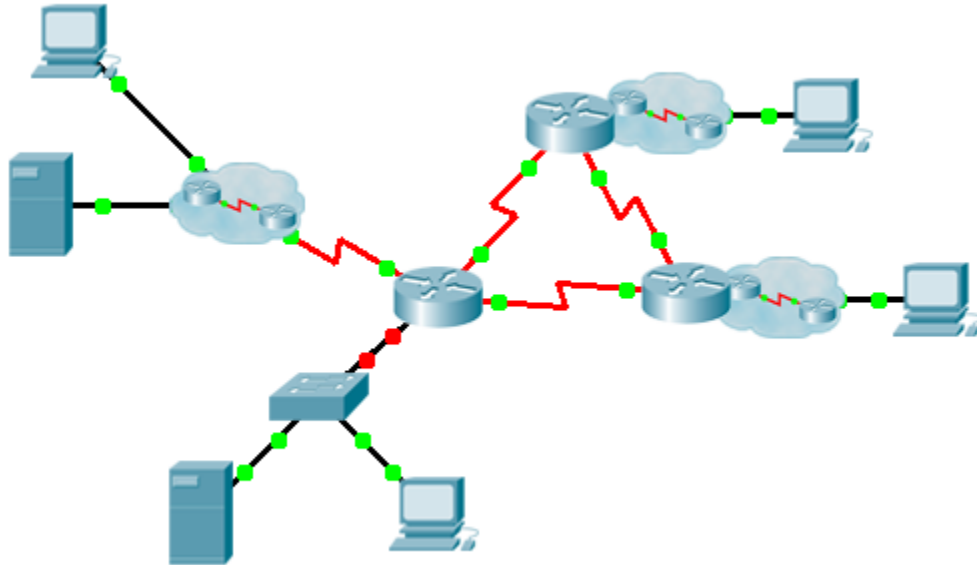# Packet Tracer – Skills Integration Challenge (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Download PacketTracer file: 10.4.1.1 Packet Tracer - Skills Integration Challenge

Topology

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
[[R1Name]]	G0/0.15	[[R1G0sub15Add]]	[[R1G0sub15SM]]	N/A
	G0/0.30	[[R1G0sub30Add]]	[[R1G0sub30SM]]	N/A
	G0/0.45	[[R1G0sub45Add]]	[[R1G0sub45SM]]	N/A
	G0/0.60	[[R1G0sub60Add]]	[[R1G0sub60SM]]	N/A
	S0/0/0	[[R1S000Add]]	255.255.255.252	N/A
	S0/0/1	[[R1S001Add]]	255.255.255.252	N/A
	S0/1/0	[[R1S010Add]]	255.255.255.252	N/A
[[R2Name]]	G0/0	[[R2G00Add]]	[[R2R3LanSM]]	N/A
	S0/0/0	[[R2S000Add]]	255.255.255.252	N/A
	S0/0/1	[[R2S001Add]]	255.255.255.252	N/A
[[R3Name]]	G0/0	[[R3G00Add]]	[[R2R3LanSM]]	N/A
	S0/0/0	[[R3S000Add]]	255.255.255.252	N/A
	S0/0/1	[[R3S001Add]]	255.255.255.252	N/A
[[S1Name]]	VLAN 60	[[S1VLAN60Add]]	[[R1G0sub60SM]]	[[R1G0sub60Add]]
[[PC1Name]]	NIC	DHCP Assigned	DHCP Assigned	DHCP Assigned

VLANs and Port Assignments Table

VLAN Number - Name	Port assignment	Network
15 - Servers	F0/11 - F0/20	[[R1-VLANsrvNet]]
30 - PCs	F0/1 - F0/10	[[R1-VLANpcNet]]
45 - Native	G0/1	[[R1-VLANntvNet]]
60 - Management	VLAN 60	[[R1-VLANmanNet]]

Scenario

This culminating activity includes many of the skills that you have acquired during this course. First, you will complete the documentation for the network. So make sure you have a printed version of the instructions. During implementation, you will configure VLANs, trunking, port security and SSH remote access on a switch. Then, you will implement inter-VLAN routing, DHCP, RIPv2, default routing, and NAT on a router. Finally, you will use your documentation to verify your implementation by testing end-to-end connectivity.

Documentation

You are required to fully document the network. You will need a print out of this instruction set, which will include an unlabeled topology diagram:

- Label all the device names, network addresses and other important information that Packet Tracer generated.
- Complete the **Addressing Table** and **VLANs and Port Assignments Table**.
- Fill in any blanks in the **Implementation** and **Verification** steps. The information is supplied when you launch the Packet Tracer activity.

