

**KOLEJ PROFESIONAL MARA BERANANG**

**DIPLOMA IN COMPUTER SCIENCE (DCS)**

|  |  |
| --- | --- |
| **COURSE NAME** | : LOCAL AREA NETWORKING TECHNOLOGIES |
| **COURSE CODE** | : CSC 2773 |
| **ACADEMIC SESSION** | : SESSION 3 2024/2025 |
| **TYPE OF ASSESSMENT** | : FINAL ASSIGNMENT |
| **DURATION** | : 3 WEEKS (31 JANUARY 2025 – 20 FEBRUARY 2025) |

**CLO 3:** Analyse LAN design based on LAN technologies using appropriate LAN design tools.

**INSTRUCTION TO CANDIDATES:**

1. This assessment consist of 6 tasks. Answer ALL the task given.
2. Any late submission will be penalized.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | |  | **Personal Details** | | | **Name** | SOFEA ALEEYA BINTI AHMAD NAZRI | | | **I/D**  **Number** | BCS2307-091 | | | **Class** | [DCS 5A] [DCS 5B] [DCS 5C] [DCS 5D] | | | **Lecturer** | / | EN. MOHD ZULHILMI BIN  MOHAMAD ZAKI | |  | PN. SITI AZEYRAH BT RAMLI | | |  |  | | --- | --- | | **Section / Question No.** | **Marks** | | Task 1 |  | | Task 2 |  | | Task 3 |  | | Task 4 |  | | Task 5 |  | | Task 6 |  | | Task 7 |  | | **Total** | **/60** | |

I hereby declare that no form of plagiarism will be tolerated in this assessment. Failure to comply will result in a failing grade for the assessment.

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Scenario**



The Ministry of Public Administration requires a secure and efficient network infrastructure to handle sensitive government data, communication between departments, and remote access for government officials. The network design needs to ensure that departments can function independently but still allow for controlled communication and centralized access to critical records. As discussed with the top management, your director has assigned you to construct the secured Local Area Networking (LAN) by following all the requirements below:

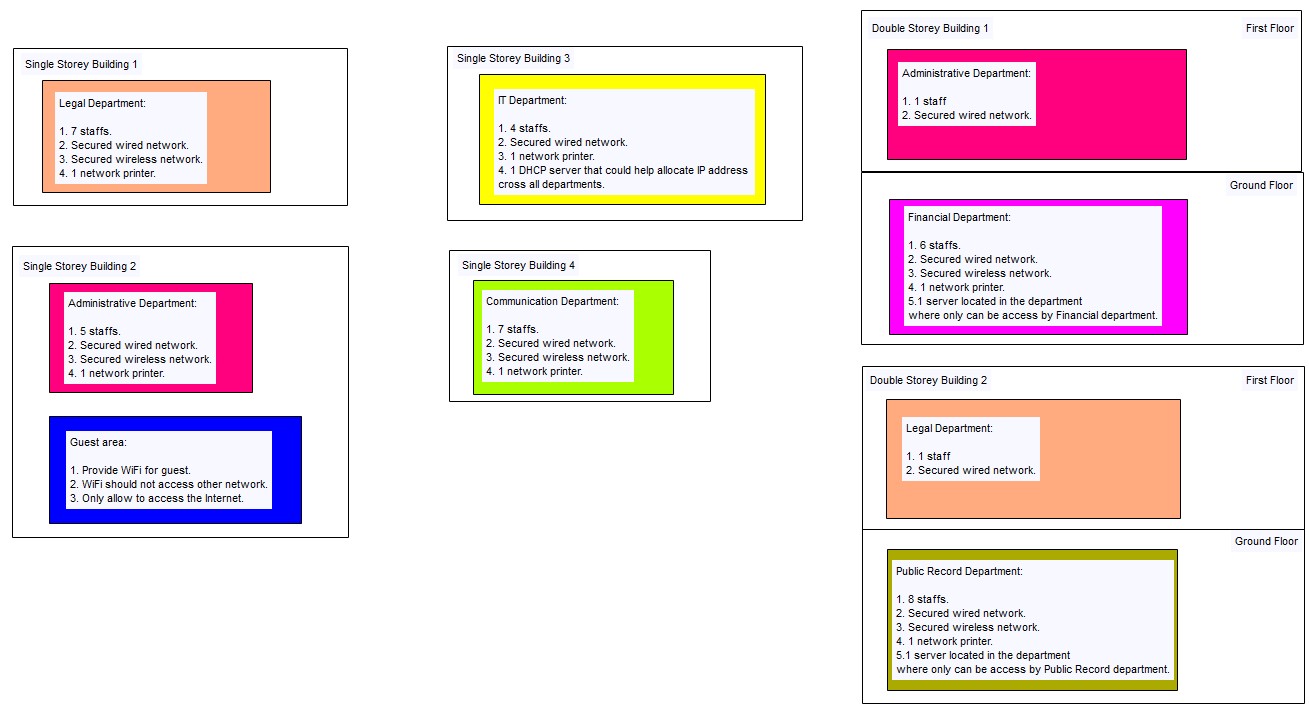
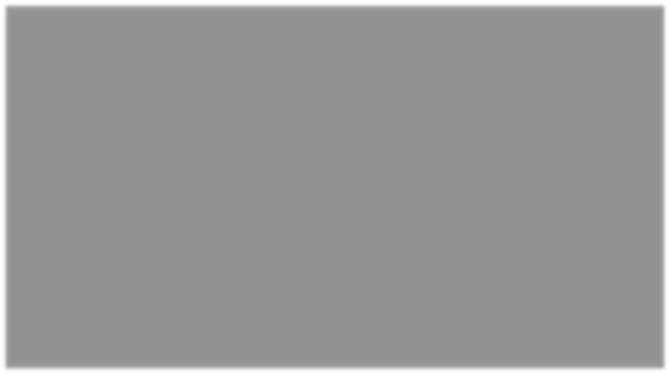
1. Should apply the hierarchical network design by suggesting any suitable LAN hardware:
   * The network must be divided into different segments, with each department having its own dedicated VLAN to minimize cross-department communication and reduce security risks.
   * The list of departments are **Legal**, **Communications**, **Financial**, **Administrative**, **IT** and **Public** **Record**.

1. Each of the users from each department will be allocated a specific subnet to improve IP address management. All of them will be given IP address by using a DHCP server that place inside the IT department.

1. Wireless and Wired Network Design:
   * Wireless Networks: Wireless access points will be available for authorized employees in their workstation area. These networks will be secured with WPA2 encryption.
   * Wired Networks: Departmental workstations should be connected via secure wired networks, especially for critical departments like Finance and Legal, to ensure fast and secure access to sensitive information.
   * Guest Network: A segregated guest Wi-Fi network will be provided in visitor areas, allowing guests to connect without accessing the main government network.

1. Printer Sharing:
   * Shared printers will be available in each department, and only department-specific users will have printing access to ensure sensitive documents are printed only by authorized personnel.

Figure 1.0



**Tasks:**

Your tasks are:

1. Demonstrate the subnetted IP addressing scheme for the suitable IP address to be used in the Ministry of Public Administration new LAN design.

1. Analyse the suitable LAN technologies and infrastructure for the ministry in a new LAN design using any suitable design tools, including:
   1. suitability of the suggested hardware
   2. suitability of the suggested LAN technologies
   3. connection of all staff across departments
   4. connection of all staff across buildings

1. Analyse the suggested LAN design applied the hierarchical network design.

1. By referring to the suggested LAN design, analyse the scalability of the implemented devices

1. By referring to the suggested LAN design, analyse the implemented LAN infrastructures that should fulfil the aspects of:
   1. fault-tolerance
   2. high-speed links

1. Choose any **three (3)** **LAN security** technologies that can be applied to the network, especially to prevent the staff from accessing confidential data on different broadcast domains in wired and wireless network traffic.

1. With relation to the suggested LAN technologies analysed in Task 2, analyse the suitability of the suggested **LAN technologies** for handling the ministry network problems.

