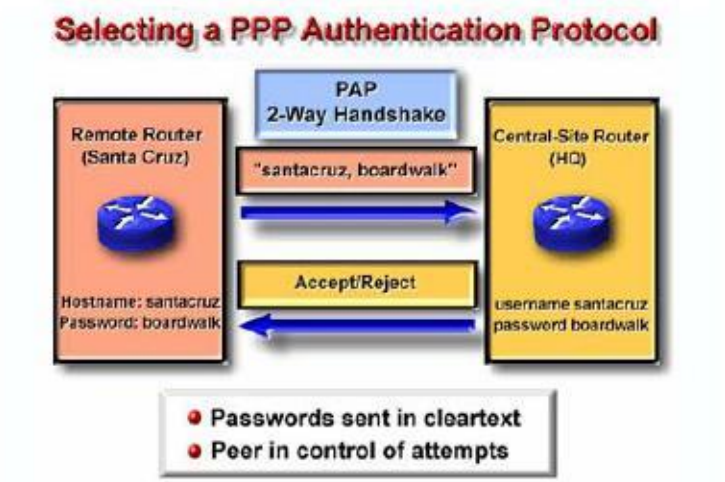
PPP supports two authentication protocols:

- PAP (Password Authentication Protocol)
- CHAP (Challenge Handshake Authentication Protocol)

PAP (Password Authentication Protocol)

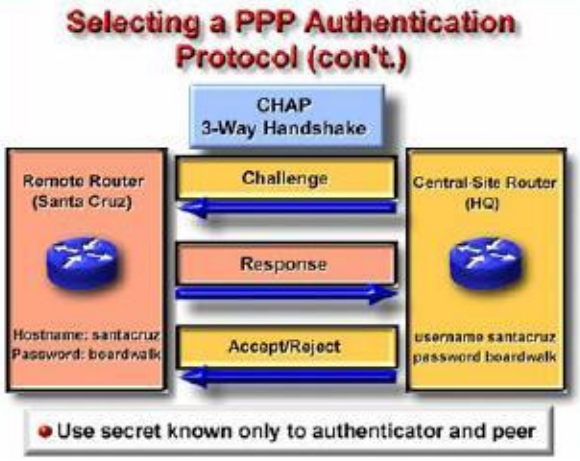
- PAP provides a simple method for a remote node to establish its identity using a two-way handshake.
- PAP is done only upon initial link establishment
- PAP is not a strong authentication protocol.
- Passwords are sent across the link in clear text.

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com



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:-

Router(config)# interface serial 0/0

Router(config-if)# encapsulation **hdlc**

(default is HDLC even if u don't configure this command)

Configuration of PPP:

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

To Enable CHAP Authentication

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

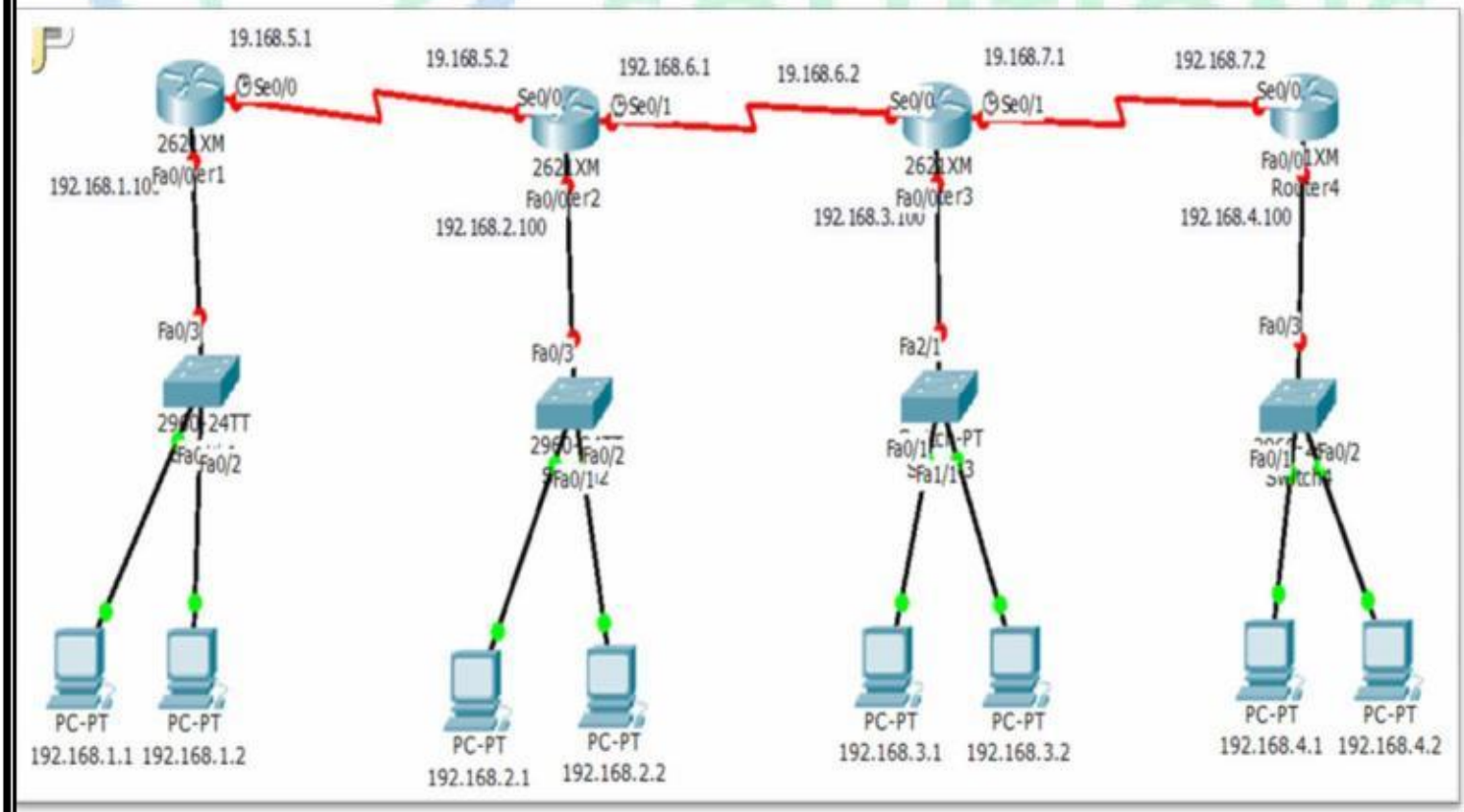
To Enable PAP Authentication:-

```
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:

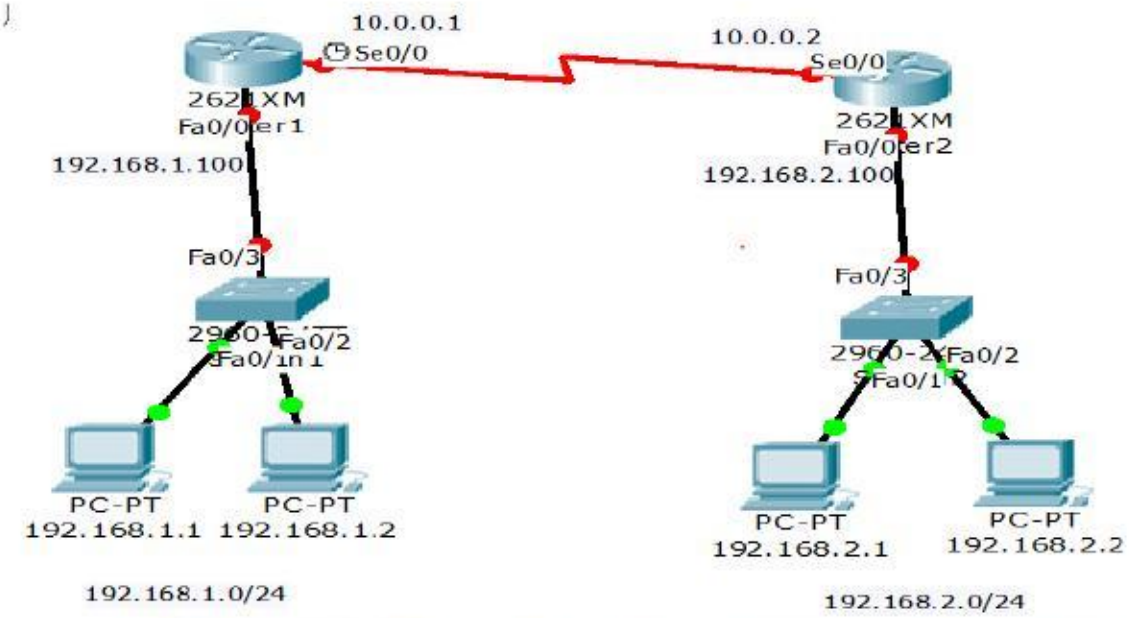
1. All the LAN and WAN should be in different networks (or should not repeat the same network) .
2. Router Ethernet IP and the LAN network assigned should be in the same network.
3. Both the interfaces of router facing each other should be in the same network.
4. All the interfaces of routers should be in the different network.

The below diagram demonstrates the above rules:



sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

LAB: BASIC IP CONFIGURATION :



ON ROUTER - 1

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**

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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 ROUTER -2

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**

%LINK-5-CHANGED: Interface Serial0/0, changed state to up

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up

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

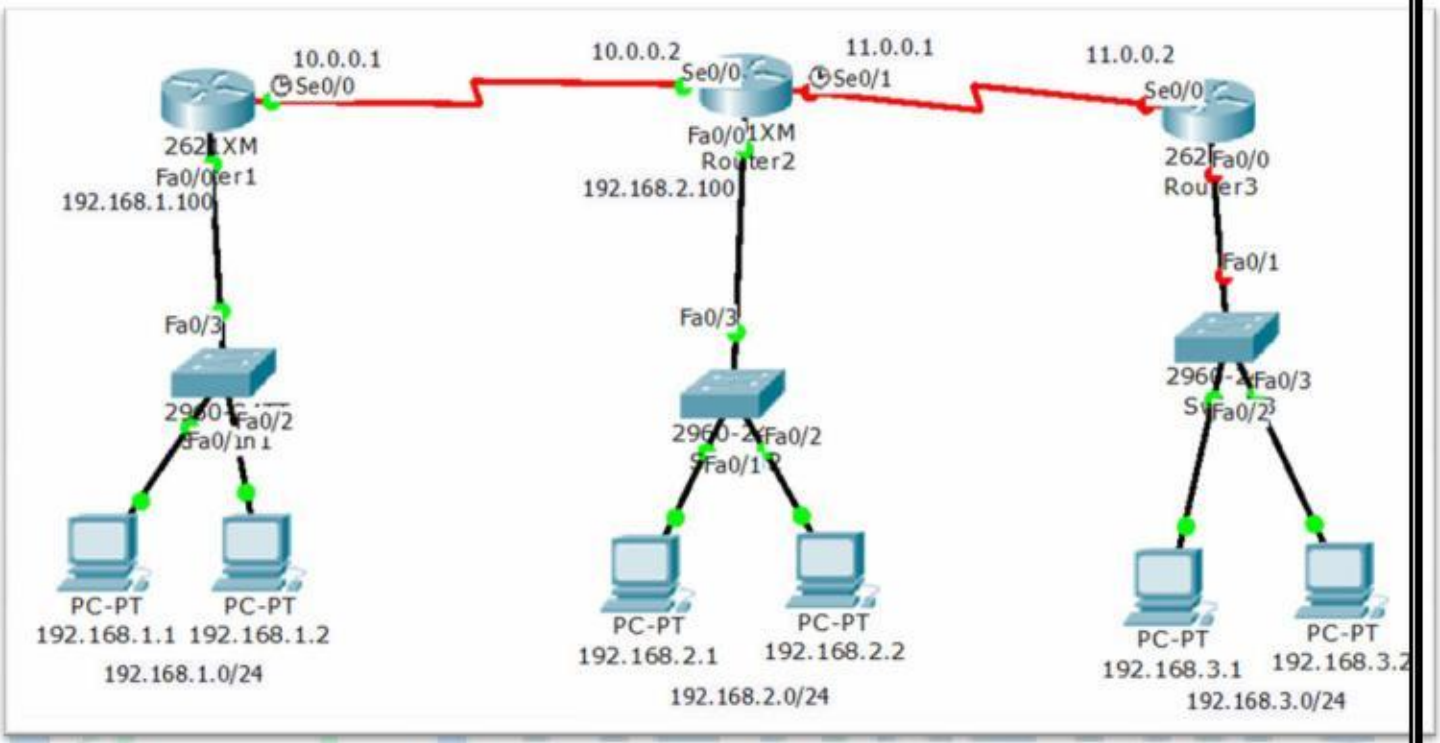
Troubleshooting the connectivity:

Router # show ip interface Brief

1) **Serial is up, line protocol is up**
   - Connectivity is fine.
2) **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
3) **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
4) **Serial is up, line protocol is down**
   - Encapsulation mismatch
   - clock rate command not given on serial interface (only applies in lab scenario)
   - if using PPP , then authentication mismatch

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

LAB : BASIC CONFIGURATION OF THREE ROUTERS



On ROUTER - 1

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**

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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 ROUTER -2

R-2>**enable**

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**

%LINK-5-CHANGED: Interface Serial0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up

R-2(config)# **interface serial 0/1**

R-2(config-if)# **ip address 11.0.0.1 255.0.0.0**

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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	11.0.0.1	YES	manual	down	down

On ROUTER- 3

Router>**enable**

Router#**conf t**

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**

%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(config-if)# end

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

```
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

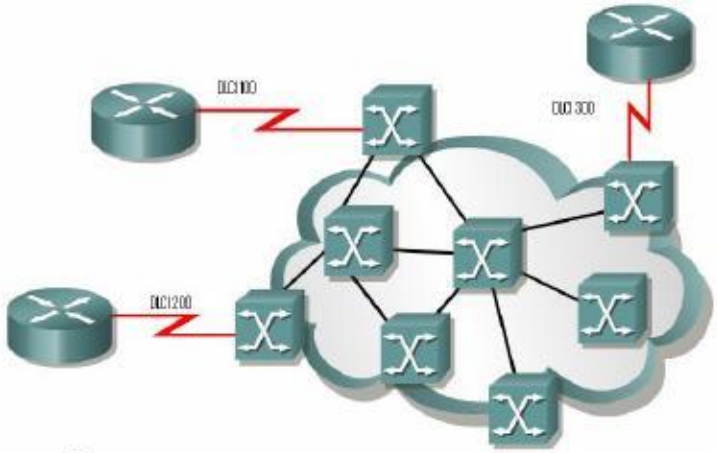
```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/20 ms
```

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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



Frame Relay virtual connection types.

a) PVC
b) SVC

A) **PVC (permanent virtual connection):-**

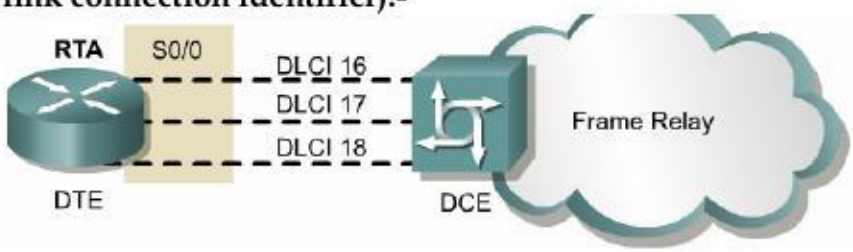
- ✓ Similar to the dedicated leased line.
- ✓ Permanent connection is used.
- ✓ When constant data has to be sent to a particular destination.
- ✓ Always use the same path.

B) **SVC (switched virtual connection)**

- ✓ Virtual connection is dynamically built when data has to be send 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

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

DLCI (data link connection identifier):-



sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

- ✓ 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.

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?

1. CISCO (Default)
2. ANSI
3. Q933A

Note:- On Cisco router LMI is auto sense able no need to configure

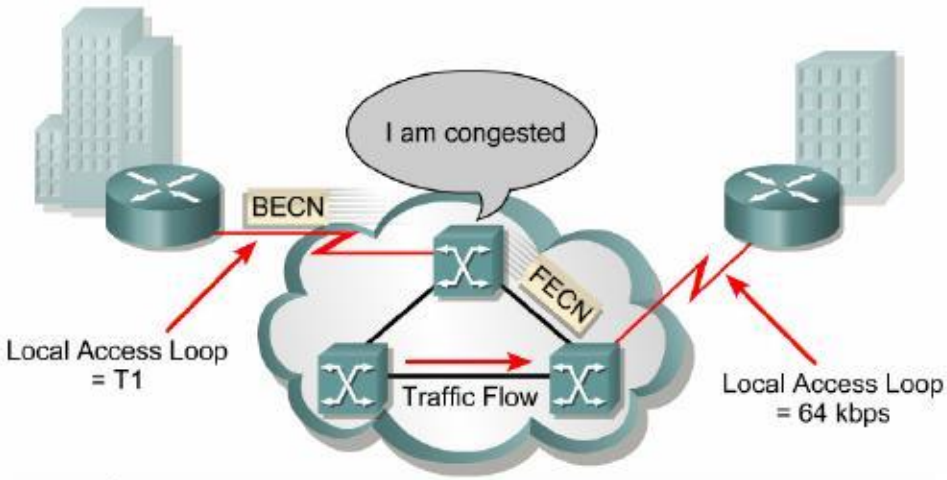
Frame relay **virtual connection status types**:-

1) **Active**: - Connection is up and operation between two DTE's exist
2) **Inactive**: - Connection is functioning between at least between DTE and DCE
3) **Deleted**: - The local DTE/DCE connection is not functioning.

