Futurenostics

Redesigning the Enterprise Network for Futurenostics

A Scalable, Secure, and Resilient Architecture

Department Of CREATIVE TECHNOLOGIES
AIR UNIVERSITY
FCAI, ISLAMABAD

AIR UNIVERSITY

Prepared By

Name	Roll Number
Muhammad Ali	241383
Zain ul Abideen	241475
Ayesha Siddiqa	241419

Submitted To

Mam Amna Sarwar

The Client: Futurenostics' Critical Network Deficiencies

Client Profile

- **Organization**: Futurenostics (Software Development Firm)
- **Size**: 120 current employees, projected to 150+
- **Locations**: Islamabad HQ + 2 planned regional branches
- **Needs**: 99%+ uptime, 24/7 critical service availability, ISO 27001 readiness.

Identified Pain Points

- **Slowness & Bottlenecks**: Frequent lag impacting developer productivity.

- **Connection Drops:** Users regularly lose wired and Wi-Fi connectivity.

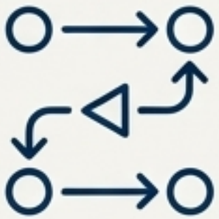
- **Critical Security Gaps**: Lack of departmental data isolation and threat monitoring (no IDS/IPS).

- **Poor Wi-Fi Coverage:** Dead spots in key office areas.

- **Single Point of Failure**: No internet redundancy, causing complete outages.

Project Objectives: Architecting for Growth and Resilience

To design and implement a robust network that solves current performance issues and provides a scalable foundation for Futurenostics' future growth.

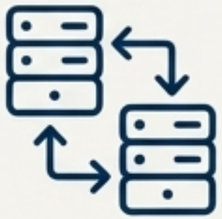


Build a Scalable Routing Fabric

Implement a multi-area OSPF design to support multi-site expansion efficiently.

Enhance Network Security

Deploy a multi-layered security model with firewalls, ACLs, and IDS/IPS to protect sensitive IP and financial data.



Guarantee High Availability

Eliminate single points of failure by implementing Dual-WAN redundancy and HSRP for internal gateway failover.

