

LỜI CẢM ƠN



*M*hóm thực hiện đề tài xin chân thành cảm ơn sự hướng dẫn tận tình của Thầy Văn Thiên Hoàng đã theo sát và giúp chúng em tìm hiểu và hoàn thành đề tài Radius Server trong suốt thời gian thực hiện.

Hutech, ngày 18 tháng 05 năm 2012

Nhóm 4 - RADIUS lớp 10LDTHM1

1/ Trần Phúc Lợi	1081020060
2/ Lương Quốc Hạnh	1081020024
3/ Lương Đăng Khoa	1081020052
4/ Huỳnh Mai Khanh	1081020048

MỤC LỤC

CHƯƠNG 1. GIỚI THIỆU RADIUS.....	2
CHƯƠNG 2. GIAO THỨC RADIUS.....	7
CHƯƠNG 3. KẾT QUẢ THỰC NGHIỆM.....	27

CHƯƠNG 1. GIỚI THIỆU RADIUS

1.1 TỔNG QUAN VỀ RADIUS

RADIUS là một giao thức dùng để chứng thực người dùng từ xa (remote access). Thông tin dùng để chứng thực được lưu tập trung ở RADIUS server. Khi cần chứng thực người dùng NAS (RADIUS client) sẽ chuyển thông tin của người dùng đến RADIUS server để tiến hành kiểm tra.

Kết quả sẽ được RADIUS server trả lại cho NAS. Thông tin được trao đổi giữa RADIUS server và RADIUS client đều được mã hóa. Có thể hiểu RADIUS server cung cấp cho RADIUS client khả năng truy xuất vào hệ thống tài khoản người dùng trên Active directory.

1.2 LỊCH SỬ HÌNH THÀNH VÀ PHÁT TRIỂN RADIUS

Giao thức Radius được định nghĩa đầu tiên trong RFC 2058 vào tháng 1 năm 1997. Cũng trong năm 1997 Radius accounting đã được giới thiệu trong RFC 2059. Sau đó vào tháng 4 năm 1997 nhiều bản RFC đã được thay thế bởi RFC 2138 và RFC 2139. Sau đó vào tháng 6 năm 2000 RFC 2865 đã chuẩn hóa Radius và thay thế cho RFC 2138. Cùng thời gian đó RFC 2866 accounting cũng đã thay thế cho RFC 2139

Hiện nay các Radius Server mã nguồn mở tính năng có thể khác nhau nhưng hầu hết chúng đều có đặc điểm chung là tìm kiếm thông tin người dùng trong tập tin văn bản, LDAP server hay các cơ sở dữ liệu khác. Các bảng ghi kế toán (accounting record) đều ghi dữ liệu vào một tập tin văn bản hay cơ sở dữ liệu sau đó chuyển đến các server bên ngoài .v.v.

Đã có kế hoạch thay thế Radius bằng giao thức Diameter. Diameter sử dụng SCTP hoặc TCP trong khi đó Radius sử dụng UDP.

RFC	Title	Date published	Obsoleted by
RFC 2058	Remote Authentication Dial In User Service (RADIUS)	January 1997	RFC 2138
RFC 2059	RADIUS Accounting	January 1997	RFC 2139
RFC 2138	Remote Authentication Dial In User Service (RADIUS)	April 1997	RFC 2865
RFC 2139	RADIUS Accounting	April 1997	RFC 2866
RFC 2548	Microsoft Vendor-specific RADIUS Attributes	March 1999	
RFC 2607	Proxy Chaining and Policy Implementation in Roaming	June 1999	
RFC 2618	RADIUS Authentication Client MIB		RFC 4668
RFC 2619	RADIUS Authentication Server MIB		RFC 4669
RFC 2620	RADIUS Accounting Client MIB	June 1999	RFC 4670
RFC 2621	RADIUS Accounting Server MIB	June 1999	RFC 4671
RFC 2809	Implementation of L2TP Compulsory Tunneling via RADIUS	April 2000	
RFC 2865	Remote Authentication Dial In User Service (RADIUS)	June 2000	
RFC 2866	RADIUS Accounting	June 2000	
RFC 2867	RADIUS Accounting Modifications for Tunnel Protocol Support	June 2000	
RFC 2868	RADIUS Attributes for Tunnel Protocol Support	June 2000	
RFC 2869	RADIUS Extensions	June 2000	
RFC 2882	Network Access Servers Requirements: Extended RADIUS Practices	July 2000	
RFC 3162	RADIUS and IPv6	August 2001	
RFC 3575	IANA Considerations for RADIUS	July 2003	
RFC 3576	Dynamic Authorization Extensions to RADIUS	July 2003	RFC 5176
RFC 3579	RADIUS Support for EAP	September 2003	
RFC 3580	IEEE 802.1X RADIUS Usage Guidelines	September 2003	
RFC 4014	RADIUS Attributes Suboption for the DHCP Relay Agent Information Option	February 2005	
RFC 4372	Chargeable User Identity	January 2006	
RFC 4590	RADIUS Extension for Digest Authentication	July 2006	RFC 5090
RFC 4668	RADIUS Authentication Client MIB for IPv6	August 2006	
RFC 4669	RADIUS Authentication Server MIB for IPv6	August 2006	
RFC 4670	RADIUS Accounting Client MIB for IPv6	August 2006	
RFC 4671	RADIUS Accounting Server MIB for IPv6	August 2006	

RFC 4675	RADIUS Attributes for Virtual LAN and Priority Support	September 2006
RFC 4679	DSL Forum Vendor-Specific RADIUS Attributes	September 2006
RFC 4818	RADIUS Delegated-IPv6-Prefix Attribute	April 2007
RFC 4849	RADIUS Filter Rule Attribute	April 2007
RFC 5080	Common RADIUS Implementation Issues and Suggested Fixes	December 2007
RFC 5090	RADIUS Extension for Digest Authentication	February 2008
RFC 5176	Dynamic Authorization Extensions to RADIUS	January 2008
RFC 5607	RADIUS Authorization for NAS Management	July 2009
RFC 5997	Use of Status-Server Packets in the RADIUS Protocol	August 2010

Hình 1. CÁC PHIÊN BẢN RFC CỦA RADIUS

1.3 ƯU VÀ NHƯỢC ĐIỂM RADIUS

1.3.1 ƯU ĐIỂM

RADIUS có phần overhead ít hơn so với TACACS vì nó sử dụng UDP, trong phần overhead không có địa chỉ đích, port đích nên các hacker khó có thể tấn công. Với cách thức phân phối dạng source code, RADIUS là dạng giao thức hoàn toàn mở rộng. Người dùng có thể thay đổi nó để làm việc với bất kì hệ thống bảo mật hiện có.

RADIUS có chức năng tính cước (accounting) mở rộng.

RADIUS thường được dùng để tính cước dựa trên tài nguyên đã sử dụng. Ví dụ như ISP sẽ tính cước cho người dùng về chi phí kết nối. Ta có thể cài đặt RADIUS Accounting mà không cần sử dụng RADIUS để xác thực và cấp quyền.

Với chức năng accounting mở rộng, RADIUS cho phép dữ liệu được gửi từ các thiết bị xuất phát cũng như là thiết bị đích, từ đó giúp ta theo dõi việc sử dụng tài nguyên (thời gian, số lượng các gói tin, số lượng byte,...) trong suốt phiên làm việc

1.3.2 NHƯỢC ĐIỂM

Chỉ mã hóa mật khẩu trong gói access-request

Không hỗ trợ truy cập ARA, Net Bios Frame Protocol Control Protocol, NASI X.25

Không cho phép người dùng thực thi các dòng lệnh trên thiết bị định tuyến.

1.4 ỨNG DỤNG RADIUS

Radius được ứng dụng rộng rãi để quản lý và chứng thực người dùng một cách tập trung cho kết nối VPN, WLAN... Với việc tổ chức quản lý người dùng theo các OU, Group được phân quyền và áp dụng các chính sách thích hợp để đáp ứng nhu cầu bảo mật dữ liệu truyền đi trên mạng. Radius còn có chức năng Accounting nhằm kiểm soát người dùng một cách chặt chẽ theo dạng file log

1.5 CÁC CÔNG NGHỆ LIÊN QUAN CỦA RADIUS

Cả RADIUS và TACACS đều là hai giao thức có chức năng tương tự nhau. TACACS (Terminal Access Controller Access Control System) và RADIUS (Remote Authentication Dial-In User Service) cả hai giao thức đều có phiên bản và thuộc tính riêng.

Chẳng hạn như phiên bản riêng của TACACS là TACACS+. RADIUS cũng có sự mở rộng khi cho phép khách hàng thêm thông tin xác định được mang bởi RADIUS.

1.5.1 TỔNG QUAN VỀ TACACS

TACACS là giao thức được chuẩn hóa sử dụng giao thức hướng kết nối (connection-oriented) là TCP trên port 49. TACACS có các ưu điểm sau :

Với khả năng nhận gói reset (RST) trong TCP, một thiết bị có thể lập tức báo cho đầu cuối khác biết rằng đã có hỏng hóc trong quá trình truyền.

TCP là giao thức mở rộng vì có khả năng xây dựng cơ chế phục hồi lỗi. Nó có thể tương thích để phát triển cũng như làm tắc nghẽn mạng với việc sử dụng sequence number để truyền lại.

Toàn bộ payload được mã hóa với TACACS+ bằng cách sử dụng một khóa bí mật chung (shared secret key). TACACS+ đánh dấu một trường trong header để xác định xem dữ liệu có mã hóa hay không.

TACACS+ mã hóa toàn bộ gói bằng việc sử dụng khóa bí mật chung nhưng bỏ qua header TACACS chuẩn. Cùng với header là một trường xác định body có được mã hóa hay không. Thường thì trong toàn bộ thao tác, body của một gói được mã hóa hoàn toàn để truyền thông an toàn.

TACACS+ được chia làm ba phần: xác thực (authentication), cấp quyền (authorization) và tính cước (accounting). Với cách tiếp cận theo module, ta có thể sử dụng các dạng khác của xác thực và vẫn sử dụng TACACS+ để cấp quyền và tính cước. Chẳng hạn như, việc sử dụng phương thức xác thực Kerberos cùng với việc cấp quyền và tính cước bằng TACACS+ là rất phổ biến.

TACACS+ hỗ trợ nhiều giao thức.

Với TACACS+, ta có thể dùng hai phương pháp để điều khiển việc cấp quyền thực thi các dòng lệnh của một user hay một nhóm nhiều user :

Phương pháp thứ nhất là tạo một mức phân quyền (privilege) với một số câu lệnh giới hạn và user đã xác thực bởi router và TACACS server rồi thì sẽ được cấp cho mức đặc quyền xác định nói trên.

Phương pháp thứ hai đó là tạo một danh sách các dòng lệnh xác định trên TACACS+ server để cho phép một user hay một nhóm sử dụng.

TACACS thường được dùng trong môi trường enterprise. Nó có nhiều ưu điểm và làm việc tốt đáp ứng yêu cầu quản lý mạng hàng ngày.

1.5.2 ƯU ĐIỂM CỦA TACACS

RADIUS không cho phép kiểm soát những lệnh mà user được và không được phép sử dụng trên router. TACACS+ tỏ ra mềm dẻo và hữu dụng hơn trong vấn đề quản lý router nhờ vào việc cung cấp 2 phương thức kiểm soát việc uỷ quyền (authentication) cả trên phương diện user và group:

Gán những câu lệnh có thể thực thi vào privilege levels và thông qua TACACS+ server để áp sự phân cấp về quyền này đến user truy cập vào.

Xác định những lệnh mà có thể thực thi trên router lên user hoặc group thông qua những cấu hình trên TACACS+ server.

CHƯƠNG 2. GIAO THỨC RADIUS

2.1. GIỚI THIỆU AAA

Các nhà quản trị mạng ngày nay phải điều khiển việc truy cập cũng như giám sát thông tin mà người dùng đầu cuối đang thao tác. Những việc làm đó có thể đưa đến thành công hay thất bại của công ty. Với ý tưởng đó, AAA là cách thức tốt nhất để giám sát những gì mà người dùng đầu cuối có thể làm trên mạng. Ta có thể xác thực (authentication) người dùng, cấp quyền (authorization) cho người dùng, cũng như tập hợp được thông tin như thời gian bắt đầu hay kết thúc của người dùng (accounting).

Như ta thấy, bảo mật là vấn đề rất quan trọng. Với mức độ điều khiển, thật dễ dàng để cài đặt bảo mật và quản trị mạng. Ta có thể định nghĩa các vai trò (role) đưa ra cho user những lệnh mà họ cần để hoàn thành nhiệm vụ của họ và theo dõi những thay đổi trong mạng. Với khả năng log lại các sự kiện, ta có thể có những sự điều chỉnh thích hợp với từng yêu cầu đặt ra.

Tất cả những thành phần này là cần thiết để duy trì tính an toàn, bảo mật cho mạng. Với thông tin thu thập được, ta có thể tiên đoán việc cập nhật cần thiết theo thời gian. Yêu cầu bảo mật dữ liệu, gia tăng băng thông, giám sát các vấn đề trên mạng,... tất cả đều có thể tìm thấy trên dịch vụ AAA.

AAA [1] cho phép nhà quản trị mạng biết được các thông tin quan trọng về tình hình cũng như mức độ an toàn trong mạng. Nó cung cấp việc xác thực (authentication) người dùng nhằm bảo đảm có thể nhận dạng đúng người dùng. Một khi đã nhận dạng người dùng, ta có thể giới hạn thẩm quyền (authorization) mà người dùng có thể làm.

Khi người dùng sử dụng mạng, ta cũng có thể giám sát tất cả những gì mà họ làm. AAA với ba phần xác thực (authentication), cấp quyền (authorization), tính cước (accounting) là các phần riêng biệt mà ta có thể sử dụng trong dịch vụ mạng, cần thiết để mở rộng và bảo mật mạng.

AAA có thể dùng để tập hợp thông tin từ nhiều thiết bị trên mạng. Ta có thể bật các dịch vụ AAA trên router, switch, firewall, các thiết bị VPN, server, ...

2.1.1. XÁC THỰC (Authentication)

Xác thực dùng để nhận dạng (identify) người dùng. Trong suốt quá trình xác thực, username và password của người dùng được kiểm tra và đối chiếu với cơ sở dữ liệu lưu trong AAA Server. Tất nhiên, tùy thuộc vào giao thức mà AAA hỗ trợ mã hóa đến đâu, ít nhất thì cũng mã hóa username và password.

Xác thực sẽ xác định người dùng là ai. Ví dụ: Người dùng có username là THIEN và mật khẩu là “L@bOnlin3” sẽ là hợp lệ và được xác thực thành công với hệ thống. Sau khi xác thực thành công thì người dùng đó có thể truy cập được vào mạng. Tiến trình này chỉ là một trong các thành phần để điều khiển người dùng với AAA. Một khi username và password được chấp nhận, AAA có thể dùng để định nghĩa thẩm quyền mà người dùng được phép làm trong hệ thống.

2.1.2. CẤP QUYỀN (Authorization)

Authorization cho phép nhà quản trị điều khiển việc cấp quyền trong một khoảng thời gian, hay trên từng thiết bị, từng nhóm, từng người dùng cụ thể hay trên từng giao thức. AAA cho phép nhà quản trị tạo ra các thuộc tính mô tả các chức năng của người dùng được phép làm. Do đó, người dùng phải được xác thực trước khi cấp quyền cho người đó.

AAA Authorization làm việc giống như một tập các thuộc tính mô tả những gì mà người dùng đã được xác thực có thể có. Ví dụ: người dùng THIEN sau khi đã xác thực thành công có thể chỉ được phép truy cập vào server VNLABPRO_SERVER thông qua FTP. Những thuộc tính này được so sánh với thông tin chứa trong cơ sở dữ liệu của người dùng đó và kết quả được trả về AAA để xác định khả năng cũng như giới hạn thực tế của người đó. Điều này yêu cầu cơ sở dữ liệu phải giao tiếp liên tục với AAA server trong suốt quá trình kết nối đến thiết bị truy cập từ xa (RAS).

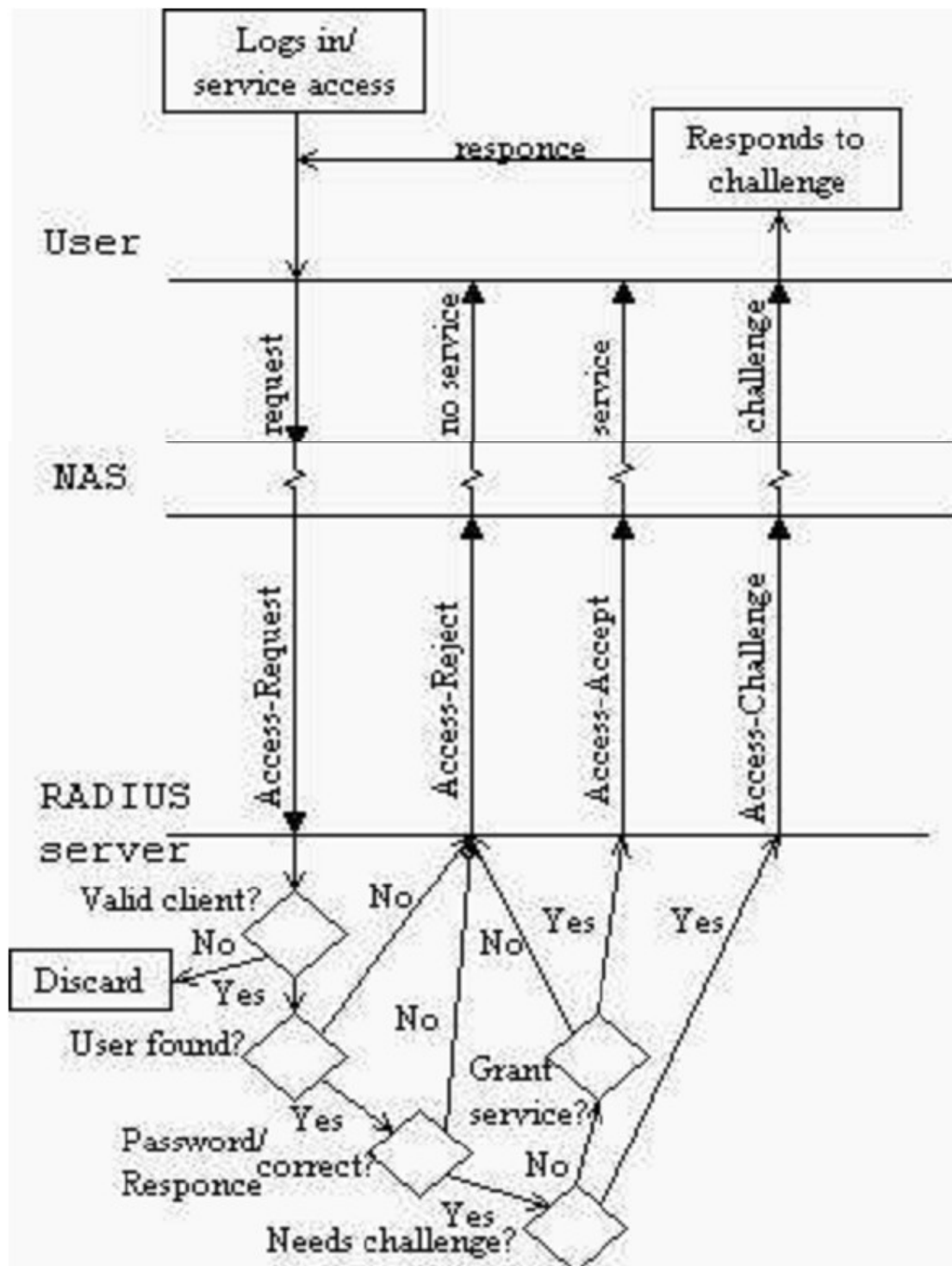
2.1.3. KẾ TOÁN (Accounting)

Accounting cho phép nhà quản trị có thể thu thập thông tin như thời gian bắt đầu, thời gian kết thúc người dùng truy cập vào hệ thống, các câu lệnh đã thực thi, thống kê lưu lượng, việc sử dụng tài nguyên và sau đó lưu trữ

thông tin trong hệ thống cơ sở dữ liệu quan hệ. Nói cách khác, accounting cho phép giám sát dịch vụ và tài nguyên được người dùng sử dụng. Ví dụ: thống kê cho thấy người dùng có tên truy cập là THIEN đã truy cập vào VNLABPRO_SERVER bằng giao thức FTP với số lần là 5 lần. Điểm chính trong Accounting đó là cho phép người quản trị giám sát tích cực và tiên đoán được dịch vụ và việc sử dụng tài nguyên. Thông tin này có thể được dùng để tính cước khách hàng, quản lý mạng, kiểm toán sổ sách.

2.2. SƠ ĐỒ NGUYÊN LÝ

2.1.4. CHỨNG THỰC VÀ CẤP QUYỀN - AUTHENTICATION and AUTHORIZATION



Hình 2. **QUÁ TRÌNH CHỨNG THỰC VÀ CẤP QUYỀN CHO NGƯỜI DÙNG**

Khi một user kết nối, NAS sẽ gửi một message dạng RADIUS Access-request tới máy chủ AAA Server, chuyển các thông tin như Username, Password , UDP port, NAS identifier và một Authentication message.

Sau khi nhận các thông tin AAA sử dụng gói tin được cung cấp như NAS Identifier, và Authentication thẩm định lại việc NAS đó có được phép gửi

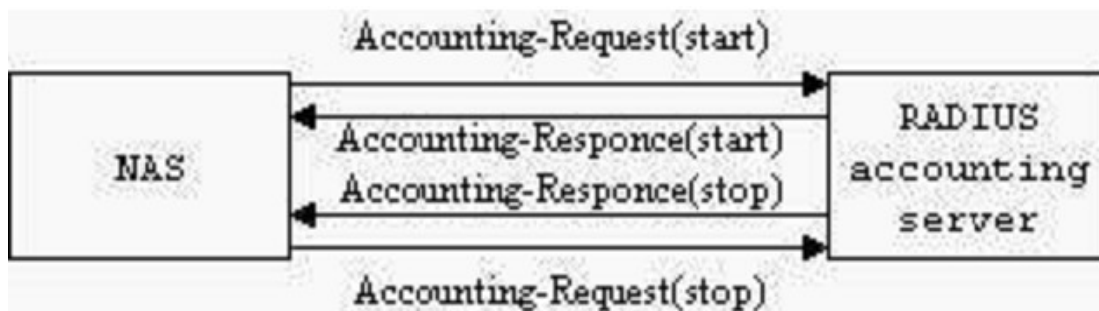
các yêu cầu đó không? Nếu có khả năng, AAA server sẽ kiểm tra thông tin username và password mà người dùng yêu cầu truy cập trong database. Nếu quá trình kiểm tra là đúng thì nó sẽ mang một thông tin trong Access-request quyết định quá trình truy cập của user đó là được chấp nhận.

Khi quá trình chứng thực bắt đầu được sử dụng, AAA server có thể trả về một RADIUS Access-Challenge mang một số ngẫu nhiên. NAS sẽ chuyển thông tin đến người dùng từ xa. Khi đó người dùng sẽ phải trả lời đúng yêu cầu xác nhận, sau đó NAS sẽ chuyển đến AAA server một RADIUS Access-Request

AAA server sau khi kiểm tra các thông tin của người dùng hoàn toàn thỏa mãn sẽ cho phép sử dụng dịch vụ, nó sẽ trả về một message dạng RADIUS Access-accept. Nếu không thỏa mãn AAA server sẽ trả về một tin RADIUS Access-reject và NAS sẽ ngắt dịch vụ.

Khi gói tin Access-accept được nhận và RADIUS Accounting đã được thiết lập, NAS sẽ gửi một gói tin RADIUS Accounting –request tới AAA server. Máy chủ sẽ thêm các thông tin vào logfile của nó, với việc NAS sẽ cho phép phiên làm việc với User bắt đầu khi nào và kết thúc khi nào. RADIUS Accounting làm nhiệm vụ ghi lại quá trình xác thực của user vào hệ thống, khi kết thúc phiên làm việc NAS sẽ gửi thông tin RADIUS Accounting-request

2.1.5. KẾ TOÁN RADIUS - (RADIUS ACCOUNTING)



Hình 3. QÚA TRÌNH YÊU CẦU KIỂM TOÁN

Khi một máy khách được cấu hình để sử dụng RADIUS kế toán, khi bắt đầu cung cấp dịch vụ nó sẽ tạo ra một gói tin bắt đầu kế toán mô tả các loại hình dịch vụ được cung cấp và người sử dụng nó đang được chuyển tới, và sẽ gửi tới máy chủ kế toán RADIUS, trong đó sẽ gửi lại một xác nhận rằng gói tin đã được nhận.

Khi kết thúc cung cấp dịch vụ máy khách sẽ tạo ra một gói kết thúc kế toán mô tả các loại hình dịch vụ đã được giao và thông số tùy ý như là thời gian trôi qua, octet vào và ra, hoặc các gói dữ liệu vào và ra. Nó sẽ gửi tới máy chủ kế toán RADIUS, và sẽ gửi phản hồi một xác nhận rằng gói tin đã được nhận.

Accounting-Request (dù cho bắt đầu hoặc kết thúc) được gửi tới máy chủ kế toán RADIUS qua mạng. Nó khuyến cáo các khách hàng tiếp tục cố gắng gửi gói tin Accounting-Request cho đến khi nhận được một xác nhận, bằng cách sử dụng một số hình thức chờ để truyền. Nếu không có phản hồi được trả về trong một khoảng thời gian, yêu cầu được gửi lại một số lần.

