Chương trình KC-01:
Nghiên cứu khoa học phát triển công nghệ thông tin và truyền thông

Đề tài KC-01-01:
Nghiên cứu một số vấn đề bảo mật và an toàn thông tin cho các mạng dùng giao thức liên mạng máy tính IP

Báo cáo kết quả nghiên cứu

MÔ HÌNH BẢO MẬT THÔNG TIN CHO CÁC MẠNG MÁY TÍNH

Quyển 2A: "Giao thức TCP/IP và giải pháp bảo mật ở các tầng khác nhau"

HÀ NỘI-2002

Báo cáo kết quả nghiên cứu

MÔ HÌNH BẢO MẬT THÔNG TIN CHO CÁC MẠNG MÁY TÍNH

Quyển 2A: "Giao thức TCP/IP và giải pháp bảo mật ở các tầng khác nhau"

Chủ trì nhóm nghiên cứu:
ThS. Đặng Hoà

MỤC LỤC

PHẦN I- GIAO THỨC MẠNG TCP/IP

CHƯƠNG 10-AN TOÀN TẦNG MẠNG
10.1 Giới thiệu
10.2 Cấu trúc, dịch vụ và giao thức an toàn tầng mạng
10.3 Sắp đặt kiến trúc dịch vụ an toàn
10.4 An toàn mức hệ thống cuối
10.5 An toàn mức mạng con
10.6 Giao thức an toàn tầng mạng
10.7 Truyền dữ liệu an toàn
10.8 Thiết lập và giải phóng kết nối
10.9 Tóm tắt

CHƯƠNG 11-AN TOÀN TẦNG GIAO VẬN
11.1 Giới thiệu
11.2 Khái quát về tầng giao vận
11.3 Độ tin cậy của mạng con
11.4 Các lớp giao vận
11.5 Các thủ tục giao vận
11.6 Dữ liệu expedited
11.7 Chất lượng dịch vụ
11.8 Kiến trúc an toàn
11.10 Các cơ chế an toàn
11.11 Các thuộc tính liên kết an toàn
11.12 Giao thức tổ hợp an toàn

CHƯƠNG 12-CÁC GIAO THỨC AN TOÀN TẦNG ỨNG DỤNG CỦA CÁC MẠNG
12.1 Sự cần thiết của các giao thức an toàn tầng ứng dụng
12.2 Nhìn từng tầng ở góc độ an toàn
12.3 An toàn tầng ứng dụng - ALS (application layer security)
12.4 Khả năng tương tác - Chìa khoá đưa tới thành công của ALS
12.5 Cài đặt ví dụ - giao thức giao dịch điện tử an toàn của Visa
12.6 Từ những bưu thiếp tới những lá thư - Thư tín điện tử an toàn
12.7 Chế ngự HTTP - An toàn ứng dụng WEB
12.8 Đừng cho tôi thấy tiền - An toàn giao dịch tiền tệ
12.9 Nếu bây giờ nó không được mã hoá....

PHẦN I
GIAO THỨC MẠNG TCP/IP

CHƯƠNG 1. GIỚI THIỆU VÀ KHÁI QUÁT

1.1 Lịch sử của TCP/IP Internet

Trong nhiều năm các cơ quan của chính phủ Mỹ đã nhận thức được tầm quan trọng và tiềm năng của công nghệ liên mạng và đã tài trợ việc nghiên cứu để cho việc liên mạng trong toàn quốc trở thành hiẹen thực. Cơ quan Các dự án Nghiên cứu Phòng vệ Cấp cao Deference Advanced Reseach Projects Agency (DARPA) đã tài trợ cho nghiên cứu công nghệ liên mạng vào giữa những năm 1970. Công nghệ này bao gồm một tập các chuẩn về mạng, chỉ ra chi tiết cách các máy tính trao đổi thông tin với nhau như thế nào, và một tập các quy ước về các mạng nối với nhau và định hướng dòng thông tin. Tên chính thức của công nghệ liên mạng do DARPA nghiên cứu là Bộ các giao thức liên mạng TCP/IP và thường được gọi là TCP/IP (tên này có từ tên của hai giao thức: Giao thức điều khiển truyền tin (Transmission Control Protocol) viết tắt là TCP và giao thức Internet (Internet Protocol) viết tắt là IP là hai giao thức chuẩn chính của bộ các giao thức này). Bộ giao thức này có thể được sử dụng để truyền tin qua bất cứ nhóm các mạng nào nối với nhau. Ví dụ, một số công ty sử dụng TCP/IP để nối tất cả các mạng trong công ty với nhau, ngay cả khi công ty không có ý định nối với các mạng bên ngoài công ty.

Dần dần công nghệ TCP/IP trở thành công nghệ cơ sở cho liên mạng lớn và cho các cơ quan nghiên cứu, trường đại học, công ty và các phòng thí nghiệm của chính phủ Mỹ nối với nhau và nối với mạng của DARPA. Và cuối cùng tên TCP/IP Internet, hay chỉ là Internet được chấp nhận. Ngày nay Internet không chỉ là mạng giới hạn trong phạm vi nước Mỹ, mà đã trở thành một mạng toàn cầu nối rất nhiều mạng của các quốc gia với nhau.

1.2 Các đặc tính của TCP/IP

Sự phổ dụng của các giao thức TCP/IP trên Internet không phải vì các giao thức này có trên Internet hay vì các cơ quan quân sự bắt phải sử dụng chúng. Các giao thức này đáp ứng những đòi hỏi của truyền dữ liệu toàn cầu vào đúng thời gian cần thiết, và chúng có một số đặc tính quan trọng sau:

- Bộ giao thức TCP/IP không bị ràng buộc vào một phần cứng hay hệ điều hành nào. TCP/IP là cách lý tưởng để liên kếtcác phần cứng và phần mềm khác nhaungay cả khi bạn sử dụng chúng ddể giao tiếp không qua Internet.
- Bộ giao thức TCP/IP độc lập với các phần cứng của mạng máy tính. Đặc tính này cho phép TCP/IP tích hợp các kiểu mạng máy tính khác nhau. Bộ giao thức TCP/IP có thể sử dụng Ethernet, token ring, dial-up line, X.25, và hầu như trên các mạng vật lý truyền tin khác nhau.
- Bộ giao thức TCP/IP có chế độ đánh địa chỉ chung cho phép các máy sử dụng TCP/IP giao tiếp với máy có địa chỉ đúng trên toàn mạng, ngay cả đối với mạng máy tính rất lớn như mạng toàn cầu.

- Bộ giao thức TCP/IP đã chuẩn hoá các bộ giao thức ở tầng trên hướng đến tính ổn định, dễ sử dụng cho các dịch vụ trên mạng.

1.3 Các dịch vụ của Internet

Không thể đánh giá những chi tiết kỹ thuật của TCP/IP mà không hiểu những dịch vụ mà bộ giao thức này đem lại. Đa số các thảo luận về dịch vụ sẽ tập trung vào các chuẩn gọi là các giao thức. Những giao thức như TCP và IP cung cấp những qui định để chuyển các thông báo (message), miêu tả chi tiết định dạng của thông báo, và miêu tả cách xử lý với các lỗi. Điều quan trọng nhất là các giao thức cho phép thảo luận các chuẩn truyền tin không phụ thuộc vaò phần cứng mạngcủa các nhà sản xuất. Các nhà lập trình không cần phải biết chi tiết những tầng thấp của truyền thông để xây dựng các phần mềm ứng dụng để chuyển và dịch dữ liệu giữa hai máy tính.

