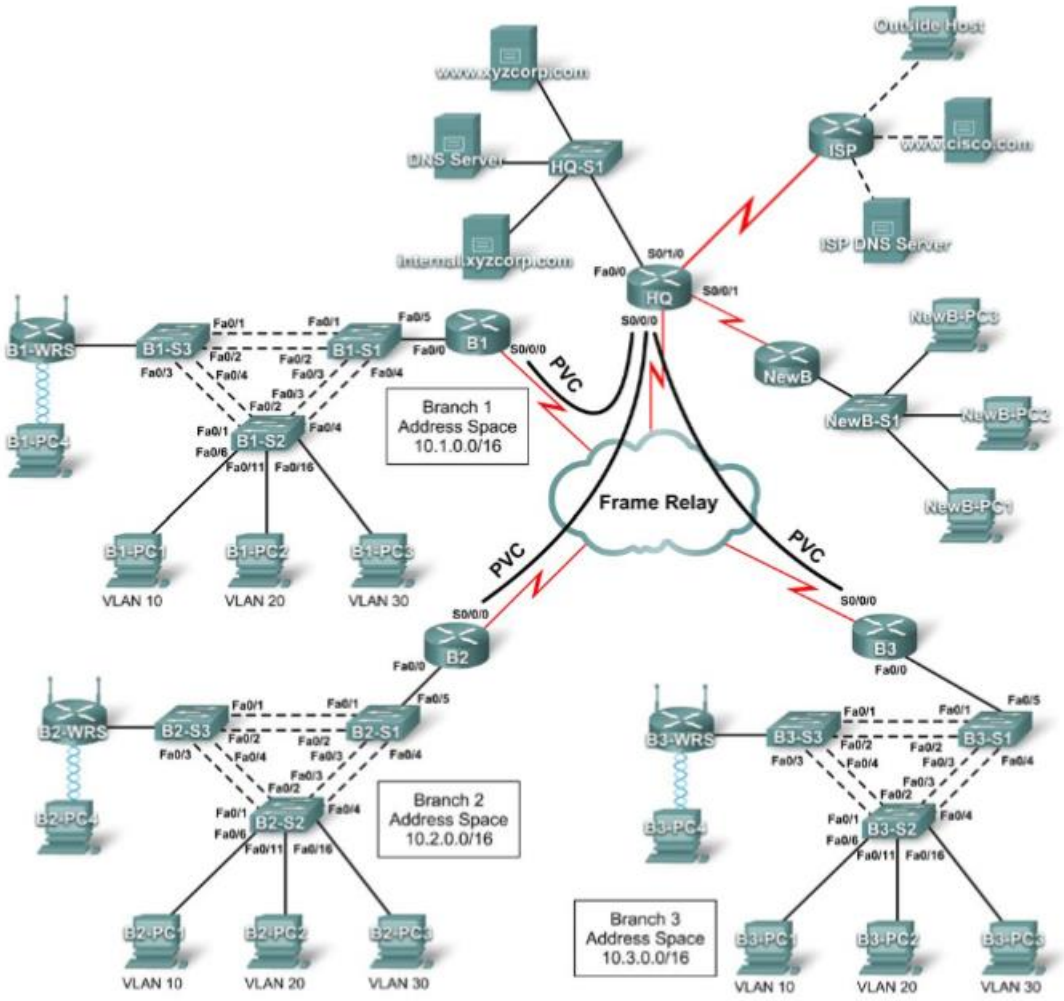
Individual Project

Topology Diagram



Addressing Table for HQ

Device	Interface	IP Address	Subnet Mask	DLCI Mappings
HQ	Fa0/0	10.0.1.1	255.255.255.0	N/A
	S0/0/0.41	10.255.255.1	255.255.255.252	DLCI 41 to B1
	S0/0/0.42	10.255.255.5	255.255.255.252	DLCI 42 to B2
	S0/0/0.43	10.255.255.9	255.255.255.252	DLCI 43 to B3
	S0/0/1	10.255.255.253	255.255.255.252	N/A
	S0/1/0	209.165.201.1	255.255.255.252	N/A

