

**PROJECT PLAN FOR NETWORK UPGRADE PROJECT FOR A BANK**

**GROUP MEMBERS:**

MD SAJEDUL ISLAM TANIM: 56090

TASNIMUL HASAN RAHAT: 54565

MR IBNUL HOSSAIN RAFI: 56784

MAHADI TALUKDER: 56334

BORNIL ADNAN: 56907

# INTRODUCTION

Due to rapid increase on reliance on digital banking services, the need for a secure and an efficient network infrastructure has risen. This project “Network Upgrade Project for a Bank”, aims at addressing the limitation that exist in a current bank’s network, such as basic security protocols, lack of redundancy and insufficient segmentation and develop and advanced topology that implements advanced security measures, incorporates redundant WAN connections and introduces VLAN segmentation. The project seeks to create a scalable network that is capable of supporting the bank’s future growth and also ensuring the safety of its critical data. Therefore, this report outlines the comprehensive project plan, detailing, scope, timeline, risk management strategies and application of configuration management tools such as GitHub and Trello for project tracking and implementation.

# SCOPE STATEMENT

## Objectives

This project aims at upgrading the bank’s network infrastructure in order to improve its security, scalability and performance. This will be implemented by use of WAN links for redundancy, VLAN segmentation for traffic management, upgraded equipment to promote higher performance and advanced firewalls for enhanced security.

## Key deliverables

* Assessing the current network infrastructure
* Designing and implementation of plan for the new network topology
* Configuration of files for all the network devices, i.e. routers, firewalls, switches, etc.
* Updated and detailed network diagrams for both the current and updated network topologies.
* Risk management strategies that are documented for the entire project lifecycle.
* GitHub repository for collaboration showing configuration management and version control processes.

## Assumptions

* Sufficient budget allocation for purchase of new equipment and software licenses.
* Cooperation from all bank branches for the testing of the infrastructure.

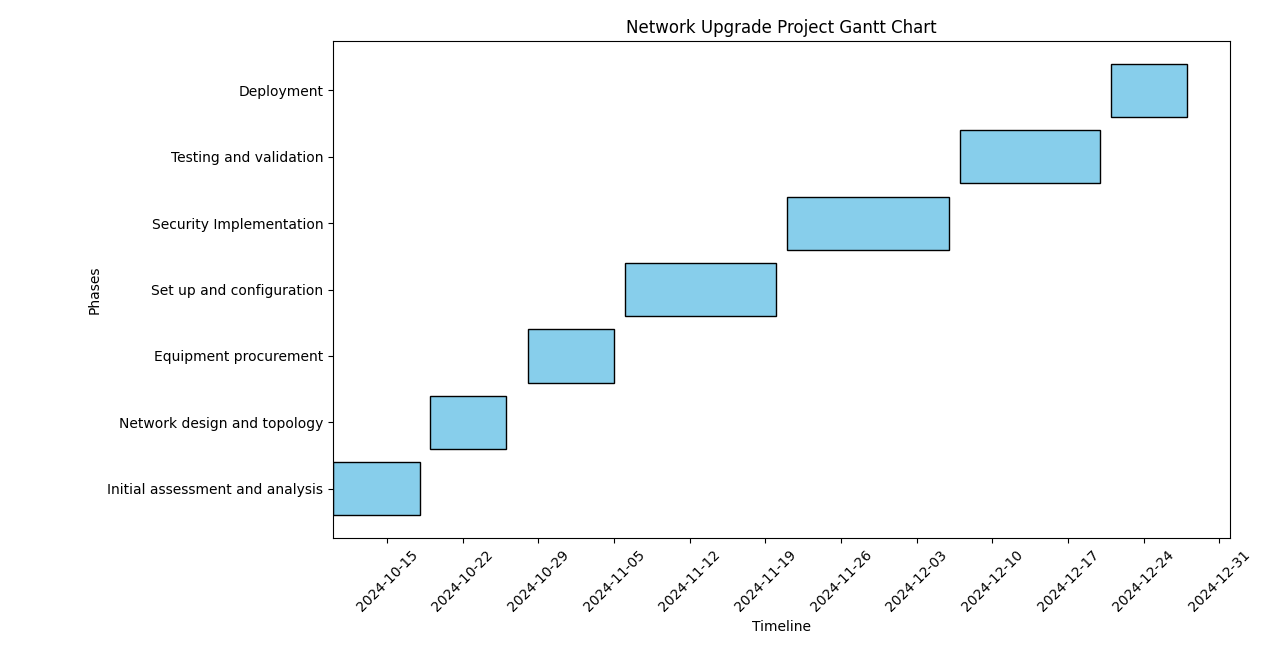
## Constraints

* A limited time frame of 14 weeks for the completion of the project.
* Minimal disruption to the banking operations during the process. This can be done during weekends or bank’s off-hours.

