

**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG**

**NGUYỄN ĐẶNG QUỲNH NHƯ'
NGUYỄN PHÚC NHI
ĐINH BẠCH KIỀU PHƯƠNG
PHẠM TRẦN HỒNG PHÚC
LÊ VIỆT TIẾN**

**BÁO CÁO ĐỒ ÁN
QUẢN TRỊ MẠNG VÀ HỆ THỐNG – NT132.P12.ANTT
TRIỂN KHAI RADIUS TRÊN WINDOWS SERVER**

Thành phố Hồ Chí Minh, tháng 11 năm 2024

**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG**

NGUYỄN ĐẶNG QUỲNH NHƯ – MSSV: 22521050

NGUYỄN PHÚC NHI – MSSV: 22521041

ĐINH BẠCH KIỀU PHƯƠNG – MSSV: 21520406

PHẠM TRẦN HỒNG PHÚC – MSSV: 22521138

LÊ VIỆT TIẾN – MSSV: 20522007

**BÁO CÁO ĐỒ ÁN
QUẢN TRỊ MẠNG VÀ HỆ THỐNG – NT132.P12.ANTT
TRIỂN KHAI RADIUS TRÊN WINDOWS SERVER**

**GIẢNG VIÊN HƯỚNG DẪN
ThS. ĐỖ HOÀNG HIỂN**

Thành phố Hồ Chí Minh, tháng 11 năm 2024

LỜI CẢM ƠN

Lời đầu tiên, chúng em xin phép gửi lời cảm ơn sâu sắc đến tập thể quý thầy cô trường Đại học Công nghệ Thông tin - Đại học Quốc gia TP.HCM, quý thầy cô khoa Mạng máy tính & Truyền thông giúp chúng em học tập và có được những kiến thức nền tảng cũng như cung cấp các tài nguyên liên quan để hoàn thành được dự án này.

Đặc biệt, chúng em xin gửi lời cảm ơn chân thành đến thầy Đỗ Hoàng Hiền. Với sự tâm huyết, được sự tận tình giảng dạy và hỗ trợ hết lòng của thầy đã cho chúng em nhiều kiến thức bổ ích. Với tình cảm sâu sắc, chân thành, chúng em xin bày tỏ lòng biết ơn đến thầy đã nhiệt tình, hết mình với sinh viên. Đó là động lực rất lớn để chúng em có thể hoàn thành tốt đồ án lần này.

Với điều kiện thời gian cũng như kinh nghiệm còn hạn chế, chúng em đã cố gắng hết mình nhưng đồ án không thể tránh được những thiếu sót. Chúng em rất hy vọng nhận được sự chỉ bảo và đóng góp ý kiến từ thầy để bổ sung, nâng cao kiến thức của mình, phục vụ và hoàn thiện hơn trong những đồ án sau này và khóa luận tốt nghiệp trong tương lai.

Chúng em xin chân thành cảm ơn!

Nhóm thực hiện

MỤC LỤC

TÓM TẮT ĐỒ ÁN.....	4
CHƯƠNG 1: TỔNG QUAN.....	6
1.1. Giới thiệu:.....	6
1.2. Đề Tài:.....	6
1.3. Mục tiêu đề tài:.....	6
CHƯƠNG 2: GIỚI THIỆU VỀ RADIUS, WINDOWS SERVER VÀ CÁC CÔNG NGHỆ LIÊN QUAN.....	8
2.1. Giới thiệu về RADIUS:.....	8
2.1.1. RADIUS:.....	8
2.1.2. Cấu trúc của RADIUS:.....	10
2.1.3. Một số dịch vụ chính trong RADIUS:.....	10
2.1.4. Ưu điểm và nhược điểm khi triển khai RADIUS:.....	11
2.1.5. Biện pháp dự phòng khi RADIUS không còn hoạt động:.....	12
2.2. Giới thiệu về Windows Server và Network Policy Server (NPS):.....	13
2.2.1. Windows Server:.....	13
2.2.2. Network Policy Server (NPS):.....	13
2.2.3. Các chức năng chính của NPS:.....	14
2.3. Giới thiệu về Active Directory:.....	14
2.3.1. Active Directory:.....	14
2.3.2. Cấu trúc của Active Directory:.....	14
2.3.3. Các chức năng chính của AD:.....	15
CHƯƠNG 3: TRIỂN KHAI HỆ THỐNG.....	16
3.1. Triển khai Active Directory:.....	17
3.2. Triển khai Network Policy and Access Server và DNS Server:.....	20
3.3. Thiết lập RADIUS và thực hiện phân quyền truy cập.....	21
3.4. Cấu hình Router (GW) trong hệ thống mạng:.....	24
3.5. Cài đặt phần mềm cho các Client.....	25
CHƯƠNG 4: ĐÁNH GIÁ THỬ NGHIỆM.....	26
4.1. Thử nghiệm cho Client kết nối với Router (GW).....	26
4.2. Thử nghiệm theo dõi và ghi lại hoạt động người dùng.....	30
CHƯƠNG 5: KẾT LUẬN.....	32
TÀI LIỆU THAM KHẢO.....	34
PHỤ LỤC LINK CÁC DEMO.....	35

TÓM TẮT ĐỒ ÁN

Đồ án tập trung vào việc nghiên cứu và triển khai hệ thống RADIUS (Remote Authentication Dial-In User Service) trên Windows Server nhằm quản lý quyền truy cập trong mạng doanh nghiệp. RADIUS được sử dụng để thực hiện xác thực, phân quyền và ghi log, mang lại khả năng bảo mật cao và quản lý tập trung hiệu quả. Công cụ Network Policy Server (NPS) tích hợp với Active Directory (AD) được chọn làm nền tảng chính để triển khai hệ thống.

Nhóm thực hiện đồ án đã xây dựng một mô hình gồm 5 máy tính, trong đó có một máy chủ RADIUS và bốn máy khách. Máy chủ RADIUS được tích hợp với Active Directory để quản lý người dùng theo nhóm (như ITADMIN và HR), phân quyền và áp dụng chính sách bảo mật. Router Cisco được cấu hình để sử dụng máy chủ RADIUS làm điểm xác thực tập trung, hỗ trợ giao thức Telnet và SSH. Hệ thống đảm bảo chỉ nhóm ITADMIN có quyền truy cập vào router, trong khi các nhóm khác bị từ chối.

Quá trình triển khai bao gồm:

- Cài đặt Active Directory và thiết lập các Organizational Units, nhóm và người dùng.
- Triển khai NPS làm máy chủ RADIUS, tích hợp với AD để áp dụng chính sách phân quyền.
- Cấu hình Router để kết nối với máy chủ RADIUS, thiết lập DHCP và quản lý kết nối từ xa.
- Thực hiện các thử nghiệm kiểm tra khả năng xác thực, phân quyền và ghi log hoạt động người dùng.

Kết quả thử nghiệm cho thấy hệ thống hoạt động chính xác theo yêu cầu đề ra. Các tài khoản thuộc nhóm ITADMIN có thể truy cập router qua Telnet/SSH, trong khi nhóm HR bị hạn chế quyền truy cập. Hệ thống cũng ghi lại đầy đủ log hoạt động, giúp quản trị viên theo dõi và phân tích các hành động của người dùng. Thông qua

việc thực hiện đồ án, nhóm đã củng cố kiến thức về quản trị mạng, triển khai dịch vụ xác thực và áp dụng chính sách bảo mật trong môi trường doanh nghiệp.

CHƯƠNG 1: TỔNG QUAN

1.1. Giới thiệu:

RADIUS (Remote Authentication Dial-In User Service) là một giao thức phổ biến và hiệu quả trong việc cung cấp các chức năng xác thực, cấp quyền và ghi log truy cập cho các hệ thống mạng. Với khả năng quản lý tập trung và bảo mật cao, RADIUS được sử dụng rộng rãi trong các tổ chức lớn, giúp quản lý quyền truy cập vào các tài nguyên mạng như Wifi, VPN, hoặc hệ thống máy chủ.

Windows Server, một hệ điều hành máy chủ toàn diện của Microsoft, cung cấp công cụ Network Policy Server (NPS) để triển khai dịch vụ RADIUS một cách đơn giản và hiệu quả. NPS tích hợp sâu với các công nghệ khác của Windows như Active Directory, giúp dễ dàng quản lý người dùng và áp dụng các chính sách bảo mật tập trung.

Triển khai RADIUS trên Windows Server không chỉ là một giải pháp mạnh mẽ trong việc bảo mật và quản lý truy cập mà còn đảm bảo khả năng mở rộng, tương thích với nhiều thiết bị và giao thức khác nhau.

1.2. Đề Tài:

Triển khai RADIUS trên Windows Server.

1.3. Mục tiêu đề tài:

Mục tiêu của đề tài là xây dựng và triển khai hệ thống RADIUS trên Windows Server để quản lý quyền truy cập của người dùng trong mạng doanh nghiệp. Trước tiên, đề tài tập trung vào việc cài đặt và cấu hình máy chủ RADIUS, tích hợp với Active Directory để quản lý người dùng theo các nhóm, chẳng hạn như nhóm ITADMIN và nhóm HR. Sau đó, hệ thống RADIUS sẽ được tích hợp với router Cisco để cung cấp dịch vụ xác thực tập trung thông qua giao thức Telnet và SSH.

Đề tài cũng đặt mục tiêu phân quyền truy cập cụ thể, chỉ cho phép nhóm ITADMIN có quyền Telnet và SSH vào router, trong khi các nhóm khác bị hạn chế. Cuối cùng, quá trình kiểm tra và đánh giá sẽ được thực hiện bằng cách sử dụng thông tin tài khoản Active Directory để xác thực người dùng trên router, đảm bảo hệ thống hoạt

động chính xác, ổn định và đáp ứng yêu cầu quản lý tập trung. Thông qua việc thực hiện các bước này, đề tài nhằm đánh giá hiệu quả của giải pháp RADIUS trong việc tăng cường bảo mật và quản lý truy cập người dùng trong thực tế.

CHƯƠNG 2: GIỚI THIỆU VỀ RADIUS, WINDOWS SERVER VÀ CÁC CÔNG NGHỆ LIÊN QUAN

2.1. Giới thiệu về RADIUS:

2.1.1. RADIUS:

RADIUS (Remote Authentication Dial-In User Service) là một giao thức mạng được sử dụng rộng rãi trong các hệ thống mạng doanh nghiệp để cung cấp các chức năng xác thực (Authentication), cấp quyền (Authorization) và ghi log (Accounting) cho người dùng khi truy cập vào các tài nguyên mạng. Giao thức này hoạt động theo mô hình client-server, trong đó máy chủ RADIUS đóng vai trò xử lý các yêu cầu xác thực từ các thiết bị mạng như router, switch hoặc access point. RADIUS không chỉ đảm bảo tính an toàn cho hệ thống mạng mà còn cung cấp giải pháp quản lý tập trung, phù hợp với các môi trường mạng quy mô lớn.

