Switching and routing essentials project for certification

Loai Ramadan Saadia

Table of Contents

1. Introduction

1.1 Company Background

Microtech Sdn. Bhd., a company that specializes in networking, has every intention of modernizing its information technology services at both its headquarters in Kuala Lumpur and its remote branch in Brunei. The administrator of the network in Brunei came up with a brand new Virtual Local Area Network (VLAN) architecture in order to improve the effectiveness of the network and increase the level of security, notably at the KL headquarters.

In addition, the Management department at headquarters will be responsible for administering the KL Server Farm via remote administration. In addition, the administrator of the network in Brunei has suggested implementing a Wireless Local Area Network (WLAN) Controller (WLC) in order to make the process of configuring the wireless network and controlling access more straightforward.

1.2 Objectives

There are a few goals and objectives in the report that is being presented. Some of them therefore proceed as follows:

• The usage of DHCPv4 to enable user interaction across different LANs on the network.

• Setting up WLC WLAN with a DHCP server, VLAN interface, and WPA2 authentication. • Installing a radius server.

• Setting up static and dynamic routes for IPv4.

• Employing port security to protect Layer 2 devices from assaults.

1.3 Network Topology Diagram

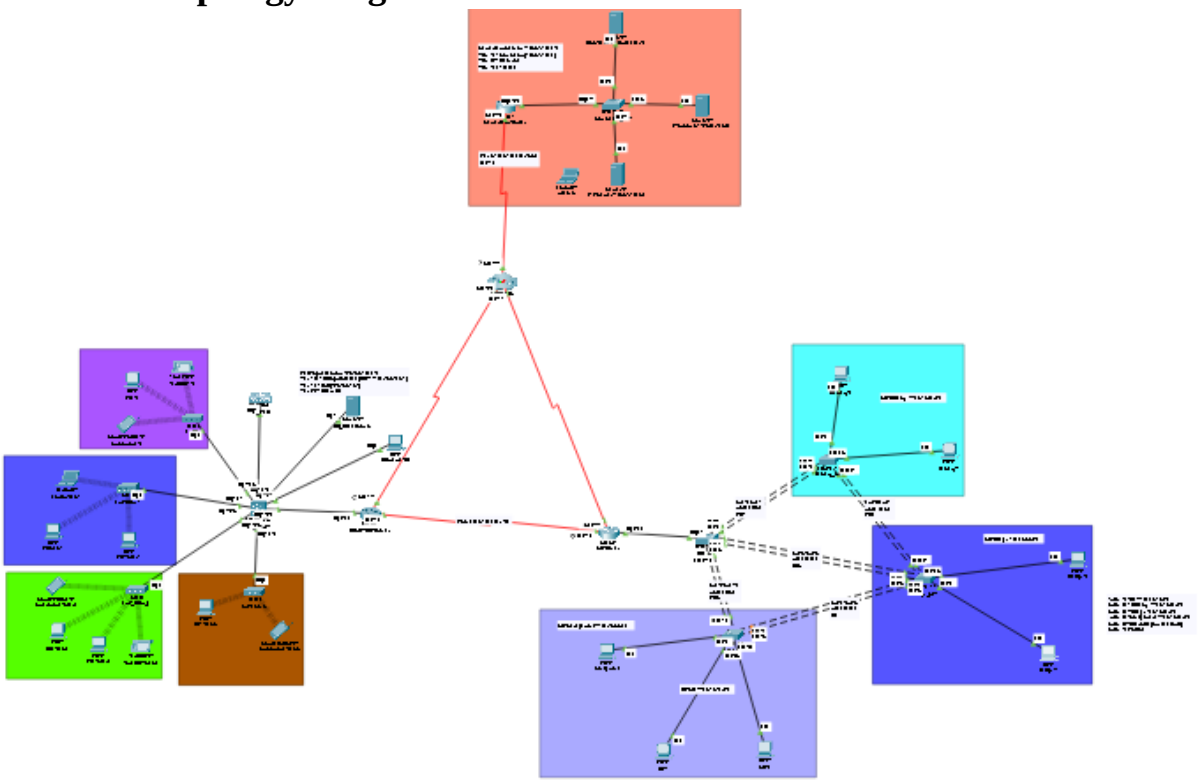


*Figure 1 – Logical Topology for **Microtech Sdn. Bhd***

2. Proposed WLAN Architecture. Explanation and Screenshots of configurations

Microtech, a networking firm, plans to set up a Wireless Local Area Network (WLAN) Controller (WLC) network architecture to improve the current setup at its remote branch in Brunei. As shown in the network diagram, the Brunei office has updated to four (4) Lightweight Access Points (LAPs) and a WLC as part of its network infrastructure.

