ANZ Project Interim Report

Table of Contents

3. Introduction

Background:

ANZ Bank is poised to extend its banking network by setting up several remote sub-banks across Sydney, Darwin, and Perth. This strategic initiative is aimed at bolstering ANZ Bank's footprint, bringing financial services closer to customers in these regions, and catering to the unique demands of each locality.

a. Design Requirements:

For HQ LAN

The HQ LAN will be developed to ensure network redundancy, incorporating multiple routers with failover capabilities. A DMZ will host a web server, allowing external access while isolating the internal network. NAT will be used to mask internal IP addresses, and internal network navigation will be supported by a DNS server. A DHCP server will automate IP address allocation. The network will include at least five routers using OSPF and static routing to ensure optimal connectivity. ACLs will restrict external access to the internal HQ LAN, permitting exceptions only for the DMZ web server and allowing selective access to remote sites for specified HQ groups. All HQ LAN users will have access to the WWW server, maintaining security and network functionality.

For Remote1 LAN

For the Remote1 LAN, the design will incorporate multiple VLANs to segment network traffic and improve security and performance. Spanning Tree Protocol (STP) will be implemented to prevent network loops and provide network redundancy. EtherChannel will be configured to aggregate bandwidth across multiple physical links, providing increased speed and fault tolerance. Switchport security will be enforced to secure access at the port level, preventing unauthorized connections. ACLs will be tailored to ensure secure access control, restricting unauthorized traffic and safeguarding network resources. A dedicated file server will be established exclusively for internal use, hosting shared files with controlled access to enhance data management. To maintain external connectivity, ACLs will specifically permit the Remote1 LAN to access a WWW server, allowing for necessary internet access while still protecting the LAN from unwanted traffic.

For Remote2 LAN (IOT)

The Remote2 LAN will be specifically designed to cater to Internet of Things (IoT) requirements. This network will facilitate multiple IoT devices such as door, fan, light and music player, all of which must be accessible from outside the Remote2 LAN to allow for remote monitoring and management. A central IoT server will be integral to the network, providing a

consolidation point for data collection, device management, and integration with external networks. Connectivity for IoT devices will be established via a secure wireless infrastructure to support flexibility and scalability. Security measures will include robust authentication and encryption protocols to ensure secure remote access while maintaining the operational integrity of the IoT devices. The design will also allow for future expansion to include additional IoT devices as necessary, maintaining scalability and adaptability as key features of the Remote2 LAN infrastructure.

b. Literature Review:

In the context of ANZ Bank's expansion and the establishment of remote sub-banks, the choice between Internet of Things (IoT) and Software-Defined Networking (SDN) technologies becomes pivotal. The decision to implement IoT in the Remote2 LAN is predicated on its ability to enhance customer service through automation, data collection, and connectivity which is essential in modern banking.

IoT, as expounded by Javed (et al., 2018), ushers in an era where the physical environment around us becomes more responsive and intelligent. This directly supports the bank's objective to integrate advanced services like smart ATMs, queue management, and enhanced security systems that understand customer preferences and improve service delivery. The IoT's inherent ability to connect a myriad of devices and sensors aligns with the bank's aim to create smart branches that can collect data on customer behavior and preferences, leading to a personalized banking experience. Contrastingly, SDN provides a high level of network programmability and centralization, which is beneficial in managing network traffic and security as indicated by Farooq (et al., 2023). However, SDN's strengths lie in backend network management, and while crucial, it does not directly contribute to customer-facing service enhancements as IoT does. Chataut (et al., 2023) elucidate the demand for automation and efficiency that IoT devices satisfy, which is harmonious with the bank's objective of efficient and automated customer service. Furthermore, the integration of IoT in healthcare, as described in the literature, shows its capacity for managing sensitive data securely—a vital requirement for banking operations.

Chataut (et al., 2023) also underlines significant challenges in IoT implementation, particularly regarding security and privacy, as IoT devices often become targets for cyberattacks. Security measures are of paramount importance in the banking industry, and as IoT technology progresses, the literature suggests a need for improved security frameworks to address vulnerabilities, advocating for advanced solutions like end-to-end security and zero-trust frameworks.

