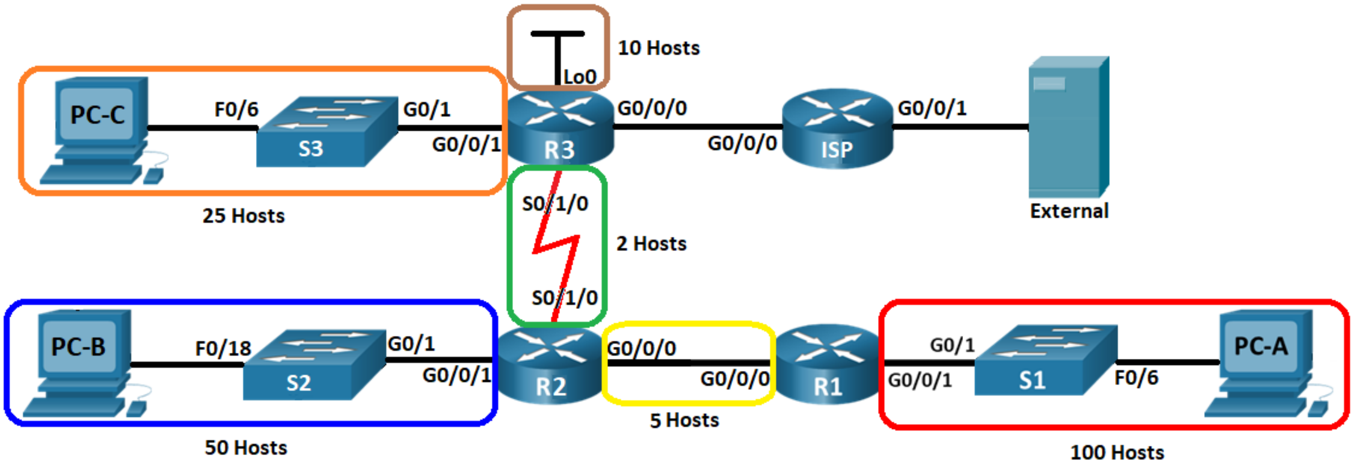
RED RIVER COLLEGE
OF APPLIED ARTS, SCIENCE AND TECHNOLOGY

NTWK-1010 Final Project

Topology



Addressing Table

Device	Interface	IP Address / Prefix	Default Gateway	Comments
R1	G0/0/0	192.168.0.241/29 2001:db8:acad:c::1/64 fe80::1	N/A	First Host
	G0/0/1	192.168.0.1/25 2001:db8:acad:a::1/64 fe80::1	N/A	First Host
R2	G0/0/0	192.168.0.242/29 2001:db8:acad:c::2/64 fe80::2	N/A	Second Host
	G0/0/1	192.168.0.130/26 2001:db8:acad:b::1/64 fe80::1	N/A	First Host
	S0/1/0	192.168.0.249/30 2001:db8:acad:e::1/64 fe80::1	N/A	First Host

R3	G0/0/0	64.100.0.2/30	N/A	Connection to ISP
		2001:db8:acad::2/64		
		fe80::2		
	G0/0/1	192.168.0.193/27	N/A	First Host
		2001:db8:acad:1::1/64		
		fe80::1		
	S0/1/0	192.168.0.250/30	N/A	Second Host
		2001:db8:acad:e::2/64		
		fe80::2		
	Lo0	192.168.0.238/28	N/A	Last Host
ISP	G0/0/0	64.100.0.1/30	N/A	Connection to R3
		2001:db8:acad::1/64		
		fe80::1		
	G0/0/1	209.165.200.225/27	N/A	Connection to External
		2001:db8:acad:200::225/64		
		fe80::225		
S1	VLAN 1	192.168.0.3/25	192.168.0.1	Third Host
S2	VLAN 1	192.168.0.132/26	192.168.0.130	Third Host
S3	VLAN 1	192.168.0.195/27	192.168.0.193	Third Host
PC-A	NIC	192.168.0.4/25	192.168.0.1	Fourth Host
		2001:db8:acad:a::4/64	fe80::1	
PC-B	NIC	192.168.0.133/26	192.168.0.130	Fourth Host
		2001:db8:acad:b::4/64	fe80::1	
PC-C	NIC	192.168.0.196/27	192.168.0.193	Fourth Host
		2001:db8:acad:1::10/64	fe80::1	
External	NIC	209.165.200.226/27	209.165.200.225	Connection to ISP
		2001:db8:acad:200::226/64	fe80::225	