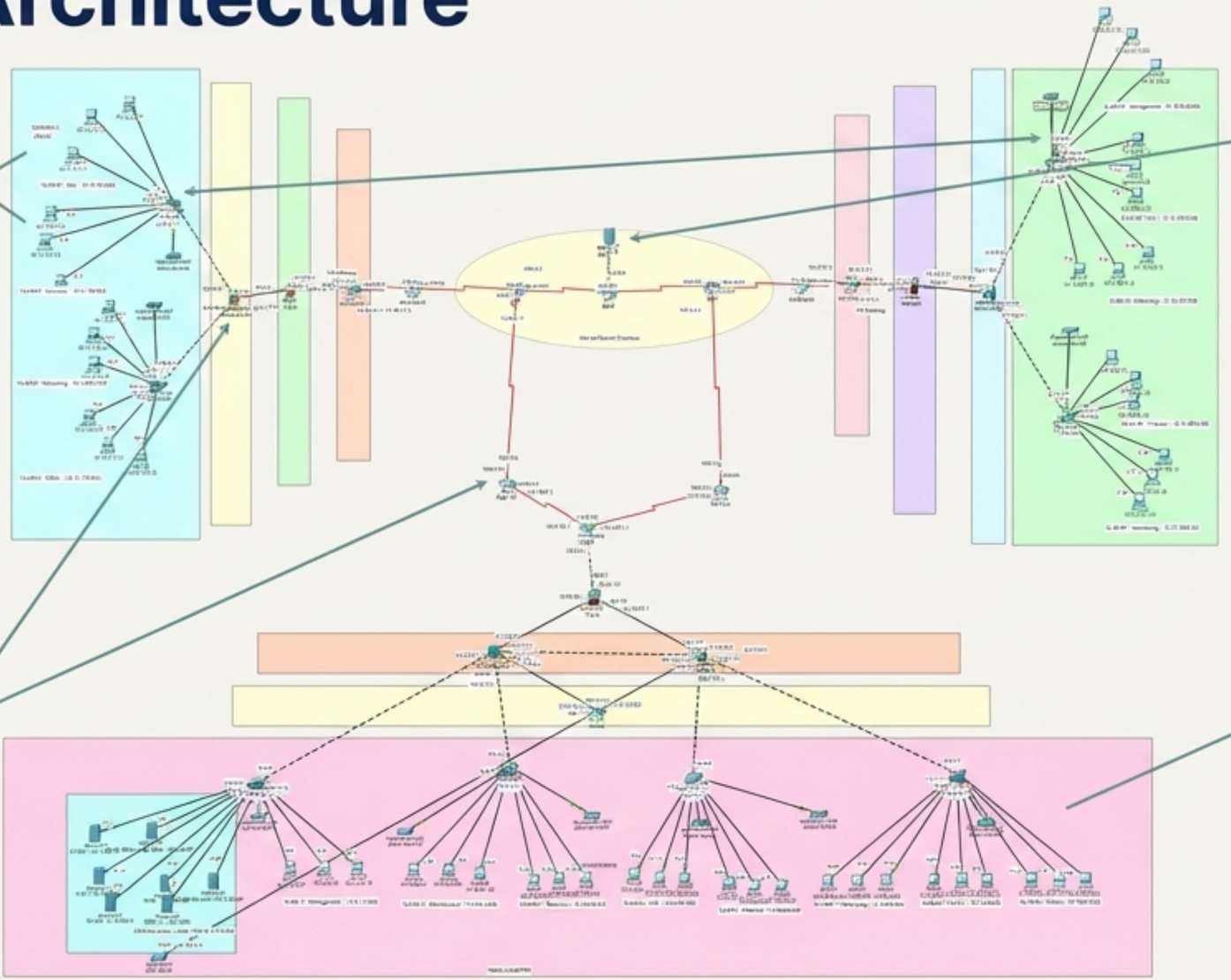
Improve Performance

Segment the network with 18 VLANs to reduce broadcast traffic and enforce departmental isolation.

Centralize Core Services

Configure dedicated servers for DHCP, DNS, and other critical applications to ensure reliable access.

The Solution: A Hierarchical, Multi-Site Network Architecture



2 **Branch Offices (A & B):** Standardized, secure branch designs capable of independent operation while maintaining full connectivity to HQ.

3 **Redundant WAN Core:** A simulated internet backbone with dual ISP connections to HQ, providing high availability and load balancing.

4 **Multi-Layer Security:** ASA Firewalls deployed at the perimeter of each site (HQ, Branch A, Branch B) to enforce security policies.

1 **Headquarters (HQ):** The central hub with core services, a dedicated Data Center, and robust internal segmentation.

The Blueprint: A Scalable IP Addressing & Subnetting Plan

Overall Strategy

- **Main Enterprise Block**
  10.10.0.0/16 provides a large, private address space for scalability.
- **Hierarchical Allocation**
  IP blocks are logically assigned to HQ, Data Center, and Branch offices.
- **WAN Backbone**
  100.0.0.0/8 is used for all point-to-point WAN links.

Scalability Metric

5%

The current design supports 4,572 hosts, using only 5% of the total capacity. This allows for over 4,300 additional users without requiring re-addressing.

VLSM Address Allocation Summary

VLAN ID	Department	Site(s)	Network Subnet	Hosts
10	Management	HQ, Branch B	10.10.10.0/24, 10.10.210.0/24	254 per subnet
20	Development	HQ, Branch A, B	10.10.20.0/24, 10.10.120.0/24, etc.	254 per subnet
30	Business	HQ, Branch A, B	10.10.30.0/24, 10.10.130.0/24, etc.	254 per subnet
40	HR	HQ	10.10.40.0/24	254
50	Finance	HQ, Branch B	10.10.50.0/24, 10.10.250.0/24	254 per subnet
60	Networking	All Sites	10.10.60.0/24, etc.	254 per subnet
70	CCTV	HQ, Branch A	10.10.70.0/24, etc.	254 per subnet
80	Servers	HQ Data Center	10.10.80.0/24	254
90	Guests	HQ	10.10.90.0/24	254

Segmenting the Enterprise: LAN Design with 18 VLANs

Strategic goal: Isolate network traffic by department to enhance security, improve performance by reducing broadcast domains, and simplify network management.

