Engineering and Aviation Science Complex (EASC)

Network Infrastructure Design Report

University of Maryland Eastern Shore

March 2026

1 Network Infrastructure Requirements

1.1 Overview

The EASC is a three-floor academic building at UMES housing offices, conference rooms, standard classrooms, lab classrooms, and a centralized server room. I designed the network to prioritize throughput, VLAN-based security, and scalability. The University of Texas at Austin IT Infrastructure Standards for Academic Buildings specifies that campus facilities require dedicated VLANs per functional zone, minimum 1 Gbps wired uplinks to instructional spaces, PoE-capable switches for WAPs and IP phones, and a centralized server room with redundant paths (UT Austin ITS, 2023). I adopted these principles across all three floors.

1.2 Per-Space Requirements

Offices (VLAN 10): Each office (101, 102, 201, 202, 301, 302) has one PC, one printer, and one VoIP phone aggregated through an 8-port wall switch. PoE (802.3af) powers the VoIP phone. QoS marks VoIP traffic DSCP EF, enforcing ITU-T G.114 requirements (<150 ms one-way delay, <1% packet loss).

Conference Rooms (VLAN 20): Each conference room (103, 203, 303) has a projector, display TV, and VoIP phone on an 8-port switch. Minimum 50 Mbps sustained uplink is required for video conferencing.

Standard Classrooms (VLAN 30): Classrooms 104–107, 204–207, and 304–307 each have a projector, display TV, and wireless router on an 8-port switch. Per-port bandwidth limiting prevents BYOD devices from saturating uplinks.

Lab Classrooms (VLAN 40): Labs 108–109, 208–209 (Floors 1–2) and Lab 308 (Floor 3) each house 8–10 student PCs, a wireless router, a projector, and a display TV aggregated through two 8-port switches. Static IPs support software licensing.

Server Room (VLAN 50, Floor 3 only): Houses the Cisco Catalyst 3650-24PS Core Switch and six servers: File Server (10.45.50.10), NMS/SIEM (10.45.50.11), Active Directory (10.45.50.12), Database (10.45.50.13), DHCP/DNS (10.45.50.14), and Web Server (10.45.50.15). LAN Gateway: 10.45.50.1.

Hallways (VLAN 60): Each floor hallway has Cisco Aironet 1832i WAPs and dome IP cameras. Floor 2 additionally has a hallway printer. All surveillance devices are isolated from Internet access.

© 2026 Sagar Patel. All rights reserved. Do not copy or redistribute without permission.

Floor	Room	VLAN	Subnet	Key Devices
F1	Offices 101, 102	10	10.34.10.x	PC, Printer, VoIP, 8-port switch, WAP
F1	Conference 103	20	10.34.20.x	Projector, Display TV, VoIP, 8-port switch
F1	Classrooms 104–107	30	10.34.30.x	Projector, Display TV, Wireless Router, 8-port switch
F1	Labs 108–109	40	10.34.40.x	8–10 Student PCs, Router, Projector, TV, 2× switch
F1	Hallway	60	10.34.60.x	2× WAP (Aironet 1832i), 2× Dome Camera
F2	Offices 201, 202	10	10.40.10.x	PC, Printer, VoIP, 8-port switch, WAP
F2	Conference 203	20	10.40.20.x	Projector, Display TV, VoIP, 8-port switch
F2	Classrooms 204–207	30	10.40.30.x	Projector, Display TV, Wireless Router, 8-port switch
F2	Labs 208–209	40	10.40.40.x	8–10 Student PCs, Router, Projector, TV, 2× switch
F2	Hallway	60	10.40.60.x	2× WAP, 2× Dome Camera, Hall Printer
F3	Offices 301, 302	10	10.45.10.x	PC, Printer, VoIP, 8-port switch, WAP
F3	Conference 303	20	10.45.20.x	Projector, Display TV, VoIP, 8-port switch
F3	Classrooms 304–307	30	10.45.30.x	Projector, Display TV, Wireless Router, 8-port switch
F3	Lab 308	40	10.45.40.x	8–10 Student PCs, Router, Projector, TV, 2× switch
F3	Server Room	50	10.45.50.x	6 servers, Cisco 3650-24PS Core Switch, GW: .50.1
All	Hallway/Surveillance	60	x.x.60.x	Dome IP Cameras, Cisco Aironet 1832i WAPs

Table 1: Room, VLAN, and device inventory for all three floors

2 Network Diagram

Figures 1–3 show the three floor plans. Each shows physical room layout, device placement per room, in-room cabling from devices to 8-port wall switches and patch panels, and floor-switch uplinks to the Core Switch in the Floor 3 server room. **Color legend:** Blue = VLAN10, Purple = VLAN20, Green = VLAN30, Orange = VLAN40, Red = VLAN50, Gray = VLAN60, Pink dashed = WAP connections.

