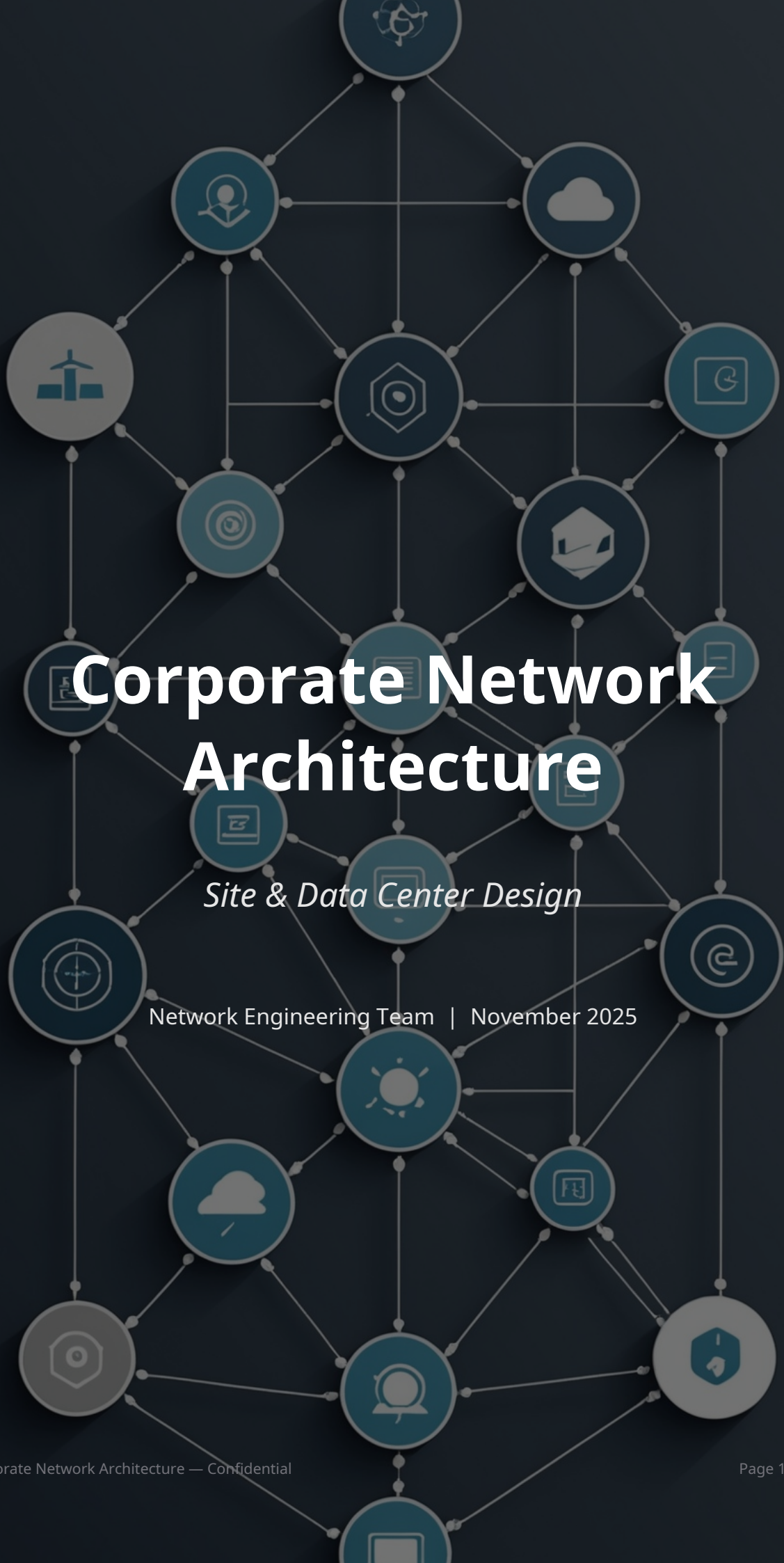




Corporate Network Architecture

Site & Data Center Design

Network Engineering Team | November 2025

Table of Contents

- Executive Overview 3
- Physical Network Topology 4
- Data Center Rack Layout 5
- WAN / Site Connectivity Diagram 6
- IP Addressing & VLAN Table 7
- Firewall & Security Zones 8
- Redundancy & Failover 9
- Wireless Coverage Plan 10
- Disaster Recovery Site 11

Executive Overview

This document presents the comprehensive network architecture for the corporate headquarters, branch sites, and central data center. It defines the physical topology, addressing scheme, security zoning, redundancy mechanisms, wireless coverage strategy, and disaster recovery posture that together ensure a resilient, secure, and scalable infrastructure.

