IT Infrastructure and Network Design

Sushanta Poudel

Summary

Problem Description

Task 2, first and foremost, has recently defined the main problem as the absence of a coherent, robust, and scalable IT network design and infrastructure plan for a significant corporate expansion. The corporation was purchasing a new multi-story corporate office building designed for some 600 users. This issue was at a scale and level of complexity completely out of line with what the organization was used to. Severe operational degradation and an inability to properly segment security, leading to an environment incapable of handling high traffic density as a level one, and sufficiently large operational costs in the near future as the second, would be the constitution of risk that the organization was willing to accept without having an engineered and detailed design. The problem can be seen essentially as a planning and design gap for large-scale enterprise-level network deployments.

Project Execution Process

A formalized **Phased/Waterfall** approach was used to execute the project. It was selected because it lends itself well to a complex design and documentation project, in which the requirements must be fully defined before any design can proceed. The process was split up into four sequential phases:

Research & Discovery: Gathering of detailed requirements specific to the 600-user capacity, multi-story building layout, and security and regulatory compliance standards.

Design & Specification: Designing of the Core, Distribution, and Access (three-tier) network topology, and development of the hierarchical IP addressing and VLAN schema, and the best choice in high-capacity enterprise-class hardware.

Documentation & Reviews: Creation of all project-level formal deliverables such as Logical and Physical Topology Diagrams, full Bill of Materials (BOM), Rack Elevation Diagrams, and the Design Rationale (initial).

Finalization and Paper Drafting: Incorporation of comments from peers and stakeholders (including those resulting from unforeseen scope creeps), finalization of all design artifacts, and completion of the technical paper that details the design decisions.

Project Outcomes

The project successfully delivered a comprehensive, validated IT infrastructure design package that serves as a secure, scalable, and cost-effective blueprint for the 600-user corporate expansion. Briefly, the outcomes deliver:

High-Capacity Network Architecture: A hierarchical, redundant 3-tier logical topology eliminating any single point of failure.

Security Segmentation with Granular Enforcement: Clear IP Addressing and VLAN Schema, describing separate zones (e.g., Data, Voice, Management, Guest) to adhere to the principle of least privilege.

Actionable Implementation Plan: Detailed Hardware and Software BOM, along with Rack Elevation Diagrams, allow implementation to be performed with precision and speed from the deployment team's end. The final design, therefore, fulfilled all success criteria as it provided a documented solution that can be verified against industry best practice for a large-scale enterprise environment.

Review of Other Work

This section provides a concise overview of three new professional works essential for assisting in the execution and justification of network infrastructure design, implementing best practices, security integration, and cost justification.

Work 1: ZTA for Enterprise Networks (Cisco, 2023)

This paper represents the Zero Trust Architecture (ZTA), which replaces the traditional perimeter-based security model, requiring the strict identification of every user and device attempting to access resources from anywhere (Cisco, 2023). It advocates for micro-segmentation, where network access is granted on a least privileged basis; such an approach has significantly limited the possibility of lateral movement in the event of a breach.

Work 2: TIA-568-D Commercial Building Telecommunications Cabling Standard (Telecommunications Industry Association, 2018)

TIA-568-D establishes technical standards for telecommunications cabling infrastructure in commercial buildings, encompassing horizontal and backbone cabling installation requirements, best practices, and administration (TIA, 2018). It sets standards for various cable types, including Cat 6A for 10Gbps horizontal runs and multi-mode fiber (OM4) for high-speed backbone connections between wiring closets and the primary data center, among others.

Work 3: Total Cost of Ownership (TCO) Analysis for Next-Generation Networking Hardware (Gartner Research, 2022)

This study presents a methodology for measuring the real financial impact of an investment in order technology over its life expectancy, rather than just the initial capital expenditure (Gartner Research, 2022). This model includes installation, electricity, cooling, maintenance, licensing costs, and important considerations such as loss-producing downtime due to failure. In effect, it suggests that a heavier upfront price of hardware would likely translate into a lower TCO because it offers better reliability, lower maintenance, and better performance.

Explanation of How Each Work Supported the Implementation

Support from ZTA (Cisco, 2023): As the foundational framework, ZTA was utilized to design the **IP Addressing and VLAN Schema Documentation**. This ensured that Objective 1.2 (Implement advanced security controls) was addressed, so that the VLAN structure must have involved mandatory micro-segmentation and not been implemented for organizational convenience. This approach has steered the definition of Access Control Lists (ACLs) to limit communications severely between segments (such as preventing access users from accessing the Management network) and supported the choice of the core switching platform with capabilities for deep security policy enforcement and deep packet inspection.

