Module 6 Mastery Part B Assessment Lab Packet Tracer - Skills Integration Challenge

Introduction

This is your final performance assessment for routers ITNW-2312. This assessment will incorporate configuration and concepts from earlier units of this course, as well your previous 2 networking courses (ITNW-1325 and ITNW-2321) Good Luck!

Objectives

Complete all configurations and set-up given for XYZ Corporation.

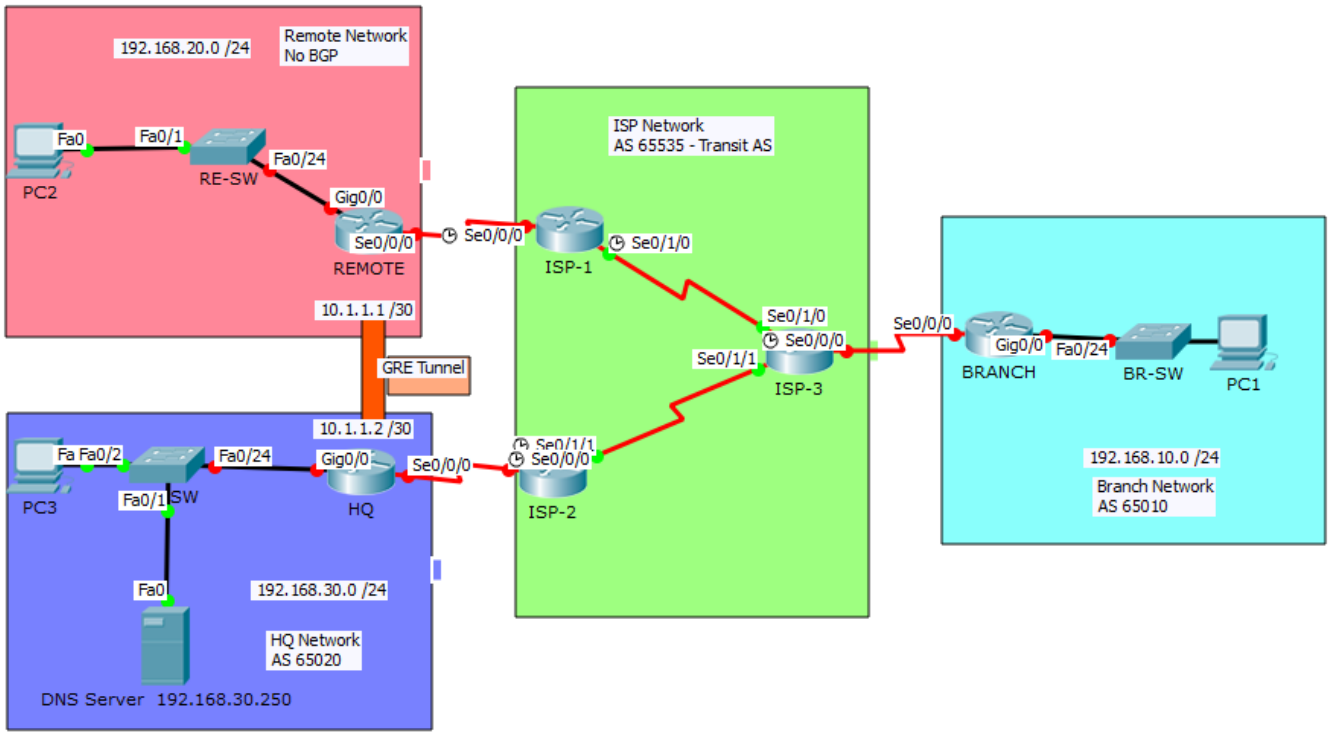
Assignment

In this Performance Assessment, the XYZ Corporation uses a combination of eBGP, PPP, and GRE WAN connections. Other technologies include DHCP, default routing, OSPF for IPv4, and SSH configurations.

Required Resources

Your Computer workstation
Cisco Packet Tracer (online)
Provided Packet Tracer File

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
ISP-1	S0/0/0	209.165.201.1	255.255.255.252	N/A
	S0/1/0	209.165.201.9	255.255.255.252	N/A
ISP-2	S0/0/0	209.165.201.17	255.255.255.252	N/A
	S0/1/1	209.165.201.13	255.255.255.252	N/A
ISP-3	S0/0/0	209.165.201.21	255.255.255.252	N/A
	S0/1/0	209.165.201.10	255.255.255.252	N/A
	S0/1/1	209.165.201.14	255.255.255.252	N/A
REMOTE	S0/0/0	209.165.201.2	255.255.255.252	N/A
	G0/0	192.168.20.1	255.255.255.0	N/A
	Tunnel 10	10.1.1.1	255.255.255.252	N/A
HQ	S0/0/0	209.165.201.18	255.255.255.252	N/A
	G0/0	192.168.30.1	255.255.255.0	N/A

	Tunnel 10	10.1.1.2	255.255.255.252	N/A
BRANCH	S0/0/0	209.165.201.22	255.255.255.252	N/A
	G0/0	192.168.10.1	255.255.255.0	N/A
PC1	NIC	DHCP		192.168.10.1
PC2	NIC	192.168.20.10	255.255.255.0	192.168.20.1
PC3	NIC	DHCP		192.168.30.1
DNS Server	NIC	192.168.30.250	255.255.255.0	192.168.30.1

Background / Scenario

In this skills integration challenge, the XYZ Corporation uses a combination of eBGP, PPP, and GRE WAN connections. Other technologies include DHCP, default routing, OSPF for IPv4, and SSH configurations.

