GIẢI TRÌNH CHỈNH SỬA

I. THÔNG TIN CHUNG:

1. Tên đồ án: **TRIỂN KHAI RADIUS TRÊN WINDOWS SERVER**
2. Nhóm: 12

II. NỘI DUNG CHỈNH SỬA

STT	Yêu cầu hình sửa	Nội dung chỉnh sửa của nhóm (trình bày ngắn gọn các ý đã chỉnh sửa)	Chú thích (Trang tương ứng với nội dung đã chỉnh sửa trong báo cáo hoặc tên file/link demo,…)
1	Các thuật toán RADIUS dùng để xác thực	□ **PAP (Password Authentication Protocol)**: Xác thực đơn giản, gửi mật khẩu dưới dạng plaintext, dễ triển khai nhưng không an toàn. □ **CHAP (Challenge-Handshake Authentication Protocol)**: Bảo mật hơn PAP, không truyền mật khẩu trực tiếp. Sử dụng chuỗi ngẫu nhiên (challenge) và giá trị băm (hash) để xác minh. Vẫn có điểm yếu trước một số tấn công. □ **MS-CHAP (Microsoft CHAP)**: Phiên bản nâng cấp của CHAP, hỗ trợ xác thực hai chiều và mã hóa dữ liệu trong quá trình xác thực. □ **EAP (Extensible Authentication Protocol)**: Khuôn khổ mở rộng, hỗ trợ nhiều phương thức: • **EAP-TLS**: Xác thực bằng chứng chỉ số, bảo mật cao nhất. • **EAP-TTLS/PEAP**: Sử dụng kênh mã hóa để bảo vệ thông	Trang 8, 9

		tin xác thực.	
2	Chuẩn của RADIUS là gì	RADIUS hoạt động theo chuẩn IEEE 802.1X, kiểm soát truy cập mạng có dây (LAN) và không dây (WLAN), với cấu trúc gồm: 1. **Supplicant (Client)**: Thiết bị người dùng gửi thông tin xác thực (tên đăng nhập, mật khẩu, chứng chỉ số) đến Authenticator. 2. **Authenticator (Thiết bị mạng)**: Switch (mạng có dây) hoặc Access Point (mạng không dây), đóng vai trò trung gian, chuyển thông tin xác thực đến Authentication Server. 3. **Authentication Server (RADIUS Server)**: Xác thực thông tin dựa trên giao thức EAP, quyết định cho phép hoặc từ chối kết nối.	Trang 9
3	Nếu RADIUS sập thì xác thực như thế nào	**Cấu hình xác thực dự phòng (Fallback Authentication)**: • **Xác thực cục bộ**: Sử dụng tài khoản và mật khẩu lưu trên thiết bị (router, switch). • **Máy chủ RADIUS dự phòng**: Cài đặt máy chủ RADIUS thứ hai để đảm bảo hoạt động liên tục. **Triển khai High Availability (HA)**: • **Cluster RADIUS Servers**:	Trang 12, 13

		Duy trì cụm máy chủ RADIUS hoạt động song song. • **Load Balancer**: Phân phối yêu cầu xác thực giữa các máy chủ RADIUS. **Xác thực cục bộ khẩn cấp**: • Quản trị viên kích hoạt tài khoản cục bộ bằng câu lệnh trên router. **Cải thiện giám sát và bảo trì**: • **Giám sát**: Sử dụng công cụ như Zabbix, Nagios để theo dõi máy chủ RADIUS. • **Backup và Restore**: Thường xuyên sao lưu máy chủ RADIUS và Active Directory để khôi phục nhanh khi cần.	
4	Các quyền cấp cho router	**Mô tả các cấp độ quyền (Privilege Levels)**: • **Level 0**: Quyền tối thiểu, chỉ các lệnh cơ bản như logout, enable, exit. • **Level 1**: Chế độ **User EXEC**, chỉ được đọc và xem thông tin hệ thống (e.g., ping, show interface). • **Level 2-14**: Tùy chỉnh quyền theo mục đích quản trị: o **Level 2**: Xử lý cơ bản (e.g., ping, traceroute). o **Level 3**: Xử lý nâng cao (e.g., debug ip packet).	Trang 22, 23

		• **Level 4-14**: Cấu hình cụ thể cho các chức năng như **interface**, **routing, ACLs**, **VLAN**, **QoS**, **backup**. • **Level 15**: Quyền cao nhất, truy cập đầy đủ vào tất cả các lệnh và cấu hình Router.	
5	Xác thực radius trước khi truy cập mạng		