Dự án: Xây dựng Hạ tầng Mạng Kết nối cho Bệnh Viện Quy mô Lớn

# Mô tả

## 1. Tổng quan:

* **Quy mô Bệnh viện**
  + Hạng Bệnh viện: 1
  + Số lượng bệnh nhân nội trú: 400
  + Số lượng bệnh nhân ngoại trú trung bình: 3000
  + Nhân sự chính: 40
  + Nhân sự khác: 950
  + Nhân lực CNTT: 10
* **Mục tiêu:** Triển khai hạ tầng mạng hoàn chỉnh, an toàn, hiệu suất cao, đáp ứng nhu cầu kết nối của 1000 người dùng, 600 máy tính và số lượng lớn thiết bị y tế. Hệ thống phải đảm bảo tính sẵn sàng cao, bảo mật thông tin bệnh nhân, hỗ trợ các ứng dụng y tế chuyên biệt và dễ dàng mở rộng trong tương lai.
* **Phạm vi:** Thiết kế, triển khai và cấu hình các thành phần mạng như switch, router, firewall, access point, server, hệ thống lưu trữ, cùng các giải pháp bảo mật và an ninh mạng.

## 2. Yêu cầu chức năng:

* **Hạ tầng mạng:**
  + Kết nối ổn định, tốc độ cao, băng thông lớn cho tất cả người dùng và thiết bị.
  + Phân chia mạng thành các VLAN để tăng tính bảo mật và quản lý.
  + Hỗ trợ các giao thức mạng cần thiết cho ứng dụng y tế (ví dụ: DICOM, HL7).
  + Đảm bảo tính sẵn sàng cao với các giải pháp dự phòng.
  + Quản lý tập trung và giám sát hiệu suất mạng.
  + Hỗ trợ kết nối cho các thiết bị y tế chuyên dụng (máy chụp X-quang, MRI, v.v.)
* **Bảo mật:**
  + Bảo vệ thông tin bệnh nhân theo các quy định hiện hành (HIPAA, GDPR, v.v.).
  + Ngăn chặn truy cập trái phép và tấn công mạng.
  + Kiểm soát truy cập internet và ứng dụng.
  + Mã hóa dữ liệu nhạy cảm.
  + Quản lý danh tính và truy cập (IAM).
* **An ninh mạng:**
  + Phát hiện và phản ứng kịp thời các mối đe dọa.
  + Hệ thống tường lửa và IPS/IDS.
  + Quét và diệt virus, malware.
  + Đào tạo nhận thức an ninh mạng cho nhân viên.
  + Thực hiện đánh giá và kiểm tra an ninh mạng định kỳ.

