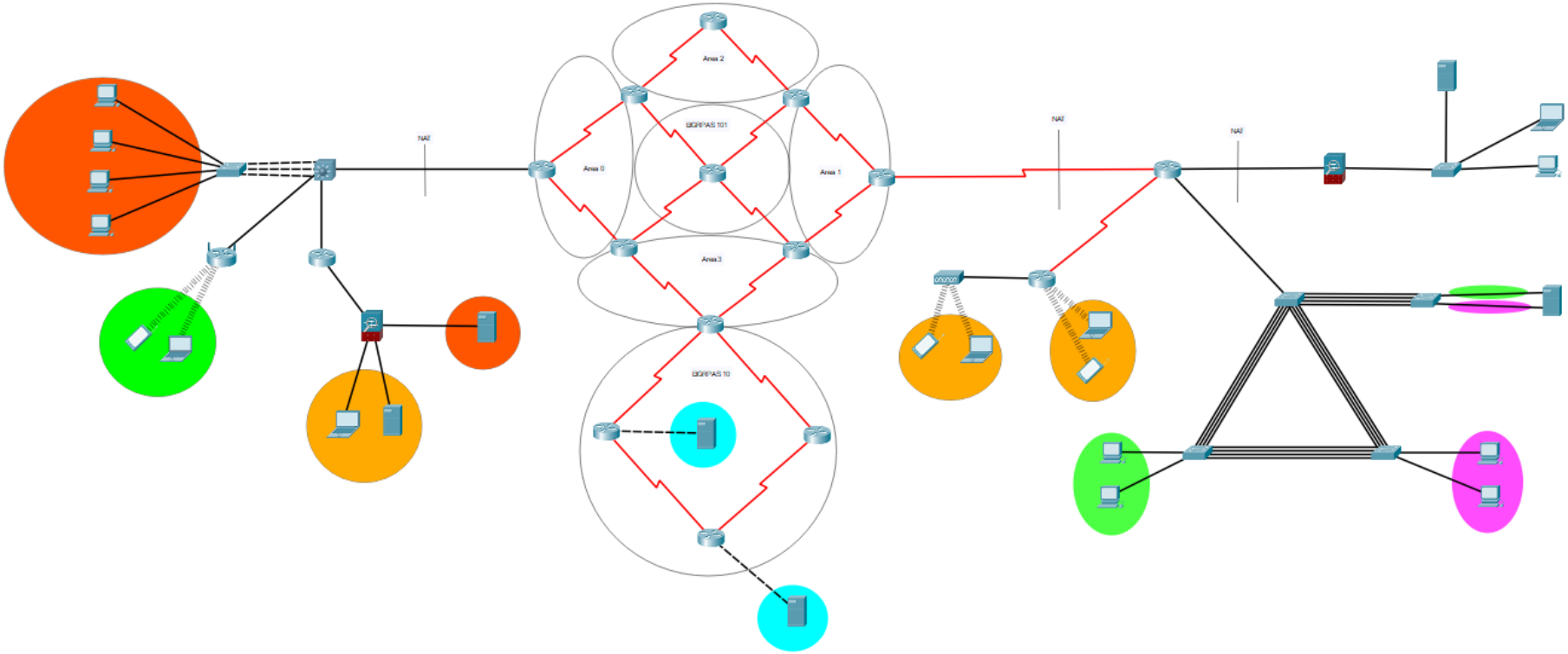
# Capstone **7C**



# What is 7C?

Capstone 7C is the third option for the last competency in Computer Networking. In this competency you will be challenged on utilizing many of the skills you have learned here to create a complex network.  The emphasis is on security, link-state routing and redundancy.