Support of TIA-568-D (TIA, 2018): This standard was the real technical specification for the **Physical Topology Diagram** and the **Hardware and Software BOM**. By applying the TIA-568-D, the design was felt to be future-proofed in the sense that it mandated Cat 6A cabling for all horizontal runs (which provides for desktop speeds of 10Gbps), along with OM4 fiber for the building backbone (providing high-capacity links between distribution switches and the core). This design thus eliminated the possibility of expensive re-cabling in the future, thus directly supporting the criteria of scalability and cost-effectiveness.

Support from TCO Analysis (Gartner Research, 2022): The TCO analysis was used for the financial justification given in the **Design Rationale and Technical Paper**. It enabled the project to argue for the inclusion of high-end, enterprise-grade modular core switching and redundant hardware (Goal 3: Deliver a Cost-Effective Plan). The TCO model demonstrated that, although these components have a higher upfront cost, their superior MTBF and savings over five years of operation (resulting in lower maintenance and energy costs) yield a lower TCO than the cheaper and less reliable alternatives.

Changes to the Project Environment

The completion of this project led to significant, positive shifts in the organization's approach to IT infrastructure, transitioning it from a reactive maintenance posture to a proactive, engineering-driven strategy.

Organizational Culture Shift

The culture change emphasized documenting all things with rigorous change management. Infrastructure changes were carried out ad-hoc and without documentation prior to the project. The professional and comprehensive design artifacts (Logical/Physical Diagrams, BOM, Rationale) created a new baseline expectation for all future IT projects. Stakeholders now understand the benefits of the 'design-first' approach, ensuring that any proposals for changes are mandatorily reviewed against the existing design standards.

Strategic and Environmental Changes

Strategic Asset Management: The infrastructure became viewed as a strategic asset in the long term. TCO analysis embedded into the Design Rationale led to the strategic decision to extend the projected life of the core network equipment from five to ten years and to specify comprehensive vendor maintenance agreements in BOM.

Risk Reduction: The Success of Goal 1 (Secure and Reliable Network) further elevated the need for security segmentation. The organization adopted an official policy requiring Zero Trust across all future IT initiatives, thus guiding the environment toward a stronger default security posture.

Scalability: The IP/VLAN hierarchical scheme, designed for scaling beyond 600 initial users (such as a multi-site WAN), is now a mandated template for any future satellite office expansions. This, in turn, enables the streamlining of planning and integration, and by extension, significantly reduces the lead time for any future projects.

Methodology

The project was handled using the **Phased/Waterfall Method**, following the linear order of the four phases to ensure complete consideration and quality of documentation before proceeding to physical implementation.

Phase 1: Research & Discovery (Requirement Gathering)

This phase focused on identifying the precise operational needs of 600 users within the environment.

Execution: Detailed user profiles were extracted from department headcount data, comprising 500 data users and 100 voice/call center users, which set the required PoE budget and port density. The four-story building layout was then analyzed to confirm that a minimum of four wiring closets would be required (one per floor), along with an additional central data center. The enterprise security standards (such as two-factor authentication being mandatory) were then factored into what would become distinct security zones in Phase 2.

Phase 2: Design & Specification (Network Engineering)

This was the heart of the engineering effort, taking the requirements established and turning them into technical specifications.

Execution: A three-tiered logical topology was designed, with attention given to defining the roles of the hardware: core switches consisting of a modular pair for redundancy, distribution switches per floor with high density, and Access switches with PoE. The private IP space of 10.0.0.0/16 was allocated and hierarchically divided (i.e., 10.10.x.x for Data, 10.20.x.x for Voice, etc.). High-availability protocols would be implemented (VRRP/HSRP for default gateway redundancy, LACP for aggregated distribution links). During this phase, unexpected scope creep ("Unanticipated Scope Creep") would prompt the inclusion of a hardware firewall cluster design.

Phase 3: Documentation and Review (Artifact Creation)

At the core of architectural design decisions lies the formal documentation of such decisions, packaged as final deliverables.

Execution: Physical and Logical Topology designs were prepared in exquisite detail using Visio diagrams detailing cable runs, patch panel layouts, and logical routing paths. The Bill of Materials with detailed model numbers and current prices was also finalized, along with a TCO justification (Work 3). Rack Elevation Diagrams were created, defining precise U-space allocation for every device (switches, servers, firewalls, PDUs) in each closet and the data center.

