INFR 2421U – Advanced Networking II

2024 Case Study

Scenario

In Winter of 2024 Ontario Tech University has asked your team for assistance in designing and deploying a new LAN and WAN infrastructure.

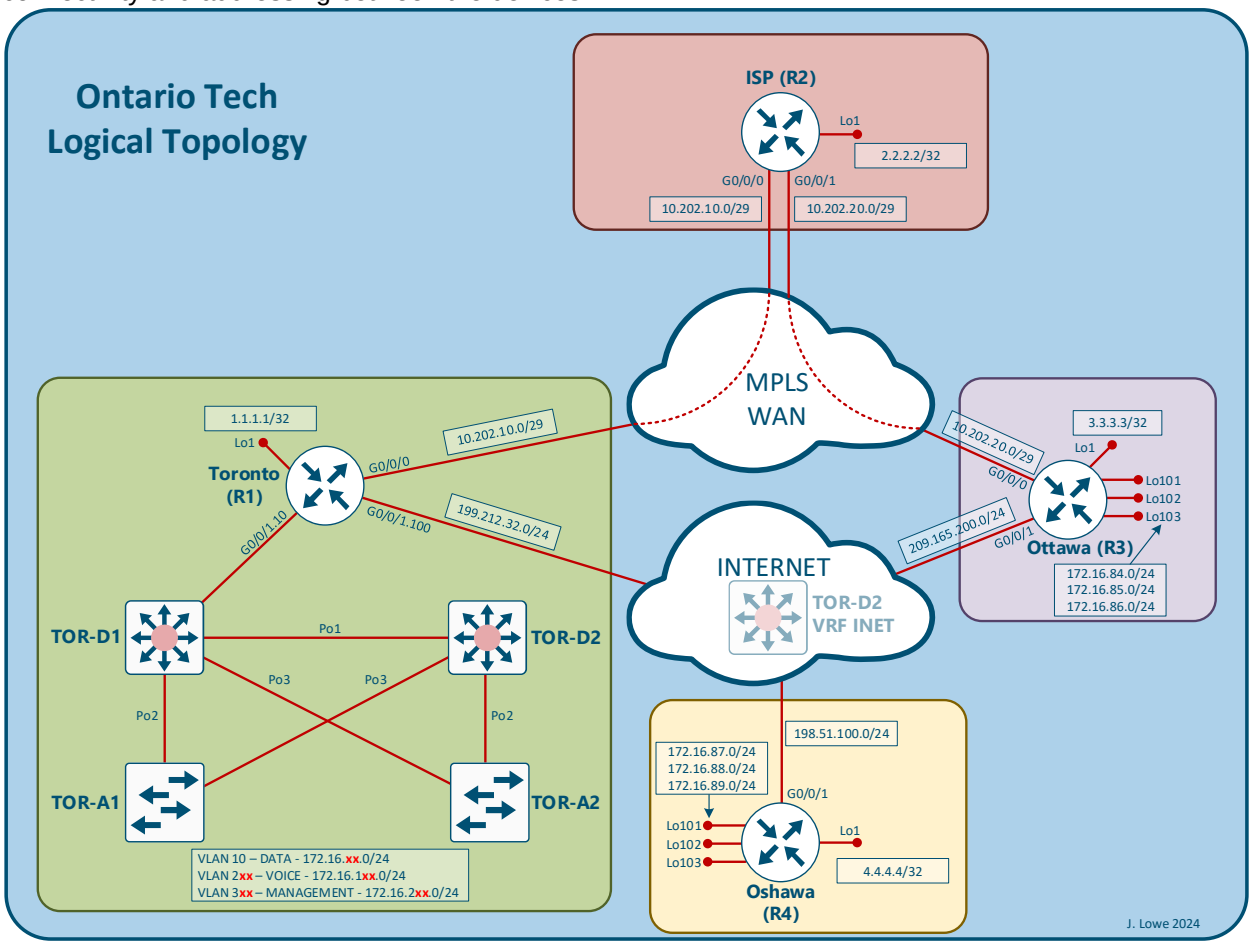
Ontario Tech currently has a campus in north Oshawa and is opening new campuses in Toronto and Ottawa. All three campuses already have Internet access through various service providers. They are looking to connect the Toronto and Ottawa campuses together through an MPLS WAN. As a backup they would also like to connect all three campuses together through the Internet using a DMVPN. The Toronto campus also needs a new switched LAN infrastructure designed and configured.

