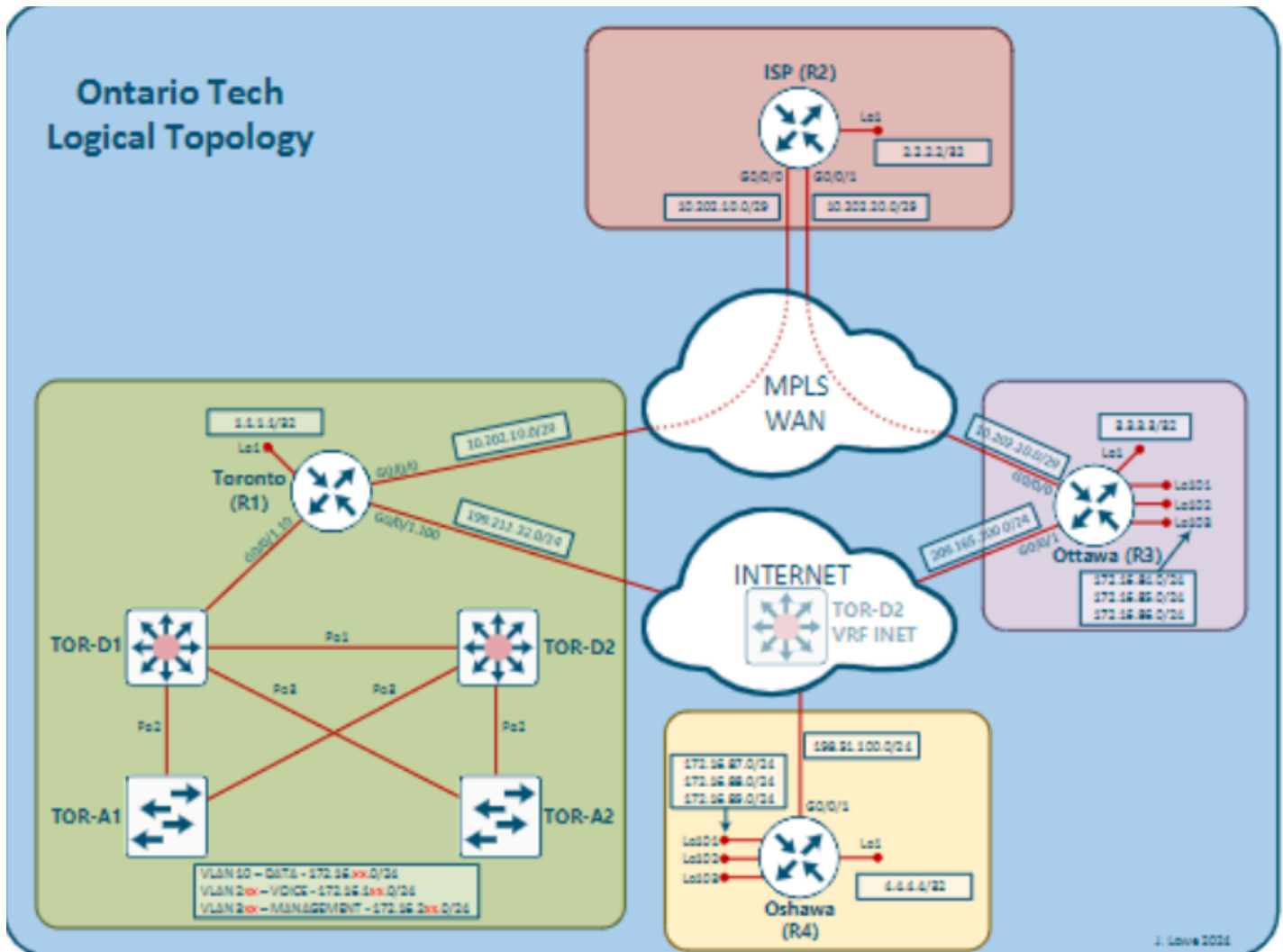