Frame relay network connections.

1)Point to Point
2)Point to Multipoint (NBMA)

Congestion indicates traffic problem in the path when more packets are transmitted in one direction.



Congestion notifications

1) FECN (forward explicit congestion notification)

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

2) BECN (backward explicit congestion notification)

FECN

- ✓ 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

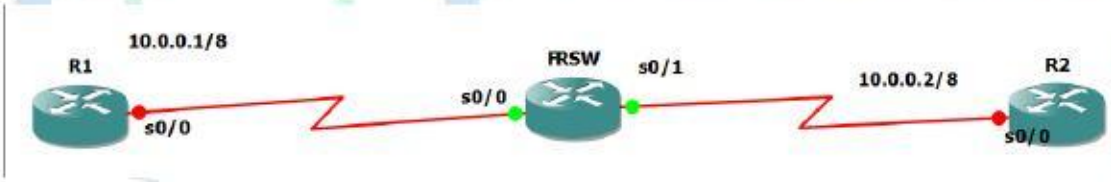
- ✓ Used by the destination (and send to source) to indicate that there is congestion.
- ✓ Used this value inside frame relay frame header in backward direction
- ✓ BCEN =0 indicates no congestion

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

LAB -1

BASIC FR IMPLEMENTATION



R1

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

R2

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


sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

 # sh run int s0/0

Sh ip int brief

On FRSW

En
Conf t
frame-relay switching *(to make the router to act as FR SWITCH)*

int s0/0
no shutdown
encapsulation frame-relay
frame-relay intf-type dce
frame-relay lmi-type cisco
frame-relay route 100 int s0/1 200

int s0/1
no shutdown
encapsulation frame-relay
frame-relay intf-type dce
frame-relay lmi-type cisco
frame-relay route 200 int s0/0 100

VERIFY
 # sh run int s0/0

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

FRSW#sh frame-relay route

Input Intf	Input Dlci	Output Intf	Output Dlci	Status
Serial0/0	100	Serial0/1	200	active

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/55/104 ms

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 00:01:02

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

ROUTING

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.

Types of Routing

1. Static Routing
2. Default Routing
3. Dynamic Routing

Static Routing

- It is configured manually by the Administrator.
- Mandatory need for the Destination Network ID
- Used for Small organizations
- Administrative distance for Static Route is 0 or 1.

Advantages:

- 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
- _____

Configuring Static Route

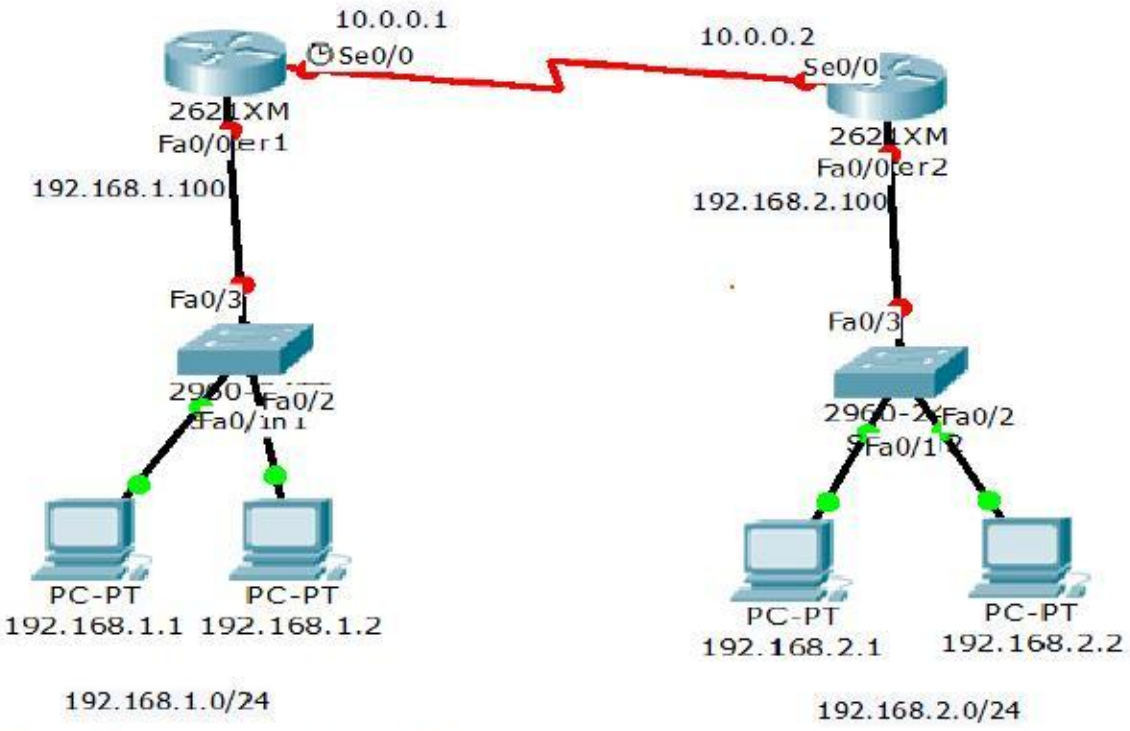
Router(config)# ip route **<Destination Network ID>** **<Destination Subnet Mask>** **<Next-hop IP address >**

Or

Router(config)# ip route **<Destination Network ID>** **<Destination Subnet Mask>** **<Exitinterface>**

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

LAB: STATIC ROUTING



STEPS:

Pre-requirement for LAB (check previous labs)

1) Design the topology (connectivity)
2) Assign the IP address according to diagram
3) Make sure that interfaces used should be in UP UP state

What we do in this lab

4) Static routing
5) 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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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.***
- ***In order to communicate we need to implement any of the routing (here in this we use static routing)***

On R-1

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

R-1#sh ip route

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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

On R-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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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

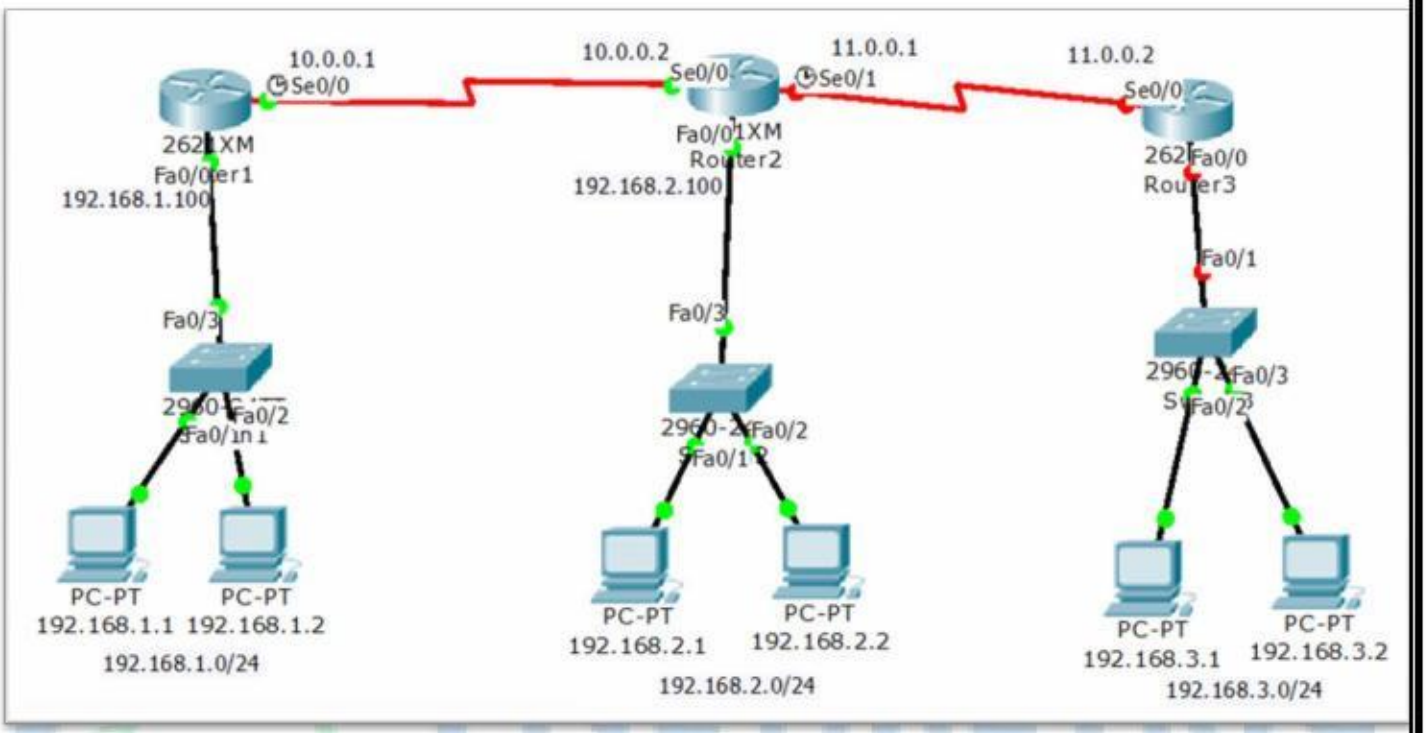
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/16/31 ms

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 = 10/15/18 ms

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

LAB : STATIC ROUTING WITH 3 ROUTERS



STEPS:

Pre-requirement for LAB (check previous labs)

1) Design the topology (connectivity)
2) Assign the IP address according to diagram
3) Make sure that interfaces used should be in UP UP state

What we do in this lab

4) Static routing
5) Verify Routing table and reachability between the LAN's (using PING and TRACE commands)

R-1#sh 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#sh ip route

Gateway of last resort is not set

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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#sh 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

On Router- 1

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**

On Router – 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**

On Router – 3

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

R-2#show ip route

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

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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

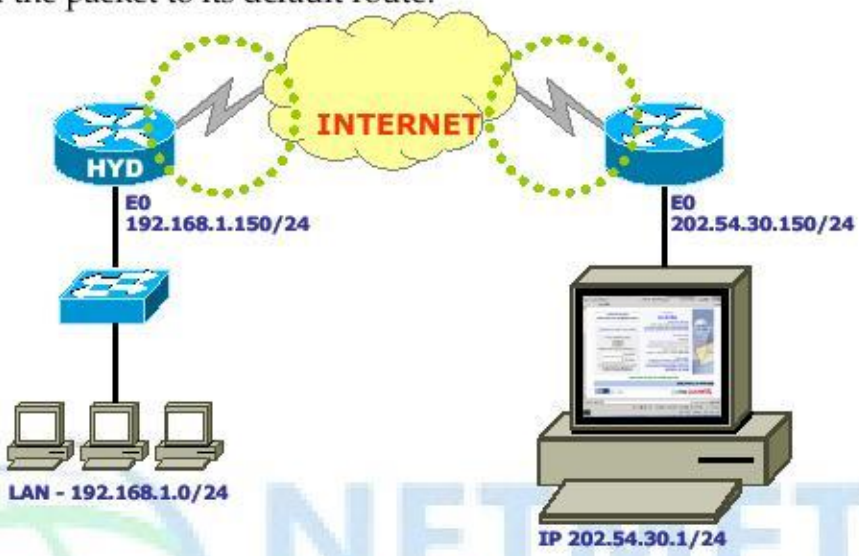
R-3#ping 192.168.1.1

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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.



Configuring Default Route

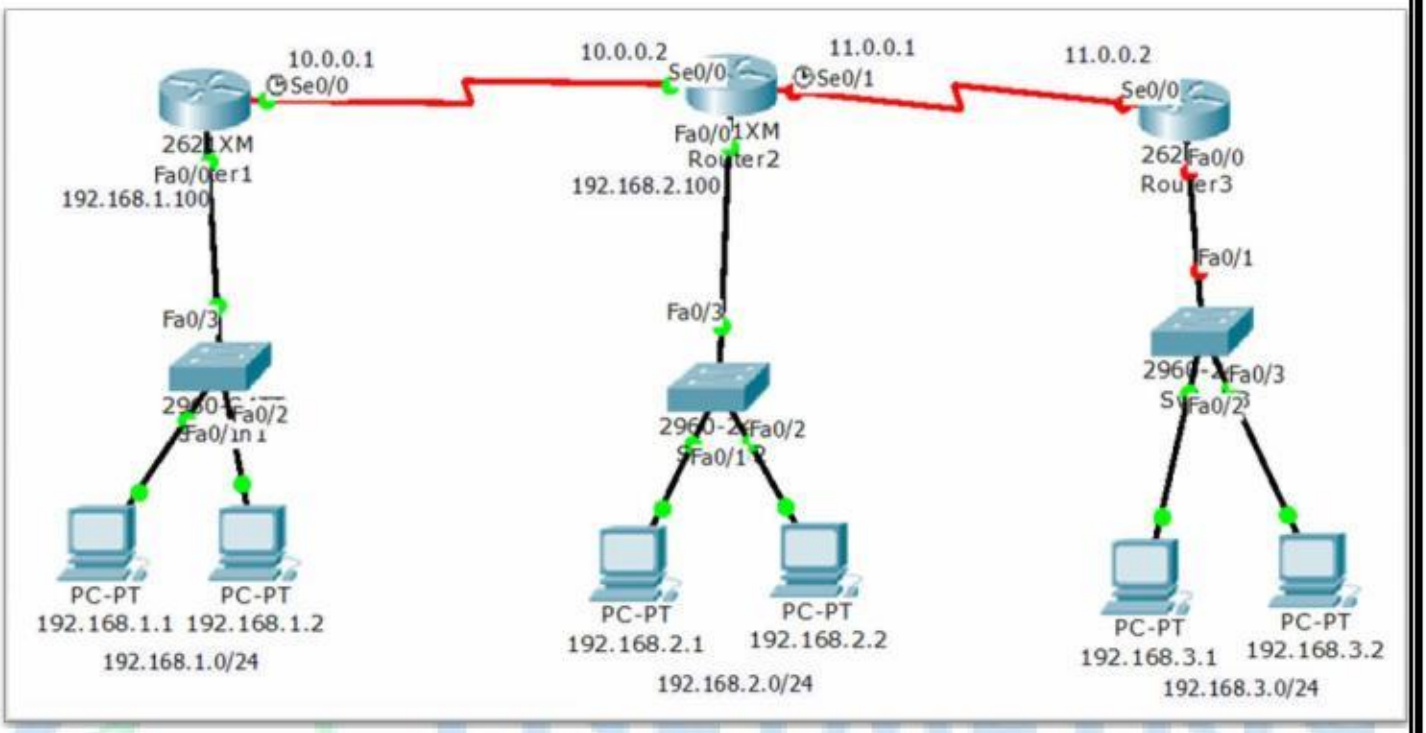
Router(config)# ip route <Destination Network ID> <Destination Subnet Mask> <Next-hop IP address >

Or

Router(config)# ip route <Destination Network ID> <Destination Subnet Mask> <Exit interface>

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

LAB : DEFAULT ROUTING



STEPS:

Pre-requirement for LAB (check previous labs)

1) Design the topology (connectivity)
2) Assign the IP address according to diagram
3) Make sure that interfaces used should be in UP UP state

What we do in this lab

4) Default route used on R1 and R3 , static routing on R2
5) Verify Routing table and reachability between the LAN's (using PING and TRACE commands)

R-1#sh 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#sh ip route

Gateway of last resort is not set

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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#sh 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

ON ROUTER- 1

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

ON ROUTER – 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**

On Router – 3

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

R-1#sh 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#sh 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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

R-3#sh 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	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**

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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

DISTANCE VECTOR PROTOCOL	LINK STATE PROTOCOL	HYBRID PROTOCOL (Advance Distance vector Protocol)
• Works with Bellman Ford algorithm • Periodic updates • Classful routing protocol • Full Routing tables are exchanged • Updates are through broadcast • Example: RIP v1, RIPv2 , IGRP	• Works with Dijkstra algorithm • Incremental updates • Classless routing protocol • Missing routes are exchanged • Updates are through multicast • Example : OSPF, IS-IS • Link state updates	• Works with DUAL algorithm • Incremental updates • Classless routing protocol • Missing routes are exchanged • Updates are through multicast • Example : EIGRP • Also called as Advance Distance vector Protocol

Classful Protocols:

- Classful routing protocol do not carry the subnet mask information along with updates
- which means that all devices in the network must use the same subnet mask
    - Ex : RIPv1 , IGRP

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

Classless Protocols:

- Classful routing protocol carry the subnet mask information along with updates
- That's why they support sub networks and default networks also
    - Ex : RIPv2 , EIGRP , OSPF, 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

ROUTING INFORMATION PROTOCOL V1

- 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 Max routers: 16
- Load Balancing of 4 equal paths
- Used for small organizations
- Periodic updates and Exchange entire routing table for every 30 seconds

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 holddown long enough for all routers in the topology to learn about the unreachable network

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

Convergence time is the time taken by the router to use alternate route if the best route is down.