Required Resources

- Laptop installed with Windows 10 or Mac OSX and connection to the Internet
- Packet Tracer version 8.0 or later
- Lab and Final Project Template.pka file to build the project in packet tracer

Scenario

In this project you are assuming the role of a junior network administrator tasked with designing and implementing a VLSM IP addressing scheme to support the host requirements outlined in the topology above. Once all intermediary and end devices (except ISP and External server) have updated IPv4 addressing, static route commands will be given to provide end-to-end IPv4 and IPv6 connectivity between LANs and the External server. Third-party vulnerability scans have discovered certain intermediary devices do not meet security best practices and will require modification. Finally you will demonstrate secure remote management access to all intermediary devices, display information using common CLI commands and answer theory questions during final project sign off with your instructor.

Objectives

Part 1: Label and Cable

Part 2: Develop and Implement VLSM IP Addressing Scheme

Part 3: Configure IP Routing

Part 4: Update Network Security Configuration

Part 5: Test and Verify IPv4 and IPv6 End-to-End Connectivity

Part 6: Use the CLI to Gather Information

Part 7: Theory Questions

Instructions

Note: Figures are included at the Appendix of this document.

Part 1: Label and Cable

Step 1: Modify the Existing Topology

a. Save a copy of your latest Lab and Final Project Template.pka and rename to Final Project.pka

b. Open Final Project.pka

c. From the physical tab on R2 and R3, drag a NIM-2T module in an empty expansion slot on R2 and R3 (*see Figure.1*)

   Note: Be sure to power down the router by clicking the power button before dragging in the expansion module. After module is installed power on the router.

d. Connect a serial DTE cable between R2 and R3 on S0/1/0 interfaces (*see Figure.2*)

Part 2: Develop and Implement VLSM IP Addressing Scheme

a. Cross reference the **LAN Addressing Table** from the midterm project to use as the original network address for your VLSM design.

   (e.g. If Laptop IPv4 Address: 1**92.168.100.127** and Subnet Mask: **255.255.255.0** then final project original network address = **192.168.100.0/24**)

   Note: If your home network subnet mask is not **255.255.255.0** please contact your instructor for design changes.

Step 1: Calculate subnet information

a. Calculate your subnets starting with the largest to smallest host requirement.

b. Fill out the table below with your calculated subnets:

Note: The network address is the first IP in a subnet and is **not** usable by a host.

Subnet Description	Number of Hosts Needed	Network Address /Prefix	First Host Address	Broadcast Address
R1 LAN	100	25	192.168.0.1	192.168.0.128
R2 LAN	50	26	192.168.0.130	192.168.0.191
R3 LAN	25	27	192.168.0.193	192.168.0.223
R3 Loopback0 (Future Expansion)	10	28	192.168.225	192.168.0.239
R1 to R2 Link	5	29	192.168.0.241	192.168.0.247
R2 to R3 Link	2	30	192.168.0.249	192.168.0.251

c. Fill out all blank spaces in the Addressing Table.

Note: The comments column indicates what host IP to assign to each device.

Step 2: Configure devices with new IP scheme

a. Configure R2 and R3 S0/1/0 interfaces with IPv6 addressing provided in the Addressing Table.

b. Modify IPv4 address, subnet mask and default gateway (where applicable) on all intermediary and end device interfaces (except ISP and External) by referencing the completed Addressing Table.

Console password: **ciscoCON1@3$**
Priv Exec password: **ciscoPRIV1@3$**

Note: To remove old loopback interfaces on R2, prefix 'no' before each interface in global config mode (e.g. `R2(config)#no interface loopback0`)

Part 3: Configure IP Routing

Note: The **bold red text** below will need to be modified to match the first three octets of your original home network address.

Step 1: Configure static routes on R1

a. From global config mode on R1, configure the following default static routes to forward any destination IPv4 or IPv6 address not apart of it's routing table toward R2 via next-hop IP.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.100.242
R1(config)#ipv6 route ::/0 2001:db8:acad:c::2
```

Step 2: Configure static routes on R2

a. From global config mode on R2, configure the following default static routes to forward any destination IPv4 or IPv6 address not a part the routing table toward R3 via next-hop IP.