## 3. Thiết kế chi tiết:

* **Kiến trúc mạng:**
  + Mô hình phân lớp 3 lớp: Core, Distribution, Access.
  + Sử dụng các switch layer 3 để định tuyến giữa các VLAN.
  + Triển khai các đường trục tốc độ cao (10Gbps hoặc hơn) giữa các lớp.
  + Cân nhắc sử dụng công nghệ SDN (Software-Defined Networking) để tăng tính linh hoạt và khả năng quản lý.
* **Phân vùng mạng:**
  + Tạo các VLAN cho các khu vực, nhóm người dùng, và loại thiết bị khác nhau (ví dụ: VLAN cho bác sĩ, VLAN cho bệnh nhân, VLAN cho quản lý, VLAN cho thiết bị y tế).
  + Áp dụng chính sách bảo mật riêng cho từng VLAN.
* **Kết nối không dây:**
  + Triển khai các access point Wi-Fi phủ sóng toàn bộ bệnh viện, đảm bảo tốc độ và độ ổn định cao.
  + Tạo các SSID riêng cho nhân viên, bệnh nhân, và khách.
  + Áp dụng các biện pháp bảo mật Wi-Fi mạnh mẽ (ví dụ: WPA3-Enterprise).
* **Hệ thống server và lưu trữ:**
  + Triển khai các server vật lý hoặc ảo để chạy các ứng dụng y tế (EMR/EHR, PACS, HIS, v.v.).
  + Sử dụng hệ thống lưu trữ SAN hoặc NAS để lưu trữ dữ liệu bệnh nhân, đảm bảo tính sẵn sàng cao và khả năng mở rộng.
  + Cân nhắc sử dụng công nghệ ảo hóa và điện toán đám mây để tối ưu hóa tài nguyên và giảm chi phí.
* **Giải pháp bảo mật:**
  + Triển khai tường lửa thế hệ mới (NGFW) với các tính năng như IPS/IDS, chống DDoS, và kiểm soát ứng dụng.
  + Sử dụng hệ thống SIEM (Security Information and Event Management) để thu thập và phân tích log từ các thiết bị mạng và bảo mật, giúp phát hiện các mối đe dọa tiềm ẩn.
  + Triển khai giải pháp bảo vệ endpoint (antivirus, EDR) cho tất cả các máy tính và thiết bị di động.
  + Mã hóa dữ liệu nhạy cảm khi truyền và lưu trữ.
  + Triển khai hệ thống quản lý danh tính và truy cập (IAM) để kiểm soát truy cập vào các tài nguyên mạng.
* **Giám sát và quản lý:**
  + Sử dụng hệ thống quản lý mạng tập trung để giám sát hiệu suất, phát hiện sự cố, và cấu hình các thiết bị mạng.
  + Triển khai hệ thống giám sát an ninh mạng để theo dõi các hoạt động bất thường và phát hiện các mối đe dọa tiềm ẩn.
  + Ghi nhật ký hoạt động mạng để phân tích và điều tra.

## 4. Triển khai và cấu hình:

* Lựa chọn các thiết bị mạng và bảo mật phù hợp, đảm bảo chất lượng và khả năng tương thích.
* Cấu hình các thiết bị theo thiết kế, đảm bảo tính bảo mật và hiệu suất cao.
* Kiểm tra và tối ưu hóa hiệu suất mạng.
* Đào tạo nhân viên về sử dụng và bảo mật hệ thống mạng.

## 5. Bảo trì và nâng cấp:

* Thực hiện bảo trì định kỳ cho hệ thống mạng.
* Cập nhật firmware và phần mềm thường xuyên.
* Theo dõi và đánh giá hiệu quả của hệ thống mạng.
* Nâng cấp hệ thống khi cần thiết để đáp ứng nhu cầu phát triển.

**Bên cạnh đó, dự án cũng cần xem xét các khía cạnh sau:**

* Tính khả dụng cao và khả năng phục hồi sau sự cố.
* Tích hợp với các hệ thống y tế hiện có (EMR/EHR, PACS, HIS, v.v.).
* Quản lý danh tính và truy cập.
* Đào tạo và hỗ trợ người dùng.
* Tuân thủ các quy định về bảo mật thông tin y tế.

Một số khía cạnh quan trọng cần được xem xét và bổ sung vào dự án xây dựng hạ tầng mạng kết nối cho Bệnh viện quy mô lớn:

## 6. Giải pháp nâng cao:

* **QoS (Quality of Service):** Ưu tiên băng thông cho các ứng dụng quan trọng như truyền hình ảnh y tế (DICOM), hội chẩn từ xa, EMR/EHR, đảm bảo hoạt động mượt mà và không bị gián đoạn.
* **Redundancy và High Availability:** Sử dụng các công nghệ như HSRP, VRRP, STP, link aggregation để đảm bảo tính liên tục của dịch vụ, ngay cả khi có sự cố xảy ra trên một số thành phần mạng.
* **Load Balancing:** Cân bằng tải giữa các server và đường truyền để tối ưu hóa hiệu suất và tránh quá tải.
* **Wireless Security:** Sử dụng các giải pháp bảo mật không dây nâng cao như NAC (Network Access Control), rogue AP detection, và wireless intrusion prevention để bảo vệ mạng Wi-Fi khỏi các mối đe dọa.
* **Network Segmentation:** Phân chia mạng thành các phân đoạn nhỏ hơn để giới hạn tác động của các cuộc tấn công và nâng cao khả năng kiểm soát truy cập.
* **Zero Trust Security:** Áp dụng mô hình Zero Trust, không tin tưởng bất kỳ thiết bị hoặc người dùng nào một cách mặc định, yêu cầu xác thực và ủy quyền liên tục để truy cập vào các tài nguyên mạng.