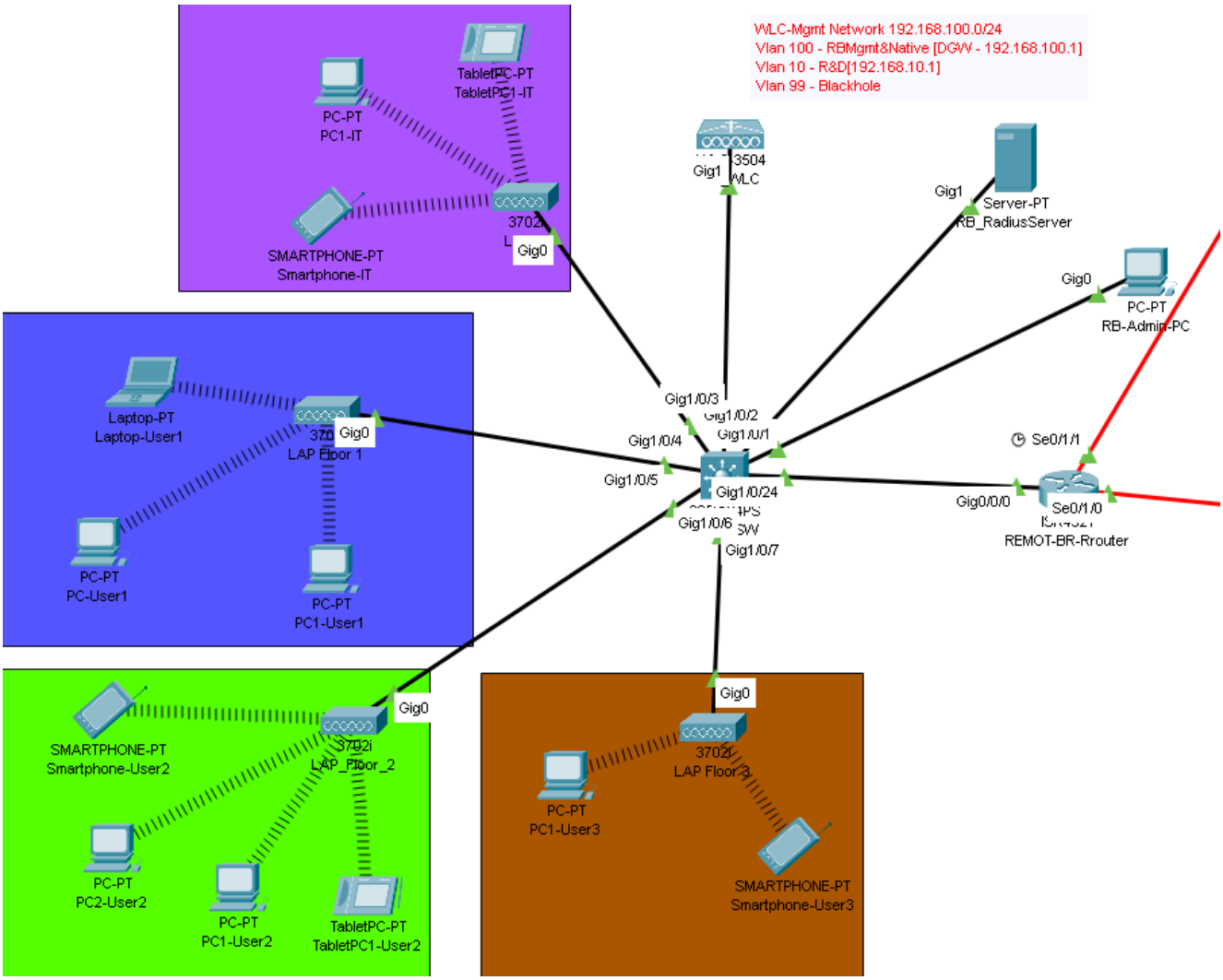


Figure 2 – Brunei Wireless Topology

An administrator PC is required to setup the LAPs across the network in order to deploy the WLC network architecture. Each access point is given an IP address of 192.168.100.0 by the WLC Management Network. The LAPs are each set up differently to suit various wireless end devices and handle 802.11 wireless connections. The "RB-Admin-PC" is shown on the network diagram to denote the administrator's computer.

2.1 Implementation of WLC WLAN

Brunei wants to create a wireless network as a first step. Assigning the administrator workstation, the IP address 192.168.100.2 and default gateway 192.168.100.1 is the first step in connecting it to the Brunei network. The IP address 192.168.100.254 that the Wireless Local Area Network (WLAN) Controller is given will provide access to the WLC registration page and will be discussed in more detail in the following section of the report.

It is advised to start the WLC configuration as soon as the IP assignment is complete. The WLC is completely under the control of the network administrator, who can change security configurations and add new WLANs among other things.

3. Types of security attacks on Layer 2

As technology develops, there are more network vulnerabilities, which leads to a lot of discrepancies. However, many argue that the Data Link Layer (Layer 2) of the Open Systems Interconnection (OSI) model is often overlooked and that higher layers of the OSI model are more important for securing a network and thwarting possible threats. Layer 2 is widely regarded as the weakest link in a system's security, according to several experts. LANs used to be managed by a single entity, which provided trust in all users and devices that were given access.

However, given the present environment with BYOD policies and more sophisticated assaults,

LANs are more vulnerable to intrusions. As a result, it is the duty of network security experts to protect both the Layer 2 LAN infrastructure and the higher Layer 3–7 levels. Understanding Layer 2 infrastructure's inner workings and related vulnerabilities is crucial for reducing assaults against it.

