# NETWORK INFRASTRUCTURE PROJECT - CONFIGURATION FILE

***Student*:** **Guillermo Padilla Keymole**

***Project*:** **Multi-Site VLAN, VPN, NAT, CME, ACLs (Montreal & Toronto)**

## Montreal Site

### Edge (Main Border Router)

***Role*:**

This router connects the Montreal LAN to the Internet and to the Toronto site via an IPSec VPN. It also performs NAT, OSPF routing, SSH access control, and provides secure remote access for administrators.

**-------------------- Basic Configuration -----------------------**

```
conf t
hostname Edge
no logging console
banner motd ^C UNAUTHORIZED ACCESS ONLY!! ^C
service password-encryption
```

**-------------------- User & SSH Access Configuration -----------------------**

```
ip domain-name mtl-tor.corp
username atohme privilege 15 secret cisco123
crypto key generate rsa modulus 1024
ip ssh version 2
ip ssh source-interface Loopback0

ip access-list standard IT_SSH_ONLY
 permit 10.240.255.0 0.0.0.127

line vty 0 4
 access-class IT_SSH_ONLY in
 login local
 transport input ssh
```

**-------------------- Interfaces Configuration -----------------------**

```
interface Loopback0
 ip address 10.240.250.2 255.255.255.255

interface GigabitEthernet0/0
 description Internet (DHCP)
 ip address dhcp
 ip nat outside
 ip virtual-reassembly in

interface GigabitEthernet0/1
 description DMZ or Link to Inside
 ip address 209.100.7.1 255.255.255.252
 ip nat inside
 ip virtual-reassembly in
 crypto map VPN-MAP
```

```
interface GigabitEthernet0/2
 description Link to Internal Network
 ip address 10.240.128.1 255.255.192.0
 ip nat inside
 ip virtual-reassembly in

interface GigabitEthernet0/3
 no ip address
 shutdown

-------------------- OSPF Routing Configuration -----------------------
router ospf 1
 router-id 1.1.1.1
 passive-interface default
 no passive-interface GigabitEthernet0/1
 no passive-interface GigabitEthernet0/2
 network 10.240.128.0 0.0.63.255 area 0
 network 209.100.7.0 0.0.0.3 area 0

-------------------- VPN IPSec Configuration -----------------------
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5

crypto isakmp key vpnpa55 address 60.100.7.1

crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
 mode tunnel

crypto map VPN-MAP 10 ipsec-isakmp
 set peer 60.100.7.1
 set transform-set VPN-SET
 match address 110

access-list 110 permit ip 10.240.255.0 0.0.0.255 10.10.15.0 0.0.0.255

-------------------- NAT Configuration -----------------------
ip access-list standard NAT_INSIDE
 permit 10.240.0.0 0.0.255.255
 permit 10.10.15.128 0.0.0.63
 permit 10.10.15.192 0.0.0.31

ip nat inside source list NAT_INSIDE interface GigabitEthernet0/0 overload

! Static NAT for Web Server (AlmaLinux)
ip nat inside source static tcp 10.240.192.2 80 interface GigabitEthernet0/0
80

-------------------- Static Routes -----------------------
ip route 10.240.192.0 255.255.224.0 10.240.128.2
ip route 10.240.224.0 255.255.240.0 10.240.128.2
ip route 10.240.255.0 255.255.255.0 10.240.128.2
ip route 60.100.7.0 255.255.255.252 209.100.7.2
```

-------------------- **Security Notes** -----------------------

- SSH access is restricted to VLAN 10 subnet using access-class.
- ACL 110 defines encrypted traffic for IPSec VPN.
- ACL NAT_INSIDE controls which subnets are allowed to NAT.

======================================================

## Montreal Site

======================================================

### R1 (Montreal LAN Core Router)

==============================

***Role***:

This router provides internal routing for the Montreal network. It distributes DHCP addresses, participates in OSPF routing, acts as a gateway for internal subnets, connects to SW1, the CME, and forwards traffic to the Edge router for Internet access.

