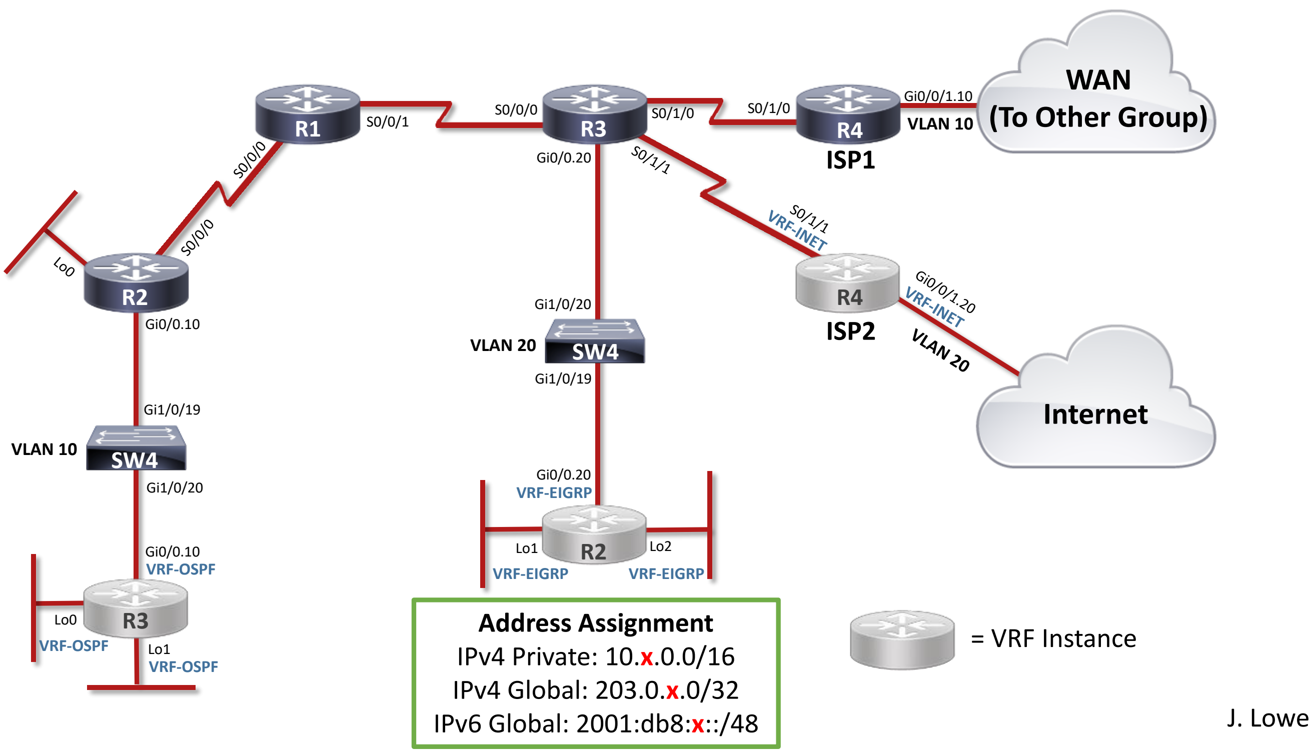
INFR 2411U – Advanced Networking I

CCNP ROUTE Case Study

Topology Diagrams

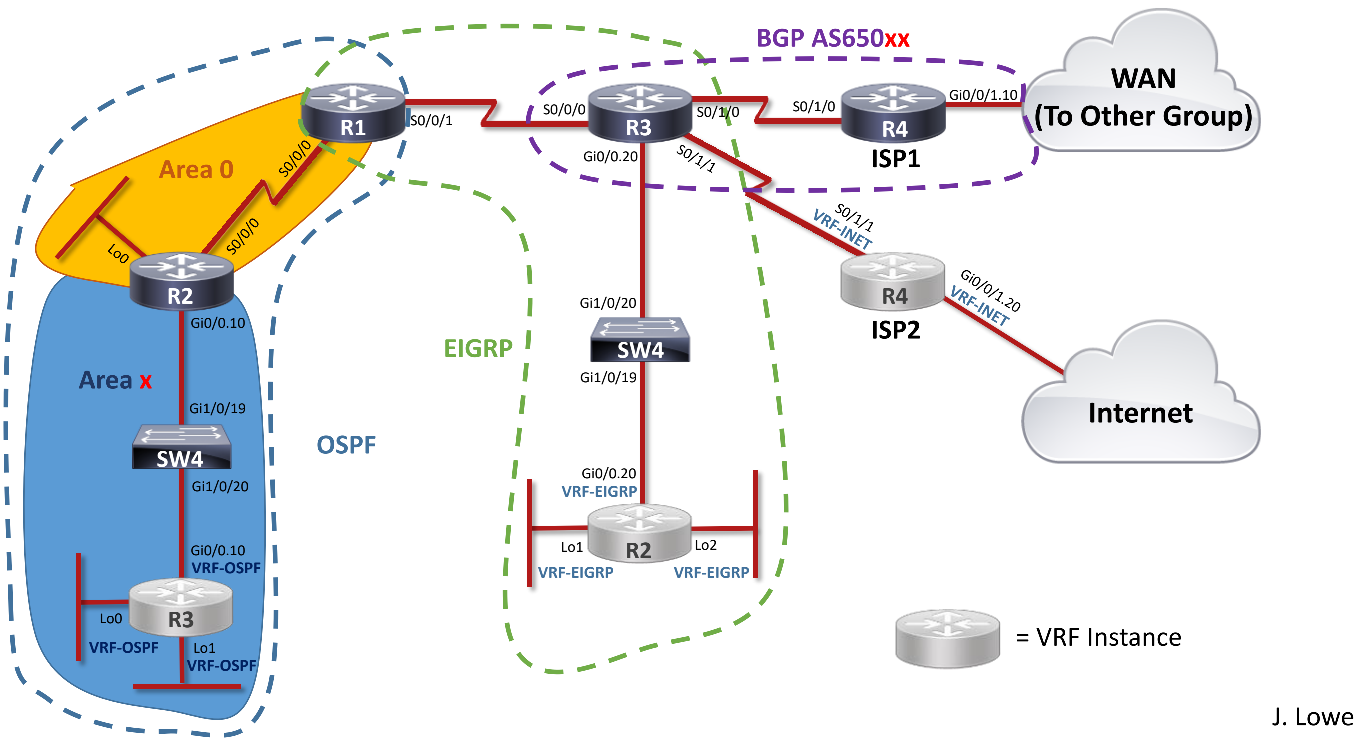
Physical/Logical Topology

This diagram represents the physical and logical topology to be deployed for the main campus of UOIT. The topology presents the physical connectivity of the devices, addressing, as well as some information about virtual interfaces and routing instances.



Routing Protocol Topology

This diagram shows the layout of the routing protocols in use at UOIT. All of the routers in the UOIT network are dual-stack and run both IPv4 and IPv6. The routing protocols in this diagram are configured to exchange both IPv4 and IPv6 routes.



Learning Objectives

To complete this assessment:

- This advanced case study for the Advanced Networking I course at the University of Ontario Institute of Technology is to be completed in teams of no more than two students.
- Assemble the network according to the given topology and instructions. After completing the network configuration, you will connect your network to another group’s network and exchange routing information so that complete connectivity exists between both networks.
- This case study tests the student’s ability to document, configure, maintain and administer an advanced enterprise network running the protocols taught in the Cisco Networking Academy CCNP ROUTE curriculum.

Scenario

In September of 2017 the University of Ontario Institute of Technology (UOIT), has asked your team for assistance in designing and deploying an enterprise network at their main campus in Oshawa.

UOIT has campuses located in both North Oshawa and downtown Oshawa. Both campuses belong to two separate Autonomous System which are connected by a dedicated WAN link through an ISP using BGP. Both networks also have dedicated internet connections through another ISP.