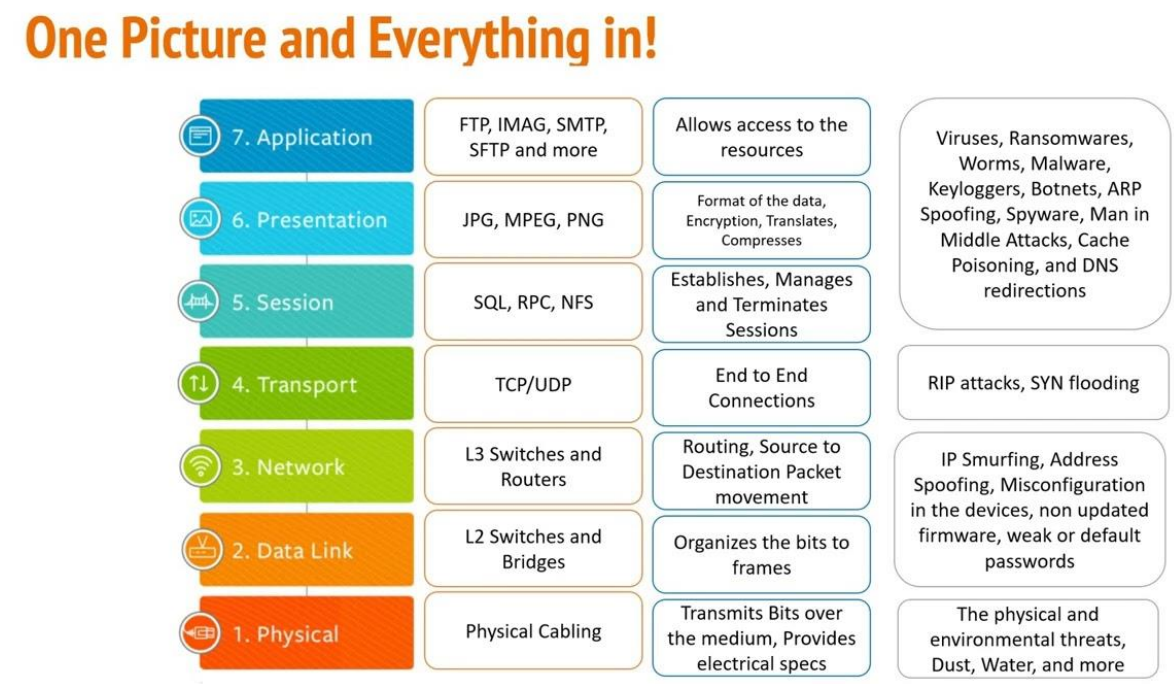


Figure 3 – Functions, Protocols and Cyberattacks examples of OSI layers.

Layer 2 (Data link layer)

The data-link layer is the software layer that is located closest to the hardware (physical layer). As a consequence of this, it incorporates all of the necessary software for running the hardware, among other things. Bridging is also used to connect networks that are connected using different physical layer protocols at this layer (such as an 802.11 LAN and an Ethernet LAN). In a manner analogous to that of physical layer protocols, data-link layer protocols are segmented into local area network (LAN) protocols, wide area network (WAN) protocols, and protocols that can be utilized for both LANs and WANs. Some data-link layer protocols, such as PPP over RS-232 or PPP over Bluetooth's RF-COMM, are able to be ported to very different mediums if there is a layer that simulates the original medium the protocol was intended for or if the protocol supports hardware-independent upper-data-link functionality. Other data-link layer protocols, such as PPP over