Các dịch vụ Internet tầng ứng dụng

Từ cách nhìn của người sử dụng, TCP/IP Internet như là một tập các chương trình ứng dụng sử dụng mạng máy tính để thực hiện các công việc truyền thông hữu ích. Những chương trình ứng dụng phổ biến được sử dụng nhiều là:

Thư điện tử. Thư điện tử cho phép người dùng tạo các bức thư và gửi đến một cá nhân hay một nhóm người, đồng thời thư điện tử cũng cho phép người dùng đọc các thư gửi đến.

Chuyển file. Các thủ tục TCP/IP cho phép xây dựng chương trình ứng dụng chuyển và nhận các file chương trình, dữ liệu với độ dài tuỳ ý. Chương trình chuyển file của TCP/IP ổn định và hai máy chuyển file trao đổi trực tiếp với nhau chứ không dựa vào máy trung gian.

Truy nhập từ xa. Đây là một ứng dụng có lẽ là thú vị nhất, truy nhập từ xa cho phép người dùng ngồi tại một máy A để nối với một máy ở xa B và thiết lập môtj phiên truy nhập tương tác. Truy nhập từ xa làm cho người dùng ở màn hình máy A cảm thấy như nối trực tiếp với máy B nhờ gửi từng ký tự ấn trên bàn phím ở máy A đến máy ở xa B và hiện từng ký tự in ra từ máy ở xa B trên màn hình máy A. Khi phiên liên lạc từ xa kết thúc, chương trình ứng dụng đưa người sử dụng trở về máy cục bộ.

World Wide Web. Đây là chương trình ứng dụng được phát triển sau ba chương trình ứng dụng phổ biến trên và có lẽ là chương trình được sử dụng nhiều nhất hiện nay. WWW sử dụng giao thức chuyển siêu văn bản (HTTP), thông tin được định dạng nhờ Ngôn ngữ ghi siêu văn bản (HTML). Các chương trình Web chủ cung cấp thông tin đa phương tiện (multimedia) trên Internet cho bất cứ ai có chương trình duyệt Web có thể được sử dụng để xây dựng hệ thông tin riêng, gọi là Intranet trên các mạng TCP/IP.

Các dịch vụ tầng mạng

Một người lập trình viết các chương trình ứng dụng sử dụng các gaio thức TCP/IP có cách nhìn Internet khác hoàn toàn với cách nhìn của người sử dụng bình thường. Tại tầng mạng, liên mạng cung cấp hai dạng dịch vụ mà tất cả chương trình ứng dụng sử dụng:

- *Dịch vụ không liên kết chuyển gói tin*. Dịch vụ này sẽ được miêu tả chi tiết sau. Việc chuyển không liên kết là sự trừu tượng của dịch vụ mà đa số các mạng chuyển đổi gói tin cung cấp. Điều này có thể hiểu đơn giản là TCP/IP Internet vạch đường cho các thông báo nhỏ từ máy này tới máy khác dựa trên địa chỉ mạng trong thông báo. Do dịch vụ không liên kết vạch đường cho mỗi gói tin một cách riêng rẽ, nên dịch vụ không đảm bảo sự ổn định, không đảm bảo chuyển theo trật tự. Quan trọng hơn, việc chuyển không liên kết gói tin coi là cơ sở cho tất cả các dịch vụ Internet làm cho các giao thức TCP/IP phù hợp với một phạm vi rộng lớn các phần cứng mạng.

- *Dịch vụ vận tải dòng dữ liệu tin cậy*. Đa số các ứng dụng cần nhiều hơn việc chuyển không liên kết gói tin vì chúng yêu cầu các phần mềm truyền thông tự động khôi phục do các lỗi truyền tin, mất gói tin, hoặc do hỏng của các chuyển đổi dọc theo đường truyền giữa nơi gửi và nơi nhận. Dịch vụ vận tải ổn định giải quyết những vấn đề đó. Dịch vụ này cho phép một ứng dụng trên một máy tính thiết lập một "liên kết" với một ứng dụng trên máy tính khác, và sau đó gửi một lượng lớn dữ liệu qua đường liên kết như là một liên kết cứng trực tiếp, cố định. Thực ra, ở bên dưới các giao thức truyền thông chia dòng dữ liệu thành các thông báo nhỏ và gửi chúng, từng thông báo một, đợi cho nơi nhận báo cho biết đã nhận được.

1.4 Các tài liệu chuẩn về TCP/IP

Bản chất mở của bộ giao thức TCP/IP đòi hỏi các tài liệu của nó phải được xuất bản và có sẵn. Tất cả các giao thức TCP/IP được xác định ở một trong ba xuất bản chuẩn. Một số các giao thức được chấp nhận như chuẩn quân sự (MIL STD). Một số khác được xuất bản như các ghi chú của kỹ thuật Internet (Internet Engineering Notes) (IEN) (các dạng xuất bản này nay đã được bãi bỏ). Đa số các thông tin về các giao thức TCP/IP được xuất tính bản dưới tên Request for Comments (RFC). RFC chứa các chi tiết mới nhất về các chuẩn của bộ TCP/IP. RFC chứa những thông tin bổ ích và lý thú và không chỉ giới hạn trong lĩnh vực giao thức truyền dữ liệu.

Một số RFC chứa những chỉ dẫn mang tính thực tiễn và đơn giản. Một số khác chứa các thông tin kỹ thuậtđược xác định trên các khái niệm trong lĩnh vực truyền dữ liệu. Trên Internet các RFC có thể được lấy nhờ các FTP vô danh (anonymous FTP) trên nhiều địa chỉ như: ftp://nic.ddn.mil/rfc/rfcxxxx.txt.

1.5 Sự phát triển tương lai và công nghệ

Cả công nghệ TCP/IP và Internet tiếp tục tiến triển. Nhiều giao thức mới đang được đề xuất; những giao thức cũ đang được sửa đổi. Sự thay đổi quan trọng nhất xuất phát không phải từ việc thêm các đường liên kết mạng, mà từ việc thêm các thông tin trao đổi.

Để đáp ứng được sự tăng thông tin trao đổi, khả năng các đường trục đã phải tăng lên nhiều lần. Hiện tại, rất khó xác định trước nhu cầu cuối cùng về khả năng trao đổi thông tin. Trong tương lai chúng ta có thể chờ đợi sự tăng không ngừng yêu cầu truyền thông. Do vậy, cần có các công nghệ truyền thông với khả năng lớn hơn để đáp ứng sự tăng nhu cầu.

Hình 1.1 tóm tắt sự mở rộng của Internet trong một số năm và minh hoạ các thành phần quan trọng trong sự mở rộng: sự thay đổi tính phức tạp nảy sinhvì nhiều nhóm tự trị quản lý các phần của Internet. Những thiết kế ban đầu cho nhiều hệ con phụ thuộc vào sự quản lý tập trung. Nhiều cố gắng nghiên cứu đã mở rộng các thiết kế đó để đáp ứng sự quản lý không tập trung.

