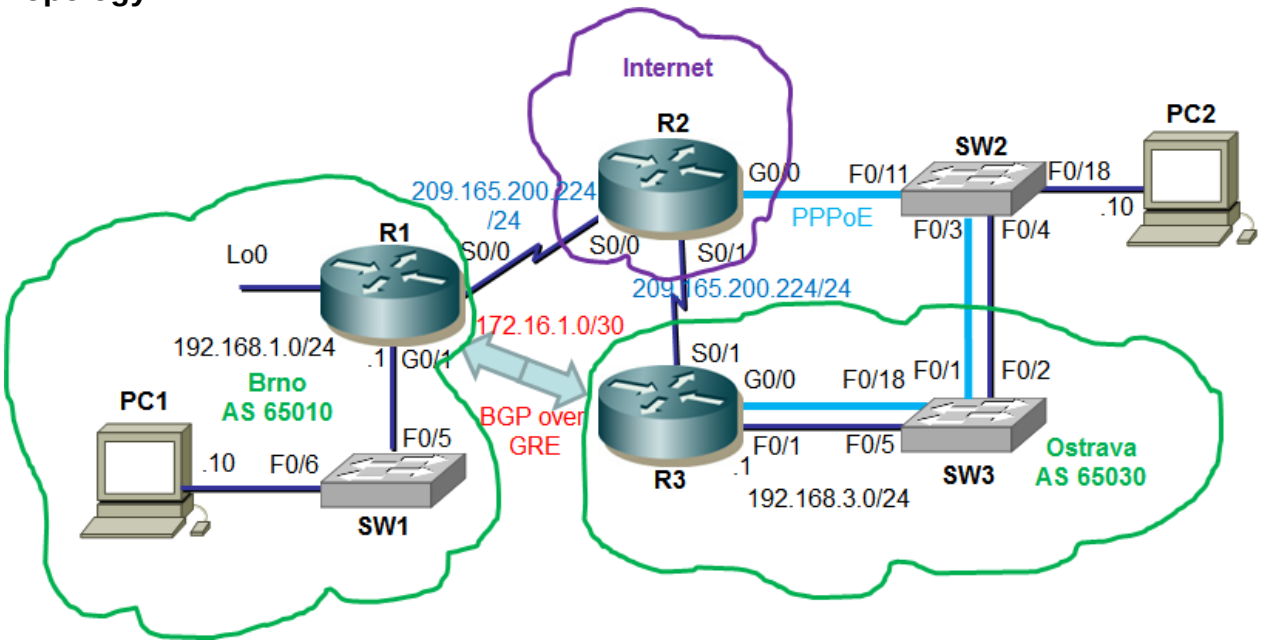
CCNA Routing and Switching: Connecting Networks

Skills Assessment Training

Topology



Assessment Objectives

Part 1: Configure Device Basic Settings

Part 2: Configure PPP Connections

Part 3: Configure IPv4 ACL for NAT

Part 4: Configuring IP Routing

Part 5: Configure GRE Tunnel with BGP

Part 6: Implement PPPoE

Part 7: Configure IP ACLs

Part 8: Monitor the Network

Scenario

The first WAN protocol you will configure is PPP with CHAP authentication. You will configure access lists to limit network access and determine the IP addresses that are used in NAT. You will also configure a GRE tunnel to allow BGP updates between the Olomouc and Brno domains. You will also configure SNMP and SPAN for network monitoring during this assessment. Network configurations and connectivity will be verified throughout the assessment by using common CLI commands.

Interface Summary Table

Device	Gigabit Ethernet 0/0	Gigabit Ethernet 0/1	Serial 0/0/0	Serial 0/0/1
R1		192.168.1.1/24	209.165.200.225/30	
		2001:DB8:ACAD:1::1/64	2001:DB8:ACAD:A::1/64	
		FE80::1	FE80::1	
R2			209.165.200.226/30	209.165.200.230/30
			2001:DB8:ACAD:A::2/64	2001:DB8:ACAD:B::2/64
			FE80::2	FE80::2
R3		192.168.3.1 / 24		209.165.200.229/30
		2001:DB8:ACAD:3::1/64		2001:DB8:ACAD:B::1/64
		FE80::3		FE80::3

Device	IP address	Subnet Mask (/prefix)	Default Gateway	
PC1	192.168.1.10	255.255.255.0	192.168.1.1	
	2001:DB8:ACAD:1::10	/64	FE80::1	
PC2	192.168.3.10	255.255.255.0	192.168.3.1	
	2001:DB8:ACAD:3::10	/64	FE80::3	

Part 1: Configure Device Basic Settings

Step 1: Configure PCs.

