Computer Network

A computer network is a system of interconnected devices to enables sharing of resources and information. Nodes in a network are connected with each other using either cable or wireless media.

Nodes can include hosts such as personal computers, phones, printers, cameras, servers as well as networking hardware. Two such devices can be said to be networked together when one device is able to exchange information with the other device.

Types of network

LANs - local area networks, linking a limited area such as a home, office or a small group of buildings

WANs - wide area networks, which link nationally or internationally

SAN – Storage Area Network

GANs - global area networks, combining all of the above with satellite mobile communication technologies

VoIP - Voice over Internet Protocol Network.

WLAN - Wireless Local Area Network

INTERNET

It is a global network of millions of private, public and organizational network. It carries a massive range of informational resources and data in form of HTTP (Hypertext Markup language) documents and applications through World Wide Web (WWW)

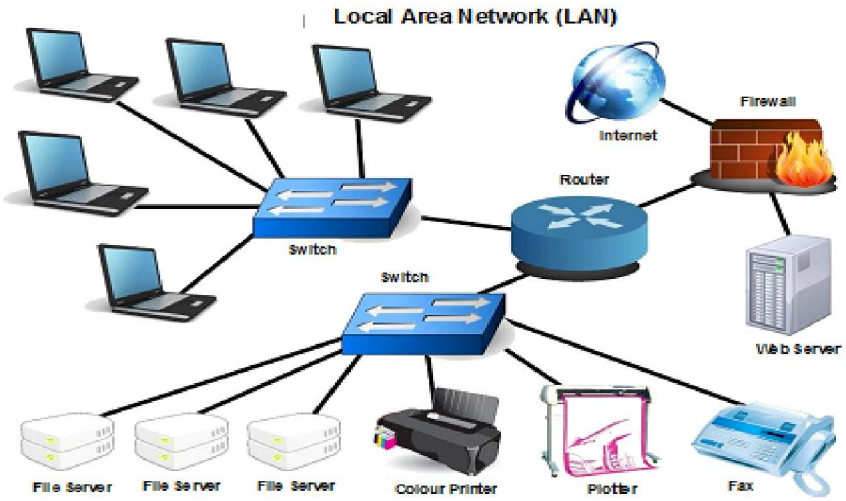
INTRANET

An intranet is an exclusive network that can be accessed only by a specific group of people and no one else. Many corporations, government agencies and universities have their own intranets.

EXTRANET

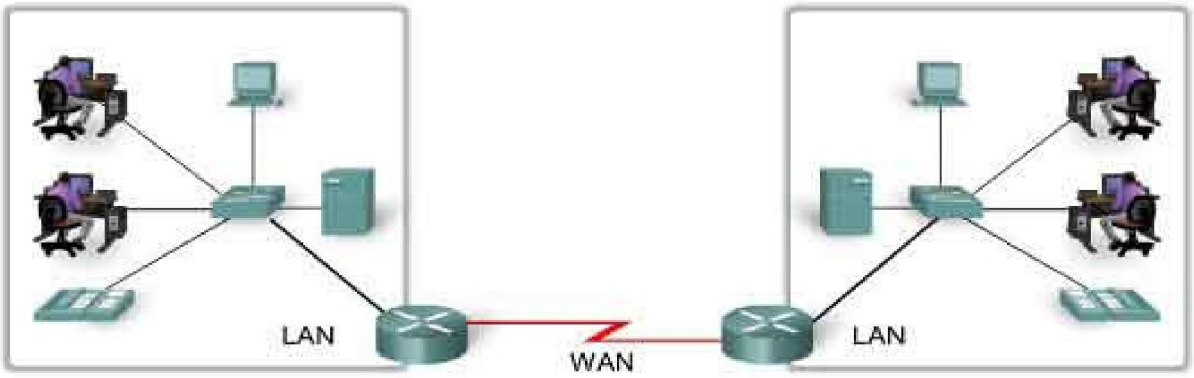
An **extranet** is a controlled private network that allows access to partners, vendors and suppliers or an authorized set of customers. **Extranets** are typically constructed using the internet with security features that restrict access to authorized individuals and digital entities.

LAN (LOCAL AREA NETWOK)



WAN (WIDE AREA NETWORK)

LANs separated by geographic distance are connected by a network known as a Wide Area Network (WAN).



Interview Questions

IQ: Explain what you know about intranet and extranet

IQ: What is the difference between LAN and WAN

Network Devices

The common networks devices use in real life to help communication are Routers, Switches, Firewall and Access Point.

Routers

The router is a network device that connects two or more network segments. The router is used to transfer information from the source to the destination.

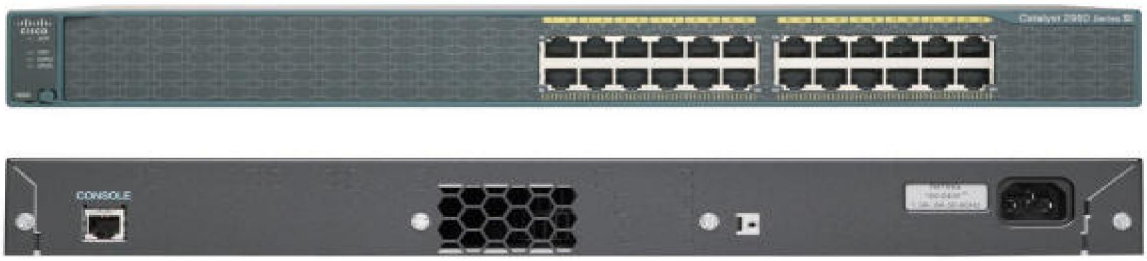
Routers send the information in terms of data packets and when these data packets are forwarded from one router to another router then the router reads the network address in the packets and identifies the destination network.

Switches

A switch is a device that is used to connect many devices together on a computer network.

Cisco Router Front and Back View

Cisco Switch Front and Back View



Router and Switch features

	Router	Switch
Function	A router is a networking device that is use to connect two or more networks	A network switch is a computer networking device that is used to connect many devices together on a computer network
Ports	2/4/5/8 ports	24/48 ports
Used in LAN, WAN	LAN,WAN	LAN
Table	Store IP address in Routing table and maintain address at its own	Store mac addresses in CAM table
Broadcast Domain	In Router, every port has its own Broadcast domain	Switch has one broadcast domain [unless VLAN implemented]
Address used for Data transmission	Uses IP address	Uses MAC address

Access Point

Access points are used for extending the wireless coverage of an existing network and for increasing the number of users that can connect to it. Wireless connectivity is typically the only available option for access points, establishing links with end-devices using Wi-Fi.

Firewall

Firewall is a network security system that is used to protect computer networks from unauthorized access. It prevents malicious access from outside to the computer network. A firewall can also be built to grant limited access to outside users.

The firewall consists of a hardware device, software program or a combined configuration of both. All the messages that route through the Firewall are examined by specific security criteria and the messages which meet the criteria are successfully traversed through the network or else those messages are blocked.

Firewalls can be installed just like any other computer software and later can be customized as per the need and have some control over the access and security features. “

Windows Firewall” is an inbuilt Microsoft Windows application that comes along with the operating system. This “Windows Firewall” also helps to prevent viruses, worms, etc.

Firewall virus protection observes traffic in the network thereby inhibiting malicious data from entering the network hence thwarting viruses. However, the virus can enter your computer through a spam link, download, or from a flash drive. Moreover, once it bypasses the firewall protection, the antivirus' role comes in handy.

Even though the firewall halts the malware and viruses from entering the system, it cannot delete the cyber threat which is infecting the system.

Antivirus

Antivirus software is a cyber security mechanism which many PCs and offices use often. Its primary function is to scan, spot, and inhibit any apprehensive or distrustful files and software from getting into the system.

Below is a comparison chart. It can help you identify the differences between the two mechanisms.

BASIS FOR COMPARISON	FIREWALL	ANTIVIRUS
Implemented in	Both hardware and software	Software only
Operations performed	Monitoring and Filtering (Specifically IP filtering)	Scanning of infected files and software.
Deals with	External threats	Internal as well as external threats.
Inspection of attack is based on	Incoming packets	Malicious software residing on a computer
Counter attacks	IP spoofing and routing attacks	No counter attacks are possible once a malware has removed

IP Addresses

Every machine on a network has a unique identifier. Just as you would address a letter to send in the mail, computers use the unique identifier to send data to specific computers on a network. Most networks today, including all computers on the Internet, use the TCP/IP protocol as the standard for how to communicate on the network. In the TCP/IP protocol, the unique identifier for a computer is called its IP address.

All IP ADDRESSES are divided into two portions: the **NETWORK ADDRESS**, and the **HOST ADDRESS**. Eg 192.168.3.1

[**192.168.3**] – Network address and **1**- Host address

There are two standards for IP addresses: IP Version 4 (IPv4) and IP Version 6 (IPv6).

Types of IP Addresses

Public (external) IP addresses

A public (or *external*) IP address is the one that your ISP *(Internet Service Provider)* provides to identify your home network to the outside world. It is an IP address that is unique throughout the entire Internet.

Private Addresses

When several computers or devices are connected to each other, either with cables or wirelessly, they can make up a private network. Each device within this network is assigned a different IP address in order to exchange files and share resources within the network.

Classes of IP Address

CLASS	IP ADDRESS RANGE	Number of Addresses	SUBNETMASK
A	10.0.0.0 - 10.255.255.255	16,777,216	255.0.0.0
B	172.16.0.0 - 172.31.255.255	1,048,576	255.255.0.0
C	192.168.0.0 - 192.168.255.255	65,536	255.255.255.0
D	224.0.0.0 - 239.255.255.255	N/A	N/A
E	240.0.0.0 - 255.255.255.255	N/A	N/A

APIPA – Automatic Private IP Addressing

Windows operating systems. With APIPA, DHCP clients can automatically self-configure an IP address and subnet mask when a DHCP server isn't available.

The IP address range is **169.254.0.1** through **169.254.255.254**.

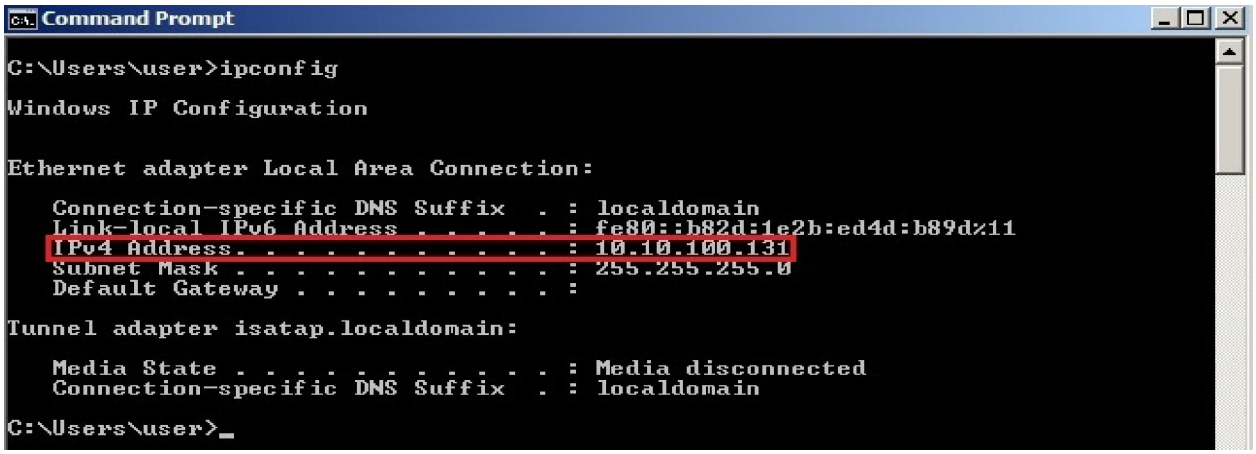
Loopback address

Loopback address is a special IP number (**127.0.0.1**) that is designated for the software loopback interface of a machine. The loopback interface has no hardware associated with it, and it is not physically connected to a network.

The loopback interface allows IT professionals to test IP software without worrying about broken or corrupted drivers or hardware.

How to find out your IP address

If you are using Windows, start the Command Prompt (Start – Programs – Accessories – Command Prompt). Enter the *ipconfig* command. You should see a field called **IP address:**



MAC address

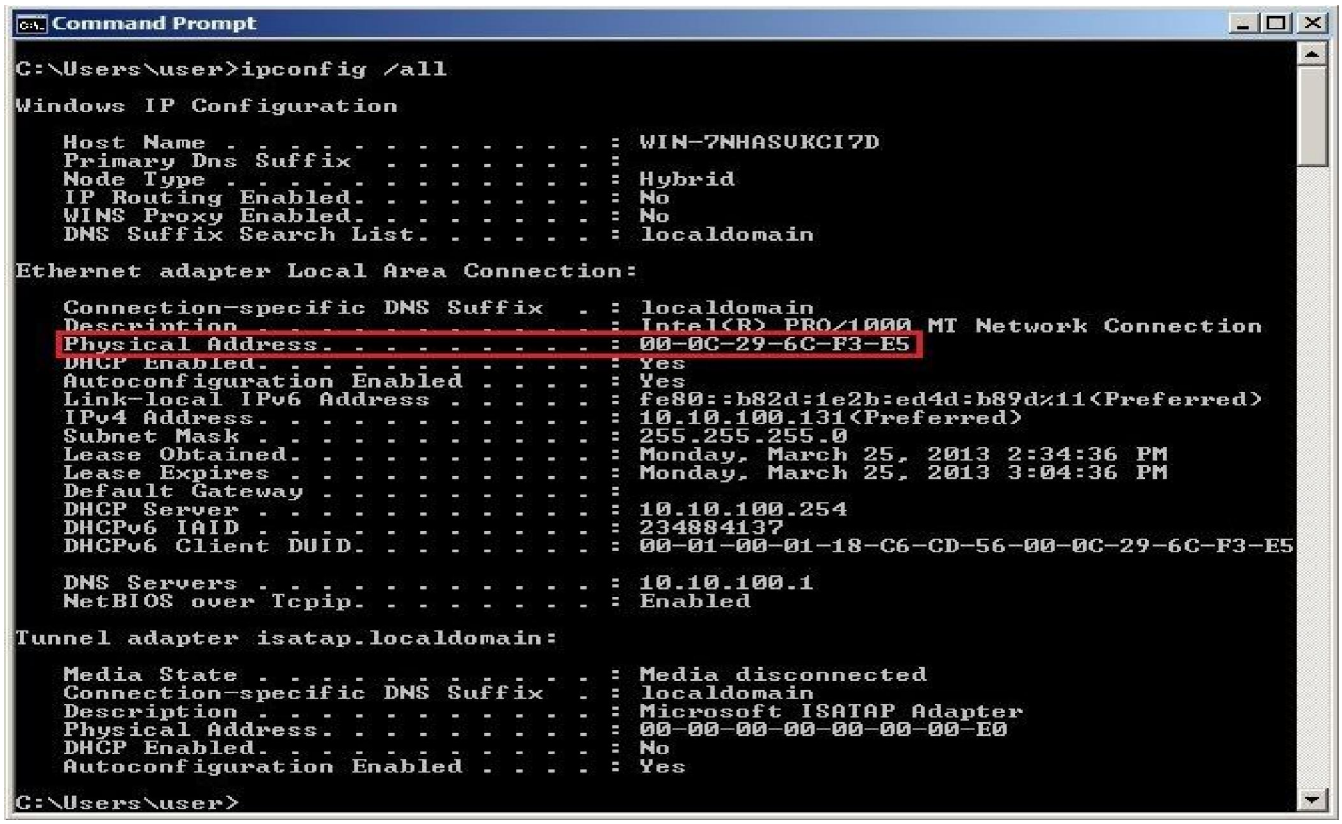
Every network card manufacturer gets a universally unique 3-byte code called the **Organizationally Unique Identifier (OUI)**. Manufacturers agree to give all NICs a MAC address that begins with the assigned OUI. The manufacturer then assigns a unique value for the last 3 bytes, which ensures that every MAC address is 7lobally unique.