Máy khách cũng có thể chuyển tiếp yêu cầu tới một máy chủ thay thế hoặc các máy chủ trong trường hợp máy chủ chính ngừng hoạt động hoặc không thể truy cập. Một máy chủ thay thế có thể được sử dụng hoặc sau khi một số cố gắng đến các máy chủ chính bị lỗi, hoặc trong một kiểu vận hành luân lượt.

Máy chủ kế toán RADIUS có thể làm cho yêu cầu của các máy chủ khác đáp ứng các yêu cầu, trong trường hợp nó hoạt động như một máy khách.

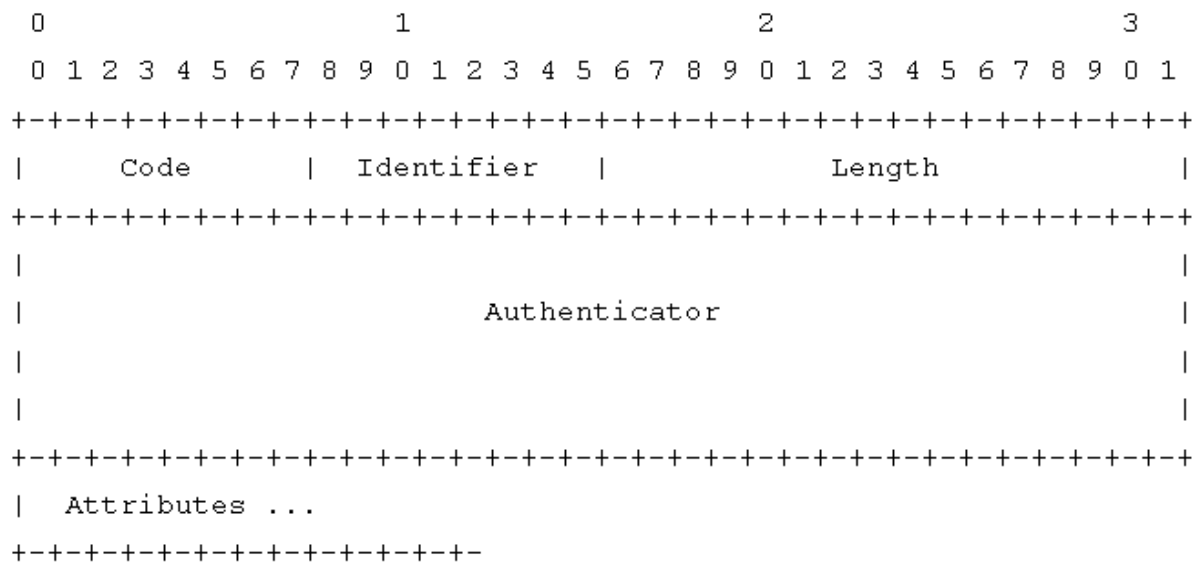
Nếu máy chủ kế toán RADIUS không thể thành công ghi lại các gói tin kế toán, nó không phải gửi một xác nhận Accounting-Response cho máy khách.

2.3. KIẾN TRÚC RADIUS

2.1.6. DẠNG GÓI CỦA PACKET

Một gói RADIUS được bao bọc trong trường dữ liệu của gói UDP, và trường địa chỉ đích có số hiệu cổng là 1812. Khi gói trả lời được tạo ra, số hiệu cổng của địa chỉ nguồn và đích được bảo lưu.

Một gói dữ liệu của RADIUS được xác định như sau (các trường được gửi đi từ trái sang phải).



Hình 4. CẤU TRÚC MỘT GÓI TIN CỦA RADIUS

- **Code:** Code field gồm một octet, xác định kiểu gói của RADIUS.

Khi một gói có mã không hợp lệ sẽ không được xác nhận

RADIUS code (decimal) được chỉ định như sau:

- 1 Access-Request
- 2 Access-Accept
- 3 Access-Reject
- 4 Accounting-Request
- 5 Accounting-Response
- 11 Access-Challenge
- 12 Status-Server (experimental)
- 13 Status-Client (experimental)
- 255 Reserved

Mã số 4 và số 4 được che đậy trong tài liệu RADIUS accounting [5]. Mã số 12 và 13 là dành riêng cho việc có thể sử dụng, nhưng nó không được đề cập ở đây.

- **Identifier (Trường định danh)**

Identifier field gồm một octet, và phù hợp với việc hỗ trợ yêu cầu và trả lời. Các máy chủ RADIUS có thể phát hiện một yêu cầu trùng lặp, nếu có các client có cùng một địa chỉ IP nguồn và UDP port và định danh trong một thời gian ngắn.

- **Length**

Length field gồm hai octet, nó bao gồm các code field, identifier, length, authentication, và trường thuộc tính (attribute field). Những byte nằm ngoài khoảng qui định bởi length sẽ được coi là những byte thừa, và sẽ bị bỏ qua khi nhận. Nếu gói ngắn hơn giá trị trường length, nó sẽ không được xác nhận và trả lời. Giá trị nhỏ nhất của trường length là 20 và giá trị lớn nhất là 4096.

- **Authenticator**

Trường authenticator gồm 16 octet. Octet lớn nhất được truyền đi đầu tiên. Giá trị này được sử dụng để xác nhận các trả lời từ RADIUS server và được sử dụng trong thuật toán ẩn mật khẩu.

Request Authenticator: Trong các gói access-request, giá trị của trường xác nhận (authenticator field) là một số ngẫu nhiên 16 byte được gọi là bộ xác nhận yêu cầu (request authenticator). Giá trị này không thể dự đoán trước và duy nhất trong suốt thời gian sống của “thông tin bí mật” (mật khẩu dùng chung giữa client và RADIUS server); Vì nếu có sự lặp lại của giá trị này có nghĩa là một attacker có thể trả lời câu hỏi này không cần sự xác nhận của RADIUS server. Do đó, bộ xác nhận yêu cầu nên có giá trị toàn cục và duy nhất theo thời gian.

Mặc dù, giao thức RADIUS không có khả năng ngăn chặn sự nghe lén phiên xác thực qua đường dây, nhưng việc sinh ra các giá trị không thể đoán

trước được cho bộ xác nhận yêu cầu có thể hạn chế rất nhiều sự kiện này. NAS và RADIUS server chia sẻ ‘thông tin bí mật’. Thông tin bí mật chung này có được sau khi giá trị của “bộ xác nhận yêu cầu” được thuật toán MD5 băm để tạo ra giá trị 16 byte. Giá trị này được XOR với mật khẩu mà user nhập vào, kết quả sẽ được đặt vào thuộc tính user-password trong gói access-accept.

Response authenticator: Giá trị của trường xác nhận (authenticator field value) trong các gói access-request, access-reject, access-challenge được coi là bộ xác nhận trả lời (response authenticator). Giá trị này được tính bởi băm MD5 chuỗi các byte của code field, identifier, length, xác nhận của gói access-request, và cộng thêm các thuộc tính trả lời và thông tin bí mật dùng chung

$$\text{ResponseAuth} = \text{D5}(\text{Code} + \text{ID} + \text{Length} + \text{RequestAuth} + \text{Attributes} + \text{Secret}).$$

where + denotes concatenation.

- **Administrative Note**

Thông tin bí mật (chia sẻ password giữa client và RADIUS server) nên ít nhất và phức tạp đó là cách lựa chọn mật khẩu tốt. Mức ưu tiên có thể chấp nhận được ít nhất là 16 octet. Điều này để đảm bảo phạm vi đủ lớn cho việc cung cấp các cơ chế bảo mật chống lại các cuộc tấn công tìm kiếm.

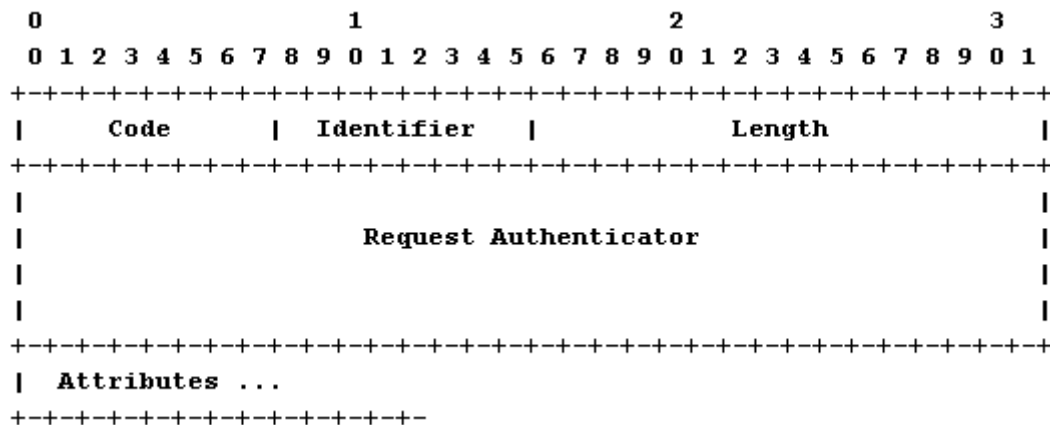
Packet type được xác định bởi code field chiếm byte đầu tiên của gói RADIUS.

- **Access-Request**

Gói access-request được gửi tới RADIUS server. Nó chuyên chở thông tin dùng để xác định xem user có được phép truy cập vào NAS và các dịch vụ được chỉ định hay không. Code field của gói phải có giá trị 1. Gói access-request phải chứa các thuộc tính user-name, user-password hoặc CHAP-password, và có thể chứa các thuộc tính NAS-IP-Address, NAS-Identifier, NAS-PORT, NAS-PORT-TYPE.

Trường identifier phải được thay đổi khi nội dung của trường thuộc tính bị thay đổi khi nội dung của trường thuộc tính bị thay đổi hoặc là đã nhận

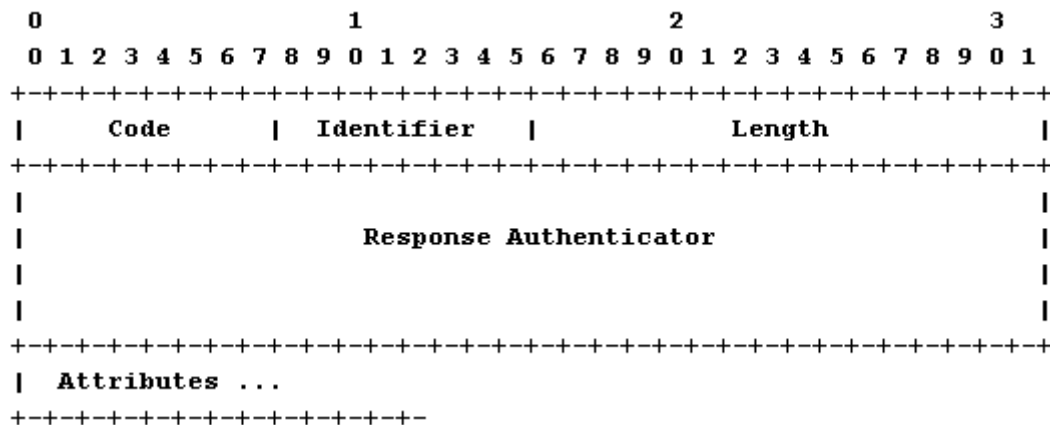
được trả lời hợp lệ cho yêu cầu trước đó. Trong trường hợp phải gửi lại gói, trường identifier không được thay đổi.



Hình 5. CẤU TRÚC GÓI ACCESS REQUEST

- **Access-accept**

Gói access-accept được gửi trả bởi RADIUS server khi tất cả các giá trị thuộc tính của gói access-request. Nó cung cấp thông tin cấu hình cần thiết để cấp phát các dịch vụ cho user. Trường code phải có giá trị 2. Gói access-accept nhận được ở NAS phải có trường danh hiệu trùng khớp với access-request tương ứng đã gửi trước đó và phải có xác nhận (response authenticator) phù hợp với thông tin bí mật dùng chung.

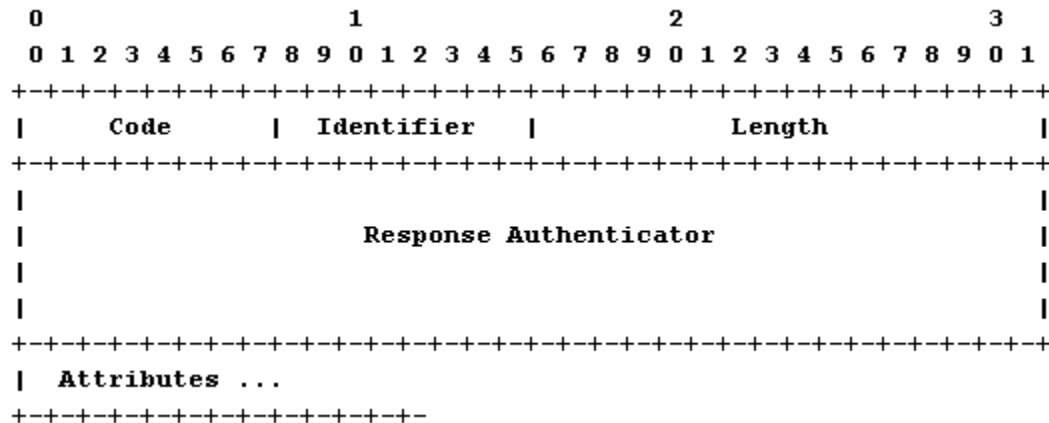


Hình 6. CẤU TRÚC GÓI ACCESS ACCEPT

- **Access-reject**

Gói access-reject được gửi trả từ RADIUS server khi có giá trị thuộc tính không được thỏa. Trường code của mã phải có giá trị 3. Gói có thể chứa 1 hoặc nhiều thuộc tính reply-message với một thông báo dạng văn bản mà NAS

sẽ hiển thị nó với user. Trường identifier của gói access-reject chính là bản sao của gói access-request tương ứng.

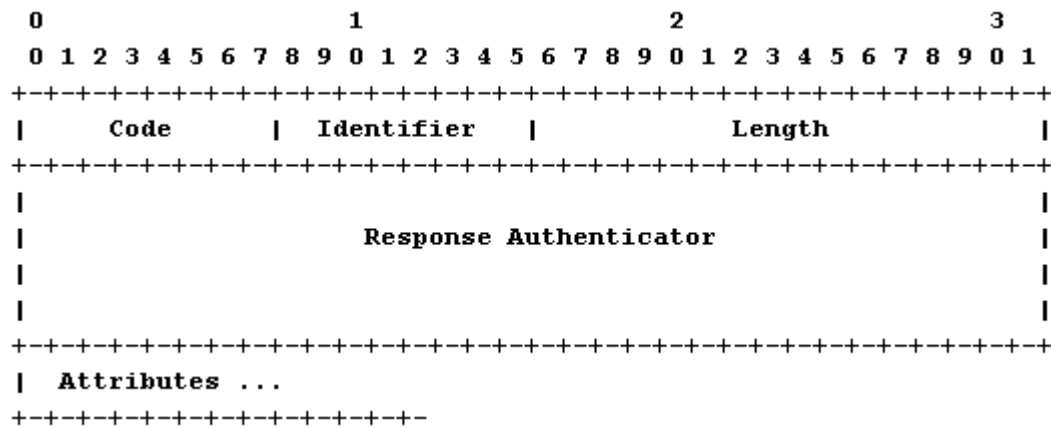


Hình 7. CẤU TRÚC GÓI ACCESS REJECT

- **Access-challenge**

Gói access-challenge được RADIUS server gửi đến user đòi hỏi thêm thông tin cần thiết mà user phải trả lời. Trường code của gói phải có giá trị 11. Gói có thể chứa 1 hoặc nhiều thuộc tính reply-message và có thể có 1 thuộc tính state. Các thuộc tính khác không được xuất hiện trong gói access-challenge. Trường identifier của gói access-challenge phải trùng khớp với gói access-request tương ứng đã gửi đi trước đó và phải có trường xác nhận (authenticator field) phù hợp với thông tin bí mật dùng chung. Nếu NAS không được trang bị challenge/ response thì gói access-challenge nhận được sẽ coi như gói access-reject.

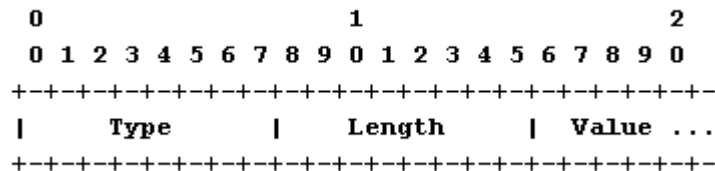
Nếu NAS được trang bị chức năng challenge/ response và gói access-challenge nhận được là hợp lệ thì NAS sẽ hiển thị thông báo và yêu cầu user trả lời thông tin mà RADIUS server yêu cầu. Sau đó NAS sẽ gửi gói access-request gốc nhưng với danh hiệu yêu cầu (request ID) và xác nhận yêu cầu (request authenticator) mới, đồng thời thuộc tính user-password cũng được thay thế bởi thông tin trả lời của user (đã được mã hóa) và có thể bao gồm cả thuộc tính state từ gói access-challenge.



Hình 8. CẤU TRÚC GÓI ACCESS CHALLENGE

- **Attributes (các thuộc tính)**

Các thuộc tính của RADIUS, chứa trong các gói yêu cầu và trả lời, mang thông tin xác thực quyền, phân quyền, cấu hình cần thiết để cấp phát các dịch vụ cho user. Giá trị các trường length của gói RADIUS sẽ qui định điểm kết thúc của các thuộc tính trong gói. Dạng của thuộc tính như sau:



Hình 9. CẤU TRÚC TRƯỜNG THUỘC TÍNH - ATTRIBUTE

- **Type**

Mỗi trường type là một octet, giá trị từ 192-223 là dành riêng cho nghiên cứu, giá trị từ 224-240 là dành cho việc thực hiện cụ thể, 241-255 là dành riêng và không nên sử dụng.

RADIUS server có thể bỏ qua các thuộc tính với một loại không rõ.

RADIUS client có thể bỏ qua các thuộc tính với một loại không rõ.

Gồm các giá trị sau:

- 1 User-Name
- 2 User-Password
- 3 CHAP-Password

4	NAS-IP-Address
5	NAS-Port
6	Service-Type
7	Framed-Protocol
8	Framed-IP-Address
9	Framed-IP-Netmask
10	Framed-Routing
11	Filter-Id
12	Framed-MTU
13	Framed-Compression
14	Login-IP-Host
15	Login-Service
16	Login-TCP-Port
17	(unassigned)
18	Reply-Message
19	Callback-Number
20	Callback-Id
21	(unassigned)
22	Framed-Route
23	Framed-IPX-Network
24	State
25	Class
26	Vendor-Specific
27	Session-Timeout
28	Idle-Timeout
29	Termination-Action
30	Called-Station-Id
31	Calling-Station-Id
32	NAS-Identifier
33	Proxy-State
34	Login-LAT-Service
35	Login-LAT-Node

- 36 Login-LAT-Group
- 37 Framed-AppleTalk-Link
- 38 Framed-AppleTalk-Network
- 39 Framed-AppleTalk-Zone
- 40-59 (reserved for accounting)
- 60 CHAP-Challenge
- 61 NAS-Port-Type
- 62 Port-Limit
- 63 Login-LAT-Port

- ***Length (trường độ dài)***

Biểu thị độ dài của thuộc tính cho các trường kiểu, length và value. Nếu thuộc tính trong gói access-request có trường độ dài không hợp lệ thì RADIUS server sẽ trả về gói access-reject. Nếu thuộc tính trong gói access-reject, access-accept, access-challenge có trường độ dài không hợp lệ thì NAS client sẽ xem như là gói access-reject hoặc là không xác nhận và trả lời.

- ***Value (trường giá trị)***

Dạng và chiều dài của trường giá trị được xác định bởi trường kiểu (type field) và trường độ dài (length field). Có 4 loại dữ liệu cho trường giá trị như sau:

Text 1-253 octets containing UTF-8 encoded 10646 [7]
characters. Text of length zero (0) MUST NOT be sent;
omit the entire attribute instead.

String 1-253 octets containing binary data (values 0 through
255 decimal, inclusive). Strings of length zero (0)
MUST NOT be sent; omit the entire attribute instead.

Address 32 bit value, most significant octet first.

Integer 32 bit unsigned value, most significant octet first.

Time 32 bit unsigned value, most significant octet first -- seconds since 00:00:00 UTC, January 1, 1970. The standard Attributes do not use this data type but it is presented here for possible use in future attributes.

2.1.7. PHƯƠNG THỨC MÃ HÓA VÀ GIẢI MÃ

Thuộc tính user-password chứa trong các gói access-request hoặc access-challenge, đặc trưng cho mật khẩu (password) của user, sẽ được ẩn trong khi truyền tới RADIUS server. Mật khẩu sẽ được thêm vào các ký tự NULL sao cho độ dài là bội của 16 byte.

MD5 băm một chiều (one-way MD5 hash) sẽ được xây dựng từ chuỗi các byte của “thông tin bí mật chung” giữa NAS và RADIUS server và thường xác nhận yêu cầu. Giá trị tính được sẽ được XOR với đoạn 16 byte đầu tiên của mật khẩu, kết quả sẽ được đặt vào 16 byte đầu tiên của trường giá trị của thuộc tính user-password.

Nếu password dài hơn 16 ký tự thì giá trị băm thứ hai được tính từ chuỗi các byte tiếp theo của “thông tin bí mật chung” và kết quả của XOR lần trước. Giá trị băm có được sẽ XOR với 16 byte tiếp theo của mật khẩu, kết quả sẽ được đặt vào 16 byte tiếp theo của trường giá trị kiểu string của thuộc tính user-password. Quá trình tiếp theo cứ tiếp diễn đến khi hết các đoạn (segment) được chia của mật khẩu (tối đa là 128 ký tự).

Giả sử gọi “thông tin bí mật chung” là S, giá trị của trường xác định yêu cầu (request authentication) 128 bit là RA. Chia mật khẩu đã được lấp đầy bởi các ký tự NULL (nếu cần) thành các phần con (chunks) p1, p2... Gọi các khối mật mã dạng văn bản (ciphertext blocks) là c(1), c(2),... và các giá trị trung gian là b1, b2... Dấu + là phép cộng chuỗi.

$$b1 = MD5(S + RA) \quad c(1) = p1 \text{ xor } b1$$

$$b2 = MD5(S + c(1)) \quad c(2) = p2 \text{ xor } b2$$

$$\begin{array}{ccc} \cdot & & \cdot \\ \cdot & & \cdot \end{array}$$

$$b_i = \text{MD5}(S + c(i-1)) \quad c(i) = p_i \text{ xor } b_i$$

The String will contain $c(1)+c(2)+\dots+c(i)$ where $+$ denotes concatenation.

Khi gói RADIUS được nhận, quá trình sẽ diễn ra ngược lại trong quá trình giải mã.

2.1.8. SỰ BẢO MẬT VÀ TÍNH MỞ RỘNG

Tất cả các message của RADIUS đều đóng gói bởi UDP Datagrams, nó bao gồm các thông tin như: message type, sequence number, length, authenticator, và một loạt các attributes values mà chúng ta đã tìm hiểu ở trên.

2.4. RADIUS RFCs

2.1.9. NGUỒN GỐC RADIUS RFC

RADIUS ban đầu được quy định trong một RFI bởi Merit Network vào năm 1991 để kiểm soát truy cập quay số tới NSFNET. Livingston Enterprises trả lời cho RFI với mô tả của một máy chủ RADIUS.

Merit Network quyết định liên hệ với Livingston Enterprises giao hàng loạt PortMaster của các Network Access Server và máy chủ RADIUS ban đầu cho Merit. RADIUS sau đó (1997) được xuất bản như RFC 2058 và RFC 2059 (phiên bản hiện tại là RFC 2865 và RFC 2866).

Hiện nay, tồn tại một số máy chủ RADIUS thương mại và mã nguồn mở. Các tính năng có thể khác nhau, nhưng hầu hết có thể thấy sử dụng trong các tập tin văn bản, máy chủ LDAP, cơ sở dữ liệu khác nhau...

Tài liệu kế toán có thể được ghi vào tập tin văn bản, cơ sở dữ liệu khác nhau, chuyển tiếp đến máy chủ bên ngoài... SNMP thường được sử dụng để giám sát từ xa và kiểm tra xem một máy chủ RADIUS còn hoạt động hay không.

Các máy chủ RADIUS proxy được sử dụng để tập trung quản lý và có thể viết lại các gói tin RADIUS (đối với lý do bảo mật, hoặc để Chuyển đổi giữa các nhà cung cấp).

Các giao thức Diameter là kế hoạch thay thế cho RADIUS. Diameter sử dụng SCTP hoặc TCP trong khi RADIUS sử dụng UDP là lớp vận chuyển.

2.1.10. GIỚI THIỆU MỘT VÀI RADIUS RFCs

2.1.10.1. RFC 2865

RFC 2865 – Remote Authentication Dial In User Service: chủ yếu mô tả về cơ chế xác thực và ủy quyền khi người dùng muốn truy cập.

Trong RFC có giới thiệu cấu trúc các gói tin cần dùng để thực hiện xác thực và ủy quyền cho người dùng truy cập và các thuộc tính dùng để mô tả trong các gói tin. Đồng thời cũng trình bày về cơ chế hoạt động và các trường hợp xảy ra khi người dùng muốn truy cập.

Một số thay đổi so với bản RFC 2138 trước đó:

- Strings nên sử dụng UTF-8 thay vì US-ASCII và nên được xử lý như là dữ liệu 8-bit.

- Integers và dates bây giờ được xác định là giá trị 32 bit không dấu.
- Danh sách cập nhật các thuộc tính có thể được bao gồm trong

Access-Challenge để phù hợp với các bảng thuộc tính.

- User-Name đề cập đến các nhận dạng truy cập mạng.
- User-Name bây giờ có thể được gửi trong Access-Accept để sử dụng

với kế toán và đăng nhập từ xa.

