Packet Tracer Final Commands

Part 1: Initialize Devices

Routers:

erase nvram or erase startup-config

reload

Switches:

erase startup-config

delete flash:vlan.dat

reload

show flash

Part 2: Configure Device Basic Settings

Step 1: Configure the Internet PC

Configure Internet PC:

IP Address: 209.165.200.230

Subnet Mask: 255.255.255.248

Default Gateway: 209.165.200.225

Step 2: Configure R1

no ip domain-lookup

hostname R1

enable secret class

password cisco

line vty 0 15 password cisco

login

service password-encryption

banner motd #Unauthorized Access is Prohibited!#

Interface S0/0/0:

int S0/0/0

description connects to R2 S0/0/0

ip address 172.16.12.1 255.255.255.252

clock rate 128000

no shutdown

ip route 0.0.0.0 0.0.0.0 S0/0/0

end

copy run start

Step 3: Configure R2:

banner motd #Unauthorized Access is Prohibited!#

Interface S0/0/0:

int S0/0/0

description connects to R1 S0/0/0

ip address 172.16.12.2 255.255.255.252

no shutdown

Interface S0/0/1:

int S0/0/1

description connects to R3 S0/0/1

ip address 172.16.23.1 255.255.255.252

clock rate 128000

no shutdown

Interface G0/0 (Simulated Internet):

int G0/0

description connects to internet

ip address 209.165.200.225 255.255.255.248

no shutdown

Interface Loopback 0 (Simulated Web Server):

description Connection to web server

ip address 10.10.10.1 255.255.255.0

no shut

exit

ip route 0.0.0.0 0.0.0.0 g0/0

end

copy run start

Step 4: Configure R3:

enable

config t

no ip domain-lookup

host R3

enable secret class

line con 0

password cisco

login

end

conf t

line vty 0 15

password cisco

end

conf t

service password-encrypion

end

conf t

banner motd #Unauthorized Access is Prohibited!#

int s0/0/1

description connects to R2

ip address 172.16.23.2 255.255.255.252

no sh

end

conf t

in Lo4

ip address 192.168.4.1 255.255.255.0

no sh

end

conf t

int Lo5

ip address 192.168.5.1 255.255.255.0

no sh

end

conf t

int Lo6

ip address 192.168.6.1 255.255.255.0

no sh

end

conf t

int s0/0/1

ip route 0.0.0.0 0.0.0.0 s0/0/1

end

Step 5: Configure S1:

enable

conf t

no ip domain-lookup

hostname S1

enable secret class

line con 0

password cisco

login

end

conf t

line vty 0 15

password cisco

login

end

conf t

service password-encryption

end

conf t

banner motd #Unauthorized Access is Prohibited!#

Step 6: Configure S3:

enable

conf t

no ip domain-lookup

hostname S3

enable secret class

line con 0

password cisco

login

end

conf t

line vty 0 15

password cisco

end

conf t

service password-encryption

end

conf t

banner motd #Unauthorized Access is Prohibited!#

Step 7: Verify network connectivity:

From R1: ping172.16.12.2

From R2: ping 172.16.23.2

Part 3: Configure Switch Security, VLANs, and Inter VLAN Routing:

Step 1: Configure S1:

vlan 31

name Accounting

vlan 33

name Engineering

vlan 99

name Management

exit

int vlan 99

ip address 192.168.99.2 255.255.255.0

no shutdown

exit

ip default-gateway 192.168.99.1

int f0/3

switchport mode trunk

switchport trunk native vlan 1

int f0/5

switchport mode trunk

switchport trunk native vlan 1

int range fa0/1-2, fa0/4, fa0/6-24, g0/1-2

switchport mode access

int fa0/6

switchport access vlan 31

int range fa0/1-2, fa0/4, fa0/7-24, g0/1-2

shutdown

Step 2: Configure S3:

vlan 31

name Accounting

vlan 33

name Engineering

vlan 99

name Management

exit

int vlan 99

ip address 192.168.99.3 255.255.255.0

no sh

exit

ip default-gateway 192.168.99.1

int f0/3

switchport mode trunk

switchport trunk native vlan 1

exit

interface range fa0/1-2, fa0/4-24, g0/1-2

switchport mode access

int f0/18

switchport mode access

switchport access vlan 33

interface range fa0/1-2, fa0/4-17, fa0/19-24, g0/1-2

shutdown

end

Step 3: Configure R1:

int g0/1.31

description Accounting LAN

encapsulation dot1q 31

ip address 192.168.31.1 255.255.255.0

int g0/1.33

description Engineering LAN

encapsulation dot1q 33

ip address 192.168.33.1 255.255.255.0

int g0/1.99

description Management LAN

encapsulation dot1q 99

ip address 192.168.99.1 255.255.255.0

exit

int g0/1

no shutdown

Step 4: Verify network connectivity:

From S1: ping 192.168.99.1

From S1: ping 192.168.31.1

From S3: ping 192.168.33.1

From S3: ping 192.168.99.1

Part 4: Configure OSPFv2 Dynamic Routing Protocol:

Step 1: Configure OSPFv2 on R1:

conf t

router ospf 1

router-id 1.1.1.1

network 172.16.12.0 0.0.0.3 area 0

network 192.168.31.0 0.0.0.255 area 0

network 192.168.33.0 0.0.0.255 area 0

network 192.168.99.0 0.0.0.255 area 0

passive-interface g0/1.31

passive-interface g0/1.33

passive-interface g0/1.99

auto-cost reference-bandwidth 1000

exit

int s0/0/0

bandwidth 128

ip ospf cost 7500

exit

Step 2: Configure OSPFv2 on R2:

conf t

router ospf 1

router-id 2.2.2.2

network 172.16.12.0 0.0.0.3 area 0

network 172.16.23.0 0.0.0.3 area 0

network 10.10.10.0 0.0.0.255 area 0

passive-interface g0/1

auto-cost reference-bandwidth 1000

int s0/0/0

bandwidth 128

int s0/0/1

bandwidth 128

int s0/0/0

ip ospf cost 7500

Step 3: Configure OSPFv2 on R3:

router ospf 1

router-id 3.3.3.3

network 172.16.23.0 0.0.0.3 area 0

network 192.168.4.0 0.0.3.255 area 0

passive-interface lo4

passive-interface lo5

passive-interface lo6

auto-cost reference-bandwidth 1000

exit

int s0/0/1

bandwidth 128

Step 4: Verify OSPF Information:

show ospf neighbor

show ip ospf interface

show ip protocols

show ip route ospf

show ip ospf interface

show run

Part 5: Implement DHCP and NAT for IPv4:

Step 1: Configure R1 as the DHCP server for VLANs 31 and 33:

ip dhcp excluded-address 192.168.31.1 192.168.31.20

ip dhcp excluded-address 192.168.33.1 192.168.33.20

ip dhcp pool ACCT

dns-server 10.10.10.11

ip domain-name ccna-sba.com

default-router 192.168.31.1

network 192.168.31.0 255.255.255.0

ip dhcp pool ENGNR

dns-server 10.10.10.11

ip domain-name ccna-sba.com

default-router 192.168.33.1

network 192.168.33.0 255.255.255.0

Step 2: Configure Static and Dynamic NAT on R2:

user webuser privilege 15 secret cisco12345

ip http authentication local

ip nat inside source static 10.10.10.10 209.165.200.229

int g0/0

ip nat outside

int g0/1

ip nat inside

end

conf t

access-list 1 permit 192.168.31.0 0.0.0.255

access-list 1 permit 192.168.33.0 0.0.0.255

access-list 1 permit 192.168.4.0 0.0.3.255

ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248

ip nat inside source list 1 pool INTERNET

Step 3: Verify DHCP and Static NAT:

On PC-A: show ip interface brief

On PC-C: show ip interface brief

From PC-A: ping <ip\_addr>

Use web browser, username: webuser, Password: cisco

Part 6: Configure and Verify Access Control Lists (ACLs):

Step 1: Restrict Access to VTY lines on R2:

ip access-list standard ADMIN-MGT

permit host 172.16.12.1

exit

line vty 0 4

access-class ADMIN-MGT in

Step 2: Secure Network from Internet Traffic:

access-list 101 permit tcp any host 209.165.200.229 eq www

access-list 101 permit icmp any any echo-reply

int g0/0

ip access-group 101 in

int s0/0/0

ip access-group 101 out

int s0/0/1

ip access-group 101 out

int g0/1

ip access-group 101 out

Step 3: Enter the appropriate CLI command needed to display the following:

show access-lists

show run

show ip nat translations

clear ip nat translations \*