RIP Version 2

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

Advantages of RIP

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

Disadvantage 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

Configuring RIPv 1

Router(config)# **router rip**

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

Configuring RIP v2

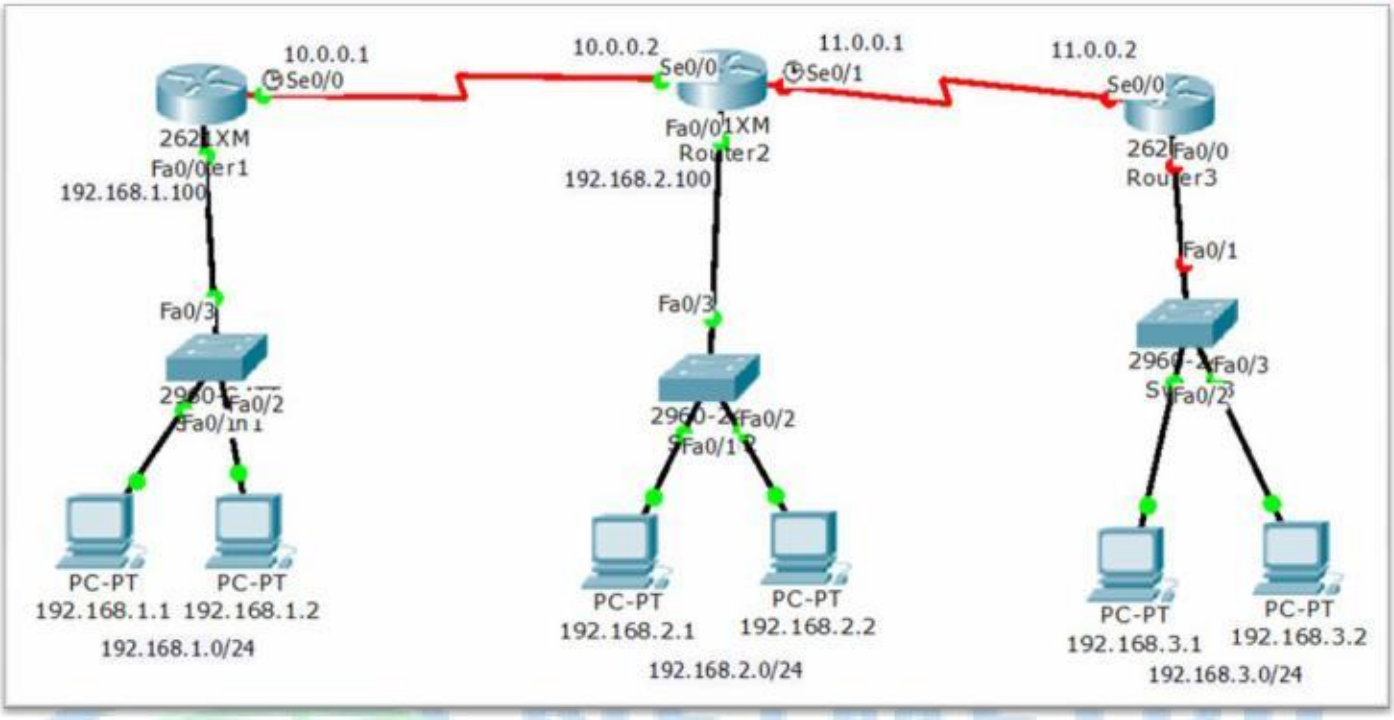
Router(config)# **router rip**

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

Router(config-router)# **version 2**

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

LAB: DYNAMIC ROUTING USING RIPV2



STEPS:

Pre-requirement for LAB (check previous labs)

1) Design the topology (connectivity)
2) Assign the IP address according to diagram
3) Make sure that interfaces used should be in UP UP state

What we do in this lab

4) Dynamic routing using RIPv2
5) Verify Routing table and reachability between the LAN's *(using PING and TRACE commands)*

R-1#sh 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#sh ip route

Gateway of last resort is not set

C 10.0.0.0/8 is directly connected, Serial0/0

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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

R-3#sh 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

ON ROUTER- 1

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**

ON ROUTER – 2

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**

On Router – 3

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#sh ip route

Gateway of last resort is not set

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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#sh 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#sh 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)

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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

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.

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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

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 – 1 – 64512 Private – 64513 – 65535

Private AS: used within the same service providers

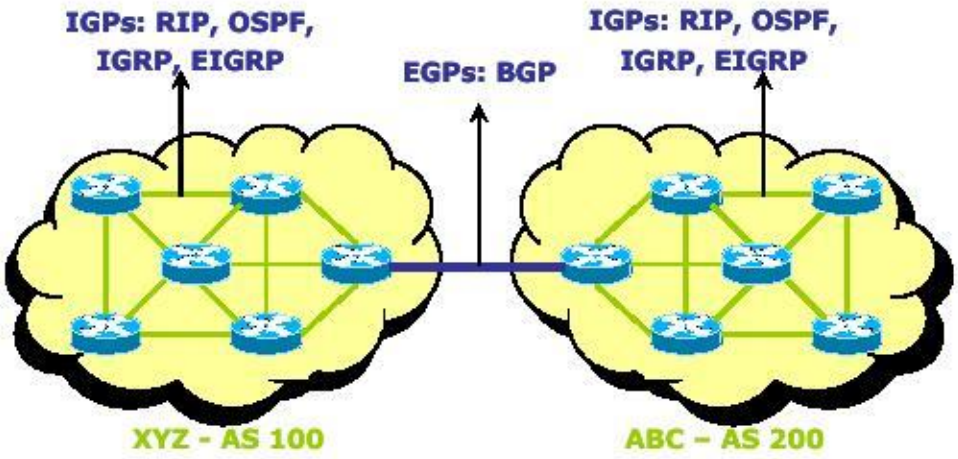
Public AS: used in between multiple service providers

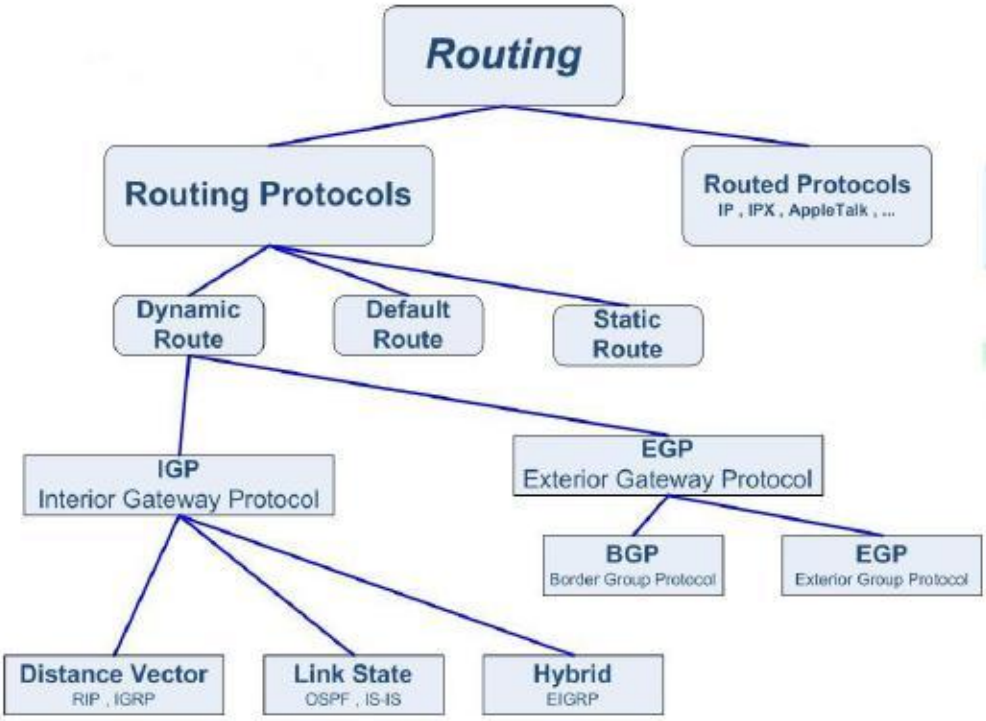
Routing Protocol Classification

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

- **IGPs** operate within an autonomous system
- **EGPs** connect different autonomous systems

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com



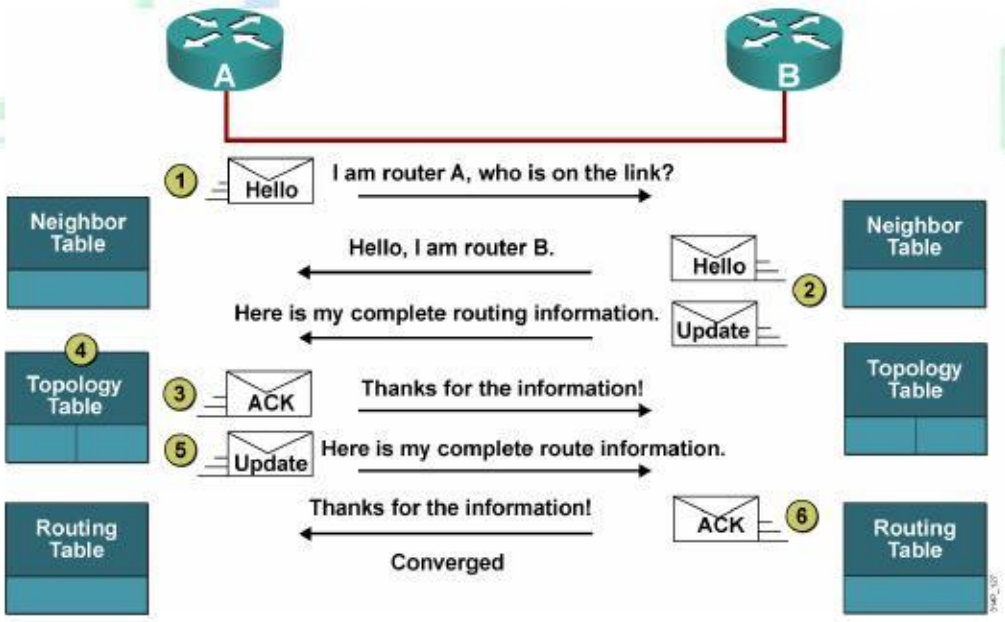


sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL

Cisco calls EIGRP a distance-vector routing protocol or sometimes an advanced distance-vector or even a hybrid routing protocol

- 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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

- 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

Disadvantages of EIGRP
- Works only on Cisco Routers

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.*

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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
```

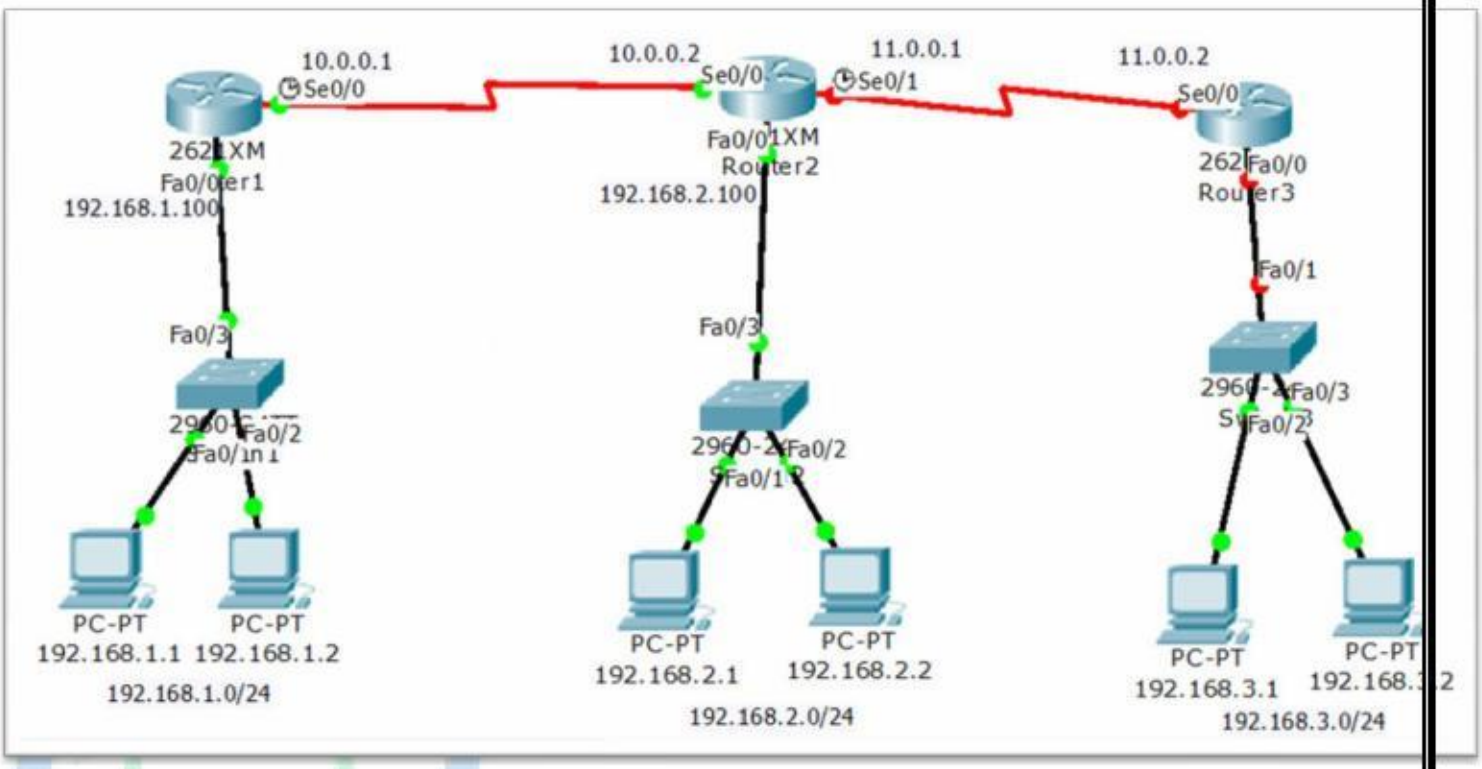
EIGRP has a maximum hop count of 100, but it can be set up to 255.

```
Pod1R1(config)#router eigrp 10
Pod1R1(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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

LAB: DYNAMIC ROUTING USING EIGRP



STEPS:

Pre-requirement for LAB (check previous labs)

1) Design the topology (connectivity)
2) Assign the IP address according to diagram
3) Make sure that interfaces used should be in UP UP state

What we do in this lab

4) Dynamic routing using EIGRP
5) Verify Routing table and reachability between the LAN's (using PING and TRACE commands)

R-1#sh 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#sh ip route

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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#sh 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

ON ROUTER- 1

R-1(config)# **router eigrp 100**

R-1(config-router)# **network 192.168.1.0**

R-1(config-router)# **network 10.0.0.0**

ON ROUTER – 2

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

ON ROUTER – 3

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 (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
0	10.0.0.1	Se0/0	10	00:03:44	40	1000	0	8
1	11.0.0.2	Se0/1	12	00:01:10	40	1000	0	7

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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#sh 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#sh 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:

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

```
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#sh 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=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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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

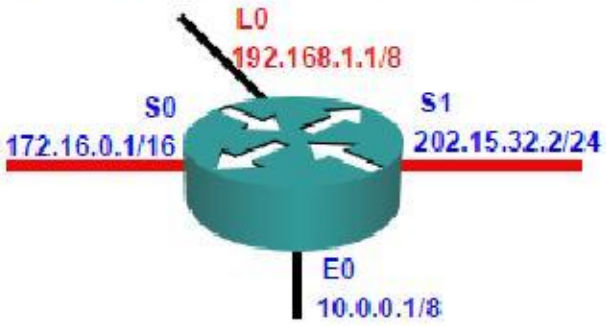
sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

OSPF

- 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

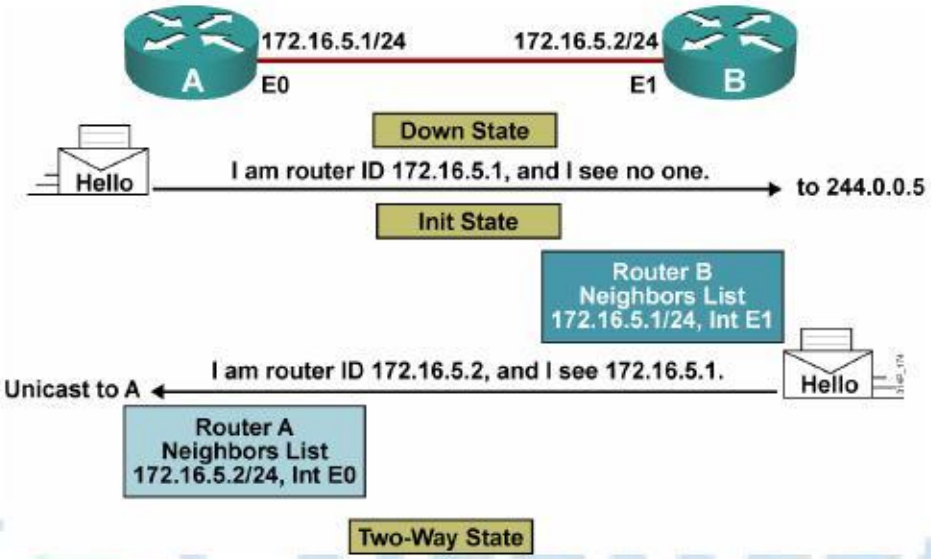
- The highest IP address of the active physical interface of the router is Router ID.
- If logical interface is configured, the highest IP address of the logical interface is Router ID



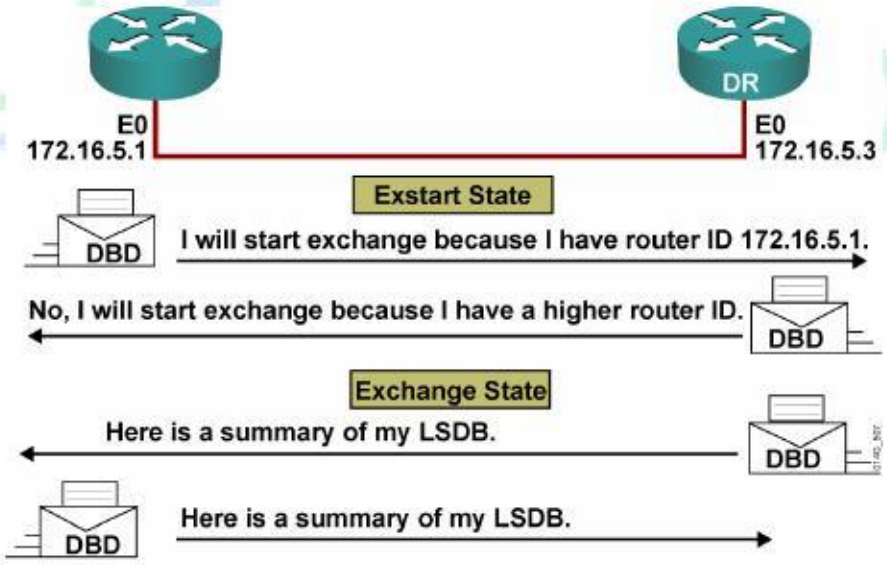
sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

OSPF SEVEN STAGE PROCESS

1) Establishing Bidirectional Communication

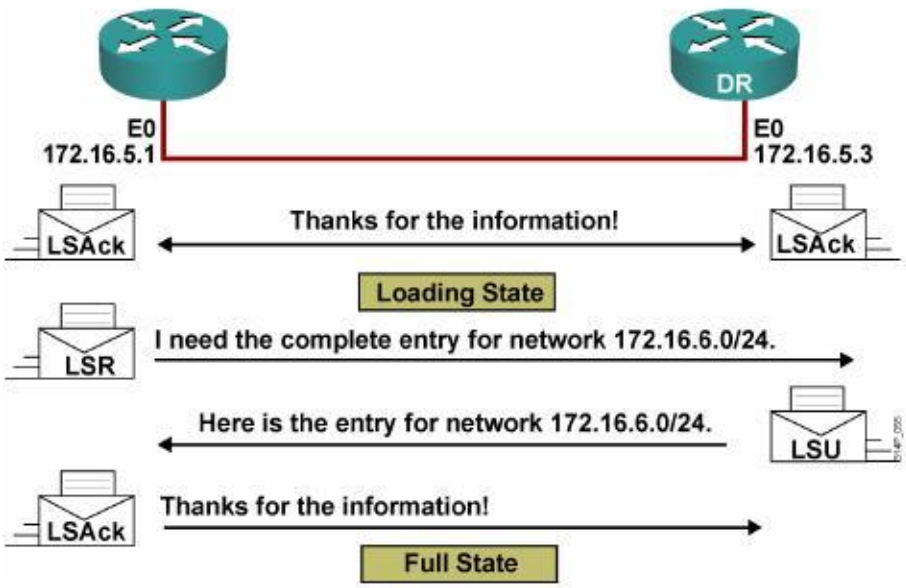


2) Discovering the Network Routes



sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

3) Adding the Link-State Entries



OSPF maintains three 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***

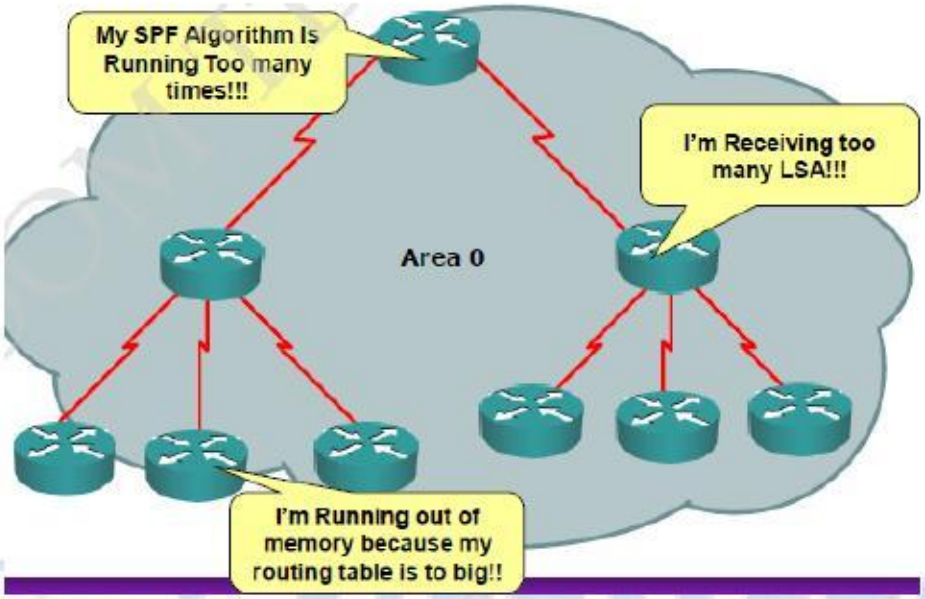
Link-State Data Structure: Network Hierarchy

Link-state routing can have hierarchical network
This two-level hierarchy consists of the following:

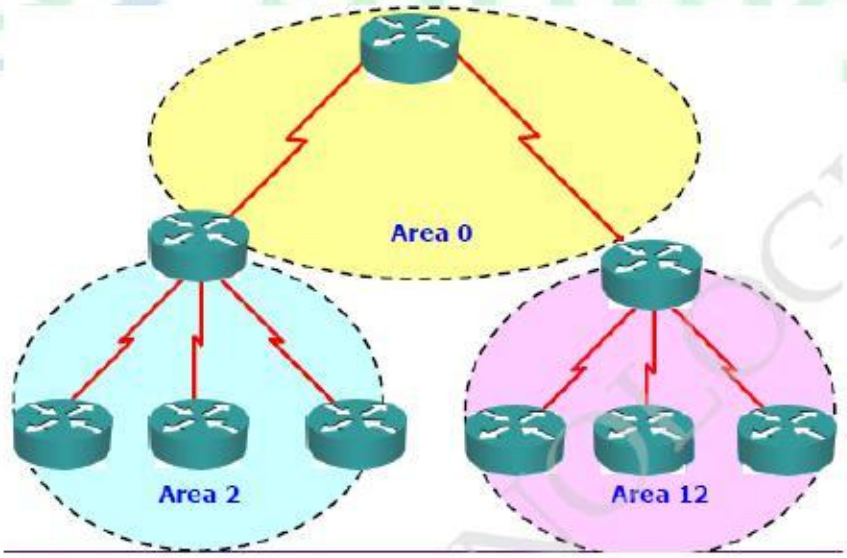
- Transit area (backbone or area 0)
- Regular areas (non-backbone areas)

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

Issue of Maintaining of large OSPF network



OSPF Multi Area



- 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.

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

- 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.

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.

Advantages of OSPF

- Open standard
- No hop count limitations
- Loop free
- Faster convergence

Disadvantages

- Consume more CPU resources
- Support only equal cost balancing
- Support only IP protocol don't work on IPX and APPLE Talk

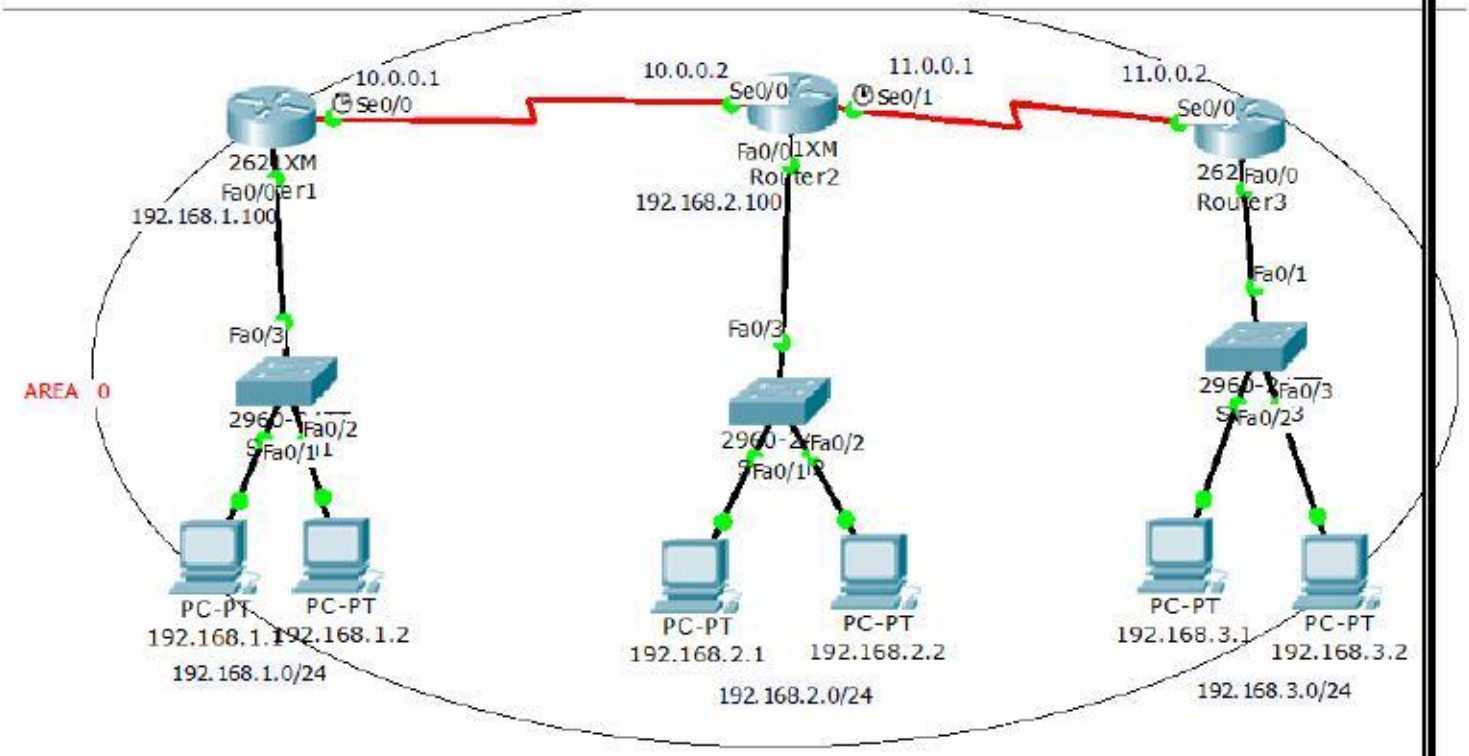
sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

Configuring OSPF

Router(config)# **router ospf <process ID >**

Router(config-router)# **network <Network ID> <wildcard mask> area <area id>**

LAB : DYNAMIC ROUTING USING OSPF IN SINGLE AREA



STEPS:

Pre-requirement for LAB (check previous labs)

1) Design the topology (connectivity)
2) Assign the IP address according to diagram
3) Make sure that interfaces used should be in UP UP state

What we do in this lab

4) Dynamic routing using OSPF single area
5) Verify Routing table and reachability between the LAN's (using PING and TRACE commands)

R-1#sh ip route

Gateway of last resort is not set

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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

R-2#sh 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#sh 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

On Router- 1

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**

On Router – 2

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

On Router – 3

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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#sh 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-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
```


sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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	5 ms	8 ms	8 ms	192.168.1.100
2	12 ms	9 ms	8 ms	10.0.0.2

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

```
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

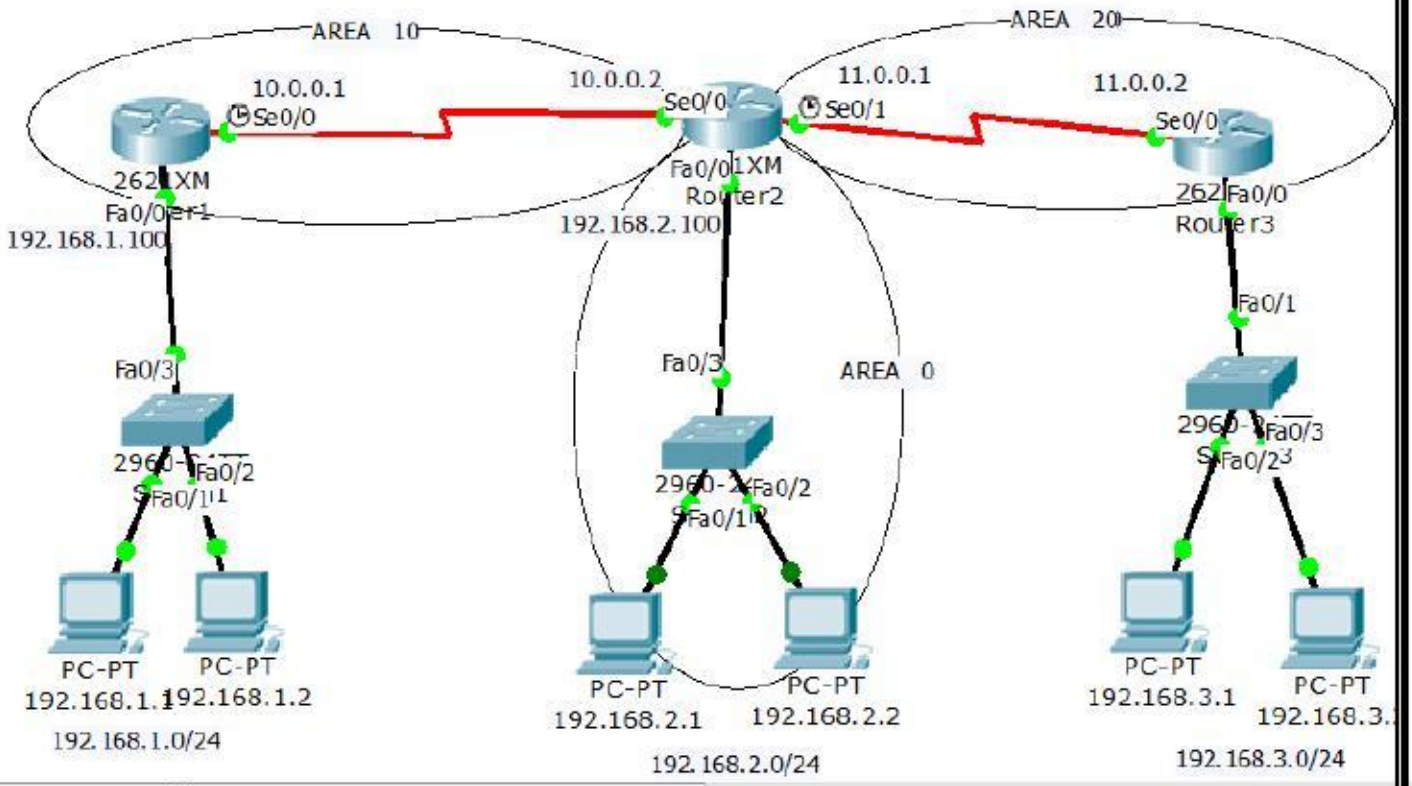
```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/16/31 ms
```

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
```


sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

LAB: DYNAMIC ROUTING USING OSPF MULTIPLE AREA



STEPS:

Pre-requirement for LAB (check previous labs)

1) Design the topology (connectivity)
2) Assign the IP address according to diagram
3) Make sure that interfaces used should be in UP UP state

What we do in this lab

4) Dynamic routing using OSPF multiple area
5) Verify Routing table and reachability between the LAN's (using PING and TRACE commands)

R-1#sh 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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

R-2#sh 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#sh 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

On Router- 1

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**

ON ROUTER – 2

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

ON ROUTER – 3

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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-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#sh 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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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	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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

ACCESS CONTROL LIST

- ACL is a set of rules which will allow 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 ACCESS LIST	EXTENDED ACCESS LIST
• The access-list number range is **1 – 99** • Can block a Network, Host and Subnet • All services are blocked. • Implemented closest to the destination. • Filtering is done based on only source IP address	• The access-list number range is **100 – 199** • Can block a Network, Host, Subnet and Service • Selected services can be blocked. • Implemented closest to the source. • Filtering is done based on source IP , destination IP , protocol, port no

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.

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)**

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

- 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

EX-1

255.255.255.255
– **255.255.255. 0**
---
0. 0. 0. 255

EX-2

255.255.255.255
– **255.255.255.240**
---
0. 0. 0. 15
==========

Ex-3

255.255.255.255
– **255.255.255.224**
---
0. 0. 0. 31

- Wildcards are used with the host or 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**

Creation of Standard Access List

Router(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>**

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

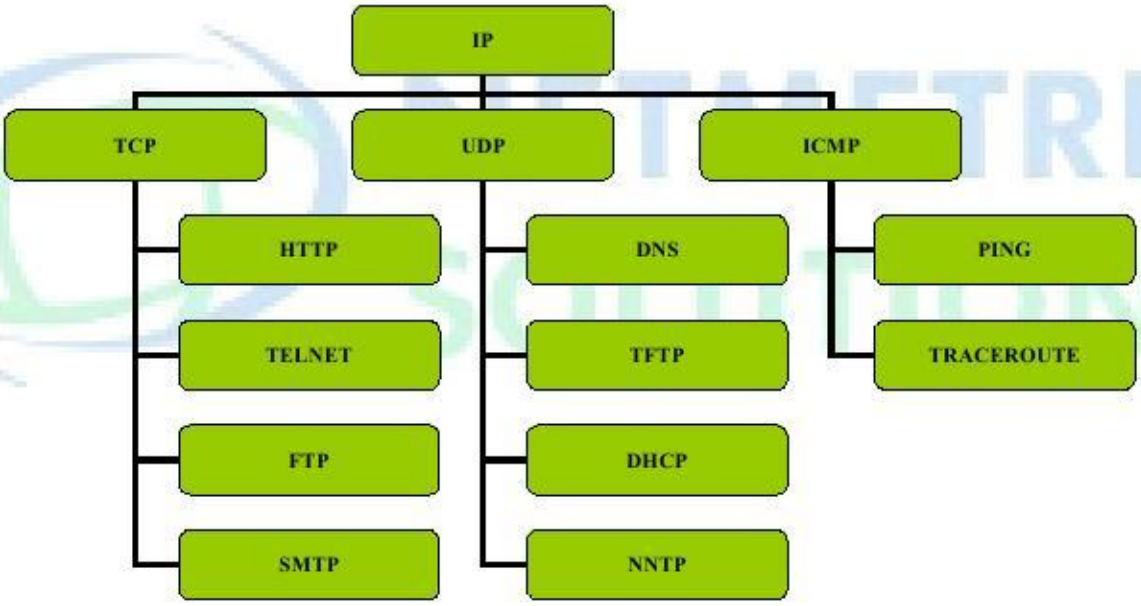
Creation of Extended Access List

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 **layer 4 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.