Your objective is to design and build the networks for Ontario Tech according to their specifications.

Topology Diagrams

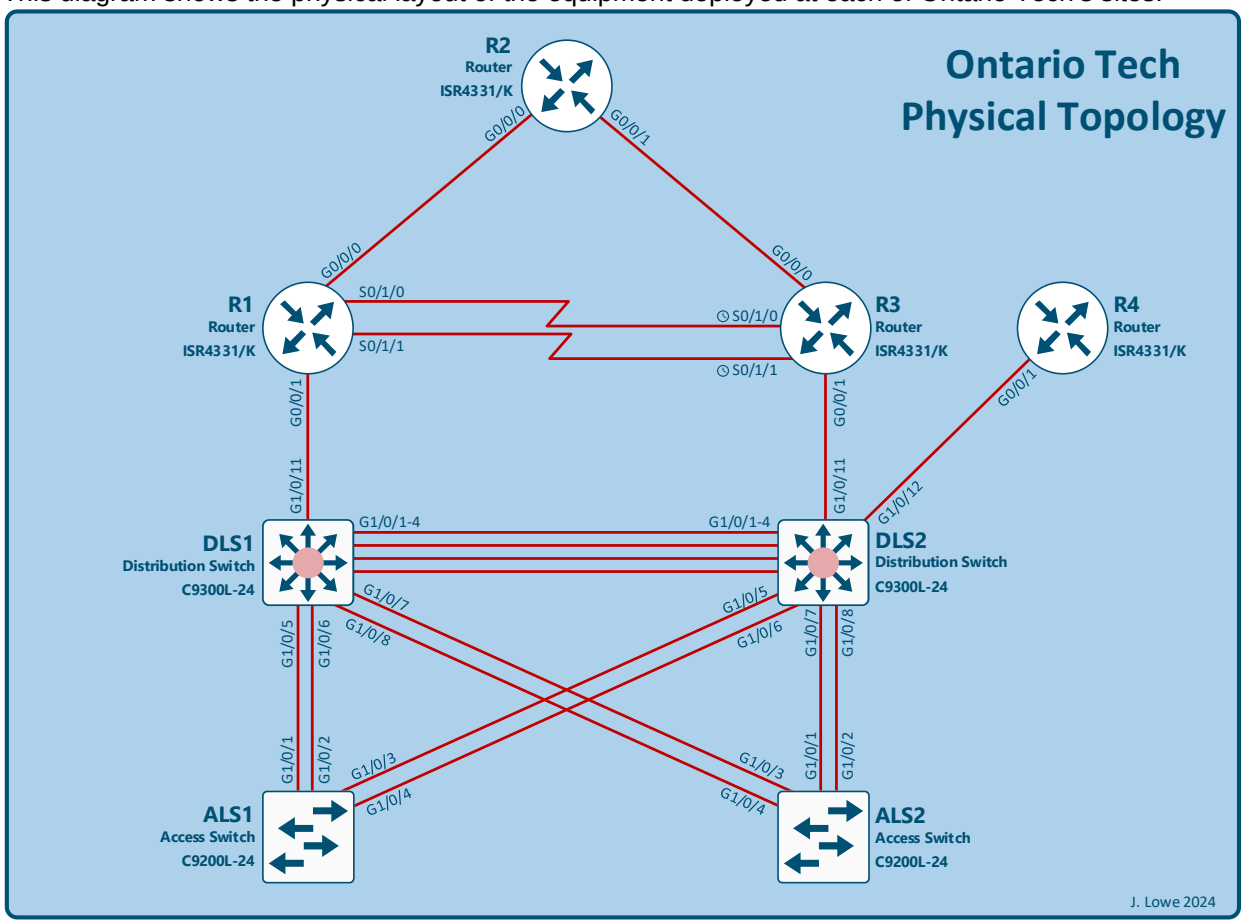
Logical Topology

This diagram represents the logical topology to be deployed for Ontario Tech. The topology presents the logical connectivity and addressing between the devices.



