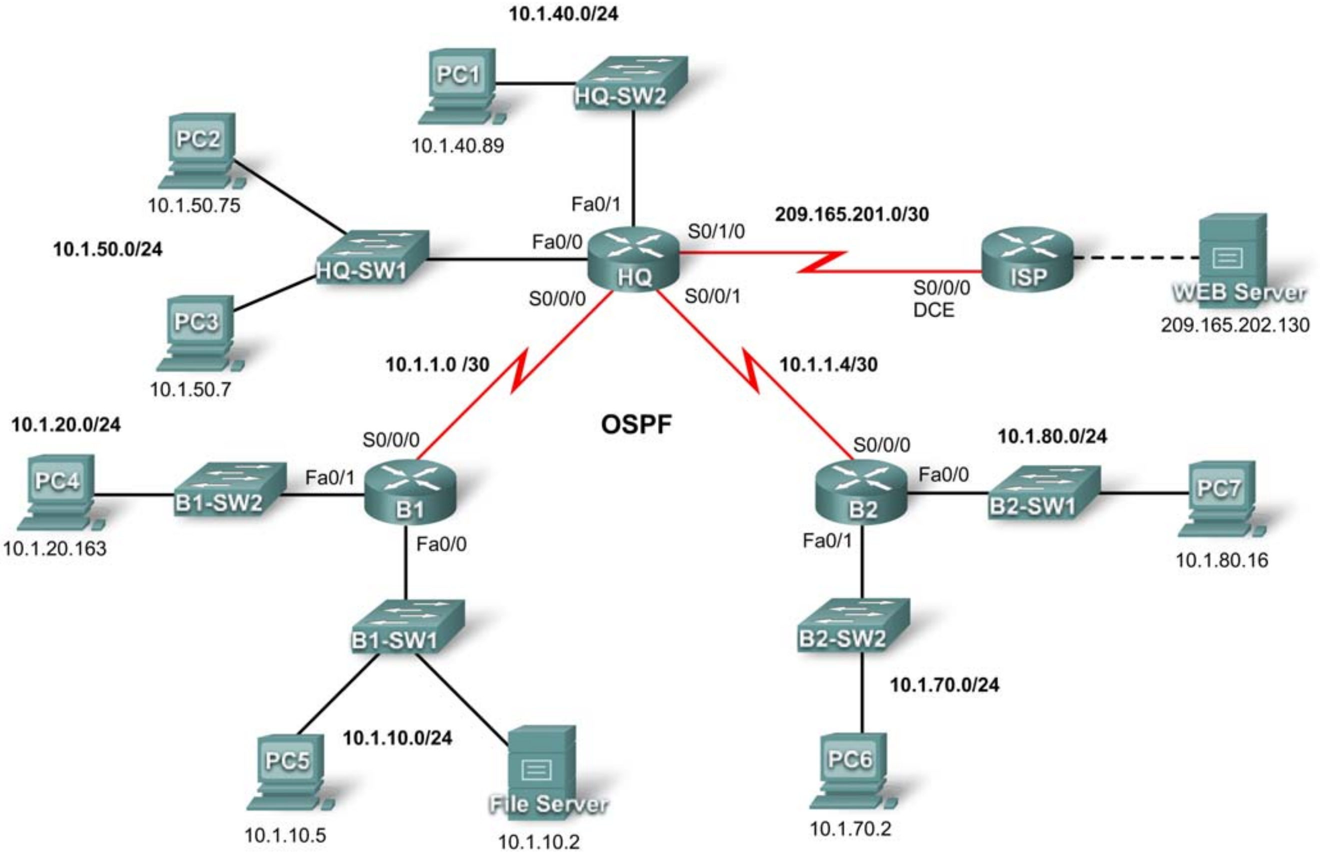
PT Activity 5.6.1: Packet Tracer Skills Integration Challenge

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask
HQ	**S0/0/0**	10.1.1.1	255.255.255.252
	S0/0/1	10.1.1.5	255.255.255.252
	S0/1/0	209.165.201.2	255.255.255.252
	Fa0/0	10.1.50.1	255.255.255.0
	Fa0/1	10.1.40.1	255.255.255.0
B1	**S0/0/0**	10.1.1.2	255.255.255.252
	Fa0/0	10.1.10.1	255.255.255.0
	Fa0/1	10.1.20.1	255.255.255.0
B2	**S0/0/0**	10.1.1.6	255.255.255.252
	Fa0/0	10.1.80.1	255.255.255.0
	Fa0/1	10.1.70.1	255.255.255.0
ISP	**S0/0/0**	209.165.201.1	255.255.255.252
	Fa0/0	209.165.202.129	255.255.255.252
Web Server	**NIC**	209.165.202.130	255.255.255.252

Learning Objectives

- Configure PPP with CHAP authentication
- Configure default routing
- Configure OSPF routing
- Implement and verify multiple ACL security policies

Introduction

In this activity, you will demonstrate your ability to configure ACLs that enforce five security policies. In addition, you will configure PPP and OSPF routing. The devices are already configured with IP addressing. The user EXEC password is **cisco,** and the privileged EXEC password is **class**.

Task 1: Configure PPP with CHAP Authentication

Step 1. Configure the link between HQ and B1 to use PPP encapsulation with CHAP authentication.

