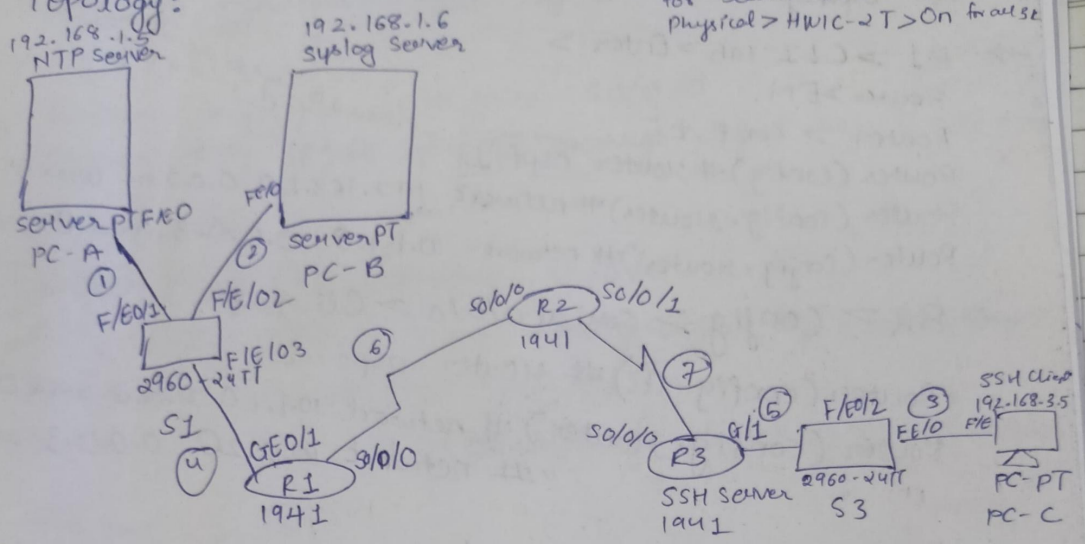
Practical 1 QIC

Topology:



For serial communication
Physical > HWIC-2T > On from slot

→ 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
C"

→ 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 ~~configure~~ command on other Routers as well. but change ospf id acc to Routers

→ Configure MD
To be done or
password M

→ R1 > CLI >
Router (con
Router (confi

→ R2 > CLI >
Router (co
R2 (confi
R2 (config
R2 "

→ R3 > C
R3 (
"

→ Verify
show i
Go to
mode i.e
Route
perform

Part B : N

→ PCA >
Key :
Selec

→ R1 >
Rou
"

→ 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 MD5pass

identifier that 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 Auth for NTP.
service timestamps log datetime msec → for format of TS.
↳ enables routers to include timestamp in the log

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 Server

Go to PC-B > Services > Syslog > On

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

Go to R1
Router# conf t
Router(config)
Router(config)# exit
Router# conf t
(Repeat)

→ 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 > Static Tab > Hostname to R3.
R3(config)# ip 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 ssh

↳ the connection with ssh can only be allowed.

We need RSA keys
R3(config
R3 (con
→ Generate R
R3 (con
How man
R3 (c
→ R3#
→ Configure
R3
R3
R3
Issue
→ Attempt
Go to P
as we have
→ Connect
R3#
R3#
→ Connect
Go to R

We need RSA keys because SSH used PEC 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 configuration)

→ 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 (Connect should fail)

as we have allowed ssh connect only.

→ Connect to R3 using SSH on PC-C

PC> ssh -l SSHadmin 192.168.3.1

password: ciscosshpa55

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: ciscosshpa55

R3# show ip ssh

R3# exit