Bluetooth's COMM, are not able to be ported because there is no layer that can simulate the original On the other hand, data-link layer protocols that are reliant on a particular physical layer may be constrained by the transmission medium in question.

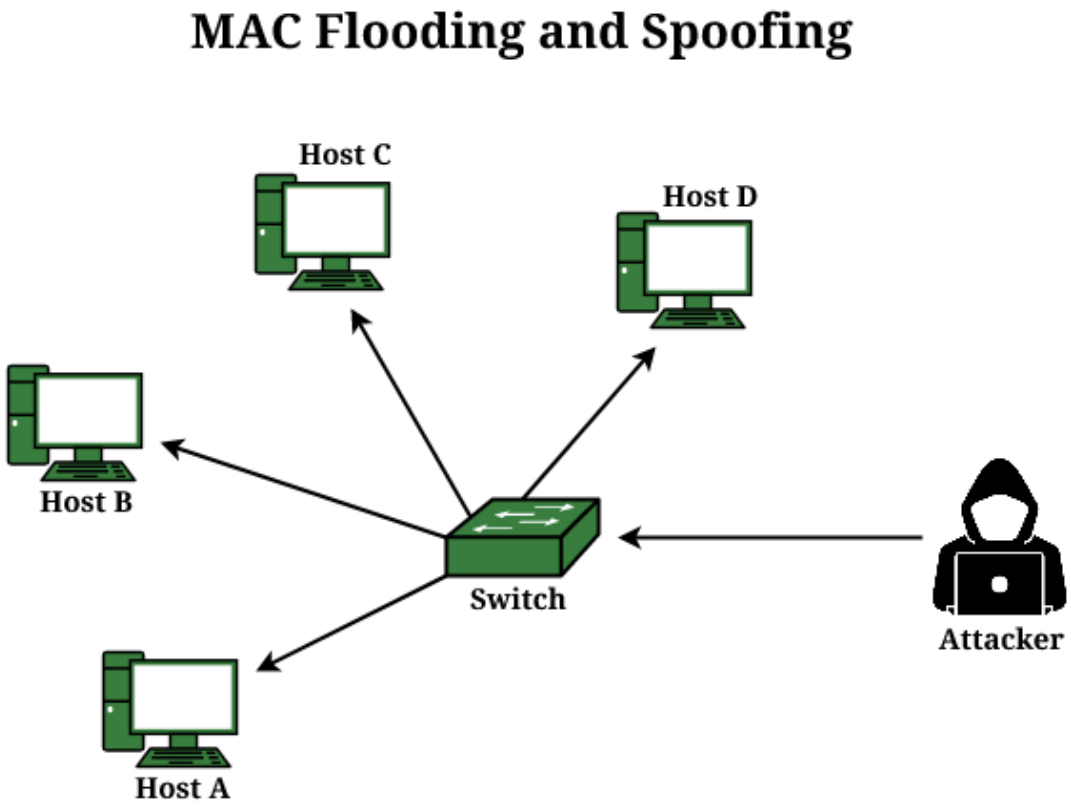
The data-link layer is responsible for receiving data bits from the physical layer and organizing them into groups known as data-link frames. This is done after the data bits have been received from the physical layer. This layer, in general, is responsible for reading the bit fields of these frames to ensure that the frames have been received in their entirety, that there are no errors in the frames, that the frame is intended for this device by using the physical address retrieved from the networking hardware on the device, and that this layer is aware of where the frame originated. Various data-link standards have different data-link frame formats and definitions. If the data is meant for the device, the data-link layer headers are stripped from the frame, and only the remaining data field is transmitted. It

