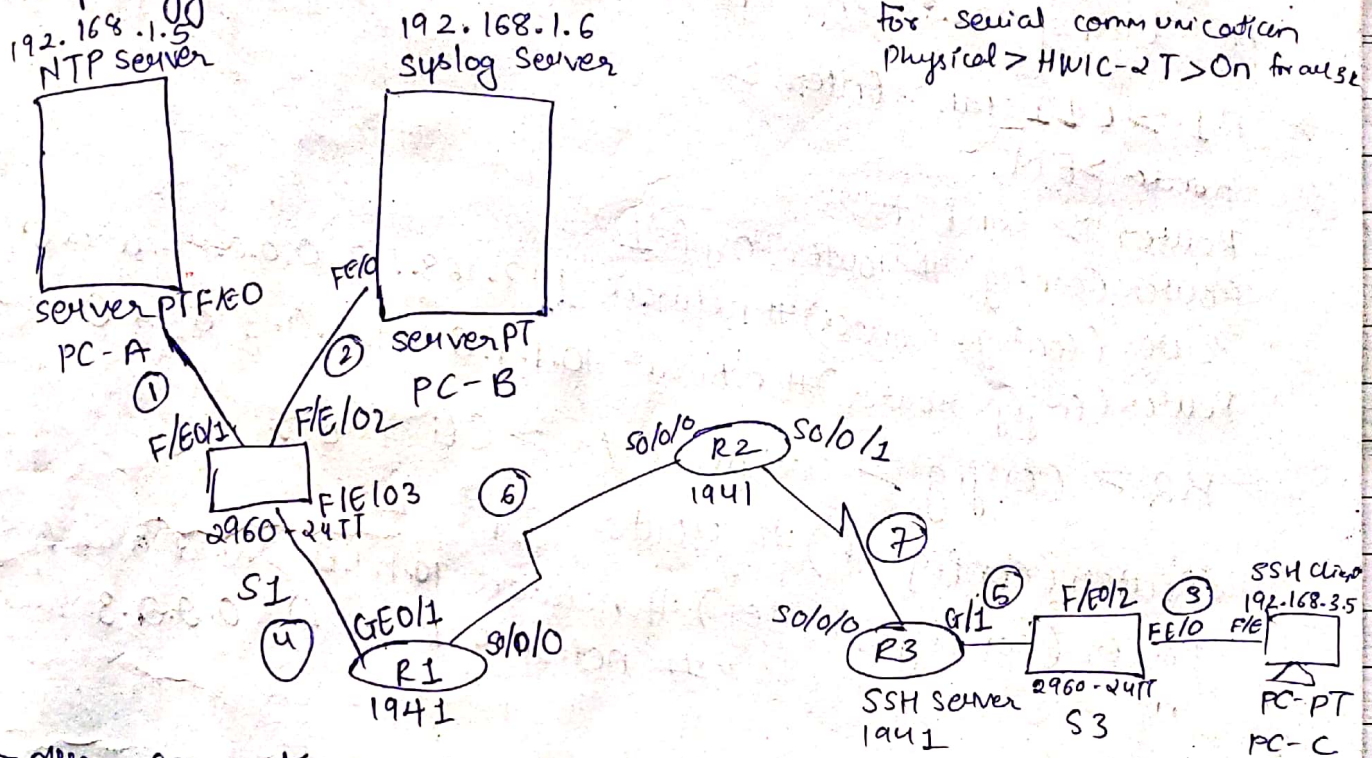
Practical 1 QIC

Topology:



For serial communication
Physical > HWIC-2T > On for all

→ After connections do the naming of the components.
For Routers naming Click on Router → config > Hostname

→ Set the IP config. PCA > Desktop > ip config > automatic > set IPv4 Add
IPV4: Add: 192.168.1.5 Subnet Mask 255.255.255.0, Dg. Gateway
DG: 192.168.1.1

PC-B > IPV4 Add: 192.168.1.6 Subnet " " DG: 192.168.1.1

PC-C > IPV4 Add: 192.168.3.5 Subnet 255.255.255.0 DG: 192.168.3.1

R1 > Config tab > Giga0/1 > IPV4: 192.168.1.1 Subnet " > On
R1 > " > Serial0/0/0 > IPV4: 10.1.1.1 Subnet 255.255.255.252 > On

R2 > Config > S0/0/0 > 10.1.1.2 Subnet " " > On
S0/0/1 > 10.2.2.2 Subnet " " > On

R3 > Config > S0/0/0 > 10.2.2.1 Subnet " " > On
G0/1 > 192.168.3.1 Subnet Auto > On

→ To check the connections properly click on message icon & Send packets

A] OSPF

We need to configure n/w such that packets can be transferred in entire network.

→ R1 > CLI tab > Enter >
Router > EN
Router > conf t
Router (config) # router ospf 1 → Process ID: used for differentiating bet multiple ospf processes on same router
Router (config-router) # network 192.168.1.0 0.0.0.255 area 0
Router (config-router) # network 10.1.1.0 0.0.0.3 area 0

→ R2 > config > serial 0/0/0 > Cli tab >
Router (config-if) # router ospf 2
Router (config-router) # network 10.1.1.0 0.0.0.3 area 0
" " # network 10.2.2.0 0.0.0.3 area 0

→ R3 > config > serial 0/0/1
Router (config-if) # router ospf 3
" (config-router) # network 192.168.3.0 0.0.0.255 area 0
" " # network 10.2.2.0 0.0.0.3 area 0

→ Check the package is being sent from PCA - PCC

→ GO to Desktop > Command Prompt > of PCA
C:\> ping 192.168.3.5 (PC C address)

Similarly from PC C CMd check pinging to PCA

→ Now do MD5 authentication:
In R1 > CLI
Router (config-router) # router ospf 1
R1 (config-router) # area 0 authentication message-digest → used for enabling message digest authentication in area 0
Do the command on other Routers as well. but change ospf id acc to Routers

→ Configure MD5 key for all routers in area 0.
To be done on serial interfaces on R1, R2 & R3.
password MD5pa55 for key 1

→ R1 > CLI >

Router (config)# interface s0/0/0
Router (config-if)# ip ospf message-digest-key 1 md5 MD5pa55

identifier and helps mapping correct key

→ R2 > CLI >

Router (config)# interface s0/0/0
R2 (config-if)# ip ospf message-digest-key 1 md5 MD5pa55
R2 (config-if)# interface s0/0/1
R2 " " # ip ospf message-digest-key 1 md5 MD5pa55

→ R3 > CLI >

R3 (config) interface s0/0/1
" " " " " "

→ Verify configurations by using the commands
show ip ospf interface
Go to Router's CLI tab enter the Global mode i.e Router#

Router# show ip ospf interface
perform the above command on all 3 Routers.

