

MỤC LỤC

	Trang
PHẦN I	11
TỔNG QUAN VỀ DoS VÀ CÁC KỸ THUẬT TẤN CÔNG	
Chương 0. GIỚI THIỆU TỔNG QUAN VỀ DoS.....	11
Chương 1. TỔNG QUÁT VỀ MẠNG INTERNET.....	12
I) Giới thiệu tổng quan về mạng internet và lịch sử phát triển của mạng Internet qua các thời kỳ.....	12
1.1) Định nghĩa về mạng Internet.....	12
1.2) Lịch sử phát triển của mạng Internet.....	13
II) Giao thức truyền thông và các mô hình tham chiếu.....	14
2.1) Giao thức truyền thông.....	14
2.2) Mô hình tham chiếu OSI.....	15
III) Tổng quan về bộ giao thức TCP/IP.....	23
3.1) Khái niệm về TCP/IP.....	23
3.2) Các giao thức của bộ giao thức TCP/IP – Các giao thức tầng Application.....	24
3.3) Các Giao Thức Tầng Transport.....	35
3.4) Các giao thức tầng internet.....	43
3.5) Các giao thức tầng Network Access.....	50
Chương 2. Tấn Công Từ Chối Dịch Vụ (Denail of Service).....	51
I) Giới thiệu về tấn công từ chối dịch vụ (DoS).....	51
1.1) Định nghĩa về tấn công từ chối dịch vụ.....	51
1.2) Đặc điểm của tấn công từ chối dịch vụ.....	52
1.3) Phân loại các kiểu tấn công từ chối dịch vụ.....	52

II) Chi tiết về các kỹ thuật tấn công từ chối dịch vụ.....	55
2.1) Tấn công kiểu SYN Flood.....	55
2.2) Kiểu tấn công Land Attack.....	57
2.3) Tấn công kiểu Smurf Attack.....	58
2.4) tấn công kiểu Ping Of Death.....	60
2.5)Tấn công kiểu DDoS.....	60

Chương 3 Xây Dựng Thủ Nghiệm Mô Hình Tấn Công

I) Giới thiệu về mô hình.....	63
1.1) Mô Hình Mạng Dùng Cho Cuộc Tấn Công theo thực tế.....	63
1.2) Mô Hình Mạng Dùng Cho Cuộc Tấn Công được xây dựng trong luận văn.....	64
1.3) Cấu hình cho Router để các mạng có thể thông nhau.....	66
II) Giới thiệu về công cụ tấn công Apache DoS.....	74
III) Thực hiện quá trình tấn công DoS.....	74
PHẦN II	77

Chương 4

Phòng Chống Tấn Công DoS Với Tập Lệnh TCP Intercept

I) Các phương pháp phòng chống tấn công.....	77
1.1) Xây dựng hệ thống FIREWALL.....	78
II) Giới thiệu về tập lệnh TCP intercept của Router Cisco 7200.....	80
2.1) Access Control List	80
2.2) Thiết lập cấu hình cho Router cisco phòng ngừa một số kiểu tấn công DoS thường gặp.....	85
2.3) các chế độ bảo vệ của TCP intercept.....	86

2.4) cấu hình TCP intercept.....	89
III) Cấu Hình TCP Intercept Ở Chế Độ Watch Mode cho mô hình thực nghiệm.....	92
Chương 5.....	95

Phát Hiện Tấn Công DoS Dùng NetFlow.

5.1) Nagios.....	95
5.2) MRTG: Phần mềm giám sát luồng chuyển động.....	95
5.3) ManageEngine Opmanager.....	96
5.4) NetFlow Analyzer.....	97

Chương 6. Tổng Kết Những Điều Đạt Được Và Chưa Đạt Được Trong Luận Văn

6.1) Những điều đạt được.....	102
6.2) Những điều chưa đạt được.....	102
6.3) Hướng phát triển.....	103
Phụ lục.....	104

PHẦN I.**TỔNG QUAN VỀ DoS VÀ CÁC KỸ THUẬT TẤN CÔNG****Chương 0. GIỚI THIỆU TỔNG QUÁT VỀ TẤN CÔNG****TỪ CHỐI DỊCH VỤ**

Tấn công DoS là phương pháp tấn công vào các hệ thống cung cấp dịch vụ dựa vào mạng internet. Đây là phương pháp tấn công khá đơn giản được giới tin tặc sử dụng vào các mục đích riêng. Tuy là phương pháp tấn công được ra đời sớm và rất dễ phát động cuộc tấn công nhưng lại rất khó để nhận biết và chống đỡ. Bản thân của phương pháp tấn công DoS là dùng số lượng máy lớn trên internet để tấn công vào các hệ thống cung cấp dịch vụ.

Mặt khác vì vấn đề chứng thực trên internet không cao, nên tấn công DoS rất khó tìm ra thủ phạm vì người tấn công có thể che giấu các vết tích bằng cách giấu hoặc thay đổi IP của mình.

Tóm lại. Tấn công từ chối dịch vụ (Tấn công DoS) là hành động của giới tin tặc, đây có thể là hành động của một người hoặc một nhóm người nào đó. Tấn công vào một mạng máy tính nhằm làm đình trệ hoạt động của mạng đó.

Chương I.**TỔNG QUAN VỀ MẠNG INTERNET****I) Giới thiệu tổng quan về mạng internet và lịch sử phát triển của mạng internet qua các thời kỳ.****1.1) Định nghĩa về mạng internet.**

Internet là một hệ thống thông tin toàn cầu, có thể được truy nhập công cộng. bao gồm nhiều mạng máy tính được liên kết lại với nhau. Hệ thống internet truyền thông tin và dữ liệu theo kiểu chuyển mạch gói. dựa trên một bộ giao thức liên mạng đã được chuẩn hóa là bộ giao thức TCP/IP. Hệ thống này bao gồm hàng ngàn mạng máy tính nhỏ hơn của các doanh nghiệp, của các viện nghiên cứu, các trường đại học và các máy tính đơn của hộ gia đình...tất cả cung cấp một khối lượng thông tin khổng lồ lên mạng internet.

Mạng internet mang lại rất nhiều tiện ích hữu dụng cho người dùng trên toàn thế giới. Một trong những tiện ích phổ thông nhất của mạng internet là hệ thống thư điện tử(email), trò chuyện trực tiếp (chat), bộ máy truy tìm dữ liệu (search engine), các dịch vụ thương mại điện tử, chuyển ngân và các lớp học trực tuyến.

Nguồn thông tin khổng lồ kèm theo các dịch vụ tương ứng, chính là hệ thống các trang web được liên kết với nhau bằng các siêu liên kết (Hyperlink) ‘WWW’ và các địa chỉ URL.

Có thể kết nối internet bằng nhiều cách, có thể kết nối bằng cách quay số, bằng băng thông rộng, bằng mạng không dây, bằng vệ tinh hay là các thiết bị cầm tay.

Hiện tại có rất nhiều công cụ để duyệt web như:

Internet Explorer có tích sẵn trong microsoft windows và phiên bản mới nhất hiện tại là IE7.

Hay là Mozilla và Mozilla firefox của tập đoàn Mozilla.

Netscape Navigator của Netscape.

Opera của opera software.

Safari của apple computer.

1.2) Lịch sử phát triển của mạng Internet.

Thuật ngữ Internet xuất hiện lần đầu tiên vào khoảng năm 1974, lúc đó mạng được gọi là ARPANET.

ARPANET là một hệ thống mạng bao gồm mạng của tổ chức quân đội, của các trường đại học và các tổ chức nghiên cứu. Hệ thống mạng ARPANET được phát triển bởi trung tâm nghiên cứu cao cấp (Advanced Research Project Agence viết tắt là ARPA). Trung tâm nghiên cứu này thuộc bộ quốc phòng MỸ (Department Of Defense - DOD). Vào cuối những năm 1960 đầu những năm 1970 trung tâm nghiên cứu cao cấp này chịu trách nhiệm chính trong việc phát triển hệ thống mạng ARPANET với mục đích dùng cho quân đội và hỗ trợ các dự án nghiên cứu khoa học lúc bấy giờ.

Đầu những năm 1980 một bộ giao thức mới được đưa ra làm bộ giao thức chuẩn cho hệ thống mạng ARPANET và các mạng của DOD với tên gọi là DARPA Internet Protocol suite. Thường được gọi là bộ giao thức TCP/IP hay còn gọi tắt là TCP.

Vào năm 1983 bộ giao thức với tên gọi là TCP/IP chính thức được công nhận là một bộ giao thức chuẩn đối với ngành quân sự MỸ. Và từ đó tất cả các máy tính nối với mạng ARPANET đều phải sử dụng bộ chuẩn mới này.

Năm 1984 ARPANET được chia thành 2 phần. phần thứ nhất vẫn gọi là ARPANET và được dùng để phục vụ cho việc nghiên cứu và phát triển. Phần thứ 2 gọi là MILNET là mạng dùng cho mục đích quân sự.

Giao thức TCP/IP ngày càng thể hiện rõ các điểm mạnh của nó, quan trọng nhất là khả năng liên kết các mạng khác với nhau một cách dễ dàng. Chính điều này cùng với các chính sách mở cửa đã cho phép các mạng dùng cho nghiên cứu và thương mại kết nối được với ARPANET, thúc đẩy việc tạo ra một siêu mạng (SuperNetwork). Năm 1980, ARPANET được đánh giá là mạng trụ cột của Internet.

Mốc lịch sử quan trọng của Internet được xác lập vào giữa thập niên 1980. Khi tổ chức khoa học quốc gia Mỹ NSF thành lập mạng liên kết các trung tâm máy tính lớn với nhau gọi là NSFNET. Nhiều doanh nghiệp đã chuyển từ ARPANET sang NSFNET và

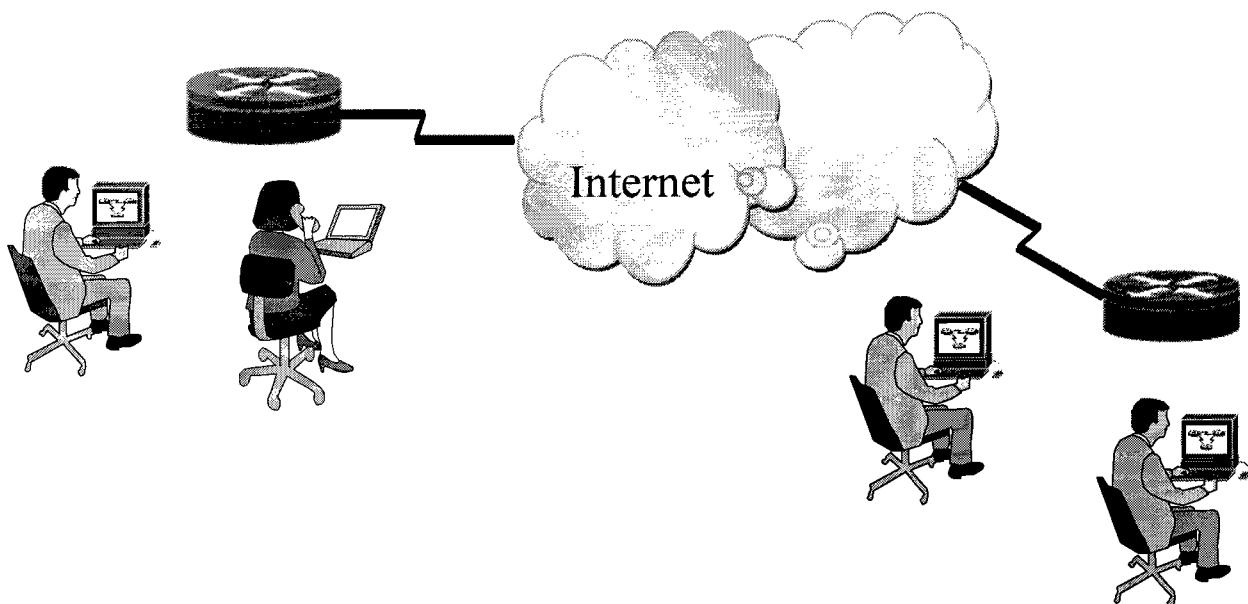
do đó sau gần 20 năm hoạt động, ARPANET không còn hiệu quả đã ngừng hoạt động vào khoảng năm 1990.

Sự hình thành mạng xương sống của NSFNET và những mạng vùng khác đã tạo ra một môi trường thuận lợi cho sự phát triển của Internet. Tới năm 1995, NSFNET thu lại thành một mạng nghiên cứu còn Internet thì vẫn tiếp tục phát triển cùng với bộ giao thức chuẩn TCP/IP.

Với khả năng kết nối mở như vậy, Internet đã trở thành một mạng lớn nhất trên thế giới, mạng của các mạng, xuất hiện trong mọi lĩnh vực thương mại, chính trị, quân sự, nghiên cứu, giáo dục, văn hóa, xã hội... Cũng từ đó, các dịch vụ trên Internet không ngừng phát triển tạo ra cho nhân loại một thời kỳ mới: kỷ nguyên thương mại điện tử toàn cầu trên Internet.

II) Giao thức truyền thông và các mô hình tham chiếu.

2.1) Giao thức truyền thông.



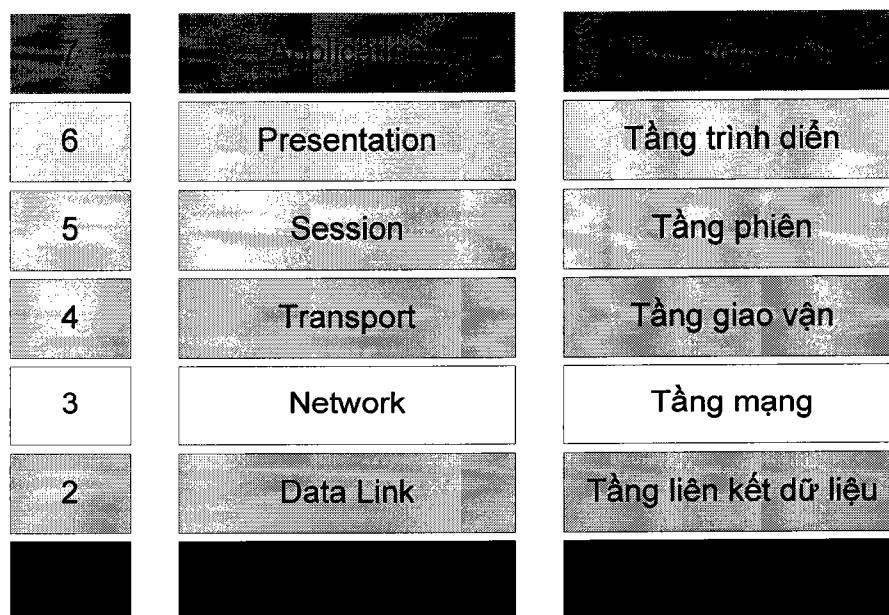
Hình 1. Mô hình mạng máy tính.

Để các mạng máy tính khác nhau làm việc được với nhau thì cần thiết phải có một bộ các phần mềm cùng làm việc theo một chuẩn nào đó. Quy tắc truyền thông là một tập hợp các quy tắc quy định phương thức truyền và nhận giữa các mạng máy tính với nhau.

Các mạng máy tính ở hiện tại được thiết kế bằng cách phân chia cấu trúc ở mức độ cao nhằm giảm độ phức tạp khi thiết kế, các giao thức mạng thường được chia thành các tầng (layer). Mỗi tầng được xây dựng dựa trên dịch vụ của tầng dưới nó và cung cấp dịch vụ cho tầng cao hơn.

2.2) Mô hình tham chiếu OSI

Mô hình OSI là viết tắt của (Open System Interconnection reference model). Là mô hình tham chiếu dùng để kết nối các hệ thống mở. Được tổ chức ISO (International Standard Organization) là tổ chức tiêu chuẩn hóa quốc tế đưa ra vào năm 1984. Các hệ thống có thể kết nối được với nhau nếu dùng chung một số quy tắc.



Hình 2. Kiến trúc phân tầng mô hình tham chiếu OSI.

Mô hình tham chiếu OSI được chia thành 7 tầng như hình vẽ trên. Chức năng của từng tầng được trình bày bên dưới.

2.2.1) Tầng vật lý: Tầng vật lý là tầng thấp nhất trong mô hình tham chiếu. Tầng này có chức năng mô tả các đặc trưng vật lý của mạng như: Loại cáp nào được dùng để nối các thiết bị mạng, các đầu nối nào được dùng, chiều dài tối đa của cáp khi nối mạng.....Mặt khác các đặc trưng vật lý còn có chức năng cung cấp các đặc trưng về điện của các tín hiệu được dùng để chuyên tín hiệu trên cáp từ một máy này đến một máy khác trên mạng. Các kỹ thuật nối mạng và tốc độ truyền tải dữ liệu trên cáp.

Tầng vật lý dùng các giá trị nhị phân 0 và 1 để biểu diễn trạng thái, các bit ở tầng vật lý truyền lên sẽ được các tầng trên xác định rõ.

Ví dụ: Tiêu chuẩn Ethernet cho cáp xoắn đôi 10 Base T xác định rõ các đặc trưng điện của cáp xoắn đôi, kích thước và dạng của các đầu nối, chiều dài tối đa của cáp khi nối mạng.

Khác với các tầng khác, tầng vật lý không có gói tin riêng do vậy tầng vật lý không có phần đầu (header) chứa thông tin điều khiển. Dữ liệu được truyền đi theo dòng bit. Có một giao thức tồn tại ở tầng vật lý dùng để quy định phương thức truyền (truyền đồng bộ, truyền không đồng bộ), tốc độ truyền....

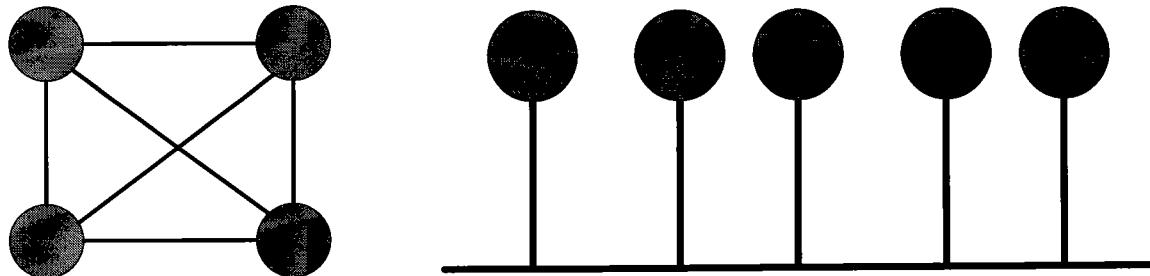
Các giao thức xây dựng cho tầng vật lý được phân thành 2 loại: Giao thức sử dụng phương thức truyền thông không đồng bộ (asynchronous) và thức sử dụng phương thức truyền thông đồng bộ (synchronous).

Phương thức truyền không đồng bộ: Không có một tín hiệu quy định cho sự đồng bộ giữa các bit giữa các máy truyền và nhận. Trong quá trình gửi và nhận dữ liệu các máy sử dụng các bít đặc biệt là START và STOP, các bít này được dùng để tách các xâu bit dùng để biểu diễn cho các ký tự trong dòng dữ liệu cần truyền đi. Giao thức này cho phép truyền một ký tự đi bất cứ khi nào mà không cần quan tâm đến các tín hiệu đồng bộ trước đó.

Phương thức truyền đồng bộ: Phương thức này cần có sự đồng bộ giữa các máy gửi và nhận, khi dùng phương thức này thì nó chèn các ký tự đặc biệt như: SYS(synchronous) , EOT(End Of Transmission) hay đơn giản hơn là chèn một cái cờ (Flag) vào giữa dòng dữ liệu của máy gửi để báo hiệu cho máy nhận, biết được đang đến hoặc đã đến.

2.2.2) *Tầng liên kết dữ liệu:* Là tầng mà ở đó ý nghĩa được gán cho các bít được truyền trên mạng, tầng liên kết dữ liệu phải quy định các dạng như: Kích thước, địa chỉ máy gửi và máy nhận của mỗi gói tin khi được gửi đi. Tầng này phải xác định được cơ chế truy nhập thông tin trên mạng và phương tiện gửi mỗi gói tin sao cho nó được đưa đến đúng người nhận.

Tầng liên kết dữ liệu có 2 phương thức liên kết dựa trên cách kết nối các máy tính, đó là phương thức “Một Điểm - Một Điểm” và “Một Điểm - Nhiều Điểm”. Với phương thức “Một Điểm - Một Điểm” thì các đường truyền riêng biệt được thiết lập để nối các cặp máy tính lại với nhau. Còn phương thức “Một Điểm - Nhiều Điểm” thì tất cả các máy tính phân chia chung một đường truyền vật lý.



Hình 3. Hai Phương thức truyền trong tầng Data Link.

Tầng liên kết dữ liệu cũng cung cấp các phương thức phát hiện và sửa lỗi cơ bản để đảm bảo dữ liệu khi nhận được giống hoàn toàn dữ liệu khi gửi đi. Nếu một gói tin có lỗi và không sửa được thì tầng liên kết dữ liệu phải chỉ ra được và thông báo cho nơi gửi gói tin biết để gửi lại.

Có 2 loại giao thức được dùng trong tầng liên kết dữ liệu là: Các giao thức hướng ký tự và các giao thức hướng bít. Các giao thức hướng ký tự được xây dựng dựa trên các ký tự đặc biệt của một bộ mã chuẩn nào đó (như ASCII), trong khi cấu trúc hướng bit thì dùng các chuỗi nhị phân (xâu bít) để xây dựng các phần tử của xâu bít (đơn vị dữ liệu) và khi nhận dữ liệu thì dữ liệu sẽ được tiếp nhận lần lượt từng bít một.

2.2.3) Tầng mạng(network layer): Tầng mạng có nhiệm vụ tìm đường cho các gói tin từ mạng này đến mạng khác hay còn gọi là định tuyến cho các gói tin (Routing), nó xác định chuyển hướng, vạch đường cho các gói tin trên mạng. Các gói tin này có thể phải đi qua nhiều chặng trước khi đến đích cuối cùng. Một trong những chức năng quan trọng của tầng mạng là tìm những tuyến đường không bị tắc nghẽn để truyền các gói tin đến đích.

Tầng mạng cung cấp các phương tiện để truyền các gói tin qua mạng, có thể truyền qua các mạng khác nhau với các kiểu mạng khác nhau. Vì vậy nó phải đáp ứng với nhiều kiểu mạng và nhiều kiểu dịch vụ được cung cấp bởi các mạng khác nhau. Hai

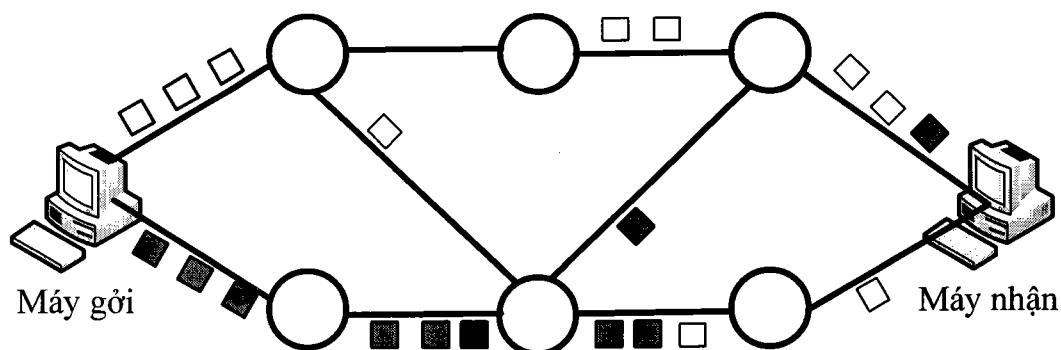
chức năng chính của mạng là tìm đường (Routing) và chuyển tiếp (replaying). Tầng mạng có vai trò quan trọng nhất khi liên kết 2 mạng khác nhau như liên kết mạng Ethernet và mạng Token ring, khi đó phải dùng một bộ tìm đường (quy định bởi tầng mạng) dùng để chuyển các gói tin từ mạng này sang mạng khác và ngược lại.

Đối với mạng chuyển mạch gói (Packet – Switch network) - gồm tập hợp các nút chuyển mạch gói nói với nhau bởi các liên kết dữ liệu, các gói dữ liệu được truyền từ một hệ thống mở đến một hệ thống mở khác trên mạng phải được chuyển qua một chuỗi các nút. mỗi nút nhận gói dữ liệu từ một đầu vào (incoming link) và chuyển tiếp nó tới một đường ra (outgoing link) hướng đến đích của gói dữ liệu. Như vậy tại mỗi nút trung gian nó phải thực hiện việc tìm đường và chuyển tiếp các gói dữ liệu.

Việc chọn đường là sự lựa chọn một con đường để truyền một đơn vị dữ liệu(một gói tin) từ trạm nguồn tới trạm đích của nó. Một kỹ thuật chọn đường phải thực hiện 2 chức năng chính sau đây:

- +Quyết định chọn đường tối ưu dựa trên các thông tin đã có về mạng tại thời điểm đó thông qua những tiêu chuẩn tối ưu nhất.

- +Cập nhập các thông tin về mạng, có nghĩa là cập nhập các thông tin dùng cho việc chọn đường, trên mạng luôn có sự thay đổi thường xuyên nên việc cập nhập thông tin dùng cho việc định tuyến là cần thiết.



Hình 4. chuyển các gói tin trong mạng chuyển mạch gói.

Có 2 phương để đáp ứng cho việc chọn đường là phương thức xử lý tập trung và phương thức xử lý tại chỗ:

Phương thức xử lý tập trung: Là phương thức được đặc trưng bởi sự tồn tại của một hoặc vài trung tâm điều khiển mạng. Các trung tâm này có chức năng lập ra các bảng đường đi tại từng thời điểm cho các nút, sau đó gởi các bảng này tới từng nút dọc theo con đường đã được chọn đó. Thông tin tổng thể của mạng dùng cho việc chọn đường chỉ cần cập nhập và lưu giữ tại các trung tâm điều khiển mạng.

Phương thức xử lý tại chỗ: Phương thức này được đặc trưng bằng việc chọn đường được thực hiện tại mỗi nút mạng. Trong từng thời điểm thì mỗi nút mạng phải duy trì các thông tin của mạng và tự xây dựng bảng chọn đường cho mình, như vậy các thông tin cần thiết cho việc chọn đường được cập nhập và lưu giữ tại mỗi nút mạng.

Các thông tin cần thiết được dùng cho việc chọn đường tại lớp mạng như sau:

- + Trạng thái của đường truyền
- + Thời gian trễ khi truyền trên mỗi đường dẫn.
- + Mức độ lưu thông trên mỗi đường.
- + Các tài nguyên khả dụng của mạng.

Khi có sự thay đổi trên mạng (ví dụ như có sự thay đổi về cấu trúc của mạng do sự cố tại một vài nút, sự phục hồi của một nút mạng bị hỏng, nối thêm một nút mới, hoặc thay đổi về mức độ lưu thông....) thì các thông tin trên cần cập nhập và lưu giữ tại cơ sở dữ liệu về trạng thái mạng.

2.2.4) *Tầng giao vận:* Tầng vận chuyển cung cấp các chức năng cần thiết giữa tầng mạng và các tầng trên, tầng giao vận là tầng cao nhất có liên quan đến các giao thức trao đổi dữ liệu giữa các hệ thống mở. Và đây cũng là tầng dưới cùng cung cấp cho người dùng các giao thức phục vụ cho việc vận chuyển.

Tầng giao vận (Transport Layer) là tầng cơ sở mà ở đó một máy tính của mạng chia sẽ thông tin với một máy khác. Tầng giao vận đồng nhất mỗi trạm bằng một địa chỉ duy nhất và quản lý sự kết nối giữa các trạm. Tầng giao vận cũng chia các gói tin lớn thành các gói tin nhỏ hơn trước khi chuyển đi. Thông thường tầng giao vận đánh số thứ tự các gói tin và đảm bảo chúng được chuyển đi đúng thứ tự.

Tầng giao vận là tầng cuối cùng chịu trách nhiệm về mức độ an toàn trong việc truyền dữ liệu, nên giao thức của tầng giao vận phụ thuộc rất nhiều vào tầng mạng. Trong tầng giao vận người ta chia tầng mạng thành các loại sau:

- + Mạng loại A: Ở loại mạng này có tỷ suất lỗi và sự cố có báo hiệu chấp nhận được (có nghĩa là mạng thuộc vào loại này có chất lượng chấp nhận được), các gói tin được giả thiết là không mất và tầng giao vận không cần cung cấp các dịch vụ phục hồi và sắp xếp thứ tự lại.

- + Mạng loại B: Có tỷ suất lỗi chấp nhận được nhưng sự cố có báo hiệu không chấp nhận được, ở mạng loại B thì tầng giao vận phải có khả năng phục hồi lại khi xảy ra sự cố.

- + Mạng loại C: Có tỷ suất lỗi không chấp nhận được (không tin cậy) hay còn gọi là giao thức không liên kết, tầng giao vận phải có khả năng phục hồi lại lỗi khi xảy ra sự cố và sắp xếp lại thứ tự các gói tin.

Dựa trên giao thức tầng mạng chúng ta có 5 lớp giao thức tầng giao vận đó là:

- + Giao thức lớp 0 (simple class - lớp đơn giản): Cung cấp khả năng rất đơn giản để thiết lập liên kết, truyền dữ liệu hay hủy bỏ liên kết trên mạng “có liên kết” loại A. nó có khả năng phát hiện và báo các lỗi nhưng không có khả năng phục hồi.

- + Giao thức lớp 1 (*Basic Error Recovery Class - lớp phục hồi lỗi cơ bản*): Dùng cho mạng loại B, ở đây các gói tin được đánh số. Ngoài ra giao thức còn có khả năng báo nhận cho nơi gửi và truyền dữ liệu khẩn. So với giao thức lớp 0 thì giao thức lớp 1 có thêm chức năng phục hồi lỗi.

- + Giao thức lớp 2 (*Multiplexing class - lớp dồn kênh*): Là một cải tiến của lớp 0, cho phép dồn một số kênh liên kết chuyển vận vào một liên kết mạng duy nhất. Đồng thời có thể kiểm soát luồng dữ liệu để tránh tắc nghẽn. Giao thức lớp 2 không có khả năng phát hiện và phục hồi lỗi do vậy nó cần đặt trên một lớp mạng loại A.

- + Giao thức lớp 3 (*Error Recovery and Multiplexing Class - lớp phục hồi lỗi cơ bản và dồn kênh*): Đây là lớp cải tiến của lớp 2 với khả năng phát hiện và phục hồi lỗi, giao thức này cần đặt trên một tầng mạng loại B.

+ Giao thức lớp 4 (*Error Detection and Recovery Class - lớp phát hiện và phục hồi lỗi*): Đây là lớp có hầu hết các chức năng của các lớp trước và còn có thêm một số khả năng khác để kiểm soát việc truyền dữ liệu.

2.2.5) Tầng phiên: Có chức năng thiết lập “các giao dịch” giữa các trạm trên mạng, nó đặt tên nhất quán cho mọi đối tượng muốn đối thoại với nhau và lập ánh xạ giữa các tên và địa chỉ của chúng. Một phiên giao dịch phải được thiết lập trước khi dữ liệu được truyền trên mạng. Tầng phiên đảm bảo cho các phiên làm việc được thiết lập và duy trì theo đúng quy định.

Tầng phiên còn cung cấp cho người sử dụng các chức năng cần thiết cho việc quản trị các phiên làm việc của mình, cụ thể là:

- + Điều phối việc trao đổi dữ liệu giữa các ứng dụng bằng cách thiết lập và giải phóng (một cách logic) các phiên.
- + Cung cấp các điểm đồng bộ để kiểm soát việc trao đổi dữ liệu.
- + Áp đặt các quy tắc cho các tương tác giữa các ứng dụng của người dùng.
- + Cung cấp cơ chế “lấy lượt” (nắm quyền) trong quá trình trao đổi dữ liệu.

Trong trường hợp mạng 2 chiều luân phiên thì phát sinh vấn đề. Hai người sử dụng luân phiên phải “lấy lượt” để truyền dữ liệu. Tầng phiên duy trì tương tác luân phiên bằng cách báo cho mỗi người sử dụng khi đến lượt họ truyền dữ liệu. Vấn đề đồng bộ hóa trong tầng phiên cũng được thực hiện như cơ chế kiểm tra/ phục hồi. Dịch vụ này cho phép xác định các điểm đồng bộ hóa trong dữ liệu đang chuyển vận và khi cần thiết có thể phục hồi phiên làm việc tại một thời điểm nào đó.

Ở một thời điểm chỉ có một người sử dụng có quyền đặc biệt được gọi các dịch vụ nhất định của tầng phiên, việc phân bổ các quyền này thông qua trao đổi các thẻ bài (Token). Ví dụ: Ai có được thẻ bài thì sẽ có quyền truyền dữ liệu, và khi người trao thẻ bài cho một người dùng khác thì cũng có nghĩa là trao quyền truyền dữ liệu cho người đó.

Tầng phiên có các hàm cơ bản sau:

+ Give Token: Cho phép người dùng chuyển thẻ bài (Token) cho một người dùng khác trong một liên kết giao dịch.

+ Please Token: Cho phép một người yêu cầu thẻ bài khi chưa có thẻ bài.

+ Give control: Dùng để chuyển tất cả các thẻ bài từ một người dùng sang một người dùng khác.

2.2.6) Tầng trình bày: Trong giao tiếp giữa các ứng dụng thông qua mạng với cùng một dữ liệu có thể có nhiều cách trình bày khác nhau. Thông thường dạng trình bày của ứng dụng nguồn và dạng trình bày của ứng dụng đích có thể khác nhau do các ứng dụng chạy trên các hệ thống hoàn toàn khác nhau. Tầng trình bày phải chịu trách nhiệm chuyển đổi dữ liệu gởi đi trên mạng từ một loại biểu diễn này sang một loại biểu diễn khác. Để làm được điều đó, tầng trình bày cung cấp một dạng biểu diễn chung dùng để truyền thông và cho phép chuyển đổi dữ liệu từ kiểu cục bộ sang kiểu trình bày chung và ngược lại.