Physical Topology

This diagram shows the physical layout of the equipment deployed at each of Ontario Tech's sites.



Learning Objectives

To complete this assessment:

- This advanced case study for the Advanced Networking II course at Ontario Tech University is to be completed in teams of no more than three students.
- Assemble the network according to the given topology and instructions.
- After completing the network configuration, verify connectivity between each of the campuses as per the requirements.

Scoring

To receive full marks, 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. **These outputs must be screenshots, not copy and pasted text**. See the final report guidelines for more details.

Specifications

NOTE: Unless otherwise specified, replace all instances of **xx** with your group number assigned on Canvas (e.g., 01, 02, 03…50).

Task 0: Initial Configurations (No marks)

Ontario Tech already has some basic configurations on the routers and switches providing basic connectivity. Copy the configurations from the **Appendix** to each of the devices. This must be done **BEFORE** you start any of the other tasks.

Important Note: VTP and VLAN information is NOT stored in the running configuration except in VTP transparent mode. You will need to manually reconfigure VTP and the VLANs each time you copy/paste your configurations into the devices. It helps to keep these commands in a separate text file that you can copy to the devices.

Task 1: Addressing

- Using the addressing table below, assign IP addresses to each of the interfaces. **Note:** some interfaces have already been pre-configured in **Task 0**. The tunnel interfaces and SVIs will be created and addressed in a later step.

Addressing Table

Device	Interface	IP Address
Toronto	G0/0/0	10.202.10.1/29
	G0/0/1.10	172.16.**xx**.1/24
	G0/0/1.100	199.212.32.**xx**/24
	Lo1	1.1.1.1/32
	Tun1	10.1.**xx**.1/24
ISP	G0/0/0	10.202.10.2/29
	G0/0/1	10.202.20.2/29
	Lo1	2.2.2.2/32
Ottawa	G0/0/0	10.202.20.3/29
	G0/0/1	209.165.200.**xx**/24
	Lo1	3.3.3.3/32
	Lo101	172.16.84.**xx**/24
	Lo102	172.16.85.**xx**/24
	Lo103	172.16.86.**xx**/24
	Tun1	10.1.**xx**.2/24
Oshawa	G0/0/1	198.51.100.**xx**/24
	Lo1	4.4.4.4/32
	Lo101	172.16.87.**xx**/24
	Lo102	172.16.88.**xx**/24
	Lo103	172.16.89.**xx**/24
	Tun1	10.1.**xx**.3/24

TOR-D1	VLAN 10	172.16.**xx**.0/24 subnet
	VLAN 2**xx**	172.16.1**xx**.0/24 subnet
	VLAN 3**xx**	172.16.2**xx**.0/24 subnet
TOR-D2	VLAN 10	172.16.**xx**.0/24 subnet
	VLAN 2**xx**	172.16.1**xx**.0/24 subnet
	VLAN 3**xx**	172.16.2**xx**.0/24 subnet
	VLAN 100	199.212.32.254/24
	VLAN 300	209.165.200.254/24
	VLAN 400	198.51.100.254/24
TOR-A1 and TOR-A2	VLAN 10	172.16.**xx**.0/24 subnet
	VLAN 2**xx**	172.16.1**xx**.0/24 subnet
	VLAN 3**xx**	172.16.2**xx**.0/24 subnet

