A picture containing text, graphics, graphic design, font

Description automatically generated

**SWITCHING AND ROUTING ESSENTIALS**

**GROUP ASSIGNMENT**

**TECHNOLOGY PARK MALAYSIA**

**CT133-3-2-SRE**

**INTAKE CODE**: APD2F2309CS(CYB)

**LECTURER**: NORIS ISMAIL

**HAND OUT DATE:** WEEK 3

**HAND IN DATE(s):** WEEK 13

**MEMBERS:**

|  |  |
| --- | --- |
| **Name** | **TP Number** |
| **ABDUL SHAFEY KHAN** | **TP071166** |
| **ABDULELAH HUSSEIN ABDULRAHMAN AL-KAF** | **TP069319** |
| **AMANULLAH GHAURI** | **TP071215** |
| **IBRAHEEM MOHAMMED IMADELDIN AWAD** | **TP070765** |
| **ABDULRAHMAN GAMIL MOHAMMED AHMED** | **TP071012** |

**Table of Contents**

[**1. Introduction** 4](#_Toc153748300)

[**2. Network Layout** 5](#_Toc153748301)

[**3. IPv4 Addressing Scheme** 6](#_Toc153748302)

[**4. LAN and Wan Configuration** 7](#_Toc153748303)

[**4.1 VLAN Configuration** 7](#_Toc153748304)

[**4.2 Inter-VLAN Configuration** 10](#_Toc153748305)

[**4.3 WAN Configuration** 10](#_Toc153748306)

[**5. Proposed WLAN Architecture** 11](#_Toc153748307)

[**5.1 WLC Configuration** 13](#_Toc153748308)

[**5.1.1 IP Address Configuration of the KT-Admin PC and Wireless LAN Controller (WLC)** 13](#_Toc153748309)

[**5.1.2 Admin Account Configuration on the WLC** 16](#_Toc153748310)

[**5.1.3 Configuration of WLC** 17](#_Toc153748311)

[**5.1.4 Wireless LAN Controller Access and Login Procedure** 18](#_Toc153748312)

[**5.1.5 Configuration of the RADIUS Authentication Servers** 20](#_Toc153748313)

[**5.1.6 Wireless Network Customization and Configuration** 21](#_Toc153748314)

[**6. EtherChannel Implementation** 31](#_Toc153748315)

[**6.1 EtherChannel Configuration** 32](#_Toc153748316)

[**7. HSRP implementation** 34](#_Toc153748317)

[**7.1 HSRP Configuration** 35](#_Toc153748318)

[**8. Server Farm Configuration** 37](#_Toc153748319)

[**8.1 VLANs Configuration in Server Farm** 37](#_Toc153748320)

[**8.2 DNS Server Configuration** 38](#_Toc153748321)

[**8.3 Web Server Configuration** 39](#_Toc153748322)

[**8.4 FTP Configuration** 40](#_Toc153748323)

[**9. Network Interconnection Verification: Tracert and Ping Commands** 41](#_Toc153748324)

[**9.1 Verifying Network Connectivity: Example 1** 41](#_Toc153748325)

[**9.2 Verifying Network Connectivity: Example 2** 42](#_Toc153748326)

[**9.3 Verifying Network Connectivity: Example 3** 43](#_Toc153748327)

[**10.1 Configuring Fundamental Security Mechanisms** 44](#_Toc153748328)

[**11. Recommendations for Additional Security Measures** 46](#_Toc153748329)

[**11.1 Recommendation #1: Access Control Lists (ACLs)** 46](#_Toc153748330)

[**11.2 Recommendation #2: Virtual Private Networks (VPNs)** 47](#_Toc153748331)

[**11.3 Recommendation #3: Secure Sockets Layer (SSL)/Transport Layer Security(TLS)** 48](#_Toc153748332)

[**12. Conclusion** 49](#_Toc153748333)

[**13. References** 50](#_Toc153748334)

**Table of Figures**

[**Figure 1: Network Layout** 5](#_Toc153749177)

[**Figure 2: IP Addressing of KL Network** 6](#_Toc153749178)

[**Figure 3: IP Addressing of Server Farm Network** 6](#_Toc153749179)

[**Figure 4: Wan Connections** 6](#_Toc153749180)

[**Figure 5: Wan Connections** 6](#_Toc153749181)

[**Figure 6: VLAN Implementation** 8](#_Toc153749182)

[**Figure 7: VLAN Implementation** 8](#_Toc153749183)

[**Figure 8: VLAN Implementation** 9](#_Toc153749184)

[**Figure 9: OSPF Routing Information with Gateway Distances** 10](#_Toc153749185)

[**Figure 23: WLAN Configuration of F3 group** 26](#_Toc153749186)

[**Figure 27:26 : Configured WLAN IDs** 30](#_Toc153749187)

[**Figure 36: Configuration of Web Server** 39](#_Toc153749188)

[**Figure 37: Configuration of FTP Server** 40](#_Toc153749189)

[**Figure 38: Successfully pings from KT** 41](#_Toc153749190)

[**Figure 39: Successfully pings from ServerFarm section** 41](#_Toc153749191)

[**Figure 40: Successfully pings from HQ** 41](#_Toc153749192)

[**Figure 41: Successful Ping Displayed** 42](#_Toc153749193)

[**Figure 42: Successful Ping Displayed** 43](#_Toc153749194)

[**Figure : Securing Unused Ports and Implementation of Blackhole** 44](#_Toc153749195)

[**Figure 44: Implemented Port Security** 45](#_Toc153749196)

[**Figure 45: Example Implementation of ACL** (PyNet Labs, 2023) 46](#_Toc153749197)

[**Figure 46: Example Implementation of VPN** (Security Wing, 2014) 47](#_Toc153749198)

[**Figure 47: Example Implementation of SSL/TLS** (Java Point, 2021) 48](#_Toc153749199)

# **1. Introduction**

Renowned networking business Microtech Sdn. Bhd. plans to upgrade its IT services for its current locations in Kuala Lumpur (HQ) and Krung Thep (Remote Branch). The network administrator at Krung Thep sees an evolution in network design, with a focus on increasing efficiency and security. As part of this strategic drive, the administrator intends to replace the present network configuration with a new VLAN architecture, with a focus on reinforcing the security infrastructure, especially at the Kuala Lumpur (HQ) branch.

Acknowledging the shifting demands of the contemporary workplace and the rising relevance of wireless connection, the Krung Thep network administrator proposes the implementation of Wireless LAN Controller (WLC) WLAN in the Krung Thep network. This initiative attempts to simplify wireless network setup and improve access management.

Microtech Sdn. Bhd. contains numerous departments scattered across multiple sites, such as Management, Human Resource (HR), Design, and Delivery, all of which are located at the KL site. Furthermore, departments such as R&D, WLC Management, and Server Farm are strategically positioned at the Krung Thep location, adding to the overall functioning and efficiency of Microtech's network infrastructure.

Cisco is the leading simulation tool for design and execution to enable this network transition, guaranteeing a resilient and dependable network architecture aligned with industry standards and best practices (Cisco, 2023). The following sections will go into further depth about the setup and implementation stages, providing insight into the methodical deployment of VLANs and WLC WLAN to optimise Microtech's network for future scalability and technological improvements.

# **2. Network Layout**

A diagram of a network

Description automatically generated

**Figure 1: Network Layout**

# **3. IPv4 Addressing Scheme**

A screenshot of a computer screen

Description automatically generated

**Figure 2: IP Addressing of KL Network**

A screenshot of a computer screen

Description automatically generated

**Figure 3: IP Addressing of Server Farm Network**

A screenshot of a computer screen

Description automatically generated

**Figure 4: Wan Connections**

A screenshot of a computer screen

Description automatically generated

**Figure 5: Wan Connections**

# **4.** **LAN and Wan Configuration**

Microtech Sdn. Bhd. understands the importance of network setup in encouraging effective communication and improving connection throughout the workplace. Local Area Networks (LANs) are the foundation of internal communication inside physical places such as the Headquarters (KL Site) and the Krung Thep (Remote Branch). These LANs provide fast data transmission, smooth collaboration, and resource sharing among devices in a limited geographical region.

Wide Area Networks (WANs), on the other hand, address a larger range of communication and data sharing. WANs are critical channels that link geographically scattered facilities like the KL Site and the Krung Thep Site in the context of Microtech's network architecture. WANs are critical for enabling dependable, secure, and high-performance communication across these distant sites, bypassing geographical barriers, and building an integrated organisational network.

## **4.1** **VLAN Configuration**

A virtual local area network (VLAN) is a logical segment of a network that enables devices to be segregated into discrete broadcast zones. Using departmental or functional groups, VLANs enhance the effectiveness and security of networks. Devices within the same VLAN can communicate directly with one another, while connections across VLANs require routing. VLANs help manage network traffic, improve performance, and make administration easier. By preventing unnecessary broadcast traffic and enhancing overall network administration, this segmentation contributes to the organisation and security of large or heterogeneous networks.