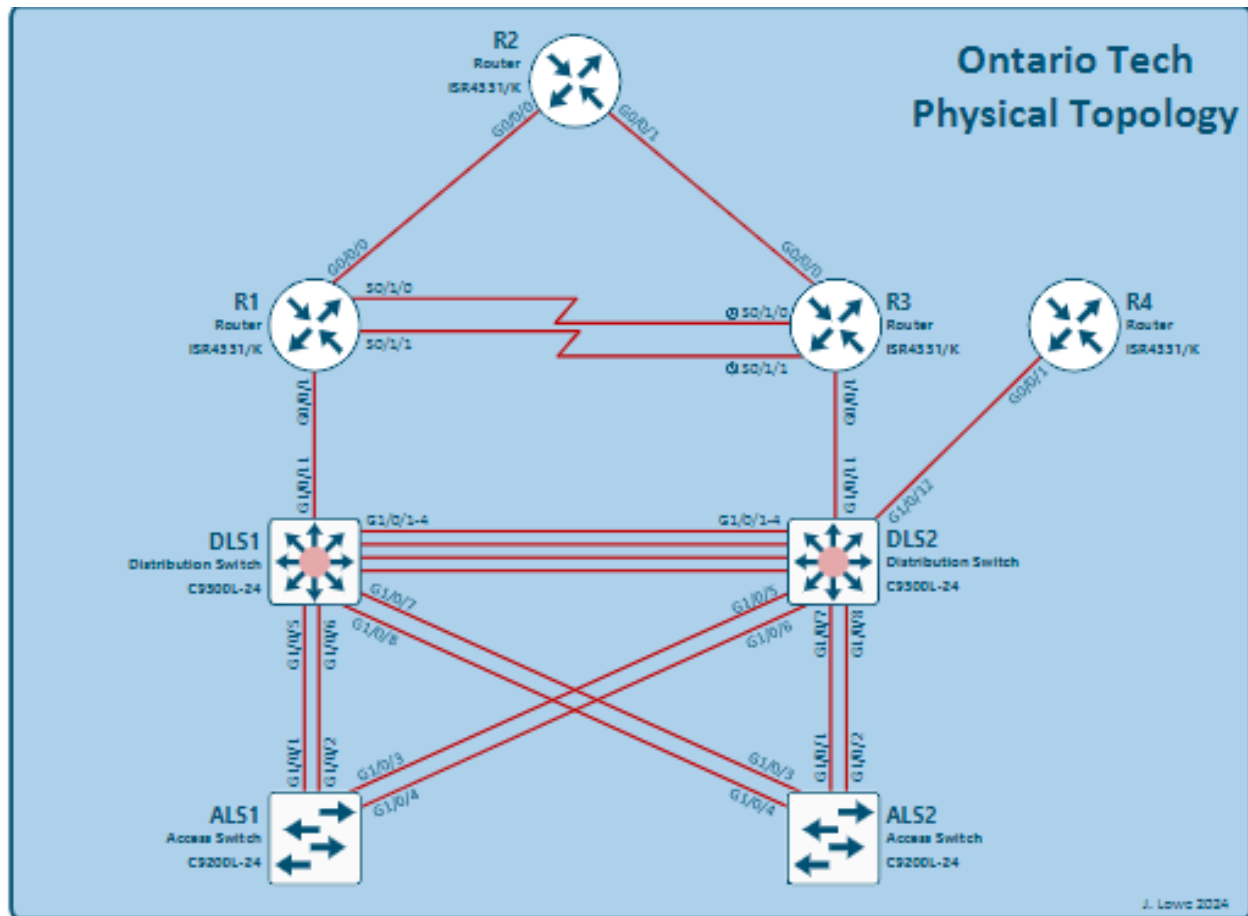