Task 2: Switch Configuration

- Configure all four switches to be in the VTP domain **OTUxx**. **TOR-D1** should be the **primary VTPv3 server** for VLANs, and the remaining switches should be set as **clients**.
- Create the following VLANs on the switches:
    - **DATA** **10**
    - **VOICE** **2xx**
    - **MANAGEMENT** **3xx**
    - **R1-INET** **100**
    - **R3-INET** **300**
    - **R4-INET** **400**
    - **NATIVE** **123**
    - **UNUSED** **999**
- Configure all switch-to-switch connections to **static trunk** links. **Disable DTP**.
- Set the native VLAN to **123** and manually prune the trunks to only allow the following VLANs:
    - **TOR-D1** to **TOR-D2**: **10,100,2xx,3xx**
    - **TOR-D1** to **TOR-A1**: **10,2xx,3xx**
    - **TOR-D1** to **TOR-A2**: **10,2xx,3xx**
    - **TOR-D2** to **TOR-A1**: **10,2xx,3xx**
    - **TOR-D2** to **TOR-A2**: **10,2xx,3xx**
- Configure interface **G1/0/11** on **TOR-D1** as a **static trunk port**. **Disable DTP** and prune the links to only allow **VLANs 10 and 100**.
- Configure interfaces **G1/0/11** and **G1/0/12** on **TOR-D2** as **static access ports**. Interface **G1/0/11** should be in **VLAN 300**, and interface **G1/0/12** should be in **VLAN 400**.
- Configure all remaining unused switch interfaces to be **shut down** and **static access ports** in **VLAN 999**. (See the topology diagrams for details)
- Enable **PAgP** EtherChannels along links between the **Access Layer** switches and **TOR-D1**. Enable **LACP** EtherChannel between the **Access Layer** switches and **TOR-D2**. Configure the Etherchannel between the **Distribution Layer** switches to be **statically** defined. Use the port channel numbers shown in the logical topology diagram. It is up to you to decide how the dynamic channel groups are formed.
- Create an SVI on each switch in the **DATA**, **VOICE**, and **MANAGEMENT** VLANs, and apply an IPv4 address from the appropriate subnets to each interface (see the Addressing Table for more details). Do not use .1 or .254 for these addresses.

Task 3: Configure Spanning Tree

- Make **TOR-D1** the spanning-tree root bridge for VLANs **10** and 3**xx** and make **TOR-D2** the root bridge for VLAN **2xx**.
- Make **TOR-D1** the backup root bridge for VLAN **2xx** and make **TOR-D2** the backup root bridge for VLANs **10** and **3xx**.
- Modify the Spanning Tree port costs on **TOR-A1** so that it chooses the **Po3** link rather than the **Po2** link as the root port for VLAN **10**. Use a value equal to **two times your group number, plus 10**, as the cost
- Configure PortFast and BPDU Guard on the **G1/0/12-24** ports on both **TOR-A1** and **TOR-A2**.
- Configure Root Guard on **TOR-D1** and **TOR-D2** ports **G1/0/5** and **G1/0/6**.

Task 4: Configure First Hop Redundancy

- Configure **TOR-D1** and **TOR-D2** to use HSRPv2 for VLANS **10**, **2xx**, and **3xx**. Make **TOR-D1** the primary gateway for VLAN **10** and **3xx** and **TOR-D2** the primary gateway for VLAN **2xx**. Enable **preemption** on both switches. Use the **last available host address** in each subnet as the HSRP virtual IP address. The HSRP group numbers should be **two times your group's number (x) plus the VLAN number**.
- Configure object tracking on **TOR-D2** so it decreases its priority for VLAN **2xx** to be less than TOR-D1's priority if **PortChannel2** goes down. Use a tracking number equal to the HSRP group number for VLAN **2xx**.
- Configure **TOR-A1** and **TOR-A2** with a default gateway address of the HSRP virtual IP address of VLAN **10**.

Task 5: Configure MPLS

Note: Typically, customer routers do not participate in MPLS at all in the real world, but we are making an exception so that ISP is not the only MPLS router in the topology.

- Enable MPLS on the link between **Toronto** and **ISP**, and the link between **Ottawa** and **ISP**.
- Set the label protocol to **LDP**.
- Force the routers to use their **Loopback 1** interfaces as the LDP router ID.