# What you will be doing:

- 2 EIGRP networks
- OSPF Multi Area
- Static Routes (default and last resort)
- Route Redistribution
- VPN over GRE
- NAT/PAT based firewalls
- Standard ACLs
- Extended ACLs
- Etherchannel (Manual, LCAP, and PAgP)
- Switching concepts (STP, SVI, VLANs, and Trunking)
- Network services (HTML, DNS, DHCP, DHCPv6, RADIUS)
- Security on all devices (SSH across the network)
- SPAN
- Redundancy (Floating Static Route)
- IPv4 FLSM and VLSM
- IPv6 Dual Stack and 6to4
- Route Summarization

# Network Addressing:

Every student will be given a different IP Address scheme.

| Name | Router IP Address Range | Public IP Address Range (Outside of NAT) | Private IP Address Range (NAT Inside) |
|---|---|---|---|
| **Student 1** | 5.2.12.0/24 | 55.10.1.0**/25** | 192.168.1.0/24 |
| **Student 2** | 20.4.10.0/24 | 55.10.1.0**/25** | 192.168.2.0/24 |
| **Student 3** | 35.6.8.0/24 | 55.10.1.0**/25** | 192.168.3.0/24 |
| **Student 4** | 50.8.6.0/24 | 55.10.4.0**/25** | 192.168.4.0/24 |
| **Student 5** | 65.10.4.0/24 | 55.10.5.160**/25** | 192.168.5.0/24 |

# Network Addressing Explained:

**Router IP Address Range:**

This range is for IP addresses within the router cluster. These may also be assigned to the servers within the router cluster.

**Public IP Address Range (Outside of NAT):**

This IP address range is designed to be used within the networks outside of the  This range is mostly optional depending on how the network is configured.

**Private IP Address Range (NAT Inside):**

This IP address range is designed to be used in the networks that are on the inside of NAT. These IP addresses can be reused depending on how NAT is configured.

## Network Security Specific Requirements:

| |
|---|
| All routers must have their own **unique passwords** |
| All routers must have passwords on VTY lines 0 to 4 with their own unique passwords |
| All switches must have their own unique console passwords |
| All switches must have unique passwords on vty lines 0 to 4 |
| Disable all unused switch ports |
| Disable all unused lines (unused console, vty, etc) |
| Configure all devices with a timeout of 2 minutes for 3 failed login attempts |
| Configure all devices to have a MOTD of “Property of Enology, keep out” |
| ***NOTICE: DO NOT INCLUDE ANY PERSONALLY USED  PASSWORDS FOR THIS ASSIGNMENT.*** |

## Other Requirements:

| |
|---|
| Include a copy of your IP Address scheme for all networks in a sensible layout |
| Include a scheme of all passwords used on the network ***NOTICE: DO NOT INCLUDE ANY PERSONALLY USED  PASSWORDS FOR THIS ASSIGNMENT.*** |
| Make sure all DNS entries are consistent |

# Part 1

Part one includes all parts shown.