**Assessment Rubrics:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Attributes** | **Tasks** | **1**  **Fair** | **2**  **Good** | **3**  **Excellent** | **Weight age** | **Marks** |
| **Articulation** | 1. Demonstrate the subnetted IP addressing scheme for the suitable IP address to be used in the Ministry of  Public  Administration new LAN design. (Considering the number of hosts given in the scenario) | Correctly discuss the suitability of the suggested IP address with the correct IP and justification.      Calculate correct IP  Subnetting table for  PCs/nodes with at least **two (2)** departments including:   * Number of borrowed bit * New Subnet mask * suitability of usable subnet address * suitability of usable host address | Correctly discuss the suitability of the suggested IP address with the correct IP addressing class and justification.      Calculate correct IP subnetting table for  PCs/nodes with at least **four (4)** of the below:   * number of borrowed bits * new Subnet mask * suitability of usable subnet address * suitability of usable host address * complete IP subnetting   table with relate to  scenario   * successfully implement the IP subnetting in the   suggested LAN design | Correctly discuss the suitability of the suggested IP address with the excellent IP addressing class and justification.    Calculate correct IP subnetting table for PCs/nodes with all of the below:   * number of borrowed bits * new Subnet mask * suitability of usable subnet address * suitability of usable host address * complete IP subnetting table with relate to   scenario   * successfully implement the subnetted IP subnetting in the suggested LAN design | 2 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Attributes** | **Tasks** | **1**  **Fair** | **2**  **Good** | **3**  **Excellent** | **Weight age** | **Marks** |
| **Design** | 2. Analyse the suitable LAN technologies and infrastructure for the ministry in a new LAN design using any suitable design tools, including: | | | | | |
| ❑ Suitability of the suggested hardware | All networked hardware are good but poorly convincing. Fulfill at least **two (2)** of below:   * buildings connection * floors connection * departments connection * Network devices connection * Connection to server room * Wireless connection | All networked hardware are good but poorly convincing. Fulfill at least **four (4)** of below:   * buildings connection * floors connection * departments connection * Network devices connection * Connection to server room * Wireless connection | All networked hardware are consistently connected and convincing including:   * buildings connection * floors connection * departments connection * Network devices connection * connection * Connection to server room * Wireless connection | 2 |  |
| ❑ Suitability of the suggested LAN technologies | * Analyse any **one (1**) LAN technology in handling ministry problems: * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_              * Discuss the suitability of the suggested LAN technologies for handling | * Analyse at least **two (2**) LAN technologies in handling ministry problems: * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_      * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_        * Discuss the suitability of the suggested LAN | * Analyse **three (3**) LAN technologies in handling ministry problems: * \_\_\_\_\_\_\_\_\_\_\_\_\_\_   \_\_     * \_\_\_\_\_\_\_\_\_\_\_\_\_\_   \_\_     * \_\_\_\_\_\_\_\_\_\_\_\_\_\_   \_\_ | 2 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Attributes** | **Tasks** | **1**  **Fair** | **2**  **Good** | **3**  **Excellent** | **Weight age** | **Marks** |
|  |  | the ministry’s network problem | technologies for handling the ministry’s network problem | ❑ Discuss the suitability of the suggested LAN technologies for handling the ministry’s network problem |  |  |
| ❑ Connection of  all staff across departments | * Partial of staffs in the same department but in different buildings and floors able to communicate to each other using virtual LAN (VLAN). * Partially create VLANs for the intended broadcast domain * Inconsistently assign ports to the created   VLANs | * All staff in the same department but in the different buildings and floors are able to communicate to each other using virtual LAN (VLAN). * Partially create VLANs for the intended broadcast domain * Correctly assign ports to the created VLANs | * All staff in the same department but in the different buildings and floors are able to communicate to each other using virtual LAN (VLAN). * Successfully create VLANs for the intended broadcast domain traffic * Correctly assign ports to the created VLANs * Correctly assign subnetted IP to the created VLAN | 2 |  |
| ❑ Connection of  all staff across buildings | All networked buildings are good but poorly convincing. Fulfill at least **two (2)** of below:   * buildings connection * VLAN connection * Network devices connection | All networked buildings are good but poorly convincing. Fulfill at least **four (4)** of below:   * buildings connection * VLAN connection * Network devices connection | All networked buildings are consistently connected and convincing including:   * buildings connection * VLAN connection * Network devices connection | 2 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Attributes** | **Tasks** | **1**  **Fair** | **2**  **Good** | **3**  **Excellent** | **Weight age** | **Marks** |
|  |  | * connection * Connection to server room * Wireless connection * excellent IP management | * connection * Connection to server room * Wireless connection * excellent IP management | * Connection to server room * Wireless connection * excellent IP management |  |  |
| **Reproduce and Process**  **Information** | 3. Analyse the suggested LAN design applied the hierarchical network design. | * All buildings and floors of the suggested LAN design partly applied network hierarchical model. * Inconsistently in show 3tiers hierarchical model in the suggested network design. | * All buildings and floors of the suggested LAN design correctly applied to the 3 tiers-network hierarchical model. * Show 3-tiers hierarchical model in the suggested network design. * Justify the effectiveness of the 3-tiers hierarchical model in the suggested network design. |  | 2 |  |
| **Gather** | 4. By referring to the suggested LAN design, analyse the  scalability of the implemented devices. | Correctly provide **one (1)** point of scalability analysis on the suggested LAN devices. | Correctly provide **two (2)** points of scalability analysis on the suggested LAN devices. | Correctly provide **three (3)** points of scalability analysis on the suggested LAN devices. | 2 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Attributes** | **Tasks** | **1**  **Fair** | **2**  **Good** | **3**  **Excellent** | **Weight age** | **Marks** |
| **Gather** | 5. By referring to the suggested LAN design, analyse the implemented LAN infrastructures that should fulfil the aspects of: | | | | | |
| (a) Fault- tolerance | Identify the general faulttolerance technology that is excellent to be used in the suggested LAN design.    Generally discuss the effect of the implemented faulttolerance technology to the suggested LAN design. | Identify the suitable faulttolerance technology that is excellent to be used in the suggested LAN design.    Analyse in detail the effects of the implemented faulttolerance technology on the suggested LAN design. |  | 2 |  |
| (b) high-speed links | Identify the general highspeed links technology that is suitable to be used in the suggested LAN design.    Generally discuss the effect of the implemented highspeed links technology to the suggested LAN design. | Identify the suitable highspeed links technology that is excellent to be used in the suggested LAN design.    Analyse in detail the effects of the implemented high-  speed links technology on the suggested LAN design. |  | 2 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Attributes** | **Tasks** | **1**  **Fair** | **2**  **Good** | **3**  **Excellent** | **Weight age** | **Marks** |
| **Collaboration** | 6. Choose any three (3) LAN  securitytechnologies that can be applied to the network, especially to prevent the staffs from accessing confidential data on different  broadcast domains in wired and wireless network traffic. | * Correctly discuss **one (1)** LAN security technologies that can be applied to the proposed LAN design, including: * broadcast domain   protection   * access mode   protection   * trunk mode   protection   * Correctly discuss wireless LAN security technology for the proposed LAN design * Partially implement the suggested security defends in the suggested LAN design | * Correctly discuss **two (2)** LAN security technologies that can be applied to the proposed LAN design, including: * broadcast domain   protection   * access mode   protection   * trunk mode   protection   * Correctly discuss wireless LAN security technology for the proposed LAN design * Correctly implement the suggested security defends in the suggested LAN design. | * Correctly discuss **three**   **(3)** LAN security technologies that can be applied to the proposed LAN design, including:   * broadcast domain   protection   * access mode   protection   * trunk mode   protection   * Correctly discuss wireless LAN security technology for the proposed LAN design * Correctly implement the suggested security defends in the suggested LAN design. | 2 |  |
| **Attributes** | **Tasks** | **1**  **Fair** | **2**  **Good** | **3**  **Excellent** | **Weight age** | **Marks** |
| **Gather** | 7. With relation to the suggested LAN technologies in Task  2, analyse the suitability of the suggested LAN technologies for handling the ministry network problems. | * Illustrate the justification of the suitability of any **one (1**) suitability of the LAN technologies based on the proposed LAN design (with screenshot evidence of the implementation in the suggested LAN design):     ❑ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_             * One of the suggested LAN technology was successfully implemented in the suggested LAN design. | • Analyse the suitability of the **two (2**) proposed LAN technologies based on the proposed LAN design (with screenshot evidence of the implementation in the suggested LAN design):     * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_      * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_           • Any **two (2)** suggested LAN technologies were successfully implemented in the suggested LAN design. | * Analyse the suitability of   **ALL** proposed LAN technologies based on the proposed LAN design  (with screenshot evidence of the implementation in the suggested LAN design):     * + \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   \_\_     * + \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   \_\_     * + \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   \_\_       * All the suggested LAN technologies were   successfully  implemented in the suggested LAN design. | 2 |  |
| **Total Marks Earned** | |  | | |  | /60 |
| **Total Percentage (30%)** | |  | | |  |  |

Task 1: Subnetted IP addressing scheme

1. Calculate borrow bits:

* Use the formula, Usable Subnet = 2 Borrow Bits – 2.
* Usable Subnet = 7 (based on number of department and guest room)
* 2 Borrow Bits – 2 ≥ 7
* 2 Borrow Bits ≥ 7 + 2
* 2 Borrow Bits ≥ 9
* 2 4 = 16
* 16 ≥ 9
* The nearest borrow bits is 4 as the value of 2 4 is more than 9 which are 16
* **The borrow bits is 4**

1. Determine the new subnet mask:

* The 4 borrow bits from the host portion will be presented as 1s in 4 bits in the octet. Refer to binary notation. 4 borrow bits have been highlighted.

|  |  |  |
| --- | --- | --- |
|  | Binary Notation | Decimal Notation |
| Subnet Mask | 11111111.11111111.11110000.0000000 | 255.255.240.0 |

1. Calculate total subnets and usable subnet:

|  |  |
| --- | --- |
| Total Subnets = 2 Borrow Bits  = 24  = 16 Subnets  16 subnets created including 2 subnets  (1st and last subnet range) | Usable Subnets = 2 Borrow Bits – 2  = 24 – 2  = 14 Subnets  14 subnets available and can be assigned to 14 group of network |

4. Calculate Total Hosts and Usable Hosts:

|  |  |
| --- | --- |
| Total Hosts = 2 Balance Host Bits  = 212  = 4096 hosts  4096 IP addresses for each subnet including 2 IP addresses for network address and broadcast address | Usable Hosts = 2 Balance Host Bits – 2  = 212 – 2  = 4094 hosts  4094 IP addresses for each subnet which can given to assign host inside the subnet. |