## 7. Các yếu tố khác cần xem xét:

* **Ngân sách:** Xác định ngân sách dự án và lựa chọn các giải pháp phù hợp.
* **Thời gian triển khai:** Lập kế hoạch triển khai chi tiết và đảm bảo hoàn thành đúng tiến độ.
* **Đào tạo và hỗ trợ:** Đào tạo nhân viên IT và người dùng cuối về cách sử dụng và bảo mật hệ thống mạng mới.
* **Tương lai:** Thiết kế hệ thống mạng có khả năng mở rộng và nâng cấp để đáp ứng nhu cầu phát triển của bệnh viện trong tương lai.
* **IoT (Internet of Things):** Xem xét việc tích hợp các thiết bị IoT y tế vào mạng lưới, đảm bảo an ninh và quản lý hiệu quả.
* **Backup và Disaster Recovery:** Thiết lập hệ thống sao lưu dữ liệu và kế hoạch phục hồi sau thảm họa để đảm bảo tính liên tục của hoạt động bệnh viện.

## 8. Quy trình thực hiện dự án:

1. **Khảo sát và thu thập yêu cầu:** Tìm hiểu kỹ về nhu cầu hiện tại và tương lai của bệnh viện, các ứng dụng y tế sử dụng, quy mô và cấu trúc tổ chức, cũng như các quy định về bảo mật thông tin y tế.
2. **Thiết kế chi tiết:** Dựa trên các yêu cầu đã thu thập, xây dựng thiết kế chi tiết bao gồm các sơ đồ mạng, danh sách thiết bị, cấu hình, giải pháp bảo mật, và kế hoạch triển khai.
3. **Lựa chọn nhà thầu:** Lựa chọn nhà thầu có kinh nghiệm và năng lực để triển khai dự án.
4. **Triển khai:** Giám sát chặt chẽ quá trình triển khai, đảm bảo tuân thủ thiết kế và hoàn thành đúng tiến độ.
5. **Kiểm thử và nghiệm thu:** Tiến hành kiểm thử toàn diện hệ thống mạng mới, đảm bảo tất cả các chức năng hoạt động ổn định và đáp ứng yêu cầu.
6. **Đào tạo và chuyển giao:** Đào tạo nhân viên IT và người dùng cuối về cách sử dụng và bảo mật hệ thống mạng mới.
7. **Bảo trì và hỗ trợ:** Cung cấp dịch vụ bảo trì và hỗ trợ sau triển khai để đảm bảo hệ thống mạng luôn hoạt động tốt.

## Kết luận:

Việc xây dựng hạ tầng mạng kết nối cho một bệnh viện quy mô lớn là một dự án phức tạp và quan trọng. Bằng cách xem xét kỹ lưỡng các yêu cầu, thiết kế chi tiết, và triển khai cẩn thận, bệnh viện có thể xây dựng một hệ thống mạng an toàn, hiệu quả, và hỗ trợ tốt cho các hoạt động khám chữa bệnh và quản lý.

# YÊU CẦU

### Bước 1 (1 điểm): Tìm ra các cấu trúc mạng phù hợp cho các tòa nhà trong bệnh viện

* Phân tích các yêu cầu về hệ thống mạng của Site chính và hai Site phụ
* Lập danh sách kiểm tra để khảo sát tại các vị trí lắp đặt
* Xác định các khu vực có tải mạng để lựa chọn cấu hình thiết bị phù hợp (bộ cân bằng tải được đặt ở các vị trí cần thiết)
* Chọn cấu trúc mạng phù hợp với kiến ​​trúc của tòa nhà, thuận tiện và thẩm mỹ
* Thiết kế việc sử dụng mạng trong môi trường không dây, áp dụng các tiêu chuẩn bảo mật mạng và thiết lập các phân vùng cho máy chủ và thiết bị mạng (ví dụ: Server farm, DMZ, Firewall, ...)

