Final Report

ANZ Bank's network expansion project

Project producer: Shuyi Huang

Table of Contents

Abstract

This report presents the design and implementation of ANZ Bank's network expansion project, focusing on the establishment of a secure, reliable, and scalable network infrastructure to support the bank's operations across new remote sub-banks in Sydney, Darwin, and Perth. The project encompasses the development of the HQ LAN, Remote1 LAN, and Remote2 LAN (IoT), each tailored to meet specific operational requirements and enhance the bank's service delivery.

Introduction

a. Background

ANZ Bank is extending its network by establishing new branches in various locations. This expansion requires a robust and secure network infrastructure to support daily banking operations and enhance customer service. The network ensures high availability, security, and scalability to meet the bank's future needs.

b. Literature review

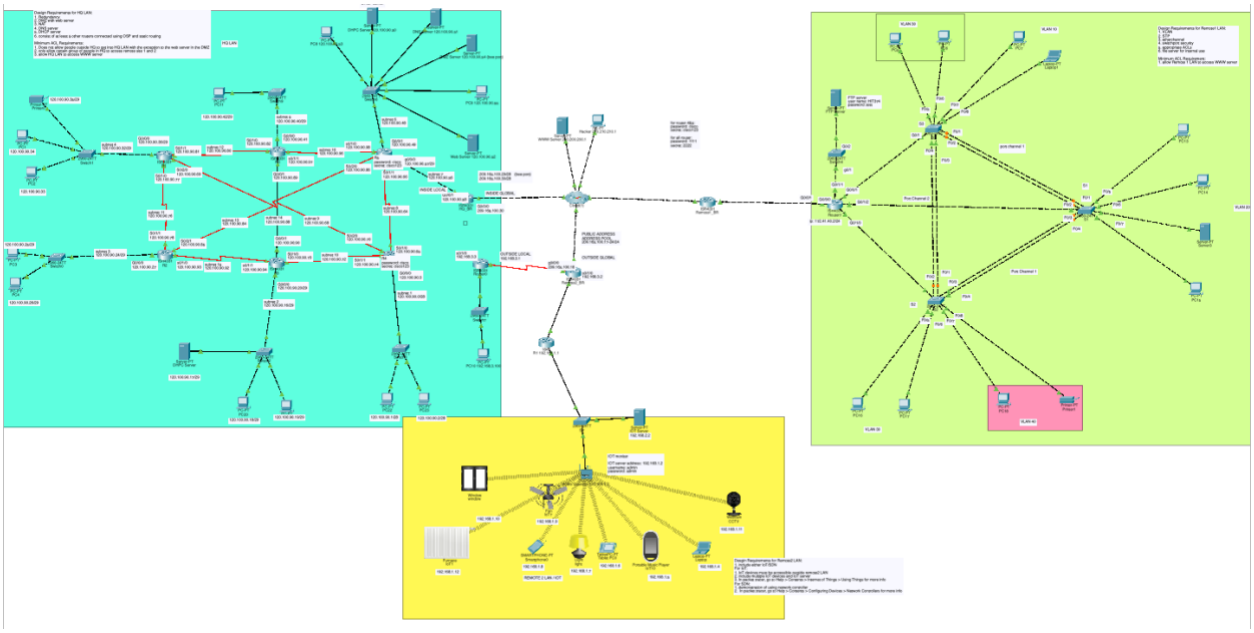
IoT and SDN technologies are pivotal for the bank's network. IoT enhances customer service through automation and data collection, essential for modern banking. It supports advanced services like smart ATMs and queue management. However, IoT also presents security challenges, necessitating robust security frameworks (Chataut et al., 2023). SDN offers network programmability and centralization, beneficial for managing network traffic and security indicated by Farooq (et al., 2023), though it does not directly enhance customer-facing services as IoT does.

c. Aim and Scope

The project aims to design and implement a network that ensures high availability, security, and performance for ANZ Bank's operations. It must protect sensitive data, be scalable for future growth, and accommodate technological advances, maintaining agility in a competitive financial industry.

Design

a. Topology



b. Description

HQ LAN

1. Redundancy

Redundancy is a critical aspect of the HQ LAN design, aimed at ensuring continuous network availability and preventing service disruptions. The network incorporates multiple interconnected routers with failover capabilities. If one router fails, the traffic is automatically redirected to another router, maintaining seamless network operations. This redundancy is essential for a banking environment that requires 24/7 uptime to support transactions, customer services, and internal operations.

