Network Components and Reasoning

The network is divided into several departments (e.g., ER, Radiology, Lab, Medical Records, Billing, IT, Admin/HR, Patient Rooms), each with its own PC and printer, as was instructed. Each devices are labeled with its respective VLAN number, subnet, and gateway. The private IP range 172.16.0.0–172.31.255.255 was provided for subnetting, and each department was assigned a unique subnet within this range to ensure proper network segmentation. Isolating department traffic (network segmentation) improves performance and limits the spread of potential attacks (Cisco, 2025).

To achieve secure wireless access, I created a staff Wi-Fi VLAN that uses WPA3-Enterprise encryption, linking it to the RADIUS server. WPA3-Enterprise encryption provides secure authentication and is commonly used in institutions, governments, and, in this case, hospitals, where network security is crucial (Cisco, 2025).

The network's main connection begins with the ISP cloud, followed by the firewall to filter incoming and outgoing traffic. This traffic passed through the core router and was then managed by the core switch. So from the core switch, the network branches out to various departments, the server farm, and the wireless network, creating a clear and efficient structure for traffic management.

Security Considerations

In real-world hospital settings, maintaining HIPAA compliance requires measures to protect Patient Health Information (PHI). For this project, the HIPAA database is stored on a central server and encrypted using AES-256 and is only accessible by certain VLANs. AES encryption is a secure cryptographic standard used to protect PHI both at rest and in transit (Tariq, 2025). I also implemented security tools, such as IDS/IPS (network layer), to monitor the network for abnormal activity (Maayan, 2023). The server farm includes essential services like EMR, PACS, DHCP, DNS, RADIUS, Backup, and Syslog/SIEM, all of which a real hospital would need.

The guest Wi-Fi VLAN is a key security feature. It is completely isolated and cannot access any of the hospital's internal resources. It was important to have a firewall to prevent guest network traffic from reaching the hospital's private network. Having a separate guest network limits "potential attackers' access and safeguards critical business data and systems" (Peppin, 2024, p. 8).

References

Cisco. (2025, May). What Is Network Segmentation? Cisco. https://www.cisco.com/site/us/en/learn/topics/security/what-is-network-segmentation.html

Cisco. (2025, October 6). WPA3 Deployment Guide. Cisco. https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/technical-reference/wpa3-dg.html

Tariq, Q. (2025, October 15). *HIPAA Encryption Standards for Developers: AES-256, TLS 1.3 & Data Integrity*. 7 Colors of Positivity. https://www.saatpro.com/2025/10/15/hipaa-encryption-standards-developers/

Maayan, G. (2023, January 27). Which Compliance Standards Require an IPS? Atlantic.net. https://www.atlantic.net/hipaa-compliant-hosting/which-compliance-standards-require-an-ips/

Peppin, R. (2024, May 30). Secure Internet & Guest Wi-Fi Security Practices. Cisco Spaces. https://spaces.cisco.com/six-best-practices-for-guest-wi-fi-security/