A screenshot of a computer

Description automatically generated

**Figure 6: VLAN Implementation**

A screenshot of a computer

Description automatically generated

**Figure 7: VLAN Implementation**

A screenshot of a computer

Description automatically generated

**Figure 8: VLAN Implementation**

In the KL branch, VLANs are intentionally constructed to enhance network performance. VLAN10, "Design," is dedicated to duties pertaining to design, whereas VLAN20, "Delivery," is dedicated to operations associated with delivery. While VLAN30, "Management," is utilised for administrative work, VLAN40, "HR," is dedicated to human resources-related operations. Unwanted traffic vanishes into VLAN100, whereas the original VLAN is VLAN99.

While VLAN60, "ServerFarm," is tasked with handling server-related activities in the Server Farm, VLAN50, "SF-Management," is in charge of overseeing the server farm. Again, both VLANs share the original VLAN99, and VLAN100 serves as a black hole for unwanted traffic.

VLAN99 is the native VLAN for routers, whereas VLAN100 acts as a black hole. While VLAN70, "R&D - Wireless," is meant for wireless research and development, VLAN80, "RBMgmt," is meant for router administration. This VLAN setup enhances network organisation and security in the KL branch.

## **4.2 Inter-VLAN Configuration**

Inter-VLAN, or communication between several Virtual Local Area Networks (VLANs), is necessary for network segmentation. Routing is required for communication between distinct VLANs; however it is simple to communicate between devices in the same VLAN. Common approaches include router sub interfaces, Layer 3 switches, and router-on-a-stick systems. These methods, which assign IP addresses to VLAN ports, enable efficient data exchange across VLANs. The optimal course of action is determined by the needs and network architecture. Inter-VLAN routing optimises network structure and enhances resource management and security under various conditions.

To promote efficient communication, VLANs including Design, Delivery, Management, HR, and supporting VLANs 99 and 100 are deployed strategically in the KL branch. The Server Farm shares a native VLAN 99 using VLANs 50 and 60 and use VLAN 100 as a BlackHole to filter out unwanted traffic. R&D Wireless and RBMgmt routers use VLANs 70 and 80. Inter-VLAN routing solutions, such Layer 3 switches or router subinterfaces, enhance network organisation and security by enabling seamless communication across various VLANs in a straightforward and efficient manner.

## **4.3 WAN Configuration**

**A screenshot of a computer program

Description automatically generated**

**Figure 9: OSPF Routing Information with Gateway Distances**

The router 'KL\_ROUTER' in our WAN setup is using the OSPF (Open Shortest Path First) routing protocol, which is denoted by the routing protocol number 'ospf 1'. The router's IP address is '8.8.8.8'. The OSPF setup indicates the existence of one area, designated as a normal area (area 0), as well as information on the networks being routed. This router, in particular, keeps routing information from numerous gateways, each with a radius of 110.

# **5. Proposed WLAN Architecture**

With the dynamics of the workplace changing and the Bring-Your-Own-Device (BYOD) trend becoming more popular, Microtech Sdn. Bhd. has the opportunity to deploy a Wireless Local Area Network (WLAN) architecture at its offices in Krung Thep (Remote Branch).

The initiative is motivated by the need to guarantee a dynamic and productive work environment by giving personnel easy access to their own devices. With personal devices like laptops, tablets, and mobile devices becoming crucial for day-to-day work, an infrastructure that is wired exclusively would be restrictive. As a result, the Wireless Local Area Network (WLAN) architecture is intended to provide personnel with the ability to interact with the network and corporate resources from any place within the service region (Kristián Košťál et al., 2019).

However, leveraging WLAN's convenience demands a strategic approach. Although technology opens new avenues for mobility and cooperation, network administrators are required to be on alert for security risks (Ali et al., 2019). For this purpose, specific devices known as modern Access Points (APs) must be implemented within the network . These devices provide strong integrated security features, such as website access limitations, while facilitating continuous connections. These safety measures work as a barrier, protecting the company from any risks that may arise from its online operations (Secure IT Store, 2022).

Furthermore, the integration of Wireless LAN Controllers (WLCs) is an essential requirement for guaranteeing the consistent and compatible setup of all APs. This addition ensures consistency across the company network by removing the repetitive manual setup process for every AP. The incorporation of WLC goes beyond configuration management and creates an effective architecture that prioritises strong user-side security measures and improves AP security (Froehlich, 2018).

To further strengthen the network infrastructure, Remote Authentication Dial-in User Service (RADIUS) server is also incorporated into the Krung Thep network. This dedicated server stands between the employees and network and acts as the main barrier against unwanted access by thoroughly confirming user credentials against a safe database (IBM, 2023). Additionally, a RADIUS server is also included in the proposed WLAN to implement enterprise-grade authentication via the use of Wireless Protected Access 2 (WPA2). WPA2, an industry-standard protocol, adds another layer of protection to wireless communications against unauthorised access (Hoch Dirraneh & Zhou, 2007).

The Krung Thep network's architecture includes a planned distribution of resources throughout the floors to provide the most effective wireless coverage. To be more precise, every level has four Lightweight Access Points (LAPs) installed to support a variety of end devices, such as smartphones, tablets, PCs, and laptops, via wireless connectivity. A router for effective packet routing to external networks, a multilayer switch for network management, a Wireless LAN Controller (WLC), a RADIUS server, an administrative PC for configuring LAPs and the RADIUS server, and other crucial parts are also deliberately placed . This comprehensive design provides a solid basis for effective network administration inside the Krung Thep network in addition to facilitating smooth wireless access (Ali et al., 2020). The topology can be observed as follows.

A diagram of a network

Description automatically generated

**Figure 10: Proposed Topology of WLAN Architecture for Krung Thep (Remote Branch)**

## **5.1 WLC Configuration**

### **5.1.1 IP Address Configuration of the KT-Admin PC and Wireless LAN Controller (WLC)**

The Wireless LAN Controller (WLC) is configured by accessing its web management interface via an external device's web browser. In this case, KT-Admin-PC acts as the WLC's configuration hub. The KT-Admin-PC  must be configured before the WLC configuration can begin, including the allocation of an Internet Protocol (IP) address. Additionally, the WLC must be set to be part of the same network as the KT-Admin-PC.

The KT-Admin-PC, a desktop device, is statically allocated the IP address 172.16.75.66 with a subnet mask prefix of /27 in this configuration. While KT-WLC is assigned the IP address 172.16.75.62, as well as a subnet mask prefix of /26.

A screenshot of a computer

Description automatically generated

**Figure 11: IP Configuration of KT-Admin-PC**

A screenshot of a computer

Description automatically generated

**Figure 12: IP Configuration of KT-WLC**

### **5.1.2 Admin Account Configuration on the WLC**

The creation of a dedicated admin account on the WLC is an important step in the configuration procedure. This administrator account serves as the gateway to the WLC's management interface, allowing authorised workers to setup and maintain the WLAN infrastructure. This operation is performed by accessing by using a web browser to visit the WLC's web management interface at https://172.16.75.62, which is the IP address of the WLC, as illustrated in the following.

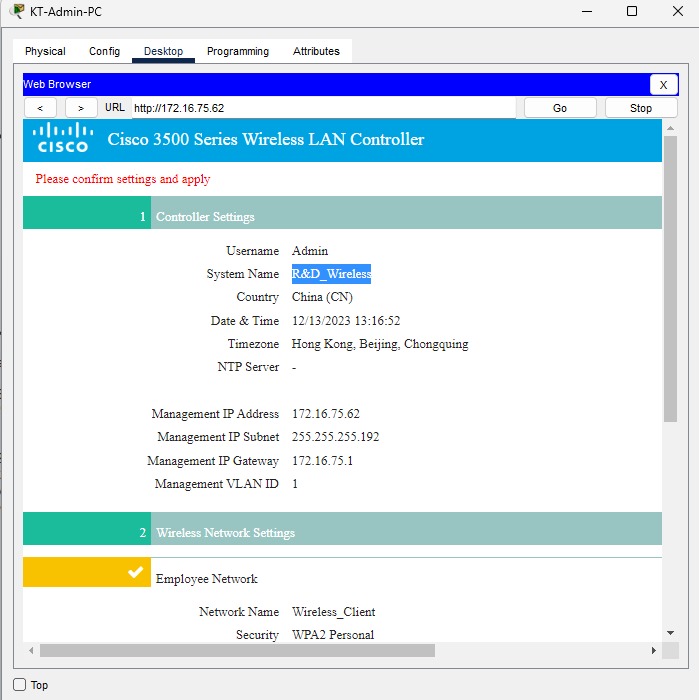
A login screen with a blue background

Description automatically generated

**Figure 13: Creating an Admin Account on the Wireless LAN Controller (WLC)**

### **5.1.3 Configuration of WLC**

The process of configuring the Wireless LAN Controller (WLC) includes modifying key initial settings necessary for smooth network operations. This information includes the System Name, Management IP address, Subnet Mask, and Default Gateway . These attributes serve as the WLC's identification, establishing its position inside the network and allowing connection with other network components. In network synchronisation and coordination, precise timezone and date-time information is important.



