NETWORK DESIGN PROPOSAL FOR AIRPORT

TEAM MEMBERS:

PIYUSH PRAKASH(RA2211003011274)

HARSHINI KASTURI(RA2211003011299)

LATHIKA KOMMINENI(RA2211003011310)

CHETNA RAJEEV(RA2211003011314)

INTRODUCTION

Airports are complex, high-security environments that rely on sophisticated networking solutions to ensure efficient operations and data security across multiple departments. As critical infrastructure, they depend on technology to manage administrative functions, flight operations, and guest services. **This project outlines a network proposal for an airport with three main user groups: Airport Authority, Flight Service Providers, and Guests.** Each has distinct needs: the Airport Authority requires a secure network for managing flight operations; Flight Service Providers need controlled access to specific airport resources; and Guests require high-speed wireless internet that is isolated from the other networks. Automatic IP allocation through DHCP and a shared password for guest Wi-Fi ensure ease of use while maintaining security. This network structure balances security, accessibility, and performance, supporting modern airport functions.

OBJECTIVES

The primary objective of this project is to design a secure and efficient network infrastructure tailored to the needs of an airport environment.

1. **Design a Secure Network Architecture**
2. **Implement Controlled Access for Flight Service Providers**
3. **Provide High-Speed Internet for Guests**
4. **Enable Automatic IP Allocation**
5. **Ensure Network Scalability and Performance**

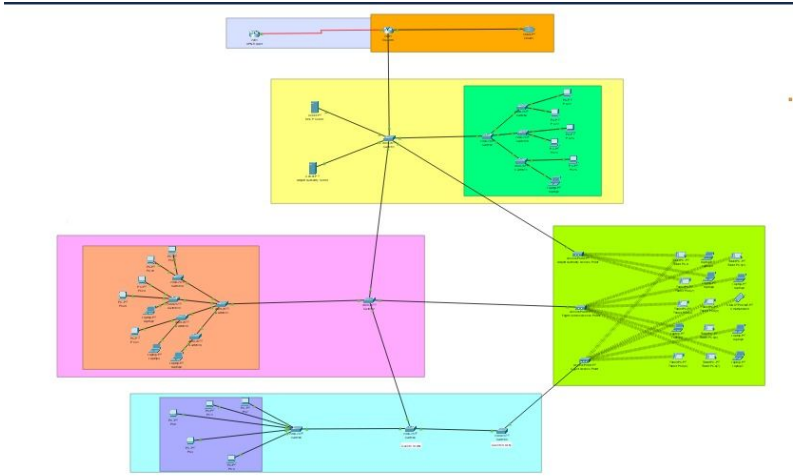
NETWORK DESIGN

The network topology primarily follows a **hybrid structure**, combining features of both **star and extended bus topologies to enhance security, facilitate segmented traffic flow, and ensure scalability.**

Star Topology: Each switch creates a star topology for its respective department, with all connected PCs and devices within that VLAN linked directly to the switch.

Extended Bus Topology: The core router extends this bus layout by connecting all switches through trunk links, allowing each VLAN to maintain its distinct traffic channel but still interconnect for cross-departmental communication.

This hybrid topology is ideal for an airport setup because it promotes both scalability and security while segmenting network traffic based on departmental needs.



NETWORK DESIGN COMPONENTS

Network Components Overview

- **Switches**: Switches manage departmental VLANs (Airport Authority: VLAN 2, Flight Services: VLAN 3, Guest Users: VLAN 4) to segment traffic, improving security and performance. They facilitate controlled inter-VLAN routing through trunk links to the router.

- **Router**: The router handles inter-VLAN communication, applies access control policies, and routes traffic between departments. It also manages NAT for internet access, acting as both internal and external gateway. Additionally, the router is responsible for maintaining VPN (Virtual Private Network) connectivity, enabling secure remote access for authorized users.

- **Access Points**: Wireless access points provide internet access to all users, with a shared password. They connect to the all the three VLANs and use DHCP to assign IP addresses.

- **DHCP Server**: The DHCP server automates IP address assignment across VLANs, ensuring devices receive correct configurations for seamless connectivity and efficient network management.