MAC addresses are usually written in the form of 12 hexadecimal digits. For example, consider the following MAC address:

```
D8-D3-85-EB-12-E3
```

How to find out your own MAC address and IP address on a PC?

If you are using Windows, start the Command Prompt (Start – Programs – Accessories – Command Prompt). Type the *ipconfig/all* command and you should see a field called Physical address under the Ethernet adapter settings:



Interview Questions

IQ: What is the difference between Private and Public IP address

IQ: Give examples of Private and Public IP addresses

IQ: What is APIPA and Loopback Address?

IQ: What Is The Difference Between Physical Address And Logical Address?
Answer:
Physical Address: It's called as MAC Address (48 bit)
Logical Address: It's Called as Ip Address (IPv4 -32 bit & IPv6 -128 bit)

DNS (Domain Name System)

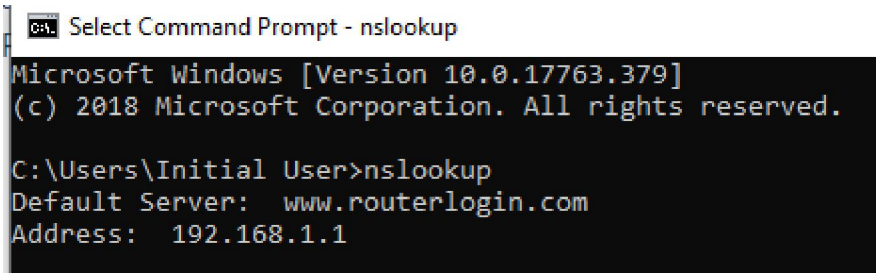
DNS (Domain Name System) is a network protocol that we use to find the IP addresses of hostnames. Computers use IP addresses but for us humans, it's more convenient to use domain names and hostnames instead of IP addresses. If you want, you could visit networkprofession.net by going directly to IP address 95.85.36.216, but typing in the domain name networkprofessional.net is probably easier.

There are thousands of DNS servers, but none of them has a complete database with all hostnames / domain names and IP addresses. A DNS server might have information for certain domains but might have to query other DNS servers if it doesn't have an answer.
There are 13 root name servers that have information for the generic top level domains like com, net, org, biz, edu or country specific domains like uk, nl, de, be, au, ca, and such.

The figure below explains the concept:

NOTE
DNS uses a well-known UDP port 53.

To verify if DNS is working = type nslookup under command prompt



Interview Question

IQ: Explain what you know about DNS

Subnet Chart

CIDR	Subnet Mask	Wildcard Mask	Total IPs	Usable IPs
/32	255.255.255.255	0.0.0.0	1	1
/31	255.255.255.254	0.0.0.1	2	0
/30	255.255.255.252	0.0.0.3	4	2
/29	255.255.255.248	0.0.0.7	8	6
/28	255.255.255.240	0.0.0.15	16	14
/27	255.255.255.224	0.0.0.31	32	30
/26	255.255.255.192	0.0.0.63	64	62
/25	255.255.255.128	0.0.0.127	128	126
/24	255.255.255.0	0.0.0.255	256	254
/23	255.255.254.0	0.0.1.255	512	510
/22	255.255.252.0	0.0.3.255	1024	1022
/21	255.255.248.0	0.0.7.255	2048	2046
/20	255.255.240.0	0.0.15.255	4096	4094
/19	255.255.224.0	0.0.31.255	8192	8190
/18	255.255.192.0	0.0.63.255	16,384	16,382
/17	255.255.128.0	0.0.127.255	32,768	32,766
/16	255.255.0.0	0.0.255.255	65,536	65,534
/15	255.254.0.0	0.1.255.255	131,072	131,070
/14	255.252.0.0	0.3.255.255	262,144	262,142
/13	255.248.0.0	0.7.255.255	524,288	524,286
/12	255.240.0.0	0.15.255.255	1,048,576	1,048,574
/11	255.224.0.0	0.31.255.255	2,097,152	2,097,150
/10	255.192.0.0	0.63.255.255	4,194,304	4,194,302
/9	255.128.0.0	0.127.255.255	8,388,608	8,388,606
/8	255.0.0.0	0.255.255.255	16,777,216	16,777,214
/7	254.0.0.0	1.255.255.255	33,554,432	33,554,430
/6	252.0.0.0	3.255.255.255	67,108,864	67,108,862
/5	248.0.0.0	7.255.255.255	134,217,728	134,217,726
/4	240.0.0.0	15.255.255.255	268,435,456	268,435,454

CIDR	Subnet Mask	Wildcard Mask	Total IPs	Usable IPs
/3	224.0.0.0	31.255.255.255	536,870,912	536,870,910
/2	192.0.0.0	63.255.255.255	1,073,741,824	1,073,741,822
/1	128.0.0.0	127.255.255.255	2,147,483,648	2,147,483,646
/0	0.0.0.0	255.255.255.255	4,294,967,296	4,294,967,294

Operating Systems for Cisco Devices

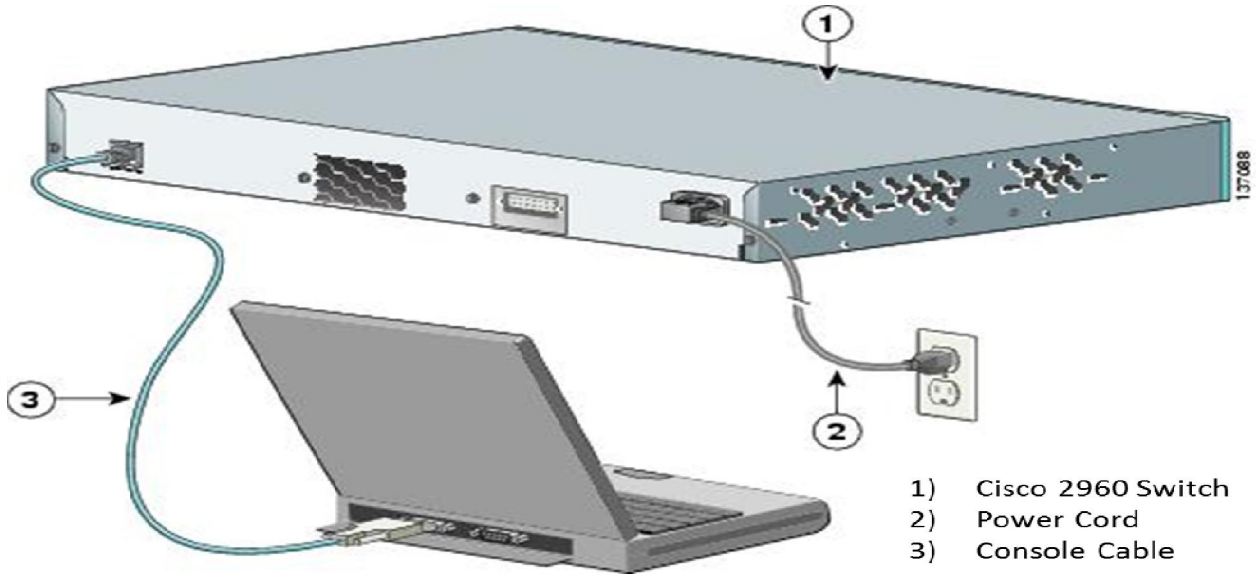
- Internetwork Operating System (IOS)
- CatOS—Catalyst Switch Operating System
- NX-OS—Nexus Operating System

Access to Cisco IOS CLI

Before we can enter any commands, we need access to the CLI. There are three options:

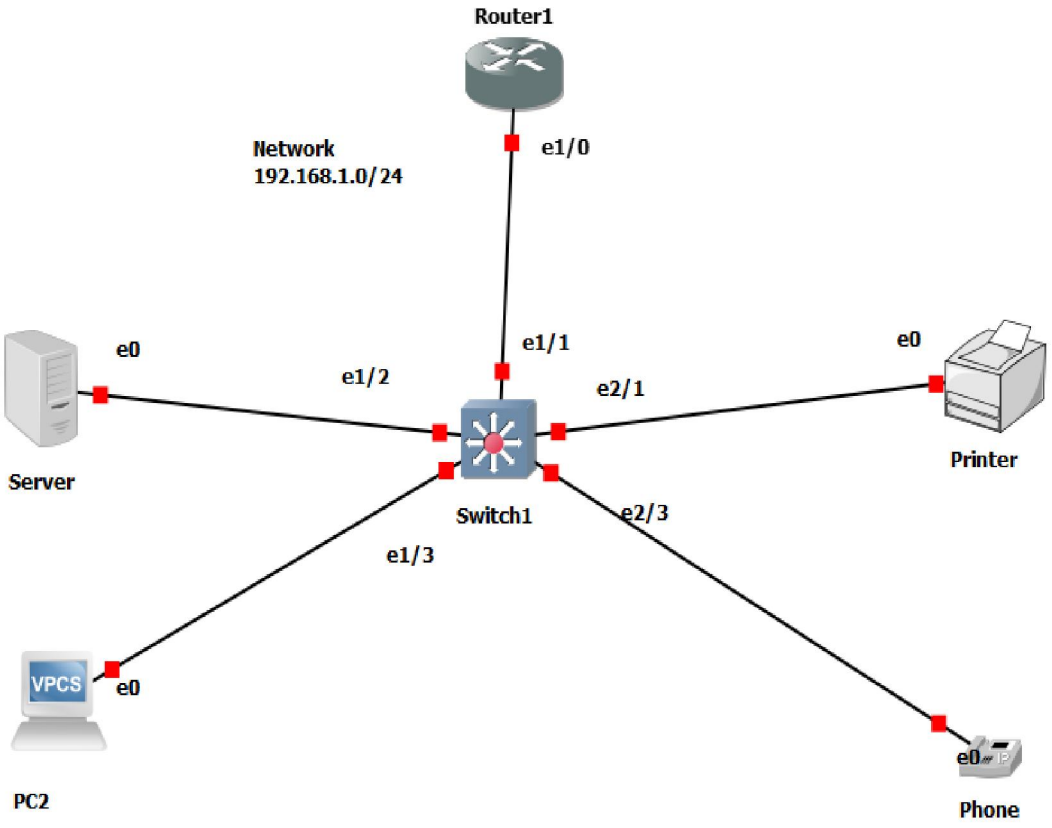
- Console
- Telnet
- SSH

The console is a physical port on the switch that allows access to the CLI. We typically use this the first time we configure the switch. Telnet and SSH are both options for remote access.



Network Setup

Lab 1



Base Configurations

1) Configure your router and switch with the following basic information.

R1>User Mode	
R1>enable	Enter Privilege mode
R1#	Privilege mode
R# conf t	Enter Configuration mode
R(config)#	Global Config mode
RI(config)#**hostname Internet_Router**	Changes hostname
Internet_Router (config)#**no ip domain-lookup**	Disables DNS lookup
Internet_Router(config)#**enable secret NPTC**	Assigns **NPTC** as the secret password
Internet_Router(config)#**service password-encryption**	Encrypts any password stored in clear text
Internet_Router(config)#**lin con 0**	Enters console port configurations
Internet_Router(config-lin)#**password c**	Sets console password to c
Internet_Router(config-lin)#**logging synchronous** have type on screen	Synchronize messages to keep what you
Internet_Router(config-lin)#**exec-timeout 45 20**	Sets timeout to 45 minutes and 20 secs
Internet_Router(config)#**lin vty 0 4**	Establishes 5 possible telnet sessions
Internet_Router(config-lin)#**pass v**	Sets v as telnet password.
Internet_Router(config-line)#**logg syn** have typed on a screen	Synchronize messages to keep what you
Internet_Router(config-line)#**exec-timeout 0 0**	Disables timeout
Internet_Router (config-line)#**exit or end**	Return to Privilege mode
Internet_Router# **wr or copy run start**	Save Config
Internet_Router# disable	Return user mode
Internet_Router > enable	Return to Privilege mode

IQ: What are the basic configuration for network devices eg Routers and Switches

Verify your configuration by show run

Building configuration...

Current configuration: 1692 bytes

Version 12.4

service timestamps debug date time msec

service timestamps log date time msec

service password-encryption

hostname Router

boot-start-marker

boot-end-marker

enable secret 5 1wedi$gX01LUMyMa64txT3oUBUQ.

noaaa new-model

noipicmp rate-limit unreachable

ipcef

no ip domain lookup

iptcpsynwait-time 5

no ip http secure-server

line con 0

exec-timeout 45 20

privilege level 15

password 7 0508

logging synchronous

linevty 0 4

exec-timeout 0 0

password 7 051D

logging synchronous

2) Assign IP address to the Router and describe the port and the network.

