**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HỒ CHÍ MINH**

**BÁO CÁO ĐỒ ÁN**

**MÔN …**

**TÊN ĐỀ TÀI**

Ngành: **CÔNG NGHỆ THÔNG TIN**Chuyên Ngành:

GVHD: SVTH: MSSV:

MSSV:

Lớp:

TP.Hồ Chí Minh, 2022

**LỜI CẢM ƠN**

Chúng em xin bày tỏ lòng kính trọng và biết ơn sâu sắc đến Thầy … đã tận tình giúp đỡ và hướng dẫn chúng em hoàn thành đồ án cơ sở này. Nhờ sự giúp đỡ nhiệt lòng của thầy mà đồ án đã hoàn thành trong 10 tuần, đúng tiến độ của nhà trường đề ra.

**MỤC LỤC**

[**Chương 1: TỔNG QUAN** 1](#_Toc451983192)

[**1.1** **Tổng quan về đồ án** 1](#_Toc451983193)

[**1.2 Nhiệm vụ đồ án** 1](#_Toc451983194)

[**1.3 Cấu trúc đồ án** 1](#_Toc451983195)

[**Chương 2: CƠ SỞ LÝ THUYẾT** 3](#_Toc451983196)

[**2.1 Giới thiệu về giao thức PPTP** 3](#_Toc451983197)

[**2.2 Nhu cầu ứng dụng** 3](#_Toc451983198)

[**2.3 Lịch sử phát triển và các RFC liên quan** 4](#_Toc451983199)

[*2.3.1* *Lịch sử phát triển* 4](#_Toc451983200)

[*2.3.2* *RFC liên quan* 4](#_Toc451983201)

[**2.4 Công nghệ áp dụng** 5](#_Toc451983202)

[**2.5 Vấn đề bảo mật của giao thức PPTP** 5](#_Toc451983203)

[*2.5.1* *Mã hóa và nén dữ liệu PPTP* 5](#_Toc451983204)

[*2.5.2* *Xác thực dữ liệu PPTP* 6](#_Toc451983205)

[**2.6 Các mô hình triển khai** 7](#_Toc451983206)

[**2.7 Ưu và nhược điểm của giao thức PPTP** 8](#_Toc451983207)

[*2.7.1 Ưu điểm* 8](#_Toc451983208)

[*2.7.2 Nhược điểm* 9](#_Toc451983209)

[**2.8 Kiến trúc xử lý tổng quát** 9](#_Toc451983210)

[*2.8.1 Các quá trình xử lý* 9](#_Toc451983211)

[*2.8.2 Ý nghĩa của từng quá trình* 10](#_Toc451983212)

[**2.9 Phân tích giá trị từng thành phần của mỗi quá trình** 10](#_Toc451983213)

[*2.9.1 Thiết lập kết nối dựa trên PPP* 10](#_Toc451983214)

[*2.9.2 Kiểm soát kết nối PPTP* 11](#_Toc451983215)

[*2.9.3 Tạo đường hầm PPTP và truyền dữ liệu* 12](#_Toc451983216)

[**Chương 3: KẾT QUẢ THỰC NGHIỆM** 14](#_Toc451983217)

[**3.1 Mục tiêu của mô hình ứng dụng** 14](#_Toc451983218)

[**3.2 Mô hình ứng dụng** 14](#_Toc451983219)

[**3.3 Yêu cầu thực hiện** 14](#_Toc451983220)

[**3.4 Các công cụ cần thiết để thực hiện mô hình** 15](#_Toc451983221)

[**3.5 Các bước triển khai** 15](#_Toc451983222)

[**3.6 Phân tích các gói tin PPTP trên Wireshark** 27](#_Toc451983223)

[**Chương 4: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN** 35](#_Toc451983224)

[**4.1 Kết luận** 35](#_Toc451983225)

[**4.2 Hướng phát triển của đồ án** 35](#_Toc451983226)

[**TÀI LIỆU THAM KHẢO** 36](#_Toc451983227)

**Chương 1: TỔNG QUAN**

* 1. **Tổng quan về đồ án**

Đồ án sẽ giới thiệu cho chúng ta biết về giao thức mạng PPTP, nhiệm vụ của giao thức PPTP. Tìm hiểu tính bảo mật dữ liệu trong giao thức này.

**1.2 Nhiệm vụ đồ án**

Giúp người dùng sử dụng trong những mục đích sau:

- Đáp ứng nhu cầu truy cập dữ liệu và ứng dụng cho người dùng ở xa, bên ngoài thông tin thông qua Internet.

- Áp dụng cho các tổ chức có nhiều văn phòng chi nhánh, giữa các văn phòng cần trao đổi dữ liệu với nhau.

- Quản lý văn phòng một cách hiệu quả, giám sát công việc từ xa.

- Trong một số tổ chức, quá trình truyền dữ liệu giữa một số bộ phận cần bảo đảm tính riêng tư, không cho phép những bộ phận khác truy cập. PPTP có thể đáp ứng tình huống này.

**1.3 Cấu trúc đồ án**

Đồ án gồm có 4 chương:

* Chương 1: Tổng quan

Phần này giới thiệu tổng quan, nhiệm vụ của đồ án, giúp chúng ta hiểu nội dung căn bản của đồ án

* Chương 2: Cơ sở lý thuyết

Phần này sẽ giới thiệu cụ thể về khái niệm PPTP, nhu cầu của ứng dụng này trong hiện tại, những công nghệ được áp dụng trong giao thức, vấn đề bảo mật trong giao thức, những mô hình để triển khai giao thức, những ưu và nhược điểm của giao thức PPTP, kiến trúc xử lý và phân tích giá trị từng thành của mỗi quá trình.

* Chương 3: Kết quả thực nghiệm

Phần này sẽ cho chúng ta thấy mô hình mục tiêu úng dụng, giới thiệu các công cụ để thực hiện và phân tích các gói tin trong wireshark.

* Chương 4: Kết luận và hướng phát triển của đồ án

Phần này sẽ rút ra những lưu ý và lời khuyên khi sử dụng giao thức PPTP và đưa ra hướng phát triển để giao thức hoàn thiện hơn.

**Chương 2: CƠ SỞ LÝ THUYẾT**

**2.1 Giới thiệu về giao thức PPTP**

Point-to-Point Tunneling Protocol (PPTP – giao thức tạo đường hầm điểm nối điểm) là một giao thức mạng cho phép chuyển giao an toàn dữ liệu từ một Client từ xa đến một máy chủ bằng cách tạo ra một mạng riêng ảo (VPN) trên TCP/IP dựa trên mạng lưới dữ liệu. PPTP hỗ trợ theo yêu cầu, đa giao thức, mạng riêng ảo trên các mạng công cộng như Internet.

Các công nghệ mạng của PPTP là một phần mở rộng của giao thức Point-to-Point truy cập từ xa được xác định bởi Internet Engineering Task Force (IETF). PPTP là một giao thức mạng mà gói gọn các gói tin PPP để truyền trên Internet công cộng khác. PPTP cũng có thể được sử dụng trong mạng LAN-to-LAN.

Phần mở rộng của PPP PPTP được giải thích trong các tài liệu mạng tên “Point-to-Point Tunneling Protocol”, PPTP dự thảo – IETF – ppext – PPTP – 00. Text. Một dự thảo của tài liệu này đã được trình lên IETF năm 1996 bởi các công ty của diễn đàn PPTP, trong đó bao gồm Tổng công ty Microsoft, Ascend Communications, truy cập 3Com/Primary, ECI Bưu chính Viễn thông và US Robotics.

**2.2 Nhu cầu ứng dụng**

Point-to-Point Tunneling Protocol (PPTP) là một công nghệ mạng hỗ trợ đa giao thức mạng riêng ảo (VPN), cho phép người dùng từ xa truy cập các mạng doanh nghiệp an toàn trên máy trạm Microsoft Windows NT, Windows 95 và hệ thống điều hành Windows 98 và giao thức điểm-điểm (PPP) cho phép hệ thống quay số vào một nhà cung dịch vụ Internet địa phương để kết nối bảo mật cho mạng công ty của họ thông qua Internet.

PPTP đóng gói các khung dữ liệu của giao thức PPP vào các IP datagram để truyền qua mạng IP (Internet hoặc Intranet). PPTP dùng một kết nối TCP (gọi là kết nối điều khiển PPTP) để khởi tạo, duy trì, kết thúc đường ngầm và một phiên bản của giao thức GRE (Generic Routing Encapsulation – đóng gói định tuyến chung) để đóng gói các khung PPP. Phần tải tin của khung PPP có thể được mật mã hoặc giải nén.

PPTP giả định tồn tại một mạng IP giữa PPTP client (VPN client sử dụng giao thức đường ngầm PPTP) và PPTP sever (VNP sever sử dụng PPTP). PPTP client có thể được nối trực tiếp qua việc quay số tới máy chủ truy nhập mạng (Network Access Sever – NAS) để thiết lập kết nối IP**.**

**2.3 Lịch sử phát triển và các RFC liên quan**

*2.3.1 Lịch sử phát triển*

Giao thức này được nghiên cứu và phát triển bởi công ty chuyên về thiết bị công nghệ viễn thông. Trên cơ sở của giao thức là tách các chức năng chung và riêng của việc truy nhập từ xa, dựa trên cơ sở hạ tầng Internet có sẵn để tạo kết nối đường hầm giữa người dùng và mạng riêng ảo. Người dùng ở xa có thể dùng phương pháp quay số tới các nhà cung cấp dịch vụ Internet để có thể tạo đường hầm riêng để kết nối tới mạng riêng ảo của người dùng đó. Giao thức PPTP được xây dựng dựa trên nền tảng của PPP, có thể cung cấp khả năng truy nhập tạo đường hầm thông qua Internet đến các điểm cuối. PPTP sử dụng giao thức đóng gói tin định tuyến chung GRE được mô tả để đóng gói và tách gói PPP. Giao thức này cho phép PPTP linh hoạt trong xử lý các giao thức khác.

Do phần mềm kết nối hỗ trợ PPTP được tích hợp trong hầu hết các hệ điều hành, triển khai PPTP Server trở nên dễ dàng hơn vì không phải cài đặt phần mềm hỗ trợ trên máy trạm. PPTP client cũng sẵn dùng trên Linux, Macintosh. Các PPTP VPN cũng được hỗ trợ bởi các thiết bị phần cứng hoặc phần mềm tường lửa, bao gồm ISA Server, Cisco Pix, SonicWall và một vài model của WatchGuard. PPTP đã từng bị chỉ trích nhiều vì nhiều khiếm khuyết về bảo mật và rất nhiều lỗi đã được chỉ ra trong các phiên bản hiện thời của giao thức. Sử dụng xác thực EAP sẽ tăng cường đáng kể khả năng bảo mật của PPTP VPN vì EAP sử dụng chứng chỉ số (digital certificates) để xác thực lẫn nhau giữa Client và máy chủ.