© 2026 Sagar Patel. All rights reserved. Do not copy or redistribute without permission.

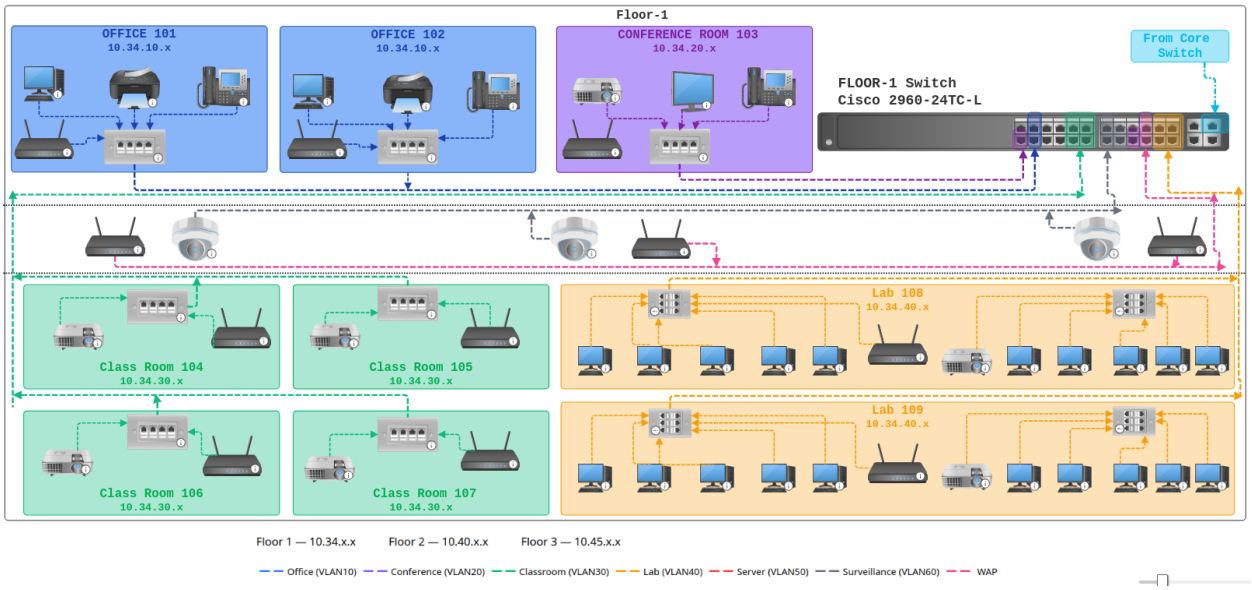


Figure 1: Floor 1 (10.34.x.x). Cisco 2960-24TC-L switch serving Offices 101–102 (VLAN10), Conference 103 (VLAN20), Classrooms 104–107 (VLAN30), Labs 108–109 (VLAN40), and hallway WAPs and dome cameras (VLAN60), with a 1 Gbps 802.1Q trunk to the Core Switch.

