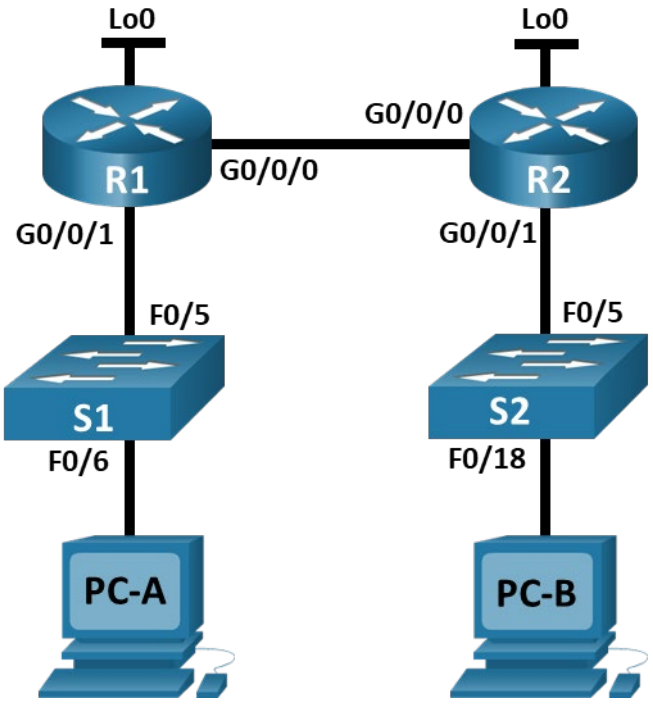
Case Study CCNA 3 – Enterprise Networking, Security and Automation

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0/0	10.67.254.2	255.255.255.252	N/A
	G0/0/1	192.168.1.1	255.255.255.0	N/A
	Lo0	10.52.0.1	255.255.255.248	N/A
R2	G0/0/0	10.67.254.1	255.255.255.252	N/A
	G0/0/1	10.67.1.1	255.255.255.0	N/A
	Lo0	209.165.201.1	255.255.255.224	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
S2	VLAN 1	10.67.1.2	255.255.255.0	10.67.1.1

Assessment Objectives

Part 1: Initialize, Reload and Configure Basic Device Settings

Part 2: Configure and verify Single Area OSPFv2

Part 3: Optimize Single Area OSPFv2

Part 4: Configure Access Control, NAT, and perform configuration backup

Scenario

In this Case Study 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, and access control lists. Further, you will backup up your working configurations to a TFTP server.

Required Resources

- 2 Routers (Cisco 4221 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable)
- 2 PCs (Windows with a terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

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 and switch and reload the devices.

Before proceeding, ask your instructor verify device initializations.

Step 2: Configure the routers.

Configuration tasks for R1 and R2 include the following:

Task	Specification
Disable DNS lookup	
Router name	R1 or R2, as appropriate
Domain name	ccna-lab.com
Encrypted privileged EXEC password	ciscoenpass
Console access password	ciscoconpass
Set the minimum length for passwords	10 characters
Create an administrative user in the local database	Username: **admin** Password: **admin1pass**
Set login on VTY lines to use local database	
Set VTY lines to accept SSH connections only	
Encrypt the clear text passwords	

Task	Specification
Int Configure interface G0/0/1	Set the Layer 3 IPv4 address Activate Interface
Configure interface G0/0/0	Set the Layer 3 IPv4 address Activate Interface
Configure interface Lo0	Configure IPv4 address
Generate an RSA crypto key	1024 bits modulus

Step 3: Configure S1 and S2.

Configuration tasks for the switches include the following:

Task	Specification
Disable DNS lookup	
Switch name	S1 or S2, as appropriate
Domain name	ccna-lab.com
Encrypted privileged EXEC password	ciscoenpass
Console access password	ciscoconpass
Shutdown all unused interfaces	
Create an administrative user in the local database	Username: **admin** Password: **admin1pass**
Set login on VTY lines to use local database	
Set VTY lines to accept SSH connections only	
Encrypt the clear text passwords	
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	

Part 2: 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	Configure a network statement for each locally attached network using a wild card mask that matches each network's subnet mask **Note**: R2 Lo0 network should not be included in the OSPF process.