Site-Specific VLAN Distribution

Headquarters (9 VLANs)

- Mgmt
- Dev
- Business
- HR
- Finance
- Networking
- CCTV
- Servers
- Guests

Each VLAN is assigned a unique /24 subnet (e.g., VLAN 10: 10.10.10.0/24).

Branch A (4 VLANs)

- Dev
- Business
- Networking
- CCTV

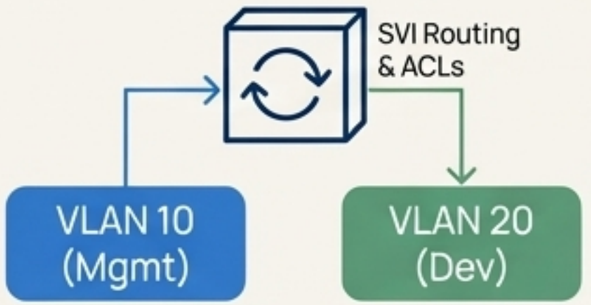
Branch B (5 VLANs)

- Mgmt
- Dev
- Business
- FInance
- Networking

Inter-VLAN Routing

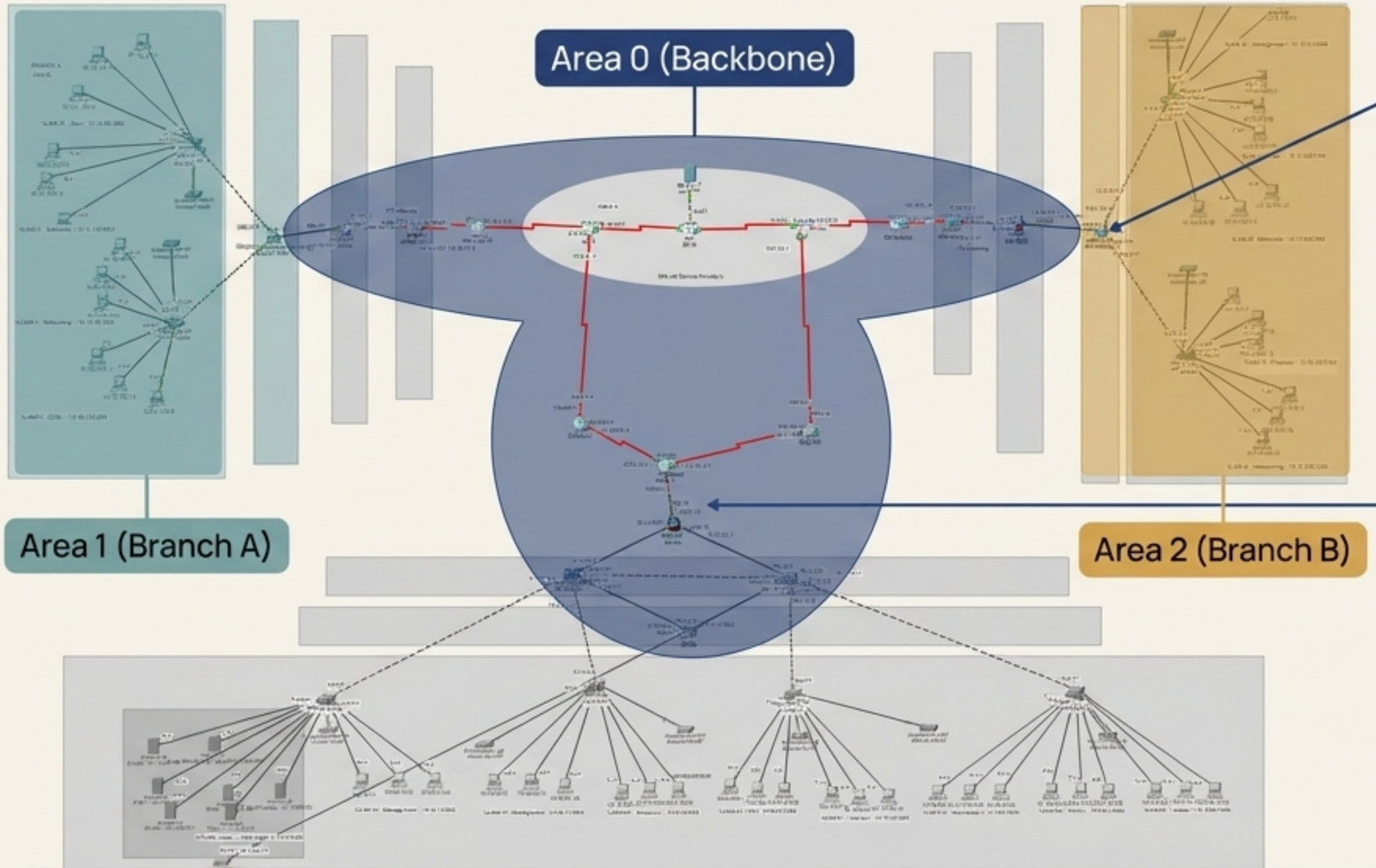
Mechanism: Implemented using Switch Virtual Interfaces (SVIs) on Layer-3 Multilayer Switches at each site.