The objective is to design and build the networks for UOIT according to the specifications.

Scoring

The total point value of each configuration task is listed next to the task. In order to receive the number of points listed each task must be fully and properly configured as described. Verification output is required for each task to show that it has been configured correctly. The command **show running-config** is not sufficient in most cases, except where specifically permitted. In some cases, a single command can be used to show successful completion of multiple tasks, so long as the report indicates which tasks are being demonstrated by the output. See the final report guidelines for more details.

Specifications

NOTE: Unless otherwise specified, replace all instances of **x** with your group number.

Task 1: Logical Setup

NOTE: show running-config is acceptable for these tasks, as long as the configuration is trimmed to only show each specific configuration.

(1 point)
- Name all devices according to the topology diagram (R1-R4, SW4).

(1 point)
- Be sure to shut down any unused ports on the routers and switches. Failure to do so will result in unexpected route selections.

(1 point)
- Turn on **ipv6 unicast-routing** on all routers.

(1 point)
- Make a VRF called VRF-OSPF on R3, a VRF called VRF-EIGRP on R2, and a VRF called VRF-INET on R4. Make sure you use the **vrf definition** command, not the **ip vrf** command.

(1 point)
- Assign route distinguishers 650**xx**:**y** where **xx** is your 2-digit group number (e.g. 01, 02, 03…10, 11, etc.) and **y** is the router number (e.g. on R2 **y** = 2) to your VRFs.

(1 point)
- Add both the IPv4 and IPv6 address families to each VRF.

(3 points)
- Assign interfaces to the VRFs as shown in the topology diagram.