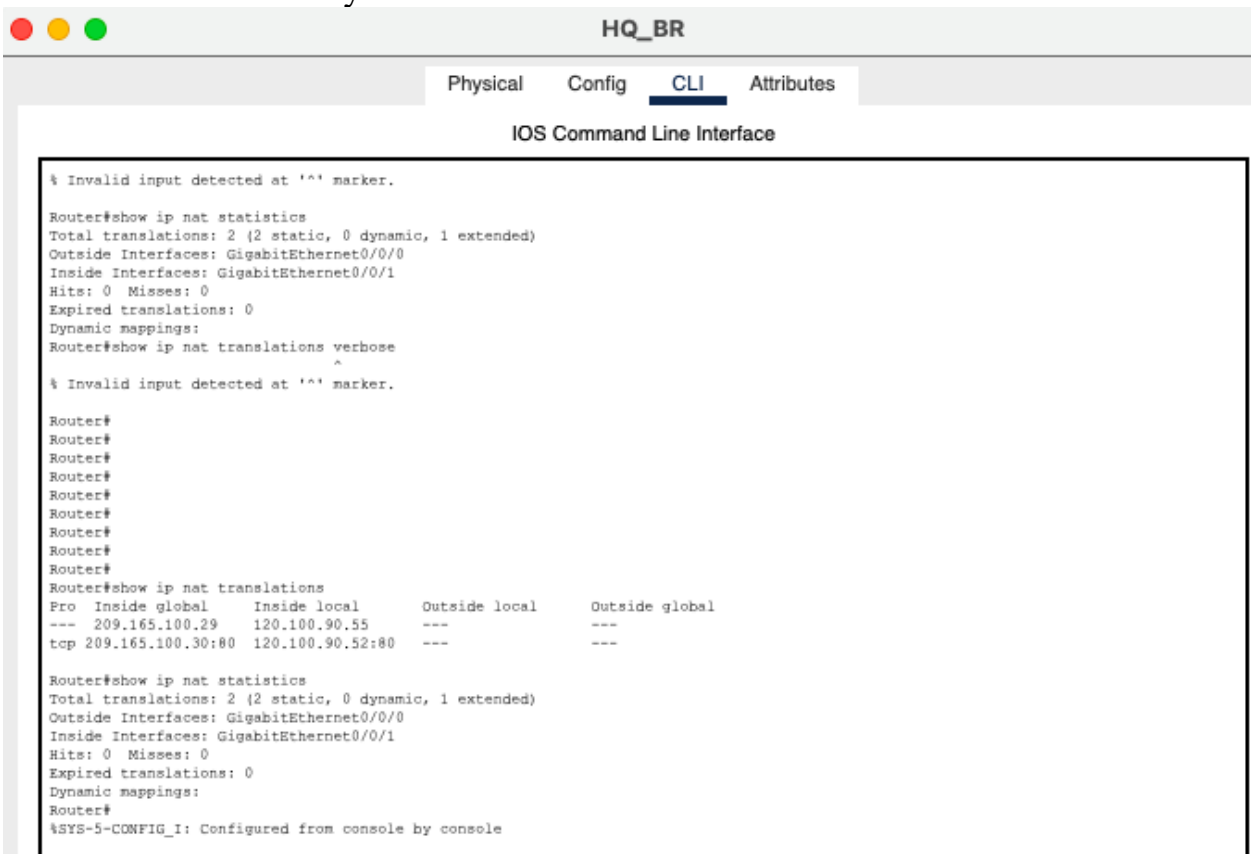
2. DMZ with Web Server

The Demilitarized Zone (DMZ) hosts a web server that allows external users to access certain services without exposing the internal network to potential threats.

The DMZ acts as a buffer zone between the external internet and the internal network, providing an additional layer of security. The web server within the DMZ is accessible to the public while keeping the internal systems isolated and protected. This setup is crucial for hosting services such as online banking applications, ensuring they are available to customers while maintaining the security of the bank's internal network.

3. Network Address Translation (NAT)

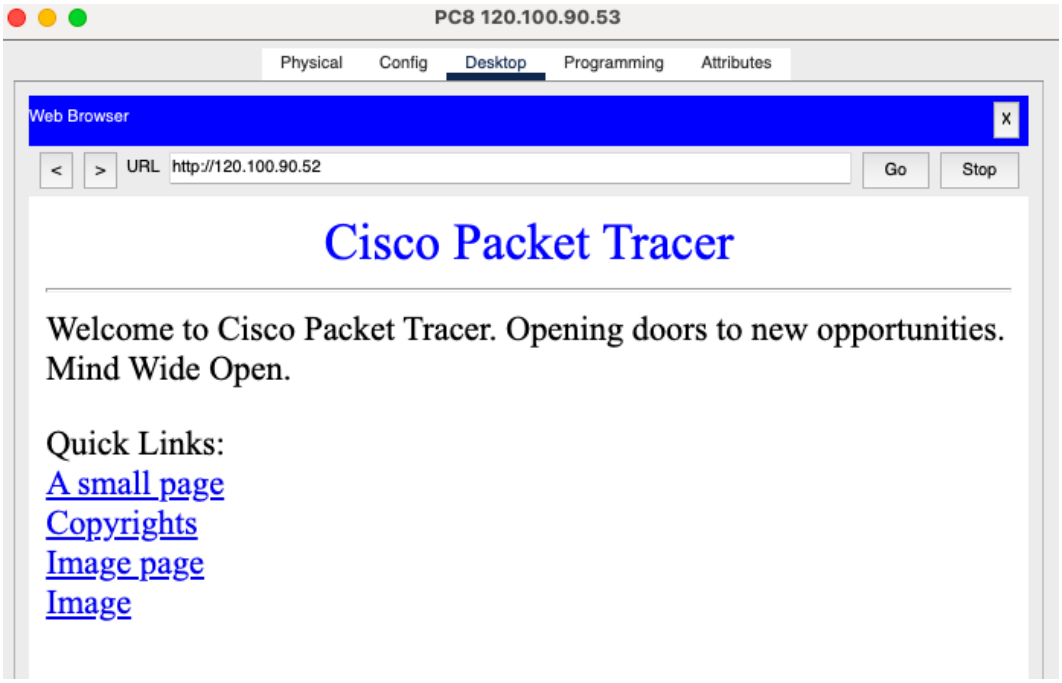
Network Address Translation (NAT) is used to mask the internal IP addresses of the HQ LAN, providing an additional layer of security. NAT translates private internal IP addresses to a public IP address for external communication. This not only conserves public IP addresses but also hides the internal network structure from external entities, making it more difficult for potential attackers to target internal devices directly.



