Enterprise Network Infrastructure Project

Prepared by: Abdelrahman Radwan, Abdelrahman Khaled, Mahmoud Safwat, Ahmed Mohamed Afifi, Mariam Dweidar
Date: August 21, 2025

Document Version Control

Version	Date	Author	works
1.0	2025-08-21	Network admin & Security Team	Design and config topology

---

Table of Contents

- A. Proposed Hardware & Software
- B. Detailed Technical Configurations (Excerpts)
- C. Glossary of Terms

---

1. Executive Summary

[Company Name] operates across two headquarters (Egypt and Saudi Arabia) and four branch offices. To support its growth and digital transformation goals, the company requires a modern, robust, and secure network infrastructure. This proposal outlines a comprehensive solution designed to provide **high availability, unparalleled security, and seamless unified communications**.

This new architecture is built upon industry-best practices and advanced technologies, ensuring **99.99% uptime** through comprehensive redundancy protocols like VRRP and MSTP. Security is ingrained at every layer, adhering to the **CIA Triad (Confidentiality, Integrity, Availability)** with enterprise-grade encryption, firewalls, and access controls. The network will natively support **high-quality Voice over IP (VoIP)** and a centralized, secure **Wi-Fi 6 (or later)** infrastructure for both corporate and guest users.

By implementing this future-proof solution, [Company Name] will gain a significant competitive advantage through improved operational efficiency, reduced risk, and a scalable platform for future innovation.

2. Project Objectives & Business Alignment

This project is designed to achieve specific, measurable outcomes that directly support [Company Name]'s business objectives.

Objective	Technical Implementation	Business Benefit
Maximize Availability	VRRP, MSTP, Eth-Trunk (LACP), BFD for sub-second failover.	Minimizes downtime, ensures continuous operation, and protects revenue.
Enhance Security	IPSec/SSL VPNs, AAA (RADIUS), IPS/IDS, WPA3, and advanced threat protection.	Protects sensitive company and customer data, ensuring compliance and trust.
Enable Unified Comms	Dedicated Voice VLANs, QoS (Prioritization), PoE, and MOS > 4.0.	Improves collaboration, reduces telephony costs, and increases productivity.
Ensure Scalability	Hierarchical OSPF/BGP design, IPv4/IPv6 Dual-Stack, modular hardware.	Supports business growth and new site deployments without major redesign.
Improve Manageability	Centralized monitoring (SNMPv3, NetStream), automation (NETCONF).	Reduces operational costs, simplifies troubleshooting, and enables proactive care.

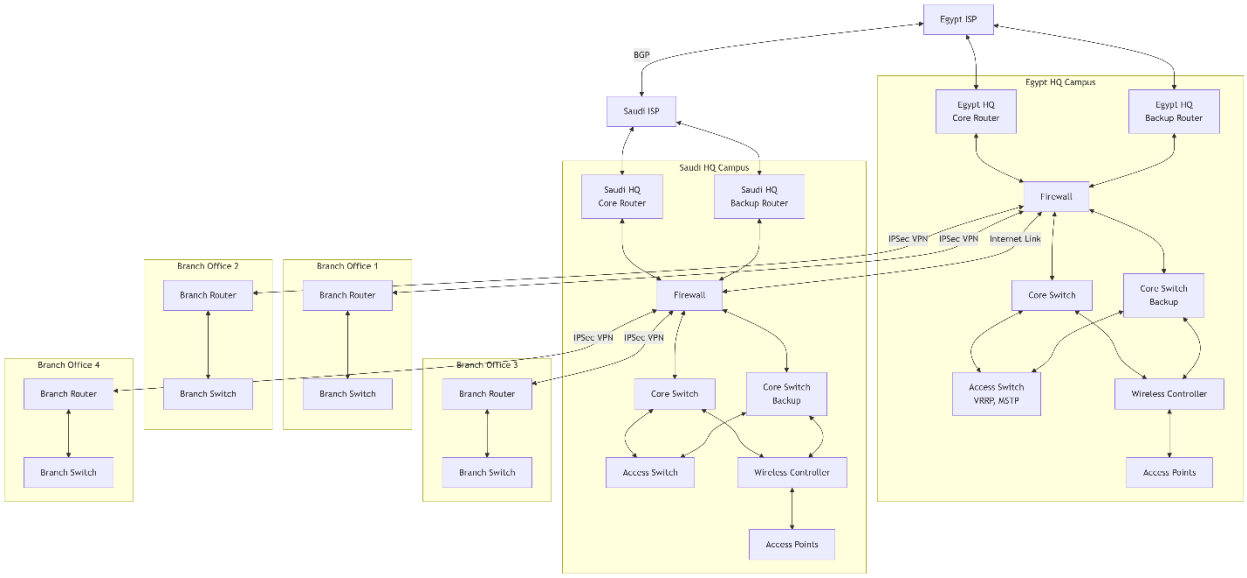
3. Current Challenges & Proposed Solution Overview