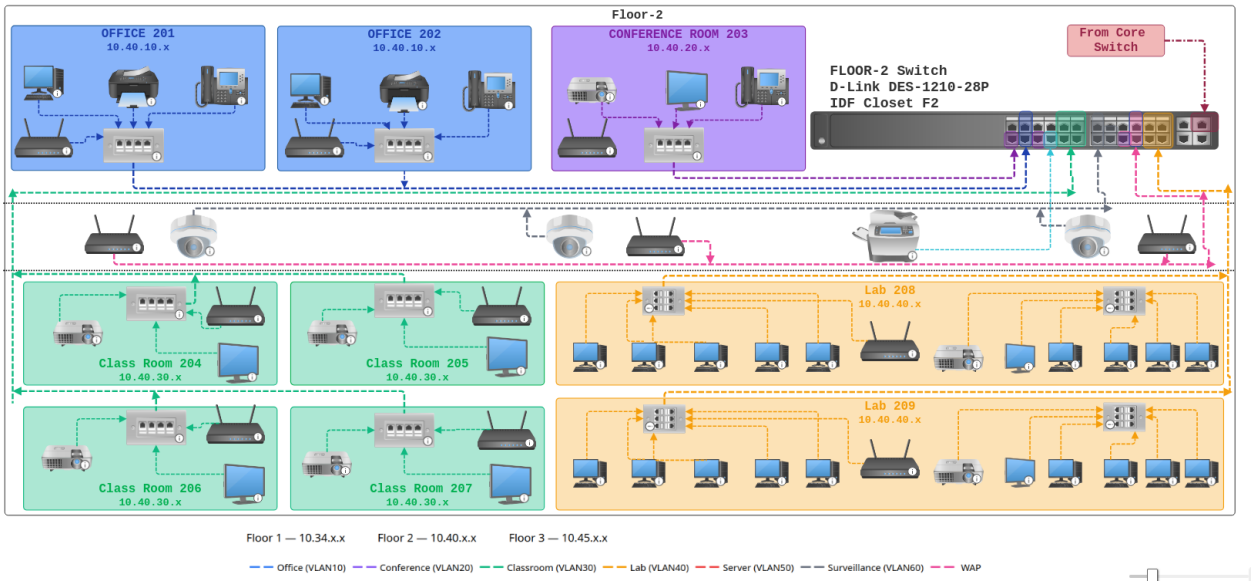


Figure 2: Floor 2 (10.40.x.x). D-Link DES-1210-28P (PoE) switch serving Offices 201–202, Conference 203, Classrooms 204–207, Labs 208–209, and hallway WAPs, dome cameras, and hall printer (VLAN60). PoE ports power the WAPs and VoIP phones; a 1 Gbps trunk runs to the Core Switch.

© 2026 Sagar Patel. All rights reserved. Do not copy or redistribute without permission.