The design follows a hierarchical core-distribution-access model with dual redundant paths at every critical layer, segmented security zones enforced by perimeter and internal firewalls, and a fully replicated disaster recovery site to guarantee business continuity.

This report is intended for network engineering, security, and operations teams responsible for implementation, auditing, and ongoing maintenance of the corporate network estate.

Physical Network Topology

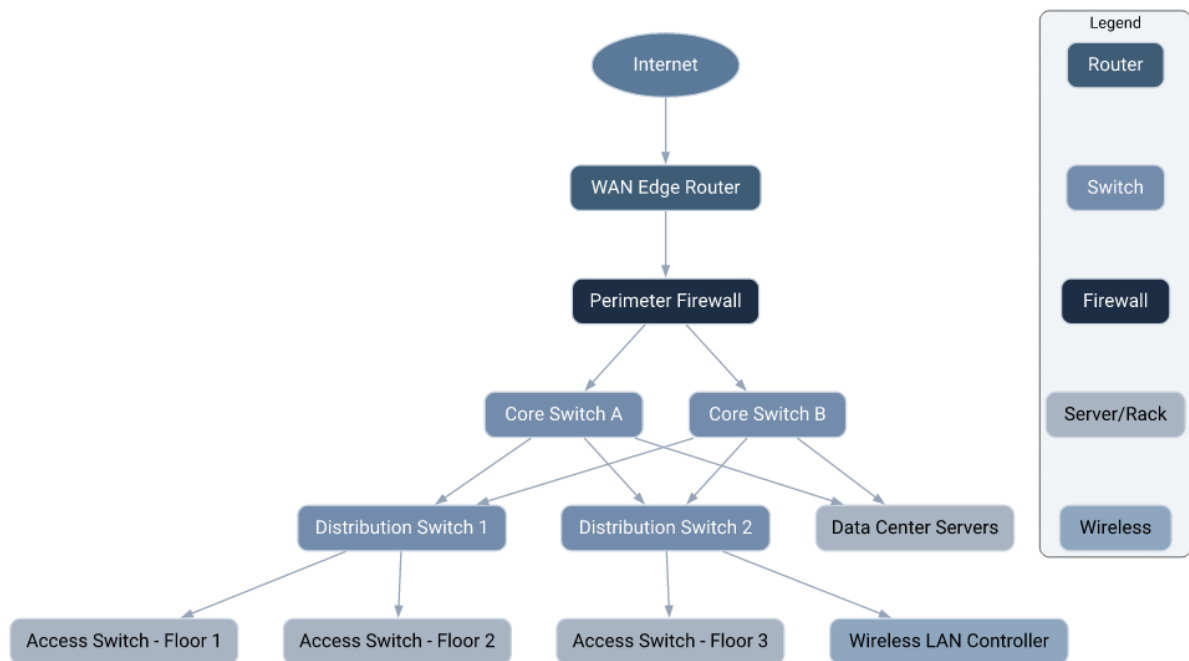


Figure 1: Physical Network Topology (Legend included)

The physical topology follows a three-tier hierarchical design consisting of core, distribution, and access layers. Redundant core switches interconnect with dual distribution switches, which fan out to per-floor access switches and the wireless LAN controller, ensuring no single point of failure between the edge and the data center.