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

- If you were to choose IP, you wouldn't be allowed to specify a specific application protocol later

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.
- One Main Advantage is Editing of ACL is Possible (i.e) 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>**

Implementation of Standard Named Access List

Router(config)**#interface <interface type><interface no>**

Router(config-if)**#ip access-group <name> <out/in>**

Creation 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>

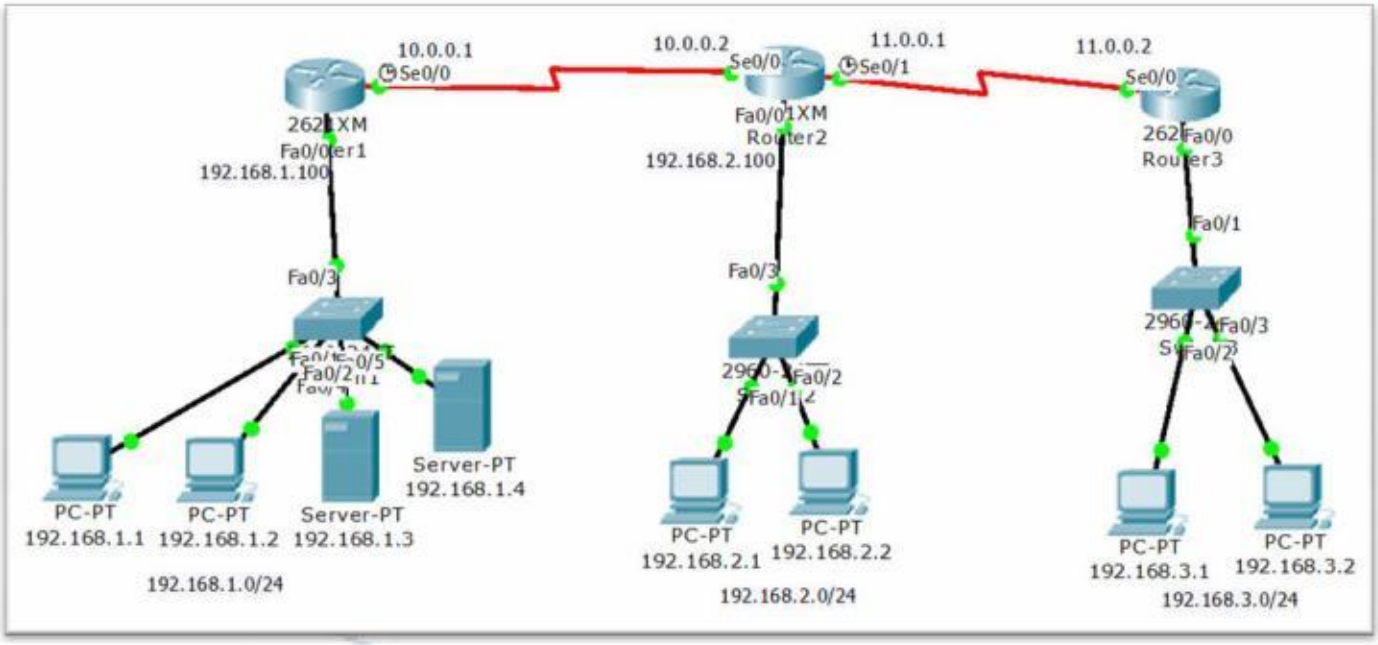
Implementation of Extended Named Access List

Router(config)**#interface <interface type><interface no>**

Router(config-if)**#ip access-group <name> <out/in>**

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

LAB – 1: IMPLEMENTING STANDARD ACCESS-LIST



Pre-requirement for LAB (check previous labs)

1) Design the topology (connectivity)
2) Assign the IP address according to diagram
3) Make sure that interfaces used should be in UP UP state
4) Any dynamic routing Protocol or static routing
5) 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 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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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.....: 192.168.1.2
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 192.168.2.1: bytes=32 time=16ms TTL=126
Reply from 192.168.2.1: bytes=32 time=22ms TTL=126
Reply from 192.168.2.1: bytes=32 time=23ms TTL=126
Reply from 192.168.2.1: bytes=32 time=11ms 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 192.168.2.1: bytes=32 time=21ms TTL=126
Reply from 192.168.2.1: bytes=32 time=23ms TTL=126
Reply from 192.168.2.1: bytes=32 time=22ms TTL=126
Reply from 192.168.2.1: bytes=32 time=23ms TTL=126

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

ON ROUTER – 2

Creating the ACL rules according to 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)#**interface fastEthernet 0/0**

R-2(config-if)#**ip access-group 15 out**

Verification:

R-2#sh 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:

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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=31ms 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=24ms TTL=126

PC>ipconfig

IP Address.....: 192.168.3.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.3.100

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

LAB 2:
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 who can telnet and who should not
- 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 only the **hosts 192.168.1.1 and 192.168.1.2** to telnet R1. any other host should be denied of they try to telnet R1

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
```


sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

Verification:

PC>ipconfig

IP Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100

PC>telnet 192.168.1.100
Trying 192.168.1.100 ...Open

User Access Verification

Password:

PC>ipconfig

IP Address.....: 192.168.1.2
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100

PC>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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

IP Address.....: 192.168.1.4
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.100

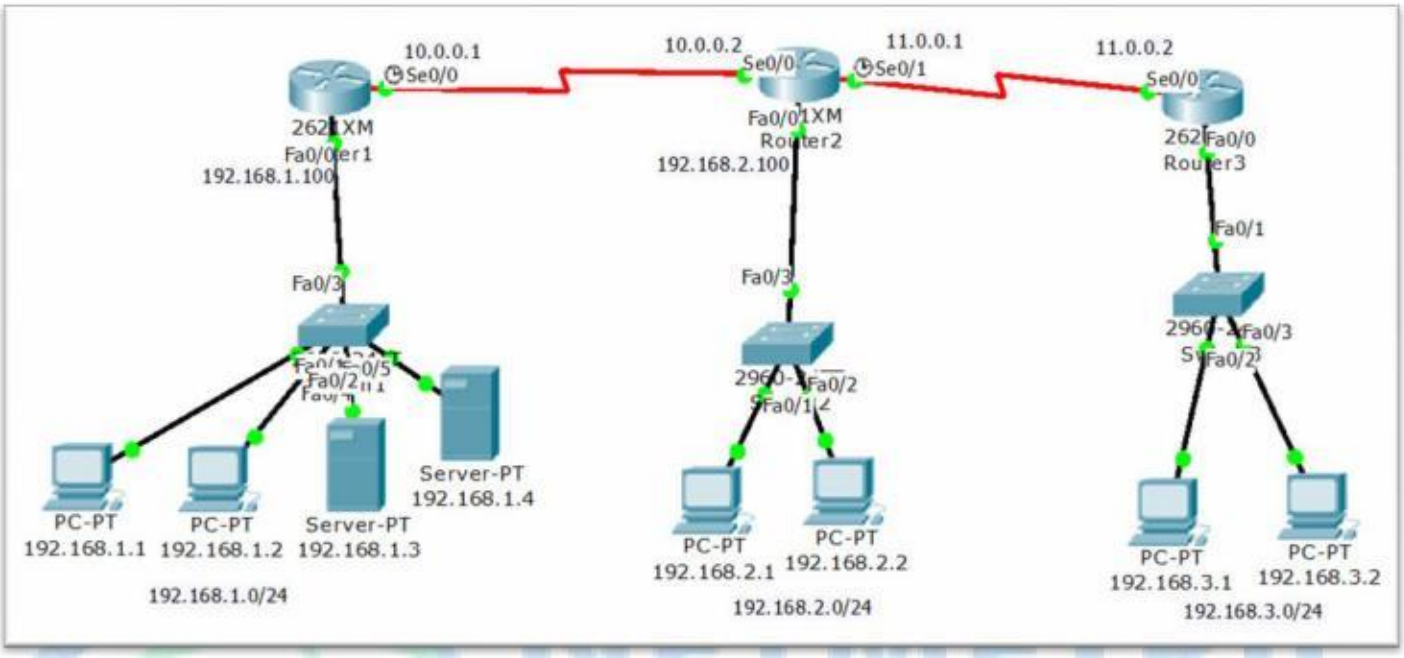
SERVER>telnet 192.168.1.100
Trying 192.168.1.100 ...
% Connection refused by remote host
SERVER>

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

---

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

LAB -3: IMPLEMENTING EXTENDED ACCESS-LIST



Pre-requirement for LAB (check previous labs)

1) Design the topology (connectivity)
2) Assign the IP address according to diagram
3) Make sure that interfaces used should be in UP UP state
4) Any dynamic routing Protocol or static routing
5) 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 should not access 192.168.1.3 HTTP service
- Deny the users on LAN 192.168.3.0 should not access 192.168.1.4 FTP service
- Deny the users on LAN 192.168.3.1 should not access 192.168.1.3 HTTP service
- Deny the users on LAN 192.168.2.0 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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

On Router – 1

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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**

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

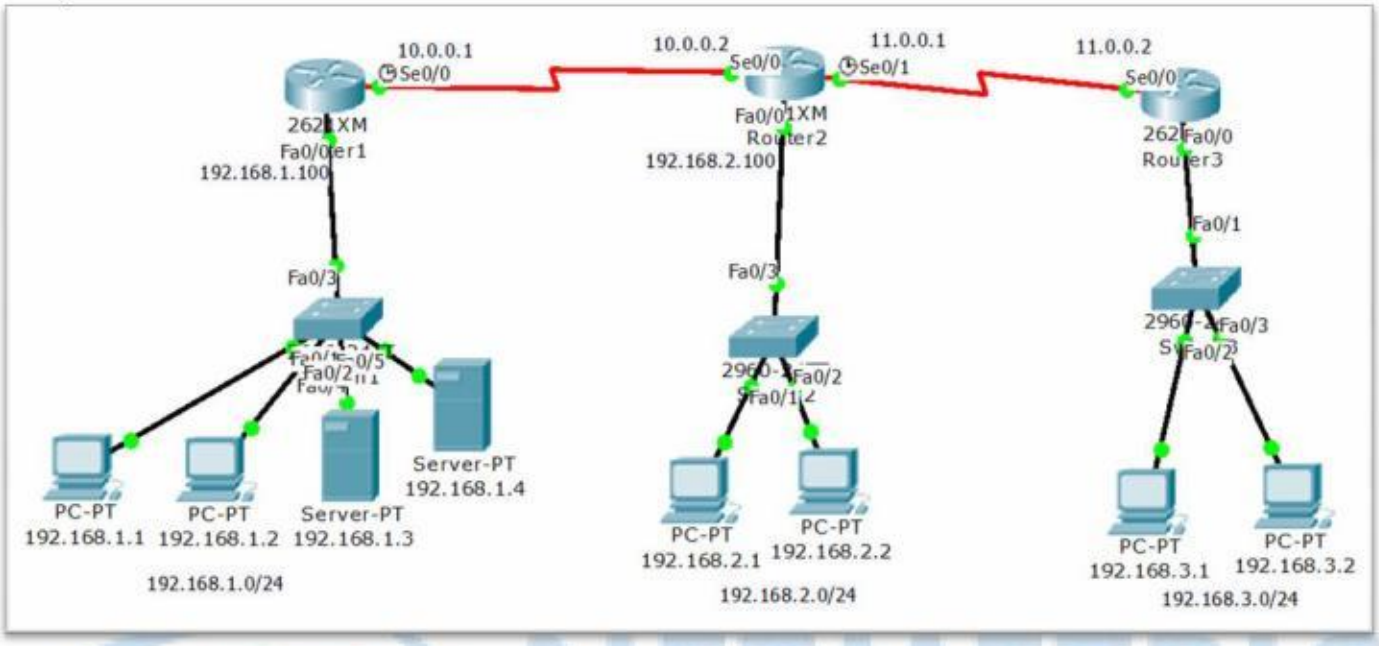
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=20ms TTL=125
Reply from 192.168.1.1: bytes=32 time=27ms TTL=125
Reply from 192.168.1.1: bytes=32 time=13ms TTL=125
Reply from 192.168.1.1: bytes=32 time=25ms TTL=125

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

LAB – 4:

IMPLEMENT THE STANDARD ACL WITH THE SAME RULES AS LAB -1 USING NAMED ACL



NOTE: Refer LAB – 3 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 – 1

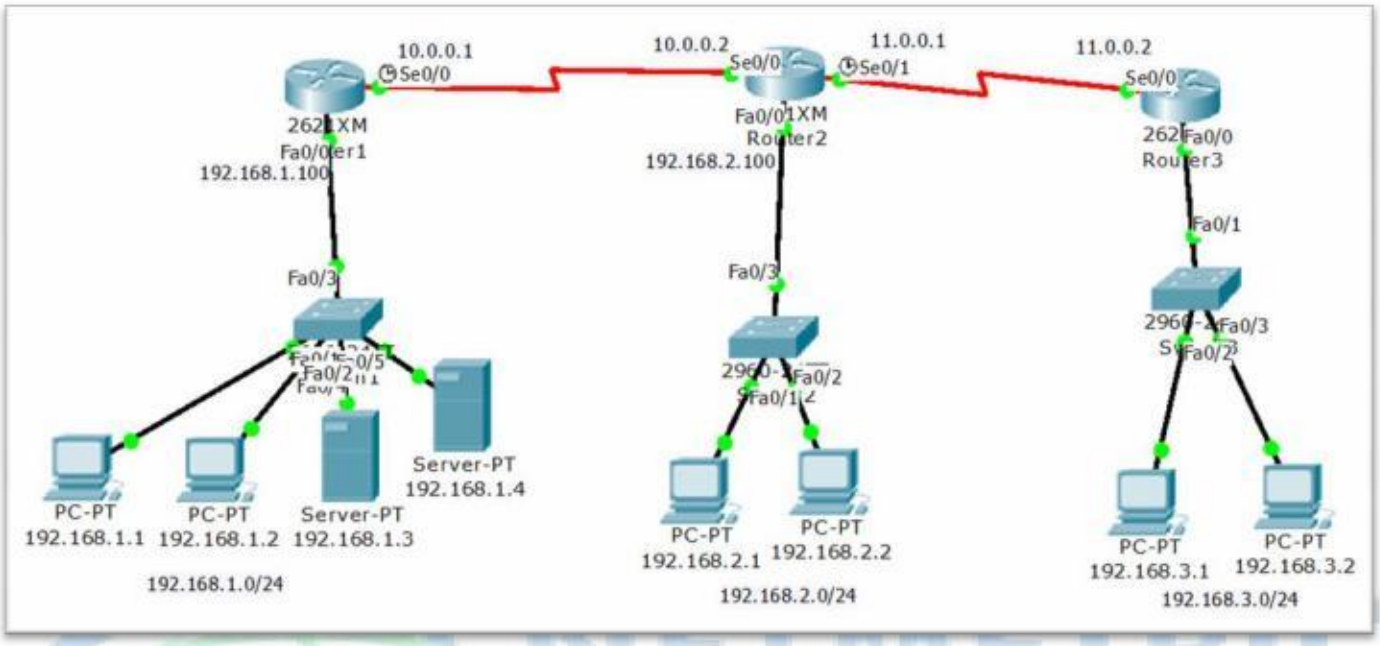
R-2#sh access-lists

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

LAB – 5

IMPLEMENT THE EXTENDED ACL WITH THE SAME RULES AS LAB -2 USING NAMED ACL



NOTE: Refer LAB – 3 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**

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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 – 3

R-1#sh 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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

NETWORK ADDRESS TRANSLATION

- 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:

1. to handle a shortage of IPv4 addresses
2. 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.

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

Types of NAT:-

1. Dynamic NAT
2. Static NAT
3. PAT

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)*

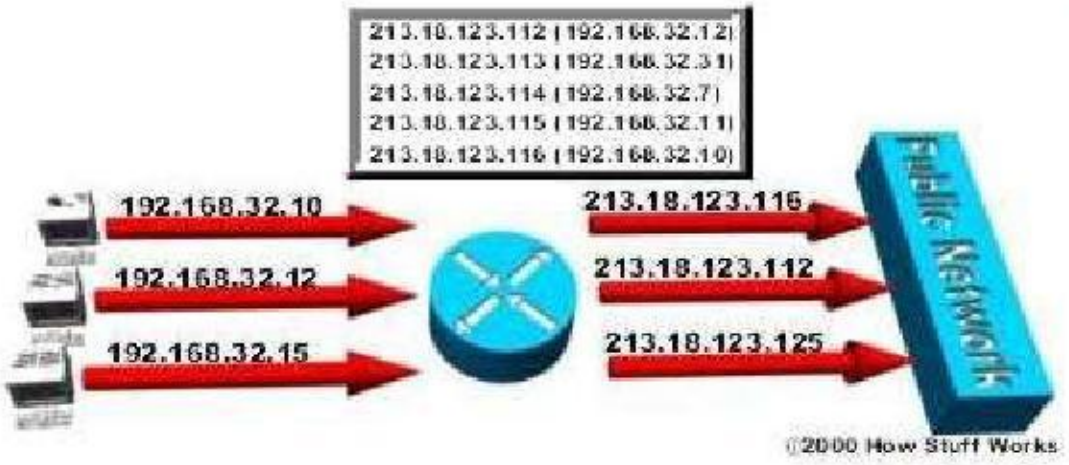
(Config)# **interface s0/0**

(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.

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com



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)*

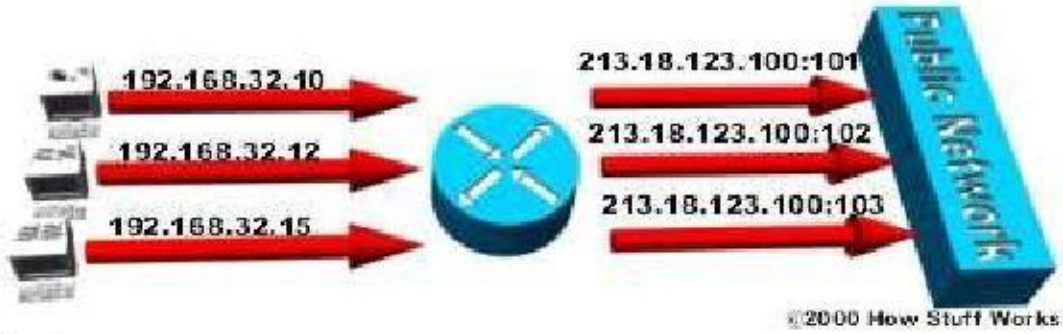
(Config)# **interface s0/0**

(Config-if)# **ip nat outside** *(interface facing towards ISP)*

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com



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**

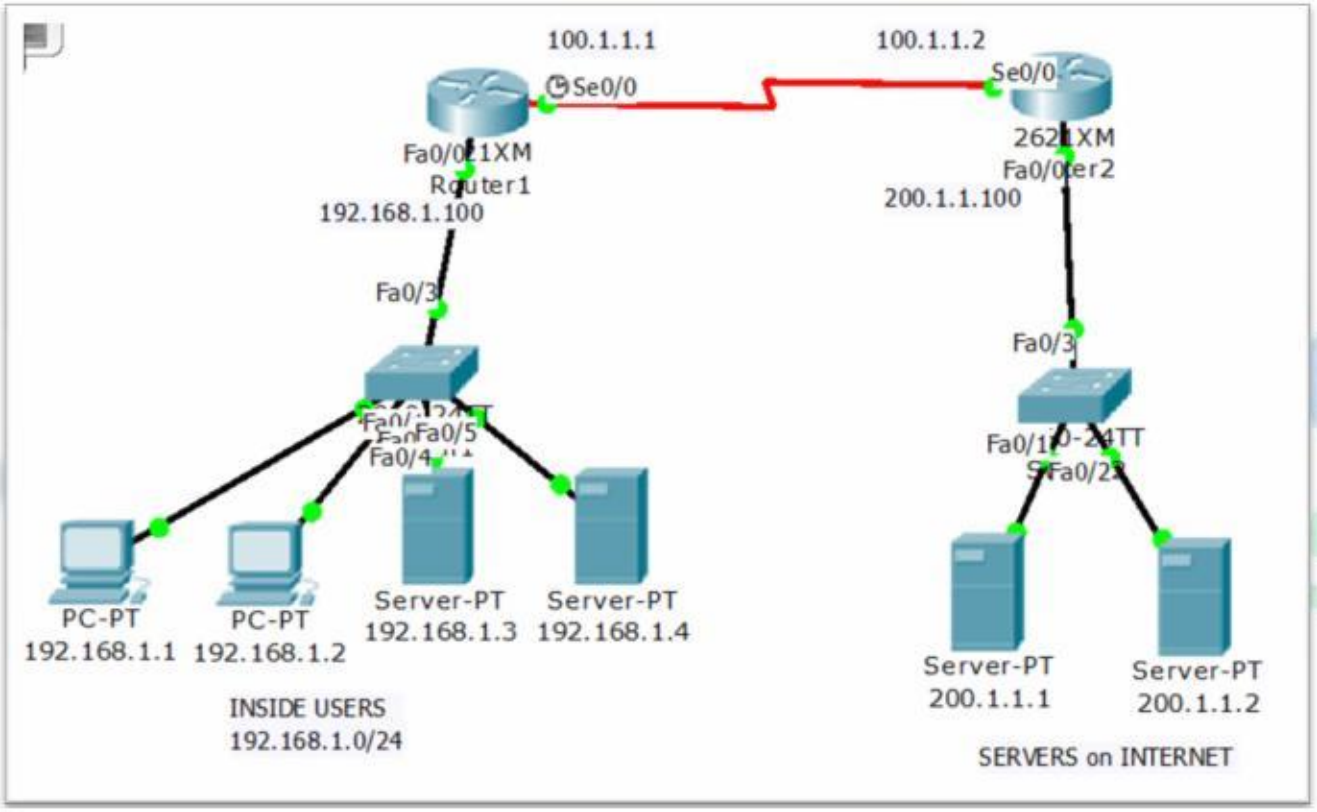
(Config-if)# **ip nat outside** *(interface facing towards ISP)*

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

LAB – 1 Implementing STATIC NAT

Configure the following translations

PRIVATE IP	PULIC 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#sh ip int brief

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.1.100	YES	manual	up	up

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