### Bước 2 (1 điểm): Danh sách các thiết bị tối thiểu, sơ đồ IP và sơ đồ đấu dây (cáp)

* Danh sách các thiết bị được khuyến nghị và thông số kỹ thuật tiêu biểu
* Sơ đồ thiết lập vật lý của mạng
* Sơ đồ kết nối WAN giữa Site chính và hai Site phụ (sử dụng công nghệ WAN mới như SD-WAN, MPLS và giao thức định tuyến OSPF)

### Bước 3 (1 point): Tính toán thông lượng cần thiết và băng thông dự kiến ​​từ ISP, sau đó đề xuất cấu hình cho mạng bệnh viện

### Bước 4 (2 điểm): Thiết kế bản đồ mạng bằng phần mềm mô phỏng Packet Tracer hoặc GNS3

### Bước 5 (2 điểm): Kiểm tra hệ thống bằng các công cụ phổ biến như ping, traceroute, v.v. trên hệ thống mô phỏng.

### Bước 6 (2 điểm): Đánh giá lại hệ thống mạng đã thiết kế thông qua các tính năng sau: độ tin cậy, dễ nâng cấp, phần mềm hỗ trợ đa dạng, an toàn, bảo mật mạng, v.v.

* Các vấn đề còn lại cho dự án
* Định hướng phát triển trong tương lai

### Bước 7 (1 điểm): Tải tẬp mô phỏng (sử dụng Packet Tracer hoặc GNS-3) và báo cáo dự án lên LMS trước thời hạn.

Trong báo cáo và bản demo kết quả, sinh viên được yêu cầu kiểm tra khả năng kết nối:

* Kết nối giữa các PC trong cùng một VLAN
* Kết nối các PC giữa các VLAN
* Kết nối các PC giữa Site chính và hai Site phụ
* Kết nối với máy chủ trong DMZ
* Không có kết nối nào từ thiết bị của Khách hàng đến PC trên LAN
* Kết nối Internet đến máy chủ Web.

# TÀI LIỆU THAM KHẢO

* Thông tin được chọn lọc từ Internet
* Tài liệu tham khảo cho môn Mạng máy tính

# THỜI GIAN

Hạn chót báo cáo: **23g, 15/12/2024**.

Bản mềm (nộp cho LMS trước hạn chót) và bản cứng (cần thiết cho buổi thuyết trình và demo).

Một ví dụ về giải pháp xây dựng mạng kết nối cho bệnh viện

# 1. Tổng Quan

* **Quy mô Bệnh viện**
  + Hạng Bệnh viện: 1
  + Số lượng bệnh nhân nội trú: 400
  + Số lượng bệnh nhân ngoại trú trung bình: 3000
  + Nhân sự chính: 40
  + Nhân sự khác: 950
  + Nhân lực CNTT: 10
* **Mục tiêu:** Xây dựng hạ tầng mạng an toàn, hiệu quả, hỗ trợ 1000 người dùng & 600 máy tính, đảm bảo tính sẵn sàng cao, bảo mật thông tin bệnh nhân, hỗ trợ ứng dụng y tế chuyên biệt.
* **Phạm vi:** Thiết kế, triển khai, cấu hình: switch, router, firewall, access point, server, lưu trữ, giải pháp bảo mật, an ninh mạng.

# 2. Yêu Cầu Chức Năng

## Hạ tầng mạng:

* Kết nối ổn định, tốc độ cao (tối thiểu 1Gbps cho người dùng, 10Gbps cho server/lưu trữ).
* Phân chia VLAN (nhân viên, bệnh nhân, khách, quản lý, thiết bị y tế, camera, v.v.)
* Hỗ trợ giao thức DICOM, HL7.
* Redundancy (link aggregation, HSRP/VRRP, STP)
* Quản lý tập trung, giám sát hiệu suất (SNMP, Syslog, NetFlow)

## Bảo mật:

* Tuân thủ quy định bảo mật thông tin y tế.
* Ngăn chặn truy cập trái phép, tấn công mạng.
* Kiểm soát truy cập internet, ứng dụng (firewall, content filtering).
* Mã hóa dữ liệu (AES-256).