5. Block size or increment number:

= 256 – subnet mask

= 256 – 240

= 16

= 16 x 256

= 240

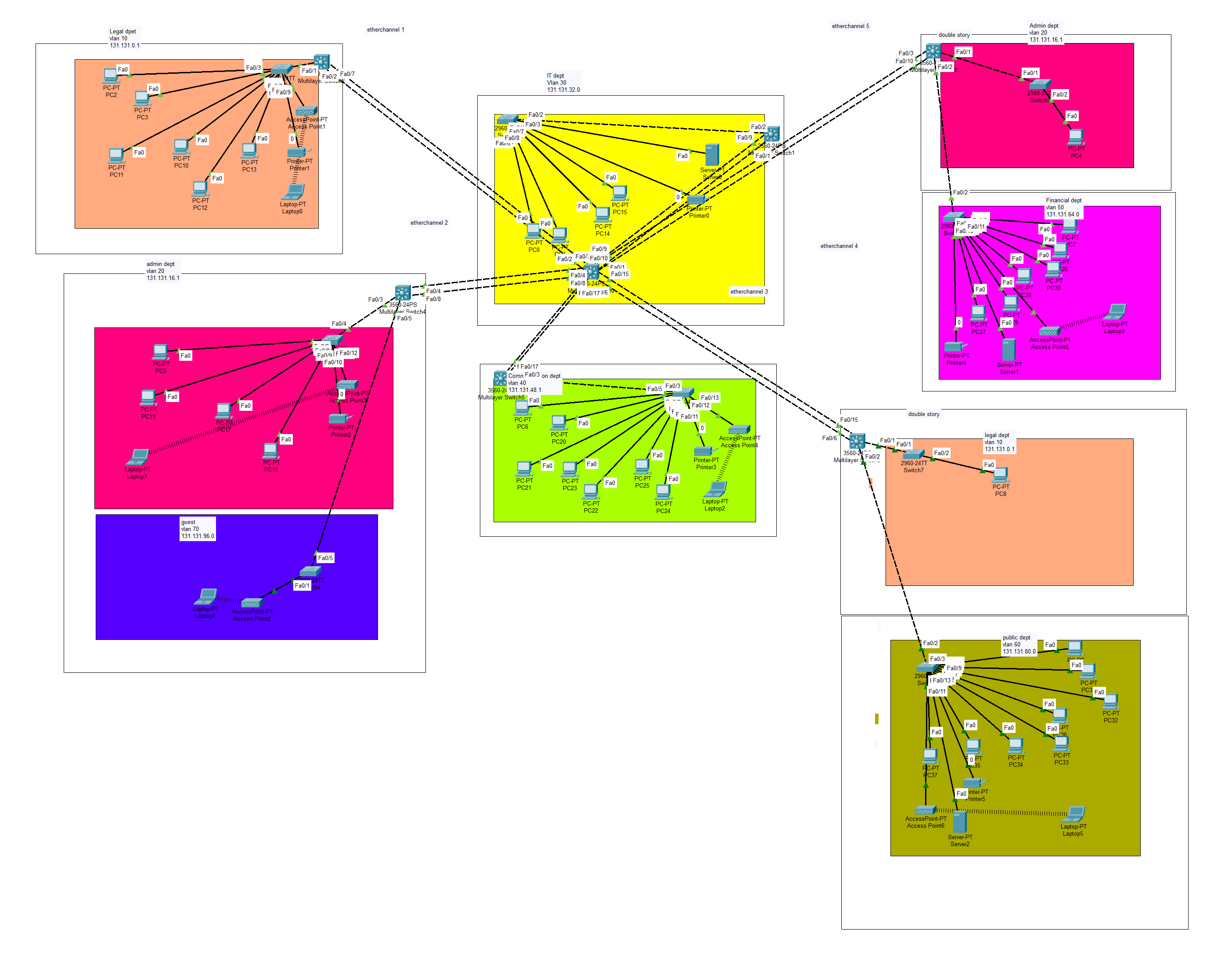
6. Listing of subnets in table:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No. | Network Add | First Host Add | Last Host Add | Broadcast Add |
| 1. | 131.131.0.0 | 131.131.0.1 | 131.131.15.254 | 131.131.15.255 |
| 2. | 131.131.16.0 | 131.131.16.1 | 131.131.31.254 | 131.131.31.255 |
| 3. | 131.131.32.0 | 131.131.32.1 | 131.131.47.254 | 131.131.47.255 |
| 4. | 131.131.48.0 | 131.131.48.1 | 131.131.63.254 | 131.131.63.255 |
| 5. | 131.131.64.0 | 131.131.64.1 | 131.131.79.254 | 131.131.79.255 |
| 6. | 131.131.80.0 | 131.131.80.1 | 131.131.95.254 | 131.131.95.255 |
| 7. | 131.131.96.0 | 131.131.96.1 | 131.131.111.254 | 131.131.111.255 |
| 8. | 131.131.112.0 | 131.131.112.1 | 131.131.127.254 | 131.131.127.255 |
| 9. | 131.131.128.0 | 131.131.128.1 | 131.131.143.254 | 131.131.143.255 |
| 10. | 131.131.144.0 | 131.131.144.1 | 131.131.144.254 | 131.131.144.255 |
| 11. | 131.131.160.0 | 131.131.160.1 | 131.131.175.254 | 131.131.175.255 |
| 12. | 131.131.176.0 | 131.131.176.1 | 131.131.191.254 | 131.131.191.255 |
| 13. | 131.131.192.0 | 131.131.192.1 | 131.131.207.254 | 131.131.207.255 |
| 14. | 131.131.208.0 | 131.131.208.1 | 131.131.223.254 | 131.131.223.255 |

7. IP subnetting in the suggested Lan:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| No. | Network Add | First Host Add | Last Host Add | Broadcast Add | VLAN name | VLAN ID |
| 1. | 131.131.0.0 | 131.131.0.1 | 131.131.15.254 | 131.131.15.255 | Legal Dept | 10 |
| 2. | 131.131.16.0 | 131.131.16.1 | 131.131.31.254 | 131.131.31.255 | Administrative Dept | 20 |
| 3. | 131.131.32.0 | 131.131.32.1 | 131.131.47.254 | 131.131.47.255 | IT Dept | 30 |
| 4. | 131.131.48.0 | 131.131.48.1 | 131.131.63.254 | 131.131.63.255 | Communication Dept | 40 |
| 5. | 131.131.64.0 | 131.131.64.1 | 131.131.79.254 | 131.131.79.255 | Financial Dept | 50 |
| 6. | 131.131.80.0 | 131.131.80.1 | 131.131.95.254 | 131.131.95.255 | Public Record Dept | 60 |
| 7. | 131.131.96.0 | 131.131.96.1 | 131.131.111.254 | 131.131.111.255 | Guest Area | 70 |
| 8. | 131.131.112.0 | 131.131.112.1 | 131.131.127.254 | 131.131.127.255 |  |  |
| 9. | 131.131.128.0 | 131.131.128.1 | 131.131.143.254 | 131.131.143.255 |  |  |
| 10. | 131.131.144.0 | 131.131.144.1 | 131.131.144.254 | 131.131.144.255 |  |  |
| 11. | 131.131.160.0 | 131.131.160.1 | 131.131.175.254 | 131.131.175.255 |  |  |
| 12. | 131.131.176.0 | 131.131.176.1 | 131.131.191.254 | 131.131.191.255 | Reserved for future needs |  |
| 13. | 131.131.192.0 | 131.131.192.1 | 131.131.207.254 | 131.131.207.255 |  |  |
| 14. | 131.131.208.0 | 131.131.208.1 | 131.131.223.254 | 131.131.223.255 |  |  |

**Task 2: Analyse the suitable LAN technologies and infrastructure**



a. suitability of suggested hardware

* The hardware devices selected for the ministry’s LAN ensure efficient, reliable, and scalable network connectivity across all buildings, floors, and departments. These devices are chosen to support VLAN segmentation, high-speed data transfer, secure access control, and wireless connectivity while ensuring seamless communication between all departments and the server room.
* Core layer switch: Cisco Catalyst 3560 Multilayer Switch

At the Core Layer, a Cisco Catalyst 3560 Multilayer Switch is implemented to handle high-speed routing between VLANs and manage network traffic across all buildings. This multilayer switch acts as the backbone of the network, ensuring that all departments are interconnected while maintaining fast data transfer and redundancy through EtherChannel. Since the Core Switch connects directly to the Distribution Layer switches in each building, it ensures that staff from different buildings and floors can communicate efficiently.

* Distribution layer switch: Cisco Catalyst 3560 Multilayer Switch

At the Distribution Layer, each building is equipped with a Cisco Catalyst 3560 Multilayer Switch, which provides VLAN segmentation and inter-VLAN routing for department networks within the building. These switches ensure that network traffic remains organized, allowing staff in the same department but in different buildings or floors to communicate without issues. The DHCP server, located in the IT Department, is directly connected to the Core Switch, ensuring that all VLANs receive dynamic IP addresses for easier network management. Additionally, the Public Record Department and Financial Department each have dedicated servers, providing secure data storage and controlled access to authorized staff.

* Access layer switch: Cisco Catalyst 2960 switches

At the Access Layer, Cisco Catalyst 2960 switches are used to connect end-user devices such as PCs, printers, and department-specific servers. Each Access Switch is VLAN-configured, ensuring that only authorized devices can communicate within a department network. These switches also provide port security to prevent unauthorized access, making them essential for protecting confidential ministry data.

* Wireles connection: Cisco Access Points (APs)

For wireless connectivity, Cisco Access Points (APs) are installed in departments that require Wi-Fi access. These APs are configured with WPA2 encryption, ensuring that only authorized users can connect while keeping wireless traffic secure.

* Servers: DHCP, Public Record, and Financial Servers

The ministry’s network includes three key servers to support operations:

1. DHCP Server (IT Department): Assigns dynamic IP addresses to all wired and wireless devices across departments, simplifying network management and preventing IP conflicts.
2. Public Record Server (Public Record Department): Stores confidential records and files, ensuring that only authorized staff from the Public Record VLAN can access it.
3. Financial Server (Financial Department): Handles sensitive financial data and transactions, with strict VLAN restrictions to prevent unauthorized access from other departments.

These servers are directly connected to the Core Switch, ensuring that they provide fast and reliable services to the required VLANs while maintaining security and access control.

* In conclusion,the suggested hardware selection fully supports the ministry’s network by providing scalable, secure, and high-performance connectivity. The Cisco 3560 Multilayer Switches at the Core and Distribution Layers, Cisco 2960 Access Switches, and Cisco Access Points ensure seamless communication across buildings, floors, and departments. Additionally, the DHCP, Public Record, and Financial Servers play a crucial role in network automation, secure data storage, and resource management, making the LAN design efficient, secure, and future-proof.

b. suitability of the suggested LAN technologies

* For this network, **three LAN technologies** have been chosen to ensure **secure, fast, and reliable communication** between the **six departments and the guest area**. These technologies help solve **network congestion, IP management, and link failure issues** while improving overall efficiency.
* VLAN:

The first **LAN technology is VLAN (Virtual Local Area Network)**. VLANs are used to **separate network traffic** for each department, ensuring that data from one department **does not mix** with another. This helps **reduce congestion** and improves **security** because each department has its own **isolated network**. For example, the **Financial Department (VLAN 50) is kept separate from the Guest VLAN (VLAN 70)**, ensuring that visitors **cannot access sensitive financial records**. VLANs also allow **staff in the same department to communicate smoothly**, even if they are in **different buildings**, by routing traffic through the **Core Switch**. This setup **organizes the network efficiently** and ensures that **each department operates securely and independently**.

* DHCP:

The second **LAN technology is DHCP (Dynamic Host Configuration Protocol)**. DHCP is responsible for **automatically assigning IP addresses** to all devices in the ministry. Without DHCP, network administrators would have to **manually configure IPs** for every computer, printer, and access point, which is time-consuming and can lead to **IP conflicts**. With a **centralized DHCP server in the IT Department**, every device gets an IP address **dynamically** based on its department VLAN. This also makes it easier for employees to **move between buildings** while still receiving the correct IP address. For example, when a new employee joins the **Communication Department**, their laptop automatically **gets an IP from VLAN 40**, allowing them to connect to the network without any manual setup. This improves **efficiency, prevents errors, and simplifies network management**.

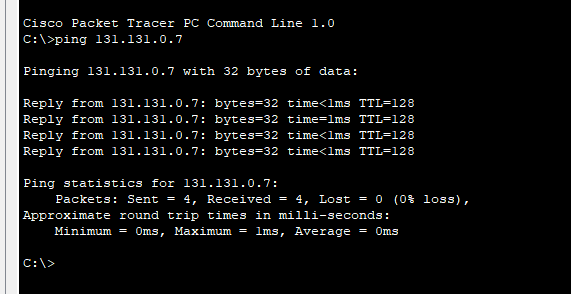
* Etherchannel:

The third **LAN technology is EtherChannel**, which is used to **increase bandwidth and improve link reliability** between the **Core Layer and Distribution Layer**. Since the ministry consists of **multiple buildings**, high-speed communication is important. EtherChannel allows **multiple physical links** between the **Core Switch and Distribution Switches** in each building to be **combined into one logical link**. This means **more data can be transferred at the same time**, reducing **bottlenecks** in the network. Additionally, if **one link fails**, traffic will **automatically switch to another available link**, ensuring that there is **no disruption in communication**. For example, if one **cable between the Core Switch and Building 2 (Administrative Department) stops working**, Etherchannel will **reroute traffic** through the remaining links, **keeping the network operational**. This improves **network speed, stability, and fault tolerance**, ensuring **smooth communication** between departments.