RADIUS (Remote Authentication Dial-In User Service) hỗ trợ nhiều thuật toán xác thực khác nhau nhằm đáp ứng nhu cầu bảo mật của các hệ thống mạng. Các thuật toán này bao gồm:

1. PAP (Password Authentication Protocol):

- Đây là phương pháp xác thực đơn giản, trong đó mật khẩu được gửi qua mạng dưới dạng *plaintext* (không mã hóa).
- Mặc dù dễ triển khai, PAP không an toàn vì thông tin xác thực có thể bị đánh cắp nếu mạng không được mã hóa.

2. CHAP (Challenge-Handshake Authentication Protocol):

- CHAP cải thiện bảo mật bằng cách không truyền mật khẩu trực tiếp.
- Quy trình:
 1. Máy chủ RADIUS gửi một chuỗi ngẫu nhiên (*challenge*) đến client.
 2. Client kết hợp chuỗi này với mật khẩu, tạo giá trị băm (hash) và gửi lại.

3. Máy chủ kiểm tra giá trị băm để xác minh thông tin.

- Phương pháp này bảo vệ mật khẩu khỏi bị đánh cắp, nhưng vẫn có điểm yếu trước các tấn công nhất định.

3. MS-CHAP (Microsoft CHAP):

- Là phiên bản cải tiến của CHAP, được Microsoft phát triển.
- Hỗ trợ xác thực hai chiều (mutual authentication) giữa client và máy chủ.
- Cung cấp khả năng mã hóa dữ liệu trong quá trình xác thực.

4. EAP (Extensible Authentication Protocol):

- EAP là khuôn khổ xác thực mở rộng, hỗ trợ nhiều phương thức xác thực khác nhau, bao gồm:
 - EAP-TLS: Sử dụng chứng chỉ số (digital certificates) để xác thực, mang lại mức độ bảo mật cao nhất.
 - EAP-TTLS và PEAP: Bảo vệ thông tin xác thực bằng cách sử dụng kênh mã hóa (tunnel).
- EAP thường được sử dụng trong các môi trường đòi hỏi bảo mật cao như mạng Wi-Fi doanh nghiệp (WPA2-Enterprise).

RADIUS hoạt động theo chuẩn IEEE 802.1X, một giao thức chuẩn cho xác thực dựa trên mạng. Nó được sử dụng để kiểm soát truy cập vào mạng có dây (LAN) và mạng không dây (WLAN). Cấu trúc chính của 802.1X bao gồm:

- Supplicant (Client):
 - + Là thiết bị người dùng như máy tính, điện thoại, hoặc bất kỳ thiết bị nào muốn kết nối vào mạng.
 - + Supplicant gửi thông tin xác thực (ví dụ: tên người dùng/mật khẩu, chứng chỉ số) đến Authenticator.
- Authenticator (Thiết bị mạng):
 - + Thường là switch trong mạng có dây hoặc access point trong mạng không dây.

- + Authenticator đóng vai trò trung gian, chuyển tiếp thông tin xác thực từ Supplicant đến Authentication Server.
- Authentication Server (RADIUS Server):
 - + Xử lý thông tin xác thực nhận được từ Authenticator.
 - + Dựa vào giao thức EAP (Extensible Authentication Protocol), RADIUS kiểm tra tính hợp lệ của thông tin xác thực và đưa ra quyết định cho phép hoặc từ chối kết nối.

2.1.2. Cấu trúc của RADIUS:

- **Máy chủ RADIUS:** Được cài đặt trên Windows Server, đóng vai trò là trung tâm xử lý yêu cầu xác thực và phân quyền. Máy chủ này kết nối với cơ sở dữ liệu Active Directory để quản lý người dùng và nhóm. Các thiết bị mạng như router gửi yêu cầu xác thực đến máy chủ RADIUS để kiểm tra quyền truy cập của người dùng.
- **Client (Thiết bị mạng):** Bao gồm các thiết bị như router hoặc switch, gửi yêu cầu xác thực đến máy chủ RADIUS khi người dùng cố gắng truy cập vào hệ thống mạng qua các giao thức như Telnet hoặc SSH. Thiết bị này thực hiện yêu cầu xác thực dựa trên các thông tin người dùng mà máy chủ RADIUS cung cấp.
- **Cơ sở dữ liệu người dùng (Active Directory):** Lưu trữ thông tin về người dùng và các nhóm người dùng như "ITADMIN" và "HR". Các nhóm này sẽ có quyền truy cập khác nhau, và Active Directory giúp quản lý quyền hạn của từng nhóm người dùng.
- **Mạng và kết nối:** Mạng nội bộ (LAN) được cấu hình với các dải IP dành cho các thiết bị và máy chủ, giúp kết nối giữa các thành phần trong hệ thống. Các thiết bị mạng sẽ giao tiếp qua mạng này để thực hiện xác thực và kiểm tra quyền truy cập.

2.1.3. Một số dịch vụ chính trong RADIUS:

- Xác thực người dùng:

RADIUS cung cấp dịch vụ xác thực người dùng khi họ cố gắng truy cập vào các tài nguyên mạng, như Wifi, VPN, hoặc các thiết bị mạng (router, switch). Máy chủ RADIUS kiểm tra thông tin người dùng từ cơ sở dữ liệu (thường là Active Directory) để xác định xem người dùng có quyền truy cập hay không.

- **Cấp quyền truy cập:**

Sau khi xác thực, RADIUS giúp cấp quyền truy cập cho người dùng dựa trên chính sách đã được cấu hình. Điều này có thể bao gồm việc cấp quyền sử dụng dịch vụ như Telnet, SSH hoặc Wi-Fi, hoặc hạn chế quyền truy cập vào các tài nguyên nhất định tùy thuộc vào nhóm người dùng.

- **Ghi log và giám sát:**

RADIUS cung cấp dịch vụ ghi nhận các hoạt động của người dùng (Accounting), bao gồm thông tin về thời gian kết nối, tài nguyên sử dụng, và các thay đổi trạng thái của phiên làm việc. Dữ liệu này hữu ích cho việc giám sát, phân tích và phát hiện các hoạt động đáng ngờ trong hệ thống mạng.

2.1.4. Ưu điểm và nhược điểm khi triển khai RADIUS:

- **Ưu điểm:**

- **Quản lý tập trung:** RADIUS giúp quản lý tất cả người dùng và quyền truy cập vào các thiết bị mạng từ một điểm trung tâm, giúp giảm thiểu việc cấu hình từng thiết bị mạng riêng lẻ.
- **Bảo mật cao:** RADIUS hỗ trợ các giao thức bảo mật mạnh mẽ như PAP, CHAP và MS-CHAP, giúp bảo vệ thông tin người dùng khi xác thực.
- **Mở rộng dễ dàng:** Hệ thống RADIUS có thể mở rộng linh hoạt để hỗ trợ số lượng người dùng lớn trong các môi trường mạng quy mô lớn.
- **Ghi log và giám sát:** Cung cấp khả năng ghi log đầy đủ về các hoạt động của người dùng, giúp quản trị viên giám sát và phát hiện các hành vi bất thường.

- **Nhược điểm:**

- Yêu cầu kiến thức chuyên môn: Việc triển khai và cấu hình hệ thống RADIUS đòi hỏi kiến thức kỹ thuật về mạng và bảo mật, có thể gặp khó khăn với những người quản trị không quen thuộc.
- Phụ thuộc vào máy chủ RADIUS: Nếu máy chủ RADIUS gặp sự cố, toàn bộ hệ thống xác thực sẽ bị gián đoạn, ảnh hưởng đến khả năng truy cập vào các tài nguyên mạng.
- Khó khăn trong việc khôi phục: Trong trường hợp hệ thống bị tấn công hoặc gặp sự cố nghiêm trọng, việc khôi phục và đảm bảo dữ liệu người dùng có thể tốn thời gian và công sức.

2.1.5. Biện pháp dự phòng khi RADIUS không còn hoạt động:

Nếu hệ thống RADIUS bị sập, các thiết bị và người dùng sẽ không thể thực hiện xác thực thông qua máy chủ RADIUS. Để đối phó với tình huống này, ta có thể triển khai các giải pháp dự phòng như sau:

- **Cấu hình xác thực dự phòng (Fallback Authentication):** Hầu hết các thiết bị mạng như Router Cisco hỗ trợ xác thực dự phòng. Nếu máy chủ RADIUS không phản hồi, thiết bị sẽ chuyển sang phương thức xác thực khác, chẳng hạn như:
 - Xác thực cục bộ (Local Authentication): Sử dụng danh sách tài khoản và mật khẩu được cấu hình trực tiếp trên thiết bị (router, switch).
 - Xác thực qua một máy chủ RADIUS khác: Triển khai một máy chủ RADIUS dự phòng và cấu hình trên thiết bị để chuyển đổi khi máy chủ chính gặp sự cố.
- **Triển khai cơ chế High Availability (HA):**
 - Cluster RADIUS Servers: Xây dựng một cụm máy chủ RADIUS hoạt động song song để đảm bảo rằng khi một máy chủ gặp sự cố, máy chủ khác sẽ tiếp quản.
 - Load Balancer: Dùng load balancer để phân phối yêu cầu xác thực

giữa các máy chủ RADIUS, đảm bảo tính sẵn sàng cao.

- **Sử dụng xác thực cục bộ:** Trong trường hợp khẩn cấp khi không có RADIUS dự phòng, quản trị viên có thể kích hoạt các tài khoản cục bộ trên router để cấp quyền truy cập bằng câu lệnh: `username admin privilege 15 secret strongpassword`
- **Cải thiện khả năng giám sát và bảo trì của hệ thống:**
 - Giám sát máy chủ RADIUS: Sử dụng các công cụ giám sát (như Zabbix, Nagios) để kiểm tra tình trạng hoạt động của máy chủ RADIUS, giúp phát hiện và khắc phục sự cố sớm.
 - Backup và Restore: Đảm bảo máy chủ RADIUS và Active Directory có bản sao lưu thường xuyên để khôi phục nhanh khi cần.

2.2. Giới thiệu về Windows Server và Network Policy Server (NPS):

2.2.1. Windows Server:

Windows Server là hệ điều hành máy chủ được phát triển bởi Microsoft, phục vụ các nhu cầu quản lý và cung cấp dịch vụ mạng trong các môi trường doanh nghiệp. Đây là nền tảng mạnh mẽ cho các ứng dụng, dịch vụ và hệ thống quản lý người dùng, bao gồm các công cụ như Active Directory, DNS, DHCP, và các dịch vụ mạng khác. Windows Server giúp các tổ chức triển khai các ứng dụng, bảo mật và quản lý tài nguyên mạng một cách hiệu quả.

2.2.2. Network Policy Server (NPS):

Network Policy Server (NPS) là một dịch vụ trong Windows Server cho phép quản trị viên triển khai và quản lý các chính sách mạng, bao gồm xác thực, cấp quyền và ghi log cho người dùng và thiết bị kết nối vào hệ thống. NPS có thể hoạt động như một máy chủ RADIUS, hỗ trợ xác thực người dùng thông qua các giao thức cho Wifi hoặc VPN.