Part 3: Optimize Single-Area OSPFv2

Step 1: Configure R1.

Configuration Tasks for R1 include the following:

Task	Specification
Configure passive interfaces	Configure all interfaces that are not directly connected to an OSPF neighbor to be passive
Configure the reference bandwidth	Adjust the reference bandwidth to 1 Gigabit
Configure Loopback 0 to report the mask it is configured with instead of a host mask	Configure Loopback0 as a point-to-point network for OSPF
Tune the timers for your network	Configure the hello time for 30 seconds

Step 2: Configure R2.

Configuration tasks for R2 include the following:

Task	Specification
Configure passive interfaces	Configure all interfaces that are not directly connected to an OSPF neighbor to be passive
Configure the reference bandwidth	Adjust the reference bandwidth to 1 Gigabit
Provide default routing for the OSPF domain	Configure a static default route with loopback 0 as the exit interface, then share the default information with other OSPF speakers
Tune the timers for your network	Configure the hello time for 30 seconds
Tune the DR/BDR election to favor R2	Set the OSPF priority for R2 to a value of 50

Part 4: Configure Access Control, NAT, and perform configuration backup

Step 1: Configure host computers.

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

Description	PC-A	PC-B
IP Address	192.168.1.50	10.67.1.50

Description	PC-A	PC-B
Subnet Mask	255.255.255.0	255.255.255.0
Default Gateway	192.168.1.1	10.67.1.1

After configuring each host computer, perform the following tests: (4 points)

Source	Target	Protocol	Expected Result
PC-A	PC-B	Ping	Success
PC-A	209.165.201.1	Ping	Success
PC-A	209.165.201.1	SSH	Success
PC-B	209.165.201.1	SSH	Success

If you get different results, troubleshoot your OSPF and host configurations.

Step 2: 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**
Control ICMP traffic	ICMP traffic from hosts on the 192.168.1.0/24 network is not allowed to the loopback on R2 (209.165.201).
Control SSH traffic	SSH is not allowed to the address 209.165.201.1
Permit traffic	All other traffic, regardless of protocol, is allowed
Apply the ACL	Filter traffic originating from R1

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

Source	Target	Protocol	Expected Result
PC-A	PC-B	Ping	Success
PC-A	209.165.201.1	Ping	Failure
PC-A	209.165.201.1	SSH	Failure
R1	209.165.201.1	Ping	Success
R1	209.165.201.1	SSH	Failure

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

Step 3: Configure NAT.

The decision has been made that the entire organization should be using addresses in the 10.0.0.0/8 network space. R1's LAN is out of compliance. There are applications and services running in the R1 LAN that cannot have their IP address changed without the entire system being rebuilt, so NAT is in order. Here are the configuration tasks at R1:

Task	Specification
Remove 192.168.1.0/24 from OSPF	Remove the appropriate network statement at R1
Create an ACL to identify hosts allowed to be translated	Create an ACL that matches the 192.168.1.0 network
Configure Port Address Translation on the outside interface of R1	Configure the NAT association between the ACL and the interface g0/0/0 so that it uses port address translation
Identify the interfaces involved in NAT	Specify inside or outside on the appropriate interfaces

Step 4: Backup all device configurations.

Task	Specification
Using the TFTP server on PC-B, backup the running configuration of all of your devices to PC-B using the TFTP protocol	

Instructor Sign-off Part:

Part 5: Cleanup

NOTE: DO NOT PROCEED WITH CLEANUP UNTIL YOUR INSTRUCTOR HAS GRADED YOUR SKILLS EXAM AND HAS INFORMED YOU THAT YOU MAY BEGIN CLEANUP.

Unless directed otherwise by the instructor, restore host computer network connectivity, and then turn off power to the host computers.

Before turning off power to the router and switch, remove the NVRAM configuration files (if saved) from both devices.

Disconnect and neatly put away all LAN cables that were used in the Final.

Router Interface Summary Table

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.