# GANTT CHART

Gantt chart displays the task against their time frame. It outlines the start date and the main phases of the project, including interdependencies between the activities.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Phase** | **Start date** | **End date** | **Duration (days)** | **Dependencies** |
| Initial assessment and analysis | 2024-10-10 | 2024-10-18 | 9 | None |
| Network design and topology | 2024-10-19 | 2024-10-26 | 8 | Initial assessment and analysis |
| Equipment procurement | 2024-10-28 | 2024-11-05 | 9 | Network design and topology |
| Set up and configuration | 2024-11-06 | 2024-11-20 | 15 | Equipment procurement |
| Security Implementation | 2024-11-21 | 2024-12-06 | 16 | Set up and configuration |
| Testing and validation | 2024-12-07 | 2024-12-20 | 14 | Security Implementation |
| Deployment | 2024-12-21 | 2024-12-28 | 8 | Testing and validation |



# NETWORK TOPOLOGY

## Current network topology

### Overview

The current network of the bank is a centralized topology that connects all bank branches to the headquarter via s single Wide Area Network (WAN) link. This setup lacks proper segmentation and redundancy thus leading to increased risk of network outages and security breaches. It contains the following components and structure:

### Current network components

**Main (Headquarter) Router**: Located at the headquarters, it manages all the incoming and outgoing traffic from and to the branch offices. It handles the communications through the WAN.

It has an IP address: 192.168.0.1

**Branch Routers**: Each bank’s branch has its own router that is connected to the headquarters’ router via a WAN link. They provide network access to the users in the branches and facilitate communication with the headquarters’ server.

IP address: 192.168.1.1, 192.168.2.1, etc. for the branches (Branch 1, 2, …).

**Firewall**: Located at the headquarters and serves as the only layer of protection between the internet and internal network of the bank. It does not incorporate advanced security features such as intrusion inspections or VPN but just uses basic filtering rules.

IP address: 192.168.0.254

**Headquarter Switch**: This is the core switch at the headquarter that connects the central router to the departments within headquarters. It does not contain segmentation such as VLANs meaning that all devices in the headquarters share same broadcast domain, a security risk and could lead to performance issues.

**Branch Switches**: Switches in the branches connects local branch router(s) to the devices and workstations operating in the branch. All the devices within a branch share the same network due to lack of segmentation.

**Servers at Headquarters**: These includes the bank’s services such as application servers and databases that are hosted at the headquarters. They are accessible to the branches’ offices via a WAN connection.

IP range: 192.168.0.100 – 192.168.0.150

**Internet Service Provider (ISP)**: ISP is used to provide internet connectivity to the headquarters. All traffic from branches and headquarters flow through same link.

## Limitations of the current network topology

* **Limited Security**: The firewall that is used in this network infrastructure only support basic features and no advanced features such as inspections and VPN capabilities for a more secure remote access.
* **Bandwidth limitations**: The WAN link used cannot sufficiently handle increased traffic with the growth of the bank, leading to performance issues.
* **Lack of redundancy:** There is single WAN link thus making the whole bank branches dependent on one single point and therefore, incase of failure at that point, all the branches lose connectivity to the internet and headquarters.
* **No segmentation:** Lacks of VLANs and subnets makes the network vulnerable to internal threats and limits the performance optimization.

## Proposed updated network topology

This new topology that aims at improving reliability, security and performance, includes advanced firewalls, VLANs, redundant connections and robust IP addressing scheme.

### Overview

The new design will have dual WAN links, multiple layers of security and VLANs. It implements a hybrid model with enhanced segmentation and redundancy.

### Its components and structure

**Dual WAN links**: Each branch to be connected to headquarters by two WAN links. One is a primary and the second a backup link for redundancy.

IP ranges:

10.0.1.1/30 – 10.0.1.2/30 for primary WAN

10.0.2.1/30 – 10.0.2.2/30 for backup WAN

**Routers at headquarters**:

Primary router and backup router (A and B) configured for high availability.

IP addresses: 192.168.0.1 for Router A and 192.168.0.2 for Router B

**Advanced Firewalls**: Firewalls with VPNs and support inspection to be implemented on the bank branches and headquarters in order to promote secured remote access.

