INDIVIDUAL ASSIGNMENT

CT133-3-2-SRE

SWITCHING AND ROUTING ESSENTIALS

APU2F2202CS (CYB), APD2F2202CS (CYB)

Weightage: 40%

MODULE CODE : CT133-3-2-SRE

Lecture Name : Noris binti Ismail

Student Name	Intake Code	TP Number
AASHRITA JAGADESWARARAO NANDAMURI	APD2F2202CS(CYB)	TP063125

Contents

1.0 INTRODUCTION

This report mainly focuses on Entire Network Layout – packet tracer, LAN, and WAN configuration. Explanation and screenshots on configuration. Layer 2 Security Mechanisms Deployment in configuration.

2.0 IP ADDRESSING & ROUTING PROTOCOLS TABLE

KL Network

DEVICE	IP ADDRESS
VLAN 10 – HR	192.168.1.1
HR - PC	192.168.1.2
VLAN 20 – Design	192.168.1.1
Design – PC	192.168.2.2
VLAN 30 - Delivery	192.168.3.1
Delivery – PC	192.168.3.2
VLAN 50 – Management	192.168.50.1
KL PC- Management	192.168.50.2
Dis_SW VLAN 50	192.168.50.10
HR_SW VLAN 50	192.168.50.11
Design_SW VLAN 50	192.168.50.12
Delivery_SW VLAN 50	192.168.50.13

Server Farm Network

SERVERS	IP ADDRESS
DNS	198.51.100.10
Web	198.51.100.20
FTP	198.51.100.30
Vlan10 - ServerFarm	198.51.100.1
SerFarm_Router GigabitEthernet0/0/0.10	198.51.100.1
SerFarm_Router Serial0/1/0	200.100.100.18

WLC Network (REMOTE)

WLC Management Network	192.168.100.0
VLAN 10 – R&D	192.168.10.1
VLAN 20 – RB Management & Native	192.168.10.1
Admin PC	192.168.100.2
GigabitEthernet0/0/0.10	192.168.10.1
GigabitEthernet0/0/0.100	192.168.100.1
Serial0/1/0	200.100.100.1
Serial0/1/1	200.100.100.5

3.0 Type of Layer 2 Attacks

Layer 2 switching setups are vulnerable to network security threats and are frequently seen in commercial clients' cable racks. It is one of the most common Layer 2 security risks, but it is also one of the most difficult to detect for network managers. Its goal is to disable or compromise network users to get access to sensitive data like passwords. The capacity of a switch to learn MAC addresses, end-station MAC address resolution through the Address Resolution Protocol (ARP-RFC 826), or DHCP server IP address allocations are all used in these sorts of attacks. Layer 2 switching setups are vulnerable to network security threats and are frequently seen in commercial clients' cable racks. It is one of the most common Layer 2 security risks, but it is also one of the most difficult to detect for network managers. Its goal is to disable or compromise network users to get access to sensitive data like passwords.

The capacity of a switch to learn MAC addresses, end-station MAC address resolution through the Address Resolution Protocol (ARP-RFC 826), or DHCP server IP address allocations are all used in these sorts of attacks. Even though IEEE 802.1x and access control lists are important components of a company's threat prevention measures, they are unable to prevent the Layer 2 security assaults detailed in this article. Any of the attacks outlined in this article would be easy for an authorized user to carry out. Fortunately, these assaults may have been averted if aspects that are already available to the public had been used. In this post, we'll go through the most prevalent Layer 2 security concerns and how to protect yourself against them by utilizing the safeguards that are already built into your system.

Type of Security Attack on Layer 2.

- Spanning Tree Protocol (STP)Attacks.

STP's main purpose is to eliminate possible loops in a network. Layer 2 LANs would ground to a standstill if there was no such protocol because loops would swamp switches with traffic. Here's where the attack comes in: attackers can introduce additional STP devices onto the network and try to modify how STP works. The assault might then impact how traffic flows over the LAN, thus jeopardizing the security of any traffic in the network. To reduce network administration disturbances, a single VLAN for management is created, as well as segregating bandwidth utilization from other departments.

- STP Attack Mitigation

STP attacks may be mitigated with technologies like PortFast and BPDU Guard. To avoid connectivity concerns, PortFast was created. This is done by skipping the listening and learning processes and immediately entering the STP forwarding state.