NPS giúp quản trị viên kiểm soát và giám sát việc truy cập mạng của người dùng thông qua các chính sách mạng được thiết lập, từ đó cải thiện tính bảo mật và giảm thiểu các rủi ro. Bằng cách tích hợp với Active Directory, NPS có thể xác thực

người dùng dựa trên các tài khoản và nhóm trong AD, tạo ra một hệ thống xác thực và phân quyền truy cập tập trung.

2.2.3. Các chức năng chính của NPS:

- Xác thực người dùng và thiết bị: NPS hỗ trợ xác thực người dùng và thiết bị kết nối vào mạng thông qua giao thức RADIUS, giúp kiểm soát truy cập.
- Quản lý chính sách mạng: NPS cho phép thiết lập và áp dụng các chính sách mạng cho phép hoặc từ chối quyền truy cập dựa trên các điều kiện như địa chỉ IP, loại kết nối, hoặc nhóm người dùng.
- Ghi log và giám sát: NPS ghi lại các sự kiện xác thực và ghi log hoạt động của người dùng, cung cấp thông tin cho việc giám sát và phân tích bảo mật.
- Tích hợp với Active Directory: NPS có thể tích hợp trực tiếp với Active Directory để xác thực và phân quyền người dùng, giúp quản lý truy cập mạng hiệu quả hơn.

2.3. Giới thiệu về Active Directory:

2.3.1. Active Directory:

Active Directory (AD) là một dịch vụ quản lý và tổ chức tài nguyên mạng trong môi trường Windows Server. Nó cung cấp một cơ sở dữ liệu phân tán, phân cấp để lưu trữ thông tin về các đối tượng như tệp, người dùng, nhóm, thiết bị ngoại vi và thiết bị mạng trong một hệ thống. AD cung cấp các công cụ và dịch vụ để quản lý, xác thực, và phân phối kiểm soát truy cập cho các tài nguyên này.

2.3.2. Cấu trúc của Active Directory:

- Domain: Là khu vực mạng quản lý các đối tượng, như người dùng và máy tính, cho phép dễ dàng quản lý và kiểm soát quyền truy cập. Mỗi domain có một cơ sở dữ liệu riêng biệt để lưu trữ thông tin.
- Domain Controller: Là máy chủ chạy dịch vụ Active Directory và lưu trữ cơ sở dữ liệu của domain. Nó cũng xử lý các yêu cầu xác thực và phân quyền từ người dùng.
- Organizational Units (OUs): Là các nhóm con trong domain, giúp tổ chức các đối tượng theo cách dễ quản lý. OUs có thể chứa người dùng, nhóm hoặc

máy tính, và cho phép phân quyền cụ thể cho từng nhóm.

- Global Catalog: Cung cấp thông tin về tất cả các đối tượng trong toàn bộ forest của AD, giúp cải thiện hiệu quả tìm kiếm và xác thực.

2.3.3. Các chức năng chính của AD:

- Xác thực người dùng: AD quản lý quá trình xác thực khi người dùng đăng nhập vào hệ thống, đảm bảo rằng chỉ người dùng hợp lệ mới có thể truy cập vào tài nguyên mạng.
- Phân quyền truy cập: AD cho phép quản lý quyền truy cập vào tài nguyên, như thư mục, file, và ứng dụng, dựa trên các nhóm và chính sách đã định.
- Quản lý chính sách bảo mật: AD hỗ trợ thiết lập và thi hành các chính sách bảo mật cho toàn bộ mạng, bao gồm mật khẩu, kiểm soát truy cập, và các yêu cầu bảo mật khác.
- Tích hợp với RADIUS: AD có thể được tích hợp với hệ thống RADIUS để xác thực người dùng khi họ truy cập vào các thiết bị mạng hoặc dịch vụ từ xa, cung cấp giải pháp quản lý truy cập tập trung.

CHƯƠNG 3: TRIỂN KHAI HỆ THỐNG

Mô hình hệ thống gồm 5 máy: 1 máy triển khai RADIUS Server và 4 máy còn lại đóng vai trò Client

Thông tin các máy:

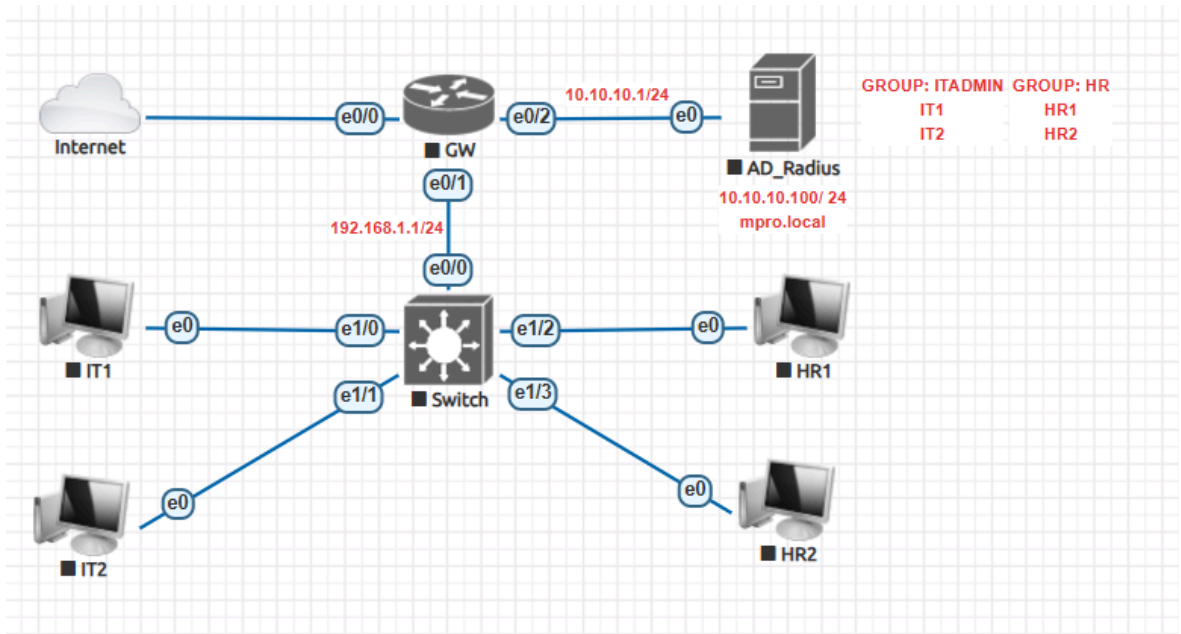
Tên	Hệ điều hành	Cấu hình máy	Tài khoản
AD_RADIUS	Windows Server 2012	2 core, RAM 8GB, 60GB	user: Administrator pass: QTM@Nhom12
IT1	Windows 7	1 core, RAM 4GB, 10GB	User: Administrator pass: QTM@Nhom12
IT2	Windows 7	1 core, RAM 4GB, 10GB	user: Administrator pass: QTM@Nhom12
HR1	Windows 7	1 core, RAM 4GB, 10GB	user: Administrator pass: QTM@Nhom12
HR2	Windows 7	1 core, RAM 4GB, 10GB	user: Administrator pass: QTM@Nhom12

Với: Windows 7 Professional

Thông tin địa chỉ IP của các máy:

Tên	Địa chỉ IP	Subnet mask	Gateway	DNS Server
AD_RADIUS	10.10.10.100	255.255.252.0	10.10.10.1	8.8.8.8, 10.10.10.100
IT1	192.168.1.2	255.255.252.0	192.168.1.1	192.168.1.1
IT2	192.168.1.3	255.255.252.0	192.168.1.1	192.168.1.1
HR1	192.168.1.5	255.255.252.0	192.168.1.1	192.168.1.1
HR2	192.168.1.4	255.255.252.0	192.168.1.1	192.168.1.1

Mô hình hệ thống mạng:

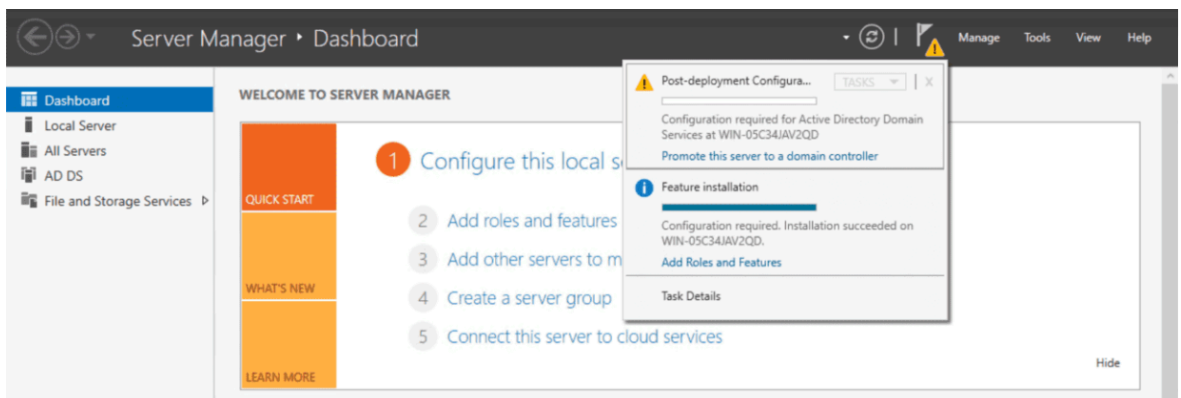


(Hình 1: Mô hình hệ thống mạng)

3.1. Triển khai Active Directory:

* Bước 1: Cài đặt Active Directory Domain Service trên máy AD_RADIUS:

- Vào Server Manager > Manage > Add Roles and Features.
- Chọn Next tại các bước Before You Begin, Installation Type, Server Selection.
- Tại bước Server Roles, chọn Active Directory Domain Services.
- Ở bước Features, chọn Group Policy Management.
- Ở bước AD DS, chọn Next.
- Ở bước Confirmation, xác nhận lại thông tin và chọn Install.
- Chờ quá trình cài đặt hoàn thành và chọn Close để kết thúc.