**Figure 14: Configuration of the Controller**

### **5.1.4 Wireless LAN Controller Access and Login Procedure**

After successfully configuring the Wireless LAN (WLAN), users must enter the admin web browser to complete further setup procedures. This is conducted by navigating to the desktop and inputting the URL https://172.16.75.62, which will start the re-entry into the network administration interface.

**Figure 15:Re-accessing the Wireless LAN Controller (WLC)**

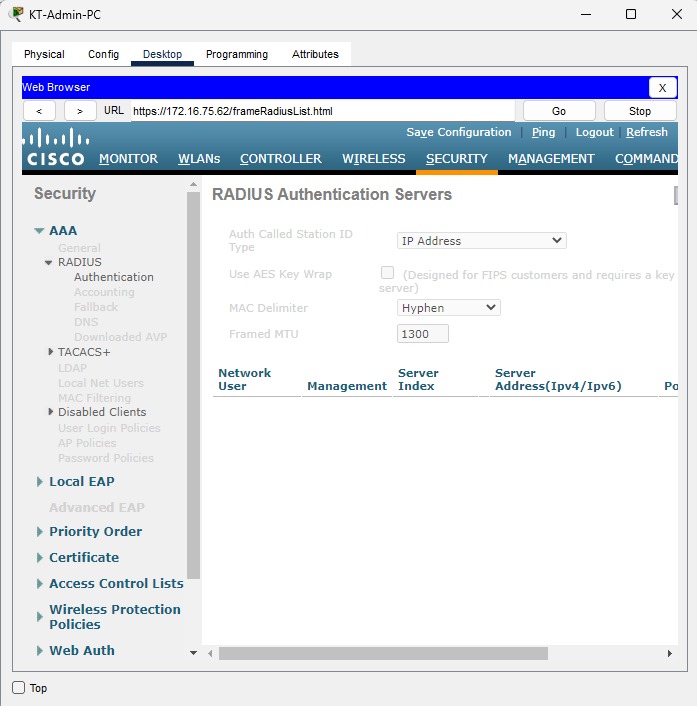
After selecting "login," a new menu prompts users to enter the previously established username and password. In this instance, the username is configured as "Admin," and the corresponding password is also set as "Admin" during the earlier configuration steps. This login authentication ensures secure access to the WLC settings and adheres to established network security protocols.



**Figure 16: User Authentication Menu**

### **5.1.5 Configuration of the RADIUS Authentication Servers**

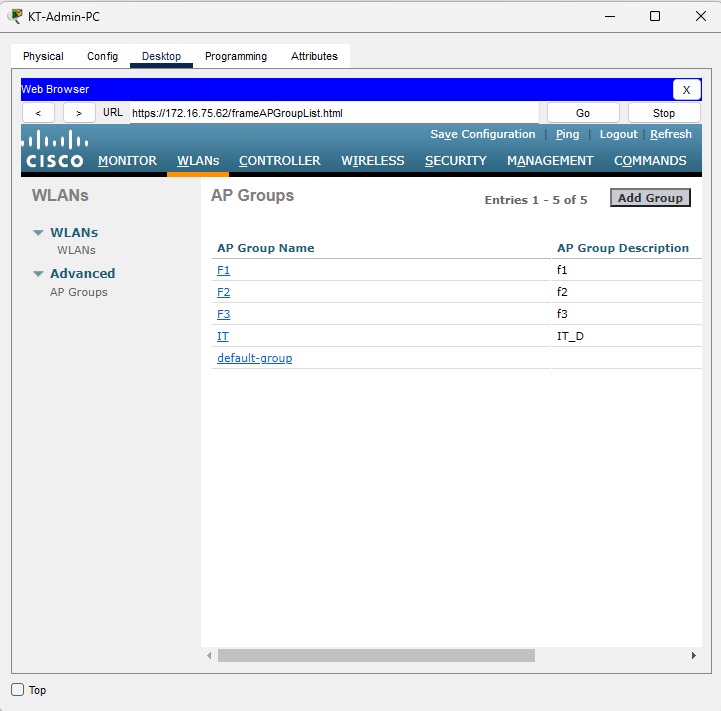
In the subsequent stage, navigating to the SECURITY section of the WLC interface and setting RADIUS Authentication Servers is a critical step for improving network security and user access management. The RADIUS (Remote Authentication Dial-In User Service) protocol acts as a rigorous authentication method, enabling the WLC to check the identity of users seeking to access the wireless network. The server IP acts as the specified point of authentication. This IP is the point where user credentials are validated before granting access to the wireless network.



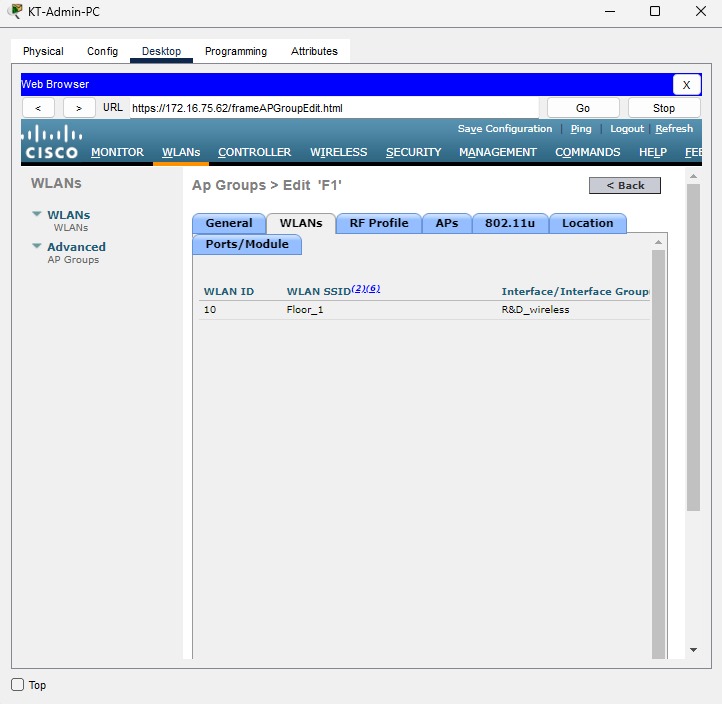
**Figure 17: Configuration of RADIUS server**

### **5.1.6 Wireless Network Customization and Configuration**

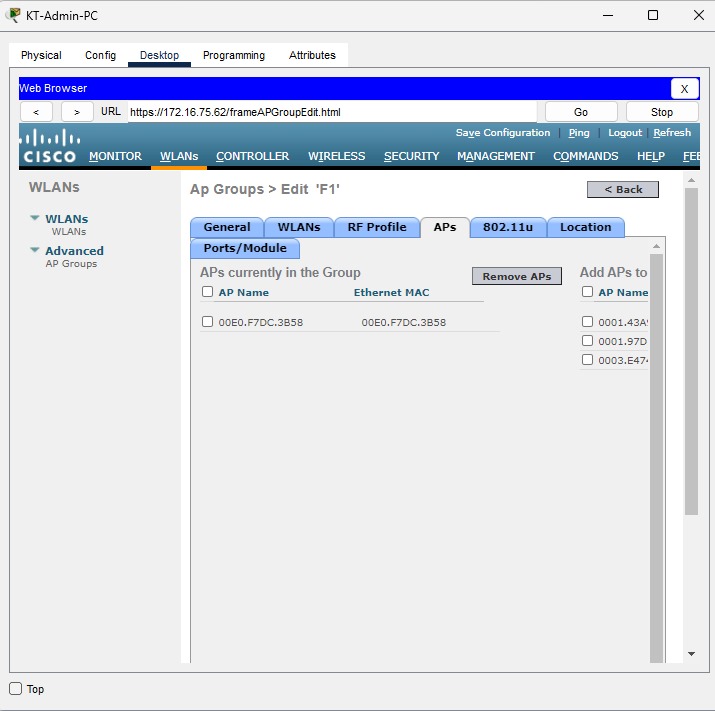
Creating a WLAN configuration is a critical step in building a reliable and effective wireless network. This procedure involves going to the WLANs tab and managing and configuring numerous AP groups. In the Wireless Local Area Network (WLAN), access point (AP) groups play a critical role in effectively managing and organising the deployment of wireless access points inside a network. The following illustrates the main AP groups created for Krung Thep along with detailed configuration for each Group.