- Address Resolution (ARP) Attacks

Every network device that is linked to an Ethernet network uses ARP. ARP uses just the target device's known IP address to obtain the MAC address for a destination device. ARP isn't secure by itself since devices are intended to trust the responses they get.

- ARP Attack Mitigation

One approach for preventing an ARP MITM attack is to have robust WEP/WAP encryption on APs. This stops unwelcome users from entering the network simply because they are close by. By requiring HTTPS, attackers are unable to access the data that is being sniffed. RSA-based public key pair authentication ensures that devices only communicate with the other designated device.

- MAC ADDRESS FLOODING ATTACK:

This procedure is followed to render the switches susceptible. According to interserver.net, Switches retain a table structure known as the MAC Table. This MAC Table contains the specific MAC addresses of the network's host computers that are connected to switch ports." This implies that data may be transmitted from the switch to the host computers. The MAC flooding attack is used to delete the MAC table by delivering many ethernet frames to the switch's memory that holds the MAC address table. As a result, data cannot be transmitted owing to the large amount of data received and recording new data will be impossible. Furthermore, the attacker can obtain personal information from the numerous victims because of the data packets that have been sent out.

- Mac address flooding attack mitigation:

Cisco switches are packed with in-built security feature against MAC flooding attacks, called as Port Security. Port Security is a feature of Cisco Switches, which give protection against MAC flooding attacks. Always take care to keep our systems safe.so it is necessary to, have tools and processes in place to prevent attackers from gaining access to the system and to respond to attacks that put it at danger. Port security can be used to prevent MAC flooding attacks. By using the switchport port-security command to enable this functionality in port security.

4.0 LAYER 2 SECURITY DEPLOYMENT TO MILIGATE THE ATTACKS

The team's strength may be judged by the squad's weakest member. The Data Link Layer (also known as Layer 2) is frequently the weakest link in a network. Because each layer of the OSI operates independently of the others, a vulnerability in one layer may have ramifications at higher levels, even if those layers are ignorant of the issue. Layer 2 requires additional attention and study due to its huge impact. Many companies can now defend themselves against Layer 2 threats. These features are activated by default on some Cisco switches; all must do is toggle the switch to use them. Harassment of groups continues to be a problem.

Hackers might utilize the breakdown of the Athena assault to target the switch's CAM table using MAC attacks. The MAC addresses of each port, as well as the VLAN settings for those ports, are also included in this data collection. Due to their limited size, large data sets cannot be stored in CAM databases. During a MAC assault, the CAM will be bombarded with entirely random MAC and IP addresses (Defending against layer 2, 2022). The network becomes overloaded when the switch's CAM table exceeds its maximum capacity. A switch port may be limited to a certain number of MAC addresses at any given time. The total number of MAC addresses that a port can obtain is limited because of this. The maximum value can be set by the administrator if it does not exceed the CAM table's limit.

It is possible to track the time of process for linking a MAC address with a port. A device with an invalid MAC address will not be recognized by a port. When the port is closed, the user will be notified, and the port itself will be closed. A Successful VLAN Hopping Attack's Components When many VLANs share a single trunk connection, the network becomes subject to a "VLAN hopping" attack. An attack can be carried out in one of two different methods. This allows it access to both VLANs' traffic, as well as the ability to monitor and interact with it (Preventing Layer 2 Attacks, 2020). Attacks that hop across VLANs might be thwarted using switch-level limitations. It's probable that administrators will need each trunk port to have its own VLAN ID. After relocating unwanted ports to a virtual local area network, you can shut them (VLAN). Turning off DTP, on the other hand, could be helpful.

When DHCP is used as a strategy, "man-in-the-middle assaults" are referred to as "man-in-the-middle attacks." It might be legitimate servers that haven't been approved yet, or it could be rogue servers set up intentionally to steal secret information in the meantime (Understanding and Preventing L2 Attacks - Security Overview 2021). To keep the illusion going, the

malicious server forwarded the stolen data to the individual it was attempting to deceive. Snooping on DHCP communication can assist prevent "man in the middle" attacks. You will be able to identify which requests should be believed and which should be disregarded with the aid of this function. Your firewall protects your network's switches, routers, and servers. It's critical to keep an eye out for unusual DHCP servers and other types of cybercriminal attack tools deployed outside the firewall. There is a database that keeps track of requests that aren't trustworthy. The demands imposed on DHCP snooping by requests originating from the Internet will be met with ease. Spoofers are criminals who perpetrate crimes by imitating another person, and MAC addresses and Internet Protocol (IP) addresses are the most typical targets of spoofing. (Don’t Overlook Layer 2 Security –Consequential for Network (Part-1), 2021)