Tầng trình bày cũng có thể dùng kỹ thuật mã hoá để mã hoá các dữ liệu trước khi truyền đi và giải mã dữ liệu khi dữ liệu đến đích nhằm bảo mật thông tin trong khi truyền đi. Ngoài ra tầng trình bày cũng có thể dùng các kỹ thuật nén sao cho chỉ cần một ít byte dữ liệu để biểu diễn thông tin khi nó được truyền trên mạng và tại đích thì tầng trình bày sẽ bung nén để có được dữ liệu ban đầu.

2.2.7) Tầng ứng dụng: Đây là tầng cao nhất trong mô hình OSI, nó xác định giao diện người sử dụng và môi trường OSI. Giải quyết các kỹ thuật mà chương trình ứng dụng dùng để giao tiếp với mạng.

Để cung cấp các phương tiện truy nhập môi trường OSI, người ta thiết lập các thực thể ứng dụng. các thực thể ứng dụng này sẽ gọi đến các phần tử dịch vụ ứng dụng (Application Service Element - ASE). Các phần tử dịch vụ ứng dụng được phối hợp với các thực thể ứng dụng thông qua các liên kết (Association) gọi là các đối tượng liên kết đơn (Single Association Object - SAO), các đối tượng liên kết đơn điều khiển việc truyền thông trong suốt vòng đời của liên kết đó, cho phép tuân tự hoá các sự kiện đến từ các phần tử dịch vụ ứng dụng, thành tố của nó.

Bản thân mô hình tham chiếu OSI không phải là một kiến trúc mạng, bởi vì nó không chỉ ra chính xác các dịch vụ và các nghi thức được sử dụng trong các tầng. Mô hình này có nhiệm vụ chỉ ra mỗi tầng cần thực hiện nhiệm vụ gì. Tổ chức ISO đã đưa ra các tiêu chuẩn cho từng tầng nhưng các tiêu chuẩn này không phải là một bộ phận của mô hình tham chiếu.

Các quy định trong mô hình tham chiếu OSI đã được sử dụng một cách rộng rãi trong lý thuyết truyền thông, hầu như trong thực tế tất cả các hệ thống truyền thông hiện tại đều sử dụng mô hình tham chiếu OSI về phương diện lý thuyết.

Tuy nhiên mô hình tham chiếu OSI ra đời sau khi bộ giao thức TCP/IP đã được sử dụng rộng rãi, khi nhiều công ty đã đưa ra các dòng sản phẩm dựa trên TCP/IP. Vì vậy mô hình OSI chỉ được sử dụng trong thực tế như một chuẩn về lý thuyết.

III) Tổng quan về bộ giao thức TCP/IP

3.1) Khái niệm về TCP/IP

TCP là viết tắt của (Transmission Control Protocol), là bộ giao thức được chuẩn hóa vào những năm đầu của thập niên 90. Nó được dùng cho mạng ARPANET vào lúc đó và dùng cho mạng INTERNET cho đến hiện tại.

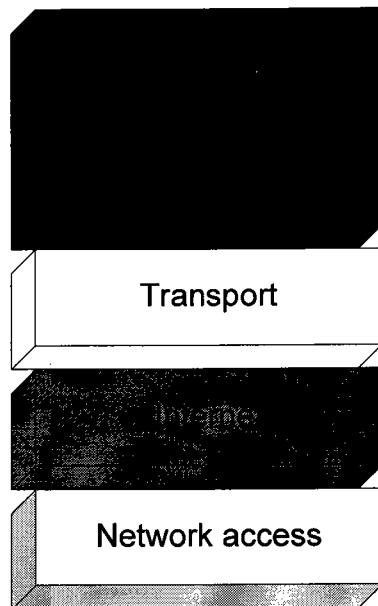
Đây là bộ giao thức được dùng như giao thức mạng và vận chuyển trên mạng internet, TCP là giao thức thuộc tầng vận chuyển và IP (Internet Protocol) là giao thức thuộc tầng mạng trong mô hình OSI. Bộ giao thức TCP/IP là bộ giao thức được sử dụng rộng rãi nhất để liên kết các máy tính và các mạng.

Hiện nay các máy tính của hầu hết các mạng có thể sử dụng giao thức TCP/IP để liên kết với nhau thông qua nhiều hệ thống mạng với kỹ thuật khác nhau. Bộ giao thức TCP/IP thật ra là một bộ giao thức cho phép các hệ thống mạng cùng làm việc với nhau thông qua việc cung cấp phương tiện truyền thông liên mạng.

Bộ giao thức TCP/IP được phân làm 4 tầng.

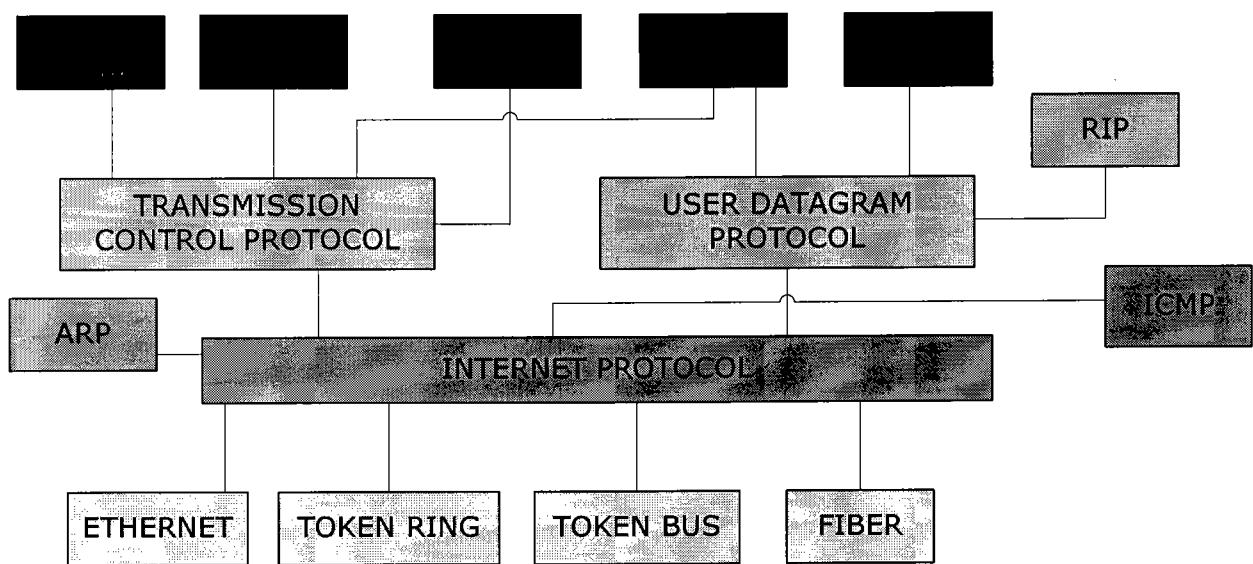
Tầng ứng dụng (application layer), Tầng giao vận (transport layer), Tầng internet (internet layer), Tầng truy cập mạng (network access layer).

Hình dưới minh họa các tầng của bộ giao thức TCP/IP



Hình 5. Mô hình 4 tầng TCP/IP.

Úng với từng tầng trong bộ giao thức TCP có các giao thức khác nhau và từng giao thức có những chức năng khác nhau. Hình bên dưới mô tả các giao thức trong bộ giao thức TCP.



Hình 6. Các giao thức tương ứng với các tầng trong TCP/IP

3.2) Các giao thức của bộ giao thức TCP/IP – Các giao thức tầng Application.

Tầng Application gồm có 5 giao thức là: FTP, TELNET, SMTP, DNS, SNMP.

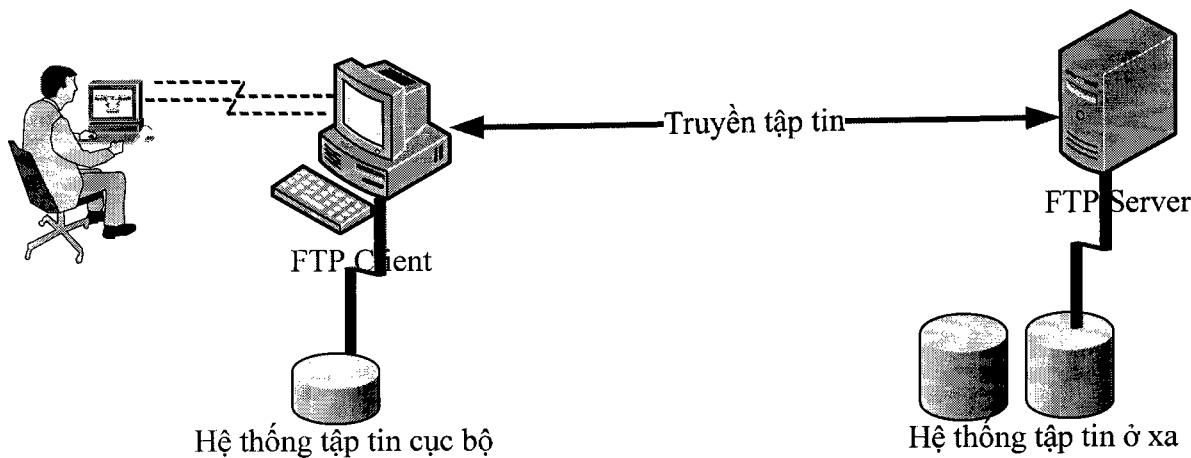
3.2.1) Giao thức FTP (File Transfer Protocol): Đây là giao thức truyền file hay là giao thức truyền tập tin. Giao thức này cho phép người dùng nhận hoặc gửi một hoặc nhiều tập tin từ máy mình đến một máy khác.

Như vậy thông qua dịch vụ FTP, người dùng tại một máy tính có thể đăng nhập và thao tác lên hệ thống tập tin được chia sẻ của một máy tính từ xa.

mục tiêu của dịch vụ FTP là:

- + Đảm bảo việc chia sẻ tập tin(chương trình máy tính hoặc dữ liệu) trên mạng.
- + Khuyến khích việc không sử dụng trực tiếp(thông qua chương trình) tài nguyên trên các máy tính khác.
- + Người dùng không cần phải quan tâm đến sự khác nhau giữa các hệ thống tập tin trên mạng.
- + Truyền dữ liệu một cách tin cậy, hiệu quả.

Mô hình dịch vụ FTP.



Hình 7. Mô hình dịch vụ FTP.

3.2.2) TELNET: Đây là một giao thức cho phép người dùng login vào một máy chủ từ một máy khác trên mạng. Được ứng dụng để login và remote máy chủ từ xa.

3.2.3) Giao thức SMTP(Simple Mail Transfer Protocol): Là giao thức dùng cho việc truyền và nhận thư điện tử (Email) giữa các máy chủ mail hay còn gọi là mail

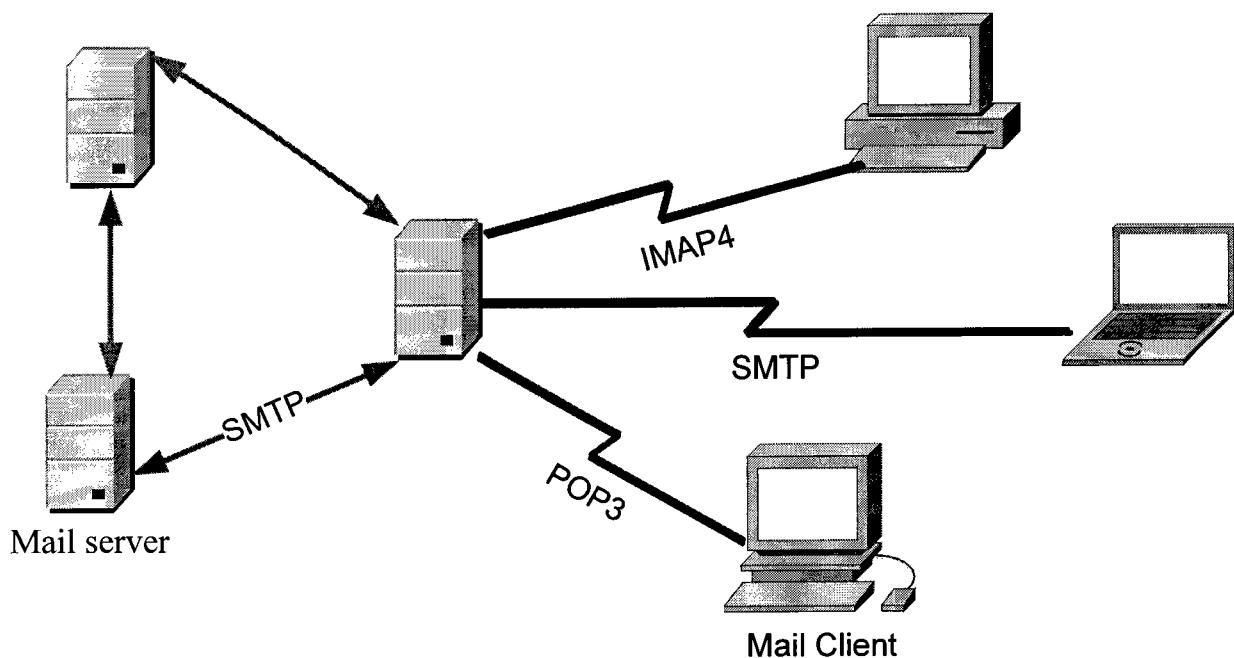
server. Có thể hình dung giao thức SMTP nôm na như là các trạm bưu điện dùng SMTP để chuyển các thùng thư của khách hàng cho nhau.

Còn các mail client thì giao tiếp với máy chủ mail thông qua các giao thức sau:

- + POP3(Post Offic Protocol version 3): Được dùng để lấy thư về từ hộp thư trên server.

- + SMTP: Được client dùng để gửi mail lên server.

- + IMAP4 (Internet Mail Access Protocol version 4): Giao thức này tương tự với giao thức POP3 nhưng có một số tính năng vượt trội hơn so với POP3. Ngoài ra IMAP4 còn cho phép gửi mail lên server.



Hình 8. Sơ đồ gửi và nhận mail giữa client và mail server.

3.2.4) DNS (Domain Name System): Dịch vụ phân giải tên miền, dịch vụ này cho phép nhận ra máy tính từ một tên miền dễ nhớ thay cho một địa chỉ IP khó nhớ.

Cụ thể là mỗi máy tính khi kết nối vào mạng internet thì nó được gán cho một địa chỉ IP xác định. Địa chỉ IP của mỗi máy là duy nhất và giúp cho máy tính có thể dễ dàng xác định đường đi đến một máy tính khác trong mạng. nhưng đối với người sử dụng thì địa chỉ IP rất khó nhớ, vì vậy cần có một dịch vụ giúp cho máy xác định đường đi dễ dàng và cũng đồng thời giúp người dùng nhớ cho người dùng. Và DNS là một dịch vụ

chuyển đổi tên máy tính thành địa chỉ IP và ngược lại để làm thuận tiện cho cả người sử dụng và cả máy tính.

Hệ thống DNS sử dụng cơ sở dữ liệu phân tán và phân cấp theo hình cây. Nên việc quản lý dễ dàng và đồng thời cũng rất thuận tiện cho việc chuyển đổi từ tên miền sang địa chỉ IP và ngược lại.

Có thể hình dung hệ thống DNS là hệ thống quản lý con người, mỗi máy tính là một con người, mỗi người có một cái tên dễ nhớ và một số chứng minh nhân dân duy nhất.

Nhưng có một điểm khác nhau là con người thì có thể trùng tên nhưng tên miền thì không thể trùng với nhau.

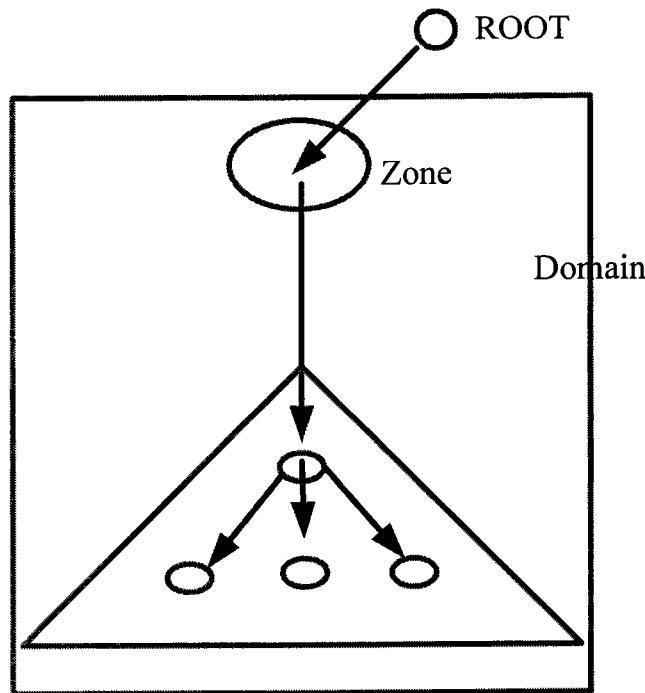
Tóm lại mục tiêu của hệ thống DNS là:

- + Địa chỉ IP thì khó nhớ đối với con người nhưng dễ dùng đối với máy tính.
- + Tên máy tính thì dễ nhớ đối với con người nhưng máy tính không dùng được.

Hệ thống DNS giúp chuyển đổi từ tên miền sang địa chỉ IP và ngược lại. Giúp cho con người dễ sử dụng và máy tính cũng làm việc dễ dàng hơn.

cấu trúc Cơ Sở Dữ Liệu của DNS.

Cơ sở dữ liệu của hệ thống DNS là hệ thống cơ sở dữ liệu phân tán và phân cấp theo hình cây. Với .ROOT SERVER là đỉnh của cây và sau đó các Domain được phân nhánh dần xuống dưới, khi một client truy vấn một tên miền nào đó thì sẽ truy vấn từ ROOT phân cấp lần xuống dưới để cuối cùng là đến DNS quản lý Domain cần truy vấn.



Hình 9. Cấu trúc phân cấp của DNS

Cấu trúc cơ sở dữ liệu phân cấp theo hình cây, ROOT quản lý toàn bộ cây và phân quyền quản lý xuống dưới. Và tiếp theo các tên miền được chuyển xuống cấp thấp hơn về phía dưới.

Zone: Hệ thống DNS cho phép phân chia tên miền để quản lý và nó chia hệ thống ra thành các Zone, trong Zone quản lý tên miền được phân chia đó và chứa các thông tin về Domain cấp thấp hơn. từ các Zone con có thể phân chia thành các Zone cấp thấp hơn và phân quyền cho các DNS server khác quản lý.

Ví dụ: Zone “.com” thì DNS server quản lý Zone “.com” chứa thông tin về các trang có đuôi “.com”, và DNS server này có khả năng chuyển quyền quản lý xuống cho các Zone cấp thấp hơn như Zone “.microsoft.com” là Zone do DNS server của Microsoft quản lý.

Root: Đây là server quản lý toàn bộ cấu trúc của hệ thống DNS. Root không chứa cơ sở dữ liệu của hệ thống DNS mà nó chỉ chuyển quyền quản lý xuống cho các DNS server cấp thấp hơn. Và do đó Root server có khả năng xác định đường đi đến một Domain bất cứ đâu trên mạng.

Domain: Tên miền, mỗi tên miền trên mạng đều được quản lý bởi ít nhất 1 DNS server, và trên đó ta khai các bản ghi của tên miền trên DNS server. Thông tin trong các bản ghi đó sẽ xác định địa chỉ IP của tên miền, các dịch vụ xác định trên internet như Web, Mail....

Sau đây là các bản ghi trên DNS server.

Tên trường	Tên đầy đủ	Mục đích
SOA	Start Of Authority	Xác định máy chủ DNS có thẩm quyền cung cấp thông tin về tên miền xác định trên DNS.
NS	Name Server	Chuyển quyền quản lý tên miền xuống một DNS thấp hơn.
A	Host	Ánh xạ xác định địa chỉ IP của một Host
MX	Mail Exchange	Xác định Host có quyền quản lý thư điện tử cho một tên miền xác định.
PTR	Pointer	Xác định chuyển từ địa chỉ IP sang tên miền
CNAME	Canonical NAME	Thường sử dụng xác định dịch vụ web hosting

Cấu trúc của một tên miền:

Domain sẽ có dạng: lable.lable.lable....lable, độ dài tối đa của một tên miền là 255 ký tự. Mỗi một lable có chiều dài tối đa là 63 ký tự. lable có thể bắt đầu bằng chữ hoặc số, và lable ép buộc chỉ có thể là chữ hoặc số hoặc dấu trừ (-), dấu chấm (.) ngoài ra không được dùng các ký tự khác.

Hầu hết tên miền được chia thành các loại sau:

.arpa: Tên miền ngược, chuyển từ đại chỉ IP sang tên miền.

.com: Các tổ chức thương mại.

.edu: Các tổ chức giáo dục.

.gov: Các cơ quan chính phủ.

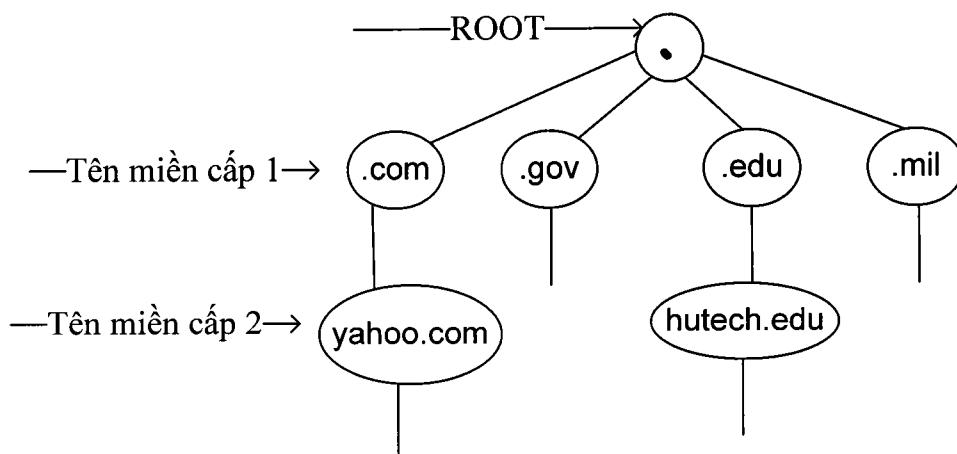
.mil: Các tổ chức quân sự, quốc phòng.

.net: Các trung tâm mạng lớn.

.org: Các tổ chức khác.

.int: Các tổ chức đa chính phủ.

Ngoài ra hiện tại thế giới còn sử dụng tên miền có hai ký tự cuối để xác định tên miền thuộc quốc gia nào (được quy định trong chuẩn ISO3166).



Hình 10. Minh họa về cấu trúc cây DNS.

Hoạt động của hệ thống DNS.

Hệ thống DNS hoạt động tại tầng 4 (Application) của mô hình TCP. Nó dùng giao thức UDP để truy vấn, và dùng cổng 53 để trao đổi thông tin về miền.

Khi một DNS client cần xác định một tên miền nào đó thì nó thực hiện truy vấn DNS. Truy vấn DNS và trả lời của hệ thống DNS sử dụng giao thức UDP (sẽ trình bày phần dưới), và dùng cổng 53 để trao đổi thông tin.

Mỗi Message truy vấn DNS sẽ bao gồm các thông tin sau:

- + Tên của miền cần truy vấn (tên đầy đủ).
- + Xác định loại bản ghi là mail, web,.....

+ Lớp tên miền.

Ví dụ: Tên miền cần truy vấn là “ hostname.example.microsoft.com”, tên miền truy vấn là địa chỉ A. thì client truy vấn sẽ hỏi “có bản ghi địa chỉ A của máy có tên là hostname.example.microsoft.com ” không? Khi client nhận được trả lời của DNS server thì nó sẽ xác định được IP của bản ghi A.

Câu hỏi đặt ra là không lẽ mỗi lần cần truy vấn DNS thì client sẽ phải hỏi DNS server? Có một số cách mà DNS client có thể tự trả lời truy vấn trước khi nó truy vấn lên DNS server. Client có thể tự trả lời bằng cách sử dụng các thông tin được lưu trong cache của mình trong những lần truy vấn trước đó. Và DNS server cũng sẽ truy vấn vào trong cache của mình để tìm thông tin mà client truy vấn, nếu không có thông tin cần tìm thì nó sẽ hỏi các DNS server kế nó để tìm thông tin trả lời cho client.

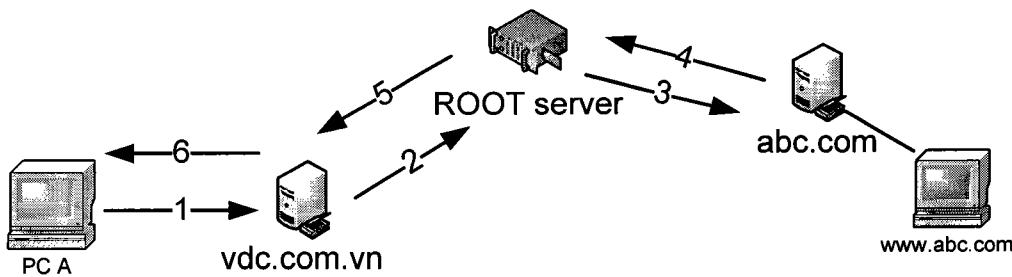
Nhìn chung thì các bước truy vấn có thể chia thành 2 bước như sau:

bước 1: Truy vấn sẽ được bắt đầu ngay tại DNS client để tìm kết quả nếu tìm thấy kết quả thì quá trình truy vấn kết thúc.

bước 2: Ngay khi DNS client không có câu trả lời thì truy vấn sẽ được chuyển lên DNS server. Khi mà DNS server nhận được truy vấn thì nó sẽ xác định xem câu trả lời truy vấn có nằm trong các bản ghi mà nó quản lý trong Zone không, nếu thông tin là phù hợp thì nó sẽ dùng thông tin đó để trả lời và kết thúc truy vấn.

Ngược lại nếu thông tin không tìm thấy trong Zone thì DNS server sẽ tìm thông tin trong cache để trả lời và kết thúc truy vấn, nếu thông tin vẫn không được tìm thấy trong cache nó sẽ nhờ DNS server khác trả lời truy vấn, quá trình cứ tiếp tục cho đến khi tìm thấy câu trả lời cho truy vấn từ DNS client.

Các cách để DNS server liên lạc với nhau tìm câu trả lời.



Hình 11. Các bước truy vấn DNS server.

Hình trên mô tả các bước truy vấn DNS server khi Root Server biết được DNS server quản lý miền cần truy vấn, hay nói cách khác là DNS server quản lý tên miền truy vấn kết nối trực tiếp với Root Server.

Bước 1. PC A truy vấn lên DNS server quản lý tên miền “vdc.com.vn”, và hỏi về máy có tên là “www.abc.com”.

Bước 2. Do DNS server “vdc.com.vn” không quản lý miền “abc.com” nên nó chuyển truy vấn lên cho Root Server.

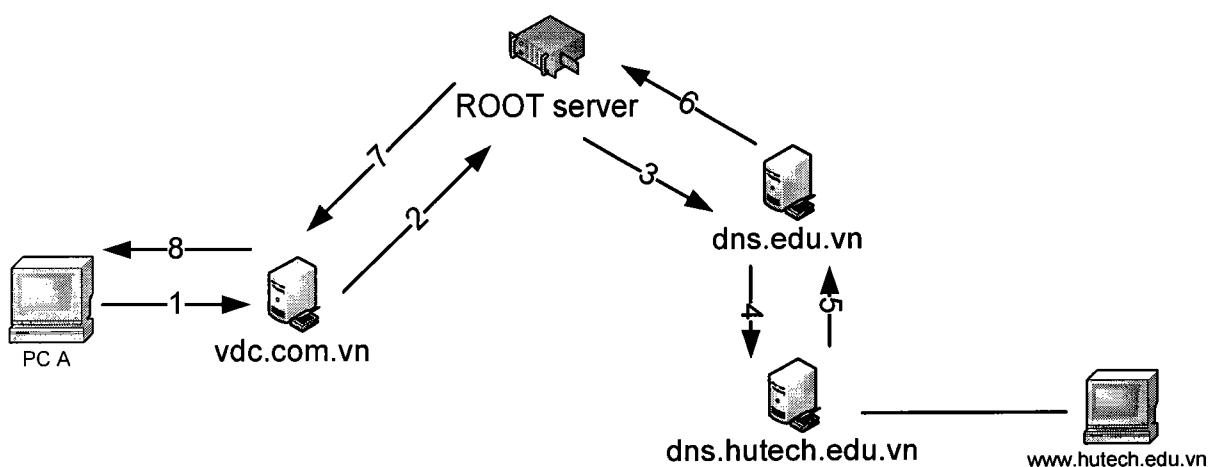
Bước 3. Root Server xác định được DNS server quản lý tên miền “www.abc.com” là server “DNS.abc.com” và nó chuyển truy vấn đến DNS server “DNS.abc.com” để trả lời.

Bước 4. DNS server “DNS.abc.com” sẽ xác định bản ghi “www.abc.com” để trả lời lại cho Root Server.

Bước 5. Root Server chuyển câu trả lời từ “DNS.abc.com” xuống cho “vdc.com.vn”.

Bước 6. DNS server “vdc.com.vn” sẽ trả lời cho PC A biết máy “www.abc.com” là máy nào và từ đó PC A có thể kết nối đến máy “www.abc.com”.

trường hợp Root Server không kết nối trực tiếp với DNS server cần truy vấn.



Hình 12. Các bước truy vấn DNS server.

Trong trường hợp Root Server không kết nối trực tiếp với DNS server cần truy vấn. thì Root Server sẽ hỏi server DNS trung gian (phân lớp theo hình cây) để hỏi server quản lý tên miền cần truy vấn. Các bước chi tiết như sau:

Bước 1. PC A truy vấn lên DNS server quản lý tên miền “vdc.com.vn”, và hỏi về máy có tên là “www.hutech.edu.vn”.

Bước 2. Do DNS server “vdc.com.vn” không quản lý miền “www.hutech.edu.vn” nên nó chuyển truy vấn lên cho Root Server.

Bước 3. Root Server không xác định được server quản lý tên miền www.hutech.edu.vn nên Root Server sẽ căn cứ vào cấu trúc phân cấp của DNS mà sẽ chuyển truy vấn xuống cho DNS server cấp thấp hơn quản lý miền “dns.edu.vn” nó xác định được DNS server này quản lý miền “dns.hutech.edu.vn”.

Bước 4. Server DNS “DNS.edu.vn” xác định được tên miền “www.hutech.edu.vn” thuộc sự quản lý của “dns.hutech.edu.vn” do vậy nó chuyển truy vấn xuống cho DNS server “dns.hutech.edu.vn”.

Bước 5. DNS server “dns.hutech.edu.vn”. sẽ lấy bản ghi của miền có tên là www.hutech.edu.vn trả về cho DNS “dns.edu.vn”.

Bước 6. DNS “dns.edu.vn” sẽ chuyển kết quả này cho Root Server.

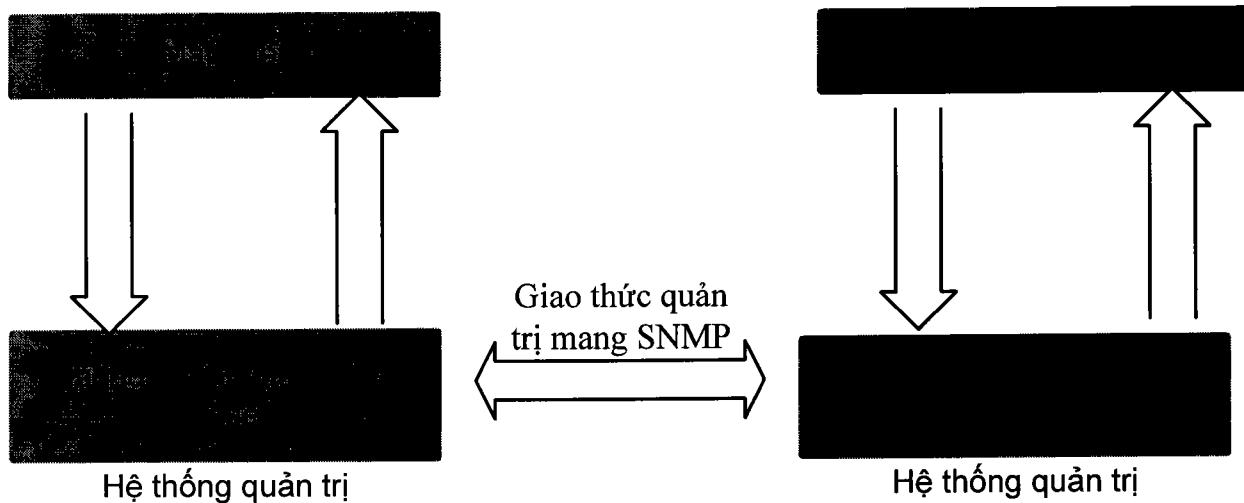
Bước 7. Root Server chuyển câu trả lời từ “DNS.abc.com” xuống cho “vdc.com.vn”.

Bước 8. DNS server “vdc.com.vn” sẽ trả lời cho PC A biết máy “www.hutech.edu.vn” là máy nào và từ đó PC A có thể kết nối đến máy “www.hutech.edu.vn”.

Với mục đích nâng cao tốc độ phục vụ cho việc tìm kiếm thông tin của DNS, thì khi xử lý các thông tin truy vấn từ Client, các DNS server lưu lại các thông tin này cho lần truy vấn sau. Các thông tin này sẽ được ghi vào bộ nhớ cache của DNS server.

Thông tin được lưu lại trong cache là các bản ghi, và thời gian sống của các bản ghi thông tin này trong cache theo mặc định là 3600 giây (1 giờ), thời gian sống (Time To Live) này có thể được tăng lên hay giảm xuống bằng cách cấu hình trong Zone.

3.2.5) *Giao thức SNMP(Simple Network Monotoring Protocol)*: Là giao thức quản trị mạng, giao thức này cung cấp những công cụ cho phép quản trị mạng từ xa. Giao thức này được thiết kế dựa trên mô hình quản trị mạng Manager/Agent bao gồm các thành phần chính như Manager, Agent, MIB. Các đối tượng bị quản lý và các quy định chuẩn. hình dưới mô tả mô hình quản lý mạng.



Hình 13. Sơ đồ quản trị dựa trên giao thức SNMP.