-------------------- **Basic Configuration** -----------------------

```
conf t
hostname R1
no ip domain-lookup
ip domain-name mtl-tor.corp
service password-encryption
banner motd ^C UNAUTHORIZED ACCESS ONLY!! ^C
```

-------------------- **User & SSH Access Configuration** -----------------------

```
username atohme privilege 15 secret cisco123
crypto key generate rsa modulus 1024
ip ssh version 2
ip ssh source-interface Loopback0

ip access-list standard IT_SSH_ONLY
 permit 10.240.255.0 0.0.0.127

line vty 0 4
 access-class IT_SSH_ONLY in
 login local
 transport input ssh
```

-------------------- **DHCP Pools** -----------------------

```
ip dhcp excluded-address 10.240.255.1 10.240.255.10
ip dhcp excluded-address 10.240.255.129 10.240.255.130
ip dhcp excluded-address 10.240.255.193 10.240.255.194
ip dhcp excluded-address 10.240.255.225 10.240.255.226

ip dhcp pool VLAN10
 network 10.240.255.0 255.255.255.128
 default-router 10.240.255.1
 dns-server 8.8.8.8
 lease 7

ip dhcp pool VLAN20
 network 10.240.255.128 255.255.255.192
 default-router 10.240.255.129
 dns-server 8.8.8.8
 lease 7
```

```
ip dhcp pool VLAN30
 network 10.240.255.192 255.255.255.224
 default-router 10.240.255.193
 dns-server 8.8.8.8
 lease 7

ip dhcp pool VLAN40
 network 10.240.255.224 255.255.255.240
 default-router 10.240.255.225
 dns-server 8.8.8.8
 option 150 ip 10.240.224.2
 lease 7
```

-------------------- **Interfaces Configuration** -----------------------

```
interface Loopback0
 ip address 10.240.250.1 255.255.255.255

interface GigabitEthernet0/0
 description Uplink to Edge
 ip address 10.240.128.2 255.255.192.0

interface GigabitEthernet0/1
 description Link to Web Server VLAN
 ip address 10.240.192.1 255.255.224.0

interface GigabitEthernet0/2
 description Routed link to SW1
 ip address 10.240.254.1 255.255.255.252

interface GigabitEthernet0/3
 description Link to CME Voice Network
 ip address 10.240.224.1 255.255.240.0
```

-------------------- **OSPF Routing Configuration** -----------------------

```
router ospf 1
 router-id 2.2.2.2
 passive-interface default
 no passive-interface GigabitEthernet0/0
 no passive-interface GigabitEthernet0/2
 network 10.240.128.0 0.0.63.255 area 0
 network 10.240.192.0 0.0.31.255 area 0
 network 10.240.250.1 0.0.0.0 area 0
 network 10.240.254.0 0.0.0.3 area 0
 network 10.240.255.0 0.0.0.127 area 0
```

-------------------- **Static Routing** -----------------------

```
ip route 0.0.0.0 0.0.0.0 10.240.128.1
```

-------------------- **Security Notes** -----------------------

- SSH access is secured via Loopback0 and restricted using ACL.
- DHCP pools are segmented per VLAN with exclusions.
- Option 150 is used to support VoIP provisioning (CME).

======================================================

## Montreal Site

======================================================

### SW1 (Montreal L3 Distribution Switch)

======================================

***Role*:**
This Layer 3 switch handles VLAN inter-VLAN routing, trunking, and local switching for the Montreal LAN. It connects end devices, trunks to other switches, provides VLAN interfaces, and routes user traffic via a routed uplink to R1.

-------------------- **Basic Configuration** -----------------------

```
conf t
hostname SW1
no ip domain-lookup
ip domain-name mtl-tor.corp
banner motd ^C UNAUTHORIZED ACCESS ONLY!! ^C
```

-------------------- **User & SSH Access Configuration** -----------------------

```
username atohme privilege 15 secret cisco123
crypto key generate rsa modulus 1024
ip ssh version 2
ip ssh source-interface Loopback0
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr

ip access-list standard IT_SSH_ONLY
 permit 10.240.255.0 0.0.0.127

line vty 0 4
 access-class IT_SSH_ONLY in
 login local
 transport input ssh
```

-------------------- **Loopback Interface** -----------------------

```
interface Loopback0
 ip address 10.240.250.3 255.255.255.255
```