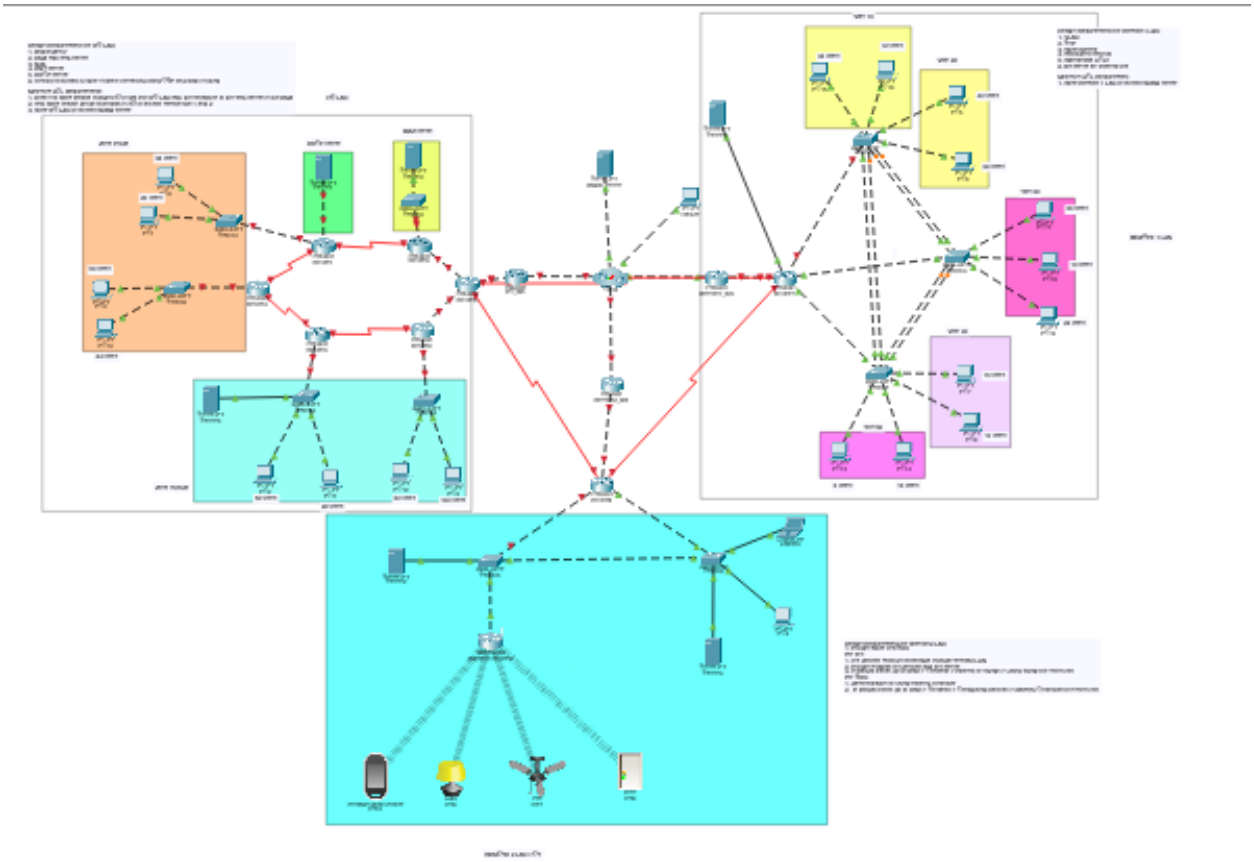
c. Aim and Scope:

The project's goal is to design and implement a network architecture that ensures high availability, security, and performance for ANZ Bank's widespread operations. Each LAN must

meet stringent security standards to protect sensitive financial transactions and personal customer data. The aim includes scalability to accommodate future growth and technological advances, ensuring that ANZ Bank remains agile in a competitive and ever-evolving financial industry landscape.