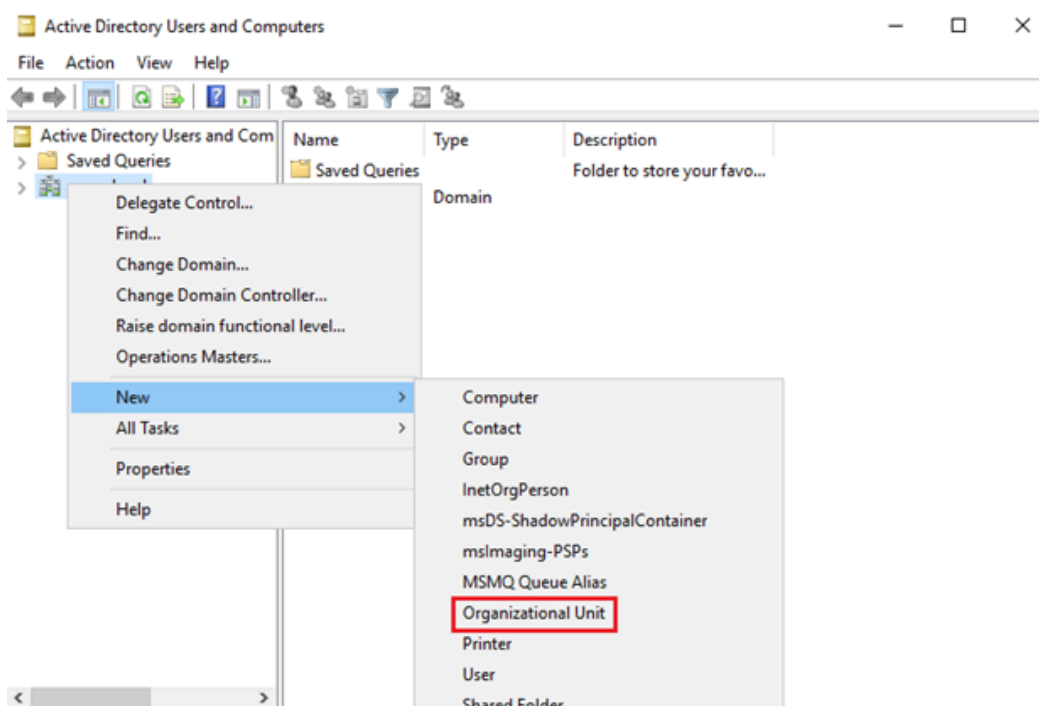
(Hình 2. Quá trình cài đặt hoàn tất)

* Bước 2: Nâng cấp máy chủ Active Directory lên Domain Controller

- Vào Server Manager sẽ thấy biểu tượng cảnh báo, nhấn vào và chọn Promote this server to a domain controller (Hình 2).
- Chọn Add new forest và gõ domain mpro.local vào mục Root domain.
- Tiếp theo, thiết lập DSRM password và các thiết lập khác.
- Thiết lập NetBIOS domain name: MPRO.
- Giữ nguyên các tùy chỉnh mặc định ở mục Paths
- Thực hiện bước Prerequisites Check hoàn thành, sau đó chọn Install và chờ quá trình nâng cấp hoàn tất.
- Sau khi hoàn tất quá trình này, máy chủ Active Directory sẽ khởi động lại và hoàn tất quá trình nâng cấp thành Domain Controller.

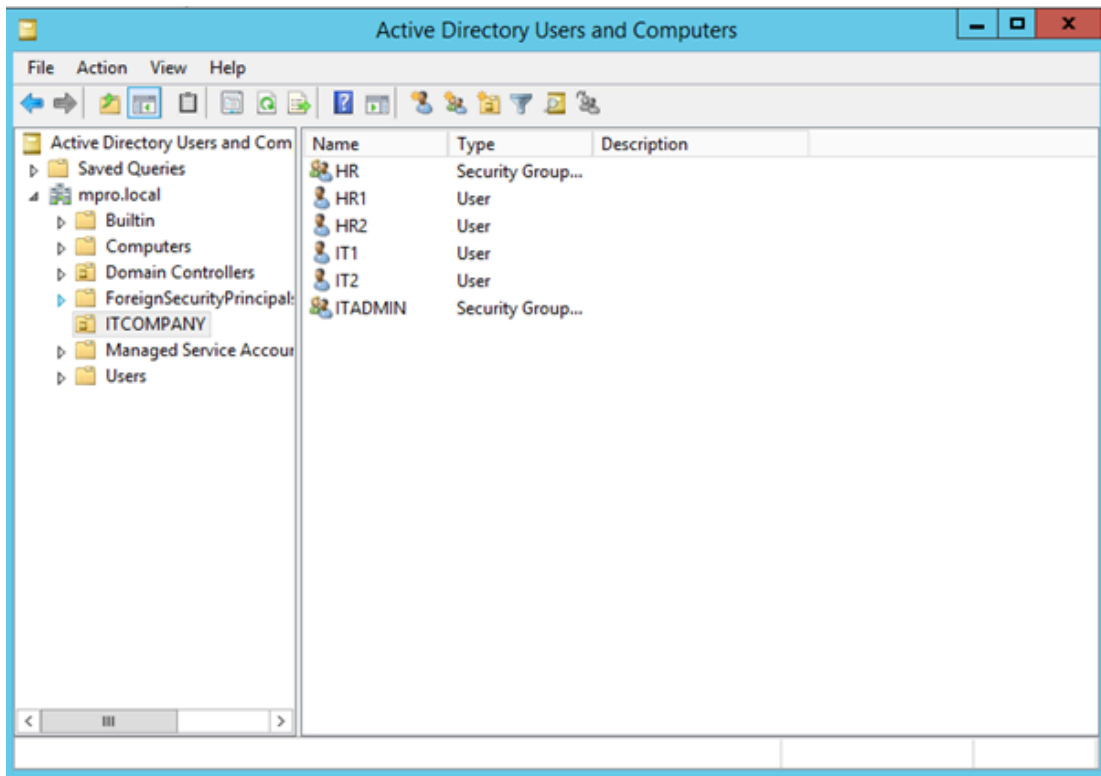
* Bước 3: Tạo một Organizational Unit trong Domain

- Đăng nhập vào máy chủ (AD_RADIUS) với tài khoản Administrator
- Vào Server Manager → Tools → Active Directory Users and Computers
- Nhấp chuột phải vào domain mpro.local → New → Organizational Unit, đặt tên cho Organizational Unit mới tạo là ITCOMPANY



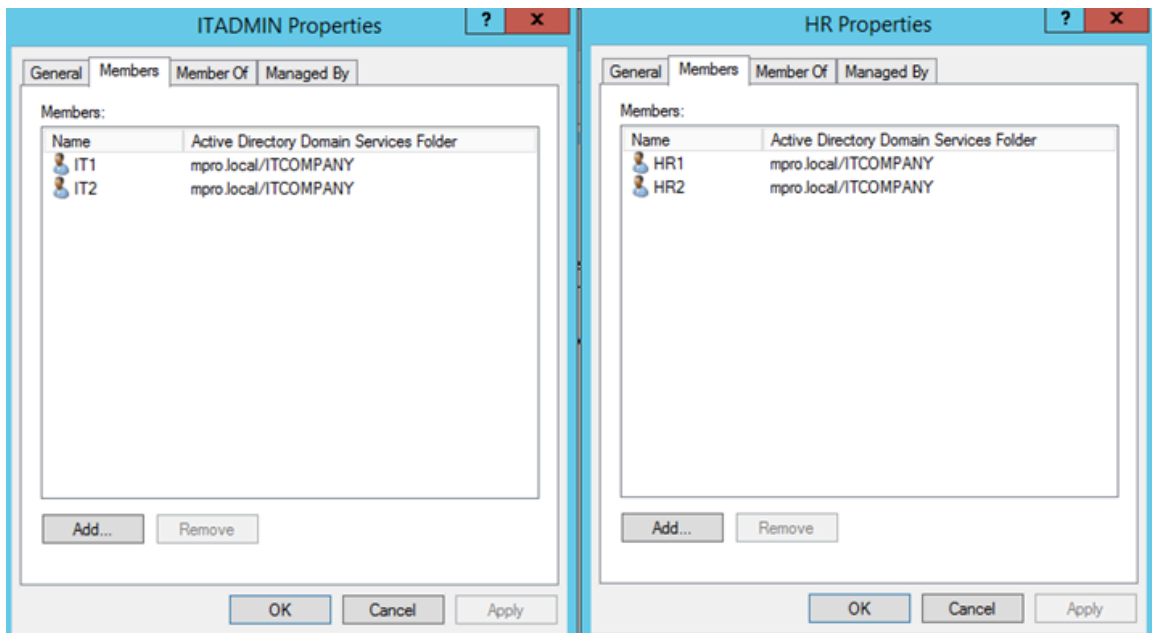
(Hình 3. Tạo Organizational Unit mới trong Domain)

- Tại đây, nhóm tiến hành tạo 2 group mới là ITADMIN và HR, và 4 user IT1, IT2, HR1 và HR2 trong ITCOMPANY



(Hình 4. Tạo User và các Group cần thiết)

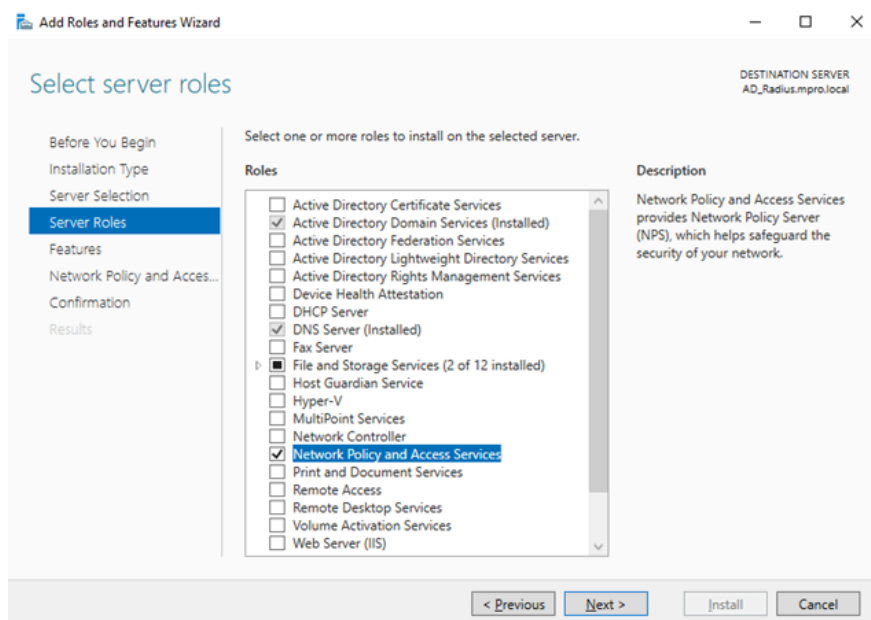
- Sau đó thực hiện thêm các User vào Group tương ứng



(Hình 5. Kiểm tra các thành viên của Group)

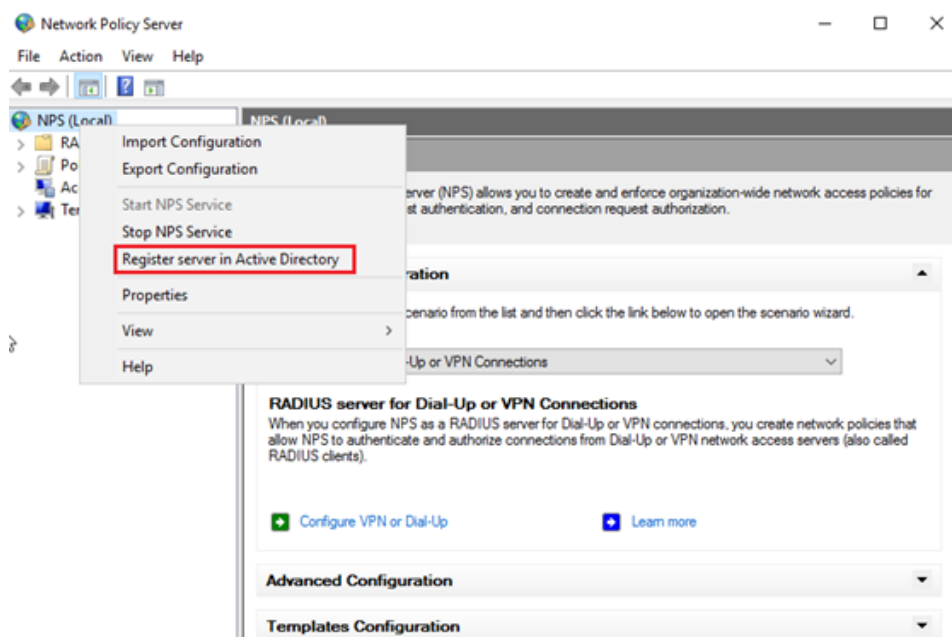
3.2. Triển khai Network Policy and Access Server và DNS Server:

- Thực hiện tương tự cài đặt ở mục 1, thay vào đó ở mục Server Role ta chọn vào “Network Policy and Access Server” và “DNS Server”.



