Практическое задание на экзамен CCNA 4

A few things to keep in mind while completing this activity:

1. Do not use the browser **Back** button or close or reload any Exam windows during the exam.
2. Do not close Packet Tracer when you are done. It will close automatically.
3. Click the **Submit Assessment** button to submit your work.

Objectives

In this Packet Tracer Skills Based Assessment, you will do as follows:

- Configure PPP encapsulation and CHAP authentication for serial links.
- Configure a GRE tunnel.
- Configure OSPF.
- Configure BGP.
- Configure standard and extended IPv4 ACLs.
- Configure IPv6 ACLs.

For the sake of time, many repetitive, but important, configuration tasks have been omitted from this assessment. Many of these tasks, especially those related to security, are essential elements of a network configuration. The intent of this activity is not to diminish the importance of full device configurations.

The IP addresses for all the devices have been configured and some of the routing configurations are already completed in this activity.

You are required to configure the devices as follows:

Remote:

- Configure PPP and CHAP authentication on the appropriate interface.
- Configure GRE tunnel.
- Configure OSPF.
- Configure standard IPv4 ACL.

Other:

- Configure standard IPv4 ACLs.

Main:

- Configure PPP and CHAP authentication on the appropriate interface.
- Configure GRE tunnel.
- Configure OSPF.
- Configure standard and extended IPv4 ACLs.
- Configure IPv6 ACLs.

Note: All the routers in AS 65001 are locked and no configurations are performed by the students. Furthermore, all the switches are pre-configured.

Addressing Table

Device	Interface	IPv4 Address	Subnet Mask	Gateway	DNS server
		IPv6 Address / Prefix			
		Link Local Address			
Remote	G0/0	192.168.0.1	255.255.255.0	N/A	N/A
		2001:DB8:ACAD::1/64			
		FE80::1			
	G0/1	192.168.1.1	255.255.255.0	N/A	N/A
		2001:DB8:ACAD:1::1/64			
		FE80::1			
	S0/0/0	209.165.200.225	255.255.255.252	N/A	N/A
		2001:DB8:ACAD:C::225/64			
		FE80::225			
	Tunnel 0	172.16.1.2	255.255.255.252	N/A	N/A
Main	G0/0	192.168.2.1	255.255.255.0	N/A	N/A
		2001:DB8:ACAD:2::1/64			
		FE80::1			
	G0/1	209.165.202.129	255.255.255.224	N/A	N/A
		2001:DB8:ACAD:B::129/64			
		FE80::129			
	S0/0/1	209.165.200.229	255.255.255.252	N/A	N/A
		2001:DB8:ACAD:A::229/64			
		FE80::229			
	Tunnel 0	172.16.1.1	255.255.255.252	N/A	N/A
Other	G0/1	192.168.3.1	255.255.255.0	N/A	N/A
		2001:DB8:ACAD:3::1/64			
		FE80::1			
	S0/0/0	209.165.200.238	255.255.255.252	N/A	N/A
		2001:DB8:ACAD:E::238/64			
		FE80::238			
ISP1	S0/0/0	209.165.200.226	255.255.255.252	N/A	N/A
		2001:DB8:ACAD:C::226/64			
		FE80::226			
	S0/0/1	209.165.200.230	255.255.255.252	N/A	N/A
		2001:DB8:ACAD:A::230/64			
		FE80::230			
	S0/1/1	209.165.200.233	255.255.255.252	N/A	N/A
		2001:DB8:ACAD:D::233/64			
		FE80::233			
Remote-PC0	NIC	DHCP		192.168.0.1	209.165.201.29
		2001:DB8::ACAD::10/64		FE80::1	2001:DB8:ACAD:E::29
		FE80::10			
Remote-PC1	NIC	DHCP		192.168.1.1	209.165.201.29
		2001:DB8::ACAD:1::10/64		FE80::1	2001:DB8:ACAD:E::29
		FE80::10			
Main-PC	NIC	DHCP		192.168.2.1	209.165.201.29
		2001:DB8:ACAD:2::10/64		FE80::1	2001:DB8:ACAD:E::29
		FE80::10			
Main-Server	NIC	209.165.202.158	255.255.255.224	209.165.202.129	209.165.201.29
		2001:DB8:ACAD:B::158/64		FE80::129	2001:DB8:ACAD:E::29

Instructions

Step 1: Configure PPP encapsulation and authentication.

a. Configure PPP encapsulation for the link between **Main** and **ISP1** and the link between **Remote** and **ISP1**.

b. Configure CHAP authentication between the links.

c. Configure the correct username and the password **321cisco** for CHAP authentication on both **Main** and **Remote**.