Chức năng của các thành phần trong sơ đồ trên.

Manager: Thành phần này có chức năng đảm bảo cho sự giao tiếp giữa người quản trị hệ thống và hệ thống quản trị. Thành phần này cho phép người quản trị kiểm soát hệ thống, phân tích dữ liệu, và khôi phục lại trạng thái cần thiết khi có sự cố xảy ra. Có thể quản trị hệ thống từ một hay một vài trạm quản trị.

Các trạm quản trị thực hiện chức năng giám sát bằng cách thu thập các thông tin cần thiết từ các đối tượng trong các cơ sở dữ liệu MIB. Các trạm quản trị có thể được thực hiện tại một Agent nào đó hay có thể thay đổi các thiết lập cấu hình về một Agent nào đó bằng cách thay đổi giá trị một vài biến trong cơ sở dữ liệu MIB.

Agent: Là thành phần cung cấp giao tiếp giữa Manager và các thiết bị vật lý, các thiết bị đang bị quản trị như: Các máy chủ, các bộ kết nối, bộ định tuyến. được gắn các Agent để đáp ứng các yêu cầu thông tin, các hoạt động từ trạm quản trị.

Management Information Base (MIB): Hay còn được gọi là cơ sở dữ liệu MIB, đây là tập hợp các đối tượng thông tin khác nhau về một loại thiết bị được quản trị, trong CSDL MIB mỗi loại tài nguyên được quản trị và biểu hiện bởi một đối tượng và MIB phản ánh trạng thái của chính đối tượng đó.

Các quy định chuẩn của giao thức quản trị mạng: Được dùng để liên kết trạm quản trị và các Agent.

Giao thức chính cho phép quản trị mạng TCP/IP là giao thức SNMP, 3 chức năng chính được mô tả trong bảng dưới.

Chức năng	nội dung
GET	Trạm quản trị thu thông tin của các đối tượng tại các Agent.
SET	Trạm quản trị thiết lập giá trị cho các đối tượng tại các Agent.
TRAP	Agent thông báo cho trạm quản trị khi các sự kiện diễn ra.

3.3) Các Giao Thức Tầng Transport

Tầng Transport có 3 giao thức là: TCP, UDP và RIP.

3.3.1) Giao thức TCP: TCP là giao thức “có liên kết” (Connection - Oriented), điều này có nghĩa là khi hai trạm muốn trao đổi dữ liệu cho nhau bằng giao thức TCP thì cần phải thiết lập liên kết TCP trước khi truyền dữ liệu cho nhau.

Khi một tiến trình ứng dụng trong một máy tính muốn truy cập vào các dịch vụ của giao thức TCP thì tất cả phải thông qua một cổng của TCP. Số hiệu của cổng TCP được thể hiện bằng 2 byte.

Một cổng TCP kết nối với một địa chỉ IP tạo thành một đầu nối TCP/IP (socket) duy nhất trong mạng. Dịch vụ TCP/IP được cung cấp nhờ vào một liên kết giữa 2 socket, một socket có thể tham gia vào nhiều liên kết với các socket khác nhau ở xa. Trước khi truyền dữ liệu giữa 2 trạm thì cần thiết phải thiết lập kết nối giữa 2 socket, và khi không còn nhu cầu truyền dữ liệu nữa thì kết nối được giải phóng.

Các thực thể ở các tầng trên sử dụng các dịch vụ TCP bằng cách gọi các hàm, có các hàm dùng cho việc yêu cầu, các hàm dùng cho việc trả lời. Trong mỗi hàm có các tham số để dùng cho việc trao đổi dữ liệu.

Các bước cần thực hiện khi mở một kết nối TCP: khi muốn mở một kết nối TCP mới giữa hai thực thể ta có thể thực hiện theo hai hướng. Thứ nhất là mở kết nối theo hướng chủ động (Active) và thứ hai là mở kết nối theo hướng bị động (Passive).

Phương thức chủ động (Active): Người sử dụng yêu cầu TCP mở một liên kết với một socket ở xa, liên kết sẽ được xác lập nếu tại socket bên kia có một hàm Passive tương ứng được mở.

Phương thức bị động(Passive): Người sử dụng yêu cầu TCP chờ đợi một yêu cầu kết nối được gởi đến từ xa thông qua một Socket(tại chỗ). Hay nói cách khác là người sử dụng mở hàm Passive có khai báo cổng TCP và các thông số khác như mức ưu tiên, mức an toàn.

Dưới đây là bảng liệt kê một vài cổng TCP phổ biến.

Số hiệu cổng	Mô tả chức năng
0	Reserved
5	Remote Job Entry
7	Echo
9	Discard
11	Systat
13	Datetime
15	Nestat
17	Quotd (quote odd day)
20	FTP (data)
21	FTP (control)

23	telnet
25	SMTP
37	Time
53	Name Server
102	ISO – TSAP
103	X.400
104	X.400 (Sending)
111	Sun RPC
139	Net BIOS Session Source
160 – 223	Reserved

Khi người dùng gửi đi yêu cầu thiết lập kết nối TCP sẽ nhận được 2 thông tin trả lời sau:

Thông số Open ID: Thông số này được TCP trả lời ngay lập tức để gán cho một liên kết cục bộ (local connection name) cho liên kết được yêu cầu, tham số này về sau được dùng để tham chiếu tới liên kết đó. Nếu trong trường hợp TCP không thể thiết lập được liên kết yêu cầu thì nó sẽ gửi trả lại một tham số Open False để thông báo.

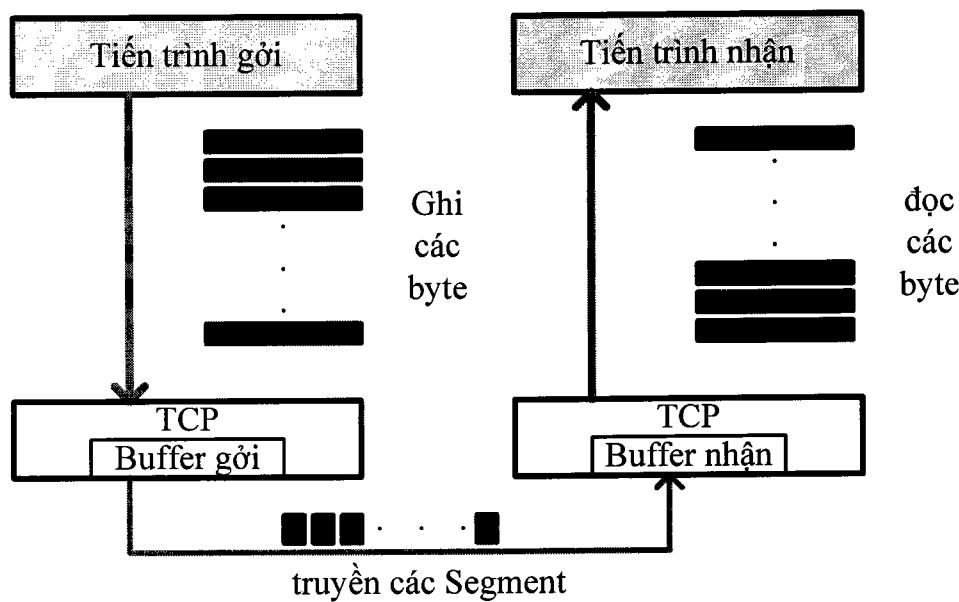
Khi TCP thiết lập thành công kết nối yêu cầu thì nó sẽ gửi một tham số Open Success để thông báo cho bên yêu cầu thiết lập kết nối biết là việc thiết lập kết nối thành công. Thông báo này được chuyển đi trong cả hai trường hợp thiết lập theo kiểu Active và Passive. Sau khi nhận được thông báo thiết lập kết nối thành công thì việc truyền và nhận dữ liệu giữa 2 trạm có thể thực hiện.

Sau khi thiết lập kết nối giữa 2 trạm thì việc truyền và nhận dữ liệu được thực hiện thông qua hai hàm *Send* và *Receive*.

Hàm Send: Dữ liệu được gửi xuống TCP theo dạng khối (các Block), khi nhận được một khối dữ liệu gửi đến thì TCP sẽ cắt vào trong bộ đệm (Buffer) của mình. Nếu như cờ PUSH được bật lên thì toàn bộ dữ liệu trong Buffer sẽ được gửi đi, kể cả khối dữ

liệu vừa được chuyển đến. Ngược lại nếu cờ PUSH không được bật thì dữ liệu sẽ được giữ lại trong bộ đệm và chỉ gửi đi khi nào cờ PUSH bật lên.

Hàm Receive: Tại trạm đích, tất cả các dữ liệu chuyển tới sẽ được lưu trong bộ đệm gắn với mỗi liên kết, nếu dữ liệu được gắn với 1 cờ PUSH thì toàn bộ dữ liệu trong bộ đệm (kể cả các khối dữ liệu được lưu từ trước) sẽ được chuyển cho người dùng. Ngược lại thì toàn bộ dữ liệu sẽ được lưu trong buffer và được gửi đi khi cờ PUSH bật lên.



Hình 14. Cách TCP truyền dữ liệu sau khi kết nối thành công.

Các bước cần thực hiện khi đóng một kết nối TCP: Có hai cách để giải phóng một kết nối TCP là dùng hàm Close hoặc hàm Abort.

Hàm Close: Hàm Close dùng để yêu cầu đóng kết nối một cách bình thường khi việc truyền và nhận dữ liệu đã hoàn tất, khi nhận được một hàm Close thì TCP sẽ truyền đi tất cả các khối dữ liệu còn lại trong bộ đệm và thông báo cho bên gửi biết rằng nó đóng kết nối. Lưu ý rằng khi người dùng gửi đi một hàm Close thì TCP sẽ vẫn tiếp tục quá trình nhận dữ liệu trên liên kết đó cho đến khi TCP đã báo cho phía bên kia biết việc mình đóng liên kết và đã chuyển giao hết toàn bộ dữ liệu cho người sử dụng.

Hàm Abort: Người dùng có thể đóng một kết nối TCP một cách bất thường và không nhận dữ liệu qua liên kết đó nữa. Vì vậy dữ liệu có thể mất đi do quá trình truyền chưa

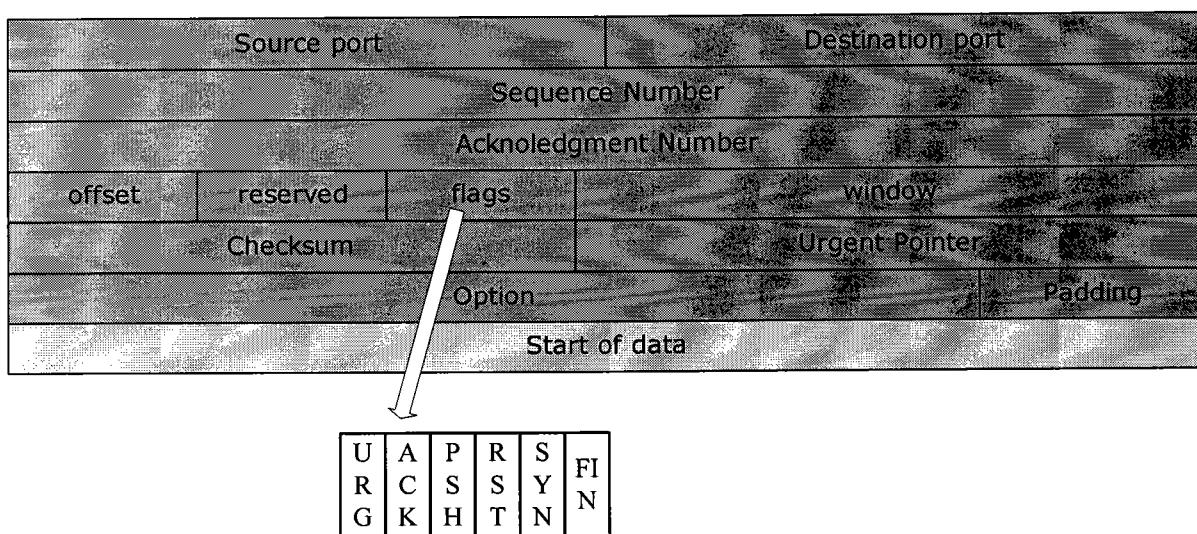
hoàn thành. TCP sẽ thông báo cho TCP ở xa biết rằng liên kết đã được hủy và TCP ở xa sẽ thông báo cho người dùng của mình biết.

một số hàm khác của TCP.

Hàm Status: Hàm này cung cấp thông tin về trạng thái hiện tại của một liên kết cụ thể, vì vậy người sử dụng có thể biết được trạng thái của kết nối bằng cách gọi hàm Status.

Hàm Error: Hàm này sẽ báo cho người sử dụng TCP biết về các yêu cầu bất hợp lệ cũng như các lỗi liên quan đến môi trường.

Đơn vị dữ liệu sử dụng trong TCP được gọi là Segment, cấu trúc các thành phần trong một Segment được mô tả trong hình dưới.



Hình 15. Cấu trúc của gói tin TCP.

Ý nghĩa các trường trong gói tin TCP.

Source port: Trường này có chiều dài 16 bit và chứa thông tin về số hiệu cổng TCP của trạm nguồn.

Destination port : Trường này có chiều dài 16 bit và chứa thông tin về số hiệu cổng TCP của trạm đích.

Acknowledgment Number (32 bit): Là số hiệu của segment tiếp theo mà trạm đích đang chờ để nhận, trường này có nghĩa là đã nhận tốt các segment mà trước đó trạm nguồn đã gửi cho trạm đích.

Data Offset (4 bit): Trường này chỉ ra vị trí bắt đầu của dòng dữ liệu.

Reserved: Dùng để dành cho sau này.

Flag: Đây là các cờ hiệu hay còn gọi là các bit điều khiển. Trong trường này gồm các cờ sau:

URG (Urgent Pointer): Đây là cờ thông báo khẩn.

ACK (Acknowledgment): Cờ báo nhận.

PSH (Push): Cờ báo chuyển.

RST (Reset): Cờ báo khởi động lại.

SYN (SYNchronous): Cờ đồng bộ.

FIN (Finish): Cờ kết thúc, không còn dữ liệu tại trạm nguồn.

Window (16 bit): Cung cấp các cơ chế để kiểm soát nguồn dữ liệu (cơ chế cửa sổ). Đây chính là số lượng các byte dữ liệu. Bắt đầu từ byte được chỉ ra trong trường ACK mà khi đó trạm đích sẵn sàng để nhận.

Check Sum(16 bit): trường này chứa mã kiểm soát lỗi cho toàn bộ segment (Header + Data).

Urgent Pointer: Con trỏ này chỉ tới số hiệu tuần tự của byte đi sau dữ liệu khẩn. Trường này chỉ có hiệu lực khi cờ URG được bật lên.

Option (độ dài thay đổi): Trường này khai báo các option của TCP, trong đó có độ dài tối đa của vùng TCP data trong một Segment.

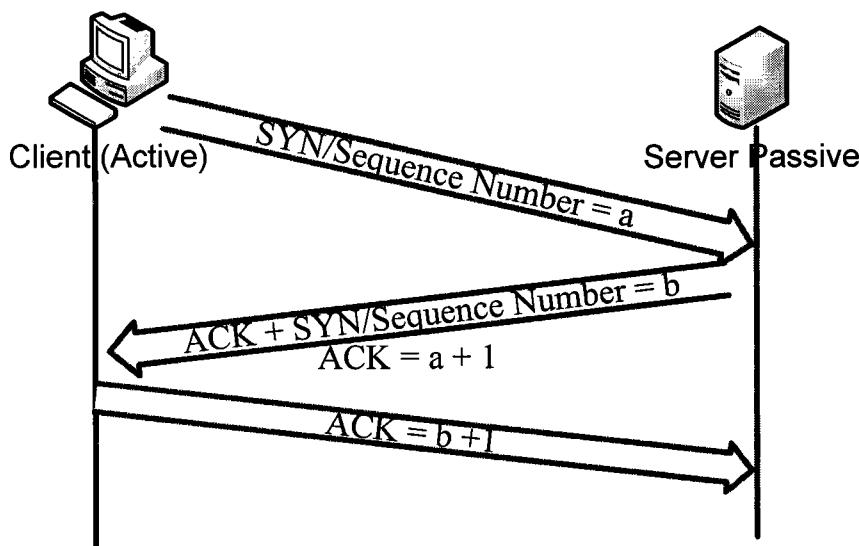
Padding (độ dài thay đổi): Phần chèn thêm vào header để luôn đảm bảo header luôn kết thúc ở bit 32, phần này toàn số 0.

Start Of Data (độ dài thay đổi): Trường này chứa dữ liệu cần truyền đi, chiều dài của trường này có thể thay đổi được bằng cách thay đổi trong trường Option.

3.3.2) Hoạt động của TCP.

Thiết lập kết nối trong giao thức TCP.

Giao thức TCP hoạt động dựa trên nguyên tắc bắt tay 3 chiều. Hình dưới mô tả giao thức bắt tay 3 chiều của TCP.



Hình 16. Cơ chế bắt tay 3 chiều của TCP.

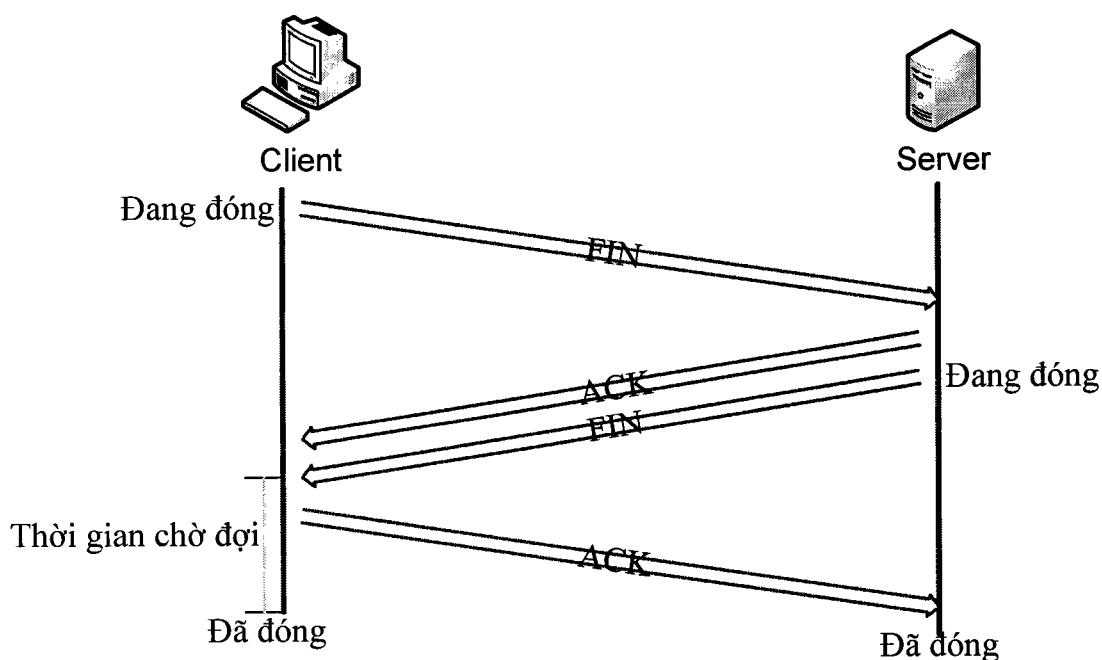
Bước 1: Để bắt đầu cho việc yêu cầu thiết lập kết nối thì Client gửi một gói tin tới server với nội dung yêu cầu thiết lập kết nối như sau: Số thứ tự khởi đầu Sequence Number = a cùng với cờ yêu cầu thiết lập kết nối Flag = SYN.

Bước 2: Sau khi server nhận được gói tin yêu cầu thiết lập kết nối từ Client, nếu chấp nhận yêu cầu thiết lập kết nối thì server sẽ gửi lại cho client một gói tin với nội dung là server có thể nhận dữ liệu từ số thứ tự $a + 1$ và số thứ tự khởi đầu tại server là b . Cùng với cờ Flag = ACK (chấp nhận kết nối).

Bước 3: Sau khi nhận được gói tin phản hồi từ server thì Client sẽ gửi trả lời lại cho server một gói tin với Flag là ACK.

Sau khi server nhận được ACK từ Client thì kết nối được thiết lập thành công và có thể bắt đầu quá trình truyền và nhận dữ liệu.

Huỷ kết nối trong giao thức TCP.



Hình 17. Quá trình giải phóng kết nối TCP.

Bước 1: Client chủ động gửi đến server một gói tin với Flag = FIN, để thông báo việc đóng kết nối.

Bước 2: Server gửi trả lại cho Client một gói tin chấp nhận đóng kết nối với Flag = ACK, tiếp theo đó server sẽ gửi tiếp cho Client một gói tin nữa để thông báo việc đóng kết nối của mình với Flag = FIN.

Bước 3: Sau khi nhận được cờ FIN từ Server, Client sẽ gửi trả lại cho server một gói tin ACK và chuyển vào trạng thái chờ có định hạn. Trong thời gian này Client sẽ trả lời ACK cho mọi khung FIN. Sau khi hết thời gian chờ đợi thì việc đóng kết nối hoàn thành.

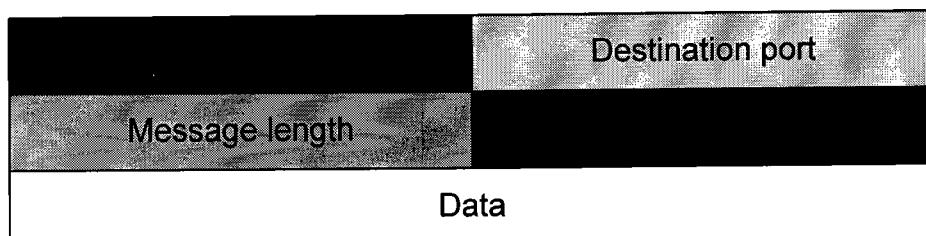
bước 4: Sau khi Server nhận được ACK từ Client thì hoàn thành quá trình giải phóng kết nối.

3.3.3) Giao thức UDP (User Datagram Protocol).

Giao thức UDP là giao thức không liên kết, giao thức này được dùng để thay thế cho giao thức TCP tùy theo yêu cầu của một số ứng dụng. Vì là giao thức không liên kết nên khác với giao thức TCP, giao thức UDP không có các chức năng tạo kết nối và huỷ kết nối. Và vì là giao thức không tin cậy nên UDP cũng không có cơ chế bảo nhận

(Acknowledgment), không sắp xếp tuần tự các gói tin đến nên có thể dẫn đến trùng hoặc mất dữ liệu trong khi truyền mà không có cơ chế thông báo cho người gửi. Vì vậy UDP là giao thức cung cấp các dịch vụ vận chuyển không tin cậy.

Cấu trúc gói tin của UDP như hình sau:



Hình 18. Cấu trúc gói tin UDP

Giao thức UDP cũng quản lý các ứng dụng chạy trên một trạm mạng bằng cách gán và quản lý số hiệu port cho từng ứng dụng. Vì hoạt động của UDP đơn giản hơn TCP nên UDP thường chạy nhanh hơn. Và UDP thường được ứng dụng cho việc gửi và nhận các ứng dụng không đòi hỏi độ tin cậy cao.

3.4) Các giao thức tầng internet.

Tầng Internet có 3 giao thức là ARP, IP và ICMP.

3.4.1) Giao thức ARP(Address Resolution Protocol): Trên một mạng cục bộ, hai máy trạm chỉ có thể liên lạc với nhau khi chúng biết địa chỉ vật lý của nhau, nhưng địa chỉ dùng để định danh các máy trên mạng lại là địa chỉ IP. Nên vấn đề đặt ra là phải làm sao ánh xạ địa chỉ IP (32 bit) và địa chỉ vật lý (48 bit) với nhau. Giao thức ARP được xây dựng với nhiệm vụ thực hiện việc chuyển đổi này. Trong trường hợp ngược lại, có nghĩa là khi cần ánh xạ một địa chỉ vật lý thành địa chỉ IP thì ta dùng giao thức RARP (Reverse Address Resolution Protocol). Hai giao thức ARP và RARP không phải là một bộ phận của giao thức IP mà giao thức IP chỉ dùng hai giao thức này khi cần thiết.

3.4.2) Giao thức IP(Internet Protocol): Giao thức IP có chức năng cung cấp khả năng kết nối các mạng con lại thành một mạng lớn (liên mạng) để truyền dữ liệu. Hay nói cách khác giao thức IP cung cấp dịch vụ truyền tải dạng không kết nối (không cần

thiết lập kết nối) khi truyền liên mạng. Chức năng thứ hai của giao thức IP là phân mảnh và tập hợp lại các gói tin để hỗ trợ cho tầng bên trên.

Địa chỉ IP là một dãy số dài 32 bit, chia làm 4 vùng (mỗi vùng 1 byte). Một địa chỉ IP được phân thành 2 phần: phần địa chỉ mạng (Network ID) và phần địa chỉ máy (Host ID). Mục đích của địa chỉ IP là dùng để định danh duy nhất một máy tính bất kỳ trên mạng.

Địa chỉ IP được phân thành 5 lớp: A, B, C, D, E. Trong đó 3 lớp đầu được dùng để gán cho các mạng, lớp D dùng cho kỹ thuật Multicasting, lớp E dành cho tương lai.

Chi tiết về các lớp IP như sau:

Địa chỉ lớp A: Lớp A dùng 1 byte cho địa chỉ mạng và 3 byte còn lại cho địa chỉ Host.



Lớp A có dãy địa chỉ từ 1 đến 126. Ví dụ: 10.0.0.0 là địa chỉ lớp A, và bít đầu tiên trong phần Network ID là bít 0. Mặt nạ(NetMask) lớp A là 255.0.0.0

Địa chỉ lớp B: lớp B dùng 2 byte cho địa chỉ mạng và 2 byte còn lại cho địa chỉ Host.



Lớp B có dãy địa chỉ từ 128 đến 191. Ví dụ: 170.16.0.0 là địa chỉ lớp B, và bít đầu tiên trong phần Network ID là bít 10. Mặt nạ(NetMask) lớp A là 255.255.0.0

Địa chỉ lớp C: Lớp C dùng 3 byte cho địa chỉ mạng và 1 byte còn lại cho địa chỉ Host



Lớp C có dãy địa chỉ từ 192 đến 223. Ví dụ: 192.168.10.0 là địa chỉ lớp C, và bít đầu tiên trong phần Network ID là bít 110. Mặt nạ(NetMask) lớp A là 255.255.255.0

Địa chỉ lớp D: Lớp D dùng cho kỹ thuật Multicasting

Multicasting



Địa chỉ lớp E: Lớp E dành riêng cho những ứng dụng trong tương lai.

Reverse for future use



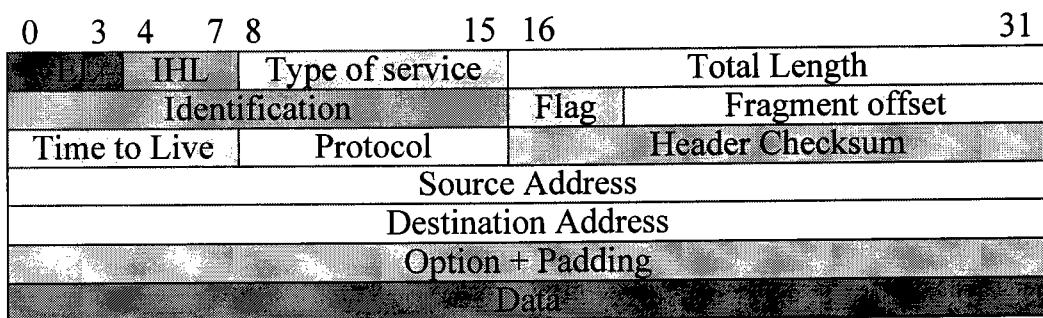
Bảng mô tả chi tiết thông tin về các lớp địa chỉ IP.

Lớp	Dạng	Mục đích	Các bít cao nhất	Khoản địa chỉ	Số bít phần nhận dạng mạng/ số bít phần nhận dạng máy	Tổng số máy tính trong một mạng
A	NHHH	Cho các tổ chức lớn	0	1.0.0.0 đến 126.0.0.0	7/24	$2^{24} - 2$. 16777214
B	NNHH	Cho các tổ chức trung bình	10	128.1.0.0 đến 191.254.0.0	14/16	$2^{16} - 2$. 65534
C	NNNH	Cho các tổ chức nhỏ	110	192.0.1.0 đến 223.255.254.0	21/8	$2^8 - 2$. 254
D		truyền nhóm	1110	224.0.0.0 đến 239.255.255.255		
E		Thí nghiệm	1111	240.0.0.0 đến 254.255.255.255		

Cấu trúc gói tin IP.

Trong giao thức IP, đơn vị dữ liệu được gọi là Datagram. Trong mỗi Datagram có phần tiêu đề (Header) chứa thông tin các thông tin cần thiết để chuyển gói dữ liệu. Ví dụ: trong phần Header có địa chỉ IP đích của dữ liệu.

Trong trường hợp địa chỉ IP nguồn và đích nằm trong cùng một mạng thì gói tin sẽ được chuyển thẳng từ nguồn tới đích. Ngược lại thì gói tin sẽ được chuyển thông qua một IP gateway trung gian. IP gateway là một thiết bị mạng đảm nhận việc luân chuyển các gói dữ liệu IP qua các mạng khác nhau.



Hình 19. Cấu trúc gói tin IP.

Ý nghĩa của các trường.

Ver: Trường này chứa thông tin về phiên bản hiện hành của giao thức IP được cài đặt.

IHL: Đây là giá trị chỉ độ dài phần đầu của gói tin IP (Internet Header Length), đây là phần thông tin bắt buộc phải có trong gói tin IP vì phần đầu của gói tin IP có chiều dài thay đổi tùy ý. Độ dài tối thiểu của trường này là 20 byte và tối đa là 60 byte.

Type of Service: Trường này chứa thông tin về dịch vụ để thông báo cho mạng biết về dịch vụ mà gói tin muốn sử dụng. Ví dụ: như độ ưu tiên, thời gian trễ, độ tin cậy.....

Total Length: Trường này có nội dung mô tả về chiều dài của toàn bộ gói tin. Chiều dài tối đa của trường này là 65535 byte.

Indentification: Cùng với Source Address và Destination Address dùng để định danh cho một datagram trong thời gian nó tồn tại trên mạng.

Flag: Trường này liên quan đến sự phân đoạn các gói tin, do khi lưu chuyển các gói tin trên mạng thì có thể các gói tin sẽ bị phân thành các gói tin nhỏ hơn. Trong trường hợp này thì trường Flag có chức năng điều khiển các phân đoạn và tái lắp ghép các phân đoạn, Giá trị của trường Flag sẽ cho biết là gói tin có bị phân đoạn hay không.

Fragment Offset: Cho biết vị trí dữ liệu thuộc phân đoạn tương ứng với đoạn bắt đầu của dữ liệu gốc. Ý nghĩa cụ thể của trường Flag là.



Bít 0: Reserve, chưa sử dụng. Bít này luôn lấy giá trị không.

Bít 1: (DF)= 0, (May Fragment)= 1. Không phân đoạn (Don't Fragment).

Bít 2: (MF)=0, (Last Fragment)= 1, phân nhiều hơn 1 đoạn (More fragment).

TTL: Là thời gian sống hay là thời gian tồn tại của một gói tin trên mạng, thường thì giá trị này do máy gửi gói tin đi gán, mục đích của TTL là giảm thời gian tồn tại bất tận của các gói tin trên mạng.

Khi một gói tin đi qua 1 bộ định tuyến trên mạng thì thời gian TTL giảm đi 1 đơn vị hay là giảm đi 1 giây, vì thời gian sống TTL tính bằng giây.

Protocol: Chỉ giao thức kế tiếp của tầng bên trên sẽ nhận gói dữ liệu, hiện tại có 2 giao thức được cài bên trên bộ IP là TCP và UDP. Nếu tầng trên là TCP thì giá trị của trường này là 6 còn nếu là UDP thì giá trị của trường này là 17.

Header Checksum: Chứa mã kiểm soát lỗi phần Header của IP.

Source Address: Chứa thông tin về địa chỉ máy gửi gói tin.

Destination Address: Thông tin về máy nhận gói tin.

Option: Các lựa chọn của người gửi, tùy vào từng chương trình.

Padding: Vùng đệm, vùng thêm vào để luôn đảm bảo cho phần Header luôn kết thúc ở bít 32, phần này thường chứa các bít 0.

Data: Trường này chứa nội dung dữ liệu cần gửi đi.

Nguyên tắc hoạt động của giao thức IP.

Khi giao thức IP được khởi động, nó sẽ tồn tại như một thực thể trong máy tính và khi đó nó sẽ thực hiện các chức năng của mình. Giao thức IP sẽ nhận yêu cầu từ tầng trên và gửi yêu cầu xuống tầng dưới nó.

Đối với thực thể IP của máy nguồn, khi nhận được yêu cầu từ tầng trên thì nó sẽ thực hiện các bước sau đây.

- + Tạo một IP Datagram dựa trên tham số nhận được.
- + Tính checksum và ghép vào phần Header của gói tin.
- + Ra quyết định chọn đường đi cho gói tin.
- + Chuyển gói tin xuống tầng dưới để truyền qua mạng.

Đối với Router, khi nhận được gói tin đi qua thì nó sẽ thực hiện các bước sau:

- + Tính lại checksum, nếu sai thì loại bỏ gói tin.
- + Giảm tham số TTL xuống 1, nếu TTL = 0 thì loại bỏ gói tin.
- + Ra quyết định chọn đường đi cho gói tin.
- + Phân đoạn gói tin nếu cần.
- + Thiết lập lại 1 số thông số trên phần Header, như TTL, Fragmentation, checksum.

Đối với trạm đích, nhận một IP datagram thì sẽ thực hiện các việc sau:

- + Tính checksum, nếu sai thì loại bỏ gói tin.
- + Tập hợp các đoạn của gói tin, nếu có phân đoạn.
- + Chuyển dữ liệu và các tham số lên tầng trên.

3.4.3) Giao thức ICMP: Là viết tắt của Internet Control Message Protocol, là giao thức điều khiển việc truyền tin trên mạng, giao thức này được dùng để trao đổi các thông tin điều khiển dòng dữ liệu, thông tin trạng thái, thông báo lỗi của bộ giao thức TCP/IP.