Router (Config) **#int e1/0**

 # Description Switch_e1/1

#No shut

#Int e1/0.10

#Description Accounts

#Encapsulation dot1Q 10

 # ip address 192.168.1.1 255.255.255.0

Verify your Port configuration

Show run int e1/0.10

Interface ethernet1/0.10

Description Accounts

Encapsulation dot1Q 10

ip address 192.168.1.1 255.255.255.0

Verify your Config: Show IP int Brief

Router# show ip int br

Interface	IP-Address	OK? Method	Status	Protocol
Ethernet1/0	unassigned	YES TFTP	up	up
Ethernet1/0.10	192.168.1.1	YES manual	up	up

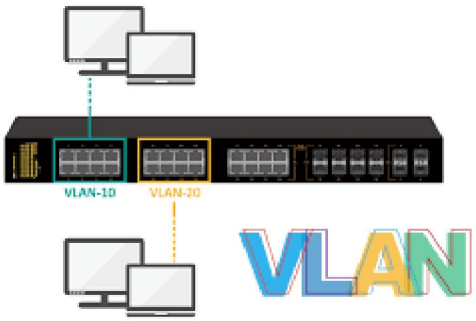
3) Configure Vlan10 on the switch and name it as Accounts

VLAN(Virtual local Area Network)

A **VLAN (Virtual local Area Network)** is a logical grouping of network users and resources connected to defined ports on a switch. By default, all ports on a switch are in the same broadcast domain. A Virtual Local Area Network, Virtual LAN, or VLAN, can be used to divide a single broadcast domain to multiple broadcast domains in a layer 2 switched networks.

Default VLAN

The **Default VLAN** is simply the VLAN which all Access Ports are assigned to until they are explicitly placed in another VLAN. In the case of Cisco switches (and most other Vendors), the Default VLAN is usually VLAN 1



What are the advantages of using VLANs?

- VLANs enable logical grouping of end-stations that are physically dispersed on a network.
- Added security by keeping devices in a certain group (or function) in a separate Broadcast domain.
- Higher performance and reduced latency

Switch (Config) #**Vlan 10**

 # Name Accounts

Verify your Config: Show vlan brief

Switch# show vlan br

VLAN	Name	status	Ports
1	default	active	Et0/0, Et0/1, Et0/2, Et0/3
			Et1/0, Et1/1, Et1/2, Et1/3
			Et2/0, Et2/1, Et2/2, Et2/3
			Et3/0, Et3/1, Et3/2, Et3/3
10	Accounts	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

4) Configure the switch virtual interface (SVI) on all the Switches

Switch Virtual Interface (SVI)

A **Switched Virtual Interface** (SVI) represents a logical layer-3 interface on a switch. There is no physical interface for the VLAN and the SVI provides the Layer 3 processing for packets from all switch ports associated with the VLAN.

SVI Configuration

Switch (config) # interface vlan **10**

ip address **192.168.1.2 255.255.255.0**

no shut

5) Configure a Switch Default Gateway

Switch Default Gateway

The switch should be configured with a default gateway if the switch will be managed remotely from networks not directly connected. A default gateway is a router that hosts use to communicate with other hosts on remote networks

Switch (config) # ip default-gateway 192.168.1.1

6) Configure Trunk Port on the switch connected to the Router and describe the port

Trunk Port –Transmit the data traffic of multiple VLANs simultaneously. Generally, a Trunk link is configured between the **switch to switch** or **switch to the router**

Switch (Config) # int e1/1

Description **Internet_router_e1/0**

#switchport trunk encapsulation dot1q

switchport mode Trunk

Verify Config: Show int trunk

Port	Mode	Encapsulation	Status	Native vlan
Et1/1	on	802.1q	trunking	1

Port Vlans allowed on trunk

Et1/1 1-4094

Port Vlans allowed and active in management domain

Et1/1 1,10

Port Vlans in spanning tree forwarding state and not pruned

7) Configure Access port to all connected PC base on the vlan

Access port – Access port belongs to and transmits the traffic of only one VLAN at a time. Any data frame received on an access port is simply supposed to belong to the VLAN configured on that port.

Switch (Config)# int e1/2

switchport access Vlan **10**

switch mode Access

Spanning-tree portfast

Switch (Config)# int e1/3

switchport access Vlan **10**

switch mode Access

Spanning-tree portfast

Switch (Config)# int e2/1

switchport access Vlan **10**

switch mode Access

Spanning-tree portfast

Switch (Config)# int e2/3

switchport access Vlan **10**

switch mode Access

Spanning-tree portfast

Configuration in a range format

Int range e1/2 – 3

switchport access Vlan **10**

switch mode Access

Spanning-tree portfast

Verify Config: Show int status

Switch# show int status

Port	Name	Status	Vlan	Duplex	Speed Type
Et1/	**Internet_router_e1/0**	connected	trunk	full	100 10/100BaseTX
Et1/2		connected	10	full	100 10/100BaseTX
Et1/3		connected	10	full	100 10/100BaseTX
Et2/1		connected	10	full	100 10/100BaseTX
Et2/3		connected	10	full	100 10/100BaseTX

8) Assign Static IP address to the PC

PC1>ip 192.168.1.**3** 255.255.255.0 192.168.1.1

PC2>ip 192.168.1.**4** 255.255.255.0 192.168.1.1

Verify Config: Show ip

Interview Question for Practice

IQ: What is difference between an access port and a trunk?

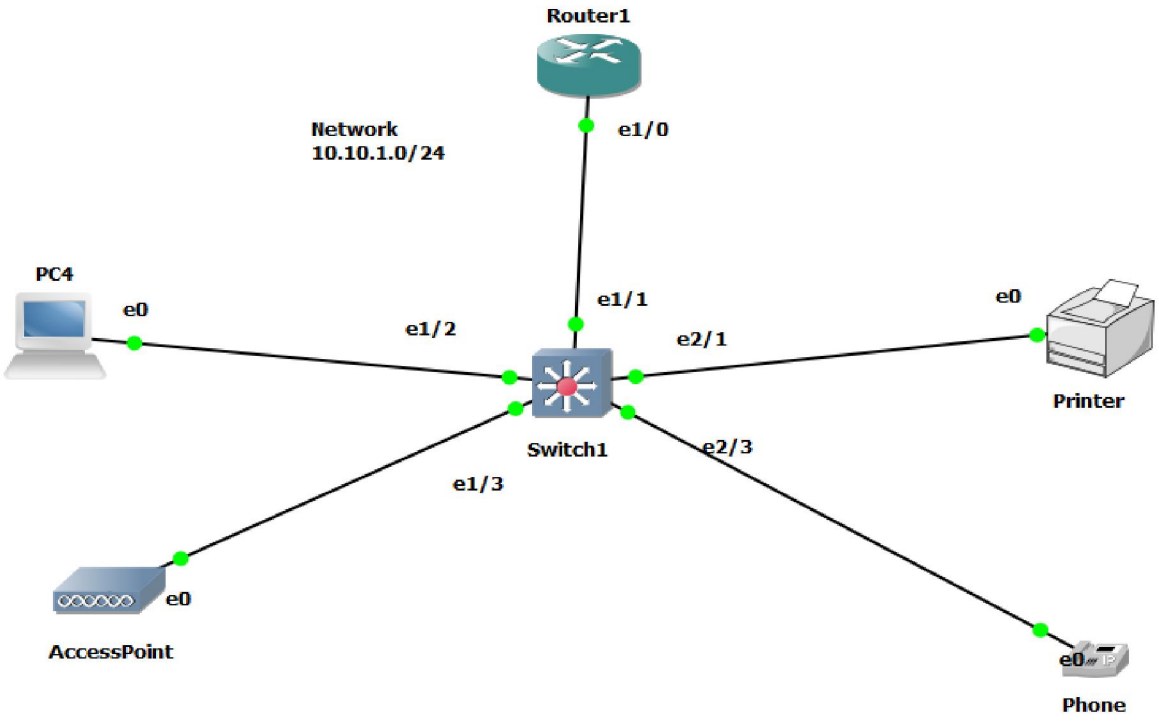
IQ: How can you add an interface to a vlan ?

IQ How do you configure a trunk link ?

IQ: Which command is used to see all vlan information?

IQ: Purpose of Vlan - Segmentation and Security

Basic Setup Assignment



1) Configure your router and Switch with basic information.

2) Assign IP address to the Router and describe the port and the network.
3) Configure the hostname of the switch(ESW1) as Data_Switch

4) Configure Trunk Port on the switch connected to the Router and describe the port
5) Configure Trunk Port on the switch connected to the Router and describe the port

6) Configure Access port to all connected device base on the vlan

7) Configure the switch virtual interface (SVI) on the Switch

8) Configure a Switch Default Gateway
9) Assign Static IP address to the PC

Dynamic Host Configuration Protocol (DHCP)

DHCP is a network protocol that is used to assign various network parameters to a device. This greatly simplifies administration of a network, since there is no need to assign static network parameters for each device.

IP addresses can be configured **statically** or **dynamically**. Normally we configure static IP addresses on network devices like routers, switches, firewalls and servers while we dynamically assign IP addresses to computers, laptops, tablets, smartphones etc

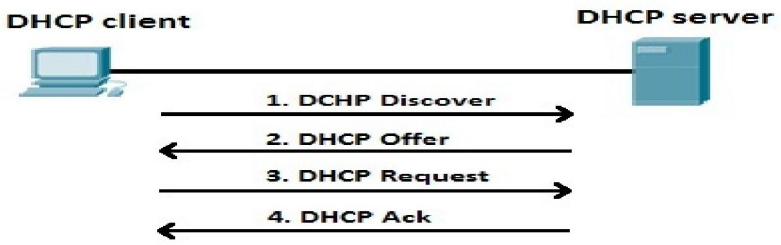
DHCP server maintains a pool of available IP addresses and assigns one of them to the host. A DHCP server can also provide some other parameters, such as:

- subnet mask
- default gateway
- domain name
- DNS server

Cisco routers can be configured and DHCP server.

DHCP process explained:

DHCP client goes through the four step process:



A DHCP client sends a broadcast packet (**DHCP Discover**) to discover DHCP servers on the LAN segment.

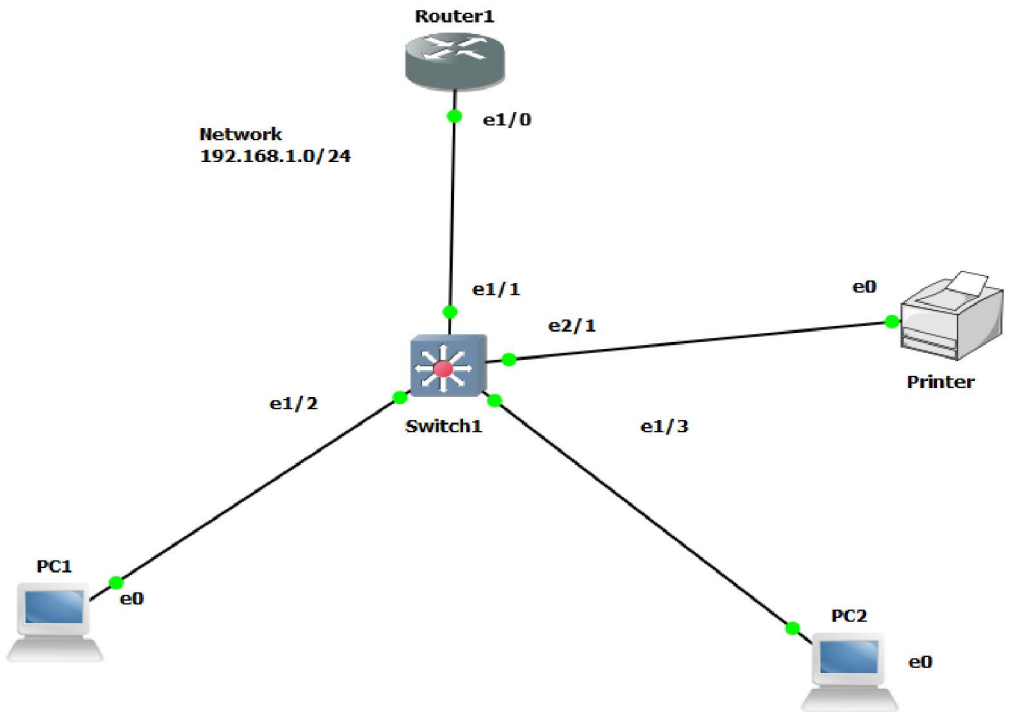
2: The DHCP servers receive the DHCP Discover packet and respond with **DHCP Offer** packets, offering IP addressing information.

3: If the client receives the DHCP Offer packets from multiple DHCP servers, the first DHCP Offer packet is accepted. The client responds by broadcasting a **DHCP Request** packet, requesting the network parameters from the server that responded first.

4: The DHCP server approves the lease with a **DHCP Acknowledgement** packet. The packet includes the lease duration and other configuration information.

NOTE
DHCP uses a well-known UDP port number 67 for the DHCP server and the UDP port number 68 for the client.

Lab Task # 2



Global Configuration

1. Configure the hostname base on the Network Diagram
2. Disable the dns lookup feature.
3. Assign Cisco as the Secret password.
4. Direct the cisco IOS to encrypt any passwords stored in clear-text.

Console Port

1. Configure the console port on all devices to log input synchronously
2. Set password to NPTC!
3. Configure the idling timeout to 1 hour and 30 second

VTY Ports

1. Allow 5 concurrent sessions of remote access
2. Configure the vty ports to log input synchronously
3. Set password to VAN
4. Configure idling timeout to 30 mins and 10 seconds
5. Save config

Verify config

- **Assign IP address to the Router**

Verify config

- **Configure the router to act as DHCP Server and reserve 10 IP addresses for static**

Internet_Router (config) #ip dhcp pool **Marketing**
Network **192.168.1.0 255.255.255.0**
default-router **192.168.1.1**
Lease **3 0** (interpreted as follows: **3** days, **0** hours and **0** minutes)
ip dhcp excluded-address **192.168.1.1 192.168.1.10**

Verify config

Show run | begin dhcp

- **Configure the Vlan on the switch and name it as follow**

Vlan 50- Marketing Department

Verify config

- **Configure the switch virtual interface (SVI) on the Switch**
- **Configure a Switch Default Gateway**
- **Configure Trunk Port base on the topology**

Verify config

- **Assign Vlan to all the PCs base on the Network topology**

Verify config

- **Obtain DHCP address to the PCs and assign static IP address to the printer.**

Verify config

Show Command for DHCP

Show run | begin DHCP

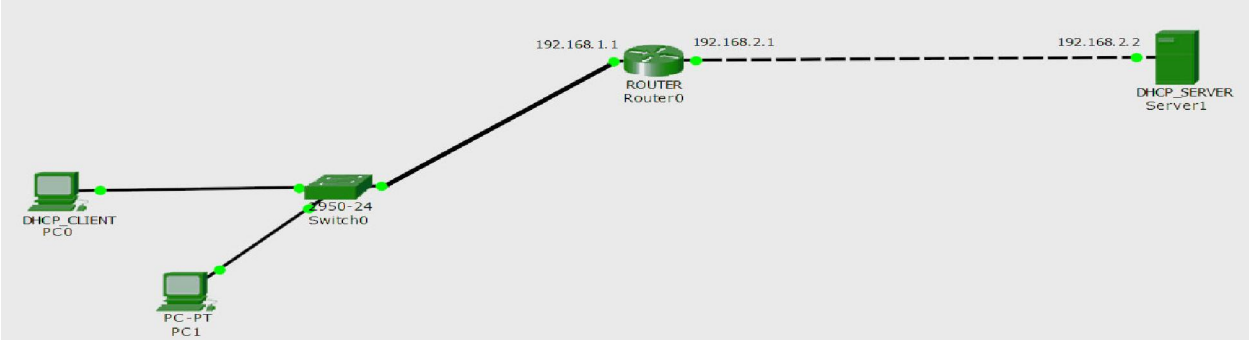
Show ip dhcp binding

LAB OBJECTIVE

- Verify if there is communication between the two PC and the printer

DHCP Helper Address/DHCP Relay Agent

DHCP relay agent is any TCP/IP host which is used to forward request and replies between DHCP server and client when the server is present on the different network. Relay agents receive DHCP messages and then generate a new DHCP message to send out on another INTERFACE.