*2.3.2 RFC liên quan*

RFC 2637 tháng 7 năm 1999.

**2.4 Công nghệ áp dụng**

PPP đóng vai trò chính trong các giao dịch dựa trên PPTP. PPTP là một sự mở rộng logic của PPP, PPTP không thay đổi dưới công nghệ PPP, nó chỉ định nghĩa một cách vận chuyển lưu lượng PPP mới qua các mạng công cộng không án toàn.

Khá giống với PPP, PPTP không không hỗ trợ nhiều kết nối. Tất cả các kết nối được hỗ trợ bởi PPTP phải là kết nối điểm – điểm, ngoài ra, PPP đáp ứng các chức năng sau trong giao dịch dựa trên PPTP:

Thiết lập và kết thúc các kết nối vật lý giữa các thực thể truyền thông cuối.

Xác thực các Client PPTP.

Mã hóa các gói dữ liệu như IPX, NetBEUI, NetBIOS, TCP/IP để tạo các gói PPP và bảo mật việc trao đổi dữ liệu giữa các nhóm liên quan.

Vì PPTP sử dụng PPP nên PPTP có thể tận dụng các tính năng của PPP.

Ngày nay, PPTP đã được hỗ trợ thêm các giao thức xác thực mở rộng (EAP) để xác thực người sử dụng. EAP được thiết kế cho các mạng không dây, nhưng đã được tích hợp vào PPTP.

**2.5 Vấn đề bảo mật của giao thức PPTP**

PPTP đưa ra nhiều dịch vụ bảo mật xây dựng sẵn khác nhau cho PPTP Server và Client. Các dịch vụ bảo mật này bao gồm: Mã hóa và nén dữ liệu, xác thực dữ liệu, kiểm soát truy cập và lọc gói tin.

PPTP đã được các nhà phân tích bảo mật tìm thấy các lỗ hổng trong giao thức. Các lỗ hổng được biết đến liên quan đến các giao thức PPP xác thực cơ bản sử dụng, thiết kế của giao thức MPPE cũng như tích hợp giữa MPPE và chứng thực PPP thành lập khóa phiên. Hơn nữa các cơ chế bảo mật được đề cập ở trên, PPTP có thể dùng chung với Filewwall và Router.

*2.5.1 Mã hóa và nén dữ liệu PPTP*

PPTP cung cấp một cơ chế mã hóa để bảo mật dữ liệu. Thay vào đó, nó sử dụng dịch vụ mã hóa được đề xuất bởi PPP. PPP sử dụng mã hóa Microsoft Point-to-Point, nó dựa trên phương pháp mã hóa chia sẻ bí mật.

*2.5.2 Xác thực dữ liệu PPTP*

PPTP hỗ trợ các cơ chế xác thực của các Microsoft sau đây:

*2.5.2.1 Giao thức xác thực có thăm dò trước của Microsoft (MS-CHAP)*

MS – CHAP là phiên bản thương mại của Microsoft và được dùng cho xác thực dựa trên PPP. Vì sự tương đồng cao với CHAP, các chức năng của MS – CHAP khá giống với CHAP. Điểm khác biệt chính giữa chúng là trong khi CHAP dựa trên RSA và thuật toán MD5 thì MS – CHAP dựa trên RSA RCA và DES. MS – CHAP được phát triển chỉ cho các sản phẩm Microsoft, nó không hỗ trợ bởi các nền khác.

*2.5.2.2 Giao thức xác thực mật khẩu (PAP)*

PAP là giao thức đơn giản và là giao thức xác thực đường quay số thông dụng nhất. Nó cũng dùng để xác thực các kết nối dựa trên PPP. Tuy nhiên nó gửi ID và mật khẩu của người dùng qua kiên kết mà không mã hóa.

Một lỗ hổng của PAP khác là các thực thể truyền thông cuối chỉ được xác thực một lần khi khởi tạo kết nối. Vì vậy nếu kẻ tấn công vượt qua được một lần thì không cần phải lo lắng về vấn đề xác thực trong tương lai nữa. Vì lý do này, PAP được xem như là một giao thức xác thực ít phức tạp và không phải là cơ chế xác thực ưa thích trong VPN.

*2.5.2.3 Kiểm soát truy cập PPTP*

Sau khi một Client PPTP từ xa được xác thực thành công, sự truy cập của nó đến các tài nguyên trong mạng bị hạn chế bởi mục đích bảo mật nâng cao. Mục tiêu này được hoàn thành bởi việc thực thi bổ sung cơ chế kiểm soát truy cập như: quyền truy cập, mức cho phép, nhóm và lọc gói PPTP. Lọc gói PPTP cho phép 1 Server trên mạng riêng chỉ chấp nhận và định tuyến các gói chỉ từ các Client PPTP đã xác thực thành công. Kết quả là chỉ có các Client PPTP đã được xác thực mới có thể truy cập lại tới mạng từ xa đã xác định. Trong cách này, PPTP không chỉ cung cấp các cơ chế xác thực, kiểm soát truy cập và mã hóa mà còn làm tăng thêm sự an toàn của mạng.

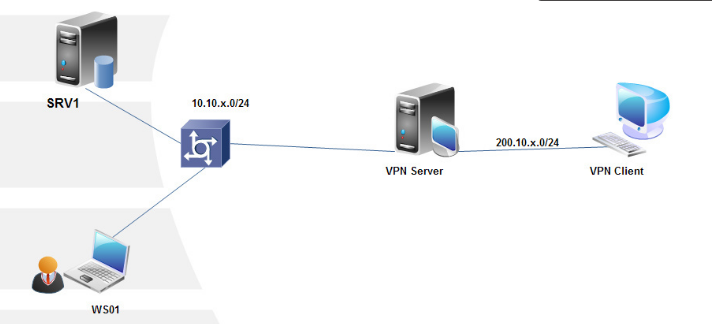
*2.5.2.4 PPTP với Firewall và Router*

Các thiết bị PPTP chấp nhận lưu lượng TCP và IP tại cổng 1723 và 47. Tuy nhiên, khi PPTP dùng chung với Wirewall và Router, lưu lượng đã được tính sẵn cho các cổng này được định tuyến qua Wirewall hoặc Router, chúng lọc lưu lượng trên cơ sở danh sách kiểm soát truy cập (ALC) và các chính sách bảo mật khác, PPTP nâng cao các dịch vụ bảo mật mà nó đưa ra.

**2.6 Các mô hình triển khai**

*2.6.1 User Remote Access LAN VPN via PPTP*

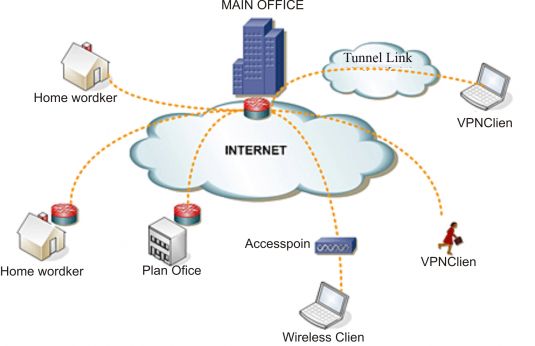
Hiện nay, yêu cầu làm việc từ xa trong một hệ thống doang nghiệp là rất lớn. Điều đáng nói là bạn làm sao có thể cấu hình một hệ thống mạng trao đổi dữ liệu qua hệ thống mạng Internet như một mạng LAN. Khi đó VPN sử dụng giao thức PPTP để thực hiện điều đó, hệ thống này tạo ra một hệ thống mạng LAN thông qua Internet.



Hình 2.1 Mô hình triển khai Remote Access LAN VNP sử dụng PPTP

*2.6.2 LAN to LAN VNP via PPTP*

Dùng để kết nối 2 chi nhánh của công ty, doanh nghiệp… lại với nhau thông qua mạng Internet tạo 1 kết nối VPN sử dụng giao thức PPTP. Hai bên có thể trao đổi, truyền dữ liệu với nhau dựa trên mạng riêng ảo VPN.



Hình 2.2 Mô hình triển khai Lan to Lan VPN thông qua PPTP

**2.7 Ưu và nhược điểm của giao thức PPTP**

*2.7.1 Ưu điểm*

*2.7.1.1 Tính có sẵn*

PPTP được hỗ trợ trong nhiều hệ điều hành như: Window NT Server, Workstation. Do đó, PPTP thực sự sẵn có trên các Platfform của người sử dụng, không cần mua thêm các phần mềm bổ sung vì Microsoft đã đưa ra cách nâng cấp PPTP trong tất cả các phiên bản Window. PPTP đã trở thành một phần của các gói tin hệ điều hành mạng. Một nhà quản trị mạng Window NT có thể thử nghiệm một VPN ngay lập tức mà không cần tốn thêm một chi phí nào.

*2.7.1.2 Tạo đường hầm đa giao thức*

Đây là một tính năng vượt trội của PPTP, giao thức PPTP có thể tạo đường hầm cho tất cả các giao thức mà máy chủ RAS cho phép, trong khi một vài phần mềm tạo đường hầm chỉ cho phép tạo đường hầm với các gói tin IP.

*2.7.1.3 Dễ thi hành*

Nhiều nhà quản trị mạng dễ dàng thực thi giao thức PPTP vì họ đã quen thuộc với cách thiết lập các giao thức mạng và RAS.

Những người sử dụng từ xa quay số kết nối tới RAS Server thông qua các ISP sử dụng Switch truy cập từ xa ( Remote Access Switch) có hỗ trợ PPTP thì chỉ cần bổ sung địa chỉ IP của RAS Server vào Profile của họ, ISP dễ dàng đóng gói các gói tin PPP theo khuôn dạng PPTP.

*2.7.1.4 Khả năng sử dụng các địa chỉ IP Private một cách đồng bộ*

Khi một người dùng VPN tạo một kết nối PPTP tới máy chủ RAS sẽ được máy chủ gán cho một địa chỉ IP. Địa chỉ này có thể là một phần trong dãy địa chỉ IP của tổ chức. Vì thế, hệ thống người sử dụng RAS có thể trực tuyến trên mạng IP của tổ chức đó.