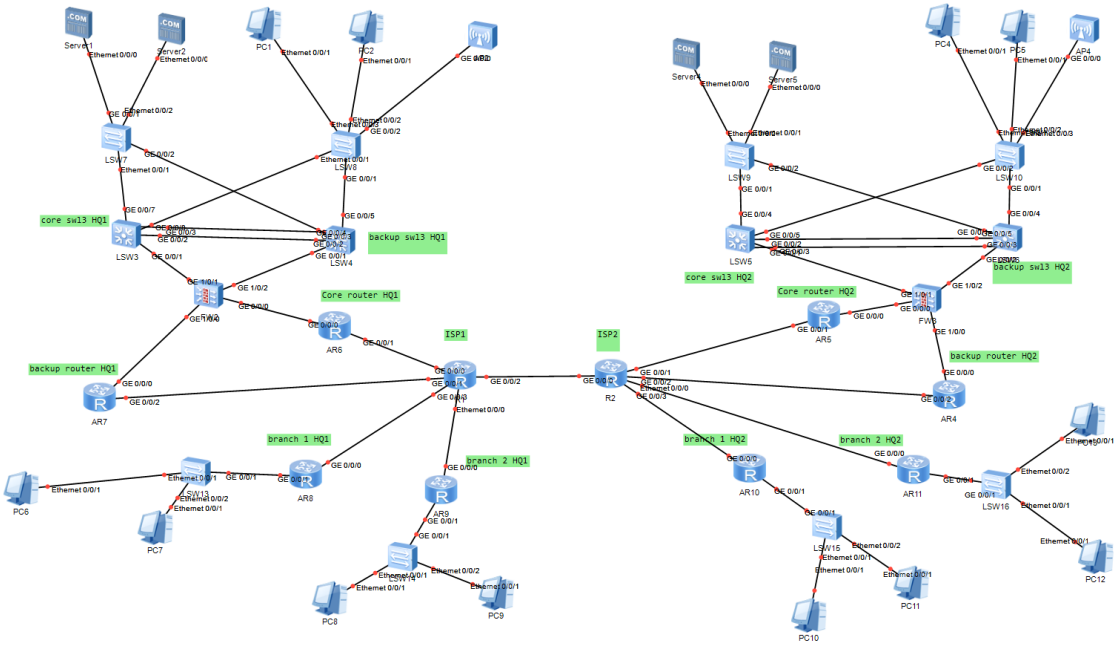
Current State Challenges:

- Potential single points of failure across the network
- Lack of integrated security between headquarters and branches
- Inconsistent voice and data quality across sites
- Limited visibility into network performance and threats
- A network architecture that is difficult to scale

Proposed Solution Overview:

Our solution is a hierarchical, multi-site WAN architecture that connects all locations securely and reliably. The design incorporates BGP routing between ISPs for robust internet connectivity and site-to-site connectivity through secure internet links.





4. Detailed Technical Architecture

4.1. Core Network Design

The network will use a robust, multi-protocol design for optimal routing and redundancy.

- **Intra-Site Routing (OSPF):** Open Shortest Path First (OSPF) will be used within each campus for fast convergence. Areas will be designed to optimize traffic flow and contain routing updates.
- **Inter-Site & Internet Routing (BGP):** Border Gateway Protocol (BGP) will manage routing between HQs and to the Internet, providing policy-based control and resilience against link failures. BGP peering between ISPs ensures efficient routing across the wide area network.
- **Gateway Redundancy (VRRP):** The Virtual Router Redundancy Protocol (VRRP) will provide default gateway redundancy for end-users, ensuring seamless failover if a core switch fails.
- **Layer 2 Redundancy (MSTP):** Multiple Spanning Tree Protocol (MSTP) will create a loop-free Layer 2 topology while allowing for multiple VLANs to be load-balanced across redundant links.