	Số các mạng	Số máy tính	Số người quản lý
1980	10	10^2	10^0
1990	10^3	10^5	10^4
1995	10^5	10^{10}	10^2

Hình 1.1 Sự tăng của Internet

CHƯƠNG 2. CẤU TRÚC PHÂN TẦNG CỦA MÔ HÌNH TCP/IP

2.1 Cấu trúc của mô hình TCP/IP

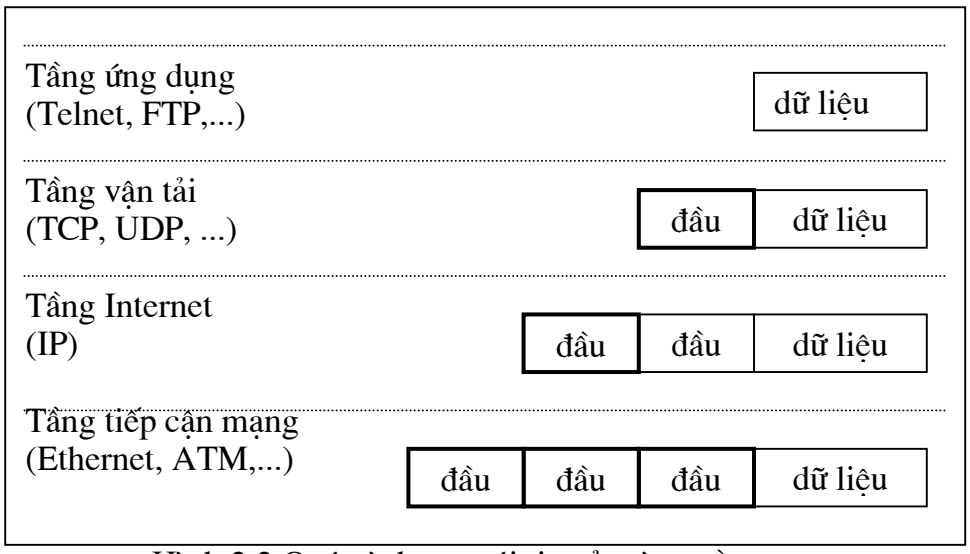
Trong khi không có một văn bản chính thức nào chuẩn hoá việc miêu tả mô hình TCP/IP như là một mô hình gồm các tầng, thì mô hình TCP/IP thường được xem như là được tạo ra từ số các tầng ít hơn là mô hình tham khảo 7 tầng. Đa số các miêu tả xác định mô hình TCP/IP gồm từ 3 cho đến 5 tầng chức năng trong cấu trúc phân tầng. Mô hình 4 tầng trong hình 2.1 cung cấp một bức tranh chấp nhận được để biểu diễn các tầng trong cấu trúc giao thức của mô hình TCP/IP.

4. Tầng ứng dụng Bao gồm các ứng dụng và các quá trình sử dụng mạng.
3. Tầng vận tải Cung cấp các dịch vụ truyền dữ liệu đầu-cuối.
2. Tầng Internet Xác định gói dữ liệu và quản lý đường truyền
1. Tầng tiếp cận mạng Bao gồm các giao thức để tiếp cận các mạng vật lý.

Hình 2.1 Các tầng trong mô hình TCP/IP

Như trong mô hình tham khảo OSI, dữ liệu được truyền từ tầng trên xuống tầng dưới khi nó được gửi đi và dữ liệu được truyền từ tângf dưới lên tầng trên khi nó được nhận. Cấu trúc 4 tầng của TCP/IP được chấp nhận vì nó thể hiện cách dữ liệu được điều khiển khi chuyển từ tầng ứng dụng cho đến tầng vật lý của mạng. Mỗi một tầng sẽ thêm thông tin điều khiển để đảm bảo rằng dữ liệu được truyền một cách chính xác. Thông tin điều khiển được gọi là "đầu" vì nó được đặt ở phía trước dữ liệu cần truyền. Mỗi tầng quan niệm tất cả thông tin nhận được từ tầng trên như là dữ liệu và tạo thông tin đầu của tầng đó và đặt vào phía trước dữ liệu nhận được. Khi nhận dữ liệu, một quá trình ngược lại được thực hiện. Mỗi tầng phân tích đầu của tầng đó và bỏ thông tin đầu đi trước khi chuyển gói thông tin cho tầng trên, và theo dòng chuyển thông tin, mỗi tầng sẽ nhận được gói thông tin gồmđầu và dữ liệu tương ứng.

Mỗi tầng có một cấu trúc dữ liệu riêng của nó. Do vậy mỗi tầng không phải quan tâm đến cấu trúc dữ liệu được sử dụng của tầng trên hay tầng dưới. Trên thực tế, cấu trúc dữ liệu của mỗi tầng được thiết kế sao cho tương ứng với cấu trúc dữ liệu của các tầng chung quanh để cho dòng thông tin được chuyển tải có hiệu quả hơn. Hình 2.2 miêu tả quá trình này.



Hình 2.2 Quá trình tạo gói tin của từng tầng

Bây giờ chúng ta sẽ xem xét kỹ chức năng của từng tầng trong mô hình TCP/IP theo hướng từ tầng dưới lên tầng trên.

2.2 Tầng tiếp cận mạng

Đây là tầng thấp nhất trong cấu trúc phân tầng của mô hình TCP/IP. Các giao thức trong tầng này cung cấp cách để hệ thống chuyển dữ liệu đến phương tiện kỹ thuật khác đang gắn liền trên mạng. Chính tầng này xác định cách sử dụng mạng vật lý để chuyển các gói thông tin của tầng mạng (IP).

Không giống những giao thức của các tầng trên, tầng tiếp cận mạng phải biết hết chi tiết của mạng vật lý ở dưới như cấu trúc gói thông tin, cách đánh địa chỉ, ... để định dạng dữ liệu chuyển xuống phù hợp với các điều kiện đặt ra của mạng vật lý. Trong mô hình TCP/IP, tầng tiếp cận mạng có thể thực hiện các chức năng của ba tầng phía dưới trong mô hình tham khảo OSI (tầng vật lý, tầng liên kết dữ liệu và tầng mạng.

Trong mô hình TCP/IP, người sử dụng thường không quan tâm đến tầng tiếp cận mạng vì thiết kế t đã dấu các chức năng cuả các tầng dưới, và các giao thức được biết rõ như IP, TCP, UDP đều là các giao thức của các tầng trên. Khi một công nghệ phần cứng mới xuất hiện, những giao thức tiếp cận mạng mới phải được phát triển sao cho mạng TCP/IP có thể sử dụng được phần cứng mới đó. Do vậy, có rất nhiều giao thức trong tầng tiếp cận mạng, mỗi một giao thức phù hợp với một chuẩn của mạng vật lý.

Các chức năng chính của tầng tiếp cận mạng là nhận gói thông tin của tầng IP ở trên và tạo gói thông tin mới để có thể chuyển trong mạng, đồng thời phải tạo được sự tương ứng giữa địa chỉ IP với địa chỉ vật lý mà mạng đang sử dụng. Một trong những tính mạnh của mô hình TCP/IP là địa chỉ IP xác định duy nhất máy

đang sử dụng trong Internet, địa chỉ IP này phải được chuyển thành địa chỉ tương ứng phù hợp với địa chỉ vật lý mà mạng vật lý cụ thể đang dùng (địa chỉ của card mạng).

2.3 Tầng Internet

Tầng ở ngay phía trên tầng tiếp cận mạng trong mô hình cấu trúc của TCP/IP là tầng Internet. Giao thức Internet (IP) chính là trái tim của mô hình TCP/IP và là giao thức quan trọng nhất trong tầng Internet. Giao thức IP cung cấp dịch vụ cơ bản để truyền gói thông tin cơ sở, và mạng TCP/IP được xây dựng trên chính dịch vụ này. Tất cả mọi giao thức của tầng phía trên (TCP, UDP) và phía dưới (Ethernet, FDDI, ATM) tầng Internet đều sử dụng IP để truyền dữ liệu. Tất cả dữ liệu, dù đến hay đi, của mô hình TCP/IP đều đi qua IP không phụ thuộc vào đích cuối cùng.