4. Domain Name System (DNS) Server

The DNS Server within the HQ LAN supports internal network navigation by resolving human-readable domain names to IP addresses. This server is crucial for the efficient functioning of network services, allowing users and applications to easily locate and communicate with other devices and services within the network. The DNS server ensures that internal resources are accessible and that network operations are smooth and efficient.

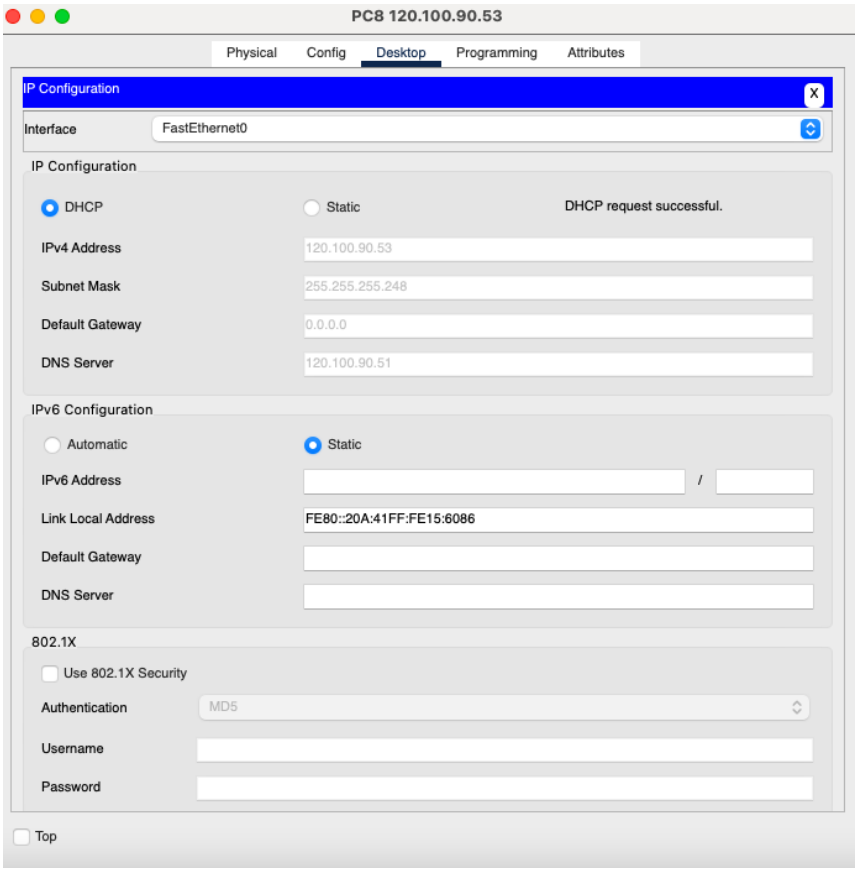
Conect by web record name



Connect by ip address

5. Dynamic Host Configuration Protocol (DHCP) Server

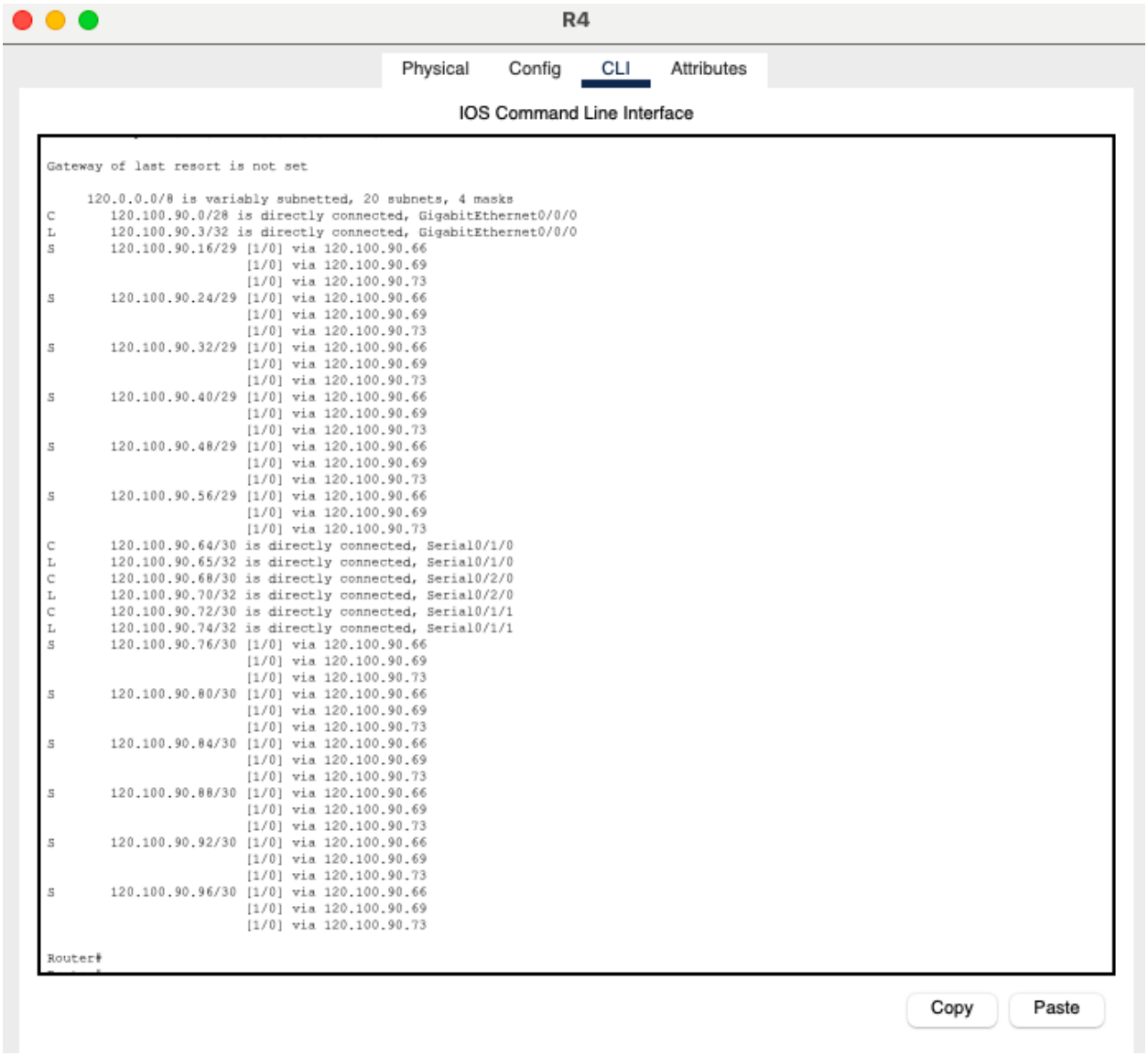
The DHCP Server automates the assignment of IP addresses to devices within the HQ LAN. This server dynamically allocates IP addresses, reducing the administrative burden of manual IP address management. The DHCP server ensures that each device has a unique IP address and can communicate effectively within the network. This automation is essential for maintaining an organized and efficient network environment.



DHCP auto contect

6. Six Routers Connected Using OSPF and Static Routing