(Hình 6: Triển khai Network Policy and Access Server và DNS Server)

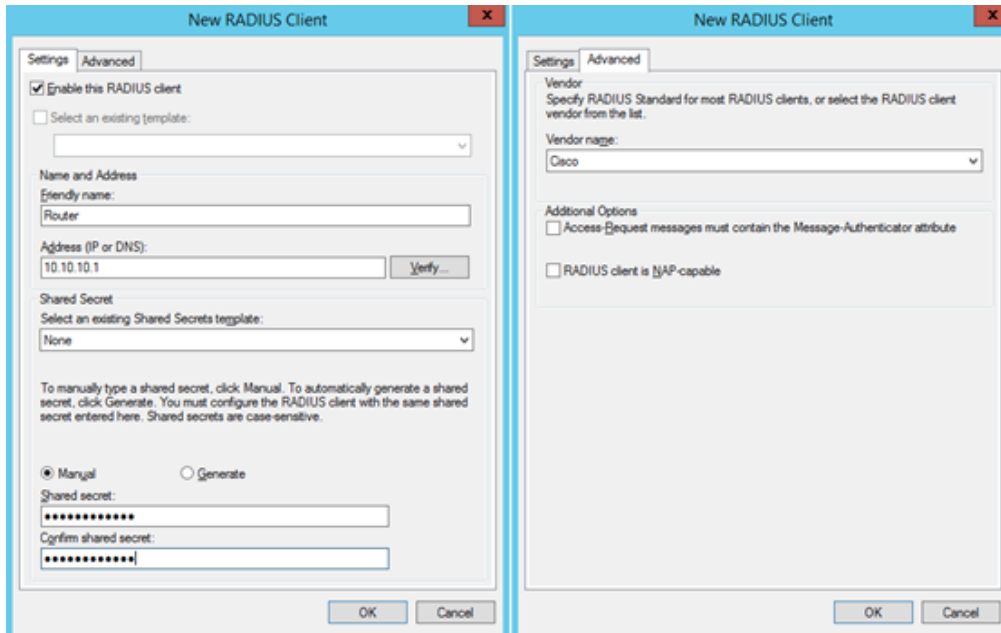
- Sau khi hoàn tất việc cài đặt, vào Server Manager → Tools → Network Policy Server.
- Chuột phải vào NPS (local) → Register server in Active Directory.



(Hình 7. Thực hiện đăng ký server trong AD)

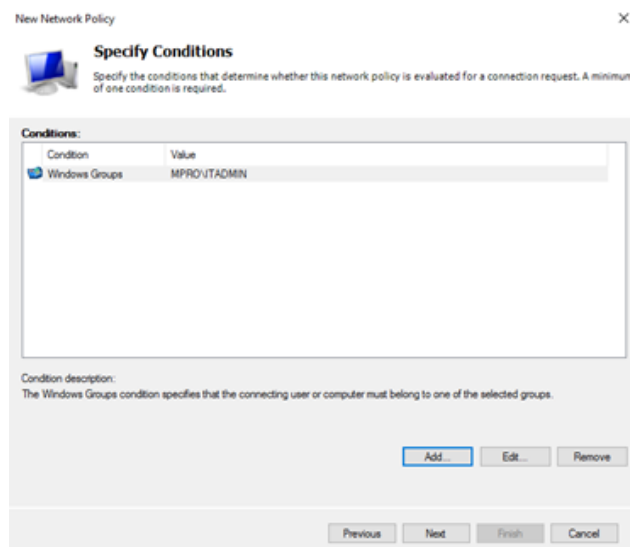
3.3. Thiết lập RADIUS và thực hiện phân quyền truy cập

- Ở mục RADIUS Clients and Servers → RADIUS Clients → New. Điền các thông tin như sau cho RADIUS Client mới.



(Hình 8: Thông tin của RADIUS Client)

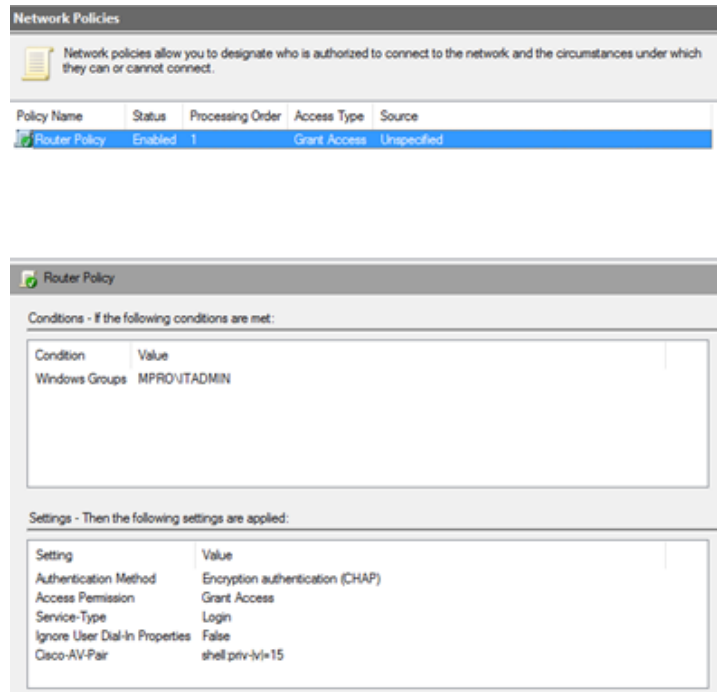
- Ở mục Network Policies, thực hiện xóa hết những chính sách có sẵn
- Sau đó thực hiện tạo chính sách, ta chuột phải vào Network Policies → New → Điền tên chính sách vào ô Policy name → Next.
- + Thêm Group ITADMIN vào Windows Group → Next.



(Hình 9: Thêm group ITADMIN vào Windows Groups)

- + Tích chọn vào ô Access granted, mục đích để chỉ những user trong group ITADMIN mới có thể truy cập được.
- + Tiếp tục cài đặt với những tùy chỉnh mong muốn: Ở đây nhóm sẽ tạo 1 chính sách chỉ những user thuộc group ITADMIN mới có thể truy cập vào Router (Cisco) thông qua Telnet và SSH với quyền cao nhất là truy cập được tất cả câu lệnh (privilege level 15) tại mục “Cisco-AV-Pair”. Bên cạnh đó ta cũng có thể tùy chỉnh privilege level tùy theo mục đích, với:
 - + Level 0 (Lowest): Chỉ được cấp quyền tối thiểu để giám sát với các lệnh như: logout, enable, disable, exit và help.
 - + Level 1 (User EXEC mode): Chỉ có quyền đọc, và truy cập vào các câu lệnh giới hạn để xem thông tin hệ thống như: ping, traceroute, telnet, show interface, show ip interface brief, ...
 - + Level 2-14 (Custom Privilege Level): Các quyền và lệnh truy cập được tùy chỉnh bởi quản trị viên. Ví dụ: một quản trị viên có thể cấp quyền cho từng mức level với các đặc quyền như sau, và có thể tùy chỉnh lại dựa trên mục đích của quản trị viên:
 - + Level 2: Basic Troubleshooting với các lệnh như show ip interface brief, ping, traceroute, show ip route, ...
 - + Level 3: Advanced Troubleshooting với các câu lệnh như debug ip packet, debug interface, show running-config, show startup-config, show ip protocols, ...
 - + Level 4: Interface Management với các câu lệnh như shutdown, no shutdown, description, ip address, interface [type][number], ...
 - + Level 5: Routing với các câu lệnh như router ospf [process id], network [network-address], passive-interface, ...
 - + Level 6: Access Control Lists (ACLs) Management với các câu lệnh như access-list, ip access-group, no access-list [number], ...

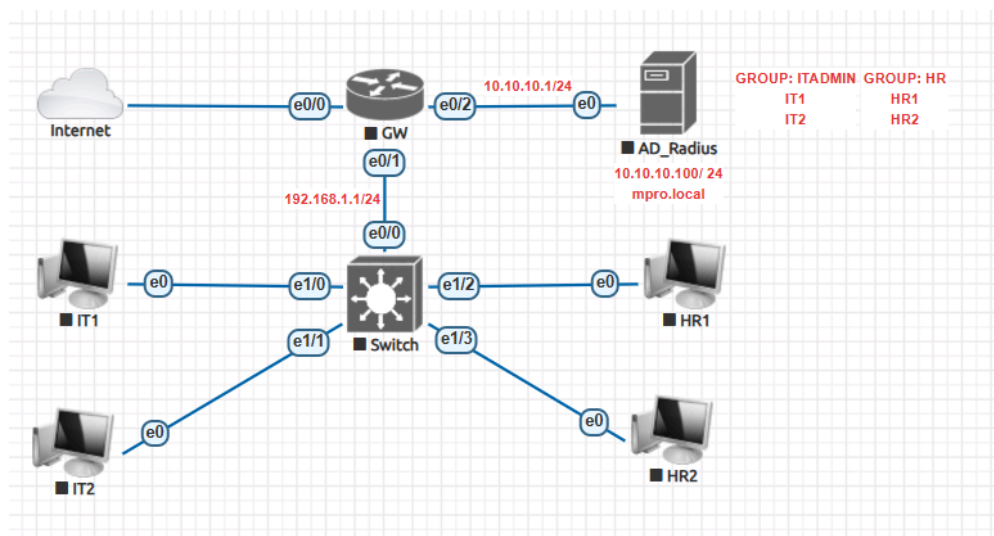
- + Level 7: VLAN Management với các câu lệnh như `vlan database`, `vlan [vlan-id]`, `name [vlan-name]`, `no vlan [vlan-id]`,...
- + Level 8: Security Configuration với các câu lệnh như `enable secret [password]`, `aaa authentication`, `crypto key generation rsa`, ...
- + Level 9: Monitoring and Logging với các câu lệnh như: `logging [host]`, `show logging`, `show processes`, `show users`, ...
- + Level 10: NAT and Firewall Configuration với các câu lệnh như `ip nat inside`, `ip nat outside`, ...
- + Level 11: Advanced NAT and Firewall Configuration với các câu lệnh như `ip nat pool`, `ip nat inside source`, `ip firewall`, ...
- + Level 12: Quality of Service (QoS) Configuration với các câu lệnh như `mls qos`, `policy-map [name]`, `class-map [name]`, `service-policy [name]`, ...
- + Level 13: System Maintenance với các câu lệnh như `clock set [hh:mm:ss]`, `ntp server [ip-address]`, `system clock`, `server timestamps`
- + Level 14: Backup and Restore Configuration với các câu lệnh như `copy running-config startup-config`, `copy running-config tftp`, `copy startup-config tftp`, `reload`, ...
- + Level 15 (Highest - Privileged EXEC mode): Toàn quyền truy cập vào tất cả các lệnh của bộ định tuyến bao gồm cả cấu hình router.