is sent in the form of a datagram all the way up to the networking layer. Before sending the complete data-link frame on to the physical layer to be sent, the data-link layer appends these and other similar header fields to the data that is brought down from upper tiers.

3.1 Mac Address Flooding

The goal of the MAC Flooding attack plan is to compromise the security of the network switches. Switches typically maintain a table structure known as the MAC Table. The network's host machines' distinctive MAC addresses that are connected to switch ports are listed in this MAC Table. With this table, the switches may now direct data leaving the ports to the intended recipients. As already demonstrated, whereas hubs broadcast data to the whole network, enabling the data to reach all hosts on the network, switches deliver data to the precise computer or machines that the data is intended to be sent to. To do this, MAC tables are employed. This MAC Table is intended to be destroyed by the MAC Flooding. The attacker sends a lot of Ethernet frames in a typical MAC Flooding assault.

Each Ethernet frame that is transmitted to the switch will have a different sender address. The switch's memory, which houses the MAC address database, is the target of the attacker. The MAC addresses of authorized users will be removed from the MAC Table. The incoming data can no longer be sent by the switch to the desired system. As a result, a significant number of incoming frames will cause all ports to become overloaded.



Since the MAC Address Database is already full, no more MAC addresses may be added. The switch will enter fail-open mode as a result, and from that point on, operate exactly like a network hub. The incoming data will be broadcast to all open ports. Let's look at the MAC Flooding attack's benefits for the attacker.