The HQ LAN features six interconnected routers configured with both Open Shortest Path First (OSPF) and static routing protocols. OSPF is used for dynamic routing, allowing the routers to exchange routing information and automatically adjust to changes in the network topology. This ensures optimal path selection and efficient data transmission. In addition to OSPF, static routing is employed for specific, predefined routes to enhance control and stability in the network. The combination of OSPF and static routing ensures that the network is both dynamic and reliable, providing robust connectivity for the bank's operations.



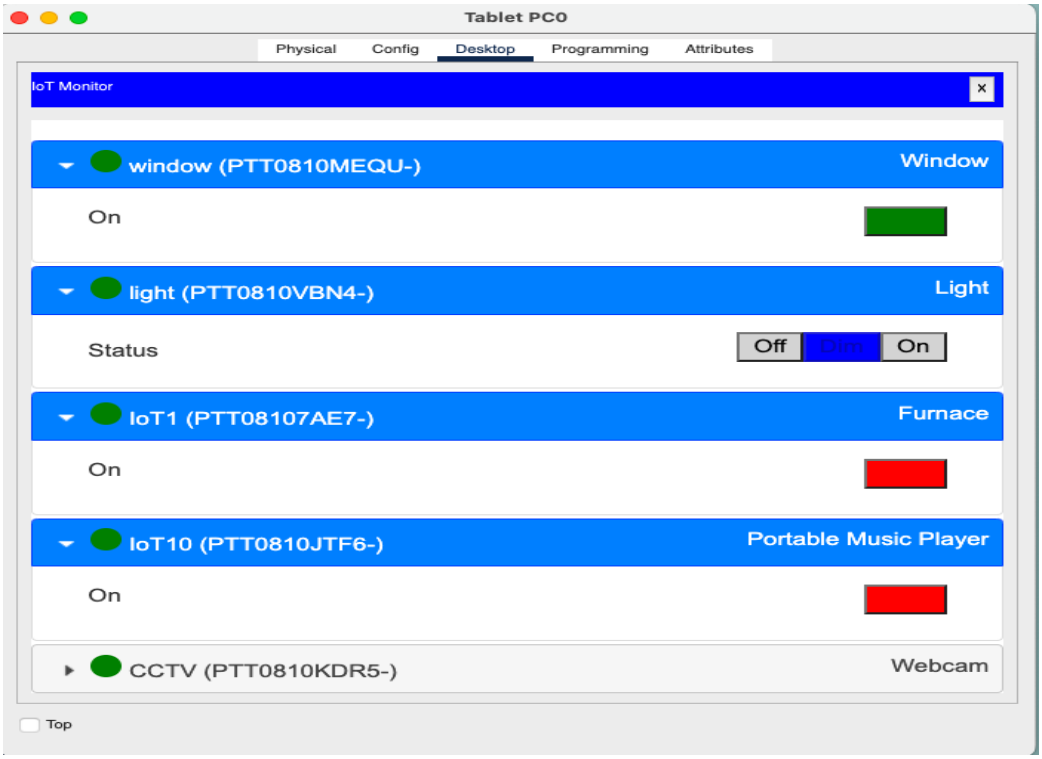
Static routing

Remote 2 lan

The Remote2 LAN (IoT) for ANZ Bank is designed to incorporate a wide array of Internet of Things (IoT) devices, enhancing the bank's operational efficiency and reducing labor costs through automation and remote monitoring capabilities. This network setup includes various IoT devices such as lights, fans, windows, CCTV cameras, furnaces, smartphones, laptops, and music players. All these devices are connected wirelessly, providing flexibility and scalability for the network.