Data Center Rack Layout

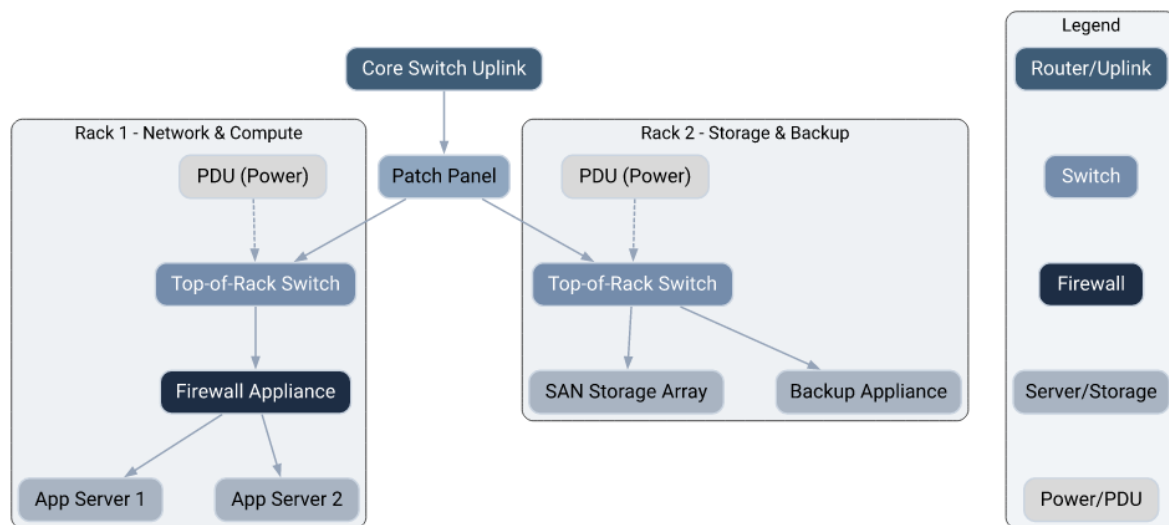


Figure 2: Data Center Rack Layout (Legend included)

The data center comprises two primary racks: Rack 1 hosts network and compute resources including the top-of-rack switch, firewall appliance, and application servers; Rack 2 hosts SAN storage and backup appliances. Both racks uplink through a shared patch panel to the core switching layer.

WAN / Site Connectivity Diagram

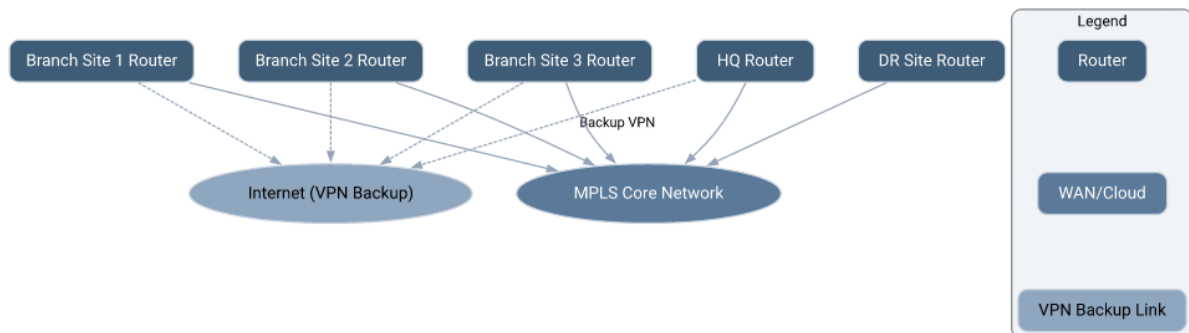


Figure 3: WAN and Site Connectivity (Legend included)

Headquarters, three branch sites, and the disaster recovery site connect via a primary MPLS core network, with Internet-based VPN tunnels providing automatic backup connectivity in the event of MPLS circuit failure at any site.

IP Addressing & VLAN Table

Table 1: VLAN and IP Addressing Scheme

VLAN ID	Name	Subnet	Gateway	Purpose
10	Management	10.10.10.0/24	10.10.10.1	Network device management
20	Servers	10.10.20.0/24	10.10.20.1	Data center servers
30	Workstations	10.10.30.0/24	10.10.30.1	Corporate end-user devices
40	VoIP	10.10.40.0/24	10.10.40.1	Voice traffic
50	Wireless	10.10.50.0/24	10.10.50.1	Wireless client access
60	DMZ	10.10.60.0/24	10.10.60.1	Public-facing services
99	Guest	10.10.99.0/24	10.10.99.1	Guest internet access