Assign static IP address information (IP address, subnet mask, default gateway) to PC1 and PC2 in the topology.

Configuration Item or Task	Specification
Configure static IP address information on PC1.	IPv4 Address: 192.168.1.10 IPv4 Subnet Mask: 255.255.255.0 IPv4 Default Gateway: 192.168.1.1 IPv6 Address / Prefix: 2001:DB8:ACAD:1::10/64 IPv6 Default Gateway: FE80::1
Configure static IP address information on PC2.	IPv4 Address: 192.168.3.10 IPv4 Subnet Mask: 255.255.255.0 IPv4 Default Gateway: 192.168.3.1 IPv6 Address / Prefix: 2001:DB8:ACAD:3::10/64 IPv6 Default Gateway: FE80::3

Step 2: Configure R1.

Configuration tasks for R1 include the following:

Configuration Item or Task	Specification
Disable DNS lookup	
Router name	R1
Encrypted privileged EXEC password	class
Console access password	cisco
Remote access configuration	Domain name: Brno.com Username: user Password: cisco RSA key: 2048 bit VTY: SSH only
Encrypt the plaintext passwords	
MOTD banner	Unauthorized Access is Prohibited!
Configure G0/1	Set the description. Set the Layer 3 IP address. IPv4 Address: 192.168.1.1 / 24 IPv6 Unicast Address: 2001:DB8:ACAD:1::1/64 IPv6 Link Local Address: FE80::1 Activate the interface.

Step 3: Configure R2.

Configuration tasks for R2 include the following:

Configuration Item or Task	Specification
Disable DNS lookup	
Router name	R2
Encrypted privileged EXEC password	class
Console access password	cisco
MOTD banner	Unauthorized Access is Prohibited!

Step 4: Configure R3.

Configuration tasks for R3 include the following:

Configuration Item or Task	Specification
Disable DNS lookup	
Router name	R3

Encrypted privileged EXEC password	class
Console access password	cisco
Remote access configuration	Domain name: Olomouc.com Username: user Password: cisco RSA key: 2048 bit VTY: SSH only
MOTD banner	Unauthorized Access is Prohibited!
Configure G0/1	Set the description. Set the Layer 3 IP address. IPv4 Address: 192.168.3.1 / 24 IPv6 Unicast Address: 2001:DB8:ACAD:3::1/64 IPv6 Link Local Address: FE80::3 Activate the interface.

Part 2: Configure PPP Connections

Step 1: Configure R1.

Configuration tasks for R1 include the following:

Task	Specification
Configure S0/0/0.	Set the description. IPv4 Address: 209.165.200.225 / 30 IPv6 Unicast Address: 2001:DB8:ACAD:A::1/64 IPv6 Link Local Address: FE80::1 Set encapsulation to **PPP**. Activate the interface.
Configure CHAP authentication on S0/0/0.	
Create a local database entry for CHAP authentication.	Username: **R2** Password: **cisco**
Configure Loopback 1 as a simulated web server with user access	Set the Layer 3 IP address: IPv4 Address: 209.165.201.1 255.255.255.252 IPv6 Unicast Address: 2001:DB8:ACAD:2::1/64 IPv6 Link Local Address: FE80::1 Enable http server Create a privileged user to access the web

Step 2: Configure R2.

Configuration tasks for R2 include the following:

Task	Specification
Configure S0/0/0.	Set the description. Set the Layer 3 IP address: IPv4 Address: 209.165.200.226 / 30 IPv6 Unicast Address: 2001:DB8:ACAD:A::2/64 IPv6 Link Local Address: FE80::2 Set the encapsulation to **PPP**. Activate the interface.
Configure CHAP authentication on S0/0/0.	
Create a local database entry for CHAP authentication.	Username: **R1** Password: **cisco**
Configure S0/0/1.	Set the description. Set the Layer 3 IP address: IPv4 Address: 209.165.200.230 / 30 IPv6 Unicast Address: 2001:DB8:ACAD:B::2/64 IPv6 Link Local Address: FE80::2 Activate the interface.