Part B : NTP ~~& Syslog server~~

→ PCA > ~~De~~ Services > NTP > Enable
Key : 1 password : NTPa55
Select Date & Time you want

→ R1 > CLI
Router (config)# ntp server 192.168.1.5 → specific IP of NTP Server
" " # ntp update-calendar → Updates the H/w Clock of Router with NTP

In R1, continue from prev step:

ntp authenticate → enables authentication on NTP packets

ntp trusted-key 1 → The packets will be verified by checking the key no. here, it is 1.

ntp authentication-key 1 md5 NTPa55 → sets an AK for NTP.

service timestamps log datetime msec → enables routers to include timestamp in the log for format of TS.

Repeat same step for all 3 Routers

→ exit the config mode of R1

Router# show clock

Check whether the clock matches the time on NTP server (fast forward as process may take time)

Do the same for all 3.

→ Part 3: Configure Routers to log messages to the Syslog

Go to PC-B > Services > Syslog > On

~~Go to R1~~

~~Router#~~ conf t

Router(config)

Router(config)#exit

Router# conf t

(Repeat)

Go to R1 > terminal

Router(config)#logging host 192.168.1.6

Repeat the same step for all 3

Exit the config mode. > Enter the

→ To see the result go to PC-B > syslog Tab >

There will be message sys-5-configured from con 2 con.

Here, the no. notifies the type of notification

0 is for critical msg & 5 for notification.

→ To check logs from Router > R1 > Router# show logging end.

Do the same for all Routers

→ Part 4: Configure R3 to support SSH connection.

~~Go to R3 > Config Tab > State Tab > Hostname to R3~~

R3(config)# ip ~~address~~ domain-name ccnasecurity.com → domain name to be given

R3(config)# username SSHadmin privilege 15 secret ciscosshpa55

R3(config)# line vty 0 4 → virtual terminal lines 0 - 4 will be open for communication

R3(config-line)# login local

R3(config-line)# transport input ~~all~~ ssh

↳ the connection with ssh can only be allowed.

We need RSA keys because SSH used PKC for securing comm.

R3(config-line)# en

R3(config)# crypto (→ cryptographic) key zeroize rsa → to remove prev keys

→ Generate RSA encryption key pair for R3.

R3(config)# crypto key generate RSA.

How many bits : 1024] Modulus size; the product of two prime numbers. the more bits → stronger keys are generated.

R3(config)# ex

→ R3# show ip ssh (View SSH configuratn)

→ Configure SSH timeouts & authentication parameters.

R3(config)# ip ssh time-out 90

R3(config)# ip ssh authentication-retries 1.

R3 " # " version 2

Issue the R3# show ip ssh to see changes.

→ Attempt to connect to R3 via Telnet from PC-C.

Go to PC-C > Cmd Prompt

PC> telnet 192.168.3.1 (Connectn should fail)

as we have allowed ssh connectn only.

→ Connect to R3 using SSH on PC-C

PC> ssh -l sshadmin 192.168.3.1

password: cisco sshpass

R3# show ip ssh

R3# exit (to close the connection)

→ Connect to R3 using SSH on R2

~~Go to R2 > CLI > static > Hostname R2~~

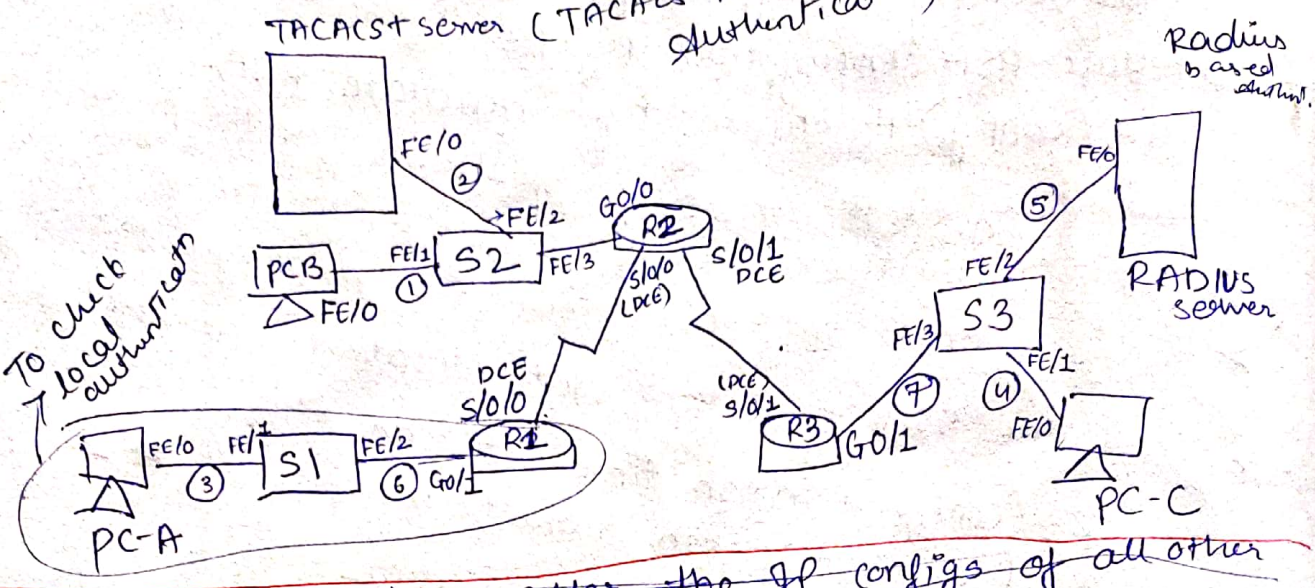
R2# ssh -v 2 -l sshadmin 10.2.2.1

password: cisco sshpass

R3# show ip ssh

R3# exit

Practical - 2 AAA authentication



→ ~~Setup serial wires after the IP configs of all other~~ end devices.

1) R1 > G0/1 > IP address = 192.168.1.1 subnet Auto > On

~~2~~ PCA > Desktop > IP Configuratn > 192.168.1.3 > subnet Auto > Default Gateway > 192.168.1.1

PCB > " " > 192.168.2.3 > subnet Auto > D.G: 192.168.2.1

T server > Desktop > IP config > 192.168.2.2 > Subnet Auto > DG: 192.168.2.1

2) R2 > G0/0 > IP Add = 192.168.2.1 > subnet Auto > On

3) R3 > 192.168.3.1, Subnet Auto > ~~DG~~ On

PC-C > Desktop > IP Config > 192.168.3.3 > Subnet Auto > DG: 192.168.3.1.