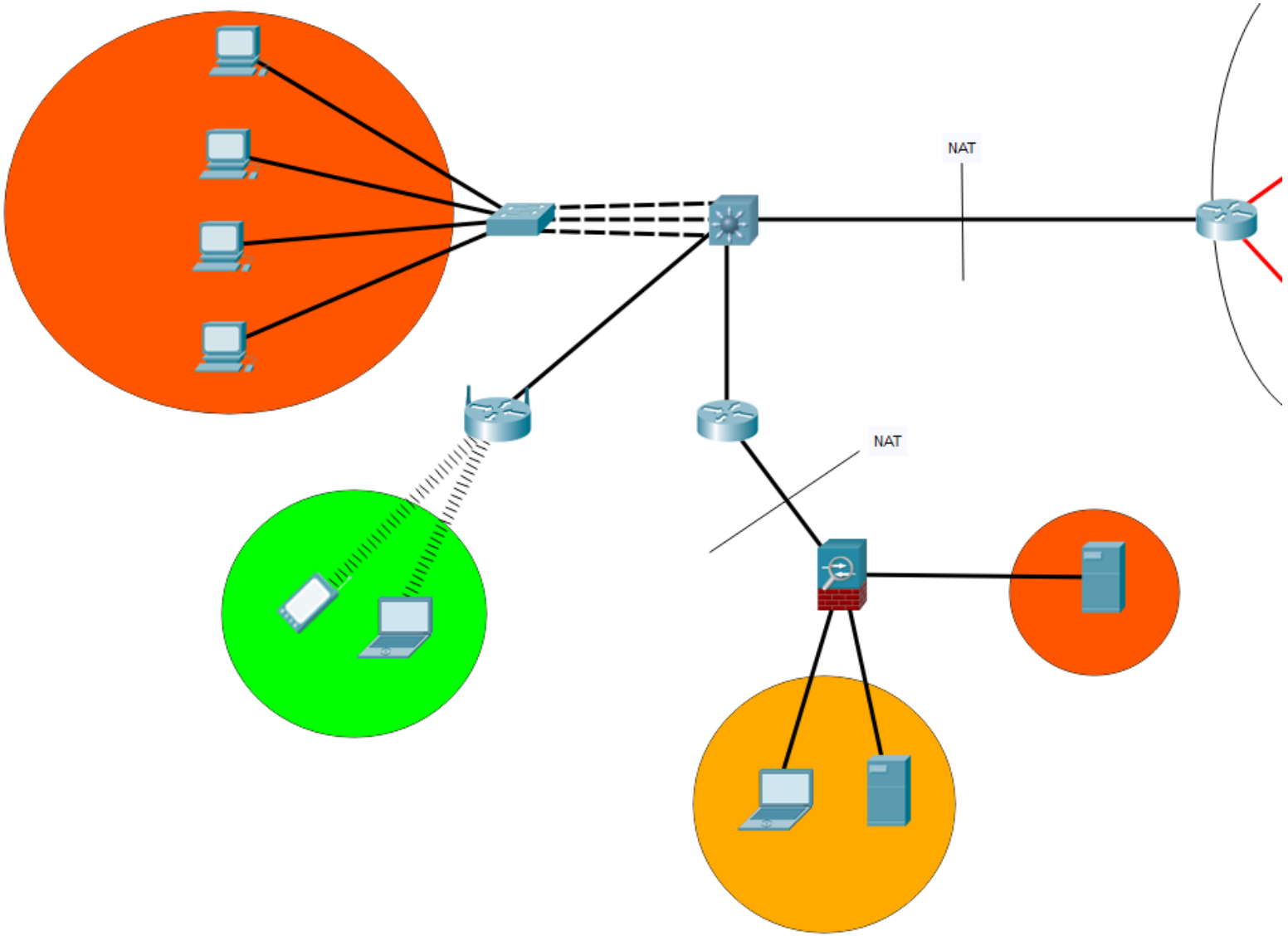



***Figure 1***

This network is from a small, locally owned LAN cafe. This LAN cafe provides 4 different services. The first service is four (4) kiosk PCs. The second service is a free WiFi network. The third service is a web server **(SRV3)** that the business owner uses to advertise his LAN cafe. The fourth service is a small management PC and a DHCP server **(SRV2)** that serves DHCP leases to the WiFi network and the 4 kiosk PCs.

The connection between R2 and L3 SW1 is the point of demarcation between these two networks.

Your task for this section is to:

| |
|---|
| The network may expand in the future, please leave at least 4 additional subnets for growth supporting at least 14 hosts |
| For direct connection networks (2 hosts) please use /30 (255.255.255.252) |
| Configure the Kiosk PCs to get DHCP addresses from SRV2. Configure the Kiosk PCs to automatically set SRV3 as their DNS server |
| The connection between SW1 and L3 SW1 is a EtherChannel |
| Configure the wireless network to not be able to communicate with the kiosk PCs |
| Give the wireless network a BSSID of 'Mikes_Cafe' and disable authentication |
| Configure **L3 SW1** to connect to **R2** using IP addresses from the router public IP address table |
| Configure the wireless router to use WPA2 Personal with AES encryption, use the password 'Enology' |
| **R2** and **L3 SW1** will be on the public IP address range |
| Configure **L3 SW1** and **SW1** to be SSH accessible from LT1. |
| For ASA1, use a 5505 Adaptive Security Appliance *(do not use a 5506)* |
| Set up the ASA to have VLANs 10 and 20, vlan 10 for **SRV2** and **LT1**, and vlan 20 for **SRV3**. |
| Set up the ASA as a firewall. Allow only HTTP requests into VLAN 20, Allow DHCP requests into VLAN 10. Allow ICMP requests to VLAN 10. Allow all connections out of VLAN 10. Only allow HTTP, HTTPS, DNS, and ICMP to SRV3. |
| **Bonus: Create a web server on SRV3 describing the LAN cafe. Give the server a DNS name and make sure that is the entry across all DNS servers on the web** |

# Part 2

Part two includes the small lower router cluster. Consisting of 4 routers and 2 Servers

