ABC Company Design Project

Joseph Rieke & Amari (AJ) Jones

Host Plan

The Host Plan defines how ABC Company has allocated network devices across its growing workforce, which currently includes 389 hosts spanning 8 departments and administrative units. The organization is spread across three buildings, each with multiple floors, and each department is mapped to a specific building and floor combination to align with available space and expected growth.

To accommodate this distribution, HP 5830 switches with 48 1-Gigabit Ethernet ports were selected. Each department's host count was analyzed to determine the number of required switches. For example, larger departments like Department 6, which has 97 hosts, require multiple switches distributed across multiple floors in Building 3. In contrast, smaller departments such as Department 5 (9 hosts) can be served by a single switch.

Switch placement is optimized to reduce cabling complexity and ensure local connectivity. Floors with multiple departments may share switches where appropriate, while high-density areas are provisioned with dedicated hardware. This strategy ensures not only reliable network performance but also scalability for future growth, as additional switches can be deployed without rearchitecting the entire network.

The completed Host Plan provides a foundational layer for the overall network design, aligning physical host locations with logical infrastructure components in a manner that balances performance, cost, and manageability.

Dept.	Host Count	Building	Floor(s)	Switches Needed	Explanation
Dept 1	56	1	2, 3	2	2 switch(es) required to support 56 hosts in Department Dept 1, located on floor(s) 2, 3 of Building 1.
Dept 2	64	2	2, 3	2	2 switch(es) required to support 64 hosts in Department Dept 2, located on floor(s) 2, 3 of Building 2.
Dept 3	29	1	1	1	1 switch(es) required to support 29 hosts in Department Dept 3, located on floor(s) 1 of Building 1.
Dept 4	27	1	1, 2	1	1 switch(es) required to support 27 hosts in Department Dept 4, located on floor(s) 1, 2 of Building 1.
Dept 5	9	2	2	1	1 switch(es) required to support 9 hosts in Department Dept 5, located on floor(s) 2 of Building 2.
Dept 6	97	3	1–3	3	3 switch(es) required to support 97 hosts in Department Dept 6, located on floor(s) 1–3 of Building 3.
Dept 7	36	2	1	1	1 switch(es) required to support 36 hosts in Department Dept 7, located on floor(s) 1 of Building 2.
Dept 8	18	3	1	1	1 switch(es) required to support 18 hosts in Department Dept 8, located on floor(s) 1 of Building 3.
Admin	12	2	1	1	1 switch(es) required to support 12 hosts in Department Admin, located on floor(s) 1 of Building 2.

Network Architecture

The Network Architecture defines the logical segmentation of ABC Company's internal data traffic using Virtual Local Area Networks (VLANs) and IP subnets. This design enables performance optimization, security enforcement, and efficient resource management across departments and buildings.

Each department has been assigned a unique VLAN ID and corresponding IP subnet. This segmentation ensures that network broadcast domains are limited to departmental boundaries, which helps reduce congestion and isolate traffic. Subnets were chosen to align with the size of each department's host requirements, ensuring adequate address space without waste. Gateway IP addresses were designated per subnet to route inter-VLAN traffic through the core router.

For example, Department 1 is assigned VLAN 10 with subnet 10.0.0.0/25, which accommodates up to 126 hosts and includes gateway 10.0.0.1. Similarly, other departments with more modest host counts are assigned appropriately smaller subnets, such as /27 or /28, to maintain efficiency in IP space utilization.

This logical architecture supports security and access control policies by enforcing VLAN-specific rules through the firewall and routing infrastructure. It also allows for future scalability, as additional VLANs and subnets can be added without impacting the existing structure.

The VLAN and subnet design is a critical backbone for the network's operation, enabling seamless departmental communication, controlled access to shared services, and organized traffic flows within the organization.