Addressing Table for Branch Routers

Device	Interface	IP Address	Subnet Mask
BX	Fa0/0.10	10.X.10.1	255.255.255.0
	Fa0/0.20	10.X.20.1	255.255.255.0
	Fa0/0.30	10.X.30.1	255.255.255.0
	Fa0/0.88	10.X.88.1	255.255.255.0
	Fa0/0.99	10.X.99.1	255.255.255.0
	S0/0/0	2nd address	255.255.255.252
BX-S1	VLAN 99	10.X.99.21	255.255.255.0
BX-S2	VLAN 99	10.X.99.22	255.255.255.0
BX-S3	VLAN 99	10.X.99.23	255.255.255.0
BX-WRS	VLAN 1	10.X.40.1	255.255.255.0

- Replace "X" with the Branch router number (B1, B2, or B3).
- The point-to-point PVCs with HQ use the second address in the subnet. HQ is using the first address.
- The WRT300N routers get the Internet address through DHCP from the Branch router.

VLAN Configuration and Port Mappings

VLAN Number	Network Address	VLAN Name	Port Mappings
10	10.X.10.0/24	Admin	BX-S2, Fa0/6
20	10.X.20.0/24	Sales	BX-S2, Fa0/11
30	10.X.30.0/24	Production	BX-S2, Fa0/16
88	10.X.88.0/24	Wireless	BX-S3, Fa0/7
99	10.X.99.0/24	Mgmt&Native	All trunks

Learning Objectives

- Configure Frame Relay in a hub-and-spoke topology
- Configure PPP with CHAP and PAP authentication
- Configure static and dynamic NAT
- Configure static and default routing

Introduction

In this comprehensive CCNA skills activity, the XYZ Corporation uses a combination of Frame Relay and PPP for WAN connections. The HQ router provides access to the server farm and the Internet through NAT. HQ also uses a basic firewall ACL to filter inbound traffic. Each Branch router is configured for inter-VLAN routing and DHCP. Routing is achieved through EIGRP as well as static and default routes. The VLANs, VTP, and STP are configured on each of the switched networks. Port security is enabled and wireless access is provided. Your job is to successfully implement all of these technologies, leveraging what you have learned over the four Exploration courses leading up to this culminating activity.

You are responsible for configuring HQ and the Branch routers, B1, B2, and B3. In addition, you are responsible for configuring every device that attaches to the network through a Branch router. The NewB router represents a new Branch office acquired through a merger with a smaller company. You do not have access to the NewB router. However, you will establish a link between HQ and NewB to provide this new Branch office with access to the internal network and the Internet.

Routers and switches under your administration have no configuration. None of the basic configurations like hostname, passwords, banners, and other general maintenance commands are graded by Packet Tracer and will not be part of the task specification. However, you are expected to configure them, and your instructor may choose to grade these commands.

Because this activity uses such a large network with close to 500 required components under the assessment items, you will not necessarily see your completion percentage increase each time you enter a command. In addition, you will not be given a specific percentage that should be complete at the end of each task. Instead, you use connectivity tests to verify each task's configurations. However, at any time you can click **Check Results** to see if a particular component is graded and if you configured it correctly.

Because the Branch routers (B1, B2, and B3) and switches are designed with scalability in mind, you can reuse scripts. For example, your configurations for B1, B1-S1, B1-S2, and B1-S3 can be directly applied to the B2 devices with only minor adjustments.

Note: This CCNA Skills Integration Challenge is also available in an open-ended version where you can choose the addressing scheme and technologies that you want to implement. You verify your configuration by testing end-to-end connectivity.

Task 1: Configure Frame Relay in a Hub-and-Spoke Topology

Step 1. Configure the Frame Relay core.