Step 1: Connections.

→ PC-A : ~~IP~~ DefG: 192.168.1.1, Subnet 255.255.255.0 IP: 192.168.1.3

PC-B : ~~IP~~ DefG: 192.168.2.1, Subnet " IP: 192.168.2.3

PC-C : ~~IP~~ DefG: 192.168.3.1, Subnet " IP: 192.168.3.3

TACACS Server: DG: 192.168.2.1, Subnet " IP: 192.168.2.2

RADIUS Server: DG: 192.168.3.1, Subnet " IP: 192.168.3.2

For Routers add serial ports and then configure

R1: G0/1 : IP: 192.168.1.1 Subnet: 255.255.255.0
s/0/0/0: IP: 10.1.1.2 subnet: 255.255.255.252

R2: G0/0: IP: 192.168.2.1 SBNT: 255.255.255.0
s0/0/0: IP: ~~192.~~ 10.1.1.1 SBnet: 255.255.255.252
s0/0/1: IP: 10.2.2.1 "

R3: G0/1: IP: 192.168.3.1 subnet: 255.255.255.0
S/0/0/1: IP: 10.2.2.2 subnet: 255.255.255.252

For Better performance & security use ospf MD5 ~~with root~~ (Next year)

Step 2: OSPF Configuration:

R1: 1) R1 (config)# line vty 0 4
2) R1 (config-line)# password admin
3) # login
4) # en
5) (config)# router ospf 1
6) # network 192.168.1.0 0.0.0.255 area 0
7) # network 10.1.1.0 0.0.0.255 area 0

R2: Repeat 1) to 4)

R2: (config)# router ospf 2
network 192.168.2.0 0.0.0.255 area 0
network 10.2.2.0 0.0.0.255 area 0
network 10.1.1.0 0.0.0.255 area 0

R3: Repeat 1) to 4)

R3: (config)# router ospf 3
network 192.168.3.0 0.0.0.255 area 0
network 10.2.2.0 0.0.0.255 area 0
#

TACACS - Terminal Access Controller Access - Control System

RADIUS - Remote Authentication Dial-in User Service

Step 3: Configure local database authentication on console

R1: R1>en
R1# conf t
R1(Config)# username Admin1 secret admin1 pass5
aaa new-model (Applying AAA security servi
aaa authentication login default local

Configure authentication for login to the device
this method should be made default
router should use locally config cred

line console 0 (console port 0 config)
login authentication default → Apply whatever setting you made default above

specifies that login authentication should be done

end
exit

→ Enter username & password.

Step 4: Configure local AAA Authentication for vty lines on R1.
Configure domain name & crypto key for SSH)

R1(config)# ip domain-name ccnasecurity.com
crypto key generate ~~RSA~~ rsa
1024

Step 5: Configure a named list AAA method for vty lines.

Named list means a group that contains specific methods
Here, we use SSH-LOGIN as named list containing all
local AAA ~~(i.e. local, TACACS+ & RADIUS logins)~~ (local creds)

R1(config)# aaa authentication login SSH-LOGIN local

specifie that settings are being configd for ~~local~~ login attemps

named list

The local creds database should be used for authentication.

Step 6: Config vty lines
(config)# line vty 0 4
login authentication SSH-LOGIN
transport input ssh
end

Step 7: verify the AAA method

PC-A > cmd > ssh -l Admin1 192.168.1.1
password admin1pa55

Part 2: Configure Server based AAA using TACACS+ R2

R2(config)# username Admin2 secret admin2pa55

* backup local DB entry for ensuring that user can login even if TACACS+ server is down.

→ Go to TACACS+ server → services → AAA

On → client name R2 , IP: 192.168.2.1

secret – tacacspa55 , server Type: TACACS+ > Add

username - Admin2 password : admin2pa55 > Add

→ Configure AAA login for console on R2

R2(config)# tacacs-server host 192.168.2.2 # tacacs-server key tacacspa55

R2(config)# aaa new-model

#aaa authentication login default group tacacs+ local

authentication should be attempted using Tacacs+ server group if it fails fall to local DB.

line console 0 # login authentication default.

#end # exit → login using username & pass

Repeat the same for RADIUS server

R3(config)# username Admin3 secret admin3pa55

→ RADIUS server → Services → AAA → On → Client Name: R3

IP: 192.168.3.1, secret - radiuspa55, server Type: Radius > Add

UN: Admin3 password: admin3pa55 > Add

radius-server host 192.168.3.2 # radius-server key radiuspass

R3(config)# aaa ...

" " group radius local

line console 0

login authentication default

#end

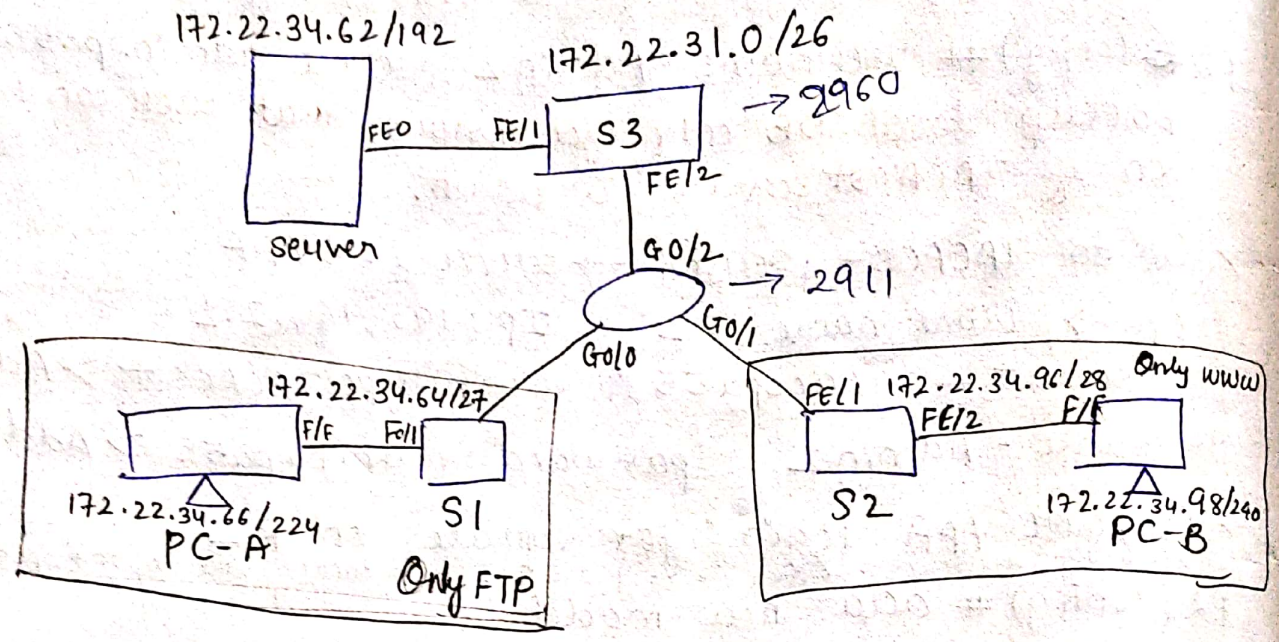
exit

To verify try to login using the UN & Pass.

