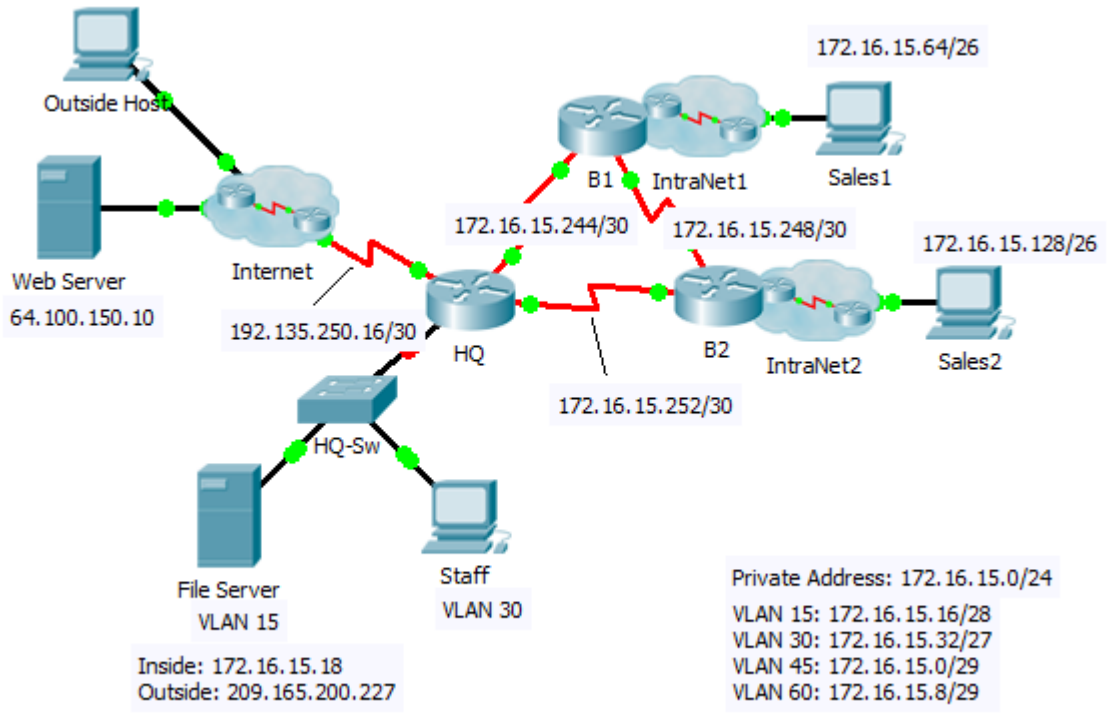
Packet Tracer – Skills Integration Challenge

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
HQ	G0/0.15	172.16.15.17	255.255.255.240	N/A
	G0/0.30	172.16.15.33	255.255.255.224	N/A
	G0/0.45	172.16.15.1	255.255.255.248	N/A
	G0/0.60	172.16.15.9	255.255.255.248	N/A
	S0/0/0	172.16.15.245	255.255.255.252	N/A
	S0/0/1	172.16.15.254	255.255.255.252	N/A
	S0/1/0	192.135.250.18	255.255.255.252	N/A
B1	G0/0	172.16.15.65	255.255.255.192	N/A
	S0/0/0	172.16.15.249	255.255.255.252	N/A
	S0/0/1	172.16.15.246	255.255.255.252	N/A
B2	G0/0	172.16.15.129	255.255.255.192	N/A
	S0/0/0	172.16.15.253	255.255.255.252	N/A
	S0/0/1	172.16.15.250	255.255.255.252	N/A
HQ-Sw	VLAN 60	172.16.15.10		
Staff	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	G1/1	
60 - Management	VLAN 60	

Scenario

This activity includes many of the skills that you have acquired during your CCNA studies. 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 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 **HQ**, **HQ-Sw**, and **Staff** 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:

HQ-Sw

- Configure remote management access including IP addressing and SSH:
  - Domain is cisco.com
  - User **HQadmin** with password **ciscoclass**
  - 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 Fa0/1, 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.

HQ

- Configure inter-VLAN routing.
- Configure DHCP services for VLAN 30. Use **LAN** as the case-sensitive name for the pool.
- Implement routing:
  - Use OSPF process ID 1 and router ID 1.1.1.1
  - Configure one network statement for the entire **172.16.15.0/24** address space
  - Disable interfaces that should not send OSPF messages.
  - Configure a default route to the Internet.
- Implement NAT:
  - Configure a standard, one statement ACL number 1. All IP addresses belonging to the **172.16.15.0/24** 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:

    209.165.200.225 and 209.165.200.226

Staff

Verify **Staff** has received full addressing information from **HQ**.

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 **HQ-Sw** 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**.
- Document any problems you encountered and the solutions in the **Troubleshooting Documentation** table below.

Troubleshooting Documentation

Problem	Solution

Suggested Scoring Rubric

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