Each of these devices is connected wirelessly, allowing for centralized control and monitoring through the network. This wireless infrastructure is integral to the bank's strategy of creating a smart and efficient environment, where physical presence is not required to manage these devices.

Given the increased attack surface introduced by IoT devices, robust security measures are essential. The network employs advanced authentication and encryption protocols to safeguard data and ensure that only authorized personnel can access and control the IoT devices. Regular security audits and updates are performed to address potential vulnerabilities and maintain the integrity of the network.



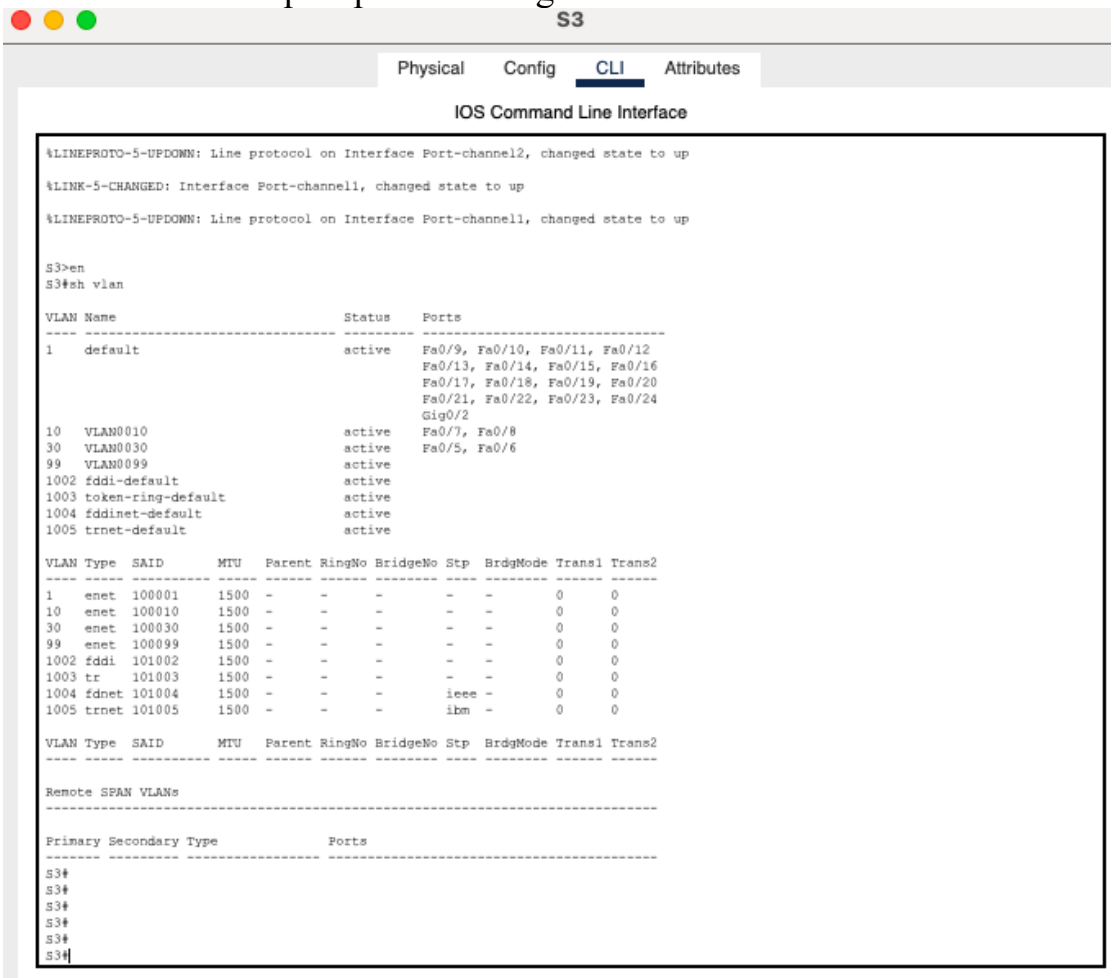
Online moniter the devices

Remote 1 lan

The Remote 1 LAN in ANZ Bank's network expansion project is designed with several key features to ensure security, efficiency, and high performance. The implementation of these features supports the bank's operational needs and enhances the overall network infrastructure.