- Giá trị thêm vào cho Service-Type, Login-Service, Framed-Protocol,

Framed-Compression, và NAS-Port-Type.

- NAS-Port có thể sử dụng tất cả 32 bit.
- Các ví dụ hiện nay bao gồm hiển thị hệ thập lục phân của các gói dữ

liệu.

- Cổng UDP nguồn phải được sử dụng kết hợp với bộ nhận dạng yêu

cầu khi xác định các bản sao.

- Nhiều thuộc tính phục có thể được cho phép trong thuộc tính

Vendor-Specific.

- Một Access-Request bây giờ yêu cầu chứa NAS-IP-Address hoặc

NAS-Identifier (hoặc có thể chứa cả hai).

- Thêm ghi chú dưới "Operations" với nhiều thông tin hơn về proxy,

truyền lại, và duy trì kết nối.

- Nếu nhiều thuộc tính với các loại tương tự có mặt đồng thời, thứ tự

các thuộc tính cùng loại phải được duy trì bởi bất kỳ proxy nào.

- Làm rõ Proxy-State.
- Làm rõ các thuộc tính không phải phụ thuộc vào vị trí trong gói tin,

miễn là thuộc tính của các loại tương tự đang được giữ theo thứ tự.

- Thêm vào phần lời khuyên của IANA.

- Cập nhật phần "Proxy" trong "Operations".
- Framed-MTU có thể được gửi trong Access-Request như là một gợi ý.
- Cập nhật lời khuyên bảo mật.
- Các chuỗi văn bản xác định như là một tập hợp con của chuỗi, để làm rõ việc sử dụng UTF-8.

2.1.10.2. RFC 2866

RFC 2866 - RADIUS Accounting: mô tả về quá trình kế toán cho máy chủ RADIUS và là bản cập nhật cho RFC 2865.

Cũng như RFC 2865, RFC 2866 cũng giới thiệu về các gói tin được dùng trong quá trình kế toán và các thuộc tính trong các gói tin đó và cũng mô tả về quá trình kế toán được diễn ra khi có yêu cầu thực hiện kế toán.

Một số thay đổi so với RFC 2139:

- Thay thế US-ASCII bằng UTF-8.
- Thêm ghi chú trong Proxy.
- Framed-IP-Address nên chứa địa chỉ IP thực tế của người sử dụng.
- Nếu Acct-Session-ID đã được gửi trong một Access-Request, nó

phải được sử dụng trong Accounting-Request cho phiên giao dịch đó.

- Các giá trị mới được thêm vào Acct-Status-Type.
- Thêm vào phần lời khuyên của IANA.
- Cập nhật tài liệu tham khảo.

Các chuỗi văn bản xác định như là một tập hợp con của chuỗi, để làm rõ việc sử dụng UTF-8.

2.1.10.3. RFC 2867

RFC 2867 - RADIUS Accounting Modifications for Tunnel Protocol Support: mô tả về việc cải biến cơ chế RADIUS Accounting để hỗ trợ cho giao thức đường hầm, cập nhật thêm cho RFC 2866.

Nhiều ứng dụng giao thức đường hầm như là PPTP và L2TP bao hàm truy cập mạng quay số. Một số, như là việc cung cấp truy cập an toàn cho mạng nội bộ công ty thông qua mạng Internet, được đặc trưng bởi đường hầm chủ động: đường hầm được tạo ra theo yêu cầu của người sử dụng cho một mục đích cụ thể.

Các ứng dụng khác gồm các đường hầm bắt buộc: đường hầm được tạo ra mà không có bất kỳ hành động từ người sử dụng và không có bất kỳ sự lựa

chọn cho phép người dùng trong vấn đề này, như một dịch vụ của nhà cung cấp dịch vụ Internet (ISP).

Thông thường, các ISP cung cấp một dịch vụ muốn thu thập dữ liệu về để thanh toán, quy hoạch mạng... Một cách để thu thập dữ liệu sử dụng trong các mạng quay số là dùng phương tiện RADIUS Accounting. Việc sử dụng RADIUS Accounting cho phép dữ liệu sử dụng quay số được thu thập tại một vị trí trung tâm, hơn là được lưu trữ tại mỗi NAS.

Để thu thập dữ liệu sử dụng về đường hầm, thuộc tính RADIUS mới là cần thiết, tài liệu này xác định những thuộc tính này. Ngoài ra, một số giá trị mới cho các thuộc tính Acct-Status-Type được đề xuất. Kiến nghị cụ thể và ví dụ về việc áp dụng các thuộc tính này cho giao thức L2TP được mô tả trong RFC 2809.

Các giá trị Acct-Status-Type mới:

- Tunnel-Start: giá trị là 9, dùng để đánh dấu việc tạo một đường hầm mới với nút khác.
- Tunnel-Stop: giá trị là 10, , dùng để đánh dấu việc hủy một đường hầm từ hoặc tới nút khác.
- Tunnel-Reject: giá trị là 11, , dùng để đánh dấu việc từ chối tạo một đường hầm với nút khác.
- Tunnel-Link-Start: giá trị là 12, dùng để đánh dấu sự tạo thành của một liên kết đường hầm.
- Tunnel-Link-Stop: giá trị là 13, dùng để đánh dấu sự phá hủy một liên kết đường hầm.
- Tunnel-Link-Reject: giá trị là 14, dùng để đánh dấu việc từ chối tạo nên một liên kết mới trong một đường hầm đang tồn tại.

Và 2 thuộc tính mới:

- Acct-Tunnel-Connection: Thuộc tính này có thể được sử dụng để cung cấp một phương tiện để nhận diện ra một phiên đường hầm cho mục đích kiểm toán.
- Acct-Tunnel-Packets-Lost: Thuộc tính này chỉ ra số gói dữ liệu bị mất trên một liên kết được đưa.

2.1.10.4. RFC 2868

RFC 2868 - RADIUS Attributes for Tunnel Protocol Support: mô tả các thuộc tính RADIUS hỗ trợ cho giao thức đường ống, cập nhật thêm cho RFC 2865.

Các thuộc tính RADIUS mới là cần thiết để chuyển các thông tin đường hầm từ máy chủ RADIUS tới điểm cuối của đường hầm.

Các thuộc tính mới:

- Tunnel-Type: Thuộc tính này chỉ ra giao thức đường hầm sẽ được sử dụng hoặc các giao thức đường hầm đang được sử dụng.
- Tunnel-Medium-Type: Thuộc tính này chỉ ra phương tiện được sử dụng để tạo đường hầm theo các giao thức (như là L2TP), điều này có thể có tác dụng trên nhiều phương tiện vận chuyển.
- Tunnel-Client-Endpoint: Thuộc tính này chứa địa chỉ của người khởi xướng cuối của đường hầm.
- Tunnel-Server-Endpoint: Thuộc tính này chứa địa chỉ của máy chủ cuối của đường hầm.
- Tunnel-Password: Thuộc tính này chứa mật khẩu dùng để xác thực tới máy chủ truy cập từ xa.
- Tunnel-Private-Group-ID: Thuộc tính này chỉ ra ID nhóm cho một phiên hầm cụ thể.
- Tunnel-Assignment-ID: Thuộc tính này được sử dụng để chỉ ra người khởi xướng đường hầm một đường hầm cụ thể để phân công một phiên.
- Tunnel-Preference: Khi máy chủ RADIUS gửi trả nhiều hơn một bộ thuộc tính đường hầm về cho người khởi xướng đường hầm, thuộc tính này được gán vào trong mỗi bộ thuộc tính đường hầm để thiết lập độ ưu tiên cho mỗi đường hầm.
- Tunnel-Client-Auth-ID: Thuộc tính này ghi rõ tên người khởi xướng đường hầm sử dụng trong giai đoạn xác nhận khởi tạo đường hầm.
- Tunnel-Server-Auth-ID: Thuộc tính này ghi rõ tên người tận cùng đường hầm sử dụng trong giai đoạn xác nhận khởi tạo đường hầm

2.1.10.5. RFC 2869

RFC 2869 – RADIUS Extensions: đưa ra gợi ý về một số thuộc tính bổ sung có thể được thêm vào RADIUS để thực hiện nhiều chức năng hữu ích khác nhau. Những thuộc tính không có trường mở rộng trải qua trước đó được nêu ra và do đó bị coi là thử nghiệm.

Extensible Authentication Protocol (EAP) là một phần mở rộng PPP cung cấp hỗ trợ cho các phương pháp xác thực bổ sung bên trong PPP. RFC này mô tả cách mà thuộc tính EAP-Message và Message-Authenticator được sử dụng để cung cấp EAP hỗ trợ bên trong RADIUS.

Tất cả các thuộc tính được bao gồm chiều dài biến Type-Length-Value 3-tuples. Giá trị thuộc tính mới có thể được thêm vào mà không lo ngại làm xáo trộn triển khai hiện có của giao thức.

CHƯƠNG 3. KẾT QUẢ THỰC NGHIỆM

3.1.MỤC ĐÍCH THỰC HIỆN ĐỀ TÀI

Xuất phát từ những lợi ích của VPN như tính linh động, thuận tiện...cho những người có đặc thù công việc phải đi công tác xa và cần dữ liệu phải quay VPN về công ty. Trong đó vấn đề bảo mật dữ liệu trên đường truyền là rất quan trọng. RADIUS là một trong những phương án chưa phải là tối ưu nhất hiện nay nhưng vẫn đáp ứng được các yêu cầu bảo mật cũng như phù hợp với cơ sở hạ tầng mạng của doanh nghiệp, tổ chức hay các trường đại học ở Việt Nam...

Vì vậy nhóm chúng em chọn đề tài RADIUS để giải quyết bài toán bảo mật dữ liệu trên đường truyền cho kết nối VPN. Với việc tổ chức quản lý người dùng theo các OU, Group được phân quyền và áp dụng các chính sách thích hợp đáp ứng nhu cầu bảo mật dữ liệu truyền đi trên mạng.

Hình 10. MÔ HÌNH CHỨNG THỰC VPN BẰNG RADIUS

3.2. YÊU CẦU HỆ THỐNG

3.2.1. PHẦN CỨNG

- Một máy dùng để triển khai RADIUS Server
- Một máy dùng làm NAS – Network Access Server
- Một máy client dùng quay VPN từ internet vào mạng .

3.2.2. PHẦN MỀM

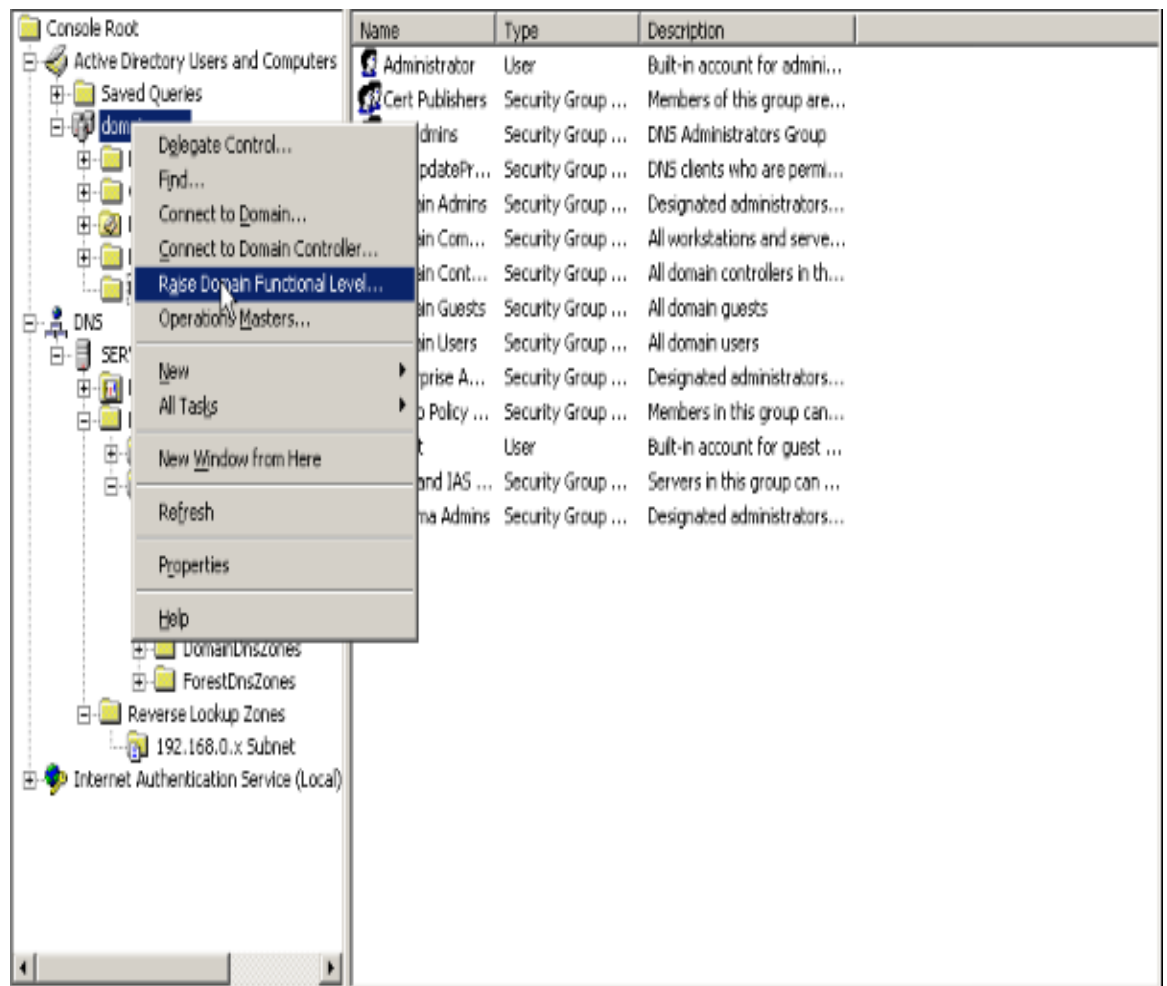
- Trên máy server cài đặt hệ điều hành Windows Server 2003

3.3. QUY TRÌNH TRIỂN KHAI

3.3.1. CÁC BƯỚC THỰC HIỆN TRÊN MÁY AD

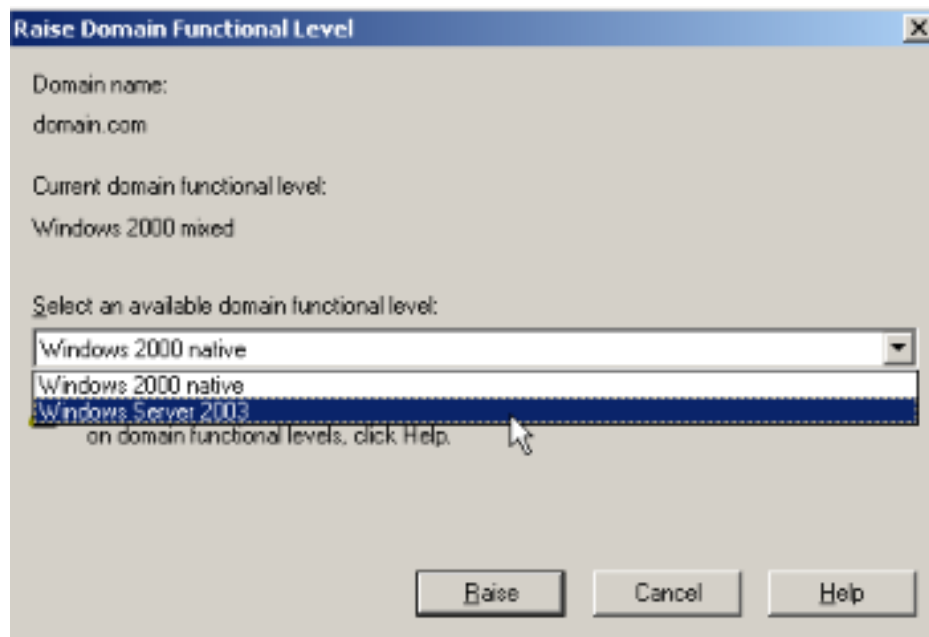
Sau khi lên Active Directory, chúng ta nâng Domain Function level để hỗ trợ cho việc xác thực bằng Radius.

Vào Start > Program > Administrative Tools > Active Directory Users and Computers > Kích chuột phải vào Domain domain.com > chọn Raise Domain Functional Level.

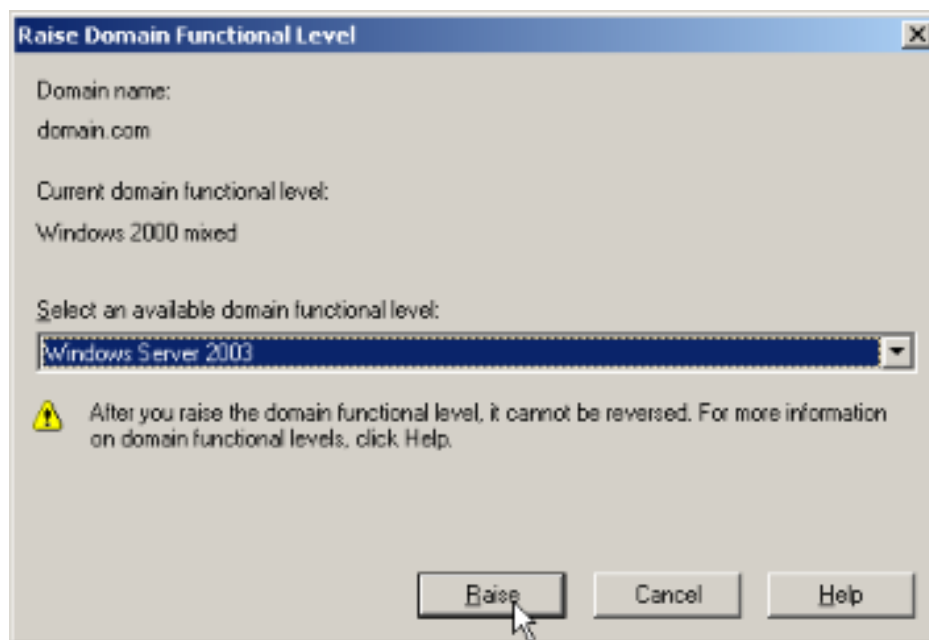


Hình 11. RAISE DOMAIN FUNCTION LEVEL

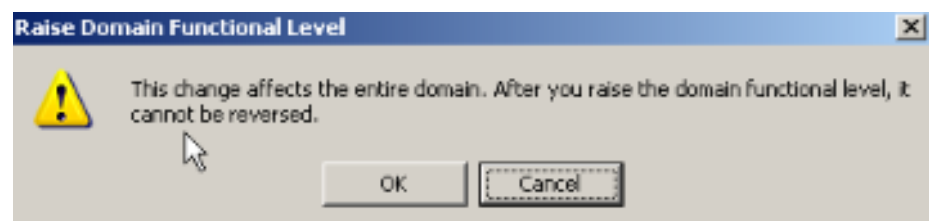
Cửa sổ Raise Domain Functional Level hiện ra ta chọn Windows Server 2003 và OK



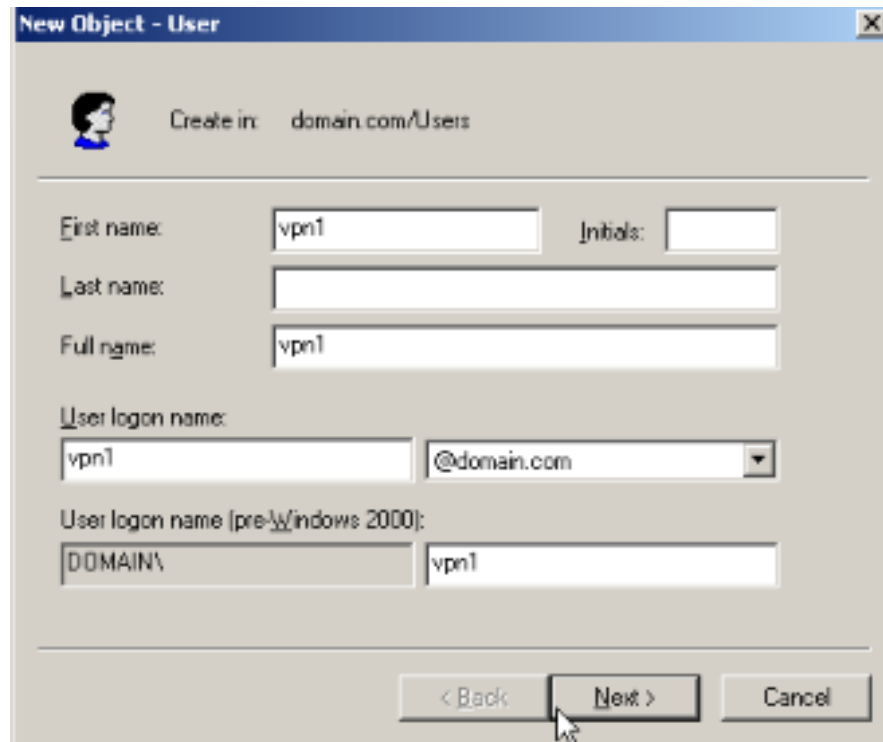
Nhấn nút Raise



Hiện thị thông báo việc thay đổi này sẽ ảnh hưởng đến toàn bộ domain. Sau khi nâng functional level thì domain sẽ không thể chuyển đổi về tình trạng ban đầu.

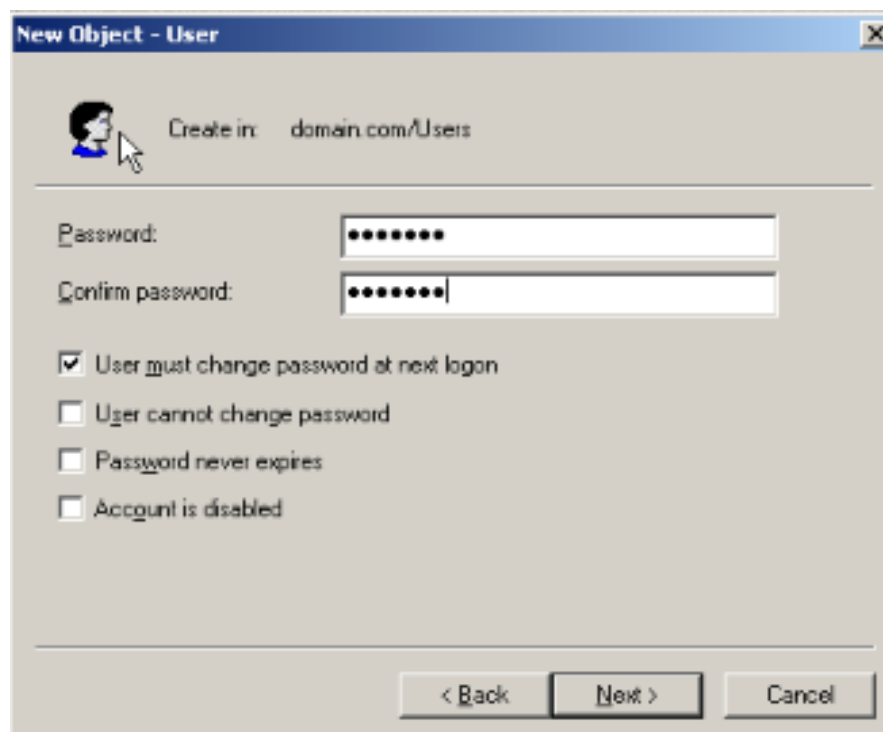


Tạo người dùng vpn1 để cho phép người dùng ở ngoài có thể quay vpn vào hệ thống

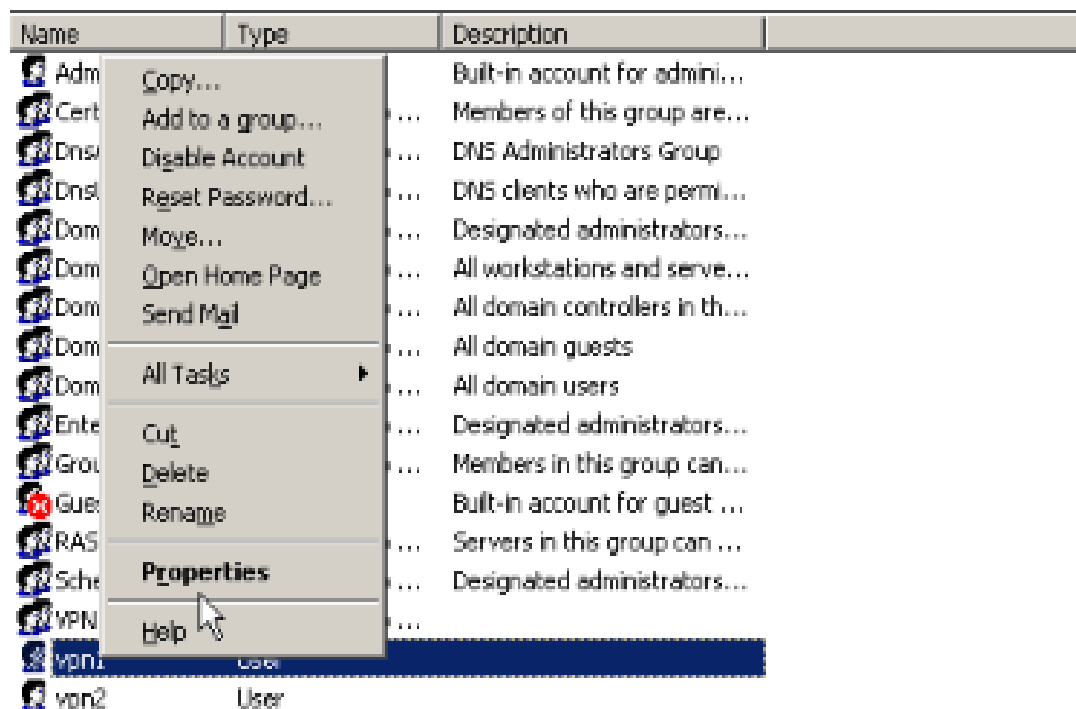


Hình 12. TẠO TÀI KHOẢN NGƯỜI DÙNG VPN

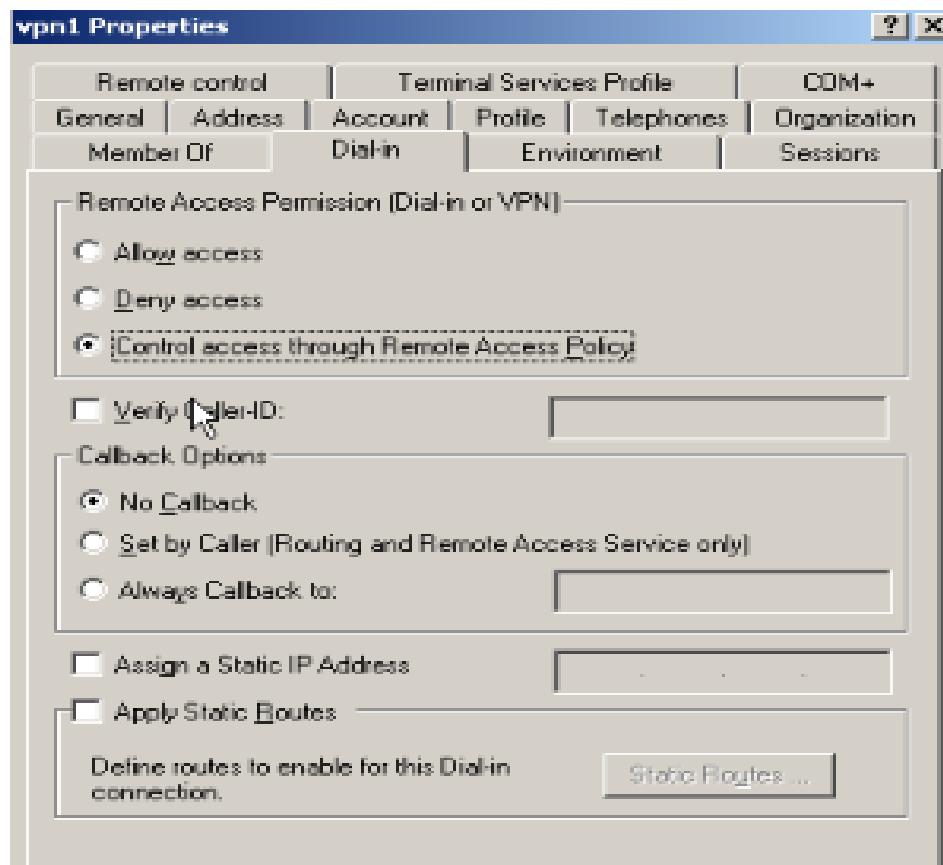
Thiết lập mật khẩu cho người dùng



Tạo người dùng Vpn2 cũng tương tự như việc tạo Vpn1



Sau đó click chuột phải vào từng user chọn properties để thiết lập các thuộc tính cần thiết cho người dùng