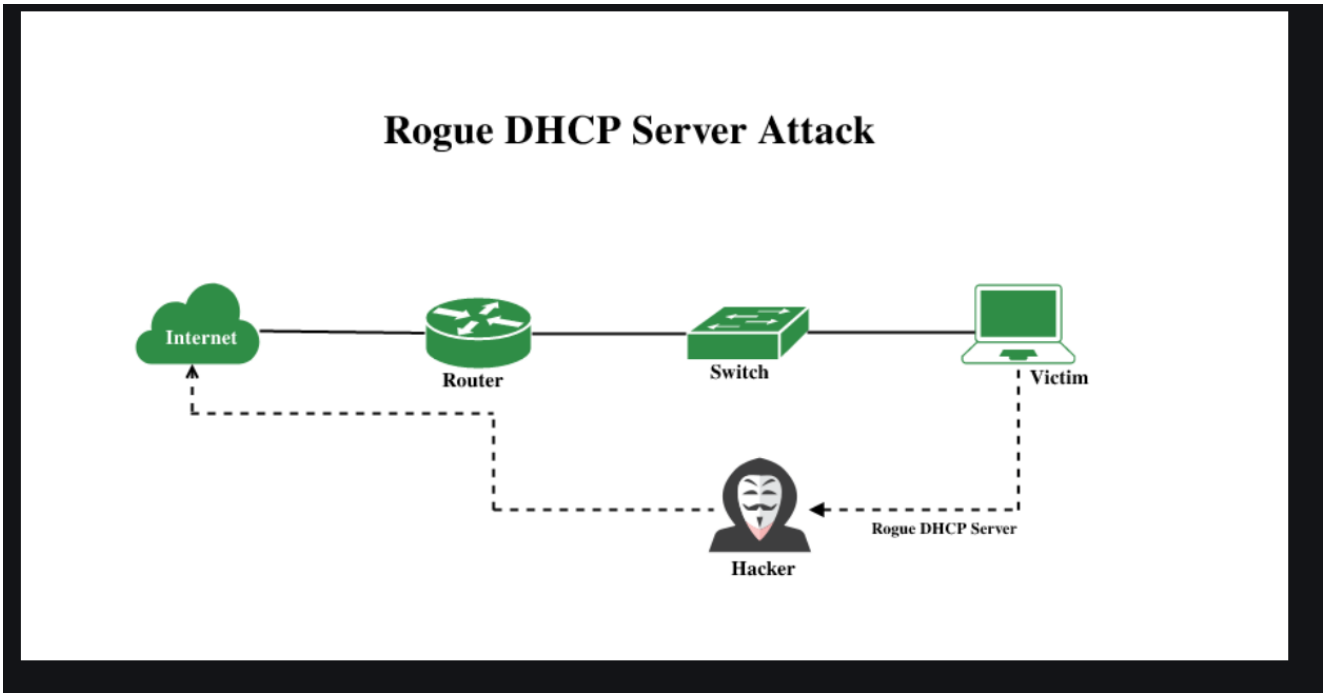
The data packets meant for the victim PC would also reach the attacker as they are both connected to the network. so that the attacker will be able to steal private information from the victim's

and other machines' communications. Generally, these sensitive data are captured using a packet analyzer.

3.2 Rogue DHCP Server

Attacks on rogue DHCP servers are on the rise, but they may be stopped. By broadcasting a duplicate IP address, the hacker sets up a rogue DHCP server and causes an IP address conflict. In order to insert rogue packets into the data stream being processed by the router, hackers attack the wireless router, which they do using ARP poisoning. With the help of spam mailers and proxy servers, this clever breach allows criminals constant access to networks, making it challenging for IT specialists to prevent or even identify a cyber-attack. The hacker then keeps an eye out for incoming connections and selectively responds with harmful messages like viruses that wreak havoc on the machines of unwary users or phoney authentication requests.

By broadcasting a duplicate IP address, the hacker configures a malicious DHCP server and causes a conflict over IP addresses. Hackers break into a network by assaulting the wireless router, which they do using ARP poisoning to introduce rogue packets into the data stream that the router is processing. It is challenging for IT specialists to prevent or even identify a cyber-attack because of this clever breach, which grants hackers constant access to networks via proxy servers and spam mailers. After that, the hacker waits for incoming connections and selectively responds with harmful messages, such as bogus authentication requests or viruses that wreak havoc on the devices of unwary victims.