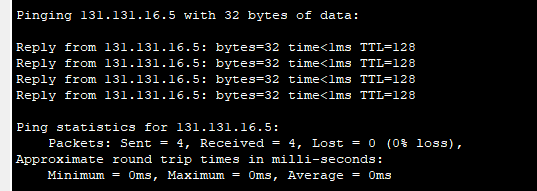
* In conclusion, these **three LAN technologies** play an important role in solving the **ministry’s network problems**. VLANs **organize the network and improve security**, DHCP **simplifies IP management**, and EtherChannel **ensures fast and reliable connections between buildings**. Together, they create a **secure, efficient, and scalable** network that supports all **departments and guest users** while maintaining **high performance and security**.

c. Connection of all staff across departments:

* All staff in the same department but in different buildings and floors are able to communicate to each other using (VLAN).



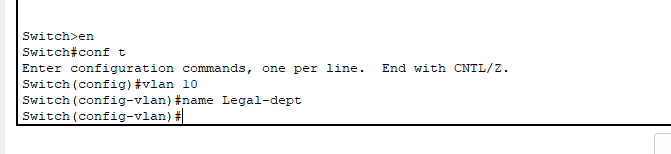
PC 13 in Legal department single storey building 1 able to communicate with PC 8 in Legal department double storey building 2.

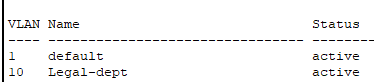


PC 18 in Administrative department double storey building 2 able to communicate with PC 4 in Administrative department double storey building 1.

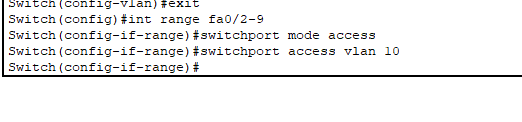
* Successfully create VLANs for the intended broadcast domain traffic

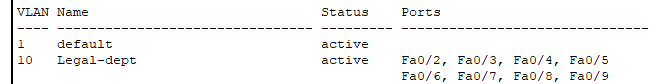
switch 1 at legal department

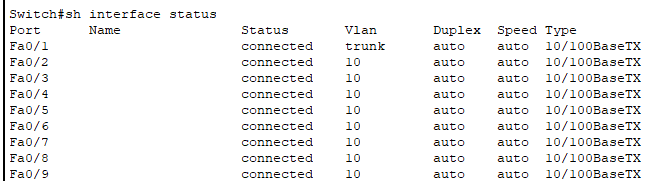




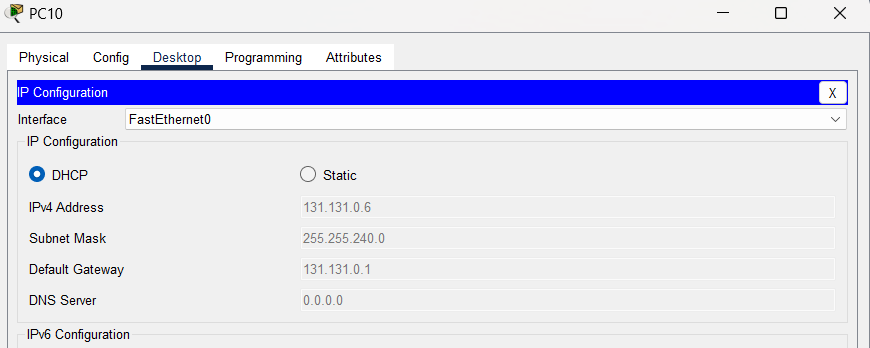
* Correctly assign ports to the created VLANs

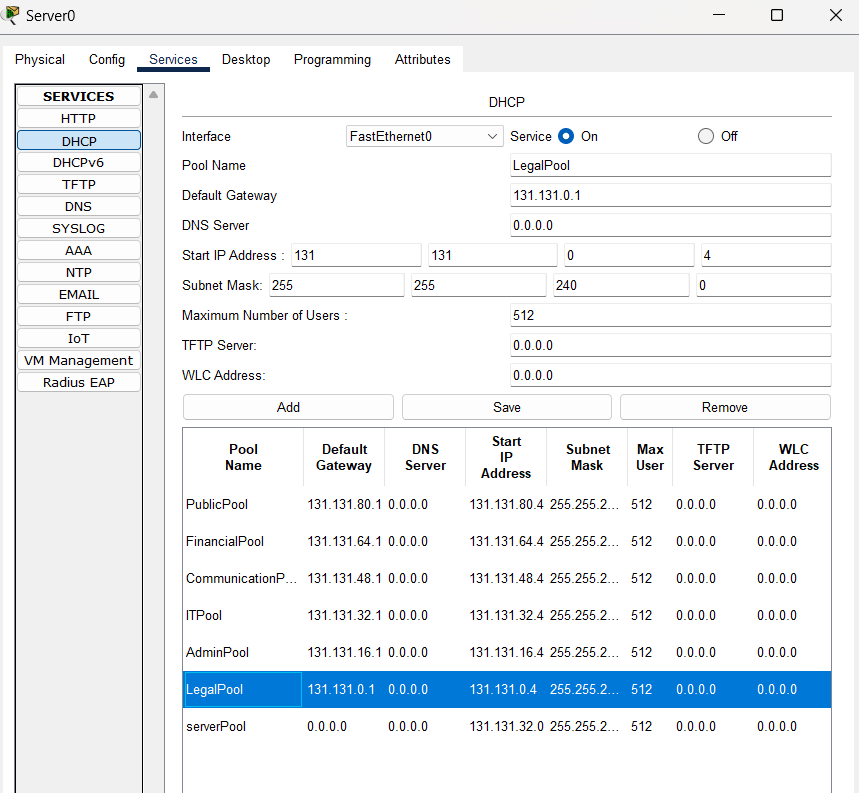






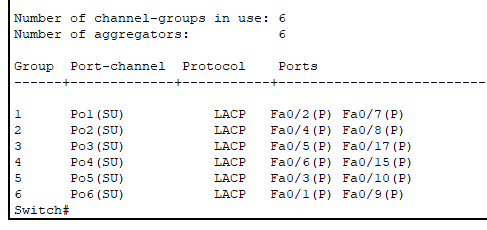
* Correctly assign subnetted IP to the created VLAN



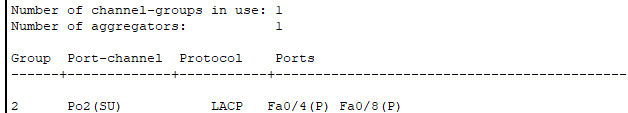


d. Connection of all staff across building.

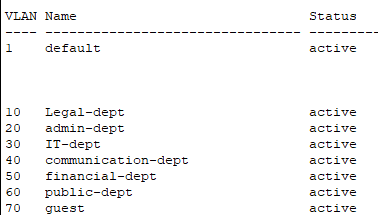
* Buildings connection

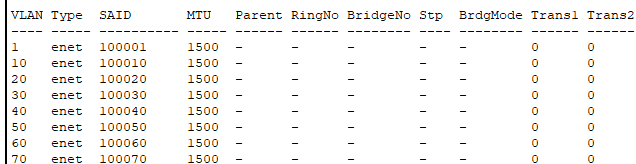


Etherchannel summary at Core switch which is at Multilayer switch 0



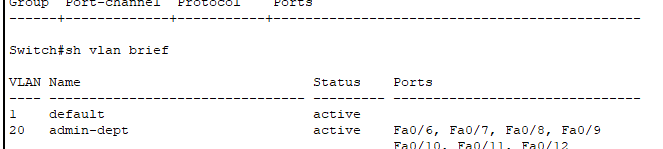
Etherchannel summary at Administrative department

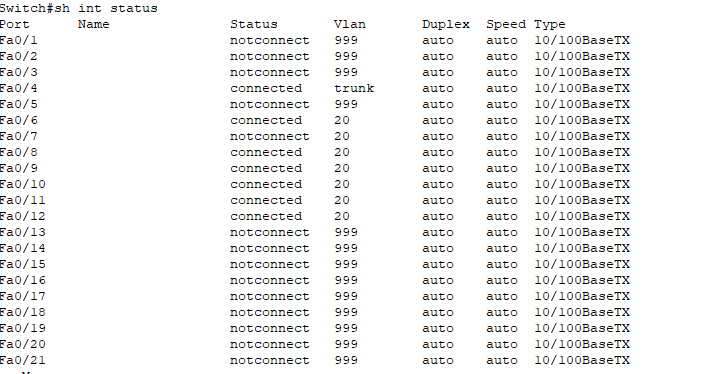




All VLANs that available in Core switch

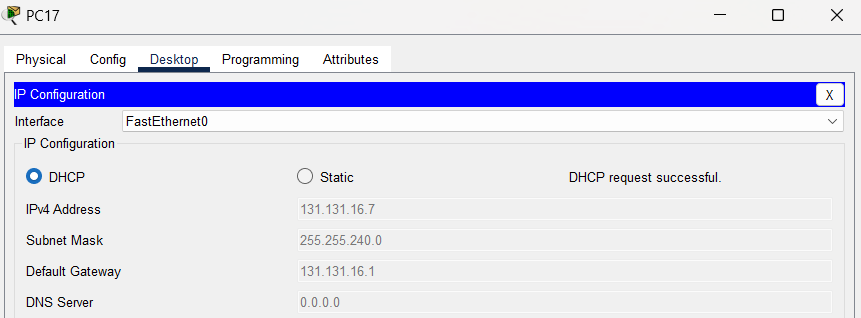
* VLAN connection



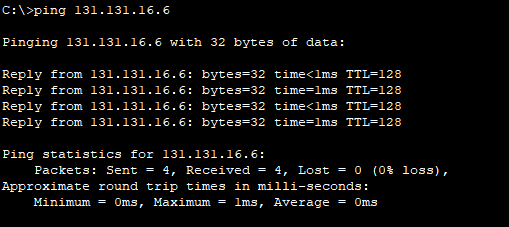


Assigned VLAN correctly to the ports

* Network devices connection

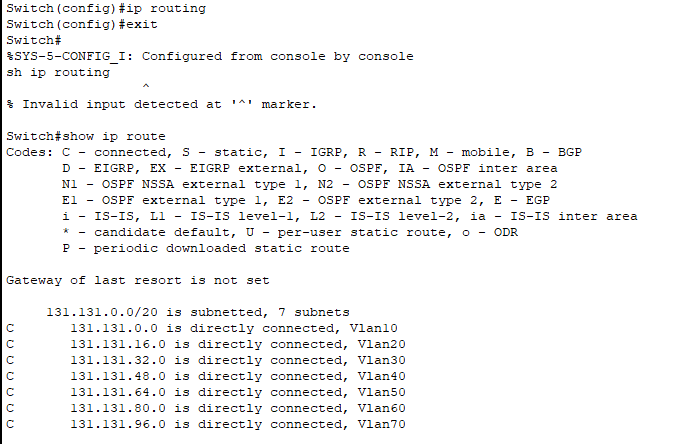


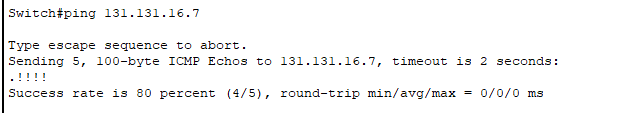
Successful DHCP request at PC 17



Ping between the PC in same department and building which are PC 17 and PC 18 at Administrative department at double storey building 1