Các tổ chức thỉnh thoảng sử dụng địa chỉ IP Private (là những địa chỉ IP chỉ được cung cấp bởi cơ quan có thẩm quyền và duy nhất) trên hệ thống mạng riêng. Cơ quan thẩm quyền Internet Assigned Numbers (IANA) sẽ thiết lập các khối địa chỉ IP Private để sử dụng trên các mạng riêng Intranet và các hệ thống mạng này không cho phép các truy cập Internet hay các truy cập qua Router. Nếu một công ty có sử dụng một tập các địa chỉ IP Private thì khi một RAS Client sử dụng giao thức PPTP để thiết lập kết nối, sẽ được cung cấp một địa chỉ trong số địa chỉ đó và truy cập tới.

*2.7.2 Nhược điểm*

Nhược điểm của giao thức PPTP là yếu kém về bảo mật, là do dùng mã hóa đồng bộ được xuất phát từ việc sử dụng mã hóa đối xứng để tạo ra khoá từ mật khẩu của người dùng. Điều này còn nguy hiểm hơn vì mật khẩu thường gửi dưới dạng phơi bày hoàn toàn trong quá trình xác nhận. Giao thức đường hầm kế tiếp (L2F) được phát triển nhằm cải thiện bảo mật.

**2.8 Kiến trúc xử lý tổng quát**

*2.8.1 Các quá trình xử lý*

Phần này cung cấp thông tin về kiến trúc của PPTP trong Windows Server. PPTP được thiết kế để cùng một phương án an toàn để đạt được các mạng riêng trên Internet.

Thông tin liên lạc an toàn được tạo ra bằng cách sử dụng giao thức PPTP, thường bao gồm 3 quá trình, mỗi quá trình trong số đó đòi hỏi phải hoàn thành công việc của quá trình trước đó.

Ba quá trình đó là:

* Thiết lập kết nối dựa trên PPP.
* Kiểm soát kết nối PPTP.
* Tạo đường hầm PPTP và truyền dữ liệu.

*2.8.2 Ý nghĩa của từng quá trình*

*2.8.2.1 Thiết lập kết nối dựa trên PPP*

Một khách hàng sử dụng PPTP để kết nối ISP bằng cách sử dụng một đường dây điện thoại tiêu chuẩn hoặc ISDN. Kết nối này sử dụng giao thức PPP để thiết lập kết nối và mã hóa các gói dữ liệu.

*2.8.2.2 Kiểm soát kết nối PPTP*

Sử dụng kết nối với Internet được thành lập bởi các giao thức PPP. Giao thức PPTP tạo ra một kết nối điều khiển từ khách hàng đến một máy chủ PPTP trên Internet. Kết nối này sử dụng giao thức TCP để thiết lập kết nối và gọi là một đường hầm PPTP.

*2.8.2.3 Tạo đường hầm PPTP và truyền dữ liệu*

Các giao thức PPTP tạo ra các gói tin IP có chứa các gói tin PPP được mã hóa mà sau đó được gửi qua đường hầm PPTP đến máy chủ PPTP. Máy chủ PPTP disassembles các gói tin IP, giải mã các gói tin PPP và sau đó gửi các gói tin giải mã đến một mạng riêng.

**2.9 Phân tích giá trị từng thành phần của mỗi quá trình**

*2.9.1 Thiết lập kết nối dựa trên PPP*

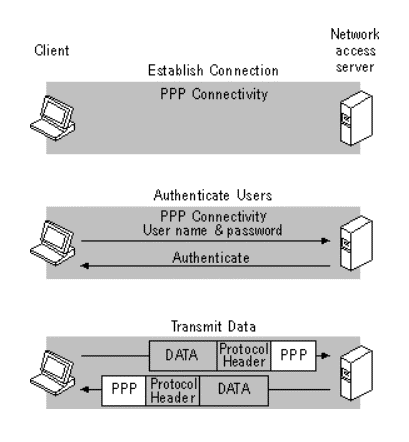
PPP là một giao thức truy cập từ xa được sử dụng bởi PPTP để gửi dữ liệu đa giao thức trên các mạng TCP/IP. PPP đóng gói IP, IPX, NetBEUI và các gói tin giữa các khung hình PPP và gửi các gói dữ liệu đóng gói đó bằng cách tạo ra một liên kết point – point giữa các máy tính gửi và nhận.

Hầu hết các phiên bản PPTP được bắt đầu bởi một khách hàng quay số lập một máy chủ truy cập mạng ISP. Giao thức đước sử dụng để tạo ra các kết nối Dial – Up giữa khách hàng và máy chủ truy cập mạng và thực hiện ba chức năng sau:

- Thiết lập và kết thúc kết nối vật lý: Các giao thức PPP sử dụng một trình tự định nghĩa trong RFC 1661 để thiết lập và duy trì kết nối giữa các máy tính từ xa.

- Xác thực người dùng: Sử dụng giao thức PPP để xác thực khách hàng.

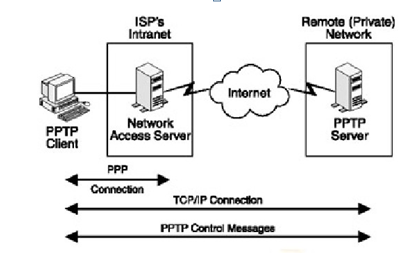
- Tạo ra các gói tin PPP có chứa IPX, NetBEUI, hoặc các gói TCP/IP: PPP tạo ra các gói tin có chứa một hoặc nhiều mã hóa giao thức TCP/IP, IPX, hoặc các gói dữ liệu NetBEUI. Bởi các gói tin được mã hóa, tất cả các trao đổi giữa máy chủ truy cập mạng và máy khách PPP là an toàn.



Hình 2.3 Mô hình Dial-up mạng kết nối PPP đến ISP

*2.9.2 Kiểm soát kết nối PPTP*

Sau khi một kết nối vật lý dựa trên PPP được thiết lập giữa PPTP Client và Server thì quá trình kiểm soát kết nối PPTP sẽ bắt đầu.



Hình 2.4 Mô hình kiểm soát trao đổi dữ liệu PPTP qua PPP

Một số thông điệp thường dùng để kiểm soát PPTP như sau:

|  |  |
| --- | --- |
| Message Types | Purpose |
| PPTP-Start-Session-Request | Bắt đầu phiên |
| PPTP-Start-Session-Reply | Trả lời để bắt đầu yêu cầu phiên |
| PPTP-Echo-Request | Duy trì phiên hoạt động |
| PPTP-Echo-Reply | Trả lời để duy trì phiên hoạt động |
| PPTP-Wan-Error-Notify | Thông báo lỗi trong giao diện PPP của Server |
| PPTP-Set-Link-Info | Cấu hình kết nối giữa Server PPTP và Clinet |
| PPTP-Stop-Session-Request | Kết thúc phiên |
| PPTP-Stop-Session-Reply | Trả lời để kết thúc yêu cầu phiên |

Bảng 2.5 Các thông điệp kiểm soát PPTP

*2.9.3 Tạo đường hầm PPTP và truyền dữ liệu*

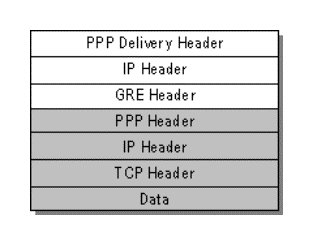
Một gói tin PPTP trải qua các giai đoạn sau:

- Bao gói dữ liệu: Thông tin gốc được mã hóa và sau đó bao gói vào bên trong một Frame PPP. Một tiêu đề PPP được thêm vào Frame.

- Bao gói Frame PPP: Frame PPP sau đó được bao gói vào trong một gói định tuyến chung (GRE) đã sửa rồi. Tiêu đề GRE sửa đổi chứa một trường ACK 4 byte và 1 bit ACK tương ứng thông báo sự có mặt của trường ACK. Trường khóa Frame GRE được thay bởi một trường có độ dài 2 byte gọi là độ dài tải và một trường độ dài 2 byte gọi là định danh cuộc gọi. PPTP Client thiết lập các truỏng này khi nó tạo đường hầm PPTP.

- Bao gói dữ liệu GRE: Một tiêu đề IP được thêm vào khung PPP và được bao gói vào trong gói GRE. Tiêu đề này chứa địa chỉ IP của PPTP Client nguồn và PPTP Server đích.

- Bao gói tầng liên kết dữ liệu: PPTP là một giao thức tạo đường hầm tầng 2, vì vậy, tiêu đề tầng liên kết dữ liệu và lần theo sự đánh dấu là các quy luật quan trọng trong đường hầm dữ liệu. Trước khi truyền phát thì tầng liên kết dữ liệu thêm vào tiêu đề chính của nó và đánh dấu cho các gói dữ liệu. Khi gói dữ liệu PPTP được truyền thành công thì bên người nhận phải xử lý các gói dữ liệu đã được đóng gói bằng đường hầm để được dữ liệu gốc.



Hình 2.6 Mô hình truyền dữ liệu

Sau khi đường hầm PPTP được thiết lập, dữ liệu người dùng được truyền giữa máy Client và máy Server PPTP. Dữ liệu được truyền trong IP datagram có chứa các gói tin PPP. Các gói dữ liệu IP được tạo ra sử dụng một phiên bản sửa đổi của giao thức GRE.

Các tiêu đề IP cung cấp các thông tin cần thiết cho các gói tin đi qua mạng Internet. Các tiêu đề GRE được sử dụng để đóng gói các gói tin PPP trong gói tin IP. Các gói tin PPP đã được tạo ra bởi RSA.

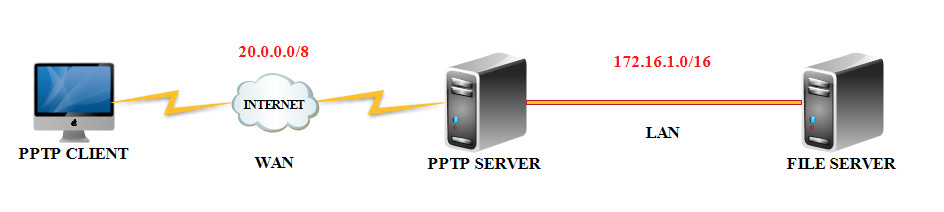
**Chương 3: KẾT QUẢ THỰC NGHIỆM**

**3.1 Mục tiêu của mô hình ứng dụng**

Mô hình úng dụng giúp chúng ta thấy được tổng quan quá trình làm việc của giao thức PPTP.