Requirements

Note: The user EXEC password is **cisco** and the privileged EXEC password is **class**

Interface Addressing

- Configure interface addressing as needed on appropriate devices.
    - Use the topology table to implement addressing on routers REMOTE, HQ, and BRANCH.
    - Configure **PC1** and **PC3** to use DHCP.

SSH - Commands are provided below, ssh is covered in your firewalls class.

- Configure **HQ** to use SSH for remote access.
    - Set the modulus to **2048**. The domain name is **CISCO.com**.
    - The username is **admin** and the password is **secureaccess**.
    - Only SSH should be allowed on the VTY lines.
    - Modify the SSH defaults: version 2; 60-second timeout; two retries.

Note: SSH commands needed for **HQ** below **-** Significance of each command is documented in *italics*.

HQ(config)# **username admin password secureaccess**

Creates a locally significant username/password word combination. These are to be used when connecting to the HQ router with SSH.

HQ(config)# **ip domain-name CISCO.com**

Creates a host domain for the router. This must be configured for SSH to work.

HQ(config)# **ip ssh version 2**

Enables SSH version 2 on the device.

HQ(config)# **ip ssh timeout 60**

HQ(config)# **ip ssh authentication-retries 2**

SSH is configured on a Cisco router with a timeout that is not to exceed 60 seconds and no more than 2 authentication retries.

HQ(config)# **crypto key generate rsa**

You will see the following output:

The name for the keys will be: HQ.CISCO.com

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]:

Type **2048**

Enables the SSH server for local and remote authentication on the HQ router and generates an RSA key pair.

Configure the VTY lines to allow SSH only

HQ(config)# **line vty 0 4***Move to VTY configuration mode for 5 VTY lines on the router.*

HQ(config)# **login local**

*Enables password checking on a per-user basis. Username and Password will be checked against the data entered with the **Username** global configuration command you did earlier in the lab (***username admin password secureaccess)**

HQ(config)# **transport input ssh**

Limits remote access to SSH connections only!!! Disables Telnet.

Verifying SSH

HQ(config)# **show ip ssh** – *Verifies ssh is enabled.*

HQ(config)# **show ssh** – *Checks the ssh connection to the device.*

PPP

- Configure the WAN link from **BRANCH** to the **ISP-3** router using PPP encapsulation and CHAP authentication.
    - Create a user **ISP-3** with the password of **cisco**.
- Configure the WAN link from **HQ** to the **ISP-2** router using PPP encapsulation and CHAP authentication.
    - Create a user **ISP-2** with the password of **cisco**.

DHCP

- On **BRANCH**, configure a DHCP pool for the BRANCH LAN using the following requirements:
    - Exclude the first 5 IP addresses in the range.
    - The case-sensitive pool name is **LAN**.
    - Include the DNS server attached to the **HQ** LAN as part of the DHCP configuration.

- Configure PC1 to use DHCP.

- On **HQ**, configure a DHCP pool for the HQ LAN using the following requirements:

- Exclude the first 10 IP addresses in the range.
- The case-sensitive pool name is **LAN**.
- Include the DNS server attached to the **HQ** LAN as part of the DHCP configuration.

- Configure PC3 to use DHCP.

Default Routing

- Configure **REMOTE** with a default route to the **ISP-1** router. Use the Next-Hop IP as an argument.

eBGP Routing

- Configure **BRANCH** with eBGP routing.
  - Configure **BRANCH** to peer with **ISP-3**.
  - Add **BRANCH's** internal network to BGP
- Configure **HQ** with eBGP routing.
  - Configure **HQ** to peer with **ISP-2**.
  - Add **HQ's** internal network to BGP.

GRE Tunneling

- Configure **REMOTE** with a tunnel interface to send IP traffic over GRE to **HQ**.
  - Configure **Tunnel 10** with appropriate addressing information.
  - Configure the tunnel source with the local exit interface.
  - Configure the tunnel destination with the appropriate endpoint IP address.

- Configure **HQ** with a tunnel interface to send IP traffic over GRE to **REMOTE**.
  - Configure **Tunnel 10** with appropriate addressing information.
  - Configure the tunnel source with the local exit interface.
  - Configure the tunnel destination with the appropriate endpoint IP address.

OSPF Routing

- Because the **REMOTE** LAN should have connectivity to the **HQ** LAN, configure OSPF across the GRE tunnel.
  - Configure OSPF process 100 on the **REMOTE** router.
  - **REMOTE** should advertise the LAN network via OSPF.
  - **REMOTE** should be configured to form an adjacency with **HQ** over the GRE tunnel.
  - Disable OSPF updates on appropriate interfaces.

- Because the **HQ** LAN should have connectivity to the **REMOTE** LAN, configure OSPF across the GRE tunnel.
    - Configure OSPF process 100 on the **HQ** router.
    - **HQ** should advertise the LAN network via OSPF.
    - **HQ** should be configured to form an adjacency with **REMOTE** over the GRE tunnel.
    - Disable OSPF updates on appropriate interfaces.

Connectivity

- Verify full connectivity from **PC2** to the **DNS Server**.
- Verify full connectivity from **PC1** to the **DNS Server**.