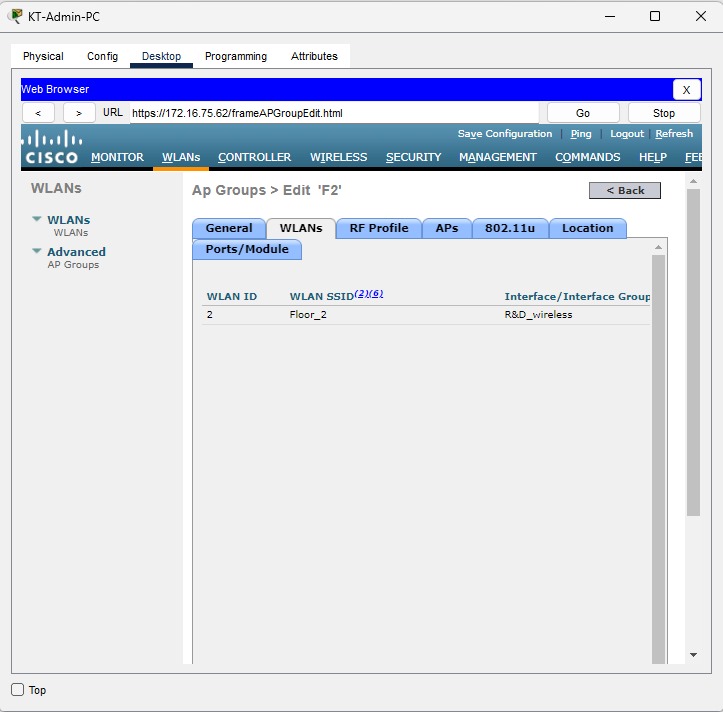
**Figure 18: Configured AP Groups**



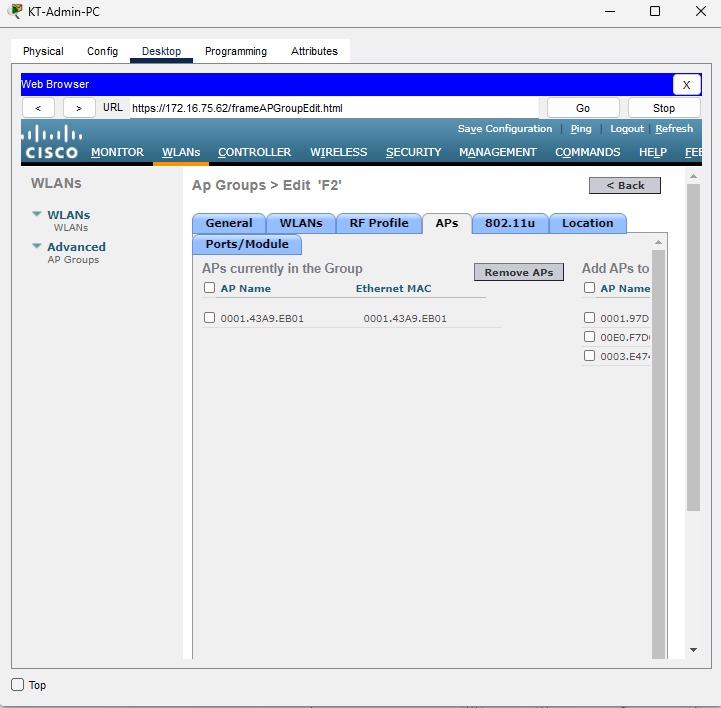
**Figure 19: WLAN Configuration of F1 group**



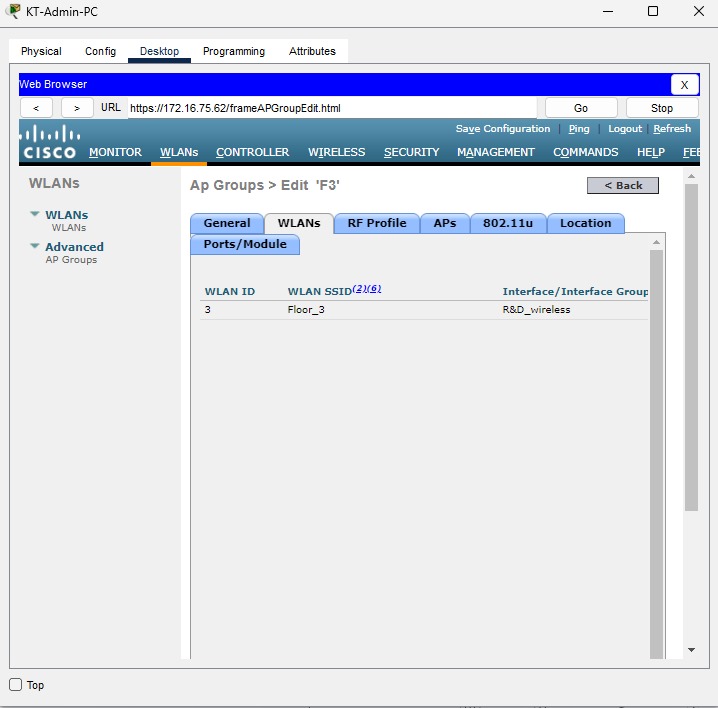
**Figure 20: Configured F1 Access Port**



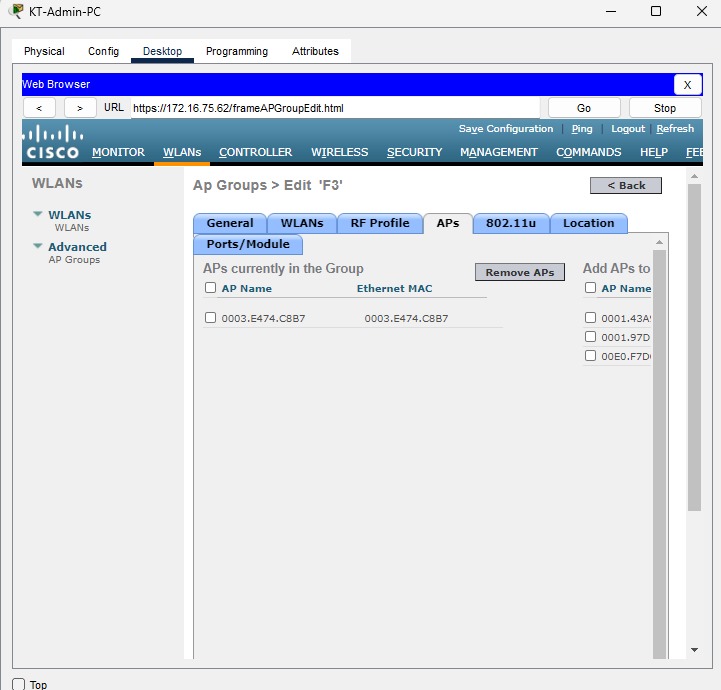
**Figure 21: WLAN Configuration of F2 group**



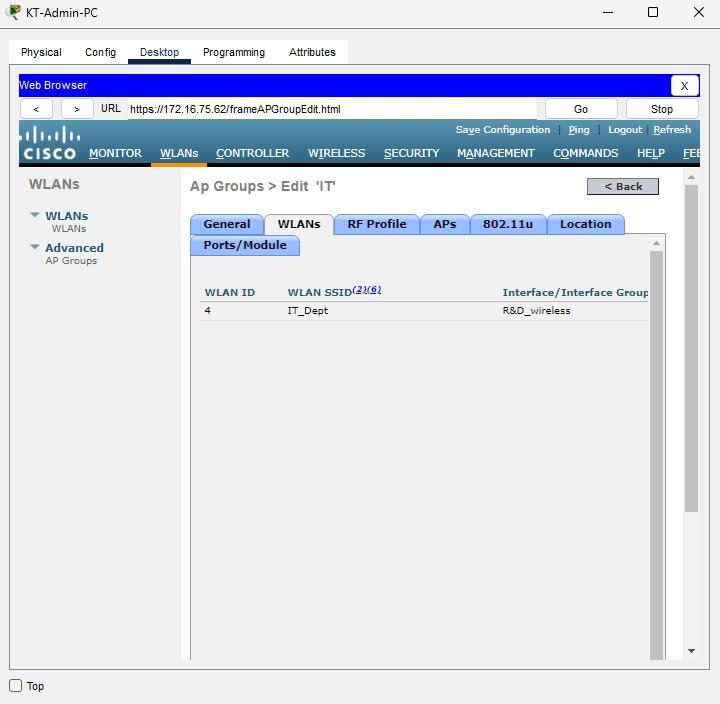
**Figure 22: Configured F2 Access Port**