Chức năng chính của giao thức Internet gồm:

- Xác định từng gói dữ liệu là đơn vị cơ sở để truyên trong Internet.
- Xác định cách đánh địa chỉ trong Internet
- Di chuyển dữ liệu giữa tầng tiếp cận mạng và tầng vận tải
- Chỉ đường đi cho các gói dữ liệu đến máy ở xa
- Thực hiện phân chia hay tổ hợp lại các gói dữ liệu

Các chương sau sẽ mô tả chi tiết từng chức năng của giao thức Internet, chúng ta xem xét một số đặc tính cơ bản của giao thức Internet. Trước hết giao thức Internet không tạo liên kết (connectionless protocol). Điều này có nghĩa là IP không trao đổi thông tin điều khiển để tạo liên kết trước khi truyền dữ liệu. IP dựa vào giao thức của tầng khác để thiết lập liên kết nếu như các dịch vụ đòi hỏi sự liên kết giữa các máy.

Giao thức IP cũng dựa vào các giao thức của các tầng khác để phát hiện và sửa sai. Vì thế đôi khi người ta gọi giao thức IP là một giao thức không tin tưởng bởi vì nó không có chứa mã sửa sai. Nhưng điều này không có nghĩa là không nên dựa vao giao thức IP, hoàn toàn ngược lại, mô hình TCP/IP dựa vào giao thức này để chuyển chính xác dữ liệu đến đích, nhưng nó không kiểm tra dữ liệu có được nhận chính xác không. Các giao thức của tầng khác trong mô hình TCP/IP sẽ cung cấp dịch vụ kiểm tra khi đòi hỏi.

2.4 Tầng vận tải

Tầng giao thức ở phía trên tầng Internet là tầng vận tải. Hai giao thức quan trọng nhất của tầng này là giao thức điều khiển truyền tin (Transmission Control Protocol (TCP)) và giao thức gói thông tin của người sử dụng (User Datagram Protocol (UDP)). Giao thức TCP là giao thức truyền dịch vụ tin tưởng với phát hiện và sửa sai đầu-cuối. Giao thức UDP là giao thức truyền dịch vụ không có liên kết

nhưng mất ít thông tin khởi đầu. Cả hai giao thức đều chuyển dữ liệu giữa hai tầng: tầng Internet và tầng ứng dụng.

Giao thức gói thông tin của người sử dụng (User Datagram Protocol (UDP))

Giao thức UDP cung cấp cho các chương trình ứng dụng khả năng sử dụng dịch vụ truyền gói thông tin, cũng như dịch vụ mà giao thức IP cung cấp, dịch vụ này cho phép các chương trình ứng dụng trao đổi các tin qua mạng với những giao thức khởi đầu ít nhất.

Giao thức UDP là giao thức gửi gói tin không liên kết và không chắc chắn. ("không chắc chắn" ở đây có nghĩa là giao thức không kiểm tra xem gói tin được truyền qua mạngđã đến đích trọn vẹn không), còn trong một máy tính thì UDP luôn truyền tin một cách tin tưởng.

Giao thức điều khiển truyền tin (Transmission Control Protocol (TCP))

Những chương trình ứng dụng đòi hỏi tầng vận tải cung cấp một dịch vụ truyền dữ liệu tin tưởng, dịch vụ đó phải kiểm tra dữ liệu được truyền qua mạng một cách chính xác và theo một trật tự xác định. Giao thức TCP là giao thức tin tưởng, có liên kết và là dòng byte dữ liệu.

Giao thức TCP xem dữ liệu mà nó gửi như là một dòng liên tục các byte, chứ không phải các gói thông tin độc lập. Do vậy, giao thức TCP quan tâm đến việc duy trì dãy dữ liệu mà các byte được gửi hay nhận.

Giao thức TCP cũng chịu trách nhiệm truyền dữ liệu nhận từ tầng IP lên cho tầng ứng dụng. Việc truyền dữ liệu một cách chính xác đến tầng ứng dụng là một chức năng quan trọng của tầng vận tải.

2.5 Tầng ứng dụng

Tầng ứng dụng là tầng trên cùng trong cấu trúc của bộ giao thức TCP/IP. Tầng này bao gồm tất cả các chương trình có sử dụng tầng vận tải để truyền dữ liệu. Có rất nhiều giao thức ứng dụng. Đa số các giao thức ứng dụngcung cấp các dịch vụ, và rất nhiều giao thức mới được tạo ra cho tầng ứng dụng. Những giao thức ứng dụng đã được sử dụng biết đến nhiều là:

- **Telnet**, là giao thức cung cấp khả năng truy nhập từ xa qua mạng
- **FTP**, là giao thức chuyển file qua mạng
- **SMTP**, là giao thức để chuyển thư điện tử
- **HTTP**, là giao thức để chuyển siêu văn bản.

Trong khi các ứng dụng FTP, SMTP, HTTP và Telnet là các ứng dụng của bộ giao thức TCP/IP được người sử dụng dùng nhiều, người quản trị sẽ làm việc với nhiều ứng dụng khác như:

- Domain Name Service (DNS) - Dịch vụ cho vùng tên, ứng dụng này chuyển đổi các địa chỉ IP thành các tên gắn với các máy trên mạng.

- Routing Information Protocol (RIP) - Giao thức thông tin đường dẫn: là giao thức mà các máy trên mạng dùng để trao đổi thông tin đường dẫn.

- Network File System (NFS) - Hệ thống file mạng: Giao thức này cho phép các file được dùng chung cho các máy trên mạng.

Chỉ người sử dụng biết một số kiến thức về mạng mới có thể dùng các giao thức như telnet và FTP. Đối với các giao thức khác như RIP thì được dùng mà không cần người sử dụng.

2.6 Hai biên quan trọng trong mô hình TCP/IP

Khái niệm phân tầng các giao thức có hai biên: biên địa chỉ giao thức ngăn cách địa chỉ của tầng thấp và tầng cao, và biên hệ điều hành ngăn cách hệ thống với các chương trình ứng dụng.

Biên địa chỉ giao thức tầng cao

Khái niệm biên phân chia phần mềm sử dụng các địa chỉ vật lý ở tầng thấp với các phần mềm sử dụng các địa chỉ IP ở tầng cao. Hình 2.3 chỉ vị trí của biên giữa tầng giao diện mạng và tầng Internet.

Tầng	Biên
Tầng ứng dụng	Phần mềm ngoài hệ điều hành
Tầng vận tải	Phần mềm trong hệ điều hành
Tầng Internet	Chỉ sử dụng các địa chỉ IP
Tầng tiếp cận mạng	Sử dụng các địa chỉ vật lý
Phần cứng	

Hình 2.3 Quan hệ giữa phân tầng theo nhận thức và các biên đối với hệ điều hành và các địa chỉ giao thức tầng cao.

Biên hệ điều hành

Hình 2.3 cũng chỉ ra một biên quan trọng khác, đó là sự phân chia phần mềm thường được coi là một phần của hệ điều hành và phần mềm không thuộc hệ điều hành. các phần mềm nằm trong hệ điều hành chuyển dữ liệu xuống cho các tầng thấp không đắt bằng các phần mềm ứng dụng chuyển dữ liệu xuống cho tầng vận tải.