Firewall & Security Zones

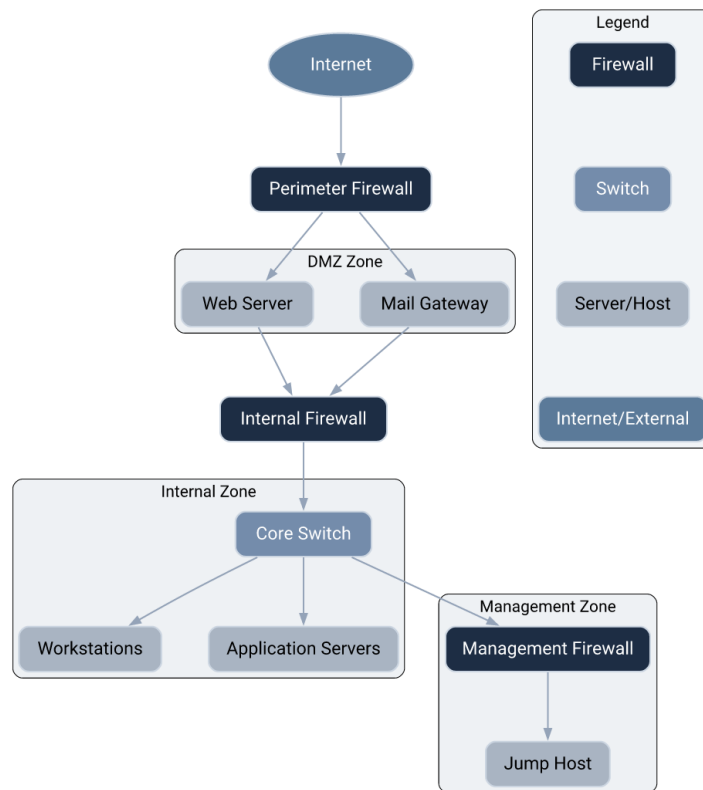


Figure 4: Firewall and Security Zones (Legend included)

Traffic is segmented into four security zones: Internet, DMZ, Internal, and Management. A perimeter firewall inspects all inbound/outbound traffic to the DMZ, while a second internal firewall enforces policy between the DMZ and internal network. A dedicated management firewall isolates administrative access via a hardened jump host.

Redundancy & Failover

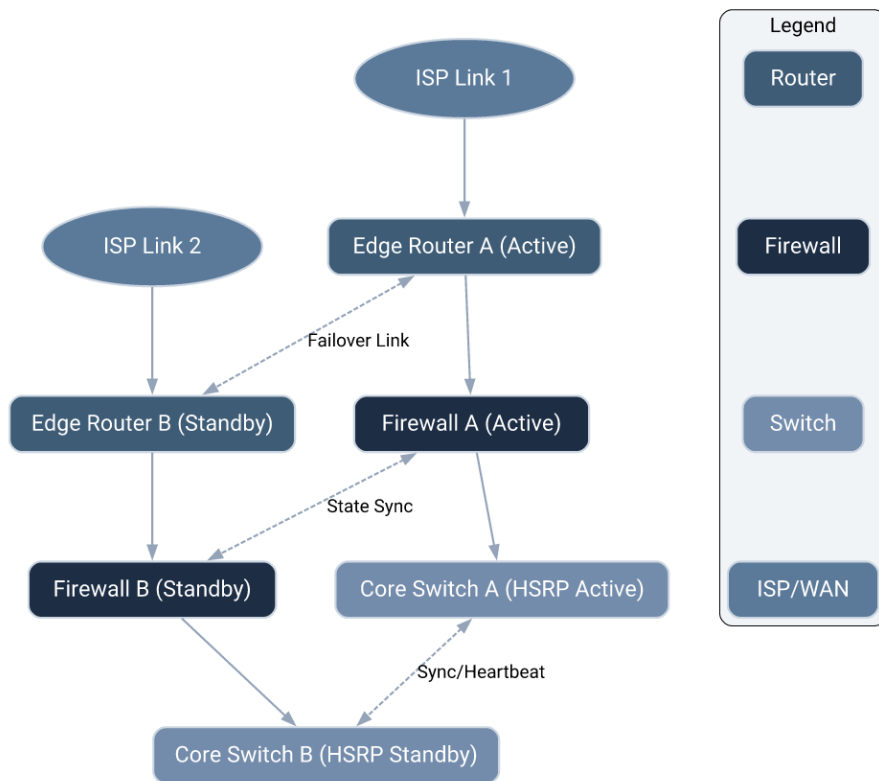


Figure 5: Redundancy and Failover Architecture (Legend included)

Every critical layer is deployed in active/standby pairs: dual ISP links terminate on redundant edge routers, dual firewalls maintain synchronized state, and dual core switches run HSRP for transparent gateway failover. Heartbeat and state-sync links ensure sub-second convergence during a failure event.