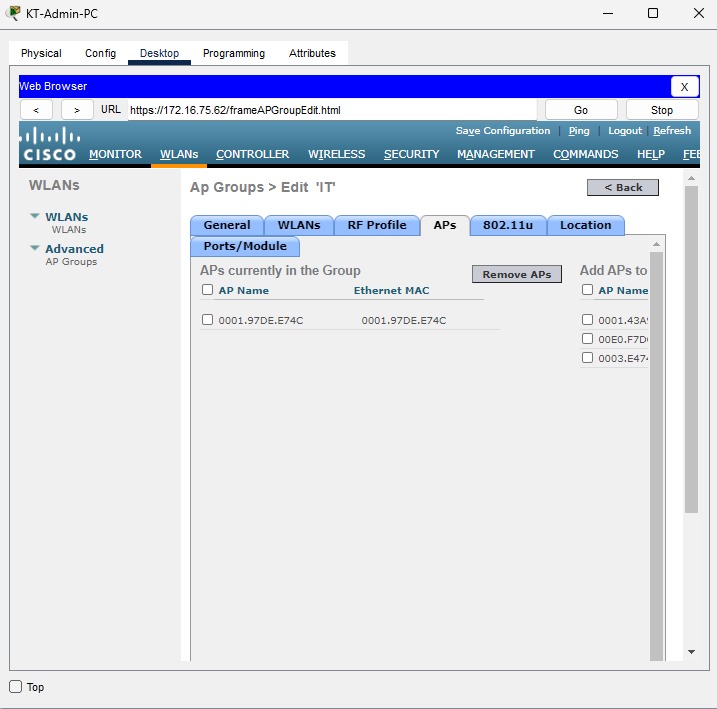
**Figure 23: WLAN Configuration of F3 group**



**Figure 24: Configured F3 Access Port**

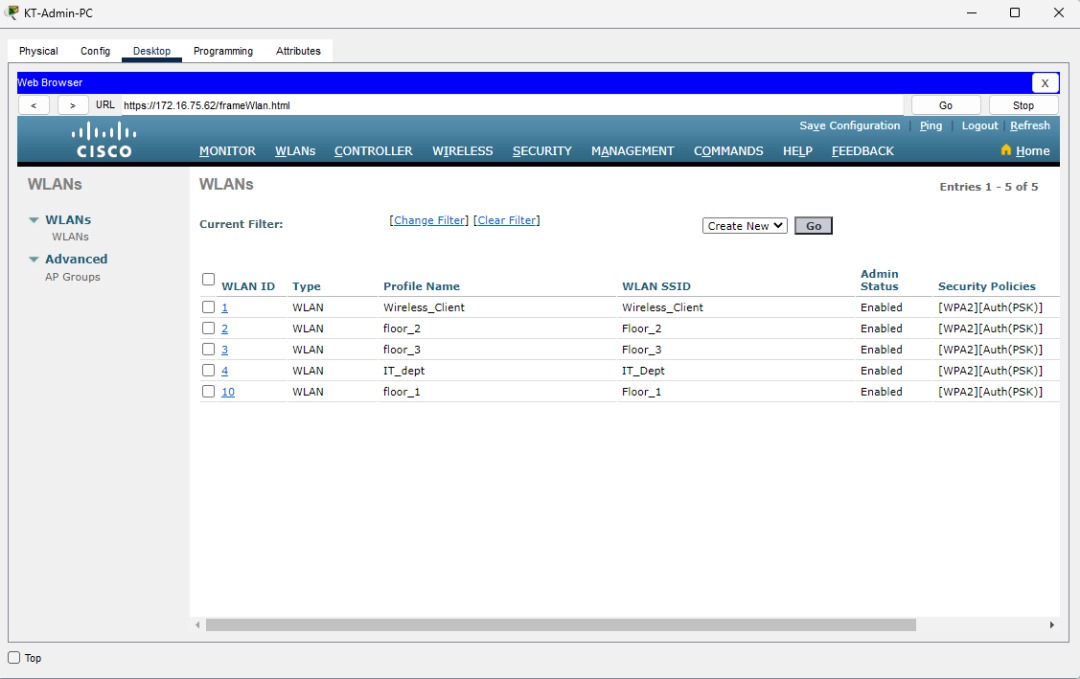


**Figure 25: WLAN Configuration of IT group**



**Figure 26: Configured IT Access Port**

Furthermore, WLAN profiles are essential elements that specify the settings of a specific wireless network. Each profile relates to a separate WLAN ID and SSID, enabling network administrators to distinguish and manage numerous wireless networks at the same time. The "Type" column specifies the WLAN's purpose or use, whereas the "Status" field shows whether the WLAN is presently active or deactivated.



**Figure 27:26 : Configured WLAN IDs**

# **6. EtherChannel Implementation**

EtherChannel, an established networking technology, provides a strong solution for improving network performance and reliability. EtherChannel, also known as link aggregation or port-channel, enables the combining of many physical Ethernet lines into a single logical link. This aggregation offers several benefits, including higher bandwidth, load balancing, and fault tolerance (Prakash, 2013). EtherChannel maximises data transport, enhances network efficiency, and assures a more robust network architecture by considering the bundled connections as a single, high-bandwidth connection (Qassim, 2009).

The implementation of EtherChannel is particularly important in the context of Microtech Sdn. Bhd.'s network upgrade, helping with data transmission optimisation and providing an efficient network architecture. The following discussion will give thorough insights into EtherChannel setup for a smooth integration into the current network environment.

A diagram of a network

Description automatically generated

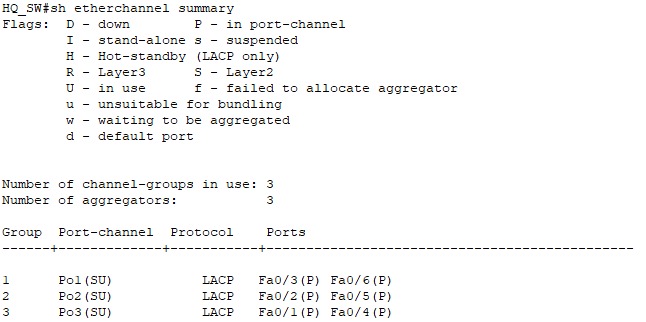
**Figure 28: Implemented EtherChannel**

## **6.1 EtherChannel Configuration**

A screenshot of a computer program

Description automatically generatedThe EtherChannel configuration was successfully configured to the HR\_SW and HQ\_SW switches. The HR\_SW configuration (see figure 13) has two channel-groups, denoted as Group 1 and Group 5, each of which use the LACP (Link Aggregation Control Protocol) protocol. Ports Fa0/1, Fa0/2, Fa0/3, and Fa0/4 are members of Group 1, which contributes to Port-channel 1, while ports Fa0/5 contribute to Port-channel 5. This design ensures great load balancing and redundancy by aggregating numerous physical ports into logical port-channels.

**Figure 29: HR\_SW EtherChannel Configuration**

In the HQ\_SW structure, a trio of channel-groups—Group 1, Group 2, and Group 3—are actively engaged, each coordinated by the LACP protocol (see figure 14). The member ports that contribute to these channel-groups are clearly listed, culminating in Port-channels 1, 2, and 3. Through the power of link aggregation, this sophisticated arrangement improves network performance by effectively utilising available connections and reinforcing the system against possible breakdowns.

**Figure 30: HR\_SW EtherChannel Configuration**

# **7. HSRP implementation**

High availability and network reliability are crucial aspects of contemporary networking, particularly for businesses such as Microtech Sdn. Bhd. that depends largely on smooth communication and data access. The Hot Standby Router Protocol (HSRP) stands out as an essential option for addressing these issues. By enabling multiple routers to operate together in a group, HSRP offers a redundancy solution by providing a single virtual IP address and gateway to the network (Sheghdara & Hassine, 2020). In the event of a router failure, HSRP guarantees a quick switchover to a backup router, reducing network downtime (Wang & Zhu, 2012). This section will dive into HSRP implementation, providing a full description of its functioning and configuration.

A diagram of a router

Description automatically generated

**Figure 31: Implemented HSRP**

## **7.1 HSRP Configuration**

The main router (KL\_ROUTER) has been assigned as the active router for Groups 10 and 20, handling the virtual IP addresses 192.168.25.5 and 192.168.25.70, respectively, (see Figure 2). The active router is in charge of routing network traffic and ensuring that the network remains operational.

A computer screen shot of a computer

Description automatically generated

**Figure 32: HSRP Configured KL\_Router (Active)**

Furthermore, the standby router (KL\_ROUTER [Standby]) is ready to take over in the event that the current router fails, minimising downtime and preserving continuous communication.

A screenshot of a computer

Description automatically generated

**Figure 33: HSRP Configured KL\_Router (Standby)**

Priorities are given to each router in the HSRP setup to establish their function in the network. KL\_ROUTER has a higher priority (110) than the backup router (100) in this case for both Group 10 and Group 20. This prioritisation guarantees that KL\_ROUTER plays an active role in load balancing and network performance optimisation.