Use the addressing tables and the following requirements.

HQ is the hub router. B1, B2, and B3 are the spokes.

- HQ uses a point-to-point subinterface for each of the Branch routers.
- B3 must be manually configured to use IETF encapsulation.
- The LMI type must be manually configured as q933a for HQ, B1, and B2. B3 uses ANSI.

Step 2. Configure the LAN interface on HQ.

Step 3. Verify that HQ can ping each of the Branch routers.

Task 2: Configure PPP with CHAP and PAP Authentication

Step 1. Configure the WAN link from HQ to ISP using PPP encapsulation and CHAP authentication.

The CHAP password is **ciscochap**.

Step 2. Configure the WAN link from HQ to NewB using PPP encapsulation and PAP authentication.

You need to connect a cable to the correct interfaces. HQ is the DCE side of the link. You choose the clock rate. The PAP password is **ciscopap**.

Step 3. Verify that HQ can ping ISP and NewB.

Task 3: Configure Static and Dynamic NAT on HQ

Step 1. Configure NAT.

Use the following requirements:

- Allow all addresses for the 10.0.0.0/8 address space to be translated.
- XYZ Corporation owns the 209.165.200.240/29 address space. The pool, XYZCORP, uses addresses .241 through .245 with a /29 mask.
- The www.xyzcorp.com website at 10.0.1.2 is registered with the public DNS system at IP address 209.165.200.246.

Step 2. Verify NAT is operating by using extended ping.

From HQ, ping the serial 0/0/0 interface on ISP using the HQ LAN interface as the source address. This ping should succeed.

Verify that NAT translated the ping with the **show ip nat translations** command.

Task 4: Configure Static and Default Routing

Step 1. Configure HQ with a default route to ISP and a static route to the NewB LAN.

Use the exit interface as an argument.

Step 2. Configure the Branch routers with a default route to HQ.

Use the next-hop IP address as an argument.

Step 3. Verify connectivity beyond ISP.

All three NewB PCs and the NetAdmin PC should be able to ping the www.cisco.com web server.

Task 5: Configure Inter-VLAN Routing

Step 1. Configure each Branch router for inter-VLAN routing.

Using the addressing table for Branch routers, configure and activate the LAN interface for inter-VLAN routing. VLAN 99 is the native VLAN.

Step 2. Verify routing tables.

Each Branch router should now have six directly connected networks and one static default route.

Task 6: Configure and Optimize EIGRP Routing

Step 1. Configure HQ, B1, B2, and B3 with EIGRP.

- Use AS 100.
- Disable EIGRP updates on appropriate interfaces.
- Manually summarize EIGRP routes so that each Branch router only advertises the 10.X.0.0/16 address space to HQ.

Note: Packet Tracer does not accurately simulate the benefit of EIGRP summary routes. Routing tables will still show all subnets, even though you correctly configured the manual summary.

Step 2. Verify routing tables and connectivity.

HQ and the Branch routers should now have complete routing tables.

The NetAdmin PC should now be able to ping each VLAN subinterface on each Branch router.

Task 7: Configure VTP, Trunking, the VLAN Interface, and VLANs

The following requirements apply to all three Branches. Configure one set of three switches. Then use the scripts for those switches on the other two sets of switches.

Step 1. Configure Branch switches with VTP.

- BX-S1 is the VTP server. BX-S2 and BX-S3 are VTP clients.
- The domain name is **XYZCORP**.
- The password is **xyzvtp**.

Step 2. Configure trunking on BX-S1, BX-S2, and BX-S3.

Configure the appropriate interfaces in trunking mode and assign VLAN 99 as the native VLAN.

Step 3. Configure the VLAN interface and default gateway on BX-S1, BX-S2, and BX-S3.

Step 4. Create the VLANs on BX-S1.

Create and name the VLANs listed in the VLAN Configuration and Port Mappings table on BX-S1 only. VTP advertises the new VLANs to BX-S1 and BX-S2.