4.2. Security Framework

Security is not an add-on but a foundational principle of this design.

- **Confidentiality:** All data between sites will be encrypted using **IPSec VPN tunnels** (AES-256 encryption). Guest Wi-Fi traffic will be isolated from the corporate network.
- **Integrity:** Protocol messages (OSPF, VRRP) will be authenticated using **MD5/SHA2** to prevent tampering.
- **Availability:** Firewalls with **Intrusion Prevention Systems (IPS)** will be deployed to mitigate threats like DDoS attacks. **AAA services** (Authentication, Authorization, Accounting) via RADIUS will control user access.
- **Access Control: 802.1X** will be implemented for network access control, ensuring only authorized devices can connect to switch ports.

4.3. Unified Communications & VoIP

The network will be engineered from the ground up to prioritize voice and video traffic.

- **Voice VLAN:** A dedicated VLAN will be configured for IP phones to isolate voice traffic from data noise.
- **Quality of Service (QoS):** Traffic will be classified and marked at the access layer. Voice packets will be assigned to a **strict-priority queue** to ensure they are never delayed by data traffic, guaranteeing crystal-clear call quality with a **Mean Opinion Score (MOS) above 4.0**.
- **Power over Ethernet (PoE):** Switches will provide PoE to power IP phones and wireless access points, simplifying cabling and power management.

4.4. Wireless Infrastructure

A centralized, secure Wi-Fi solution will be deployed.

- **Centralized Management:** Wireless Access Points (APs) will be managed by a central **Wireless LAN Controller (WLC)** using the **CAPWAP** protocol, simplifying configuration and monitoring.
- **Multiple SSIDs:** Separate SSIDs will be broadcast for corporate users (using WPA2-Enterprise/WPA3 security) and guests (using a captive portal for access).
- **Advanced Security: Wireless Intrusion Detection System (WIDS)** will be enabled to detect and contain rogue access points.

4.5. Network Management & Monitoring

Proactive management is key to maintaining health and performance.

- **SNMPv3:** Secure SNMP will be used for monitoring device health, interface errors, and traffic levels.
- **NetFlow/NetStream:** This technology will provide deep visibility into traffic patterns, helping to identify top talkers, applications in use, and potential security threats.
- **Syslog:** All network devices will send their logs to a central syslog server for archival and analysis, crucial for auditing and troubleshooting.

- **Automation:** Protocols like **NETCONF/YANG** will be leveraged for automated configuration backups and consistent device provisioning.

5. Project Scope & Deliverables

In-Scope:

- Supply and installation of new core routers, switches, firewalls, and WLCs at both HQ locations
- Upgrade of branch office routers and switches
- Deployment of new wireless access points across all sites
- Configuration of all routing, security, QoS, and wireless policies
- Implementation of network management and monitoring tools
- Documentation and knowledge transfer for [Company Name]'s IT team

Out-of-Scope:

- Procurement of end-user devices (laptops, IP phones)
- Application software development or configuration
- Structured cabling unless specifically identified as deficient

Final Deliverables:

- A fully operational, tested enterprise network
- As-built network design documentation
- IP Address Management (IPAM) database
- Standard Operating Procedure (SOP) documents for common tasks
- Training sessions for administrative staff

6. Benefits & Return on Investment (ROI)

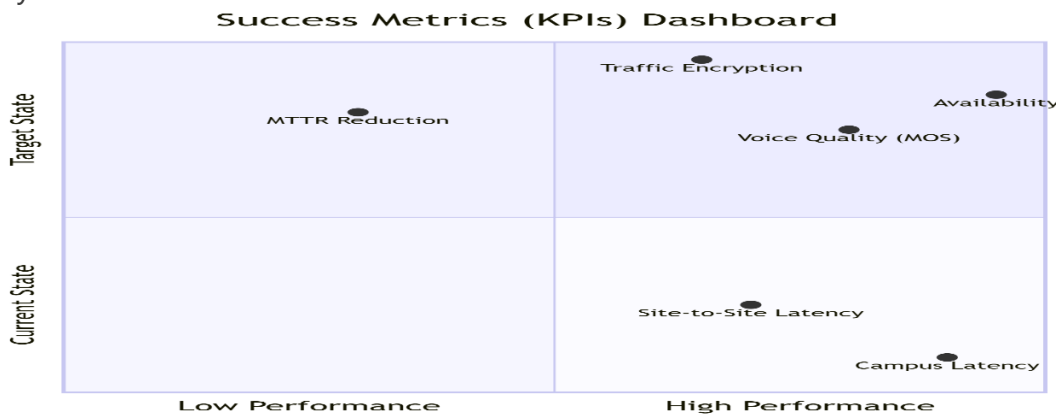
- **Operational Efficiency:** Automation and centralized management reduce the time spent on routine network tasks