Logical Topology



Physical Topology



Addressing Table (Done)

Toronto	G0/0/0	10.202.10.1/29
	G0/0/1.10	172.16.34.1/24
	G0/0/1.100	199.212.32.34/24
	Lo1	1.1.1.1/32
	Tun1	10.1.34.1/24
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	209.165.200.34/24
	Lo1	3.3.3.3/32
	Lo101	172.16.84.34/24
	Lo102	172.16.85.34/24
	Lo103	172.16.86.34/24
	Tun1	10.1.34.2/24
Oshawa	G0/0/1	198.51.100.34/24
	Lo1	4.4.4.4/32
	Lo101	172.16.87.34/24
	Lo102	172.16.88.34/24
	Lo103	172.16.89.34/24
	Tun1	10.1.34.3/24
TOR-D1	Vlan 10	172.16.34.2/24
	Vlan 234	172.16.134.2/24

	Vlan 334	172.16.234.2/24
TOR-D2	Vlan 10	172.16.34.3/24
	Vlan 234	172.16.134.3/24
	Vlan 334	172.16.234.3/24
	Vlan 100	199.212.32.254/24
	Vlan 300	209.165.200.254/24
	Vlan 400	198.51.100.254/24
TOR-A1	Vlan 10	172.16.34.4/24
	Vlan 234	172.16.134.4/24
	Vlan 334	172.16.234.4/24
TOR-A2	Vlan 10	172.16.34.5/24
	Vlan 234	172.16.134.5/24
	Vlan 334	172.16.234.5/24

Task 1: Addressing Deliverable configs (Done)

Ip address (Ip address) (subnet mask)

Vlan (vlan number)

Task 2: Switch Configurations (Done)

NOTE: REMEMBER TO REDO VTP AND VLAN CONFIGURATIONS EVERY TIME YOUR DOING CONFIGURATIONS

- 1. 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.**

VTP server switch

Vtp domain OTU34

Vtp version 3

Vtp mode server

Exit

Vtp primary

Vtp client switch

Vtp domain OTU34

Vtp version 3

Vtp mode client

- 2. Create the following VLANs on the switches**

Show command: show vlan brief

vlan 10

name DATA

vlan 234

name VOICE

vlan 334

name MANAGEMENT

vlan 100

name R1-INET

vlan 300

```
name R3-INET
vlan 400
name R4-INET
vlan 123
name NATIVE
vlan 999
name UNUSED
```

3. Configure all switch-to-switch connections to static trunk links. Disable DTP.

```
TOR-D1
Interface range g1/0/1-4,G1/0/7-8, G1/0/5-6
Switchport mode trunk
Switchport nonegotiate
```

```
TOR-D2
Interface range g1/0/1-4, G1/0/5-6, g1/0/7-8
Switchport mode trunk (static trunks)
Switchport nonegotiate(disables DTP)
```

```
TOR-A1
Interface range g1/0/1-2, g1/0/3-4
Switchport mode trunk
Switchport nonegotiate
```

```
TOR-A2
Interface range g1/0/1-2, g1/0/3-4
Switchport mode trunk (static trunks)
Switchport nonegotiate(disables DTP)
```

4. Set the native VLAN to 123 and manually prune the trunks to only allow the following VLANs:

Show command: `show interface interface-name switchport`

(Make sure to do the All commands on Receiving ports or else native vlan mismatch)

```
TOR-D1 to TOR-D2:
Interface range g1/0/1-4
Switchport trunk native vlan 123
Switchport trunk allowed vlan 10,100,234,334
```

TOR-D1 to TOR-A1:

Interface range g1/0/5-6
Switchport trunk native vlan 123
Switchport trunk allowed vlan 10,234,334

TOR-A1 to TOR-D1

Interface range g1/0/1-2
Switchport trunk native vlan 123
Switchport trunk allowed vlan 10,234,334

TOR-D1 to TOR-A2:

Interface range g1/0/7-8
Switchport trunk native vlan 123
Switchport trunk allowed vlan 10,234,334

TOR-A2 to TOR-D1

Interface range g1/0/3-4
Switchport trunk native vlan 123
Switchport trunk allowed vlan 10,234,334

TOR-D2 to TOR-A1:

Interface range g1/0/5-6
switchport trunk native vlan 123
switchport trunk allowed vlan 10,234,334

TOR-A1 to TOR-D2

Interface range g1/0/3-4
Switchport trunk native vlan 123
Switchport trunk allowed vlan 10,234,334

TOR-D2 to TOR-A2:

Interface range g1/0/7-8
Switchport trunk native vlan 123
Switchport trunk allowed vlan 10,234,334