```
R2(config)#ip route 0.0.0.0 0.0.0.0 192.168.100.250
R2(config)#ipv6 route ::/0 2001:db8:acad:e::2
```

b. From global config mode on R2, configure the following static routes to forward R1 LAN destination IPv4 or IPv6 address toward R1 via next-hop IP.

```
R2(config)#ip route 192.168.100.0 255.255.255.128 192.168.100.241
R2(config)#ipv6 route 2001:db8:acad:a::/64 2001:db8:acad:c::1
```

Step 3: Configure static routes on R3

a. From global config mode on R3, configure the following static routes to forward R1 and R2 LAN destination IPv4 or IPv6 address toward R2 via next-hop IP.

```
R3(config)#ip route 192.168.100.0 255.255.255.128 192.168.100.249
R3(config)#ip route 192.168.100.128 255.255.255.192 192.168.100.249
R3(config)#ipv6 route 2001:db8:acad:a::/64 2001:db8:acad:e::1
R3(config)#ipv6 route 2001:db8:acad:b::/64 2001:db8:acad:e::1
R3(config)#ipv6 route 2001:db8:acad:c::/64 2001:db8:acad:e::1
```

Step 4: Modify NAT configuration on R3

a. To provide IPv4 access to the external server, network address translation (NAT) needs to be modified with the following commands on R3.