Phase 4: Finalization and Drafting of Paper (Completion)

This stage brought about quality assurance and final signoffs.

Execution: All comments received from the peer review were addressed thoroughly. One such comment included adding specific QoS policies to prioritize Voice (VLAN 10.20.x.x) traffic over data traffic in the Distribution switch configuration guides. All documents were ensured to be consistent, and the technical paper was finalized, which provides a detailed explanation of the architectural rationale.

Project Goals and Objectives

The project's three main goals were successfully accomplished. In detail, Goal 1 was achieved in the following way:

Goal 1: Design a Secure and Reliable Network Infrastructure (600 Users).

Objective 1.1: Define a resilient and redundant network topology that minimizes single points of failure and maximizes availability for 600 users.

Accomplishment: Achieved. The Logical Topology Diagram (Artifact 1) verified the accomplishment of this objective by providing redundant three-tier architecture:

Core Layer: Two modular switches were configured in high-availability mode (VSS/StackWise), thereby removing the core as a possible single point of failure.

Distribution Layer: Each of the four Distribution switches (one per floor) was connected to both Core switches via aggregated fiber links using LACP, providing link and device redundancy.

Redundant Power Supplies: All Core and Distribution switches specified in the BOM come equipped with dual hot-swappable power supplies to ensure uninterrupted operations.

Objective 1.2: Apply advanced security controls by means of network segmentation and policy implementation, e.g., firewall policy, in order to safeguard internal resources.

Accomplishment: Achieved. Four main segments were defined in the IP Addressing and VLAN Schema Documentation (Artifact 2): Data (VLAN 10), Voice (VLAN 20), Management (VLAN 50), and Guest (VLAN 99). A very strong security perimeter was enforced nicely in line with ZTA principles (Work 1).

Control Implementation: Inter-VLAN routing is limited to the Core, where Stateful ACLs restrict lateral communications among segments (e.g., Data users cannot access the Management network) unless expressly required for some offering, thereby safeguarding critical resources. This helped protect the resources from further threats with the successful integration of a dedicated hardware cluster firewall ("Unanticipated Scope Creep") externally.

Project Timeline

An autumn 2024 timeframe was provided for the project's execution. The project timeline was overall maintained by absorbing the lost time during the subsequent documentation phase, despite the three-day delay that Phase 2 suffered due to unforeseen scope creep.

Milestone	Projected Start Date	Projected End Date	Actual Start Date	Actual Completion Date	Difference
Phase 1: Research & Discovery (7 days)	10/14/2024	10/22/2024	10/14/2024	10/22/2024	**On Time**
Phase 2: Design & Specification (12 days)	10/23/2024	11/07/2024	10/23/2024	11/10/2024	**+3 Days**
Phase 3: Documentation & Review (8 days)	11/08/2024	11/18/2024	11/11/2024	11/20/2024	**-1 Day** (Compressed)
Phase 4: Finalization & Drafting (5 days)	11/19/2024	11/25/2024	11/21/2024	11/25/2024	**On Time**

Explanation of Timeline Differences

The main deviation occurred in **Phase 2,** resulting in a three-day delay. This occurred due to unanticipated stakeholder requirements to incorporate specifications for the hardware firewall cluster (refer to "Unanticipated Scope Creep").

Time was subsequently made-up during **Phase 3** (Documentation & Review). The eight original days of this phase were shortened slightly to seven days of active work. This was due to the comprehensive scoping of technical details for the firewall cluster in Phase 2, which allowed for efficient drafting of documentation in Phase 3. The project was successfully delivered on the anticipated date of November 25, 2024, by completing subsequent phases.

Unanticipated Scope Creep

Problem description

During Phase 2 (Design & Specification), a stakeholder requested that the scope be expanded on a mandatory basis to include technical design and the selection of **a highly available hardware firewall cluster** that manages all ingress/egress traffic, including site-to-site VPN capabilities. In the beginning, the project was to address an internal LAN design (switching, cabling, IP/VLAN segmentation) without including a hardware firewall per se. This was an unanticipated request that, if not handled properly, would have caused tremendous timeline and resource-related issues.

Resolution

There was a successful resolution to the problem, following a controlled change management procedure:

> **Impact Assessment:** The project manager quickly assessed that the request was critical to the organization's security posture and thus aligned with Goal 1 (Secure Network). The core network topology (switching, IP schema) remained unchanged; all that needed their

attention was the integration of the firewall cluster between the Core switches and the ISP handoff.