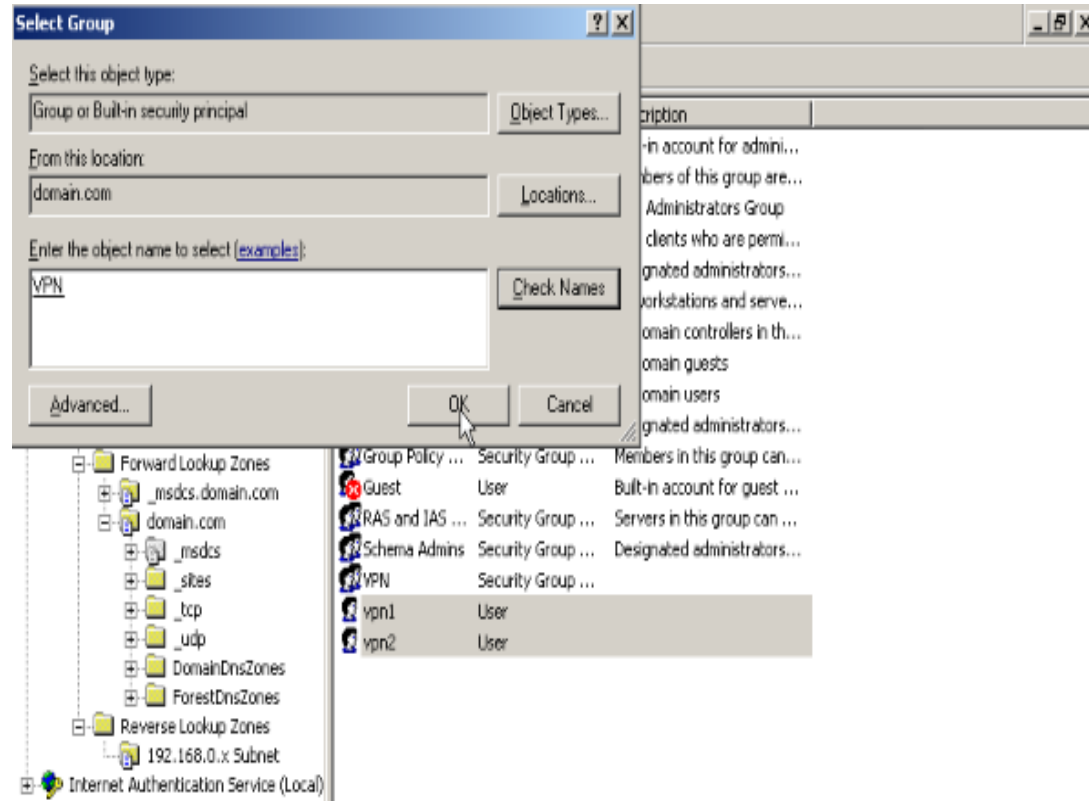


Hình 13. THIẾT LẬP CÁC THUỘC TÍNH CHO NGƯỜI DÙNG VPN

Chọn tab Dial in và check vào dòng Remote Access Permission đó là Chính sách truy cập từ xa thông qua điều khiển truy cập.

User vpn2 làm tương tự như các bước thực hiện với User vpn1

Sau khi cho phép 2 user vpn1, vpn2 thực hiện chính sách truy cập từ xa thông qua điều khiển truy cập. Bước tiếp thêm 2 user vào Group.



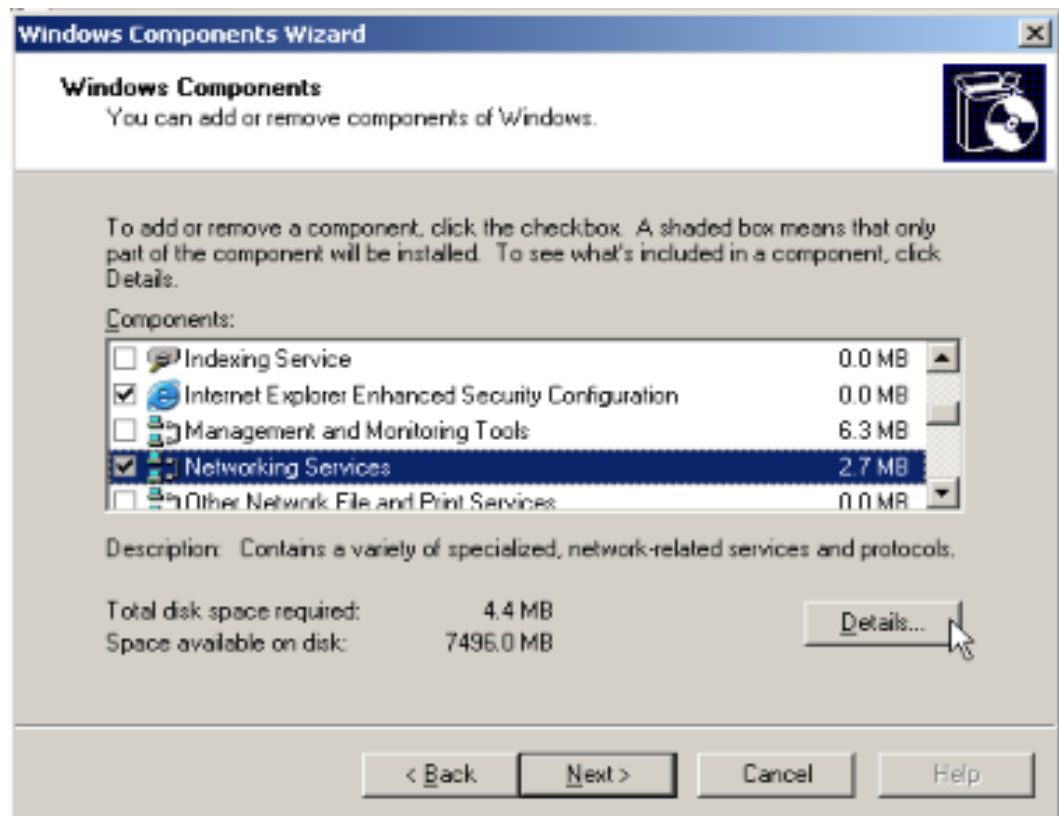
Hình 14. TẠO GROUP NGƯỜI DÙNG VPN



Việc thêm 2 user vào group đã thành công.

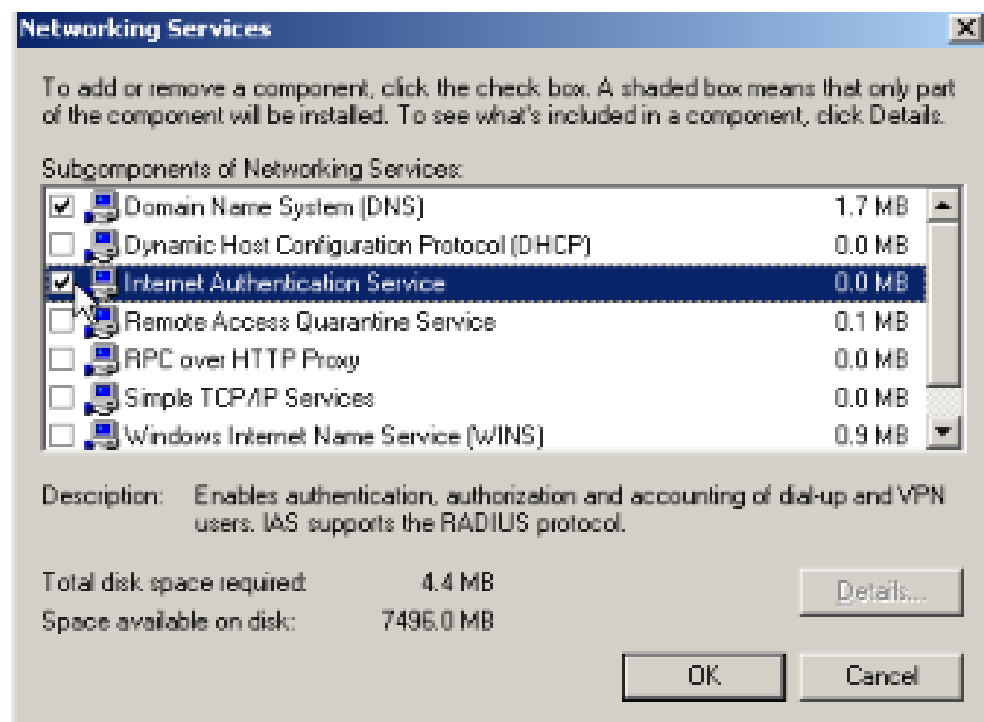
Tiếp tục cài đặt dịch vụ IAS trên Active Directory như sau:

Vào Start > Settings > Control Panel > chọn Add or Remove Programs
> chọn Add/Remove Windows Components

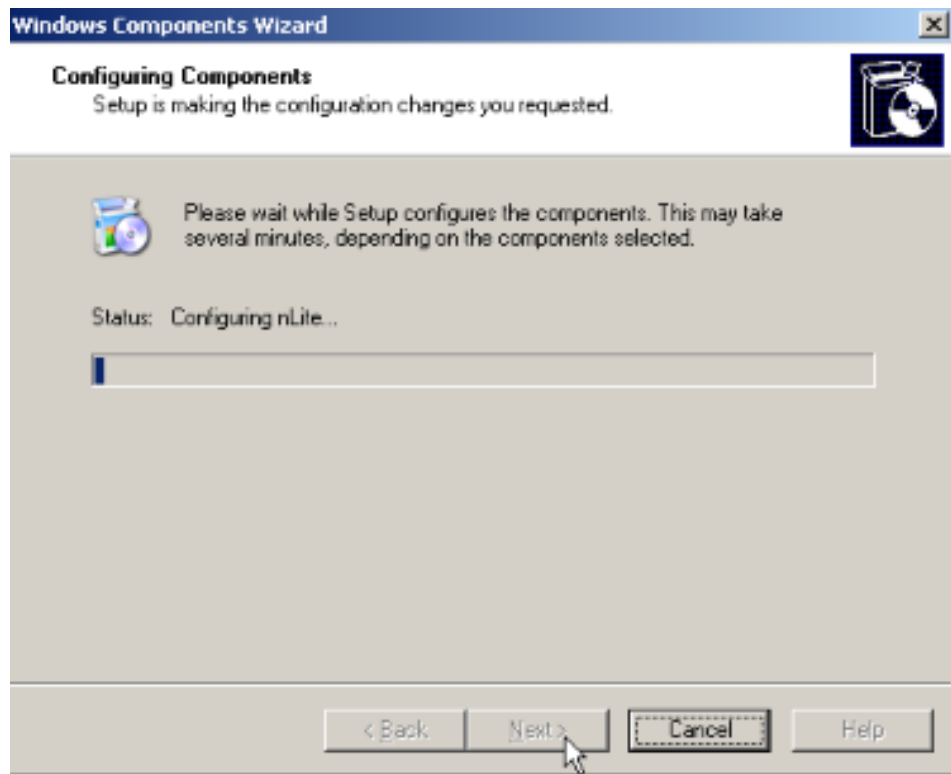


Hình 15. CÀI ĐẶT DỊCH VỤ CHỨNG THỰC - IAS

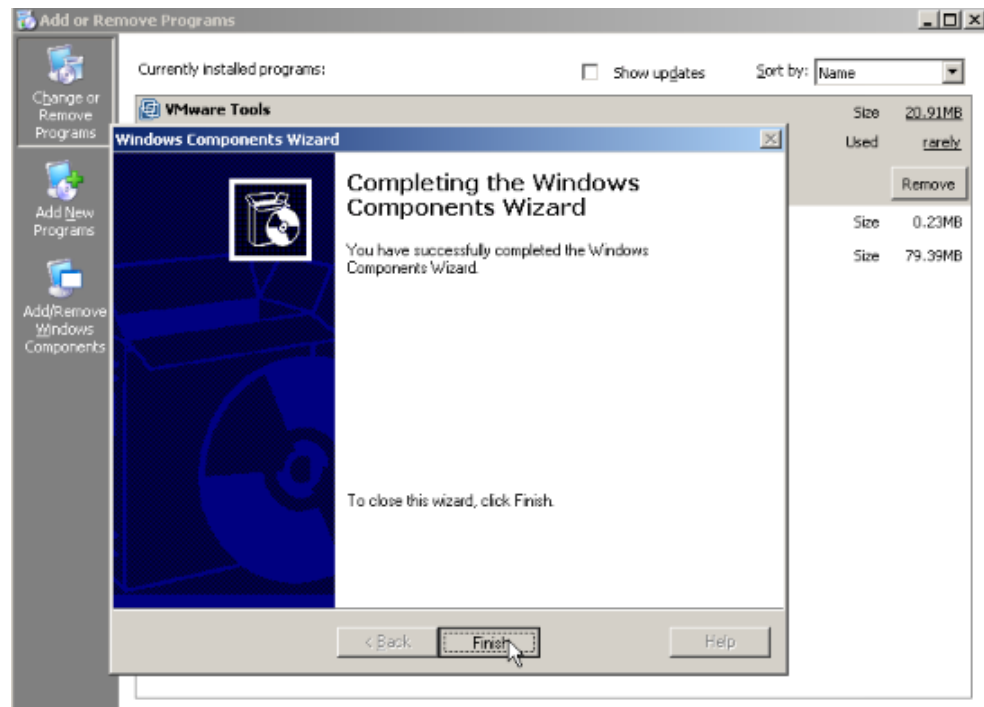
Cửa sổ Windows Components Winzard hiện ra > ta chọn mục Networking Services > chọn Internet Authentication Service > kích OK để tiến hành cài đặt dịch vụ này



Hiển thị quá trình cài đặt thêm các thành phần



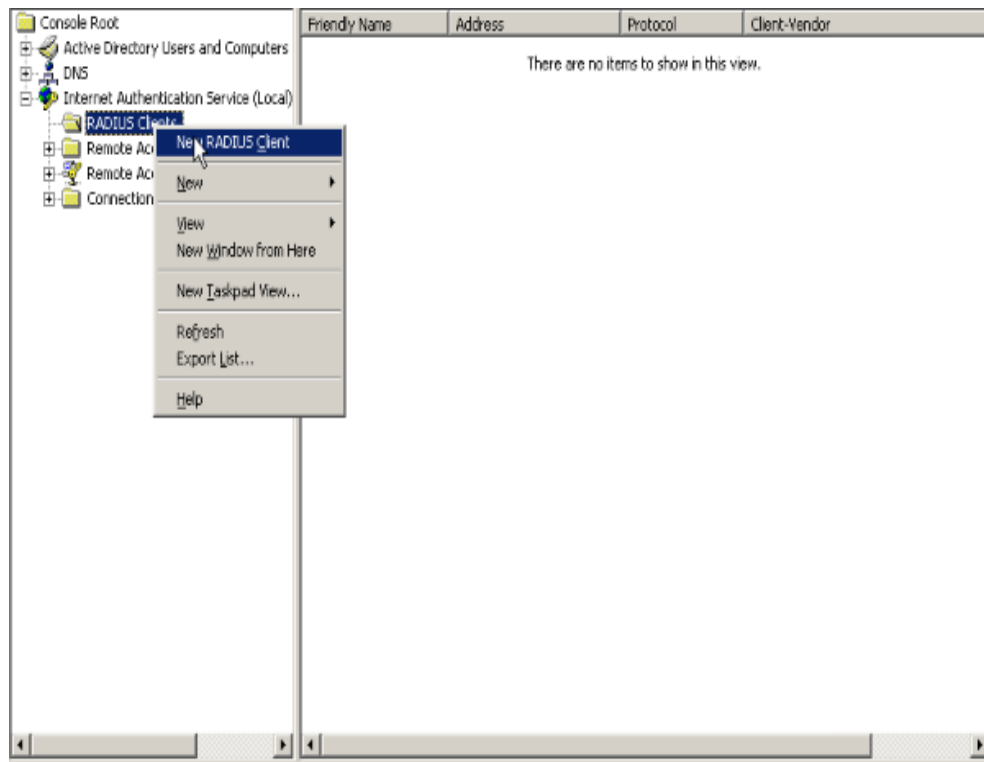
Hoàn tất quá trình cài đặt các thành phần



Sau khi cài đặt xong cửa sổ Internet Authentication Service có giao diện như sau

Tại giao diện Internet Authentication Service

Ta tiến hành tạo Radius Client > kích chuột phải vào Radius Client > chọn New Radius Client



Hình 16. TẠO RADIUS CLIENT

Cửa sổ New Radius Client xuất hiện ta điền các thông tin sau:

Friendly Name : NAS

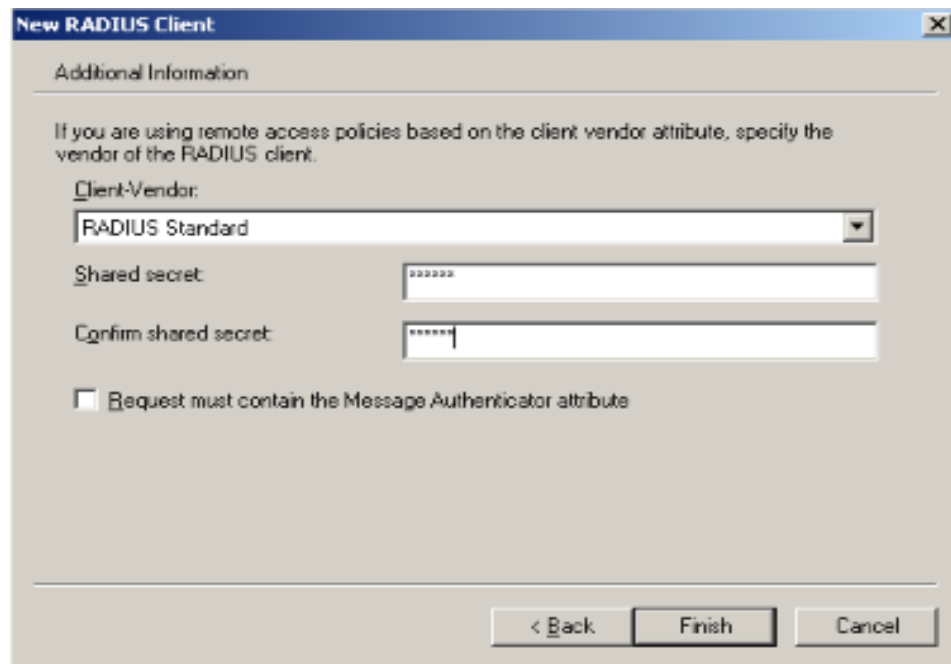
Client address (IP or DNS) : 192.168.0.3 (nhập IP của Server VPN
đường mạng trong) chọn Next

 A screenshot of the 'New RADIUS Client' dialog box. The title bar says 'New RADIUS Client'. The main area is titled 'Name and Address' and contains the instruction: 'Type a friendly name and either an IP Address or DNS name for the client.' There are two input fields: 'Friendly name:' with the text 'NAS' entered, and 'Client address (IP or DNS):' with the text '192.168.0.3' entered. To the right of the second field is a 'Verify...' button. At the bottom of the dialog are three buttons: '< Back', 'Next >', and 'Cancel'.

Cửa sổ Additional Information xuất hiện.

Tại mục Client Vendor chọn Radius Standard

Tại mục Shared secret và Confirm shared secret : ta nhập key vào > chọn Next > và chọn Finish để kết thúc



New RADIUS Client

Additional Information

If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client.

Client-Vendor: RADIUS Standard

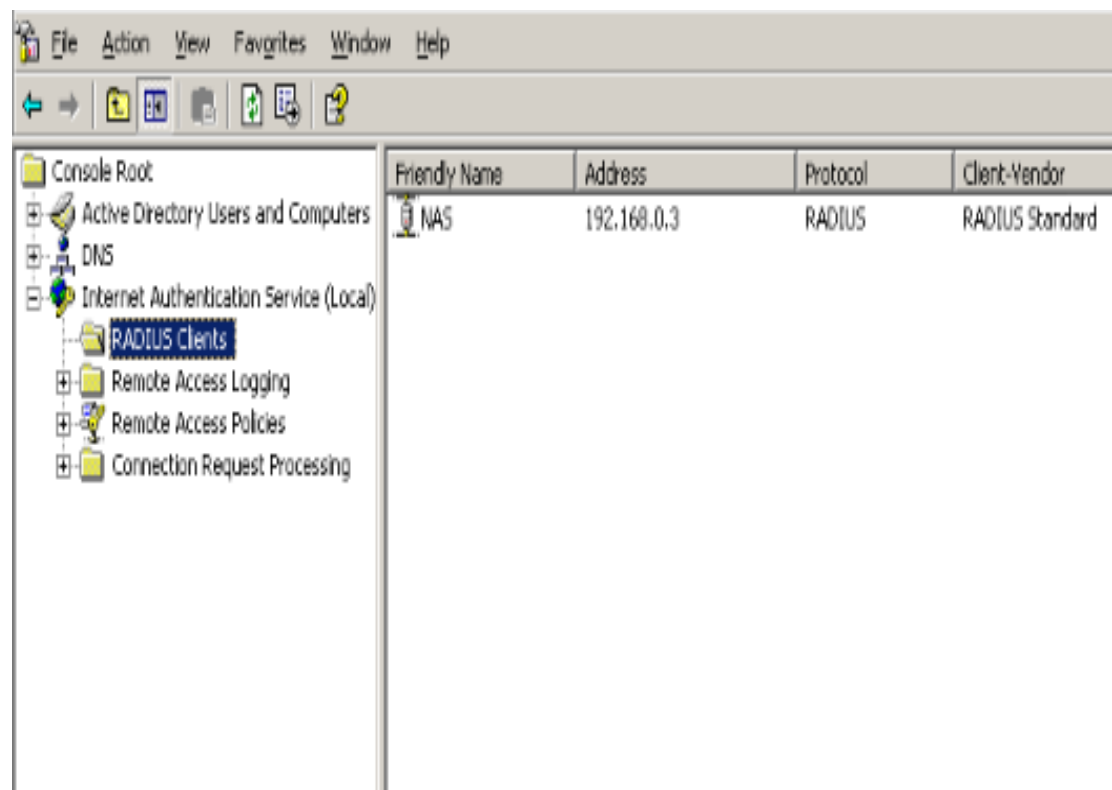
Shared secret: *****

Confirm shared secret: *****

☐ Request must contain the Message Authenticator attribute

< Back Finish Cancel

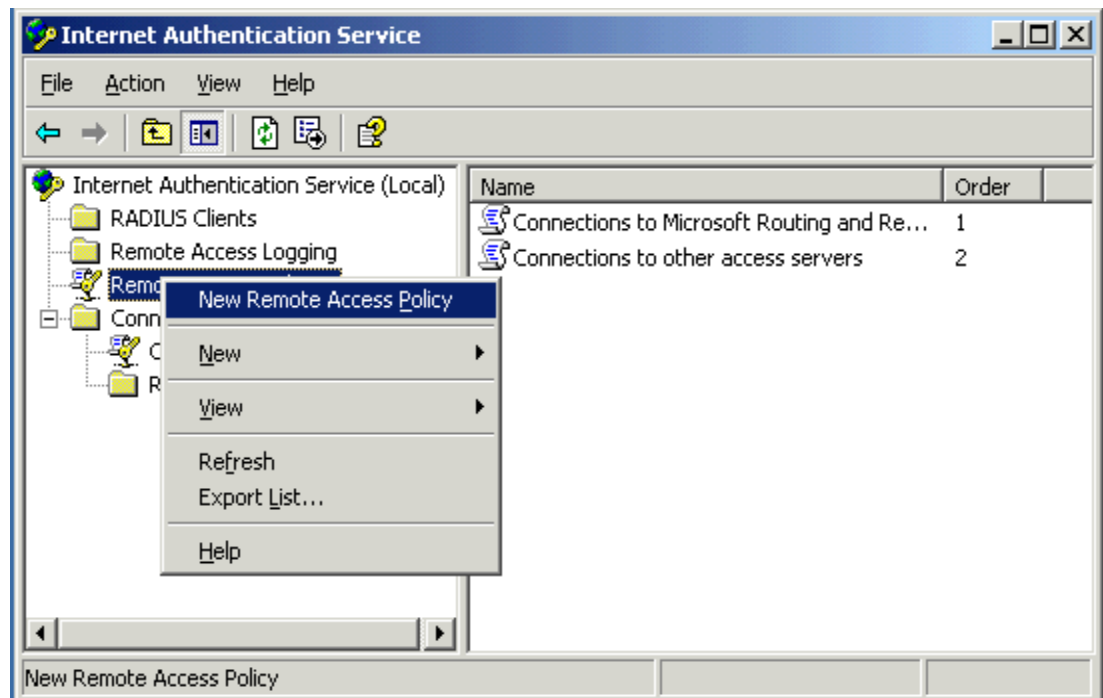
Bảng dưới minh họa Radius Client có tên NAS địa chỉ Ip: 192.168.0.3 đã được tạo thành công.