Thông thường ICMP được gửi đi khi một gói tin không đến được đích, hay là một router không còn đủ không gian nhớ để lưu gói tin đến...

Chức năng điều khiển dòng dữ liệu: Chức năng này được gọi đến khi một trạm nguồn gửi dữ liệu đến quá nhanh khiến cho trạm đích hay Router không thể xử lý kịp, thì trạm đích hay router này sẽ gửi trả lại cho trạm nguồn một ICMP để thông báo về việc tạm ngưng gửi dữ liệu.

Thông báo lỗi: Khi mà không xác định được đích đến của gói tin thì Router sẽ gửi trả lại cho trạm nguồn một ICMP *Destination Unreachable* để thông báo cho trạm nguồn biết việc gói tin không thể đến đích.

Kiểm tra hoạt động của các trạm làm việc: Để kiểm tra máy trạm có đang hoạt động hay không, ta có thể dùng lệnh PING. Lệnh này thường được dùng để kiểm tra kết nối giữa 2 trạm.

Ví dụ: Ta ping đến một máy tính có địa chỉ IP là 192.168.2.1

Start -> run -> cmd.

Ping 192.168.2.1 ta sẽ có kết quả như hình sau:

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\voviet&trandai>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Documents and Settings\voviet&trandai>
```

Hình 20. Kết quả lệnh ping khi 2 máy chưa thông với nhau.

Request timed out là kết quả nhận được khi ta thực hiện lệnh ping, điều này có nghĩa là sự kết nối giữa 2 máy chưa thông nhau hay hiện thời máy 192.168.2.1 không hoạt động.

Một ví dụ khác ta sẽ ping tới máy có IP 10.0.0.6 và sẽ cho kết quả như hình sau:

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\voviet&trandai>ping 10.0.0.6

Pinging 10.0.0.6 with 32 bytes of data:
Reply from 10.0.0.6: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\voviet&trandai>
```

Hình 21. Kết quả lệnh ping khi 2 máy thông nhau.

Khi nhận được phản hồi như hình trên có nghĩa là 2 máy kết nối thành công và có thể thực hiện việc truyền và nhận dữ liệu giữa 2 máy.

3.5) Các giao thức tầng Network Access.

Tầng Network access gồm có 4 giao thức là: Ethernet, Token Ring , Token Bus và Fiber.

Chương 2

Tấn Công Từ Chối Dịch Vụ

(Denial of Service)

I) Giới thiệu về tấn công từ chối dịch vụ (DoS).

Trong thực tế có rất nhiều cách tấn công vào mạng internet nói chung và tấn công vào các mạng của các tổ chức, các doanh nghiệp thông qua mạng internet. Với nhiều mục đích khác nhau. Tấn công nhằm ăn cắp thông tin nhạy cảm, tấn công nhằm gây thiệt hại cho đối thủ về cơ sở hạ tầng công nghệ thông tin....

Người tấn công hay là hacker thường dùng các công cụ như virus, worm, trojan. Các lỗi bảo mật hệ thống mà người quản trị chưa fix kịp, hay đơn giản là dựa vào lỗi sơ suất của người dùng để ăn cắp các thông tin về tài khoản, về thẻ tín dụng.

Tấn công từ chối dịch vụ là hành động của giới tin tặc, có thể là của một người hoặc một nhóm người nào đó. Tấn công vào một mạng máy tính nhằm làm đình trệ hoạt động của mạng đó.

1.1) Định nghĩa về tấn công từ chối dịch vụ

Tấn công từ chối dịch vụ là hành động của giới tin tặc, một người hay một nhóm người nào đó. Lợi dụng vào đặc điểm hay lỗi bảo mật, lỗi an toàn thông tin của hệ thống dịch vụ để tấn công, nhằm làm ngưng trệ hoặc ngăn cản người dùng truy cập dịch vụ đó.

Thông thường tấn công từ chối dịch vụ làm cho hệ thống bị sụp đổ hoặc làm treo, tê liệt hệ thống, hoặc tê liệt từng phần của hệ thống. Buộc người quản trị hệ thống phải ngừng cung cấp dịch vụ và khởi động lại hệ thống.

Tóm lại tấn công từ chối dịch vụ là kiểu tấn công làm cho các dịch vụ mạng bị tê liệt, không còn khả năng đáp ứng được yêu cầu nữa. Loại tấn công này ảnh hưởng đến nhiều hệ thống, rất dễ thực hiện nhưng lại rất khó bảo vệ hệ thống khỏi sự tấn công DoS.

1.2) Đặc điểm của tấn công từ chối dịch vụ.

Đặc điểm của cuộc tấn công từ chối dịch vụ là các cuộc tấn công này không lấy cắp thông tin của hệ thống, mục đích cuối cùng của nó thường chỉ làm cho hệ thống bị tê liệt, không hoạt động được. Đôi khi nó gây ra hỏng hóc hệ thống và vì vậy làm mất mát thông tin trong hệ thống.

Nhưng vì mục tiêu của tấn công từ chối dịch vụ là tấn công vào các hệ thống phục vụ khách hàng, mà việc ngừng hoạt động một thời gian nhất định của các hệ thống dịch vụ thường gây ra các thiệt hại không thể ước tính chính xác được. Những thiệt hại đó là: thiệt hại về máy móc do hỏng hóc sau cuộc tấn công, thiệt hại về việc sút giảm uy tín của nhà cung cấp dịch vụ, thiệt hại gián tiếp của khách hàng khi không truy nhập được dịch vụ.

Một số cuộc tấn công DoS trong lịch sử.

Ngày 7/3/2000, website yahoo.com đã phải ngưng phục vụ hàng trăm triệu user trên toàn thế giới nhiều giờ liền. Vài giờ sau, Yahoo đã tìm ra nguyên nhân gây nên tình trạng này, họ đang phải gánh chịu một đợt tấn công DDoS với quy mô vài ngàn máy tính liên tục gửi hàng triệu request đến các server dịch vụ làm các server này không thể phục vụ các user thông thường khác.

Vài ngày sau, một sự kiện tương tự diễn ra nhưng có phần “ồn ào” hơn do một trong các nạn nhân mới là hãng tin CNN, amazon.com, buy.com, Zdnet.com, E-trade.com, Ebay.com Tất cả các nạn nhân là những gã khổng lồ trên Internet thuộc nhiều lĩnh vực khác nhau. Theo ước tính tổng thiệt hại do cuộc tấn công này gây ra lên đến 1.2 triệu USD, nhưng không đáng kể bằng sự mất mát về lòng tin của khách hàng, sự giảm sút uy tín của các công ty là không thể tính được.

Và mới đây nhất tại Việt Nam, đó là cuộc tấn công DoS vào website thương mại điện tử vietcore.

1.3) Phân loại các kiểu tấn công từ chối dịch vụ

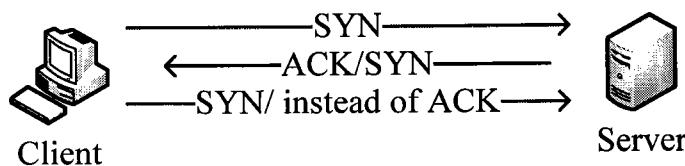
Có rất nhiều cách để phân loại tấn công DoS, nhưng ta có thể phân loại tấn công DoS theo các tính chất sau: Tấn công phá hoại dựa trên tính giới hạn hoặc không thể phục hồi của tài nguyên mạng.

1.3.1) Tấn công thông qua kết nối.

Tấn công kiểu SYN flood.

Đây là cách tấn công dựa trên phương thức hoạt động của kết nối TCP/IP, hacker bắt đầu quá trình yêu cầu thiết lập một kết nối TCP/IP đến mục tiêu cần tấn công và sẽ không gửi trả gói tin ACK cho mục tiêu. Điều này khiến cho mục tiêu luôn rơi vào trạng thái chờ (đợi gói tin ACK trả lời từ phía yêu cầu thiết lập kết nối). Đồng thời hacker gửi liên tục các gói SYN ACK để yêu cầu thiết lập kết nối mới.

Có một cách khác để tấn công thông qua kết nối, đó là giả mạo địa chỉ IP nguồn của gói tin yêu cầu thiết lập kết nối SYN ACK và kết quả cũng giống như trường hợp trên, máy tính đích cũng rơi vào trạng thái chờ vì các gói tin SYS ACK không thể đi đến đích do địa chỉ IP nguồn là không có thật. Kiểu tấn công SYN flood được các hacker áp dụng để tấn công một hệ thống mạng có băng thông lớn hơn hệ thống của hacker.



Hình 22. Tấn công kiểu SYN Flood.

1.3.2) Lợi dụng chính nguồn tài nguyên của nạn nhân để phát động cuộc tấn công.

Kiểu tấn công Land Attack.

Kiểu tấn công này cũng tương tự như kiểu tấn công SYN flood, nhưng hacker sử dụng chính địa chỉ IP của mục tiêu cần tấn công để làm IP nguồn trong gói tin dùng để yêu cầu thiết lập kết nối, với mục đích đẩy mục tiêu vào một vòng lặp vô tận khi cố gắng thiết lập kết nối với chính mình.

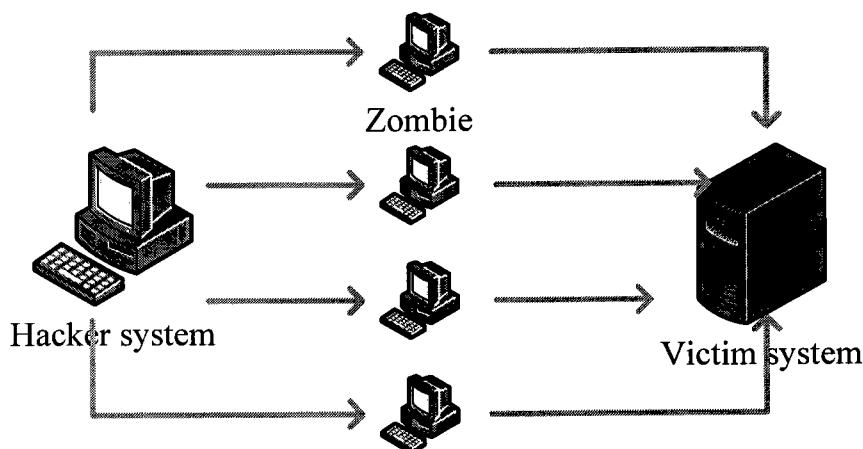
Kiểu tấn công UDP flood.

Hacker gởi gói tin UDP echo với địa chỉ ip nguồn là cổng loopback của chính mục tiêu cần tấn công, hoặc của một máy tính trong cùng mạng. Với mục tiêu sử dụng cổng UDP echo (port 7) để thiết lập việc gởi và nhận các gói tin echo trên 2 máy tính (hoặc giữa mục tiêu với chính nó nếu mục tiêu có cấu hình cổng loopback), khiến 2 máy tính này dần dần sử dụng hết băng thông của chúng, và cản trở việc chia sẻ tài nguyên mạng của các máy tính khác trong mạng.

1.3.3) Tấn công vào băng thông

Tấn công kiểu DDoS (Distributed Denial of Service), tấn công từ chối dịch vụ phân tán.

Đây là kiểu tấn công rất nguy hiểm vì hacker xâm nhập vào nhiều hệ thống máy tính khác nhau, cài đặt các chương trình điều khiển từ xa vào các hệ thống này. Và sẽ kích hoạt đồng thời các chương trình này tại một thời điểm để đồng loạt tấn công vào một mục tiêu. Với DDoS hacker có thể huy động hàng trăm thậm chí hàng ngàn máy tính cùng tham gia tấn công vào mục tiêu tại một thời điểm, làm cho băng thông của mục tiêu bị tiêu tốn hết trong nháy mắt.



Hình 23. Tấn công từ chối dịch vụ phân tán DDoS

1.3.4) Sử dụng nguồn tài nguyên khác.

Hacker sẽ lợi dụng nguồn tài nguyên mà nạn nhân cần sử dụng để tấn công, hacker có thể thay đổi dữ liệu và tự sao chép dữ liệu mà nạn nhân cần lén nhiều lần, làm cho CPU bị quá tải và các quá trình xử lý dữ liệu bị đình trệ.

Tấn công kiểu Smurf Attack

Kiểu tấn công này cần một hệ thống rất quan trọng đó là mạng khuyếch đại, hacker dùng địa chỉ của máy tính cần tấn công để gửi gói ICMP echo cho toàn bộ mạng (broadcast). Các máy tính trong toàn bộ mạng sẽ gửi gói tin ICMP Reply cho máy tính mà hacker muốn tấn công. Kết quả là máy tính này sẽ không thể xử lý kịp thời một lượng lớn thông tin và dẫn tới treo máy.

Tấn công kiểu Tear Drop.

Trong mạng chuyền mạch gói, dữ liệu được chia thành nhiều gói nhỏ và mỗi gói tin có một giá trị offset riêng và có thể truyền theo nhiều đường khác nhau để tới đích. Tại đích dựa vào giá trị của trường offset mà các gói tin được kết hợp lại như ban đầu. Lợi dụng điều này các hacker tạo ra nhiều gói tin có giá trị offset trùng lặp nhau, và gửi đến mục tiêu cần tấn công. Kết quả là máy tính đích không thể sắp xếp lại các gói tin này và bị treo do phải dùng hết tài nguyên để xử lý.

1.3.5) Phá hoại dựa trên cấu hình phần cứng.

Dựa vào việc cấu hình thiếu an toàn như việc không chứng thực quá trình gửi và nhận các bản tin cập nhập của router. Hacker có thể tác động trực tiếp hoặc từ xa để thay đổi cấu hình router làm cho người dùng không thể sử dụng được dịch vụ.

Ví dụ: Hacker có thể thay đổi cấu hình DNS làm cho quá trình biên dịch tên miền sang IP và IP sang tên miền bị sai lệch, hậu quả làm cho các yêu cầu đến từ máy trạm không đến đúng tên miền mong muốn mà bị chuyển sang một miền khác.

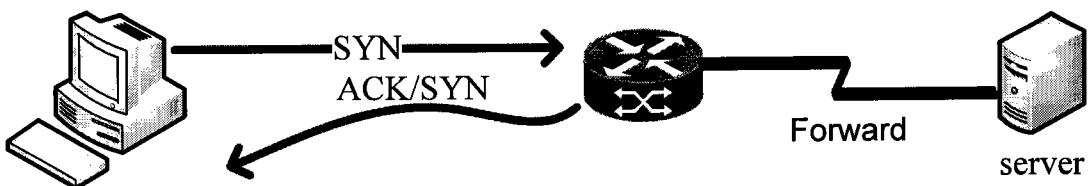
Tương tự, hacker có thể lợi dụng quyền hạn của nạn nhân đối với thiết bị mà có thể phá hoại hoặc đánh sập các thiết bị mạng như router, switch...

II) Chi tiết về các kỹ thuật tấn công từ chối dịch vụ

2.1) Tấn công kiểu SYN Flood

Như đã trình bày ở trên, SYN Flood là kiểu tấn công dựa vào cơ chế bắt tay 3 chiều trong kết nối TCP. Cơ chế bắt tay 3 chiều của TCP được trình bày ở mục 3.3.2 trong chương 1, đã trình bày rõ về hoạt động của TCP.

Trong phần này chỉ trình bày về việc Hacker lợi dụng cơ chế bắt tay 3 chiều trong hoạt động của TCP để phát động tấn công DoS vào hệ thống. Hình bên dưới mô tả cho kiểu tấn công SYN Flood.



Hình 24. Nguyên tắc tấn công kiểu SYN Flood

Hacker bắt đầu cuộc tấn công DoS theo kiểu SYN Flood bằng việc gửi một gói tin yêu cầu thiết lập kết nối đến Server muốn tấn công, theo nguyên tắc của bộ giao thức TCP thì server của nạn nhân sẽ gửi trả lại cho máy của hacker một gói ACK/SYN, nhưng vì địa chỉ IP của hacker là giả nên gói tin phản hồi từ Server không thể đến đích. Vì vậy Server của nạn nhân cũng sẽ không nhận được ACK phản hồi từ máy của hacker. Đồng thời trên server cũng vẫn phải dành một phần tài nguyên của hệ thống để kết nối cho máy Client, sau một thời gian Server sẽ tiếp tục gửi lại gói tin SYN/ACK để xác nhận lại lần nữa, kết nối vẫn tiếp tục mở.

Nếu như Hacker tiếp tục gửi các gói tin tương tự cho đến khi Server không tiếp nhận được yêu cầu thiết lập nào nữa thì lúc đó có nghĩa là hệ thống đã bị phá vỡ.

Tấn công kiểu SYN Flood là tấn công dựa vào kết nối, vì vậy hacker chỉ cần một đường truyền có băng thông nhỏ là có thể đánh sập một hệ thống có băng thông lớn gấp nhiều lần. Và vì địa chỉ IP có thể đổi được một cách dễ dàng nên việc xác định thủ phạm rất khó khăn.

Mặc dù tấn công kiểu SYN Flood không có mục đích tấn công vào cơ sở dữ liệu, nó chỉ tấn công vào một số dịch vụ của hệ thống, các dịch vụ không bị tấn công vẫn có thể tồn tại và hoạt động bình thường nhưng mặc khác thì nó sẽ làm tiêu hao toàn bộ tài

nguyên của hệ thống, từ đây sẽ dẫn đến việc tắt nghẽn hệ thống hay là làm cho hệ thống hoạt động không được như mong muốn.

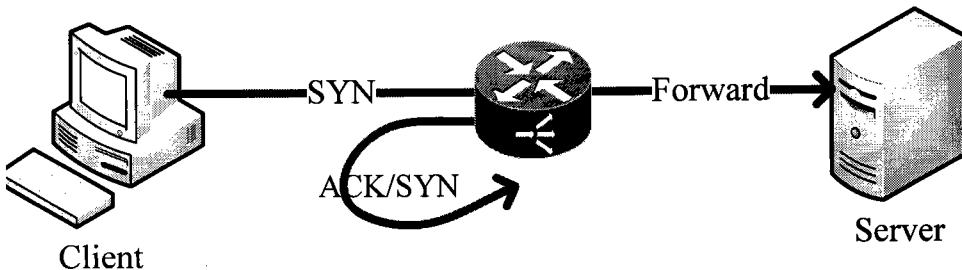
Dấu hiệu nhận biết cuộc tấn công kiểu SYN Flood: Khi ta nhận được một số lượng lớn các gói tin xuất hiện trên mạng mà không có các gói tin trả lời, như vậy, có thể mạng của ta đã bị tấn công dưới hình thức SYN Flood. Lúc này có thể sử dụng lệnh **netstat** để nhận biết một cuộc tấn công với một số lượng lớn các half-open connection. Bên cạnh đó, để người quản trị mạng nhận biết được rằng các gói tin gửi như vậy là có thực hay không.

Cách giảm thiểu hậu quả và ngăn ngừa cuộc tấn công kiểu SYN Flood.

Để phòng tránh cũng như giảm bớt khả năng tấn công kiểu SYN vào hệ thống mạng của mình, chúng ta có thể dùng các cách sau:

- + Dựng FIREWALL cho hệ thống.
- + Cấu hình ACL trên Router.
- + Thiết lập các chính sách bảo mật trên server

2.2) Kiểu tấn công Land Attack.



Hình 25. Nguyên tắc tấn công kiểu Land Attack.

Theo kiểu tấn công này thì Hacker cũng bắt đầu cuộc tấn công bằng cách gởi một gói tin yêu cầu thiết lập kết nối TCP đến Server cần tấn công. Nhưng trong phần địa chỉ IP nguồn của gói tin thì Hacker dùng địa chỉ IP của chính server này.

Khi Server nhận được yêu cầu thiết lập kết nối thì sẽ phản hồi lại cho máy yêu cầu thiết lập kết nối một gói ACK/SYN. Nhưng vì địa chỉ IP nguồn trong gói tin yêu cầu thiết lập kết nối chính là IP của Server nên Server sẽ nhận được gói

ACK/SYN của chính mình gửi và sẽ gửi trả tiếp một gói ACK để thiết lập kết nối, nhưng vì thiết lập kết nối với chính mình nên không thể kết nối được đồng thời quá trình gửi và nhận các gói tin thiết lập cứ tiếp tục diễn ra. Nên cuối cùng thì hệ thống sẽ bị tê liệt do Server dùng hết tài nguyên để cố thiết lập kết nối với chính mình.

2.3) Tấn công kiểu Smurf Attack

Đây là một trong các phương thức tấn công từ chối dịch vụ, Attacker tấn công hệ thống bằng cách sử dụng các gói tin ICMP có địa chỉ nguồn giả mạo là của nạn nhân để gửi đến địa chỉ Broadcast của subnet tương ứng với IP đó. Cuộc tấn công Smurf nhằm vào lớp Network của các host nhằm từ chối tất cả các dịch vụ đến Host.

Địa chỉ Broadcast: Là địa chỉ IP được dùng để đại diện cho tất cả các host trong mạng. Phần host_id chứa các bit 1. Nó dùng để gửi một gói tin đến tất cả các host trên một phân đoạn mạng.

Ví dụ: 192.168.255.255 là địa chỉ Broadcast của mạng 192.168.0.0/16

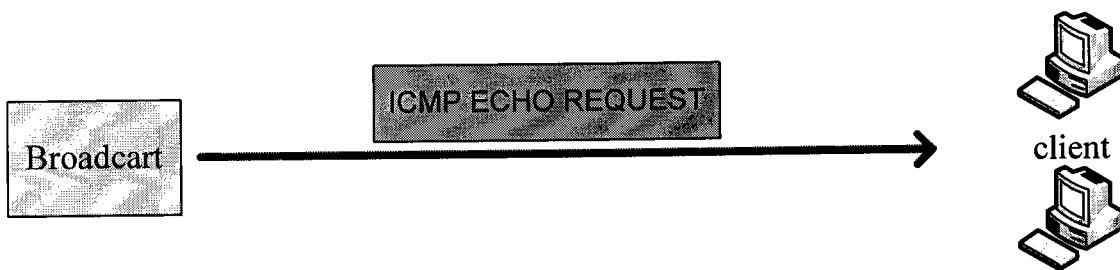
Dựa vào đặc tính của địa chỉ broadcast, nếu như ta gửi một gói tin đến địa chỉ 192.168.255.255 thì nó sẽ tự động forward đến tất cả các máy trong mạng 192.168.0.0. Nếu như ở đây ta sử dụng một địa chỉ lớp A thì số lượng máy trong mạng rất lớn, chính điều này sẽ dẫn đến các gói tin ồ ạt gửi đến các máy trong cùng mạng. Nó sẽ làm cho băng thông của mạng bị giảm sút nghiêm trọng, gây ra tình trạng tắc nghẽn mạng, ngập lụt mạng bằng các gói tin ICMP.

Hai thành phần chính của tấn công Smurf là việc sử dụng các gói tin giả mạo địa chỉ IP của nạn nhân và địa chỉ broadcast. Trong cuộc tấn công Smurf, Attacker sẽ giả mạo địa chỉ nguồn trong ICMP echo request và gửi chúng đến một địa chỉ broadcast. Khi mỗi máy trên mạng nhận và đáp ứng trả lại cho địa chỉ nguồn mà Attacker sử dụng để giả mạo. Minh họa các bước của cuộc tấn công Smurf:

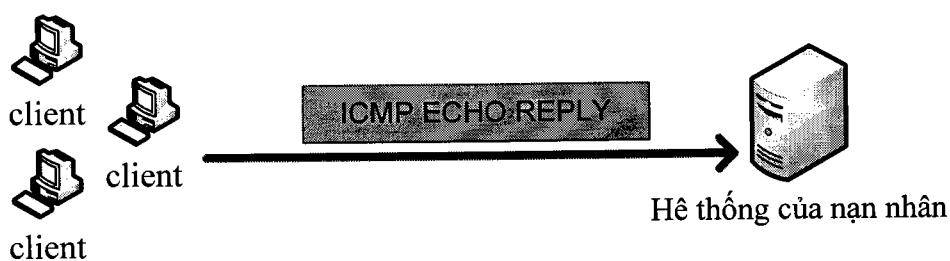
Bước 1.



Bước 2.



Bước 3.



Hình 26. Các bước của quá trình tấn công kiểu Smurf.

Khi tất cả các máy tính trung gian nhận được các gói ICMP Request và đồng loạt trả lời thì khi đó hệ thống của nạn nhân sẽ bị tràn ngập bởi các gói tin ICMP Reply. Hậu quả của cuộc tấn công này gây ra là làm tràn ngập băng thông hệ thống, làm cho hệ thống bị treo và không thể phục vụ các yêu cầu của người dùng.

Một dấu hiệu để nhận biết hệ thống mạng bị tấn công DoS kiểu Smurf là tốc độ truy nhập mạng nội bộ và mạng Internet bị giảm sút. Và vì tấn công kiểu Smurf có thể nhắm tới bất kỳ hệ thống mạng nào, không chỉ là mạng nội bộ các công ty mà có thể tấn công vào các nhà cung cấp dịch vụ internet ISP nhằm làm giảm khả năng cung cấp dịch vụ của các ISP.

Chính vì các ICMP được gửi đến từ một Host và với số lượng lớn hoặc cực lớn nên đây chính là dấu hiệu mà các nhà quản trị mạng dễ dàng nhận biết hệ thống có bị tấn công kiểu Smurf hay không.

Cách giảm thiểu hậu quả và ngăn ngừa cuộc tấn công kiểu Smurf.

Ta có thể cấu hình Access List trên Router để cấm các gói ICMP Request được gửi đến từ một Broadcast với số lượng lớn.

Thiết lập các chính sách bảo mật trên server.

2.4) *tấn công kiểu Ping Of Death*

Đây cũng là một kiểu tấn công DoS dựa vào các gói tin ICMP. phương thức tấn công này được thực hiện bằng cách gửi một số lượng lớn các gói tin ICMP đến một máy đích nào đó bằng lệnh Ping. Ping of Death là một cuộc tấn công dựa vào lớp mạng (lớp thứ ba của mô hình OSI) của máy đích với mục đích loại bỏ tất cả các dịch vụ đang hoạt động trên máy nạn nhân.

Attacker sẽ gửi một số lượng lớn các gói tin ICMP đến nạn nhân. Vấn đề nằm ở chỗ, hệ thống của nạn nhân sẽ không biết sẽ giải quyết như thế nào đối với các gói tin có kích thước lớn hơn kích cỡ max của nó (65535). Vì vậy, sẽ làm cho hệ thống của nạn nhân không hoạt động bình thường hoặc là bị treo. Ví dụ: đối với người dùng WinNT trước đây, thì có thể xác định được hiện tượng này khi gặp màn hình màu xanh của Windows.

Mặc định các gói ICMP gửi đi khi ta thực hiện lệnh Ping là 32 byte. Nhưng Attacker có thể thay đổi kích thước của gói tin ICMP khi ping để tấn công nạn nhân.

Ví dụ : c:>ping -l 1500 it.hutech.edu.vn thì khi này kích thước của gói ICMP là 1500 byte.

Dấu hiệu nhận biết cuộc tấn công kiểu Ping Of Death là trên server nạn nhân bị tràn ngập bởi các gói ICMP Request và dẫn đến máy tính bị treo.

Cách giảm thiểu hậu quả và ngăn ngừa cuộc tấn công kiểu Ping Of Death.

- + Liên tục cập nhật bản vá lỗi do nhà sản xuất cung cấp.
- + Sử dụng Big Firewall.
- + Cấu hình cho router loại bỏ các gói tin có kích thước khác thường, trước khi nó có thể đến được server.

2.5) *Tấn công kiểu DDoS (tấn công từ chối dịch vụ phân tán).*

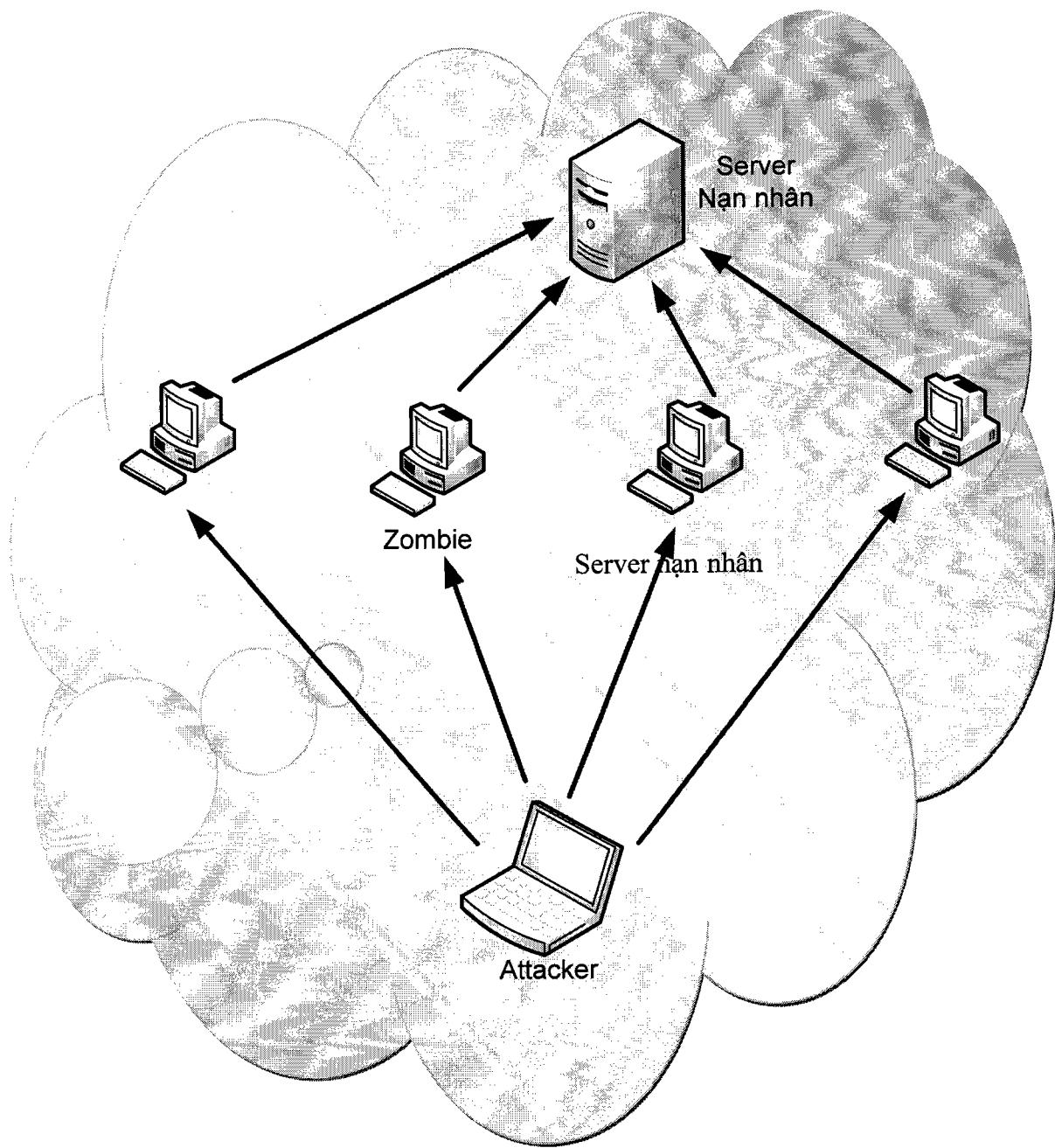
Đây là một biến thể hay là một thế hệ sau của tấn công từ chối dịch vụ, kiểu tấn công này có thể gây ngập hệ thống bằng các gói tin TCP SYN, UDP SYN, hay là các gói

ICMP. Các gói tin này được gởi đến hệ thống của nạn nhân từ nhiều nguồn khác nhau. Và mục đích cuối cùng là làm cho hệ thống của nạn nhân bị tắt nghẽn và gây nên sự ùn tắc dữ liệu.

Tấn công từ chối dịch vụ phân tán nguy hiểm là vì các Hacker dùng các phần mềm gián điệp hay các loại trojan cài vào các hệ thống máy tính của người dùng internet và chiếm quyền điều khiển của họ. Sau khi chiếm quyền điều khiển thì các máy tính này trở thành các Zombie để dùng cho cuộc tấn công DoS sau này. Các trojan mà hacker dùng có thể là Trinoo, Tribe flood network-TFN, Wintrinoo, TFn2K ...

Một khi mà Attacker muốn tấn công vào một hệ thống nào đó thì sẽ ra lệnh cho các máy Zombie này tấn công vào hệ thống của nạn nhân với số lượng lớn, có thể lên đến hàng triệu máy tính cho một đợt tấn công.

Để nhận biết một đợt tấn công DDoS thì đơn giản, vì khi này hệ thống bị tràn ngập các gói tin. Nhưng việc phòng chống thì rất khó khăn vì tấn công từ chối dịch vụ hay tấn công từ chối dịch vụ phân tán đều rất hiệu quả. Để hệ thống có thể hoạt động tốt nhất và ít xảy ra sự cố thì yêu cầu hệ thống phải được bảo vệ ở mức cao nhất có thể.



Hình 27. Mô hình tấn công kiểu DDoS.