Step 5. Verify that VLANs have been sent to BX-S2 and BX-S3.

Use the appropriate commands to verify that S2 and S3 now have the VLANs you created on S1. It may take a few minutes for Packet Tracer to simulate the VTP advertisements. A quick way to force the sending of VTP advertisements is to change one of the client switches to transparent mode and then back to client mode.

Task 8: Assign VLANs and Configure Port Security

Step 1. Assign VLANs to access ports.

Use the VLAN Configuration and Port Mappings table to complete the following requirements:

- Configure access ports
- Assign VLANs to the access ports

Step 2. Configure port security.

Use the following policy to establish port security on the BX-S2 access ports:

- Allow only one MAC address
- Configure the first learned MAC address to "stick" to the configuration
- Set the port to shut down if there is a security violation

Step 3. Verify VLAN assignments and port security.

Use the appropriate commands to verify that access VLANs are correctly assigned and that the port security policy has been enabled.

Task 9: Configure STP

Step 1. Configure BX-S1 as the root bridge.

Set the priority level to 4096 on BX-S1 so that these switches are always the root bridge for all VLANs.

Step 2. Configure BX-S3 as the backup root bridge.

Set the priority level to 8192 on BX-S3 so that these switches are always the backup root bridge for all VLANs.

Step 3. Verify that BX-S1 is the root bridge.

Task 10: Configure DHCP

Step 1. Configure DHCP pools for each VLAN.

On the Branch routers, configure DHCP pools for each VLAN using the following requirements:

- Exclude the first 10 IP addresses in each pool for the LANs.
- Exclude the first 24 IP addresses in each pool for the wireless LANs.
- The pool name is **BX_VLAN##** where **X** is the router number and **##** is the VLAN number.
- Include the DNS server attached to the HQ server farm as part of the DHCP configuration.

Step 2. Configure the PCs to use DHCP.

Currently, the PCs are configured to use static IP addresses. Change this configuration to DHCP.

Step 3. Verify that the PCs and wireless routers have an IP address.

Step 4. Verify connectivity.

All PCs physically attached to the network should be able to ping the www.cisco.com web server.

Task 11: Configure a Firewall ACL

Step 1. Verify connectivity from Outside Host.

The Outside Host PC should be able to ping the server at www.xyzcorp.com.

Step 2. Implement a basic firewall ACL.

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

1. Allow inbound HTTP requests to the www.xyzcorp.com server.

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

Step 3. Verify connectivity from Outside Host.

The Outside Host PC should not be able to ping the server at www.xyzcorp.com. However, the Outside Host PC should be able to request a web page.

Task 12: Configure Wireless Connectivity

Step 1. Verify the DHCP configuration.

Each BX-WRS router should already have IP addressing from the DHCP of the BX router for VLAN 88.

Step 2. Configure the Network Setup/LAN settings.

The "Router IP" on the **Status** page in the GUI tab should be the first IP of the 10.X.40.0 /24 subnet. Leave all other settings at the default.

Step 3. Configure the wireless network settings.

The SSIDs for the routers are **BX-WRS_LAN** where the **X** is the Branch router number.

The WEP key is **12345ABCDE**

Step 4. Configure the wireless routers for remote access.

Configure the administration password as **cisco123** and enable remote management.

Step 5. Configure the BX-PC4 PCs to access the wireless network using DHCP.

Step 6. Verify connectivity and remote management capability.

Each wireless PC should be able to access the www.cisco.com web server.

Verify remote management capability by accessing the wireless router through the web browser.

Task 13: Network Troubleshooting

Step 1. Break the network.

One student leaves the room, if necessary, while another student breaks the configuration.

Step 2. Troubleshoot the problem.

The student returns and uses troubleshooting techniques to isolate and solve the problem.

Step 3. Break the network again.

The students switch roles and repeat steps 1 and 2.