Implementation

Note: All devices in the topology except **[[R1Name]]**, **[[S1Name]]**, and **[[PC1Name]]** are fully configured. You do not have access to the other routers. You can access all the servers and PCs for testing purposes.

Implement to following requirements using your documentation:

[[S1Name]]

- Configure remote management access including IP addressing and SSH:
  - Domain is cisco.com
  - User **[[UserText]]** with password **[[UserPass]]**
  - Crypto key length of 1024
  - SSH version 2, limited to 2 authentication attempts and a 60 second timeout
  - Clear text passwords should be encrypted.
- Configure, name and assign VLANs. Ports should be manually configured as access ports.
- Configure trunking.
- Implement port security:
  - On F0/1, allow 2 MAC addresses that are automatically added to the configuration file when detected. The port should not be disabled, but a syslog message should be captured if a violation occurs.
  - Disable all other unused ports.
- Configure VTY lines to be accessible via SSH only

[[R1Name]]

- Configure inter-VLAN routing.
- Configure DHCP services for VLAN 30. Use **LAN** as the case-sensitive name for the pool.
- Implement routing:
  - Use RIP version 2
  - Disable automatic summarization
  - Configure one network statement for the entire **[[DisplayNet]]** address space
  - Configure a default route to the Internet.
- Implement NAT:
  - Configure a standard, one statement ACL number 1. All IP addresses belonging to the **[[DisplayNet]]** address space are allowed.
  - Refer to your documentation and configure static NAT for the File Server.
  - Configure dynamic NAT with PAT using a pool name of your choice, a /30 mask, and these two public addresses:
    - **[[NATPoolText]]**
  - Bind the NAT pool to ACL 1 and configure PAT. Packet Tracer does not grade this command.

- Activate NAT on all appropriate interfaces.

[[PC1Name]]

Verify **[[PC1Name]]** has received full addressing information from **[[R1Name]]**.

Verification

All devices should now be able to ping all other devices. If not, troubleshoot your configurations to isolate and solve problems. A few tests include:

- Verify remote access to **[[S1Name]]** by using SSH from a PC.
- Verify VLANs are assigned to appropriate ports and port security is in force.
- Verify OSPF neighbors and a complete routing table.
- Verify NAT translations and statics.
  - **Outside Host** should be able to access **File Server** at the public address.
  - Inside PCs should be able to access **Web Server**.

Suggested Scoring Rubric

Packet Tracer scores 70 points. Documentation is worth 30 points.

