**Networking Switching and Vlan Concepts**

**Author: Elvis Omorusi**

**Date :15/04/2024**

**Description:**

You have been tasked with designing an Internetwork, which includes three Local Area Network (LAN), for an Irish insurance company. This Internetwork will include a headquarter office and 2 branch offices.

After liaising with the insurance company to define the scope of the network, you will now create a prototype to present to the insurance company. This prototype will be accompanied by an explanation of each network feature and will be used to confirm the requirements of the new network.

**Requirements:**

**Requirement 1:**

* Operations VLAN 10(Prefix Length 25)
* Governance VLAN 20 (Prefix Length 27)

I made the two VLANS 10 and 20 with the respective prefix, prefix 25 can accommodate up to a 128 host, that is more that enough for the 100 users, while the prefix 27 can accommodate up to 30 host yet again, more than enough for the Governance VLAN.

**Requirement 2:**

**I set up the dhcp server in the HQ router, without having the need to use a separate dhcp server to assing the ip address . I tried to implement the dhcp snooping and limit the number of dhcp request each device can request from the server.**

**Requirement 3:**

**Ways I mitigated the attacks.**

.

* MAC Table Attacks: Using the "switchport port-security" command, I set up the switch to automatically secure each port and control aging. By restricting the amount of MAC addresses that are permitted on a port, this command aids in enforcing security by preventing unwanted access
* VLAN Attacks: By decreasing the attack surface and preventing unwanted access, turning off unused ports and manually activating those that are in use improves network security. In addition to optimizing resource allocation, this technique reduces potential hazards and guarantees effective network performance. You can improve network infrastructure security and efficiency by giving priority to connections that are really necessary.
* STP Attacks I used Portfast and BPDU guard to prevent the stp attacks
* DHCP Attacks: for the dhcp attack I tried implementing the dhcp snooping to filter the message and set limits for the untrusted ports. I separated the trusted ports and the untrusted ones.

**Requirement 5:**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

I enabled smooth network connectivity by setting up an IP static route on both routers. I ensured connectivity between various network parts by defining the path that network traffic would take through the configuration of static routes. Pinging successfully between networks was made possible by this configuration, which improved network accessibility and allowed for effective data transmission.

**Conclusion:**

Through the headquarters router, the server assigns DHCP addresses successfully, enabling devices to connect to the network without any problems. One unsatisfied regret, though, is not being able to completely implement attack prevention measures. There can be holes or weaknesses in the network's defenses despite efforts to strengthen security.