VLAN ID	Dept.	Subnet Address	Subnet Mask	Host Range	Gateway	Explanation
10	Dept 1	10.0.0.0	255.255.255.	10.0.0.1 - 10	10.0.0.1	VLAN 10 assigned to Dept 1 with subnet 10.0.0.0/255.255.255.128 to logically segment traffic and assign a unique gateway (10.0.0.1).
20	Dept 2	10.0.0.128	255.255.255.	10.0.0.129 -	10.0.0.129	VLAN 20 assigned to Dept 2 with subnet 10.0.0.128/255.255.255.128 to logically segment traffic and assign a unique gateway (10.0.0.129).
30	Dept 3	10.0.0.128	255.255.255.	10.0.0.129 -	10.0.0.129	VLAN 30 assigned to Dept 3 with subnet 10.0.0.128/255.255.255.192 to logically segment traffic and assign a unique gateway (10.0.0.129).
40	Dept 4	10.0.0.192	255.255.255.	10.0.0.193 -	10.0.0.193	VLAN 40 assigned to Dept 4 with subnet 10.0.0.192/255.255.255.192 to logically segment traffic and assign a unique gateway (10.0.0.193).
50	Dept 5	10.0.0.128	255.255.255.	10.0.0.129 -	10.0.0.129	VLAN 50 assigned to Dept 5 with subnet 10.0.0.128/255.255.255.224 to logically segment traffic and assign a unique gateway (10.0.0.129).
60	Dept 6	10.0.2.128	255.255.255.	10.0.2.129 -	10.0.2.129	VLAN 60 assigned to Dept 6 with subnet 10.0.2.128/255.255.255.128 to logically segment traffic and assign a unique gateway (10.0.2.129).
70	Dept 7	10.0.1.128	255.255.255.	10.0.1.129 -	10.0.1.129	VLAN 70 assigned to Dept 7 with subnet 10.0.1.128/255.255.255.192 to logically segment traffic and assign a unique gateway (10.0.1.129).
80	Dept 8	10.0.0.224	255.255.255.	10.0.0.225 -	10.0.0.225	VLAN 80 assigned to Dept 8 with subnet 10.0.0.224/255.255.255.224 to logically segment traffic and assign a unique gateway (10.0.0.225).
90	Admin	10.0.1.0	255.255.255.	10.0.1.1 - 10	10.0.1.1	VLAN 90 assigned to Admin with subnet 10.0.1.0/255.255.255.224 to logically segment traffic and assign a unique gateway (10.0.1.1).
100	DMZ	10.0.0.144	255.255.255.	10.0.0.145 -	10.0.0.145	VLAN 100 assigned to DMZ with subnet 10.0.0.144/255.255.255.240 to logically segment traffic and assign a unique gateway (10.0.0.145).

Structured Cabling Plan

1. Cabling Standards

Horizontal Cabling: Cat6 Ethernet cabling will connect workstations, VoIP phones, and wireless access points to switches in local IDFs.

Backbone Cabling: Multimode fiber optic cabling will be used to connect IDFs to MDFs across floors and between buildings.

2. IDF/MDF Designation

Each floor will include at least one Intermediate Distribution Frame (IDF).

Main Distribution Frames (MDFs) will be located in:

- Building 2, Floor 1 (core router, firewall, internet access)
- Secondary MDFs in Buildings 1 and 3 for cross-building redundancy.

Floor-by-Floor IDF/MDF Assignments

Building	Floor	Role	Purpose
1	1	IDF	Supports Departments 3 and 4
1	2	IDF	Supports Departments 1 and 4
1	3	IDF	Supports Department 1
2	1	MDF	Core routing and access layer for Admin and Dept 7
2	2	IDF	Supports Departments 2 and 5
2	3	IDF	Supports Department 2
3	1	IDF	Supports Departments 6 and 8
3	2	IDF	Supports Department 6
3	3	IDF	Supports Department 6

3. Cable Pathways

Cable trays and ladder racks will be installed in ceilings for horizontal cabling.

Vertical risers in conduits will carry fiber and copper cables between floors.

Patch panels in each IDF will organize connections for easy maintenance.

Horizontal cabling will be limited to 90 meters or less per TIA-568 standards.

Vertical fiber risers will interconnect IDFs to their respective MDFs on each floor stack.

Inter-building backbone runs will use armored, gel-filled fiber routed through underground conduits with weatherproof enclosures at building entrances.