```
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#sh ip int 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#**conf terminal**
ISP(config)# **ip route 0.0.0.0 0.0.0.0 100.1.1.1**

Configuring 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)

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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#sh 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:

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

R-1#sh 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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

LAB – 2

Implement Dynamic NAT and make sure 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 LAB – 1**
- **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**

Configuring 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)

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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#sh 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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

LAB – 3

Implement PAT (Dynamic NAT Overload) and make sure 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 LAB – 2**
- **Remove the dynamic 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**

Configuring 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)

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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#sh ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
tcp	50.1.1.1:1029	192.168.1.1:1029	100.1.1.2:23	100.1.1.2:23
tcp	50.1.1.1:1026	192.168.1.2:1026	100.1.1.2:23	100.1.1.2:23
tcp	50.1.1.1:1024	192.168.1.3:1026	100.1.1.2:23	100.1.1.2:23
tcp	50.1.1.1:1025	192.168.1.4:1026	100.1.1.2:23	100.1.1.2:23

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

LAB – 4

Implement PAT (Dynamic NAT Overload) and make sure 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 LAB – 3**
- **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** ***overload***

R-1(config)**#no ip nat pool CCNA 50.1.1.1 50.1.1.1 netmask 255.255.255.248**

R-1(config)**#no access-list 55**

Configuring 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:

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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#sh ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
tcp	100.1.1.1:1029	192.168.1.1:1029	100.1.1.2:23	100.1.1.2:23
tcp	100.1.1.1:1026	192.168.1.2:1026	100.1.1.2:23	100.1.1.2:23
tcp	100.1.1.1:1024	192.168.1.3:1026	100.1.1.2:23	100.1.1.2:23
tcp	100.1.1.1:1025	192.168.1.4:1026	100.1.1.2:23	100.1.1.2:23

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

Hub	Switch
• It is a Physical layer device (Layer 1) • It has no intelligence. • It works with 0's and 1's (Bits) • It always do broadcasts • It works with shared bandwidth • **It has 1 Broadcast Domain** • **It has 1 Collision Domain** • Collisions are identified using Access Methods called CSMA/CD and CSMA/CA	• It is Datalink layer device (Layer 2) • Its is An Intelligent device • It works with Physical addresses (i.e. MAC addresses) • It uses broadcast and Unicast • It works with fixed bandwidth • It has **1 Broadcast domain** • **Number of Collision domains depends upon the number of ports.** • It maintains a MAC address table

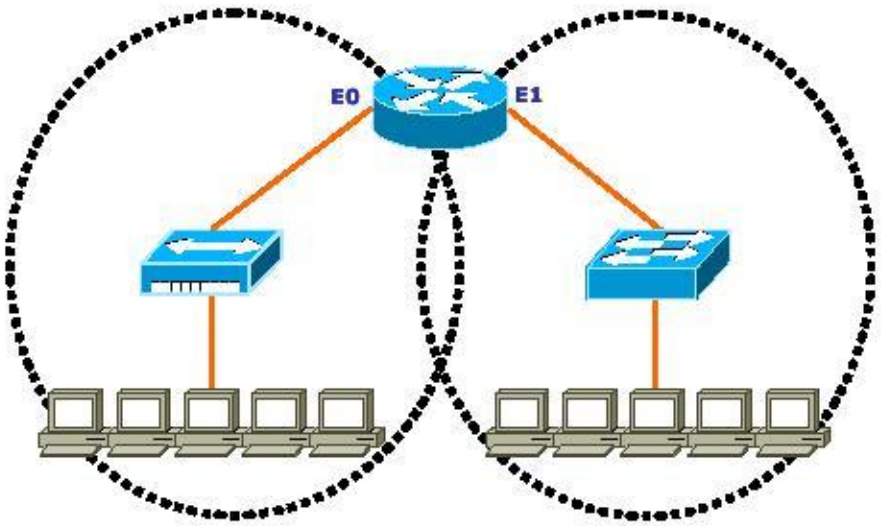
Broadcast Domain

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

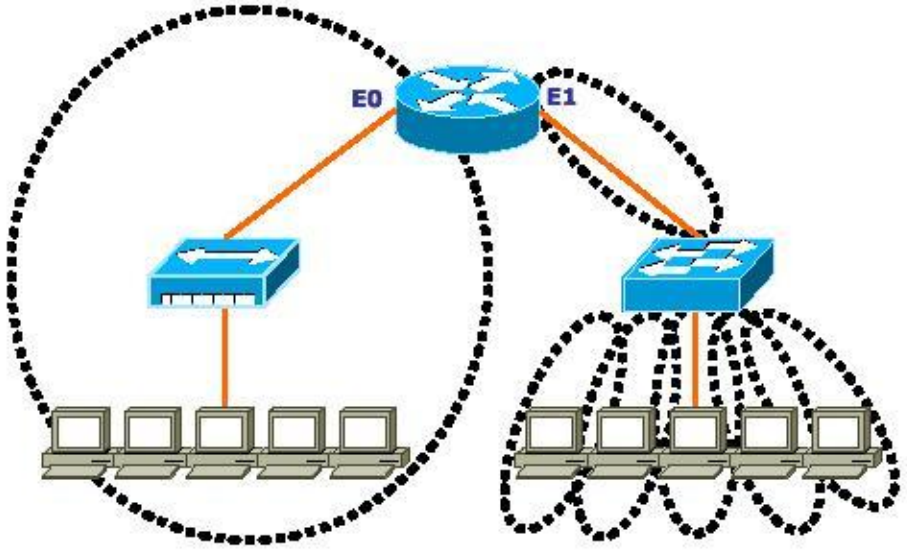
Collision domain

- 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.

Broadcast Domains

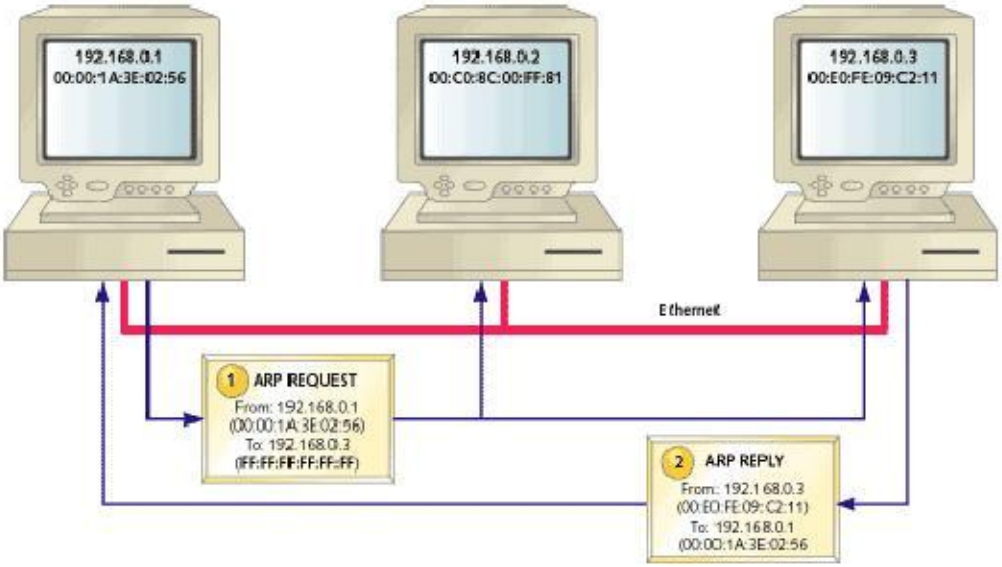


Collision Domains



Address resolution protocol

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



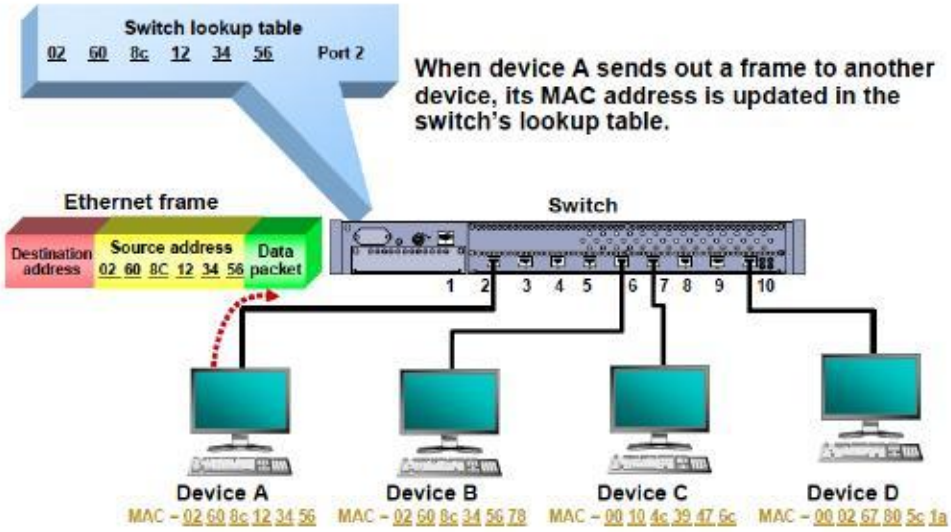
sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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:

1) 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.



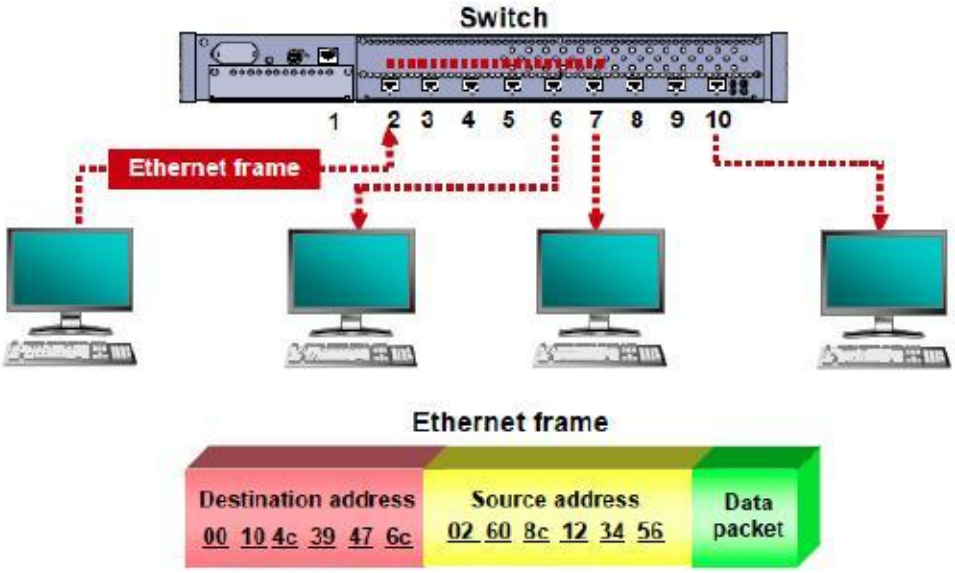
The switch learning process works like this:

- 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.

2) 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.

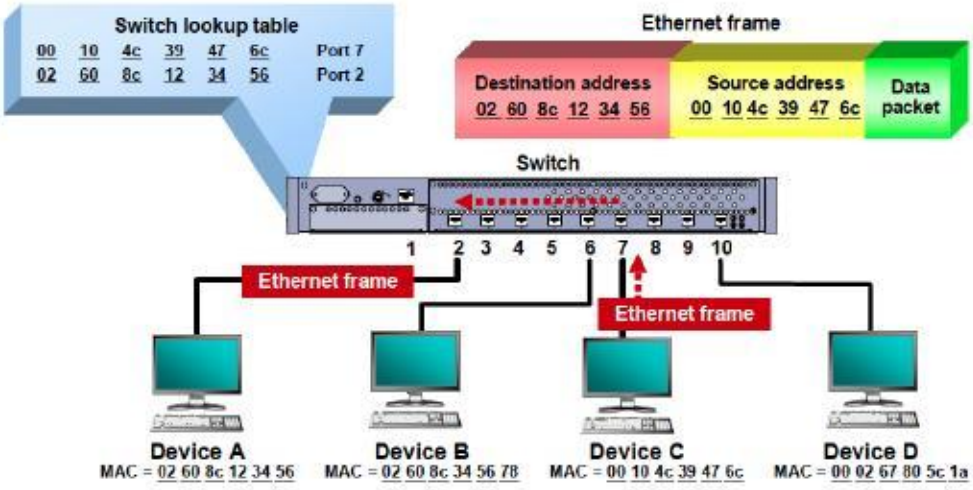
sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com



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.