2.7 Nhu cầu liên mạng Internet

Mô hình TCP/IP trên được thiết kế do nhu cầu liên mạng khi các mạng máy tính ra đời phục vụ nhu cầu của người dùng.

Khi thiết kế các hệ thống truyền thống, những người thiết kế gặp phải hai vấn đề lớn:

- Không có một mạng nào có thể phục vụ hết cac nhu cầu của mọi người sử dụng
- Người sử dụng muốn một sự liên kết toàn cầu

Vấn đề thứ nhất có tính kỹ thuật. Các mạng cục bộ cung cấp các đường truyền thông với tốc độ cao, nhưng bị giới hạn về không gian; các mạng diện rông trải ra trên những khoảng cách lớn nhưng không thể cung cấp các đường liên kết với tốc độ lớn. Không có một công nghệ mạng nào thoả mãn mọi nhu cầu, chính vì lẽ đó các nhà thiết kế đã phải xem xét sự tích hợp các công nghệ phần cứng.

Vấn đề thứ hai là tự nhiên. Một cách tổng thể, chúng ta muốn có khả năng trao đổi giữa bất kỳ hai điểm nào. Cụ thể, chúng ta không muốn một hệ thống truyền thông bị ràng buộc bởi các biên của các mạng vật lý.

Mục đích là xây dựng một liên mạng hợp tác tổng thể ủng hộ dịch vụ truyền thông toàn cầu. Trong mỗi mạng, các máy tính sử dụng hệ thống phần cứng cụ thể. Hệ phần mềm mới, chèn vào giữa các cơ cấu truyền thông độc lập với công nghệ sẽ che đi những chi tiết cụ thể của tầng tấp và làm cho tất cả các mạng hiện ra như là một mạng lớn. Cơ chế liên mạng như vậy được gọi là nối các mạng lại hay là Internet.

Khái niệm dịch vụ toàn cầu là quan trọng, và trong thiết kế các nhà tạo ra Internet muốn che đậy kiến trúc Internet ở phía dưới, do vậy Internet:

- Không yêu cầu người dùng hoặc các chương trình ứng dụng hiểu chi tiết của các đường liên kết cứng
- Không trao quyền cho hình thái liên kết mạng. Người lập trình không phải hiểu hình thái liên kết mạng khi viết các chương trình ứng dụng.

Trong kiến trúc Internet, các giao thức của mô hình TCP/IP coi tất cả các mạng đều như nhau. Một mạng cục bộ như Ethernet, một mạng diện rộng, hoặc một đường liên kết điểm tới điểm giữa hai máy đều được coi như một mạng.

CHƯƠNG 3. CÁC ĐỊA CHỈ INTERNET

3.1 Địa chỉ Internet

Một hệ truyền thống cung cấp dịch vụ truyền thông toàn cầu nếu nó cho phép một máy bất kỳ trao đổi với một máy bất kỳ khác. Để cho Internet trở thành hệ toàn cầu, cần phải thiết lập một phương pháp có tính toàn cầu chấp nhận được để xác định những máy tính găns vào mạng.

Giao thức IP chuyển dữ liệu giữa các máy bằng các gói tin. Mỗi gói tin được gửi đến địa chỉ chứa trong phần địa chỉ đích (Destination Address) ở đầu của gói tin. Địa chỉ đích là địa chỉ IP gồm 32 bit có chứa đủ thông tin để xác định duy nhất mạng và máy trên mạng đó.

Mỗi địa chỉ IP gồm phần địa chỉ mạng và địa chỉ máy, nhưng định dạng của những phần này không như nhau cho các địa chỉ IP. Các bit cho địa chỉ mạng được sử dụng để xác định mạng, và các bit cho địa chỉ máyđể xác định máy trên mạng. Số lượng các bit này khác nhau phụ thuộc vào nhóm các địa chỉ. Có tất cả 5 nhóm chữ cái, trong đó có 3 nhóm chính. Bảng 3.1 sau sẽ tóm tắt đặc tính của mỗi nhóm địa chỉ.

Nhóm	Các bit trong byte đầu tiên	Khoảng của địa chỉ mạng	Số byte của địa chỉ mạng	Số byte của địa chỉ máy
A	0xxxxxxx	0.0.0.0-127.0.0.0	1	3
B	10xxxxxx	128.0.0.0-191.255.0.0	2	2
C	110xxxxx	192.0.0.0-223.255.255.0	3	1
D và E	111xxxxx	224.0.0.0-255.255.255.0		

Bảng 3.1 Các nhóm địa chỉ Internet

Bằng cách kiểm tra vài bit của một địa chỉ IP, phần mềm IP có thể xác định nhanh nhóm địa chỉ , và do vậy biết được cấu trúc của địa chỉ.

Chúng ta có thể tính được số mạng cho mỗi nhóm địa chỉ (A, B và C) và số máy cho mỗi mạng theo bảng 3.2, tuy nhiên không phải toàn bộ số địa chỉ đó đều được dùng để đánh địa chỉ cho các máy, một số địa chỉ sẽ được quy ước dùng cho việc khác (chi tiết sẽ được trình bày sau).

Nhóm	Số mạng của một nhóm	Số máy cho một mạng
A	128	256^3=16.777.216
B	64*256=16.128	256^2=65.536
C	32*256^2=2.097.152	256

Bảng 3.2 Số máy có thể cho một mạng

Dưới đây liệt kê một số đặc tính của địa chỉ IP:

- Nếu như bit đầu tiên của địa chỉ IP là 0, đó là địa chỉ nhóm mạng nhóm A. Bit đầu tiên của địa chỉ nhóm A xác định nhóm địa chỉ. Bảy bit sau xác định mạng và 24 bit cuối xác định máy. Có ít hơn 128 mạng thuộc nhóm A, nhưng mỗi mạng của nhóm A có thể bao gồm hàng triệu máy.
- Nếu như hai bit đầu tiên của địa chỉ IP là 10, đó là địa chỉ nhóm mạng nhóm B. Hai bit dầu tiên của địa chỉ nhóm B xác định nhóm địa chỉ. 14 bit sau xác định mạng, và 16 bit cuối xác định máy. Có hàng nghìn mạng thuộc nhóm B và mỗi mạng của nhóm B có thể bao gồm hàng nghìn máy.
- Nếu ba bit đầu tiên của địa chỉ IP là 110, đó là địa chỉ nhóm mạng nhóm C. Ba bit đầu tiên của địa chỉ nhóm C xác định nhóm địa chỉ. 21 bit sau xác định mạng và 8 bit cuối xác định máy. Có hàng triệu mạng thuộc nhóm C, nhưng mỗi mạng của nhóm C có ít hơn 254 máy.
- Nếu như ba bit đầu tiên của địa chỉ IP là 111, đó là địa chỉ đặc biệt đã được quy định trước. Chúng thường được gọi là địa chỉ nhóm D, nhưng những địa chỉ này không chỉ một mạng cụ thể nào. Địa chỉ này thường hướng đếnmột nhóm các máy tính trong cùng một thời gian. Địa chỉ này được sử dụng để xác định một nhóm máy tính dùng chung một giao thức, chứ không phải một nhóm máy tính trong cùng một mạng.