Cables entering each IDF will pass through grommeted openings and be secured with Velcro straps or cable combs for strain relief and organization.

4. Patch Panels and Racks

Each IDF/MDF will contain:

- Two 48-port patch panels for copper terminations.

- One 12- or 24-port fiber patch panel (depending on distance and redundancy).
- 42U 4-post server racks to house switches and panels.
- Cable management arms and horizontal/vertical organizers to keep patch cords cleanly routed.
- Grounding and bonding infrastructure following ANSI/TIA-607 standards.

5. Labeling and Documentation

All cables and ports will be labeled at both ends.
IDF maps and patch panel diagrams will be included in final documentation.

6. Compliance and Testing

All cable runs will be tested for continuity and throughput using certified Fluke testers.
Cabling will meet or exceed bandwidth requirements for 1Gbps and 10Gbps uplinks.

7. Expansion Readiness

Conduit space and rack units will be reserved for Buildings 4 and 5.
Extra cable slack will be coiled in trays to support future re-terminations.

Building	Floor	Cable Type	Purpose	Estimated Length (ft)	Connected Between	Explanation
1	1	Cat6	Horizontal	1200	IDF to Hosts	Supports Depts 3 & 4
1	2	Cat6	Horizontal	1400	IDF to Hosts	Supports Depts 1 & 4
1	3	Cat6	Horizontal	800	IDF to Hosts	Supports Dept 1
2	1	Cat6	Horizontal	1000	MDF to Hosts	Supports Admin & Dept 7
2	2	Cat6	Horizontal	900	IDF to Hosts	Supports Depts 2 & 5
2	3	Cat6	Horizontal	700	IDF to Hosts	Supports Dept 2
3	1	Cat6	Horizontal	1500	IDF to Hosts	Supports Depts 6 & 8
3	2	Cat6	Horizontal	1000	IDF to Hosts	Supports Dept 6
3	3	Cat6	Horizontal	1000	IDF to Hosts	Supports Dept 6
1	B1-B2	Fiber	Backbone	300	IDF to MDF	Inter-building fiber run
2	B2-B3	Fiber	Backbone	300	IDF to MDF	Inter-building fiber run
All	Stacked	Fiber	Backbone	200	Vertical risers	Floor-to-floor fiber risers

Equipment and Cost Summary

The equipment plan for ABC Company's network design outlines the essential hardware components required to support the organization's current operations and anticipated growth. The selected equipment emphasizes reliability, scalability, and cost-efficiency while accommodating the logical and physical network architecture.

Key infrastructure components include HP 5830 switches, Cisco ISR routers, Fortinet FortiGate firewalls, and UniFi wireless access points. These were chosen to balance performance and

manageability while integrating seamlessly with the organization’s VLAN-based logical segmentation and three-building deployment layout.

The HP 5830 switches provide 48-port gigabit connectivity and are distributed across floors and departments. A core Cisco router enables inter-VLAN routing and external WAN connectivity. The FortiGate firewall secures both the internal network and DMZ. Wireless connectivity is provided by UniFi APs, with four units deployed per floor, ensuring strong coverage across each building's 15,625 square foot floors.

Structured cabling is provisioned using Cat6 Ethernet cable rolls to support inter-floor and intra-building links. Fiber optic cabling is deployed for vertical risers and inter-building backbone connectivity. To facilitate structured cabling, the equipment plan also includes patch panels, keystone wall jacks, cable management systems, labeling kits, and supporting installation hardware.

Professional installation services and specialized tools such as punchdown tool kits and cable testers have been included to ensure a standards-compliant and reliable deployment. Labor costs cover the structured cabling, switch installations, AP mounting, patch panel terminations, and full network testing.

All equipment, cabling, labor, and accessory costs have been itemized and tallied for budgeting purposes.

The total projected equipment cost for the implementation is $65,585. This total includes spare capacity and headroom for future expansion, ensuring long-term return on investment and simplified lifecycle management.

This equipment plan provides a solid foundation for a high-performance, secure, and scalable enterprise network.