ID:[[indexAdds]][[indexNames]]

```
**************************************************
ISOMORPH ID KEY:
ID = XY where;
 X = indexAdds for /24 private address space
 Y = indexNAMES for device names
Note: Each seed contains variables that are independent
of the other seeds. You do not need to test all the
various combinations.
==================================================
ISOMORPH ID = 00
==================================================
!HQ!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
en
conf t
ip dhcp pool LAN
 network 172.16.15.32 255.255.255.224
 default-router 172.16.15.33
interface GigabitEthernet0/0
 no shutdown
interface GigabitEthernet0/0.15
 encapsulation dot1Q 15
 ip address 172.16.15.17 255.255.255.240
 ip nat inside
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 172.16.15.33 255.255.255.224
```

```
 ip nat inside
interface GigabitEthernet0/0.45
 encapsulation dot1Q 45 native
 ip address 172.16.15.1 255.255.255.248
interface GigabitEthernet0/0.60
 encapsulation dot1Q 60
 ip address 172.16.15.9 255.255.255.248
router rip
 version 2
 no auto-summary
 network 172.16.0.0
!
ip nat pool TEST 209.165.200.225 209.165.200.226 netmask 255.255.255.252
ip nat inside source list 1 pool TEST overload
ip nat inside source static 172.16.15.18 209.165.200.227
ip route 0.0.0.0 0.0.0.0 Serial0/1/0
access-list 1 permit 172.16.0.0 0.0.255.255
interface s0/0/0
 ip nat inside
interface s0/0/1
 ip nat inside
interface s0/1/0
 ip nat outside
end
wr
!!!!!!!!!!!!!!!!!!!!!!
!HQ-Sw!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!
en
conf t
int vlan 60
ip add 172.16.15.10 255.255.255.248
no shut
ip default-gateway 172.16.15.9
vlan 15
name Servers
vlan 30
name PCs
vlan 45
name Native
vlan 60
name Management
interface range fa0/1 - 10
switchport mode access
switchport access vlan 30
interface fa0/1
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
```

```
switchport port-security violation restrict
interface range fa0/11 - 20
switchport mode access
switchport access vlan 15
interface g0/1
switchport mode trunk
switchport trunk native vlan 45
interface range fa0/21 - 24 , g0/2
shutdown
ip domain-name cisco.com
crypto key gen rsa
1024

user HQadmin pass ciscoclass
service password-encryption
ip ssh version 2
ip ssh auth 2
ip ssh time 60
line vty 0 15
login local
transport input ssh


========================================================
ISOMORPH ID = 11
========================================================
!Admin!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
en
conf t
ip dhcp pool LAN
 network 10.10.10.192 255.255.255.192
 default-router 10.10.10.193
interface GigabitEthernet0/0
 no shutdown
interface GigabitEthernet0/0.15
 encapsulation dot1Q 15
 ip address 10.10.10.161 255.255.255.224
 ip nat inside
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 10.10.10.193 255.255.255.192
 ip nat inside
interface GigabitEthernet0/0.45
 encapsulation dot1Q 45 native
 ip address 10.10.10.129 255.255.255.240
interface GigabitEthernet0/0.60
 encapsulation dot1Q 60
 ip address 10.10.10.145 255.255.255.240
router rip
 version 2
```

```
 no auto-summary
 network 10.0.0.0
!
interface s0/0/0
 ip nat inside
interface s0/0/1
 ip nat inside
interface s0/1/0
 ip nat outside
!
ip nat pool TEST 198.133.219.128 198.133.219.129 netmask 255.255.255.252
ip nat inside source list 1 pool TEST overload
ip nat inside source static 10.10.10.162 198.133.219.130
ip route 0.0.0.0 0.0.0.0 Serial0/1/0
access-list 1 permit 10.0.0.0 0.255.255.255
end
wr
!!!!!!!!!!!!!!!!!!!!!!!!
!Admin-Sw!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
en
conf t
int vlan 60
ip add 10.10.10.146 255.255.255.240
no shut
ip default-gateway 10.10.10.145
vlan 15
name Servers
vlan 30
name PCs
vlan 45
name Native
vlan 60
name Management
interface range fa0/1 - 10
switchport mode access
switchport access vlan 30
interface fa0/1
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
interface range fa0/11 - 20
switchport mode access
switchport access vlan 15
interface g0/1
switchport mode trunk
switchport trunk native vlan 45
interface range fa0/21 - 24 , g0/2
shutdown
```

```
ip domain-name cisco.com
crypto key gen rsa
1024

user Admin pass letmein
service password-encryption
ip ssh version 2
ip ssh auth 2
ip ssh time 60
line vty 0 15
login local
transport input ssh


=============================================================
ISOMORPH ID: 22
=============================================================
!Central!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
en
conf t
ip dhcp pool LAN
 network 192.168.45.128 255.255.255.192
 default-router 192.168.45.129
interface GigabitEthernet0/0
 no shutdown
interface GigabitEthernet0/0.15
 encapsulation dot1Q 15
 ip address 192.168.45.65 255.255.255.192
 ip nat inside
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.45.129 255.255.255.192
 ip nat inside
interface GigabitEthernet0/0.45
 encapsulation dot1Q 45 native
 ip address 192.168.45.17 255.255.255.240
interface GigabitEthernet0/0.60
 encapsulation dot1Q 60
 ip address 192.168.45.33 255.255.255.240
router rip
 version 2
 no auto-summary
 network 192.168.45.0
!
interface s0/0/0
 ip nat inside
interface s0/0/1
 ip nat inside
interface s0/1/0
 ip nat outside
```

```
!
ip nat pool TEST 64.100.32.56 64.100.32.57 netmask 255.255.255.252
ip nat inside source list 1 pool TEST overload
ip nat inside source static 192.168.45.66 64.100.32.58
ip route 0.0.0.0 0.0.0.0 Serial0/1/0
access-list 1 permit 192.168.45.0 0.0.0.255
end
wr
!!!!!!!!!!!!!!!!!!!!!!!!
!Cnt-Sw!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
en
conf t
int vlan 60
ip add 192.168.45.34 255.255.255.240
no shut
ip default-gateway 192.168.45.33
vlan 15
name Servers
vlan 30
name PCs
vlan 45
name Native
vlan 60
name Management
interface range fa0/1 - 10
switchport mode access
switchport access vlan 30
interface fa0/1
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
interface range fa0/11 - 20
switchport mode access
switchport access vlan 15
interface g0/1
switchport mode trunk
switchport trunk native vlan 45
interface range fa0/21 - 24 , g0/2
shutdown
ip domain-name cisco.com
crypto key gen rsa
1024

user CAdmin pass itsasecret
service password-encryption
ip ssh version 2
ip ssh auth 2
ip ssh time 60
```

```
line vty 0 15
login local
transport input ssh
```