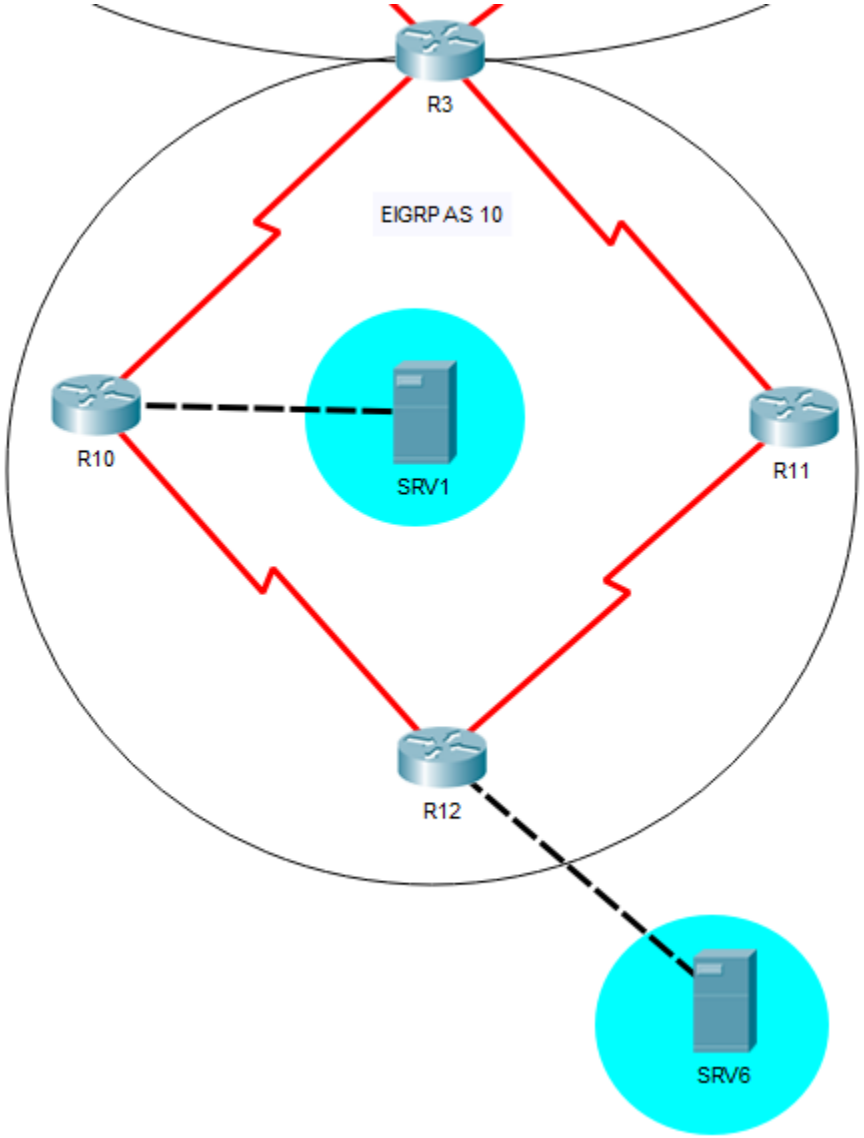


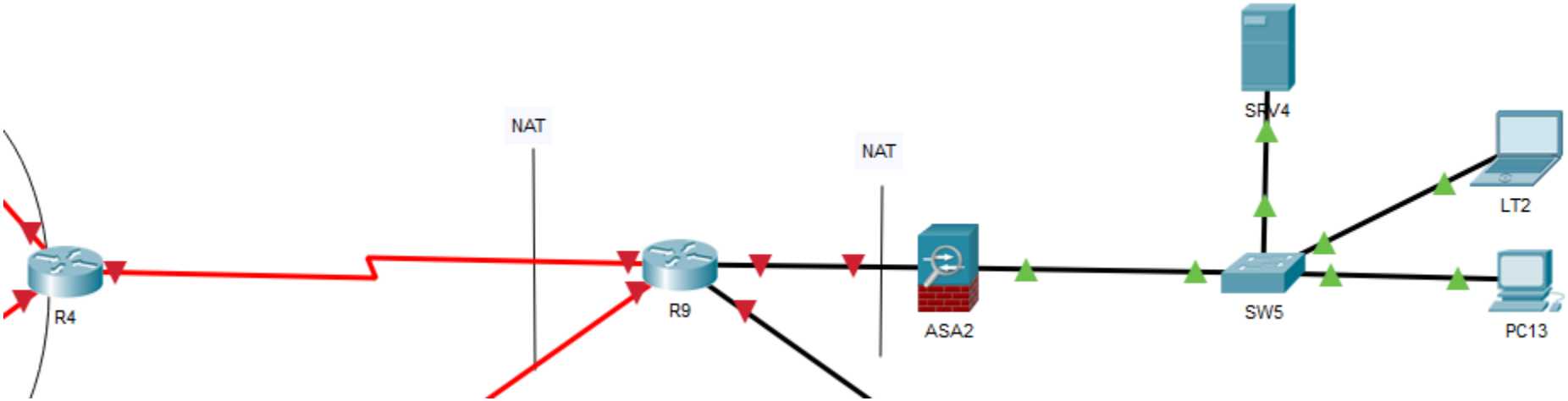

***Figure 2***

This is a small ISP network that serves a couple of functions. It has a web server that stores the configurations for all of the servers in TFTP **(SRV1)** and an email server that is a service provided by the domain for ISP.
Your task for this section is to:

| |
|---|
| Create an EIGRP group of those 4 routers with an ASN of 10 |
| Configure all serial links to use public IP address range |
| Use route redistribution to merge routes from OSPF area 3 (in a different section) with the AS (AS 10) |
| Configure SRV1 to become only a TFTP server. This will be the TFTP server for storing running router configurations from R0, R1, R2, R3, R4, R5, R6, R7, R8, R10, R11, R12 |