Benefit: Enables controlled communication between departments while maintaining segmentation, with policies enforced by ACLs.



Building the Backbone: OSPF Multi-Area Routing for Scalability

OSPF (Open Shortest Path First) was selected for its scalability, fast convergence, and support for hierarchical, multi-area design.

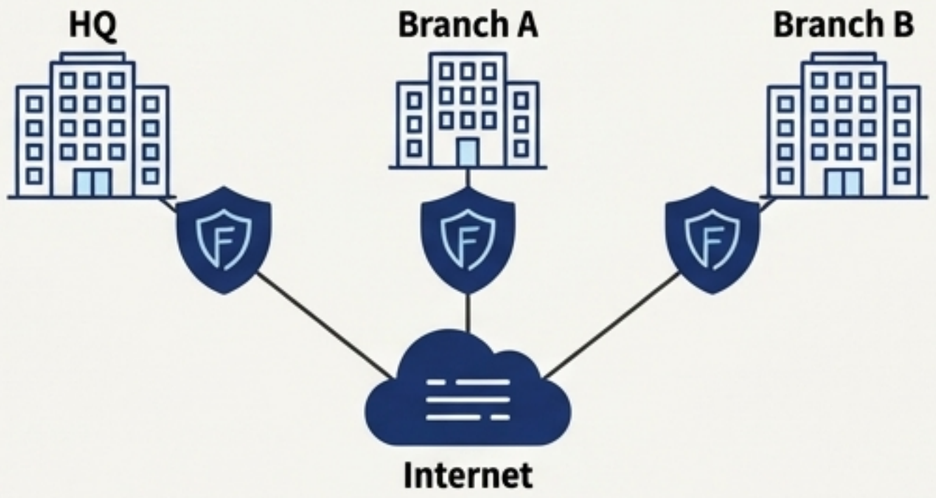


Area Border Routers (ABRs): Devices like BA-Edge-R and BB-Edge-R connect Area 1 and 2 to the Area 0 backbone, summarizing routes.

Backbone Routers: Devices like HQ-Core-R handle the high-volume traffic across the core network.