Step 3: Configure R3.

Configuration tasks for R3 include the following:

Task	Specification
Configure S0/0/1.	Set the description. Set the Layer 3 IP address: IPv4 Address: 209.165.200.229 / 30 IPv6 Unicast Address: 2001:DB8:ACAD:B::1/64 IPv6 Link Local Address: FE80::3 Activate the interface.

Part 3: Configure IPv4 ACL for NAT

Step 1: Configure R1.

Configuration tasks for R1 include the following:

Task	Specification
Create NAT (PAT) configuration.	Inside interface g0/1 Outside interface s0/0/0
Configure an ACL for NAT translation.	Standard access list 1 Permit the network that is attached to g0/1 to be translated.

Step 2: Configure R3.

Configuration tasks for R1 include the following:

Task	Specification
Create NAT (PAT) configuration.	Inside interface g0/1 Outside interface s0/0/1
Configure an ACL for NAT translation.	Standard access list 3 Permit the network that is attached to g0/1 to be translated.

Part 4: Configure IP Routing

Step 1: Configure IP routing on R1.

a. Configuration tasks for R1 include the following:

Task	Specification
Configure an IPv4 default route.	Default route to R2 via the exit interface.
Enable IPv6 routing.	
Enable EIGRPv3 routing and router ID	AS: **1** Router ID: **1.1.1.1**
Configure the appropriate IPv6 interfaces for EIGRP	

Step 2: Configure IP routing on R2.

a. Configuration tasks for R2 include the following:

Task	Specification
Enable IPv6 routing.	
Enable EIGRPv3 routing and router ID	AS: **1** Router ID: **2.2.2.2**
Configure the appropriate IPv6 interfaces for EIGRP	

Step 3: Configure IPv6 routing on R3.

a. Configuration tasks for R3 include the following:

Task	Specification
Configure an IPv4 default route.	Default route to R2 via the exit interface with an administrative distance of 200.
Enable IPv6 routing.	
Enable EIGRPv3 routing and router ID	AS: **1** Router ID: **3.3.3.3**
Configure the appropriate IPv6 interfaces for EIGRPv3	

Step 4: Verify network connectivity.

Verify connectivity using the **ping** command to verify connectivity for both IPv4 and IPv6 networks.

From	Command	To	Expected Results
PC1	Ping	192.168.3.10 (PC2)	Ping should not be successful.
PC1	Ping	2001:DB8:ACAD:3::10 (PC2)	Ping should be successful.
PC1	Ping	209.165.200.229 (R3)	Ping should be successful.
PC2	Ping	192.168.1.10 (PC1)	Ping should not be successful.
PC2	Ping	2001:DB8:ACAD:1::10 (PC1)	Ping should be successful.
PC2	Ping	209.165.200.225 (R1)	Ping should be successful.
PC1	Ping	209.165.201.1 (simulated web server)	Ping should be successful.
PC1	Ping	2001:DB8:ACAD:2::1 (simulated web server)	Ping should be successful.
PC2	Ping	209.165.201.1 (simulated web server)	Ping should not be successful.
PC2	Ping	2001:DB8:ACAD:2::1 (simulated web server)	Ping should be successful.

Part 5: Configure GRE Tunnel with BGP

Step 1: Configure GRE tunnel with BGP routing on R1.

Configuration tasks for R1 include the following:

Task	Specification
Configure tunnel 0.	Set IPv4 address (use 172.16.1.0/30 subnet). Set the tunnel source interface. Set the tunnel destination IP address.
Configure a host route.	Set the host route to the tunnel destination with a /32 mask. Use the exit interface.
Configure BGP.	Configure AS 65010 Configure neighbor statement Configure network statements for only networks connected to the Lo1 and G0/1.

Step 2: Configure GRE tunnel with BGP routing on R3.

Configuration tasks for R3 include the following:

Task	Specification
Configure tunnel 0.	Set IPv4 address (use 172.16.1.0/30 subnet) Set the tunnel source interface. Set the tunnel destination IP address.
Configure a host route	Set the host route to the tunnel destination with a /32 mask. Use the exit interface.
Configure BGP.	Configure AS 65030 Configure neighbor statement Configure network statements for only network connected to G0/1 interface.

