Lab 2: Wireless Router/Enterprise Router

Overview: In this lab project, you will learn how to configure switches and routers in wireless environment, followed by an enterprise-based environment. Specifically, you will learn how to apply Virtual Local Area Network (VLAN), Dynamic Host Configuration Protocol (DHCP), Port forwarding, Secure Shell (SSH), and Network Address Translation (NAT) in practice.

Phase I Network Diagram

Deploy the following architecture where **XX** is your Laboratory Group #.

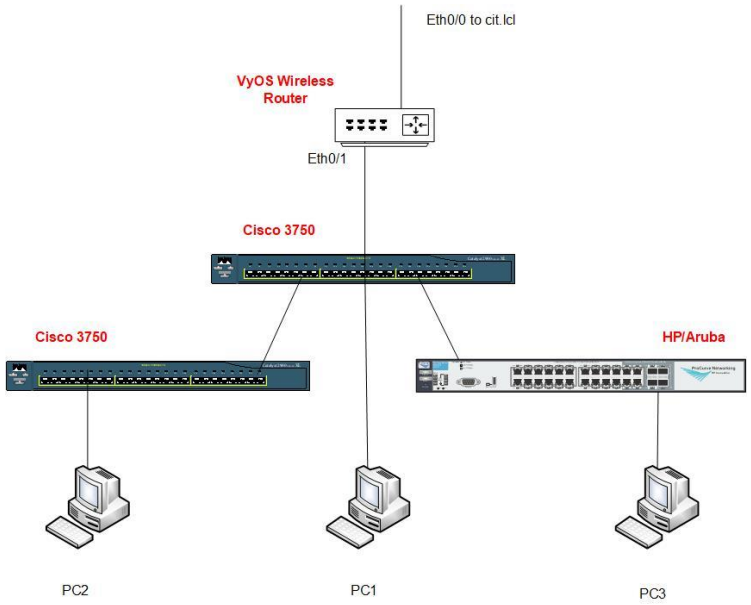

Figure 1 – Network Architecture for Lab2, Phase 1

Primary Objectives

- The VyOS device has a default user of "vyos" with a password of "CNIT240-344". Create an additional user for each group member and change the default password for the "vyos" user.
- Connect to the console port of the VyOS device serially with the speed of 115200 using PuTTY or SecureCRT.
- The VyOS wireless router has a static Wide Area Network (WAN) interface of 10.25.XX.254 on one of the Ethernet interfaces, with a default gateway of 10.25.XX.1 and subnet mask of 255.255.255.0
- Configure Wireless network on VyOS machine including:
    - Minimal Wireless Interface configuration.
        - Internet Protocol (IP) address 172.16.XX.1/24.
        - description – "Group XX Wireless Network".
        - wireless channel.
        - wireless mode.
        - wireless type – access point.
        - wireless Service Set Identifier (SSID) – "c240-344gXX".
        - wireless security mode and password.
        - wireless country code.

    - Configure DHCP for the wireless network including.
        - Default router.
        - DNS services.
        - Range of addresses from 172.16.XX.100 to 172.16.XX.200.
    - NAT to leave the private wireless network
- Configure the management interfaces for both VyOS (10.25.XX.254) can be accessed remotely using SSH through the Computer and Information Technology Virtual Private Network (CIT VPN). Configure both Cisco 3750s and the HP/Aruba so each can be reached remotely using SSH from within the 192.168.XX.0 /24 network. Creating an alternate method to attach the 3 switches without using the serial cables from within your private network.
- Local Area Network (LAN) interface on an Ethernet interface of VyOS device with DHCP service enabled. The range of the IP addresses will be ***.*.*.100** to ***.*.*.200** to serve VLAN XX network at 192.168.XX.0 /24, VLAN 1XX (sub interface or virtual interface) network at 192.168.1XX.0/24, and VLAN2XX (sub interface or virtual interface) network at 192.168.2XX.0/24 where XX is your group number.
- NAT will need to be used for all networks inside the private network. NAT will permit the traffic outside on the WAN port.
- Configure VLANs on the VyOS device and 3 switches such that PCs will automatically join different VLANs and based on the port they connect to and have Internet access.
- Port forwarding.
    - Put PC1 in VLAN 1XX and install Internet Information Services (IIS) web server on PC1.
    - Verify the web server is accessible when PC2 is on VLAN 1XX, VLAN XX, and VLAN 2XX.
    - Configure port forwarding such that your web server is accessible for any PCs in the CIT-VPN.
- Disable the Wireless Access Point to reduce WiFi interferences in Knoy.