Địa chỉ IP thường được viết như nhóm 4 chữ số thập phân cách nhau bằng một dấu chấm. Mỗi chữ số thập phân có giá trị trong khoảng 0-255 (đó là giá trị số thập phân chứa trong một byte). Bởi vì các bit xác định nhóm và các bit xác định mạng liền nhau trong một byte, nên chúng ta có thể kết hợp chúng với nhau. Khi xét giá trị của byte đầu tiên:

- giá trị nhỏ hơn 128 để chỉ địa chỉ nhóm A; byte đầu tiên là địa chỉ mạng và 3 bytes sau là địa chỉ máy.
- giá trị từ 128 - 191 để chỉ địa chỉ nhóm B; hai byte đầu là địa chỉ mạng và 2 bytes cuối là địa chỉ máy.
- giá trị từ 192 - 223 để chỉ địa chỉ nhóm C; 3 bytes đầu là địa chỉ mạng và byte cuối là địa chỉ máy.
- giá trị lớn hơn 223 để chỉ địa chỉ đã được đặt trước. Chúng ta có thể không quan tâm đến địa chỉ này.

Chúng ta thử xét một số ví dụ. Địa chỉ 28.100.0.29 là địa chỉ nhóm A, vì bit đầu tiên là 0 hay giá trị của byte đầu tiên nhỏ hơn 128, vì vậy địa chỉ máy là 100.0.29 chiếm 3 bytes và địa chỉ mạng 28 chiếm 1 byte. Địa chỉ 193.177.16.5 là địa chỉ nhóm C, vì 3 bit đầu tiên là 110 hay giá trị của byte đầu tiên trong khoảng 192 - 223, do vậy địa chỉ máy là 5 trên mạng có địa chỉ 193.177.16.

Chú ý là không phải tất cả các địa chỉ mạng và địa chỉ máy đều có thể dùng được. Như đã nói địa chỉ có giá trị byte đầu tiên lớn hơn 223 đã được đặt trước. Hai địa chỉ nhóm A là 0 và 127 để sử dụng cho các trường hợp đặc biệt. Địa chỉ mạng 0 là địa chỉ đối với đường dẫn ngầm định và địa chỉ 127 là địa chỉ quay lại (loopback address). Đường dẫn ngầm định để đơn giản thông tin đường dẫn mà IP

phải thực hiện. Địa chỉ quay lại đơn giản các chương trình ứng dụng trên mạng, cho phép địa chỉ của máy cục bộ cũng được coi như địa chỉ của máy ở xa. Chúng ta sử dụng các địa chỉ này khi đặt cấu hình máy.

3.2 Địa chỉ để chỉ đường liên kết mạng

Chúng ta nói rằng địa chỉ Internet dùng để xác định máy, tuy nhiên điều này không hoàn toàn chính xác. Xét trường hợp một máy (cổng dẫn đường) gắn với hai mạng vật lý, khi đó máy này sẽ có hai địa chỉ Internet, mỗi địa chỉ tương ứng với một mạng vật lý, hay là tương ứng với đường mạng liên kết tới máy. Vậy địa chỉ Internet dùng để xác định đường liên kết tới máy.

Cũng còn một số địa chỉ máy nữa để dùng cho các trường hợp đặc biệt. Trong tất cả các mạng, máy có địa chỉ 0 và 255 đã được đặt trước. Địa chỉ IP với các bit của địa chỉ máy có giá trị 0 để xác định địa chỉ của chính mạng đó. Ví dụ địa chỉ 193.100.100.0 để chỉ địa chỉ mạng 193.100.100. Những địa chỉ trong dạng này được sử dụng trong các bảng đường dẫn hướng đến toàn mạng. Địa chỉ IP với các bit của địa chỉ máy có giá trị 1 để xác định địa chỉ cho toàn máy trên mạng. Ví dụ địa chỉ 193.100.100.255 để xác định địa chỉ cho tất cả các máy trên mạng 193.100.100. Gói thông tin gửi đến địa chỉ 193.100.100.255 được gửi đến tất cả các máy trên mạng 193.100.100.0.

Giao thức IP sử dụng phần địa chỉ mạng để vạch đường dẫn cho các gói tin chuyển giữa các mạng. Khi gói tin đến đúng mạng thì phần địa chỉ của máy được sử dụng để chuyển gói tin đến đúng máy.

3.3 Mạng con (subnets)

Cấu trúc chuẩn của địa chỉ IP có thể thay đổi một cách cục bộ bằng cách sử dụng một số bit của địa chỉ máy cho địa chỉ của mạng. Như vậy tạo thêm được một số địa chỉ cho mạng nhưng lại giảm bớt số địa chỉ của máy trên một mạng. Những mạng mới được tạo ra trên mạng lớn cũ gọi là mạng con (subnets).

Các cơ sở thường sử dụng mạng con để vượt qua trở ngại về hình thái của mạng (topology) hoặc những vấn đề tổ chức của chinhs cơ sở. Việc chia thành những mạng con làm giảm việc quản trị các máy một cách tập trung. Với cách đánh địa chỉ chuẩn, người quản trị chịu trách nhiệm quản trị cho tất cả địa chỉ máy trên mạng. Bằng cách tạo các mạng con, thì một số bộ phận của mạng tự chịu trách nhiệm quản trị các máy trong mạng con của mình.

Việc chia thành các mạng con có thể được sử dụng để vượt qua sự khác biệt về phần cứng hay khoảng cách giữa các máy. Các cổng dẫn đường IP có thể liên kết các mạng vật lý khác nhau nếu mỗi mạng vật lý có địa chỉ mạng riêng. Việc phân chia một mạng thành nhiều mạng con tạo cho các mạng con một địa chỉ mạng riêng.

Một mạng con được xác định nhờ một số che bit (bit mask) trên địa chỉ IP. Nếu như bit tương ứng trên số che bit được bật (có giá trị bằng 1) thì bit tương ứng trên địa chỉ IP được hiểu là bit của địa chỉ mạng. Còn bit tương ứng trên số che bit bị tắt (có giá trị bằng 0) thì bit tương ứng trên địa chỉ IP được hiểu là bit của địa chỉ máy. Địa chỉ của mạng con được xác định nhờ số che bit chỉ có giá trị cục bộ, đối với toàn bộ phần còn lại của Internet thì địa chỉ được hiểu như là địa chỉ IP chuẩn.

Ví dụ một cơ sở nhỏ có địa chỉ nhóm C có thể sử dụng số che bit là 255.255.255.192 để chia địa chỉ mạng thành 4 địa chỉ mạng con. Mạng 1 có địa chỉ máy từ 0 - 63, mạng 2 có địa chỉ máy từ 64 - 127, mạng 3 có địa chỉ máy từ 128 - 191, và mạng 4 có địa chỉ máy từ 192 - 255 (trong trường hợp này thì hai mạng con có địa chỉ từ 0 - 63 và 192 - 255 không được sử dụng vì địa chỉ mạng toàn 0 hay toàn 1).

3.4 Nhược điểm của cách đánh địa chỉ Internet

Địa chỉ Internet có một vài nhược điểm. Nhược điểm dễ thấy nhất là địa chỉ hướng tới đường liên kết chứ không hướng tới máy. nếu máy chuyển từ mạng này sang mạng khác thì địa chỉ IP của nó phải được thay đổi. Chúng ta xét trường hợp, một người có một máy tính cầm tay đang được gắn với một mạng, như vậy máy này đang được gán cho một địa chỉ IP, do điều kiện làm việc người này chuyển máy của mình đến một nơi mới với một mạng vật lý mới. Nhưng do không thể gán địa chỉ IP thường xuyên cho máy, máy này phải đổi địa chỉ IP khi đến nơi làm việc mới cho phù hợp với địa chỉ của mạng vật lý mới.

