Cisco Lab

In this lab you will configure a small network to support IPv4 connectivity, switch security, inter VLAN routing, RIPv2 dynamic routing protocol and DHCP. You have five main tasks to achieve:

Task 1: Build the Network

Task 2: Configure Device Basic Settings

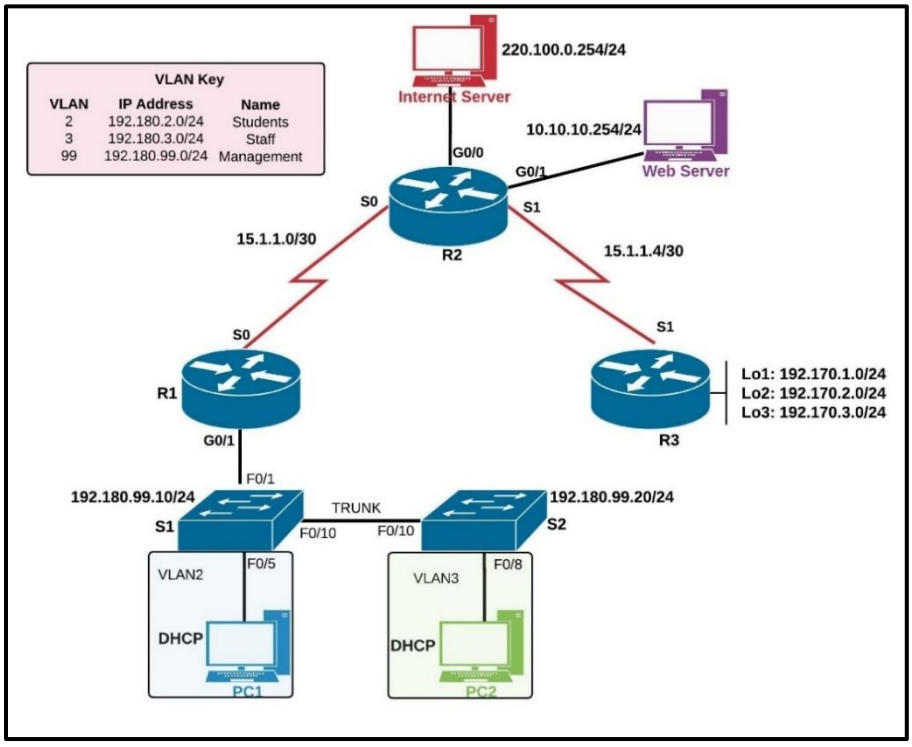
Task 3: Configure Switch Security, VLANs, and Inter-VLAN Routing

Task 4: Configure RIPv2 Dynamic Routing Protocol

Task 5: Configure DHCPv4

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

Network Topology



VLAN Table

VLAN	IP Address	Name
2	192.180.2.0 /24	Student
3	192.180.3.0 /24	Staff
99	192.180.99.0 /24	Management

IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	n/a	n/a	n/a
	S0/0/0	10.1.1.1	255.255.255.252	n/a
R2	G0/0	220.100.0.1	255.255.255.0	n/a
	G0/1	10.10.10.1	255.255.255.0	n/a
	S0/0/0	10.1.1.2	255.255.255.252	n/a
	S0/0/1	10.1.1.6	255.255.255.252	n/a
R3	S0/0/1	10.1.1.5	255.255.255.252	n/a
	Lo1	192.170.1.1	255.255.255.0	n/a
	Lo2	192.170.2.1	255.255.255.0	n/a
	Lo3	192.170.3.1	255.255.255.0	n/a
S1	VLAN 99	192.180.99.10	255.255.255.0	192.180.99.1
S2	VLAN 99	192.180.99.20	255.255.255.0	192.180.99.1
PC1	NIC	Via DHCP		
PC2	NIC	Via DHCP		

Part 1: Build the Network on Packet Tracer.

Part 2: Configure Device Basic Settings

Step 1: Configure R1.

Configuration tasks for R1 include the following:

Configuration Item or Task	Specification
Disable DNS lookup	
Router name	R1
Encrypted privileged exec password	class
Console access password	cisco
Telnet access password	cisco
Encrypt the clear text passwords	
MOTD banner	Unauthorized Access is Prohibited!
Interface S0/0/0	Set the description Set the IPv4 address. Refer to Topology diagram for address information. Set the clocking rate to 128000 Activate Interface
Default routes	Configure a default IPv4 route out S0/0/0.

Note: Do not configure G0/1 at this time.

Step 2: Configure R2.

Configuration tasks for R2 include the following:

Configuration Item or Task	Specification
Disable DNS lookup	
Router name	R2
Encrypted privileged exec password	class
Console access password	cisco
Telnet access password	cisco
Encrypt the clear text passwords	
MOTD banner	Unauthorized Access is Prohibited!
Interface S0/0/0	Set the description Set the IPv4 address from the IP address table. Activate Interface
Interface S0/0/1	Set the description Set the IPv4 address from the IP address table. Set clocking rate to 128000 Activate Interface
Interface G0/0	Set the Description Set the IPv4 address in the topology diagram. Activate Interface
Interface G0/1	Set the description. Set the IPv4 address in the topology diagram. Activate Interface
Default route	Configure a default IPv4 route out Interface G0/0.

Step 3: Configure R3.

Configuration tasks for R3 include the following:

Configuration Item or Task	Specification
Disable DNS lookup	
Router name	R3
Encrypted privileged exec password	class
Console access password	cisco
Telnet access password	cisco
Encrypt the clear text passwords	
MOTD banner	Unauthorized Access is Prohibited!
Interface S0/0/1	Set the description Set the IPv4 address from the IP address table. Activate Interface
Interface Loopback 10	Set the IPv4 address from the IP address table.
Interface Loopback 20	Set the IPv4 address from the IP address table.
Interface Loopback 30	Set the IPv4 address from the IP address table.
Default routes	Configure a default IPv4 route out S0/0/1

Step 4: Configure S1.

