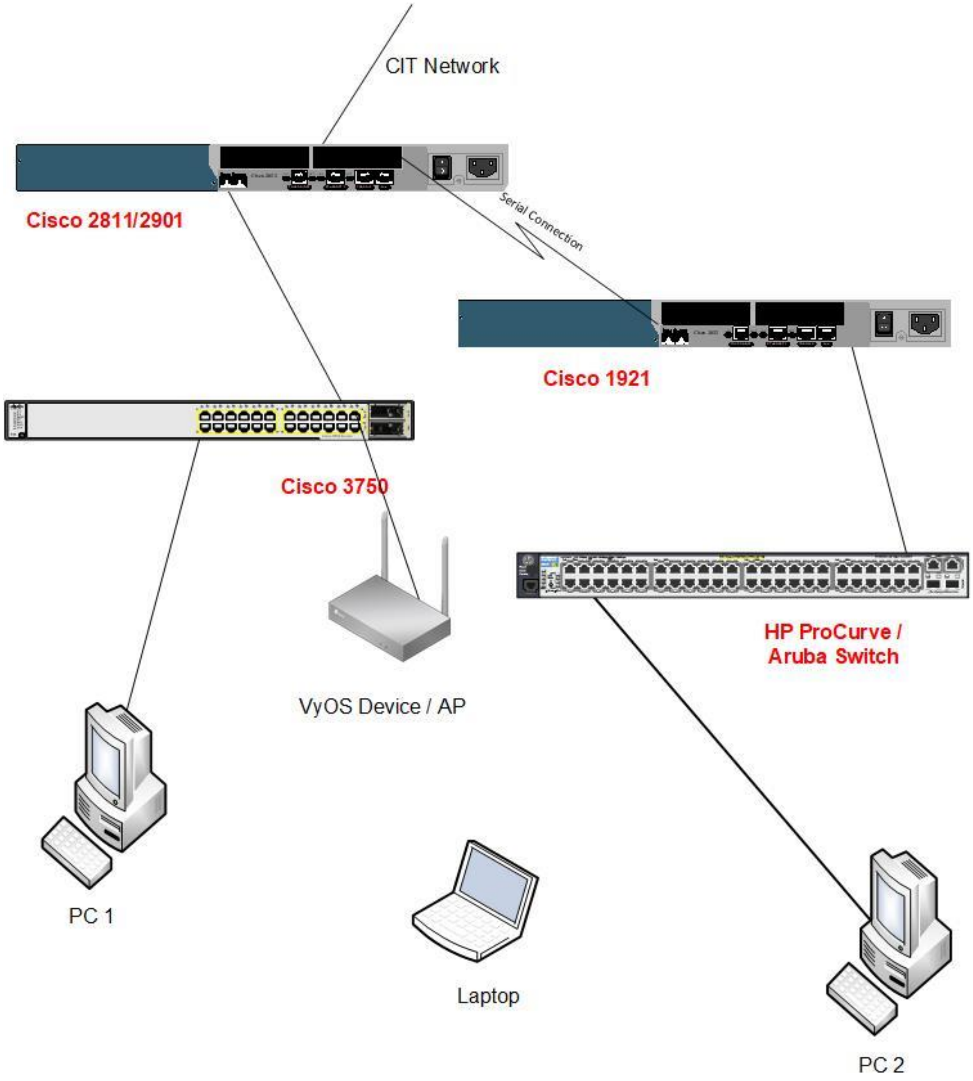
Lab 4: Routing, NAT, and ACL

Overview:

In Lab 4, utilize routers and switches to build larger scope of network. The goal is to gain deeper insight in Virtual Local Area Networks (VLANs) and Network Address Translation/Port Address Translation (NAT/PAT), and distance vector routing protocols, i.e., Routing Information Protocol (RIP) version 2, and familiarize with the use Access Control Lists (ACLs).



Objectives:

1. Form the network above with the CIT network connection uplink port set to 10.25.XX.254 on the network address range assigned to the group at the beginning of class (10.25.XX.0/24) networks where XX represents the group number.

2. Disable or remove the Spanning Tree Protocol (STP) enabled in Lab 3. Remove the uplink for the Cisco 1921 for the 10.17.XX0/24 network from the configuration including specific interfaces and default routes, etc.

3. The two routers are connected with high-speed serial ports via the blue High Speed Serial Interface (HSSI) cable in the lab cable supplies distributed at the beginning of the semester. Create a IP address range using Classless Inter-Domain Routing (CIDR) with the best use of IP address space per lecture discussions in the 192.168.(50+XX).0 network. The WAN protocol is Point-to-Point Protocol (PPP).

4. Setup Routing Information Proutocol (RIP) version 2 on the routers for your network. Please use the "no auto-summary" option.

5. Each Cisco 2811/2901 and 1921 will have a link to a specific switch, one switch should be a Hewlett Packard (HP) ProCurve/Aruba and the other a Cisco 3750. The switches and routers may need reconfigured from previous labs.

6. The Cisco switch will have a VyOS Device that needs configured as an Access Point (AP) only wit

7. h a Linux laptop connecting via wireless.

8. The switches should have 5 VLANs (except Group 01 will only have 4) on each which are able to communicate across the routed network where Port 1 is configured for VLAN XX, Port 2 is configured for VLAN 1XX, and Port 3 is configured for VLAN 2XX. The 4th VLAN 172 is connected to the VyOS Device that needs configured as an AP and should be able to communicate with all devices in and out.

9. The IP addresses of all the computers while plugged into the specific ports are set to Dynamic Host Configuration Protocol (DHCP) starting at 100 with 100 available addresses in the following IP address ranges: 192.168.XX.0/24; 192.168.1XX.0/24; 192.168.2XX.0/24 on the Cisco router; 172.30.1.0/24 on the VyOS Device that needs configured as an AP; 192.169.XX.0/24; 192.169.1XX.0/24; 192.169.2XX.0/24 on the HP switch.

10. Connections outside of this private network should be configured through NAT/PAT.

11. Configure ACL/Firewall rules such that only devices on the VyOS Device that needs configured as an AP can use Trivial File Transfer Protocol (TFTP) to a TFTP server that is to be added by the group. Additionally, set only the 192.168.XX.0/24 and 192.168.2XX.0/24 networks can access the CIT network to view a web browser.

12. Configure the switches, routers and computers such that each computer can ping all other computers in the diagram.

HINTS:

1) NAT needs to be configured to simulate the real-world situations
2) Default route maybe necessary on the edge router
3) Please keep copy the configuration files in a Notepad or other editor to save off device.