(Hình 10: Tổng quan chính sách)

3.4. Cấu hình Router (GW) trong hệ thống mạng:

- Thực hiện cấu hình ip cho các interface của GW tương ứng với hệ thống mạng



- Ở interface e0/1 của GW, ta tạo một DHCP pool có tên “LAN”, pool này sẽ cấp phát địa chỉ IP từ mạng 192.168.1.0/24 cho các thiết bị trong mạng LAN của GW. Các thiết bị này có gateway mặc định là 192.168.1.1 và sử dụng máy chủ DNS 8.8.8.8 để phân giải tên miền

```

GW(config)#int e0/1
GW(config-if)#ip add 192.168.1.1 255.255.255.0
GW(config-if)#no sh
GW(config-if)#
*Nov 24 10:55:38.779: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
*Nov 24 10:55:39.780: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to up
GW(config-if)#ip dhcp pool LAN
GW(dhcp-config)#network 192.168.1.0 255.255.255.0
GW(dhcp-config)#default-router 192.168.1.1
GW(dhcp-config)#dns-server 8.8.8.8
GW(dhcp-config)#exit

```

(Hình 11: Cấu hình DHCP pool cho GW)

- Ta cấu hình GW sử dụng máy chủ RADIUS tại IP 10.10.10.100/24 để xác thực người dùng truy cập vào thiết bị và ghi nhận logs của tài khoản.

```

GW(config)#aaa new-model
GW(config)#radius server mpro.local
GW(config-radius-server)#$4 10.10.10.100 auth-port 1812 acct-port 1813
GW(config-radius-server)#key Sysadmin@123
GW(config-radius-server)#exit

```

(Hình 12: Cấu hình RADIUS server trên GW)

- Thiết lập mọi kết nối từ xa qua Telnet và SSH sẽ được thông qua máy chủ RADIUS và yêu cầu người dùng nhập user/ password để có thể truy cập chế độ cấu hình của GW

```

GW(config)#aaa authentication login AD-AUTH group radius local
GW(config)#line vty 0 4
GW(config-line)#transport input telnet ssh
GW(config-line)#login authentication AD-AUTH
GW(config-line)#exit
GW(config)#enable password Sysadmin@123

```

(Hình 13: Thiết lập kết nối từ xa cho GW)

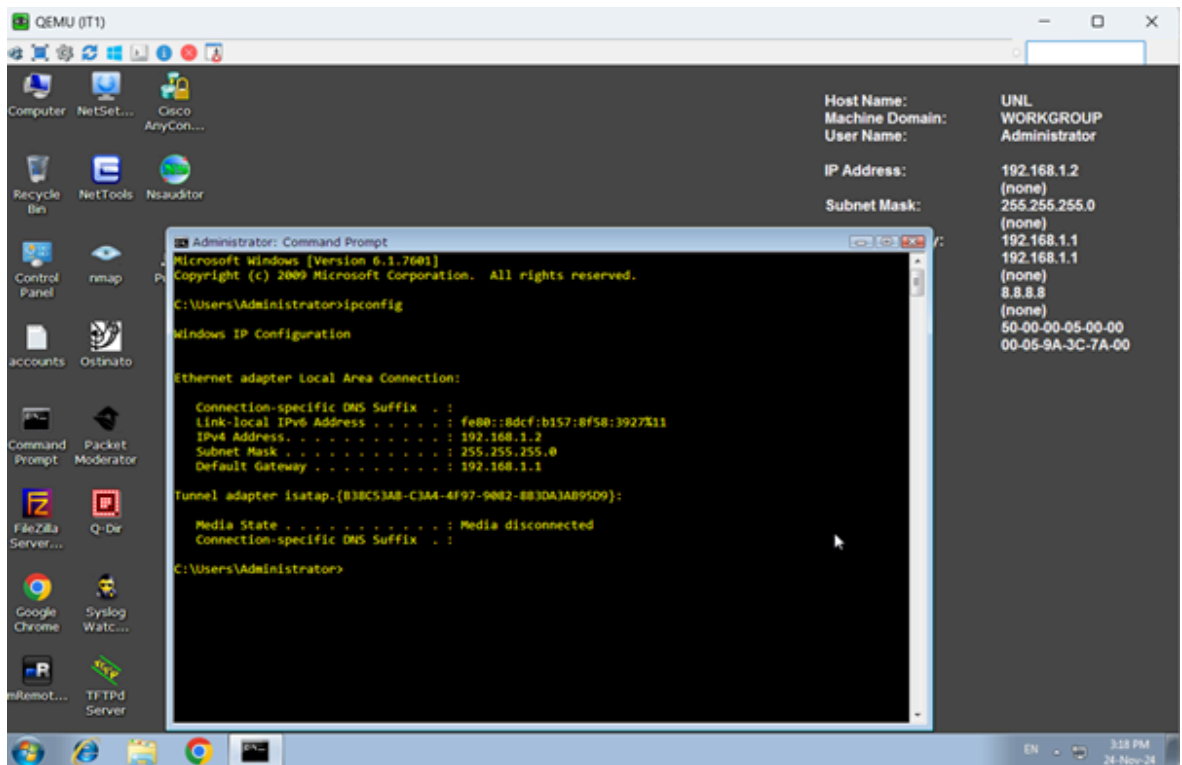
3.5. Cài đặt phần mềm cho các Client

- Trên các máy Client, ta cài đặt thêm PuTTY để có thể thực hiện Telnet đến GW

CHƯƠNG 4: ĐÁNH GIÁ THỬ NGHIỆM

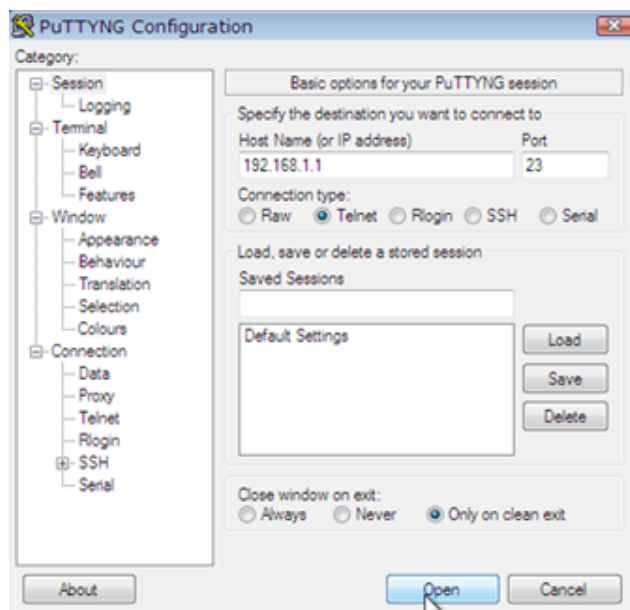
4.1. Thử nghiệm cho Client kết nối với Router (GW)

- Kiểm tra địa chỉ IP của máy IT1: máy có IP là 192.168.1.2 → phù hợp với cấu hình trước đó



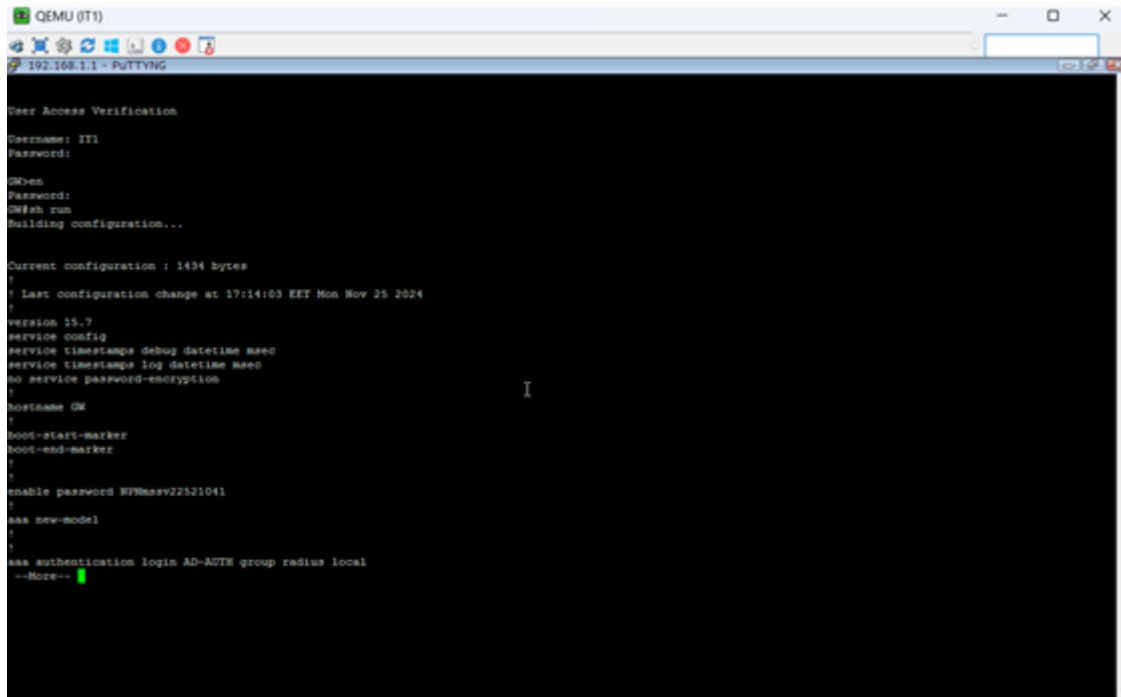
(Hình 14: Địa chỉ IP của máy IT1)

- Trên máy IT1, sử dụng PuTTY để thực hiện Telnet đến GW



(Hình 15: Thực hiện Telnet đến GW)

