Network Security Assessment Report

Date: Aug-2025
Assessor: Aditya Shrivastava
Scope: Review of institutional multi-department network topology including wired and wireless infrastructure, servers, and distribution layers.

---

1. Observations

- **Topology Structure:**
  - Centralized MAN router connecting multiple distribution switches.
  - Departmental segmentation is visible but VLANs are not explicitly labeled.
  - Multiple wireless access points in AI/ML, AI/DS, and Library segments.
  - Critical servers (DNS, WEB, EMAIL) are in a central Server Room, connected via a Server Switch.
- **Potential Risk Points:**
  - **Wireless Access:** Open depiction of wireless endpoints suggests possible insecure configurations.
  - **Flat Layer 2 Segments:** No visible inter-VLAN routing or ACLs to restrict lateral movement between departments.
  - **Single Points of Failure:** MAN router and each distribution switch appear to have no redundancy.
  - **Device Naming Exposure:** Device hostnames in diagram could aid attackers in reconnaissance.
  - **Printer Security:** Network printers across departments may be unsecured and can be exploited.

---

2. Strengths

- Centralized server placement simplifies security monitoring and maintenance.
- Department-based grouping can facilitate VLAN segregation if implemented.
- Logical mapping of devices makes incident response planning easier.

---

3. Key Risks & Threats

Risk Area	Potential Impact	Likelihood
Unsecured Wi-Fi	Unauthorized network access, data theft	High
Lack of VLAN Segregation	Lateral movement in case of compromise	High
No Redundancy	Network downtime in case of switch/router failure	Medium
Printer Exploitation	Data leakage, foothold for attackers	Medium
Lack of Access Control	Unauthorized access to servers or sensitive systems	High

---

4. Recommendations

1. **Implement VLAN Segmentation** – Separate departments logically, enforce ACLs between VLANs.
2. **Secure Wireless Networks** – Use WPA3, disable SSID broadcast where possible, enable RADIUS authentication.
3. **Add Redundancy** – Deploy backup MAN router and redundant links between key distribution switches.
4. **Harden Printers** – Change default credentials, disable unused services, restrict access via IP filtering.
5. **Server Hardening** – Apply OS and application patches, enable firewalls, and segment server VLAN.
6. **Monitoring & Logging** – Deploy centralized SIEM to track anomalies across all departments.

Overall Security Posture: Moderate Risk – While the network has an organized topology, the lack of visible segmentation, potential unsecured wireless networks, and single points of failure make it susceptible to internal and external threats. Immediate improvements to wireless security, VLAN configuration, and redundancy are advised.