**BASIC ROUTER SECURITY CONFIG:**

**Set hostnames on Routers:**

En

Conf t

Hostname R1

**Set enable password ‘cisco’ on Routers:**

Enable password cisco

**View password in running config. Is it encrypted?**

En

\*enter password\*

Sh running-config

**Enable password encryption on Routers:**

En

Conf t

Service password-encrpytion

**View password in running config. Is it encrypted?**

Do sh run

…yes it is encrypted (7)...

**Disable password encryption on each router:**

En

Conf t

No service password-encryption

exit

**View password in running config. Is it encrypted?**

En

Sh running-config

**BASIC ROUTER SECURITY CONFIG PT. 2**

**Set hostnames:**

En

Conf t

Hostname R1

**Set enable password to ‘cisco’:**

En

Conf t

En password cisco

Do sh run

**Set enable secret to ‘ccna’:**

En

Conf t

Enable secret ccna

**To access privileged exec mode, what passwords are needed?**

Only password needed, not secret

**View running config. Which PW is encrypted?**

Secret is encrypted

**Enable password encryption and view running config. What has changed?**

En

Conf t

Service password-encryption

Do sh run

**Save config and reload router:**

En

Sh run

Sh start

Running-config startup-config

Write

**BASIC ROUTER SECURITY CONFIG PT. 3**

**Change hostname of Router 1 to R1:**

En

Conf t

Hostname R1

**Set enable secret of R1 to ‘cisco’:**

En

Conf t

Enable secret cisco

Set console password of R1 to ‘ccna’ and make it required to connect to R1 by console port:

En

Conf t

Line console 0

login

Password ccna

**Check running config:**

End

Exit

\*enter password\*

En

Sh cdp run

**Enable password encryption:**

En

Conf t

Service password encryption

**Save config:**

Copy run start

**BASIC SERIAL CONNECTION CONFIG**

**Use CDP to discover which interfaces are used to connect routers and switches:**

On all devices:

En

Show cdp neighbors

**Identify which end of serial cable attaching R1 and R2 is DCE and which is DTE:**

DCE devices provides clock signal..

On R1:

en

Sh controllers serial 0

**Set clock rate on DCE end to 64 kb/s:**

En

Conf t

Interface serial 0

Clock rate 64000

**Set IP addresses of serial interface of R1 and R2 to 192.168.0.1/24 and 192.168.0.2/24:**

En

Conf t

Ip address 192.168.0.1 255.255.255.0

R2:

En

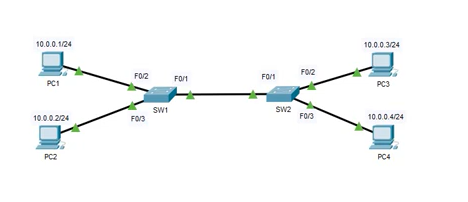
Conf t

Ip address 192.168.0.2 255.255.255.0

**Ping between routers to test connectivity:**

Ping 192.168.0.1 (ping R1 from R2)

**VLAN CONFIG:**

****

**Ping between computers to test connectivity:**

Ping addresses of each other PC from PC1

Ping \*ip address\*

**1196943755**

**Assign pc1 and pc3 to vlan1, and pc2 and pc4 to vlan2:**

On SW1:

En

Conf t

Interface fastethernet 0/2

Switchport mode access

Switchport access vlan 1

Int fastethernet 0/3

Switchport mode access

Switchport access vlan 2

Do sh int

On SW2:

En

Conf t

Interface fastethernet 0/2

Switchport mode access

Switchport mode access vlan 1

Interface fastethernet 0/3

Switchport mode access

Switchport access vlan 2

Dh sh int

**Attempt to ping between pc1 and pc3, and then pc2 and pc4. Why does PC1 -> PC3 work, but PC2 and PC4 not?**

We cannot ping because sw1 and sw2 are part of native vlan, vlan 1. So only traffic from vlan 1 can be passed on

**Configure interfaces connecting SW1 and SW2 as trunk interfaces: (to allow all traffic not just native traffic)**

On sw1:

En

Conf t

Interface fastethernet 0/1

Switchport mode trunk

On sw2:

Interface fastethernet 0/1

Switchport mode trunk

**Ping between computers. Which succeed/fail?**

**-**

**VLAN CONFIG: TRUNK ENCAPSULATION:**

****

**Ping between PCs to test connectivity:**

Ping \*ip address dest\*

**Assign pc2 and pc3 to vlan 2:**

On sw1:

En

Conf t

Int fastethernet 0/3

Switchport mode access

Switchport access vlan 2

On sw2:

En

Conf t

Int fasterthernet 0/2

Switchport mode access

Switchport access vlan 2

**Create a trunk between sw1 and sw2:**

On sw1:

En

Conf t

Interface fastethernet 0/1

Switchport mode trunk encapsulation dot1q

Switchport mode trunk

On sw2:

Int fasterthernet 0/1

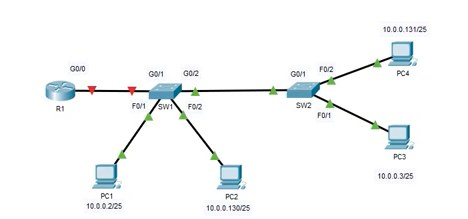
Switchport mode trunk encapsulation dot1q

Switchport mode trunk

**Ping between PCs to test connectivity:**

Pc1 is in native vlan so will not be about to comm with pc2 or pc3 but pc2 and pc3 should be able to communicate over trunk

**INTER-VLAN ROUTING (ROUTER ON A STICK):**

****

**Ping between PCs. which ones succeed?**

Only pings in same subnet work (10.0.0.2 and 10.0.0.3) for example

**Assign PC1 and PC# to VLAN 13, and PC2 to VLAN 24:**

On sw1:

En

Conf t

Interface f0/1

Switchport mode access

Switchport access vlan 13

Interface f0/2

Switchport mode access

Switchport access vlan 24

On sw2:

En

Conf t

Interface f0/1

Switchport mode access

Switchport access vlan 13

Interface f0/2

Switchport mode access

Switchport access vlan 24

**Creat trunk link between SW1 and SW2:**

To allow connection between sw1 and sw2 from multiple (same) vlans…

On SW1:

En

Conf t

Interface g0/2

Switchport mode trunk

On sw2:

En

Conf t

Interface g0/1

Switchport mode trunk

**Configure inter-vlan routing by using subinterfaces on R1s G0/0 interface. Use address 10.0.0.1/25 for vlan 13 and 10.0.0.129/25 for vlan 24:**

Pings to a diff vlan do not work… to make them…we need inter-vlan routing via ROAS:

On r1:

En

Conf t

Int g0/0

No shutdown

Interface g0/0.13 (subinterface config mode)

Encapsulation dot1q 13

Ip address 10.0.0.1 255.255.255.128

Int g0/0.24

Encapsulation dot1q 24

Ip address 10.0.0.129 255.255.255.128

Int g0/1

Switchport mode trunk

**Test connectivity via ping between PCs:**

Ping all pcs from 1

**LOCAL USERNAME/PASSWORD DATABASE:**



**Create the following users on R1:**

**Username: ccna / password: cisco (or secret to create encrypted password)**

**Username: ccnp / password CISCO**

R1:

En

Conf t

Username ccna password cisco

Username ccnp password CISCO

**Configure the console line to use the local user database to authenticate users:**

Line console 0

Login local

End

**Logout of the router, and login again with each account. Are the passwords case sensitive?**

Usernames are not case sensitive. Passwords are case sensitive.

**Create a third user on R1:**

**Username: CCNA / password: router**

En

Conf t

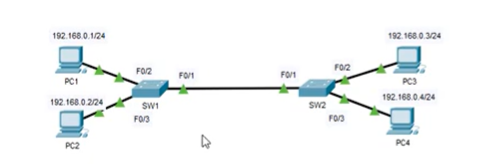
Username CCNA password router

**Login to the router with the CCNA account. Logout and login with ccna account. Which password do you use? Check the running-config to confirm:**

Do sh run

This did not add another user, but replaced current ccna user by changing password

**NAMING VLANS:**



**Set hostnames for switches to SW1 and SW2 respectively:**

En

Conf t

Hostname SW1

On switch 2:

en

Conf t

Hostname SW2

**Create 2 vlans on each switch, with the following names;**

**VLAN 13: Management**

**VLAN 24: Engineering**

Sw1:

En

Conf t

Sh run brief

Vlan 13

Sh vlan brief

Name Management

Vlan 24

Name Engineering

End

Sw2:

En

Conf t

Sh run brief

Vlan 13

Sh vlan brief

Name Management

Vlan 24

Name Engineering

End

**Place PC1 and PC3 into VLAN 13. And PC2 and PC4 into VLAN 24:**

SW1:

En

Conf t

Interface F0/2

Switchport access vlan 13  
Interface f0/3

Switchport access vlan 24

Do sh vlan br

SW2:

En

Conf t

Interface f0/2

Switchport access vlan 13

Interface f0/3

Switchport access vlan 24

Do sh vlan br

**Configure a trunk link between SW1 and SW2:**

En

Conf t

Int f0/1

Switchport mode trunk

End  
Sh interfaces trunk

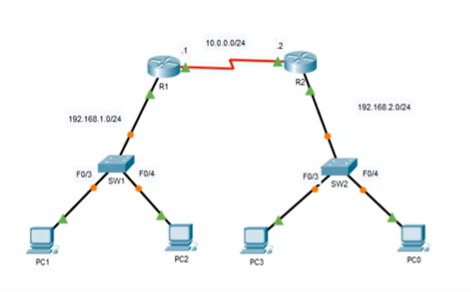
**Save running config of switches:**

write

**Test all PCs in same VLAN can ping each other:**

Ping IPs in same vlan

**CDP (CISCO DISCOVERY PROTOCOL):**

****

**Use cdp to identify which interfaces are used to connect the routers and switches:**

On sw1/any router or switch:

En

Sh cdp neighbors

(Only router and switch neighbours will be shown)

**Determine which side of the serial connection between R1 and R2 is DCE, and which is DTE. Set a clock rate of 64 kb/s on the DCE side:**

On r1:

En

Sh controllers s2/0

Conf t

Interface s2/0

Clock rate 64000

**What are the default CDP send and hold timers? Confirm this with a show command on one of the devices:**

On r1:

En

Sh cdp interface

**Disable CDP globally on R1 and attempt to view CDP neighbors:**

On r1:

En

Conf t

No cdp run

Do sh cdp neighbor

**Enable CDP globally on R1 and immediately view CDP neighbors again. Do SW1 and R2 appear instantly?**

On r1:

En

Conf t

Cdp run

Do sh cdp neighbor

(cdp send time is 60 secs, can take time for neighbours to reappear)

**Disable CDP on the switch interfaces connected to PCs:**

On sw:

En

Conf t

Interface range f03 - 4

No cdp enable

**CDP (CISCO DISCOVERY PROTOCOL) PT. 2**

****

**Use CDP to identify which interfaces are used to connect the routers and switches:**

On device

Ewn

Sh cdp neighbors

**Use CDP to identify the routers/switch model of neighbouring devices from each device:**

En

Sh cdp neighbor detail

Or

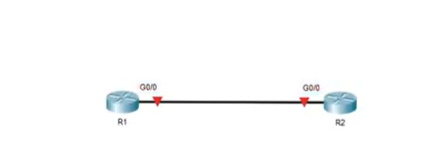
Sh cdp entry (device name) sw1

**Use CDP to identify the IOS version of neighbouring devices from each device:**

En

Sh version

**LOOPBACK INTERFACE CONFIG:**

****

**Set the IP addresses of physical interfaces connecting the two routers as follows, and enable them:**

**R1: 192.168.1.1/24**

**R2: 192.168.1.2/24**

On router 1:

En

Conf t

Interface g0/0

Ip address 192.168.1.1 255.255.255.0

No shutdown

On router 2:

En

Conf t

Interface g0/0

Ip address 192.168.1.2 255.255.255.0

No shutdown

**Create a loopback interface on each router:**

**R1: 1.1.1.1/32**

**R2: 2.2.2.2/32**

On router 1:

En

Conf t

Int loopback 0

Ip address 1.1.1.1 255.255.255.255

On router 2:

En

Conf t

Int loopback 0

Ip address 2.2.2.2 255.255.255.255

**From each router, attempt to ping both the local loopback interface and the loopback interface of the remote router:**

ping…

**Remove the loopback interface of each router:**

On router:

En

Conf t

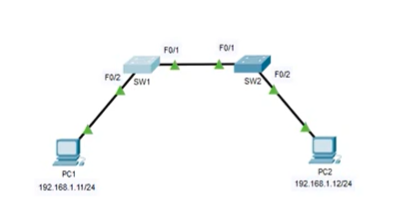
Do sh ip int br

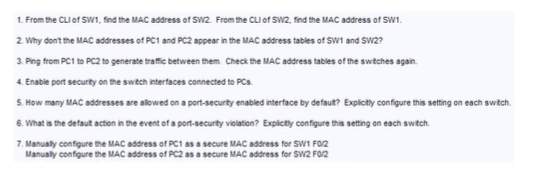
Conf t

No int loopback 0

Do sh int br

**PORT SECURITY:**

****



1. On sw1

En

Sh mac address-table

1. -
2. -
3. On sw1, switchport sec can only be used on access ports…

En

Conf t

Switchport mode access

Switchport port-security

1. On sw

En

Sh port-security

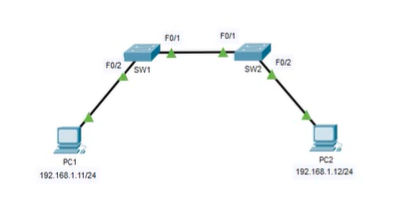
Switchport port-security maximum 1

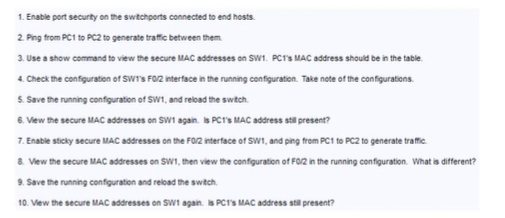
1. On sw

Switchport port-security violation ?

Switchport port-security violation (protect/restrict/shutdown)

**PORT SECURITY PT. 2:**

****



1. On sw1

En

Conf t

Interface f0/2

Switchport mode access

Switchport port-security

1. Ping…
2. On sw1

En

Sh port-security address

1. On sw1

En

Sh running-config

1. On sw1

En

Write

Reload

1. On sw1

En

Sh port-security address

1. On sw1

En

Conf t

Inter f0/2

Switchport port-security mac-address sticky

Ping…

1. On sw1

En

Sh port-security address

Sh run

Sticky addresses are saved to the running-config of the switch

1. On sw1

Write

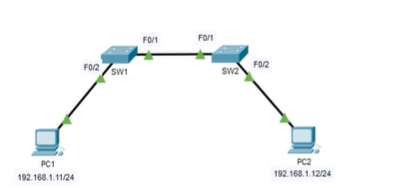
Reload

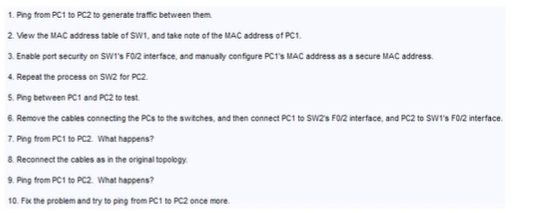
1. On sw1

En

Sh port-security address

**PORT SECURITY PT. 3:**

****

****

1. Ping…
2. On sw1

En

Sh mac address-table

1. On sw1

En

Conf t

Int f0/2

Switchport

mode access

Switchport port-security

Switchport port-security mac-address (address of pc1 paste here)

1. Repeat on sw2 for pc2:

En

Conf t

Int f0/2

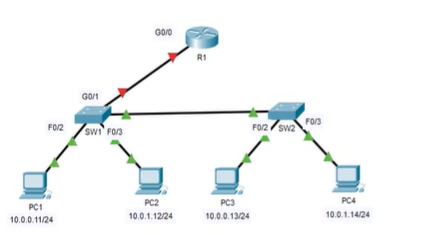
Switchport mode access

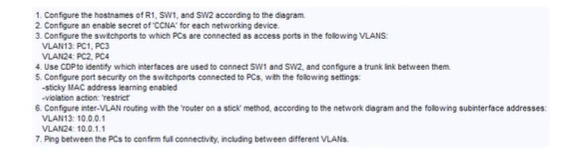
Switchport port-security

Switchport port-security mac-address (address of pc2)

1. Ping
2. -
3. Ping
4. -
5. Ping
6. Shutdown, no shutdown

**REVIEW CONFIGURATION LAB 1:**





1. On r1

En

Conf t

Hostname R1

On sw1:

En

Conf t

Hostname SW1

On sw2:

En

Conf t

Hostname SW2

1. On sw2

En

Conf t

Enable secret CCNA

On sw1:

En

Conf t

Enable secret CCNA

On R1:

En

Conf t

Enable secret CCNA

1. On sw1:

En

Conf t

Interface f0/2

Switchport mode access

Switchport access vlan 13

Int f0/3

Switchport mode access

Switchport access vlan 24

On sw2:

En

Conf t

Int f0/2

Switchport mode access

Switchport mode access vlan 13

Int f0/3

Switchport mode access

Switchport mode access vlan 24

1. On sw2:

Do sh cdp neighbours… to find which int is connecting switches

En

Conf t

Int f0/1

Switchport mode trunk

On sw1:

En

Conf t

Int f0/1

Switchport mode trunk

1. On sw1

En

Conf t

Int range f0/2 - 3

Switchport port-security

Switchport port-security mac-address sticky

Switchport port-security violation restrict

On sw2:

En

Conf t

Int range f0/2 - 3

Switchport port-security

Switchport port-security mac-address sticky

Switchport port-security violation restrict

1. Sw 1:

Int g0/1

Switchport mode trunk

On r1:

En

Conf t

Int g0/0

No shutdown

Int g0/0.13

Encapsulation dot1q 13

Ip address 10.0.0.1 255.255.255.0

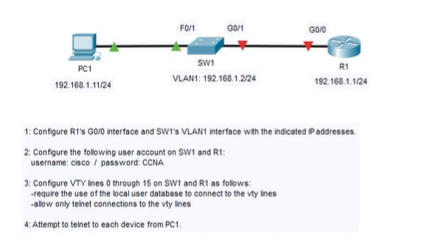
Int g0/0.24

Encapsulation Dot1q 24

Iup address 10.0.1.1 255.255.255.0

1. Ping

**TELNET / VTY LINES:**

****

1. On sw1

En

Conf t

Int vlan 1

Ip address 192.168.1.2 255.255.255.0

On r1:

En

Conf t

Int g0/0

Ip address 192.168.1.1 255.255.255.0

No shutdown (router int admin down by default)

1. On r1:

En

Conf t

Username cisco password CCNA

On sw1:

En

Conf t

Username cisco password CCNA

1. Vty = virtual tele type (usually 0 - 4 and 5 - 15)

On sw1:

Vty 0 15

Login local

Transport input ? (all, none, ssh, telnet)

Transport input telnet

On r1:

Line vty 0 15

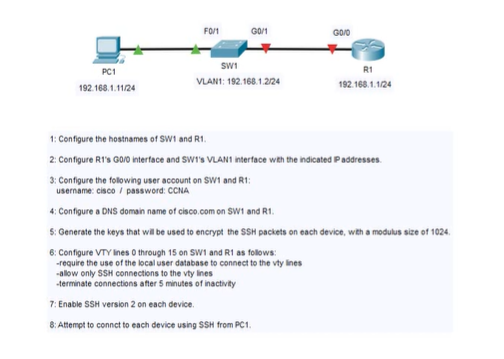
Login local

Transport input telnet

Do sh run

1. Ping

**SSH / VTY LINES:**

****

1. On sw1

En

Conf t

Hostname SW1

On r1:

En

Conf t

Hostname R1

1. On r1:

En

Conf t

Int g0/0

Ip address 192.168.1.1 255.255.255.0

No shutdown

On sw1:

En

Conf t

Int vlan 1

Ip add 192.168.1.2 255.255.255.0

No shutdown

1. Sw1:

En

Conf t

Username Cisco password CCNA

On r1:

En

Conf t

Username cisco password CCNA

1. On r1:

En

Conf t

Ip domain-name cisco.com

On sw1:

En

Conf t

Ip domain-name cisco.com

1. On sw1:

Crypto key generate rsa

1024

On r1:

En

Conf t

Crypto key generate rsa

1024

1. On r1:

En

Conf t

Line vty 0 15

Login local

Transport input ssh

Exec-timeout 5 (minutes)

On sw1:

En

Conf t

Line vty 0 15

Login local

Transport input ssh

Exec-timeout 5

1. On sw1

En

Conf t

Ip ssh version 2

On r1:

En

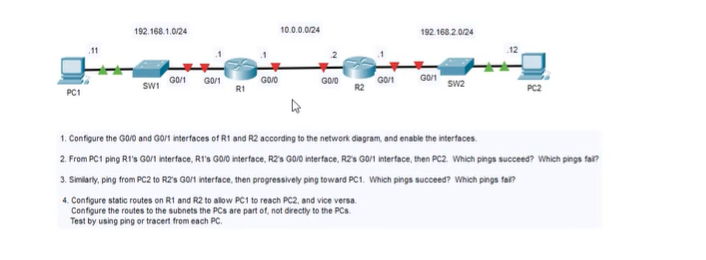
Conf t

Ip ssh version 2

1. Ping over input…

On pc1: ssh-l cisco (username configured) (ip address)

**STATIC ROUTING:**

****

1. On r1:

En

Conf t

Int g0/0

Ip address 10.0.0.1 255.255.255.0

No shutdown

Int g0/1

Ip address 192.168.1.1 255.255.255.0

No shutdown

On r2:

En

Conf t

Int g0/0

Ip address 10.0.0.2 255.255.255.0

No shutdown

Int g0/1

Ip address 192.168.2.1 255.255.25.0

No shutdown

1. Ping
2. Ping
3. On r1:

En

Conf t

Ip route 192.168.2.0 255.255.255.0 10.0.0.2

Do sh ip route

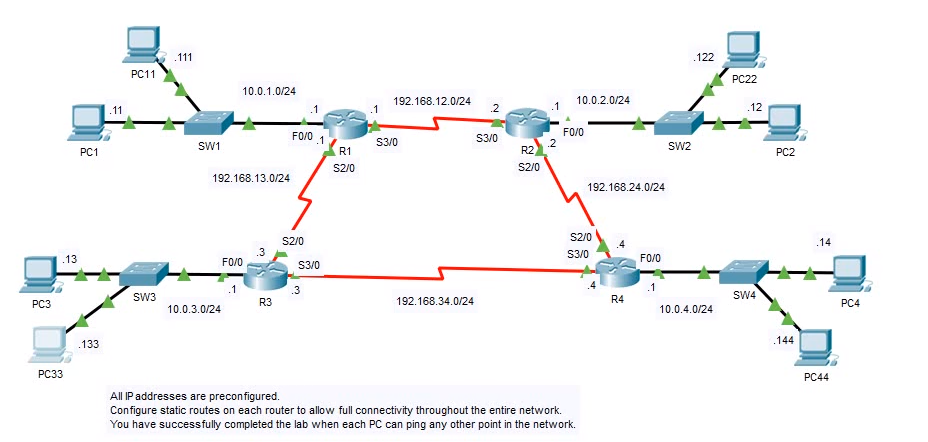
On r2:

En

Conf t

Ip route 192.168.1.0 255.255.255.0 g0/0

**STATIC ROUTING PT. 2:**

****

**On r1:**

En

Conf t

Ip route 192.168.24.0 255.255.255.0 192.168.12.2

Ip route 192.168.34.0 255.255.255.0 192.168.13.3

Ip route 10.0.3.0 255.255.255.0 192.168.13.3

Ip route 10.0.2.0 255.255.255.0 192.168.12.2

Ip route 10.0.4.0 255.255.255.0 192.168.12.2

On r2:

En

Conf t

Ip route 192.168.13.0 255.255.255.0 192.168.12.1

Ip route 192.168.34.0 255.255.255.0 192.162.24.4

Ip route 10.0.1.0 255.255.255.0 192.168.12.1

Ip route 10.0.3.0 255.255.255.0 192.192.168.12.1

Ip route 10.0.4.0 255.255.255.0 192.168.24.4

On r3:

Ip route 192.168.12.0 255.255.255.0 192.168.13.1  
Ip route 192.168.24.0 255.255.255.0 192.168.34.4

Ip route 10.0.1.0 255.255.255.0 192.168.13.1

Ip route 10.0.4.0 255.255.255.0 192.168.34.4

Ip route 10.0.2.0 255.255.255.0 192.168.13.1

On r4:

Ip route 192.168.12.0 255.255.255.0 192.168.24.2

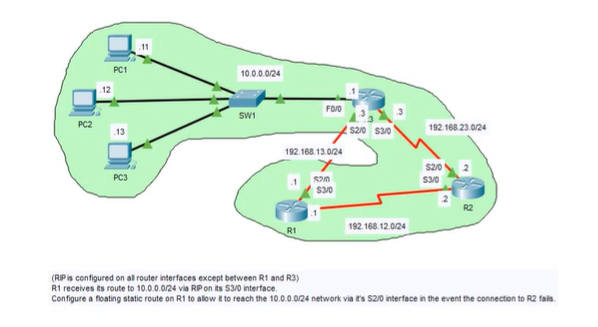
Ip route 192.168.13.0 255.255.255.0 192.168.34.3

Ip route 10.0.2.0 255.255.255.0 192.168.24.2

Ip route 10.0.3.0 255.255.255.0 192.168.34.3

Ip route 10.0.1.0 255.255.255.0 192.168.34.3

**STATIC ROUTING PT. 3:**



On r1:

En

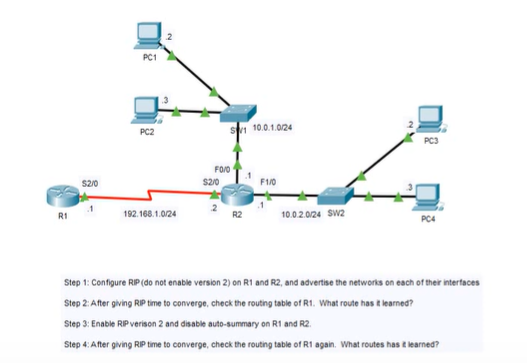
Conf t

Ip route 10.0.0.0 255.255.255.0 192.168.13.3 (add 121 to end to add an AD value higher than RIP… meaning this will only kick in if RIP goes down)

Do sh ip route

Floating static route = route only added into table when regular route not available, such as when interface goes down

**RIP PT. 1:**



1. On r1:

En

Conf t

Router rip

Network 192.168.1.0

On r2:

En

Conf t

Router rip

Network 192.168.1.0

Network 10.0.0.0 (this will include 10.0.1.0 and 10.0.2.0 networks)

On r1:

Do sh ip route

3. On r1:

En

Conf t

Version 2

No auto-summary

On r2:

En

Conf t

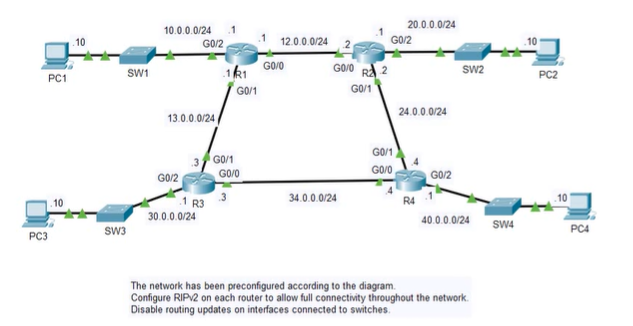
Version 2

No auto-summary

On r1:

Do sh ip route

**RIP PT. 2:**

****

On r1:

En

Conf t

Router rip

Version 2

No auto-summary

Net 10.0.0.0

Net 12.0.0.0

Net 13.0.0.0

passive -interface g0/2

On r2:

En

Conf t

Router rip

Version 2

No auto-summary

Net 20.0.0.0

Net 12.0.0.0

Net 24.0.0.0

Passive interface g0/2

On r3:

En

Conf t

Router rip

Version 2

No auto-summary

Net 30.0.0.0

Net 13.0.0.0

Net 34.0.0.0

Passive-interface g0/2

On r4:

En

Conf t

Router rip

Version 2

No auto-summary

Net 40.0.0.0

Net 24.0.0.0

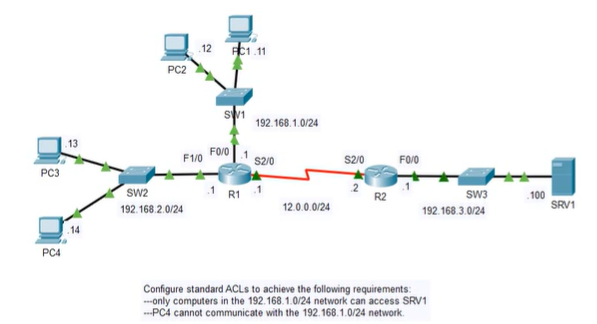
Net 34.0.0.0

passive -interface g0/2

End

Sh ip protocols

**STANDARD ACLs:**

****

Standard acls control only base on source address

Extended can control on source and destination address

On r2 (we go here as it is closest to destination - srv1):

En

Conf t

Access-list 1 permit 192.168.1.0 0.0.0.255

Do sh access-list

Int f0/0

Ip access-group 1 out (we are filtering traffic going out to srv1)

Ping server

1. On r1:

En

Conf t

Access-list 1 deny host 192.168.2.14

Access-list 1 permit any (naturally, acl will deny all traffic, have to turn it off with this cmd)

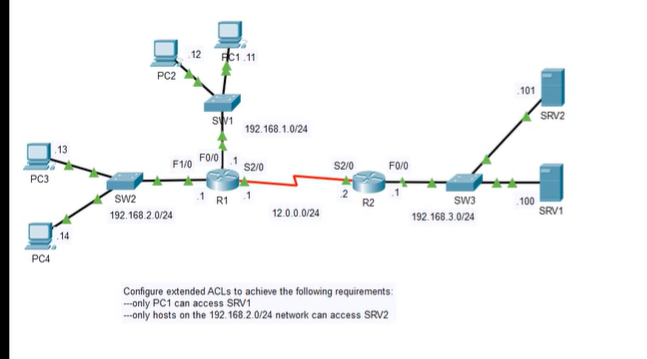
Do sh access-list

Int f0/0 (closest to destination)

Ip access-group 1 out

Ping

**EXTENDED ACLs:**



Extended ACLs must be applied closest to source…

On r1:

En

Conf t

Access-list 100 permit ip host 192.168.1.11 host 192.168.3.100

Access-list 100 deny ip any host 192.168.3.100

2. On r1:

Access-list 100 permit ip 192.168.2.0 0.0.0.255 host 192.168.3.101 (srv2)