Practical 3

PC1 needs only FTP access while PC2 only web access
Both comps should ping server but not each other

Topology:



Extended ACLs are applied on the router close to source

Device		IP Add	Subnet	DG
R1	G0/0	172.22.34.65		
	G0/1			
	G0/2			

For R1

[Note: To calculate wildcard mask
255.255.255.255 – Subnet mask]

R1 > en
conf t
access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
eqval to ftp

#access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
source ip range
wildcard mask
destination

interface G0/0
ip access-group 100 in (inbound traffic)
ex 4 To verify ~~ping~~ ftp server from PC-A (ftp server ip)

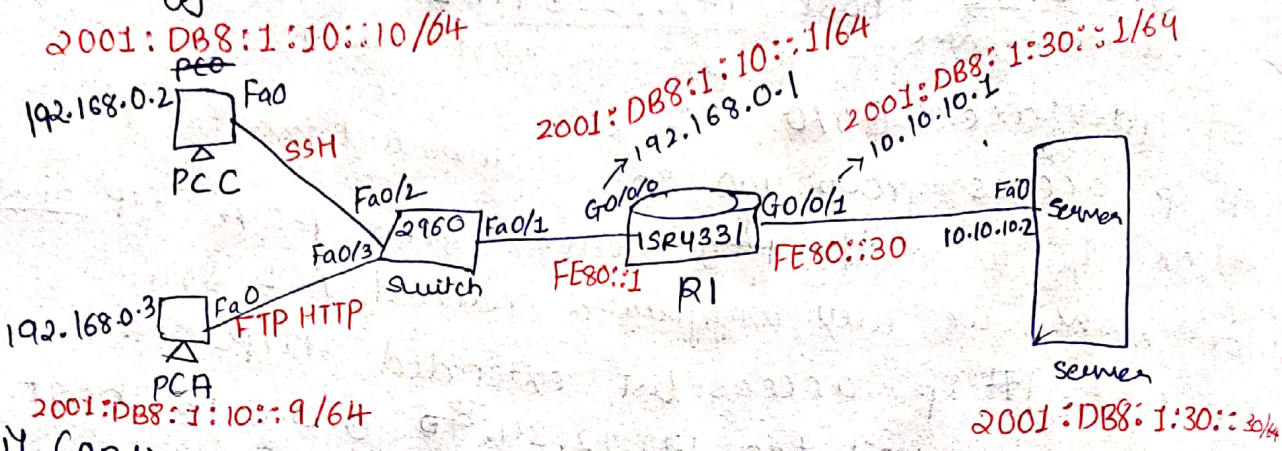
=> For WWW, we will configure a named ACL
R1(config)# ip access-list extended HTTP-ONLY
#permit tcp 172.22.34.~~64~~ 96 0.0.0.15 host 172.22.~~34~~ 34.~~62~~ 62 eq www
#permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
#en
#i/f G0/1
#ip access-group HTTP-ONLY in

To verify go to PC-B browser & enter the url http://172.22.34.62

Practical 4

a) Configure IP ACLs to Mitigate attacks and IPV6 ACLs
b) Verify connectivity among devices before firewall config.
b) Use ACLs to ensure that remote access can only be done PCC
c) Configure ACLs to mitigate attacks.
d) Configuring IPV6 ACLs.

Topology:



i) Configurations: ISRs provide capabilities like firewall, vpn, etc along with routers.

For R1: Interface: G0/0/0 > On
IPv4 Add: 192.168.0.1 Subnet: Auto
→ Interface: G0/0/1 (Do not On)
IPV4 Add: 10.10.10.1 Subnet: 255.255.255.252 > On

For Server: Desktop > IP Config > Let IPV 4 & 6 remain default
IPV4 Add: 10.10.10.2
Subnet: 255.255.255.252 DG: 10.10.10.1

For PC-C: Desktop > IP > Let it remain default
IPv4 Add: 192.168.0.2 Subnet: 255.255.255.0
DG: 192.168.0.1

For PC-A: same as above just change the IPV4: 192.168.0.3

→ In R1,

R1(config)# ip route 192.168.0.0 255.255.255.0 10.10.10.2

ip route → configure a static route
192.168.0.0 255.255.255.0 → destination n/w & subnet
10.10.10.2 → next hop address.

It means, that any traffic destined for destination should be forwarded to the next hop ip address.

→ To verify connection ping the server from both PCs

part b) Since Remote Access is to be done from PC-C:

R1(config)# enable secret enpa55 → (pswd for enable cmd)

#line console 0

password conpa55 (verified before entering the Router (b4 enable))

#login

#exit

#ip domain-name ccnasecurity.com (SSH config step)

#username admin secret adminpa55

#line vty 0 4

#login local #transport input ssh

#exit

#crypto key generate rsa

:1024

Go to PC-C command prompt > telnet 10.10.10.1

Connection should fail:

>ssh -l admin 10.10.10.1

password: adminpa55

Part C)

2001:0DB8:0001:0010:0000:0000:0001

n/w portion — host portion

→ Configure IPv6 Address:

→ For PC-A > Desktop > IPV6 > static

Add: 2001:DB8:1:10::9 /64 (states the no. of bits that indicate n/w portion)

Link local address FE80::260:70FF:FE2E:A307 (Default)

DG: FE80::1

→ For Server: ''

Add: 2001:DB8:1:30::30 /64

Link local Address – FE80::230:F2FF:FE24:D043 (Default)

DG: FE80::30

→ For R1

First R1(config)# mode paste the following commands.