Một nhược điểm nữa của hệ thống địa chỉ Internet là địa chỉ nhóm C là địa chỉ được dùng phổ biến nhất. Nhưng khi mạng với địa chỉ nhóm C phát triển lên trên 255 máy, địa chỉ của mạng bắt buộc phải đổi thành địa chỉ nhóm B. Điều này có thể là một vấn đề nhỏ nhưng thật ra đổi địa chỉ cho tất cả các máy trong mạng là một việc tiêu tốn nhiều thời gian, và nhiều khi không dễ gì tìm ra lỗi. Người quản trị của mạng đó bắt buộc phải dừng hoạt động của mạng, đổi địa chỉ của tất cả các máy, sau đó phục hồi lại các đường truyền sử dụng địa chỉ Internet.

Một nhược điểm khác trong hệ thống địa chỉ Internet không dễ thấy khi chúng ta khảo sát việc vạch đường dẫn. Vì việc vạch đường dẫn từ mạng này tới mạng khác dựa trên phần địa chỉ mạng trong địa chỉ IP, đối với máy có hai địa chỉ IP thì việc vạch đường dẫn dẫn đến máy đó phụ thuộc vào địa chỉ IP đang dùng.

3.5 Trật tự byte trong mạng

Để tạo Internet độc lập với tất cả các kiến trúc máy của các nhà sản xuất hoặc phần cứng mạng. Các nhà thiết kế phải xác định một biểu diễn chuẩn cho dữ liệu . Xét trường hợp, khi một máy chuyển một số nguyên 32 bit đến máy khác. Phần cứng vận tải của mạng chuyển dãy các bit từ máy gửi đến máy nhận mà không thay đổi trật tự gửi. Tuy nhiên, không phải tất cả các máy đều lưu số nguyên 32 bit theo cùng một cách. Trên một số máy (gọi là Litle Endian), địa chỉ thấp nhất

chứa byte bậc thấp của số nguyên. Trên máy khác (gọi là Big Endian), địa chỉ thấp nhất chứa byte bậc cao của số nguyên. Do vậy, việc sao trực tiếp các byte từ máy này sang máy khác có thể làm thay đổi giá trị của số.

Trật tự byte chuẩn cho các số nguyên là đặc biệt quan trọng trong Internet vì các gói tin chứa các số nhị phân chỉ thông tin như địa chỉ đích, độ dài gói tin. Các giá trị này phải được hiểu như nhau đối với cả nơi gửi và nơi nhận. Các giao thức TCP/IP giải quyết vấn đề này bằng cách xác định trật tự byte chuẩn trong mạng và tất cả các máy phải sử dụng cho các trường nhị phân trong các gói tin. Mỗi máy chuyển các giá trị nhị phân t ừ biểu diễn cục bộ của máy sang biểu diễn chuẩn trong mạng khi gửi gói tin đi, và chuyển từ biểu diễn chuẩn trong mạng sang biểu diễn địa phương của máy khi nhận gói tin.

Chuẩn Internet đối với trật tự byte chỉ rằng các số nguyên được gửi với các byte quan trọng nhất trước (tức là theo Big Endian).

CHƯƠNG 4. TƯƠNG ỨNG ĐỊA CHỈ INTERNET VỚI ĐỊA CHỈ VẬT LÝ

4.1 Giới thiệu

Trong sơ dồ địa chỉ TCP/IP, mỗi máy được gắn một địa chỉ 32 bit và mạng Internet như là một mạng ảo khi chỉ sử dụng địa chỉ này để gửi và nhận các gói tin. và chúng ta cũng biết rằng hai máy trên cùng một mạng vật lý có thể trao đổi được với nhau khi và chỉ khi chúng biết các địa chỉ vật lý của nhau. Vấn đề là làm cách nào các máy và các cổng dẫn đường tương ứng địa chỉ IP đến đúng địa chỉ vật lý khi chúng cần gửi các gói tin qua mạng vật lý.

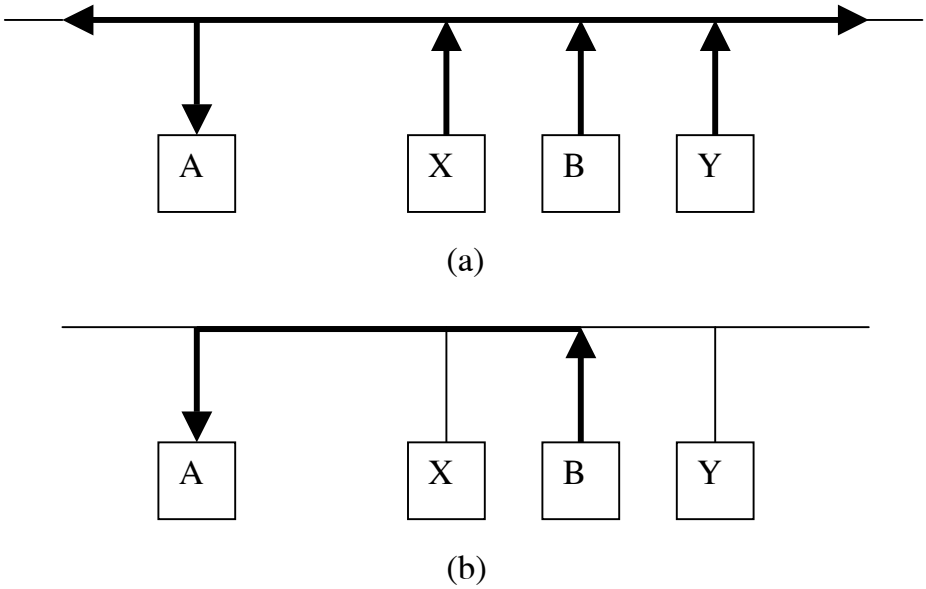
Xét hai máy A và B có chung một mạng vật lý. Mỗi máy có địa chỉ IP là I_A và I_B và địa chỉ vật lý P_A và P_B. Mục đích là tạo một phần mềm ở mức thấp, phần mềm che các địa chỉ vật lý và cho phép các chương trình ở mức cao chỉ làm việc với các địa chỉ IP. Tuy nhiên, cuối cùng việc truyền thông phải được thực hiện trong mạng vật lý nhờ sử dụng địa chỉ vật lý mà phần cứng cung cấp. Giả thiết là máy A muốn gửi gói tin đến máy B qua mạng vật lý mà cả hai máy đang nối vào, nhưng máy A chỉ biết địa chỉ Internet I_B của máy B. Câu hỏi đặt ra là: làm cách nào máy A tương ứng địa chỉ I_B của máy B tới địa chỉ vật lý P_B của nó.

Vấn đề tương ứng địa chỉ mức cao IP tới địa chỉ vật lý được biết là vấn đề giải quyết địa chỉ và ddã được giải quyết nhờ nhiều cách. Một số thủ tục giữ các bảng trong mỗi máy, và bảng đó chứa các địa chỉ mức cao và mức thấp. Một số thủ tục khác giải quyết vấn đề bằng cách mã các địa chỉ vật lý trong các địa chỉ mức cao. Chương này sẽ giải quyết vấn đề nêu trên.