TOR-A2 to TOR-D2

Interface range g1/0/1-2
Switchport trunk native vlan 123
Switchport trunk allowed vlan 10,234,334

5. **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.**

Interface g1/0/11 (TOR-D1)

```
Switchport mode trunk
Switchport Nonegotiate
Switchport trunk allowed vlans 10, 100
```

6. **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.**

Interface g1/0/11

```
Switchport mode access
Switchport access vlan 300
exit
```

Interface g1/0/12

```
Switchport mode access
Switchport access vlan 400
```

7. **Configure all remaining unused switch interfaces to be shut down and static access ports in VLAN 999. (See the topology diagrams for details)**

TOR-D1 and TOR-D2

Interface range g1/0/9-24, g1/1/1-4

Shut

Switchport mode access

Switchport access vlan 999

ALS1 and ALS2

Interface range g1/0/5-24, g1/1/1-4

Shut

Switchport mode access

Switchport access vlan 999

- 8. 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**

TOR-D1

```
Interface range g1/0/7-8
Channel-group 3 mode active pagp
Exit
!
Interface range g1/0/5-6
Channel-group 2 mode desirable nonsilent LACP
Exit
!
Interface range g1/0/1-4
Channel-group 1 mode on (ON/OFF)
End
```

TOR-D2

```
Interface range g1/0/5-6
Channel-group 3 mode active
Exit
!
Interface range g1/0/7-8
Channel-group 2 mode desirable nonsilent
Exit
!
Interface range g1/0/1-4
Channel-group 1 mode on
Exit
```

TOR-A1

```
Interface range g1/0/3-4
channel-group 3 mode active
exit
!
Interface range g1/0/1-2
Channel-group 2 mode desirable nonsilent
Exit
```

TOR-A2

```
Interface range g1/0/3-4
Channel-group 3 mode active
Exit
!
Interface range g1/0/1-2
Channel-group 2 mode desirable nonsilent
exit
```

9. 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.

TOR-D1

```
Interface vlan 10
Ip address 172.16.34.2 255.255.255.0
No shut
Exit
Interface vlan 234
Ip address 172.16.134.2 255.255.255.0
No shut
Exit
Interface vlan 334
Ip address 172.16.234.2 255.255.255.0
No shut
exit
```

TOR-D2

```
Interface vlan 10
Ip address 172.16.34.3 255.255.255.0
No shut
Exit
Interface vlan 234
Ip address 172.16.134.3 255.255.255.0
No shut
Exit
Interface vlan 334
Ip address 172.16.234.3 255.255.255.0
No shut
Exit
Interface vlan 100
Ip address 199.212.32.254 255.255.255.0
No shut
```

```
Exit
Interface vlan 300
Ip address 209.165.200.254 255.255.255.0
No shut
Exit
Interface vlan 400
Ip address 198.51.100.254 255.255.255.0
No shut
exit
```

```
TOR-A1
Interface vlan 10
Ip address 172.16.34.4 255.255.255.0
No shut
Exit
Interface vlan 234
Ip address 172.16.134.4 255.255.255.0
No shut
Exit
Interface vlan 334
Ip address 172.16.234.4 255.255.255.0
No shut
Exit
```

```
TOR-A2
Interface vlan 10
Ip address 172.16.34.5 255.255.255.0
No shut
Exit
Interface vlan 234
Ip address 172.16.134.5 255.255.255.0
No shut
Exit
Interface vlan 334
Ip address 172.16.234.5 255.255.255.0
```

Task 3: Configure Spanning Tree (Done)

- 1. Make TOR-D1 the spanning-tree root bridge for VLANs 10 and 3xx and make TOR-D2 the root bridge for VLAN 2xx.**

TOR-D1

Config t

Spanning-tree vlan 10 root primary

Exit

Config t

Spanning-tree vlan 334 root primary

Exit

TOR-D2

Config t

Spanning-tree vlan 234 root primary

exit

- 2. Make TOR-D1 the backup root bridge for VLAN 2xx and make TOR-D2 the backup root bridge for VLANs 10 and 3xx**