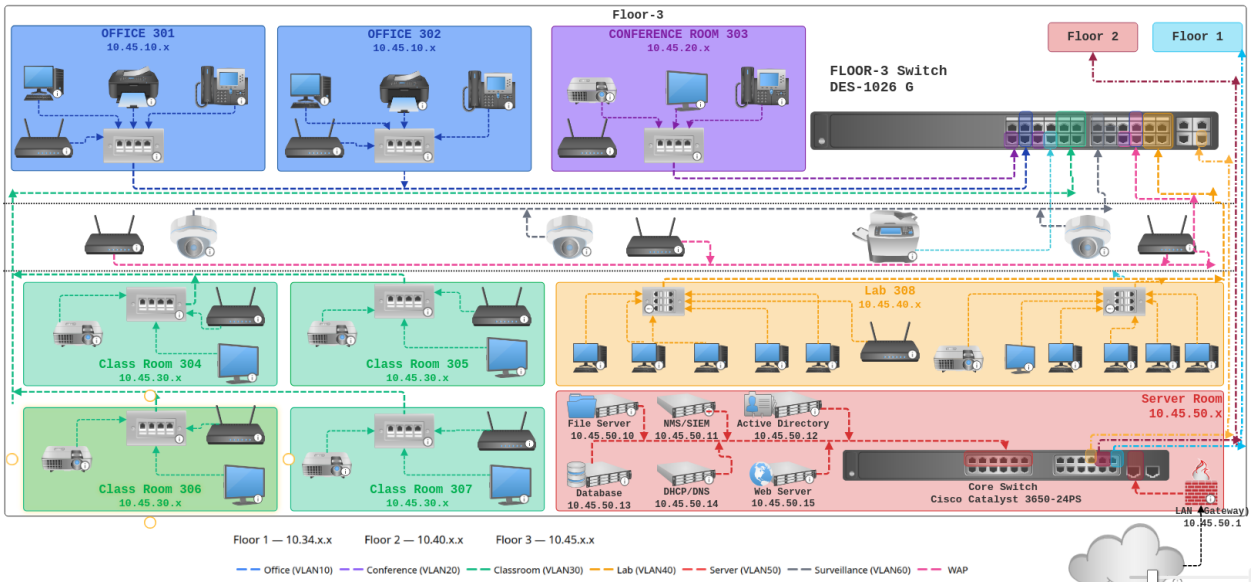


Figure 3: Floor 3 (10.45.x.x) and server room. D-Link DES-1026G floor switch serving Offices 301–302, Conference 303, Classrooms 304–307, and Lab 308. Server Room (VLAN50): File .10, NMS/SIEM .11, AD .12, DB .13, DHCP/DNS .14, Web .15. Core Switch: Cisco Catalyst 3650-24PS, LAN gateway 10.45.50.1. Uplinks to Floors 1 and 2 are shown top right.

3 Network Configuration Plan

3.1 VLAN Design and IP Addressing

Six VLANs partition the network by function. The IP second octet encodes the floor (34 = F1, 40 = F2, 45 = F3); the third octet encodes the VLAN. Each /24 subnet provides 254 usable addresses. The .1 address of each subnet is the Core Switch SVI default gateway.

VLAN	Name	Purpose	Gateway	Inter-VLAN Policy
10	Staff/Mgmt	Offices	x.x.10.1	Full access to all resources + Internet
20	Faculty/Conf	Conference rooms	x.x.20.1	Faculty resources + Internet; no student VLAN
30	Student	Classrooms (BYOD)	x.x.30.1	Internet + Web Server only; blocked from VLANs 10, 50
40	Lab	Lab classrooms	x.x.40.1	File Server only; blocked from AD, DHCP/DNS, NMS
50	Server	Server room	10.45.50.1	Accessible only per ACL from authorized VLANs
60	Surveillance	Cameras, WAPs	x.x.60.1	No Internet; reachable only by NMS/SIEM (.50.11)

Table 2: VLAN definitions and inter-VLAN access policies

Key addressing rules: Infrastructure devices (switches, WAPs, servers, cameras) receive static addresses. Office PCs and VoIP phones receive DHCP leases from 10.45.50.14. Lab PCs are statically assigned (.20–.30) for software licensing. Core Switch SVIs are the sole inter-VLAN routing point — no distributed routing.

© 2026 Sagar Patel. All rights reserved. Do not copy or redistribute without permission.

3.2 Core Configuration Parameters

Inter-VLAN Routing: Cisco Catalyst 3650-24PS acts as the Layer 3 router using SVIs. Extended ACLs applied outbound on each SVI enforce the policy matrix above. The Core Switch is also the STP root bridge for all VLANs.

DHCP/DNS: The DHCP/DNS Server at 10.45.50.14 serves all dynamic VLANs. Core Switch SVIs use `ip helper-address 10.45.50.14` to forward DHCP broadcasts as unicast. Lease times: 8 hours (students), 24 hours (staff). Internal DNS resolves all server FQDNs (e.g., `fileserver.easc.umes.edu` → `10.45.50.10`).

Trunking: All uplinks between floor switches and the Core Switch are 802.1Q trunks carrying VLANs 10, 20, 30, 40, 50, 60, and 99. Native VLAN is set to unused VLAN 99 to prevent double-tagging attacks. VoIP phone ports use Cisco voice VLAN configuration on the same physical port as the data VLAN.

QoS: MLS QoS enabled globally on the Core Switch. VoIP traffic (VLAN 10, 20) is marked DSCP EF (46) in the strict-priority queue. Video conferencing traffic is marked DSCP AF41. Student/lab data uses default DSCP CS0.

Wireless: Cisco Aironet 1832i WAPs broadcast two SSIDs per floor. *EASC-Staff* uses WPA3-Enterprise with 802.1X authentication against AD (10.45.50.12), mapped to VLAN 10. *EASC-Student* uses WPA3-Personal PSK, mapped to VLAN 30. Radio Resource Management (RRM) assigns channels automatically across all floors. WAP uplink ports are 802.1Q trunks carrying both VLANs.

4 Network & Device Security Plan

I apply defense-in-depth across physical, data link, network, transport, and application layers. Cryptography underpins confidentiality and integrity for all traffic types.