Tạo ra một đường hầm để đáp ứng nhu cầu truy cập, trao đổi dữ liệu của người dùng ở xa nhau hay các chi nhánh trong một công ty thông qua mạng riêng ảo VPN, đảm bảo tính riêng tư.

**3.2 Mô hình ứng dụng**



Hình 3.1 Mô hình triển khai của PPTP

**3.3 Yêu cầu thực hiện**

* Chuẩn bị 3 máy PC.
* PPTP SERVER: 2 card mạng.
* FILE SERVER trong LAN.
* PPTP CLIENT giả lập trong WAN.

Địa chỉ từng PC được thể hiện trong bảng sau

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **PPTP CLIENT** | **PPTP SERVER** | **FILE SERVER** |
| **WAN IP** | IP Address | 20.0.0.2 | 20.0.0.1 | Disable |
| Subnet Mask | 255.0.0.0 | 255.0.0.0 |
| Default Gateway |  |  |
| **LAN**  **IP** | IP Address | Disable | 172.16.1.1 | 172.16.1.2 |
| Subnet Mask | 255.255.0.0 | 255.255.0.0 |
| Default Getway |  | 172.16.1.1 |

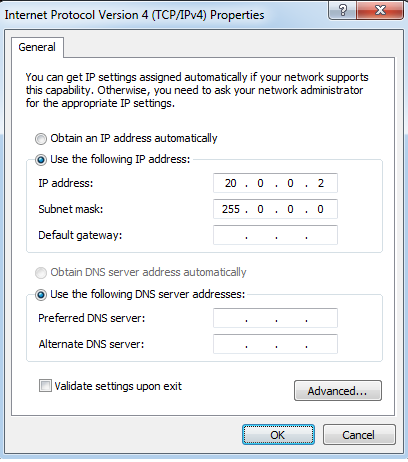
Bảng 3.2 Bảng địa chỉ cụ thể

**3.4 Các công cụ cần thiết để thực hiện mô hình**

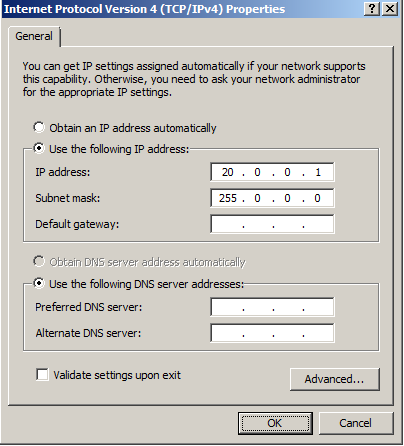
* Windows server 2008.
* Wireshark.

**3.5 Các bước triển khai**

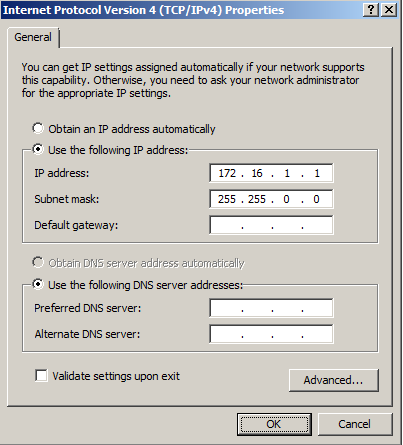
* **Bước 1**: Đặt IP cho 3 máy
* Máy PPTP CLIENT:



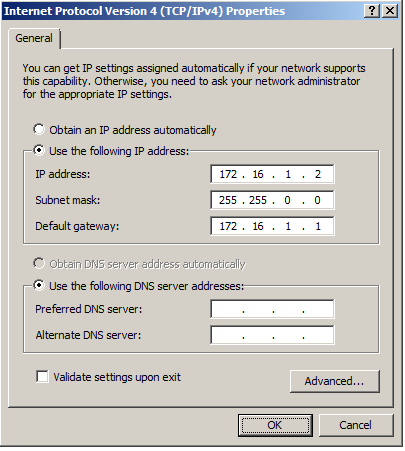
* Máy PPTP SERVER:
* Card WAN:



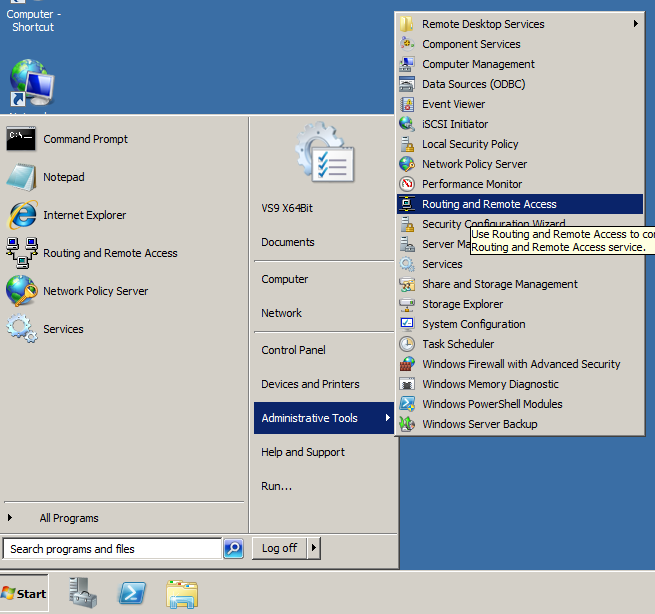
* Card LAN:



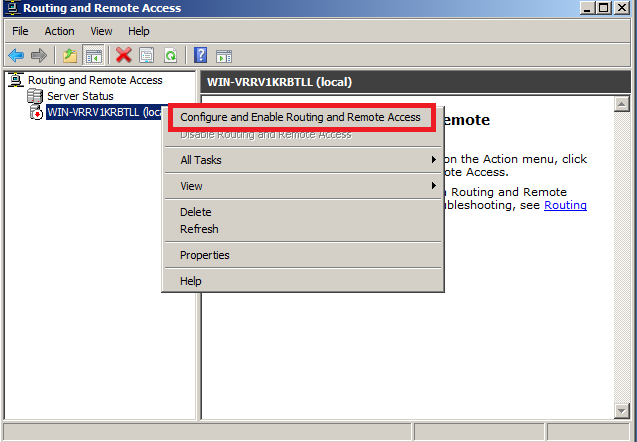
* Máy FILE SERVER:



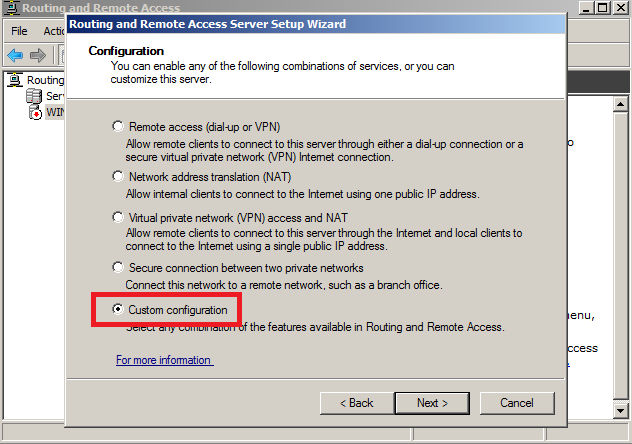
* **Bước 2**: Cấu hình trên máy PPTP SERVER
* **Mở Routing and remote access**:



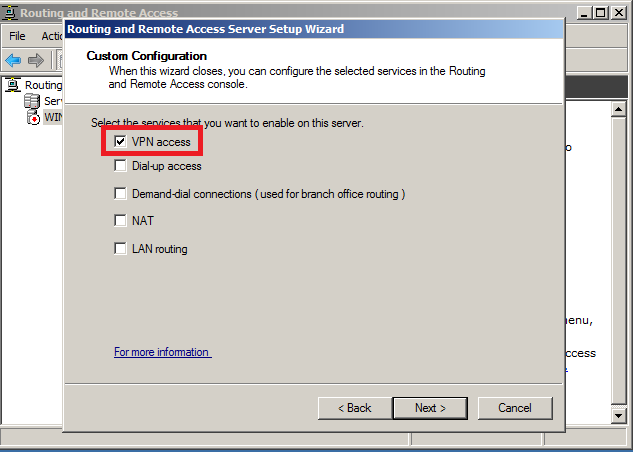
* Nhấp phải chuột lên tên Server chọn **Configure and Enable Routing and Remote Access**:



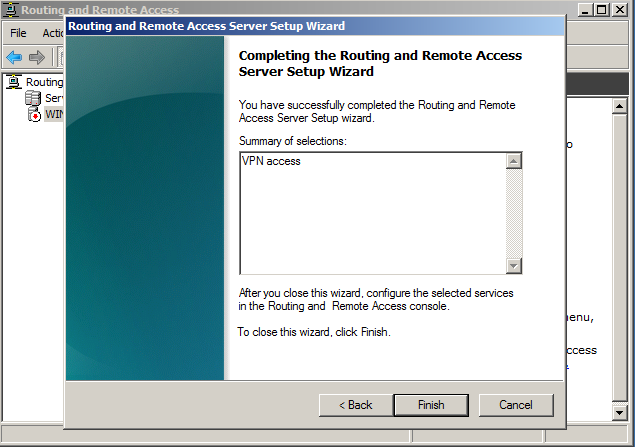
* Chọn **Custom configuration**:



* Chọn **VPN**:



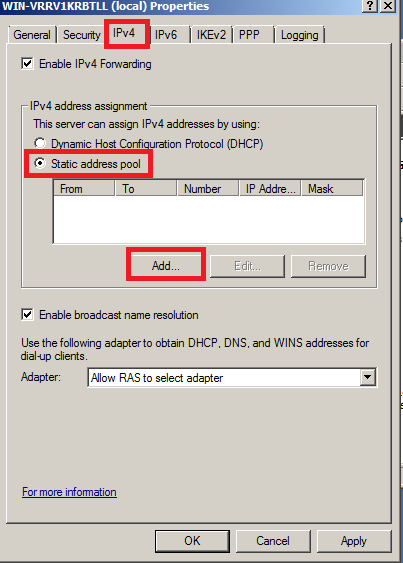
* Chọn **Finnish** để kết thúc:



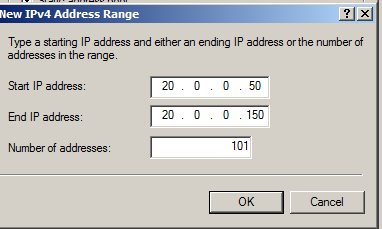
* Màn hình kết quả:



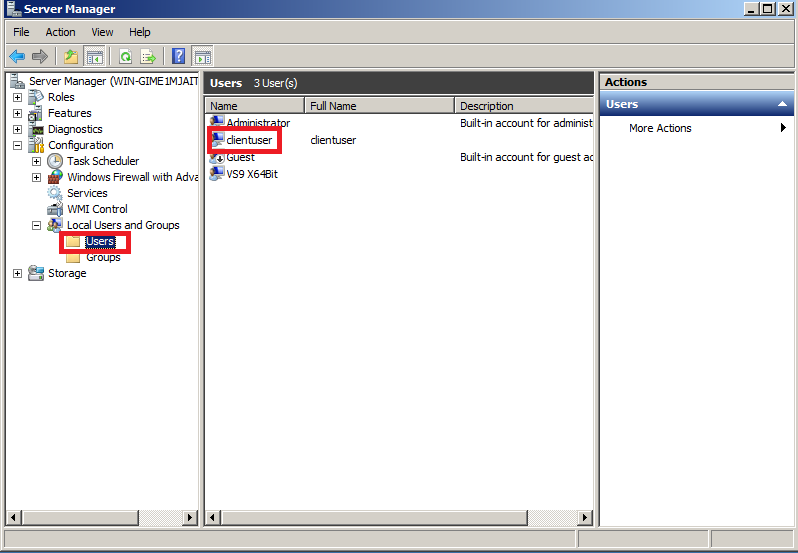
* Chuột phải tên server chọn **properties** → Tab **ipv4** → Check **Static address pool**:



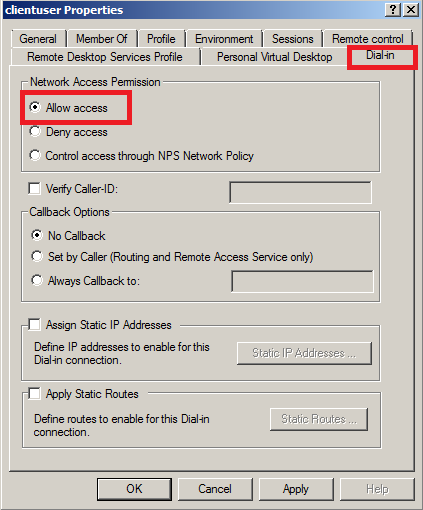
* Chọn **New**:



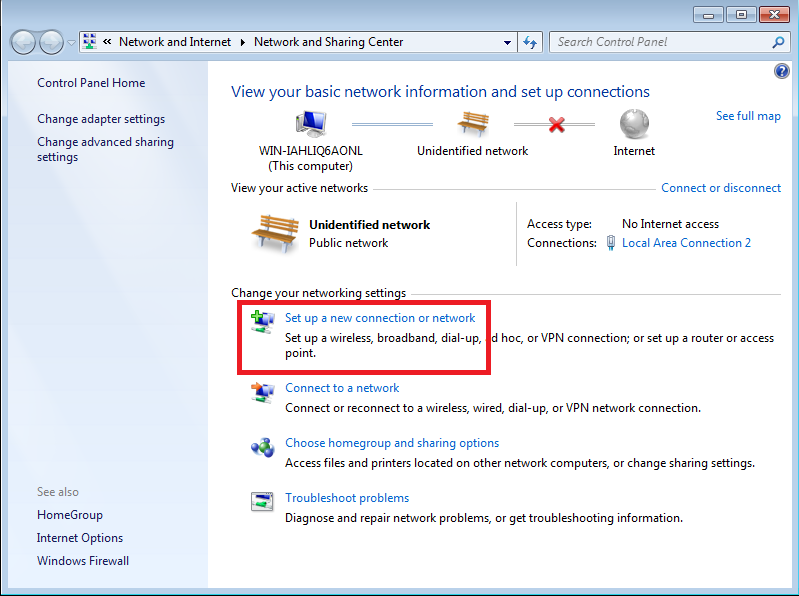
* **Bước 3**: Tạo User trên máy PPTP SERVER để CLIENT dùng User này kết nối:



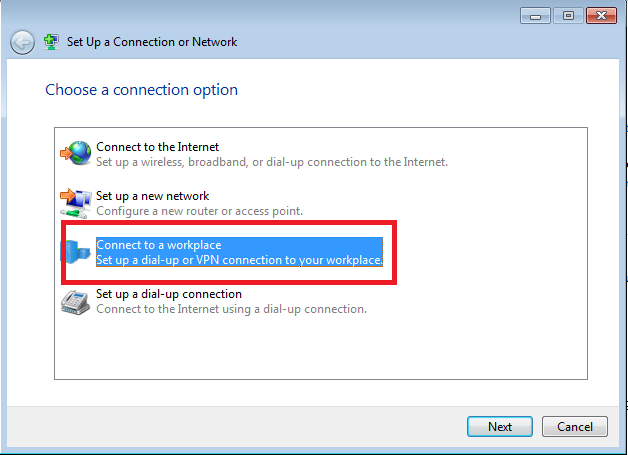
* Cấp quyền Allow Access cho uer clientuser: Kích chuột phải lên clientuser chọn **properties →Tab Dial-in →** check vào **Allow Access**:



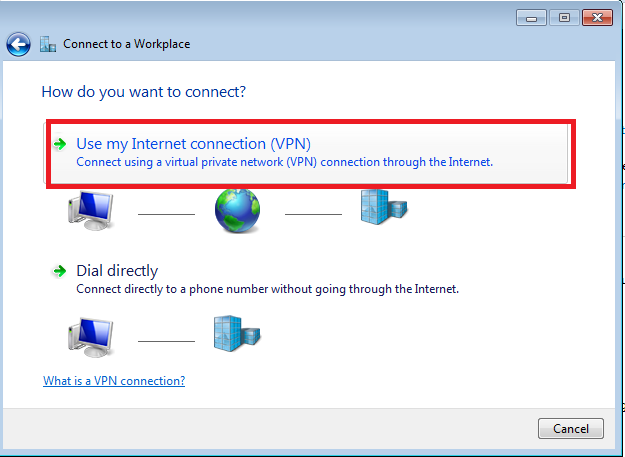
* Bước 4: Tạo kết nối từ máy CLIENT:
* Mở **Netwwork connections** → Nhấn vào **network and sharing center** → Chọn **setup a connect or network**:



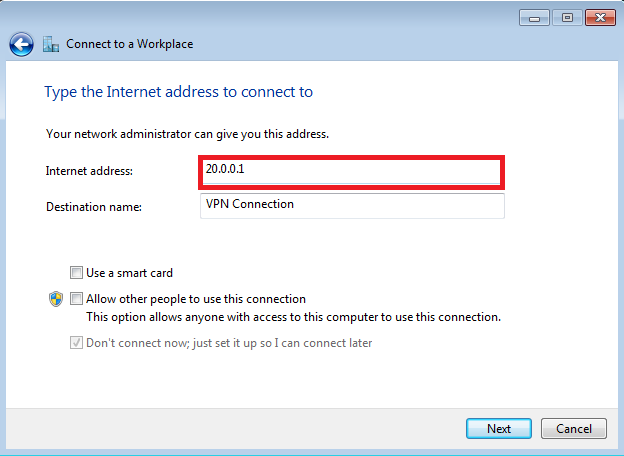
* Chọn **connected to a workplace**:



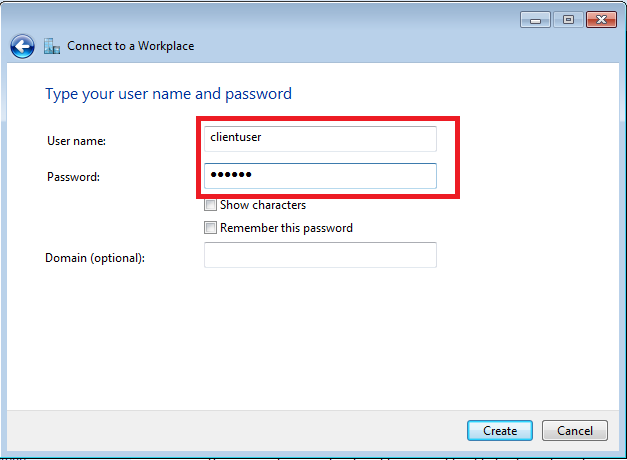
* Chọn **use internet connection (VPN):**



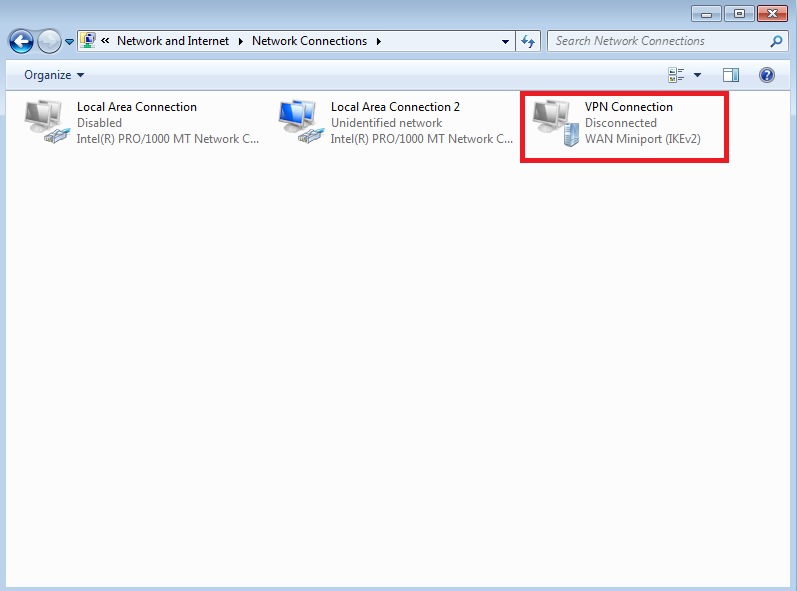
* Nhập IP card Wan của PPTP SERVER vào:



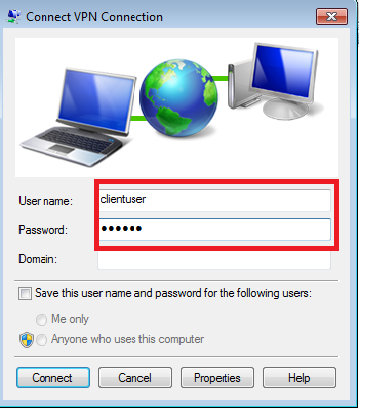
* Nhập user và password vào để kết nối đến PPTP SERVER:



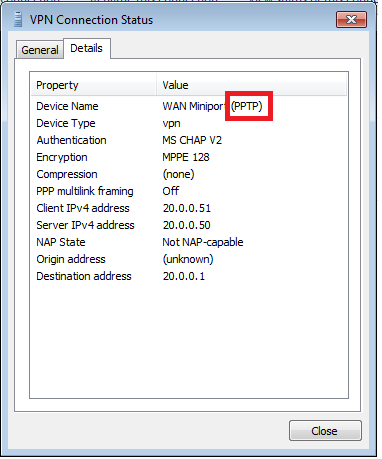
* Nhập xong sẽ hiện ra biểu tượng “ VPN connection” như hình dưới:



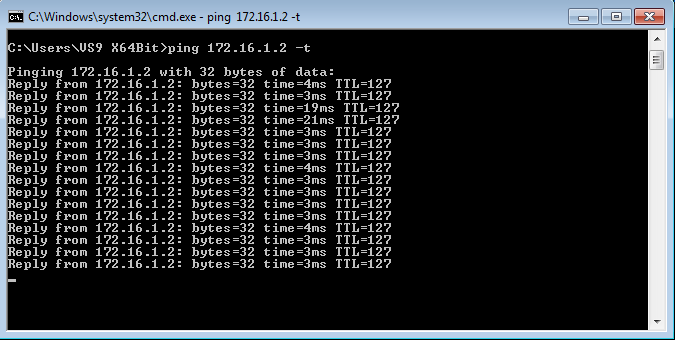
* Connect từ CLIENT:



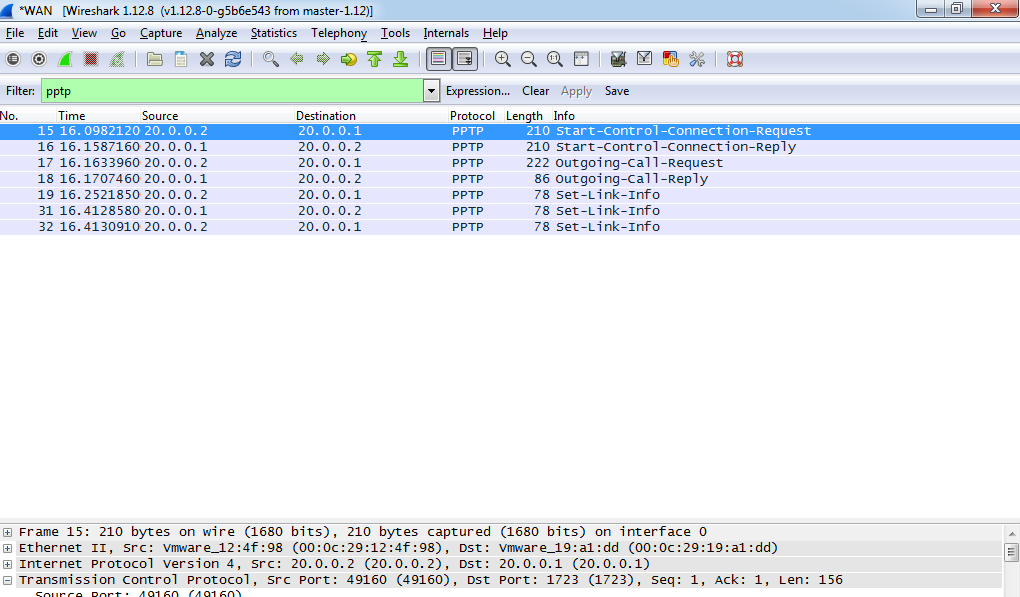
* Xem giao thức PPTP:



* Client ping pc trong mạng:

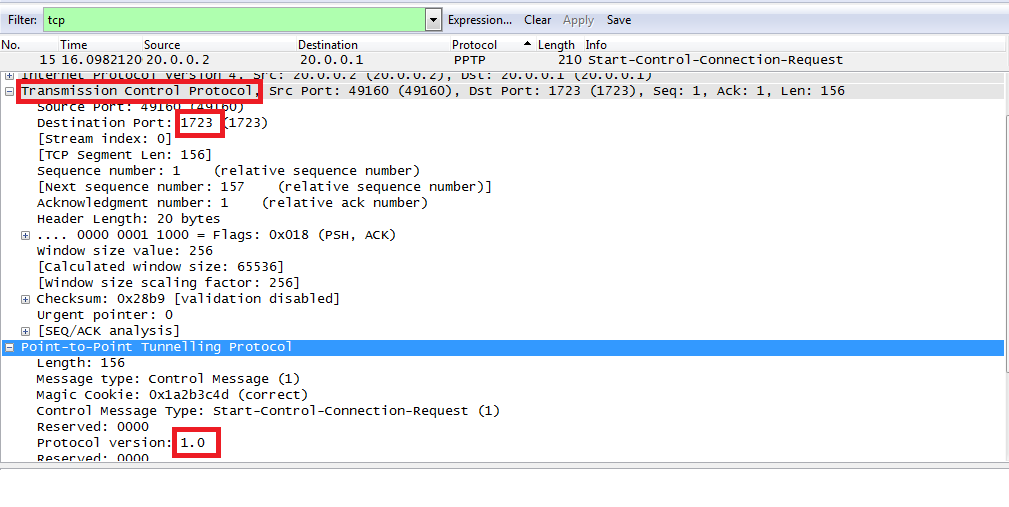


**3.6 Phân tích các gói tin PPTP trên Wireshark**



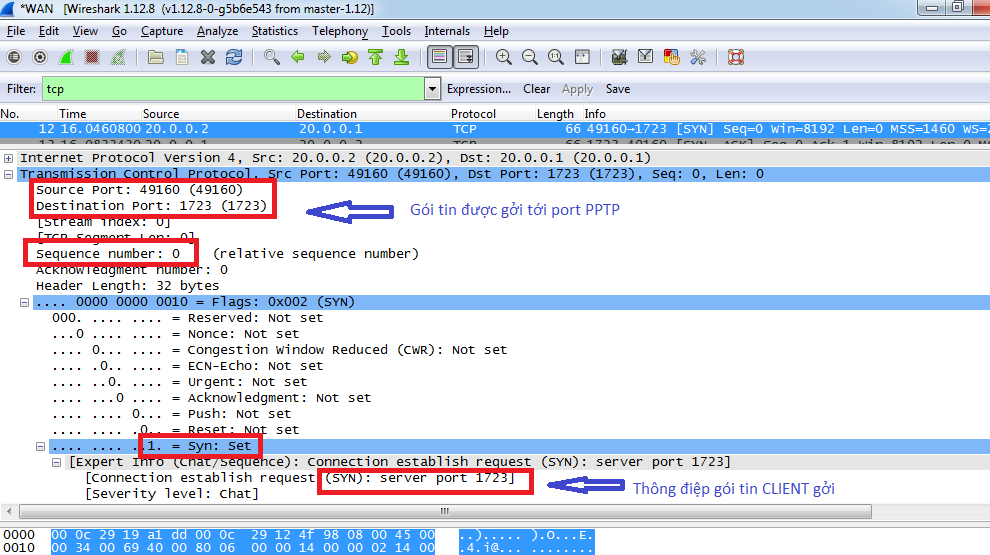
Hình 3.3 Các gói tin PPTP

PPTP chạy trên nền TCP, port 1723, sử dụng phiên bản 1.0:

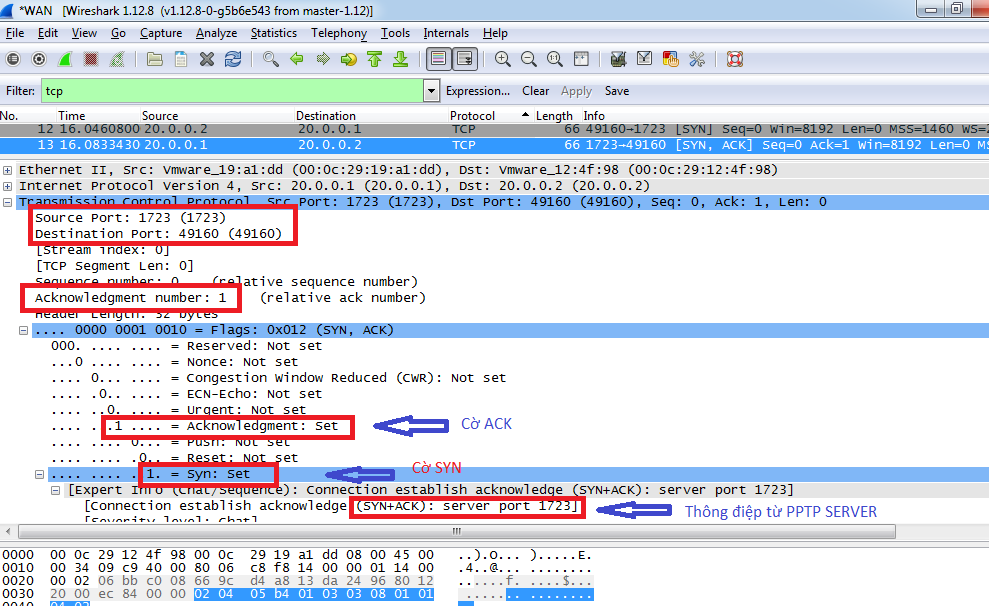


Hình 3.4 Thông tin của giao thức PPTP

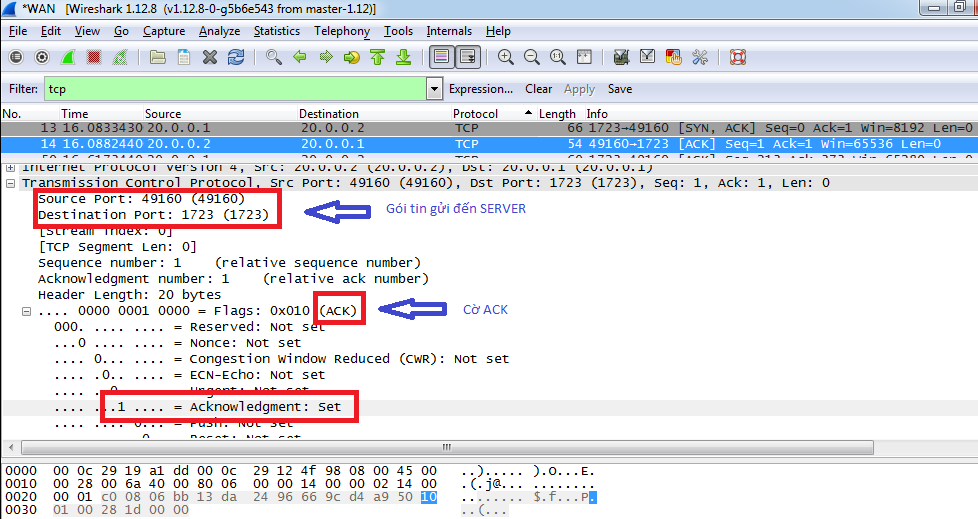
Tiến trình tạo kết nối VPN sử dụng PPTP được bắt đầu bằng tiến trình bắt tay 3 bước của giao thức TCP. CLIENT sẽ mở *port* gửi gói tin TCP SYN đến *port 1723* của SERVER để mở kết nối dich vụ VPN:

Hình 3.5 Gói tin CLIENT gửi đến SERVER yêu cầu mở Port kết nối

Sau khi nhận yêu cầu mở kết nối từ CLIENT thì SERVER sẽ tiến hành gửi lại gói tin TCP SYN-ACK chấp nhận thiết lập kết nối:

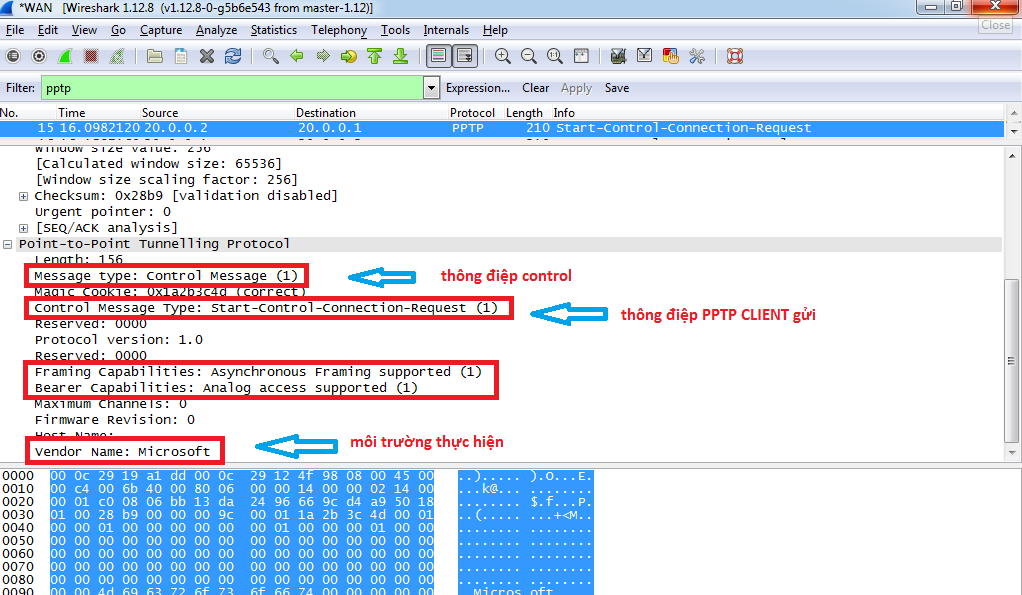
 Hình 3.6 Gói tin mở kết nối từ SERVER gửi cho CLIENT

CLIENT gửi lại gói tin TCP ACK để chấp nhận kết nối này:



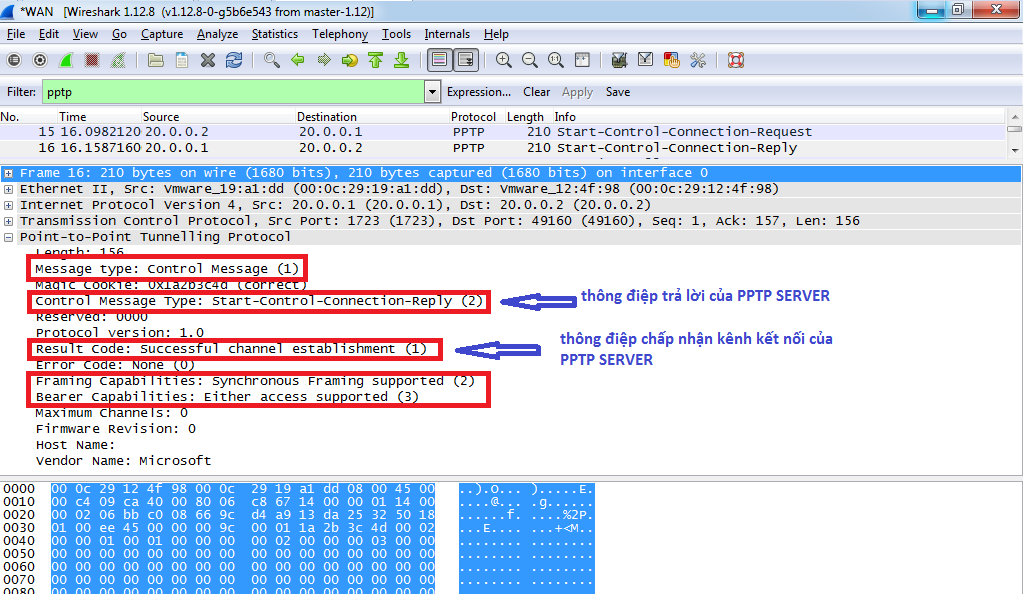
Hình 3.7 Gói tin CLIENT gửi SERVER để chấp nhận kết nối

Khi kết nối được mở, CLIENT sẽ gửi gói tin *Control Messenger* bằng giao thức PPTP với yêu cầu *Start-Control-Connection-Request*, gói tin chứa thông tin về môi trường hoạt động của VPN là nhà cung cấp *Microsoft*:



Hình 3.8 Gói tin Start-Control-Connection-Request do CLIENT gửi

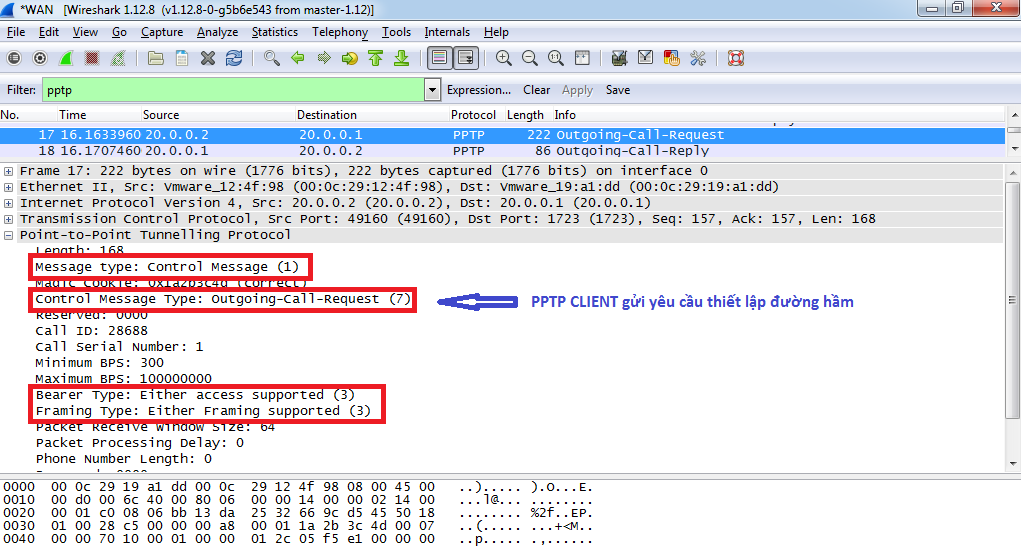
Sau khi nhận được yêu cầu từ CLIENT thì SERVER sẽ *Reply* lại gói thông tin thông qua giao thức PPTP:



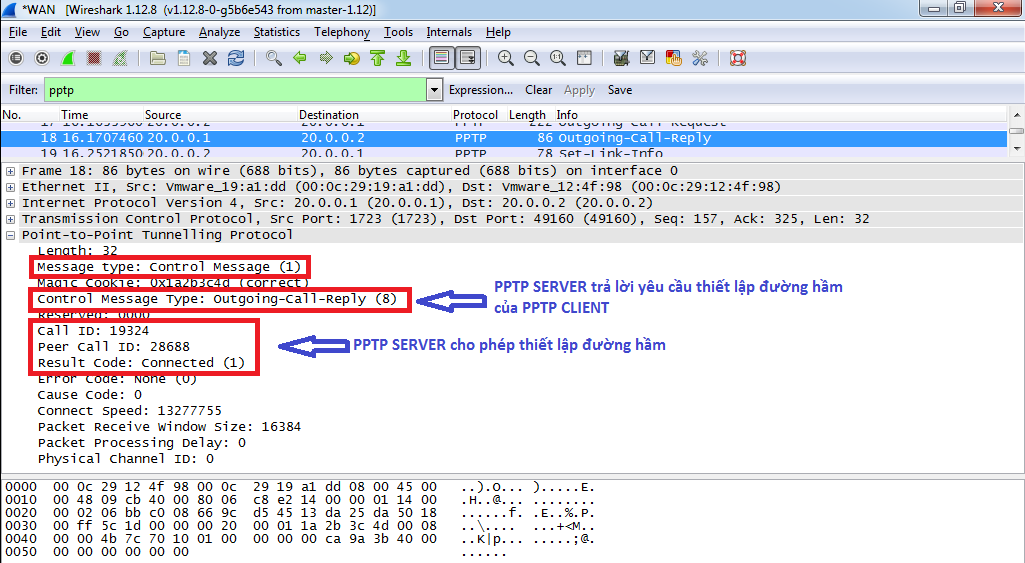
Hình 3.9 Gói tin Start-Control-Connection-Reply do PPTP SERVER phản hồi

PPTP SERVER trả về kết quả *Result code*: *Successful channel establishment* chấp nhận kênh kết nối, *Synchronous Framing supported* ( hỗ trợ khung đồng bộ), *Either access supported* ( hỗ trợ truy cập song công).

