CCNAv7 ENSA

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	S/0/0/0	10.67.254.2	255.255.255.0	N/A
	G0/0	192.168.1.1	255.255.255.0	N/A
	Tunnel 0	172.16.1.1	255.255.255.252	NA
R2	S0/0/1	10.67.253.2	255.255.255.252	N/A
	G0/0	10.10.1.1	255.255.255.0	N/A
	Tunnel 0	172.16.1.2	255.255.255.252	NA
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
S2	VLAN 1	10.10.1.2	255.255.255.0	10.10.1.1

Assessment Objectives

Part 1: Initialize, Reload and Configure Basic Device Settings

Part 2: Configure GRE tunnel

Part 3: Configure and Single Area OSPFv2

Part 4: Optimize Single Area OSPFv2

Part 5: Configure Access Control, NAT, and perform configuration backup

Scenario

In this Case Study (CS) you will configure the devices in a small network. You must configure a router, switch and PCs to support IPv4 connectivity for supported hosts. Your router and switch must also be managed securely. You will configure Single-Area OSPFv2, NAT, GRE, and access control lists. Further, you will backup up your working configurations to a TFTP server.

Required Resources

- Packet Tracer 8.0 or later

Instructions Part 1: Initialize, Reload and Configure Basic Device Settings

Step 1: Initialize and reload routers and switches.

Erase the startup configurations and VLANs from the router, switch, and reload the devices.

```
R1  Router#erase startup-config
R1  Router#reload
R2  Router#erase startup-config
R2  Router#reload
S1  Switch#delete vlan.dat
S1  Switch#erase startup-config
S1  Switch#reload
S2  Switch#delete vlan.dat
S2  Switch#erase startup-config
S2  Switch#reload
```

Step 2: Configure the routers.

Configuration tasks for **R1** and **R2** include the following:

Task	Specification
Disable DNS lookup	
Router name (case sensitive)	R1 or R2, as appropriate
Domain name (case sensitive)	ccna-lab.com
Encrypted privileged EXEC password (case sensitive)	ciscoenpass
Console access password (case sensitive)	ciscoconpass
Create a user with an encrypted password in the local database (case sensitive)	Username: **admin** Encrypted Password: **admin1pass**
Set login on VTY lines 0 to 4 to use local database	
Set VTY lines 0 to 4 to accept SSH connections only	
Encrypt the clear text passwords	
Configure an MOTD Banner (case sensitive)	Warning! Copying during test is Plagiarism.
Configure interface S0/0/0 – R1 Configure interface S0/0/1 – R2	Set the description Set the Layer 3 IPv4 address Activate Interface

Configure interface G0/0	Set the description Set the Layer 3 IPv4 address Activate Interface
Generate an RSA crypto key	1024 bits modulus
Configure default route to ISP	Use the exit interface

```
R1   Router>en
R1   Router#conf t
R1   Router(config)#no ip domain lookup
R1   Router(config)#hostname R1
R1   R1(config)#ip domain-name ccna-lab.com
R1   R1(config)#enable secret ciscoenpass
R1   R1(config)#line console 0
R1   R1(config-line)#password ciscoconpass
R1   R1(config-line)#login
R1   R1(config-line)#exit
R1   R1(config)#username admin secret admin1pass
R1   R1(config)#line vty 0 4
R1   R1(config-line)#login local
R1   R1(config-line)#transport input ssh
R1   R1(config-line)#exit
R1   R1(config)#service password-encryption
R1   R1(config)#banner motd "Warning! Copying during test is Plagiarism."
R1   R1(config)#int s0/0/0
R1   R1(config-if)#description Connection to R3
R1   R1(config-if)#ip address 10.67.254.2 255.255.255.0
R1   R1(config-if)#no shut
R1   R1(config-if)#int g0/0
R1   R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1   R1(config-if)#description Connection to S1
R1   R1(config-if)#no shut
R1   R1(config-if)#exit
R1   R1(config)#crypto key generate rsa
R1   R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
```

R2	Router>en
R2	Router#no ip domain lookup
R2	Router#conf t
R2	Router(config)#no ip domain lookup
R2	Router(config)#hostname R2
R2	R2(config)#ip domain-name ccna-lab.com
R2	R2(config)#enable secret ciscoenpass
R2	R2(config)#line console 0
R2	R2(config-line)#password ciscoconpass
R2	R2(config-line)#login
R2	R2(config-line)#exit
R2	R2(config)#username admin secret secret1pass
R2	R2(config)#line vty 0 4
R2	R2(config-line)#login local
R2	R2(config-line)#transport input ssh
R2	R2(config-line)#exit
R2	R2(config)#service password-encryption
R2	R2(config)#banner motd "Warning! Copying during test is Plagiarism."
R2	R2(config)#int s0/0/1
R2	R2(config-if)#ip address 10.67.253.2 255.255.255.252
R2	R2(config-if)#description Connection to A
R2	R2(config-if)#no shut
R2	R2(config-if)#int g0/0
R2	R2(config-if)#description Connection to S2
R2	R2(config-if)#ip address 10.10.1.1 255.255.255.0
R2	R2(config-if)#no shut
R2	R2(config-if)#exit
R2	R2(config)#crypto key generate rsa
R2	R2(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1

Step 3: Configure S1 and S2.