Category	Item	Desc.	Quantity	Unit Cost	Notes	Total Cost
Switches	HP 5830	48-port Gigabit switch	12	$2,500	Includes spares and future growth	$30,000
Routers	Cisco ISR 4431	Core router with dual WAN	1	$5,000	Main routing device in Building 2	$5,000
Firewalls	FortiGate 60F	DMZ/Internal firewall	1	$1,500	Protects email/proxy servers	$1,500
Access Points	Ubiquiti UniFi AP	Wireless access point	6	$180	2 per building	$1,080
Cabling	Cat6 Ethernet Cable	1000 ft roll	5	$120	Used for building/floor interconnects	$600
Servers	Dell PowerEdge R740	Email & proxy servers	2	$6,000	Housed in DMZ	$12,000
UPS	APC Smart-UPS	Uninterruptible power supply	3	$800	One per building	$2,400
Racks	Standard 42U Rack	Equipment rack	3	$1,000	One per building MDF	$3,000
Labor	Installation Services	Cabling, AP mounts, switch installs	1	$7,500	Contractor fee, all buildings	$7,500
Tools	Punchdown Tool Kits	For terminations at patch panels	3	$85	1 per building	$255
Tools	Cable Testers	Cat6 & fiber certification tools	1	$1,800	Fluke-level testing device	$1,800
Accessories	Wall Plates & Keyston	Data ports for wall drops	100	$3	2 drops per host est.	$300
Accessories	Cable Labels & Velcro	Labeling + bundling materials	1	$150	Roll set for structured cabling	$150
					Total	$65,585