Phase II Network Diagram

Deploy the following architecture where **XX** is your Laboratory Group #. Replace the VyOS device with a Cisco 2811/2901 router. Addresses in Phase 2 will be static in specific locations and DHCP when it comes to PC configuration.

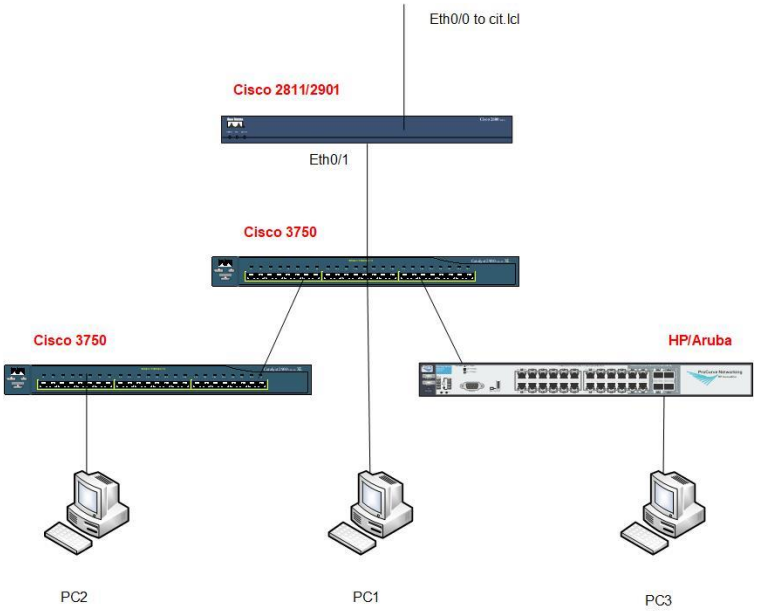

Figure 2 – Network Architecture for Lab2, Phase 2

- Deploy IEEE 802.1Q VLANs to Figure 2.
    - Each switch should have VLAN XX, VLAN 1XX, and VLAN 2XX set and any device plugged into the VLAN will receive IP addressing via DHCP. Assign at least one port to each VLAN.
    - NAT will need to be implemented to have access outside the private network.
    - Configure router appropriately for VLANs and all appropriate interfaces and sub interfaces.
    - Identify the effect of the VLAN tag on the Ethernet header and trailer.
    - Identify the extent of the MAC broadcast domain and the contention domain(s).
    - Each client MUST be able to access the cit.lcl network and the Internet.
    - Be able to explain network operations.
- Configure the management interfaces for both the Cisco Router ports (10.25.XX.254) can be accessed remotely using SSH through the Computer and Information Technology Virtual Private Network (CIT VPN). Configure both Cisco 3750s and the HP/Aruba so each can be reached remotely using SSH from within the 192.168.XX.0 /24 network. Creating an alternate method to attach the 3 switches without using the serial cables from within your private network.
- Monitor the amount of traffic between each of the interfaces associated with a particular VLAN using Wireshark on PC2 (the Ubuntu machine).
    - Compare and contrast the per VLAN statistics with the overall statistics of traffic traversing a particular interface (the uplink to the router, for instance).
    - Compare the number of ingress and egress frames. Explain.
    - What is the correlation between octets and frames?
- Using Wireshark, capture an 802.1Q tag within a Frame from your host in transit to a location outside your network.
    - Describe each fields' purpose and function.
    - Compare and contrast with a frame that does not contain an 802.1Q tag from the same host to the same external location.