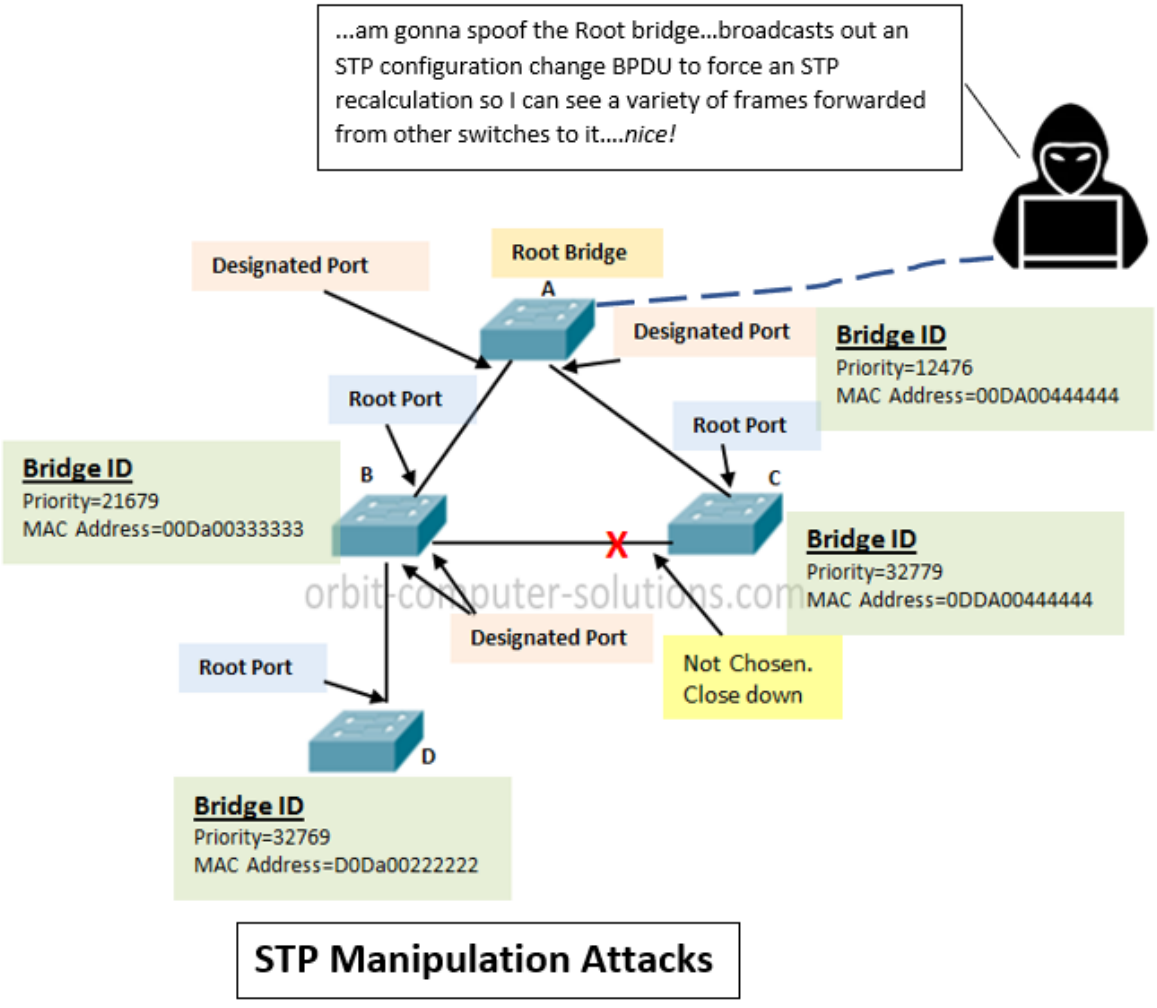
Attacks on rogue DHCP servers are on the rise, but they may be stopped. By broadcasting a duplicate IP address, the hacker sets up a rogue DHCP server and causes an IP address conflict. Then, instead of using the router, the hacker will attempt to convince machines to connect to the rogue device. After that is done, the hacker is essentially free to do whatever he wants, from stealing data to infecting your computer with harmful software so that he can remotely manage it. A recent press briefing featured a government official who said that Iran had installed phoney wireless networks in

nations like Iraq and Afghanistan so they could easily monitor conversations while individuals were utilizing Wi-Fi hotspots.

3.3 STP manipulation

An adversary can infiltrate a network with a rogue switch if they have access to switch ports that can also function as trunk ports. Keep in mind that the "dynamic desired" mode is the default setting for all of the ports on Cisco switches. This indicates that if the ports are still in that mode, an attacker can attach a rogue switch to the network wall jack in his cubicle, and the switch will negotiate a trunk link with another switch in the firm.

At that time, he has the opportunity to establish a second connection to the second switch belonging to that company, after which he will have the ability to control the rogue switch's spanning tree priority. If he configures his rogue switch to have a lower priority than any other switch in the organization, then in theory the majority of the company's traffic will go through that switch.