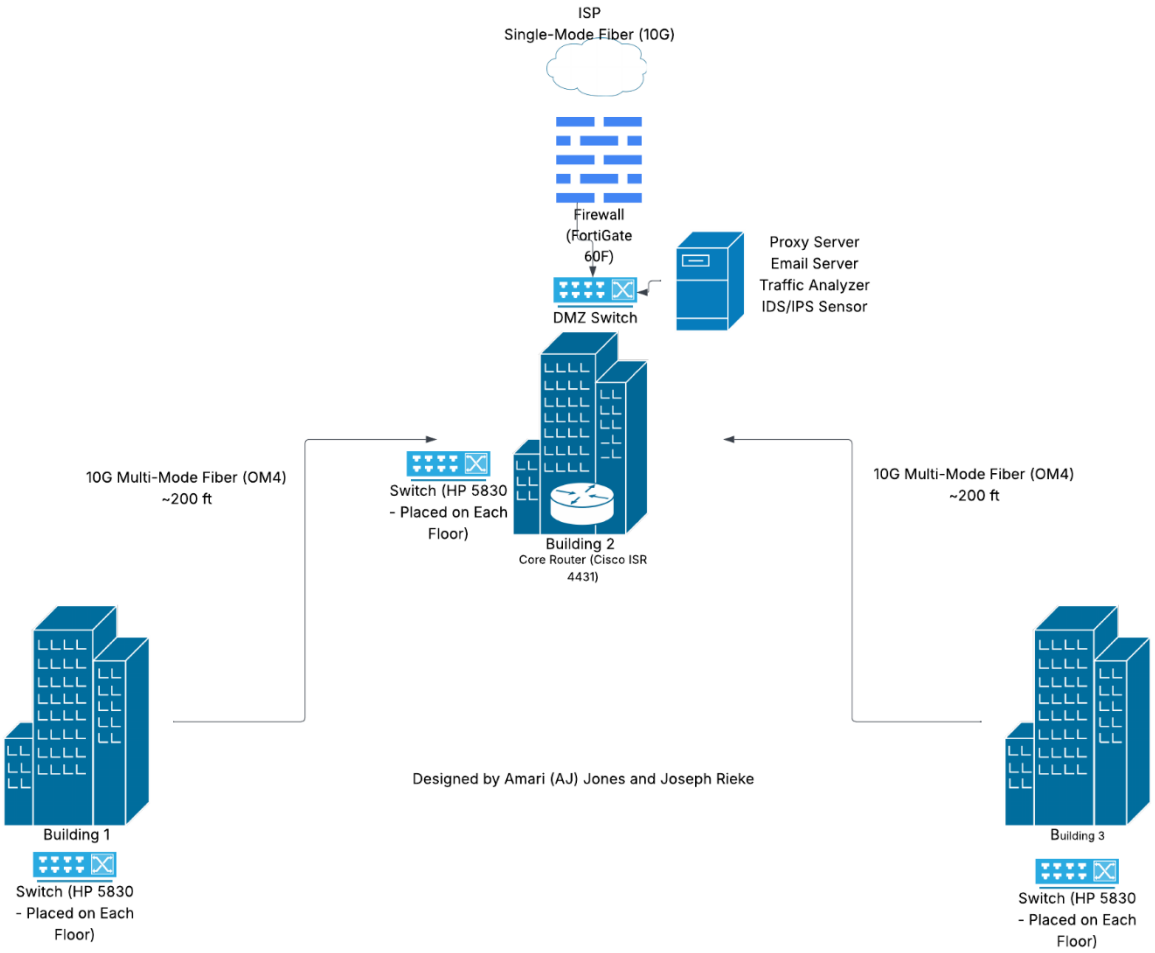
Network Diagram Summary

This section provides an overview of the logical and physical network topology designed for ABC Company. The network consists of three buildings interconnected using a tree/star topology. Switches are distributed by floor, and a central router and firewall manage inter-VLAN routing and external access. The DMZ is protected by a dedicated firewall.