Negotiated Resolution: The stakeholder agreed that, because it would require at least three extra days in Phase 2 to conduct the design research, sizing, and BOM integration, they would rather prioritize security and accept the offered time extension.

Integration: The three days were spent sizing the cluster to make sure it was appropriate for handling simultaneous traffic from 600 users, choosing a model, integrating its placement in the Logical Diagram (connecting to the Core switches), and updating the BOM (Artifact 3) for necessary licensing and hardware costs.

Through a formal and immediate approach to the change, the project team was able to integrate a necessary security feature into the delivery while steering the overall schedule in the right direction (the time block was recouped later).

Conclusion

Actual Results and Potential Effects

The project concluded successfully, delivering a comprehensive 600-user enterprise network design package on 25 November 2024. The actual results included a detailed, actionable plan that allowed the organization to commence procurement and installation activities.

Potential Effects:

Risk Mitigation: A redundant three-tier topology and redundant hardware selections significantly reduce the likelihood of an outage occurring across the network, resulting in direct cost savings due to avoided downtime.

Futureproofing: With respect to the TIA-568-D standards (Work 2) and Cat 6A cabling, the physical plant is well-equipped to support future speed demands (10Gbps+) and prevent the organization's cabling investment from becoming a liability for the next few decades.

Operational Efficiency: The standardized IP/VLAN schema provides a significantly easier environment for network monitoring, troubleshooting, and general administration, resulting in reduced operational expenses (OpEx) for the IT support staff.

Project Success Evaluation

Based on the framework for evaluation established within the project proposal (Task 2), the project is considered a success because it was secure, scalable, and cost-effective for a 600-user environment.

Criteria	**Evaluation**	**Justification**
Secure	**Successful**	Achieved Objective 1.2 by implementing a robust VLAN segmentation plan (Artifact 2) and successfully integrating a dedicated hardware firewall cluster ("Unanticipated Scope Creep") between the Core network and the internet edge. The design adheres to ZTA principles (Work 1).
Scalable	**Successful**	Achieved Objective 2.1 by allocating the **10.0.0.0/16** private IP address space, allowing for ample expansion beyond 600 users and future multi-site integration. The selection of a modular Core switch

		allows for capacity and feature upgrades without a forklift replacement.
Cost-Effective	**Successful**	Achieved Objective 3.1 by justifying the higher initial capital expenditure of enterprise-grade hardware using the **Total Cost of Ownership (TCO)** model (Work 3). The rationale demonstrated that superior reliability and a longer lifecycle led to a lower long-term financial impact compared to budget alternatives.

