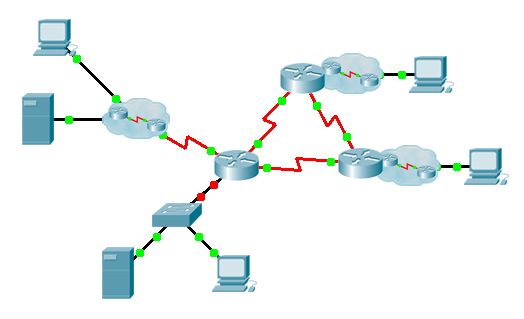
Packet Tracer – Skills Integration Challenge

1. Topology



Private Address: 192.168.45.0/24

VLAN 15: 192.168.45.64/26

VLAN 30: 192.168.45.128/26

VLAN 45: 192.168.45.16/28

VLAN 60: 192.168.45.32/28

Staff

VLAN 30

File Server

VLAN 15

Inside: 192.168.45.66

Outside: 64.100.32.58

B2 IntraNet2

Web Server

65.100.150.10

Outside Host

B1 IntraNet1

192.168.45.192/28

192.168.45.0/30

Internet

Sales1

HQ

Sales2

192.168.45.208/28

192.168.45.8/30

192.168.45.3/30

128.107.50.64/30

HQ-Sw

1. Addressing Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask | Default Gateway |
| HQ | G0/0.15 | 192.168.45.65 | 255.255.255.192 | N/A |
| G0/0.30 | 192.168.45.129 | 255.255.255.192 | N/A |
| G0/0.45 | 192.168.45.17 | 255.255.255.240 | N/A |
| G0/0.60 | 192.168.45.33 | 255.255.255.240 | N/A |
| S0/0/0 | 192.168.45.1 | 255.255.255.252 | N/A |
| S0/0/1 | 192.168.45.10 | 255.255.255.252 | N/A |
| S0/1/0 | 192.107.50.66 | 255.255.255.252 | N/A |
| B1 | G0/0 | 192.168.45.193 | 255.255.255.240 | N/A |
| S0/0/0 | 192.168.45. | 255.255.255.252 | N/A |
| S0/0/1 | 192.168.45.2 | 255.255.255.252 | N/A |
| B2 | G0/0 | 192.168.45.209 | 255.255.255.240 | N/A |
| S0/0/0 | 192.168.45.9 | 255.255.255.252 | N/A |
| S0/0/1 | 192.168.45.6 | 255.255.255.252 | N/A |
| HQ-Sw | VLAN 60 | 192.168.45.34 |  |  |
| Staff | NIC | DHCP Assigned | DHCP Assigned | DHCP Assigned |

1. 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 |  |

1. 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.

1. 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:

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

1. 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:
  1. Domain is cisco.com
  2. User \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ with password \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
  3. Crypto key length of 1024
  4. SSH version 2, limited to 2 authentication attempts and a 60 second timeout
  5. Clear text passwords should be encrypted.
* Configure, name and assign VLANs. Ports should be manually configured as access ports.
* Configure trunking.
* Implement port security:
  1. 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.
  2. Disable all other unused ports.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Configure inter-VLAN routing.
* Configure DHCP services for VLAN 30. Use **LAN** as the case-sensitive name for the pool.
* Implement routing:
  1. Use OSPF process ID 1 and router ID 1.1.1.1
  2. Configure one network statement for the entire \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ address space
  3. Disable interfaces that should not send OSPF messages.
  4. Configure a default route to the Internet.
* Implement NAT:
  1. Configure a standard, one statement ACL number 1. All IP addresses belonging to the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ address space are allowed.
  2. Refer to your documentation and configure static NAT for the File Server.
  3. Configure dynamic NAT with PAT using a pool name of your choice, a /30 mask, and these two public addresses:
     1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

1. 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.
  1. **Outside Host** should be able to access **File Server** at the public address.
  2. Inside PCs should be able to access **Web Server**.
* Document any problems you encountered and the solutions in the **Troubleshooting Documentation** table below.

1. Troubleshooting Documentation

|  |  |
| --- | --- |
| Problem | Solution |
|  |  |
|  |  |
|  |  |
|  |  |

1. Suggested Scoring Rubric

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