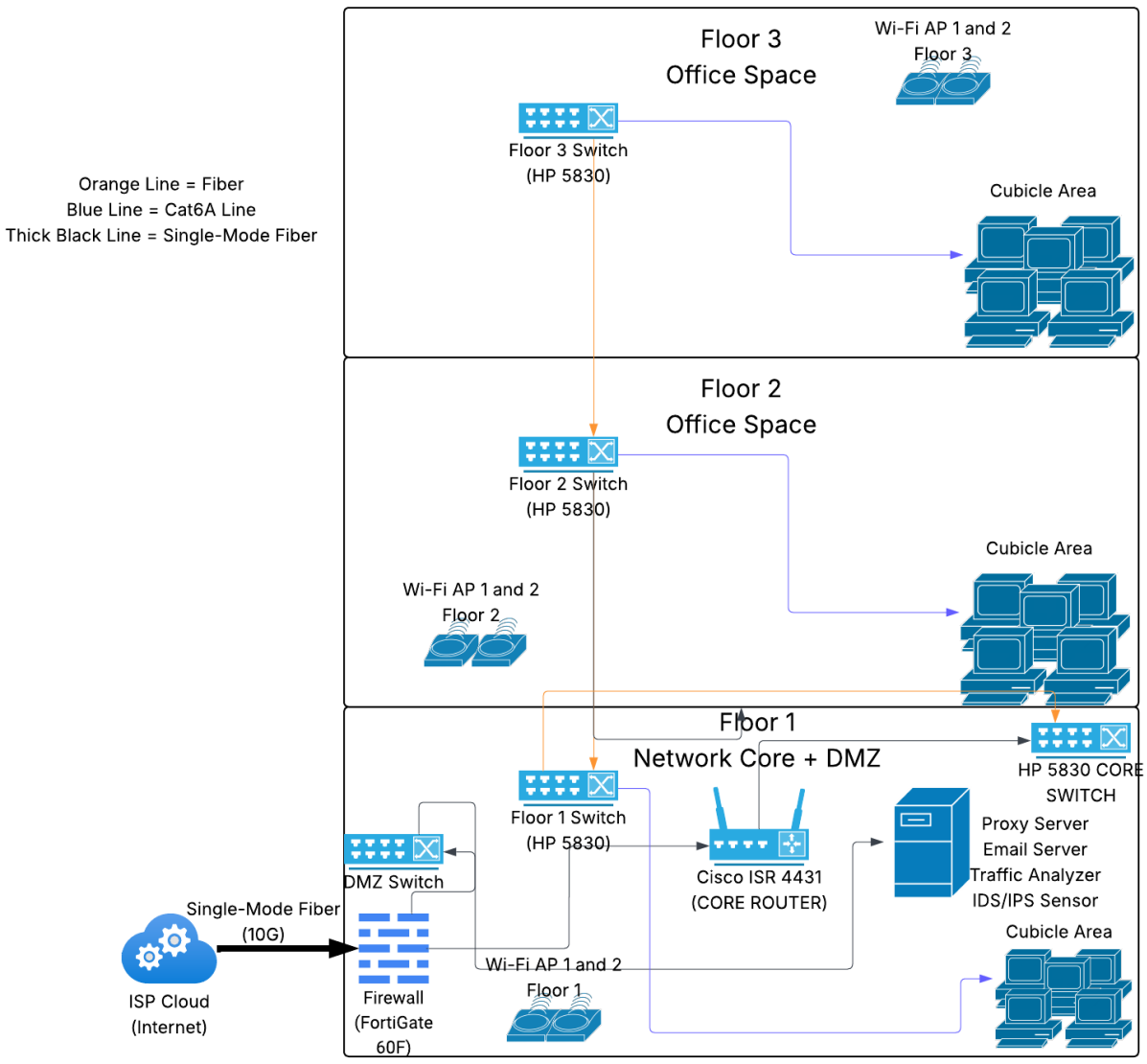
1. Topology Overview

The network uses a hybrid tree/star topology with the following characteristics:

- Each building has its own switch stack per floor.
- Building 2 houses the core router, firewall, and DMZ.
- All switches connect upward to the router in a tree design.
- VLANs are used to segment departments logically.
- The firewall manages traffic between the DMZ and internal LANs.



Designed by Amari (AJ) Jones and Joseph Rieke



Network Security Design

1. Security Overview

The network security design for ABC Company is built around the CIA triad principles: Confidentiality, Integrity, and Availability. The design ensures that all organizational data is protected from unauthorized access, alterations, and service disruptions.

2. Firewall Architecture & DMZ

The network includes an external firewall protecting the DMZ and an internal firewall separating critical systems. The DMZ hosts publicly accessible services such as the email and proxy servers. Firewall rules follow a default-deny approach, only allowing approved traffic.

External Firewall Rules:
• Block packets with spoofed internal IPs.
• Block known blacklist IPs.
• Allow only traffic destined to approved IP ranges.
• Block all pings and broadcasts.
Internal Firewall Rules:
• Block/Allow based on source/destination IP and port.
• Block public IPs except 10.0.0.0/8 range.
• Only allow white-listed external sources into DMZ.

3. Intrusion Prevention

Intrusion detection and prevention systems (IDS/IPS) are deployed to monitor traffic. Traffic anomaly detection and port scanning defense are part of the infrastructure.

4. Encryption & VPNs

Sensitive data is encrypted using AES-256 symmetric encryption. VPNs are implemented for remote users with multi-factor authentication (MFA). Transport Layer Security (TLS) is used for email and web communication encryption.

5. Authentication & Access Control

User authentication is based on centralized credentials and MFA. Access is managed through Active Directory group policies and role-based access control (RBAC).

6. Backup & Disaster Recovery

Critical data is backed up nightly to offsite locations. UPS systems and failover server clusters support business continuity. A full disaster recovery plan outlines procedures for hardware failure, natural disaster, and cyberattacks.

Redundancy and Scalability Plan

1. Core Network Redundancy

Core Router Redundancy: The main router located in Building 2 is paired with a hot-standby router configured using HSRP (Hot Standby Router Protocol) or VRRP.

Firewall Redundancy: A secondary FortiGate firewall operates in active-passive failover mode, ensuring security continuity if the primary firewall fails.

2. Switch Redundancy

Building-Level Redundancy:

- Each floor has multiple switches with uplinks to at least two IDFs or to the MDF.
- Inter-switch links (ISLs) use Spanning Tree Protocol (STP) or Rapid STP to avoid loops while enabling backup paths.

Stacked Switch Configurations:

- Where appropriate, stackable HP 5830 switches are used to enable unified control and resilience within a floor.