Access-list 100 deny ip any host 192.168.3.101

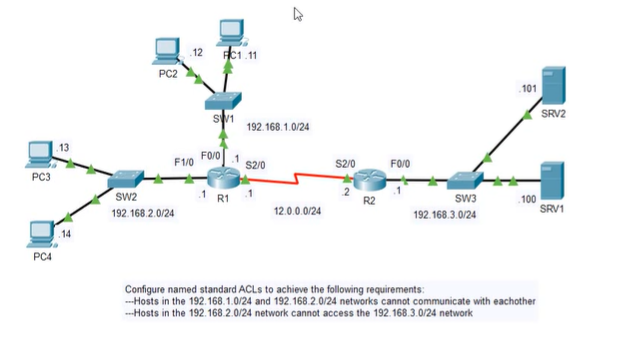
Access-list 100 permit ip any any (implicit deny on all other traffic, must remove with this)

Int s2/0

Ip access-group 100 out

ping

**NAMED ACLs:**

****

1. On r1:

En

Conf t

Ip access-list standard 2to1

Deny 192.168.2.0 0.0.0.255

Permit any

Exit

Ip access-list standard 1to2

Deny 192.168.1.0 0.0.0.255

Permit any

Exit

Int f0/0

Ip access-group 2to1 out

Int f1/0

Ip access-group 1to2 out

Ping

1. On r2:

En

Conf t

Ip access-list standard 2to3

Deny 192.168.2.0 0.0.0.255

Permit any

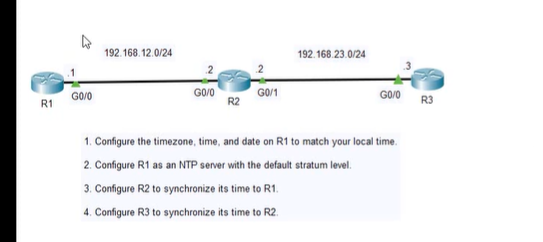
Exit

Int f0/0

Ip access-group 2to3 out

ping

**NTP (NETWORK TIME PROTOCOL):**

****

1. ON R1:

En

Sh clock

Sh clock detail

Conf t

Clock timezone <timeone> <hours offset UTC> <minutes offset>

Do sh clock

Exit

Clock set

Clock set <current time> <day> <month> <year>

To configure R1 as ntp server….

Ntp master <stratum number> 8

On r2:

En

Sh clock

Conf t

Clock timezone <timezone> <stratum above master> 9

Ntp server 192.168.12.1

Exit

After some time…

Sh clock detail

Sh ntp associations

On r3:

En

Conf t

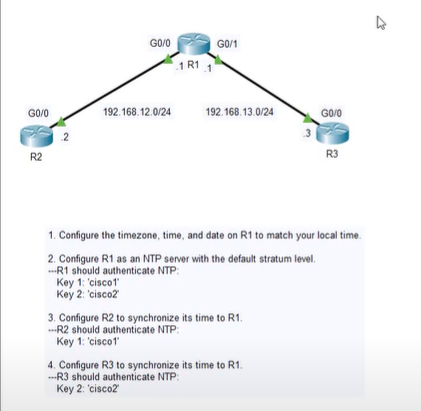
Clock timezone <timezone> <stratum above master> 9

Ntp server 192.168.23.2

Exit

Sh ntp associations

**NTP PT. 2:**

****

1. ON R1:

En

Clock set 12:00:00 aug 2019

Conf t

Clock timezone <timezone> <stratum> \*JST 9\*

Ntp master

Ntp authenticate

Ntp authentication-key 1 md5 cisco1

Ntp authentication-key 2 md5 cisco2

Ntp trusted-key 1

Ntp trusted-key 2

1. On r2:

En

Conf t

Click timezone JST 9

Ntp authenticate

Ntp authentication-key 1 md5 cisco1

Ntp trusted-key 1

Ntp server 192.168.12.1 key 1

1. On r3:

En

Conf t

Clock timezone JST 9

Ntp authenticate

Ntp authentication-key 2 md5 cisco2

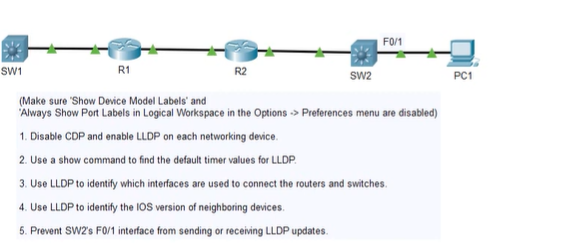
Ntp trusted-key 2

Ntp server 192.168.13.1 key 2

Sh clock detail

Sh ntp associations

**LLDP (Link Layer Discovery Protocol):**



1. On sw1:

En

Conf t

No cdp run

Lldp run

On r1:

En

Conf t

No cdp run

Lldp run

On r2:

En

Conf t

No cdp run

Lldp run

On sw2:

En

Conf t

Np cdp run

Lldp run

1. On sw1:

En

Sh lldp

1. On sw1

Sh lldp neighbours

Repeat on r1 and r2 and sw2

1. On all network devices

Sh lldp neighbors detail

1. On sw2

En

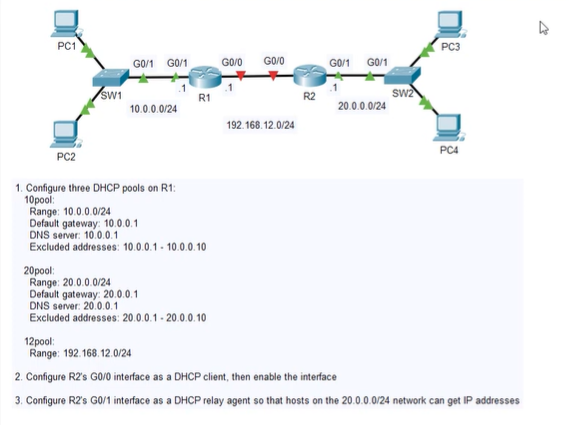
Conf t

Int f0/1

No lldp receive

No lldp transmit

**DHCP (Dynamic Host COnfig. Protocol):**

****

1. On r1

En

Conf t

Ip dhcp pool 10pool

Network 10.0.0.0 255.255.255.0

Default-router 10.0.0.1

Dns-server 10.0.0.1

Exit

Ip dhcp excluded-address 10.0.0.1 10.0.0.10

Ip dhcp pool 20pool

Network 20.0.0.0 255.255.255.0

Default-router 20.0.0.1

Dns-server 20.0.0.1

Exit

Ip dhcp excluded-address 20.0.0.1 20.0.0.10

Ip dhcp pool 12pool

Network 192.168.12.0 255.255.255.0

Exit

1. On r2:

En

Conf t

Int g0/0

Ip address dhcp

No shut

1. On r2:

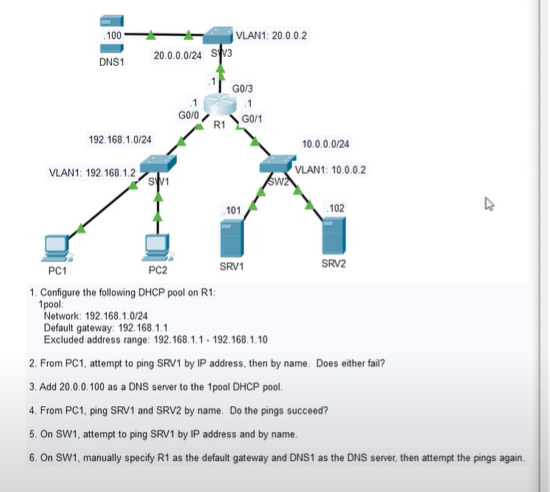
En

Conf t

Int g0/1

Ip helper-address 192.168.12.1

**DNS (DOMAIN NAME SERVER):**

****

1. On r1:

En

Conf t

Ip dhcp excluded-address 192.168.1.1 192.168.1.10

Ip dhcp pool 1pool

Network 192.168.1.0 255.255.255.0

Default-router 192.168.1.1

Dns-server 20.0.0.100

On pc1:

ipconfig /release

Ipconfig /renew

Ping

1. -
2. -
3. -
4. -
5. On sw 1:

En

Conf t

Ip default-gateway 192.168.1.1

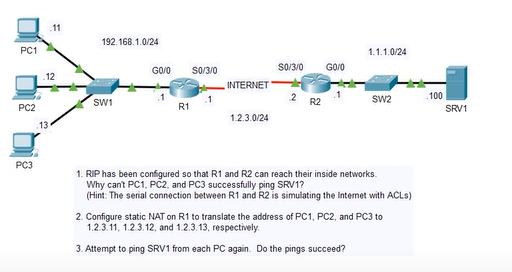
Ip name-server 20.0.0.100

Exit

Ping 10.0.0.101

Ping srv1

**STATIC NAT:**

****

1. -
2. On r1:

En

Conf t

Int g0/0

Ip nat inside

Int s0/3/0

Ip nat outside

Exit

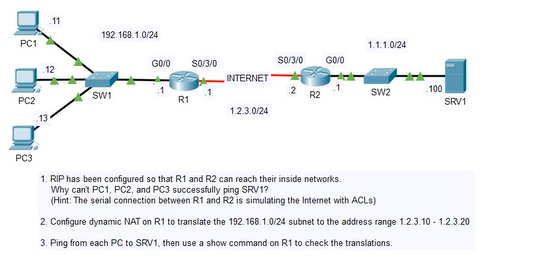
Ip nat inside source static 192.168.1.11 1.2.3.11

Ip nat inside source static 192.168.1.12 1.2.3.12

Ip nat inside source static 192.168.1.13 1.2.3.13

1. Ping

**DYNAMIC NAT (NETWORK ADDRESS TRANSLATION):**

****

1. -
2. On r1:

En

Conf t

Int g0/0

Ip nat inside

Int s0/3/0

Ip nat outside

Exit

Access-list 1 permit 192.168.1.0 0.0.0.255

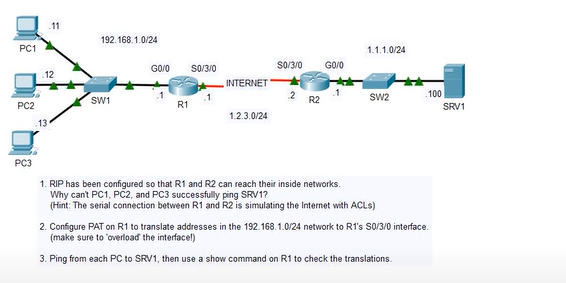
Ip nat pool pool1 1.2.3.10 1.2.3.20 netmask 255.255.255.0