Wireless Coverage Plan

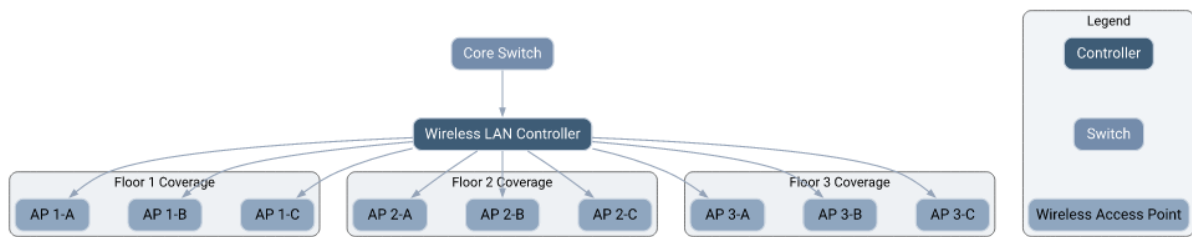


Figure 6: Wireless Coverage Plan (Legend included)

Wireless coverage is provided across three floors, each served by a cluster of access points managed centrally by the wireless LAN controller, which uplinks through the core switch. This centralized model enables consistent roaming, unified policy enforcement, and simplified RF management across the site.

Disaster Recovery Site

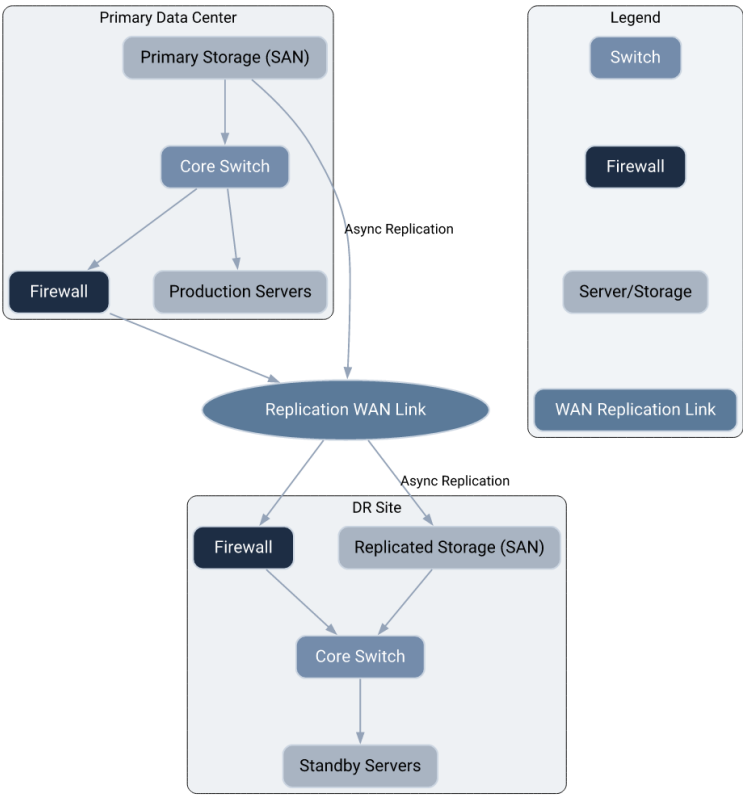


Figure 7: Disaster Recovery Site Architecture (Legend included)

The disaster recovery site mirrors the primary data center's core switching, firewall, server, and SAN storage tiers. Asynchronous replication over a dedicated WAN link keeps DR storage current, enabling rapid failover of production workloads in the event of a primary site outage.