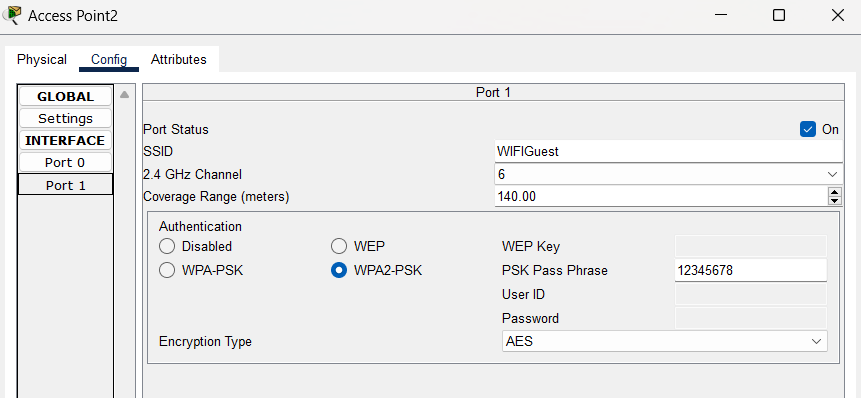
* Connection to server room



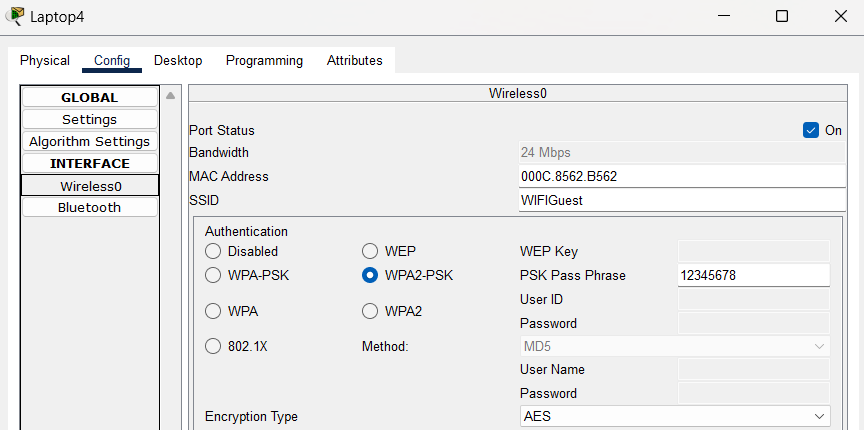


Ip routing at Core switch

* Wireless connection

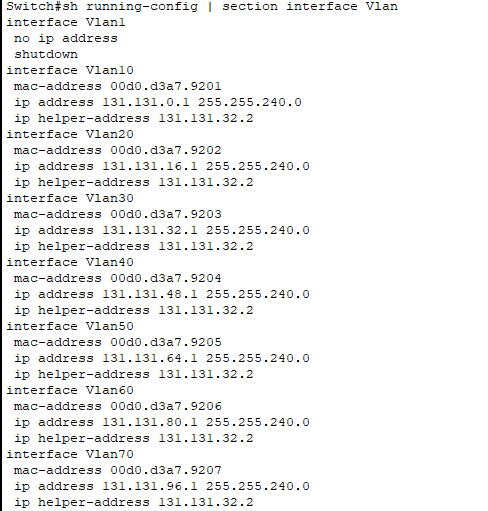


Configuration of Access Point in Guest area

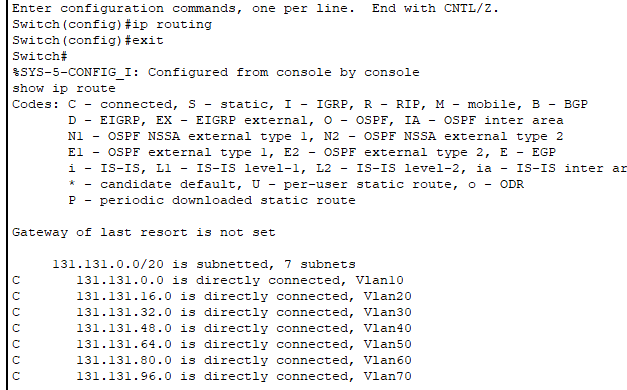


Configuration of Laptop in guest area

* Excellent IP management

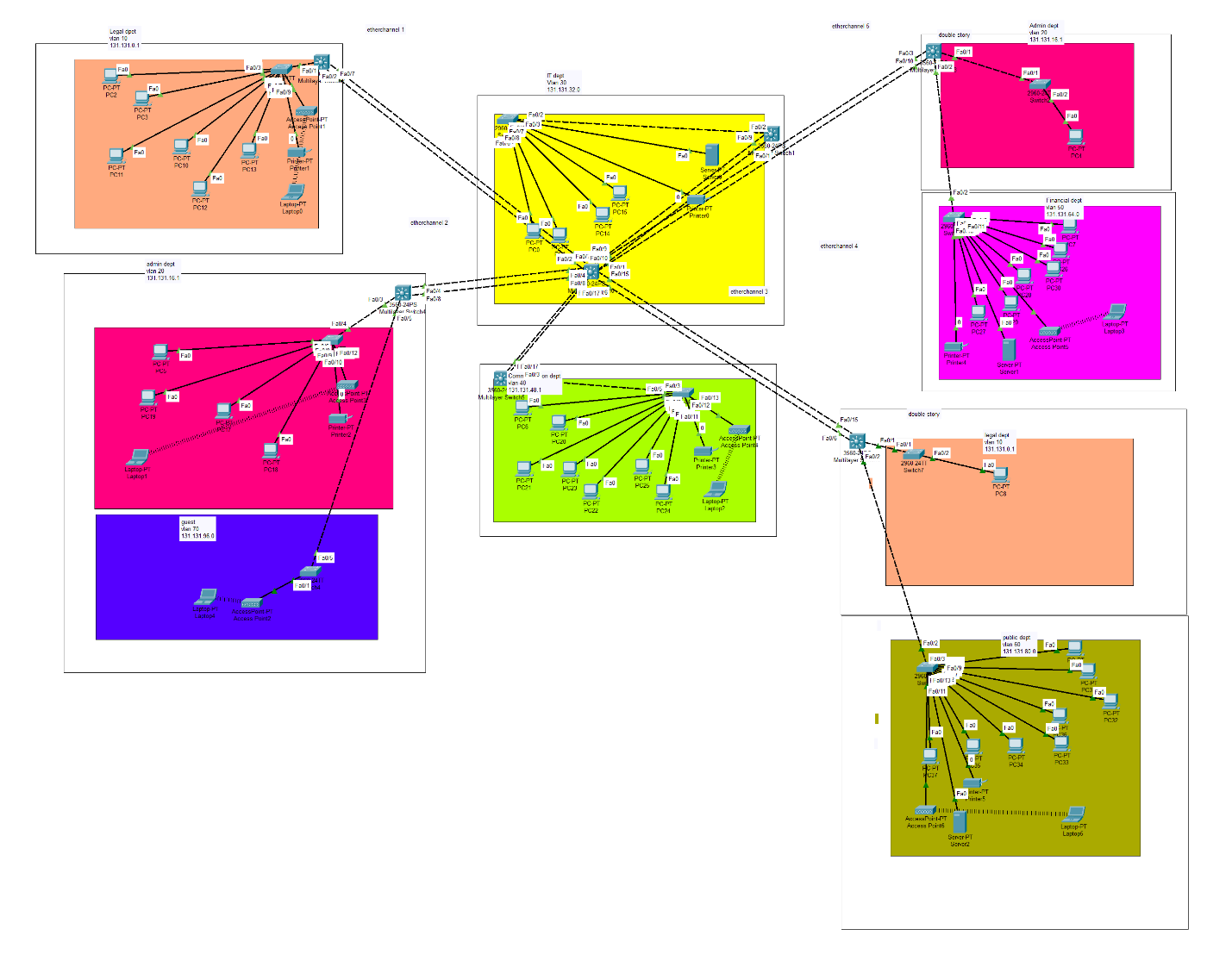


Check ip management at Core switch



Ip routing at Core switch

**Task 3: Analyse the suggested LAN design applied the hierarchical network design.**

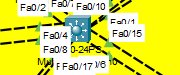


The hierarchical network design ensures secure, scalable, and efficient communication across the ministry’s six departments and guest area. This model is chosen because it improves organization, reduces congestion, supports redundancy, and allows for future expansion. By dividing the network into three layers which are Core, Distribution, and Access, by this it simplifies management, troubleshooting, and scalability. This structure ensures that each department’s VLAN is well-organized, and any troubleshooting or upgrades can be done without affecting the entire LAN.

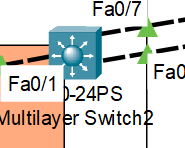
A key advantage of this design is reducing network congestion. In a flat network, all devices share one broadcast domain, causing delays and traffic overload. By using VLANs, traffic is logically separated, ensuring that broadcasts remain within their assigned department. For example, Legal VLAN 10 does not interfere with Financial VLAN 50, preventing unnecessary data from slowing down the network. The Guest VLAN 70 is also isolated, ensuring visitors can only access the internet and not internal ministry data. This setup improves speed, optimizes bandwidth, and enhances security.