| Configure SRV1 to become an NTP server. All the routers that are stored on TFTP (as mentioned before) will also be synced to this NTP server. |
| Configure SRV6 to become an Email server. |
| Configure SRV6 to become a DNS server. Add isp.net as the network section that houses R3, R10, R11, R12, SRV1, SRV6 |
| Configure DNS on SRV6 to have a CNAME entry of email.isp.net for SRV6 |
| Configure DNS on SRV6 to have a CNAME entry of tftp.isp.net for SRV1 |
| Configure DNS on SRV6 to have a CNAME entry of R#.isp.net for R3, R10, R11, and R12 |
| Add SRV6 to the isp.net domain. |
| Add all routers in this section to the isp.net domain as well |

# Part 3

Part three includes the top half of the rightmost network *(This does not include the wireless network or the etherchannel network)*



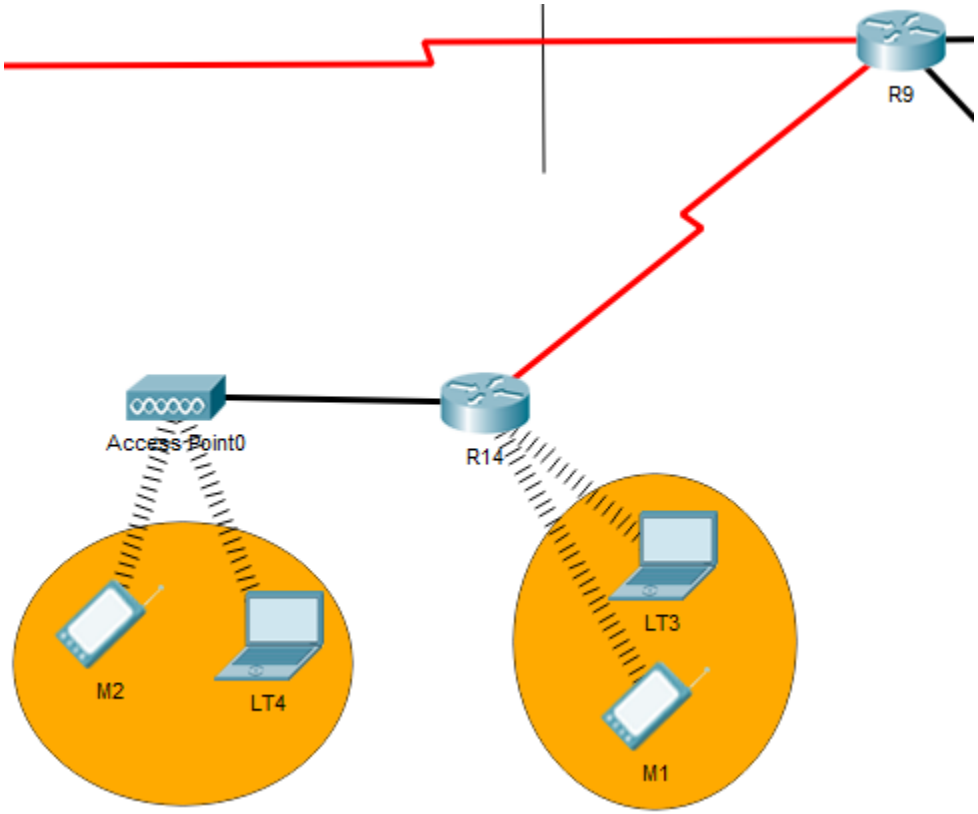
These are the main networks for a larger business operating in the area.