References

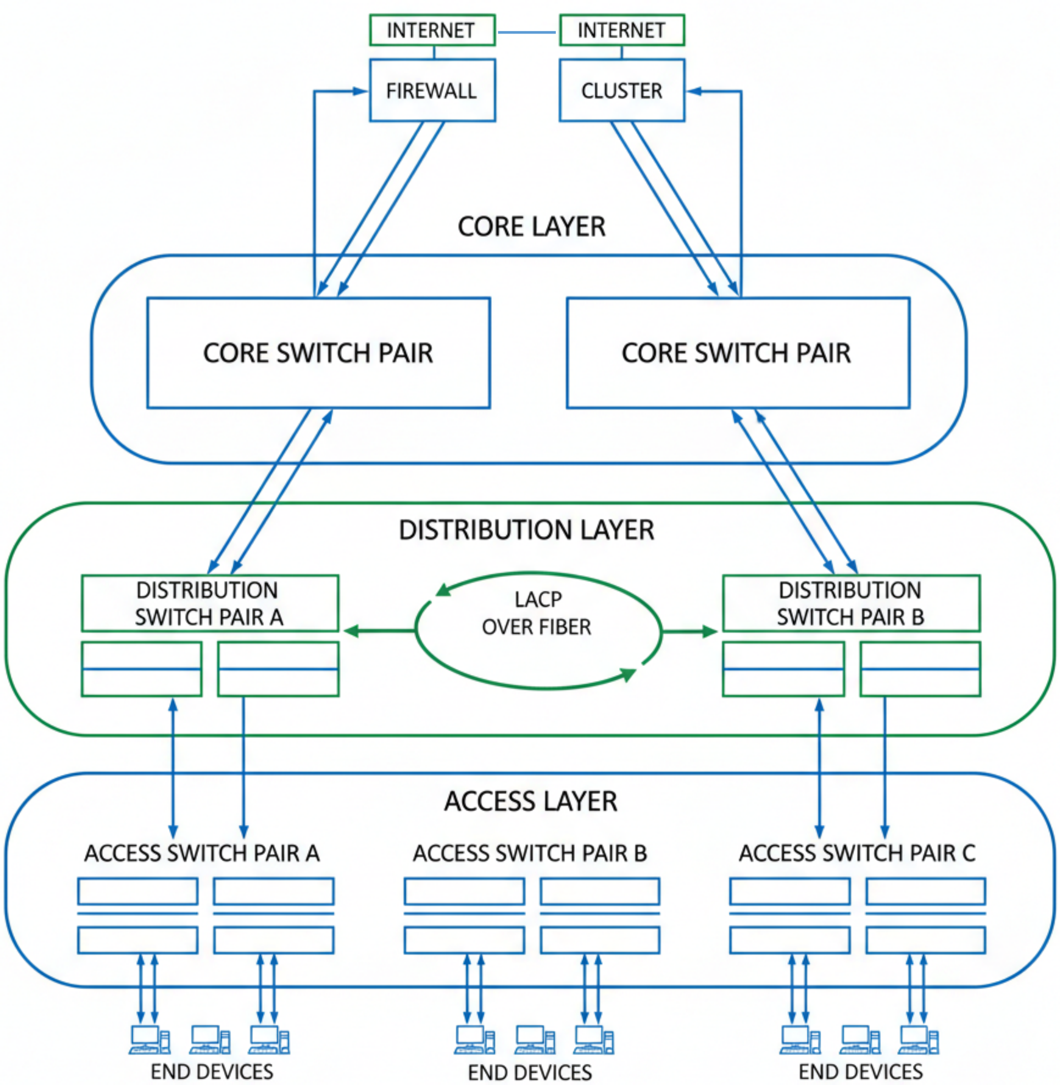
Cisco. (2023). *Zero Trust Architecture for Enterprise Networks*. White Paper.

Gartner Research. (2022). *Total Cost of Ownership (TCO) Analysis for Next-Generation Networking Hardware*. Research Note.

Telecommunications Industry Association (TIA). (2018). *TIA-568-D Commercial Building Telecommunications Cabling Standard*.

Appendix A

Logical Topology Diagram Snippet



Description: This is a simplified, high-level drawing that depicts the targeted architecture of the network. It illustrates the Core, Distribution, and Access layers, representing a logical connection between them.

Relation with Project: It directly supports Objective 1.1 to provide a visual demonstration of the three-tiered redundant topology implementation. It shows the Core switch pair connecting to the Internet through the Firewall Cluster, while Distribution switches are connected redundantly over fiber (LACP).

Appendix B

IP Addressing and VLAN Schema Table

Description: The table documents the hierarchical IP addressing scheme and the VLANs associated with network segmentation.

Relationship with Project: This artifact was the primary deliverable for Objectives 1.2 and 2.1. The deliverable ensured the network was both secure (via segmentation) and scalable (via hierarchical subnetting).

Network Segment	VLAN ID	IP Subnet (Hierarchical)	Purpose & Security Notes
Corporate Data	10	10.10.1.0/20	General user access. Least privilege ACLs apply.
Voice/VoIP	20	10.20.1.0/20	Prioritized traffic (QoS) only. Access to phone servers.
Servers/DC	30	10.30.1.0/24	Restricted access. Heavily firewalled from other segments.
Management	50	10.50.1.0/28	Network engineer access only. Strict ACLs and monitoring.
Guest/IoT	99	10.99.1.0/24	Isolated network access to the Internet only.

Appendix C

Hardware Bill of Materials (BOM) Snippet

Description: A partial listing from the finalized BOM, detailing the high-value equipment required for the core network. It includes pricing for use in the TCO analysis.

Relation to Project: This artifact served as the primary deliverable for Objective 3.1, offering an actionable list for procurements and financial justification. It specifies enterprise-grade equipment that meets security and scalability requirements.

Item Type	Manufacturer	Model Number	Unit Price	Quantity	Total Cost
Core Switch (Modular)	Vendor X	Nexus-9000-A	$35,000	2	$70,000
Distribution Switch (L3)	Vendor Y	Catalyst-3850-B	$6,500	4	$26,000
Access Switch (PoE+)	Vendor Y	Catalyst-2960-C	$1,500	25	$37,500
Hardware Firewall Cluster	Vendor Z	FortiGate-200E	$12,000	2	$24,000