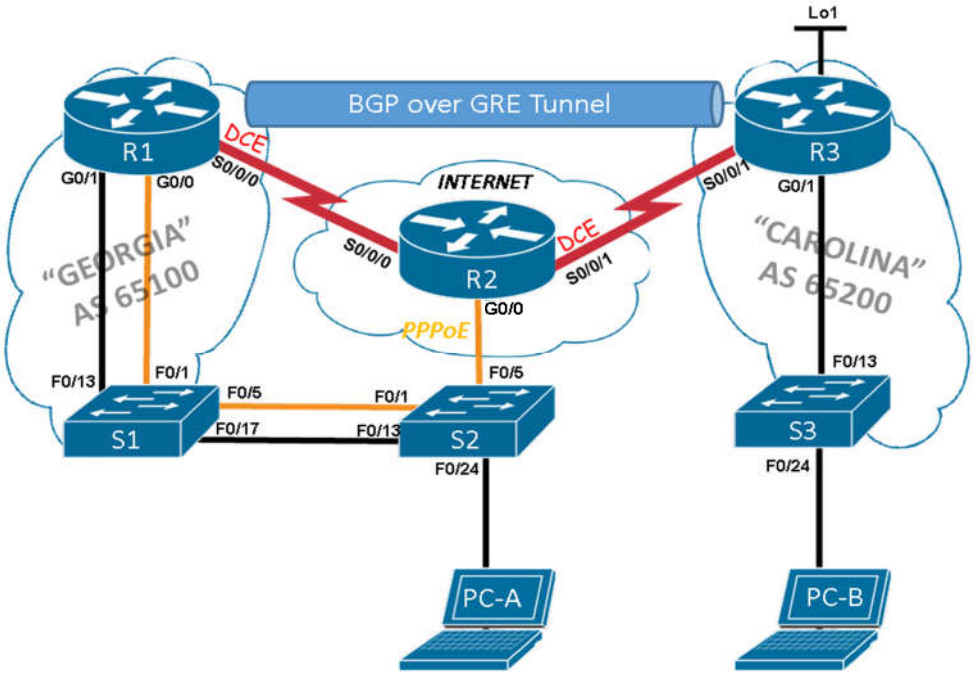
Semester 4: Practice Hands-on Exam



Device	*Interface*	*IP Address*	*Subnet Mask*	*Default Gateway*
R1	S0/0/0	198.198.12.1	255.255.255.252	N/A
	S0/0/0	2001:ACAD:CAFE:12::1	/64	N/A
	S0/0/0	FE80::1	N/A	N/A
	G0/1	172.16.1.1	255.255.255.0	N/A
	G0/1	2001:ACAD:CAFE:1::1	/64	N/A
	G0/1	FE80::1	N/A	N/A
	Tunnel0	192.168.13.1	255.255.255.252	N/A
R2	S0/0/0	198.198.12.2	255.255.255.252	N/A
	S0/0/0	2001:ACAD:CAFE:12::2	/64	N/A
	S0/0/0	FE80::2	N/A	N/A
	S0/0/1	198.198.23.1	255.255.255.252	N/A
	S0/0/1	2001:ACAD:CAFE:23::1	/64	N/A
	S0/0/1	FE80::2	N/A	N/A
R3	S0/0/1	198.198.23.2	255.255.255.252	N/A
	S0/0/1	2001:ACAD:CAFE:23::2	/64	N/A
	S0/0/1	FE80::3	N/A	N/A
	Loopback1	200.150.100.1	255.255.255.255	N/A
	Loopback1	2001:ACAD:CAFE:3333::1	/64	N/A
	G0/1	172.16.3.1	255.255.255.0	N/A
	G0/1	2001:ACAD:CAFE:3::1	/64	N/A
	G0/1	FE80::3	N/A	N/A
	Tunnel0	192.168.13.2	255.255.255.252	N/A
PC-A	NIC	172.16.1.100	255.255.255.0	172.16.1.1
PC-A	NIC	2001:ACAD:CAFE:1::100	/64	FE80::1
PC-B	NIC	172.16.3.100	255.255.255.0	172.16.3.1
PC-B	NIC	2001:ACAD:CAFE:3::100	/64	FE80::3

---

1) **Connect all devices per the topology diagram with the correct cables.**

2) **Configure basic security parameters for R1, R2 and R3.**
   a. Configure the hostnames as applicable (reference the topology).
   b. Disable DNS lookup.
   c. Set the domain to **CISCO-LAB.com**.
   d. Set an encrypted priv. exec. password to **ciscoenpass**.
   e. Set the console password to **ciscoconpass**.
   f. Configure vty to accept SSH only.

g. Add a user and password to the local database for SSH
   - username: **admin**
   - password: **sshpass**

h. Generate an RSA key for SSH (1024 bit modulus).

i. Creating a MOTD banner stating **unauthorized access is prohibited**.

j. Encrypt all clear text passwords.

3) Configure basic security parameters for S1, S2 and S3.

a. Configure the hostnames as applicable (reference the topology).

4) Configure the Layer 3 interfaces for R1, R2 and R3

a. For R1, R2, and R3 set IPv4 and IPv6 addresses for the appropriate serial interfaces. Add descriptions for each active interface.

b. Configure the LAN interfaces (FastEthernet or GigabitEthernet, depending on your router) for R1 and R3.

c. For R3, configure Loopback1 with appropriate IPv4 and IPv6 addresses, as a simulated web server, with user access:
   - enable http server
   - ensure that http uses the local database for authentication
   - create user named **webadmin** with a password of **cisco** privilege 15

d. For all routers, ensure appropriate interfaces have been activated.