Task 6: Configure DMVPN Phase 3

- Configure a **Tunnel1** interface on **Toronto**, **Ottawa**, and **Oshawa**.
    - Set the tunnel interfaces on all three routers to use **multipoint GRE**.
    - Set the tunnel **source** on all three routers to be the interface connecting to the Internet.
    - Set the tunnel **key** on all three routers to be **three times your group number**.
    - Set the IP address of the tunnel interfaces as follows:
        - **Toronto**: **10.1.xx.1/24**
        - **Ottawa**: **10.1.xx.2/24**
        - **Oshawa**: **10.1.xx.3/24**
- Set the bandwidth of the tunnel interface to **1,000,000** and the delay to **two times your group number plus 20**.
- Configure NHRP in a hub-and-spoke topology, where **Toronto** is the hub:
    - Use a **network ID** of **xx**.
    - Set the **NHRP authentication** value as the first letter of each of your group member's names, in all capitals (for example, John, Mary, and Luke would use **JML** as the authentication password).
    - On **Toronto**, configure NHRP to **dynamically** map **multicast** traffic for the tunnel endpoints.

- On **Ottawa** and **Oshawa**, configure **Toronto's** tunnel IP as the **next hop server**.
- On **Ottawa** and **Oshawa**, statically map **Toronto's** tunnel IP address to its Internet IP address.
- On **Ottawa** and **Oshawa**, statically map **multicast** addresses to **Toronto's** Internet IP address.
- Configure **Toronto** to send **NHRP redirects**, and **Ottawa** and **Oshawa** to use **NHRP shortcuts** to enable Phase 3 DMVPN.

- Secure the DMVPN tunnels using IPSec:
  - Configure the following IKE policy:
    - ISAKMP policy number: **xx**
    - Hash: **SHA 512**
    - Encryption: **AES 256**
    - DH group number: **14**
    - Authentication: **Pre-shared Key**
    - Pre-shared key: Group member first initials and group number (e.g., **JML50**) for all addresses (**0.0.0.0**)
  - Configure the following IPSec transform set:
    - Transform set name: Group member first initials and group number followed by "_TRANS" (e.g., **JML50_TRANS**)
    - Encryption: **AES 256**
    - Hash: **SHA 512 HMAC**
    - Use **Transport** mode
  - Configure the following IPSec profile:
    - Profile name: Group member first initials and group number followed by "_PROFILE" (e.g., **JML50_PROFILE**).
    - Use the transform set created previously.
    - Assign this profile to the tunnel interface on all three routers.

Task 7: Configure Routing

- Enable EIGRP Named Mode for the IPv4 address family on all four routers. Name your EIGRP process **OntarioTechxx**. Use **xx** as the AS number for the EIGRP process.
- Use the following router IDs on each device:
  - **Toronto**: **1.1.1.1**
  - **ISP: 2.2.2.2**
  - **Ottawa**: **3.3.3.3**
  - **Oshawa**: **4.4.4.4**
- On **Toronto**, **Ottawa**, and **Oshawa** enable EIGRP on the DMVPN tunnel interfaces (not the physical interfaces).
- On **Toronto**, **ISP**, and **Ottawa**, enabled EIGRP on the MPLS interfaces.
- On **Toronto**, enable EIGRP on the **G0/0/1.10** interface and make it **passive**.
- Enable EIGRP on all loopbacks on all four routers.
- On **Toronto**, configure an EIGRP summary route for **172.16.0.0/16** on the **tunnel interface** to trigger the DMVPN spokes to perform next-hop resolution for any addresses in the LAN subnets.
- Create a static default route on **TOR-D1** and **TOR-D2** with a next hop of **Toronto's G0/0/1.10** interface.
- On **Toronto**, create a static route to **172.16.0.0/16** with a next hop of **172.16.xx.254**

Task 8: Configure IP Services

- Configure the correct time zone (**EST UTC-5**) and daylight savings time (**EDT UTC-4**) settings on all routers and switches (use the default summer-time settings).
- Set the clock on **ISP** with the correct time and date.
- Configure **ISP** to be a **stratum 2 NTP server**.
- Configure **Toronto**, **Ottawa**, **Oshawa** to synchronize their time with **ISP** using **ISP**'s Loopback 1 interface.
- Configure **TOR-D1**, **TOR-D2**, **TOR-A1**, and **TOR-A2** to synchronize their time with **Toronto** using **Toronto**'s Loopback 1 interface.