3) Forwarding and Filtering processes:

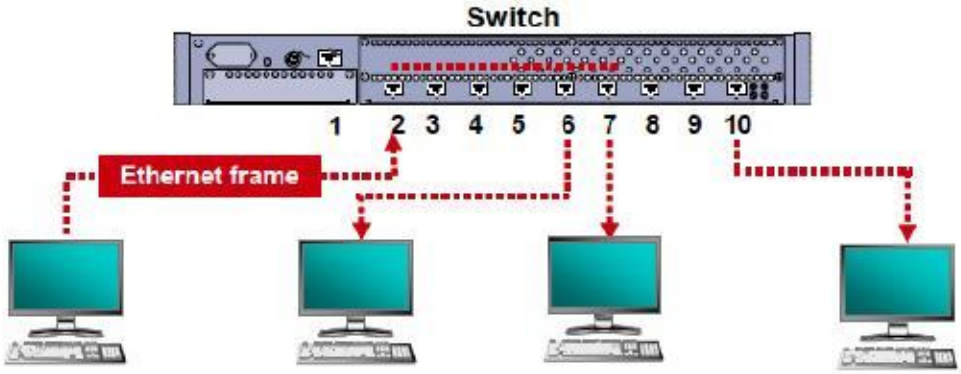
When a switch has learned the locations of the devices connected to it, the switch is ready to either forward or filter frames based on the destination MAC address of the frame and the contents of the switch lookup table.

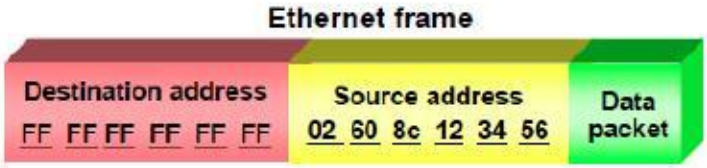


The switch has already found the port of device A by its MAC address 02 60 8c 12 34 56 and switch port number 2. The switch recognizes device C with a MAC address 00 10 4c 39 47 6c when it replies to port 7 on the switch. The switch will receive the incoming frame, examine the destination address of 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.

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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

Types of Switches

- **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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

Cisco's Hierarchical Design Model

Cisco divided the Switches into 3 Layers

1. **Access Layer Switches**
   Switches Series: 1900 & 2900
2. **Distribution Layer Switches**
   Switches Series: 3550 , 3560
3. **Core Layer Switches**
   Switches Series : 4500 , 6500

Access Layer Switch

Catalyst 1900

Catalyst 2900

Distribution Layer Switch

3550 switch

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

Core Layer Switches (4500, 6500)

Switching Modes

Three types of Switching Mode:

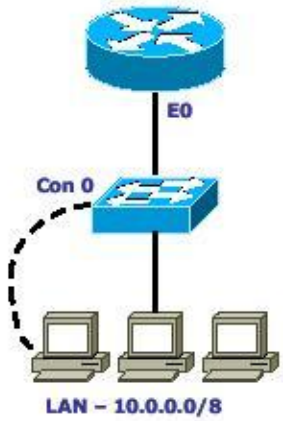
- **Store & Forward**
  - A Default switching method for distribution layer switches.
  - Latency : High
  - Error Checking : Yes
- **Fragment Free**
  - It is also referred to as Modified Cut-Through
  - A Default Switching method for access layer switches.
  - Latency : Medium
  - Error Checking :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

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 Switch.

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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.



Emulation Software

IN 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

IN LINUX

- # minicom -s

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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 to a Switch

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

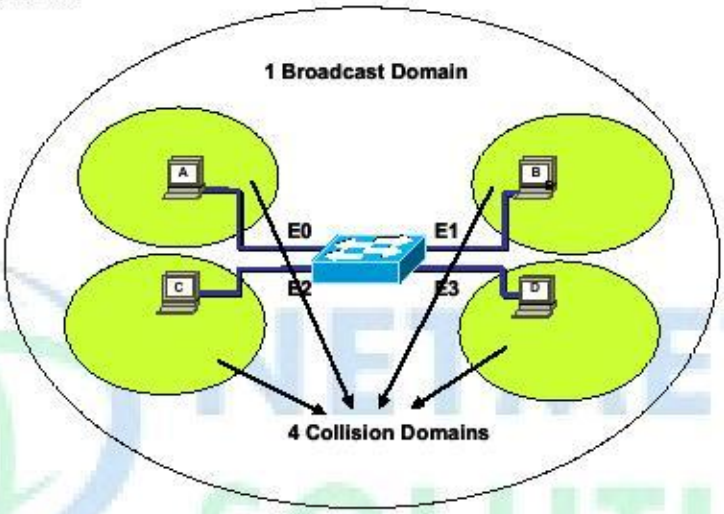
To assign Default Gateway to a Switch

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

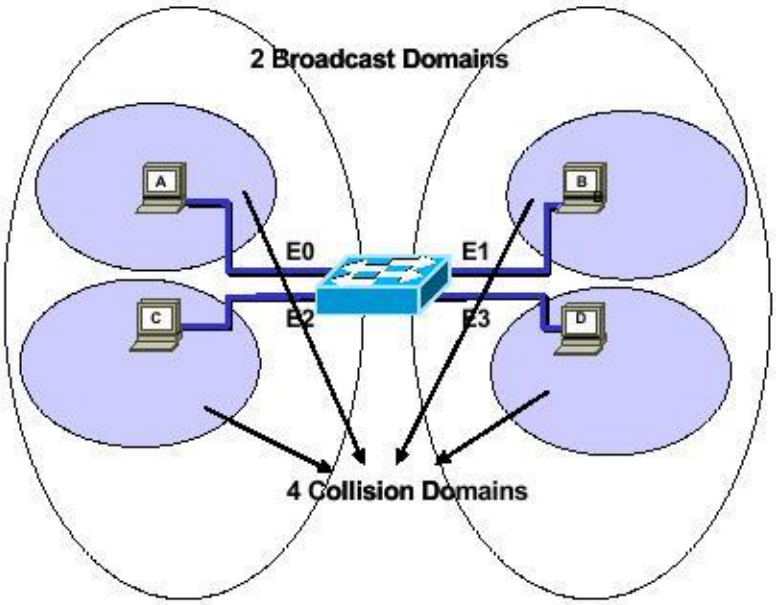
VIRTUAL LAN

- A Layer 2 Security
- Divides a Single Broadcast domain into Multiple Broadcast domains.
- By default all ports of the switch are in VLAN1. This 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



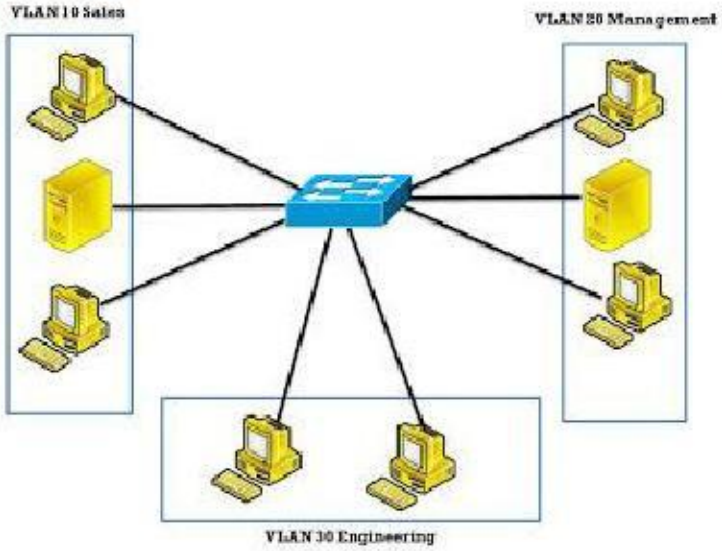
- By default, routers allow broadcasts only within the originating network, but switches forward broadcasts to all segments.
- The reason it's called a flat network is because it's one Broadcast domain, not because its design is physically flat. (Flat Network Structure)
- Network adds, moves, and changes 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.

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com



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



sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

There are two different ways of creating vlans

1) 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>
```

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

Verify using

```
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  fa 0/1  -  5 , f0/12 , f0/17
```

Dynamic VLAN

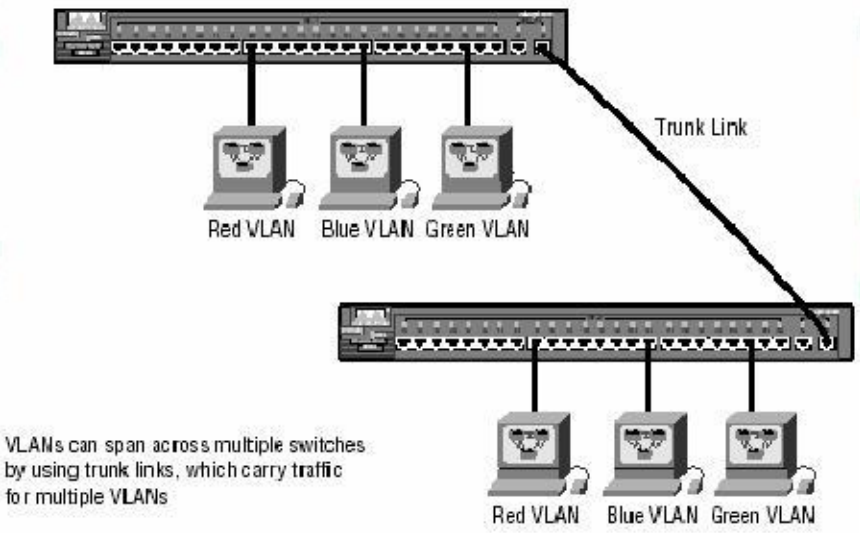
- Dynamic VLAN's are based on the MAC address of a PC
- Switch automatically assigns the port to a VLAN
- Each port can be a member of multiple VLAN's
- For Dynamic VLAN configuration, a software called VMPS(VLAN Membership Policy Server) is needed

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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.



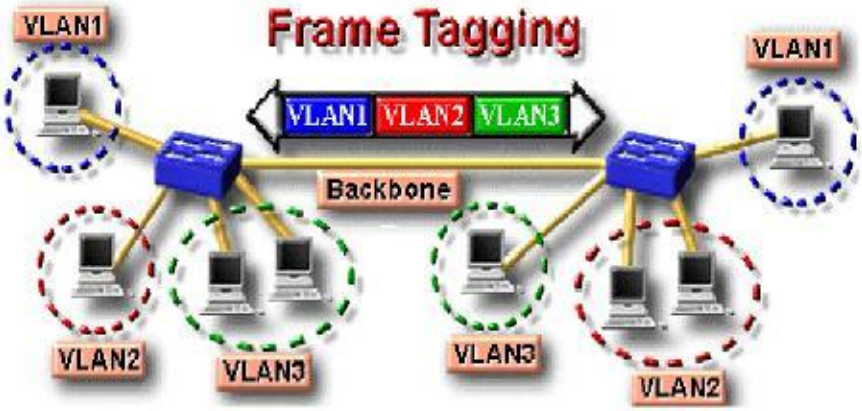
VLANs can span across multiple switches by using trunk links, which carry traffic for multiple VLANs

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

- The below two trunking protocols responsible for frame tagging process
  - **Inter-Switch Link (ISL)**
  - **IEEE 802.1Q**



ISL	IEEE 802.1Q
• It's a Cisco proprietary • It works with Ethernet, Token ring, FDDI • It adds 30 bytes of tag • All VLAN traffic is tagged • Frame is not modified	• Open standard, we can use on different vendors switches. • It works only on Ethernet • Only 4 Byte tag will be added to original frame. • Unlike ISL, 802.1q does not encapsulate the frame. It modifies the existing Ethernet frame to include the VLAN ID

Trunking Configuration –

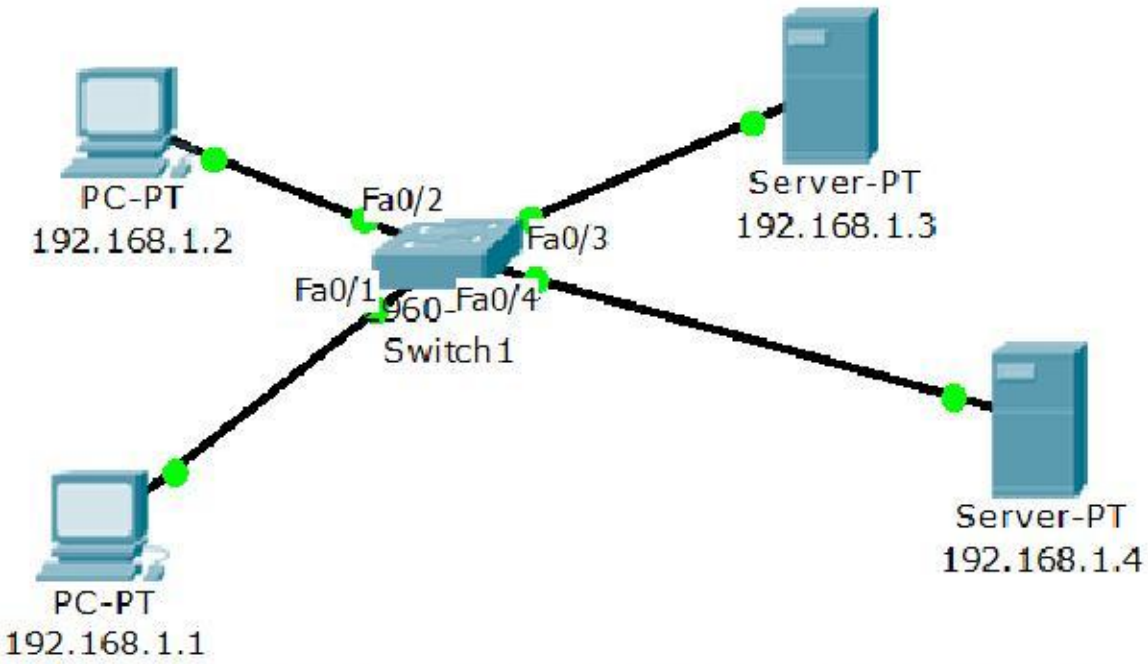
Switch(config)# interface **<interface type> <interface no.>**

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk encapsulation dot1q/ISL

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

LAB -IMPLEMENTING VLAN



Steps:

1) Ping between 192.168.1.1 and 192.168.1.3
2) Create VLAN 20
3) Shift port f0/3 , f0/4 in to VLAN 20
4) Ping between 192.168.1.1 and 192.168.1.3

Switch#sh 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	

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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**

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

Switch(config-if)**#exit**

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

Switch#sh 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=11ms TTL=128
Reply from 192.168.1.2: bytes=32 time=9ms TTL=128
Reply from 192.168.1.2: bytes=32 time=7ms 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.

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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.

LAB -2 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#sh 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
```


sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

There are no active ports in that vlans

30 VLAN0030 active

TASK :

- **Configure port fa0/8 in to vlan 10**
- **Configure multiple ports (4 – 7 and 10) to vlan 20**

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

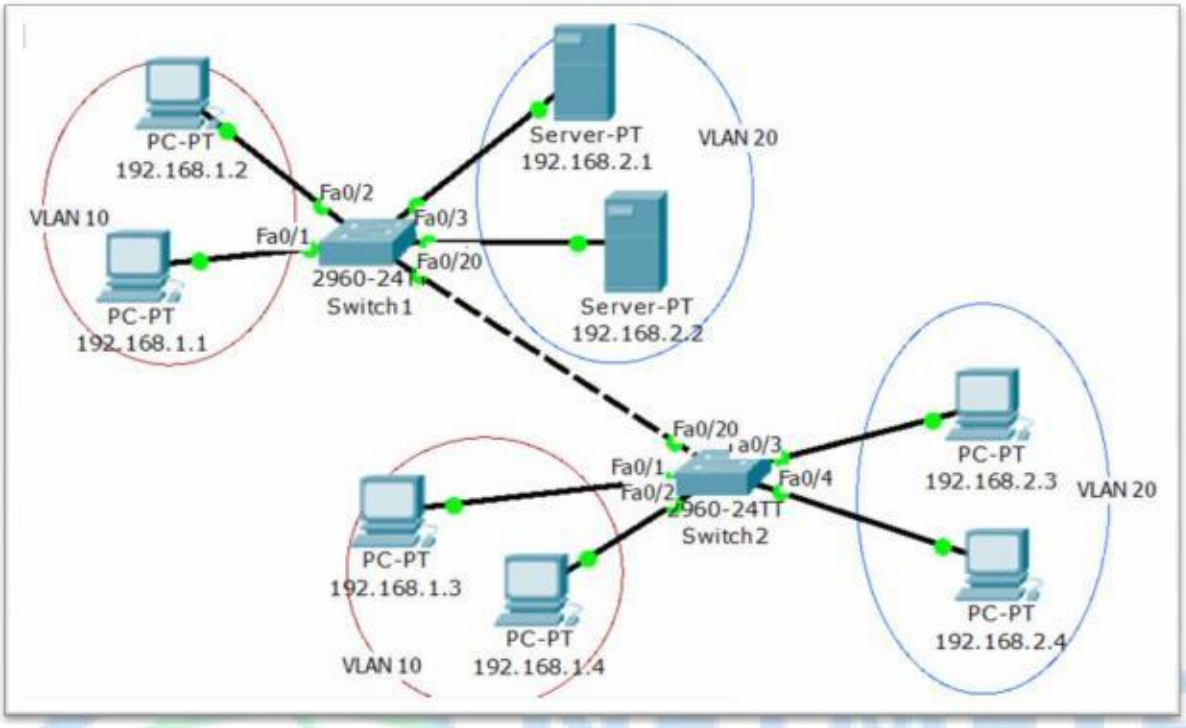
Switch(config)**#interface range f0/4 - 7 , f0/10**
Switch(config-if-range)**#switchport mode access**
Switch(config-if-range)**#switchport access vlan 20**

Switch#sh 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**

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

LAB: TRUNKING



On SW-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#sh 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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

```
                                  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 SW-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

% Access VLAN does not exist. Creating vlan 20

SW-2(config-if-range)#end
```

SW-2#sh 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
```


sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=13ms TTL=128
Reply from 192.168.1.2: bytes=32 time=9ms TTL=128
Reply from 192.168.1.2: bytes=32 time=8ms TTL=128
Reply from 192.168.1.2: bytes=32 time=8ms TTL=128

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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

SW-2(config)**#int f0/20**

SW-2(config-if)**#switchport mode trunk**

SW-2(config-if)**#switchport trunk encapsulation dot1q**

SW-1#sh 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#sh 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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

TASK :

Configure The Trunk Link Such That It Only Allow The Vlan 10 , 20, 30 , 40 Traffic Should Only Be Allowed (No Other Vlan Traffic Should Be Send

On Both switches (SW1/SW2)

SW-x(config)**#int 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#sh 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#sh 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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

```
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#sh 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#sh 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
```


sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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

SW-1#sh 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#sh 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
```


sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

V LAN TRUNKING PROTOCOL

- 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.
- **Note:** Switches Should be configure with same Domain. Domain are not Case sensitive.