#no access-list 1

#access-list 100 permit tcp host 192.168.0.2 host 192.168.0.1

only source IP — only destination

eg (22) SSH port

ex

conf t
interface G0/0/0
ipv6 address 2001:DB8:1:10::1/64
" " FE80::1 link-local
exit

interface G0/0/1
ipv6 address 2001:DB8:1:30::1/64
ipv6 address FE80::30 link-local
ex

ipv6 unicast-routing
ipv6 route 2001:DB8:1:10::1/64 2001:DB8:1:30::30

→ Go to PCA > Desktop > Browser Url > http://2001:DB8:1:30::30
same for PCC

→ R1 (config)#

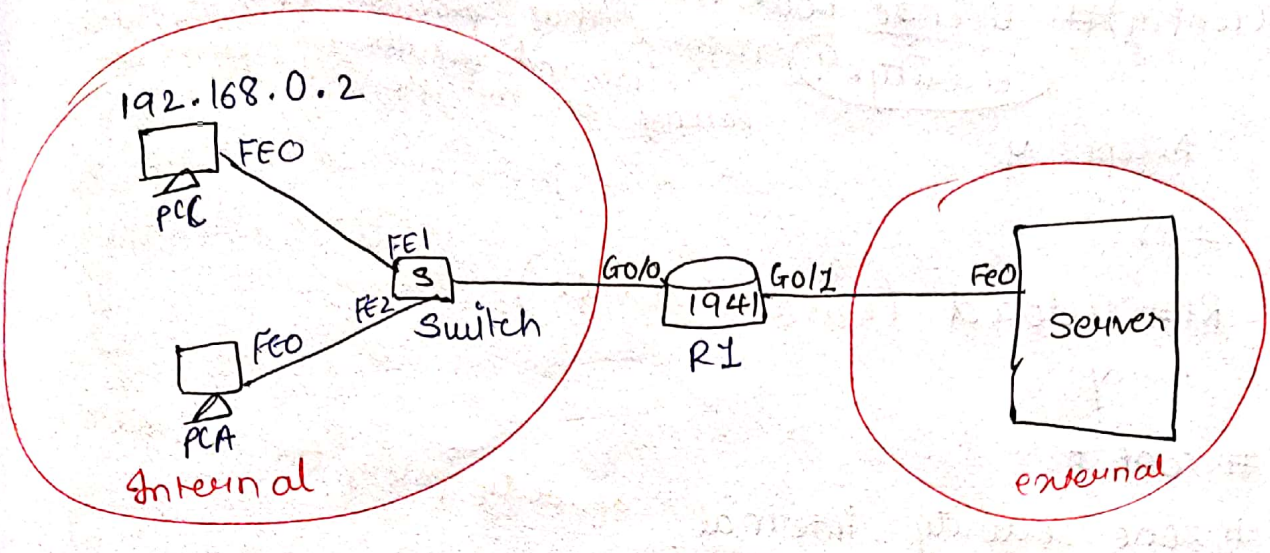
ipv6 access-list HTTP
permit tcp host 2001:DB8:1:10::9 host 2001:DB8:1:30::30
~~http~~ eq www
" " eq 443 HTTPS port
ex

int/f G0/0/0
ipv6 traffic-filter HTTP in

→ Go to PCA > Browser, put the same URI, it should open
→ do the same for PCC it should not open.

Practical 5

ZPW - A firewall feature of Cisco routers. It applies firewall rules on logical zones instead of interfaces



Device Name	IP4 Address	Subnet Mask	Default Gateway
PC-C	192.168.0.2	Auto	192.168.0.1
PC A	192.168.0.3	Auto	192.168.0.1
R1 G0/0	192.168.0.1	Auto	—
R1 G0/1	10.10.10.1	255.255.255.252	—
server	10.10.10.2	255.255.255.252	10.10.10.1

→ Go to R1 to enable SSH connection.

→ R1(config)# enable secret enpa55
#line console 0
password conpa55
login
exit
#ip domain-name ccnasecurity.com
#username admin secret adminpa55
#line vty 0 4
login local
exit
crypto key generate rsa (same NVRAM)

R1 # show version

R1 (config)# license boot module c1900 technology-package
(c1900 → Router series)
securityk9 package that provides VPN & Firewall capabilities
The command installs the license and package on the router.

Accept : Y

ex

R1# reload (Restart device)

Y

R1 # conf t

zone security internal — security policy for internal zone

ex

zone security external — external zone

ex # ex

show version.

R1 # Conf t

ip access-list extended 101 — create an ext. ACL named 101 to filter IP traffic

permit ip 192.168.0.0 (source n/w) 0.0.0.255 (wildmask) any

ex → permits all ip traffic from ~~ab~~ source range

class-map type inspect match-all ~~1001~~ 101

create a class-map "101" of type inspect

match access-group name 101

ex → matches the class-map traffic to criteria defined in ACL.

policy-map type inspect 101 →

create policy-map "101" of type inspect

class ~~tg~~ type inspect 101

associate class 101 with policy 101

inspect # ex # ex

Here, the router is told to perform stateful inspection on traffic flows matched by class-map 101

(config)# zone-pair security 101 source internal destination external. traffic flow from internal to external

service-policy type inspect 101

ex

interface gi 0/0

zone-member security internal

ex

#interface gi 0/1
zone-member security external
ex # ex
copy running-config startup-config

Go to pc C and ping the server
ping 10.10.10.2

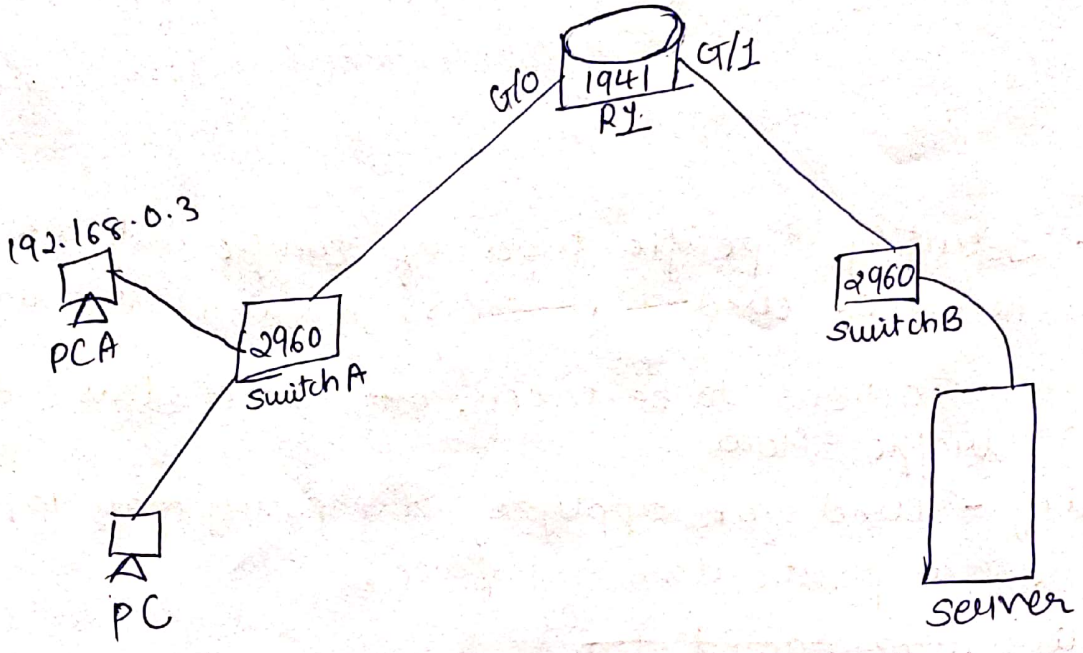
Class map - Identify specific types of traffic within a network. Used for QOS. Traffic classifican

policy-map - The actions to be taken. ~~base~~ on a classified traffic flow

service policy - used for applying the policy map 101 to a particular interface.