-------------------- **VLAN Interfaces** -----------------------

```
interface Vlan10
 ip address 10.240.255.1 255.255.255.128
 ip helper-address 10.240.254.1

interface Vlan20
 ip address 10.240.255.129 255.255.255.192
 ip helper-address 10.240.254.1

interface Vlan30
 ip address 10.240.255.193 255.255.255.224
 ip helper-address 10.240.254.1

interface Vlan40
 ip address 10.240.255.225 255.255.255.240
 ip helper-address 10.240.254.1
```

```
-------------------- Interfaces Configuration -----------------------
interface GigabitEthernet0/0
 description Routed Link to R1
 no switchport
 ip address 10.240.254.2 255.255.255.252

interface GigabitEthernet0/1
 switchport access vlan 10
 switchport mode access

interface GigabitEthernet0/2
 switchport access vlan 40
 switchport mode access

interface GigabitEthernet0/3
 switchport access vlan 20
 switchport mode access

interface GigabitEthernet1/0
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30,40
 switchport mode trunk
 channel-group 1 mode active

interface GigabitEthernet1/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30,40
 switchport mode trunk
 channel-group 1 mode active

interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30,40
 switchport mode trunk

interface GigabitEthernet1/2 to 3/3
 switchport access vlan 99
 switchport mode access
 shutdown

-------------------- OSPF Routing Configuration -----------------------
router ospf 1
 router-id 5.5.5.5
 passive-interface default
 no passive-interface GigabitEthernet0/0
 network 10.240.254.0 0.0.0.3 area 0
 network 10.240.255.0 0.0.0.127 area 0
 network 10.240.255.128 0.0.0.63 area 0
 network 10.240.255.192 0.0.0.31 area 0
 network 10.240.255.224 0.0.0.15 area 0

-------------------- Static Routing -----------------------
ip route 0.0.0.0 0.0.0.0 10.240.254.1

-------------------- STP & Switching -----------------------
spanning-tree mode pvst
spanning-tree extend system-id
```

```
-------------------- Notes -----------------------
- VLAN 99 used for unused ports (shutdown for security).
- Inter-VLAN routing is enabled on SW1 using VLAN interfaces.
- Trunks and EtherChannel configured correctly.
- SW1 operates as an L3 switch instead of using ROAS on R1.
```

======================================================

## Montreal Site

======================================================

### SW2 (Montreal Access Switch)

=============================

***Role***:
Layer 2 Access Switch for VLAN 30 (Public Wi-Fi zone). Connected to SW1 via EtherChannel, and hosts end devices on VLAN 30. Includes SSH restriction and uses a default gateway for VLAN routing handled by SW1.

```
-------------------- Basic Configuration -----------------------
conf t
hostname SW2
no ip domain-lookup
ip domain-name mtl-tor.corp
banner motd ^C UNAUTHORIZED ACCESS ONLY!! ^C

-------------------- User & SSH Access Configuration -----------------------
username atohme privilege 15 secret cisco123
crypto key generate rsa modulus 1024
ip ssh version 2
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr

ip access-list standard IT_SSH_ONLY
 permit 10.240.255.0 0.0.0.127

line vty 0 4
 access-class IT_SSH_ONLY in
 login local
 transport input ssh

-------------------- VLAN Interface -----------------------
interface Vlan30
 ip address 10.240.255.194 255.255.255.224

-------------------- Interface Configuration -----------------------
interface GigabitEthernet0/1
 switchport access vlan 30
 switchport mode access

interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface GigabitEthernet1/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode active
```

```
interface GigabitEthernet1/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode active

interface GigabitEthernet0/0, 0/2-0/3, 1/2-3/3
 switchport access vlan 99
 switchport mode access
 shutdown
```

-------------------- **Static Routing** -----------------------

```
ip route 10.240.255.0 255.255.255.128 10.240.255.193
```

-------------------- **STP & Switching** -----------------------

```
spanning-tree mode pvst
spanning-tree extend system-id
```

-------------------- **Notes** -----------------------

- VLAN 30 used for public Wi-Fi zone devices.
- VLAN 99 used for unused ports, all shut down for security.
- SW2 does not perform routing — it uses SW1 as the gateway.
- EtherChannel is properly configured for trunking via Port-channel1.
- SSH is restricted to subnet 10.240.255.0/25 using ACL IT_SSH_ONLY.

======================================================

**Transit / Headquarters (HQ) Router**

======================================================

**HQ (Transit Router Between Montreal & Toronto)**

=============================================

***Role*:**
Acts as a transit router between the Edge Router and R2 (Toronto). Routes external and internal traffic between networks, advertises public/external networks via OSPF, and enforces SSH ACL security. Has a Loopback for management and external routing logic.