There is a DHCP server having IP address 192.168.2.2 and there is a router in middle which we wants as DHCP relay agent has an IP address 192.168.1.1

Configuration

The ip helper address command is used for configuring the router as a dhcp relay agent, giving 192.168.2.2 the address of DHCP_server.

Router (Config) #int e1/0

Description **Switch_e1/1**

#No shut

#Int e1/0.**10**

#Description Accounts

#Encapsulation dot1Q **10**

ip address **192.168.1.1 255.255.255.0**

 # ip helper-address 192.168.2.2

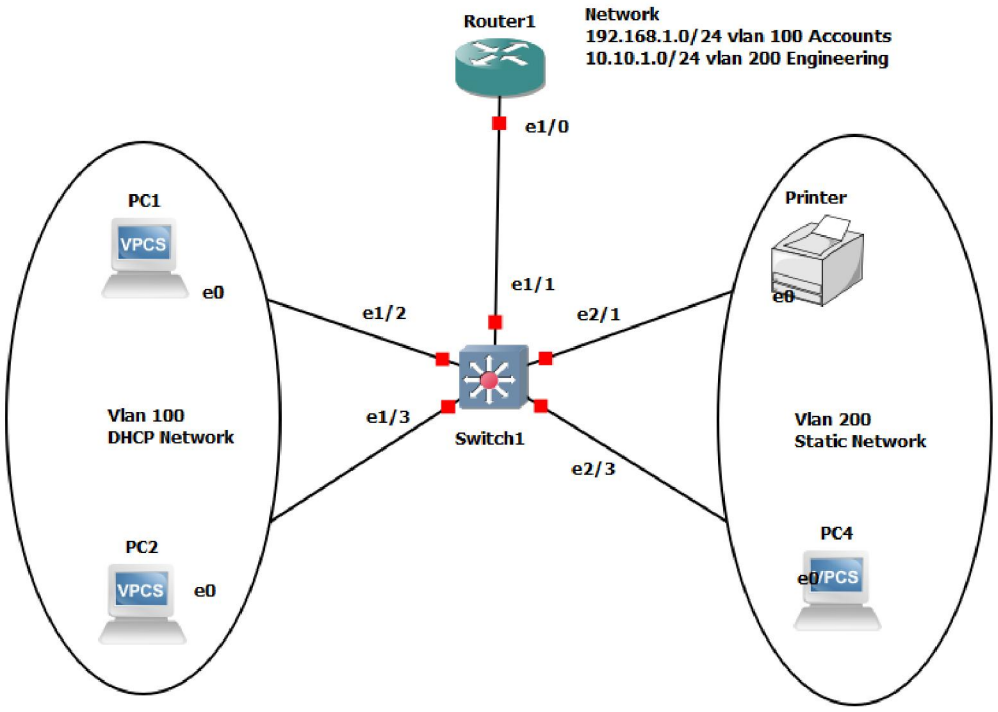
Interview Questions For Practice

QI: What is DHCP herlper address?

IQ: What is DHCP ?

IQ: How does DHCP work?

Lab Task#3



Global Configuration

1. Configure the hostname base on the Network Diagram
2. Disable the dns lookup feature.
3. Assign IK@ as the Secret password.
4. Direct the cisco IOS to encrypt any passwords stored in clear-text.

Console Port

5. Configure the console port on all devices to log input synchronously
6. Set password to @NPTC
7. Configure the idling timeout to 1 hour and 50 mins

VTY Ports

8. Allow 5 concurrent sessions of remote access
9. Configure the vty ports to log input synchronously
10. Set password to Pa$$co

11. Configure idling timeout to 50 mins and 10 seconds
12. Save config

Verify config

- **Assign IP address to the Router and describe the port and Network**

Router (Config)**#int e1/0**

 # Description Switch_e1/1

#No shut

#Int e1/0.100

#Description Accounts

#Encapsulation dot1Q 100

 # ip address 192.168.1.1 255.255.255.0

#Int e1/0.200

#Description Engineering

#Encapsulation dot1Q 200

 # ip address 10.10.1.1 255.255.255.0

Verify config

- **Configure the router to act as DHCP Server and exclude 20 IP addresses from the Accounts Scope**

Internet_Router(config)# ip dhcp pool **Accounts**

Network **192.168.1.0 255.255.255.0**
#default-router **192.168.1.1**
Lease **3 0**
ip dhcp excluded-address **192.168.1.1 192.168.1.20**

Verify config

Show run | begin dhcp

- **Configure the Vlan 100 and 200 on the switch and name it as follow**

Vlan 100- Accounts Department

Vlan 200 – Engineering Department

Verify config

- **Configure the switch virtual interface (SVI) using vlan 100 on the Switch**
- **Configure a Switch Default Gateway**
- **Configure Trunk Port to the port connected to the Router and the switch and describe the port connections**

Verify config

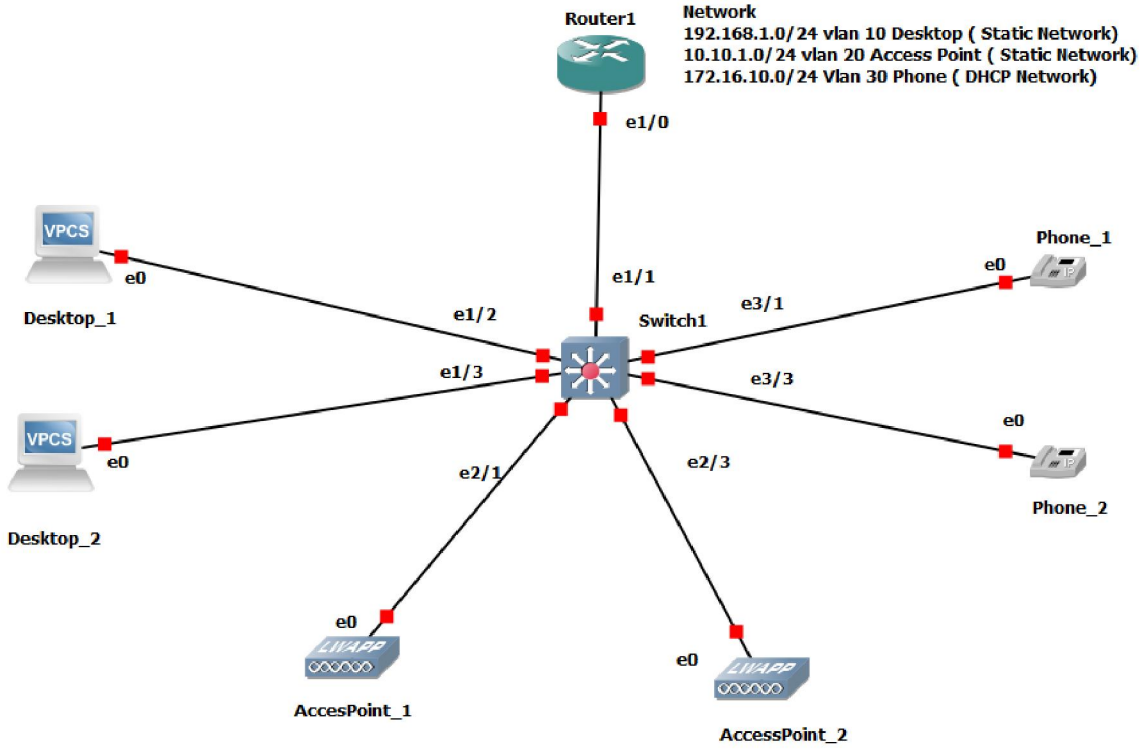
- **Assign Vlan to all the PCs and the printer base on the Network topology**

Verify config

- **Obtain DHCP address to the PCs and assign static IP address to the printer and PC 4.**

Verify config

DHCP Lab Assignment



Global Configuration

1. Configure the hostname base on the Network Diagram
2. Disable the dns lookup feature.
3. Assign IKE as the Secret password.
4. Direct the cisco IOS to encrypt any passwords stored in clear-text.

Console Port

5. Configure the console port on all devices to log input synchronously
6. Set password to NPTC
7. Configure the idling timeout to 1 hour and 30 mins

VTY Ports

8. Allow 5 concurrent sessions of remote access
9. Configure the vty ports to log input synchronously

10. Set password to V
11. Configure idling timeout to 15 mins and 10 seconds
12. Save config

Verify config

- **Assign IP address to the Router and describe the port and Network**

Verify config

- **Configure the router to act as DHCP Server and exclude 10 IP addresses from the Phone Scope**

Verify config

Show run | begin dhcp

Verify config

- **Configure vlan on the switch and name it as stated on the topology**
- **Configure the switch virtual interface (SVI) using vlan 10 on the Switch**
- **Configure a Switch Default Gateway**

Verify config

- **Configure Trunk Port to the port connected to the Router and describe the port connections**

Verify config

- **Assign Vlan to all connected devices base on the Network topology**

Verify config

- **Obtain DHCP address to connected DHCP Network and manually configured the static devices**

Lab Objective

Ensure communication among the entire device

Routing

Routing is the process of sending packets from a host on one network to another host on a different remote network. This process is usually done by routers. Routers examine the destination IP address of a packet, determine the next-hop address, and forward the packet. Routers use routing tables to determine a next hop address to which the packet should be forwarded.

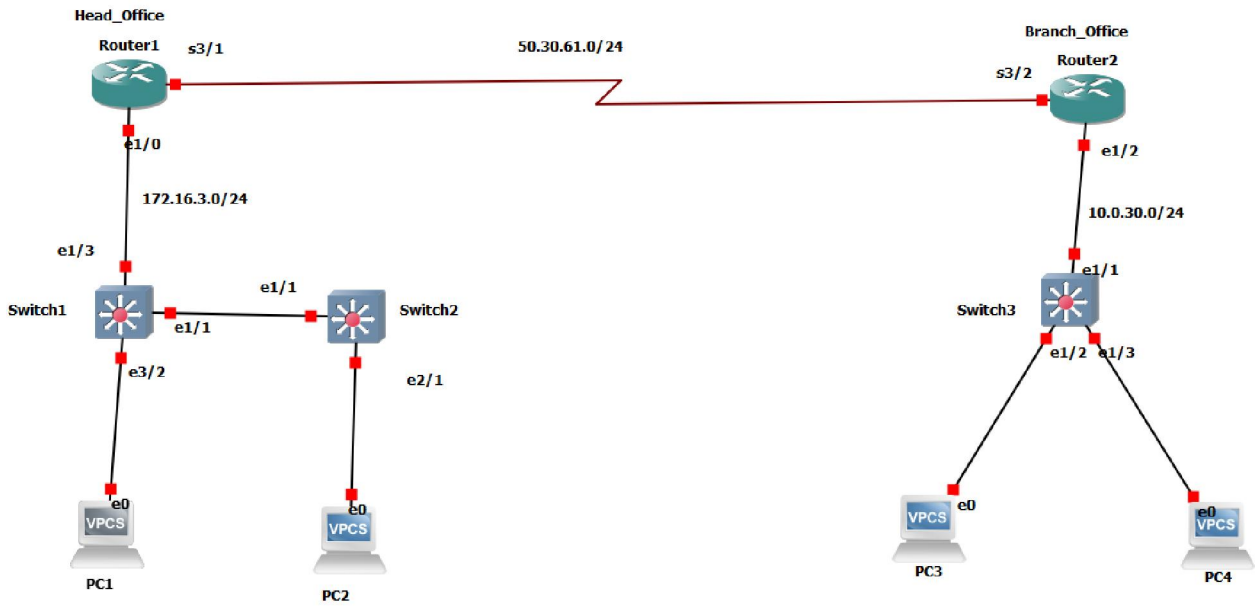
Routing Protocols

These are protocols which help Routing Protocols to carry their information from one router to another example: **Static routing** and **dynamic routing** such as OSPF, EIGRP, RIP, and BGP to figure out what paths traffic should take

Static Routing

Static routing is when you statically configure a **router** to send traffic for particular destinations in preconfigured directions

Lab Task # 4



Global Configuration

1. Configure the hostname base on the Network Diagram
2. Disable the dns lookup feature.
3. Assign IKE as the Secret password.