## An ninh mạng:

* Phát hiện, phản ứng kịp thời mối đe dọa (IPS/IDS, SIEM).
* Tường lửa, chống DDoS.
* Quét virus, malware.
* Đào tạo nhận thức an ninh mạng.

# 3. Thiết Kế Chi Tiết

## 3.1. Kiến trúc mạng:

### Mô hình 3 lớp:

* Core Layer: 2 switch Cisco Catalyst 9500 (redundant, 40Gbps uplink)
* Distribution Layer: 4 switch Cisco Catalyst 9300 (2 switch/tầng, 10Gbps uplink)
* Access Layer: Các switch Cisco Catalyst 2960X/3560CX (PoE cho IP phone, camera, AP)

### VLAN:

* VLAN 10: Nhân viên
* VLAN 20: Bệnh nhân (guest access)
* VLAN 30: Quản lý
* VLAN 40: Thiết bị y tế
* VLAN 50: Camera
* VLAN 100: Server/lưu trữ

### Định tuyến:

* Router Cisco ISR 4331 (kết nối Internet, VPN)
* OSPF cho định tuyến nội bộ

### Kết nối không dây:

* Cisco Aironet 3800 series APs (phủ sóng toàn bộ)
* SSID nhân viên, bệnh nhân (cách ly, portal captive)
* WPA3-Enterprise

## 3.2. Server & Lưu trữ:

### Máy chủ:

* 2x Dell PowerEdge R740xd (VMware ESXi, ứng dụng y tế, EMR/EHR)
* 1x Dell PowerEdge R440 (Active Directory, file server)

### Lưu trữ:

* Dell EMC Unity 380F (SAN)
* Synology RS3618xs (NAS, backup)

## 3.3. Bảo mật:

* **Tường lửa:**
  + Fortinet FortiGate 600E (NGFW, IPS/IDS, chống DDoS, web filtering)
* **Bảo vệ endpoint:**
  + Symantec Endpoint Protection (antivirus, EDR)
* **Quản lý danh tính:**
  + Microsoft Active Directory
  + Cisco ISE (NAC)
* **Mã hóa:**
  + BitLocker (ổ cứng)
  + VPN (truy cập từ xa)

## 3.4. Giám sát & Quản lý:

* **SolarWinds Network Performance Monitor (NPM)**
* **SolarWinds Security Event Manager (SEM)**
* **Cisco Prime Infrastructure**
* **Zabbix**

## 4. Triển khai & Cấu hình

* Lựa chọn thiết bị theo bản thiết kế
* Cấu hình VLAN, định tuyến, QoS, bảo mật
* Kiểm tra, tối ưu hóa hiệu suất
* Đào tạo nhân viên IT

## 5. Bảo trì & Nâng cấp

* Bảo trì định kỳ
* Cập nhật firmware, phần mềm
* Theo dõi, đánh giá hiệu quả
* Nâng cấp khi cần thiết
* Thiết kế hệ thống mạng có khả năng mở rộng và nâng cấp để đáp ứng nhu cầu phát triển của bệnh viện trong tương lai.

## 6. Các giải pháp nâng cao:

* **QoS (Quality of Service):** Ưu tiên băng thông cho các ứng dụng quan trọng như truyền hình ảnh y tế (DICOM), hội chẩn từ xa, EMR/EHR, đảm bảo hoạt động mượt mà và không bị gián đoạn.
* **Redundancy và High Availability:** Sử dụng các công nghệ như HSRP, VRRP, STP, link aggregation để đảm bảo tính liên tục của dịch vụ, ngay cả khi có sự cố xảy ra trên một số thành phần mạng.
* **Load Balancing:** Cân bằng tải giữa các server và đường truyền để tối ưu hóa hiệu suất và tránh quá tải.
* **SDN (Software-Defined Networking):** Áp dụng SDN để tự động hóa việc quản lý và cấu hình mạng, tăng tính linh hoạt và khả năng thích ứng với thay đổi (Cisco ACI).
* **Wireless Security:** Sử dụng các giải pháp bảo mật không dây nâng cao như NAC (Network Access Control), rogue AP detection, và wireless intrusion prevention để bảo vệ mạng Wi-Fi khỏi các mối đe dọa.
* Hệ thống dự phòng nguồn điện (UPS)
* Hệ thống camera giám sát