- **Risk Mitigation:** Enhanced security and redundancy directly reduce the financial and reputational risk associated with downtime and data breaches
- **Productivity Gains:** A highly reliable network with superior voice and video capabilities removes barriers to employee collaboration
- **Cost Avoidance:** A scalable design avoids costly "rip-and-replace" projects in the future. Consolidating voice and data onto a single network reduces telecom expenses

7. Success Metrics (KPIs)

We will measure the success of this project against the following Key Performance Indicators (KPIs):

- **Availability: > 99.99% network uptime** across all critical sites
- **Voice Quality:** Mean Opinion Score (MOS) **> 4.0** for all VoIP calls
- **Network Performance: < 1ms** latency within campus; **< 50ms** latency between sites
- **Security: 99%** of inter-site traffic encrypted; **zero** successful cyber intrusions stemming from network vulnerabilities
- **Operation:** Reduction in Mean Time to Resolution (MTTR) for network issues by **50%**



Appendices

Appendix A: Proposed Hardware & Software

Location	Device Role	Proposed Model	Quantity
Egypt HQ	Core Router	AR6300 Series	2
	Core Switch	S12700 Series	2
	Firewall	USG6000 Series	1
	Access Points	AP8050DN	30
Saudi HQ	Core Router	AR6300 Series	2
	Core Switch	S12700 Series	2
	Firewall	USG6000 Series	1
	Access Points	AP8050DN	30
All Branches	Branch Router	AR2200 Series	4
	Access Switch	S5730 Series	8

Appendix B: Detailed Technical Configurations (Excerpts)

Sample OSPF Configuration:

```
router id 172.16.255.1
area 0
 authentication-mode md5


 network 172.16.0.0 0.0.255.255
```

Sample VRRP Configuration with Tracking:

```
interface Vlanif20
ip address 172.16.20.2 255.255.255.0
 vrrp vrid 1 virtual-ip 172.16.20.1
 vrrp vrid 1 priority 120
 vrrp vrid 1 track interface GigabitEthernet0/0/1 reduced 40 vrrp vrid 1 virtual-ip 172.16.20.1
 vrrp vrid 1 priority 120
 vrrp vrid 1 track interface GigabitEthernet0/0/1 reduced 40
```

Sample BGP Configuration (for ISP connectivity):

```
router bgp 65001
 neighbor 203.0.113.1 remote-as 65002
 network 10.1.0.0 mask 255.255.0.0
 network 10.2.0.0 mask 255.255.0.0
```

Appendix C: Glossary of Terms

- **BGP (Border Gateway Protocol):** The protocol that manages how packets are routed across the internet between autonomous systems.
- **CAPWAP:** Control And Provisioning of Wireless Access Points protocol.
- **IPSec:** A secure network protocol suite that authenticates and encrypts data packets.
- **OSPF (Open Shortest Path First):** A routing protocol used to determine the best path for packets within a single network.

- **QoS (Quality of Service):** Technology that manages network traffic to reduce packet loss, latency, and jitter.
- **VLAN (Virtual LAN):** A logical subnetwork that can group devices together, even if they are not connected to the same network switch.
- **VRRP (Virtual Router Redundancy Protocol):** A protocol that provides automatic assignment of available network routers to hosts.

8. Conclusion & Next Steps

This proposed network infrastructure provides a robust, secure, and scalable foundation that will empower [Company Name]'s digital business for years to come. It is engineered to meet today's demands while being flexible enough to adopt the technologies of tomorrow.

We recommend the following next steps:

1. **Technical Deep-Dive Meeting:** A meeting with your IT technical team to review detailed configurations
2. **Hardware Finalization:** A joint session to finalize the bill of materials based on exact port density and performance requirements
3. **Project Kick-Off:** To establish timelines, communication channels, and formalize the project team