-------------------- **Basic Configuration** -----------------------

```
conf t
hostname HQ
no ip domain-lookup
ip domain-name mtl-tor.corp
banner motd ^C UNAUTHORIZED ACCESS ONLY!! ^C
```

-------------------- **User & SSH Access Configuration** -----------------------

```
username atohme privilege 15 secret cisco123
crypto key generate rsa modulus 1024
ip ssh version 2
ip ssh source-interface Loopback0

ip access-list standard IT_SSH_ONLY
 permit 10.240.255.0 0.0.0.127

line vty 0 4
 access-class IT_SSH_ONLY in
 login local
 transport input ssh

-------------------- Interface Configuration -----------------------
interface Loopback0
 ip address 209.100.78.10 255.255.255.255

interface GigabitEthernet0/0
 description Link to R2
 ip address 209.100.7.2 255.255.255.252

interface GigabitEthernet0/1
 description Link to Edge Router
 ip address 60.100.7.2 255.255.255.252

interface GigabitEthernet0/2-0/3
 shutdown

-------------------- Static Routes -----------------------
ip route 0.0.0.0 0.0.0.0 209.100.7.1
ip route 10.240.224.0 255.255.240.0 209.100.7.1

-------------------- OSPF Routing Configuration -----------------------
router ospf 1
 router-id 3.3.3.3
 passive-interface default
 no passive-interface GigabitEthernet0/0
 no passive-interface GigabitEthernet0/1
 network 60.100.7.0 0.0.0.3 area 0
 network 209.100.7.0 0.0.0.3 area 0
 network 209.100.78.10 0.0.0.0 area 0
```

**-------------------- Notes -----------------------**

- HQ serves as a middle point between Montreal (Edge) and Toronto (R2).
- Management interface uses Loopback0 (209.100.78.10).
- SSH traffic is limited via ACL (only 10.240.255.0/25 subnet is allowed).
- *Uses two static routes*: one for default, one for internal corporate networks.
- OSPF is configured with all interfaces but set passive by default (except G0/0 and G1/1).

```
=====================================================
Montreal CME (VoIP Router)
=====================================================
```

**CME (Call Manager Express)**

```
==========================
```

*Role*:

CME serves as the VoIP gateway for the Montreal network. It connects to R1 for routing, handles IP telephony using Cisco Unified CME services, and supports multiple ePhones (VoIP clients) with assigned numbers. Uses static routing and has no domain lookup enabled.

-------------------- **Basic Configuration** -----------------------

```
conf t
hostname CME
no ip domain-lookup
ip domain-name voip.project
banner motd ^C VoIP Router - Authorized Access Only ^C
```

-------------------- **Interface Configuration** -----------------------

```
interface GigabitEthernet0/0
 description Link to R1
 ip address 10.240.224.2 255.255.240.0
 duplex full
 speed 1000

interface Ethernet0/0
 shutdown
```

-------------------- **Static Route** -----------------------

```
ip route 0.0.0.0 0.0.0.0 10.240.224.1
ip default-gateway 10.240.224.1
```

-------------------- **Telephony Service Configuration** -----------------------

```
telephony-service
 max-ephones 10
 max-dn 10
 ip source-address 10.240.224.2 port 2000
 auto assign 1 to 10
 max-conferences 4 gain -6
 transfer-system full-consult
 create cnf-files version-stamp Jan 01 2002 00:00:00
```

-------------------- **ePhone & Directory Numbers** -----------------------

```
ephone-dn 1
 number 1001

ephone-dn 2
 number 1002

ephone 1
 mac-address 000C.2934.F56F
 type CIPC
 button 1:1

ephone 2
 mac-address 000C.2934.F56E
 type CIPC
 button 1:2
```

-------------------- **Notes** -----------------------

- This device provides local VoIP communication for users in the Montreal network.
- Static routing is used to reach R1 (default gateway 10.240.224.1).
- Phones auto-registered with DN 1001 and 1002.
- Supports CIPC softphones using port 2000.

```
======================================================
Toronto R2 Router
======================================================
```