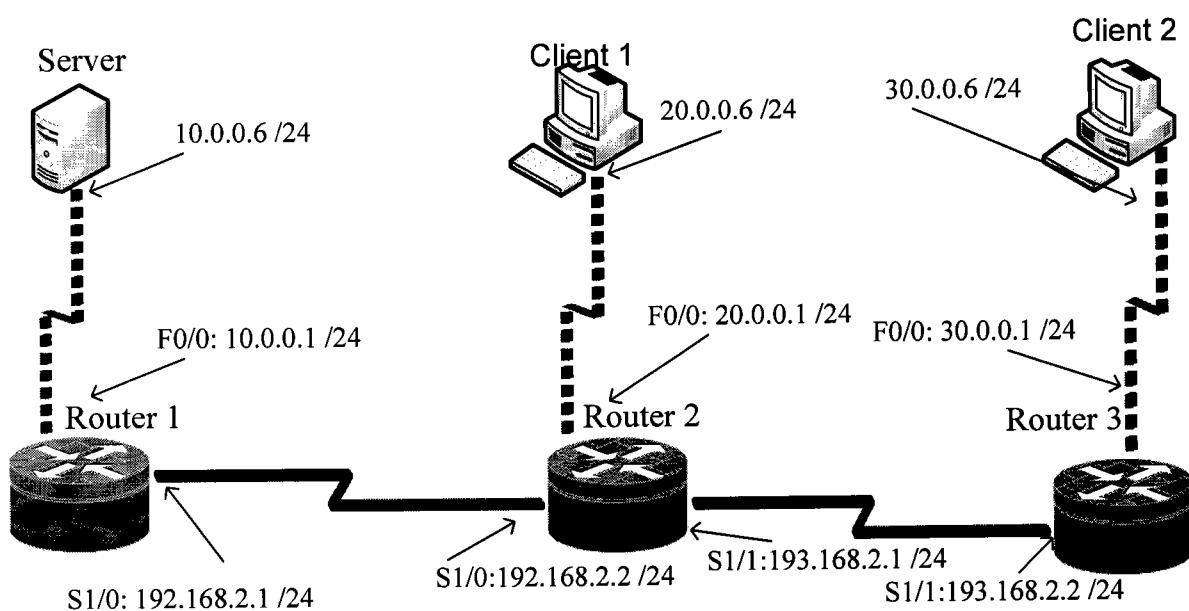
Chương 3

Xây Dựng Mô Hình Tấn Công Thực Nghiệm

I) Giới thiệu về mô hình.

1.1) Mô Hình Mạng Dùng Cho Cuộc Tấn Công theo thực tế.

Trong phạm vi của luận văn này, em xin trình bày quá trình xây dựng hệ thống mạng dùng để mô phỏng cho quá trình tấn công DoS. Hệ thống mạng thực tế được mô tả trong hình sau:



Hình 28. Mô hình mạng khi dùng thiết bị thật.

Trong mô hình này cần có các thiết bị sau:

- + 3 máy vi tính đại diện cho 3 mạng khác nhau.
 - Một máy dùng làm Server và chạy các dịch vụ mạng như webserver.
 - Một máy dùng làm Client 1, máy này dùng để tấn công vào Server.
 - Một máy dùng làm Client 2, máy này sẽ truy cập web khi Server đang bị tấn công.
- + 3 Router Cisco 7200.

Tất cả các máy tính trên đều có card mạng và được cài Drive đầy đủ.

Ta kết nối các router vào các máy như hình bên trên.

Cổng Serial 1/0 của Router 1 có địa chỉ IP là 192.168.2.1 /24, sẽ nối với cổng Serial 1/0 của Router 2 có IP là 192.168.2.2 /24.

Cổng Serial 1/1 của Router 2 có IP là 193.168.2.1 /24, sẽ nối với cổng Serial 1/0 của Router 3 có địa chỉ IP là 193.168.2.2 /24.

Cổng FastEthernet F0/0 của Router 1 có IP là 10.0.0.1 /24, sẽ nối với máy Server.

Cổng FastEthernet F0/0 của Router 2 có IP là 20.0.0.1 /24, sẽ nối với máy Client 1.

Cổng FastEthernet F0/0 của Router 3 có IP là 30.0.0.1 /24, sẽ nối với máy Client 2.

1.2) Mô Hình Mạng Dùng Cho Cuộc Tấn Công Được xây dựng trong luận văn.

Yêu cầu của luận văn là phải xây dựng một hệ thống dùng để mô phỏng cuộc tấn công, hệ thống gồm 3 Router Cisco. Nhưng một phần do chi phí quá cao nên các router này em dùng phần mềm mô phỏng Router là Dynamic.

Vì là dùng phần mềm để thay cho Router thật nên thiết bị thật cần chuẩn bị để xây dựng mạng có vài sự thay đổi, và có một vài thay đổi về cách kết nối các thiết bị với nhau so với các thiết bị thật.

Chi tiết về cách kết nối cũng như các thiết bị cần thiết sẽ được trình bày chi tiết sau đây:

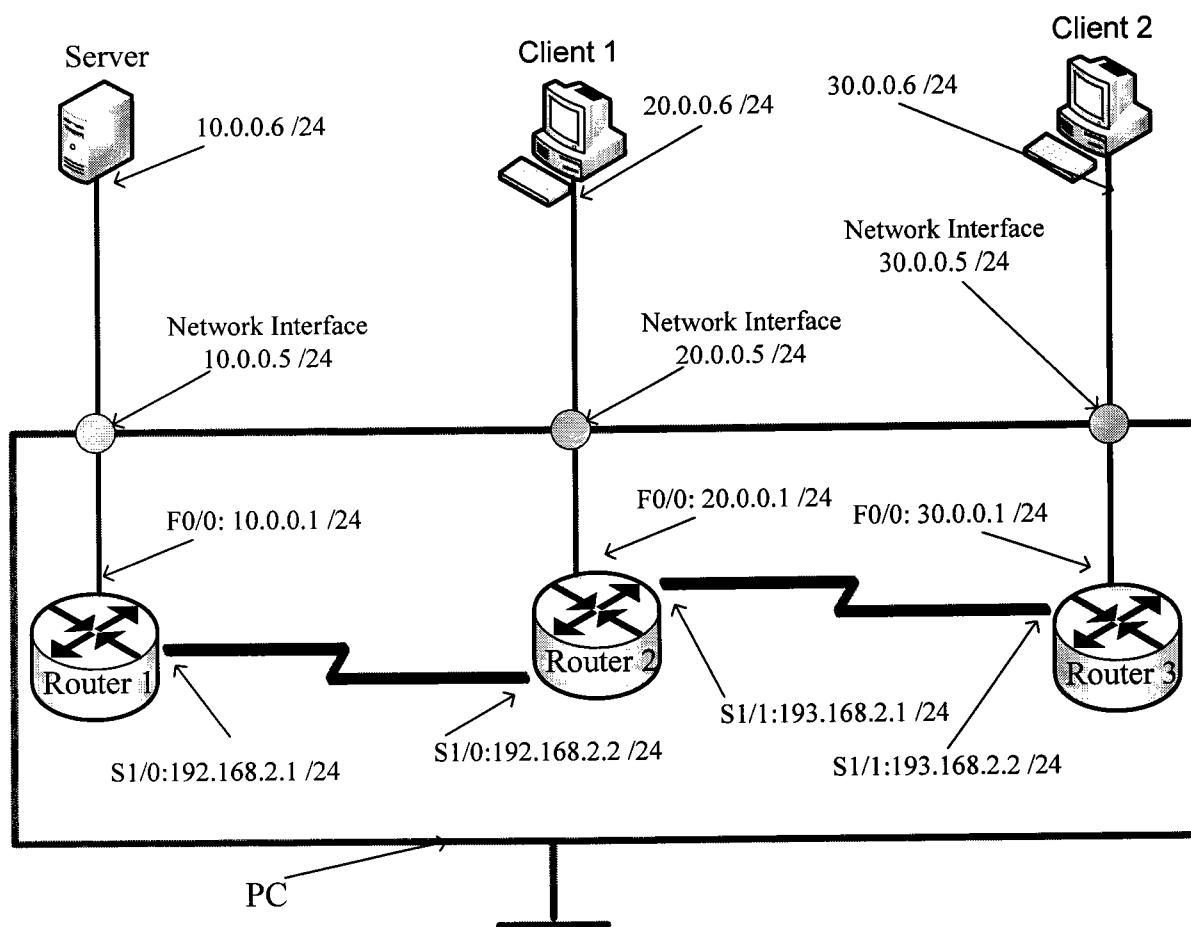
Các thiết bị cần dùng:

+ 4 máy vi tính, 6 card mạng.

- Một máy dùng làm Server và chạy các dịch vụ mạng như webserver.
- Một máy dùng làm Client 1, máy này dùng để tấn công vào Server.
- Một máy dùng làm Client 2, máy này sẽ truy cập web khi Server đang bị tấn công.
- Một máy với cấu hình mạnh gắn 3 card mạng, dùng để chạy 3 Router Dynamic.

Các máy tính Server, Client 1, Client 2 đều phải gắn card mạng và cài Driver đầy đủ.

Mô hình kết nối thiết bị như sau:



Hình 29. Mô hình kết nối mạng dùng phần mềm Dynamic.

Trong mô hình này các Router cũng kết nối với nhau thông qua cổng Serial. Cụ thể như sau:

Cổng Serial 1/0 của Router 1 có địa chỉ IP là 192.168.2.1 /24, sẽ nối với cổng Serial 1/0 của Router 2 có IP là 192.168.2.2 /24.

Cổng Serial 1/1 của Router 2 có IP là 193.168.2.1 /24, sẽ nối với cổng Serial 1/0 của Router 3 có địa chỉ IP là 193.168.2.2 /24.

Nhưng vì 3 Router này cùng nằm bên trong một máy tính, nên các cổng FastEthernet từ các router sẽ kết nối với các card mạng tại máy tính này. Cụ thể:

Cổng FastEthernet F0/0 của Router 1 có IP là 10.0.0.1 /24 sẽ Map card với card mạng thứ nhất của PC. Và card mạng thứ nhất sẽ có IP là 10.0.0.5 /24. Máy Server sẽ có IP là 10.0.0.6 /24 với Default Getway là 10.0.0.1 và kết nối vào card mạng thứ nhất. Như vậy ta đã có được 1 mạng là 10.0.0.0/24 thông qua Router 1 để có thể nối với các mạng còn lại.

Cổng FastEthernet F0/0 của Router 2 có IP là 20.0.0.1 /24 sẽ Map card với card mạng thứ hai của PC. Và card mạng thứ hai có IP là 20.0.0.5 /24. Máy Client 1 sẽ có IP là 20.0.0.6 /24 với Default Getway là 20.0.0.1 sẽ Map card vào card mạng thứ hai. Như vậy ta đã có được mạng thứ 2 là 20.0.0.0/24 thông qua Router 2 để có thể nối với các mạng còn lại.

Cổng FastEthernet F0/0 của Router 3 có IP là 30.0.0.1 /24 sẽ Map card với card mạng thứ ba của PC. Và card mạng thứ ba có IP là 30.0.0.5 /24. Máy Client 2 sẽ có IP là 30.0.0.6 /24 với Default Getway là 30.0.0.1 sẽ Map card vào card mạng thứ hai. Như vậy ta đã có được mạng thứ 3 là 30.0.0.0/24 thông qua Router 3 để có thể nối với mạng 10.0.0.0 và 20.0.0.0.

Kết luận: Như vậy thông qua 4 máy vi tính và 6 card mạng, phần mềm giả lập Router. Ta đã xây dựng được một mô hình gồm 3 hệ thống mạng khác nhau được kết nối lại với nhau thông qua 3 Router.

1.3) Cấu hình Router

Để cấu hình cho Router, tại màn hình Destop. Double Click vào biểu tượng của Dynamic server. Tiếp theo chạy File *StartingRouter.net*. Tại cửa sổ Dynagen, đánh lệnh list để xem có bao nhiêu Router và trạng thái cũng như version của các Router.

```

Dynagen
Reading configuration file...
Network successfully started
Dynagen management console for Dynamips
=> list
Name      Type       State      Server          Console
R1        7200      stopped    localhost:7200  2001
R2        7200      stopped    localhost:2299  2002
R3        7200      stopped    localhost:7200  2003
=>

```

Hình 30. Trạng thái các Router.

Lần lượt Start 3 Router R1, R2, R3 lên. Sau khi Start xong thì ta dùng lệnh list để kiểm tra lại lần nữa xem tất cả 3 Router đã thực sự chạy chưa. Nếu tất cả 3 Router đều ở trạng thái Running thì việc khởi động Router hoàn thành.

```

Dynagen
Reading configuration file...

Network successfully started
Dynagen management console for Dynamips

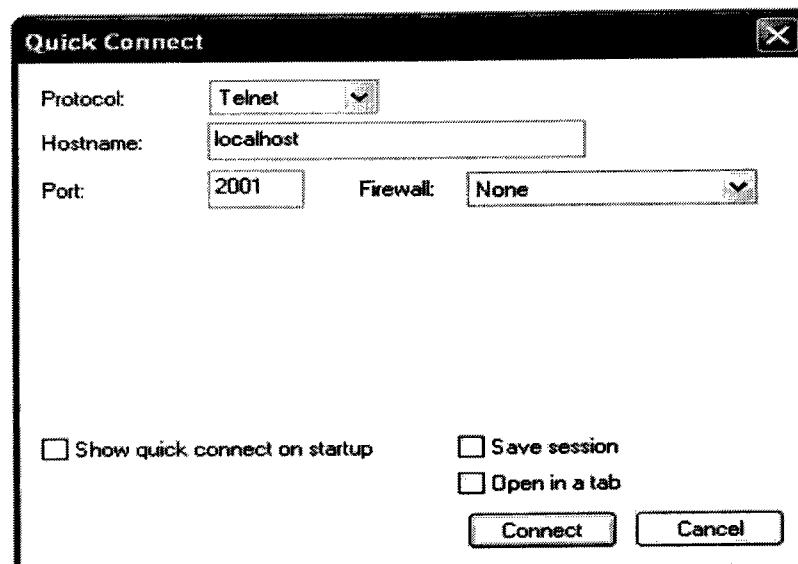
=> start R1
100-C7200 'R1' started
=> start R2
100-C7200 'R2' started
=> idlepc get R2 2
R2 already has an idlepc value applied.
=> idlepc get R3
R3 already has an idlepc value applied.
=> start R3
100-C7200 'R3' started
=> idlepc get R3 3
R3 already has an idlepc value applied.
=> list
Name      Type      State      Server      Console
R1        7200      running    localhost:7200  2001
R2        7200      running    localhost:7200  2002
R3        7200      running    localhost:7200  2003
=>

```

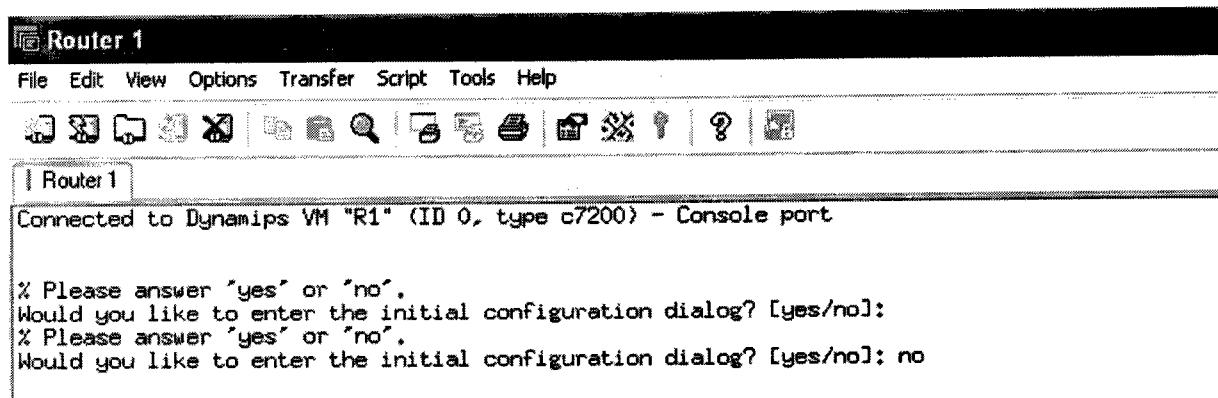
Hình 31. Trạng thái các Router sau khi Start.

Cấu hình cho Router 1

Để bắt đầu quá trình cấu hình cho Router R1, ta mở chương trình SecureCRT, đây là console để thao tác lên Router. Ở mục protocol ta chọn Telnet, mục Hostname nhập vào localhost, và mục Port ta nhập vào port của Router R1 là 2001. Cuối cùng nhấn connect để kết nối với Router R1.



Sau khi màn hình console hiện ra, chọn No như hình dưới.



tiếp theo dùng lệnh sau:

Router>enable

Router#configure terminal

Router(config)#hostname Router_1 #đổi tên Router

Router_1(config)#interface s1/0 #cấu hình cho cổng Serial 0/0

Router_1(config-if)#ip add 192.168.2.1 255.255.255.0 # thiết lập IP cho cổng S0/0

Router_1(config-if)#clock rate 64000

Router_1(config-if)#no shut

Router_1(config-if)#{}

*Dec 6 15:10:42.311: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up

*Dec 6 15:10:43.315: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up

Router_1(config-if)#exit

Router_1(config)#

Router_1(config-if)#interface f0/0 #cấu hình cho cổng FastEthernet 0/0

Router_1(config-if)#ip add 10.0.0.1 255.255.255.0

Router_1(config-if)#no shut

Router_1(config-if)#

*Dec 6 15:11:36.783: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up

*Dec 6 15:11:37.783: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router_1(config-if)#exit

Router_1(config)#router rip

Router_1(config-router)#network 192.168.2.0

Router_1(config-router)#network 10.0.0.0

Router_1(config-router)#

Router_1(config-router)#exit

Router_1(config)#exit

Router_1#

Router_1#show ip interface brief

Interface	IP-Address	OK? Method Status	Protocol
FastEthernet0/0	10.0.0.1	YES manual up	up
Serial1/0	192.168.2.1	YES manual up	up

Sau khi nhập lệnh *show ip interface brief* nếu máy báo kết quả như bảng trên thì việc cấu hình và quảng bá cho Router_1 đã thành công.

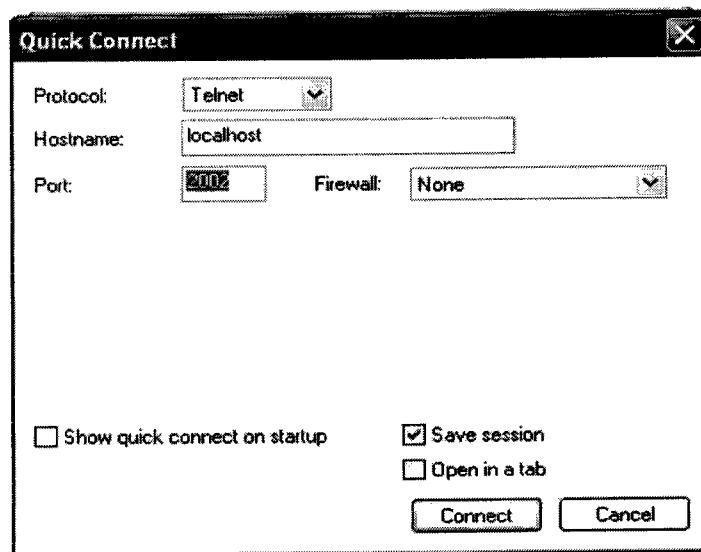
Trên Router_1 ta cấu hình 2 cổng: S1/0 có IP là 192.168.2.1

F0/0 có IP là 10.0.0.1

Và Router_1 quảng bá 2 mạng là : 192.168.2.0 và 10.0.0.0

Cấu hình cho Router 2

việc cấu hình Router_2 làm tương tự Router_1. Nhưng khi kết nối ta chọn cổng kết nối là 2002. Vì trong file StartingRouter.net cổng kết nối của Router_2 có giá trị là 2002.



tiếp sau đây là lệnh cấu hình cho Router_2

Would you like to enter the initial configuration dialog? [yes/no]:

% Please answer 'yes' or 'no'.

Would you like to enter the initial configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>enable

Router#configure terminal

Router(config)#

Router(config)#hostname Router_2

Router_2(config)#interface s1/0 # cấu hình cho cổng Serial 1/0

```
Router_2(config-if)#ip add 192.168.2.2 255.255.255.0
Router_2(config-if)#clock rate 64000
Router_2(config-if)#no shut
Router_2(config-if)#
*Dec 6 20:50:21.403: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
*Dec 6 20:50:22.407: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/0, changed state to up
Router_2(config-if)#exit
```

```
Router_2(config)#interface s1/1          # cấu hình cho cổng Serial 1/1
Router_2(config-if)#ip add 193.168.2.1 255.255.255.0
Router_2(config-if)#clock rate 64000
Router_2(config-if)#no shut
Router_2(config-if)#
*Dec 6 20:51:07.427: %LINK-3-UPDOWN: Interface Serial1/1, changed state to up
*Dec 6 20:51:08.431: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/1, changed state to up
```

```
Router_2(config)#interface f0/0
Router_2(config-if)#ip add 20.0.0.1 255.255.255.0
Router_2(config-if)#no shut
*Dec 6 20:51:54.119: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state
to up
*Dec 6 20:51:55.119: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
Router_2(config-if)#exit
```

```

Router_2(config)#router rip
Router_2(config-router)#network 192.168.2.0
Router_2(config-router)#network 193.168.2.0
Router_2(config-router)#network 20.0.0.0
Router_2(config-router)#exit
Router_2(config)#exit
Router_2#show ip interface brief

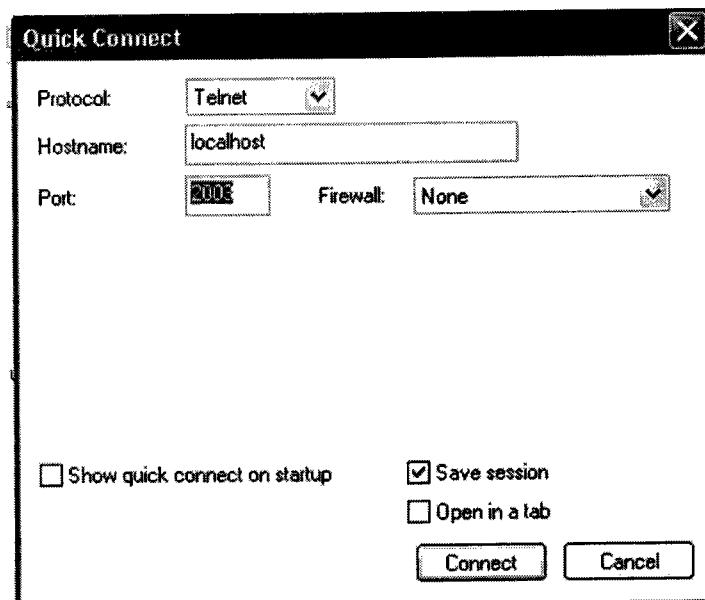
```

Interface	IP-Address	OK? Method Status	Protocol
FastEthernet0/0	20.0.0.1	YES manual up	up
Serial1/0	192.168.2.2	YES manual up	up
Serial1/1	193.168.2.1	YES manual up	up

Trạng thái của các cổng Serial 1/0, Serial 1/1, FastEthernet 0/0. Đều UP và các giao thức đều UP. Nên việc cấu hình cho Router_2 đã thành công.

Cấu hình cho Router 3.

Chúng ta kết nối Router 3 vào console như hình dưới. 2 tab protocol và hostname giống như Router 1 và Router 2, chỉ thay đổi ở tab port là 2003.



phân lệnh cấu hình cho Router 3.

Would you like to enter the initial configuration dialog? [yes/no]:

% Please answer 'yes' or 'no'.

Would you like to enter the initial configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>enable

Router#configure terminal

Router(config)#

Router(config)#hostname Router_3

Router_3(config)#interface s1/0

Router_3(config-if)#ip add 193.168.2.2 255.255.255.0

Router_3(config-if)#clock rate 64000

Router_3(config-if)#no shut

Router_3(config-if)#exit

*Dec 6 20:51:07.427: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up

*Dec 6 20:51:08.431: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up

Router_3(config)#interface f0/0

Router_3(config-if)#ip add 30.0.0.1 255.255.255.0

Router_3(config-if)#no shut

Router_3(config-if)#exit

*Dec 6 20:51:54.119: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up

*Dec 6 20:51:55.119: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router_2(config)#router rip

Router_2(config-router)#network 193.168.2.0

Router_2(config-router)#network 30.0.0.0

Router_2#show ip interface brief

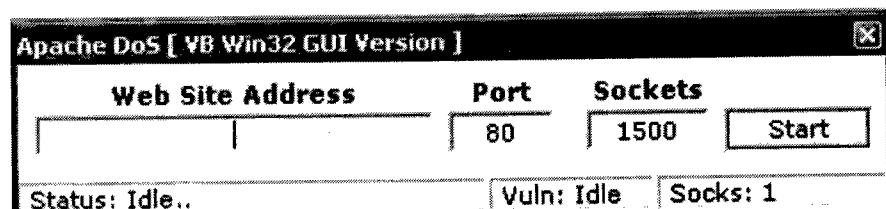
Interface	IP-Address	OK? Method Status	Protocol
FastEthernet0/0	30.0.0.1	YES manual up	up
Serial1/0	193.168.2.2	YES manual up	up

Như vậy trong luận văn này em đã trình bày xong việc xây dựng mô hình mạng gồm 3 hệ thống mạng khác nhau là: 10.0.0.1 /24, 20.0.0.1 /24 và 30.0.0.1/ 24, dùng cho việc Demo quá trình tấn công DoS.

II) Giới thiệu về công cụ tấn công Apache DoS.

Apache DoS là công cụ dùng để thực hiện cuộc tấn công DoS theo kiểu SYN Flood. Để thực hiện quá trình DoS, trước tiên cần cài đặt chương trình Apache DoS lên máy đóng vai trò là Attacker.

Sau đó khởi động chương trình Apache DoS và nhập địa chỉ IP hay tên Website muốn tấn công vào ô “Web site Address”, nhập số lượng socket muốn mở, mặc định là 1500 socket.



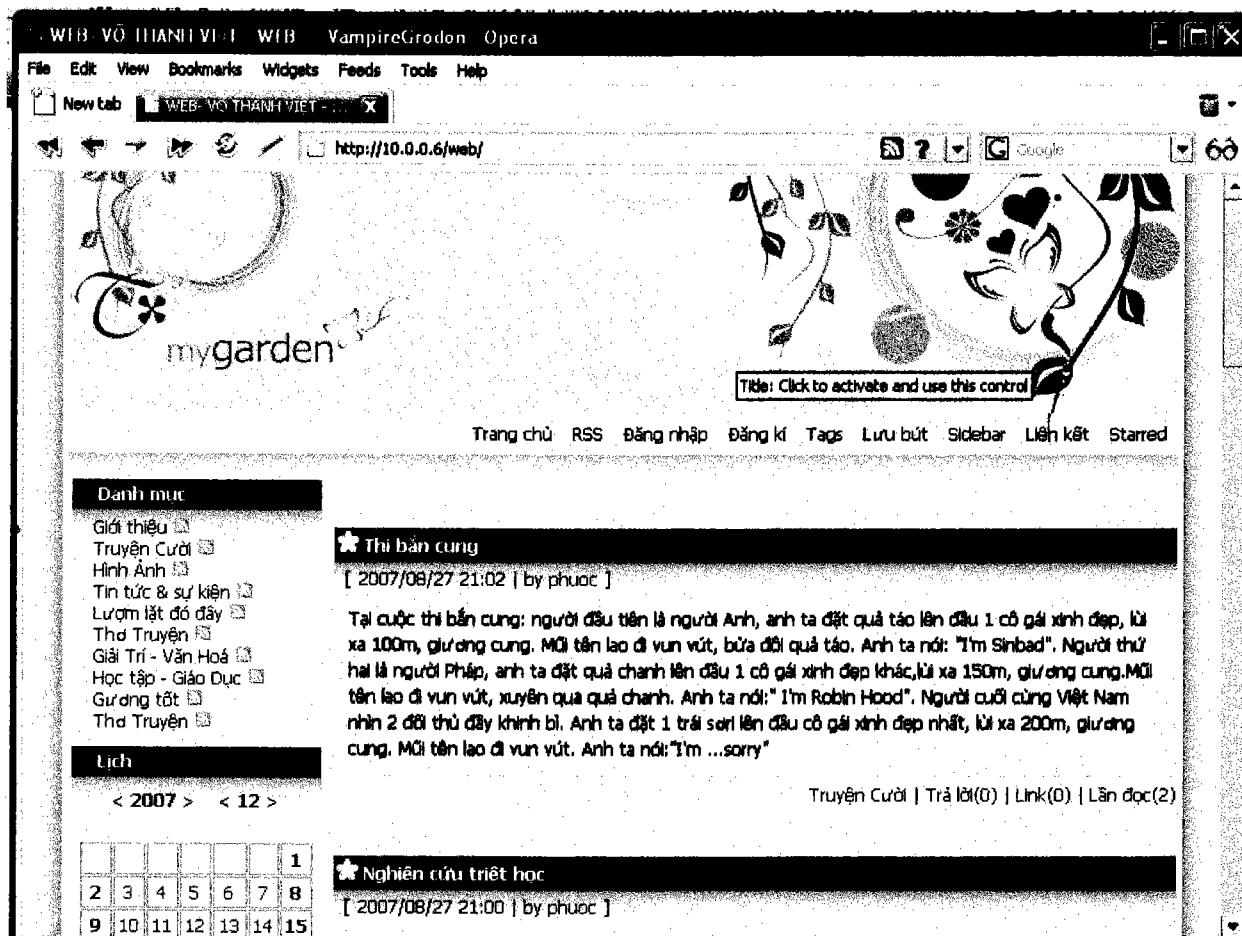
Hình32. Chương trình Apache DoS.

Apache DoS có thể mở một khối lượng lớn socket trên server và từ đó làm tràn bộ đệm của webserver. Làm cho Websever không còn khả năng phục vụ các user bình thường khác.

III) thực hiện quá trình tấn công DoS

Bước 1.

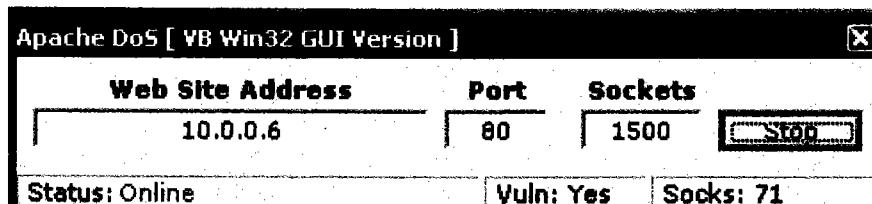
Máy tính của mạng 30.0.0.0 đóng vai trò là người dùng, có thể truy nhập vào web site đặt tại máy 10.0.0.6 bình thường khi cuộc tấn công chưa xảy ra.



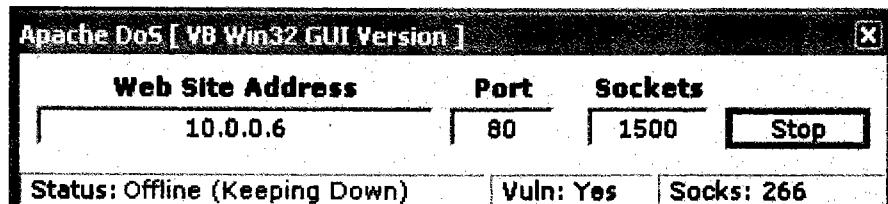
Hình33. Hình ảnh Web site hoạt động bình thường.

Bước 2.

Tại máy tính đóng vai trò Attacker, khởi động chương trình Apache DoS và nhập vào địa chỉ của Webserver để bắt đầu quá trình tấn công.



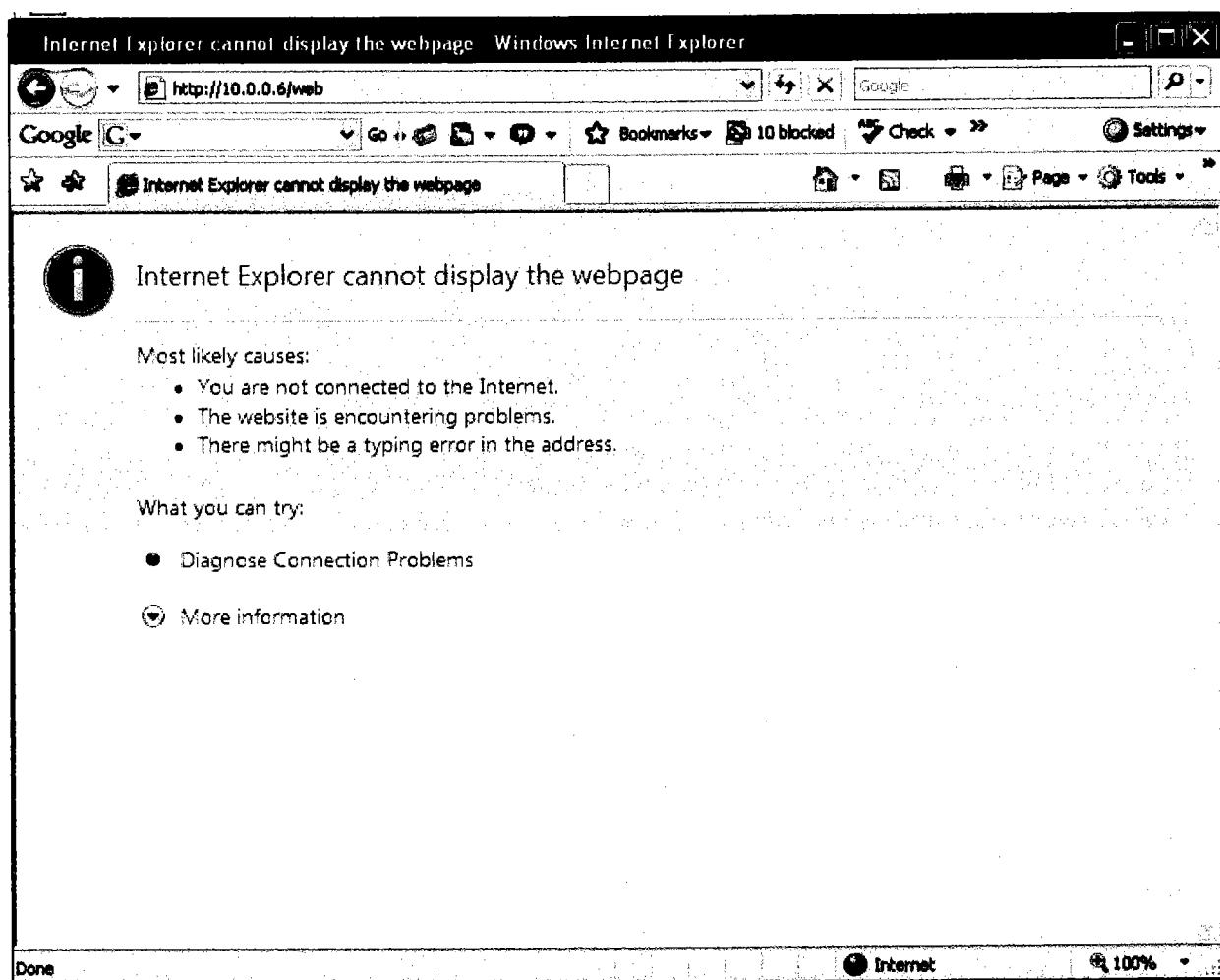
Hình 34. Hoạt động của Apache DoS khi tấn công vào Website.