~~so, the policy map named 101~~
This means that the traffic passing through that interface / direction will be subject to actions defined in policy map 101.

Practical 6



Device ~~IP Add~~	IPV4 Address	Subnet	D.G
PC	192.168.0.2	255.255.255.0	192.168.0.1
Server	10.10.10.2	255.255.255.252	10.10.10.1
R1 G0/0	~~192.168.0.0~~ 192.168.0.1	255.255.255.255	—
R2. G0/1	10.10.10.1	255.255.255.252	—

Test the connection

Step 1:

Go to R1

```
# ip domain-name ccnasecurity.com
# username admin secret adminpass
# line vty 0 4
# login local
# exit
# crypto key generate rsa
  1024
# ex
# show version
# license boot module c1900 technology-package securityk9
  -Y
# ex
# reload
  Y
```

R1 # mkdir iosips — create a new directory named iosips

```
# conf t
# ip ips config location flash:iosips   (configure location where IPS signatures are stored)
# ip ips name iosips                    (set name for IPS config; we have set it as "iosips")
# ip ips signature-category             (enter the signature category menu)
# category all                          (the config should be applied to all signature categories)
# retired true                          (Retiring a signature means it is no longer actively used for detection)
# ex
# category ios_ips basic                (creates a new category named ios_ips with label "basic")
# retired false                         (To keep signature in ios_ips category active)
# ex
# ex
# int gi 0/1                            (enables IPS on gi 0/1 for outbound traffic)
# ip ips iosips out                     (Meaning: The traffic leaving this interface will be inspected by the IPS using iosips config.)
# ip ips notify log
```

#ex

R1# clock set (current server time) & date

Go to server > services > NTP > copy the time paste on the above command

```
# conf t
# service timestamps log datetime msec
# logging host 10.10.10.2
# ip ips signature-definition
# signature 2004 0 → subsign also 0
# status
# retired true
# enabled true
# retired false
# ex
# engine
# event-action produce-alert
# event-action deny-packet-inline
# ex
# ex
# ex
# -Y
```

signature id

used for echo request

drop the packet in the path.

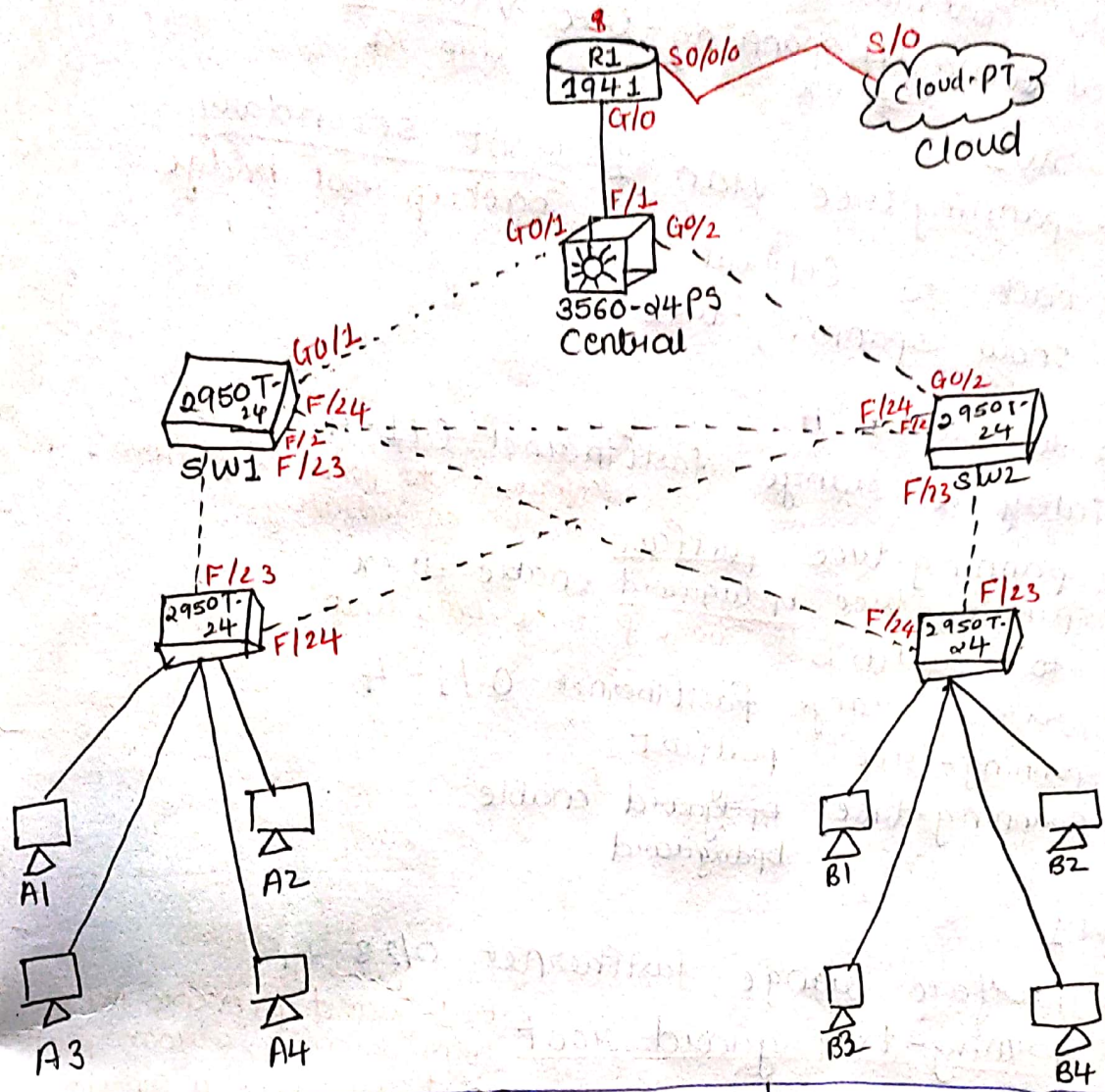
Connect the PCA ~~tot~~ Now and check whether it can ping the server. ~~fro~~ Do the same from PC the connectn should not happen. And log should be maintained in the server.