3. Backbone and Uplink Redundancy

Fiber Backbone Links:

- Dual fiber runs connect each IDF to the MDF with primary and secondary paths.
- Buildings 1 and 3 are each connected to Building 2 with at least two diverse fiber paths through separate underground conduits.

4. Wireless Redundancy

AP Coverage Overlap: Wireless access points are positioned with 20–30% coverage overlap to ensure seamless failover between adjacent APs.

Controller Failover: If UniFi Controller is used, it is hosted with backup snapshots and remote access for recovery.

5. Scalability Features

VLAN Range Allocation:

- Current VLANs range from 10 to 90. VLANs 100–199 are reserved for Buildings 4 and 5.

Trunk Ports and Uplink Capacity:

- All switch uplinks are 1Gbps by default with option to upgrade to 10Gbps.
- Link Aggregation Control Protocol (LACP) is supported for link bundling.

Rack and Power Provisioning:

- IDFs and MDFs have open rack units and dual power supplies.
- Additional circuits are available in each IDF for expansion.

Compliance and QoS Plan

1. Compliance Considerations

Regulatory Compliance Goals:

- HIPAA (Health Insurance Portability and Accountability Act): Ensures protection of sensitive personal data in healthcare-related transactions.
- PCI-DSS (Payment Card Industry Data Security Standard): Protects cardholder information for any payment processing activities.

Security Measures Supporting Compliance:

- Use of AES-256 encryption for data-in-transit.
- TLS-secured communications for email, web access, and VPN tunnels.
- Deployment of firewalls with strict access control lists (ACLs) and intrusion prevention systems (IPS).
- Role-Based Access Control (RBAC) policies via Active Directory to limit system access to authorized users only.
- Centralized logging and event monitoring to support audit requirements.
- Daily offsite backups and full disaster recovery plans.

2. QoS (Quality of Service) Implementation

Traffic Classification and Prioritization:

- VoIP traffic will be prioritized using DSCP (Differentiated Services Code Point) markings, specifically EF (Expedited Forwarding) class.
- Video conferencing traffic will be classified as high-priority but secondary to VoIP.
- Business-critical application traffic (e.g., ERP systems, email servers) will receive medium-high priority.
- Best-effort class for non-critical traffic (e.g., general web browsing).

QoS Techniques to Be Applied:

- Queuing mechanisms (Priority Queuing or Weighted Fair Queuing) on switches and routers.
- Traffic policing to prevent bandwidth hogging by non-critical services.
- Bandwidth reservation on WAN links to ensure minimum guaranteed service levels for VoIP and video.

Switch and Router QoS Features:

- All HP 5830 switches and Cisco ISR 4431 routers will have QoS settings enabled.
- Access Control Lists (ACLs) will be used to classify and mark traffic at the network edge.
- Core routers will enforce QoS policies end-to-end across the VLANs and routed interfaces.

3. Ongoing Compliance and QoS Maintenance

- Annual audits to review compliance with HIPAA/PCI-DSS requirements.
- Quarterly QoS reviews to adjust traffic prioritization based on application performance reports.
- Firmware updates for switches, routers, firewalls, and wireless controllers to ensure security patches are applied.

Wireless Access Point (AP) Coverage Plan

1. Coverage Assumptions

Access Point Model: Ubiquiti UniFi UAP-AC-Pro or equivalent
Effective Coverage Area per AP: ~5,000 sq ft (indoors, with wall attenuation considered)
Target Coverage Overlap: 20% to support roaming and fault tolerance

2. AP Allocation by Floor

Each building includes 3 floors, each measuring 15,625 sq ft:

APs Required per Floor: 15,625 / 5,000 = ~3.1

Planned Deployment: 4 APs per floor to allow for overlap and minor coverage shifts

3. Building-Wide Deployment Plan

Building	Floors	APs per Floor	Total APs
1	3	4	12
2	3	4	12
3	3	4	12
Total			36

4. Deployment Guidelines

APs will be centrally placed on each floor, with even spacing to ensure consistent coverage.
Each AP will be connected via Cat6 cabling to its nearest IDF.
APs will be powered using PoE (Power over Ethernet) switches where available.
Signal overlap is engineered to ensure client handoff during roaming is smooth and interruption-free.