```
R3(config)no access-list 1 permit 192.168.1.0 0.0.0.255
R3(config)access-list 1 permit 192.168.100.0 0.0.0.255
R3(config)interface s0/1/0
R3(config-if)ip nat inside
```

Part 4: Update Network Security Configuration

Step 1: Configure basic security measures on R3 and S3

a. Enter a login message to warn about unauthorized access and to contact your academic email for access.

b. Encrypt all clear-text passwords.

c. Change the passwords:

1) Set the privileged exec password to **ciscoPRIV1@3$**

2) Set the console password to **ciscoCON1@3$**

d. Both R3 and S3 should only accept SSH connections (disable telnet):

1) Configure the username **SSHadmin** with an encrypted password of **ciscoSSH1@3$**

2) Users should be disconnected after 5 minutes of inactivity.

3) SSH version 2 should be used.

e. Disable all unused switchports on S3

Step 2: Configure additional security measures on R3

a. Configure R3 to require a minimum 12-character password.

b. R3 should not allow SSH logins for 2 minutes if 3 failed login attempts occur within 1 minute.

Part 5: Test and Verify IPv4 and IPv6 End-to-End Connectivity

Use the ICMP and SSH protocols to test IPv4 and IPv6 connectivity between network devices.

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

From	To	Protocol	IP Address	Result	Points
PC-A	R1 G0/0/1	IPv4	192.168.0.1	Successful	2 points
		IPv6	*2001:db8:acad:a::1*	Successful	1 point
	R1 G0/0/0	IPv4	192.168.0.241	Successful	2 points
		IPv6	*2001:db8:acad:c::1*	Successful	1 point
	S2 VLAN 1	IPv4	192.168.0.132	Successful	2 points
PC-B	R2 G0/0/1	IPv4	192.168.0.130	Successful	2 points
		IPv6	*2001:db8:acad:b::1*	Successful	1 point
	R2 G0/0/0	IPv4	192.168.0.242	Successful	2 points
		IPv6	*2001:db8:acad:c::2*	Successful	1 point
	R2 S0/1/0	IPv4	192.168.0.249	Successful	2 points
		IPv6	*2001:db8:acad:e::1*	Successful	1 point
	S1 VLAN 1	IPv4	192.168.0.3	Successful	2 points
PC-C	R3 G0/0/1	SSH	192.168.0.193	Successful	4 points
		IPv6	*2001:db8:acad:1::1*	Successful	1 point
	R3 S0/1/0	IPv4	192.168.0.250	Successful	2 points
		IPv6	*2001:db8:acad:e::2*	Successful	1 point
	R3 Lo0	IPv4	192.168.0.238	Successful	3 points
	PC-A	IPv4	192.168.0.4	Successful	2 points
		IPv6	*2001:db8:acad:a::4*	Unsuccessful	1 point
	PC-B	IPv4	192.168.0.133	Successful	2 points
		IPv6	*2001:db8:acad:b::4*	Unsuccessful	1 point
	S3 VLAN 1	SSH	192.168.0.195	Successful	4 points
	External	IPv4	*209.165.200.226*	Unsuccessful	2 points
		IPv6	*2001:db8:acad:200::226*	Unsuccessful	2 points

Console Password: **ciscoCON1@3$**
Priv Exec Password: **ciscoPRIV1@3$**
SSH credentials: username: **SSHadmin** password: **ciscoSSH1@3$**

Note: To achieve full points for SSH, banner MOTD must be displayed and access to priv exec mode.

Total Points for Part 5

_____/44

Part 6: Use the CLI to Gather Information

Step 1: Issue the appropriate CLI command need to display the following on S3:

Description	Command	Points
Switch Model	show version	1 point
Total Flash Memory	show flash	1 point
Configuration Register	show version	1 point

Step 2: Enter the appropriate CLI command needed to display the following on R3:

Command Description	Command	Points
Display the IPv6 routing table.	show ipv6 route	1 point
Display information about the intermediary devices connected to R3. Information should include Device ID, Local Interface, Hold time, Capability, Platform, and Port ID.	show cdp neighbor	1 point
Display logging information on the terminal (vty) lines	show logging	1 point
Monitor the status of ICMP messages on a cisco router with debugging	debug ip icmp	1 point

Step 3: Enter the appropriate CLI command needed to display the following on PC-C:

Command Description	Command	Points
Display the number of hops required to a reach a destination IP address	tracert <destination IP address>	1 point
Display a domain-name associated to an IP address and vice versa	nslookup <ip address/domain name>	1 point
Display PC-C host routing table	netstat -r	1 point

Total Points for Part 6

_____/10

Part 7: Theory Questions:

During the Final Project sign off, your instructor may ask questions on the following topics:

Broadcast domain boundaries

Packet and segment header fields

Application layer protocols

TCP and UDP well known application port numbers

Types of IPv4 and IPv6 addresses

Number of host and network bits in a IPv4 or IPv6 address given the prefix

DNS hierarchy

Troubleshooting commands (ping, tracert, nslookup, etc)

Part 8: Cleanup

Online Delivery:

Save your and upload Final Project.pka file to LEARN dropbox.

Contact your instructor for Final Project sign off.

Appendix

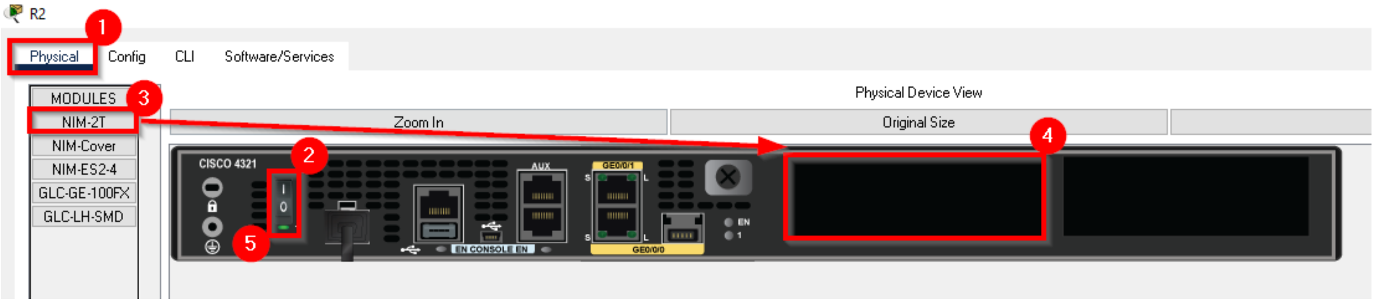


Figure 1

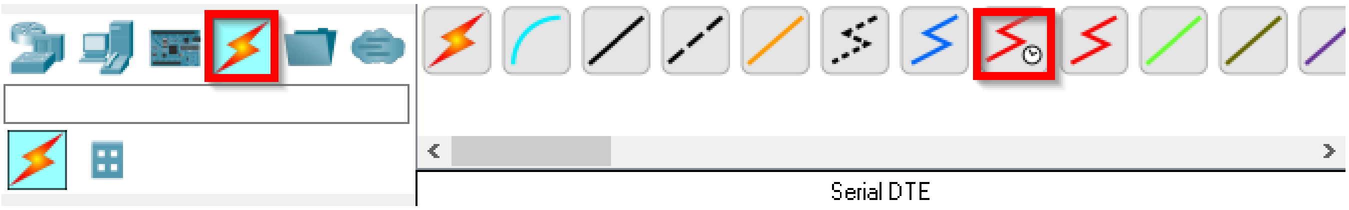


Figure 2

Last revised July 2021