Hình35. Trạng thái bị đánh sập hoàn toàn của website đặt tại máy 10.0.0.6**Bước 3.**

Sau khi tấn công DoS và trạng thái của Website trên công cụ Apache DoS là offline (Keeping Down) thì lúc này có nghĩa là website đã bị sập hoàn toàn.

Tại máy tính Đóng vai trò là người dùng không thể truy nhập vào Website như bình thường.

**Hình 36.** Người dùng không thể truy nhập web khi server đang bị tấn công.

Kết quả sau khi bị tấn công DoS bằng Syn Flood, webserver đã bị tràn bộ đệm và không thể đáp ứng nhu cầu của người dùng .

PHẦN II. CÁC PHƯƠNG PHÁP PHÒNG CHỐNG TẤN CÔNG

Chương 4

Phòng chống tấn công DoS với tập lệnh *TCP intercept*

I) Các phương pháp phòng chống tấn công

Trong thực tế có rất nhiều cách để có thể thực hiện tấn công DoS, nhưng đặc điểm nổi bật của phương pháp này là sử dụng một số lượng lớn máy tính để làm tràn ngập mạng bằng các gói tin. Vì vậy để bảo vệ hệ thống trước các đợt tấn công DoS hay DDoS thì việc trước tiên người quản trị hệ thống cần phải nắm rõ thông tin cũng như cách thức hoạt động của từng phương pháp tấn công. Nắm rõ cách nhận biết cho từng trường hợp cụ thể để có thể phần nào khắc phục và làm giảm bớt cường độ khi có cuộc tấn công xảy ra.

Trong phạm vi nghiên cứu của luận văn em không hi vọng sẽ bảo vệ hệ thống an toàn tuyệt đối trước các phương pháp tấn công DoS, em chỉ tập trung nghiên cứu một số phương pháp nhằm phòng chống lại các phương pháp tấn công DoS thường gặp như SYN Flood, Ping Of Death.

Để thực hiện được điều này thì với vai trò của người quản trị hệ thống nên thực hiện các chính sách bảo vệ sau:

- + Cần phải sử dụng một hệ thống có sự bảo vệ, với các ứng dụng thì điều cần thiết là phải thường xuyên cập nhập các bản vá lỗi. Siết chặt việc quản lý cơ sở dữ liệu.
- + Nên bật tất cả các Firewall có trong hệ điều hành.
- + Thiết lập các chính sách bảo mật trên Server.
- + Cài đặt các hệ thống phát hiện xâm nhập bất hợp pháp.
- + Sử dụng các công cụ Scan hệ thống để quét thường xuyên và phát hiện kịp thời khi có cuộc tấn công nhằm có hướng khắc phục cụ thể.

+ Backup dữ liệu thường xuyên và lưu giữ cẩn thận tại một nơi khác để có thể phục hồi hệ thống khi cần thiết.

Trong trường hợp hệ thống đang phải gánh chịu các đợt tấn công DoS thì có thể giảm nhẹ cường độ của cuộc tấn công bằng các cách sau:

+ Có thể mở rộng băng thông khi đang bị tấn công, đây là giải pháp tình thế và rất tốn kém, nhưng đây là một trong các giải pháp có thể dùng để giải quyết trong tình thế cấp bách để mở rộng băng thông nhằm đáp ứng phần nào nhu cầu trong giờ cao điểm.

+ Thiết lập các Router nhằm theo dõi thông tin trên mạng.

Tuy nhiên, nơi tốt nhất để có thể ngăn chặn các cuộc tấn công DoS không nằm trong hệ thống mạng của các doanh nghiệp mà là nằm ở các nhà cung cấp dịch vụ ISP. Ví dụ: họ có thể hạn chế băng thông của một luồng thông tin cụ thể nào đó vào bất cứ lúc nào. Đáng tiếc một điều là không phải nhà cung cấp dịch vụ nào cũng có thể làm được điều này, vì vậy tốt nhất là các doanh nghiệp, các nhà quản trị cho các doanh nghiệp nên thảo luận rõ với các nhà ISP về vấn đề bảo vệ an ninh Website trước khi ký hợp đồng với họ.

1.1) Xây dựng hệ thống FIREWALL

Thuật ngữ Firewall hay còn gọi là tường lửa đã xuất hiện từ rất lâu. Đây là phương pháp nhằm ngăn cản sự truy nhập bất hợp pháp vào một hệ thống mạng. Tường lửa đóng vai trò như một trạm kiểm soát các dữ liệu trước khi đi vào hệ thống. Tùy theo khả năng của từng cá nhân, từng doanh nghiệp mà có thể trang bị cho hệ thống của mình những bức tường lửa khác nhau. Đó có thể là phần mềm, có thể là các thiết bị phần cứng. Nhưng mục tiêu cuối cùng là ngăn cản những gói tin, những truy cập không mong muốn đi vào hệ thống.

Tường lửa được ứng dụng vào mạng làm cho hệ thống mạng trở nên an toàn hơn và tường lửa thường được dùng để ngăn cách một mạng nội bộ với một mạng khác. Ví dụ: Như là ngăn cách giữa mạng nội bộ của một công ty với hệ thống mạng internet. Hay là ngăn cách giữa các phòng ban với nhau trong cùng một hệ thống mạng.

Có nhiều cách để phân loại tường lửa, có thể phân loại theo chức năng hay có thể phân loại tường lửa theo cấu trúc. Phân loại tường lửa theo cấu trúc là tường lửa bằng phần cứng hay là các phần mềm.

Trên thị trường hiện nay có rất nhiều thiết bị phần cứng có vai trò là Firewall, một số sản phẩm Firewall có chất lượng được đánh giá cao như:

Router tích hợp tính năng Firewall của tập đoàn Cisco.

Tập đoàn Cisco là tập đoàn chuyên về các thiết bị mạng như Router, Bridge, Switch,.....và các dòng sản phẩm Router tích hợp tính năng Firewall. Các dòng sản phẩm có tích hợp Firewall của cisco như Router các đời: serial 2500, 2800..và các dòng sản phẩm cao cấp như serial 3600, serial 7200.

Các dòng sản phẩm trên ngoài chức năng định tuyến còn tích hợp các tính năng bảo vệ hệ thống mạng như mã hóa bằng phần cứng, hệ thống phát hiện và ngăn chặn xâm nhập bất hợp pháp, mạng liên ảo, các tính năng Firewall, ngăn chặn virus,...

Thiết bị Firewall của tập đoàn FortiNet đó là dòng sản phẩm tích hợp bảo vệ Fortigate.

Thiết bị bảo mật Fortigate là dòng sản phẩm của tập đoàn FortiNet, được phân phối độc quyền tại TPHCM qua công ty Hozitech. Các sản phẩm của FortiNet có tích hợp nhiều tính năng bảo vệ hệ thống.

Fortigate có nhiều dòng sản phẩm như: FortiGate 60, FortiGate 100A, FortiGate 200A, FortiGate 300A.

Dòng Fortigate Advance có các dòng sau: FortiGate-5140 ATCA, FortiGate-5050 ATCA, FortiGate-5020 ATCA , FortiGate-5001/5005

Fortigate là dòng sản phẩm tích hợp. tất cả trong một với nhiều tính năng như:

Firewall: Chống lại các xâm nhập.

Antivirus: Đảm bảo hệ thống không bị nhiễm virus.

IPS: Chống lại các tấn công độc hại.

Antispam: Giảm việc nhận các mail không mong muốn.

Web filters: Ngăn chặn truy cập các trang web không mong muốn.

VPN: Cung cấp các kết nối truy xuất an toàn.

Checkpoint Safe@Office 255.

Safe@Office 255 là một trong những dòng sản phẩm bảo mật đầu tiên, đây là dạng tường lửa dành cho các doanh nghiệp nhỏ, hệ thống văn phòng với số lượng user ít. Safe@Office 255 tích hợp các tính năng tường lửa, DNS động, VPN và các tính năng phòng chống Virus cho email. Ngoài ra các tính năng này được cập nhật tự động các thông tin update thông qua internet một khi có các tính năng mới như tự động cập nhập danh sách các virus.

BizGates

Đây là một giải pháp bảo mật mới cho hệ thống mạng của các doanh nghiệp vừa và nhỏ. Sản phẩm được phân phối bởi Công Ty Cổ Phần Công Nghệ Hà Nội (HaNoiTJSC), đây cũng là một dòng sản phẩm bảo mật tích hợp mới.

BizGates cung cấp giải pháp bảo mật tích hợp sẵn trong thiết bị với đầy đủ các tính năng bảo mật, kết nối VPN và quản trị cao cấp, có thể triển khai ở mọi tổ chức sử dụng kết nối từ mạng nội bộ vào Internet, kết nối các chi nhánh với nhau. Hỗ trợ Firewall thế hệ 3 (statefull inspection), VPN. Đặc biệt, dòng sản phẩm BizGates Security Gateway 20K có khả năng cân tải trên 6 đường kết nối Internet, hỗ trợ 256 kết nối theo mô hình Site-to-Site và 1000 kết nối Home-to-Site tại một thời điểm.

Hiện tại BizGate có các dòng sản phẩm sau:

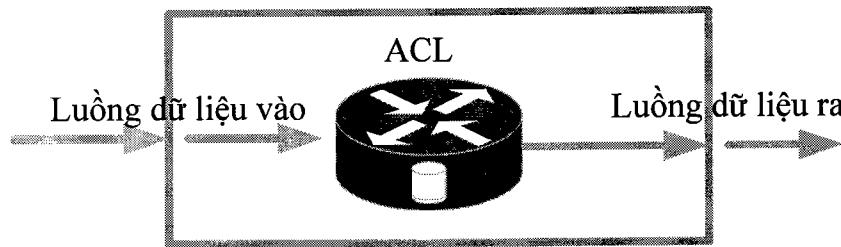
Biz-5K, Biz-2K, Biz-2K-W, Biz-20K.

II) Giới thiệu về tập lệnh TCP intercept của Router Cisco 7200.

TCP intercept là một trong những đặc tính của bộ Cisco IOS Firewall, thường được dùng để phòng chống các cuộc tấn công DoS kiểu TCP SYN flood.

2.1) Access Control List (ACL):

ACL hay còn gọi là danh sách điều khiển truy nhập, chức năng của Access Control List là lọc gói tin nhằm ngăn cản và làm giảm bớt các gói tin không cần thiết đi vào mạng. Một danh sách điều khiển truy nhập có thể chứa nhiều quy luật điều khiển do người quản trị hệ thống đặt ra.



Hình 37. Luồng dữ liệu vào và ra khỏi ACL

Các gói tin đi vào và ra khỏi hệ thống mạng sẽ được kiểm tra bởi các điều kiện trong danh sách truy nhập. Nếu như thỏa mãn các điều kiện được đặt ra thì router sẽ cho phép gói tin đi qua, ngược lại thì Router sẽ loại gói tin khỏi mạng. Đối với IP traffic có các loại ACL sau:

- + Access List (IP Standard): dùng để kiểm tra địa chỉ IP nguồn
- + Access List (IP extended): được dùng để kiểm tra địa chỉ IP đích, IP nguồn của gói tin, kiểm tra các Port như UDP, TCP, ICMP.....
- + Named ACL: Có thể dùng để chỉ định ACL là Standard hay Extended.

cấu trúc tổng quát của danh sách điều khiển truy nhập.

Router(config)#**access-list <Access List Number>**{ permit|deny} <condition>

<Access List Number>: đây là giá trị của ACL cho IOS biết nó là loại ACL nào.

Giá trị của IP Standard ACL từ 1 -> 99.

 Extended ACL từ 100 -> 199.

 từ 1000 -> 1099 là của IP SAP

Giá trị của IPX Standard ACL từ 800 -> 899.

 Extended ACL từ 900 -> 999.

<condition>: Đây là điều kiện của ACL, đối với mỗi ACL khác nhau có các điều kiện khác nhau, các điều kiện này được quy định bởi người quản trị. Thông thường đây là thông tin về giao thức và địa chỉ.

Ví dụ : Router(config)# access-list 199 permit tcp any any eq www

Trong ví dụ trên là tạo một Extended ACL cho phép một truy cập bất kỳ vào dịch vụ www. Đây là Extended ACL vì *<Access List Number>* có giá trị là 199, và Permit là cho phép.

Các câu lệnh trong ACL sẽ được thực thi một cách tuần tự từ trên xuống dưới và từ trái sang phải.

Các gói tin khi đi qua Interface có cấu hình ACL thì nó sẽ bị phân tích và kiểm tra, nếu như Interface đó được cấu hình ACL với chiều inbound thì gói tin sẽ được kiểm tra trước khi định tuyến. Ngược lại nếu như Interface cấu hình là Outbound thì nó sẽ được định tuyến trước khi lọc. Trong trường hợp gói tin không thỏa điều kiện trong danh sách điều khiển truy nhập thì sẽ bị cấm.

2.1.1) Cấu trúc Standard Access List

Router(config)#access-list <access-list-number>{ deny | permit } <source [source-wildcard]>

Trong cấu trúc này *<access-list-number>* có giá trị nằm trong khoảng từ 1 đến 99.

<source [source-wildcard]> đây là địa chỉ của một mạng hay một máy , nơi sẽ gửi gói tin.

Ví dụ: Tạo một Standard ACL cấm mạng 192.168.2.0 truy nhập vào Router.

Router(config)# access-list 10 deny 192.168.2.0 0.0.0.255

Router(config)# access-list permit ip any

2.1.2) Cấu trúc Extended Access List

Router(config)#access-list<access-list-number>{ deny | permit }<protocol source [source-wildcard] ><source-qualifiers destination [destination-wildcard]><destination-qualifiers [log | log-input]>

Trong cấu trúc này chỉ khác Standard ACL ở các trường:

<protocol source [source-wildcard]> đây là tên hoặc là số của một giao thức, nó có thể là trong các từ sau: EIGRP, GRE, IGMP, IGRP, IP, IPINIP, OSPF, TCP hoặc UDP. Hoặc cũng có thể là một số integer nằm trong khoảng từ 0 đến 255, mô tả cho cổng của một giao thức IP.

<source-qualifiers destination [destination-wildcard]> tùy chọn này mô tả chi tiết hơn về thông tin của gói tin. Đây là tùy chọn có thể có hoặc không.

<destination-qualifiers [log | log-input]> đây là tùy chọn có hoặc không, tùy chọn này lưu lại các gói tin bị cấm.

Ví dụ: Tạo một Extended ACL cho phép các máy tính trong mạng 193.168.2.0 truy cập vào web của mạng 10.0.0.0.

```
Router(config)# access-list 150 permit tcp 192.168.2.0 0.0.0.255 10.0.0.0 0.0.0.255 eq 80.
```

```
Router(config)# access-list 110 deny tcp any any log.
```

Named ACL: Ngoài cách dùng số để cho IOS hiểu đó là loại ACL nào thì ta cũng có thể dùng thẳng tên ACL để biểu diễn cho loại ACL.

Ví dụ: Tạo một extended ACL với tên là webcam.

```
Router(config)# ip access-list extended webcam
```

```
Router(config-ext-nacl)#permit tcp 192.168.2.0 0.0.0.255 10.0.0.0 0.0.0.255 eq 80
```

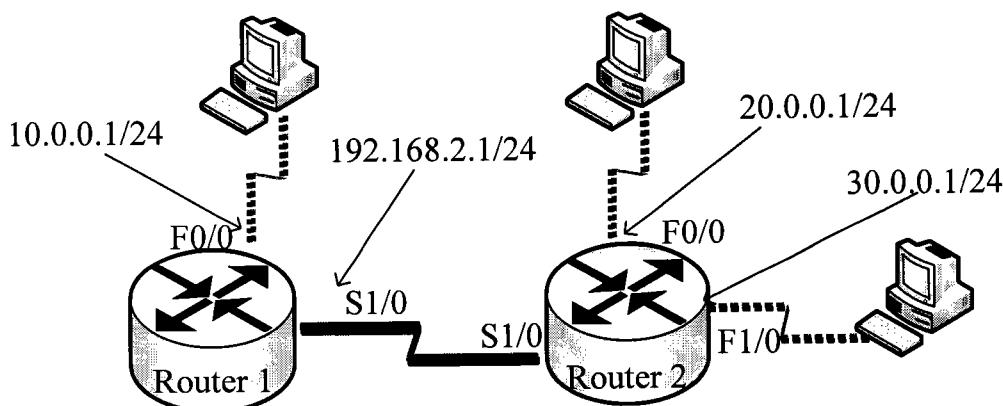
Trong trường hợp ta dùng tên để đặt cho ACL thì tên đó không được có khoảng trắng, không được có dấu chấm và ký tự đầu tiên phải được bắt đầu bằng chữ cái.

2.1.3) Cách gán cổng cho ACL

Sau khi tạo xong ACL, hay là tạo xong các quy tắc ra vào mạng thì sau đó phải gán ACL đó vào một interface nào đó của router. Theo quy tắc thì một ACL chỉ được gán một lần vào một interface theo một hướng nhất định là đi vào (inbound) hay đi ra (outbound). Tùy theo đặc điểm của từng hệ thống mạng mà người quản trị hệ thống sẽ

có những chính sách bảo mật khác nhau. Từ đó sẽ có những cách gắn ACL lên các interface khác nhau đối với mỗi hệ thống mạng.

Ví dụ: Gắn ACL cho hệ thống mạng như hình dưới, chỉ thiết lập ACL trên Router 1.



Hình 38. Mô hình dùng để gắn ACL cho Router 1.

- + Tạo ACL1 để cấm mạng 20.0.0.0 truy cập vào dịch vụ web của mạng 10.0.0.0, nếu có bất cứ gói tin nào yêu cầu truy cập dịch vụ web của mạng 10.0.0.0 mà có địa chỉ nguồn là 20.0.0.0 thì đánh rót tại cổng Serial 1/0 của Router 1.
- + Tạo ACL2 để cấm các máy trong mạng 10.0.0.0 truy cập đến mạng 30.0.0.0, nếu có bất cứ gói tin nào có địa chỉ nguồn là 10.0.0.0 và địa chỉ đích là 30.0.0.0 thì đánh rót tại cổng F0/0 của Router 1.

Lệnh cấu hình.

```
Router(config)# ip access-list extended ACL1
```

```
Router(config-ext-nacl)#deny tcp 20.0.0.0 0.0.0.255 10.0.0.0 0.0.0.255 eq 80
```

```
Router(config)# interface S1/0
```

```
Router(config)# ip access-group ACL1 in
```

```
!
```

```
Router(config)# ip access-list extended ACL2
```

```
Router(config-ext-nacl)#deny tcp 10.0.0.0 0.0.0.255 30.0.0.0 0.0.0.255 eq 80
```

```
Router(config)# interface F0/0
```

```
Router(config)# ip access-group ACL2 out
```

2.1.4) Cách xóa ACL

Để xóa một ACL ta chỉ việc thêm từ khóa **no** trước lệnh ACL là được.

Ví dụ: Muốn xóa ACL1 ta thực hiện như sau:

```
Router(config)# no ip access-list extended ACL1.
```

Để xem một ACL ta dùng lệnh *show access-list<access-list number || named>*

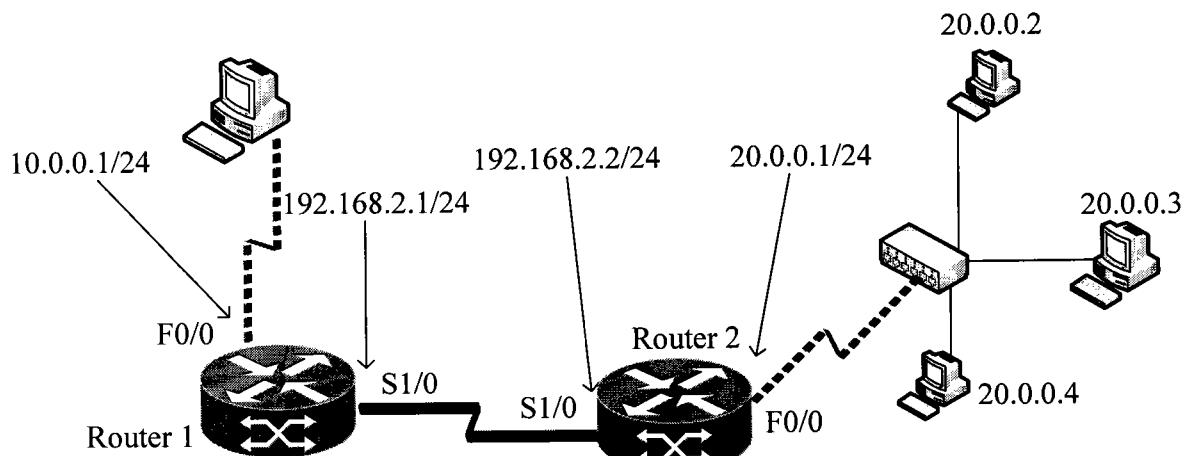
```
Router(config)# show ip access-list ACL1.
```

2.2) Thiết lập cấu hình cho Router cisco phòng ngừa một số kiểu tấn công DoS thường gặp.

2.2.1) Lọc lưu lượng một số dịch vụ.

Router cisco cung cấp một số lệnh cho phép cấu hình để chỉ cho phép một số host nhất định trong mạng được quyền telnet đến router, các host còn lại sẽ bị cấm nếu như không được quy định trong ACL.

Mô hình mạng.



hình 39. Mô hình dùng để lọc dữ liệu.

Ví dụ: cấu hình Router để chỉ cho phép host có ip là 20.0.0.2 và 20.0.0.4 có quyền telnet đến Router 1, các host còn lại bị cấm.

```
Router(config)# access-list 110 permit host 20.0.0.2 any eq 23
```

```
Router(config)# access-list 110 permit host 20.0.0.4 any eq 23
```

```
Router(config)# access-list 110 deny ip any any
```

```
Router(config)# line vty 0 4
```

```
Router(config)# access-class 101 in
```

Ngoài ra Cisco còn cung cấp các lệnh quy định về việc cho phép các host lấy thông tin định tuyến từ Router. Đó là dịch vụ SNMP, đây là công cụ quản lý mạng mà Router cung cấp để cho người quản trị có thể lấy các thông tin cần thiết về việc định tuyến của Router cũng như của hệ thống.

Để có thể lấy được thông tin định tuyến từ Router, hay lấy cấu hình của Router. Chỉ cần kích hoạt dịch vụ SNMP trên Router thông qua tập lệnh Access list. Cấu trúc lệnh SNMP như sau:

```
Router(config)# access-list 10 permit host 10.0.0.1.
```

```
Router(config)# snmp-server community net-management to 10.
```

2.3) Các chế độ bảo vệ của TCP intercept

Đặc trưng của TCP intercept là hỗ trợ cho việc chống lại các đợt tấn công từ chối dịch vụ theo kiểu SYN Flood, việc này được thực hiện bằng cách kiểm tra các yêu cầu thiết lập kết nối TCP từ đó có thể chặn những yêu cầu kết nối thuộc dạng tấn công và chấp nhận các yêu cầu kết nối hợp lệ. Trong tập lệnh TCP intercept bao gồm các chế độ ngăn chặn tấn công sau:

- + Ngăn chặn các gói TCP SYN được gửi tới Server từ các Client để kiểm tra, nếu các gói tin này phù hợp với danh sách truy nhập (access list), thì khi đó thì Router sẽ thiết lập kết nối đến Client với tư cách là đại diện của Server đích, nếu như quá trình thiết lập thành công thì khi đó Router sẽ chuyển kết nối này đến Server. Và từ lúc này kết nối TCP được thiết lập trực tiếp giữa Server và Client. Và theo cách này thì các kết nối

ảo hay nói cách khác là các kết nối mà địa chỉ IP là không thật sẽ không thể nào kết nối đến được với Server.

TCP intercept sẽ tiếp tục giám sát kể cả khi kết nối thành công và được chuyển đến cho Server thì quá trình giám sát vẫn tiếp tục trong suốt thời gian kết nối tồn tại.

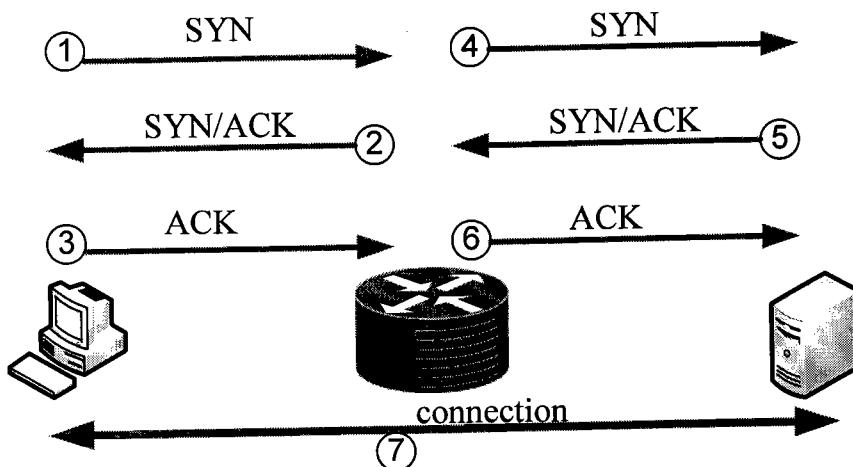
Trong trường hợp các yêu cầu là không hợp lệ, thì lúc này TCP Intercept sẽ linh hoạt ngắt kết nối tạm thời đó để bảo vệ server nhưng vẫn tiếp tục cho phép các yêu cầu kết nối hợp lệ.

Khi thiết lập các kết nối có sử dụng các chính sách bảo vệ TCP Intercept, thì có thể dùng nhiều chế độ bảo vệ như. Có thể chọn chế độ kiểm tra tất cả các yêu cầu thiết lập kết nối TCP hoặc là chỉ kiểm tra một vài yêu cầu thiết lập kết nối đến từ một số mạng đặc biệt hoặc là yêu cầu đến từ một số server đặc biệt. Ngoài ra còn có thể cấu hình cho số lượng kết nối và giới hạn của các kết nối đang tồn tại.

2.3.1) Intercept Mode.

Là chế độ mà khi một máy gửi yêu cầu thiết lập kết nối TCP đến server thì Router sẽ nhận gói tin SYN lại và đại diện cho Server để phản hồi lại yêu cầu kết nối đó. Vì Router đóng vai trò là đại diện của server nên nó sẽ thay cho server thiết lập kết nối đến máy yêu cầu.

Nếu máy nguồn yêu cầu thiết lập kết nối gửi trả lại cho Router gói ACK thì khi này chứng tỏ đây không phải là người tấn công, và lúc này Router sẽ thiết lập kết nối như bình thường. Khi hoàn tất quá trình kết nối với máy Client, Router sẽ thiết lập một kết nối khác đến server và sau đó nối 2 kết nối này với nhau. Trong suốt quá trình thiết lập kết nối TCP, router trong suốt với cả Client và Server. Vì vậy trong Trường hợp ngược lại, nếu Router không nhận được ACK phản hồi từ client thì Router sẽ loại bỏ gói tin.



Hình 40. Hình ảnh Router đại diện cho server thiết lập kết nối TCP.

Với cách tiếp cận này nếu có tấn công TCP SYN xảy ra, router sẽ cung cấp 1 vùng đệm cho server, server sẽ không bị ảnh hưởng gì bởi flood. router bắt tay với các half-open connections, và sau khoảng thời gian timeout router sẽ xoá tất cả các kết nối này ra khỏi bảng TCP connection table của nó. Trên thực tế thì những request hợp lệ sẽ được cho phép kết nối tới router bên trong ngay sau khi hoàn thành tiến trình bắt tay 3 bước với router.

2.3.2) Watch Mode

Đây là chế độ được thiết lập để khi Client gửi yêu cầu thiết lập kết nối SYN đến Server

thì router sẽ chuyển gói tin này đến server, và đồng thời Router sẽ tiếp tục theo dõi kết nối

này cho đến khi kết nối này được thiết lập.

Nếu trong một khoảng thời gian quy định mà kết nối không hoàn tất quá trình bắt tay thì Router sẽ gửi một gói tin yêu cầu Reset đến Server để xóa trạng thái kết nối.

Nếu máy nguồn không trả lời lại mà đồng thời có nhiều kết nối mở giống như vậy nữa, thì router biết là máy bên trong đang bị tấn công DoS theo kiểu SYN Flood và nó sẽ chặn ngay các gói tin tiếp theo.

2.4) Cấu hình TCP intercept

+ Cấu trúc lệnh intercept(*enable intercept*)

Router(config)#**ip tcp intercept list <access-list-number>**

Ví dụ: Lệnh sau dùng để bật chế độ TCP Intercept cho phép bắt kỳ gói tin tcp nào đến Web Server có địa chỉ 192.168.1.0/24

Router(config)# ip access-list extended ACL1

Router(config)# permit tcp any 192.168.1.0 0.0.0.255 eq 80

Router(config)#ip tcp intercept list ACL1

Intercept mode là chế độ chủ động, vì vậy khi các gói tin đến từ các mạng bên ngoài muốn kết nối với server thì Router sẽ chủ động chặn các gói tin này lại để kiểm tra và thiết lập kết nối sau khi thành công thì mới forward kết nối này đến server.

+*Thiết lập chế độ Random-Drop.*

Đây là chế độ làm giảm lưu lượng các gói tin đi qua mạng khi có sự tăng lưu lượng đột ngột hay số lượng kết nối vượt mức giới hạn. Theo mặc định nếu số lượng kết nối không hoàn thành quá trình bắt tay vượt quá 1100 hay số lượng kết nối đến mạng trong vòng một phút cuối vượt quá 1100 thì TCP intercept sẽ linh hoạt xử lý để bảo vệ trạng thái cân bằng của mạng. Cách xử lý của router lúc này là khi có một kết nối mới đến thì kết nối cũ nhất sẽ bị xóa khỏi mạng, đồng thời chế độ intercept sẽ giảm thời gian *timeout* đi một nữa, vì vậy thời gian thiết lập kết nối chỉ còn 1/2.

Cấu trúc lệnh thiết lập chế độ Random-Drop.

Router(config) # **ip tcp intercept drop-mode { oldest | random }**

Ngoài ra ta có thể thiết lập các giá trị trong TCP intercept như:

+ *Thay đổi thời gian Times-out* để quy định thời gian hủy một kết nối khi không hoàn tất.

Mục tiêu: Cấu hình Router để chặn tất cả và kiểm tra các kết nối TCP đến Web Server.

Các bước cấu hình TCP intercept cho Router. Trong lệnh dưới, nếu sau 160 giây mà client và server không hoàn tất kết nối thì kết nối sẽ bị hủy.

Router(config)# ip tcp intercept connection-timeout 160 .

+ Thiết lập giới hạn kết nối để báo động khi số lượng kết nối không hoàn thành vượt mức. Trong lệnh dưới intercept sẽ báo động nếu số lượng kết nối không hoàn thành vượt quá 200, và ngừng báo động khi số lượng kết nối không hoàn thành giảm xuống còn 120.

Router(config)#ip tcp intercept max-incomplete high 200.

Router(config)#ip tcp intercept max-incomplete low 120

2.4.1) Cấu hình TCP intercept (Intercept Mode) phòng chống tấn công DoS

- + Tạo ACL 199 để so sánh (match) các kết nối TCP đến Port 80.
- + Cấu hình TCP intercept dùng ACL 199 và mode Random – drop.
- + Báo động khi số kết nối Half-Open Sessions lên đến 200
- + Dừng báo động khi số kết nối Half-Open Sessions giảm xuống còn 120
- + Set thời gian time out đến các kết nối inactive là 160 giây

+ Tạo ACL và cấu hình Intercept.

Router_1(config-if)#access-list 199 permit tcp any any eq 80

Router_1(config-if)#ip tcp intercept drop-mode random

Router_1(config-if)#ip tcp intercept list 199 ! Cho phép chế độ TCP Intercept áp dụng cho Extended ACL 199

Router_1(config-if)#ip tcp intercept connection-timeout 160 !Sau 160s giữa client và server không trao đổi, thì kết nối sẽ bị hủy

Router_1(config-if)#ip tcp intercept max-incomplete low 120

Router_1(config-if)#ip tcp intercept max-incomplete high 200

Router_1(config-if)#ip tcp intercept one-minute low 350

Router_1(config-if)#ip tcp intercept one-minute high 550

!

Kiểm tra

Router_1# debug ip tcp intercept

2.4.2) Cấu hình TCP intercept (Watch Mode) phòng chống tấn công DoS.

Mục tiêu: cấu hình để Router giám sát các kết nối TCP phòng chống tấn công DoS.

Các bước cấu hình TCP intercept cho Router.