Một số khía cạnh quan trọng cần được xem xét và bổ sung vào bản thiết kế chi tiết để đảm bảo tính toàn diện và hiệu quả của hệ thống mạng cho Bệnh viện Mắt:

## 6. Sơ đồ mạng:

* Cung cấp sơ đồ mạng logic và sơ đồ mạng vật lý chi tiết, thể hiện rõ ràng các thành phần mạng, kết nối, VLAN, địa chỉ IP, và các giải pháp bảo mật được triển khai.
* Sơ đồ mạng nên dễ hiểu, trực quan, và có thể được sử dụng để tham khảo trong quá trình triển khai, vận hành, và bảo trì hệ thống.

## 7. Cấu hình chi tiết:

* Cung cấp cấu hình chi tiết cho từng thiết bị mạng, bao gồm:
  + Switch: Cấu hình VLAN, trunking, STP, port security, QoS, v.v.
  + Router: Cấu hình định tuyến (OSPF), NAT, ACL, VPN, v.v.
  + Firewall: Cấu hình các rule, policy, IPS/IDS, chống DDoS, web filtering, v.v.
  + Access point: Cấu hình SSID, bảo mật, roaming, v.v.
  + Server: Cấu hình hệ điều hành, ứng dụng, dịch vụ, bảo mật, v.v.

## 8. Kế hoạch triển khai:

* Xây dựng kế hoạch triển khai chi tiết, bao gồm các bước thực hiện, thời gian, nguồn lực, và các rủi ro tiềm ẩn.
* Kế hoạch triển khai nên được chia thành các giai đoạn rõ ràng, đảm bảo không ảnh hưởng đến hoạt động của bệnh viện.

## 9. Đánh giá rủi ro và kế hoạch khắc phục sự cố:

* Tiến hành đánh giá rủi ro toàn diện cho hệ thống mạng, xác định các mối đe dọa tiềm ẩn và các điểm yếu có thể bị khai thác.
* Xây dựng kế hoạch khắc phục sự cố chi tiết, bao gồm các quy trình xử lý khi xảy ra sự cố mạng, mất điện, thiên tai, hoặc các tình huống khẩn cấp khác.

## 10. Đào tạo và chuyển giao:

* Xây dựng chương trình đào tạo chi tiết cho nhân viên IT và người dùng cuối, bao gồm các nội dung về cách sử dụng, bảo mật, và xử lý sự cố mạng cơ bản.
* Chuyển giao toàn bộ tài liệu thiết kế, cấu hình, và vận hành hệ thống cho bệnh viện.

## 11. Hợp đồng bảo trì và hỗ trợ:

* Đề xuất các gói dịch vụ bảo trì và hỗ trợ sau triển khai, bao gồm hỗ trợ kỹ thuật từ xa, bảo trì định kỳ, và nâng cấp hệ thống.

## 12. Ngân sách dự án:

* Xây dựng bảng ngân sách chi tiết, bao gồm chi phí thiết bị, phần mềm, triển khai, đào tạo, và bảo trì.

## 13. Quy trình thực hiện dự án:

1. **Khảo sát và thu thập yêu cầu:** Tìm hiểu kỹ về nhu cầu hiện tại và tương lai của bệnh viện, các ứng dụng y tế sử dụng, quy mô và cấu trúc tổ chức, cũng như các quy định về bảo mật thông tin y tế.
2. **Thiết kế chi tiết:** Dựa trên các yêu cầu đã thu thập, xây dựng thiết kế chi tiết bao gồm các sơ đồ mạng, danh sách thiết bị, cấu hình, giải pháp bảo mật, và kế hoạch triển khai.
3. **Lựa chọn nhà thầu:** Lựa chọn nhà thầu có kinh nghiệm và năng lực để triển khai dự án.
4. **Triển khai:** Giám sát chặt chẽ quá trình triển khai, đảm bảo tuân thủ thiết kế và hoàn thành đúng tiến độ.
5. **Kiểm thử và nghiệm thu:** Tiến hành kiểm thử toàn diện hệ thống mạng mới, đảm bảo tất cả các chức năng hoạt động ổn định và đáp ứng yêu cầu.
6. **Đào tạo và chuyển giao:** Đào tạo nhân viên IT và người dùng cuối về cách sử dụng và bảo mật hệ thống mạng mới.
7. **Bảo trì và hỗ trợ:** Cung cấp dịch vụ bảo trì và hỗ trợ sau triển khai để đảm bảo hệ thống mạng luôn hoạt động tốt.