5. Scalability and Monitoring

Spare APs (at least 2 per building) will be kept for failover or unexpected coverage gaps.
Controller software will monitor signal strength and automatically balance client load.
Future buildings (4 and 5) will adopt a similar 4 APs/floor standard, adaptable to layout.

Instructor Questions

1. *Are there any specific bandwidth requirements per department that should influence switch or uplink selection?*
   Currently, there are no explicit bandwidth requirements per department provided. However, based on departmental host counts, we assume standard office traffic with occasional high-bandwidth use (e.g., file transfers, video conferencing). Uplinks between floor switches and the core router are provisioned as Gigabit Ethernet. High-density departments (e.g., Dept 6 with 97 hosts) may benefit from 10GbE uplinks to prevent congestion. Future expansion could justify link aggregation (LACP) for additional bandwidth.

2. *Should redundancy be required at the router or core layer for high availability?*
   While not explicitly required, we recommend introducing router and core switch redundancy to ensure high availability and business continuity. This could include a secondary core router in failover mode (e.g., HSRP or VRRP), redundant power supplies, and UPS for all core network devices. Optional dual-homing switches to different routers may also be implemented.

3. *Are there preferred vendors for switches, routers, or firewalls to standardize with?*
   The current design uses HP 5830 switches, Cisco ISR 4431 for routing, and Fortinet FortiGate 60F for firewall protection. If vendor standardization is required, we can adjust to a Cisco-only or HP Aruba stack. Otherwise, the proposed mix provides both performance and cost efficiency.

4. *Is wireless access expected in all departments, and should wireless VLANs be planned as well?*
   Yes, wireless access is expected throughout all buildings. Two access points per building (total: 6) are already provisioned. We recommend implementing separate VLANs for wireless clients, possibly segmented by internal staff, guest access, and IoT devices. Wireless VLANs can be centrally managed via a controller or cloud-managed AP platform (e.g., UniFi Controller).

5. *Are there any compliance standards (e.g., HIPAA, PCI-DSS) that must be factored into security design?*
   Compliance requirements were not explicitly stated. However, the network design aligns with common best practices for compliance: AES-256 encryption, MFA and RBAC, IDS/IPS monitoring, and daily offsite backups. If specific regulations apply (e.g., HIPAA or PCI-DSS), we can refine firewall rules, logging, and access control accordingly.

6. *Should expansion planning consider remote workers or satellite offices?*
   Yes — remote work capability has been considered. VPN support with multi-factor authentication (MFA) is implemented. Expansion to support satellite offices can be accommodated via site-to-site VPNs or additional VLAN routing. IP addressing has been subnetted to allow future scalability.

7. *Should the DMZ include any other services besides email and proxy (e.g., FTP, VPN endpoint)?*
   Currently, the DMZ includes an email server, proxy server, and traffic analyzer. It would be beneficial to expand the DMZ to include a VPN endpoint, FTP/SFTP server (if external transfers are needed), or public-facing web/app services. These can be added securely via DMZ isolation and firewall rules.

8. *Is VoIP or video conferencing expected, and should QoS policies be implemented for that traffic?*
   If VoIP or video conferencing is expected (likely given growth and remote work needs), then QoS policies should be implemented: prioritize UDP traffic, use DSCP marking, and apply priority queuing at switches/routers. This ensures low-latency paths and reliable performance for real-time communication.

Final Documentation & Questions

1. Project Summary

This document concludes the network design for ABC Company as part of the CIS 4348 Design Project. The network has been planned to support 389 hosts across 8 departments and administrative units, distributed over three buildings with potential for expansion to two additional buildings. The design incorporates scalability, security, and performance through VLAN segmentation, core routing, DMZ security, and modern hardware.

Key deliverables from this project include:

- Host planning with switch distribution (Step 1)
- Logical network architecture including VLANs and subnets (Step 2)
- Physical topology with device assignments and building-floor mapping (Step 3)
- Security infrastructure and firewall policies (Step 4)
- Equipment list with quantities and cost estimates (Step 5)
- Network diagrams with descriptive summaries (Step 6)