4. Direct the Cisco IOS to encrypt any passwords stored in clear-text.

Console Port

5. Configure the console port on all devices to log input synchronously
6. Set password to NPTC
7. Configure the idling timeout to 1 hour and 30 mins

VTY Ports

8. Allow 5 concurrent sessions of remote access
9. Configure the vty ports to log input synchronously
10. Set password to V
11. Configure idling timeout to 15 mins and 10 seconds
12. Save config

Verify the above steps using the proper Show command

13. Assigning IP Addresses and port description

1. Assign IP addresses to all the devices and describe the port base on the topology.

Verify the above steps using the proper Show command

- Show ip int br on the Router
- Show run int (base on the topology)
-

14. Configure the Branch Office to act as DHCP Server and exclude 10 IP addresses from the Vlan 20 Scope

Vlan and Trunk

15. **Configure Vlan 10 on Switch 1 & 2**
16. **Configure Vlan 20 on Switch 3**
17. **Configure the switch virtual interface (SVI) using respective vlan on the Switch**
18. **Configure a Switch Default Gateway**
19. **Configure Trunk Port base on the topology**
20. **Configure Access port base on the topology**
21. **Disable all port on the switches which are not connected.**

Verify the above steps using the proper Show command

- Show vlan brief
- Show int trunk
- Show int status

Lab Objective

Ensure communications among all devices

Static Routing

Configuration Example for Static Routes

Configuration using next hope address

Headoffice (config)#ip route 10.0.30.0 255.255.255.0 50.30.61.2

10.0.3.0 = destination network

255.255.255.0 = subnet mask

50.30.61.2 = next-hop address

To get to the destination network of 10.0.30.0, with a subnet mask of 255.255.255.0, send all packets to 50.30.61.2

10.0.30.0 = destination network

255.255.255.0 = subnet mask

S3/1 = exit interface

Configuration Using Exiting Interface

Headoffice(config)#ip route 10.0.30.0 255.255.255.0 s3/1

Read this to say: To get to the destination network of 10.0.30.0, with a subnet mask of 255.255.255.0, send all packets out interface Serial 3/1

Configuration using next hope address

Branchoffice(config)#ip route 172.16.3.0 255.255.255.0 50.30.61.1

To get to the destination network of 172.16.3.0, with a subnet mask of 255.255.255.0, send all packets to 50.30.61.1

172.16.3.0 = destination network

Configuration Using Exiting Interface

255.255.255.0 = subnet mask

Branchoffice(config)#ip route 172.16.3.0 255.255.255.0 s3/2

S3/2 = exit interface

Read this to say: To get to the destination network of 172.16.3.0, with a subnet mask of 255.255.255.0, send

all packets out interface Serial 3/1

Router # show ip route

When using the **Show ip route** command, you can identify where packets should be routed to in two ways:

- The next-hop address
- The exit interface

Headoffice# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

50.0.0.0/28 is subnetted, 1 subnets

C 50.30.60.48 is directly connected, Serial3/1

10.0.0.0/24 is subnetted, 1 subnets

S 10.0.3.0 [1/0] via 50.30.60.52

Default Routing

Configure Default Routing using project # 4

Remove the Static route and defined a default route.

Head office (config) #no ip route **10.0.3.0 255.255.255.0 s3/1**

Default Route

A default route is used by router to forward traffic from unknown destinations to other routers.

Configuration using next hop address

Headoffice(config)**#ip route 0.0.0.0 0.0.0.0 50.30.61.2**	Send all packets destined for networks not in my routing table to **50.30.61.2**

Configuration Using Exiting Interface

Router(config)**#ip route 0.0.0.0 0.0.0.0 s3/1**	Send all packets destined for networks not in my routing table out my Serial 3/1 interface

Branchoffice(config)**#ip route 0.0.0.0 0.0.0.0 50.30.61.1**	Send all packets destined for networks not in my routing table to **50.30.61.1**
Router(config)**#ip route 0.0.0.0 0.0.0.0 s3/2**	Send all packets destined for networks not in my routing table out my Serial 3/1 interface

Verifying Static Routes

Interview Questions for Practice

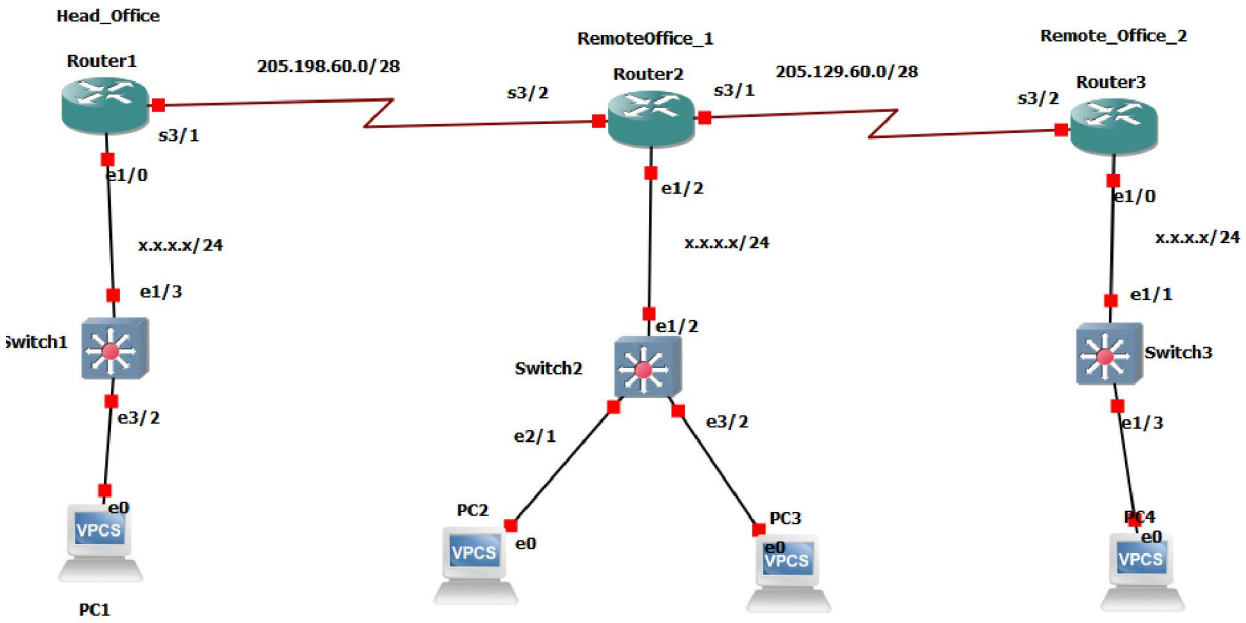
IQ: Define Static Routing?

IQ: What is Default Route?

IQ: What is Routing Protocol?

IQ: What is IGP?

Static task #5



Global Configuration

1. Configure the hostname base on the Network Diagram
2. Disable the dns lookup feature.
3. Assign IKE as the Secret password.
4. Direct the cisco IOS to encrypt any passwords stored in clear-text.

Console Port

5. Configure the console port on all devices to log input synchronously
6. Set password to NPTC
7. Configure the idling timeout to 1 hour and 30 mins

VTY Ports

8. Allow 5 concurrent sessions of remote access
9. Configure the vty ports to log input synchronously
10. Set password to V
11. Configure idling timeout to 15 mins and 10 seconds
12. Save config

Verify the above steps using the proper Show command

Assigning IP Addresses and port description

- **Choose your own local ip addresses to all the devices base on the topology.**

Verify the above steps using the proper Show command

- **Configure the Remoteoffice_1 to act as DHCP Server and exclude 10 IP addresses from the Vlan 200 Scope**

Vlan and Trunk

1. Configure Vlan 100 Name as Accounts on Switch1
2. Configure Vlan 200 Name as Stores on Switch 2
3. Configure Vlan 300 Name as Production on Switch 3
4. Configure Trunk Port base on the topology
5. Configure the switch virtual interface (SVI) using respective vlan on the Switch
6. Configure a Switch Default Gateway
7. Configure Access port base on the topology
8. Disable all port on the switches which are not connected.
9. Save Config

Verify the above steps using the proper Show command

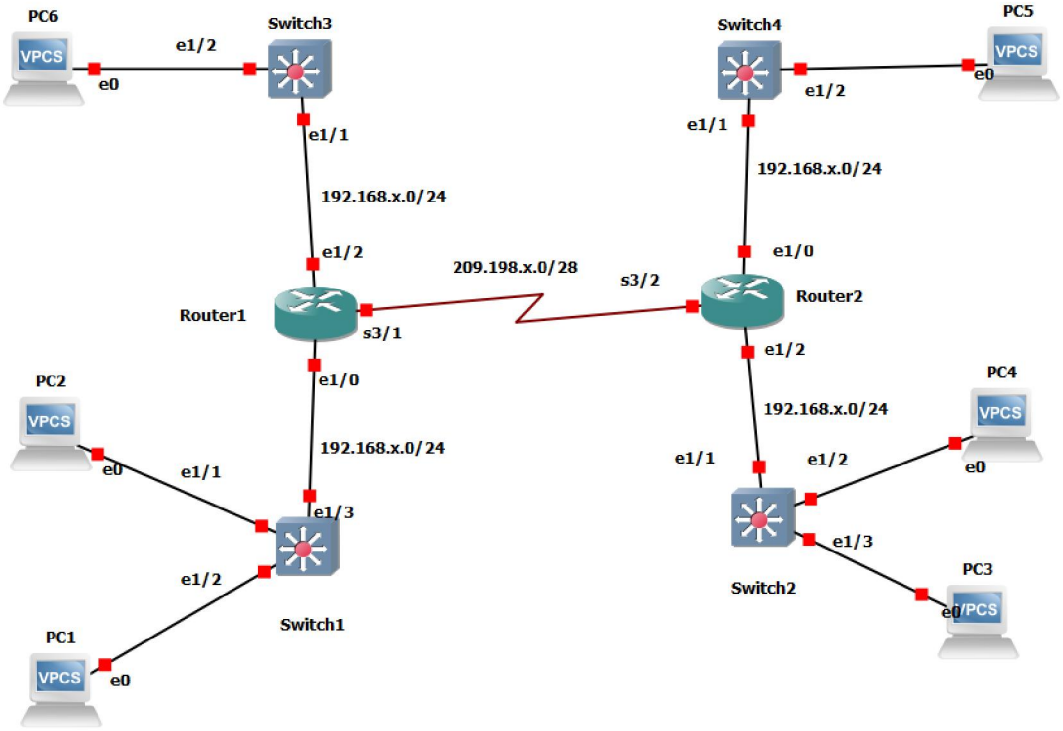
- **Configure the Static route Base on the topology**

Verify the above steps using the proper Show command

Lab Objective

Ensure communication among all devices

Static Lab Assignment



Global Configuration

1. Configure the hostname base on the Network Diagram
2. Disable the dns lookup feature.
3. Assign E as the Secret password.
4. Direct the cisco IOS to encrypt any passwords stored in clear-text.

Console Port

5. Configure the console port on all devices to log input synchronously
6. Set password to NP
7. Configure the idling timeout to 2 hour and 30 mins

VTY Ports

8. Allow 5 concurrent sessions of remote access
9. Configure the vty ports to log input synchronously
10. Set password to V
11. Configure idling timeout to 15 mins and 20 second

Verify the above steps using the proper Show command

- **Assign IP addresses to all the devices base on the topology.**

Verify the above steps using the proper Show command

- **Configure the Site_2 router to act as DHCP Server and exclude 10 IP addresses from the Vlan 104 Scope**

Vlan and Trunk

1. Configure Vlan 101 Name as Accounts on Switch1
2. Configure Vlan 102 Name as Directors on Switch 2
3. Configure vlan 103 on switch 3
4. Configure Vlan 104 on switch 4
5. Configure Trunk Port base on the topology
6. Configure Access port base on the topology
7. Disable all port on the switches which are not connected.
8. Save Config

Verify the above steps using the proper Show command

- **Configure the Static route Base on the topology**

Verify the above steps using the proper Show command

Lab Objective

Ensure communication among all devices

Enhanced Interior Gateway Routing Protocol (EIGRP)

Enhanced Interior Gateway Routing Protocol (EIGRP) is an advanced distance-vector routing protocol that is used on a computer network for automating routing decisions and configuration. The protocol was designed by Cisco Systems as a proprietary protocol, available only on Cisco routers.

It is a Cisco proprietary protocol, so all routers in a network that is running EIGRP must be Cisco routers.

EIGPR uses the concept of autonomous systems. An autonomous system is a set of EIGRP enabled routers that should become EIGRP neighbors. Each router inside an autonomous system must have the same autonomous system number configured; otherwise routers will not become neighbors.

EIGRP Neighbors

EIGRP must establish neighbor relationships with other EIGRP neighboring routers before exchanging routing information. To establish neighbor relationships, routers send hello packets every couple of seconds. Hello packets are sent to the multicast address of 224.0.0.10.

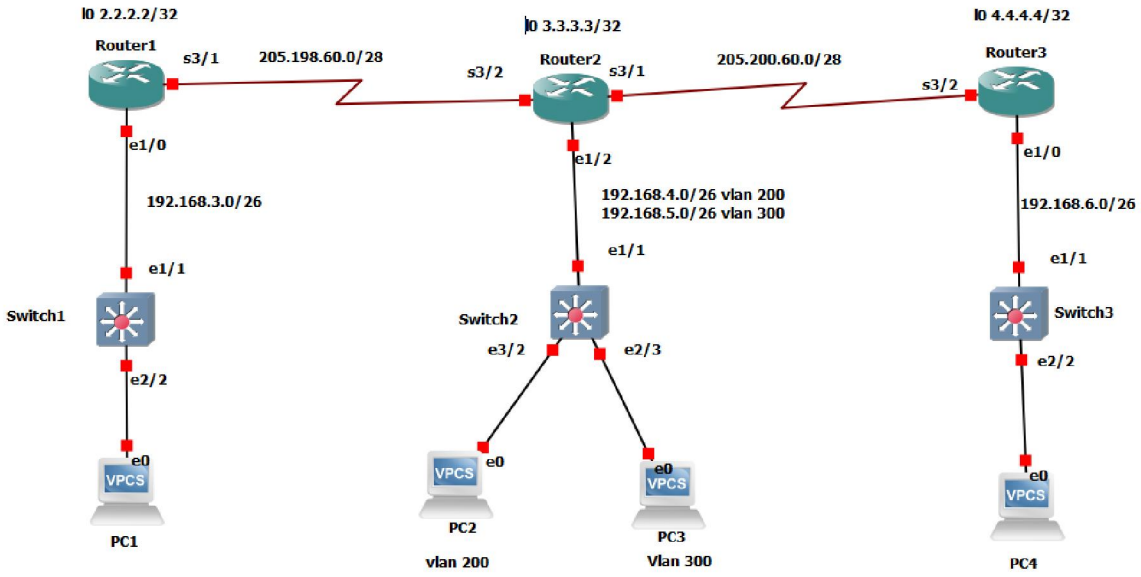
NOTE
On LAN interfaces hellos are sent every 5 seconds. On WAN interfaces every 60 seconds.

Routers send hello packets every couple of seconds to ensure that the neighbor relationship is still active. By default, a router considers the neighbor to be down after a hold-down timer has expired. Hold-down timer is, by default, three times the hello interval. On LAN network the hold-down timer is 15 seconds.