**Lưu ý quan trọng:**

* Bản thiết kế chi tiết cần được điều chỉnh và tùy chỉnh dựa trên yêu cầu cụ thể, khảo sát hiện trạng, và ngân sách của Bệnh viện Mắt.
* Việc triển khai dự án nên được thực hiện bởi các chuyên gia mạng và bảo mật có kinh nghiệm, đảm bảo tuân thủ các tiêu chuẩn và quy định hiện hành.
* Bệnh viện cần có một đội ngũ IT nội bộ đủ năng lực để vận hành và bảo trì hệ thống mạng sau khi triển khai.

# Kết luận:

Việc thiết kế và triển khai một hệ thống mạng toàn diện cho Bệnh viện quy mô lớn đòi hỏi sự đầu tư về thời gian, công sức và tài chính. Tuy nhiên, một hệ thống mạng được thiết kế tốt sẽ mang lại nhiều lợi ích cho bệnh viện, bao gồm:

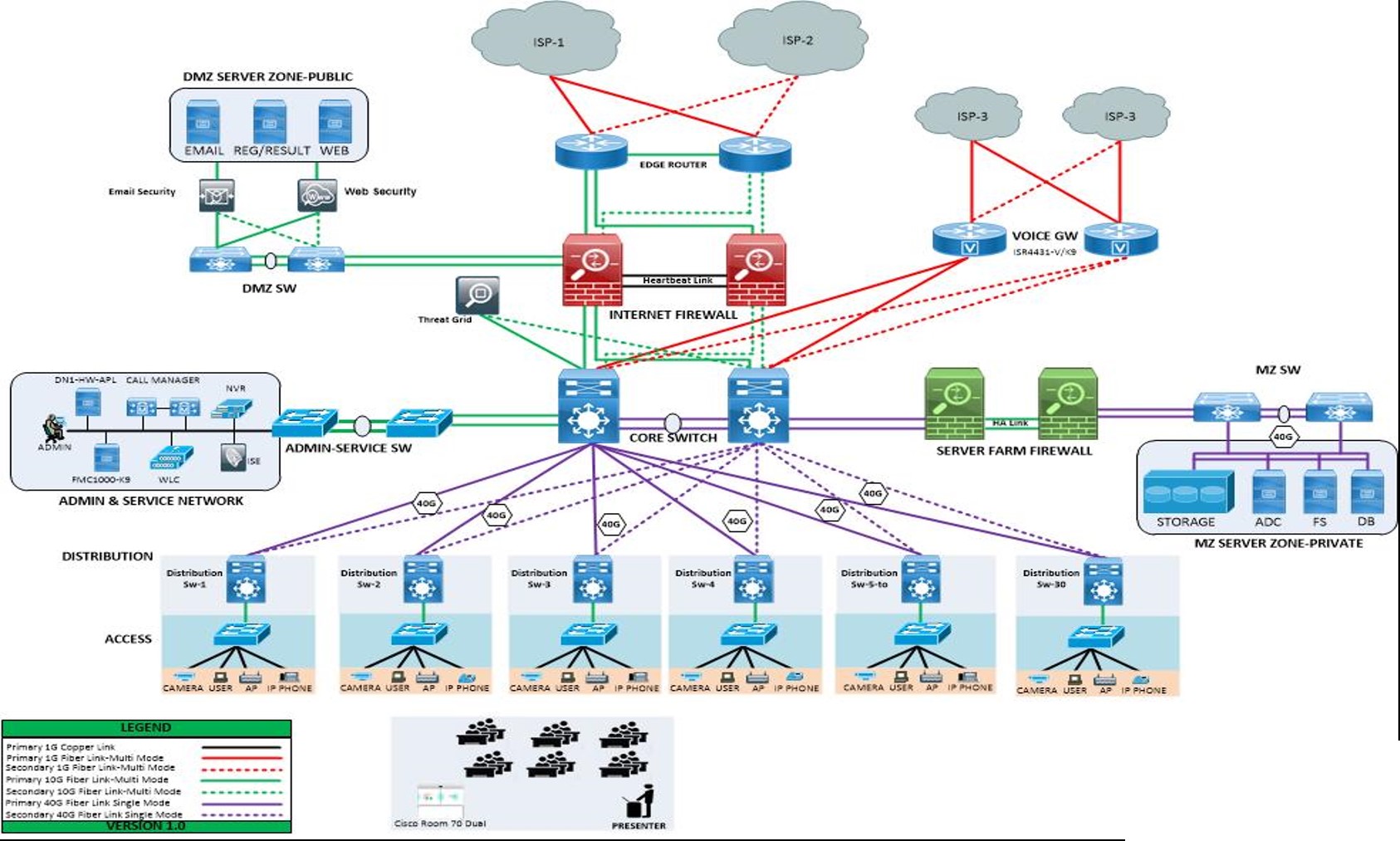
* **Nâng cao hiệu quả hoạt động:** Hỗ trợ các quy trình khám chữa bệnh, quản lý bệnh viện, và nghiên cứu y khoa.
* **Cải thiện trải nghiệm bệnh nhân:** Cung cấp các dịch vụ trực tuyến, truy cập thông tin y tế, và giải trí cho bệnh nhân.
* **Đảm bảo an toàn thông tin:** Bảo vệ thông tin nhạy cảm của bệnh nhân và bệnh viện.
* **Tăng cường khả năng cạnh tranh:** Nâng cao hình ảnh và uy tín của bệnh viện.