Can you ping the PC from server?

Echo request is for ping.

Layer 2 security

Practical 7



Device	IP	Subnet	DG
R1 S/0/0	201.10.10.1	255.255.255.0	
R1 G0/0	192.168.29.1	255.255.255.0	
PC A1	10.10.10.20	255.255.255.0	
B1	10.10.10.10	" " "	

Secure the Router & switches with password & ssh
Set the Hostname & display name of all switches.

→ Go to central switch to make it a root bridge.
central #(config)# spanning-tree vlan 1 root primary
vlan id — root bridge
ex

→ In SW1
#spanning-tree vlan 1 root secondary
backup root bridge

→ Go back to central
show spanning-tree

→ Go to switch A
interface range fastEthernet 0/1-4
configure the ports to go from 1 state to another immediately.
spanning-tree portfast
spanning-tree bpduguard enable # ex
Bridge Protocol Data Unit

→ Go to switch B
interface range FastEthernet 0/1-4
spanning-tree portfast
spanning-tree ~~bpdguard~~ enable
bpduguard

→ SW1
interface range fastEthernet 0/23-24.
spanning-tree guard root
Root guard prevents the port from becoming a root port if it receives a superior BPDU.

→ SW2
interface range fastEthernet 0/23-24
spanning-tree guard root

→ SWA : (Repeat same for SWB)
interface range f 0/1-22
switchport mode access
access configuration for switchports
switchport port-security maximum (2)
max no. of mac addresses allowed.
enables port security mode that restricts no. of MAC add
switchport port-security violation shutdown
if violation is dectected shutdown
switchport port-security mac-address sticky
Dynamically learn the mac-add of devices connected to a port and securing them

Go to SWA (Repeat for SWB)
#ex #ex #ex
login to SWA using password.
SWA# show port-security interface f 0/1
conf t
interface range fastEthernet 0/5 - 22
shutdown

Spanning tree protocol: A layer 2 network protocol.
select root bridge, root port
It is used to prevent looping within a n/w topology

Layer 2 switch operates at layer 2 of OSI i.e. Datalink
Layer 2 uses MAC address to determine where data goes. Switch has a table that has the details of which port is connected to which MAC address.

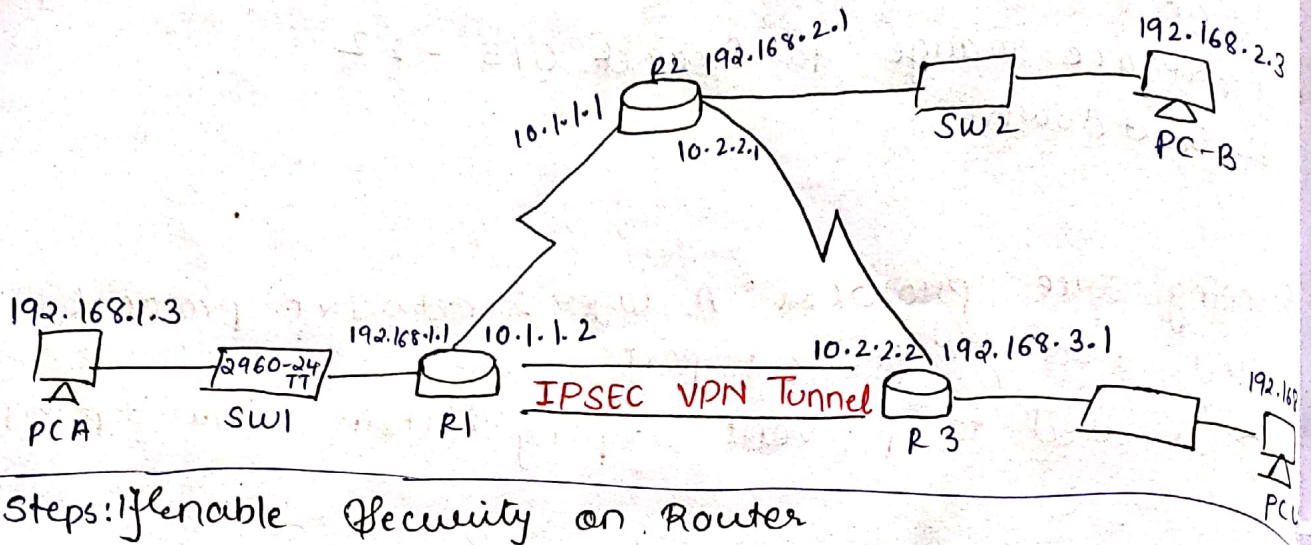
BPDU - Message exchanged ~~with~~ between switches participating in a spanning tree protocol. They are used for electing the root bridge, determine the best path to the root bridge, and prevent network loops by managing port states.

Bridge Protocol Data Unit

Practical # 9

Configure IPsec VPN using CLI

→



Steps: 1) Enable Security on Router
conpass, enpass and SSH

2) Configure OSPF

On R1: Router Ospf 1
network 192.168.1.0 0.0.0.255 area 0
network 10.1.1.0 0.0.0.3 area 0
#ex

On R2: Router Ospf 1
network 192.168.2.0 0.0.0.255 area 0
network 10.2.2.0 0.0.0.3 area 0
network 10.1.1.0 0.0.0.3 area 0
#ex

On R3: Router Ospf 1
network 192.168.3.0 0.0.0.255 area 0
network 10.2.2.0 0.0.0.3 area 0
#ex

→ Test by ping cmd from PC-A to PC-C

3) Enable security package. (for both R1 & R3)

R1 → R1(config)# license boot module c1900 technology-package security k9
-y
→ reload.

Identify the traffic of interest on R1

R1(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

Configure ACL 110 to identify traffic from R1 to R3 (This traffic will trigger the IPsec VPN to be implemented when data flows betn R1 & R3).

5. Configure the IKE phase 1 Ipsec policy on R1 → defines params for securing

R1(config)# crypto isakmp policy 10

ISAKMP - Internet Security Association and Key Management Protocol.

The above command is used to configure cryptographic parameters included in ISAKMP policy 10, where 10 is the priority of the policy.