Show Command (EIGRP)

- **Show run | begin router** – shows the real configuration the eigrp
- **Show ip route** – display summary information about all routes for the specified protocol.
- **Show ip eigrp neighbor**- The neighbor table keeps a record of the IP addresses of routers that have a direct physical connection with this router

EIGRP Lab # 6



Global Configuration

1. Configure the hostname base as follows

   R1-WorcesterRouter
   R2-NatickRouter
   R3-BostonRouter

2. Disable the dns lookup feature.

3. Assign RING as the Secret password.
4. Direct the cisco IOS to encrypt any passwords stored in clear-text

Console Port

5. Configure the console port on all devices to log input synchronously
6. Set password to PTC

7. Configure the idling timeout to 40mins and 30 sec

VTY Ports

8. Allow 5 concurrent sessions of remote access
9. Configure the vty ports to log input synchronously
10. Set password to CR

11. Configure idling timeout to 60 mins and 60 seconds
12. Save config

- **Assign IP address and port description base on the topology and verify the interface.**

  Verify if the IP interface is up and can ping each other.

- **Configure the Natick_router to act as DHCP Server and exclude 10 IP addresses from the Vlan 200 Scope**

- **Configure the vlan below and assign it to the respective PCs**

  Switch1- Vlan100
  Switch2- Vlan 200 and 300
  Switch3- Vlan400

- **Create the loop back interface on all the routers**

Loopback Interface/Addresses

A loopback interface is a **logical**, **virtual** interface in a Cisco Router. A loopback interface is not a physical interface like Fast Ethernet interface or Gigabit Ethernet interface.

The loopback interface is used to identify the device. While any interface address can be used to determine if the device is online, the loopback address is the preferred method. Whereas interfaces might be removed or addresses changed based on network topology changes, the loopback address never changes.
When you ping an individual interface address, the results do not always indicate the health of the device.

Loopback Configuration Guide

WorcesterRouter # **conf t**

WorcesterRouter **(config)# int l0**

WorcesterRouter **(config)# ip add 2.2.2.2 255.255.255.255**

NatickRouter # **conf t**

NatickRouter **(config)# int l0**

NatickRouter **(config)# ip add 3.3.3.3 255.255.255.255**

BostonRouter# **conf t**

BostonRouter**(config)# int l0**

BostonRouter(config)# ip add 4.4.4.4 255.255.255.255

- **Configure all the routers with the EIGRP using (autonomous system) AS 100**

Verify your config with the following show command

1. Verify EIGRP neighbors

Verify EIGRP learned routes and connectivity

EIGRP Configuration Guide

```
WorcesterRouter# configure terminal
WorcesterRouter(config)# router eigrp 100
WorcesterRouter(config-router)# network 2.2.2.2  0.0.0.0
WorcesterRouter(config-router)# network 192.168.3.0   0.0.0.63
WorcesterRouter(config-router)# network 205.198.60.0   0.0.0.15
WorcesterRouter(config-router)# no auto-summary
WorcesterRouter(config-router)# exit

NatickRouter# configure terminal
NatickRouter(config)# router eigrp 100
NatickRouter(config-router)# network 3.3.3.3  0.0.0.0
NatickRouter(config-router)# network 192.168.4.0   0.0.0.63
NatickRouter(config-router)# network 192.168.5.0   0.0.0.63
NatickRouter(config-router)# network 205.200.60.0   0.0.0.15
NatickRouter(config-router)# network 205.198.60.0   0.0.0.15
NatickRouter(config-router)# no auto-summary
NatickRouter(config-router)# exit

BostonRouter# configure terminal
Boston(config)# router eigrp 100
BostonRouter(config-router)# network 4.4.4.4  0.0.0.0
BostonRouter(config-router)# network 192.168.6.0   0.0.0.63
BostonRouter(config-router)# network 205.200.60.0   0.0.0.15
BostonRouter(config-router)# no auto-summary
BostonRouter(config-router)# exit
```

Verify your config with the following show command

- Show ip route – display summary information about all routes for the specified protocol.

- Show ip eigrp neighbor- The neighbor table keeps a record of the IP addresses of routers that have a direct physical connection with this router

EIGRP automatic & manual summarization

Route summarization is a method of representing multiple networks with a single summary address. It is often use in large networks with many subnets because it reduces the number of routes that a router must maintain and minimizes the traffic used for routing updates. Two methods for summarizing routes exist: automatic summarization and manual summarization.

EIGRP automatic summarization

By default, EIGRP has the auto summary feature enabled. Because of this, routes are summarized to classful address at network boundaries in the routing updates.

The manual summarization in EIGRP is configured on the per-interface basis. The syntax of the command is:

(config-if)ip summary-address eigrp ASN SUMMARY_ADDRESS SUBNET_MASK

So if we want to summarize the route on Router 1 the configuration should be done on router 2 with the interface going to router 1

```
NatickRouter# configure terminal
        #Int s3/2
        #ip summary-address eigrp 100 192.168.0.0   255.255.0.0
```

Interview Questions

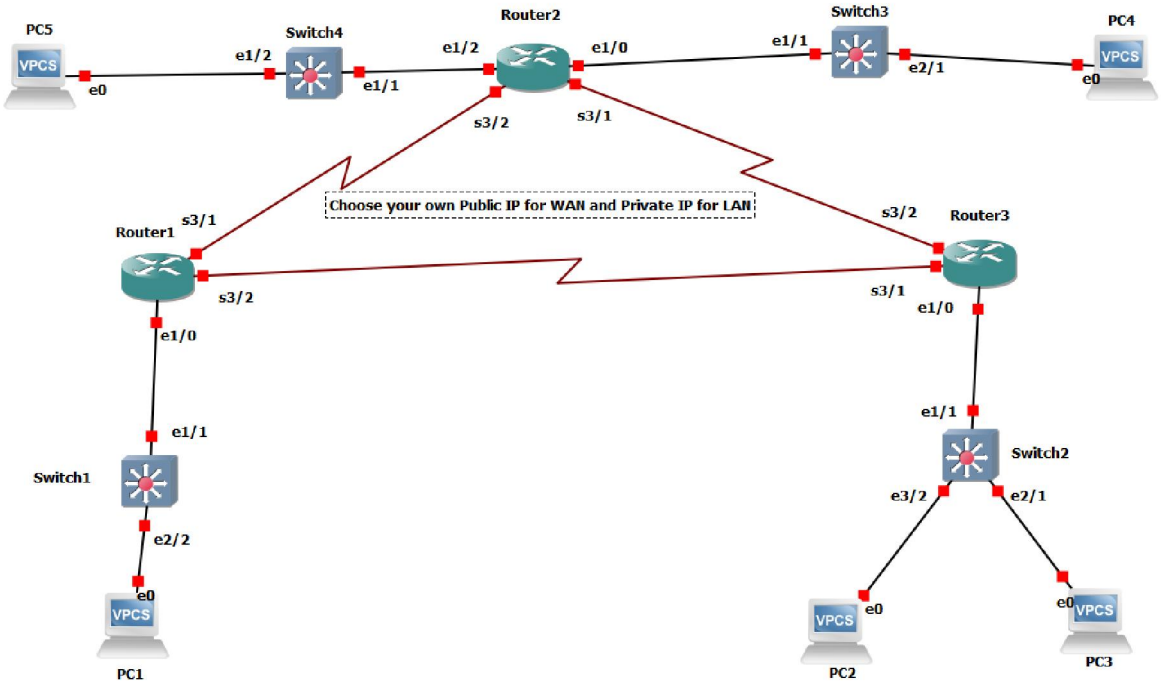
IQ: why no auto-summary command used in EIGRP?

IQ: IQ: How we configure EIGRP?

IQ: Give some commands to troubleshoot EIGRP?

IQ: What is AD for EIGRP?

EIGRP Assignment



Global Configuration

1. Configure the hostname base as follows

   R1- Router_1
   R2-Router_2
   R3-Router_3
   R4-Router_4

2. Disable the dns lookup feature.

3. Assign RING as the Secret password.
4. Direct the cisco IOS to encrypt any passwords stored in clear-text

Console Port

5. Configure the console port on all devices to log input synchronously
6. Set password to TC
7. Configure the idling timeout to 20mins and 20 sec

VTY Ports

8. Allow 5 concurrent sessions of remote access
9. Configure the vty ports to log input synchronously
10. Set password to CR
11. Save config

- **Assign IP address and port description base on the topology and use your own public IP addresses on WAN.**

Verify if the IP interfaces are up and can ping each other.

- **Configure all the routers with the EIGRP using autonomous system (AS) 400**

Verify your config with the following show command

Verify EIGRP neighbors

Verify EIGRP topology
Verify EIGRP learned routes and connectivity

Lab Objective

Ensure communication among all devices

Open Shortest Path First (OSPF)

Open Shortest Path First (**OSPF**) is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing (LSR) algorithm and falls into the group of interior gateway protocols (IGPs), operating within a single autonomous system (AS). It is defined as OSPF Version 2 for IPv4. The updates for IPv6 are specified as OSPF Version3

OSPF is an open standard industry protocol, which can also be used with non-Cisco devices like Juniper Routers running OSPF have to establish neighbor relationships before exchanging routes. Because OSPF is a link state routing protocol, neighbors don't exchange routing tables. Instead, they exchange information about network topology.

By default, OSPF sends hello packets every 10 second on an Ethernet network (Hello interval). A dead timer is four times the value of the hello interval, so if a router on an Ethernet network doesn't receive at least one Hello packet from an OSFP neighbor for 40 seconds, the routers declares that neighbor to be down.

OSPF areas

OSPF uses the concept of areas. An area is a logical grouping of contiguous networks and routers. All routers in the same area have the same topology table, but they don't know about routers in the other areas. The main benefits of creating areas is that the size of the topology and the routing table on a router is reduced, less time is required to run the SFP algorithm and routing updates are also reduced.

Each area in the OSPF network has to connect to the backbone area (area 0). All router inside an area must have the same area ID to become OSPF neighbors. A router that has interfaces in more than one area (area 0 and area 1, for example) is called **Area Border Router (ABR)**. A router that connects an OSPF network to other routing domains (EIGRP network, for example) is called **Autonomous System Border Router (ASBR)**.

NOTE

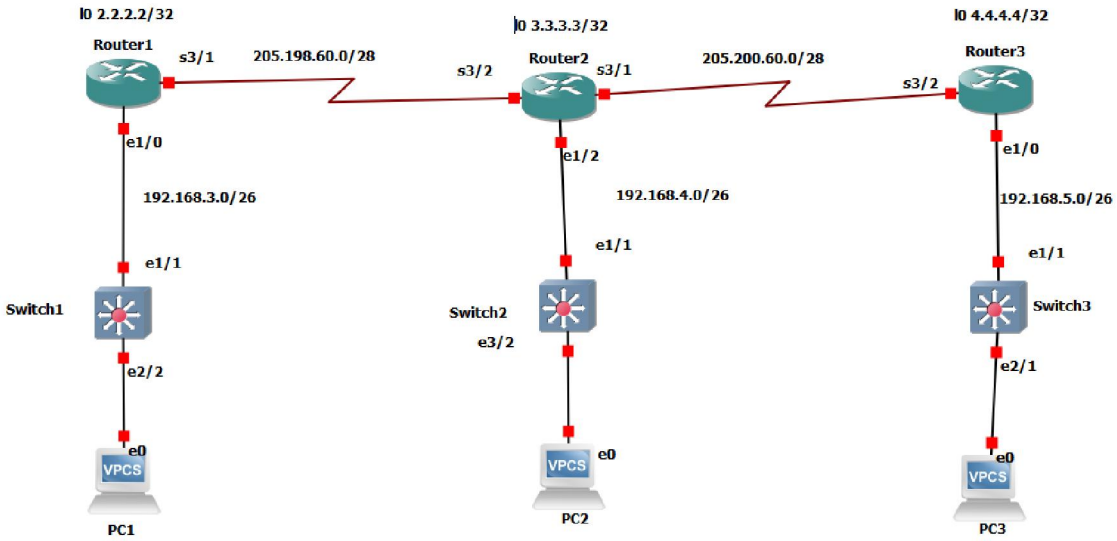
In OSPF, manual route summarization is possible only on ABRs and ASBRs.

What is the difference between EIGRP and OSPF

The following table lists the differences between OSPF and EIGRP:

Protocol	Type of routing	Metric	Manual summarization	Load balancing	Administrative distance	Cisco proprietary	Multicast address
EIGRP	advanced distance vector	composite of bandwidth and delay	on all routers	equal and unequal cost load balancing	90	Yes	224.0.0.10
OSPF	link state	cost	only on ABRs and ASBRs	equal cost load balancing	110	No	224.0.0.5, 224.0.0.6

OSPF Lab #7



Global Configuration

1. Configure the hostname base as follows

   R1- HeadOffice
   R2-Remote_Office_1
   R3-Remote_Office_2

2. Disable the dns lookup feature.

3. Assign RING as the Secret password.
4. Direct the cisco IOS to encrypt any passwords stored in clear-text

Console Port

5. Configure the console port on all devices to log input synchronously

6. Set password to PTC
7. Configure the idling timeout to 40mins and 30 sec

VTY Ports

8. Allow 5 concurrent sessions of remote access
9. Configure the vty ports to log input synchronously
10. Set password to CR
11. Configure idling timeout to 60 mins and 60 seconds
12. Save config

Assigning IP Addresses

- **Assign IP address and describe the port base on the topology and verify the interface.**

  Verify if the IP interfaces are up and can ping each other.

- **Configure all the routers with the OSPF using AS 10 and an Area 100**

Configuration Guide

Router_R1(config)#**router ospf 10**

 # Network 2.2.2.2 0.0.0.0 area 100

 # Network 192.168.3.0 0.0.0.63 area 100

#Network 205.198.60.0 0.0.0.15 area 100

Router_R2 (config)#**router ospf 10**

 # Network 3.3.3.3 0.0.0.0 area 100

 # Network 192.168.4.0 0.0.0.63 area 100

 # Network 205.198.60.0 0.0.0.15 area 100

#Network 205.200.60.0 0.0.0.15 area 100

Router_R3(config)#**router ospf 10**

 # Network 4.4.4.4 0.0.0.0 area 100

 # Network 192.168.5.0 0.0.0.63 area 100

 # Network 205.200.60.0 0.0.0.15 area 100

Verify your config with the following show command

Show run | sec ospf

Show ip OSPF neighbors

Interview Questions

QI: What is OSPF routing protocol?

QI: Mention some characteristics of OSPF?