- + Tạo ACL 199 để so sánh (match) các kết nối TCP đến Port 80.
- + Router sẽ Reset các kết nối nếu chúng ở trạng thái Half-open hơn 15 giây.
- + Bắt đầu Resetting Half-Open Sessions khi số Session lên đến 200.
- + Dừng Resetting Half-Open Sessions khi số Session giảm xuống còn 120

+ *Tạo ACL và cấu hình watch mode.*

Router_1(config-if)#access-list 199 permit tcp any any eq 80

Router_1(config-if)#ip tcp intercept list 199

Router_1(config-if)# ip tcp intercept mode watch

Router_1(config-if)# ip tcp intercept watch-timeout 15

Router_1(config-if)# ip tcp intercept max-incomplex high 200

Router_1(config-if)# ip tcp intercept max-incomplex low 120

Router_1(config-if)# ip tcp intercept connection-timeout 160

Router_1(config-if)#ip tcp intercept drop-mode random

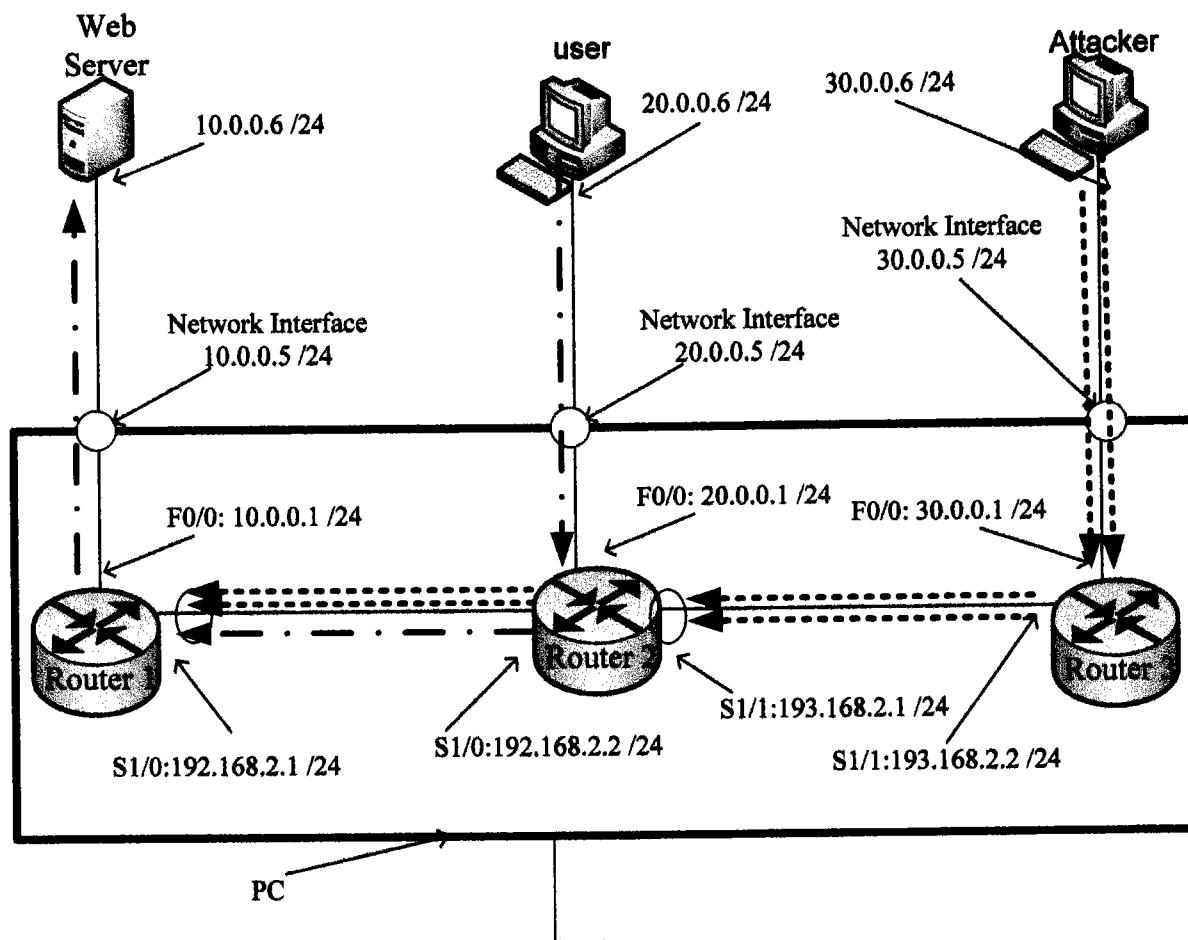
!

Kiểm tra

Router_1# debug ip tcp intercept.

III) Cấu Hình TCP Intercept Ở Chế Độ Watch Mode cho mô hình thực nghiệm.

Mục tiêu: Hạn chế sự tác động của cuộc tấn công DoS vào hệ thống khi được bảo vệ bởi TCP intercept. Sau khi cấu hình intercept thì máy tính đóng vai trò Attacker sẽ tấn công máy Webser và máy tính còn lại vẫn có thể truy cập web khi server đang bị tấn công.



Hình 41. Hình ảnh luồng dữ liệu tấn công và luồng dữ liệu hợp lệ.

Dựa trên cuộc tấn công của Attacker là công cụ tấn công dạng SYN Flood, vì vậy cấu hình TCP Intercept cho Router 1 để chống lại các đợt tấn công DoS.

+ Đầu tiên là cấu hình access list cho máy webserver. Cho phép bất kỳ máy nào cũng có thể truy cập dịch vụ web tại host 10.0.0.6.

Router> enable

Router# config terminal

Router(config)# hostname Router_1

Router_1(config)# access-list 150 permit tcp any host 10.0.0.6 eq www

+ Kích hoạt và cấu hình TCP intercept trên Router 1, Cho phép chế độ TCP intercept áp dụng cho access list 150.

Router_1(config)#ip tcp intercept list 150

+ Cấu hình intercept ở chế độ Watch mode

Router_1(config)# ip tcp intercept mode watch

+ Thiết lập thời gian timeout, nếu client và server không hoàn tất kết nối trong 240 giây thì hủy kết nối.

Router_1(config)# ip tcp intercept connection-timeout 60

+ Cấu hình giới hạn kết nối không hoàn tất, nếu số lượng kết nối không hoàn tất lên đến 200 thì báo động. Và tắt chế độ báo động khi số lượng kết nối giảm xuống còn 120.

Router_1(config)# ip tcp intercept max-incomplex high 15

Router_1(config)# ip tcp intercept max-incomplex low 100

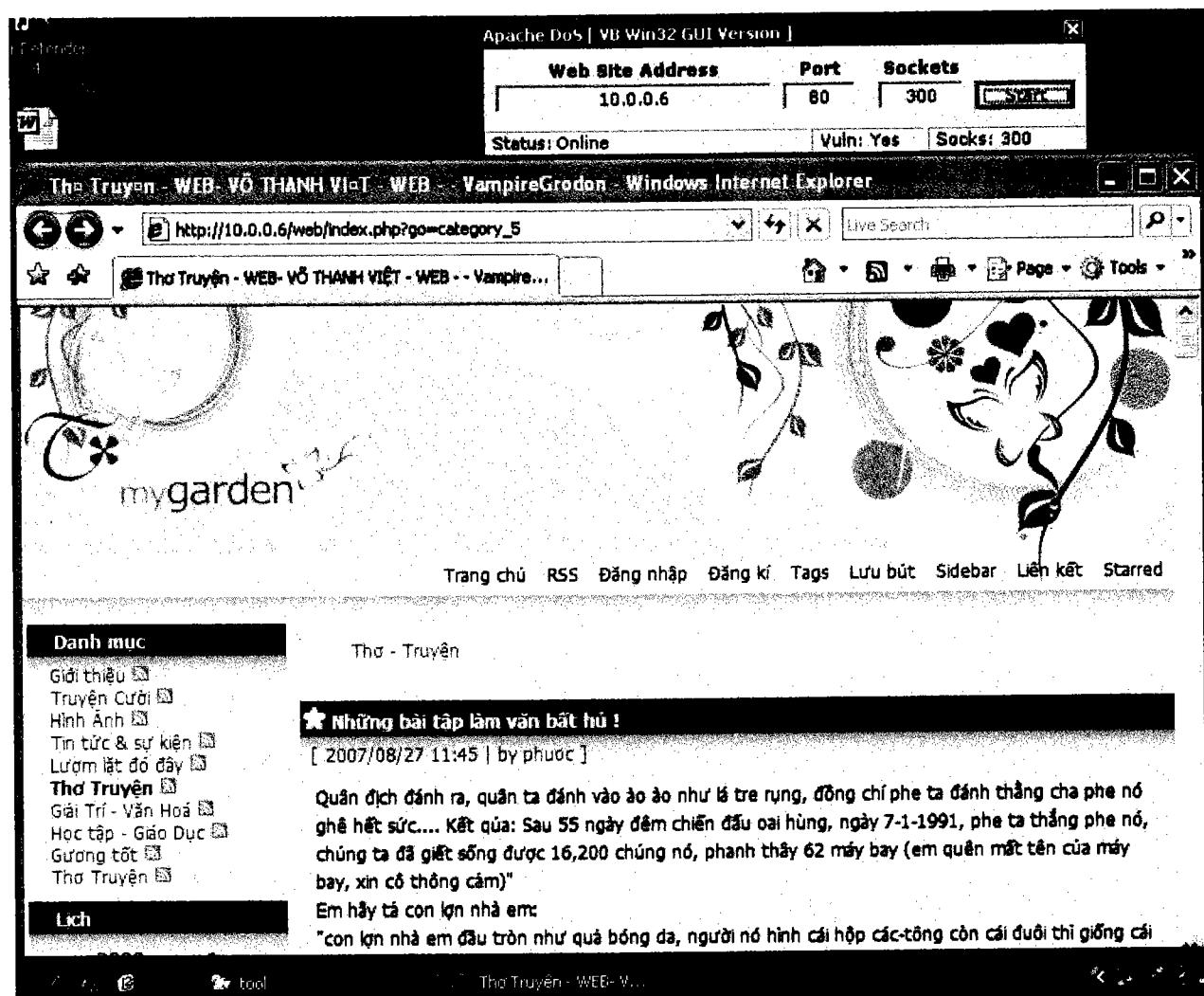
+ Cấu hình giới hạn kết nối. Báo động nếu trong một phút cuối mà có số lượng kết vượt quá 350, ngừng báo động khi số lượng giảm xuống 200.

Router_1(config)# ip tcp intercept one-minute low 170

Router_1(config)# ip tcp intercept one-minute high 160

Sau khi cấu hình TCP Intercept cho Router R1 xong. Tiếp theo dùng công cụ Apache DoS tại máy tính Attacker để tấn công webserver và máy tính đóng vai trò User vẫn có thể truy cập web khi cuộc tấn công đang diễn ra.

Kết quả là khi ta chạy hết số lượng socket là 1500 nhưng webserver vẫn không bị down (khi không cấu hình cho Router thì server thường bị Down khi chạy khoảng 270 socket), vì khi các gói tin yêu cầu thiết lập kết nối đến từ máy tính của Attacker khi qua Router đã bị lọc bỏ những gói bị nghi ngờ là tấn công.



Hình 42. Khi webserver bị tấn công và người dùng vẫn hoạt động bình thường.

Chương 5.

Phát hiện tấn công DoS cùng với NetFlow.

Hệ thống mạng đang ngày càng trở nên thành phần không thể thiếu và góp phần rất lớn vào sự thành công của doanh nghiệp, dù là một doanh nghiệp lớn hay nhỏ. Vì vậy khi hệ thống mạng không hoạt động một cách trơn tru, bị lỗi hay phức tạp hơn là hệ thống mạng đang phải gánh chịu những đợt tấn công phá hoại từ internet thì sẽ gây nên những tổn thất cho doanh nghiệp.

Vào một ngày bình thường khi mở máy lên. Khách hàng và nhân viên không thể trao đổi với nhau, nhân viên không thể truy cập được các thông tin cần thiết, hay không dùng được email hay các dịch vụ in ấn. Tất cả sẽ làm cho doanh thu bị giảm sút.

Với tư cách là người quản trị hệ thống, việc phát hiện sớm các cuộc tấn công và có biện pháp ngăn ngừa cụ thể cho hệ thống của mình là một điều cần thiết. Hiện tại có rất nhiều phần mềm giám sát hệ thống, có thể giúp người quản trị theo dõi và phân tích hệ thống một cách chi tiết và liên tục để theo dõi hệ thống của mình. Nhằm có những biện pháp cụ thể đối với từng trường hợp khi hệ thống xảy ra sự cố một cách kịp thời.

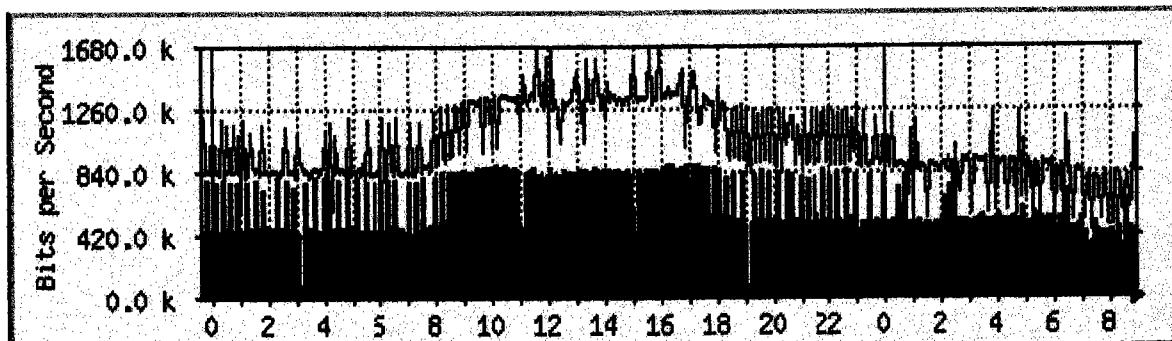
Các phần mềm giám sát và phân tích mạng hiện tại có thể giám sát: **Hệ thống máy chủ và dịch vụ, các bản ghi máy chủ (File Log), các trình ứng dụng, dữ liệu và website, hệ thống Mail và kết nối Wan.**

5.1) Nagios

Đây là phần mềm giám sát mạng mã nguồn mở, phần mềm này được thiết kế chạy trên nền Linux, Nagios là một màn hình dịch vụ và máy chủ được thiết kế nhằm thông báo tới người quản trị hệ thống các vấn đề về mạng một cách sớm nhất khi xảy ra sự cố. Trình tiện ích giám sát chạy liên tục trên máy chủ và các dịch vụ mà người quản trị có thể thiết lập trên plugins, khi hệ thống gặp vấn đề thì trình giám sát sẽ gửi các thông báo tới người quản trị hệ thống theo nhiều cách như: email, instant message, sms,... thông tin về trạng thái hiện tại, lịch sử truy nhập, các báo cáo có thể được truy nhập qua trình duyệt Web.

5.2) MRTG: Phần mềm giám sát luồng chuyển động

Multi Router Traffic Grapher (MRTG) là một công cụ để giám sát luồng chuyển động nạp vào trên các liên kết mạng. MRTG tạo các trang HTML mang các hình ảnh PNG, đưa ra sự thể hiện sống động, trực giác về luồng chuyển động này như sau:

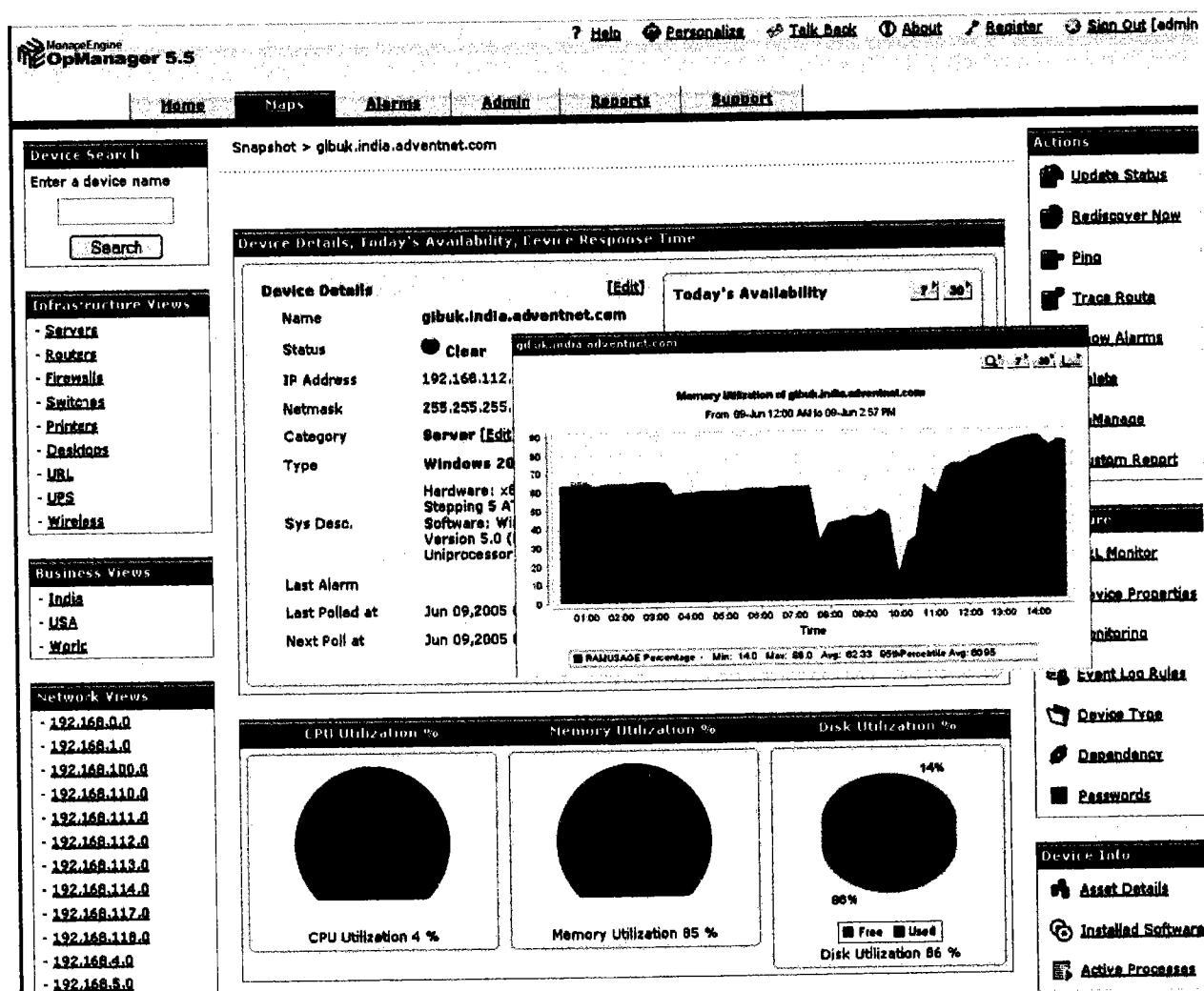


Hình 42.biểu đồ phân tích luồng dữ liệu bằng MRTG

5.3) ManageEngine Opmanager

OpManager là một phần mềm giám sát mạng phổ biến được hàng ngàn các nhà quản trị thông tin trên toàn thế giới sử dụng. Sử dụng phiên bản OpManager miễn phí, bạn có thể giám sát **20 thiết bị quan trọng nhất** như: Các Router, các máy chủ, Switch, các máy chủ email, hệ thống tường lửa, máy in, vv... OpManager giám sát các thiết bị này một cách tích cực đảm bảo tính sẵn sàng, trạng thái và cảnh báo nhanh chóng bằng email hoặc SMS, khi phát hiện ra một vấn đề. OpManager cũng tạo ra các báo cáo và biểu đồ để phân tích hiệu suất của thiết bị trong từng giai đoạn.

Giao diện phần mềm:



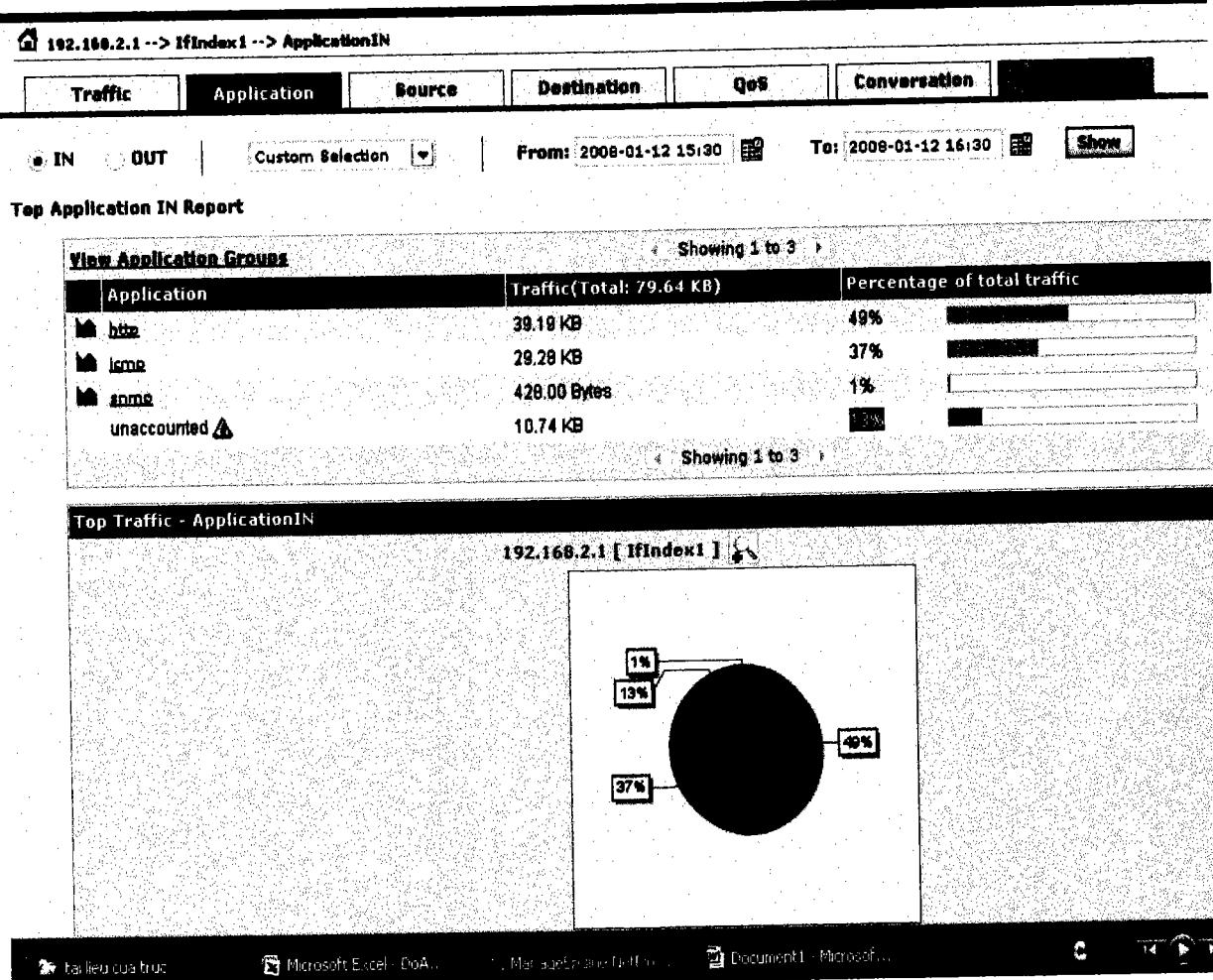
Hình 43. Hình ảnh của ManageEngine Opmanager.

5.4) NetFlow Analyzer

NetFlow là phần mềm theo dõi và phân tích hệ thống dựa vào dịch vụ SNMP, nhà quản trị hệ thống có thể dùng NetFlow để theo dõi và ghi nhận các thay đổi trên hệ thống mạng từ đó có thể đưa ra những kết luận chính xác cho trạng thái hiện tại của hệ thống.

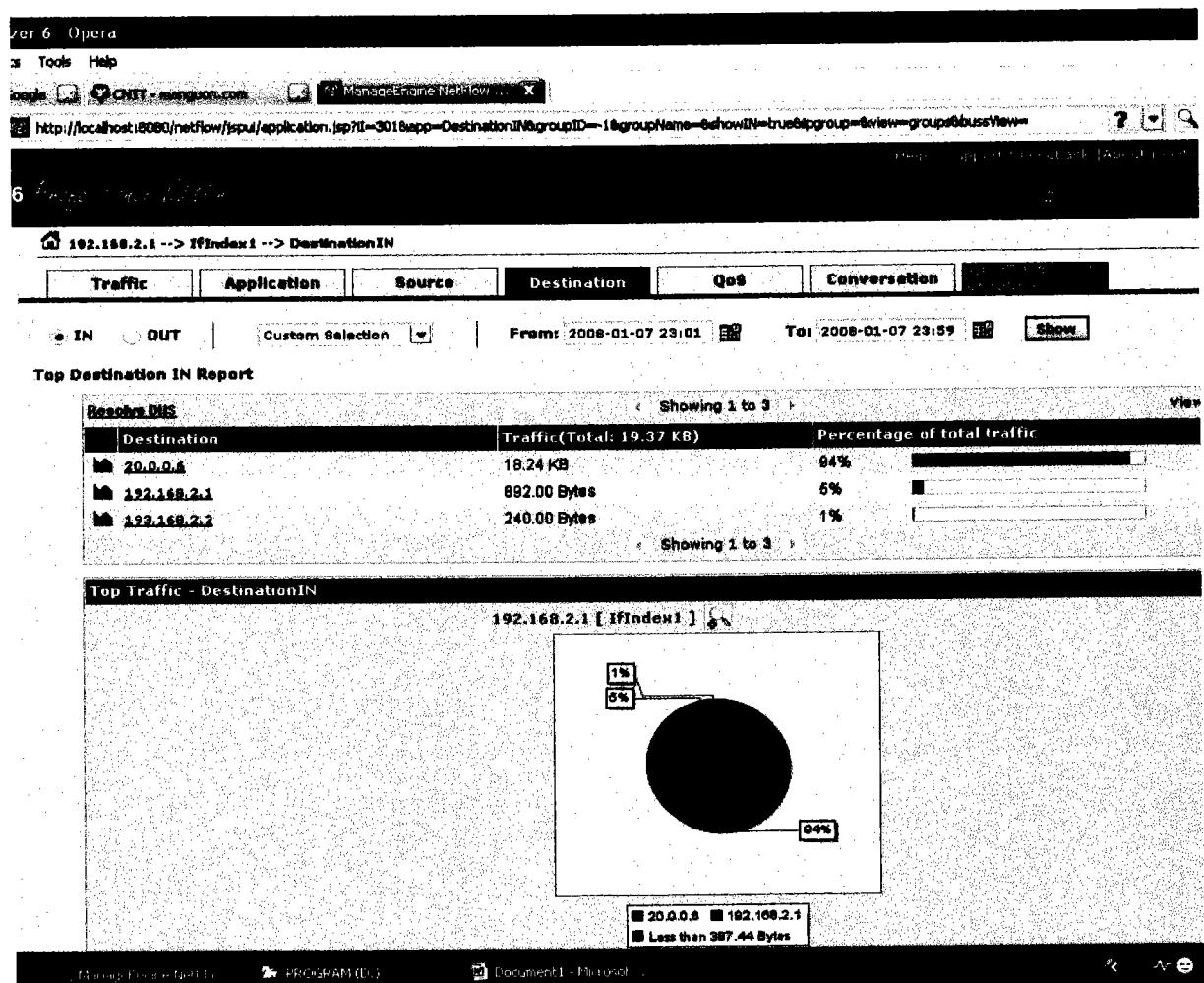
NetFlow có thể xác định được các ứng dụng nào đang chạy trên hệ thống và chiếm bao nhiêu phần trăm băng thông. Trong ví dụ bên dưới có 4 ứng dụng đang chạy là ICMP chiếm 37%, SNMP chiếm 1% , HTTP chiếm 49% và 13% còn lại dùng cho các ứng dụng khác của hệ thống.

Đây là hình ảnh khi hệ thống hoạt động bình thường, các người dùng truy nhập web và ping qua lại với nhau.



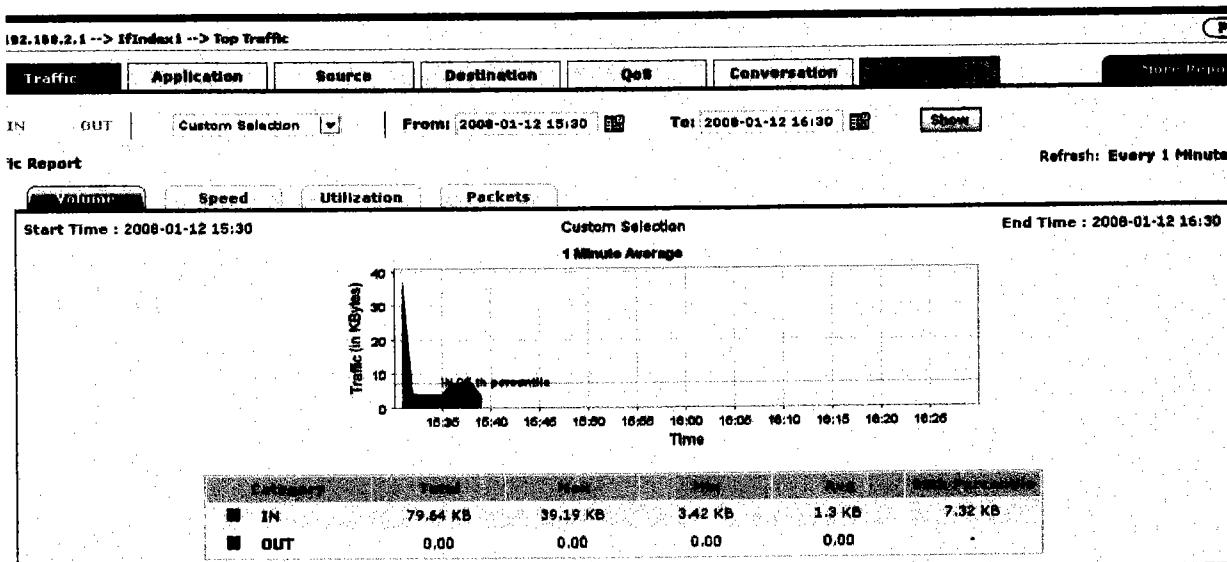
Hình 44. Hình ảnh các ứng dụng đang chạy trên hệ thống.

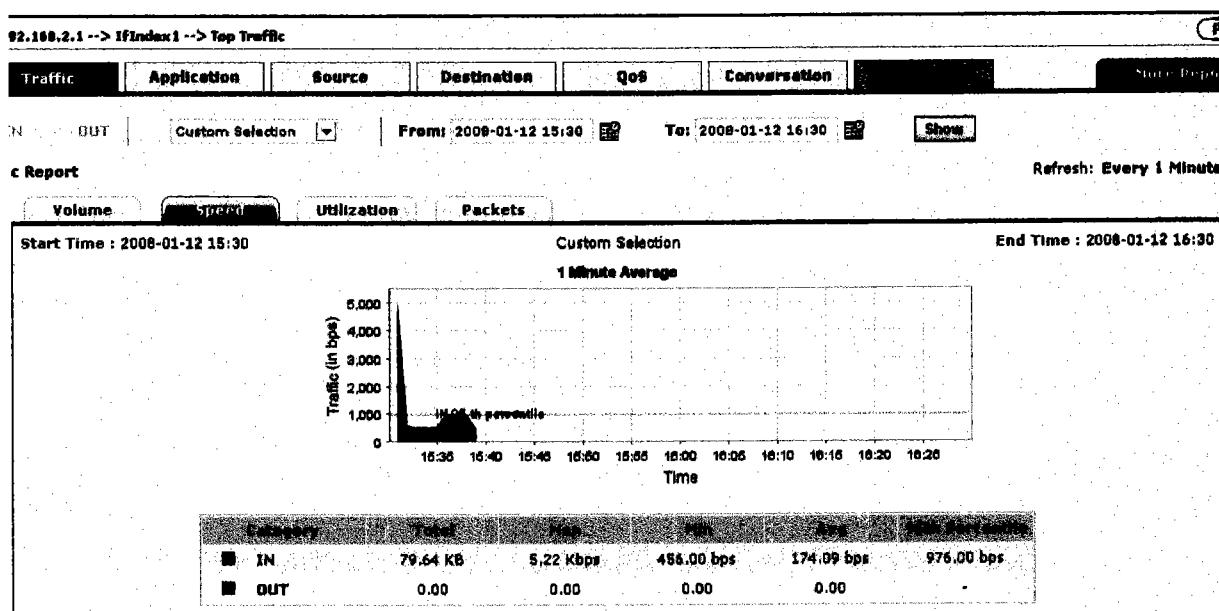
Ngoài ra NetFlow còn cung cấp cho nhà quản trị biết các dịch vụ chạy trên hệ thống được xuất phát từ đâu. Vì vậy nếu khi hệ thống nhận quá nhiều yêu cầu từ một Host thì có thể ngăn chặn hoặc loại bỏ truy cập để tránh khỏi sự tấn công vào hệ thống.



Hình 45. Host 20.0.0.6 chiếm 94% lưu lượng trên hệ thống.

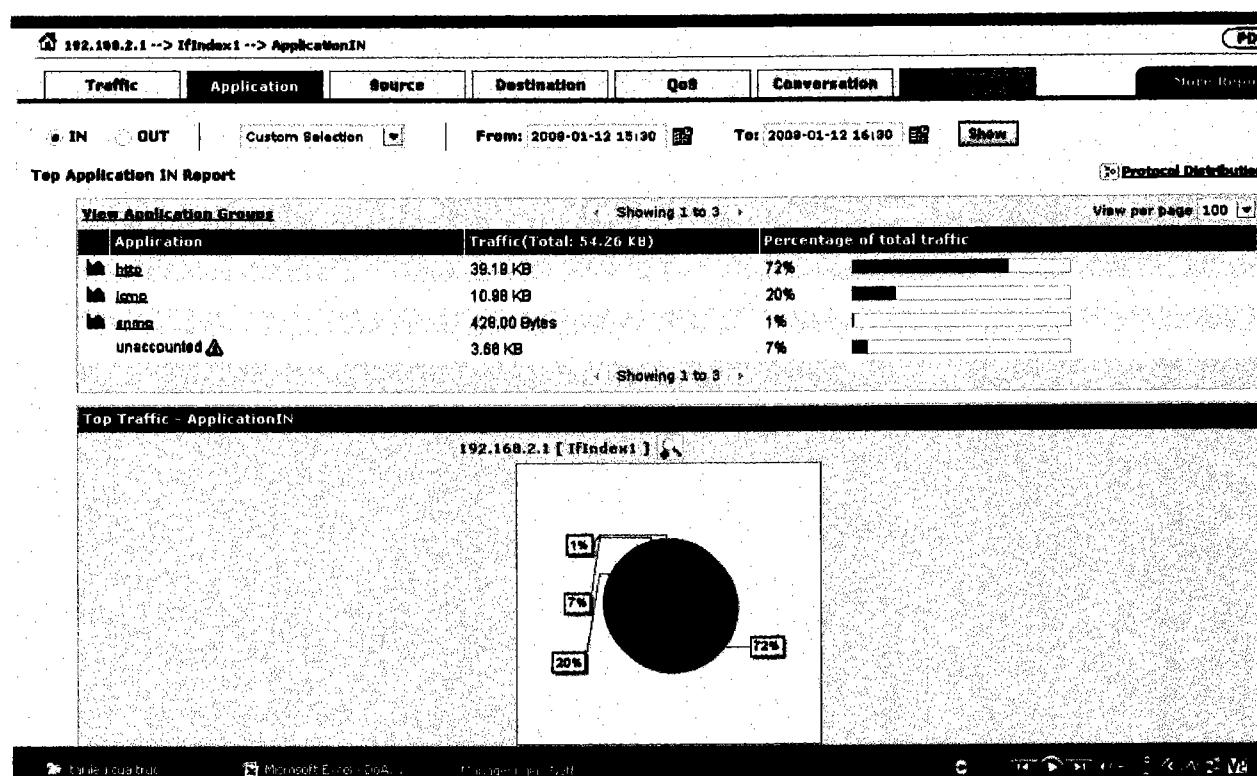
NetFlow cung cấp cho nhà quản trị biểu đồ về lưu lượng trên hệ thống. trong trường hợp hệ thống hoạt động bình thường ta có biểu đồ bên dưới.