Task 9: Testing (Include Screenshots in Report)

- To verify connectivity, execute the following TCL script on all devices **except ISP**. **ISP** will not have all the customer routes.

```
tclsh

foreach address {
10.1.xx.1
10.1.xx.2
10.1.xx.3
172.16.xx.1
172.16.84.xx
172.16.85.xx
172.16.86.xx
172.16.87.xx
172.16.88.XX
172.16.89.XX
172.16.xx.254
172.16.1xx.254
172.16.2xx.254
} { ping $address }

tclquit
```

- Test that **Toronto** and **Ottawa** are using the MPLS WAN to reach each other's subnets, and the DMVPN over the Internet as a backup:
  - Do a traceroute from **Ottawa** to the **DATA** SVI on **TOR-A2** to show that it is going through the ISP over the MPLS WAN (you should see an MPLS label in the trace).
  - Shut down the MPLS WAN interfaces on **Toronto** and **Ottawa** (**Gig0/0/0**).
  - Run the TCL script above on all devices **except ISP**. The pings should still all be successful.
  - Do another traceroute from **Ottawa** to the **DATA** SVI on **TOR-A2** to show that packets are now going through the Internet over the DMVPN tunnel.
  - Bring the MPLS WAN interface back up before continuing.
- Check that ISAKMP and IPSec SAs are being created on the three tunnel interfaces and that you are seeing packets **encrypted/decrypted**.
- Check that **Toronto** has NHRP mappings for both **Ottawa** and **Oshawa**, showing NHRP and DMVPN are working.
- Check that **Ottawa** and **Oshawa** have NHRP **shortcuts** to each other, showing phase 3 DMVPN is working.

- Check that the clock is synchronized on all devices via NTP. ISP should be stratum 2 and the other routers should be stratum 3. All four switches should be stratum 4.
- Check that HSRP interface tracking is working by shutting down interface **PortChannel2** on **TOR-D2**. **TOR-D1** should take over as the HSRP active router for VLAN **2xx**. Bring the **PortChannel2** interface back up and verify that **TOR-D2** takes back the active role.

Appendix

Initial Configurations

Toronto (R1):

```
hostname Toronto
!
no ip domain lookup
!
interface Loopback1
 ip address 1.1.1.1 255.255.255.255
 ip nat inside
!
interface GigabitEthernet0/0/0
 description Link to MPLS Cloud
 ip address 10.202.10.1 255.255.255.248
 no shutdown
!
interface GigabitEthernet0/0/1
 description Trunk Link to D1
 no ip address
 no shutdown
!
interface GigabitEthernet0/0/1.10
 description Link to D1 Local LAN
 encapsulation dot1Q 10
 ip nat inside
!
interface GigabitEthernet0/0/1.100
 description Link to D1 Internet
 encapsulation dot1Q 100
 ip nat outside
!
interface Serial0/1/0
 shutdown
!
interface Serial0/1/1
 shutdown
!
interface GigabitEthernet0
 shutdown
!
ip nat inside source list NAT-ACL interface GigabitEthernet0/0/1.100 overload
ip route 0.0.0.0 0.0.0.0 199.212.32.254
!
ip access-list standard NAT-ACL
 20 permit 1.1.1.1
 10 permit 172.16.0.0 0.0.255.255
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
end
```