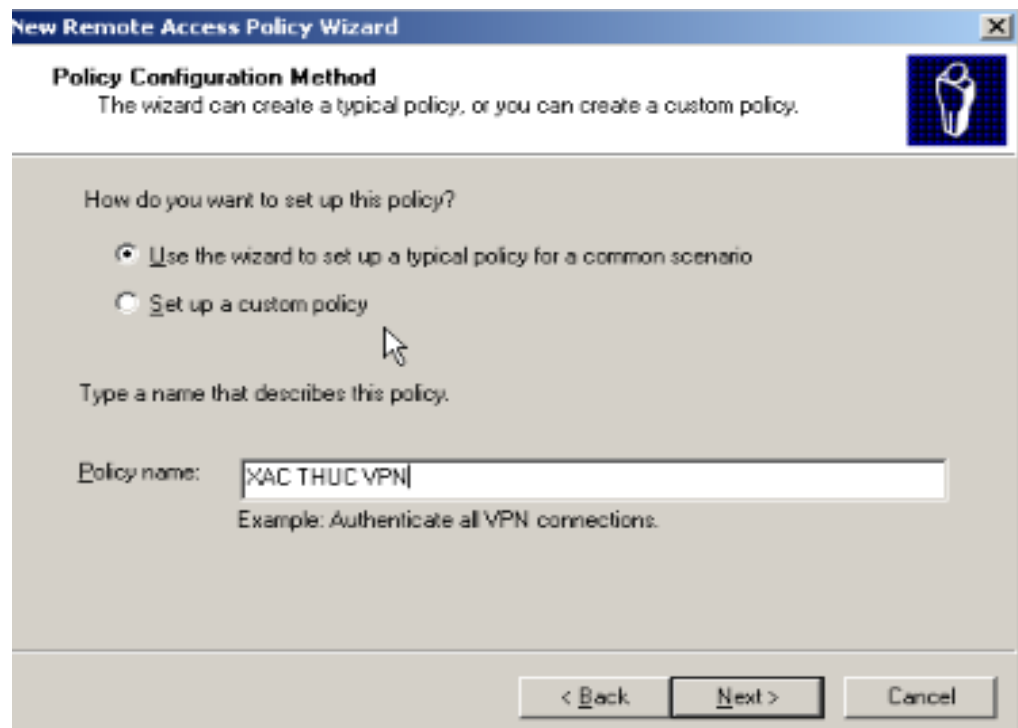
Friendly Name	Address	Protocol	Client-Vendor
NAS	192.168.0.3	RADIUS	RADIUS Standard

Remote Access Policies cho phép chúng ta tạo ra một Policy để cho phép Group hay User được phép truy cập vào thông qua Policy
Tại giao diện Internet Authentication Service

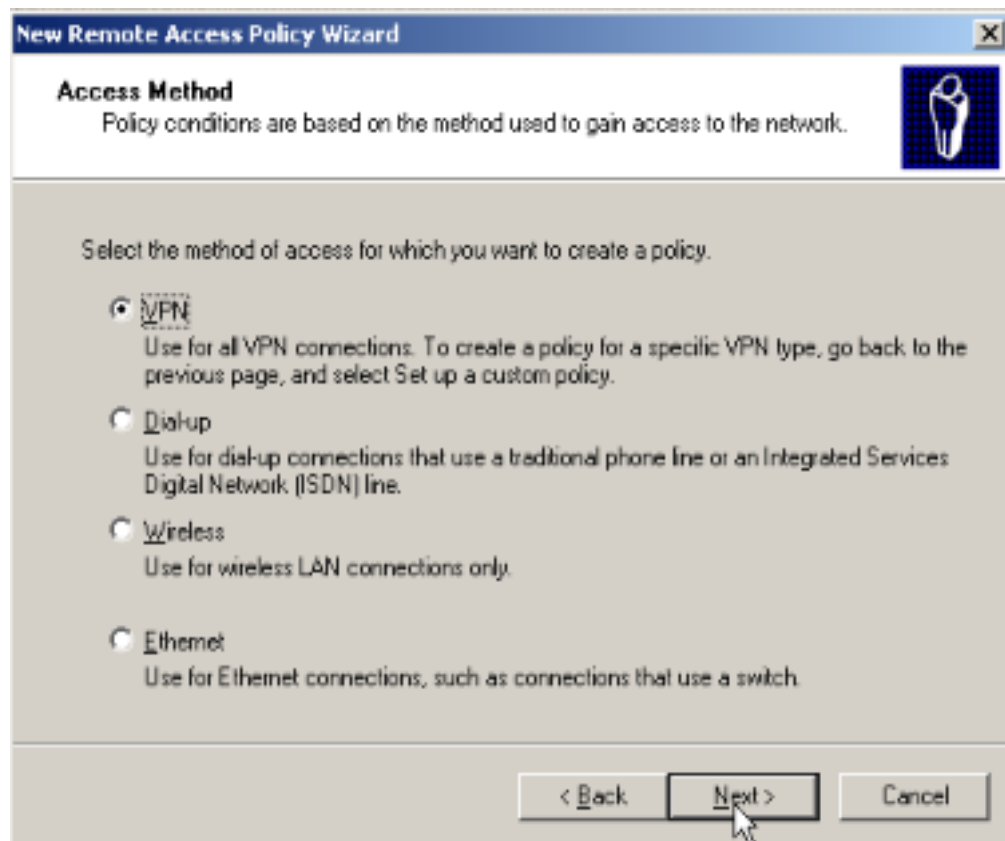
Ta tiến hành tạo Remote Access Policies > chuột phải chọn New Remote Access Policy > chọn Next



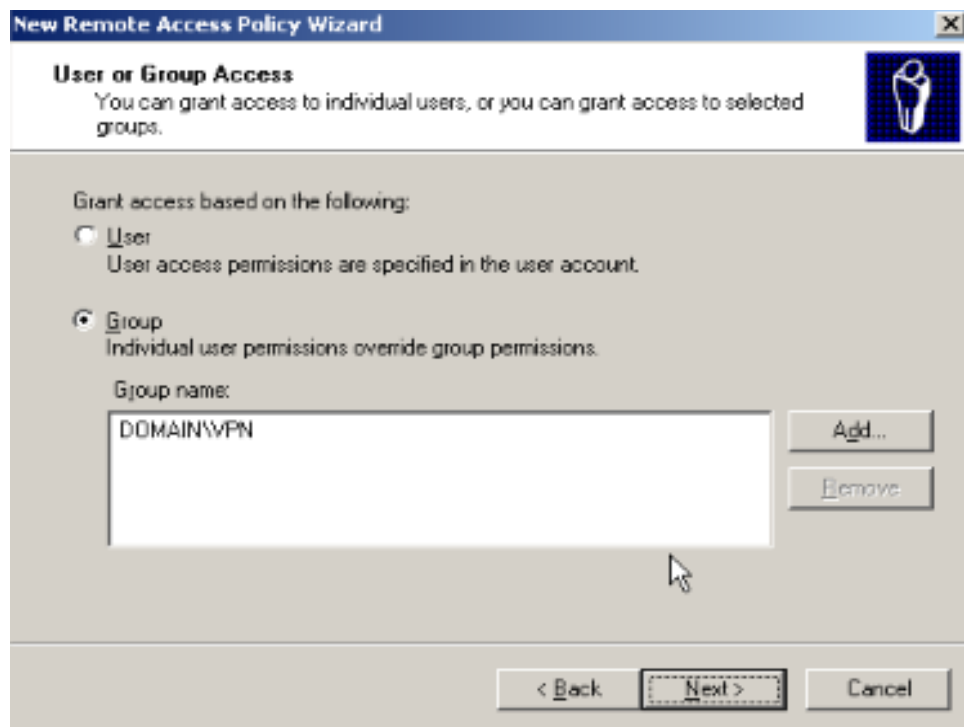
Hình 17. TẠO CHÍNH SÁCH QUẢN LÝ TRUY CẬP TỪ XA
Cửa sổ Policy Configuration Method xuất hiện ta nhập tên vào mục Policy Name > kích Next để tiếp tục



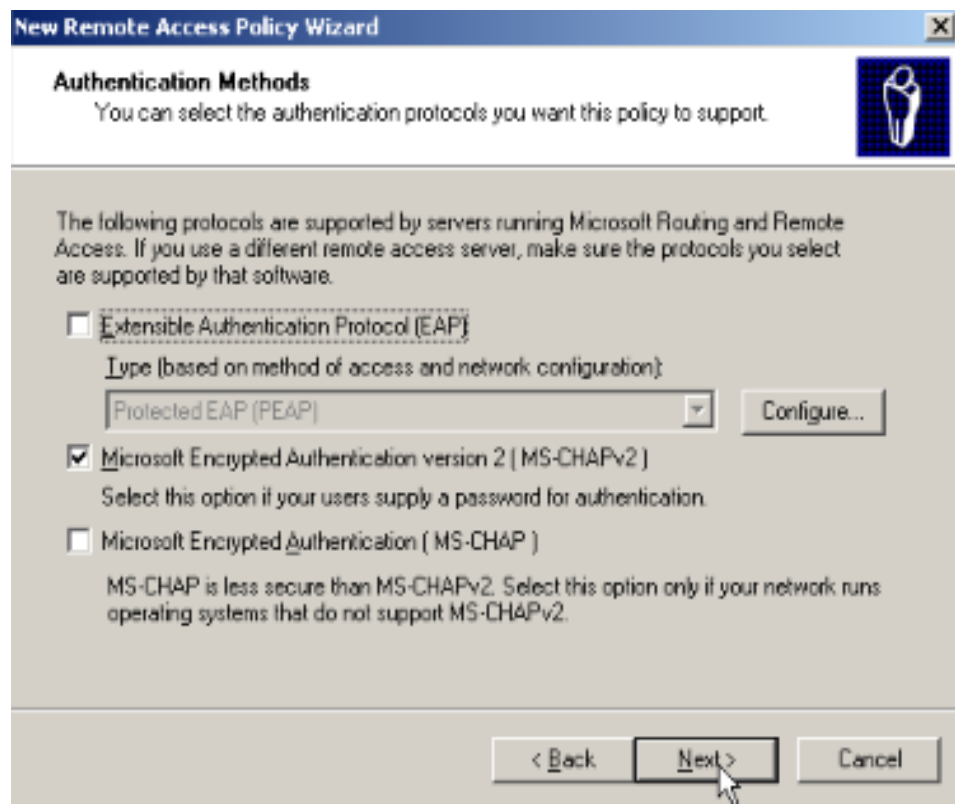
Tại mục Access Method ta chọn kiểu VPN > kích Next để tiếp tục



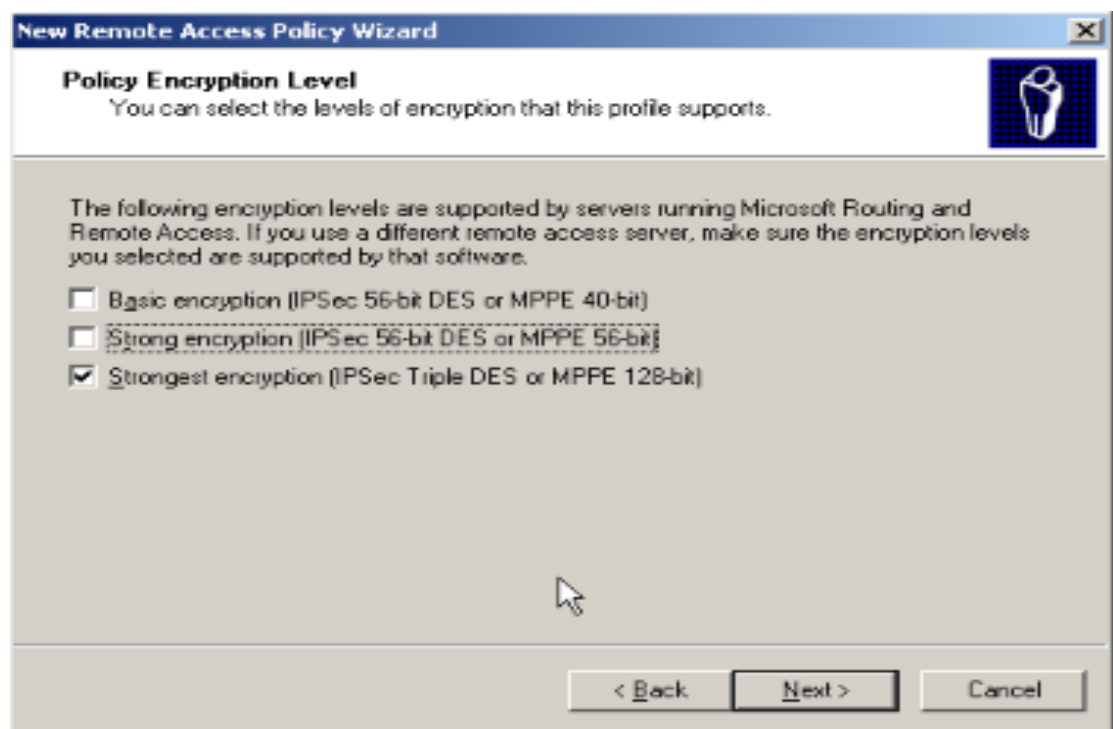
Tại mục User or Group Access ta chọn Group và chọn Add > để Add Group VPN mà chúng ta đã tạo tại Server Domain Controller



Tại mục Authentication Methods chúng ta chọn chứng thực : Microsoft Encrypted Authentication version 2 (MS-CHAPv2) kích Next để tiếp tục

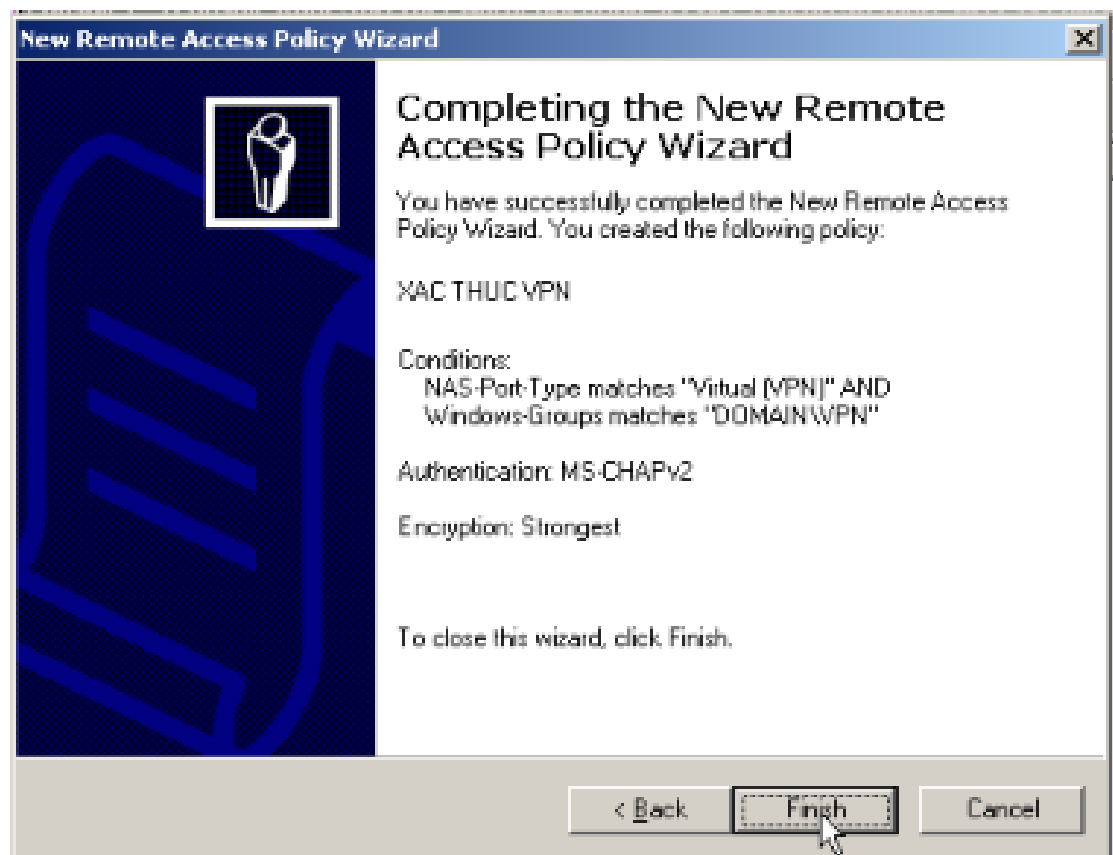


Tại mục Policy Encryption Level ta chọn Strongest Encryption (IPsec Triple DES or MPPE 128bit) kích Next để tiếp tục và hoàn tất quá trình

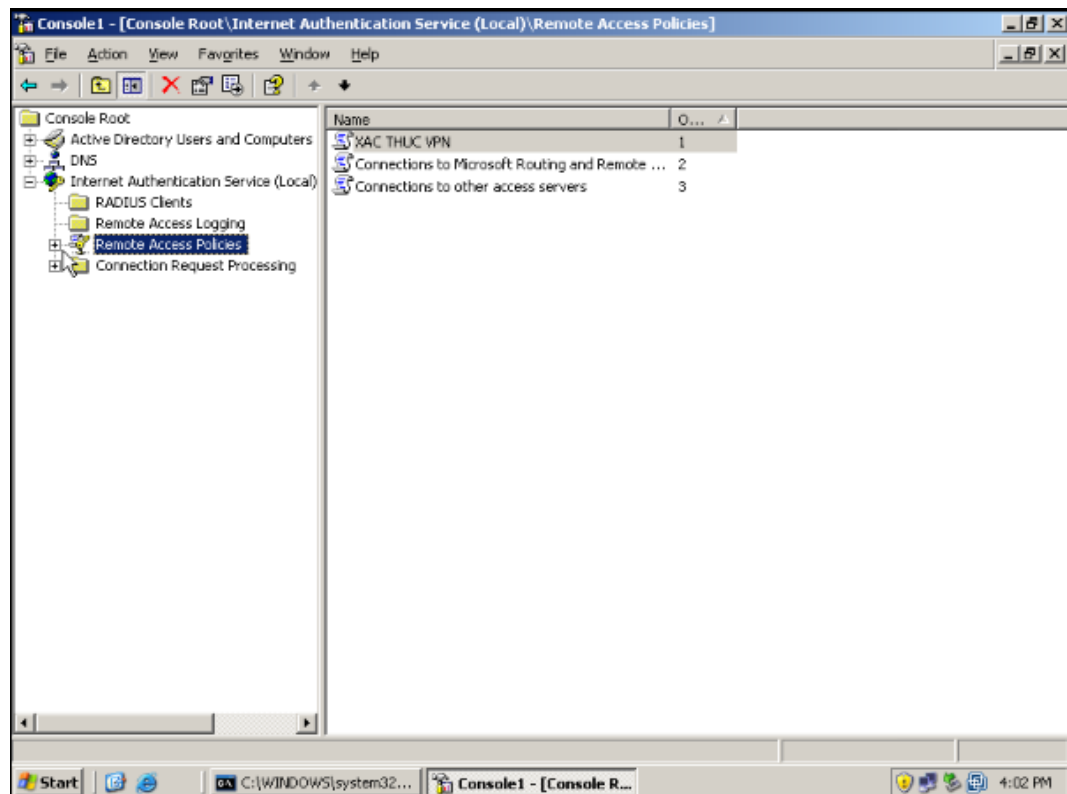


Hình 18. CHỌN PHƯƠNG THỨC MÃ HÓA CHO KẾT NỐI VPN

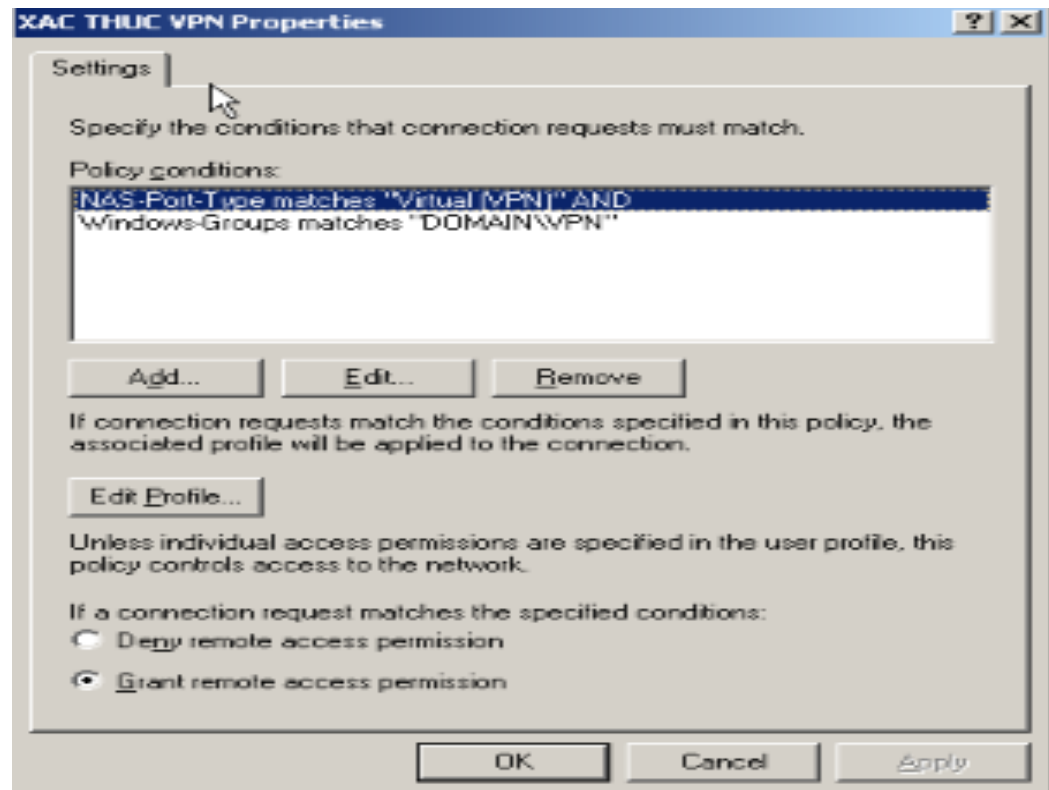
Kích Next để tiếp tục và hoàn tất quá trình tạo Remote Access Policies



Chúng ta tùy chỉnh thêm VPN Site vừa tạo tại Remote Access Policies bằng cách kích chuột phải chọn Properties



Ta chọn Grant remote access permission để sử dụng Remote Access Policies này > Apply và OK