Step 2: Configure a GRE tunnel with routing.

a. Configure a GRE tunnel between **Main** and **Remote**.

b. Configure OSPF **1** to route the traffic between the LANs of **Main** and **Remote** through the GRE tunnel. Summarize the networks attached to **Remote**.

Step 3: Configure BGP.

Configure BGP between **ISP1** in Internet cluster and 209.165.202.128/27 network on **Main**.

a. Use AS number **65020** for **Main**.

b. Configure **ISP1** as the BGP neighbor.

c. Only advertise the **209.165.202.128 / 27** network into BGP.

Step 4: Configure ACLs for NAT.

a. Configure a standard access list numbered **1** on **Remote** to allow NAT for hosts in network **192.168.0.0 /23**.

b. Configure a standard access list numbered **1** on **Main** to allow NAT for hosts in network **192.168.2.0 /24**.

c. Configure a standard access list numbered **1** on **Other** to allow NAT for hosts in network **192.168.3.0 /24**.

Step 5: Configure a standard ACL to restrict remote access to the Other router.

A standard ACL named **VTY_ADMIN** is configured to limit access via VTY to the **Other** router. This ACL will only allow hosts from the LAN attached to the G0/1 interface and the hosts from the LANs on **Remote** router to access the **Other** router. All the other connections to VTY should fail.

a. Configure one ACL named **VTY_ADMIN** with three ACEs in the following order:

1) Allow any hosts from the LAN attached to the G0/1 interface of **Other** router to access the router.
2) Allow the hosts from the LANs in the **Remote** network to **Other** router remotely.
3) All other remote connections are denied.

b. Apply the ACL to the appropriate interface.

Note: Use the public IPv4 addresses in the ACLs when the private IPv4 addresses have been mapped to public IPv4 addresses.

Step 6: Configure an extended ACL to restrict access to the Main LAN.

a. Configure an extended ACL named **HTTP_ACCESS** that allows **Remote** LANs, **Other** LANs and the LAN inside **Main** to access **Main-Server** via the web browser.

Configure this ACL with the following 5 ACEs in the following order:

1) Allow the hosts from the **Remote** network to access the **Main-Server**.
2) Allow the hosts from the **Other** LANs to access the **Main-Server**.
3) Allow the internal network **192.168.2.0 /24** to access the **Main-Server**.
4) Allow ICMP replies to **Main-Server** from any networks.
5) Explicitly deny all other traffic from accessing the **Main-Server**.

b. Apply the ACL to the **Main** G0/1 interface.

Note: Use the public IPv4 addresses in the ACLs when the private IPv4 addresses have been mapped to public IPv4 addresses.

Step 7: Configure an IPv6 access list to restrict access to the Main LAN.

a. Configure an IPv6 access list named **HTTP6_ACCESS** that
allows **Remote** LANs, **Other** LANs and the LAN inside **Main** to access **Main-Server** via the web browser.

b. Configure this ACL with the following 6 ACEs in the following order:

1) Allow the hosts from the **Remote** (2001:DB8:ACAD::/64) to access the **Main-Server**.
2) Allow the hosts from the **Remote** (2001:DB8:ACAD:1::/64) to access the **Main-Server**.
3) Allow the hosts from the **Other** LANs to access the **Main-Server**.
4) Allow the internal network 2001:DB8:ACAD:2::/64 to access the **Main-Server**.
5) Allow ICMP from **Main-Server** to the other networks.
6) Explicitly deny all other traffic from accessing the **Main-Server**.

c. Apply the ACL to the **Main** G0/1 interface.