# **8. Server Farm Configuration**

The Server Farm plays an essential role in the network's overall operation and efficiency, acting as the backbone for hosting critical applications, databases, and services (GeneSys, 2023). Configuring the Server Farm is an important step in optimising network performance and assuring continuous resource access . In this part, network administrators will look at the server farm setup of Microtech Sdn. Bhd. The emphasis will be on developing a well-organized and resilient infrastructure that matches with the company's operating objectives, from defining server responsibilities to implementing effective security measures.

## **8.1 VLANs Configuration in Server Farm**

Microtech Sdn. Bhd. has built a well-organized Virtual LAN (VLAN) structure inside the server farm environment in the VLAN setup for ServerFarm\_SW (refer to Figure 4). VLAN 1 is the default VLAN for public connection, while VLAN 50 (administration) is devoted to network administration services, providing a secure environment for administrative duties.

Furthermore, VLAN 60 (ServerFarm) is dedicated to server farm-related operations, supporting effective communication and traffic management within this essential network segment. VLAN 99 (Native) is the default VLAN for untagged traffic, whereas VLAN 100 (BlackHole) is reserved for specialised network needs.

A screenshot of a computer

Description automatically generated**Figure 34: ServerFarm\_SW VLAN Configuration**

## **8.2 DNS Server Configuration**

The main DNS server is configured to the IP address 195.200.50.34 in the DNS server setup for Microtech Sdn. Bhd.'s network (as seen in figure 19). This DNS server is critical in converting human-readable domain names into machine-readable IP addresses, allowing for smooth network connection and data retrieval.

The DNS server has a static IPv4 address of 195.200.50.34, a subnet mask of 255.255.255.240, and a default gateway of 195.200.50.33. This static setup guarantees that domain names and IP addresses are consistently and reliably associated, contributing to the efficient operation of network services. Furthermore, IPv6 is configured to be automatic, creating a link-local address (FE80::201:43FF:FE18:A87D) and using the same DNS server (195.200.50.34).

A screenshot of a computer

Description automatically generated

**Figure 35: Configuration of DNS Server**

## **8.3 Web Server Configuration**

The IPv4 address for Microtech Sdn. Bhd.'s network is statically allocated as 195.200.50.36, with a matching subnet mask of 255.255.255.240, in the configuration of the web server for Microtech Sdn. Bhd.'s network. The default gateway address is 195.200.50.33, which allows for connectivity with external networks.

Furthermore, the DNS server is set to 195.200.50.34, guaranteeing that the web server can resolve domain names for easy access to internet resources. This setting is required for the effective operation of web services as well as dependable network connection.

In terms of IPv6, the web server is set to use automatic addressing, which results in a link-local address (FE80::2E0:A3FF:FEEC:9CC1). This dual-stack method provides IPv4 and IPv6 protocol compatibility, enabling the web server to interact efficiently in a variety of network situations.

The 802.1X security feature is enabled, with MD5 authentication used for safe access control. The web server's unique link local IPv6 address (FE80::2E0:A3FF:FEEC:9CC1) improves its network visibility and accessibility.

A screenshot of a computer

Description automatically generated

**Figure 36: Configuration of Web Server**

## **8.4 FTP Configuration**

The IPv4 address of the FTP server inside Microtech Sdn. Bhd.'s network is statically set to 195.200.50.35, with a subnet mask of 255.255.255.240. The default gateway is set at 195.200.50.33, which allows for external network connectivity.

Similarly, the DNS server is listed as both 195.200.50.34 and 195.200.50.33, ensuring that the FTP server may resolve domain names seamlessly. This strong DNS setup ensures consistent access to web resources and improves the server's overall operation.

The FTP server uses automatic addressing for IPv6, resulting in a link-local address of FE80::206:2AFF:FECD:B095. This dual-stack method provides IPv4 and IPv6 protocol compatibility, allowing the FTP server to interact efficiently in a variety of network situations.

On the FTP server, the 802.1X security capability is enabled, with MD5 authentication for safe access management. The FTP server's unique link-local IPv6 address (FE80::206:2AFF:FECD:B095) improves its network visibility and accessibility.

A screenshot of a computer

Description automatically generated

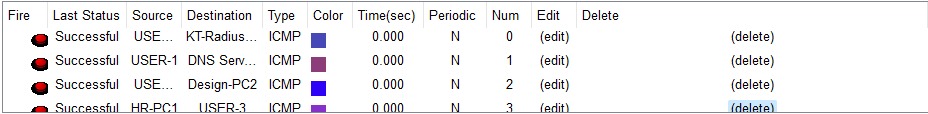
**Figure 37: Configuration of FTP Server**

# **9. Network Interconnection Verification: Tracert and Ping Commands**

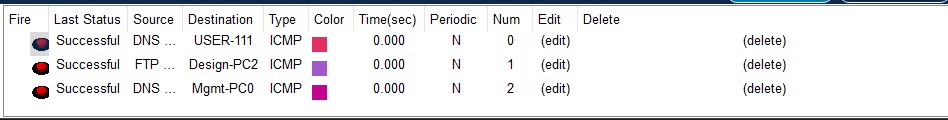
This section focuses on verifying the successful interconnection of networks within the Microtech Sdn. Bhd. infrastructure. Utilizing Tracert and Ping commands, the objective is to demonstrate the seamless communication and connectivity between different segments of the network. By examining the traceroute and ping results, network administrators can validate the effectiveness of the implemented configurations and ensure efficient data transmission across the interconnected network components.

## **9.1 Verifying Network Connectivity: Example 1**

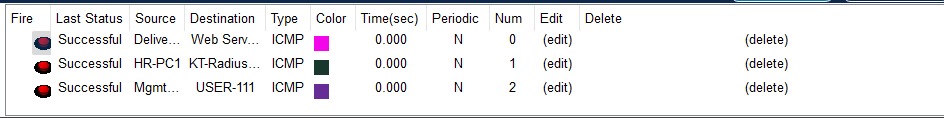
All ping attempts via the Cisco interface are successful, as demonstrated in the following figures. The network connectivity is robust, with consistent and reliable communication observed across various IP addresses.



**Figure 38: Successfully pings from KT**



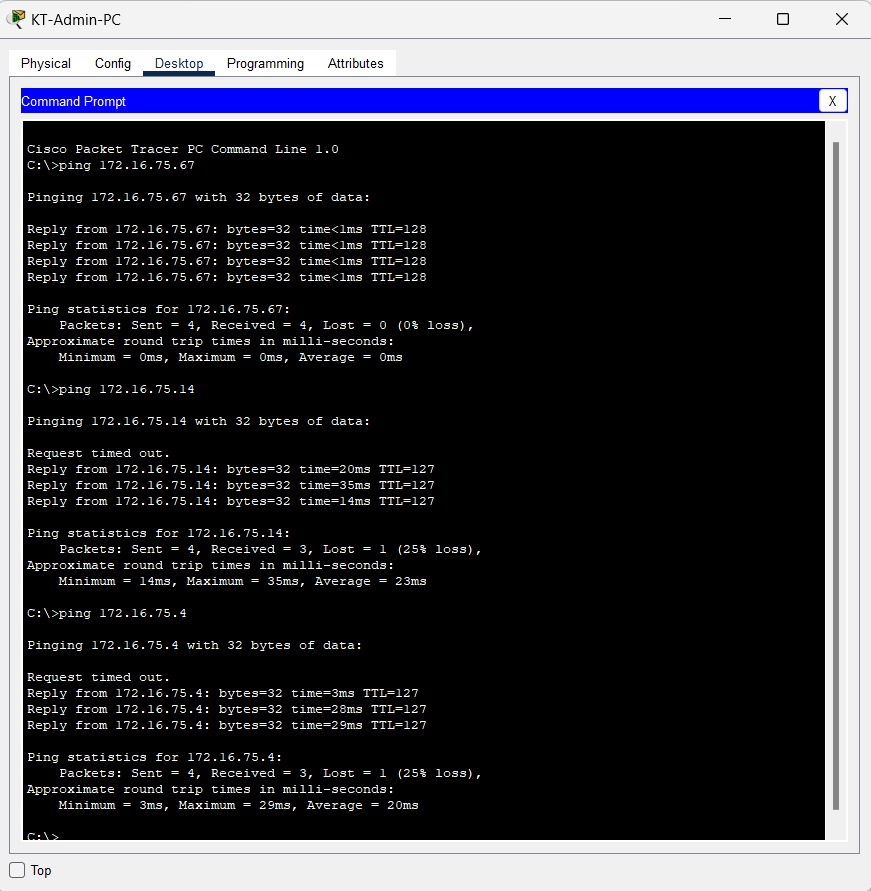
**Figure 39: Successfully pings from ServerFarm section**