ISP (R2):

```
hostname ISP
!
no ip domain lookup
!
interface Loopback1
 ip address 2.2.2.2 255.255.255.255
!
interface GigabitEthernet0/0/0
 description Link to MPLS Cloud
 ip address 10.202.10.2 255.255.255.248
 no shutdown
!
interface GigabitEthernet0/0/1
 description Link to MPLS Cloud
 ip address 10.202.20.2 255.255.255.248
 no shutdown
!
!
interface GigabitEthernet0
 shutdown
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
end
```

Ottawa (R3):

```
hostname Ottawa
!
no ip domain lookup
!
interface Loopback1
 ip address 3.3.3.3 255.255.255.255
 ip nat inside
!
interface Loopback1
 ip nat inside
!
interface Loopback101
 ip nat inside
!
interface Loopback102
 ip nat inside
!
interface Loopback103
 ip nat inside
!
interface GigabitEthernet0/0/0
 description Link to MPLS Cloud
 ip address 10.202.20.3 255.255.255.248
 no shutdown
!
interface GigabitEthernet0/0/1
 description Link to Internet
```

```
 ip nat outside
 no shutdown
!
!
interface Serial0/1/0
 no ip address
 clock rate 64000
 shutdown
!
interface Serial0/1/1
 no ip address
 clock rate 64000
 shutdown
!
interface GigabitEthernet0
 shutdown
!
ip nat inside source list NAT-ACL interface GigabitEthernet0/0/1 overload
ip route 0.0.0.0 0.0.0.0 209.165.200.254
!
!
ip access-list standard NAT-ACL
 20 permit 3.3.3.3
 10 permit 172.16.0.0 0.0.255.255
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
end
```

Oshawa (R4):

```
hostname Oshawa
!
no ip domain lookup
!
interface Loopback1
 ip address 4.4.4.4 255.255.255.255
 ip nat inside
!
interface Loopback101
 ip nat inside
!
interface Loopback102
 ip nat inside
!
interface Loopback103
 ip nat inside
!
interface GigabitEthernet0/0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0/1
 description Link to Internet
 ip nat outside
 no shutdown
```

```
!
interface GigabitEthernet0
 shutdown
!
ip nat inside source list NAT-ACL interface GigabitEthernet0/0/1 overload
ip route 0.0.0.0 0.0.0.0 198.51.100.254
!
ip access-list standard NAT-ACL
 20 permit 4.4.4.4
 10 permit 172.16.0.0 0.0.255.255
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
end
```

TOR-D1 (D1):

```
hostname TOR-D1
!
ip routing
!
no ip domain lookup
!
vlan 100
 name R1-INET
!
interface GigabitEthernet0/0
 shutdown
!
!
interface range GigabitEthernet1/0/12-24, GigabitEthernet1/1/1-4,AP1/0/1
 shutdown
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
end
```

TOR-D2 (D2):

```
hostname TOR-D2
!
vrf definition INET
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
ip routing
!
no ip domain lookup
!
vlan 100
```

```
 name R1-INET
!
vlan 300
 name R3-INET
!
vlan 400
 name R4-INET
!
interface GigabitEthernet0/0
 shutdown
!
interface range GigabitEthernet1/0/13-24, GigabitEthernet1/1/1-4,AP1/0/1
 shutdown
!
interface Vlan100
 vrf forwarding INET
 ip address 199.212.32.254 255.255.255.0
!
interface Vlan300
 vrf forwarding INET
 ip address 209.165.200.254 255.255.255.0
!
interface Vlan400
 vrf forwarding INET
 ip address 198.51.100.254 255.255.255.0
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
end
```

TOR-A1 (A1):

```
hostname TOR-A1
!
no ip domain lookup
no ip routing
!
interface GigabitEthernet0/0
 shutdown
!
interface range GigabitEthernet1/0/5-24,GigabitEthernet1/1/1-4
 shutdown
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
end
```

TOR-A2 (A2):

```
hostname TOR-A2
!
no ip domain lookup
no ip routing
!
```

```
interface GigabitEthernet0/0
 shutdown
!
interface range GigabitEthernet1/0/5-24,GigabitEthernet1/1/1-4
 shutdown
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
end
```