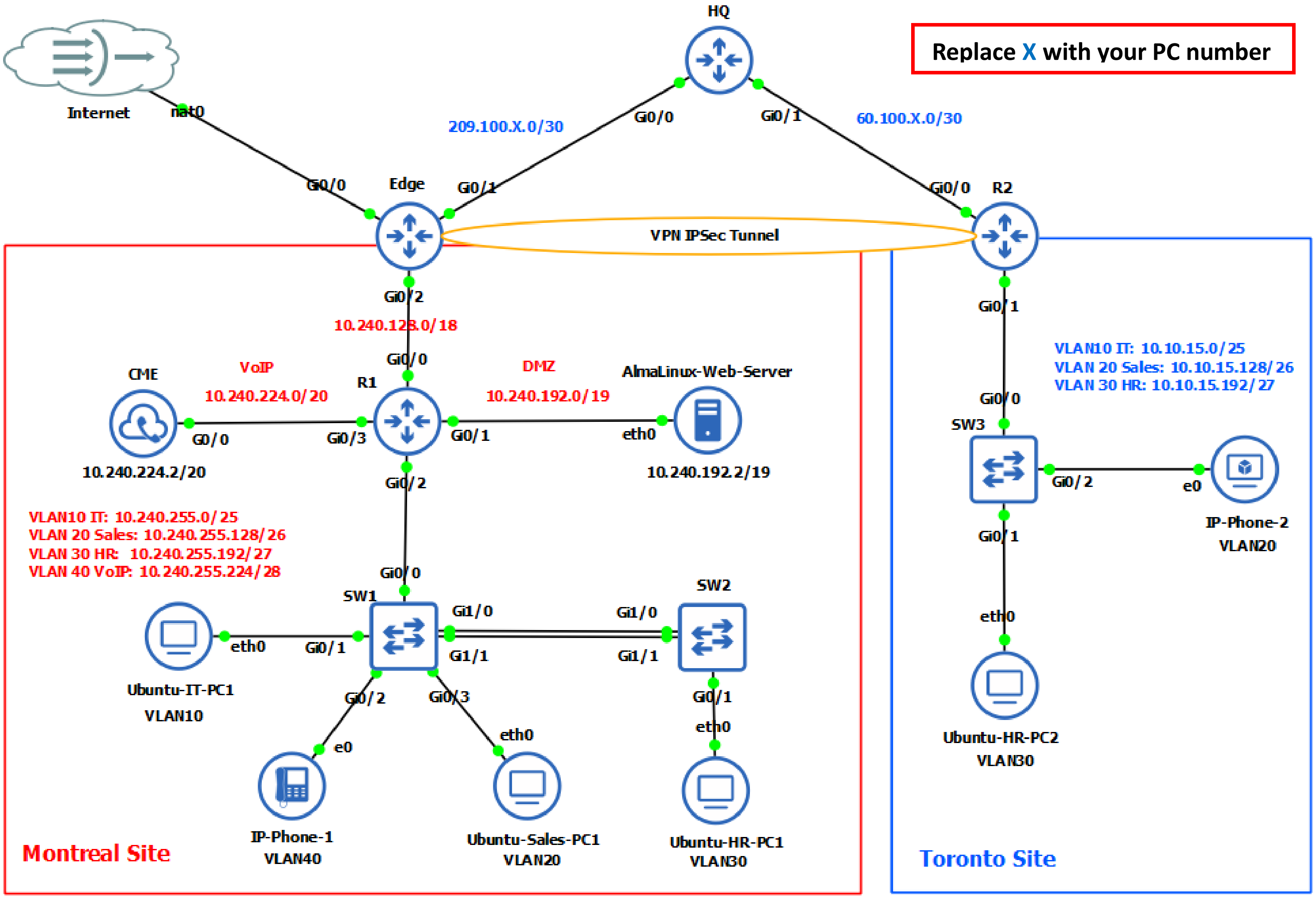
NETWORK DESIGN AND IMPLEMENTATION PROJECT

420-637-AB-Integration of Networking Services

Teacher: Antoine Tohme

1. Specifications

Topology



Replace X with your PC number

Network Design and Configuration Tasks

1. Network Segmentation and IP Addressing

Create the following VLANs and subnets for user groups across the two sites:

Montreal Site

- **VLAN 10 – IT:** 10.240.255.0/25
- **VLAN 20 – Sales:** 10.240.255.128/26
- **VLAN 30 – HR:** 10.240.255.192/27
- **VLAN 40 – VoIP:** 10.240.255.224/28

Toronto Site

- **VLAN 10 – IT:** 10.10.15.0/25
- **VLAN 20 – Sales:** 10.10.15.128/26
- **VLAN 30 – HR:** 10.10.15.192/27

---

2. Public Website Hosting (DMZ)

- Deploy a **Linux-based web server (AlmaLinux)** in the **DMZ** network at the **Montreal** site: 10.240.192.0/19.
- Configure an appropriate **NAT rule** on the router **Edge** to allow HTTP access to the AlmaLinux Web Server from the Internet.

---

3. Redundancy

- Provide for the redundancy of links between switches in **Montreal site.**

---

4. Routing and Communication

Ensure full end-to-end connectivity using the following strategies:

- **VLAN and Inter-VLAN routing** using Layer 3 switch/router interfaces.
- Configure **DHCP servers** to dynamically assign IPs to end-user devices.
- Implement **OSPF** to enable communication between all internal networks across sites.
- Use **default static routes** where needed.

5. Site-to-Site Access

- The **Toronto site must access** both the DMZ services and internal VLANs of the Montreal site.
- The **Montreal site must access** Toronto's internal services.

---

6. VPN Connectivity

- Establish an **IPSec VPN tunnel** between the **Montreal** and **Toronto** sites.
- Encrypt inter-site traffic to secure communications.

---

7. IP Telephony Implementation

- Deploy **local VoIP services** at both sites **Montreal** and **Toronto**.

---

8. Internet Access via NAT

- Configure **NAT** on the **Edge router** at the Montreal site to allow all internal hosts to access the Internet.
- Only public-facing services (web server) should be exposed externally.

---

9. Network Security Measures

- Apply security best practices:
  - Enable **SSH** access on all network devices (routers and switches).
  - Configure **Access Control Lists (ACLs)** to **allow SSH access only from the IT subnet** (10.240.255.0/25 in Montreal).

---

2. Evaluation

Validation

- **Individual validation** will be conducted by the teacher
- Students must demonstrate all test cases live or provide screenshots, based on the **Tests.pdf** file (e.g., ping between VLANs, web server access, SSH ACL validation, etc.)

Grading Rubric

Criteria	**Description**
Not Done	Task or requirement is completely missing or not started
Partially Done	Task is incomplete or contains significant gaps/errors
Done Right	Task is mostly complete with only minor issues
Completed	Task is fully completed and meets all technical and functional requirements with no issues

Evaluation grid

Task description	Weight (%)
Logical Topology	15
Communication on the Montreal Site (IP addressing / Routing / Ping)	10
Communication on the Toronto Site (IP addressing / Routing / Ping)	10
Communication Between the Two Sites (Routing / Ping)	10
NAT (Network Address Translation)	10
IPSec VPN Tunnel	10
IP Telephony (VoIP)	10
SSH / ACL Configuration	10
Accessible Web Server (DMZ)	5
Total	**100**