4.1 Cryptographic Controls

Symmetric — AES-256 and ChaCha20-Poly1305: EASC-Staff wireless uses WPA3-Enterprise with AES-256-GCMP, providing authenticated encryption (confidentiality + integrity in one pass). Management sessions from the NMS/SIEM (10.45.50.11) to all switches use TLS 1.3 with ChaCha20-Poly1305. This stream cipher combined with the Poly1305 MAC delivers high-throughput authenticated encryption without hardware AES acceleration, making it ideal for VLAN 60 IP cameras with limited processing resources.

Asymmetric — RSA-4096 and ECC P-384: All switches use RSA-4096 SSH host keys (192-bit equivalent security) for management access. Telnet is disabled. The 802.1X EAP-TLS process between staff devices, WAPs, and the AD RADIUS server uses ECDSA P-384 signatures. P-384 provides RSA-7680-equivalent security at a fraction of the key size, enabling faster authentication handshakes on wireless without perceptible delay.

Hashing and MACs — SHA-256/384 and HMAC: AD (10.45.50.12) stores credentials using bcrypt with SHA-256. SNMPv3 AuthPriv mode uses HMAC-SHA-256 for message authentication and AES-128 for traffic encryption on all monitoring sessions. TLS 1.3 session tickets on the Web Server (10.45.50.15) are HMAC-bound to prevent replay. Internal PKI certificates are signed with SHA-384, exceeding NIST SP 800-57 minimums. All servers use BitLocker AES-256 full-disk encryption for data at rest.

© 2026 Sagar Patel. All rights reserved. Do not copy or redistribute without permission.

4.2 Network Access Control and Port Security

802.1X: All wired access ports on all three floor switches enforce 802.1X port authentication against AD/RADIUS (10.45.50.12). Staff devices use EAP-TLS (certificate-based); student devices use EAP-PEAP (username/password). Unauthenticated devices land in VLAN 99 and are redirected to the remediation portal on the Web Server (10.45.50.15).

DHCP Snooping: Enabled on all floor switches; only the trunk uplink port is trusted. Prevents rogue DHCP servers on any access port.

Dynamic ARP Inspection (DAI): Enabled on untrusted VLANs 30, 40, and 60. Blocks ARP poisoning and man-in-the-middle attacks by validating ARP packets against the DHCP snooping binding table.

IP Source Guard: Binds each access port to a specific IP-MAC pair from the DHCP snooping table, preventing IP address spoofing at the port level.

Device Hardening: Unused ports shut down and placed in VLAN 99. SSHv2 only (Telnet disabled). SNMPv3 AuthPriv enforced. TACACS+ centralized authentication via AD. Console and VTY timeout: 5 minutes. PortFast + BPDU Guard on all access ports.

Physical Security: Server room uses RFID badge access with all events logged to NMS/SIEM. IDF closets on Floors 1 and 2 are locked. Dome cameras in all hallways (VLAN 60) record continuously to the NMS/SIEM with 30-day retention.

5 Network Monitoring Plan

5.1 Architecture

The NMS/SIEM server at 10.45.50.11 is the centralized monitoring hub. Zabbix collects performance metrics via SNMPv3 AuthPriv polling from all switches, WAPs, and servers. Wazuh with Elastic Stack aggregates syslogs from all switches, 802.1X authentication records from NPS, DHCP lease events, and camera motion alerts. All devices forward syslog at severity 0–5 to 10.45.50.11. NetFlow v9 is enabled on the Cisco 3650-24PS to export per-flow records (source/dest IP, port, protocol, byte count) to the NMS for traffic baseline and anomaly analysis.

© 2026 Sagar Patel. All rights reserved. Do not copy or redistribute without permission.