To gain access to a network or steal the identity of a victim, cybercriminals will utilize forged MAC addresses. Spoofing attacks aimed at IP addresses have the potential to overwhelm switches and bring them down. IP Even the most advanced attacks, such as MAC and IP spoofing, are rendered impossible using Source Guard. This function may check for both MAC and IP spoofing at the same time. This feature must be enabled for Source Guard to work effectively since it uses the DHCP snooping database to identify known IP spoofing threats. To accomplish MAC spoofing, Source Guard requires a router with DHCP Option 82 enabled. When this feature is enabled, any attempt to impersonate IP or MAC addresses will be detected (Common Layer 2 Threats, Attacks & Mitigation, 2017).

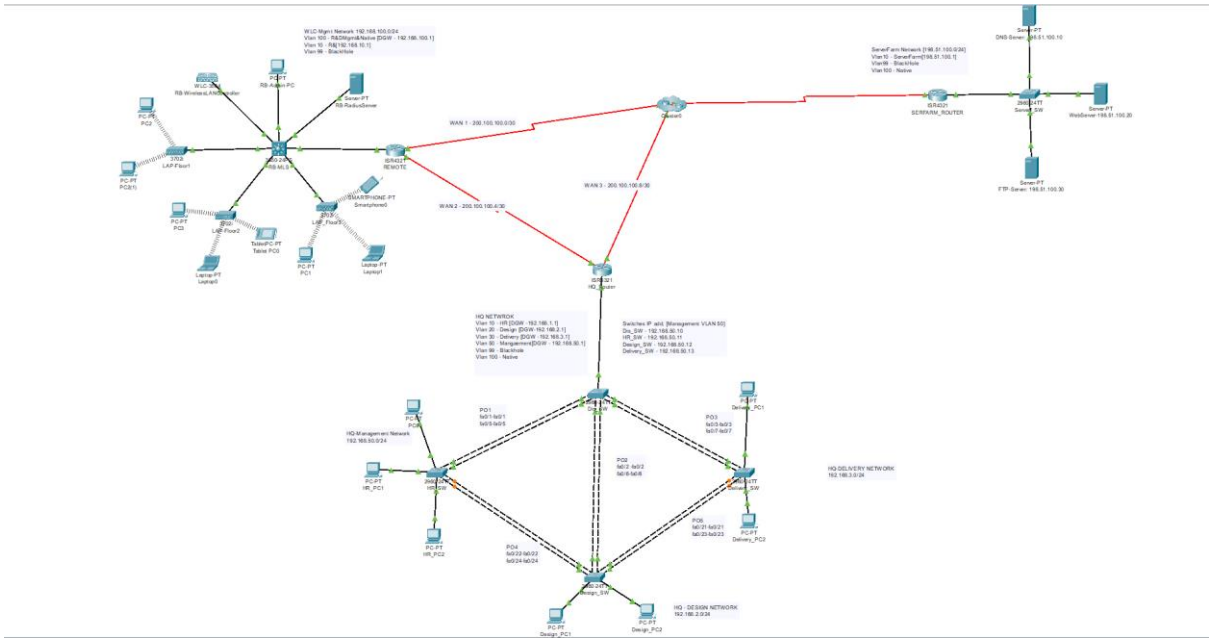


Figure 1:Topology

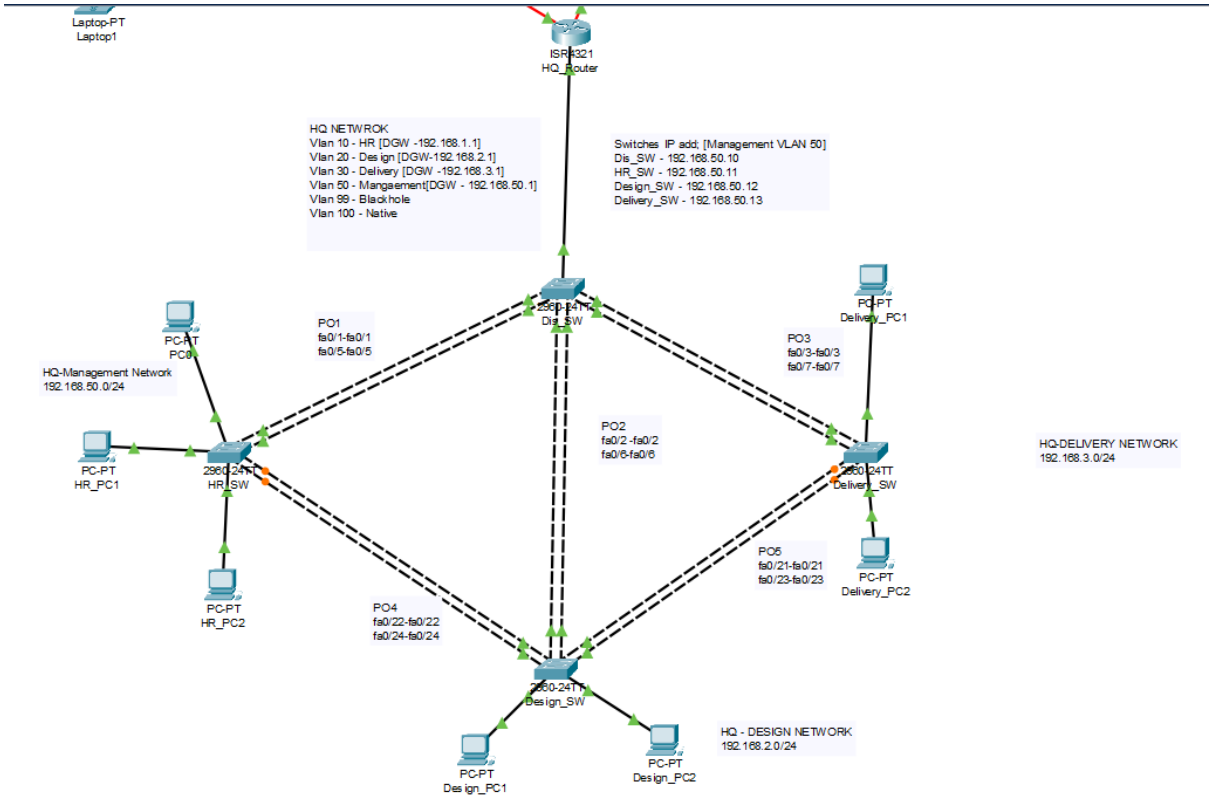


Figure 2:HQ

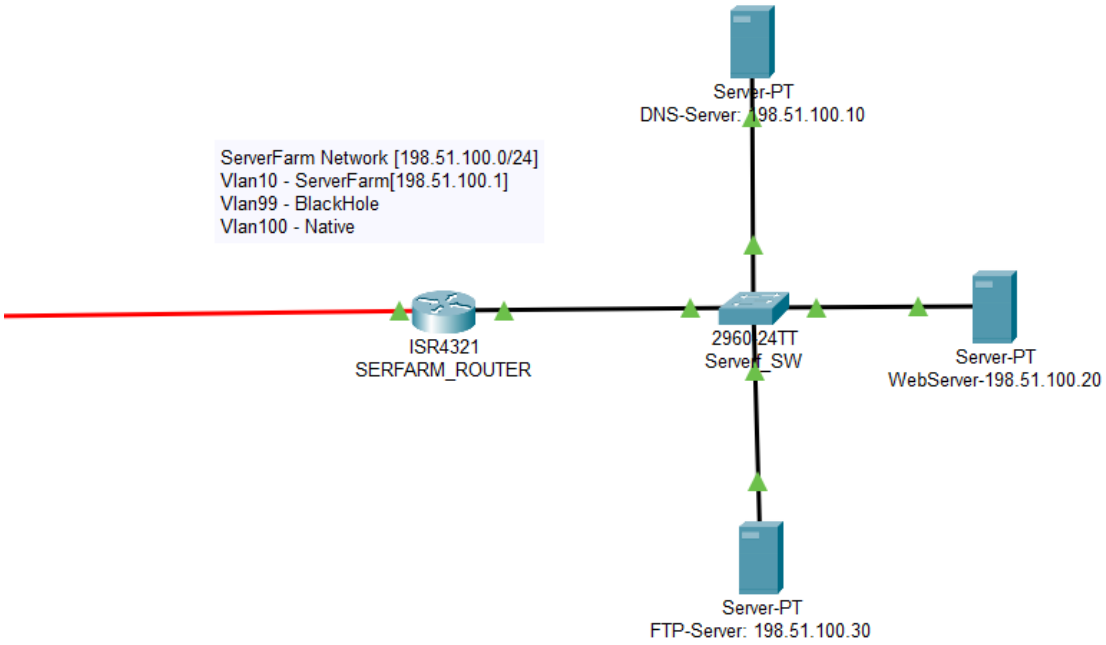


Figure 3: Server Farm

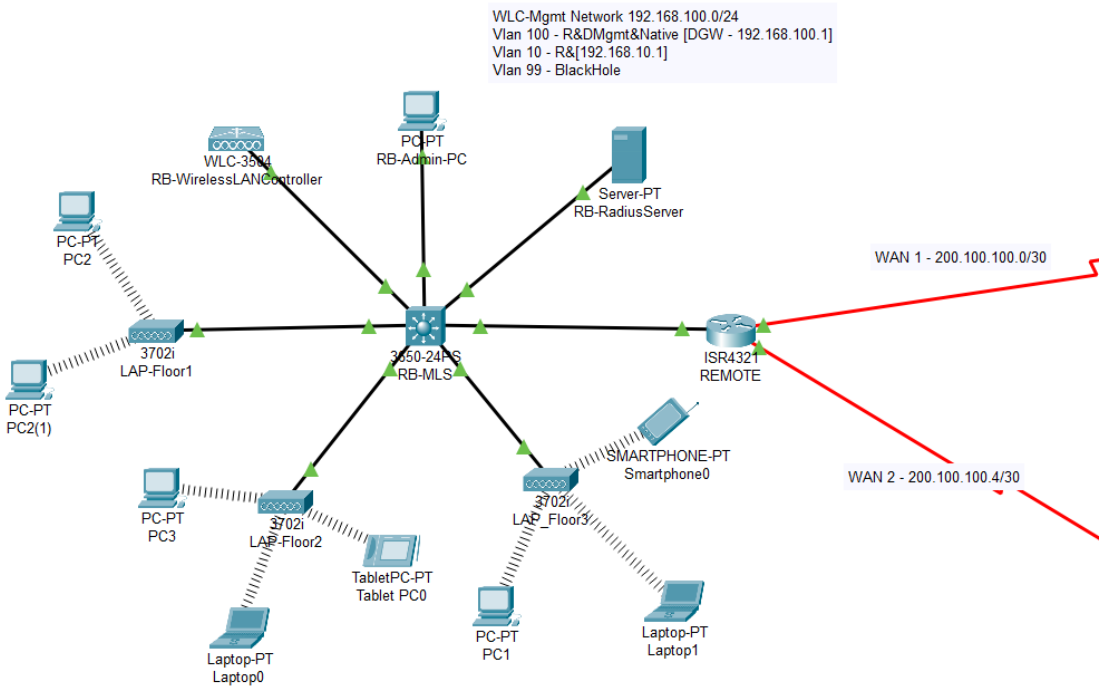
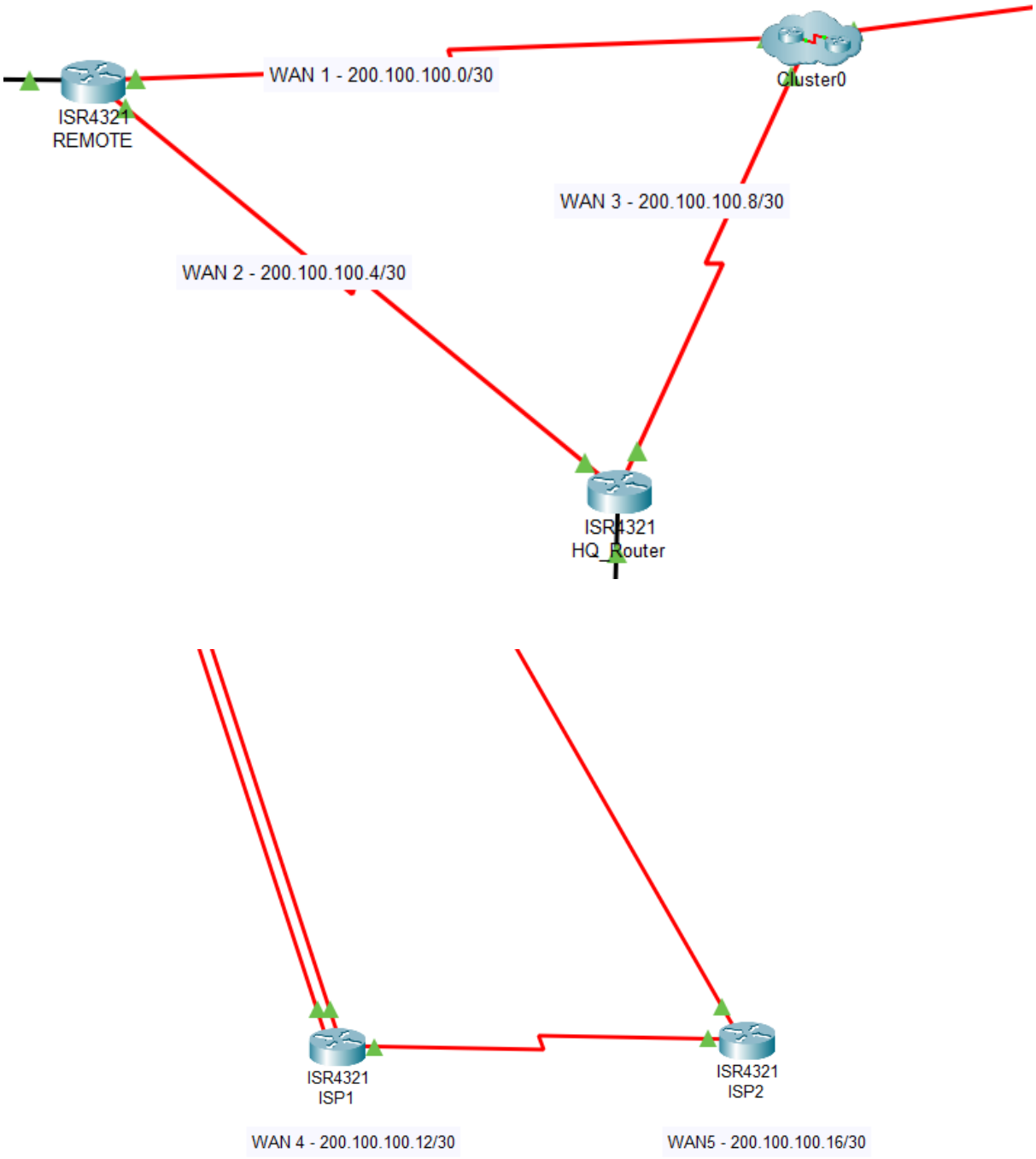