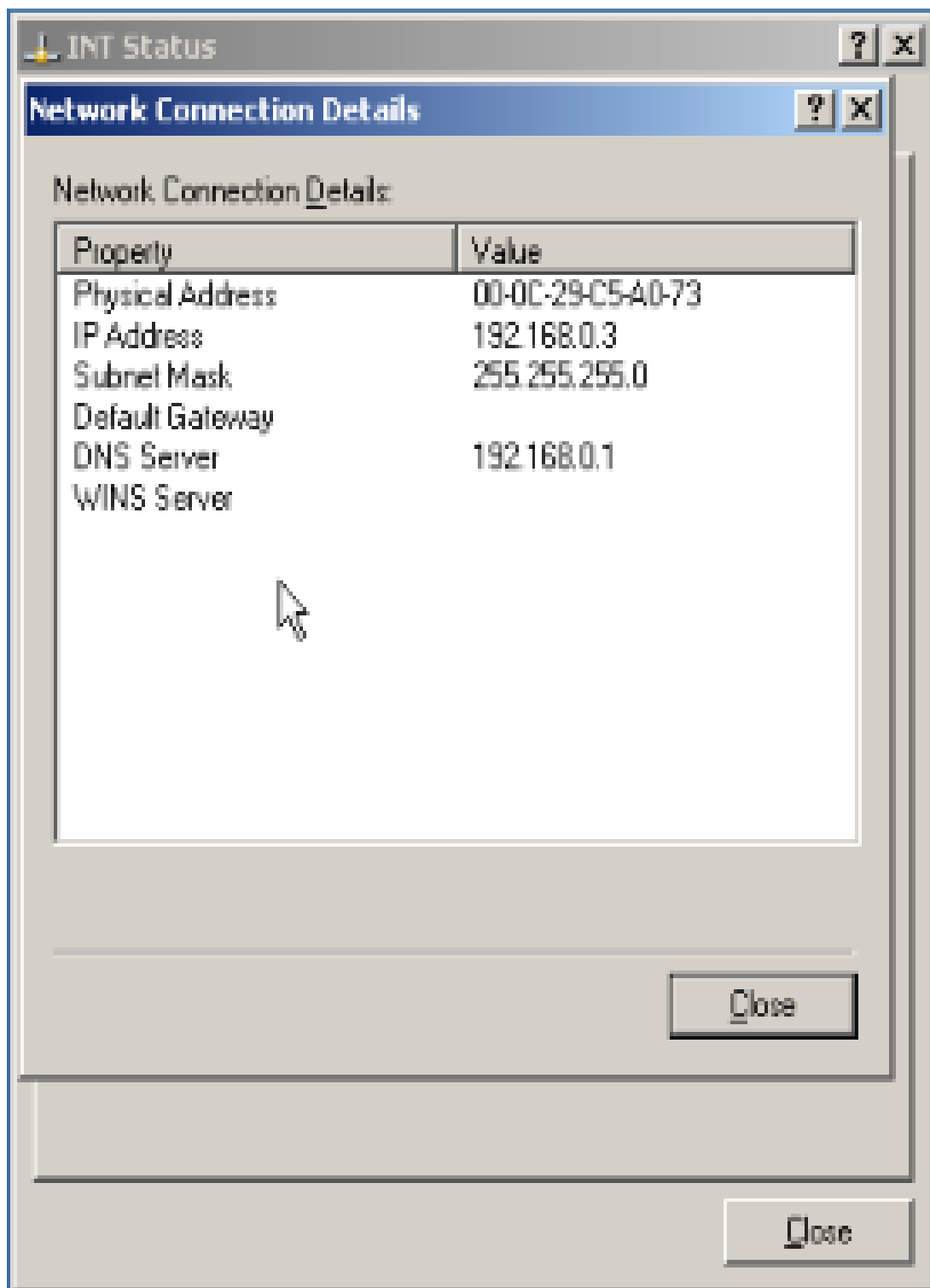
3.3.2. CÁC BƯỚC THỰC HIỆN TRÊN MÁY NAS

Gán địa chỉ Ip cho card mạng bên trong:

Ip: 192.168.0.3

Subnet mask: 255.255.255.0

Dns Server: 192.168.0.1



Hình 19. THIẾT LẬP IP CHO NAS – NETWORK ACCESS SERVER

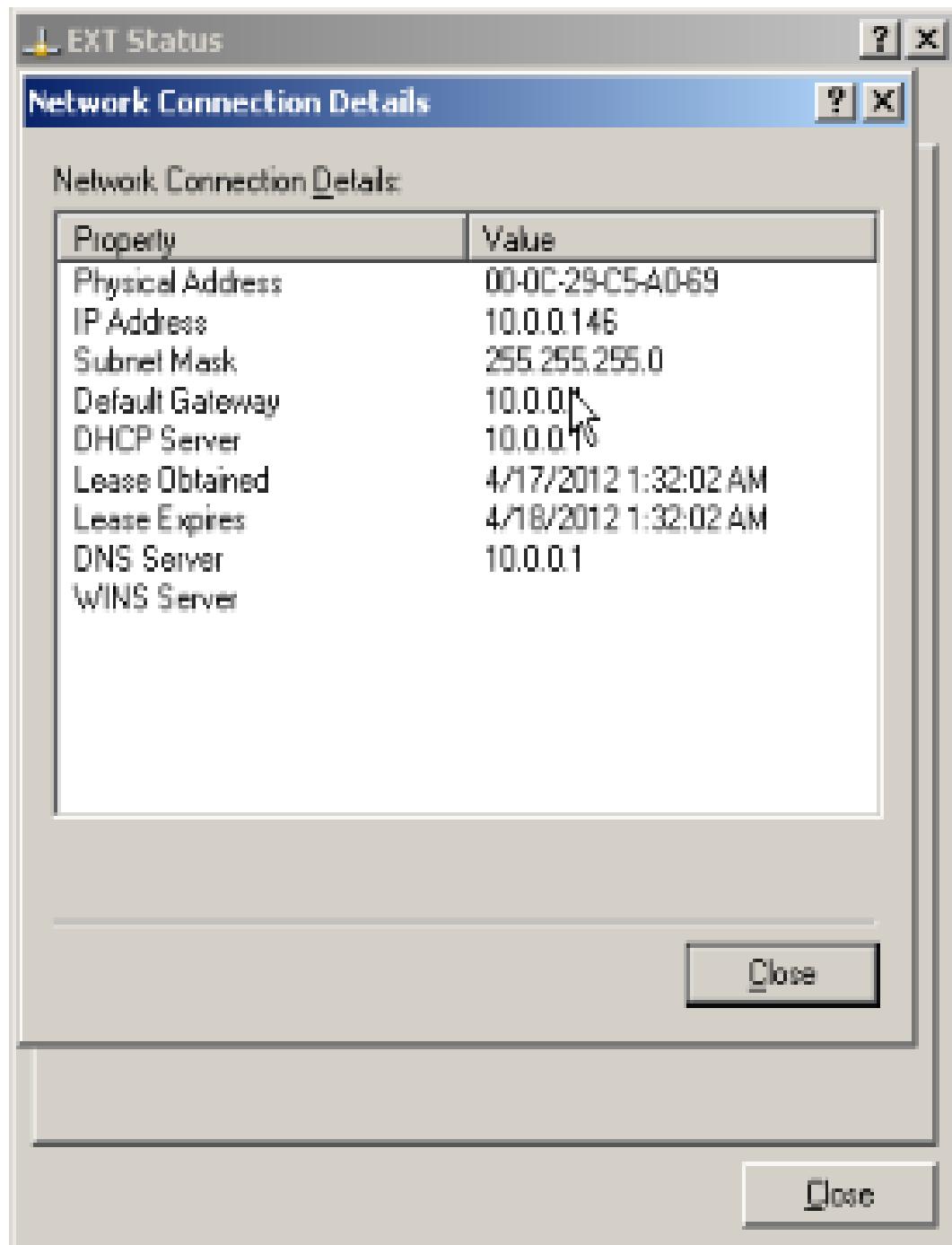
Gán địa chỉ Ip cho card mạng bên ngoài:

Ip: 10.0.0.146

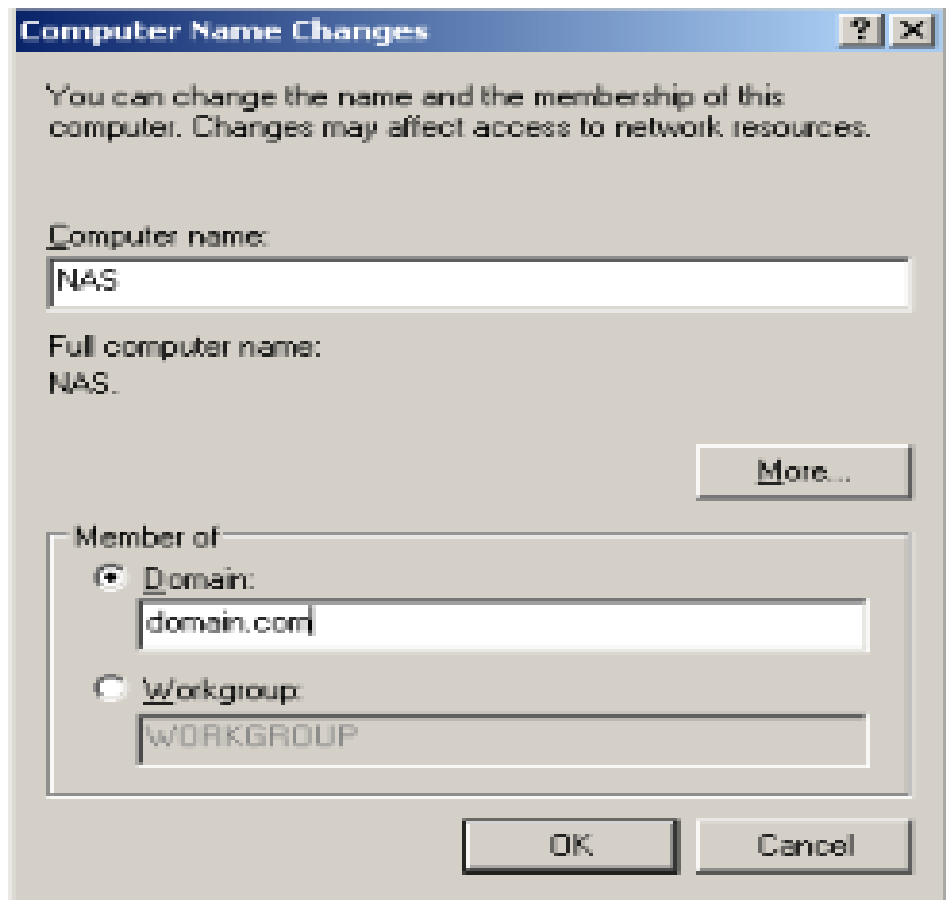
Subnet mask: 255.255.255.0

Default gateway: 10.0.0.1

Dns Server: 10.0.0.1



Click phải Icon My Computer trên chọn Properties – Chọn tab Computer Name – nhập tên domain.com vào member of:



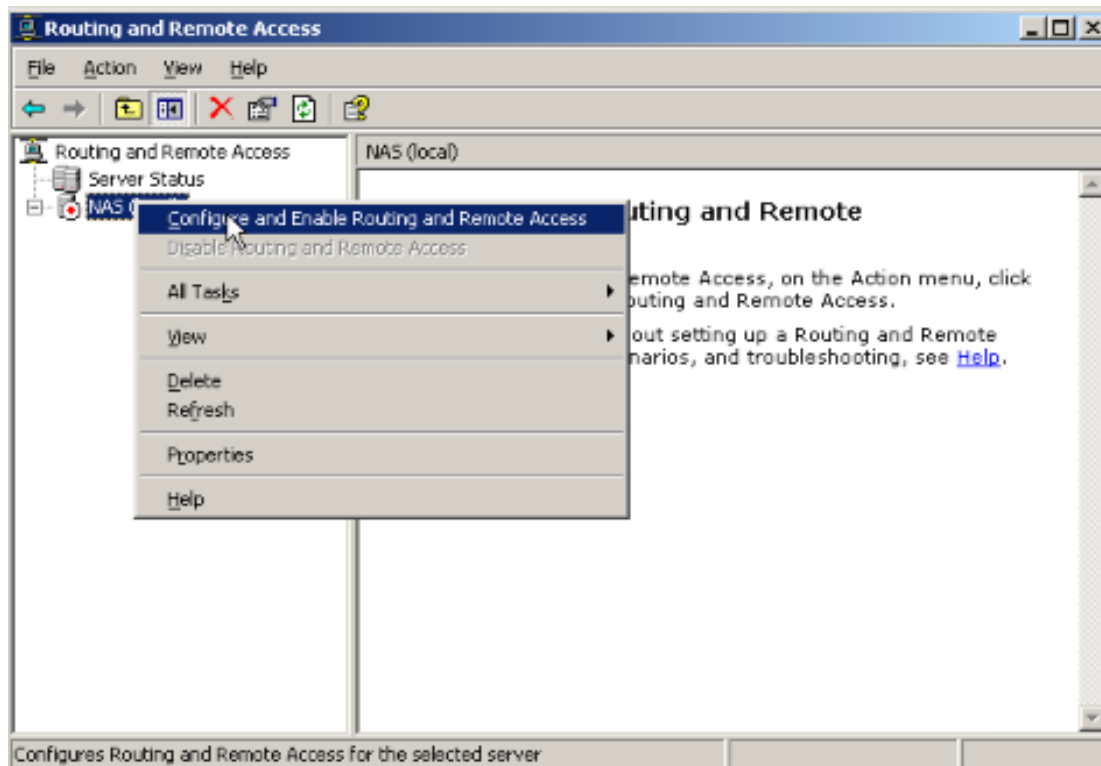
Hình 20. ĐẶT TÊN MÁY NAS

Thiết lập tên cho máy radius Client



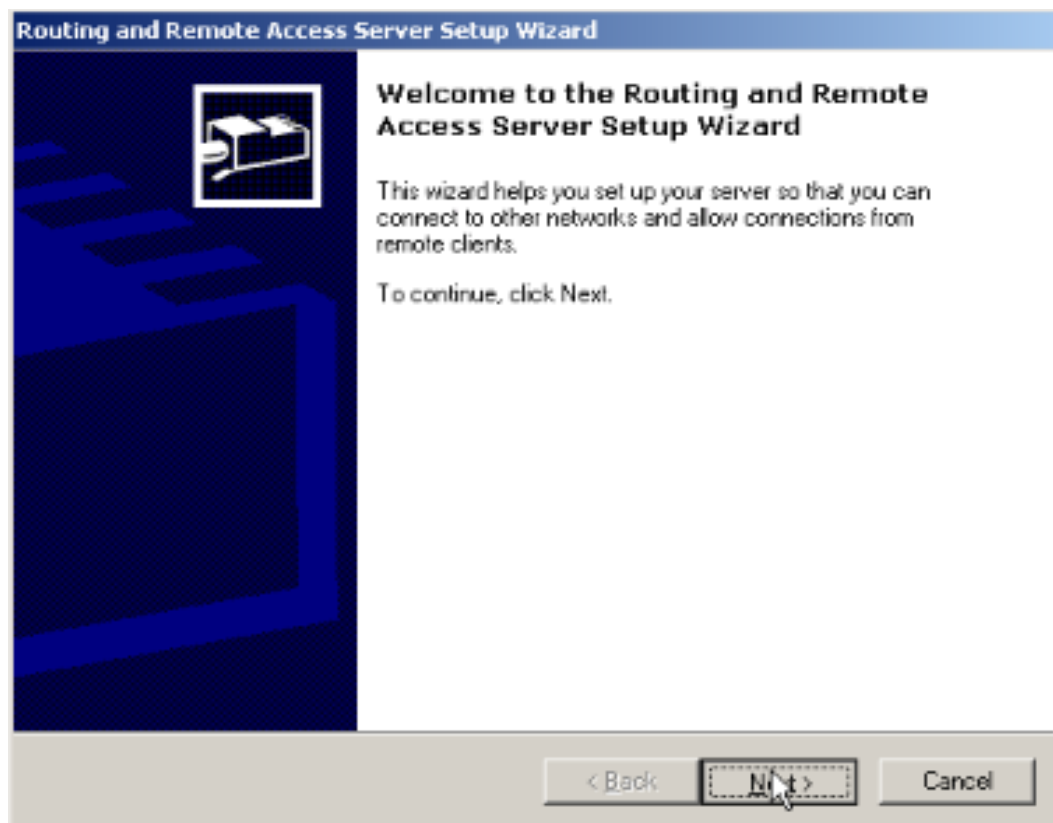
Hệ thống yêu cầu nhập mật khẩu quản trị

Vào Start > Program > Administrative Tools > Routing and Remote Access



Hình 21. CẤU HÌNH VÀ BẬT ROUTING AND REMOTE ACCESS

Right click chọn Configure and Enable Routing and Remote Access



Click Next

Routing and Remote Access Server Setup Wizard

Configuration
You can enable any of the following combinations of services, or you can customize this server.

☒ **Remote access (dial-up or VPN)**
Allow remote clients to connect to this server through either a dial-up connection or a secure Virtual Private Network (VPN) Internet connection.

☐ **Network address translation (NAT)**
Allow internal clients to connect to the Internet using one public IP address.

☐ **Virtual Private Network (VPN) access and NAT**
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.

☐ **Secure connection between two private networks**
Connect this network to a remote network, such as a branch office.

☐ **Custom configuration**
Select any combination of the features available in Routing and Remote Access.

For more information about these options, see [Routing and Remote Access Help](#).

< Back Next > Cancel

Chọn Remote access (dial-up or VPN)

Routing and Remote Access Server Setup Wizard

Remote Access
You can set up this server to receive both dial-up and VPN connections.

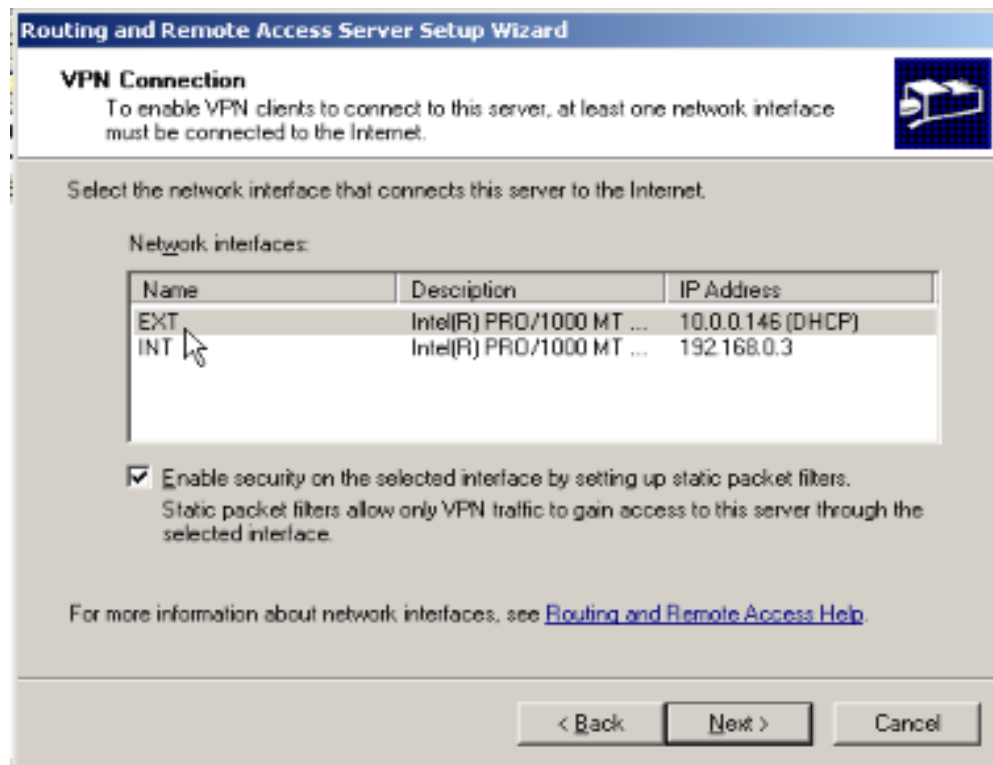
☒ **VPN**
A VPN server (also called a VPN gateway) can receive connections from remote clients through the Internet.

☐ **Dial-up**
A dial-up remote access server can receive connections directly from remote clients through dial-up media, such as a modem.

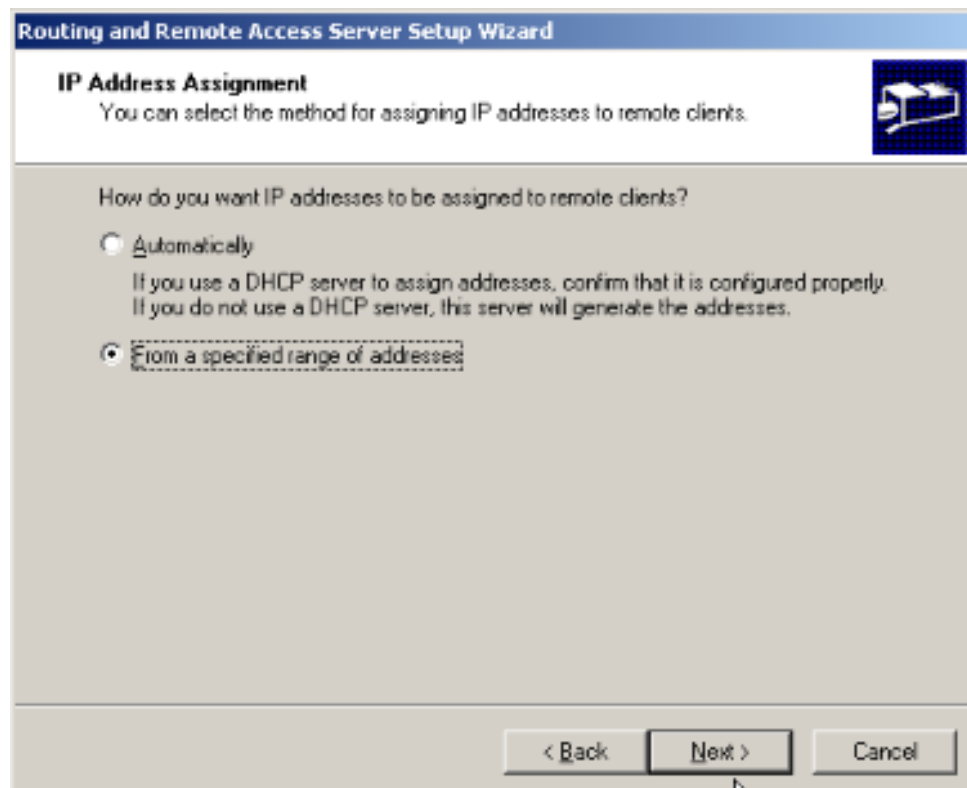
< Back Next > Cancel

Chọn VPN

Tại mục VPN Connection > chọn Card Lan ngoài mạng



Tại mục IP Address Assignment > chọn From a speccified range of addresses



Tại mục Address Range Assignment > kích chọn New

Routing and Remote Access Server Setup Wizard

Address Range Assignment
 You can specify the address ranges that this server will use to assign addresses to remote clients.

Enter the address ranges (static pools) that you want to use. This server will assign all of the addresses in the first range before continuing to the next.

Address ranges:

From	To	Number

New... Edit... Delete

< Back Next > Cancel

Nhập dãy IP để cấp cho User khi quay số từ ngoài vào

Routing and Remote Access Server Setup Wizard

Address Range Assignment
 You can specify the address ranges that this server will use to assign addresses to remote clients.

New Address Range

Type a starting IP address and either an ending IP address or the number of addresses in the range.

Start IP address: 192.168.0.100

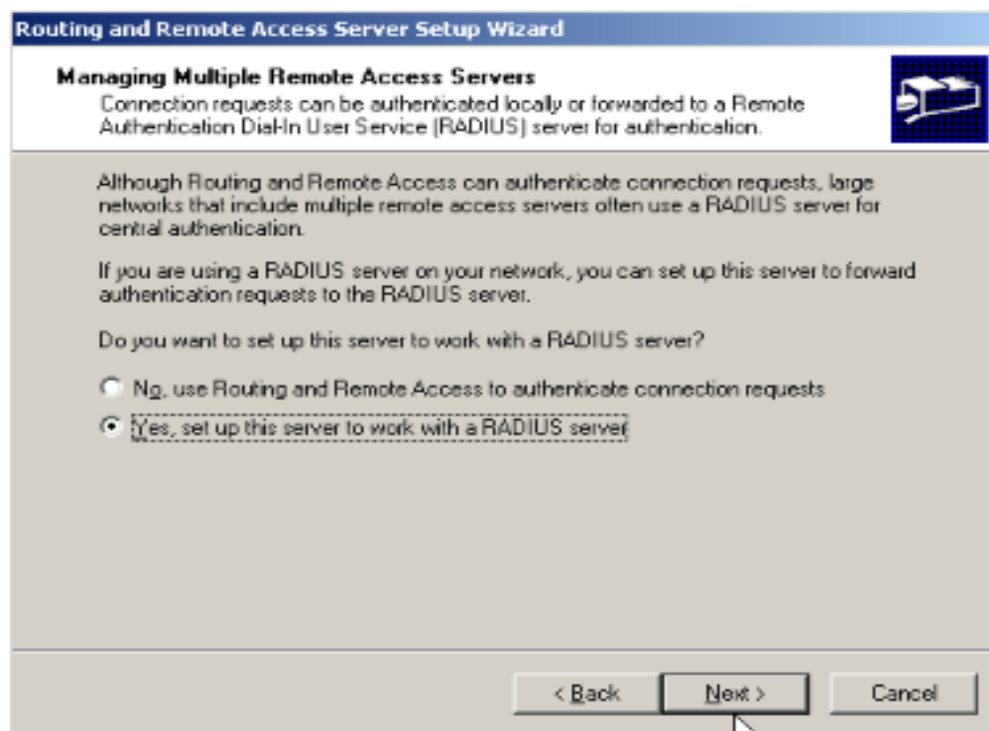
End IP address: 192.168.0.109

Number of addresses: 10

OK Cancel

< Back Next > Cancel

Chọn Yes, set up this server to work with a RADIUS server > Để chúng thực qua máy RADIUS server



Routing and Remote Access Server Setup Wizard

Managing Multiple Remote Access Servers

Connection requests can be authenticated locally or forwarded to a Remote Authentication Dial-In User Service (RADIUS) server for authentication.