Ip nat inside source list 1 pool1

Sh ip nat translations

Clear ip nat translation \*

**PAT (PORT ADDRESS TRANSLATION):**

****

2. On r1:

En

Conf t

Int g0/0

Ip nat inside

Int s0/3/0

Ip nat outside

Exit

Access-list 1 permit 192.168.1.0 0.0.0.255

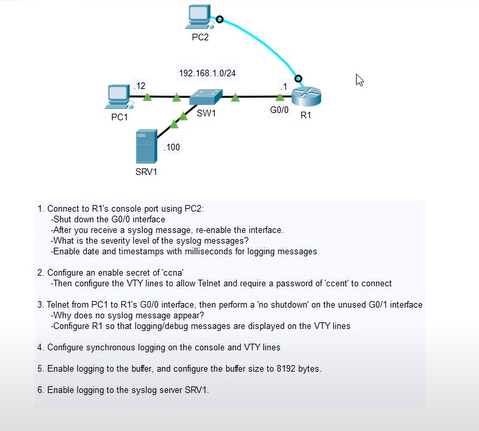
Ip nat inside source list 1 interface s0/3/0 overload (overload allows router to translate multiple hosts)

1. Ping

Sh ip nat translations

Clear ip nat translation \*

**SYSLOG:**

****

1. On r1:

En

Conf t

Int g0/0

Shutdown

No shutdown

(LINK-<number>) represent syslog severity level

Exit

Service timestamps log datetime msec

1. On r1:

En

Conf t

En secret ccna

Line vty 0 15

Password ccent

Login

Transport input telnet

1. On PC1:

<telnet <ip>>

Password <enter>

On r1:

Int g0/1

No shutdown

End

Terminal monitor (enables syslog messages to vty lines)

Conf t

Int g0/1

Shutdown

1. **On r1:**

**To enable synchronous logging so that errors don't show up in middle of lines, but on new line:**

Line con 0

Logging synchronous

Line vty 0 15

Logging synchronous

1. On r1:

En

Sh logging

Conf t

Logging buffered

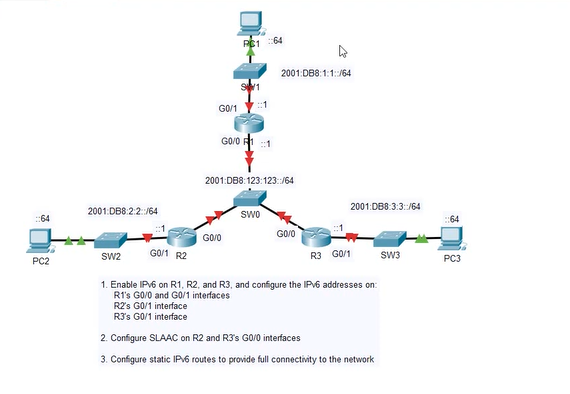
Do sh logging

Logging buffered 8192

5. On r1:

Logging 192.168.1.100

**IPv6**

****

1. On r1:

En

Conf t

Ipv6 unicast-routing

Int g0/0

Ipv6 add 2001:db8123:123::1/64

No shut

Int g0/1

Ipv6 add 2001:db8:1:1::/64

No shut

Exit

Do sh ip int br

On r2:

En

Conf t

Int g0/1

Ipv6 add 2001:db8:2:2::1/64

No shut

On r3:

En

Conf t

Int g0/1

Ipv6 add 2001:db8:3:3::1/64

Not shut

1. On r3:

En

Conf t

Int g0/0

No shut

Ipv6 add auto

On r2:

En

Conf t

Int g0/0

No shut

Ipv6 add auto

1. On r1:

Ipv6 route 2001:db8:3:3::/64 <paste R2’s address>

IPv6 route 2001:db8:2:2::/64 <paste R3’s route>

On r3:

Ipv6 route 2001:db8:2:2::/64 v<paste R2’s address>

Ipv6 route 2001:db8:1:1::/64 2001:db8:123:123::1

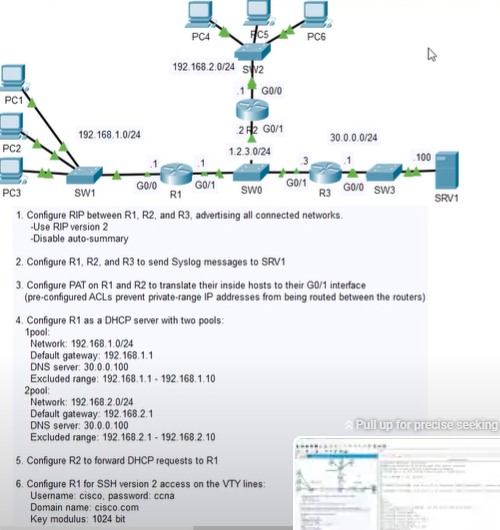
On r2:

Ipv6 route 2001:db8:3:3::/64 <past r3’s address>

Ipv6 route 2001:db8:1:1::/64 2001:db8:123:123::1

Ping…

**REVIEW CONFIG LAB 2:**

****

1. On r1:

En

Conf t

Router rip

Network 1.2.3.0

Network 192.168.1.0

Version 2

No auto-summary

On r2:

En

Conf t

Router rip

Version 2

No auto-summary

Network 1.2.3.0

Network 192.168.2.0

On r3:

En

Conf t

Router rip

Version 2

No auto-summary

Network 30.0.0.0

Network 1.2.3.0

Do sh ip rip database

1. On r1, r2 and r3:

Logging host 30.0.0.10-0

1. On r1:

En

Conf t

Int g0/0

Ip nat inside

Int g0/1

Ip nat outside

Exit

Access-list 1 permit 192.168.1.0 0.0.0.255

Ip nat inside source list 1 interface g0/1 overload

On r2:

En

Conf t

Int g0/0

Ip nat inside

Int g0/1

Ip nat outside

Exit

Access-list 1 permit 192.168.2.0 0.0.0.255

Ip nat inside source list 1 interface g0/1 overload

1. On r1:

Ip dhcp excluded-address 192.168.1.1 192.168.1.10

Ip dhcp excluded-address 192.168.2.1 192.168.2.10

Ip dhcp pool 1pool

Network 192.168.1.0 255.255.255.0

Default-router 192.168.1.1

Dns-server 30.0.0.100

Exit

Ip dhcp pool 2pool

Network 192.168.2.0 255.255.255.0

Default-router 192.168.2.1

Dns-server 30.0.0.100

Exit

On pc4:

Ipconfig /release

Ipconfig /renew

Failed

Must config r2 as relay agent

On r2:

En

Conf t

Int g0/0

Ip helper-address 1.2.3.1

6. On r1:

Hostname R1

Ip domain-name cicso.com

Username cisco password ccna

Crypto key generate rsa

Modulus size: 1024

Line vty 0 15

Login local

Transport input ssh

Exit

Ip ssh version 2

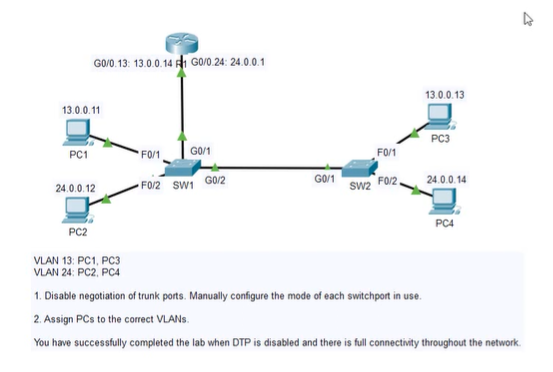
\*try to ssh from r1 to pc1\*

N pc1:

Ssh -l cisco 192.168.1.1

Password: cisco

**DTP / VLANS:**

****

1. On sw1:

En

Sh int g0/2 switchport

Conf t

Switchport nonegotiate

Switchport mode trunk

Int g0/1

Switchport mode trunk

Switchport nonegotiate

In range f0/1 - 2

Switchport mode access

Switchport no negotiate

Int f0/1

Switchport access vlan 13

In f0/2

Switchport access vlan 24

On sw2:

En

Conf t

Int g0/1

Switchport mode trunk

Switchport nonegotiate

Int range f0/1 - 2

Switchport mode access

Switchport nonegotiate

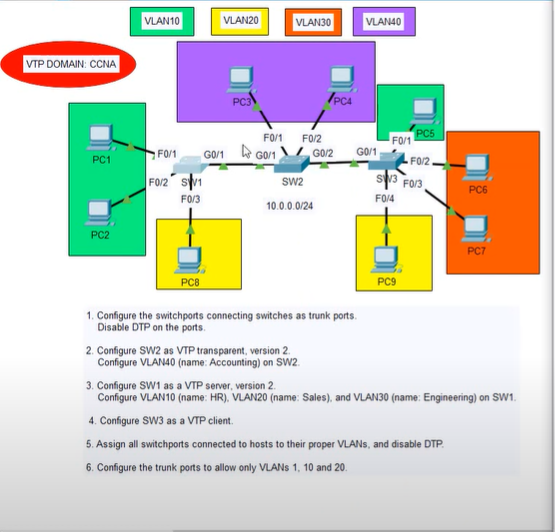
Int f0/1

Switchport access vlan 13

Int f0/2

Switchport access vlan 24

**VTP (VLAN TRUNKING PROTOCOL):**



1. On sw1:

En

Conf t

Int g0/1

Switchport mode trunk

Switchport nonegotiate

Exit

On sw2:

En

Conf t

Int range g0/1 - 2

Switchport mode trunk

Switchport nonegotiate

On sw3:

En

Conf t

Int g0/1

Switchport mode trunk

Switchport nonegotiate

1. On sw2

En

Conf t

Vtp mode transparent

Vtp domain CCNA

Vtp version 2

Vlan 40

Name Accounting

Do sh vlan br

1. On sw1

En conf t

Vtp domain CCNA

Vtp version 2

Vtp mode server

Vlan 10

Name HR

Vlan 20

Name Sales

Vlan 30

Name Engineering

Exit

1. On sw3:

Vtp mode client

Do sh vtp status

1. On sw3:

Int f0/1

Switchport mode access  
Switchport access vlan 10

Switchport nonegotiate

Int range f0/2 - 3

Switchport mode access

Switchport access vlan 30

Switchport nonegotiate

Int f0/4

Switchport mode access

Switchport access vlan 20

Switchpoort nonegoaite

On sw2:

Int range f0/1 - 2

Switchport mode access

Switchport access vlan 40

Switchport nonegotiate

On sw1:

Int range f0/1-2

Switchport mode access

Switchport access vlan 10

Switchport nonegotiate

Int f0/3

Switchport mode access

Switchport access vlan 20

Swithcport noneogtiate

1. On sw1:

Int g0/1 switchport trunk allowed vlan 1,10, 20

Do sh int trunk

On sw2:

Int range g0/1 - 2

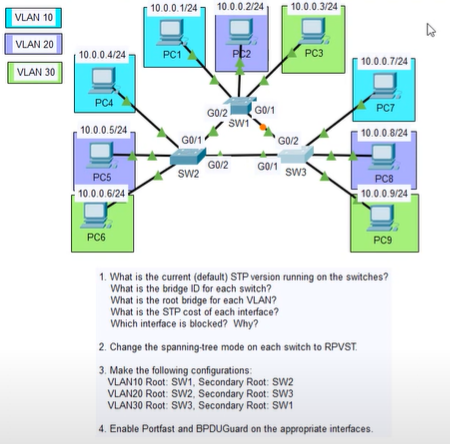
Switchport trunk allowed vlan 1,10,20

On sw3:

Int g0/1

Switchport trunk allowed vlan 1,10,20

**STP (SPANNING TREE PROTOCOL):**

****

1. ON SW1:

En

Sh spanning-tree summary

\*find stp version\*

To find bridge id:

Sh spanning tree

\*lowest is root bridge\*

Port blocked on g0/1 sw1 as its id is higher

1. On all switches:

En

Conf t

Spanning-tree mode rapid-pvst

1. On sw1:

Spanning-tree vlan 10 root primary

Spanning-tree vlan 20 root secondary

On sw2:

Spanning-tree vlan 20 root primary

Spanning-tree vlan 10 root secondary

On sw3:

Spanning-tree vlan 30 root primary

Spanning-tree vlan 20 root secondary

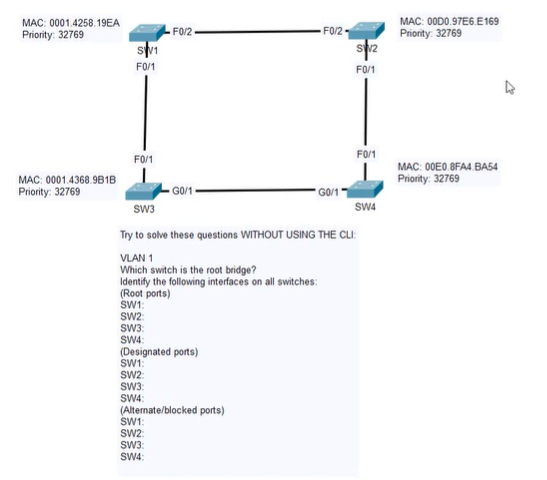
1. On all sw:

Int range f0/1 - 3

Spanning-tree portfast

Spanning-tree bpduguard enable

**STP ELECTION:**

****

**SW1 = ROOT BRIDGE**

**ROOT PORTS:**

**SW1: -**

**SW2: F0/2**

**SW3: F0/1**

**SW4: G0/1**

**DESIGNATED PORTS:**

**SW1: F0/1 F0/2**

**SW2: -**

**SW3: G0/1**

**SW4: F0/1**

**ALTERNATE/BLOCKING PORTS:**

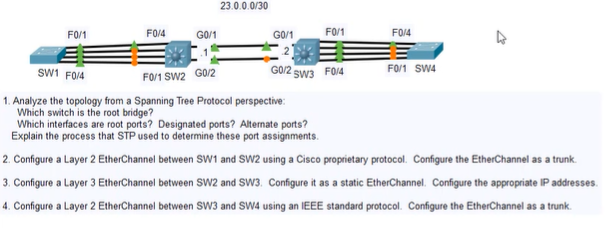
**SW1:**

**SW2:**

**SW3:**

**SW4: f0/1 (HIGHER COST TO ROOT BRIDGE)**

**ETHERCHANNEL:**

****

1. Root bridge = sw1 as all ports green/forwarding

Interfaces closest to root bridge are root ports

Block ports are those furthest from root bridge (highest cost)

1. On sw1:

En

Conf t

Int range f0/1 - 4

Channel-group 1 mode desirable

Do sh etherchannel summary

Int port-channel 1

Switchport mode trunk

On sw2:

En

Conf t

Int range f0/1 - 4

Shutdown

Channel-group 2 mode auto

Int po2 (portchannel 2)

Switchport trunk encapsulation dot1q

Switchport mode trunk

Int range f0/1 - 4

No shutdown

Do sh etherchannel summary

1. On sw2:

En

Conf t

Ip routing

Int range g0/1 - 2

No switchport

Channel-group 1 mode on

Int po1

Ip address 23.0.0.1 255.255.255.0

On sw3:

En

Conf t

Ip routing

Int range g0/1 - 2

No switchport

Channel-group mode 1

Ip address 23.0.0.2 255.255.255.0

Do sh eth summary

Do ping 23.0.0.1

1. On sw3:

En

Conf t

Int range f0/1 - 4

Channel-group mode active

Int po2

Switchport trunk encapsulation dot1q

Switchport mode trunk

On sw4:

En

Conf t

Int range f0/1 - 4

Shutdown

Channel-group 1 mode active

Int po1

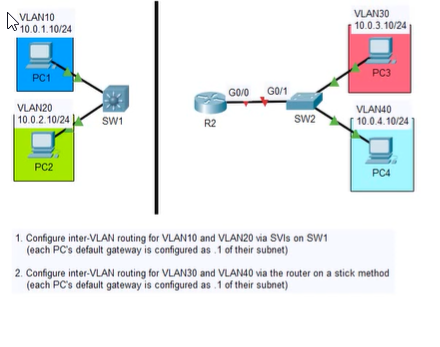
Switchport mode trunk

Int range f0/1 - 4

No shutdown

Do sh etherchannel summary

**INTERVLAN ROUTING (SVI, ROUTER ON A STICK):**



1. On sw1:

En

Conf t

Ip routing

Int vlan 10

Ip address 10.0.1.1 255.255.255.0

No shutdown

Int vlan 20

Ip address 10.0.2.1 255.255.255.0

No shutdown

Do sh vlan br

1. On sw2:

En

Conf t

Int g0/1

Switchport mode trunk

On r2:

En

Conf t

Int g0/0

No shutdown

Int g0/0.30

Encapsulation dot1q 30

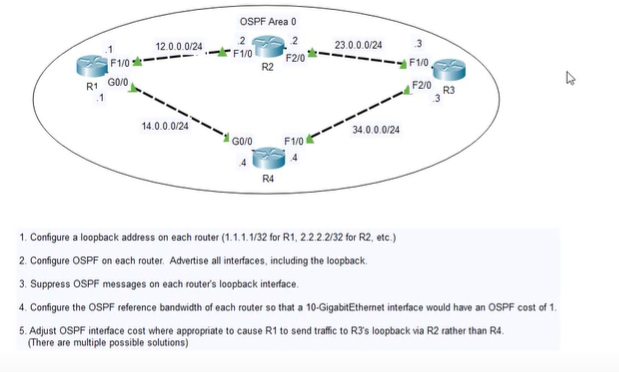
Ip address 10.0.3.1 255.255.255.0

Int g0/0.40

Encapsulation dot1q 40

Ip address 10.0.4.1 255.255.255.0

**OSPF (SINGLE AREA):**

****

1. On r1:

En

Conf t

Int L0

Ip address 1.1.1.1 255.255.255.255

Exit

On r2:

En

Conf t

Int L0

Ip address 2.2.2.2 255.255.255.255

On r3:

En

Conf t

Int L0

Ip address 3.3.3.3 255.255.255.255

On r4:

En

Conf t

Int L0

Ip address 4.4.4.4 255.255.255.255

1. On r1:

Router OSPF <router id> 1

Network 12.0.0.0 0.255.255.255 area 0

Network 14.0.0.0 0.0.255.255 area 0

Network 1.1.1.1 0.0.0.0.0 area 0

On r2:

Router ospf <process id> 2

Network 0.0.0.0 255.255.255.255 area 0 (shortcut to cover all interfaces)

On r3:

Router ospf 3

Network 0.0.0.0 255.255.255.255 area 0

On r4:

Router ospf 4

Network 0.0.0.0 255.255.255.255 area 0

On r1:

Do sh ip ospf neighbor

1. On ALL routers:

Passive interface L0

1. On r1:

Auto-cost reference-bandwidth 10000

Repeat on all routers!

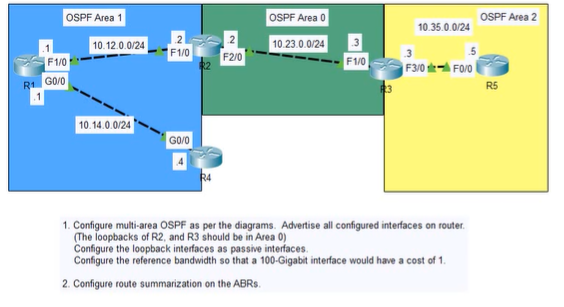
1. On r1:

Int g0/0

Ip ospf cost 10000

Repeat on all routers

**OSPF (MULTI AREA):**

****

1. On r1:

En

Conf t

Router ospf 1

Network 0.0.0.0 255.255.255.255 area 1

Passive-interface L0

Auto-cost reference-bandwidth 100000

On r2:

En conf t

Router ospf 1

Network 10.12.0.0 0.0.0.255 area 1

Network 10.23.0.0 0.0.0.255 area 0

Network 2.2.2.2 0.0.0.0 area 0

Passive-interface l0

Auto-cost reference-bandwidth 100000

On r3:

En

Conf t

Router ospf 1

Network 10.23.0.0 0.0.0.255 area 0

Network 10.35.0.0 0.0.0.255 area 0

Network 3.3.3.3 0.0.0.0 area 0

Passive-interface 10

Auto-cst reference-bandwidth 100000

On r4:

En

Conf t

Router ospf 1

Network 0.0.0.0 255.255.255.255 area 1

Passive-interface l0

Auto-cost reference-bandwidth 100000

Router 5:

En

Conf t

Router ospf 1

Network 0.0.0.0 255.255.255.255 area 0

Passive-interface l0

Auto-cost reference-bandwidth 100000

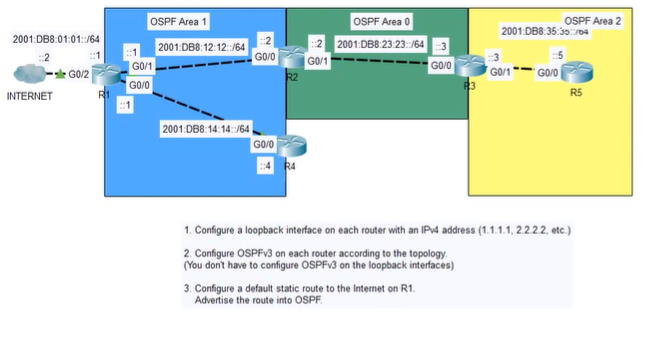
1. On r3:

Area 0 range 10.0.0.0 255.0.0.0

On r2:

Are 0 range 10.0.0.0 255.0.0.0

**OSPFV3 FOR IPV6:**

****

1. On r1:

En

Conf t

Int l0

Ip address 1.1.1.1 255.255.255.255

Exit

On r2:

En

Conf t

Int l0

Ip address 2.2.2.2 255.255.255.255

Exit

On r3:

En

Conf t

Int l0

Ip address 3.3.3.3 255.255.255.255

Exit

On r4:

En

Conf t

Int l0

Ip address 4.4.4.4 255.255.255.255

Exit

On r5:

En

Conf t

Int l0

Ip address 5.5.5.5 255.255.255.255

1. On r1:

Ipv6 router ospf 1

Int g0/0

Ipv6 ospf 1 area 1

Int g0/1

Ipv6 ospf 1 area 1

R4:

Ipv6 router ospf 1

R2:

Int g0/0

Ipv6 ospf 1 area 1

Int g01

Ipv6 ospf 1 area 1

R3:

Int g0/0

Ipv6 ospf 1 area 0

Int g0/1

Ipv6 ospf 1 area 2

R5:

Int g0/0

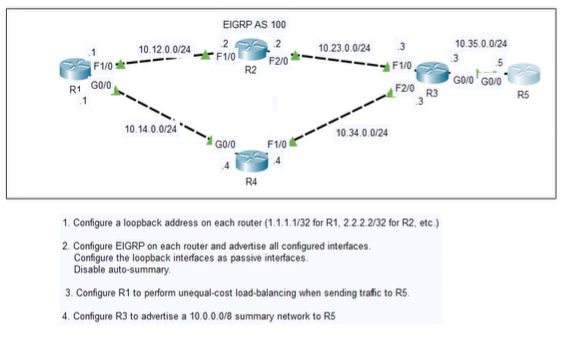
Ipv6 ospf 1 area 2

1. On r1:

Ipv6 route ::/0 2001:db8:01:01::2

Ipv6 router ospf 1

**EIGRP:**

****

1. On r1:

En

Conf t

Int l0

Ip address 1.1.1.1 255.255.255.255

On r2:

En

Conf t

Int l0

Ip address 2.2.2.2 255.255.255.255

On r3:

En

Conf t

Int l0

Ip address 3.3.3.3 255.255.255.255.

On r4:

En

Conf t

Int l0

Ip address 4.4.4.4 255.255.255.255

On r5:

En

Conf t

Int l0

Ip address 5.5.5.5 255.255.255.255

1. On r1:

Router eigrp <AS number> 100

Network 10.0.0.0

Network 1.1.1.1 0.0.0.0.0

Passive-interface l0

No auto-summary

On r2:

Router eigrp 100

Network 10.0.0.0

Network 2.2.2.2 0.0.0.0

passive -interface l0

No auto-summary

On r3

Router igrp 100

Network 10.0.0.0

Network 3.3.3.3 0.0.0.0

Passive-interface l0

No auto-summary

On r4:

Router eigrp 100

Network 10.0.0.0

Network 4.4.4.4 0.0.0.0

Passive-interface l0

No auto-summary

On r5:

Router eigrp 100

Network 10.0.0.0

Network 5.5.5.5 0.0.0.0

Passive-interface l0

No auto-summary

On r1:

Do sh ip route

Routes with D = learned by EIGRP

Do sh ip eigrp topology

1. On r1:

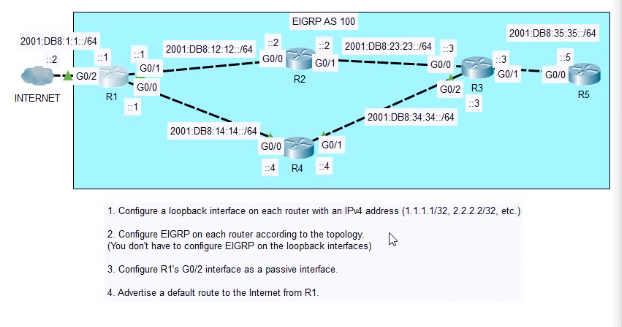
Variance 2

1. On r3:

Int g0/0

Ip summary-address eigrp 100 10.0.0.0

**EIGRP FOR IPV6:**

****

1. On r1:

En

Conf t

Interface l0

Ip address 1.1.1.1 255.255.255.255

1. On routers:

Ipv6 router eigrp 100

No shutdown

1. On r1:

Int g0/0

Ipv6 eigrp 100

Int g0/1

Ipv6 eigrp 100

Int g0/2

Ipv6 eigrp 100

1. On r1:

Int g0/0

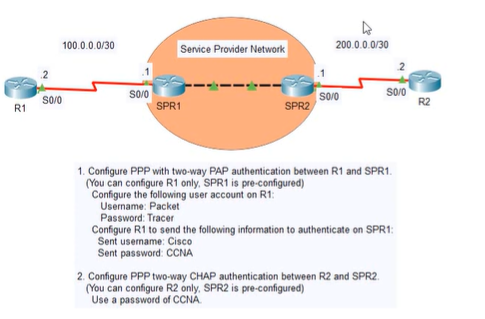
Ipv6 summary-address eigrp 100 ::/0

Int g0/1

Ipv6 summary-address eigrp 100 ::/0

On r5: do sh ip route

**PPP WITH PAP AND CHAP AUTHENTICATION:**



1. On r1:

En

Sh interfaces s0/0

\*encapsulation is HDLC\*

Ping 100.0.0.1

\*fails\*

Conf t

Int s0/0

Encapsulation ppp

Do sh ip int br

Exit

Username Packet password Tacer

Int s0/0

Ppp authentication pap

Ppp pap sent-username Cisco password CCNA

Do sh ip int br

Do ping 100.0.0.1

1. On r2:

En

Sh int s0/0

Ping 200.0.0.1

Username SPR2 password CCNA

Int s0/0

Shutdown

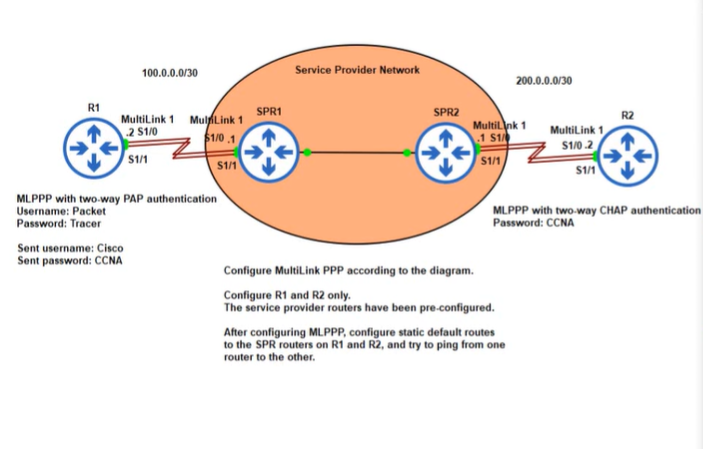
Encapsulation ppp

Ppp authentication chap

No shutdown

Do sh ip int br

Do ping 200.0.0.1

**MULTILINK PPP:  
**

1. ON R1:

En

Conf t

Username Packet password Tracer

Interface multilink 1

Ppp multilink

Ppp multilink group 1

Ppp authentication pap

Ppp pap sent-username Cisco password CCNA

Ip address 100.0.0.2 255.255.255.252

Do sh run int multi 1

Int s1/0

Encapsulation ppp

Ppp multilink group 1

No shutdown

Int s1/1

Encapsulation ppp

Ppp multi group 1

No shutdown

End

Sh ppp all

Sh ppp multilink

Ping 100.0.0.1

On R2:

En

Conf t

Username SPR2 (should be same as inside router) password CCNA (should be same on other outside router)

Int multi 1

Ppp multi group 1

Ppp authentication chap

Ip address 200.0.0.2 255.255.255.252

Do sh run int multi 1

Int s1/0

Encapsulation ppp

Ppp multilink group 1

No shutdown

Int s1/1

Encapsulation ppp

Ppp multilink group 1

No shutdown

End

Sh ppp all

Sh ppp multi

IP ROUTE 0.0.0.0 0.0.0.0 200.0.0.1

Do sh ip route

On R1:

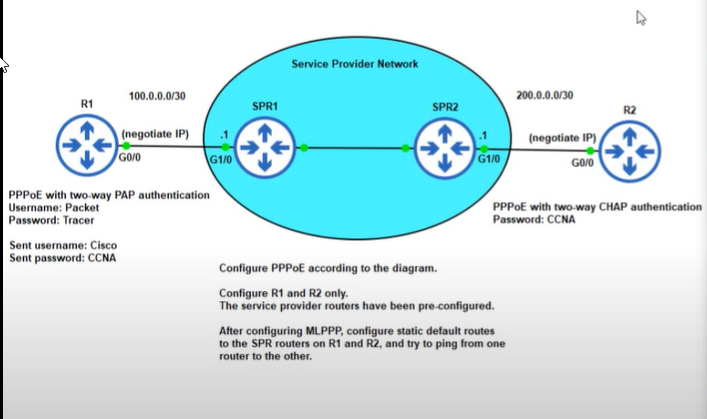
En

Conf t

Ip route 0.0.0.0 0.0.0.0 100.0.0.1

Do sh ip route

**PPPOE:**

****

On r1:

En

Conf t

Username packet password tracer

Interface dialer 1

Mtu 1492

Encapsulation ppp

Ip address negotiated

Ppp authentication pap

Ppp pap sent-username cisco password ccna

Dialer pool 1

Do sh run int dialer 1

Int g0/0

pppoe-client dial-pool-number 1

No shutdown

End

Sh ip int br

On r2:

Username spr2 password ccna

Int dialer 1

Mtu 1492

Encapsulation ppp

Ip address negotiated

Ppp authentication chap

Dialer pool 1

Int g0/0

Pppoe-client dial-pool-number 1

Sh ip int br

Conf t

Ip route 0.0.0.0 0.0.0.0 200.0.0.1

Do sh ip route

On r1:

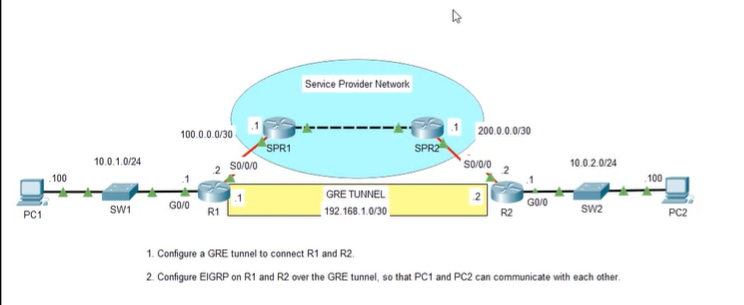
Conf t

Ip route 0.0.0.0 0.0.0.0 100.0.0.1

Do sh ip route

Do ping 200.0.0.2

**GRE:**

****

1. On r1:

En

Conf t

Int tunnel 0 (t0)

Ip address 192.168.1.1 255.255.255.252

Tunnel source s0/0/0

Tunnel destination 200.0.0.2

On r2:

En

Conf t

Int tunnel 0

Ip address 192.168.1.2 255.255.255.252

Tunnel source s0/0/0

Tunnel destination 100.0.0.2

Do sh ip route

(musst config default route so r1 and r2 can reach each other):

Ip route 0.0.0.0 0.0.0.0 200.0.0.1

On r1:

Conf t

Ip route 0.0.0.0 0.0.0.0 100.0.0.1

1. On r1:

Router eigrp 100

Network 10.0.1.0 0.0.0.255

Network 192.168.1.0 0.0.0.3

On r2:

Router eigrp 100

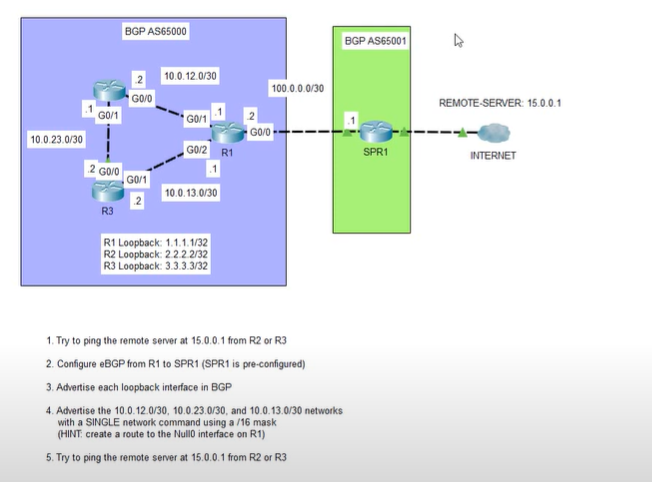
Network 10.0.2.0 0.0.0.255

Network 192.168.1.0 0.0.0.3

Do sh ip route

Ping host to host

**BGP:**

****

1. On r2:

En

Sh ip route

On r1:

En

Conf t

Router bgp (as #) 65000

Neighbor 100.0.0.1 remote-as 65001

3. On r1:

Do sh ip route

Network 1.1.1.1 mask 255.255.255.255

Network 2.2.2.2 mask 255.255.255.255

Network 3.3.3.3 mask 255.255.255.255

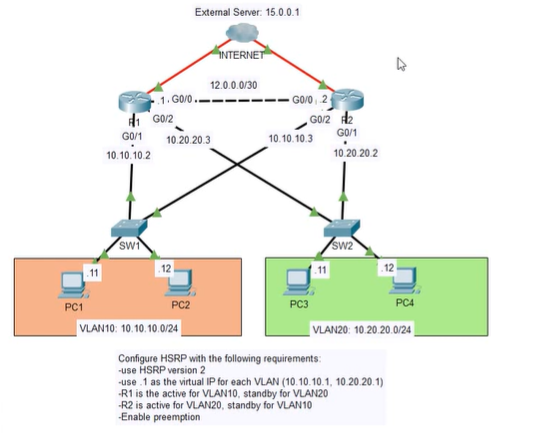
Do sh ip route

Network 10.0.0.0 mask 255.255.0.0

Exit

Ip route 10.0.0.0 255.255.0.0 null0 (discards anything it receives)

**HSRP:**

****

1. On r1:

En conf t

Int g0/1

Standby 10 (grouup number) ip (virtual ip) 10.10.10.1

\*check default priority\*

Do sh standby

\*its 100\*

Standby 10 priority 110

Standby version 2

Standby 10 preempt

On r2:

En

Conf t

Int g0/2

Standby ver 2

Standby 10 ip 10.10.10.1

Try to ping from host

Configure vlan 20:

On r2:

Int g0/1

Standby ver 2

Standby 20 ip 10.20.20.1

Standby 20 preempt

On r1:

Conf t

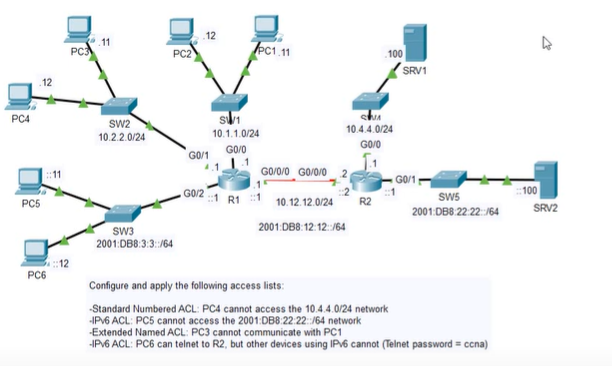
Int g0/2

Standby ver 2

Standby 20 ip 10.20.20.1

Standby 20 priority 90

**IPV4 AND IPV6 ACLS:**

****

1. ON R2:

En

Conf t

Access-list 1 deny host 10.2.2.12

Access-list 1 permit any

Int g0/0

Ip access-group 1 out

1. On r1:

En

Conf t

Ipv6 access-list g0/2\_IN (name)

Deny ipv6 host 2001.db8:3:3::11 2001:db8:22:22::/64 (destination)

Permit ipv6 any any

Int g0/2

Ipv6 traffic-filter g0/2\_IN in

1. On r1:

En

Conf t

Ip access-list extended g0/1\_IN

Deny ip host 10.2.2.11 host 10.1.1.11

Permit ip any any

Int g0/1

Ip access-group g0/1\_IN in

1. On r2:

En

Conf t

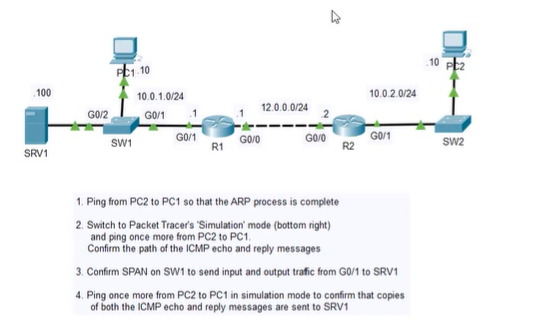
Ipv6 access-list TELNET

Permit tcp host 2001:db8:3:3::12 any eq telnet

Line vty 0 15

Ipv6 access-class TELNET in

**SPAN:**

****

1. ON SW1:

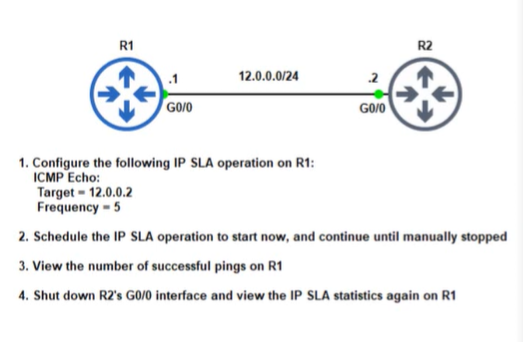
En

Conf t

Monitor session 1 source

Monitor session 1 destination interface g0/2

**IP SLA:**

****

1. On r1:

En

Conf t

Ip sla 1

Icmp-echo 12.0.0.2

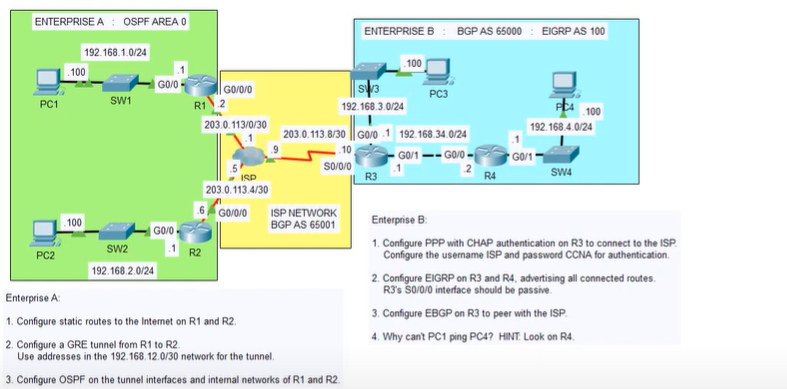
Frequency 5

1. In global config

Ip sla schedule 1 start-time <when> now <how often> life forever

4. Sh ip sla statistics

**REVIEW CONFIG LAB 3:**

****

1. On r1:

En

Conf t

Ip route 0.0.0.0 0.0.0.0 g0/0/0

On r2:

En

Conf t

Ip route 0.0.0.0 0.0.0.0 g0/0/0

1. On r2:

Int t0

Tunnel source g0/0/0

Tunnel destination 203.0.113.2

Ip address 192.168.12.2 255.255.255.252

Exit

On r1:

Int t0

Tunnel source g0/0/0

Tunnel destination 203.0.113.6

Ip address 192.168.12.1 255.255.255.252

Exit

Ping

1. On r1:

Router ospf 1

Net 192.168.2.0 0.0.0.255 area 0

Network 192.168.12.0 0.0.0.3 area 0

Do sh ip ospf neigh

ENTERPRISE B:

1. On r3:

En

Ping 203.0.113.9

\*fail\*

Conf t

Username ISP password CCNA

Int s0/0/0

Shutdown

Encapsulation ppp

Ppp authentication chap

No shutdown

Do ping 203.0.113.9

1. On r3:

Router eigrp 100

Network 203.0.113.8 0.0.0.3

Network 192.168.3.0 0.0.0.255

Network 192.168.34.0 0.0.0.255

Passive-interface s0/0

On r4:

En

Conf t

Router eigrp 100

Network 192.168.34.0 0.0.0.255

Network 192.168.4.0 0.0.0.0.255

Do hs ip route

1. On r3:

Router bgp 65000

Neighbor 203.0.113.9 remote-as 65001

Network 192.168.3.0 mask 255.255.255.0

Network 192.168.34.0 mask 255.255.255.0

Network 192.168.4.0 mask 255.255.255.0