(1 point)
- Create the VLANs on the switch as indicated in the topology diagram. Gi1/0/19 & Gi1/0/20 should both be set as static trunk links. Set VTP to Transparent mode.

(1 point)
- Set the clock rate of each serial link to 64,000 bps on all DCE interfaces.

Task 2: Addressing

- **(2 points)** Where possible, design your addressing scheme in a hierarchical method that allows for easy summarization. Create a diagram with your IPv4 and IPv6 addresses clearly labeled, and include it in your final report.
- **(1 point)** Assign R3 s0/1/1 the IPv4 address 203.0.x.1/29 and R4 s0/1/1 the IPv4 address 203.0.x.2/29.
- **(1 point)** Assign R3 s0/1/0 the IPv4 address 172.16.x.1/30 and R4 s0/1/0 the IPv4 address 172.16.x.2/30.
- **(1 point)** Assign R3 s0/1/1 the IPv6 address 2001:DB8:x:ABCD::1/64 and R4 s0/1/1 the IPv6 address 2001:DB8:x:ABCD::2/64.
- **(1 point)** Assign R4 Gi0/0/1.10 (VLAN 10) the IPv4 address 199.212.32.x/24.
- **(1 point)** Assign R4 Gi0/0/1.20 (VLAN 20) the IPv4 address 203.1.1.x/24 and the IPv6 address 2001:DB8:0:0::x/64.
- **(1 point)** Assign a /24 IPv4 subnet and a /64 IPv6 subnet to each Loopback interface. Use the pools shown in the diagram. Assign the first address in the range to the router interface.
- **(1 point)** Assign a /30 IPv4 subnet and a /64 IPv6 subnet to each point-to-point link between routers. Use the pools shown in the diagram. Give the lower numbered router the first address in each range, and the other router the second address.
- **(1 point)** Statically configure link-local addresses on each router interface to be FE80::y, where y is the router number (e.g. R3 would have FE80::3 on all of its interfaces).

NOTE: ISP1 only runs IPv4, and does not support IPv6. ISP2 supports both IPv4 and IPv6 using the global addresses assigned to you.

Task 3: Configure OSPF

- **(1 point)** Use a process number equal to your group number.
- **(1 point)** Set the bandwidth of all interfaces appropriately.
- **(1 point)** Change the OSPF reference bandwidth to 100Gbps.
- **(6 points)** Enable OSPFv3 on R1, R2, and R3 for both IPv4 and IPv6 address families, on the interfaces indicated in the diagram. (Note that the commands all start with "**ospfv3**", not the older "**ipv6 router ospf**" or "**ip ospf**" commands).
- **(1 point)** Use the router number as the router ID (e.g., on R1 use 1.1.1.1). Use this router ID for IPv4, IPv6, and the VRF address families as applicable.
- **(1 point)** Change the network type on the loopback interfaces so that the routes are advertised with the correct subnet mask.
- **(1 point)** Configure all Loopback interfaces as passive.
- **(2 points)** Configure area x as a totally stubby area for both IPv4 and IPv6.
- Note that on R3 in the VRF address family (IPv4 and IPv6) you must include the following command for your routes to show up in the routing table: **capability vrf-lite**

Task 4: Configure EIGRP

- **(1 point)** Use an AS number equal to your group number.
- **(1 point)** Set the bandwidth of all interfaces appropriately.
- **(6 points)** Enable EIGRP Named Mode on R1, R2, and R3, for both IPv4 and IPv6, as indicated in the diagram. Name your EIGRP process **CASE2017**
- **(1 point)** Use /32 wlidcard masks for each interface in your **network** commands.
- **(1 point)** Use the router number as the router ID (e.g., on R1 use 1.1.1.1). Use this router ID for IPv4, IPv6, and the VRF address families as applicable
- **(1 point)** By default, all IPv6 interfaces participate in EIGRP Named Mode. Remove EIGRP from interfaces where it is not required (check **show ipv6 eigrp interface)**.
- **(1 point)** Configure all Loopback interfaces as passive.
- **(1 point)** Configure R2 VRF-EIGRP as a stub router in both IPv4 and IPv6, advertising only connected routes.

Task 5: Configure Redistribution and Summarization

- **(4 points)** Perform mutual redistribution between EIGRP and OSPF on R1 for both IPv4 and IPv6. For EIGRP metrics use the following values:

  Bandwidth: 1 Gbps
  Delay: 200 µsec
  Reliability: 255/255
  Load: 1/255
  MTU: 1500

- **(2 points)** Create a static default route on R3 pointing to the IPv4 address of ISP2 (R4). Do the same for IPv6.
- **(1 point)** Create a static default route on R4 to 203.1.1.254 (a gateway on the Internet).
- **(1 point)** Distribute the default route for IPv4 and IPv6 via redistribution into EIGRP, using the metrics given previously for R1.
- **(1 point)** On R1, originate a default route into OSPFv3, only as long as there is a default route already in R1's routing table.
- **(1 point)** Create a static route on R4 to the 2001:db8:x::/48 subnet. Be sure this route is created in the VRF-INET VRF.
- **(2 points)** Summarize the IPv4 routes in OSPF Area x to the most efficient summary address and advertise it into Area 0.
- **(2 points)** Create a single EIGRP summary route on the R1 interface to R3, summarizing all of the IPv6 routes in the OSPF network as efficiently as possible.