# Phụ lục

## Sơ Đồ Mạng cho Bệnh Viện Mắt

**Lưu ý:** Các sơ đồ dưới đây mang tính chất minh họa và có thể được điều chỉnh dựa trên yêu cầu thực tế và khảo sát hiện trạng của bệnh viện.

### 1. Sơ Đồ Mạng Logic



* **VLAN 10 (Nhân viên):** Máy tính, điện thoại IP của nhân viên.
* **VLAN 20 (Bệnh nhân):** Truy cập mạng cho bệnh nhân (guest access).
* **VLAN 30 (Quản lý):** Máy tính, điện thoại IP của ban quản lý.
* **VLAN 40 (Thiết bị y tế):** Các thiết bị y tế kết nối mạng.
* **VLAN 50 (Camera):** Hệ thống camera giám sát.
* **VLAN 100 (Server/Lưu trữ):** Máy chủ và hệ thống lưu trữ.

### 2. Sơ Đồ Mạng Vật Lý (Ví dụ)

* Sơ đồ này sẽ phức tạp hơn, thể hiện các kết nối vật lý giữa các thiết bị, bao gồm:
  + Cáp mạng (loại, tốc độ)
  + Kết nối dự phòng (link aggregation)
  + Vị trí đặt các thiết bị (phòng máy chủ, các tầng, khu vực)
  + Thông tin về địa chỉ IP

**Các điểm quan trọng cần lưu ý:**

* **Tính sẵn sàng cao:** Sử dụng các công nghệ như HSRP/VRRP trên các router và switch lớp Core/Distribution để đảm bảo tính liên tục của dịch vụ.
* **Bảo mật:** Triển khai tường lửa, IPS/IDS, và các biện pháp bảo mật khác để bảo vệ hệ thống khỏi các mối đe dọa.
* **Phân vùng mạng:** Sử dụng VLAN để phân chia mạng thành các khu vực riêng biệt, tăng cường bảo mật và quản lý.
* **Hiệu suất:** Sử dụng các đường truyền tốc độ cao và QoS để đảm bảo hiệu suất tốt cho các ứng dụng quan trọng.

**Bản thiết kế chi tiết sẽ bao gồm các sơ đồ mạng đầy đủ và chi tiết hơn, cũng như cấu hình cụ thể cho từng thiết bị.**