**Figure 40: Successfully pings from HQ**

## **9.2 Verifying Network Connectivity: Example 2**

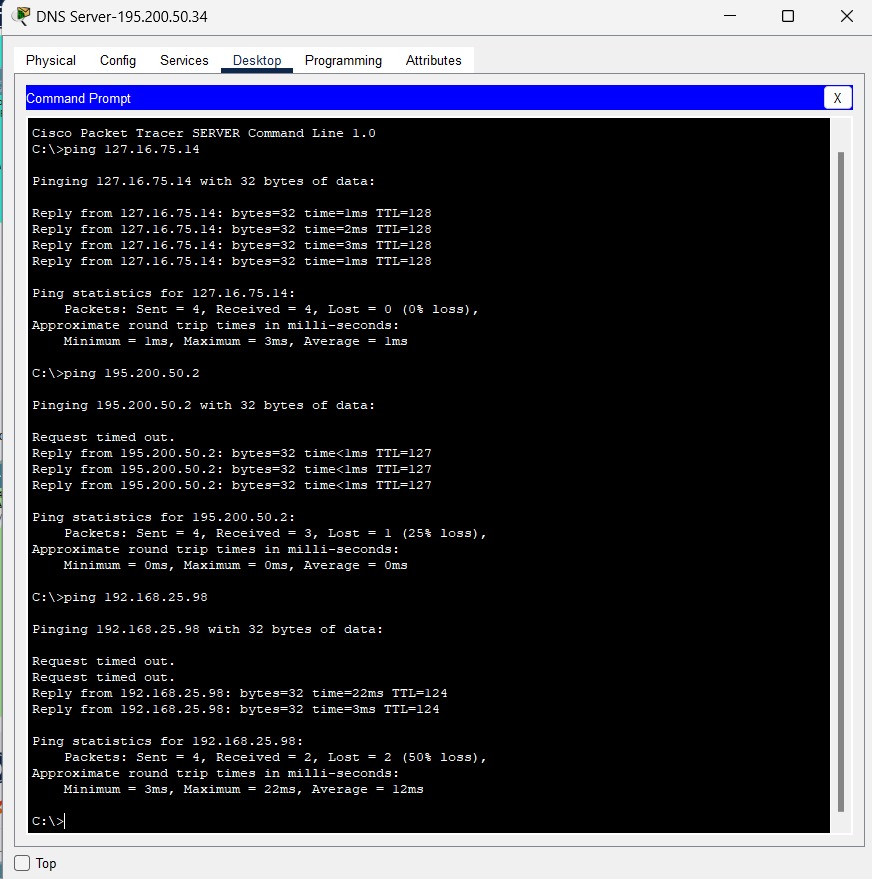
The Ping commands issued from the KT-Admin-PC demonstrate strong network connection and all pings are positively received.



**Figure 41: Successful Ping Displayed**

## **9.3 Verifying Network Connectivity: Example 3**

All ping commands from the DNS Server (195.200.50.34) command prompt are positive, indicating successful communication with the target nodes.



**Figure 42: Successful Ping Displayed**

**10. Strengthening Layer 2 Security: Attack Mitigation Strategies**

Throughout its router and switch architecture, Microtech Sdn. Bhd. must implement critical security measures. The primary objective is to address potential security vulnerabilities ahead of time by studying four Layer 2 security threats and then implementing powerful mitigation mechanisms (Cusack & Lutui, 2015). The network intends to strengthen its defences against possible attacks by carefully deploying these safety procedures, ensuring the safeguarding of key data and resources with an emphasis on confidentiality, integrity, and availability. The following discussion will provide a thorough evaluation of each security attack, as well as full descriptions of the related mitigation strategies.

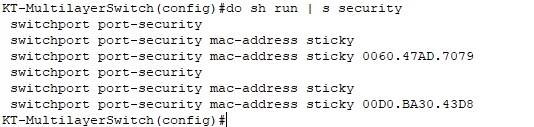
## **10.1 Configuring Fundamental Security Mechanisms**

A computer screen shot of a computer

Description automatically generatedTo eliminate possible security risks and prevent unauthorised access, all ports that are not actively in use are routinely deactivated in this context. VLANs (Virtual Local Area Networks) are used to properly separate and control network traffic, hence improving overall security. Active ports are carefully set to fit operating needs, whereas inactive ports are decommissioned. Furthermore, the use of a black hole method (VLAN100) assists to reject or reroute undesirable or harmful traffic, strengthening the network against possible attacks. This technique contributes to the development of a strong security position, ensuring that the network is well-protected and resilient to diverse security threats.

**Figure : Securing Unused Ports and Implementation of Blackhole**

The introduction of port security features on the switch is the next security method. Port security is an important strategy for controlling and restricting access to network resources by managing the MAC (Media Access Control) addresses of connected devices. The switchport is configured in this configuration to enforce port security, ensuring that only authorised devices may connect to the network. Furthermore, using sticky MAC addresses enables the switch to dynamically learn and save the MAC addresses of devices connecting to the protected ports. By linking MAC addresses with authorised devices, this improves security by prohibiting unauthorised devices from getting network access.



**Figure 44: Implemented Port Security**

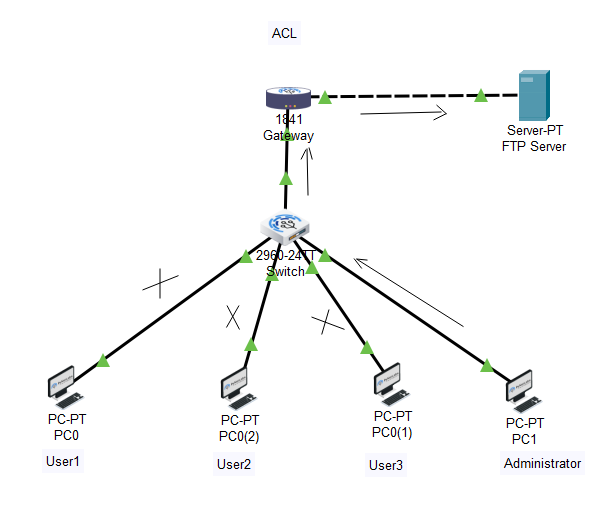
# **11. Recommendations for Additional Security Measures**

Microtech Sdn. Bhd. recognises the necessity of extra measures beyond the foundations in the goal of comprehensive network security. This section discusses three critical recommendations for improving the organization's security infrastructure.

## **11.1 Recommendation #1: Access Control Lists (ACLs)**

Microtech Sdn. Bhd. must consider the implementation of Access Control Lists (ACLs) which is an essential tool in the field of network security. ACLs act as virtual gatekeepers, coordinating data traffic entry and egress inside the network architecture. The organisation achieves complete control over access rights by carefully configuring ACLs, specifying rules that govern user or system interaction with defined resources (Sameer, 2021).

Furthermore, Access Control Lists (ACLs) provide a dynamic method for Microtech Sdn. Bhd. to enforce network security rules and regulatory compliance. The organisation may restrict the flow of traffic by carefully establishing rules inside the ACL configuration, permitting, or refusing access depending on stated criteria (Sulaiman & Saripurna, 2021). This level of control extends beyond just limiting access; it allows Microtech Sdn. Bhd. to support effective network administration, optimise bandwidth usage, and identify possible problems by selectively allowing or blocking traffic (Sameer, 2021).

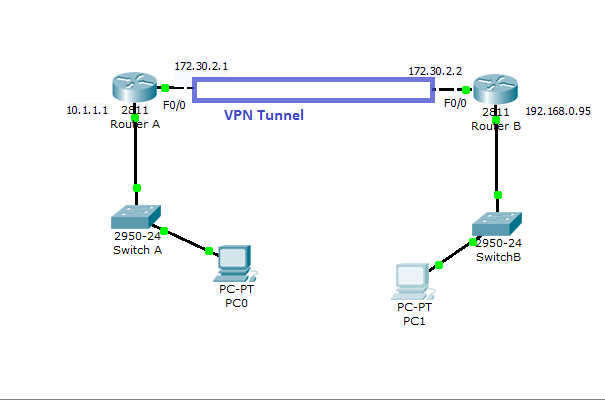


**Figure 45: Example Implementation of ACL** (PyNet Labs, 2023)

## **11.2 Recommendation #2: Virtual Private Networks (VPNs)**

The deployment of Virtual Private Networks (VPNs) appears as a critical proposal in strengthening Microtech Sdn. Bhd.'s security environment. VPNs act as encrypted tunnels between distant users and the organization's network, protecting data flows. This encryption method preserves the confidentiality and integrity of sensitive data, which is especially important when workers use the network from remote locations (Iqbal & Imam Riadi, 2019).

Furthermore, VPNs give an extra degree of protection by verifying users before authorising network access. This authentication procedure, which often employs strong measures such as two-factor authentication (2FA), offers an additional barrier against unauthorised access. By adding VPNs into its security framework, Microtech Sdn. Bhd. not only protects its data from possible eavesdropping and interception, but it also strengthens its defences against unauthorised entrance, complying with current best practices in network security (Veer & Gupta, 2016).