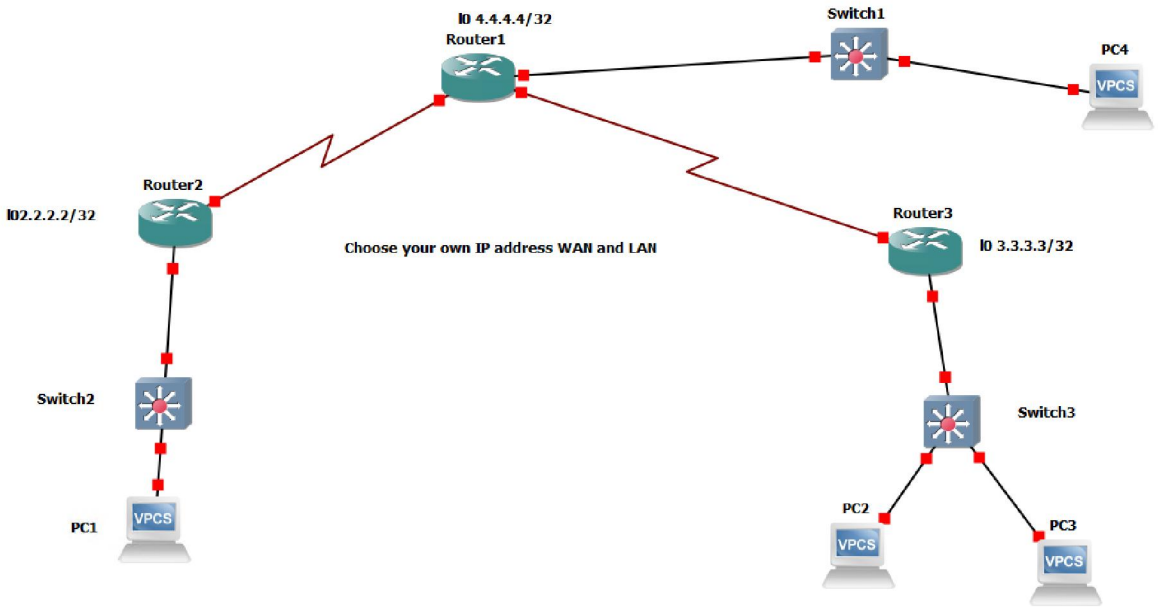
QI: What is the benefit of dividing the entire network into areas?

QI: what is Backbone Area?

Q1: Explain ABR?

QI: What is the AD for OSP

Ospf Assignment



Global Configuration

1. Configure the hostname base on the Network Diagram
2. Disable the dns lookup feature.
3. Assign IKE as the Secret password.
4. Direct the cisco IOS to encrypt any passwords stored in clear-text.

Console Port

5. Configure the console port on all devices to log input synchronously
6. Set password to N

7. Configure the idling timeout to 1 hour and 30 mins

VTY Ports

8. Allow 5 concurrent sessions of remote access
9. Configure the vty ports to log input synchronously
10. Set password to R
11. Configure idling timeout to 40 mins and 10 seconds
12. Save config

Verify the above steps using the proper Show command

Vlan and Trunk

13. Configure Vlan 10 Name as headoffice on Switch1
14. Configure Vlan 20 Name as Stores on Switch 2
15. Configure Vlan 30 Name as Accounts on Switch 3
16. Configure Trunk Port base on the topology
17. Configure Access port base on the topology
18. Disable all port on the switches which are not connected.
19. Save Config

Verify the above steps using the proper Show command

Assigning IP Addresses

- **Assign Ip addresses to all the devices base on the topology.**

Verify the above steps using the proper Show command

- **Configure all the routers with the OSPF using AS 100 and an Area 50**

Verify the above steps using the proper Show command

Lab Objective

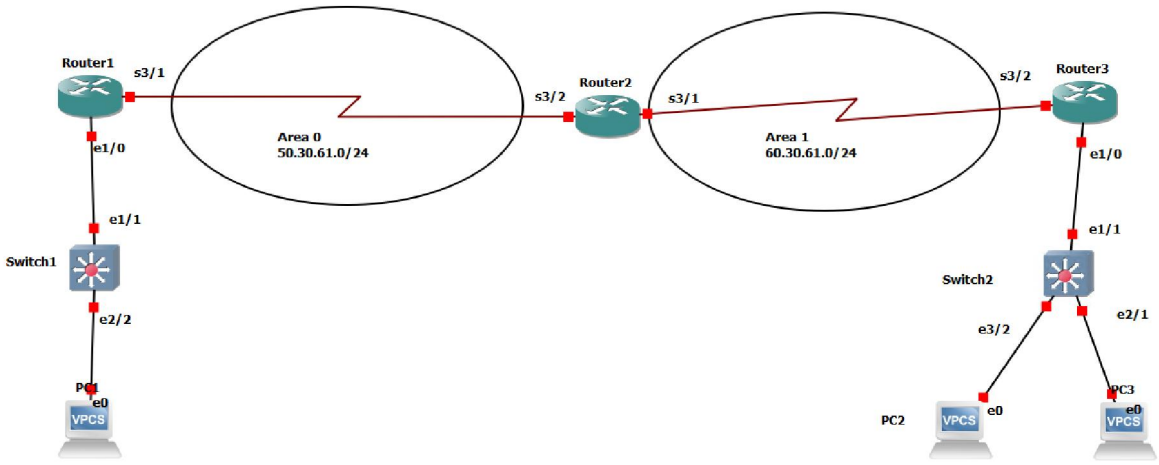
Ensure communication among all the devices

OSPF with Multi Area

You can have multiple areas to contain your routing updates within your area, thereby the ospf database would be smaller resulting in faster convergence. If there is a link instability in your area that will not disturb other areas, if you have multiple areas.

Summarization is also a very big benefit of this structure, and everyone should consider making their networks contiguous.

Lab Task 8



Global Configuration

1. Configure the hostname as follow

   R1- Russia_Router

R2-China_Router
R3-UK_Router
EWS1- Russia_Switch
ESW2- UK_Switch

2. Disable the dns lookup feature.
3. Assign Pa$$ as the Secret password.
4. Direct the cisco IOS to encrypt any passwords stored in clear-text.

Console Port

5. Configure the console port on all devices to log input synchronously
6. Set password to w0rd
7. Configure the idling timeout to 1 hour and 30 mins

VTY Ports

8. Allow 5 concurrent sessions of remote access
9. Configure the vty ports to log input synchronously
10. Set password to 100k
11. Configure idling timeout to 15 mins and 10 seconds
12. Save config

Verify the above steps using the proper Show command

Vlan and Trunk

13. Configure Vlan 450 on Russia_Switch and name it as Data
14. Configure Vlan 20 and 10 on UK_switch and name it as Data and Voice respectively
15. Configure Trunk Port base on the topology
16. Configure Access port base on the topology by using vlan 10 for port 2 and 20 for port 1
17. Disable all port on the switches which are not connected.

Verify the above steps using the proper Show command

Assigning IP Addresses

- **Assign IP addresses to all the devices and describe the port base on the topology.**

Verify the above steps using the proper Show command

- Show ip int br on the Router

- Show IP on the PC

DHCP Server

- **Configure Russia routers as DHCP server using it respective Network.**

Verify by obtaining DHCP ip address on all the PCs

OSPF Network

- **Configure ospf on the entire routers using AS 20**

Verify the above steps using the proper Show command

Configure route on the border router using the respective area

Configuration Guide for Multi Area System

China_Router (Config) # router ospf **20**

Network **50.30.61.0 0.0.0.255** area **0**

Network **60.30.61.0 0.0.0.255** area **1**

OSPF summarization

Route summarization helps reduce OSPF traffic and route computation. OSPF, unlike EIGRP, doesn't support automatic summarization. Also, unlike EIGRP, where you can summarize routes on every router in an EIGRP network, OSFP can summarize routes only on ABRs and ASBRs.

The following command is used for OSPF summarization:

(config-router) area AREA_ID range IP_ADDRESS MASK

So if we want to summarize the route on Router 1 the configuration should be done on router 2

China_Router (Config) # router ospf **20**

area **1** range **172.16.0.0 255.255.0.0**

Redistribution of Protocols

Route redistribution is when you take a **route** from one **routing** protocol and distribute it into another protocol. By default, routers only advertise and share **routes** with other routers running the same protocol.

Small companies mostly run one routing protocol like OSPF, EIGRP or static. As the company get bigger and buy more than one company that run different protocols. Then you will need to redistribute your route.

Redistribution Configuration for different Different EIGRP AS Number

Router eigrp 100

Redistribute eigrp 200

Router eigrp 200

redistributeeigrp100

Redistribution Configuration for different Different OSPF AS Number

Router ospf 1

Redistribute ospf 2 subnet

Router ospf 2

Redistribute ospf 1 subnet

Redistribution Configuration with mixed OSPF & EIGRP Environment

Router ospf 1

Redistribute eigrp 500 subnets

Router eigrp 500

Redistribute ospf 1 metric 5000 10 255 255 65535

Redistribution configuration with default route and EIGRP

ip route 0.0.0.0 0.0.0.0 s3/1

router eigrp 1

redistribute static

Redistribution configuration with default route and OSPF

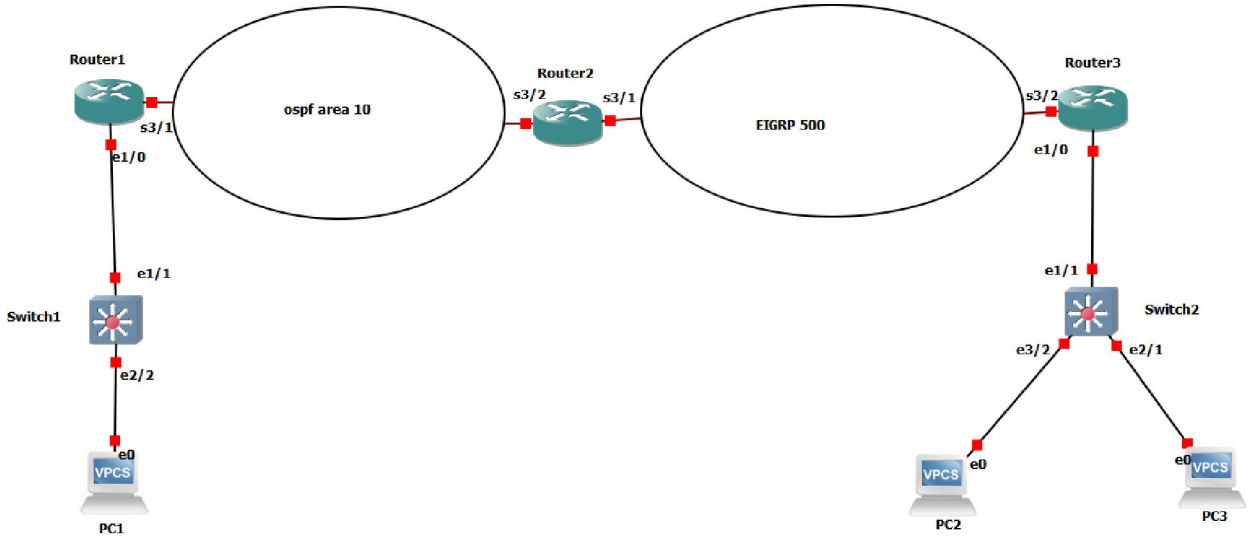
ip route 0.0.0.0 0.0.0.0 s3/1

router ospf 1

default-information originate

OSPF TO EIGRP Redistribution

Lab # 9



Global Configuration

1. Configure the hostname as follow

   R1- Singapore_Router
   R2-Germany_Router
   R3-Worcester_Router
   EWS1- Singapore_Switch

ESW2- Worcester_Switch

2. Disable the dns lookup feature.
3. Assign Pa$$w0rd as the Secret password.
4. Direct the cisco IOS to encrypt any passwords stored in clear-text.

Console Port

5. Configure the console port on all devices to log input synchronously
6. Set password to W0rd
7. Configure the idling timeout to 1 hour and 30 mins

VTP Ports

8. Allow 5 concurrent sessions of remote access
9. Configure the vty ports to log input synchronously
10. Set password to Vod
11. Configure idling timeout to 15 mins and 10 seconds
12. Save config

Verify the above steps using the proper Show command

Vlan and Trunk

13. Configure Vlan 10 on Worcester_Switch and name it as Data
14. Configure Vlan 20 on Singapore_switch and name it as Data
15. Configure Trunk Port base on the topology
16. Configure Access port base on the topology
17. Disable all port on the switches which are not connected.

Verify the above steps using the proper Show command

Assigning IP Addresses

- **Assign your own IP addresses to create network to all the devices and describe the port base on the topology.**

Verify the above steps using the proper Show command

- Show ip int br on the Router
- Show IP on the PC

DHCP Server

- **Configure both routers as DHCP server using it respective Network and reserved 10 IPs**

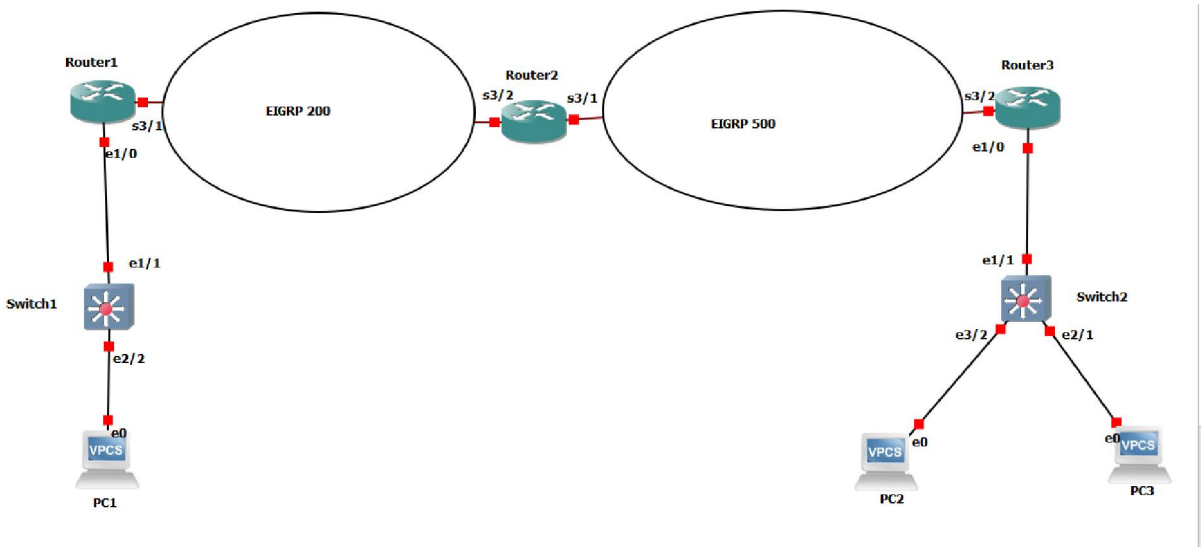
Verify by obtaining DHCP ip address on all the PCs

- **Configure EIGRP and OSPF on the entire routers base on the topology**

Verify the above steps using the proper Show command

- **Configure redistribution route on the border router**

Redistribution Assignment



Global Configuration

1. Configure the hostname as follow

   R1- Singapore_Router
   R2-Germany_Router
   R3-Worcester_Router
   EWS1- Singapore_Switch
   ESW2- Worcester_Switch

2. Disable the dns lookup feature.
3. Assign Pa$$w0rd as the Secret password.

4. Direct the cisco IOS to encrypt any passwords stored in clear-text.

Console Port

5. Configure the console port on all devices to log input synchronously
6. Set password to W0rd
7. Configure the idling timeout to 1 hour and 30 mins

VTP Ports

8. Allow 5 concurrent sessions of remote access
9. Configure the vty ports to log input synchronously
10. Set password to Vod
11. Configure idling timeout to 15 mins and 10 seconds
12. Save config

Verify the above steps using the proper Show command

Vlan and Trunk

13. Configure Vlan 10 on Worcester_Switch and name it as Data
14. Configure Vlan 20 on Singapore_switch and name it as Data
15. Configure Trunk Port base on the topology
16. Configure Access port base on the topology
17. Disable all port on the switches which are not connected.
18.