→ #encryption aes 256 → key-size

To configure encryption settings within Ipsec with algorithm AES (Adv encryption std). AES is an symmetric key alogorithm that works by using Block cipher.

→ #authentication pre-share

The authentication method is set to pre-shared keys. It means both devices should have same key.

→ # group 5

sets the Diffie-Hellman (DH) group to group 5 for the IKE negotiations. DH is a key exchange protocol used to establish a shared secret between two devices communicating over an insecure network

→ # ex

→ # crypto isakmp key VPNpa55 address 10.2.2.2] ?

Specifies the pre-shared key to be used for IKE Phase 1 negotiation with R3.

IKE Phase 1: Internet Key Exchange Phase 1 is the 1st step in establishing a secure connectn like VPN here, the device authenticate each other and negotiate security params such as encryption methods & authentication mechanisms. (Basically an agreement on how they will exchange the data)

6) Configure IKE phase 2 IPsec policy on R1

In phase 2, devices establish the params for encrypting & authenticating the actual data to be transmitted betn them.

crypto ipsec transform-set VPN-SET esp-aes (encapsulating security payload protocol) esp-sha-hmac (Hashed message Authentication code) (secured Hash algorithm)

A transform set is collection of security parameters that define how data is encrypted, authenticate & protected during transmission.

→ The above command configures the router to use AES encryption with SHA-HMAC authentication for securing IPsec communication when using "VPN-SET" transform set.

crypto map VPN-MAP 10 ipsec-isakmp

creates a cryptomap named with a sequence number of 10 & associates it with both IPsec & ISAKMP, meaning that this crypto map will handle both phase 1 & 2 negotiation.

→ Crypto maps are a config object used to define the policy for IPsec. They are applied to interfaces to determine which traffic should be encrypted and sent over the tunnel.

description VPN connection to R3

Adds a description to the crypto map

~~R1~~ set peer 10.2.2.2

specifies the other device with which we communicate

set transform-set VPN-SET

Associates the VPN-SET with VPN-MAP.

match address 110

specifies that ACL 110 determines which traffic will be protected by this crypto map. Only the traffic matching the condn in 110 will be encrypted & sent over the tunnel.

#

configure crypto map on the outgoing interface
interface s1/0/0
crypto map VPN-MAP.

3) Do the same for R3

4) verify the IPsec VPN

→ show crypto ipsec sa
The no. of params should be zero.

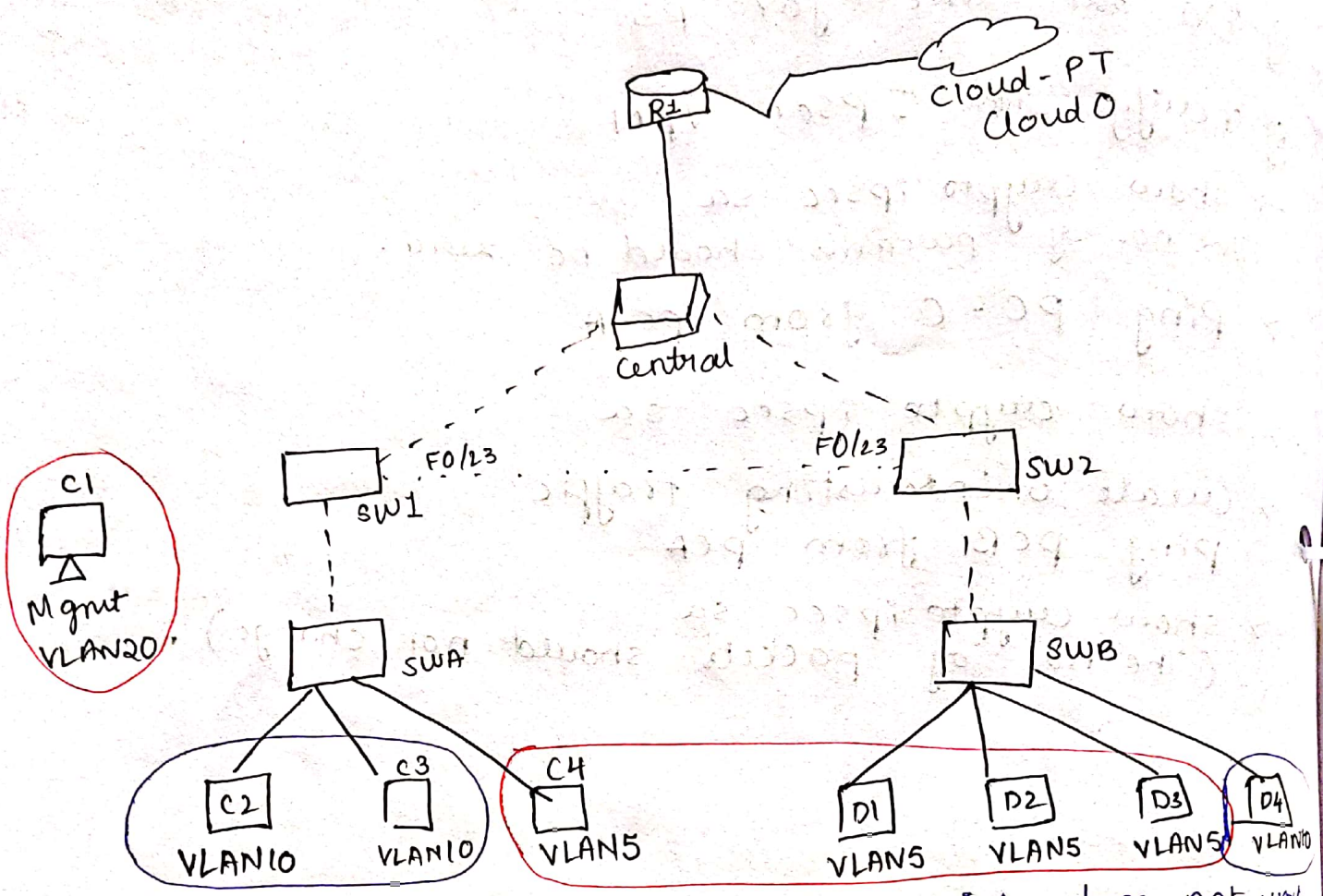
→ Ping PC-C from PC-A

→ show crypto ipsec sa

→ Create uninteresting traffic
ping PCB from PCA

→ show crypto ipsec sa
(The no. of packets should not change).

Practical - 8
Layer 2 VLAN Security



Redundant links- Backups in case a link does not work.

Trunk - A communication line designed to carry multiple signals simultaneously.

Step 1:

Verify connectivity in devices on the same VLAN

Step 2: Create a Redundant link betn SW1 and SW2