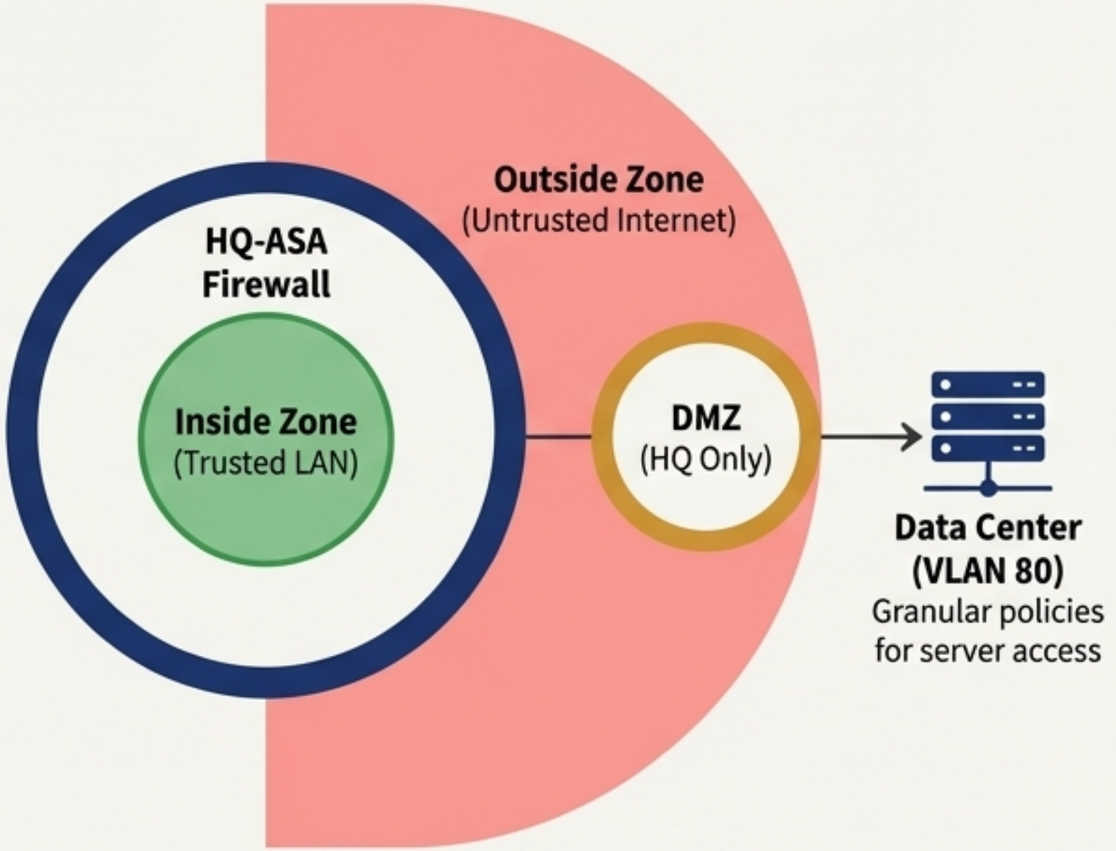
Fortifying the Enterprise: A Multi-Layered Security Architecture

Three-Tier Firewall Model



Firewall	Location	Primary Responsibility
HQ-ASA	HQ Perimeter	Main internet gateway defense, NAT for all HQ traffic, protection of the central Data Center.
BA-ASA	Branch A Perimeter	Secures Branch A from external threats and enforces local access policies.
BB-ASA	Branch B Perimeter	Secures Branch B from external threats and enforces local access policies.

Zone-Based Security



NAT Implementation: All firewalls perform Network Address Translation (NAT), mapping internal private IP addresses to a public IP for secure internet access.

Enforcing Policy: Granular Control with Access Control Lists (ACLs)

Objective: To enforce the principle of least privilege, ensuring departments and users can only access the resources necessary for their roles.