***Role*:**
R2 is the primary gateway router for the Toronto site. It performs inter-VLAN routing using ROAS (Router-on-a-Stick) and provides DHCP services to all VLANs in Toronto. It also serves as the IPSec VPN tunnel endpoint for secure communication with the Montreal network.

```
-------------------- Basic Configuration -----------------------
conf t
hostname R2
no ip domain-lookup
ip domain-name mtl-tor.corp
banner motd ^C Toronto Site Router – Authorized Access Only ^C

-------------------- Local User -----------------------
username atohme privilege 15 secret vpnpa55

-------------------- Interfaces -----------------------
interface GigabitEthernet0/0
 ip address 60.100.7.1 255.255.255.252
 crypto map VPN-MAP

interface GigabitEthernet0/1
 no ip address

interface GigabitEthernet0/1.10
 encapsulation dot1Q 10
 ip address 10.10.15.1 255.255.255.128

interface GigabitEthernet0/1.20
 encapsulation dot1Q 20
 ip address 10.10.15.129 255.255.255.192

interface GigabitEthernet0/1.30
 encapsulation dot1Q 30
 ip address 10.10.15.193 255.255.255.224

interface Loopback0
 ip address 60.100.78.10 255.255.255.255

-------------------- DHCP Pools -----------------------
ip dhcp excluded-address 10.10.15.1 10.10.15.10
ip dhcp excluded-address 10.10.15.129 10.10.15.139
ip dhcp excluded-address 10.10.15.193 10.10.15.198

ip dhcp pool VLAN10_TorontoSite
 network 10.10.15.0 255.255.255.128
 default-router 10.10.15.1
 dns-server 8.8.8.8
 lease 7

ip dhcp pool VLAN20_TorontoSite
 network 10.10.15.128 255.255.255.192
 default-router 10.10.15.129
 dns-server 8.8.8.8
 option 150 ip 10.240.224.2
 lease 7

ip dhcp pool VLAN30_TorontoSite
 network 10.10.15.192 255.255.255.224
 default-router 10.10.15.193
 dns-server 8.8.8.8
 lease 7

-------------------- VPN Configuration -----------------------
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5

crypto isakmp key vpnpa55 address 209.100.7.1

crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
 mode tunnel

crypto map VPN-MAP 10 ipsec-isakmp
 set peer 209.100.7.1
 set transform-set VPN-SET
 match address 110

access-list 110 permit ip 10.10.15.0 0.0.0.255 10.240.255.0 0.0.0.255

-------------------- Static Routing -----------------------
ip route 0.0.0.0 0.0.0.0 60.100.7.2
ip route 10.240.224.0 255.255.240.0 60.100.7.2
ip route 209.100.7.0 255.255.255.252 60.100.7.2

-------------------- SSH Remote Access -----------------------
ip ssh version 2
ip ssh source-interface Loopback0

ip access-list standard IT_SSH_ONLY
 permit 10.240.255.0 0.0.0.127

line vty 0 4
 access-class IT_SSH_ONLY in
 login local
 transport input ssh

-------------------- OSPF Configuration -----------------------
router ospf 1
 router-id 4.4.4.4
 passive-interface default
 no passive-interface GigabitEthernet0/0
 no passive-interface GigabitEthernet0/1
 network 10.10.15.0 0.0.0.255 area 0
 network 60.100.7.0 0.0.0.3 area 0
 network 60.100.78.10 0.0.0.0 area 0
```

-------------------- **Notes** -----------------------

- R2 performs inter-VLAN routing for 3 subnets (VLAN10, VLAN20, VLAN30) using subinterfaces.
- DHCP is configured for each VLAN with excluded address ranges.
- VPN is established between 60.100.7.1 (R2) and 209.100.7.1 (Edge router).
- SSH access restricted using standard ACL `IT_SSH_ONLY` from trusted management subnet.
- Option 150 in VLAN20 provides TFTP server IP (CME) to IP phones.

=====================================================

## Toronto SW3 Switch

=====================================================

***Role***:

SW3 is an access layer switch at the Toronto site. It provides Layer 2 connectivity for VLAN 20 and VLAN 30 users and connects to upstream switches or routers via a trunk port.

-------------------- **Basic Configuration** -----------------------

```
conf t
hostname SW3
no ip domain-lookup
banner motd ^C Toronto SW3 – Access Layer Switch ^C
```

-------------------- **VLAN Configuration** -----------------------

```
interface GigabitEthernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface GigabitEthernet0/1
 switchport mode access
 switchport access vlan 30

interface GigabitEthernet0/2
 switchport mode access
 switchport access vlan 20
```

-------------------- **Spanning Tree** -----------------------

```
spanning-tree mode pvst
spanning-tree extend system-id
```

-------------------- **SSH Encryption** -----------------------

```
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
```

-------------------- **Services** -----------------------

```
ip cef
ip http server
ip http secure-server
```

-------------------- **Notes** -----------------------

- Interface Gi0/0 is a trunk uplink to carry multiple VLANs.
- Interfaces Gi0/1 and Gi0/2 are assigned to VLAN 30 and VLAN 20 respectively.
- SSH encryption algorithms are enabled, though no SSH access control is applied locally.
- The switch is operating at Layer 2 only.