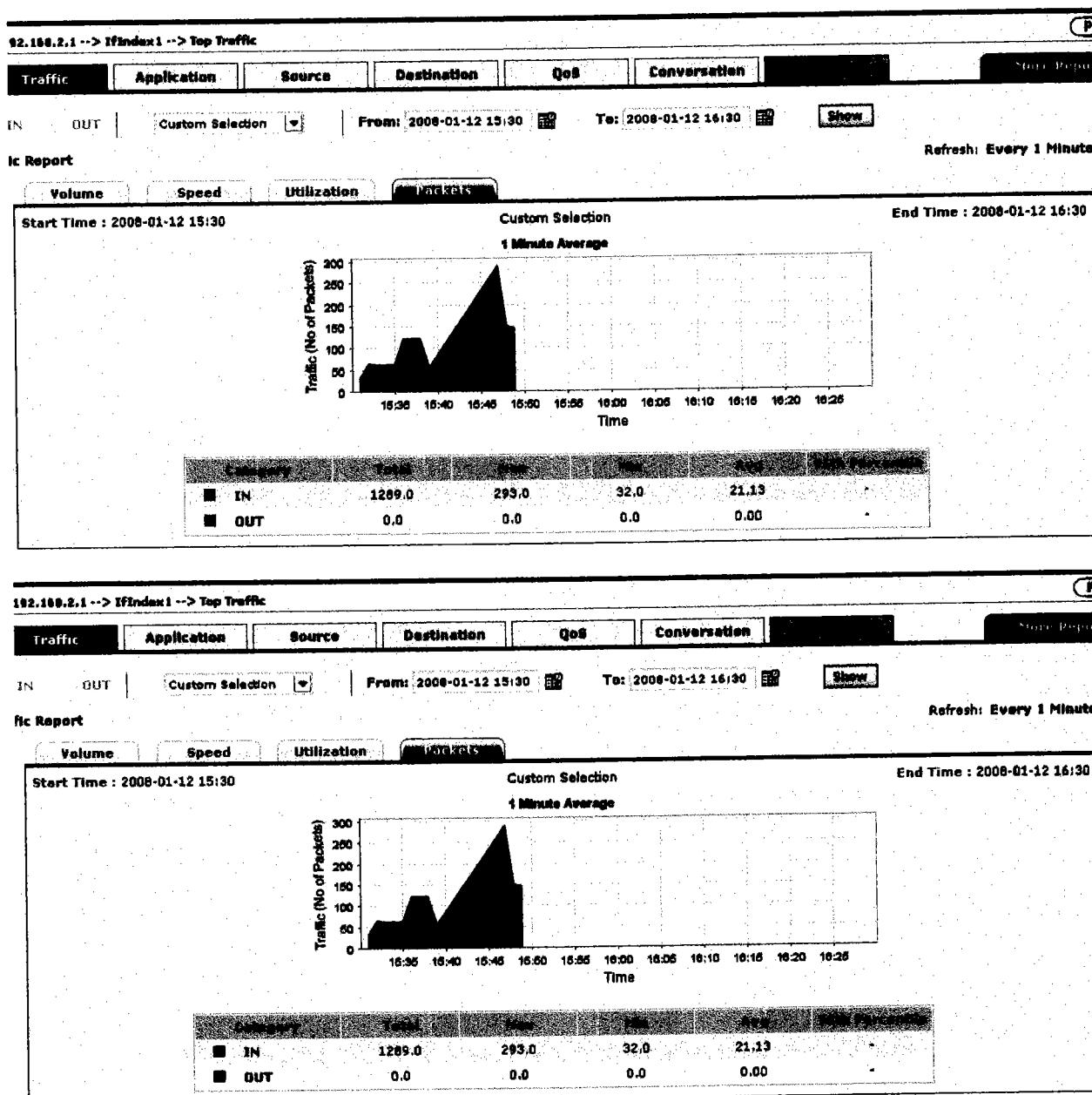


Hình 46. Biểu đồ về lưu lượng trên hệ thống.

Hình ảnh các ứng dụng và đường truyền trên mạng khi hệ thống bị tấn công DoS.



Hình 47. Các ứng dụng chạy trên hệ thống khi bị tấn công.



Hình 48. Số lượng các gói tin trên đường truyền tăng lên đột biến khi hệ thống bị tấn công.

Kết luận: Với NetFlow nhà quản trị hệ thống sẽ có những nǎm bắt kịp thời về trạng thái hệ thống của mình sớm nhất và có những biện pháp thích hợp nhất để hệ thống có thể hoạt động ổn định hơn và có thể tránh được các sự cố đáng tiếc.

Chương 6.

Tổng Kết Những Điều Đạt Được Và Chưa Đạt Được Trong Luận Văn

6.1) Những điều đạt được

Xây dựng và quản trị hệ thống mạng windows. Nắm vững các kỹ thuật tấn công DoS, cách thực hiện và phòng chống cho từng kiểu tấn công.

Dùng công cụ tấn công DoS kiểu SynFlood để hiện thực quá trình tấn công DoS trên mô hình thử nghiệm và cấu hình TCP Intercept để phòng chống thành công cho Website.

Xây dựng thành công mô hình phòng chống tấn công DoS có thể áp dụng vào thực tế cho bất kỳ hệ thống mạng nào.

Xây dựng thành công hệ thống nhận dạng cuộc tấn công DoS bằng Netflow.

6.2) Những điều chưa đạt được

Trong quá trình thực hiện luận văn em đã gặp một số khó khăn sau:

Vì không đủ kinh phí để thực hiện trên mô hình thật nên em thực hiện chạy giả lập chương trình bằng phần mềm Dynamic.

Do em xây dựng hệ thống phòng chống tấn công bằng phần mềm nên chưa đạt hiệu suất tối ưu cho hệ thống mạng, vì Intercept chưa nhận biết được đâu là luồng dữ liệu thật và luồng dữ liệu tấn công, nên khi cuộc tấn công xảy ra thì Intercept hạn chế lưu lượng qua Router. Điều này dẫn đến có một số kết nối hợp lệ bị từ chối khi phòng chống tấn công DoS bằng TCP Intercept.

Thời gian thực hiện luận văn có hạn nên em chưa nghiên cứu các kỹ thuật tấn công còn lại để đưa ra những biện pháp phòng chống cụ thể cho từng kiểu tấn công mà em chỉ tập trung nghiên cứu kiểu tấn công SynFlood.

6.3) Hướng phát triển

Trong tương lai, do sự phức tạp trong các kỹ thuật tấn công có sự khác nhau nên có thể phát triển đề tài bằng cách nghiên cứu bổ sung và xây dựng các hệ thống nhận biết tấn công, hệ thống phát hiện xâm nhập để bảo vệ hệ thống tốt hơn.

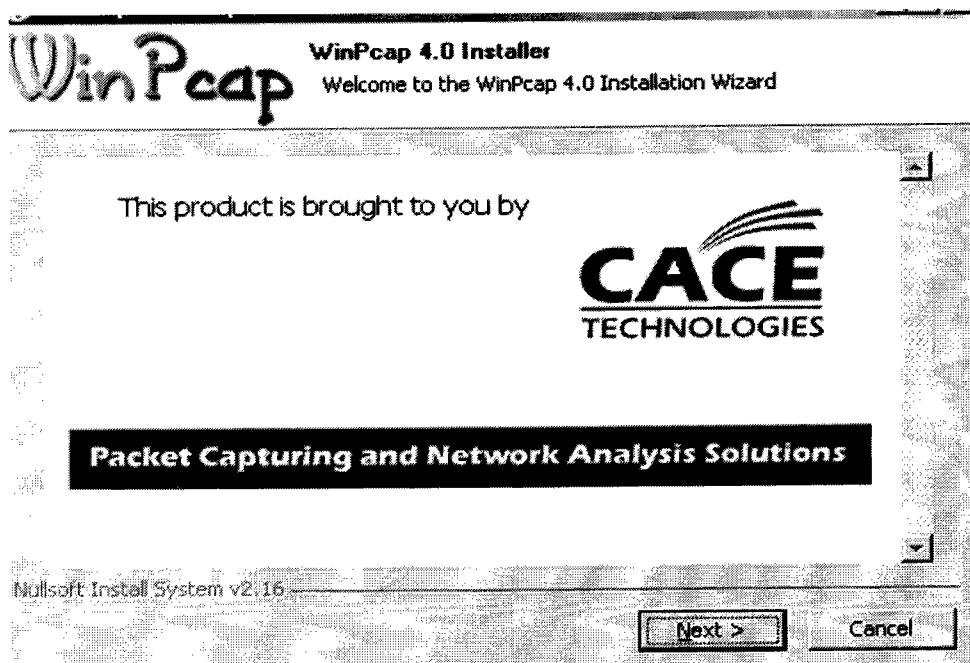
Có thể phát triển luận văn trên Server Linux thay cho Server Windows và nghiên cứu về tấn công DoS và xây dựng hệ thống phòng chống tấn công DoS trên nền IPv6 thay cho IPv4 trong luận văn.

Phụ lục.

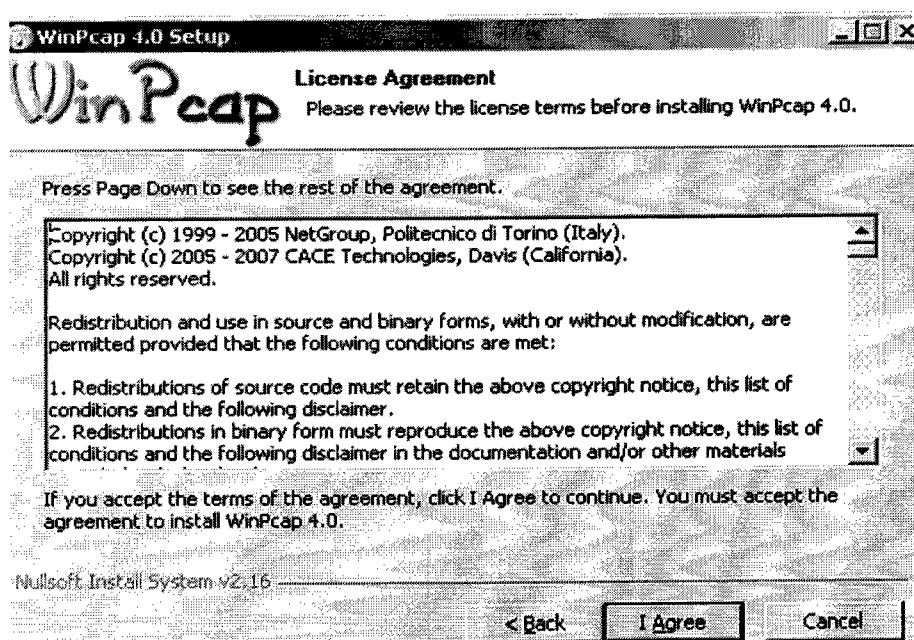
1) *Cấu hình cho Router để các mạng có thể thông nhau.*

1.1) *Cài đặt WinPcap 4.0.*

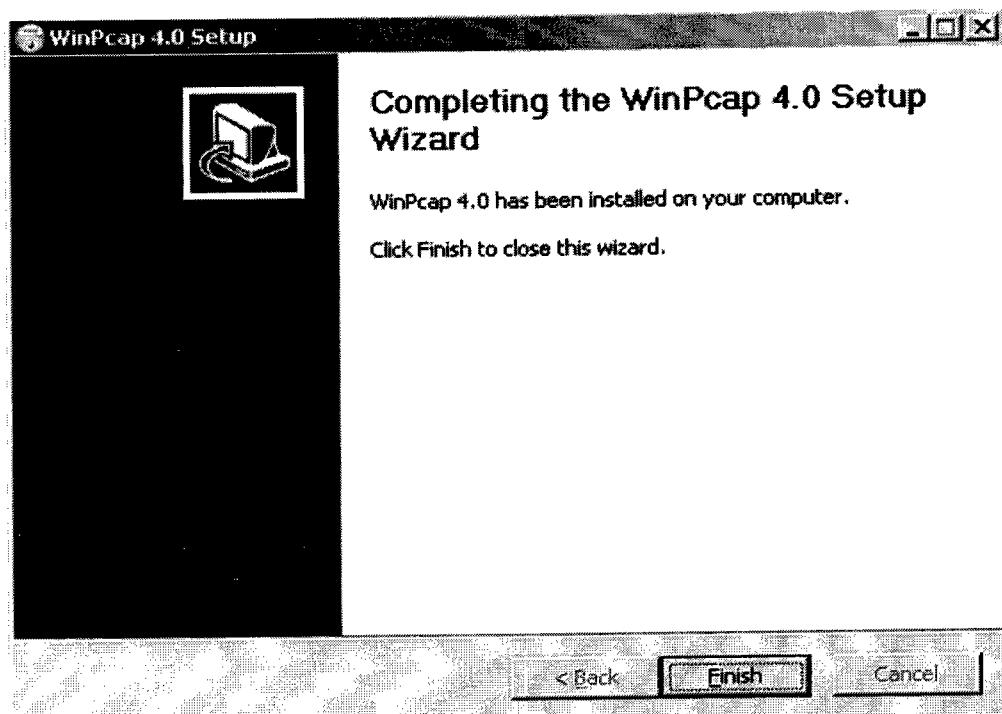
Để tiến hành quá trình cài đặt, click vào file WinPcap.exe và chọn Next như hình bên dưới.



Cửa sổ tiếp theo hiện ra, chọn I Agree và chọn next để tiến hành quá trình cài đặt.

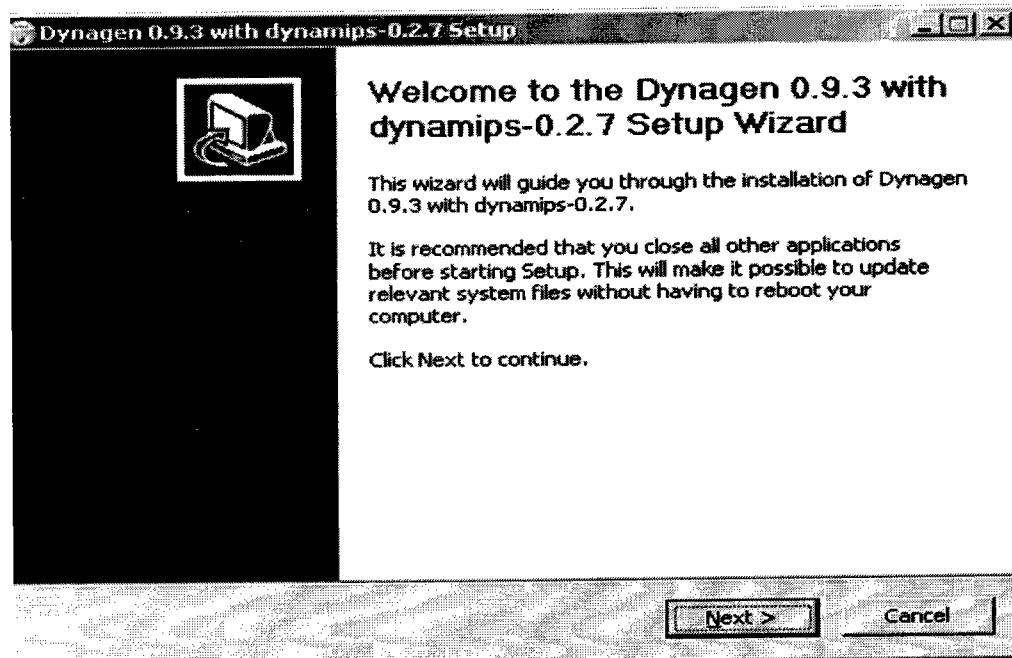


Cuối cùng chọn finish để hoàn thành quá trình cài đặt WinPcap lên máy.

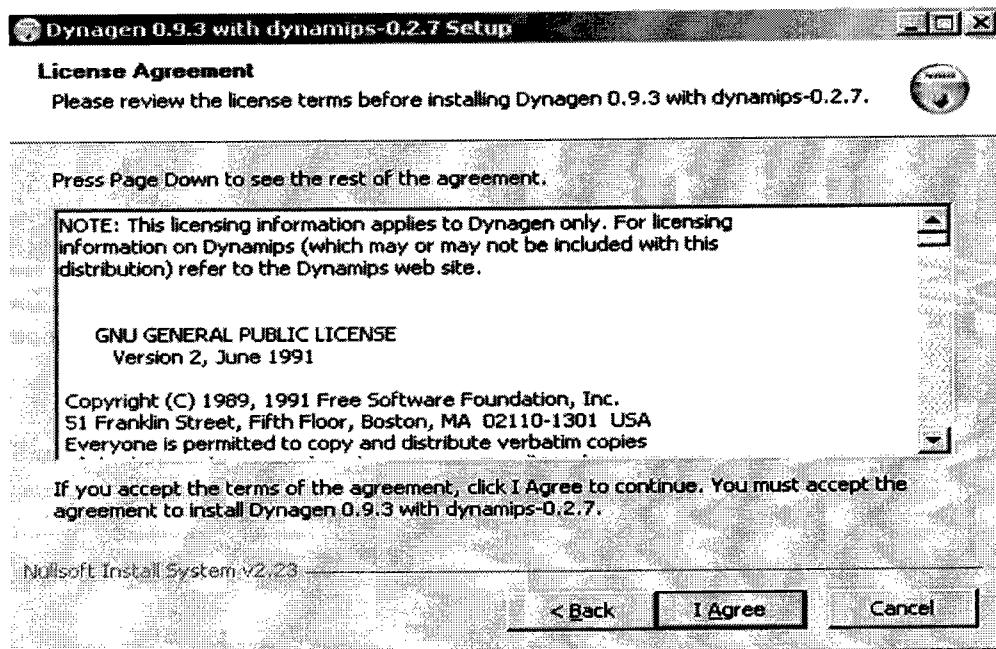


1.2) Tiến hành cài đặt Dynamic (Dynagen).

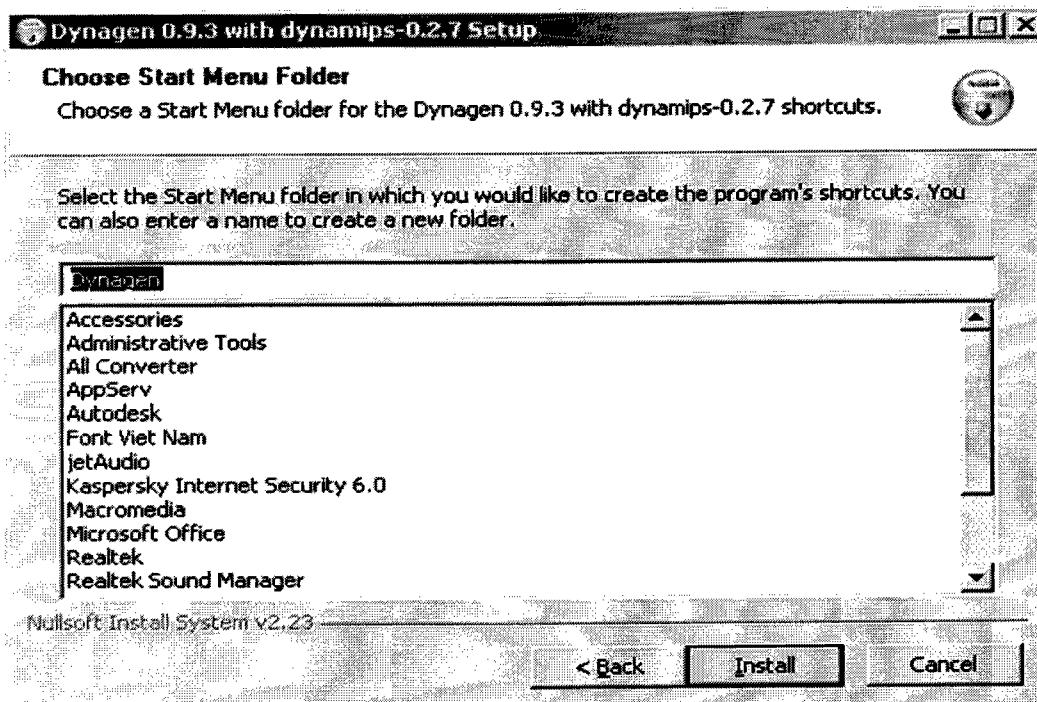
Để tiến hành quá trình cài đặt, click vào file Dynagen.exe và chọn Next khi cửa sổ Dynamips setup wizard hiện ra như hình bên dưới.



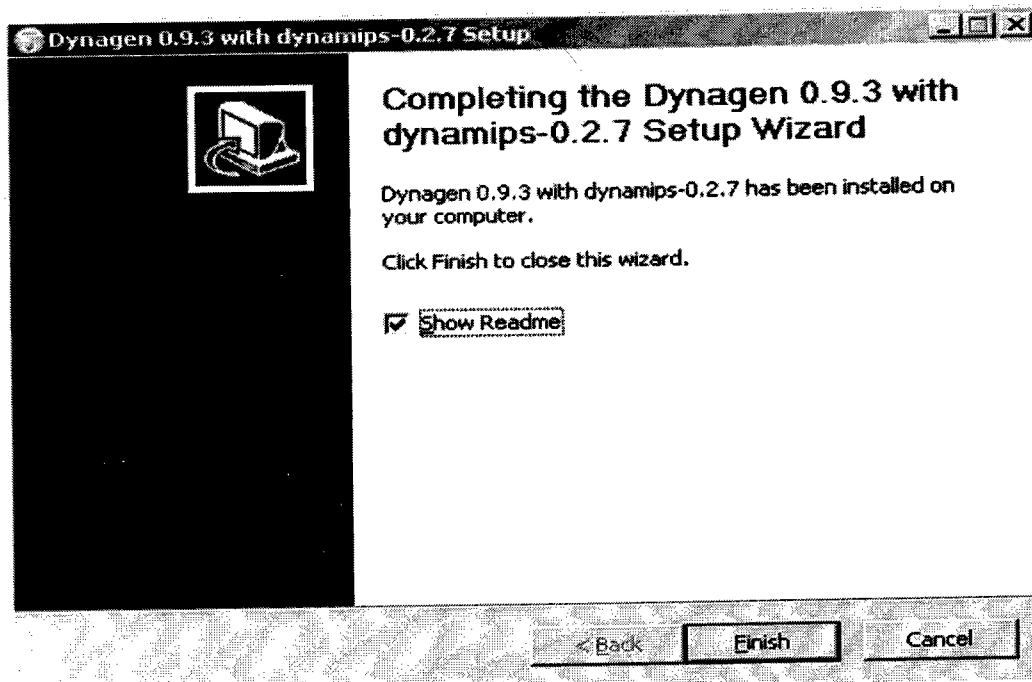
Cửa sổ tiếp theo hiện ra, chọn I Agree



Tiếp theo chọn install để bắt đầu quá trình cài đặt Dynagen lên máy.



Chờ đợi giây lát và chọn finish để hoàn thành quá trình cài đặt.



1.3) Tạo file StartingRouter.net

để Dynagen có thể chạy được thì cần thiết phải tạo ra file *StartingRouter.net*, nội dung của file này thể hiện cho kết nối vật lý của thiết bị. Sau đây là nội dung file *StartingRouter.net* dùng cho mô hình mạng được mô tả bên trên. Có thể soạn thảo file này bằng Notepad và save lại với <filename>.net>

```
#-----code-----
autostart = False      # khi khởi động lên tất cả các Router đều ở trạng thái Stop.

[localhost:7200]

workingdir = C:\Program Files\Dynamicips      #các file tự sinh ra khi chương
trình hoạt động sẽ được lưu trong thư mục này.

[[7200]]

image = D:\soft\utility\Dynamic\c7200-jk9o3s-mz.123-18.bin      #chỉ
đường dẫn đến nơi lưu IOS.
```

npe = npe-400

ram = 96

mmap = True

ghostios = True

sparsemem = True

#----- định nghĩa Router 1-----

[[Router R1]]

model = 7200 # Router R1 đời 7200.

console = 2001 # cổng kết nối 2001.

confreg = 0x2102

slot2 = PA-2T #Slot 2 sẽ gắn module gồm 2 cổng Serial.

slot3 = PA-2FE-TX #Slot 3 sẽ gắn module gồm 2 cổng FastEthernet.

S1/0 = R2 S1/0 #cổng Serial1/0 của Router R1 kết nối với cổng Serial1/0 của Router R2.

F0/0 = NIO_gen_eth:\Device\NPF_{4FFC4BCE-707B-4DB2-8348-CE0F817A5FAE}
#gắn cổng FastEthernet F0/0 của Router R1 với card mạng thứ nhất.

#----- định nghĩa Router 2-----

[[router R2]]

model = 7200

console = 2002

confreg = 0x2102

S1/1 = R3 S1/0 #cổng s1/1 của Router R2 kết nối với cổng S1/0 của Router R3.

#----- định nghĩa Router 3-----

-
[[router R3]]

model = 7200

console = 2003

confreg = 0x2102

#----- End-----

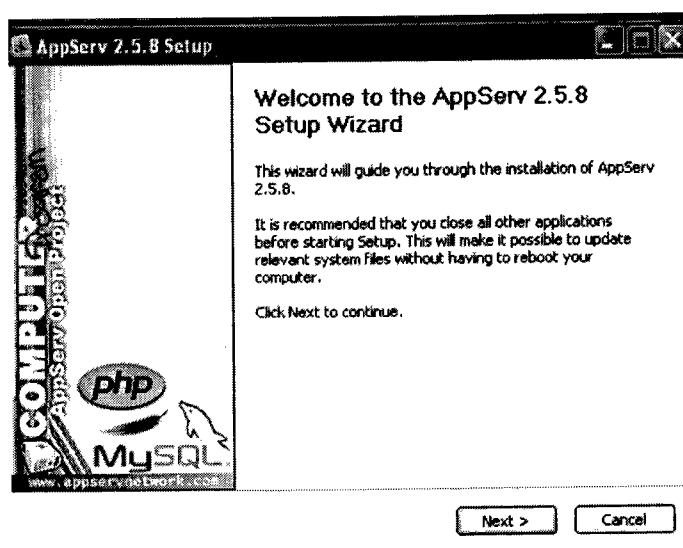
Sau khi hoàn thành File *StartingRouter.net* có nghĩa là đã hoàn thành việc kết nối vật lý giữa các thiết bị mạng và máy tính với nhau.

II) Dụng Webserver và giới thiệu về công cụ tấn công Apache DoS.

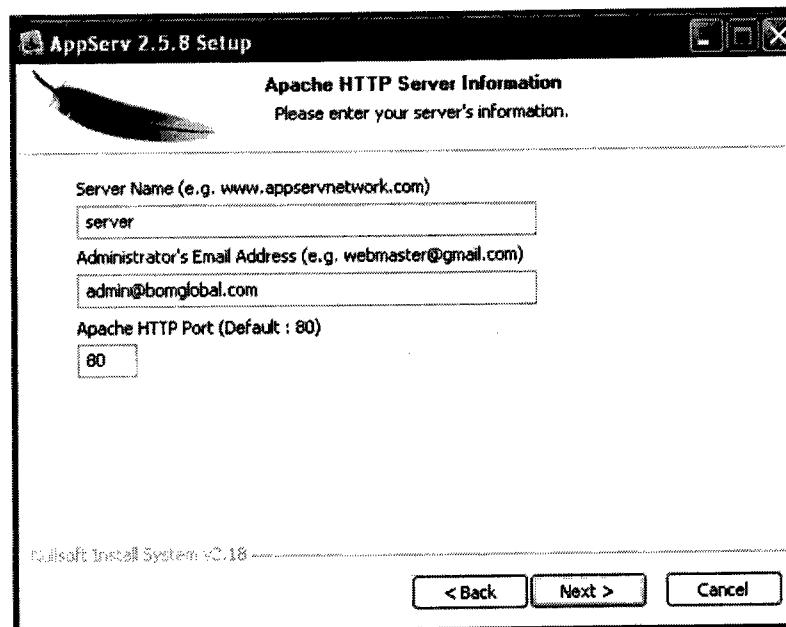
2.1) Dụng Apache Webserver.

Để xây dựng webserver bằng Apache, em download phần mềm *appserv-win32-2.5.8.exe*. Và tiến hành cài đặt chương trình theo trình tự các bước bên dưới.

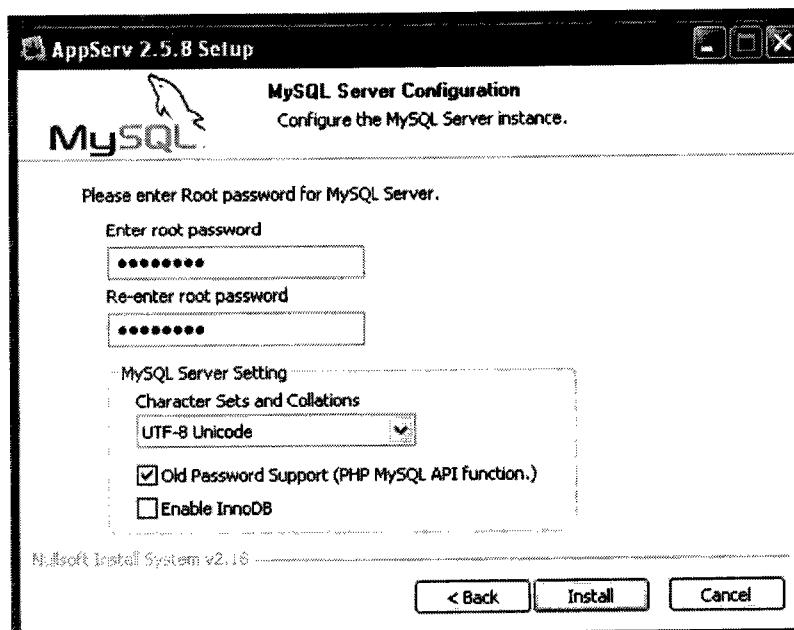
B1. Click vào file vừa download về để chạy setup.



B1. Nhấn Next để tiếp tục cho đến khi cửa sổ Apache HTTP server Information hiện ra, nhập vào thông tin về server name và email của người quản trị web server.



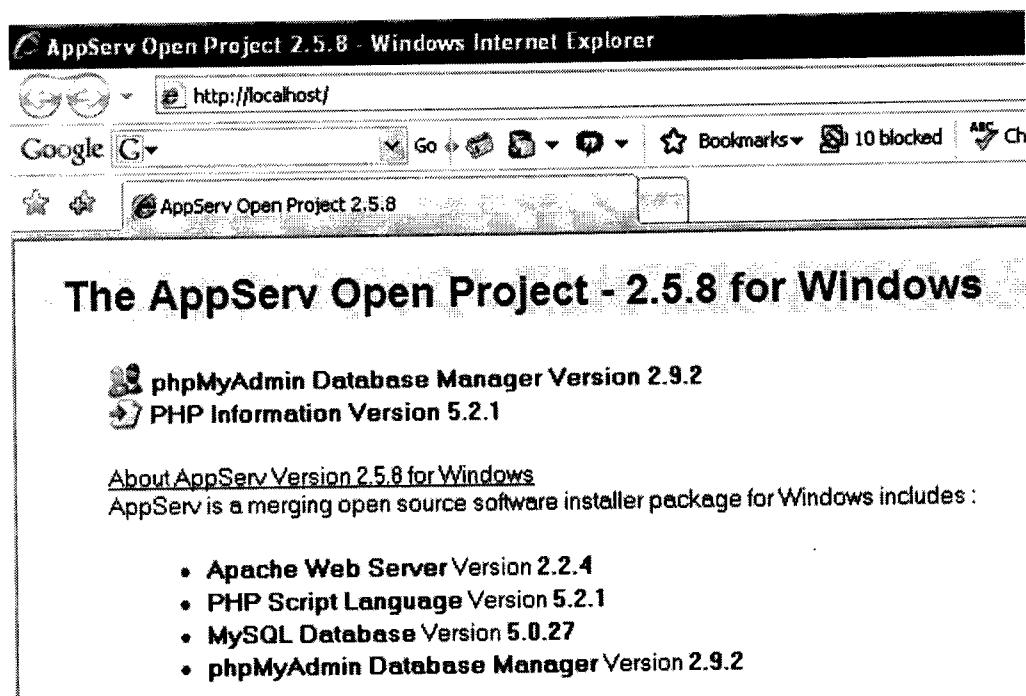
B3. nhập vào password của Root. Đây là quyền quản trị trong Database của MySqlServer.



B4. Quá trình cài đặt Apache Webserver được bắt đầu và cuối cùng nhấn Finish để hoàn thành quá trình cài đặt và Start dịch vụ lên.

2.2) Cấu hình website.

Bước tiếp theo copy toàn bộ Forum vào trong thư mục WWW của Apache. Và mở IE lên, nhập vào địa chỉ localhost để cấu hình cho Mysql server.



Để tạo Database cho website, vào trong phpMyAdmin Database Manager, sau đó nhập vào user và Password mà ta dùng khi cài đặt Apache.

The screenshot shows the phpMyAdmin 2.9.2 interface. On the left, there is a sidebar with various icons and a dropdown menu for "Database". The main area has a heading "localhost" and a "Create new database" form. The "Create" button is highlighted. On the right, there is a sidebar with various configuration options and links. The "Create" button is also present here.

Để tạo Database cho website, chọn tab Create new Database và nhập vào tên Database muốn tạo, cuối cùng nhấn Create để tạo.

Đến đây là hoàn thành quá trình xây dựng Apache Webserver. Ta có thể duyệt web bằng cách mở IE và nhập vào địa chỉ website. Ví dụ như sau “<http://localhost/myweb>” .