Additionally, the hierarchical model prevents network failures through built-in redundancy. In a flat network, a single switch failure could disrupt the entire network. In contrast, the hierarchical model ensures backup paths. If a fiber optic link between buildings fails, traffic reroutes through an alternate path, keeping communication uninterrupted. If an Access Layer switch fails, only that department is affected, while the rest of the network remains functional. This improves reliability and minimizes downtime.

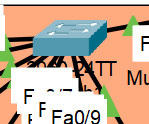
Each network layer plays a specific role in maintaining efficiency:

****

* Core Layer: Based on diagram above the core switch is located at server room, Core layer acts as the network backbone, connecting all buildings via high-speed fiber optic links. The Multilayer Core Switch handles VLAN routing and connects to the DHCP server in the IT Department, which dynamically assigns IPs to all devices.



* Distribution Layer: Based on diagram above the distribution switch is located at Legal department single storey 1. Distribution switch connects each building’s switches to the Core Layer, managing VLAN routing and traffic flow. Single-story buildings have one distribution switch, while double-story buildings have a switch per floor, ensuring floor-to-floor connectivity. This allows staff in different buildings or floors to communicate as if they were in the same location.



* Access Layer: Based on diagram above, access layer switch is located at Legal department single storey 1. It connects end-user devices (PCs, printers, Wi-Fi access points) to the network. Each department has its own VLAN and Access Switch, ensuring secure communication within departments. For example, Financial Department’s server is only accessible to VLAN 50 users.

Another key benefit of this model is scalability. If the ministry expands, new departments or staff can be added easily without redesigning the entire network. Adding a new department requires only a new VLAN, Access Switch, and connection to the Distribution Switch, making growth simple and cost-effective.

In conclusion, the 3-tier hierarchical model provides a structured, high-performance, and secure network. It reduces congestion, improves security, prevents total failures through redundancy, and allows easy future expansion. This design ensures the ministry’s network remains efficient, stable, and scalable for long-term needs.

**Task 4: By referring to the suggested LAN design, analyse the scalability of the implemented devices.**

The suggested LAN design is highly scalable, meaning that new departments, staff, and network devices can be added without major changes to the existing network. The hierarchical structure, VLAN segmentation, and high-performance network devices allow for future expansion while maintaining efficiency. First the Core Layer uses a high-performance Multilayer Switch, which acts as the main network backbone. This device supports multiple VLANs, high-speed data transfer, and inter-VLAN routing, making it capable of handling more traffic as the network grows.

Secondly, The Distribution Layer consists of managed switches in each building, which control VLAN traffic and security policies. These switches can support additional VLANs, meaning that if new departments or floors are added in ministry’s network, they can simply be assigned to a new VLAN without changing the network structure. The use of trunk links between Distribution and Core switches ensures that new VLANs can be added and managed easily.

Lastly, The Access Layer, which includes Access Switches, Wi-Fi Access Points, and end-user devices (PCs, printers, servers), is designed to support growth. If more staff are hired, new devices can simply be plugged into the existing Access Switches, and DHCP will automatically assign them an IP. Additionally, wireless expansion is possible by adding more Access Points to improve Wi-Fi coverage. For instance, if the Guest Area needs to support more users, an additional Wi-Fi AP can be installed, ensuring that more guests can connect without slowing down the network.

The suggested LAN devices are highly scalable, allowing for easy expansion without requiring a complete redesign ministry’s network. The Core Layer can handle more VLANs, the Distribution Layer supports additional buildings or floors, and the Access Layer allows for more staff and wireless users. This ensures that the ministry’s network can grow efficiently while maintaining security and performance.

**Task 5: By referring to the suggested LAN design, analyse the implemented LAN infrastructures that should fulfil the aspects of**

The suggested LAN design is structured to ensure high reliability and performance by incorporating fault-tolerance mechanisms and high-speed links. These technologies help prevent network failures, minimize downtime, and improve data transfer speeds, ensuring that all departments and buildings remain connected efficiently.

a) Fault tolerance

To enhance fault tolerance, the LAN design implements EtherChannel, a technology that combines multiple physical connections into a single logical link. This prevents network failure by ensuring redundant paths between switches and buildings. If one link fails, traffic is automatically rerouted through the remaining active links, maintaining connectivity without interruption. Without EtherChannel, a single cable failure could disconnect an entire department or building, but with this setup, network downtime is minimized. Additionally, EtherChannel supports load balancing, meaning network traffic is evenly distributed across multiple links, reducing congestion and improving overall network performance. For example, in the ministry’s LAN design, each building is connected to the Core Switch using multiple Ethernet links bundled with EtherChannel. If one link fails, the remaining links keep the building connected, preventing service disruptions for department staff.

b) High-speed links

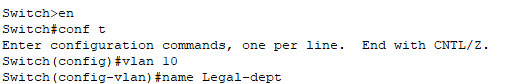
To ensure high-speed communication, the LAN design uses EtherChannel technology to aggregate multiple Ethernet connections between the Core, Distribution, and Access Layer switches. This increases bandwidth and improves data transfer speeds between buildings and departments. Instead of relying on a single Ethernet link, which could become a bottleneck, EtherChannel allows multiple links to work together, handling higher amounts of traffic efficiently. This setup is essential for ensuring smooth communication across VLANs, allowing departments to transfer data quickly without delays. For example, the IT Department’s DHCP server can efficiently assign IP addresses to all departments without slow response times, as EtherChannel helps manage traffic flow efficiently.

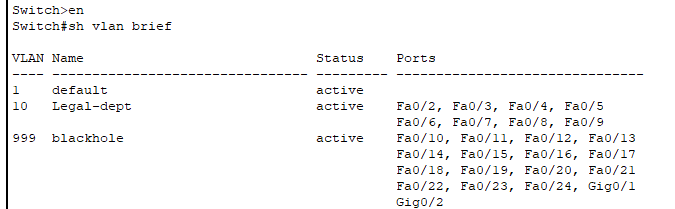
In conclusion, the fault-tolerance and high-speed link technologies used in the ministry’s LAN design significantly improve network reliability, efficiency, and scalability. EtherChannel prevents network failures by providing redundant paths, while also ensuring high-speed data transmission by combining multiple Ethernet links. Together, these technologies create a robust, high-performance network that supports the ministry’s long-term needs.

**Task 6: Choose any three (3) LAN security technologies that can be applied to the network, especially to prevent the staff from accessing confidential data on different broadcast domains in wired and wireless network traffic.**

To ensure a secure and well-protected LAN infrastructure, the ministry’s network implements multiple security technologies to prevent unauthorized access to confidential data across different VLANs in both wired and wireless networks. These security measures help protect sensitive government data, restrict staff access to only authorized VLANs, and prevent security breaches.

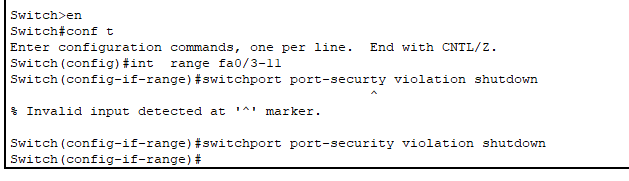
**1. VLAN Segmentation – Broadcast Domain Protection**

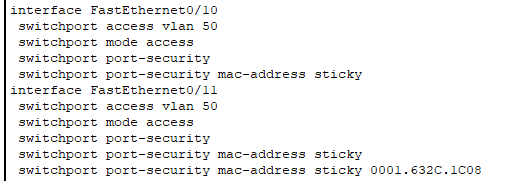




The first security measure applied is VLAN segmentation, which ensures broadcast domain protection by separating network traffic for each department. In the ministry’s LAN, each department is assigned a unique VLAN, ensuring that staff can only communicate within their own department unless explicitly allowed. Without VLANs, all users would be on the same broadcast domain, meaning staff from one department could access resources from another department. VLAN segmentation prevents this by logically isolating different departments, ensuring that Legal Department staff cannot access Financial Department files, and IT staff cannot access Public Record data unless explicitly authorized. Example Legal Department (VLAN 10) cannot communicate with Financial Department (VLAN 50) unless inter-VLAN routing is enabled.

**2. Port security (violation shutdown) – Access Mode Protection**





The second security measure is Port Security (Violation Shutdown), which ensures access mode protection at the Access Layer switches. Each department has a dedicated VLAN, meaning that only authorized devices should be able to connect to department network ports. Port security restricts each switch port to only allow a specific number of MAC addresses. If an unauthorized device connects to a port, the switch automatically shuts down the port, preventing unauthorized access. This is especially important in sensitive departments such as the Financial and Public Record Departments, where confidential government data must be protected.

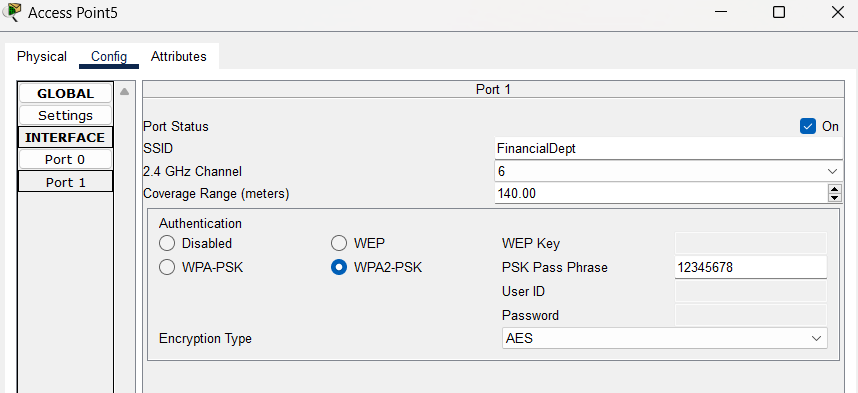
**3. Switchport nonegotiate – Trunk mode protection**