Step 3: Verify network connectivity.

Verify connectivity using the **ping** command using the IPv4 address.

From	Command	To	Expected Results
PC1	Ping	209.165.201.1 (simulated web server)	Ping should be successful.
PC1	Ping	192.168.3.10 (PC2)	Ping should be successful.
PC2	Ping	209.165.201.1 (simulated web server)	Ping should be successful.
PC2	Ping	192.168.1.10 (PC1)	Ping should be successful.

Part 6: Implement PPPoE

Step 1: Configure PPPoE router.

Configuration tasks for R2 include the following:

Task	Specification
Copy and paste the provided configuration to R2	username Cust1 password ciscopppoe ip local pool PPPoEPOOL 10.0.0.1 10.0.0.10 interface virtual-template 1 ip address 10.0.0.254 255.255.255.0 mtu 1492 peer default ip address pool PPPoEPOOL ppp authentication chap callin exit bba-group pppoe global virtual-template 1 exit interface g0/0 pppoe enable group global no shutdown

Step 2: Configure R3 as a PPPoE client.

Configuration tasks for R3 include the following:

Task	Specification
Configure G0/0 for PPPoE connectivity.	Enable PPPoE on G0/0 interface The client uses dial pool number 1 Activate the interface
Configure the dialer interface 1.	Create the virtual dialer 1 interface Negotiate the IP address from the North Reduce the MTU to 1492 to accommodate the PPP headers Create dialer pool 1 Enforce and assign the chap authentication: username Cust1 / password ciscopppoe Activate the interface
Configure a static default route.	Configure a static default route using the dialer 1 as the exit interface

Step 3: Verify network connectivity.

Verify connectivity using the **ping** command.

From	Command	To	Expected Results
PC1	Ping	192.168.3.10 (PC2)	Ping should be successful.
PC2	Ping	192.168.1.10 (PC1)	Ping should be successful.
R3	Ping	10.0.0.254	Ping should be successful.
PC2	Ping	209.165.201.1 (simulated web server)	Ping should be successful.

Part 7: Configure IP ACLs

Step 1: Configure IP Access List on R1.

Task	Specification
Configure an IPv4 extended access list named ICMP_ACCESS	Deny all pings to the R1 LAN.
Place the ACL at the correct interface and direction	
Ping from PC2 to PC1.	Ping should not be successful.
Ping from PC1 to PC2	Ping should be successful.

Step 2: Configure IPv6 Access List on R3.

Task	Specification
Configure an IPv6 extended access list named LIMIT_ACCESS	Deny all pings to network 2001:DB8:ACAD:3::/64
Place the ACL at the correct interface and direction	
Ping from PC2 to PC1.	Ping should not be successful.
Ping from PC1 to PC2	Ping should be successful.

Part 8: Monitor the Network

Step 1: Configure SNMPv3 on R1.

Configuration tasks for SNMPv3 authentication using an ACL on R1 are the following:

Task	Specification
Create a standard access list to permit only the LAN containing PC1.	Access List: **SNMP-ACCESS**
Using the **snmp-server view** command, configure an SNMP view include specified MIB	SNMP view: **SNMP-RO** MIB included: **ISO**

Using the **snmp-server group** command, configure the SNMP group, SNMP version with authentication and encryption and limit access using an ACL.	Group: **SNMP** Version: **3** Authentication and encryption: **required** Access: **read-only** by using ACL **SNMP-ACCESS**
Using the **snmp-server user** command, add an SNMP user as a member of the **SNMP** using SNMPv3 with authentication and encryption.	Username: JOE Group: SNMP Authentication / Password: SHA / cisco12345 Encryption / Password: AES 128 / cisco54321
Configure an SNMPv3 user on PC1 using an SNMP manager	Use the SNMPv3 setting configured on R1

Step 2: Configure SPAN on S2.

Configuration tasks include the following:

Task	Specification
Issue the SPAN command to monitor the traffic on S2.	Session number: **1** Source switch port on S2: **F0/3**
Issue the SPAN command to capture the traffic on S2.	Session number: **1** Destination switch port on S2: **F0/18**