4. Design

a. Topology



b. Description:

The network topology is designed to ensure high availability through redundancy, indicated by multiple interconnected routers and failover protocols, essential for the 24/7 banking environment. Security measures include a demilitarized zone (DMZ) for safely hosting the web

server, along with Access Control Lists (ACLs) to manage traffic flow and protect sensitive network segments. Network Address Translation (NAT) is employed at the edge of the network to safeguard internal IP addresses, while Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) services streamline navigation and IP management.

Routing within the network is handled by Open Shortest Path First (OSPF) and static routing, optimizing path selection for transactional data and maintaining network efficiency. The integration of IoT in the Remote2 LAN, indicated by wireless connections to various devices, sets the foundation for smart banking functionalities and customer service enhancements, centralized through an IoT server for data and device management.

c. Limitations:

The design's limitations include its complexity, which necessitates skilled IT personnel for management, the challenges associated with scalability and integrating new devices or branches, and the elevated security risks due to the increased attack surface introduced by IoT devices. The costs associated with the initial setup and ongoing maintenance of such an advanced network could be significant. Furthermore, ensuring interoperability among diverse network components and IoT integrations could pose challenges, and there is potential for performance issues if misconfigurations occur within the complex network setup. Regular monitoring, auditing, and optimization will be required to manage these limitations and maintain service quality.

d. IP address for topology:

HQ LAN IP Address:

Devices	IP address	Subnet mask	Default Gateway	
Pc 9	10.0.0.1	255.255.255.0	10.0.0.1	
Pc 1	10.0.0.2	255.255.255.0	10.0.0.1	
Pc 0	10.0.0.3	255.255.255.0	10.0.0.1	
Pc 10	10.0.0.4	255.255.255.0	10.0.0.1	
Pc 2	10.0.0.5	255.255.255.0	10.0.0.1	
Pc 11	10.0.0.6	255.255.255.0	10.0.0.1	
Pc 12	10.0.0.7	255.255.255.0	10.0.0.1	
Pc 3	10.0.0.8	255.255.255.0	10.0.0.1	
HQ_BR	10.0.1.1	255.255.255.0	10.0.1.1	
R_HQ	10.0.2.1	255.255.255.0	10.0.2.1	
R0 (ROUTER)	10.0.3.1	255.255.255.0	10.0.3.1	
R1	10.0.3.2	255.255.255.0	10.0.3.1	
R2	10.0.3.3	255.255.255.0	10.0.3.1	
R3	10.0.3.4	255.255.255.0	10.0.3.1	
R4	10.0.3.5	255.255.255.0	10.0.3.1	
Zone inside server	10.0.4.1	255.255.255.0	10.0.4.1	
DMZ server	10.0.5.1	255.255.255.0	10.0.5.1	
DHCF server	10.0.6.1	255.255.255.0	10.0.6.1	

Using VLSM, allocate IP addresses

LAN	**Subnet ID/prefix**	**1st Host IP**	**Last Host IP**	**Broadcast Address**
Pc9 (33 users)	10.0.0.0/24	10.0.0.1	10.0.0.62	10.0.0.63
Pc1 (20 users)	10.0.0.64/30	10.0.0.65	10.0.0.94	10.0.0.95
Pc0 (50 users)	10.0.0.96/29	10.0.0.97	10.0.0.158	10.0.0.159
Pc10 (24 users)	10.0.0.160/30	10.0.0.161	10.0.0.190	10.0.0.191
Pc2 (50 users)	10.0.0.192/29	10.0.0.193	10.0.0.254	10.0.0.255
Pc11 (20 users)	10.0.1.0/30	10.0.1.1	10.0.1.30	10.0.1.31
Pc12 (50 users)	10.0.1.32/29	10.0.1.33	10.0.1.94	10.0.1.95
Pc3 (100 users)	10.0.1.96/29	10.0.1.97	10.0.1.224	10.0.1.225
HQ_BR-R6	10.0.1.224/31	10.0.1.225	10.0.1.226	10.0.1.227
R6-R0	10.0.1.228/30	10.0.1.229	10.0.1.228	10.0.1.229
R0-R1	10.0.1.230/30	10.0.1.231	10.0.1.232	10.0.1.233
R1-R4	10.0.1.234/30	10.0.1.235	10.0.1.236	10.0.1.237
R4-R3	10.0.1.238/30	10.0.1.239	10.0.1.240	10.0.1.241
R3-R2	10.0.1.242/30	10.0.1.241	10.0.1.244	10.0.1.245