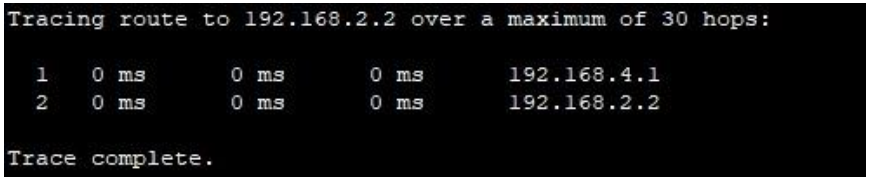
DHCP VLAN POOL CONFIGURATION

VLAN	VLAN Subnet	DHCP Pool Name	Range of IP Addresses	Gateway IP Address	DNS Server IP	Description
VLAN 2	`192.168.2.0/24`	`VLAN2-Pool`	`192.168.2.2 - 192.168.2.100`	`192.168.2.1`	`192.168.2.1`	DHCP Pool for Airport Authority (VLAN 2)
VLAN 3	`192.168.3.0/24`	`VLAN3-Pool`	`192.168.3.2 - 192.168.3.100`	`192.168.3.1`	`192.168.3.1`	DHCP Pool for Flight Service Providers (VLAN 3)
VLAN 4	`192.168.4.0/24`	`VLAN4-Pool`	`192.168.4.2 - 192.168.4.100`	`192.168.4.1`	`192.168.4.1`	DHCP Pool for Guests (VLAN 4)

TESTING AND VALIDATION

Packet Tracer was utilized to simulate and test the designed network. Packet Tracer is a network simulation tool that provides a virtual environment for designing, configuring, and testing network scenarios. The simulation process involves:

- **Network Topology Design:** The network topology, including routers, switches, PCs, servers, and other devices, was designed within Packet Tracer based on the specified requirements.



- **Configuration Implementation:** Using the designed topology, configurations were implemented on routers, switches, and other network devices according to the provided guidelines. Cisco Packet Tracer allows users to configure devices with a user-friendly interface similar to actual Cisco devices.
- **DHCP and IP Address Allocation:** Dynamic Host Configuration Protocol (DHCP) functionality and IP address allocation were tested to ensure that devices received the correct IP addresses dynamically and that devices in the server room had static IP assignments.

CONCLUSION AND FUTURE WORK

The proposed network design provides a secure, scalable, and efficient solution for airport operations. Using a hybrid star topology and VLAN segmentation, the network ensures isolated yet interconnected departmental traffic, enhancing both security and manageability. Access Control Lists (ACLs) and a centralized DHCP server streamline network management and support effortless device connectivity. With dedicated VLANs and IP ranges, this design meets current needs while supporting future expansion, ensuring reliable performance, data security, and high-speed connectivity.

Lessons Learned

- **Network Segmentation**: VLANs and ACLs are essential for secure, isolated departmental traffic and preventing unauthorized access.
- **Scalable, Flexible Topology**: The hybrid star design supports growth and adapts to future needs without disruption.
- **Efficient IP Management**: DHCP automatic IP assignment, reducing errors and streamlining management, especially for high-traffic guest areas.
- **Security vs. Accessibility**: Balancing security for internal operations with accessible guest access is key.
- **Future-Proof Design**: A scalable structure ensures the network can meet evolving requirements, minimizing costly redesigns.

REFERENCES

- Cisco Systems, Inc. (2020). Cisco Networking Basics: A Comprehensive Guide to Networking Fundamentals. Cisco Press.
- Tan, K. (2021). Network Design and Implementation: A Guide to Best Practices. Wiley & Sons.
- Cisco Systems, Inc. (2019). Configuring VLANs and Inter-VLAN Routing in Cisco Packet Tracer. Cisco Networking Academy.
- Cisco Systems, Inc. (2022). Configuring DHCP on Cisco Routers and Switches. Cisco Documentation. Retrieved from: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/xe-3s/iad-xe-3s-book/
- Baker, P. (2018). Designing Enterprise Networks: Principles and Best Practices. Pearson Education.
- Cai, D., & Li, Y. (2020). Implementing Secure Network Infrastructure: A Practical Guide to Security Protocols and Strategies. Springer.
- Cisco Systems, Inc. (2022). Configuring DHCP on Cisco Routers and Switches. Cisco Documentation. Retrieved from: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/xe-3s/iad-xe-3s-book/
- Hughes, C., & Stepanek, M. (2019). Understanding and Implementing Network Security Solutions. McGraw-Hill Education.

THANK YOU