Key Security Policies Implemented

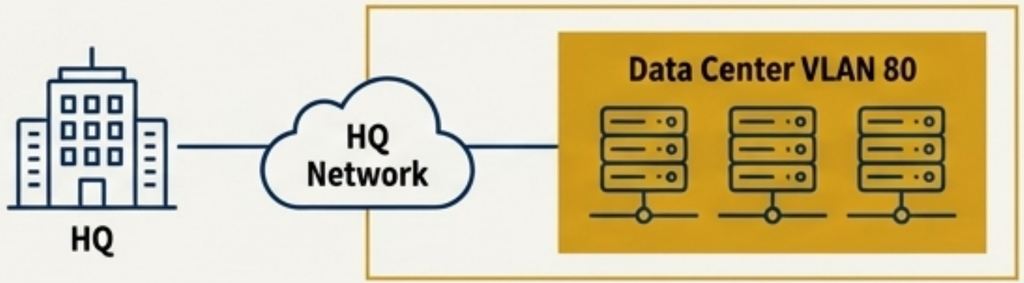
Policy ID	Rule Description	Source VLAN(s)	Destination VLAN(s)	Action
ACL-GUEST-ISO	Isolate Guest users from all internal resources.	Guest (90)	Any Internal	**DENY**
ACL-CCTV-LIMIT	Restrict CCTV cameras to only communicate with the Data Center.	CCTV (70)	All except Servers (80)	**DENY**
ACL-FIN-HR-SEP	Prevent direct access between Finance and HR departments.	Finance (50)	HR (40)	**DENY**
ACL-HR-FIN-SEP	Prevent direct access between HR and Finance departments.	HR (40)	Finance (50)	**DENY**
ACL-MGMT-ACCESS	Allow Management full access for administrative purposes.	Management (10)	Any	**ALLOW**

Port Security

- Implemented on all user-facing access ports.
- **Configuration**: Maximum of 1 MAC address per port.
- **Violation Action**: `shutdown` – the port is automatically disabled if an unauthorized device is connected, preventing rogue access.

Powering the Business: Centralized Server Infrastructure

A dedicated and secured VLAN 80 (10.10.80.0/24) hosts all critical enterprise servers at HQ.

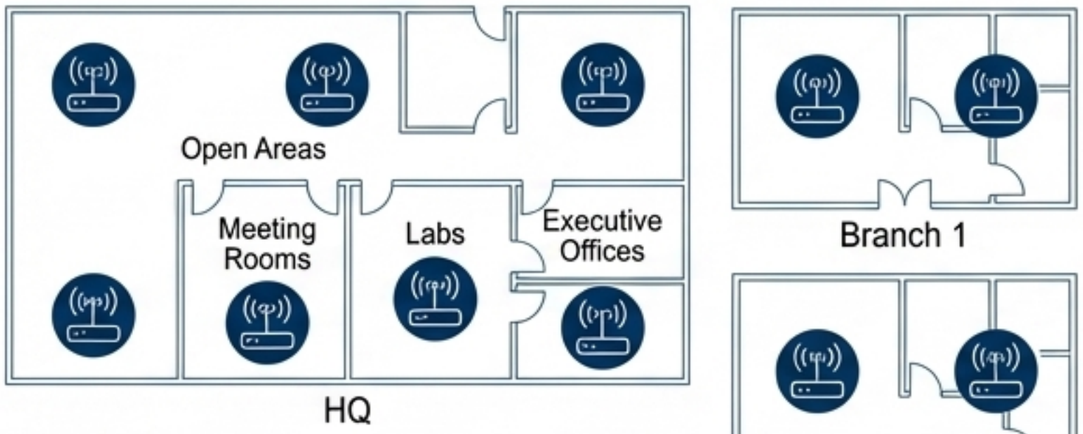


Core Services Deployed

Server	IP Address	Service	Purpose
DHCP-Server	10.10.80.10	DHCP	Provides dynamic IP assignment for all 18 VLANs across all 3 sites.
DNS-Server	10.10.80.20	DNS	Manages internal name resolution for `futurenostics.local`.
Web-Server	10.10.80.30	HTTP/S	Hosts the company's internal web portal and documentation.
FTP-Server	10.10.80.40	FTP	Facilitates secure file sharing for the development teams.
Mail-Server	10.10.80.50	SMTP/IMAP	Handles all internal corporate email communication.
AD-Backup	10.10.80.60	AD / Backup	Manages user authentication and critical data backups.