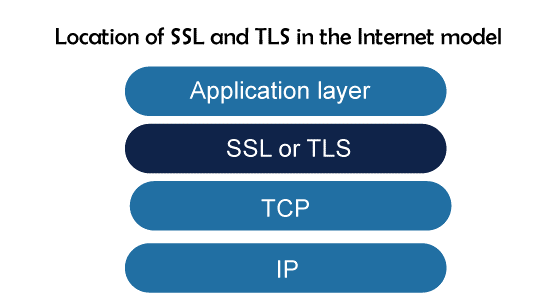


**Figure 46: Example Implementation of VPN** (Security Wing, 2014)

## **11.3 Recommendation #3: Secure Sockets Layer (SSL)/Transport Layer Security(TLS)**

Microtech Sdn. Bhd.'s safety measures may be strengthened further by using Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocols. SSL/TLS protocols are cryptographic protocols that allow clients and servers to communicate securely (Satapathy & Livingston, 2016). These policies protect sensitive information from possible interception or manipulation by encrypting data during transmission, boosting the organization's commitment to data integrity and confidentiality.

SSL/TLS usage extends beyond safeguarding data in transit; it also serves an important role in authenticating server identities, ensuring that users connect to genuine and trustworthy destinations. This dual-layered feature improves overall security by preventing possible man-in-the-middle attacks and building trust in users about the validity of network resources they access. Integrating SSL/TLS into an organization's security policy greatly adds to the creation of a secure and resilient digital environment (Hichem Mrabet et al., 2020).



**Figure 47: Example Implementation of SSL/TLS** (Java Point, 2021)

# **12. Conclusion**

In conclusion, Microtech Sdn. Bhd.'s commitment to update its information technology infrastructure is an important step towards creating a strong, efficient, and secure network environment. The installation of a Wireless Local Area Network (WLAN) at Krung Thep shows the company's commitment to modernising network accessibility while considering the different functions of its departments. Using Cisco as the primary simulation tool guarantees a dependable and industry-standard foundation for these developments.

Network administrators handled the complexities of WLAN architecture, LAN, and WAN setups, EtherChannel implementation, HSRP, and server farm configurations throughout the project. The investigation of security mechanisms and attacks at Layer 2, as well as the implementation of mitigation strategies, demonstrates Microtech's commitment to preserving crucial data and resources. Furthermore, the suggestions for ACL implementation, VPN, and SSL/TLS integration provide a proactive approach to improving overall security posture.

Microtech Sdn. Bhd. is well-positioned to strike a balance between modern technology and strong security protocols to support its planned network infrastructure upgrade. This comprehensive strategy not only protects network resource privacy, reliability, and accessibility, but also lays the groundwork for a robust and future-ready digital infrastructure.

# **13. References**

Ali, A. M., Dhimish, M., Alsmadi, M. M., & Mather, P. (2020). Algorithmic Identification of the Best WLAN Protocol and Network Architecture for Internet-Based Applications. *Journal of Information & Knowledge Management*, *19*(01), 2040011. https://doi.org/10.1142/s0219649220400110

Ali, A., Dhimish, M., & Mather, P. (2019). WLAN Protocol and Network Architecture Selection for Real-time Applications - White Rose Research Online. *Whiterose.ac.uk*. https://eprints.whiterose.ac.uk/177699/1/Manuscript.pdf

Cisco. (2023, August 18). *Cisco Packet Tracer 8.x new features - Packet Tracer Network*. Packet Tracer Network. https://www.packettracernetwork.com/features/

Cusack, B., & Lutui, R. (2015). *Innovating additional Layer 2 security requirements for a Innovating additional Layer 2 security requirements for a protected stack protected stack*. 81–86. https://doi.org/10.4225/75/57b69e28d938f

Froehlich, A. (2018). *The on-premises vs. cloud-managed WLAN architecture debate*. Networking; TechTarget. https://www.techtarget.com/searchnetworking/feature/On-premises-vs-cloud-managed-WLAN-Which-is-right-for-you

Gandhi, V. (2014, September). *A Study on Wireless LAN Fundamentals, Architecture, Benefits and Its Security Risks*. Ssrn.com. https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=2503782

GeneSys. (2023). *Short Message Service Technical Reference - Server Farm and Switchover Considerations*. Genesys.com. https://help.genesys.com/pureconnect/mergedprojects/wh\_tr/mergedprojects/wh\_tr\_sms/desktop/server\_farm\_switchover\_considerations.htm

Hichem Mrabet, Belguith, S., Adeeb Alhomoud, & Abderrazak Jemai. (2020). A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis. *Sensors*, *20*(13), 3625–3625. https://doi.org/10.3390/s20133625

Hoch Dirraneh, H., & Zhou, H. (2007). IJARCCE Implementation of WLAN network with strong authentication. *International Journal of Advanced Research in Computer and Communication Engineering ISO*, *3297*. https://doi.org/10.17148/IJARCCE.2017.61042

IBM. (2023, September 7). *IBM Documentation*. Ibm.com. https://www.ibm.com/docs/en/sevone-npm/6.6?topic=notes-release-wireless-lan-controller-collector-660

Iqbal, M., & Imam Riadi. (2019, May 19). *Analysis of Security Virtual Private Network (VPN) Using OpenVPN*. ResearchGate; The Society of Digital Information and Wireless Communications (SDIWC). https://www.researchgate.net/publication/333198144\_Analysis\_of\_Security\_Virtual\_Private\_Network\_VPN\_Using\_OpenVPN

Java Point. (2021). *Transport Layer Security | Secure Socket Layer (SSL) and SSL Architecture - javatpoint*. Www.javatpoint.com. https://www.javatpoint.com/transport-layer-security-secure-socket-layer-ssl-and-ssl-architecture

Kristián Košťál, Rastislav Bencel, Ries, M., Trúchly, P., & Kotuliak, I. (2019). High Performance SDN WLAN Architecture. *Sensors*, *19*(8), 1880–1880. https://doi.org/10.3390/s19081880

Prakash, B. (2013). Hypervisors, Virtualization, and Networking. *Elsevier EBooks*, 387–416. https://doi.org/10.1016/b978-0-12-401673-6.00016-7

PyNet Labs. (2023, September 4). *What is Access Control List (ACL)? - PyNet Labs*. PyNet Labs. https://www.pynetlabs.com/what-is-access-control-list/

Qassim, Y. T. (2009, June). *Applying Reliability Solutions to a Cooperative Network*. ResearchGate; Zarqa University. https://www.researchgate.net/publication/331560115\_Applying\_Reliability\_Solutions\_to\_a\_Cooperative\_Network

Sameer, A. (2021, July). *Access Control Lists (ACLs)*. ResearchGate; unknown. https://www.researchgate.net/publication/353236150\_Access\_Control\_Lists\_ACLs

Satapathy, A., & Livingston, J. (2016, November 17). *A Comprehensive Survey on SSL/ TLS and their Vulnerabilities*. ResearchGate; Foundation of Computer Science. https://www.researchgate.net/publication/310761924\_A\_Comprehensive\_Survey\_on\_SSL\_TLS\_and\_their\_Vulnerabilities

Secure IT Store. (2022). *Cisco Access Points | SecureITStore.com*. Secureitstore.com. https://www.secureitstore.com/Access-Points.asp

Security Wing. (2014). *Cisco VPN Configuration in IOS Routers | securitywing*. Securitywing.com. https://securitywing.com/cisco-vpn-configuration/

Sheghdara, M., & Hassine, J. (2020). Automatic retrieval and analysis of high availability scenarios from system execution traces: A case study on hot standby router protocol. *Journal of Systems and Software*, *161*, 110490–110490. https://doi.org/10.1016/j.jss.2019.110490

Sulaiman, O. K., & Saripurna, D. (2021). *Network Security System Analysis Using Access Control List (ACL)*. *5*(2), 192–197. https://doi.org/10.30645/ijistech.v5i2.131

Veer, K., & Gupta, H. (2016, March 4). *A New Approach for the Security of VPN*. ResearchGate; unknown. https://www.researchgate.net/publication/307090754\_A\_New\_Approach\_for\_the\_Security\_of\_VPN

Vivek Kumar Soni, & Rohit Mendiratta. (2008). *Next-generation WLAN architecture for high performance networks*. https://doi.org/10.1049/cp:20080161

Wang, F., & Zhu, C. (2012). HSRP Protocol Based on High Reliable Redundant Campus Network Design. *Communications in Computer and Information Science*, 107–114. https://doi.org/10.1007/978-3-642-31968-6\_13

*What is SSL (Secure Sockets Layer)?* (2023). Cloudflare. https://www.cloudflare.com/learning/ssl/what-is-ssl/