1. VLAN (Virtual Local Area Network):

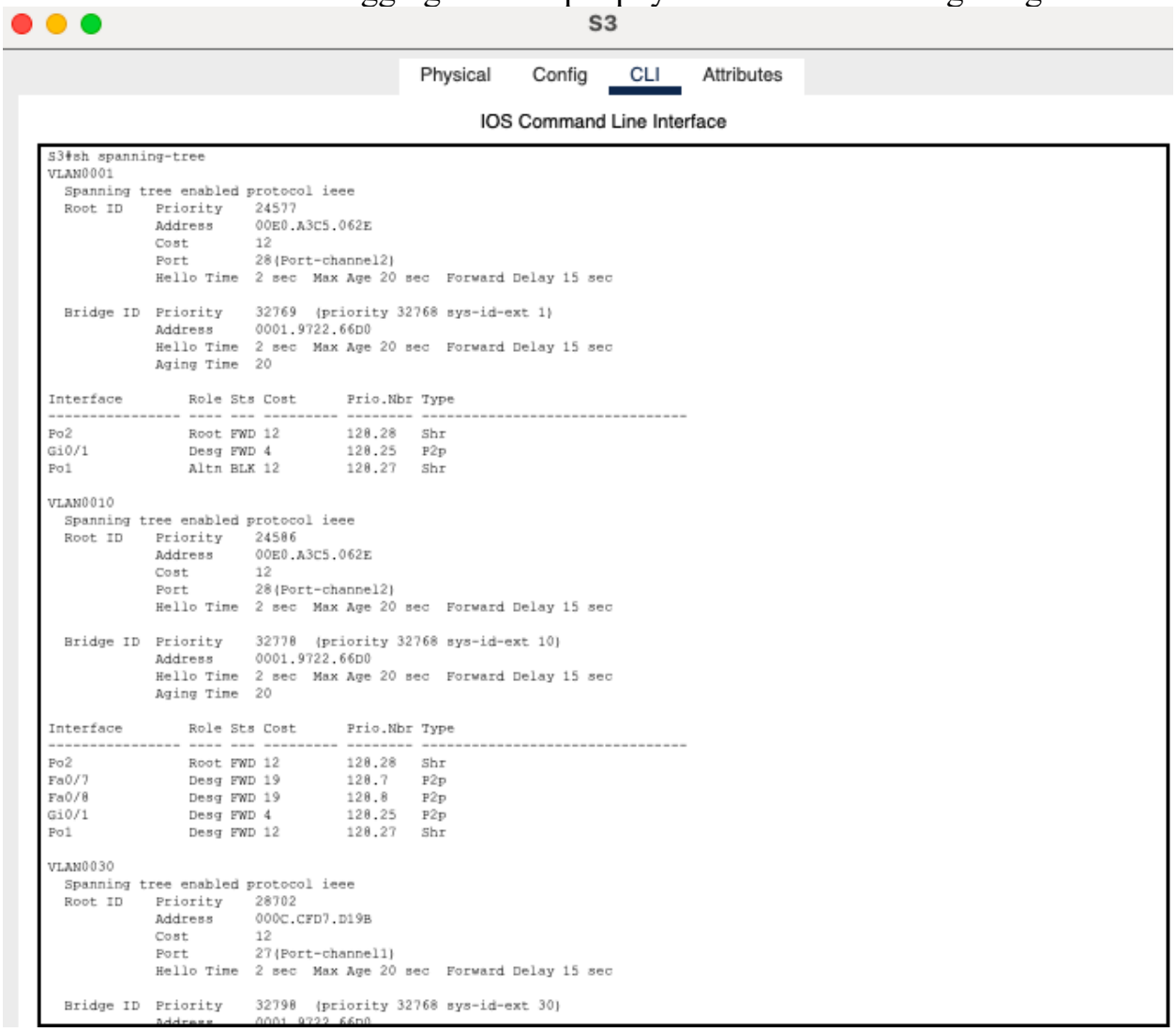
VLANs are implemented to segment network traffic logically. This enhances security and performance by isolating different types of traffic, ensuring that sensitive data is kept separate from general user traffic.



2. STP (Spanning Tree Protocol):

STP is configured to prevent network loops, which can cause significant network disruptions. By ensuring that there are no loops in the network, STP maintains network stability and redundancy. In case of a link failure, STP automatically reconfigures the network topology to maintain continuous service.
EtherChannel:

EtherChannel is used to aggregate multiple physical links into a single logical link.



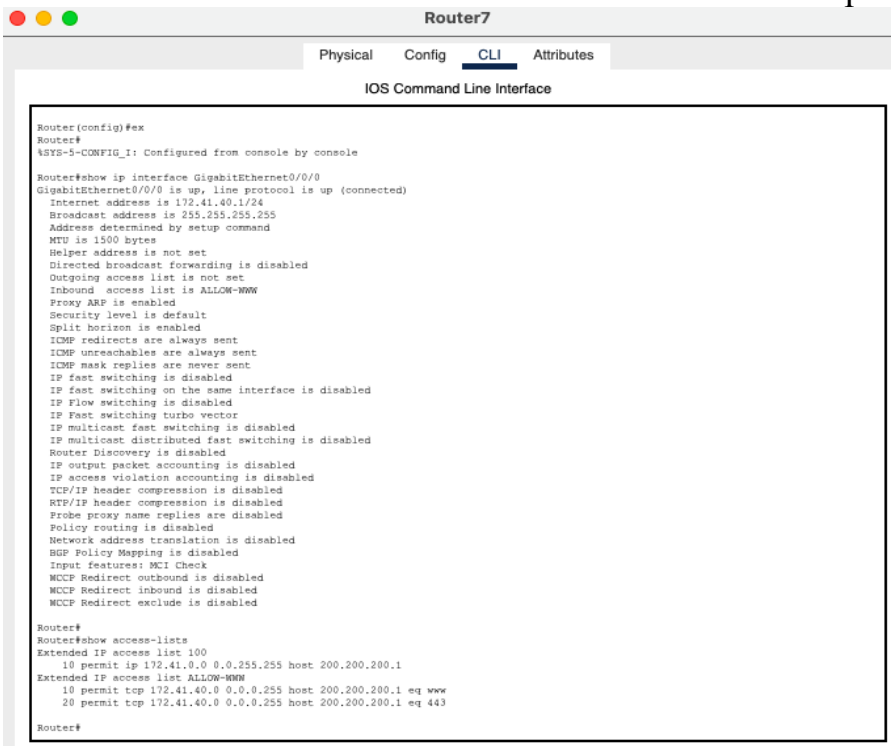
3. Switchport Security:

Switchport security is enforced to control access at the port level, preventing unauthorized devices from connecting to the network. This enhances the security

of the LAN by limiting the number of devices that can connect to a switch port and specifying which devices are allowed based on their MAC addresses. This measure helps protect against unauthorized access and potential security breaches.

4. Appropriate ACLs (Access Control Lists):

ACLs are implemented to control the flow of traffic into and out of the network. ACLs ensure that only authorized traffic is allowed, providing an additional layer of security. This is crucial for protecting sensitive information and maintaining the integrity of the network. This allows for centralized data management, making it easier for employees to access, share, and store documents securely. The file server enhances collaboration and ensures that data is backed up and managed efficiently.



Analysis

The network design for ANZ Bank successfully addresses the critical requirements of security, reliability, and scalability. The integration of advanced technologies such as OSPF, static routing, VLANs, STP, EtherChannel, and robust security protocols ensures a resilient network infrastructure. The implementation of IoT devices in the Remote2 LAN enhances operational efficiency and reduces costs through automation and remote management. The analysis highlights the strategic

importance of these technologies in achieving ANZ Bank's goals and positions the bank for future growth and technological advancements.

Limitations

The network design's complexity requires skilled IT personnel for management. Scalability and integration of new devices or branches pose challenges. The initial setup and maintenance costs are significant. Ensuring interoperability among diverse components and managing security risks, especially with IoT, are critical challenges.

IP addressing for your topology

Remote1 LAN IP Address table:

Devices	Interface	IP address	Subnet mask	Default Gateway
Pc5	Vlan 30	172.41.30.2	255.255.255.0	172.41.10.1
Pc6	Vlan 30	172.41.30.3	255.255.255.0	172.41.10.1
Pc7	Vlan 10	172.41.10.4	255.255.255.0	172.41.10.1
Latop1	Vlan 10	172.41.10.5	255.255.255.0	172.41.10.1
Pc13	Vlan 20	172.41.20.2	255.255.255.0	172.41.20.1
Pc14	Vlan 20	172.41.20.3	255.255.255.0	172.41.20.1
Pc15	Vlan 20	172.41.20.4	255.255.255.0	172.41.20.1
server	Vlan 20	172.41.20.5	255.255.255.0	172.41.20.1
Pc16	Vlan 30	172.41.30.4	255.255.255.0	172.41.30.1
Pc17	Vlan 30	172.41.30.5	255.255.255.0	172.41.30.1

Pc18	Vlan 40	172.41.40.2	255.255.255.0	172.41.40.1
Printer	Vlan 40	172.41.40.3	255.255.255.0	172.41.40.1
S1	Vlan 99	172.41.99.1	255.255.255.0	N/A
S2	Vlan 99	172.41.99.2	255.255.255.0	N/A
S3	Vlan 99	172.41.99.3	255.255.255.0	N/A
FTP Server	N/A	10.10.10.1	255.0.0.0	10.10.10.1
Router 7		172.41.40.2	255.255.255.0	
Romote 1 BR		172.41.50.1	255.255.255.0	

Vlan network

Ports	Assignments	Network
S1 (F0/5, F0/6, F0/7, F0/8)	Vlan 10	172.41.10.0/24
S2 (F0/5, F0/6, F0/70	Vlan 20	172.41.20.0/24
S3 (F0/5, F0/6, F0/7, F0/8)	Vlan 30	172.41.30.0/24

HQ lan

Original ip address (120.100.90.0/20)

subnet	Subnet address	prefix	1st host address	Last host address	broadcast
Subnet 1	120.100.90.0	/28	120.100.90.1	120.100.90.14	120.100.90.15

Subnet 2	120.100.90.16	/29	120.100.90.17	120.100.90.22	120.100.90.23
Subnet 3	120.100.90.24	/29	120.100.90.25	120.100.90.30	120.100.90.31
Subnet 4	120.100.90.32	/29	120.100.90.33	120.100.90.38	120.100.90.39
Subnet 5	120.100.90.40	/29	120.100.90.41	120.100.90.46	120.100.90.47
Subnet 6	120.100.90.48	/29	120.100.90.49	120.100.90.54	120.100.90.55
Subnet 7	120.100.90.56	/29	120.100.90.57	120.100.90.62	120.100.90.63
Subnet 8	120.100.90.64	/30	120.100.90.65	120.100.90.66	120.100.90.67
Subnet 9	120.100.90.68	/30	120.100.90.69	120.100.90.70	120.100.90.71
Subnet 10	120.100.90.72	/30	120.100.90.73	120.100.90.74	120.100.90.75
Subnet 11	120.100.90.76	/30	120.100.90.77	120.100.90.78	120.100.90.79
Subnet 12	120.100.90.80	/30	120.100.90.81	120.100.90.82	120.100.90.83
Subnet 13	120.100.90.84	/30	120.100.90.85	120.100.90.86	120.100.90.87
Subnet 14	120.100.90.88	/30	120.100.90.89	120.100.90.90	120.100.90.91