STP Manipulation Attacks

Rogue switch with, for example, priority 0 broadcasts its "superior BPDUs," causing the STP topology to convert again. His rogue switch will eventually become the root bridge, and all traffic will be routed through this switch. This provides him with the opportunity to monitor all communications within the organization.

Additionally, it will reroute traffic from links between other switches that have a high bandwidth to a link that has 100 Mbps on the rogue switch. Because of this, the speed of the network will be considerably impacted.

4. Layer 2 Security Deployment to mitigate the Attacks

4.1Mitigate mac address flooding.

By applying these mechanisms, you can mitigate mac address flooding.

1. Port security:

   As a common defensive mechanism against MAC Flooding attacks, port security is frequently employed. The number of MAC addresses that can be learned on ports that are connected to end stations is restricted by the configuration of the switches in the network. Together with the conventional MAC address database, there is additionally a compact table with safe MAC addresses that is kept. In addition to that, the MAC address table utilizes this table as a subset. Cisco switches can be purchased with a port security system already installed inside of them.
2. Authentication with AAA server:

   Following the discovery of MAC addresses, these addresses are first subjected to validation against an authentication, authorization, and accounting server (AAA Server), and then the addresses are filtered according to their results.
3. Implement IEEE 802.1X suites:

   Implementing IEEE 802.1X suites will make it possible for a AAA server to explicitly install packet filtering rules based on information dynamically acquired about clients, including the MAC address. This will allow packet filtering rules to be more efficient.

4.2 Mitigate Rogue DHCP Server:

By applying these mechanisms, you can mitigate Rough DHCP Server.

1. Activate the DHCP Snooping Feature:

   The DHCP snooping feature is a function that may be enabled on network switches to stop malicious DHCP servers from connecting to the network. In order for it to function properly, it restricts the distribution of IP addresses to clients to approved DHCP servers only and blocks traffic coming from untrusted sources.
2. Disable unused switch ports:

   Because rogue DHCP servers can be linked to unused switch ports, it is imperative that you disable any unused switch ports that are present on your network in order to prevent unauthorized access.

4.3 Mitigate STP manipulation:

1. Use Port Security:

   Applying port security is one method that can assist in preventing unauthorized devices from gaining access to a network. This can be accomplished by configuring each port to only allow traffic from a certain MAC address or VLAN. However, this can also be done by hand.

2. Use BPDU Guard:

   Turning on BPDU guard on all of the ports in your computer can assist prevent malicious switches from connecting to your network. When it detects that a BPDU message has been sent from an unauthorized switch, BPDU guard will immediately disable the port in question.

5. Conclusion

In a nutshell, all of the necessary needs have been accounted for in the development of the prototype network that Microtech Sdn. Bhd has created. This requires taking into consideration the entirety of the WLAN architecture and putting into action various mitigation strategies. Some examples of these include the utilization of a firewall, the security of ports, the IEEE 802.1X protocols, static ARP mapping, physical security measures, and network segmentation. Attacks on Layer 2 require these preventative measures to be successful.

However, despite the availability of these security procedures, Layer 2 may still be susceptible to cyberattacks; this fact must be brought to the attention of readers. The likelihood of such assaults can be lessened if the configuration settings for these security measures are adjusted appropriately.

1. References

geeksforgeeks. (2022). *What is Rogue DHCP Server Attack?* Retrieved March 5, 2023, from GeeksForGeeks: https://www.geeksforgeeks.org/what-is-rogue-dhcp-server-attack/

Jithin. (2016). *What is MAC Flooding? How to prevent it?* Retrieved March 5, 2023, from interServer: https://www.interserver.net/tips/kb/mac-flooding-prevent/

orbitco. (2020). *Network Security – STP Manipulation Attacks*. Retrieved March 5, 2023, from Orbit-Computer-Solutions.

Popeskic, V. (2023). *STP Layer 2 attack – Manipulating Spanning Tree Protocol settings*. Retrieved March 5, 2023, from HOW DOES INTERNET WORK: https://howdoesinternetwork.com/2012/stp-attack