- Khi terminal hiện ra, thực hiện đăng nhập với tài khoản của user IT1 đã tạo trong AD trước thuộc Group ITADMIN (username: IT1, password: QTM@8), kết quả ta vào được giao diện cấu hình của GW → Thành công.



```
QEMU (IT1)
192.168.1.1 - PUTTYNG

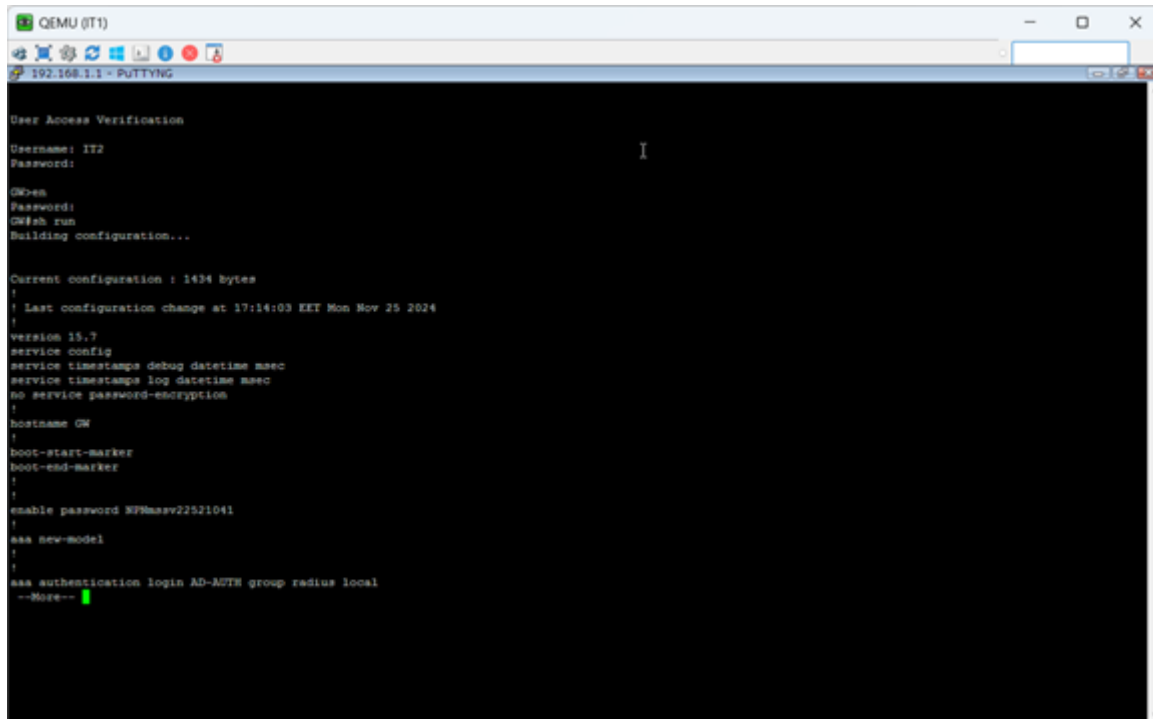
Dear Access Verification
Username: IT1
Password:

QWden
Password:
QWish run
Building configuration...

Current configuration : 1434 bytes
!
! Last configuration change at 17:14:03 EET Mon Nov 25 2024
!
version 15.7
service config
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname GW
!
boot-start-marker
boot-end-marker
!
!
enable password $FW$asv22521041
!
aaa new-model
!
!
aaa authentication login AD-AUTH group radius local
--More--
```

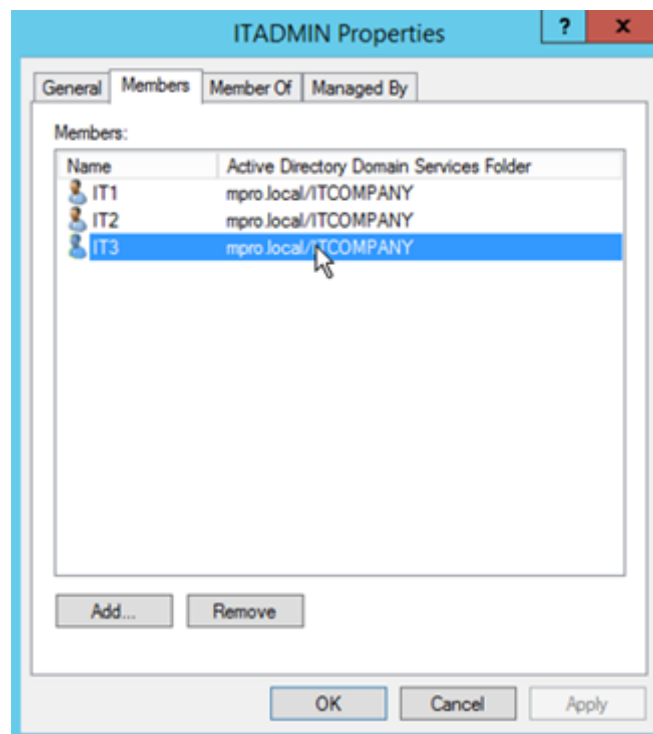
(Hình 16: Kết quả của user IT1 khi Telnet đến GW)

- Thử lại với tài khoản của user IT2, kết quả ta cũng vào được giao diện cấu hình của GW → Thành công.

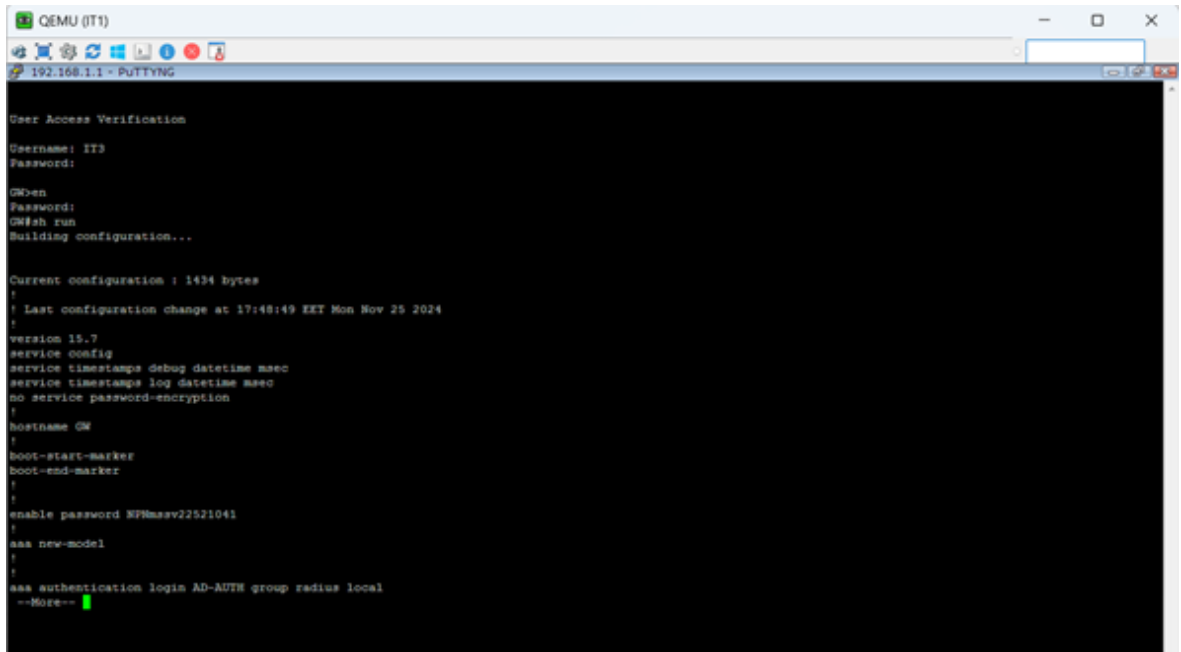


(Hình 17: Kết quả của user IT2 khi Telnet đến GW)

- Thử tạo một user IT3 khác trong group ITADMIN, sau đó thực hiện tương tự như hai user trên. Nhận thấy ta cũng vào được giao diện cấu hình của GW

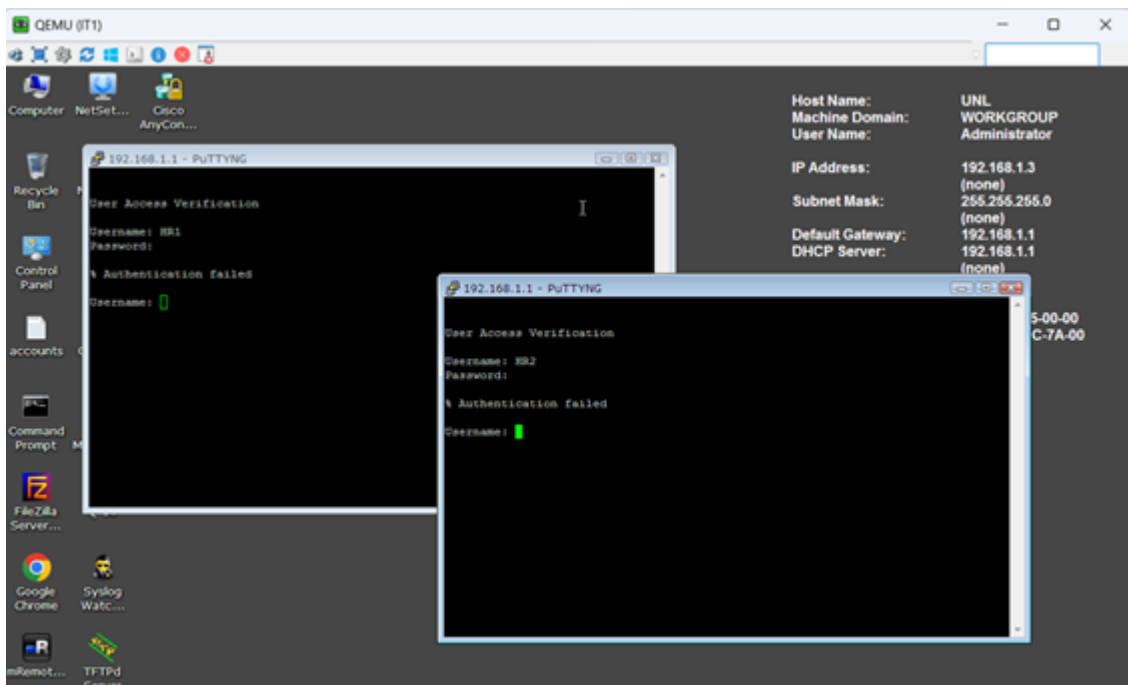


(Hình 18: Thêm user IT3 vào group ITADMIN)



(Hình 19: Kết quả của user IT3 khi Telnet đến GW)

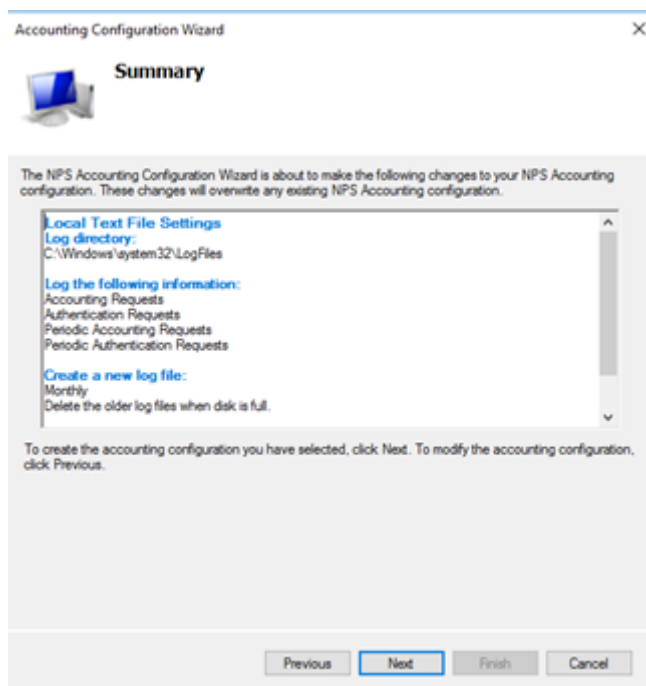
- Thử với tài khoản của user HR1 và HR2 → không truy cập được → chính sách hoạt động đúng với mong muốn. Do HR1 và HR2 không thuộc group ITADMIN nên không thể truy cập vào GW được.