Although Routing and Remote Access can authenticate connection requests, large networks that include multiple remote access servers often use a RADIUS server for central authentication.

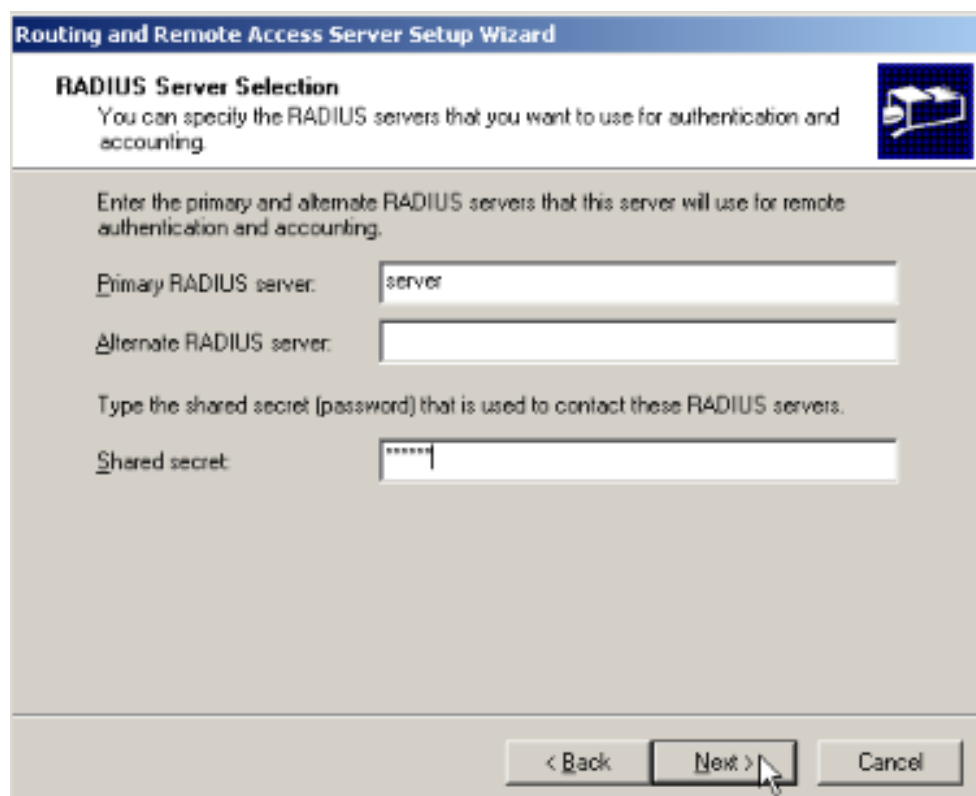
If you are using a RADIUS server on your network, you can set up this server to forward authentication requests to the RADIUS server.

Do you want to set up this server to work with a RADIUS server?

☐ No, use Routing and Remote Access to authenticate connection requests
☒ Yes, set up this server to work with a RADIUS server

< Back Next > Cancel

Tại mục RADIUS Server Selection ta nhập
 RADIUS Server : server
 Shared Secret : 123456



Routing and Remote Access Server Setup Wizard

RADIUS Server Selection

You can specify the RADIUS servers that you want to use for authentication and accounting.

Enter the primary and alternate RADIUS servers that this server will use for remote authentication and accounting.

Primary RADIUS server:

Alternate RADIUS server:

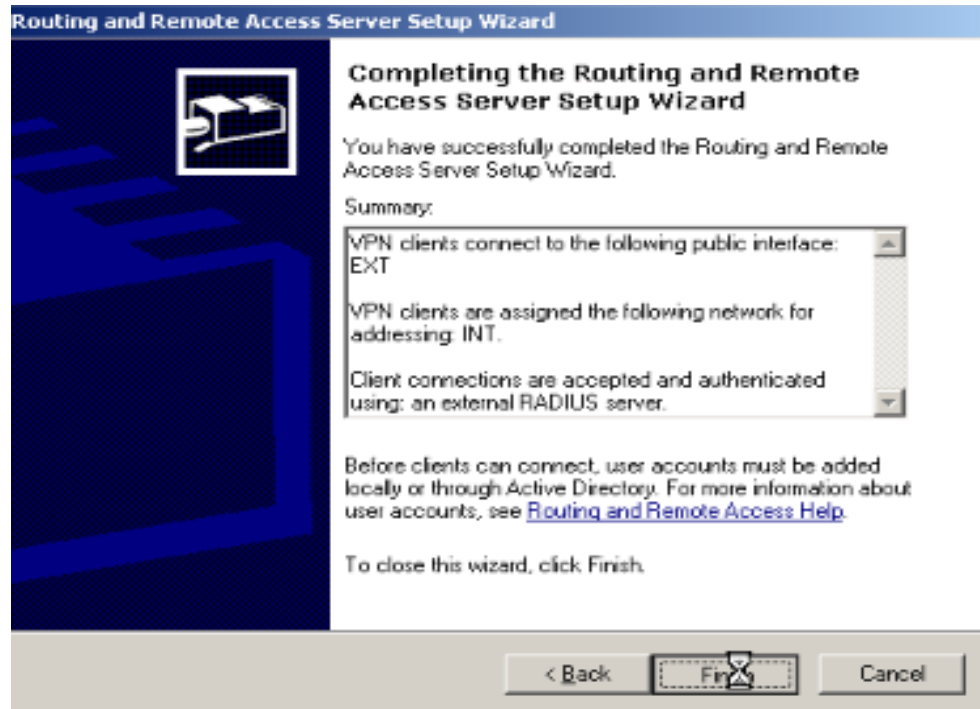
Type the shared secret (password) that is used to contact these RADIUS servers.

Shared secret:

< Back Next > Cancel

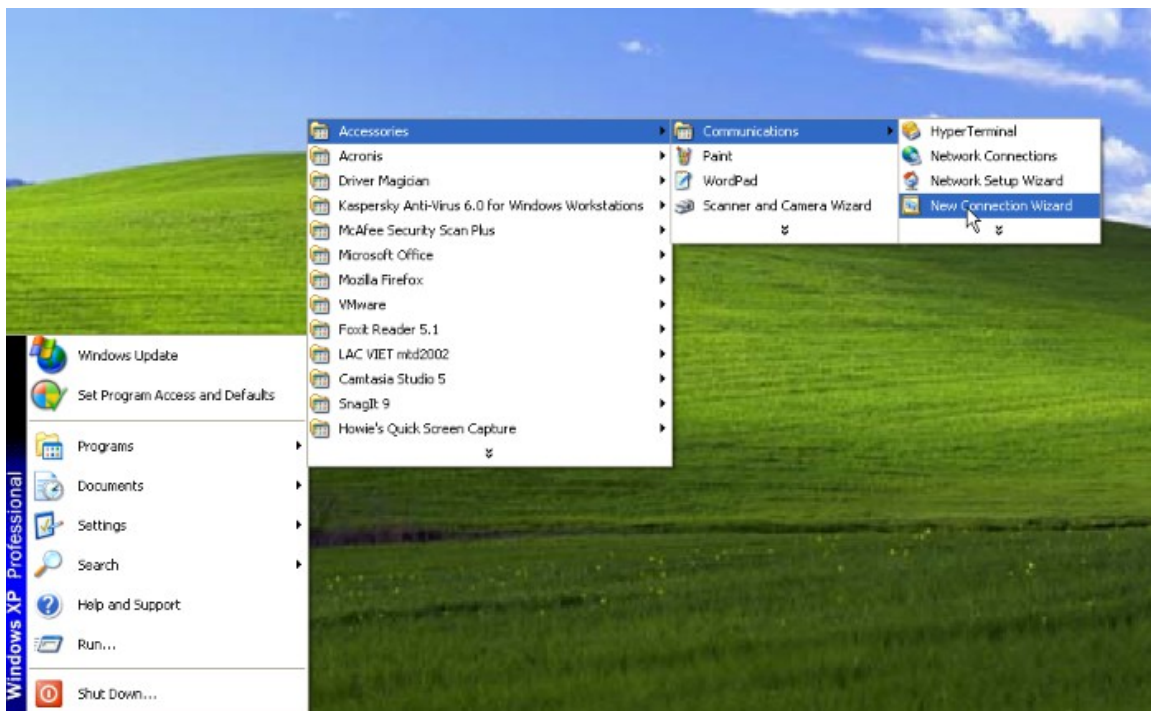
Hình 22. THIẾT LẬP CÁC THÔNG SỐ BẢO MẬT CHO NAS

Kích Next để hoàn tất quá trình cài đặt Routing and Remote Access



3.3.3. CLIENT TẠO KẾT NỐI

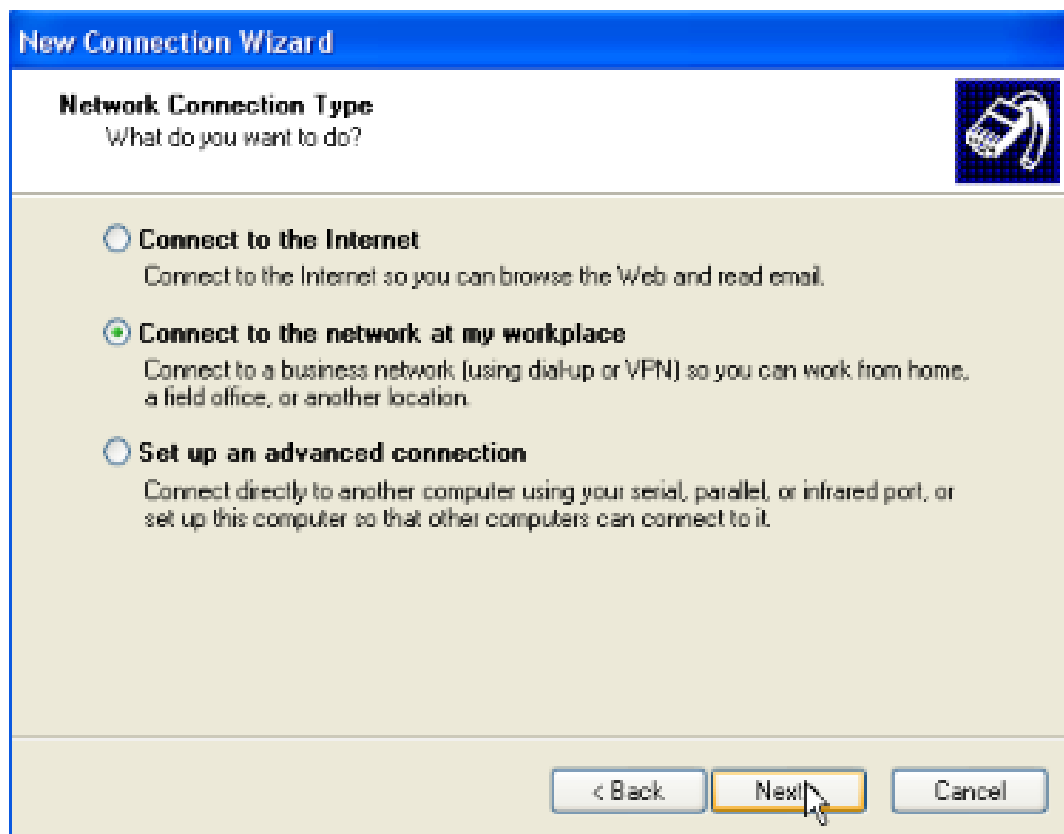
Start > program > Accessories > New Connection Wizard >



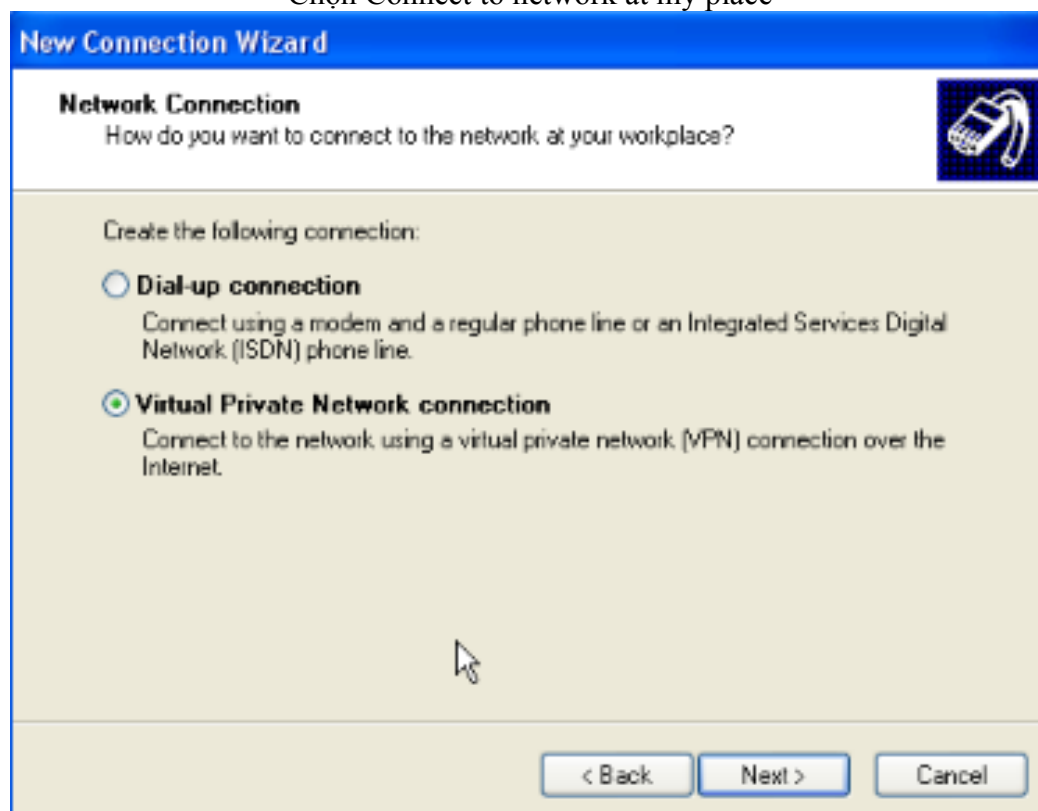
Hình 23. TẠO MỘT KẾT NỐI VPN ĐỂ NGƯỜI DÙNG QUAY SỐ



Click next để tiếp tục



Chọn Connect to network at my place



Chọn Virtual Private Network Connection

New Connection Wizard

Connection Name
Specify a name for this connection to your workplace.

Type a name for this connection in the following box.

Company Name

VPN

For example, you could type the name of your workplace or the name of a server you will connect to.

< Back Next > Cancel

Nhập tên kết nối

New Connection Wizard

VPN Server Selection
What is the name or address of the VPN server?

Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.

Host name or IP address (for example, microsoft.com or 157.54.0.1)

10.0.0.146

< Back Next > Cancel

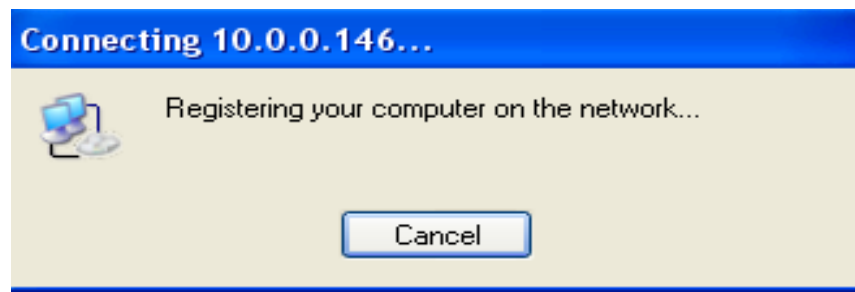
Nhập địa chỉ Ip hay tên máy của Vpn server



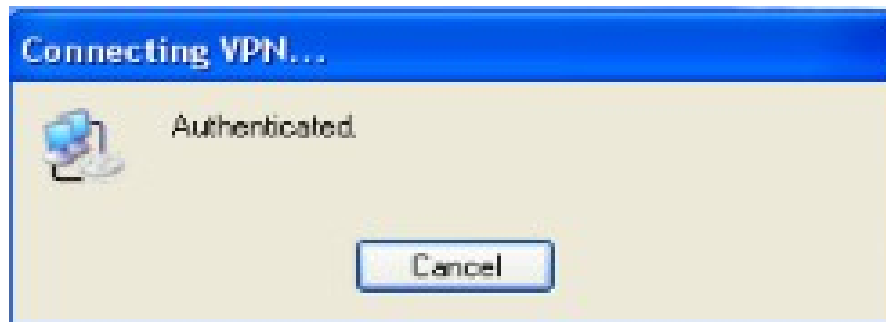
Nhấn Finish hoàn tất quá trình tạo kết nối



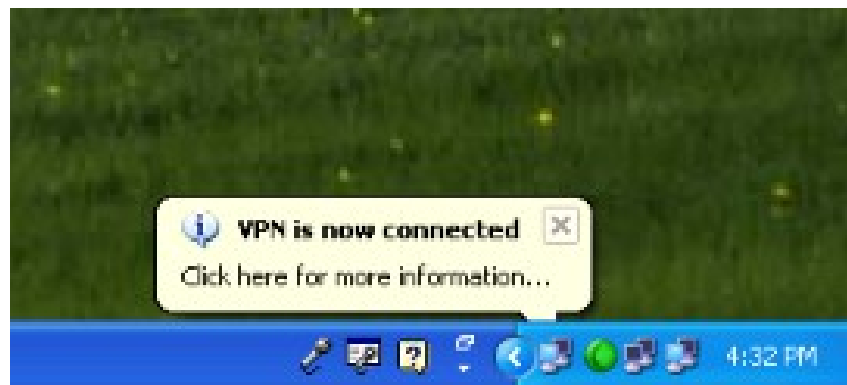
Nhập tài khoản và mật khẩu mà Radius Server đã tạo, chọn connect



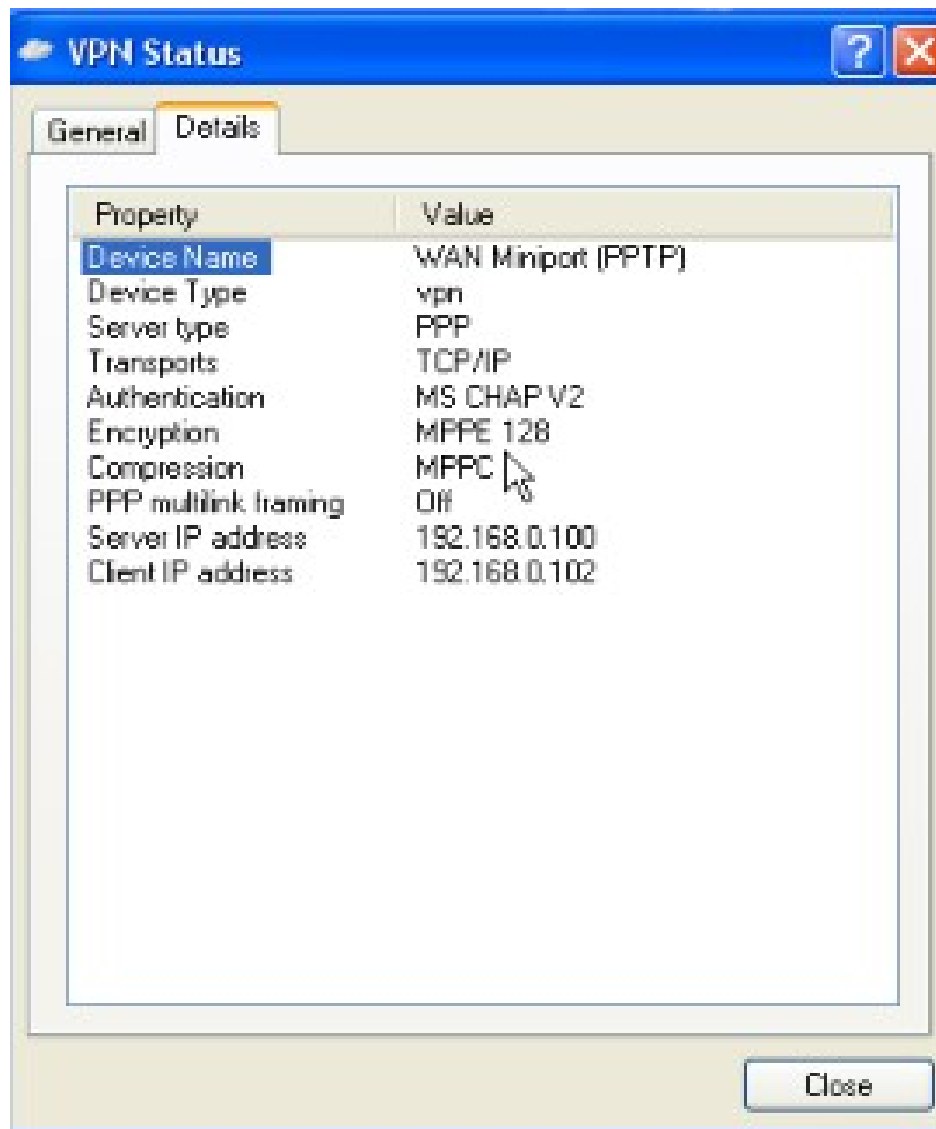
Hiện thị tiến trình đăng ký của máy vpn client vào mạng



Việc xác thực bằng tên và mật khẩu thành công.



Hiện thị thêm biểu tượng đã kết nối vpn



Hình 24. KIỂM TRA KẾT NỐI THÀNH CÔNG

Vpn server đã cấp cho Vpn Client

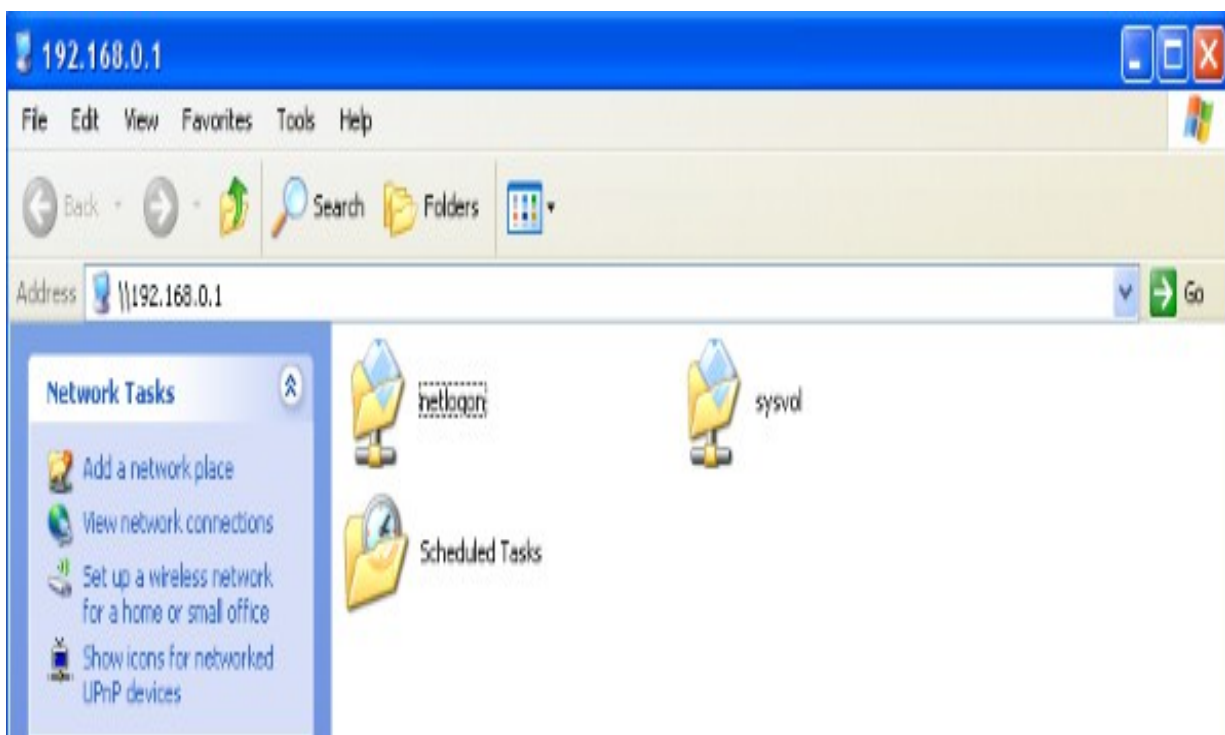
Địa chỉ ip: 192.168.0.102

Giao thức xác thực: MS CHAP 2

Giao thức mã hóa: MPPE 128

```
C:\WINDOWS\system32\cmd.exe - ping 192.168.0.3
C:\Documents and Settings\admin>ping 10.0.0.146
Pinging 10.0.0.146 with 32 bytes of data:
Control-C
^C
C:\Documents and Settings\admin>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=1ms TTL=127
Reply from 192.168.0.1: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.0.1:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C
^C
```

Dùng lệnh ping kiểm tra việc thông mạng.
Kết quả ping thành công vào Radius Server