Verify the above steps using the proper Show command

Assigning IP Addresses

- **Assign your own IP addresses to create network to all the devices and describe the port base on the topology.**

Verify the above steps using the proper Show command

- Show ip int br on the Router
- Show IP on the PC

DHCP Server

- **Configure both routers as DHCP server using it respective Network and reserved 10 IPs**

Verify by obtaining DHCP ip address on all the PCs

- **Configure EIGRP on both sides and redistribute the different AS number base on the topology**

Verify the above steps using the proper Show command

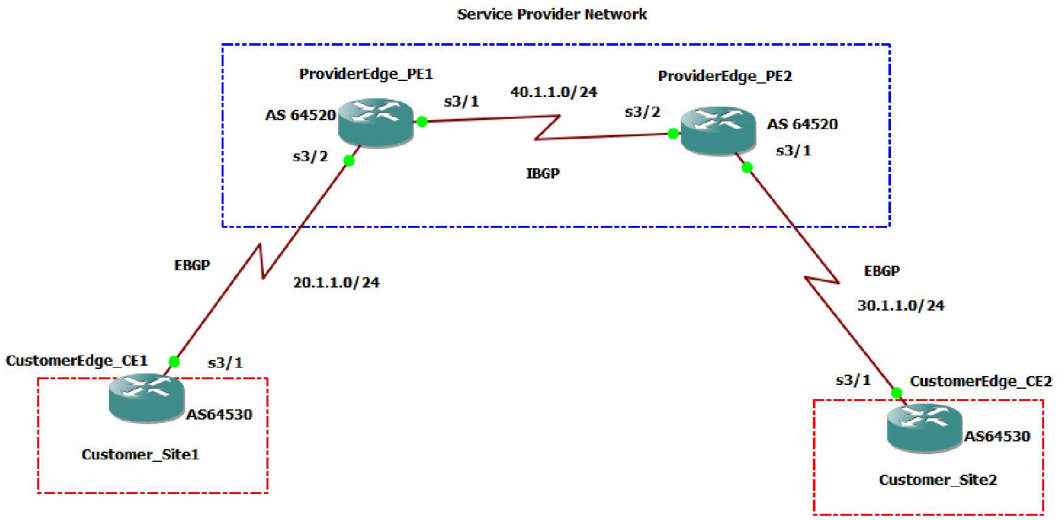
Border Gateway Protocol (BGP)

BGP stands for Border Gateway Protocol and it is the main dynamic routing protocol used on the Internet. BGP is for the large networks and normally used for connecting different ISPs.

The Border Gateway Protocol makes routing decisions based on paths, network policies, or rule-sets configured by a network administrator and is involved in making core routing decisions.

When BGP runs between two peers in the same autonomous system (AS), it is referred to as *Internal BGP* (**iBGP** or Interior Border Gateway Protocol). When it runs between different autonomous systems, it is called *External BGP* (**eBGP** or Exterior Border Gateway Protocol). Routers on the boundary of one AS exchanging information with another AS are called *border* or *edge routers* or simply eBGP *peers* and are typically connected directly

BGP lab #10



Customer Edge (CE) router sits at the edge of a customer site and is typically owned by the customer.

Provider Edge (PE) router sits at the edge of the provider's network, connecting one or several CE routers.

Global Configuration

1. Configure the hostname
2. Disable the dns lookup feature.
3. Assign Pa$$w0rd as the Secret password.
4. Direct the cisco IOS to encrypt any passwords stored in clear-text.

Console Port

5. Configure the console port on all devices to log input synchronously
6. Set password to Pass
7. Configure the idling timeout to 1 hour and 0 mins

VTP Ports

8. Allow 5 concurrent sessions of remote access

9. Configure the vty ports to log input synchronously
10. Set password to Pass
11. Configure idling timeout to 20 mins and 10 seconds
12. Save config

Verify the above steps using the proper Show command

- **Assign IP address and describe the port base on the topology and verify the interface.**

Verify if the IP interfaces are up and can ping each other

Configuration Guide for BGP

PE1 Router

ProviderEdge_PE1(config)# **router bgp 64520**

ProviderEdge_PE1(config-router)#**neighbor 40.1.1.2 remote-as 64520**

ProviderEdge_PE1(config-router)#**neighbor 20.1.1.2 remote-as 64530**

PE2 Router

ProviderEdge_PE2(config)# **router bgp 64520**

ProviderEdge_PE2(config-router)#**neighbor 40.1.1.1 remote-as 64520**

ProviderEdge_PE2(config-router)#**neighbor 30.1.1.1 remote-as 64530**

CE1Router

CustomerEdge_CE1(config)# **router bgp 64530**

CustomerEdge_CE1(config-router)#**neighbor 20.1.1.1 remote-as 64520**

CE2 Router

CustomerEdge_CE2(config-if)# router bgp 64530

CustomerEdge_CE2(config-router)#neighbor 30.1.1.2 remote-as 64520

Show command for BGP

- Show run | sec bgp
- show ip bgp

- show ip bgp summary
- show ip bgp neighbors

ProviderEdge_PE1#show ip bgp summary

BGP router identifier 40.1.1.1, local AS number 64520

BGP table version is 1, main routing table version 1

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
20.1.1.2	4	64530	23	23	1	0	0	00:17:54	0
40.1.1.2	4	64520	16	17	1	0	0	00:12:05	0

Route Source	Administrative Distance Values
Connected interface	0
Static route	1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route	5
External Border Gateway Protocol (eBGP)	20
EIGRP	90
IGRP	100
OSPF	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Internal BGP(iBGP)	200

General BGP Interview Questions most face in **networking job interview.**

What you know about BGP, explain some basic characteristics?

BGP is a path-vector protocol with following common characteristics:

- Uses TCP to transfer data, this ensures reliable delivery of protocol updates (port 179)
- Sends updates only after network changes (no periodic updates)
- Periodically sends keepalive messages to verify TCP connections.
- The protocol metric is called path vector or attributes.

What is default administrative distance for BGP?

Following are the default administrative distance for BGP routes:

External BGP route=20
EGP route=140

External EIGRP route=170
Internal BGP route=200

Name few well known BGP metric's attributes?

BGP path selection depends on the following attributes values:

- Weight(Cisco proprietary attributes)
- Local Preference (highest local value will be preferred, default value is 100)
- Originate
- AS path length
- Origin code
- MED
- eBGP path over iBGP path
- Shortest IGP path to BGP next hop
- Oldest path
- Router ID
- Neighbor IP address

What Are Different BGP Message Types?

Open: Open message is Used to create a neighbor relationship and exchange BGP=parameters, including AS number and authentication values.
Keep-alive: These keepalive messages are sent periodically to keep the neighbor relation-ship. If the Keep-alive messages are not received within a Hold timer than BGP neighbor-ship will be break down.
Update messages: These messages are used to exchanges Path Attributes and the associated prefix /l ength that use those attributes.
Notification: In BGP notifications are used to report BGP problem or errors. It results in a reset of neighbor relationship.

What is IBGP and EBGP ?

IBGP works within the single AS and transfer BGP routes within a single autonomous system.
EBGP: BGP running between autonomous systems. By default, eBGP neighbors must be directly connected.

Name some BGP Timers?

- **Keepalive Interval:**The time interval in seconds, between sending keep-alive messages. The default keepalive timer is 60
  seconds.
- **Hold Time:** Interval in seconds, after which the neighbor will be considered unavailable. The default is hold down time is 180 seconds.

What are the different Neighbor Adjacency States Of Bgp?

It is an important concept regarding BGP Interview Questions, following are Neighbor Adjacency States Of Bgp:

Idle: The BGP process is either administratively down or waiting for new neighbor adjacency.
Connect: During the BGP process, if the TCP connection is successful, it will continue to the Open=Sent state. In case it fails, it will continue to the Active state.
Active: BGP will try another TCP three way handshake to create a connection to remote BGP-neighbor. If it is successful, it will move to the Open-Sent state.
Open-sent: The TCP connection exists, and a BGP Open message has been sent to the peer, but the matching Open

message has not yet been received from the other router.
Open-confirm: When an Open message has been received from neighbor router, a BGP Neighbor Adjacency is complete. A hold down timer will starts once this done.
Established: All BGP neighbor parameters matched, the neighbor relationship has been established and the peers can now exchange Update messages.

Can router on different subnet become BGP neighbor ?

The answer is Yes. BGP router become neighbors on different subnets. Instead, BGP use a TCP connection between the neighbor routers to pass BGP messages on the same or different subnet.

Which TCP port BGP use?

Border Gateway Protocol uses TCP port number 179 for creating connection. (Most common BGP interview question

What is BGP path selection criteria?

If no path selection policies are configured for BGP on the Cisco router. Then router will go to each next step only if the values match the previous one.

1. The maximum weight value (local to the router).
2. The maximum value of local preference (for the whole AS).
3. Prefer the local route of the router (next hop = 0.0.0.0).
4. The shortest path through autonomous systems. (shortest AS_PATH)
5. The minimum value of the origin code (IGP <EGP <incomplete).
6. The minimum value of MED (distributed between autonomous systems).
7. The eBGP path is better than the iBGP path.
8. Choose a path through the nearest IGP neighbor.
9. Select the oldest route for the eBGP path.
10. The neighbor with the lowest BGP router ID
11. In last the neighbor with the smallest IP addresses

(This is a very important BGP interview Questions to remember.)

What is transit AS?

With Transit AS you can transmitted traffic of other autonomous systems.

What is Split-horizon?

Split horizon is a rule that a routing information will not be send back to router from which it is received. Mean a routing information will not send back in a direction from which side he received. This is a very important concept and used for preventing the routing loop in a network.

(Alternatively you may asked this question in BGP interview questions.)

What are Loop prevention mechanism in BGP?

There are two mechanisms to prevent loops in BGP:

- When we are advertising to an eBGP router/peer, a BGP router adds its own A SN to the AS-PATH. If a BGP router receives an update & route advertisement lists an AS-PATH with its own ASN, then the router ignores that route.

- When a router learns routes from an iBGP peer, that router does not advertise the same routes to another
  iBGP peer.

What is eBGP multihop?

When eBGP peers or routers are not directly connected with each other. And there are one or more non BGP peers to reach BGP router. You are required to configure eBGP multihop to enables the non BGP routes to pass through the BGP neighbor relationship & exchange update-messages.

What is BGP TLL Security ?

BGP TTL Security is a Security technique and Mechanism, which is used to implemented/enhance the security of of the TCP connection between BGP peers. You can secure BGP connection by disconnecting "faked TCP reset packets" from any other sources by using the BGP TTL Security.

Explain BGP Neighborhood relationships?

In BGP you are required to manually configure each neighbor in order to establish a neighborhood relationship. There are type of neighbors in BGP:

- **An internal BGP neighbor (iBGP neighbor)** is a neighbor that resides on the same AS as the local router. iBGP neighbors do not have to be directly connected.
- **An external BGP neighbor (eBGP neighbor) i**s a neighbor that is in an AS other than the local router. EBGP neighbors must be directly connected by-default.

Troubleshooting Commands and Tip

Show Commands -- With these commands, you should be able to troubleshoot 98% of the problems you will incur.

Show running-config (sh run)

Shows the running-configuration of the entire device or routing protocols, interfaces, vlans, basic configs, etc

Additional show run commands with pipe include show run | section shows an entire section eg sh run | section eigrp, show run interface shows the running-config of a specific interface eg sh run int f1/0

Show ip interface brief (sh ip int br) – Layer 3

Shows each interface on the device and its status o use to verify IP addresses and whether the interface is shutdown or open

Show vlan-switch (sh vlan-s) – Layer 2 – only useful on switches

Shows the vlans configured on switches and which vlan access ports are in use to verify vlan information is correct

Show interface trunk (sh int tr) – Layer 2 – only useful on switches

Shows the interfaces that are configured as trunks or use to verify proper interfaces are trunking

Show ip route (sh ip ro)(a.k.a. routing table) -- Layer 3

Shows routes that the device you are on has connectivity to o shows directly connected, static and dynamic routing protocol routes

Common Troubleshooting Scenarios

Q. **What do I check if my ping does not work**?

A. There are a few things to check. 99% of the time the problem is with the IP addresses. Use the sh ip int br command on both devices and see if they are correctly configured and are not shutdown. You can also do a sh run int command to check the subnet masks are correct.

If these are ok, see if the devices have a switch in between them. If they do, use the sh int status command to verify that the switch ports are configured correctly for access and/or the proper vlan is configured on the switch. Also use the sh int tr command to ensure that the proper ports are trunking and not shutdown.

If all of the above are correct, use the wr command to save the config of the switch in between them and reload it. The switches sometimes get stuck.

Q. **I don't see all the routes I'm expecting to see in my routing table.**

A. **First, verify if you have many routes missing or just one.**

Are the networks being advertised properly? Can you ping it? **NO PING = NO ROUTING PROTOCOL PROPOGATION.**

Configuring wrong IP addresses/subnet masks, ports being shutdown and misconfiguring vlan information are some of the most common mistakes you will make.

Key Point to Memorize

- **Memorize the basic configuration**
- **Memorize how to assign IP addresses on both router and PC**
- **Memorize how to configure DHCP on a router**
- **Memorize how to configure vlan on a switch**
- **Memorize how to configure trunk port and access port**
- **Memorize how to configure static and dynamic routes**
- **Memorize the show commands on Router and switches**