| |
|---|
| Configure the link between R4 and R9 with one public IP address space (R9 will only use 1 IP address on the connection between R4 and R9 for all the NAT inside stub networks) |
| Every other network will go through NAT Overload |
| ASA2 will be configured with RoaS. There will be 2 vlans for this physical network, one serving SRV4, and another serving LT2 and PC13. |
| Shut down all unused ports on SW5 and configure the enable password of ‘mike’ and the console and vty lines 0 to 4 passwords as ‘class’ |
| Configure SW5 with a SPAN port that goes to PC13 |
| Configure SRV4 to be a DHCP server for LT2 and PC13. |
| **Bonus: Create a web server on SRV4 describing the business. Give the server a DNS name and make sure that is the entry across all DNS servers on the web** |

*Recommendation: Configure R9 last after finishing Parts 3, 4, and 5.*

# Part 4

Part four includes the small wireless network off of R9.

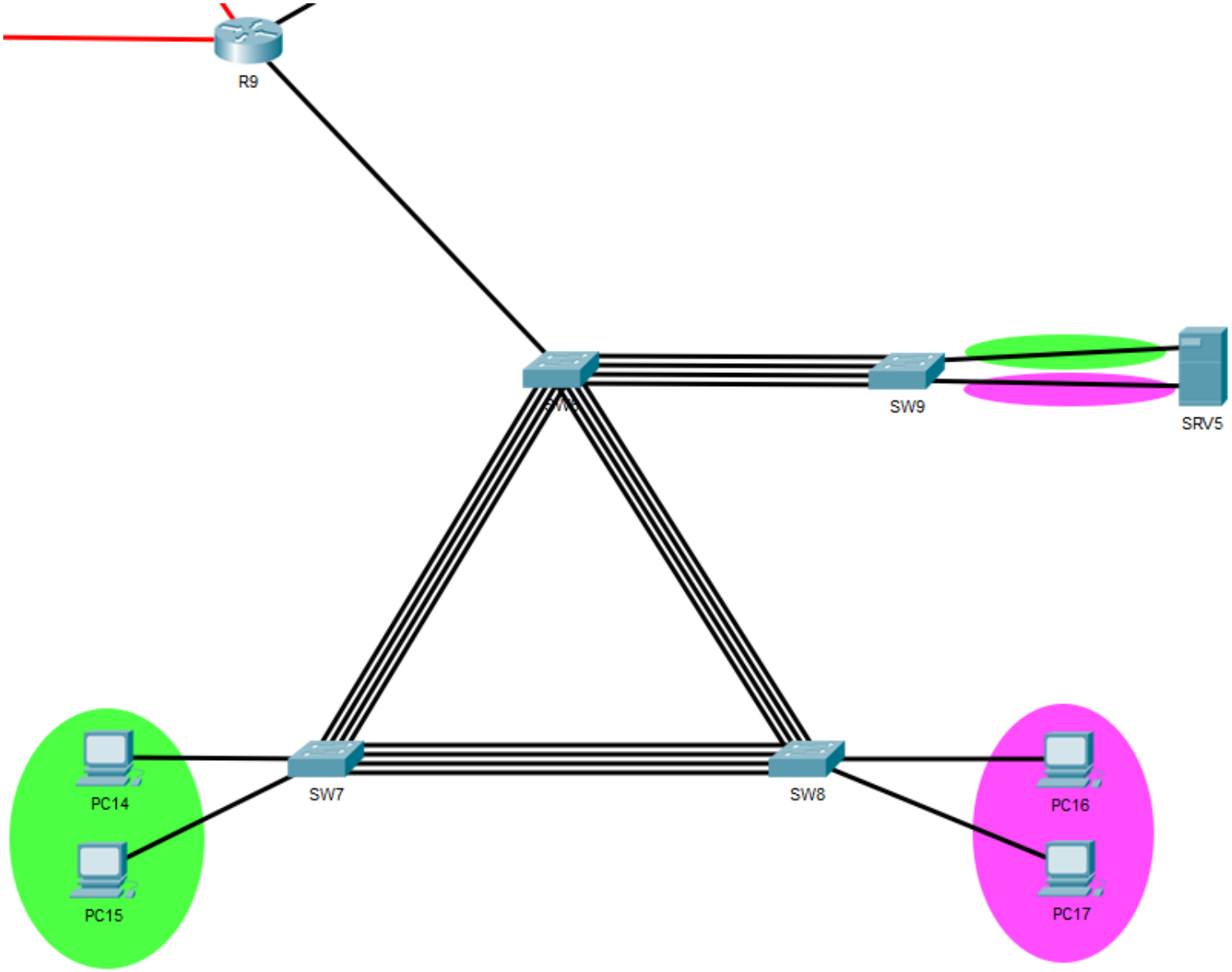


This is a simple network. There is not much to do on this network because Packet Tracer's simulation of wireless connectivity is limited. You will be setting this up as if it were 2 different wireless networks, one for public free WiFi, and one for corporation WiFi.

| |
|---|
| Make the AP the 'public wifi' network. Give it an SSID of 'Corporation_Public_WiFi'. Also give it a password of 'Corporation_Public_WiFi'. Use WPA-PSK with the encryption type of AES. |
| Connect M2 and LT4 to 'Corporation_Public_WiFi' |
| Configure R14 with a HWIC-AP-AG-B expansion slot card |
| Configure R14 to have 3 networks, one to R9. One to the Access Point, and one to LT3 and M1. |
| Configure R14 with 2 DHCP pools, one for the network with LT3 and M1, and the other for the Access Point network. These must be seperate networks |
| Configure R14 with open authentication, WPA, WPA-PSK key of 'Enology123' |
| Configure R14 with an SSID of 'Corporation_WiFi' |
| Configure R9 to filter between the two networks ('Corporation_public_WiFi' and 'Corporation_WiFi' networks) |
| The Access Point network ('Corporation_public_WiFi') Should not be able to access the rest of the corporation networks. All traffic should go right out to R4. This should be accomplished with an ACL |