The password for CHAP authentication is **cisco123**.

Step 2. Configure the link between HQ and B2 to use PPP encapsulation with CHAP authentication.

The password for CHAP authentication is **cisco123**.

Step 3. Verify that connectivity is restored between the routers.

HQ should be able to ping both B1 and B2. The interfaces may take a few minutes to come back up. You can switch back and forth between Realtime and Simulation mode to speed up the process. Another possible workaround to this Packet Tracer behavior is to use the **shutdown** and **no shutdown** commands on the interfaces.

Note: The interfaces may go down at random points during the activity because of a Packet Tracer bug. The interface normally comes back up on its own if you wait a few seconds.

Step 4. Check results.

Your completion percentage should be 29%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Configure Default Routing

Step 1. Configure default routing from HQ to ISP.

Configure a default route on HQ using the *exit interface* argument to send all default traffic to ISP.

Step 2. Test connectivity to Web Server.

HQ should be able to successfully ping Web Server at 209.165.202.130 as long as the ping is sourced from the Serial0/1/0 interface.

Step 3. Check results.

Your completion percentage should be 32%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Configure OSPF Routing

Step 1. Configure OSPF on HQ.

- Configure OSPF using the process ID 1.
- Advertise all subnets except the 209.165.201.0 network.
- Propagate the default route to OSPF neighbors.
- Disable OSPF updates to ISP and to the HQ LANs.

Step 2. Configure OSPF on B1 and B2.

- Configure OSPF using the process ID 1.
- On each router, configure the appropriate subnets.
- Disable OSPF updates to the LANs.

Step 3. Test connectivity throughout the network.

The network should now have full end-to-end connectivity. All devices should be able to successfully ping all other devices, including Web Server at 209.165.202.130.

Step 4. Check results.

Your completion percentage should be 76%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Implement Multiple ACL Security Policies

Step 1. Implement security policy number 1.

Block the 10.1.10.0 network from accessing the 10.1.40.0 network. All other access to 10.1.40.0 is allowed. Configure the ACL on HQ using ACL number 10.

- Use a standard or extended ACL? _______________
- Apply the ACL to which interface? _______________
- Apply the ACL in which direction? _______________

____

____

____

____

____

Step 2. Verify that security policy number 1 is implemented.

A ping from PC5 to PC1 should fail.

Step 3. Check results.

Your completion percentage should be 80%. If not, click **Check Results** to see which required components are not yet completed.

Step 4. Implement security policy number 2.

Host 10.1.10.5 is not allowed to access host 10.1.50.7. All other hosts are allowed to access 10.1.50.7. Configure the ACL on B1 using ACL number 115.

- Use a standard or extended ACL? _______________
- Apply the ACL to which interface? _______________
- Apply the ACL in which direction? _______________

____

____

____

____

____

Step 5. Verify that security policy number 2 is implemented.

A ping from PC5 to PC3 should fail.

Step 6. Check results.

Your completion percentage should be 85%. If not, click **Check Results** to see which required components are not yet completed.

Step 7. Implement security policy number 3.

Hosts 10.1.50.1 through 10.1.50.63 are not allowed web access to Intranet server at 10.1.80.16. All other access is allowed. Configure the ACL on the appropriate router and use ACL number 101.

- Use a standard or extended ACL? _______________
- Configure the ACL on which router? ______________
- Apply the ACL to which interface? _______________
- Apply the ACL in which direction? _______________

Step 8. Verify that security policy number 3 is implemented.

To test this policy, click PC3, then the **Desktop** tab, and then **Web Browser**. For the URL, type in the IP address for the Intranet server, 10.1.80.16, and press **Enter**. After a few seconds, you should receive a Request Timeout message. PC2 and any other PC in the network should be able to access the Intranet server.

Step 9. Check results.

Your completion percentage should be 90%. If not, click **Check Results** to see which required components are not yet completed.

Step 10. Implement security policy number 4.

Use the name **NO_FTP** to configure a named ACL that blocks the 10.1.70.0/24 network from accessing FTP services (port 21) on the file server at 10.1.10.2. All other access should be allowed.

Note: Names are case-sensitive.

- Use a standard or extended ACL? _______________
- Configure the ACL on which router? ______________
- Apply the ACL to which interface? _______________
- Apply the ACL in which direction? _______________

Step 11. Check results.

Packet Tracer does not support testing FTP access, so you will not be able to verify this policy. However, your completion percentage should be 95%. If not, click **Check Results** to see which required components are not yet completed.

Step 12. Implement security policy number 5.

Since ISP represents connectivity to the Internet, configure a named ACL called **FIREWALL** in the following order:

1. Allow only inbound ping replies from ISP and any source beyond ISP.
2. Allow only established TCP sessions from ISP and any source beyond ISP.
3. Explicitly block all other inbound access from ISP and any source beyond ISP.

- Use a standard or extended ACL? _______________
- Configure the ACL on which router? ______________
- Apply the ACL to which interface? _______________
- Apply the ACL in which direction? _______________

____

____

____

____

____

Step 13. Verify that security policy number 5 is implemented.

To test this policy, any PC should be able to ping ISP or Web Server. However, neither ISP nor Web Server should be able to ping HQ or any other device behind the ACL. **FIREWALL**

Step 14. Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.