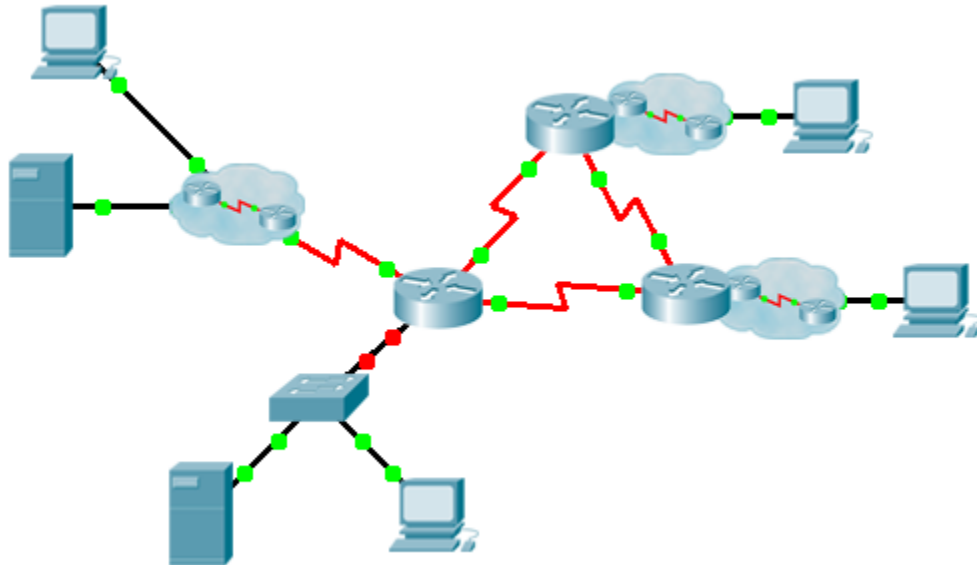


## Packet Tracer – Skills Integration Challenge

### Topology



## Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
	G0/0.15			N/A
	G0/0.30			N/A
	G0/0.45			N/A
	G0/0.60			N/A
	S0/0/0		255.255.255.252	N/A
	S0/0/1		255.255.255.252	N/A
	S0/1/0		255.255.255.252	N/A
	G0/0			N/A
	S0/0/0		255.255.255.252	N/A
	S0/0/1		255.255.255.252	N/A
	G0/0			N/A
	S0/0/0		255.255.255.252	N/A
	S0/0/1		255.255.255.252	N/A
	VLAN 60			
	NIC	DHCP Assigned	DHCP Assigned	DHCP Assigned

## VLANs and Port Assignments Table

VLAN Number - Name	Port assignment	Network
15 - Servers	F0/11 - F0/20	
30 - PCs	F0/1 - F0/10	
45 - Native	G0/1	
60 - Management	VLAN 60	

## 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 \_\_\_\_\_, \_\_\_\_\_, and \_\_\_\_\_ 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:

- Configure remote management access including IP addressing and SSH:
  - Domain is cisco.com
  - User \_\_\_\_\_ with password \_\_\_\_\_
  - 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
- 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 \_\_\_\_\_ 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 \_\_\_\_\_ 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:
    - Bind the NAT pool to ACL 1 and configure PAT. Packet Tracer does not grade this command.
    - Activate NAT on all appropriate interfaces.

Verify \_\_\_\_\_ has received full addressing information from \_\_\_\_\_.

### 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 \_\_\_\_\_ 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.