Subnet 15	120.100.90.92	/30	120.100.90.93	120.100.90.94	120.100.90.95
Subnet 16	120.100.90.96	/30	120.100.90.97	120.100.90.98	120.100.90.99

Cloud

Original ip address : 172.22.0.0 /20

	Ip address	prefix	1 host	Last host	broadcast
Subnet 1	172.22.0.0	/28	172.22.0.1	172.22.0.14	172.22.0.15
Subnet 2	172.22.0.16	/29	172.22.0.17	172.22.0.22	172.22.0.23
Subnet 3	172.22.0.24	/29	172.22.0.25	172.22.0.30	172.22.0.31
Subnet 4	172.22.0.32	/29	172.22.0.33	172.22.0.38	172.22.0.39
Subnet 5	172.22.0.40	/29	172.22.0.41	172.22.0.46	172.22.0.47
Subnet 6 r-r	172.22.0.48	/30	172.22.0.49	172.22.0.50	172.22.0.51
Subnet 7 r-r	172.22.0.52	/30	172.22.0.53	172.22.0.54	172.22.0.55
Subnet 8 r-r	172.22.0.56	/30	172.22.0.57	172.22.0.58	172.22.0.59
Subnet 9 r-r	172.22.0.60	/30	172.22.0.61	172.22.0.62	172.22.0.63

Ospf table

	Network address	prefix	Wildcard mask
Subnet 1	120.100.90.0	/28	0.0.0.15
Subnet 2	120.100.90.16	/29	0.0.0.7

Subnet 3	120.100.90.24	/29	0.0.0.7
Subnet 4	120.100.90.32	/29	0.0.0.7
Subnet 5	120.100.90.40	/29	0.0.0.7
Subnet 6	120.100.90.48	/29	0.0.0.7
Subnet 7	120.100.90.56	/29	0.0.0.7
Subnet 8	120.100.90.64	/30	0.0.0.3
Subnet 9	120.100.90. 68	/30	0.0.0.3
Subnet 10	120.100.90.72	/30	0.0.0.3
Subnet 11	120.100.90.76	/30	0.0.0.3
Subnet 12	120.100.90.80	/30	0.0.0.3
Subnet 13	120.100.90.84	/30	0.0.0.3
Subnet 14	120.100.90.88	/30	0.0.0.3
Subnet 15	120.100.90.92	/30	0.0.0.3
Subnet 16	120.100.90.96	/30	0.0.0.3

Conclusion

The network expansion project for ANZ Bank is a strategic initiative aimed at enhancing operational efficiency, security, and customer service across new remote sub-banks. By addressing ethical considerations and planning for future growth and technological advancements, the bank can ensure a resilient and adaptable network infrastructure that meets current and future needs.

References

Chataut, R. and Phoummalayvane, A. (2023) Unleashing the power of IOT: A comprehensive review of IOT applications, advancements, and future prospects in healthcare, agriculture, Smart Homes, smart cities, and Industry 4.0 [Preprint]. doi:10.20944/preprints202306.0002.v1.

Farooq, M.S., Riaz, S. and Alvi, A. (2023) 'Security and privacy issues in software-defined networking (SDN): A systematic literature review', Electronics, 12(14), p. 3077. doi:10.3390/electronics12143077.

2. motion detector, CCTV and Siren IOT smart devices simulation using Packet Tracer (2022) *YouTube*. Available at: https://www.youtube.com/watch?v=A3bfsLExPzk (Accessed: 02 June 2024).

DHCP DNS and web server configuration in Cisco packet tracer | DHCP server configuration | DHCP lab (2023) *YouTube*. Available at: https://www.youtube.com/watch?v=ZTNwwevT7S8 (Accessed: 02 June 2024).

Free CCNA 200-301 Course 29-10: Nat lab exercise (2022) *YouTube*. Available at: https://www.youtube.com/watch?v=r5wDTS9jw0M (Accessed: 02 June 2024).

FTP server using cisco packet tracer || CCNA videos easy learning tutorials (2021) *YouTube*. Available at: https://www.youtube.com/watch?v=Mk5WUsHOK0Y (Accessed: 02 June 2024).

How to configure a smart home design in Cisco packet tracer | IOT devices configure | end devices (2020) *YouTube*. Available at: https://www.youtube.com/watch?v=vjPWanGskek (Accessed: 02 June 2024).

Molenaar, R. (2023) *Per vlan spanning tree (PVST)*, *NetworkLessons.com*. Available at: https://networklessons.com/spanning-tree/per-vlan-spanning-tree-pvst (Accessed: 02 June 2024).

Packet tracer 6.2.4 - configure EtherChannel (2021) *YouTube*. Available at: https://www.youtube.com/watch?v=9Hp2TYpFPQM (Accessed: 02 June 2024).

PacketTracerNetwork (no date) *Packet tracer 8.2- IOT devices configuration*, *Packet Tracer Network*. Available at: https://www.packettracernetwork.com/internet-of-things/pt7-iot-devices-configuration.html (Accessed: 02 June 2024).