Packet Tracer – Skills Integration Challenge
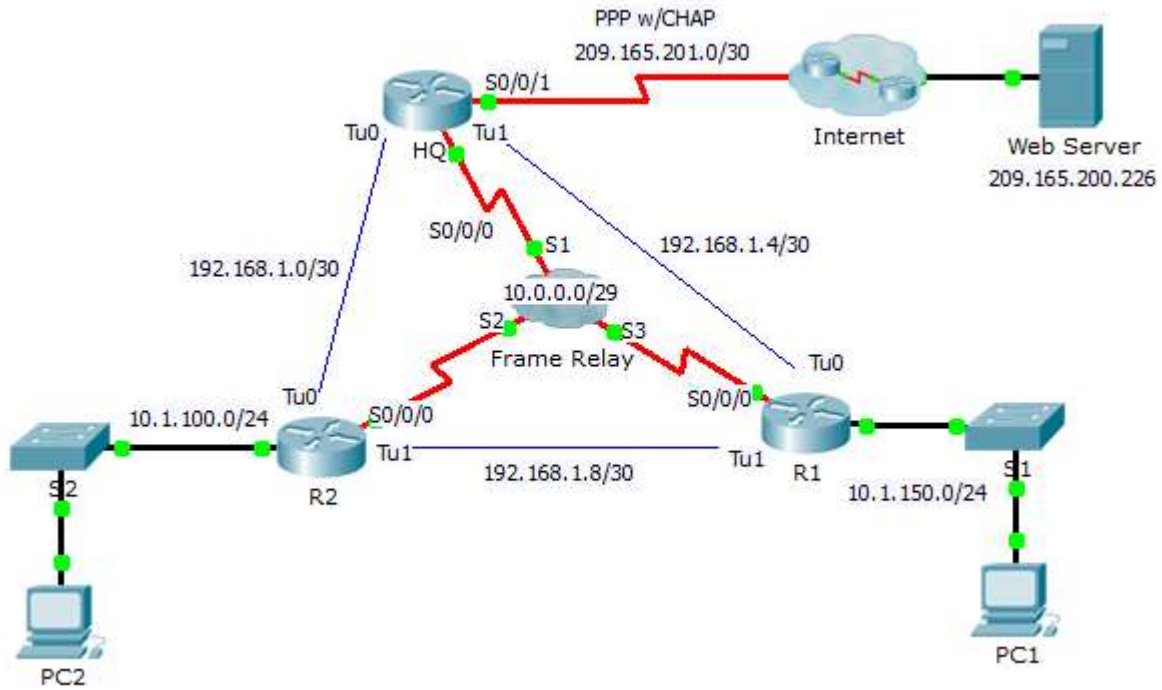
Topology

Addressing Table

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
HQ	S0/0/0	10.0.0.1	255.255.255.248	N/A
	S0/0/1	209.165.201.2	255.255.255.252	N/A
	Tu0	192.168.1.1	255.255.255.252	N/A
	Tu1	192.168.1.5	255.255.255.252	N/A
R1	G0/0	10.1.150.1	255.255.255.0	N/A
	S0/0/0	10.0.0.3	255.255.255.248	N/A
	Tu0	192.168.1.6	255.255.255.252	N/A
	Tu1	192.168.1.9	255.255.255.252	N/A
R2	G0/0	10.1.100.1	255.255.255.0	N/A
	S0/0/0	10.0.0.2	255.255.255.248	N/A
	Tu0	192.168.1.2	255.255.255.252	N/A
	Tu1	162.168.1.10	255.255.255.252	N/A
Web	NIC	209.165.200.226	255.255.255.252	209.165.200.225
PC1	NIC	10.1.150.10	255.255.255.0	10.1.150.1
PC2	NIC	10.1.100.10	255.255.255.0	10.1.100.1

DLCI Mappings

From / To	HQ	R1	R2
HQ	-	103	102
R1	301	-	302
R2	201	203	-

Background

This activity allows you to practice a variety of skills, including configuring Frame Relay, PPP with CHAP, NAT overloading (PAT), and GRE tunnels. The routers are partially configured for you.

Requirements

Note: You only have console access to router R1 and telnet access to router HQ. The username is **admin** and the password is **adminpass** for telnet access.

R1

- Configure full mesh Frame Relay.
  - Configure Frame Relay encapsulation.
  - Configure a map to each of the other routers using the **broadcast** keyword.
  - The LMI type is ANSI.

- Configure GRE tunnels to the other routers.
  - Configure the source port and the destination address.
  - Configure the IP address for the tunnel interface according to the **Addressing Table**.

HQ

- Configure **HQ** to use PPP with CHAP on the link to the Internet. **ISP** is the router hostname. The password for CHAP is **cisco**.
- Configure GRE tunnels to the other routers.
  - Configure the source port and the destination address.
  - Configure the IP address for the tunnel interface according to the **Addressing Table**.
- Configure NAT to share the public IP address configured on interface s0/0/1 with the entire class A private range.
  - Configure access-list 1 for use with NAT.
  - Identify the inside and outside interfaces.

Verify End-to-End Connectivity

- All end devices should now be able to ping each other and the **Web Server**.
- If not, click **Check Results** to see what configurations you may still be missing. Implement necessary fixes and retest for full end-to-end connectivity.