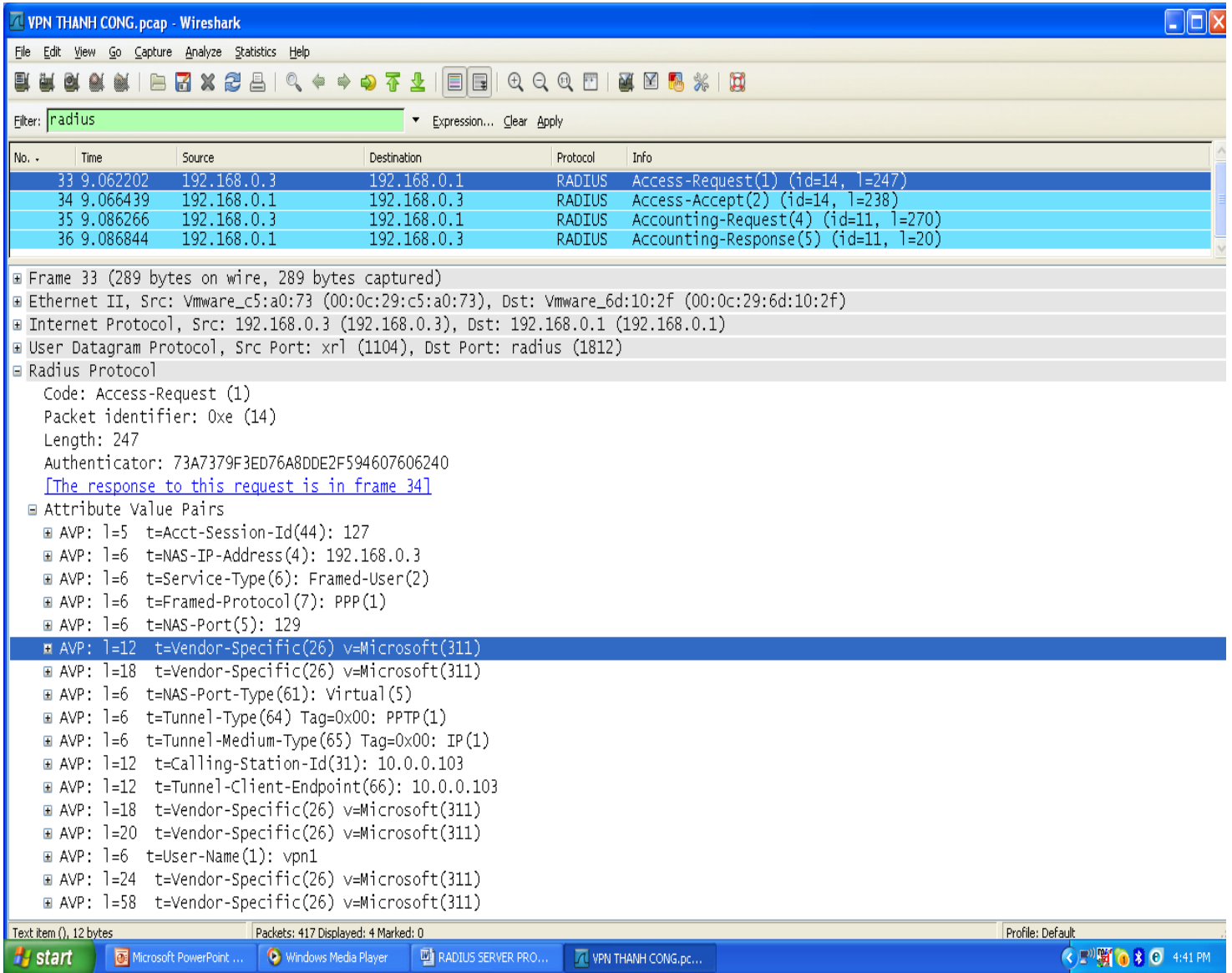
Hình 25. NGƯỜI DÙNG TRUY CẬP RADIUS SERVER ĐỂ LẤY DỮ LIỆU

Client lấy dữ liệu của Radius Server thành công

3.3.4. KẾT QUẢ PHÂN TÍCH GÓI TIN RADIUS

3.3.4.1. GÓI ACCESS REQUEST

Chúng ta tiến hành bắt các gói tin radius khi người dùng quay vpn vào để yêu cầu chứng thực



Hình 26. KẾT QUẢ TỔNG QUÁT GÓI TIN ACCESS REQUEST

3.3.4.1.1. CÁC TRƯỜNG GÓI ACCESS REQUEST

Radius Protocol

Code: Access-Request (1)

Packet identifier: 0xe (14)

Length: 247

Authenticator: 73A7379F3ED76A8DDE2F594607606240

[The response to this request is in frame 34]

Hình 27. CÁC TRƯỜNG TRONG GÓI ACCESS REQUEST

- **Code field:** Khi user quay vpn vào NAS thì lúc đó NAS chuyển các thông tin của user đến Radius Server, với mã code = 1
- **Packet identifier:** là trường nhận dạng, trường này có chiều dài 1 octet. Trường này tập hợp tất cả các thông tin yêu cầu chứng thực và các dịch vụ của người dùng trả lời cho người dùng trong gói access accept.
- **Length:** là chiều dài gói tin chiếm 2 octets. Chứa các trường như mã nhận dạng, thông tin chiều dài gói, nội dung yêu cầu xác thực và các thuộc tính .
- **Authenticator:** là trường xác thực. Trường này có 16 octet và hầu hết là các octet quan trọng. Trường này dùng để trao đổi thông tin trong quá trình chứng thực giữa Radius Server.

3.3.4.1.2. PHÂN TÍCH CÁC THUỘC TÍNH TRONG GÓI ACCESS REQUEST

- ▣ Attribute Value Pairs
 - ▣ AVP: l=5 t=Acct-Session-Id(44): 127
Acct-Session-Id: 127
 - ▣ AVP: l=6 t=NAS-IP-Address(4): 192.168.0.3
NAS-IP-Address: 192.168.0.3 (192.168.0.3)
 - ▣ AVP: l=6 t=Service-Type(6): Framed-User(2)
Service-Type: Framed-User (2)
 - ▣ AVP: l=6 t=Framed-Protocol(7): PPP(1)
Framed-Protocol: PPP (1)
 - ▣ AVP: l=6 t=NAS-Port(5): 129
NAS-Port: 129

Hình 28. CÁC THUỘC TÍNH TRONG GÓI ACCESS REQUEST

- **Acct – session – ID** là thuộc tính mã số của một phiên làm việc giữa người dùng và Radius Server. Mã số này dùng để trả lời các yêu cầu cho từng phiên làm việc.
- **NAS-IP-Address**: trường mô tả địa chỉ ip của Radius client
- **Service type**: Là trường mô tả loại dịch vụ được yêu cầu bởi người dùng
- **Frame protocol**: Trường mô tả giao thức kết nối
- **NAS port**: Là trường mô tả cổng mà NAS sử dụng để tạo kết nối đến Radius server

```
AVP: l=6 t=User-Name(1): vpn1
    User-Name: vpn1
AVP: l=24 t=Vendor-Specific(26) v=Microsoft(311)
    VSA: l=18 t=MS-CHAP-Challenge(11): A9E2854126BAB1BBF0791B0E66AB8796
        MS-CHAP-Challenge: A9E2854126BAB1BBF0791B0E66AB8796
AVP: l=58 t=Vendor-Specific(26) v=Microsoft(311)
    VSA: l=52 t=MS-CHAP2-Response(25): 00002ACC1D4F5C4FC69040429CC66E27D48C0000000000000...
```

**Hình 29. CÁC THUỘC TÍNH BẢO MẬT TRONG GÓI
ACCESS REQUEST**

- **User – name** là thông tin tài khoản người dùng
- **MS – CHAP – Challenge** là trường password của người dùng được mã hóa.

3.3.4.2. GÓI ACCESS ACCEPT

Sau khi người dùng được xác thực thành công thì Radius Server sẽ gửi gói Access Accept (cho phép truy cập) tới người dùng và cung cấp các dịch vụ mà người dùng đã yêu cầu trong gói Access Request

34	9.066439	192.168.0.1	192.168.0.3	RADIUS	Access-Accept(2) (id=14, l=238)
35	9.086266	192.168.0.3	192.168.0.1	RADIUS	Accounting-Request(4) (id=11, l=270)
36	9.086844	192.168.0.1	192.168.0.3	RADIUS	Accounting-Response(5) (id=11, l=20)

Internet Protocol	Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.3 (192.168.0.3)
User Datagram Protocol	Src Port: radius (1812), Dst Port: xrl (1104)
Radius Protocol	
Code: Access-Accept (2)	
Packet identifier: 0xe (14)	
Length: 238	
Authenticator: 0E87C07AFE6A8063E41B12B6BD3F3EDC	
[This is a response to a request in frame 33]	
[Time from request: 0.004237000 seconds]	
Attribute Value Pairs	
AVP: l=6 t=Framed-Protocol(7): PPP(1)	Framed-Protocol: PPP (1)
AVP: l=6 t=Service-Type(6): Framed-User(2)	Service-Type: Framed-User (2)
AVP: l=32 t=Class(25): 468704cc000001370001c0A8000101cd1c7c4361e9280000...	
AVP: l=42 t=Vendor-Specific(26) v=Microsoft(311)	
VSA: l=36 t=MS-MPPE-Recv-Key(17): 800B5E8EA4FF66B8CF1BB2637C2A66AE1720F2EB8675CBA3...	
AVP: l=42 t=Vendor-Specific(26) v=Microsoft(311)	
VSA: l=36 t=MS-MPPE-Send-Key(16): 800CDFD8AB42A593FF6E82BB85E6144A3E0886D6F0ED2548...	
AVP: l=51 t=Vendor-Specific(26) v=Microsoft(311)	
VSA: l=45 t=MS-CHAP2-Success(26): 00533D463643363437313844413636363331463733343230...	
AVP: l=15 t=Vendor-Specific(26) v=Microsoft(311)	
VSA: l=9 t=MS-CHAP-Domain(10): \000DOMAIN	
AVP: l=12 t=Vendor-Specific(26) v=Microsoft(311)	
VSA: l=6 t=MS-MPPE-Encryption-Policy(7): Encryption-Required(2)	
AVP: l=12 t=Vendor-Specific(26) v=Microsoft(311)	
VSA: l=6 t=MS-MPPE-Encryption-Types(8): RC4-128(4)	

Hình 30. GÓI ACCESS ACCEPT

3.3.4.2.1. CÁC TRƯỜNG GÓI ACCESS ACCEPT

▣ Radius Protocol

Code: Access-Accept (2)

Packet identifier: 0xe (14)

Length: 238

Authenticator: 0E87C07AFE6A8063E41B12B6BD3F3EDC

[This is a response to a request in frame 33]

[Time from request: 0.004237000 seconds]

Hình 31. CÁC TRƯỜNG TRONG GÓI ACCESS ACCEPT

- **Code field:** là trường Radius Server gửi gói cho phép truy cập đến NAS với mã code = 2. Radius server sẽ gửi thông tin cấu hình cần thiết để cung cấp dịch vụ cho người dùng.
- **Packet identifier** là trường nhận dạng của gói access accept là một bản sao của trường nhận dạng Access Request
- **Length** là trường chiều dài của gói access accept
- **Trường Authenticator** dùng để xác nhận mã nhận dạng gói tin, chiều dài gói, mã bí mật và các thuộc tính mà người dùng đã gửi trong gói access request ...

3.3.4.2.2. PHÂN TÍCH NỘI DUNG GÓI ACCESS ACCEPT

▣ Attribute Value Pairs

▣ AVP: l=6 t=Framed-Protocol(7): PPP(1)

Framed-Protocol: PPP (1)

▣ AVP: l=6 t=Service-Type(6): Framed-User(2)

Service-Type: Framed-User (2)

Hình 32. CÁC THUỘC TÍNH TRONG GÓI ACCESS ACCEPT

Framed – Protocol thuộc tính này định nghĩa một giao thức được sử dụng để tạo kết nối giữa người dùng và Radius Server và gửi cho NAS.

Service – Type căn cứ vào những dịch vụ mà người dùng đã gửi đến Radius Server trong gói Access Request và Service – Type là trường dùng để mô tả những dịch vụ mà Radius Server cho phép người dùng sử dụng.

```
■ VSA: l=36 t=MS-MPPE-Recv-Key(17): 800B5E8EA4FF66B8CF1BB2637C2A66AE1720F2EB8675CBA3...
    MS-MPPE-Recv-Key: 800B5E8EA4FF66B8CF1BB2637C2A66AE1720F2EB8675CBA3...
■ AVP: l=42 t=Vendor-Specific(26) v=Microsoft(311)
■ VSA: l=36 t=MS-MPPE-Send-Key(16): 800CDFD8AB42A593FF6E82BB85E6144A3E0886D6F0ED2548...
    MS-MPPE-Send-Key: 800CDFD8AB42A593FF6E82BB85E6144A3E0886D6F0ED2548...
■ AVP: l=51 t=Vendor-Specific(26) v=Microsoft(311)
■ VSA: l=45 t=MS-CHAP2-Success(26): 00533D463643363437313844413636363331463733343230...
    MS-CHAP2-Success: 00533D463643363437313844413636363331463733343230...
■ VSA: l=6 t=MS-MPPE-Encryption-Policy(7): Encryption-Required(2)
    MS-MPPE-Encryption-Policy: Encryption-Required (2)
■ AVP: l=12 t=Vendor-Specific(26) v=Microsoft(311)
■ VSA: l=6 t=MS-MPPE-Encryption-Types(8): RC4-128(4)
    MS-MPPE-Encryption-Types: RC4-128 (4)
```

Hình 33. CÁC THUỘC TÍNH BẢO MẬT TRONG GÓI ACCESS ACCEPT

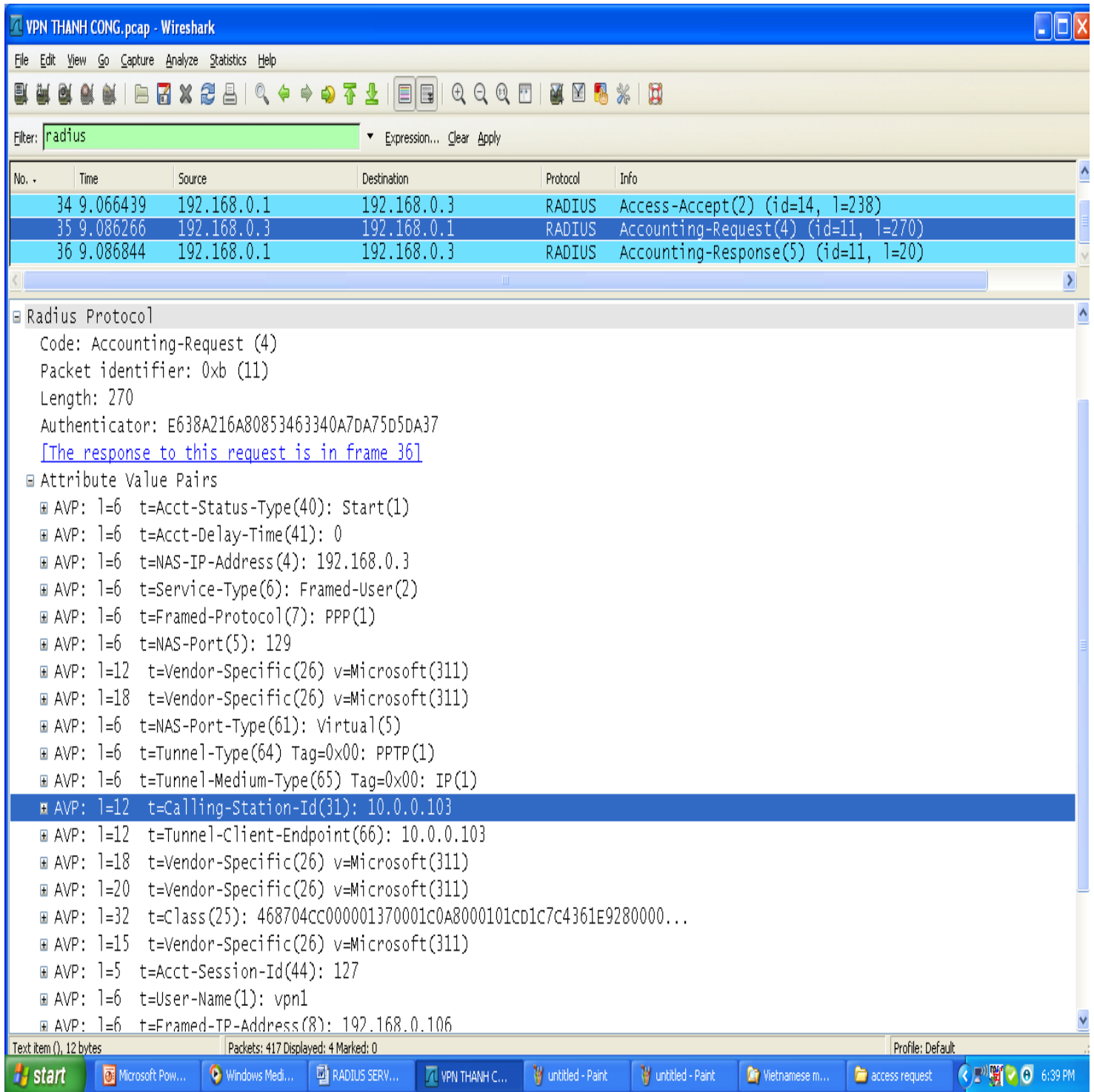
MS-MPPE-Recv-Key và **MS-MPPE-Send-Key** là quá trình trao đổi khóa .

MS-CHAP2-Success: quá trình mã hóa thành công.

MS-MPPE-Encryption-Policy: Chính sách mã hóa.

MS-MPPE-Encryption-Types: Quy định kiểu mã hóa.

3.3.4.3. GÓI ACCOUNTING REQUEST



Hình 34. GÓI ACCOUNTING REQUEST

Sau khi xác thực người dùng NAS gửi gói yêu cầu kiểm toán đến Radius server để kiểm toán những dịch vụ được yêu cầu bởi người dùng.

Khi nhận gói yêu cầu kiểm toán Radius server sẽ ghi lại những dịch vụ, thuộc tính và các thông tin cần xác thực của người dùng để bắt đầu quá trình kiểm toán.

Sau đó Radius server sẽ gửi gói trả lời đáp ứng yêu cầu kiểm toán đến NAS

3.3.4.3.1. CÁC TRƯỜNG TRONG GÓI ACCOUNTING REQUEST

Radius Protocol

Code: Accounting-Request (4)

Packet identifier: 0xb (11)

Length: 270

Authenticator: E638A216A80853463340A7DA75D5DA37

[\[The response to this request is in frame 36\]](#)

Hình 35. CÁC TRƯỜNG TRONG GÓI ACCOUNTING REQUEST

Code field là trường mô tả gói yêu cầu kiểm toán được gửi từ NAS đến Radius Server.

Packet Identifier là trường dùng để nhận dạng yêu cầu kiểm toán.

Length là chiều dài của gói yêu cầu kiểm toán

Authenticator là trường dùng để mô tả các thông tin cần xác thực trong quá trình kiểm toán

3.3.4.3.2. PHÂN TÍCH THUỘC TÍNH GÓI ACCOUNTING REQUEST

34	9.066439	192.168.0.1	192.168.0.3	RADIUS	Access-Accept(2) (id=14, l=238)
35	9.086266	192.168.0.3	192.168.0.1	RADIUS	Accounting-Request(4) (id=11, l=270)
36	9.086844	192.168.0.1	192.168.0.3	RADIUS	Accounting-Response(5) (id=11, l=20)

Attribute Value Pairs

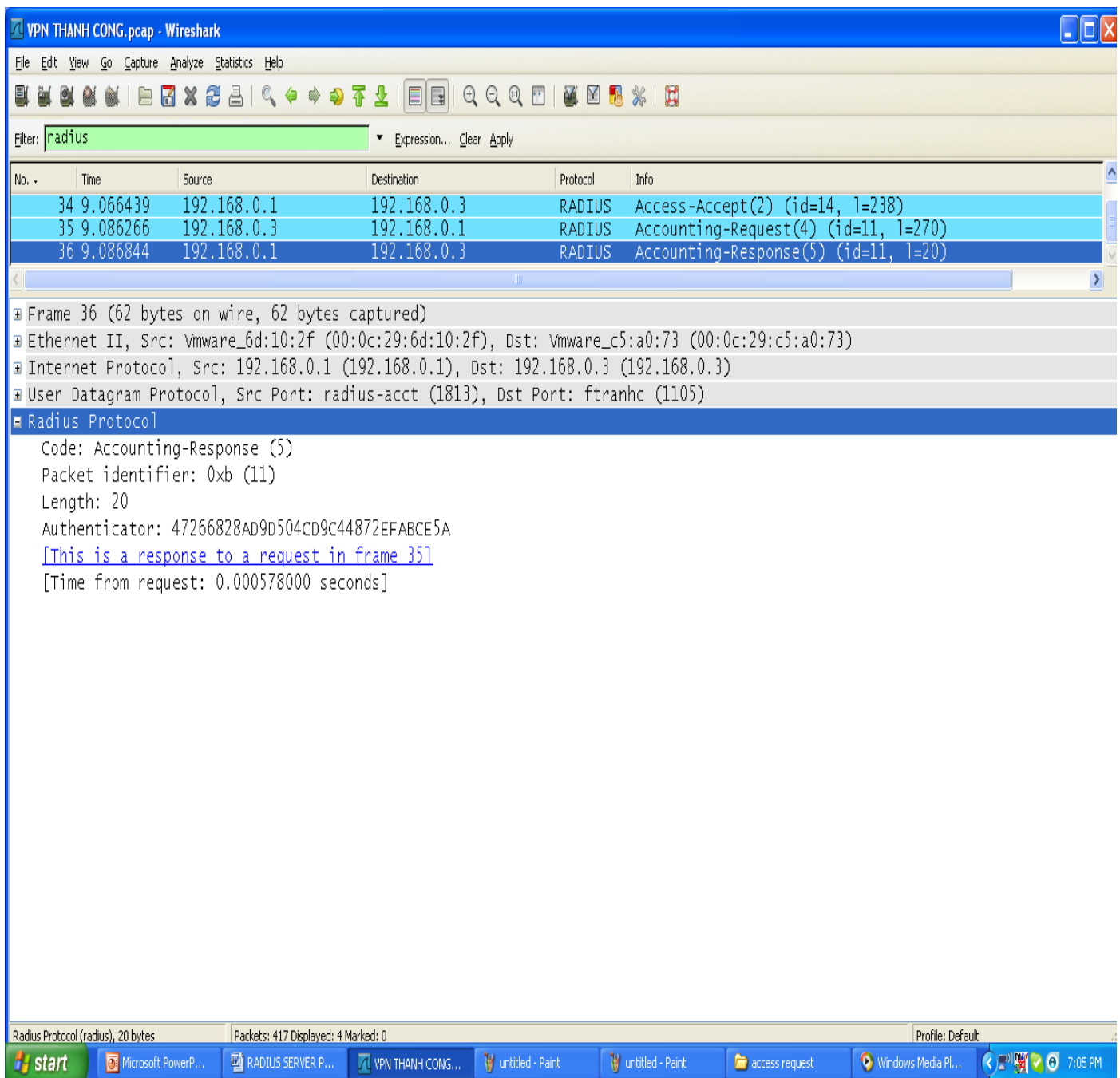
- AVP: l=6 t=Acct-Status-Type(40): Start(1)
- AVP: l=6 t=Acct-Delay-Time(41): 0
- AVP: l=6 t=NAS-IP-Address(4): 192.168.0.3
- AVP: l=6 t=Service-Type(6): Framed-User(2)
- AVP: l=6 t=Framed-Protocol(7): PPP(1)
- AVP: l=6 t=NAS-Port(5): 129
- AVP: l=12 t=Vendor-Specific(26) v=Microsoft(311)
- AVP: l=18 t=Vendor-Specific(26) v=Microsoft(311)
- AVP: l=6 t=NAS-Port-Type(61): Virtual(5)
- AVP: l=6 t=Tunnel-Type(64) Tag=0x00: PPTP(1)
- AVP: l=6 t=Tunnel-Medium-Type(65) Tag=0x00: IP(1)
- AVP: l=12 t=Calling-Station-Id(31): 10.0.0.103
- AVP: l=12 t=Tunnel-Client-Endpoint(66): 10.0.0.103
- AVP: l=18 t=Vendor-Specific(26) v=Microsoft(311)
- AVP: l=20 t=Vendor-Specific(26) v=Microsoft(311)
- AVP: l=32 t=Class(25): 468704cc000001370001c0A8000101cd1c7c4361e9280000...
- AVP: l=15 t=Vendor-Specific(26) v=Microsoft(311)
- AVP: l=5 t=Acct-Session-Id(44): 127
- AVP: l=6 t=User-Name(1): vpn1
- AVP: l=6 t=Framed-IP-Address(8): 192.168.0.106
- AVP: l=6 t=Framed-MTU(12): 1400
- AVP: l=4 t=Acct-Multi-Session-Id(50): 23
- AVP: l=6 t=Acct-Link-Count(51): 1
- AVP: l=6 t=Event-Timestamp(55): Apr 17, 2012 16:52:34.000000000
- AVP: l=6 t=Acct-Authentic(45): RADIUS(1)

Hình 36. CÁC THUỘC TÍNH GÓI ACCOUNTING REQUEST

Gói Accounting Request chứa tất cả các thuộc tính cũng như các dịch vụ ... mà người dùng đã yêu cầu trong gói Access Request được gửi trước đó.

3.3.4.4. GÓI ACCOUNTING RESPOND

Sau khi xác nhận các yêu cầu kiểm toán hoàn tất Radius Server gửi gói accounting respond cho người dùng.



Hình 37. CÁC TRƯỜNG GÓI ACCOUNTING RESPOND

Code field là trường mô tả đã bắt đầu quá trình kiểm toán.

Packet Identifier là trường nhận dạng của gói kiểm toán. Nó là bản sao của trường nhận dạng trong gói Accounting Request được gửi trước đó.

Length là chiều dài của gói

Authenticator chứa tất cả các thuộc tính đã được gửi trong gói yêu cầu kiểm toán trước đó.

3.4. TÀI LIỆU THAM KHẢO

- Trang google
- Trang youtube
- Trang Wikipedia
- Và các forum chuyên mạng máy tính như: VNPro, quantrimang, vietchuyen, nhatnghe.....