Figure 4: Remote Branch



WAN Connections:

1. WAN 1 – 200.100.100.0/30
2. WAN 2 – 200.100.100.4/30
3. WAN 3 – 200.100.100.8/30
4. WAN 4 – 200.100.100.12/30

5. WAN 5 – 200.100.100.16/30

5.0 CONCLUSION

In both the corporate and residential spheres, network security is a critical component. Wireless routers, which are commonly found in modern houses with high-speed internet connections, might pose a security concern if they are not properly protected. You may reduce the chances of data loss, sabotage, or theft by putting in place a strong network security system. This structure is both durable and dependable, making it a good choice for the job. WLCs are an example of technology that can help with network management and productivity. When various technologies, guidelines, and devices are taken in conjunction, they may build networks which are steady, protect, and trustable.

REFERANCES:

- ARP Poisoning: What it is & How to Prevent ARP Spoofing Attacks. (n.d.). Retrieved from VARONIS: https://www.varonis.com/blog/arppoisoning#:~:text=Properly%20controlling%20physical%20access%20to,a%20machine%20on %20the%20network.
- ARP Spoofing. (n.d.). Retrieved from imperva: https://www.imperva.com/learn/applicationsecurity/arp-spoofing/
- MAC Flooding attack What is it, what is it for and how to completely mitigate it? (n.d.). Retrieved from Informatique Mania: https://www.informatiquemania.com/en/linformatique/inondation-mac/
- Mitigate STP Attacks. (n.d.). Retrieved from CCNA: https://ccna-200-301.online/mitigate-stpattacks/