Phía PPTP CLIENT tiếp tục gửi gói tin *Outgoing-Call-Request*:

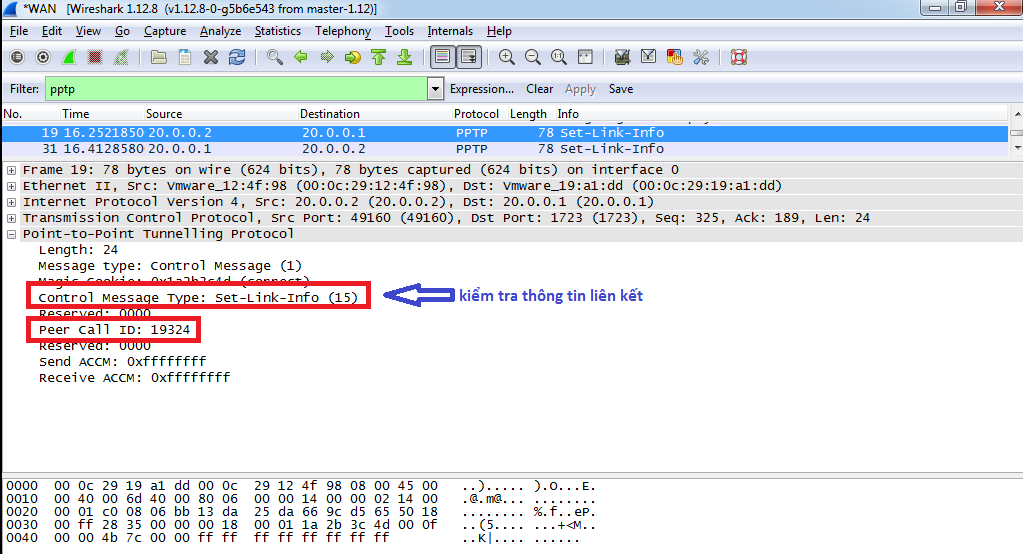
Hình 3.10 Outgoing-Call-Request từ CLIENT

Phía PPTP SERVER sau khi nhận được gói tin yêu cầu này thì sẽ Reply lại CLIENT một gói tin thông báo chấp nhận thành lập kết nối:



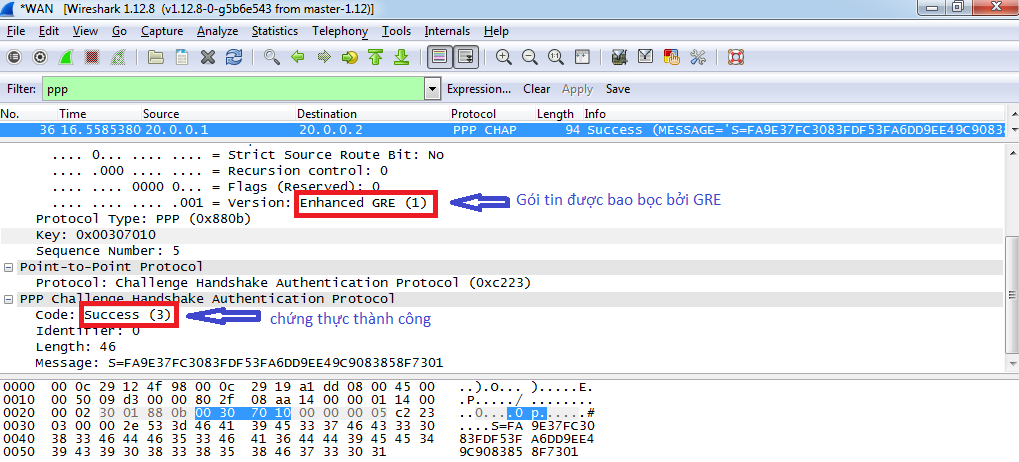
Hình 3.11 Gói tin Outgoing-Call-Reply từ PPTP SERVER

Sau đó, PPTP SERVER và CLIENT sẽ tiến hành gửi gói *Set-Link-Info* sử dụng *Call ID* để thiết lập và kiểm tra đường truyền:



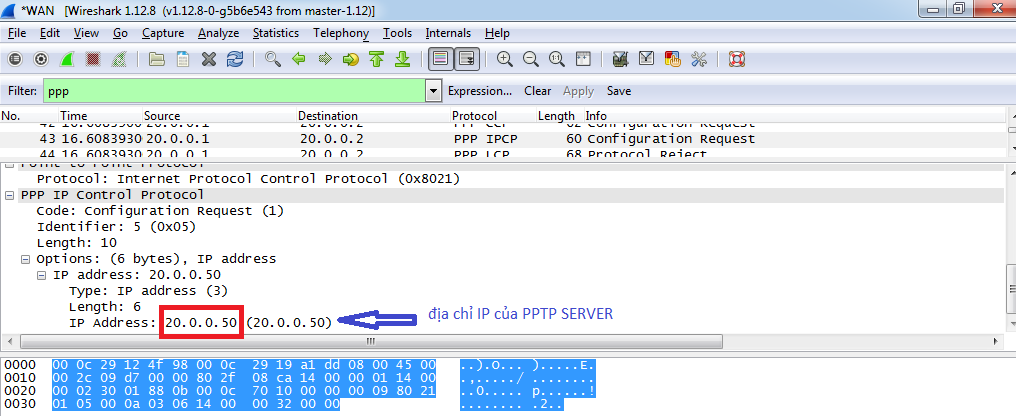
Hình 3.12 Gói tin thiết lập, kiểm tra

Sau khi quá trình mã hóa dữ liệu từ CLIENT thì SERVER sẽ tiến hành tạo mãng băm và thực hiện so sánh với mãng băm nhận từ CLIENT. Nếu kết quả giống nhau thì SERVER sẽ gửi gói tin *Success* đến CLIENT:



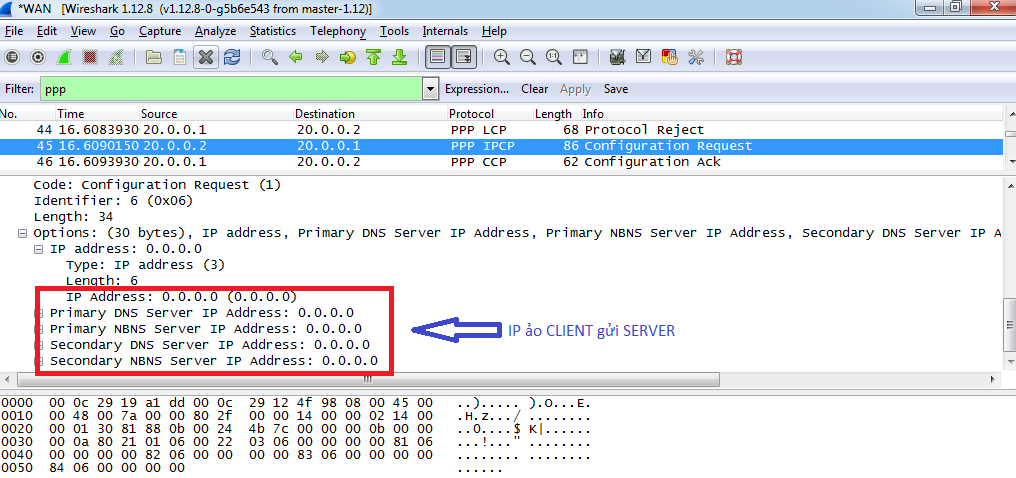
Hình 3.13 Gói tin chứng thực thành công gửi từ PPTP SERVER

Sau khi thành công, PPTP SERVER sẽ tiến hành cấp phát địa chỉ IP cho CLIENT. Địa chỉ IP sẽ nằm trong khoảng giới hạn mà ta đã quy định trong qua trình cài đặt VPN:



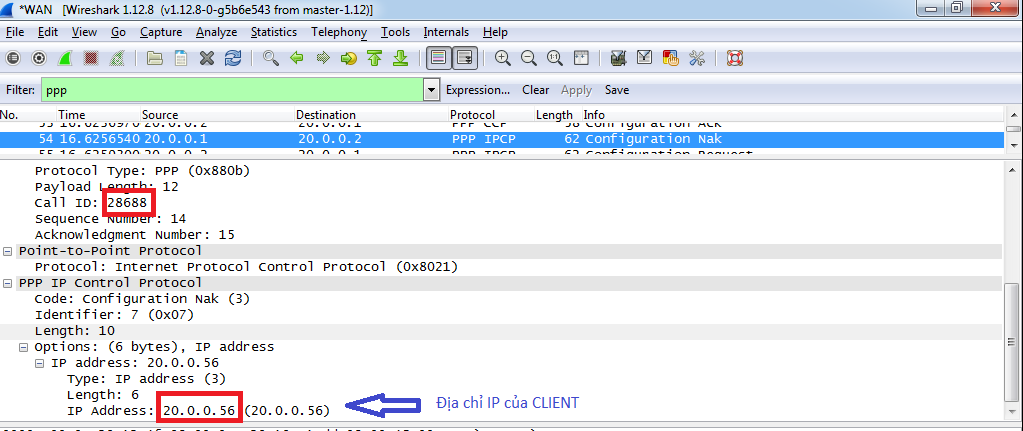
Hình 3.14 Địa chỉ IP ảo của PPTP SERVER

CLIENT gửi yêu cầu cấu hình IP bằng giao thức PPP IPCP:



Hình 3.15 Gói tin yêu cầu IP ảo từ CLIENT gửi đến SERVER

SERVER sẽ gửi đến CLIENT đại chỉ IP thông qua PPP IPCP:



Hình 3.16 Thông số IP của CLIENT nhận từ SERVER

Sau quá trình này thì kết nối VPN đã thành công.

**Chương 4: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN**

**4.1 Kết luận**

*4.1.1 Ưu điểm*

* Giao thức PPTP dễ dàng sử dụng vì được tích hợp sẵn trong nhiều hệ điều hành như: Window NT Server, Workstation.
* Giao thức PPTP có thể tạo đường hầm cho tất cả các máy chủ mà RAS cho phép.
* Dễ thi hành.
* Sử dụng địa chỉ IP Private một cách đồng bộ.

*4.1.2 Nhược điểm*

Nhược điểm lớn nhất là tính bảo mật và toàn vẹn dữ liệu còn yếu kém.

**4.2 Hướng phát triển của đồ án**

* Giao thức PPTP được áp dụng thực tế ở các doanh nghiệp, công ty.
* Sử dụng các giao thức VPN khác bảo mật hơn như: L2TP, SSTP, IPSEC… nhằm ngăn chặn các cuộc tấn công của hacker.

**TÀI LIỆU THAM KHẢO**

[1] <https://en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol>

[2]<http://searchnetworking.techtarget.com/definition/Point-to-Point-Tunneling-Protocol>

[3]<http://www.chimica.unipd.it/luigino.feltre/pubblica/unix/winnt_doc/pppt/understanding_pptp.html>