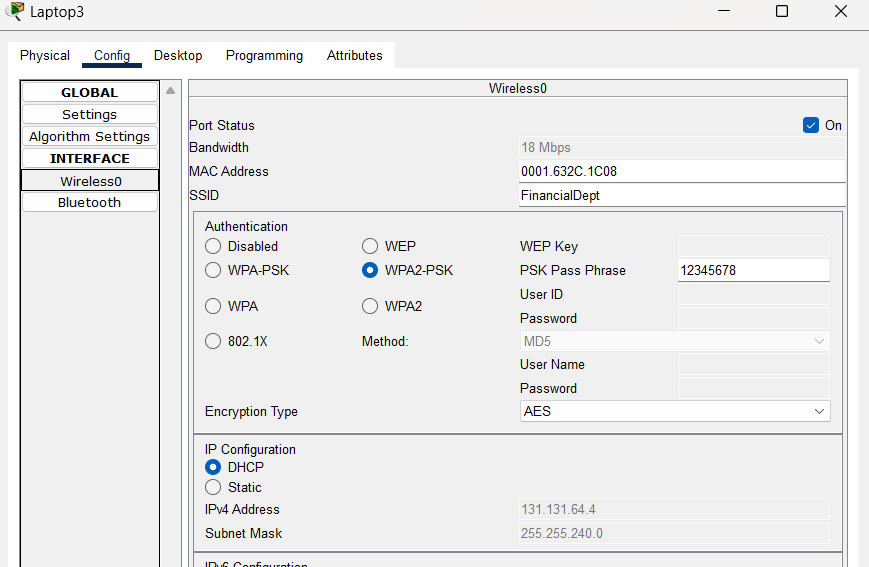


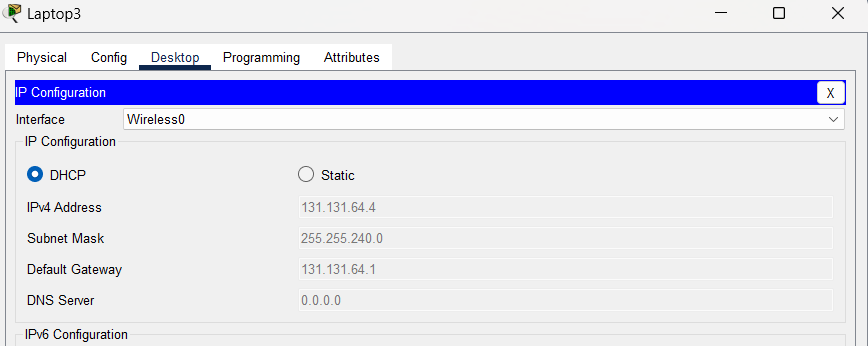


The third security measure is switchport nonegotiate, which provides trunk mode protection by disabling Dynamic Trunking Protocol (DTP) on all trunk ports between Core, Distribution, and Access Layer switches. Without this configuration, an attacker could force a switch into trunk mode, gaining access to multiple VLANs and potentially intercepting sensitive ministry data. By manually configuring trunk ports and disabling negotiation, only authorized VLANs can pass through, ensuring that department traffic remains isolated and secure.

**4. WPA 2 – Wireless LAN security**







For wireless LAN security, WPA2 encryption is implemented on all Access Points (APs) to protect wireless traffic from unauthorized access. Since some ministry departments rely on Wi-Fi for connectivity, enforcing strong encryption ensures that only authorized personnel can access the network. Additionally, the Guest VLAN (VLAN 70) is completely isolated from internal ministry networks, ensuring that visitors can only access the internet and not government resources.

In conclusion, the ministry’s LAN security strategy effectively prevents unauthorized access to confidential data across different broadcast domains in both wired and wireless networks. By implementing VLAN segmentation, port security, trunk mode protection, and WPA2 encryption, the network ensures that staff can only access authorized resources within their own department while restricting access to sensitive information from other departments. VLAN segmentation isolates network traffic, preventing unauthorized cross-department communication, while port security (violation shutdown) ensures that only authorized devices can connect to the network. Additionally, switchport nonegotiate secures trunk links by preventing unauthorized VLAN access, and WPA2 encryption protects wireless connections, ensuring that only verified users can access the ministry’s Wi-Fi. These security measures work together to maintain a safe, efficient, and controlled network environment, ensuring data integrity and confidentiality while preventing potential security breaches.

**Task 7: With relation to the suggested LAN technologies analysed in Task 2, analyse the suitability of the suggested LAN technologies for handling the ministry network problems.**

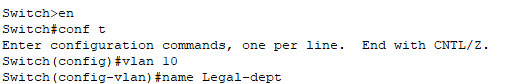
**1. VLAN**

**Suitability Analysis: Reasons using VLANs**

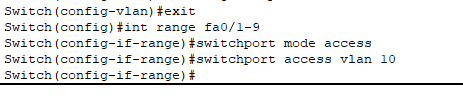
VLANs help segment department networks, ensuring that staff from different departments cannot access each other’s data unless authorized. This improves security, reduces congestion, and organizes network traffic. For example, Legal department cannot access data from Public Record department

Configuration creating VLAN :

* Step 1: First go to access switch at department that want to configure
* Step 2: Create VLAN by give VLAN ID and VLAN name



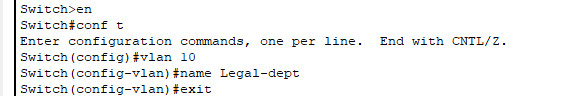
* Step 3: Assign port that are use in the department to VLAN



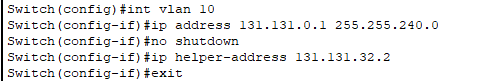
* Step 4: Set mode trunk to port where it connected to Distribution switch



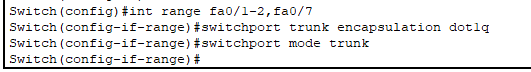
* Step 5: Now setup VLAN at Distribution and Core layer switch, go to multilayer switch for Distribution layer and Core layer
* Step 6: Then create VLAN by assign VLAN ID and VLAN name



* Step 7: After that go to VLAN interface to assign IP address and IP helper-address. IP helper-address is based on IP address assign at server that have DHCP service.

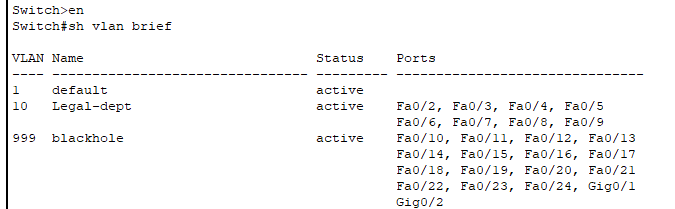


* Step 8: Now assign port that connected to access switch and multilayer switch to trunk mode

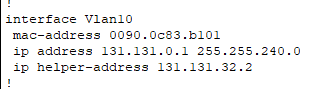


Note that the step that apply at Distribution layer switch is exactly same to configuration VLAN at Core layer switch

* Step 9: Check if the VLAN is successfully created at Access layer switch



* Step 10: Check if VLAN is successfully created at Core and Distribution layer switch





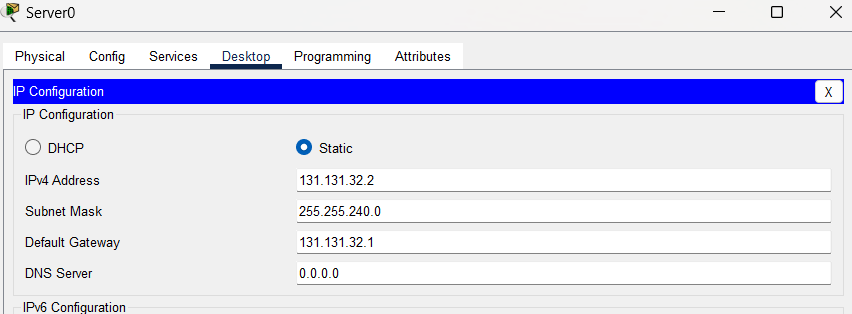
**2. DHCP server**

**Suitability Analysis: Reasons using DHCP**

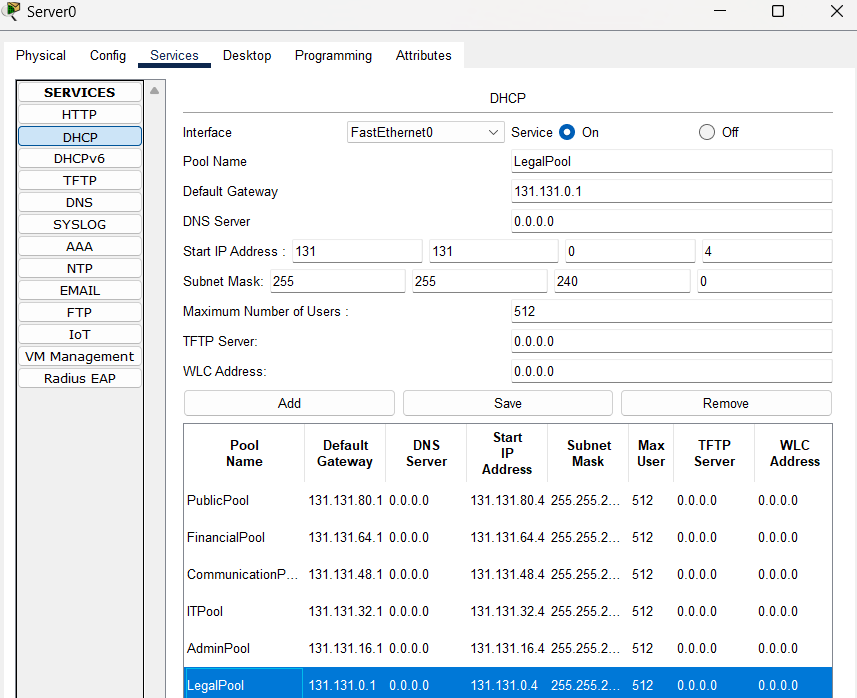
The DHCP server in the IT Department ensures that all devices receive dynamic IP addresses automatically. This eliminates manual IP configuration, prevents conflicts, and simplifies network management.

Configuration DHCP

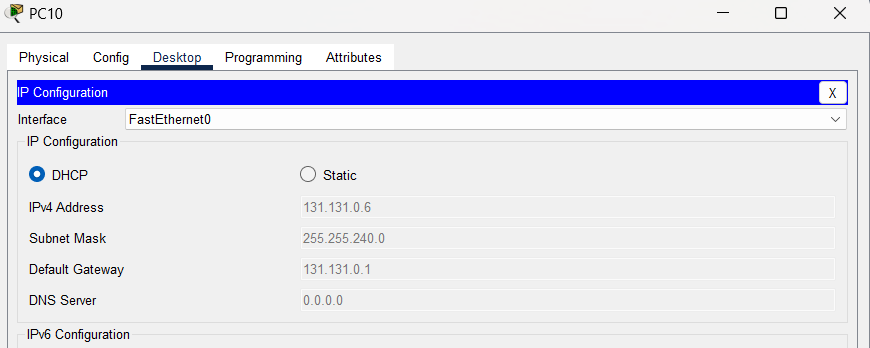
* Step 1: Assign IP address and default gateway to DHCP server. The IP address is assign based VLAN where the server at and same goes to default gateway.