Configuration tasks for S1 include the following:

Configuration Item or Task	Specification
Disable DNS lookup	
Switch name	S1
Encrypted privileged exec password	class
Console access password	cisco
Telnet access password	cisco
Encrypt the clear text passwords	
MOTD banner	Unauthorized Access is Prohibited!

Step 5: Configure S2

Configuration tasks for S2 include the following:

Configuration Item or Task	Specification
Disable DNS lookup	
Switch name	S2
Encrypted privileged exec password	class
Console access password	cisco
Telnet access password	cisco
Encrypt the clear text passwords	
MOTD banner	Unauthorized Access is Prohibited!

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

Step 1: Configure S1.

Configuration tasks for S1 include the following:

Configuration Item or Task	Specification
Create the VLAN database	Use Topology VLAN table to create and name each of the listed VLANS.
Assign the management IP address.	Assign the IPv4 address to the Management VLAN.
Assign the default-gateway	Assign the first IPv4 address in the Management subnet as the default-gateway.
Force trunking on Interface F0/10	Use VLAN 1 as the native VLAN.
Force trunking on Interface F0/1	Use VLAN 1 as the native VLAN.
Configure all other ports as access ports	Use the interface range command.
Assign F0/5 to VLAN 2	
Shutdown all unused ports	

Step 2: Configure S2.

Configuration tasks for S2 include the following:

Configuration Item or Task	Specification
Create the VLAN database	Use Topology VLAN Table to create each of the listed VLANS. Name each VLAN.
Assign the management IP address	Assign the IPv4 address to the Management VLAN.
Assign the default-gateway	Assign the first IP address in the Management subnet as the default-gateway.
Force trunking on Interface F0/10	Use VLAN 1 as the native VLAN.
Configure all other ports as access ports	Use the interface range command.
Assign F0/8 to VLAN 3	
Shutdown all unused ports	

Step 3: Configure R1.

Configuration tasks for R1 include the following:

Configuration Item or Task	Specification
Configure 802.1Q subinterface .2 on G0/1	Description Students LAN Assign VLAN 2. Assign the first available address to this interface.
Configure 802.1Q subinterface .3 on G0/1	Description Staff LAN Assign VLAN 3. Assign the first available address to this interface.
Configure 802.1Q subinterface .99 on G0/1	Description Management LAN Assign VLAN 99. Assign the first available address to this interface.
Activate Interface F0/1	

Step 4: Verify network connectivity.

Use the **ping** command to test connectivity between the switches and R1.

Use the following table to methodically verify connectivity with each network device. Take corrective action to establish connectivity if a test fails:

From	To	IP Address	Ping Results Snapshot
S1	R1, VLAN 99 address		
S2	R1, VLAN 99 address		
S1	R1, VLAN 2 address		
S2	R1, VLAN 3 address		

Part 4: Configure RIPv2 Dynamic Routing Protocol

Step 1: Configure RIPv2 on R1.

Configuration tasks for R1 include the following:

Configuration Item or Task
Configure RIP Version 2
Advertise all directly connected Networks
Set all LAN interfaces as passive
Disable automatic summarization

Step 2: Configure RIPv2 on R2.

Configuration tasks for R2 include the following:

Configuration Item or Task
Configure RIP Version 2
Advertise all directly connected Networks
Set the Ethernet interfaces as passive
Disable automatic summarization

Step 3: Configure RIPv2 on R3.

Configuration tasks for R3 include the following:

Configuration Item or Task
Configure RIP Version 2
Advertise all directly connected IPv4 Networks
Set all IPv4 LAN (Loopback) interfaces as passive
Disable automatic summarization

Step 4: Verify RIP information.

Verify that RIP is functioning as expected. Enter the appropriate CLI command to discover the following information:

Question	Student Answer
What command displays the RIP Process ID, Router ID, Routing Networks, and passive interfaces configured on a router?	
What command displays only RIP routes?	
What command displays the RIP section of the running-configuration?	

Part 5: Configure Dynamic Host Configuration Protocol (DHCP)

Step 1: Configure R1 as the DHCP server for VLANs 2 and 3.

Configuration Item or Task on R1	Specification
Reserve the first 10 IP addresses in VLAN 2 for static configurations	
Reserve the first 10 IP addresses in VLAN 3 for static configurations	
Create a DHCP pool for VLAN 2	Name: STUDENTS Network: VLAN 2 Network DNS-Server: 10.10.10.10 Set the default gateway.
Create a DHCP pool for VLAN 3	Name: STAFF Network: VLAN 3 Network DNS-Server: 10.10.10.10 Set the default gateway.

Step 2: Verify PCs received IPs from DHCP server.

You may need to type ipconfig /renew to force PCs to acquire IPs from DHCP servers

Configuration Task	Specification	Acquired IP Snapshot
Verify PC1 received an IP from DHCP server	Type ipconfig in a command prompt, and provide the acquired IP	
Verify PC2 received an IP from DHCP server	Type ipconfig in a command prompt, and provide the acquired IP	

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

Step 1: Restrict access to VTY lines on R2.

Configuration Item or Task	Specification
Configure a named access list to only allow R1 to telnet to R2	ACL Name: **SECURE**
Apply the named ACL to the VTY lines	
Allow only telnet access to VTY lines	
Verify ACL is working as expected	Report how you verified.

Step 2: Enter the appropriate CLI command needed to display the following:

Command Description	Student Input (command)
Display the matches an access-list has received since the last reset.	
Reset access-list counters.	
What command is used to display what ACL is applied to an interface and the direction that it is applied?	

*****