Enabling Mobility: A Secure and Optimized Wireless Design

Coverage Strategy

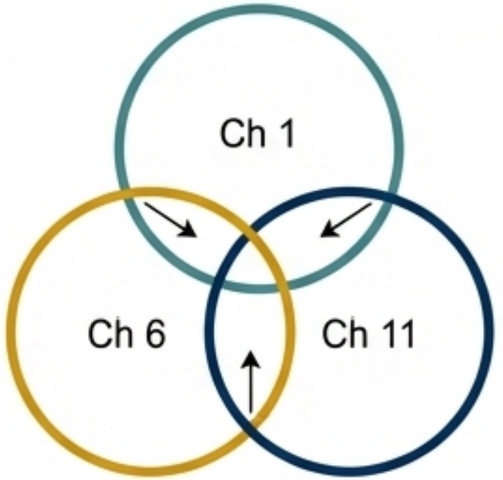


HQ: 6 Access Points strategically placed for 95%+ coverage across open areas, meeting rooms, labs, and executive offices.

Branches: 2 APs per branch to cover main office areas and secure rooms.

Optimized Channel Allocation

Goal: Minimize co-channel interference and maximize throughput.



2.4 GHz Band: Non-overlapping channels 1, 6, and 11 are used across adjacent APs.

5 GHz Band: Higher-capacity channels are leveraged for performance-critical areas like the Dev Lab.

Secure Guest Network Isolation

SSID: Futurenostics-Guest

VLAN: Segregated on VLAN 90 (10.10.90.0/24)

Security

- Complete isolation from all internal corporate resources.
- Internet-only access.
- Bandwidth limited to 5 Mbps per client to protect performance for corporate users.

Validation: Network Performance and Connectivity Test Results

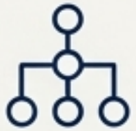
A comprehensive suite of tests was conducted to measure latency and packet loss across all segments of the network.

Test Scenario	Path Example	Measured Latency	Target	Status
Intra-VLAN (L2)	HQ Dev PC ↔ HQ Dev Printer	**< 1ms**	< 2ms	✓ PASS
Inter-VLAN (L3)	HQ Mgmt (VLAN 10) ↔ HQ Dev (VLAN 20)	**2.1ms**	< 5ms	✓ PASS
HQ ↔ Branch A	HQ Server (VLAN 80) ↔ BA Dev (VLAN 20)	**4.5ms**	< 100ms	✓ PASS
HQ ↔ Branch B	HQ Mgmt (VLAN 10) ↔ BB Mgmt (VLAN 10)	**4.8ms**	< 100ms	✓ PASS
Branch A ↔ Branch B	BA Dev (VLAN 20) ↔ BB Dev (VLAN 20)	**5.1ms**	< 100ms	✓ PASS

The network meets and exceeds all performance goals, providing a fast and reliable experience for all users, both within and between sites. All tests showed 0% packet loss.

Exceeding Expectations: Advanced Features and Creative Extensions

To ensure the network is truly enterprise-grade, several features beyond the core requirements were implemented to enhance resilience, security, and scalability.

	Feature	Implementation Detail	Benefit to Futurenostics
	**Dual-WAN Redundancy**	Two edge routers at HQ with load balancing configured.	Guarantees 99.9%+ internet uptime, eliminating a critical single point of failure.
	**HSRP Gateway Failover**	Hot Standby Router Protocol between two L3 switches in HQ.	Provides seamless internal gateway failover, ensuring continuous LAN connectivity.
	**IDS/IPS Threat Detection**	Simulation of ICMP Flood and Port Scan attack detection.	Provides real-time threat monitoring and protection against common network attacks.
	**Hierarchical OSPF Design**	Multi-Area (0, 1, 2) implementation with ABRs.	Reduces routing overhead and improves scalability as more branches are added.
	**Automated Port Security**	Access ports automatically shut down upon MAC violation.	Prevents unauthorized device connections and enhances physical security.

The Complete Architecture: A Fully Integrated Enterprise Network