# Part 5

Part five contains the etherchannel network off of R9

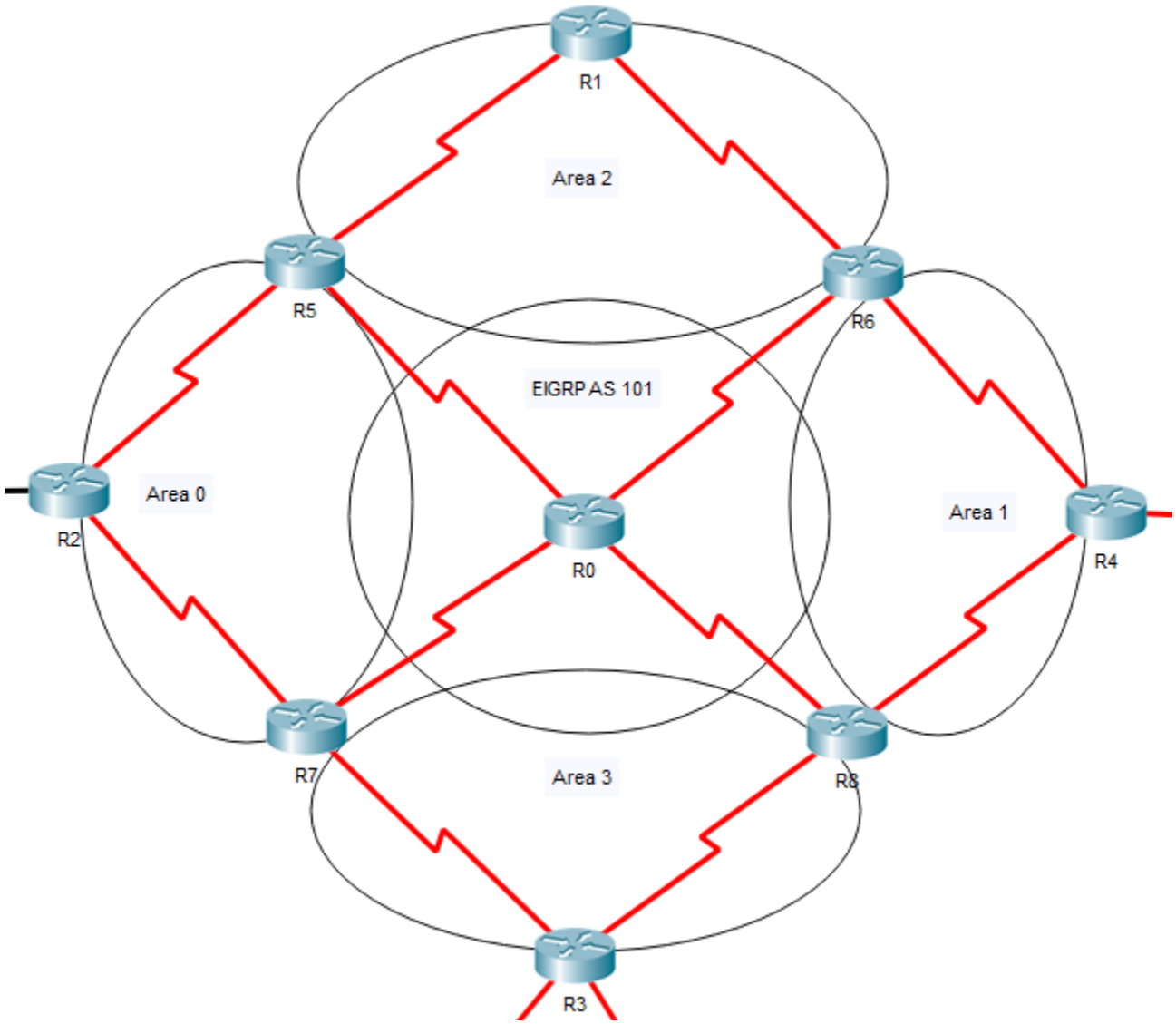


This is the center of the corporation computers. There are 2 main VLANs, sales and support. The green network with PC14 and PC15 is the sales VLAN. The purple network with PC16 and PC17 is the support network. Both share  SRV5 running 1 DNS server for both VLANs and each have a DHCP server off of SRV5. Each VLAN will be given 2 lines to make an etherchannel

| |
|---|
| Configure all switches to have 2 etherchannel networks. One will be running an etherchannel for VLAN10 and the other two lines will be running an etherchannel for VLAN20 |
| SW9 will have 2 lines going to SRV5. one line will be used for VLAN10 only, and the other for VLAN 20 only. |
| Configure SRV5 with two NM-1CFE expansion slot cards |
| Configure SRV5 with 2 DHCP pools, one for VLAN 10, and one for VLAN 20 |
| Configure SRV5 with 1 DNS server on VLAN 10 |
| Configure R9 with an access list that permits communication between VLAN 20 and SRV5 on VLAN 10 |
| Configure R9 with an access list that disallows communication between VLAN 10 and VLAN 20 |

# Part 6

Part 6 is the architecture of the ISP network.



This is the heart of the ISP network. This forms the backbone in which all of the other smaller networks will connect. It uses 4 OSPF areas and 1 EIGRP area. All the areas are shared with route redistribution.

| |
|---|
| Create 4 OSPF areas<br>OSPF area 0: R2, R5, R7<br>OSPF area 1: R4, R6, R8<br>OSPF area 2: R1, R5, R6<br>OSPF area 3: R3, R7, R8 |
| Create 1 EIGRP area<br>EIGRP AS 101: R0, R5, R6, R7, R8 |
| Create a floating static route from R2 to R4 taking the path of R2-R5-R0-R8-R4 |
| Create a backup floating static route from R2 to R4 taking the path of R2-R7-R0-R6-R4 |
| Make sure all packets from R3 go through R7 first |
| Make sure there are no routing loops |