5.2 Alert Thresholds and SIEM Correlation Rules

Metric	Method	Threshold / Alert	Response
Switch CPU	SNMPv3 poll	>70% for 5 min	Page admin; check for storm
Interface utilization	SNMP ifOctets	>80% of capacity	Capacity review
WAP client count	Cisco WLC MIB	>40 clients/AP	Deploy additional 1832i
DHCP pool utilization	DHCP syslog	>85% consumed	Expand scope
Packet loss / RTT	ICMP probes	>1% loss or >50 ms	Check port, cable, CPU
Failed 802.1X auth	NPS logs → SIEM	>10 failures/60 s	Auto port shutdown
IP camera offline	ICMP probe	Any offline	Physical inspection
Inter-VLAN ACL deny	Core syslog	VLAN30/40 → VLAN50 deny	Security incident ticket
Data exfiltration	NetFlow	>500 MB/hr server → external IP	SIEM alert; isolate host
Lateral movement	NetFlow + SIEM	Single IP → 5+ hosts/60 s	SIEM alert; investigate

Table 3: Alert thresholds and MITRE ATT&CK aligned SIEM rules (T1021 Lateral Movement, T1110 Credential Stuffing, T1041 Exfiltration)

5.3 Continuous Improvement

Weekly automated reports from Grafana + InfluxDB (fed by NetFlow) show total traffic per VLAN, top-10 IPs per floor, and protocol distribution. Configuration backups run nightly via TFTP to the File Server (10.45.50.10) with SHA-256 checksums logged to the SIEM for change detection. SIEM threat intel feeds update weekly with new CVEs for Cisco IOS, D-Link firmware, and Windows Server. If EASC expands to a fourth floor, the Core Switch has spare 1G SFP ports and the 10.50.x.x block is reserved for that expansion.

© 2026 Sagar Patel. All rights reserved. Do not copy or redistribute without permission.

6 Hardware Summary

Device	Model	Location	Role / Key Specs
Core Switch	Cisco Catalyst 3650-24PS	F3 Server Rm	Layer 3 SVIs, inter-VLAN routing, STP Root, WLC; 24×1G PoE+, 4×1G SFP
Floor 1 Switch	Cisco Catalyst 2960-24TC-L	F1 IDF	Layer 2 access, 802.1X; 24×1G + 2×1G SFP
Floor 2 Switch	D-Link DES-1210-28P	F2 IDF	Layer 2 + PoE for WAPs/VoIP; 24× PoE, 193W budget
Floor 3 Switch	D-Link DES-1026G	F3 IDF	Layer 2 access; 24×10/100, 2×1G uplink
Wireless AP	Cisco Aironet 1832i	All floors	802.11ac Wave 2, WPA3-Enterprise, 802.3af PoE, 3×3 MU-MIMO
File Server	Windows Server 2022	F3 Server Rm	Shared storage, nightly backups; 10.45.50.10
NMS / SIEM	Wazuh + Zabbix + Elastic	F3 Server Rm	Monitoring, security event mgmt; 10.45.50.11
Active Directory	Windows Server 2022	F3 Server Rm	802.1X RADIUS, group policy, PKI CA; 10.45.50.12
Database Server	Linux (PostgreSQL)	F3 Server Rm	Application and reporting DB; 10.45.50.13
DHCP / DNS Server	Windows Server 2022	F3 Server Rm	Dynamic IP assignment, internal DNS; 10.45.50.14
Web Server	Ubuntu 22.04 (Nginx)	F3 Server Rm	Internal portal, 802.1X remediation; 10.45.50.15

Table 4: Hardware inventory with roles and static IP assignments

References

[1] University of Texas at Austin, Information Technology Services. (2023). *Network infrastructure standards for academic buildings.* https://it.utexas.edu/infrastructure

[2] Cisco Systems. (2024). *Cisco Catalyst 3650 series switches data sheet.* https://www.cisco.com/c/en/us/products/switches/catalyst-3650-series-switches/datasheet.html

[3] Cisco Systems. (2024). *Aironet 1832i access point data sheet.* https://www.cisco.com/c/en/us/products/wireless/aironet-1800-series-access-points/datasheet.html

[4] National Institute of Standards and Technology. (2022). *Guide to enterprise patch management planning* (SP 800-40 Rev. 4). https://doi.org/10.6028/NIST.SP.800-40r4

[5] MITRE Corporation. (2024). *MITRE ATT&CK enterprise matrix.* https://attack.mitre.org

[6] Internet Engineering Task Force. (2018). *The Transport Layer Security (TLS) protocol version 1.3* (RFC 8446). https://datatracker.ietf.org/doc/html/rfc8446

© 2026 Sagar Patel. All rights reserved. Do not copy or redistribute without permission.