**Switch at headquarters**: A switch that supports internal routing and VLANs. VLANs IP addresses:

VLAN 10: 192.168.10.0/24: for user traffic  
VLAN 20: 192.168.20.0/24: for traffic management  
VLAN 30: 192.168.30.0/24: for user traffic

**Switches at branches**:

Switches that have been upgraded to support segmentation for better security and performance. For instance, branch 1 VLANs:

192.168.101.0/24: user VLAN   
192.168.102.0/24: management VLAN

**ISPs**: Dual Internet Service Providers configured to provide load balancing capabilities and redundancy.

### Improvements from the current network topology

Enhanced security: with the advanced firewalls, VLANs and VPNs to protect sensitive data.

**Network security enhancements will include:**

* Security policies and firewall rules: Configured with default policy to block any incoming and outgoing traffic unless allowed in the firewall rules. This involves applications of specific allowed rules and Intrusion prevention system.
* VPN Configurations: Setting for instance an IPSec VPN between the headquarters and branches in for securing WAN connections.   
  Also establishing remote access VPN for the remote workers so as to provide a secure work tunnel for them to access internal systems using MFA for additional security.

Optimized performance: Improved bandwidth management and network speed because of application of segmented traffic and load balancer.

Redundancy: Use of redundant routers and WAN links in order to eliminate a single point of failure.

# Risk and issues management strategy

## Risks during changeover period:

Configuration errors: In case of incorrect settings for instance IP addresses could lead to services disruption.

Equipment failure: Cases of equipment failures during the installation process.

Cybersecurity threats: During the transition period the network maybe vulnerable to potential attacks.

## Mitigation strategies

For configuration issues, virtual testing environment could be used to validate the configurations before live deployment

For equipment failure: deployment of backup devices and equipment.

Security checks and enhanced monitoring implementation during the deployment phase to mitigate cybersecurity threats.

# Change request management process

**Change review and approval process**

Any changes implemented will be documented and reviewed before its implementation. There will be weekly review meetings by the team to perform evaluation requests based on the risk, impact and priorities.

For each change request made, it will go through the following steps:

* Request submission: A team member presents the request with detailed information, i.e. scope, purpose and its impact.
* Review: Request reviewed by the group leader for feasibility and completeness.
* Approval: The request is the approved or rejected by the change control board and on approval, the changes are then scheduled for implementation.
* Implementation: After the changes have been approved, they are implemented.
* Post-implementation review: Assessment of success and logs encountered after the changes are implemented.

**Roles and responsibilities**

* Team leader: Maked reviews and approvals of the changes to ensure that it aligns with the project goals.
* Network engineer: Implements the approved changes and in document notes down the steps taken.
* Quality assurance: QA verifies that the changes are successful and makes sure no disruptions are encountered.
* Configuration manager: Does maintenance and updating of configuration files in GitHub

# Configuration management using GitHub

Created a repository in GitHub for tracking and managing configuration files and the network diagrams, developed using cisco packet tracer.

Components of the repository:

/ Configurations:

/ Diagrams:

/ Documentation:

# CONCLUSION

The network upgrade project for the bank has an aim of transforming the existing network infrastructure to enhance the reliability, security and performance. Thus, the new design incorporates advanced firewalls that have VPN capabilities, dual WAN links for redundancy and the VLAN segmentation to enable optimized traffic management. This is so as to address the current network limitations such as lack of segmentation and single point of failure. To enhance this, we came up with a project plan that outlines risk management strategy, ensuring mitigation of potential issues like equipment failures and configuration errors., configuration management and version control that are managed via GitHub to allows the team’s collaboration efficiently and ensure that network configurations integrity is maintained throughout the project. Therefore, with the structured approach, this project sets a future foundation for the bank’s growth to ensure that its data remains secure and services uninterrupted.

# REFERENCES

1. Del Giudice, P.S., Amoza, F.R. and Yasin, M., 2012. Designing WAN Topologies under Redundancy Constraints (pp. 293-312). InTech.
2. Gantt, "What is a Gantt Chart?", Gantt.com: <https://www.gantt.com/>
3. GitHub, "GitHub Documentation," GitHub Docs: <https://docs.github.com/en>
4. Deal, R., 2005. The complete Cisco VPN configuration guide. Cisco Press.
5. Londhe, A., 2019. Bank Network Architecture. Medium. Available at: <https://medium.com/@londheanushka/bank-network-architecture-7b9d9f6bf003>
6. Ahmad, M.K.A., Rosalim, R.V., Beng, L.Y. and Fun, T.S., 2010. Security issues on banking systems. International Journal of Computer Science and Information Technologies, 1(4), pp.268-272.
7. Tsai, M.C., Chien, Y.Y. and Cheng, C.C., 2018. Upgrading service quality of mobile banking. International Journal of Mobile Communications, 16(1), pp.82-115.