5) Configure PPP with Authentication

a. Configure the link from R1 to R2 for CHAP authentication; configure **ciscoppp** as the password.

b. Configure the link from R2 to R3 for PAP authentication; configure **ciscoppp** as the password (remember to configure the sent password).

6) Configure IP Routing

a. For R1, configure an IPv4 default route (administrative distance of **205**) to R2, using the appropriate interface.

b. For R3, configure an IPv4 default route to R2, using the appropriate interface.

c. For R1, R2, and R3 enable EIGRPv6 routing with AS **99**.

d. Set the router-id for each respective router (R1 - **1.1.1.1**, R2 - **2.2.2.2**, R3 - **3.3.3.3**).

e. For R1, R2, and R3 configure the appropriate IPv6 interfaces for EIGRPv6.

7) Configure NAT

a. On R3, configure a standard ACL (**access-list 1**) that will permit the network attached to G0/1 to be translated via NAT

b. On R3, configure **PAT** using S0/0/1's IP address (remember to enable overload functionality)

c. Configure appropriate interfaces as inside/outside

8) Verify Network Connectivity

a. IPv4 ping from PC-A to PC-B should not be successful.

b. IPv6 ping from PC-A to PC-B should be successful

c. IPv4 ping from PC-A to R3 simulated web server (Lo1) should not be successful.

d. IPv6 ping from PC-A to R3 simulated web server (Lo1) should be successful.

e. IPv4 ping from PC-B to PC-A should not be successful.

f. IPv6 ping from PC-B to PC-A should be successful

g. IPv4 ping from PC-B to R1 S0/0/0 should be successful.

h. IPv4 ping from PC-B to R3 simulated web server (Lo1) should be successful.

9) Configure GRE Tunnel w/ eBGP

a. For R1 and R3, create a GRE tunnel interface using the identifier **tunnel0** and assign appropriate IPv4 addresses

b. For R1 and R3, respectively, configure the tunnel using each router's serial interface as the tunnel source and the distant ends IP address as the tunnel destination

c. IPv4 ping from R1 to R3 tunnel IP address should be successful.

d. IPv4 ping from R3 to R1 tunnel IP address should be successful.

10) Configure eBGP

a. For R1 and R3, configure the identified AS numbers for BGP

b. For R1 and R3, configure neighbors statement

c. For R1, add LAN network to the BGP table so it is advertised to R3.

d. For R3, add LAN network and Simulated Web to the BGP table so it is advertised to R1.

11) Verify Network Connectivity

a. IPv4 ping from PC-A to R3 simulated web server (Lo1) should be successful.

b. IPv4 ping from PC-A to PC-B should now be successful.

c. IPv4 ping from PC-B to R3 simulated web server (Lo1) should be successful.

d. IPv4 ping from PC-B to PC-A should now be successful.

12) Implement PPPoE

a. On R2, input the following commands:

- **username R1PPP password ciscoppp**
- **ip local pool PPP_POOL 192.168.1.1 192.168.1.10**
- **interface virtual-template 1**
  - **ip address 192.168.1.254 255.255.255.0**
  - **mtu 1492**
  - **peer default ip address pool PPP_POOL**
  - **ppp authentication chap callin**
  - **exit**
- **bba-group pppoe global**
- **virtual-template 1**
- **exit**
- **interface g0/0**
  - **pppoe enable group global**
  - **no shutdown**

b. On R1, enable PPPoE on G0/0 and configure interface to use dial pool number **1**; ensure the interface is activated.

c. On R1, create a virtual dialer interface 1 and configure the dialer interface as required:

- MTU of **1492**
- IP address will be **negotiated** from R2
- Configure PPP encapsulation
- Create dialer pool **1**
- Enforce CHAP with username of **R1PPP** and password of **ciscoppp**.

d. On R1, configure a default static route using the virtual dialer as the exit interface.

13) Verify Network Connectivity

a. IPv4 ping from PC-A to PC-B should be successful.

b. IPv4 ping from PC-B to PC-A should be successful.

c. IPv4 ping from R1 to R2 PPPoE virtual interface (192.168.1.254) should be successful.

d. IPv4 ping from PC-B to R3 simulated web server (Lo1) should be successful.

14) Configure IP ACLs

a. For R3, configure an extended access list named **PING_BLOCK** that denies all pings to the R3 LAN; place ACL on the correct interface in the appropriate direction.

b. Verify IPv4 ACL:
   i. IPv4 ping from PC-B to PC-A should be successful
   ii. IPv4 ping from PC-A to PC-B should not be successful.

c. For R1, configure an IPv6 extended access list named **IPV6_PING_BLOCK** that denies all pings to the 2001:ACAD:CAFE:1::/64 network ; place ACL on the correct interface in the appropriate direction.

d. Verify IPv6 ACL:
   i. IPv6 ping from PC-B to PC-A should not be successful
   ii. IPv6 ping from PC-A to PC-B should be successful.

Configure SNMPv3

e. On R3, create a standard ACL (**SNMP_PERMIT**) that will permit the SNMP management station (PC-B) to retrieve SNMP information from R3.

f. On R3, configure an SNMP view that includes iso MIB.

g. On R3, configure the SNMP group, version, authentication and encryption, with appropriate ACL utilization, and read-only access.

h. On R3, create an SNMP user named **USER** as a member of the SNMP group, using SNMPv3 with SHA authentication (password **ciscosnmp**) and AES128 encryption (password **ciscoaes**).

i. Configure a SNMPv3 user on PC-B using SNMP management software.

15) Configure IP SLA

a. On R1, configure an IP SLA to ping the Loopback on R3 every 20 sec until you manually stop the IP SLA.

16) Configure SPAN

a. On S2, configure a session (1) for **monitoring** of traffic with a source port of F0/1.

b. On S2, configure a session (1) for **capturing** traffic with a destination port of F0/24.