Configuration tasks for the switches include the following:

Task	Specification
Disable DNS lookup	
Switch name (case sensitive)	S1 or S2, as appropriate
Domain name (case sensitive)	ccna-lab.com
Encrypted privileged EXEC password (case sensitive)	ciscoenpass
Console access password (case sensitive)	ciscoconpass
Shutdown all unused interfaces	
Create a user with an encrypted password in the local database (case sensitive)	Username: **admin** Encrypted Password: **admin1pass**
Set login on VTY lines 0 to 15 to use local database	
Set all VTY lines to accept SSH connections only	
Encrypt the clear text passwords	
Configure an MOTD Banner (case sensitive)	Warning! Copying during test is Plagiarism.
Generate an RSA crypto key	1024 bits modulus
Configure Management Interface (SVI) for VLAN 1 (the Management VLAN)	Set the Layer 3 IPv4 address
Configure Default Gateway	

```
S1   Switch>en
S1   Switch#conf t
S1   Switch(config)#no ip domain lookup
S1   Switch(config)#hostname S1
S1   S1(config)#ip domain-name ccna-lab.com
S1   S1(config)#enable secret ciscoenpass
S1   S1(config)#line console 0
S1   S1(config-line)#password ciscoconpass
S1   S1(config-line)#login
```

S1	S1(config-line)#exit
S1	S1#sh ip interface br
S1	S1#conf t
S1	S1(config)#int range f0/3-24,g0/2
S1	S1(config-if-range)#shut
S1	S1(config-if-range)#exit
S1	S1(config)#username admin secret admin1pass
S1	S1(config)#line vty 0 15
S1	S1(config-line)#login local
S1	S1(config-line)#transport input ssh
S1	S1(config-line)#exit
S1	S1(config)#service password-encryption
S1	S1(config)#banner motd "Warning! Copying during test is Plagiarism."
S1	S1(config)#crypto key generate rsa
S1	S1(config)#interface vlan 1
S1	S1(config-if)#ip address 192.168.1.2 255.255.255.0
S1	S1(config-if)#no shut
S1	S1(config-if)#exit
S1	S1(config)#ip default-gateway 192.168.1.1
S2	Switch>en
S2	Switch#conf t
S2	Switch(config)#no ip domain lookup
S2	Switch(config)#hostname S2
S2	S2(config)#ip domain-name ccna-lab.com
S2	S2(config)#enable secret ciscoenpass
S2	S2(config)#line console 0
S2	S2(config-line)#password ciscoconpass
S2	S2(config-line)#login
S2	S2(config-line)#end
S2	S2#sh ip int br
S2	S2#conf t
S2	S2(config)#int range f0/2-24,g0/2
S2	S2(config-if-range)#shut
S2	S2(config-if-range)#exit
S2	S2(config)#username admin secret admin1pass
S2	S2(config)#line vty 0 15
S2	S2(config-line)#login local
S2	S2(config-line)#transport input ssh
S2	S2(config-line)#exit
S2	S2(config)#service password-encryption
S2	S2(config)#banner motd "Warning! Copying during test is Plagiarism."
S2	S2(config)#crypto key generate rsa
S2	S2(config)#interface vlan 1
S2	S2(config-if)#ip address 10.10.1.2 255.255.255.0
S2	S2(config-if)#no shut
S2	S2(config-if)#exit
S2	S2(config)#ip default-gateway 10.10.1.1

Part 2: Configure GRE tunnel

Step 1: Configure R1 and R2.

Configuration Tasks for **R1** and **R2** include the following:

Task	Specification
Configure the GRE tunnel interface Tunnel 0	Set the Layer 3 IPv4 address Set tunnel source and tunnel destination

```
R1   R1#conf t
R1   R1(config)#int tunnel 0
R1   R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1   R1(config-if)#tunnel source s0/0/0
R1   R1(config-if)#tunnel destination 10.67.253.2
R1   R1(config-if)#no shut
R2   R2#conf t
R2   R2(config)#int tunnel 0
R2   R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2   R2(config-if)#tunnel source s0/0/1
R2   R2(config-if)#tunnel destination 10.67.254.2
R2   R2(config-if)#no shut
```

Part 3: Configure Single Area OSPFv2

Configuration tasks for **R1** and **R2** include the following:

Task	Specification
Configure the OSPF routing process	Use process id 1
Manually configure the router id	Use 0.0.0.1 for R1 and 0.0.0.2 for R2
Task	**Specification**
Configure network statements	Use the network command to advertise local area (LAN) networks and use the wild card mask that matches each network’s subnet mask. **Note**: Ensure R1 and R2 is neighbored via the tunnel.

```
R1   R1(config)#router ospf 1
R1   R1(config-router)#router-id 0.0.0.1
R1   R1(config-router)#do sh ip route conn
R1   R1(config-router)#network 172.16.1.0 0.0.0.3 area 0
R1   R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R2   R2(config)#router ospf 1
R2   R2(config-router)#router-id 0.0.0.2
R2   R2(config-router)#do sh ip route conn
R2   R2(config-router)#network 10.10.1.0 0.0.0.255 area 0
R2   R2(config-router)#network 172.16.1.0 0.0.0.3 area 0
```

Part 4: Optimize Single-Area OSPFv2

Step 1: Configure R1 and R2.