* Step 2: Create IP pool, by fill in pool name, default gateway, start IP address, subnet mask the save. Those things that need to be fill up is based on VLAN created. Example VLAN 10



* Step 3: Lastly check if DHCP request is successful



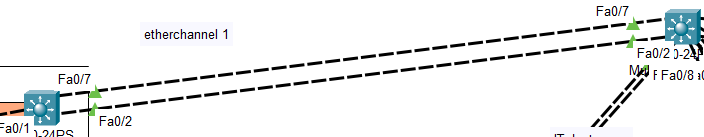
**3. Etherchannel**

**Suitability Analysis: Reasons using EtherChannel**

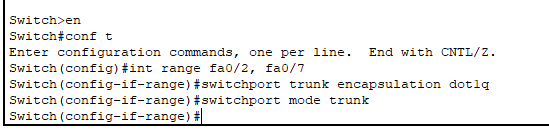
EtherChannel bundles multiple links between Core and Distribution switches, improving bandwidth, redundancy, and preventing single points of failure.

Configuration Etherchannel

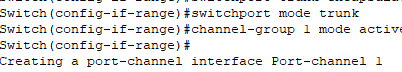
* Step 1: Connect two cables between Core layer switch and Distribution layer switch



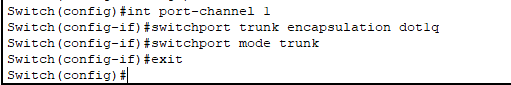
* Step 2: Setup trunk mode for each port that are used for EtherChannel. Based on diagram both Core and Distribution layer switch use port fa0/7 and fa0/2.



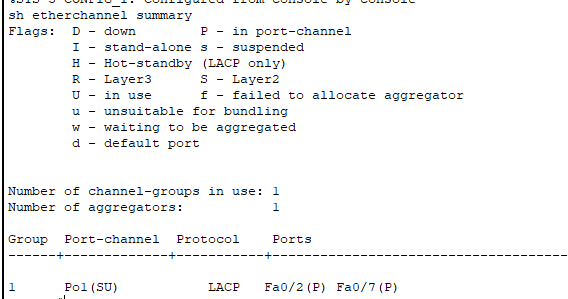
* Step 3: Go to interface of port that are use for etherchannel and create etherchannel. Here etherchannel group 1 is created



* Step 4: Lastly set the etherchannel into trunk mode



* Step 5: Check if the etherchannel is successfully created



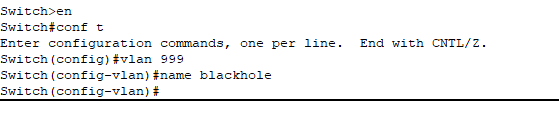
**4. Black hole**

**Suitability Analysis: Reasons using Blackhole VLAN**

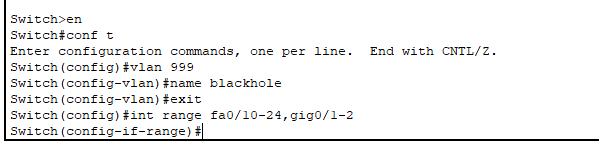
Unused switch ports must be assigned to a Blackhole VLAN to prevent unauthorized connections or rogue device access.

Configuration blackhole

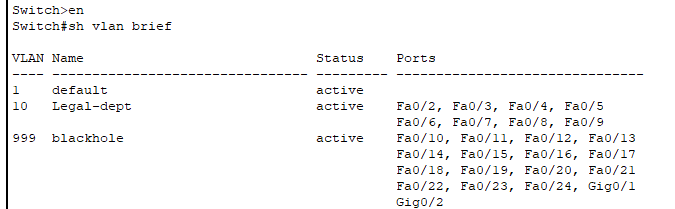
* Step 1: Go access layer switch and identify which port is not use or port that assign to VLAN 1
* Step 2: Create blackhole VLAN by assign VLAN ID and VLAN name



* Step 3: Go to interface port that are not use or that is assign to VLAN 1, then assign all the port to VLAN blackhole



* Step 4: Now check if the blackhole is successfully created and assigned to unused port or port that assign to VLAN 1



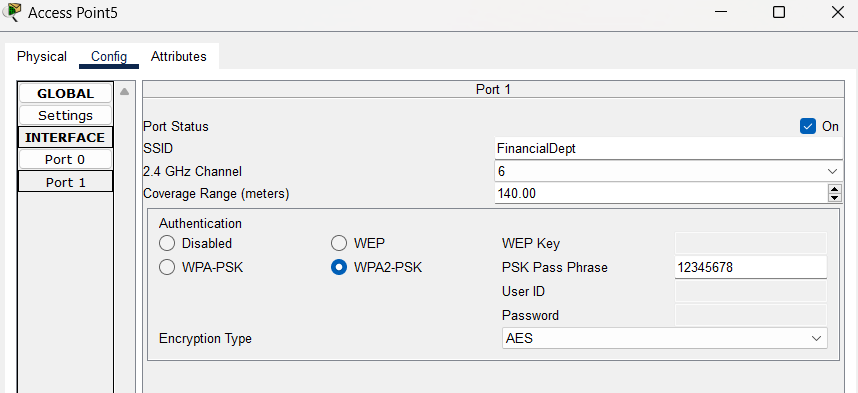
**5. WPA 2 wireless security**

**Suitability Analysis: Reasons using WPA2**

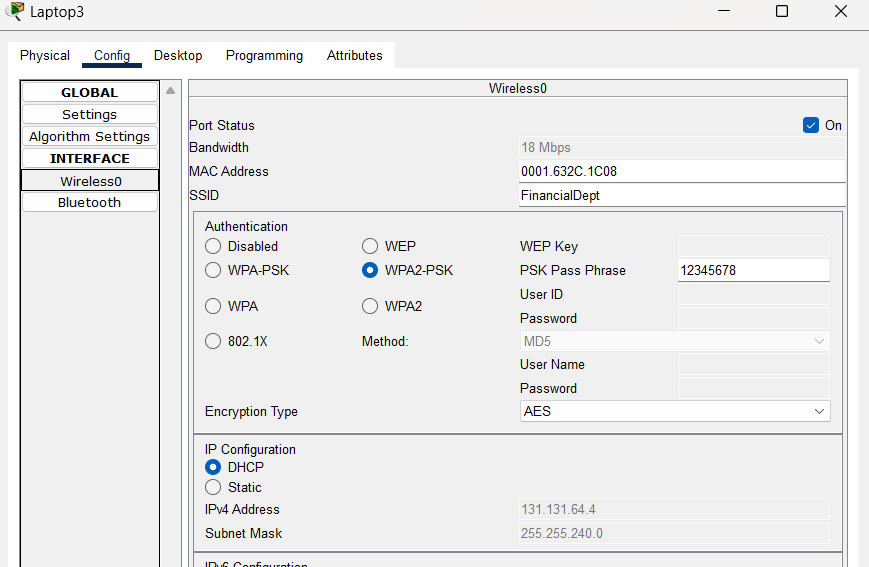
WPA2 ensures secure Wi-Fi access, preventing unauthorized users from accessing the ministry’s wireless network.

Configuration WPA2

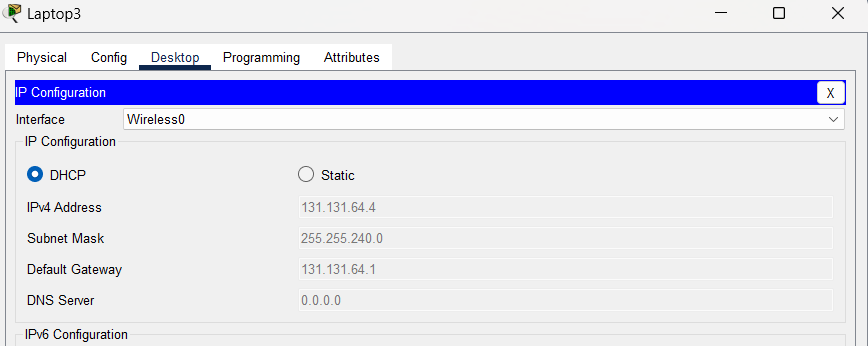
* Step 1: Configure Access Point by assign SSID, choose WPA2-PSK and assign PSK Pass Phrase



* Step 2: Connect one device to Access Point by wireless. Choose WPA2-PSK, the fill in the SSID and PSK Pass Phrase.



* Step 3: Check if connection is successful by monitor the DHCP IP addressing.



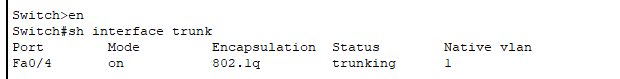
**6. Nonegotiate:**

**Suitability Analysis: Reasons using Nonegotiate**

By default, switches negotiate trunking using DTP (Dynamic Trunking Protocol), which can be exploited. Manually setting trunk mode and disabling negotiation prevents VLAN hopping attacks.

Configurations nonegotiate

* Step 1: Choose port that is in trunk mode. Us show interface trunk



* Step 2: Then assign it to nonegotiate



* Step 3: Check if nonegotiate is successfully applied using command “show running-config | include interface|switchport”



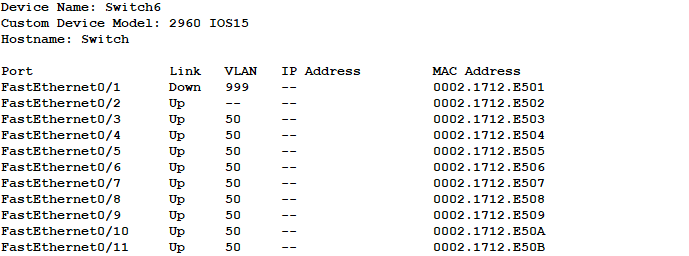
**7. Violation shutdown:**

**Suitability Analysis: Reasons using Violation Shutdown**

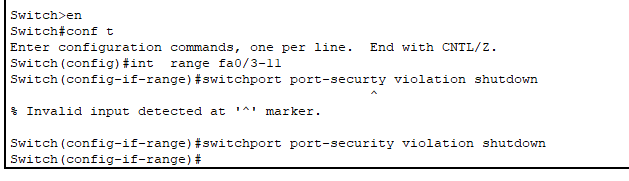
Port security restricts unauthorized MAC addresses from connecting. If a violating device is detected, the port is shut down to prevent unauthorized access.

Configurations violation shutdown

* Step 1: Analysis which port has been assign to specific VLAN, example VLAN 50



* Step 2: Go to switch and go inside all interface that use VLAN 50 for example. Then set to switchport port-security violation shutdown



* Step 3: Then monitor if switchport port-security violation shutdown is successfully applied.Using “show running-config | include interface|switchport”