VTP Modes
VTP Mode are of three types:

- **Server Mode**
  - A Switch configured in Server mode can Add , Modify and Delete VLAN's
  - A Default VTP mode for all switches
- **Client Mode**
  - A switch configured in Client mode cannot Add , Modify and Delete its 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**
  - A switch configured in a Transparent Mode can Add, Modify and Delete VLAN configurations.
  - Changes in one transparent switch will not affect any other switch.

Benefits of VLAN Trunking Protocol (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

VTP Configuration in config mode

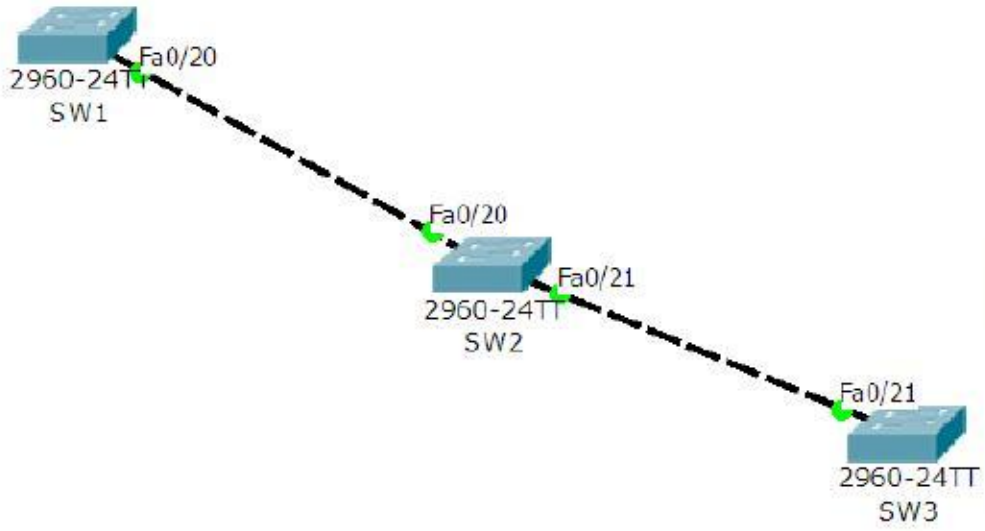
```
Switch(config)# VTP Domain <Name>
Switch(config)# VTP Password <password>
Switch(config)# VTP version 2
Switch(config)# VTP Mode <server/client/transparent>
```


sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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>

LAB : VTP



1) Trunking has to be enabled (vtp advertisements are send only on trunk ports)
2) Configure VTP on all switches
3) Create vlans on server and verify on client and transparent switch
4) 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#sh vtp status
SW1**#sh vtp password**
VTP Password: cisco123

Task -1 Trunking has to be enabled (vtp advertisements are send only on trunk ports)

On SW1 (SERVER)

SW-1(config)#interface fastEthernet 0/20

SW-1(config-if)#switchport mode trunk

SW-1(config-if)#switchport trunk encapsulation dot1q

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

SW2 (TRANSPARENT)

To configure trunking

SW-2(config)#interface range fastEthernet 0/20 - 21

SW-2(config-if)#switchport mode trunk

SW-2(config-if)#switchport trunk encapsulation dot1q

SW3 (CLIENT)

SW-3(config)#interface fastEthernet 0/21

SW-3(config-if)#switchport mode trunk

SW-3(config-if)#switchport trunk encapsulation dot1q

SW1#sh interfaces trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/20	on	802.1q	trunking	1

Task -2 Configure VTP on all switches

SW1

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

SW2

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

SW3

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

SW1#sh 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#sh vtp password
VTP Password: cisco

SW-3#sh 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#sh interfaces trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/20	on	802.1q	trunking	1
Fa0/21	on	802.1q	trunking	1

SW-3#sh 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

SW1
Conf t

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

```
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
  end
```

R1#sh 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#sh 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
```


sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

SW-2#sh 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 #sh 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#sh vlan

```
VLAN Name                        Status    Ports
---- ------------------------------ --------- -------------------------------
1    default                      active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
```


sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

```
                                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
```

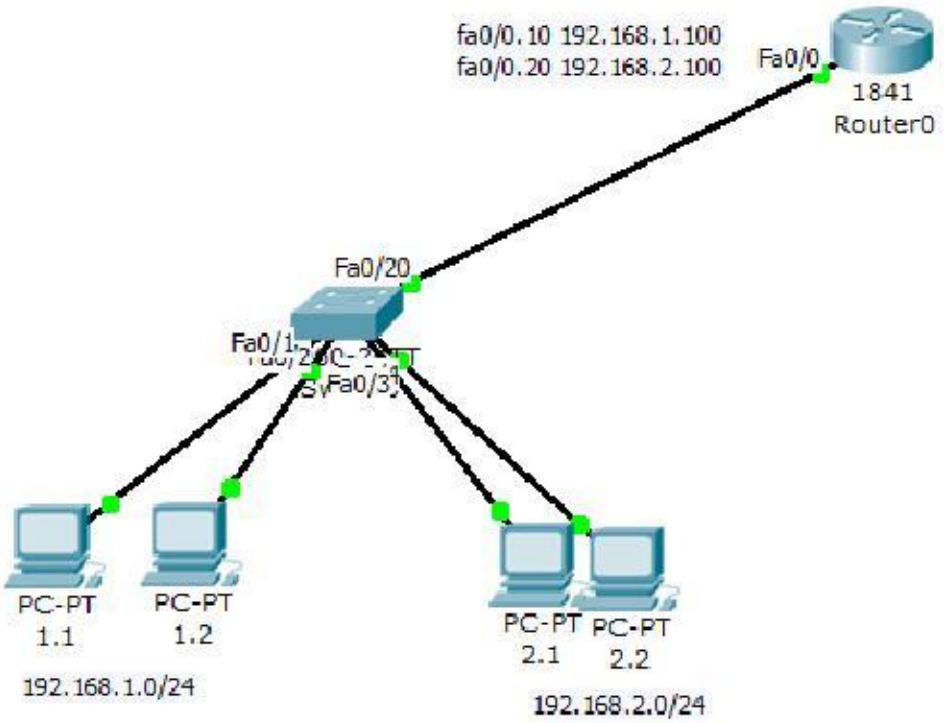
SW3 # sh vlan

```
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***

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

LAB : INTER VLAN-ROUTING USING ROUTER



Steps :

1) create vlan and shift the ports
2) configure on switch fa0/20 as trunk port
3) Create sub interfaces on router port fa0/0
4) Verify connectivity between vlans (ping 192.168.1.1 ---192.168.2.1)

Task -1

create vlan and shift the ports

On SW-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
```


sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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#sh 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)**#int fa0/0**
R-1(config-if)# **no shutdown**
R-1(config-if)# **exit**

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

R-1(config)#**int 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 add 192.168.1.100 255.255.255.0**
R-1(config-sub-if)# **exit**

R-1(config)#**int 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 add 192.168.2.100 255.255.255.0

Router#sh ip int 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 -4 verify connectivity
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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

SPANNING TREE PROTOCOL

- Spanning Tree Protocol (STP) uses Spanning Tree Algorithm to avoid the 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

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 directly connected to the root bridge, or
  - 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.

    1. Root port with the least cost (Speed) connecting to the root bridge.
    2. The bridge with the Best (Lowest) Switch ID.
    3. Lowest Physical Port Number.

- **Designated port**

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

- A designated port will always in Forward Mode

- **Non Designated port**
  - All the Port or ports which are blocked by STP to avoid switching loop.
  - A Non Designated port Will Always in Blocked Mode.

STP port states

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

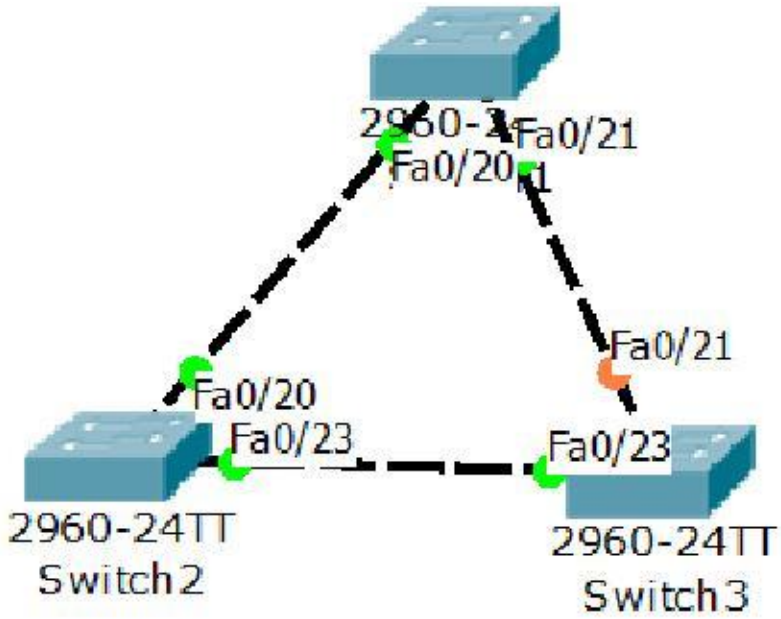
Switch - Port States

- **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.

Typical Costs of Different Ethernet Networks

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com



SW-1#sh 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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

%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
```


sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

```
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
```


sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

IP Network Addressing

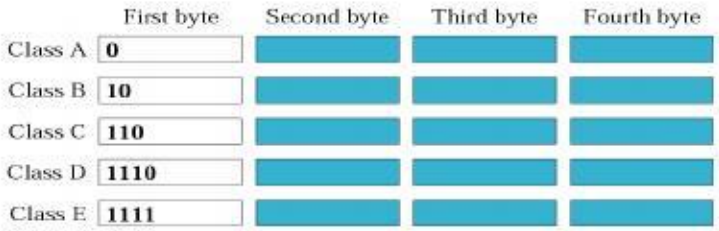
- **INTERNET** → world's largest public data network, doubling in size every nine months
- IPv4, defines a 32-bit address - 2^{32} (4,294,967,296) IPv4 addresses available
- The first problem is concerned with the eventual depletion of the IP address space.
- Traditional model of classful addressing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

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



Techniques to reduce address shortage in IPv4

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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

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

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

IPV6 Address Types:

UNICAST

1) Global unicast

- like public IP (routable) , 2000:: and 2001::

2) site local (unique local)

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

- like *private ip (routable)*
- any address whichever starts with **FC or FD** in the first two numbers

3) link local

- default IPV6 address on every ipv6 enabled interface
- (non routable) FE80::

MULTICAST

- starts with FF00::

ANY CAST

- 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.

Assigning the IPV6 address

1) Static
2) Autoconfiguration
   a. Statefull (via DHCP)
   b. Stateless (device gets IP IPv6 add by including the MAC add)

LAB : BASIC IPV6 ADDRESS CONFIGURATION

TASK -1

Configure IPv6 address according to scenario diagram

R1

hostname R1

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

```
int fa0/0
ipv6 address fc00:11:11:11::1/64
no shutdown

int s1/0
ipv6 address 2001:12:12:12::1/64
no shutdown
clock rate 64000
```

R1#sh 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
```

R2

```
hostname 222
 int fa0/0
 ipv6 address fc00:22:22:22::1/64
 no shutdown

 int s1/0
 ipv6 address 2001:12:12:12::2/64
 no shutdown
 clock rate 64000
```

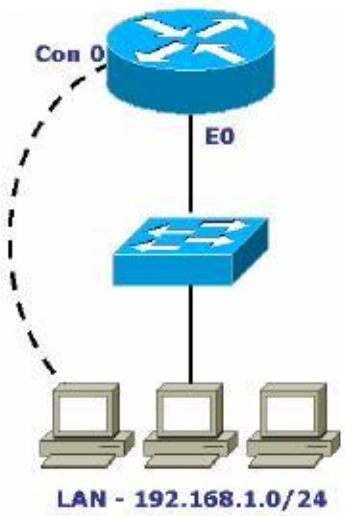
222#sh ipv6 int brief

```
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
```


sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

PASSWORD REVERTING ON CISCO ROUTERS:

1. console connection
2. open hyperterminal window
3. power on the router
4. press **CTRL+ SHIFT + BREAK** to enter in to Rommon mode



5. **Modular routers**
   - Rommon1> **confreg 0x2142**
   - Rommon2> **reset**

   Or

   on fixed routers
   - **> o/r 0x2142**
   - **>i**

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**

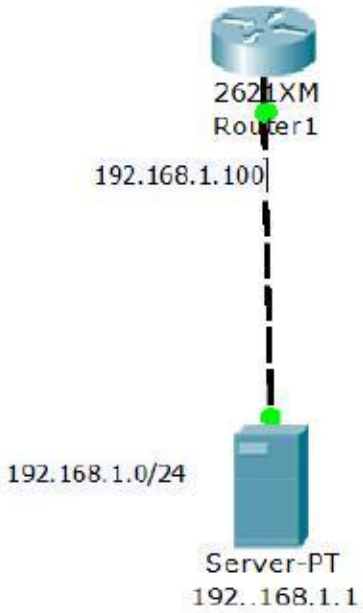
Change the passwords (overwrite with new passwords)

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

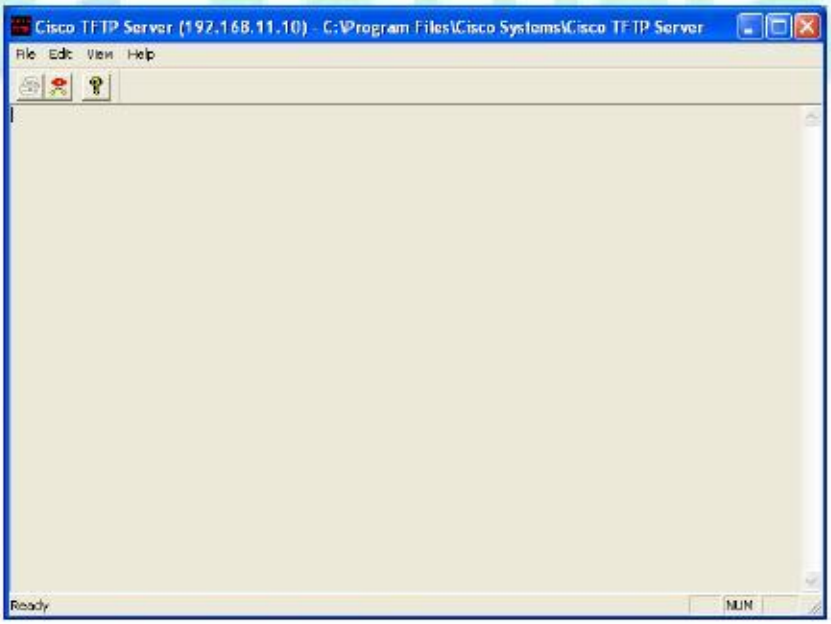
After reloading check for configurations are same and you are able to login with new passwords.

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

LAB :
BACKUP AND RESTORE IOS AND CONFIGS



- *Install TFTP application on PC and make sure that it is running on PC (it is open and minimized)*



sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

- **BACKUP OF IOS :**
  - # copy flash tftp
- **RESTORE or UPGRADE IOS**
  - # copy TFTP Flash
- **BACKUP OF CONFIGS**
  - # copy startup-config TFTP
- **RESTORE CONFIGS**
  - # copy TFTP running-config

R-1#sh ip int 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#sh 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)
```


sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

BACKUP OF IOS

```
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

```
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...
    eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
    eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...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)
```

BACKUP OF CONFIGS

```
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]
```


sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

537 bytes copied in 0.006 secs (89000 bytes/sec)

TO RESTORE CONFIGS 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
```

==========
==========

Commands Step By Step For Configuring An Ip Address To Ther Router And Tftp For A Router Which Has No Ios In Flash In Order 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**

==========

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

LAB:
Restoring the IOS from TFTP in to IOS (in case if there is no IOS present in the flash)

TASK : Delete the existing IOS from the flash

R-1#sh 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.
```


sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

```
 (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
```


sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com

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>

sikandarbaadshah@gmail.com , Sikandar@netmetric-solutions.com