(Hình 20: Kết quả của HR1 và HR2 khi Telnet đến GW)

4.2. Thử nghiệm theo dõi và ghi lại hoạt động người dùng

- Thực hiện triển khai Accounting trên máy AD_RADIUS: Mở Server Manager → Tools → Network Policy Server → Accounting → Configure Accounting → Chọn vào ô Log to a text file on the local computer → Next (3 lần). Mục đích để ghi nhận yêu cầu xác thực và cấp quyền đồng thời quản lý logs theo chu kì.



(Hình 21: Triển khai Accounting trên AD_RADIUS)

- Sau đó, truy cập theo đường dẫn C:\Windows\system32\LogFiles để xem nhật ký hoạt động của người dùng.


```
"NS1","IAS",11/24/2024,16:02:30,1,"IT1","MPRO\IT1",,,,,,"10.10.10.1",2,9,"10.10.10.1","Router",,,,,,1,16,"
"NS1","IAS",11/24/2024,16:14:59,3,,,"MPRO\IT2",,,,,,9,"10.10.10.1","Router",,,,,,1,,16,"
"NS1","IAS",11/25/2024,15:42:34,1,"IT1","mpro.local/ITCOMPANY/IT1",,,,,,"10.10.10.1",2,9,"
"NS1","IAS",11/25/2024,15:42:34,2,,,"mpro.local/ITCOMPANY/IT1",,,,,,9,"10.10.10.1","Router
"NS1","IAS",11/25/2024,15:45:37,1,"IT2","mpro.local/ITCOMPANY/IT2",,,,,,"10.10.10.1",3,9,"
"NS1","IAS",11/25/2024,15:45:37,2,,,"mpro.local/ITCOMPANY/IT2",,,,,,9,"10.10.10.1","Router
"NS1","IAS",11/25/2024,15:49:43,1,"IT3","mpro.local/ITCOMPANY/IT3",,,,,,"10.10.10.1",3,9,"
"NS1","IAS",11/25/2024,15:49:43,2,,,"mpro.local/ITCOMPANY/IT3",,,,,,9,"10.10.10.1","Router
"NS1","IAS",11/25/2024,15:50:36,1,"HR1","MPRO\HR1",,,,,,"10.10.10.1",2,9,"10.10.10.1","Rou
"NS1","IAS",11/25/2024,15:50:36,3,,,"MPRO\HR1",,,,,,9,"10.10.10.1","Router",,,,,,1,,48,"
"NS1","IAS",11/25/2024,15:51:01,1,"HR2","MPRO\HR2",,,,,,"10.10.10.1",3,9,"10.10.10.1","Rou
"NS1","IAS",11/25/2024,15:51:01,3,,,"MPRO\HR2",,,,,,9,"10.10.10.1","Router",,,,,,1,,48,"
"NS1","IAS",11/27/2024,13:04:42,1,"IT1","mpro.local/ITCOMPANY/IT1",,,,,,"10.10.10.1",2,9,"
"NS1","IAS",11/27/2024,13:04:42,2,,,"mpro.local/ITCOMPANY/IT1",,,,,,9,"10.10.10.1","Router
"NS1","IAS",11/27/2024,13:08:17,1,"IT1","mpro.local/ITCOMPANY/IT1",,,,,,"10.10.10.1",2,9,"
"NS1","IAS",11/27/2024,13:08:17,2,,,"mpro.local/ITCOMPANY/IT1",,,,,,9,"10.10.10.1","Router
"NS1","IAS",11/27/2024,13:08:43,1,"IT2","mpro.local/ITCOMPANY/IT2",,,,,,"10.10.10.1",3,9,"
"NS1","IAS",11/27/2024,13:08:43,2,,,"mpro.local/ITCOMPANY/IT2",,,,,,9,"10.10.10.1","Router
"NS1","IAS",11/27/2024,13:08:59,1,"HR1","MPRO\HR1",,,,,,"10.10.10.1",4,9,"10.10.10.1","Rou
"NS1","IAS",11/27/2024,13:08:59,3,,,"MPRO\HR1",,,,,,9,"10.10.10.1","Router",,,,,,1,,48,"
"NS1","IAS",11/27/2024,13:09:16,1,"HR3","MPRO\HR3",,,,,,"10.10.10.1",5,9,"10.10.10.1","Rou
"NS1","IAS",11/27/2024,13:09:16,3,,,"MPRO\HR3",,,,,,9,"10.10.10.1","Router",,,,,,1,,16,"
"NS1","IAS",11/27/2024,13:10:20,1,"IT4","mpro.local/ITCOMPANY/IT4",,,,,,"10.10.10.1",4,9,"
"NS1","IAS",11/27/2024,13:10:20,2,,,"mpro.local/ITCOMPANY/IT4",,,,,,9,"10.10.10.1","Router
```

(Hình 22: Logs ghi nhận được trên AD_RADIUS (NSI))

- Từ Hình 22, Ta có thể thấy được thông tin những phiên đăng nhập của các user IT1, IT2, IT3, HR1 và HR2 khi Telnet đến Router GW → Ghi nhận được nhật ký hoạt động của người dùng thành công.

CHƯƠNG 5: KẾT LUẬN

Trong quá trình nghiên cứu và triển khai áp dụng RADIUS trên Windows Server, nhóm đã có cơ hội đánh giá và hiểu rõ hơn về quản trị mạng và hệ thống trong môi trường doanh nghiệp.

Nhóm chúng em cũng nhận thấy những ưu điểm của RADIUS, đặc biệt là khi tích hợp với các dịch vụ như Active Directory và NPS (Network Policy Server). Hệ thống này cho phép quản trị viên dễ dàng áp dụng các chính sách truy cập, ghi nhận log chi tiết các hoạt động kết nối, từ đó nâng cao tính minh bạch và khả năng giám sát trong quản trị mạng.

Tổng kết các hoạt động chính:

- *Quản lý Người Dùng và Tài Khoản:* Sử dụng Active Directory để quản lý quyền truy cập và đặc quyền người dùng một cách hiệu quả, giảm rủi ro về an ninh thông tin và đảm bảo sự nhất quán trong toàn bộ hệ thống.

- *Bảo Mật Hệ Thống:* Triển khai các chính sách trong NPS để áp dụng các cấu hình bảo mật chuẩn hóa cho tất cả các máy tính trong mạng, giúp ngăn chặn các mối đe dọa bảo mật và bảo vệ thông tin quan trọng.

- *Thách Thức và Học Hỏi:* Trong quá trình thực hiện đồ án, nhóm đã đối mặt với một số thách thức như sự hiểu biết về các chính sách cụ thể và quản lý chúng. Một bất cập lớn khác đó là việc triển khai hệ thống trên nền tảng EVE-NG nên hay xảy ra tình trạng lỗi trong việc cài đặt nền tảng và tích hợp các thiết bị Cisco. Tuy nhiên, những thách thức này đã tạo ra cơ hội để học hỏi và phát triển kỹ năng quản trị mạng của nhóm.

- *Tương Lai Phát Triển:* Trong tương lai, nhóm đề xuất mở rộng việc áp dụng RADIUS vào các lĩnh vực khác nhau của hệ thống, cũng như có thể tích hợp với các công nghệ bảo mật tiên tiến như mã hóa mạnh mẽ và xác thực đa yếu tố hơn để phù hợp với môi trường mạng ngày càng phức tạp và nguy hiểm.

Kết Luận Chung: Việc triển khai RADIUS trên Windows Server không chỉ dừng lại ở mục tiêu học thuật mà còn mở ra những cơ hội ứng dụng thực tiễn trong việc xây dựng hệ thống mạng an toàn, hiệu quả và đáng tin cậy. Qua đó, nhóm tin

rằng việc nghiên cứu và triển khai này sẽ mang lại nhiều lợi ích cho tổ chức và là một bước tiến quan trọng trong việc xây dựng một môi trường mạng an toàn cho người dùng.

TÀI LIỆU THAM KHẢO

STT	Tên tài liệu
1	Phòng Thí nghiệm An toàn Thông tin. Lab 04: Triển khai Active Directory trên Windows Server, Lab 5: Triển khai các dịch vụ trên Windows Server, Môn Quản trị mạng và Hệ thống, Trường Đại học Công nghệ Thông tin, ĐHQG Thành phố Hồ Chí Minh.
2	thanhnt118. Tổng Quan Về Active Directory (2020). https://ccna88.wordpress.com/2020/05/25/tong-quan-ve-active-directory/
3	RADIUS Server là gì? Giải pháp quản lý quyền truy cập mạng. https://sunccloud.vn/radius-server-la-gi
4	[2025] Windows Server là gì? Lý do nên chọn Windows Server?. https://vinahost.vn/windows-server-la-gi/
5	NPS server là gì? Những tính năng Network Policy Server trong hạ tầng mạng https://bizflycloud.vn/tin-tuc/nps-server-20240822110148188.htm
6	Cisco IOS - Privilege Levels https://learningnetwork.cisco.com/s/blogs/a0D3i000002eeWTEAY/cisco-ios-privilege-levels

PHỤ LỤC LINK CÁC DEMO

Video các Demo và những file liên quan:

<https://drive.google.com/drive/folders/1AJkmfuTV Cv5ucXe8wErEAe2P31lbrI8x?usp=sharing>

Với:

- demo1.mp4: video thực hiện thử nghiệm cho Client kết nối với Router (GW).
- demo2.mp4: video thực hiện thử nghiệm theo dõi và ghi lại hoạt động người dùng.
- RADIUS SERVER.zip: file bài lab thực hiện các cấu hình và cài đặt nhóm đã thực hiện trên nền tảng EVE-NG..
- RouterCLI.docx: các dòng lệnh cấu hình cho Router.