TOR-D1

Config t

Spanning-tree vlan 234 root secondary

TOR-D2

Config t

Spanning-tree vlan 10 root secondary

Spanning-tree vlan 334 root secondary

3. **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**

TOR-A1

```
Interface port-channel 2  
Spanning-tree vlan 10 cost 78
```

```
Interface port-channel 3  
Spanning-tree vlan 10 cost 68
```

4. **Configure PortFast and BPDU Guard on the G1/0/12-24 ports on both TOR-A1 and TOR-A2**

TOR-A1 and TOR-A2:

```
interface range GigabitEthernet1/0/12-24  
spanning-tree portfast trunk  
spanning-tree bpduguard enable
```

(You need to change D1 and D2's configurations you kinda messed it up)

5. **Configure Root Guard on TOR-D1 and TOR-D2 ports G1/0/5 and G1/0/6.**

TOR-D1 and TOR-D2:

```
interface GigabitEthernet1/0/5  
spanning-tree guard root  
exit  
interface GigabitEthernet1/0/6  
spanning-tree guard root
```

Task 4: Configure First Hop Redundancy

- 1. 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**

TOR-D1

```
Interface vlan 10
Standby version 2
Standby 78 ip 172.16.34.254
Standby 78 priority 150
Standby 78 preempt
Exit
Interface vlan 234
Standby version 2
Standby 302 ip 172.16.134.254
Standby 302 preempt
exit
Interface vlan 334
Standby version 2
Standby 402 ip 172.16.234.254
Standby 402 priority 150
Standby 402 preempt
Exit
```

TOR-D2

```
Interface vlan 10
Standby version 2
Standby 78 ip 172.16.34.254
Standby 78 preempt

Interface vlan 234
Standby version 2
Standby 302 ip 172.16.134.254
Standby 302 priority 150
Standby 302 preempt
```

```
Interface vlan 334
Standby version 2
Standby 402 ip 172.16.234.254
Standby 402 preempt
```

2. **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.**

Show command: show standby

```
TOR-D2
track 302 interface Port-Channel2 line-protocol
```

```
Interface vlan 234
Standby 302 track 302 decrement 60
```

3. **Configure TOR-A1 and TOR-A2 with a default gateway address of the HSRP virtual IP address of VLAN 10.**

TOR-A1

```
interface vlan 10
No standby 78 ip 172.16.34.253
Ip default-gateway 172.16.34.254
```

TOR-A2

```
Interface vlan 10
No standby 78 ip 172.16.34.253
Ip default-gateway 172.16.34.254
```

Task 5: Configure MPLS

1. **Enable MPLS on the link between Toronto and ISP, and the link between Ottawa and ISP**

2. Set the label protocol to LDP

3. 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.

o Set the tunnel interfaces on all three routers to use multipoint GRE.

Show command: show dmvpn detail

o Set the tunnel source on all three routers to be the interface connecting to the Internet. o Set the tunnel key on all three routers to be three times your group number.

o 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*

Configure NHRP in a hub-and-spoke topology, where Toronto is the hub:

o Use a network ID of xx.

o 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).

o 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.

o On Ottawa and Oshawa, statically map Toronto's tunnel IP address to its Internet IP address.

o On Ottawa and Oshawa, statically map multicast addresses to Toronto's Internet IP address.

o Configure Toronto to send NHRP redirects, and Ottawa and Oshawa to use NHRP shortcuts to enable Phase 3 DMVPN.

Toronto Router

```
Interface tunnel1
Ip address 10.1.34.1 255.255.255.0
Tunnel mode gre multipoint
Tunnel source g0/0/1.100
Tunnel key 102
Bandwidth 1000000
Delay 88
!
Ip nhrp network-id 34
Ip nhrp authentication AR
Ip nhrp map multicast dynamic
Ip nhrp redirect
```

Ottawa Router

```
Interface tunnel1
Ip address 10.1.34.2 255.255.255.0
Tunnel mode gre multipoint
Tunnel source g0/0/1
Tunnel key 102
Bandwidth 1000000
Delay 88
!
Ip nhrp network-id 34
Ip nhrp authentication AR
Ip nhrp map 10.1.34.1 199.212.32.0
Ip nhrp nhs 10.1.34.1
Ip nhrp shortcut
Ip nhrp map multicast 199.212.32.0
```