Remote1 LAN IP Address:

Devices	IP address	Subnet mask	Default Gateway	
Pc15	10.1.0.1	255.255.255.0	10.1.0.1	
Pc16	10.1.0.2	255.255.255.0	10.1.0.1	
Pc5	10.1.0.3	255.255.255.0	10.1.0.1	
Pc6	10.1.0.4	255.255.255.0	10.1.0.1	
Pc17	10.1.0.5	255.255.255.0	10.1.0.1	
Pc18	10.1.0.6	255.255.255.0	10.1.0.1	
Pc19	10.1.0.7	255.255.255.0	10.1.0.1	
Pc7	10.1.0.8	255.255.255.0	10.1.0.1	
Pc8	10.1.0.9	255.255.255.0	10.1.0.1	
Pc13	10.1.1.0	255.255.255.0	10.1.0.1	
Pc14	10.1.1.1	255.255.255.0	10.1.0.1	
R7	10.2.0.1	255.255.255.0	10.2.0.1	
Remote1_BR	10.3.0.1	255.255.255.0	10.3.0.1	

LAN	Subnet ID/prefix	1st Host IP	Last Host IP	Broadcast Address
Pc15 (34users)	10.1.0.0/24	10.1.0.1	10.1.0.62	10.1.0.63
Pc16 (12 users)	10.1.0.64/30	10.1.0.65	10.1.0.78	10.1.0.79
Pc5 (40 users)	10.1.0.80/28	10.1.0.81	10.1.0.142	10.1.0.143
Pc6 (90 users)	10.1.0.144/30	10.1.0.145	10.1.1.14	10.1.1.15
Pc17 (30 users)	10.1.1.16/31	10.1.1.17	10.1.1.46	10.1.1.47
Pc18 (10 users)	10.1.1.48/29	10.1.1.49	10.1.1.62	10.1.1.63
Pc19 (22 users)	10.1.1.64/28	10.1.1.65	10.1.1.94	10.1.1.95
Pc7 (15 users)	10.1.1.96/29	10.1.1.97	10.1.1.126	10.1.1.127
Pc8 (10 users)	10.1.1.128/29	10.1.1.129	10.1.1.142	10.1.1.143
Pc13 (5 users)	10.1.1.144/28	10.1.1.145	10.1.1.174	10.1.1.175
Pc14 (15 users)	10.1.1.176/29	10.1.1.177	10.1.1.206	10.1.1.207
Remote1_br-R7	10.1.1.208/29	10.1.1.209	10.1.1.210	10.1.1.211

Remote2 LAN (IOT) IP Address:

Devices	IP address	Subnet mask	Default Gateway	
Server 2	192.168.0.10	255.255.255.0	192.168.0.1	
wireless	192.168.0.10	255.255.255.0	192.168.0.1	
R8	192.168.0.1	255.255.255.0	192.168.0.1	
Remote_BR	192.168.1.1	255.255.255.0	192.168.1.1	
Server 4	192.168.2.1	255.255.255.0	192.168.2.1	
Pc4	192.168.3.1	255.255.255.0	192.168.3.1	
latop	192.168.4.1	255.255.255.0	192.168.4.1	

5. Conclusion

In summary, the network expansion plan for ANZ Bank is strategically designed to ensure reliable, secure, and innovative banking services across new remote sub-banks. The network architecture incorporates redundancy, advanced security measures, and IoT capabilities, aligning with the bank's objectives to enhance customer service and manage data efficiently. While the design promises scalability and robust operations, it acknowledges challenges such as complexity, security risks associated with IoT, and the need for skilled management. The initiative positions ANZ Bank to grow and adapt in the dynamic financial sector while emphasizing the need for vigilance in security and system integrity.

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.

Javed, F. *et al.* (2018) 'Internet of things (IOT) operating systems support, networking technologies, applications, and challenges: A comparative review', *IEEE Communications Surveys & Tutorials*, 20(3), pp. 2062–2100. doi:10.1109/comst.2018.2817685.