Configuration Tasks for **R1** and **R2** include the following:

Task	Specification
Configure passive interfaces	Configure all interfaces that are not connected to an OSPF router.

```
R1   R1(config-router)#passive-interface g0/0
R1   R1(config-router)#passive-interface s0/0/0
R2   R2(config-router)#passive-interface g0/0
R2   R2(config-router)#passive-interface s0/0/1
```

Part 5: Configure Access Control, NAT, and perform configuration backup

Step 1: Configure NAT on R1.

Task	Specification
Create an ACL to identify hosts allowed to be translated	Create a numbered ACL 1 that matches the 192.168.1.0/24 network
Configure Port Address Translation on the outside interface of R1	Configure the NAT association between the ACL and the interface S0/0/0 so that it uses port address translation - PAT
Identify the interfaces involved in NAT	Specify the NAT inside or the NAT outside on the appropriate interfaces.

```
R1   R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
R1   R1(config)#ip nat inside source list 1 int s0/0/0 overload
R1   R1(config)#int g0/0
R1   R1(config-if)#ip nat inside
R1   R1(config)#int S0/0/0
R1   R1(config-if)#ip nat outside
```

Step 2: Configure NAT on R2.

Task	Specification
Create an ACL to identify hosts allowed to be translated	Create a numbered ACL 1 that matches the 10.10.1.0 network
Configure Port Address Translation on the outside interface of R2	Configure the NAT association between the ACL and the interface S0/0/1 so that it uses port address translation - PAT
Task	**Specification**
Identify the interfaces involved in NAT	Specify the NAT inside or the NAT outside on the appropriate interfaces.

```
R2   R2(config)#access-list 1 permit 10.10.1.0 0.0.0.255
R2   R2(config)#ip nat inside source list 1 int s0/0/1 overload
R2   R2(config)#int g0/0
R2   R2(config-if)#ip nat inside
R2   R2(config)#int s0/0/1
R2   R2(config-if)#ip nat outside
```

Step 3: Configure host computers.

Configure the host computers PC-A and PC-B with IPv4 addresses.

Description	PC-A	Backup	PC-B
IP Address	192.168.1.50	192.168.1.51	10.10.1.50
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
Default Gateway	192.168.1.1	192.168.1.1	10.10.1.1
DNS Server	209.165.201.2		209.165.201.2

Step 4: Test connectivity

Source	Target	Protocol	Expected Result
PC-A	PC-B	Ping	Success
PC-A	8.8.8.8	Ping	Success
PC-A	www.cisco.com	HTTP	Success
PC-B	8.8.8.8	Ping	Success

Step 5: Configure Access Control on R2.

Create and apply an access control list on R2 named **R2-SECURITY** to do the following:

Task	Specification
Create an access control list	**R2-SECURITY**(case sensitive)
Control HTTP and HTTPS specific traffic	The hosts from the 10.10.1.0/24 network are not allowed to reach the webserver at 209.165.201.2
Permit traffic	Allow all other traffic, regardless of protocol.
Apply the ACL	Filter traffic originating from R2(apply the best practice)

```
R2:
ip access-list extended R2-SECURITY
deny tcp 10.10.1.0 0.0.0.255 host 209.165.201.2 eq www
deny tcp 10.10.1.0 0.0.0.255 host 209.165.201.2 eq 443
permit ip any any

int g0/0
ip access-group R2-SECURITY in
```

After configuring and applying the ACL, perform the following tests:

Source	Target	Protocol	Expected Result
PC-A	PC-B	Ping	Success
PC-B	R1	SSH	Success
PC-B	www.cisco.com	HTTP	Failure

If you get different results, double-check your ACL configuration and application.

Step 6: Backup all device configurations.

Task	Specification
Using the Backup server on LAN A, backup the startup configuration of all of your devices to Backup server using the TFTP protocol	Use the following filename (case sensitive) when saving the configuration at the server. R1-confg R2-confg S1-confg S2-confg

R1	R1#copy running-config tftp	S1	S1#copy running-config tftp
R2	R2#copy running-config tftp	S2	S2#copy running-config tftp

Part 6: Save your Packet Tracer and upload to NetAcad

a. Save the configuration of each device in your Packet Tracer

b. Save the Packet Tracer file itself.

c. Upload to NetAcad. (***Upload only the Packet Tracer file***). ***DO NOT COMPRESS.***