Oshawa

```
Interface tunnel1
Ip address 10.1.34.3 255.255.255.0
Tunnel mode gre multipoint
Tunnel source g0/0/1
Tunnel key 102
Bandwidth 1000000
Delay 88
!
Ip nhrp network-id 34
Ip nhrp authentication AR
Ip nhrp map 10.1.34.1 199.212.32.0
Ip nhrp nhs 10.1.34.1
Ip nhrp shortcut
Ip nhrp map multicast 199.212.32.0
```

Secure the DMVPN tunnels using IPSec:

- o 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)*

Routers with DMVPN: Toronto, Ottawa and Oshawa

```
Crypto isakmp policy 34
Authentication pre-share
Encryption aes 256
hash sha512
Group 14
Exit
crypto isakmp key AR34 address 0.0.0.0 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

```
crypto ipsec transform-set AR34_TRANS esp-aes 256 esp-sha512-hmac
Mode transport
Exit
```

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

Toronto Router

```
crypto ipsec profile AR34_PROFILE
set transform-set AR34_TRANS
exit
!
interface Tunnel1
crypto ipsec profile AR34_PROFILE
```

Ottawa Router:

```
crypto ipsec profile AR34_PROFILE
set transform-set AR34_TRANS
exit
interface Tunnel1
crypto ipsec profile AR34_PROFILE
Exit
```

Oshawa Router:

```
crypto ipsec profile AR34_PROFILE
set transform-set AR34_TRANS
exit
interface Tunnel1
crypto ipsec profile AR34_PROFILE
Exit
```

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:

o Toronto: 1.1.1.1

o ISP: 2.2.2.2

o Ottawa: 3.3.3.3

o 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

Toronto router:

```
Router eigrp OntarioTech34
Address-family ipv4 unicast autonomous-system 34
No Eigrp router-id 1.1.1.1
!
network 10.1.34.1 0.0.0.0
network 172.15.34.1 0.0.0.0
network 199.212.32.34 0.0.0.0
network 1.1.1.1 0.0.0.0
Network 10.202.10.1 0.0.0.0
Af-interface tunnel1
No shut
Summary-address 172.16.0.0 255.255.0.0
Exit
Af-interface g0/0/0
No shut
Exit
Af-interface g0/0/1.10
Passive-interface
exit
Af-interface g0/0/1.100
No Passive-interface
Exit
Af-interface loopback1
No shut
End
Config t
ip route 172.16.0.0 255.255.0.0 172.16.34.254
```

ISP Router:

```
Router eigrp OntarioTech34
Address-family ipv4 unicast autonomous-system 34
Eigrp router-id 2.2.2.2
Network 10.202.10.2 0.0.0.0
Network 10.202.20.2 0.0.0.0
Network 2.2.2.2 0.0.0.0
!
Af-interface g0/0/0
No shut
Exit
Af-interface g0/0/1
No shut
exit
Af-interface loopback1
No shut
```

Ottawa router:

```
Router eigrp OntarioTech34
Address-family ipv4 unicast autonomous-system 34
Eigrp router-id 3.3.3.3
!
Network 10.1.34.2 0.0.0.0
Network 3.3.3.3 0.0.0.0
Network 172.16.84.34 0.0.0.0
Network 172.16.85.34 0.0.0.0
Network 172.16.86.34 0.0.0.0
Network 10.202.20.3 0.0.0.0
Af-interface tunnel1
No shut
Exit
Af-interface g0/0/0
No shut
Exit
Af-interface loopback1
No shut
Exit
Af-interface loopback102
No shut
Exit
af-interface loopback103
```

No shut
Exit

Oshawa router