Task 6: Configure MP-BGP

- **(1 point)** The BGP AS number is 650**xx**, where **xx** is your 2-digit group number (e.g. 01, 02, 03…10, 11, etc.).
- **(1 point)** Use router ID **x**.y.**y**.**y**, where **x** is your group number and **y** is the router number (e.g. Group 5 would use 5.3.3.3 on R3)
- **(2 points)** Configure iBGP neighbor relationships between R3 and R4 as shown in the topology diagram.
- **(2 points)** Configure R3 and R4 to advertise themselves as the next hop for all IPv4 routes they exchange with each other.
- **(1 point)** The configuration should use MP-BGP to carry both IPv4 and IPv6 routes (IPv6 will be configured in Task 8).
- **(1 point)** Advertise all subnets of the 10.**x**.0.0/16 networks, except any /32 routes, from R3 to R4. Do not add any static or summary routes to accomplish this.
- **(1 point)** Also advertise the 172.16.**x**.0/30 subnet.
- **(2 points)** Configure R3 to set a Local Preference of 500 on all routes received from R4

Task 7: Configure NAT

- **(2 points)** Configure NAT on R3 for all IPv4 connections to the Internet. Specifically, use NAT Overload (PAT) so that all outbound connections from 10.**x**.0.0/16 will be translated to the IP address assigned to the s0/1/1 interface of R3.
- **(1 point)** Create a static NAT mapping for the IPv4 address of R2's Loopback interface to the global address 203.0.**x**.3

NOTE: because we are using global IPv6 addresses on all of our subnets (given to us by our ISP), we do not need NAT for IPv6 connections to the Internet.

Task 8: Connecting Pods

NOTE: for this task you and your **partner group** must be working on two pods in the same rack (e.g. pods 1 & 2, pods 3 &4, etc.). The pods have been connected together through a switch at the bottom of the rack. The R4 Gi0/0/1.10 interfaces on both pods are connected to the common switch.

- **(1 point)** Create a tunnel interface on R3 running GRE over IPv4. The tunnel source should be s0/1/0 and the destination should be the address of the **other pods** R3 s0/1/0 interface. Give the tunnel interface the IPv6 address FEC0:1::**x**/64. The tunnel should not have any IPv4 address.
- **(2 points)** Configure MP-BGP on both R3 routers and form eBGP neighbor relationships between them using their FEC0:1::/64 addresses. These BGP routers should exchange only IPv6 routes.
- **(1 point)** Advertise all subnets of the 2001:db8:**x**::/48 from R3 to the **other pod**, except any /128 routes you may have in your routing table.
- **(1 point)** Form an eBGP neighbor relationship between R4 on your pod an R4 on the **other pod**. This relationship should be made using the IPv4 addresses on your Gi0/0/1.10 interfaces.
- **(1 point)** Advertise all IPv4 routes available on R4 to the other group via MP-BGP.
- **(2 points)** Configure R4 to set the MED to 50 on all IPv4 routes sent to the **other pod**.

Task 9: Testing

(3 points)
- Verify that you have full reachability from one end of the network to the other end of the other group's network. All devices should be able to reach all other devices using either IPv4 or IPv6, with the exception of R4 on the VRF-INET VRF, which should only be able to ping inbound to 203.0.**x**.3 (which translates to R2's Loopback interface). Create TCL scripts that can be run to test this connectivity on any router in the network, and include them in your final report. Keep in mind that VRFs will need to be included in the ping commands on some routers to properly test connectivity.

(1 point)
- A web server has been configured to respond to HTTP requests on 198.51.100.1 port 80. From R3, in the VRF-OSPF VRF, telnet to this address on port 80, type GET, and verify that you receive a web response.

Additional Tasks

Security

- In addition to the configuration tasks, UOIT has asked that you help secure their new network. They have asked that you configure at least one additional security feature for each routing protocol in use (OSPF, EIGRP, and BGP). Different features should be configured for each protocol.
- Additionally, they have asked you to configure three more security features in the network that are unrelated to any specific routing protocol (configuring a username and password is not sufficient).
- UOIT has asked that you include the details of these configurations in your case study report. The details should include, for each security feature:
  1. What the chosen security feature does
  2. Why you chose that specific feature
  3. Where you implemented the feature in your network
  4. The configurations you used to implement the feature