```
Router eigrp OntarioTech34
Address-family ipv4 unicast autonomous-system 34
Eigrp router-id 4.4.4.4
!
Network 10.1.34.2 0.0.0.0
Network 4.4.4.4 0.0.0.0
Network 172.16.87.34 0.0.0.0
Network 172.16.88.34 0.0.0.0
Network 172.16.89.34 0.0.0.0
Af-interface tunnel1
No shut
Exit
Af-interface loopback1
No shut
Exit
Af-interface loopback102
No shut
Exit
af-interface loopback103
No shut
Exit
```

```
TOR-D1
ip route 0.0.0.0 0.0.0.0 172.16.34.1
```

```
TOR-D2
ip route 0.0.0.0 0.0.0.0 172.16.34.1
```


Task 8:

- 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.

All Routers and switches

```
clock timezone EST -5  
clock summer-time EDT recurring
```

ISP Router

clock set hh:mm:ss month day year
clock set 10:30:00 Mar 17 2024

ntp master 2

Toronto, Ottawa and Oshawa Routers

ntp server 2.2.2.2

TOR-D1, TOR-D2, TOR-A1, and TOR-A2 switches

ntp server 1.1.1.1

Task 9: Testing

Testing

tclsh

foreach address {

10.1.34.1

10.1.34.2

10.1.34.3

172.16.34.1

172.16.84.34

172.16.85.34

172.16.86.34

172.16.87.34

172.16.88.34

172.16.89.34

172.16.34.254

172.16.134.254

172.16.234.254 } { ping \$address }

tclquit

TOR-D1#show vtp status

VTP Version capable : 1 to 3
VTP version running : 3
VTP Domain Name : OTU34
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : f86b.d951.3900

Feature VLAN:

VTP Operating Mode : Primary Server
Number of existing VLANs : 13
Number of existing extended VLANs : 0
Maximum VLANs supported locally : 4096
Configuration Revision : 3
Primary ID : f86b.d951.3900
Primary Description : TOR-D1
MD5 digest : 0x5C 0x63 0x33 0xD1 0xCE 0xCC 0xFF 0xB0
0xD7 0x63 0x3D 0xC2 0x4A 0xD5 0x87 0x02

Feature MST:

VTP Operating Mode : Transparent

Feature UNKNOWN:

VTP Operating Mode : Transparent

TOR-D1#show vlan brief

VLAN Name	Status	Ports
1 default	active	Ap1/0/1
10 DATA	active	
100 R1-INET	active	
123 NATIVE	active	
234 VOICE	active	
300 R3-INET	active	
334 MANAGEMENT	active	
400 R4-INET	active	
999 UNUSED	active	Gi1/0/9, Gi1/0/10, Gi1/0/12 Gi1/0/13, Gi1/0/14, Gi1/0/15

	Gi1/0/16, Gi1/0/17, Gi1/0/18
	Gi1/0/19, Gi1/0/20, Gi1/0/21
	Gi1/0/22, Gi1/0/23, Gi1/0/24
	Gi1/1/1, Gi1/1/2, Gi1/1/3
	Gi1/1/4
1002 fddi-default	act/unsup
1003 trcrf-default	act/unsup
1004 fddinet-default	act/unsup
1005 trbrf-default	act/unsup

TOR-D2#show vtp status

VTP Version capable	: 1 to 3
VTP version running	: 3
VTP Domain Name	: OTU34
VTP Pruning Mode	: Disabled
VTP Traps Generation	: Disabled
Device ID	: f86b.d91f.2400

Feature VLAN:

VTP Operating Mode	: Client
Number of existing VLANs	: 13
Number of existing extended VLANs	: 0
Maximum VLANs supported locally	: 4096
Configuration Revision	: 3
Primary ID	: f86b.d951.3900
Primary Description	: TOR-D1
MD5 digest	: 0x5C 0x63 0x33 0xD1 0xCE 0xCC 0xFF 0xB0 0xD7 0x63 0x3D 0xC2 0x4A 0xD5 0x87 0x02

Feature MST:

VTP Operating Mode : Transparent

Feature UNKNOWN:

VTP Operating Mode : Transparent

TOR-D2#show vlan brief

VLAN Name	Status	Ports
1 default	active	Ap1/0/1
10 DATA	active	
100 R1-INET	active	
123 NATIVE	active	
234 VOICE	active	
300 R3-INET	active	Gi1/0/11
334 MANAGEMENT	active	
400 R4-INET	active	Gi1/0/12
999 UNUSED	active	Gi1/0/9, Gi1/0/10, Gi1/0/13 Gi1/0/14, Gi1/0/15, Gi1/0/16 Gi1/0/17, Gi1/0/18, Gi1/0/19 Gi1/0/20, Gi1/0/21, Gi1/0/22 Gi1/0/23, Gi1/0/24, Gi1/1/1 Gi1/1/2, Gi1/1/3, Gi1/1/4
1002 fddi-default	act/unsup	
1003 trcrf-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trbrf-default	act/unsup	

TOR-A1#show vtp status

VTP Version capable : 1 to 3
VTP version running : 3
VTP Domain Name : OTU34
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : 7cad.4f0d.9880

Feature VLAN:

VTP Operating Mode : Client
Number of existing VLANs : 13
Number of existing extended VLANs : 0
Maximum VLANs supported locally : 1024
Configuration Revision : 3
Primary ID : f86b.d951.3900
Primary Description : TOR-D1
MD5 digest : 0x5C 0x63 0x33 0xD1 0xCE 0xCC 0xFF 0xB0
0xD7 0x63 0x3D 0xC2 0x4A 0xD5 0x87 0x02

Feature MST:

VTP Operating Mode : Transparent

Feature UNKNOWN:

VTP Operating Mode : Transparent

TOR-A1#show vlan brief

VLAN Name	Status	Ports
1 default	active	
10 DATA	active	
100 R1-INET	active	
123 NATIVE	active	
234 VOICE	active	
300 R3-INET	active	
334 MANAGEMENT	active	
400 R4-INET	active	
999 UNUSED	active	Gi1/0/5, Gi1/0/6, Gi1/0/7 Gi1/0/8, Gi1/0/9, Gi1/0/10 Gi1/0/11, Gi1/0/12, Gi1/0/13 Gi1/0/14, Gi1/0/15, Gi1/0/16 Gi1/0/17, Gi1/0/18, Gi1/0/19 Gi1/0/20, Gi1/0/21, Gi1/0/22 Gi1/0/23, Gi1/0/24, Gi1/1/1 Gi1/1/2, Gi1/1/3, Gi1/1/4
1002 fddi-default	act/unsup	
1003 trcrf-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trbrf-default	act/unsup	

TOR-A2#show vtp status

VTP Version capable : 1 to 3
VTP version running : 3
VTP Domain Name : OTU34
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : 7cad.4f71.8a00

Feature VLAN:

VTP Operating Mode : Client
Number of existing VLANs : 13
Number of existing extended VLANs : 0
Maximum VLANs supported locally : 1024
Configuration Revision : 3
Primary ID : f86b.d951.3900
Primary Description : TOR-D1
MD5 digest : 0x5C 0x63 0x33 0xD1 0xCE 0xCC 0xFF 0xB0
0xD7 0x63 0x3D 0xC2 0x4A 0xD5 0x87 0x02

Feature MST:

VTP Operating Mode : Transparent

Feature UNKNOWN:

VTP Operating Mode : Transparent

TOR-A2#show vlan brief

VLAN Name	Status	Ports
1 default	active	
10 DATA	active	
100 R1-INET	active	
123 NATIVE	active	
234 VOICE	active	
300 R3-INET	active	
334 MANAGEMENT	active	
400 R4-INET	active	
999 UNUSED	active	Gi1/0/5, Gi1/0/6, Gi1/0/7 Gi1/0/8, Gi1/0/9, Gi1/0/10 Gi1/0/11, Gi1/0/12, Gi1/0/13 Gi1/0/14, Gi1/0/15, Gi1/0/16 Gi1/0/17, Gi1/0/18, Gi1/0/19 Gi1/0/20, Gi1/0/21, Gi1/0/22 Gi1/0/23, Gi1/0/24, Gi1/1/1 Gi1/1/2, Gi1/1/3, Gi1/1/4
1002 fddi-default	act/unsup	
1003 trcrf-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trbrf-default	act/unsup	