4.2 Giải quyết nhờ tương ứng động

Các nhà thiết kế các giao thức TCP/IP đã tìm ra một giải pháp sáng tạo cho vấn đề giải quyết địa chỉ cho các mạng như Ethernet có khả năng truyền thông rộng rãi. Giải pháp cho phép các máy mới thêm vào mạng mà không cần phải biên dịch lại các mã nguồn, và không cần duy trì một cơ sở dữ liệu trung tâm. Để tránh duy trì bảng các tương ứng địa chỉ, các nhà thiết kế đã chọn sử dụng giao thức bậc thấp để gắn địa chỉ một cách động. Giao thức Giải quyết địa chỉ - Address Resolution Protocol (ARP) cung cấp cơ chế hiệu quả và dễ duy trì cho giải pháp.

Tư tưởng của giao thức ARP là đơn giản và có thể thấy trong hình 4.1: khi máy A muốn giải quyết địa chỉ Internet I_B của máy B, nó truyền thông rộng rãi một gói tin đặc biệt hỏi máy có địa chỉ Internet I_B gửi trả lời có địa chỉ vật lý P_B. Tất cả các máy trong mạng đều nhận được yêu cầu (do khả năng truyền thông rộng rãi), nhưng chỉ máy B công nhận địa chỉ IP nhận được và gửi câu trả lời có chứa địa chỉ vật lý của nó. Khi máy A nhận được câu trả lời, nó sử dụng địa chỉ vật lý để gửi gói tin trực tiếp đến máy B. Như vậy, Giao thức Giải quyết Địa chỉ ARP cho phép một máy tìm được địa chỉ vật lý của máy đích trên cùng một mạng vật lý khi biết địa chỉ IP của máy đích.



Hình 4.1 Giao thức ARP. Để xác định địa chỉ vật lý P_B của máy B khi biết địa chỉ Internet I_B, (a) máy A truyền thông rộng rãi một yêu cầu ARP chứa địa chỉ I_B tới mọi máy, và (b) máy B trả lời bằng một gói tin ARP có chứa cặp địa chỉ (I_B, P_B).

4.3 Cache giải quyết địa chỉ

Truyền thông rộng rãi tiêu tốn nhiều thời gian của các máy trên mạng, vì nó yêu cầu tất cả các máy trong mạng đều phải giải quyết vấn đề. Để giảm chi phí cho truyền thông, máy sử dụng giao thức ARP duy trì một nơi cất giữ (cache) của những cặp địa chỉ IP - địa chỉ vật lý tìm được sao cho không phải sử dụng giao thức ARP lặp đi lặp lại. Mỗi khi máy nhận được trả lời ARP, nó lưu địa chỉ IP và địa chỉ vật lý tương ứng trong một nơi đặc biệt để tìm sau này. Khi máy cần phải tìm một địa chỉ vật lý mới, trước hết nó tìm ở nơi cất giữ, nếu không thấy thì nó mới gửi gói tin ARP đi. Kinh nghiệm chỉ ra rằng dù chỉ một nơi cất giữ (cache) nhỏ thôi cũng có giá trị. Do có nơi cất giữ cặp địa chỉ IP - địa chỉ vật lý, có cách để làm cho giao thức ARP tinh tế hơn. Khi máy gửi gửi gói tin ARP, nó gửi luôn cặp địa chỉ IP-địa chỉ vật lý của nó để các máy nhận cập nhật luôn thông tin nơi cất giữ các cặp địa chỉ trước khi xử lý gói tin ARP để tránh khỏi phải gửi nhiều gói tin ARP sau này.

4.4 Thực hiện của giao thức ARP

Sự thực hiện truyền thông rộng rãi yêu cầu ARP để tìm sự tương ứng địa chỉ có thể trở thành phức tạp. Máy đích có thể đã tắt hoặc bận không trả lời. Nếu như vậy, máy yêu cầu không nhận được câu trả lời hoặc câu trả lời bị chậm. Do Ethernet là hệ thống gửi có cố gắng tốt nhất, yêu cầu ARP truyền thông rộng ban đầu có thể bị mất (khi đó máy gửi phải gửi lại yêu cầu). Do vậy, máy gửi phải lưu lại gói tin đã gửi để nó có khả năng gửi lại. Thật ra, máy phải quyết định khi nào cho phép các chương trình ứng dụng tiếp tục trong khi nó xử lý yêu cầu ARP.

Cuối cùng, xét trường hợp khi máy A đã nhận được cặp địa chỉ tương ứng của máy B, nhưng phần cứng của máy B bị hỏng, hoặc bị thay thế. Mặc dù địa chỉ của máy B đã bị thay thế, song nơi cất giữ địa chỉ cache của máy A chưa kịp cập nhật làm cho không thể thực hiện được việc nhận. Trường hợp này chỉ ra rằng, phần mềm ARP coi bảng tương ứng địa chỉ như nơi cất giữ và bỏ đi những cặp tương ứng sau những khoảng thời gian cố định. Như vậy phải thiết lập lại thời gian cho cặp lưu trong cache khi một yêu cầu ARP mới chuyển đến chứa cặp địa chỉ tương ứng.

Máy nhận phải giải quyết hai dạng của gói tin ARP. Nếu như gói tin ARP là yêu cầu, máy nhận phải xét xem nó có phải là máy đích không. Nếu phải, phần mềm ARP hình thành câu trả lời bằng cách cung cấp địa chỉ vật lý của nó, và gửi gói tin trả lời thẳng đến máy yêu cầu. Đồng thời máy nhận cũng cập nhật cặp địa chỉ tương ứng của máy gửi nếu như cặp đó không có trong cache. Nếu như địa chỉ IP chứa trong yêu cầu không phù hợp với địa chỉ IP của máy nhận, thì gói tin ARP coi như không được để ý đến.

4.5 Tóm tắt

Các địa chỉ IP được gán độc lập với địa chỉ vật lý của máy. Để gửi gói tin Internet, phần mềm mạng phải tương ứng địa chỉ IP với địa chỉ vật lý để gửi gói dữ liệu. Giao thức Giải quyết Địa chỉ ARP thực hiện việc giải quyết động sử dụng hệ truyền thông ở mức thấp.

Một máy sử dụng ARP tìm địa chỉ phần cứng của máy khác bằng cách truyền thông rộng rãi yêu cầu ARP. Trong yêu cầu có chứa địa chỉ IP phù hợp với máy của mình thì gửi gói tin ARP trả lời về cho máy yêu cầu. Để cho giao thức ARP hiệu quả, mỗi máy lưu cặp địa chỉ IP-địa chỉ vật lý vào một nơi (cache). Cache có khả năng làm giảm nhiều yêu cầu truyền thông rộng rãi.

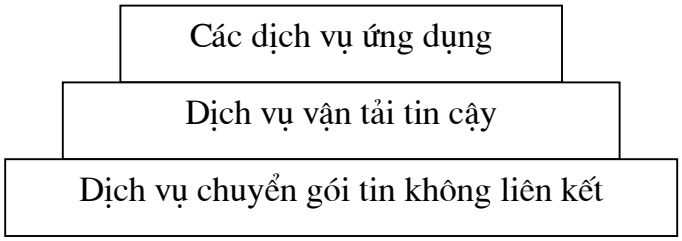
CHƯƠNG 5. GIAO THỨC INTERNET: CHUYỂN GÓI TIN KHÔNG CÓ LIÊN KẾT

5.1 Giới thiệu

Chương này xem xét yêu tố cơ bản của chuyển không liên kết và thảo luận dịch vụ được giao thức Internet (IP) cung cấp như thế nào, giao thức IP là một trong hai giao thức chính được sử dụng trong liên mạng. Định dạng của các gói tin IP sẽ được nghiên cứu và chúng ta sẽ thấy chúng hình thành nên cơ sở cho toàn bộ truyền thông của Internet. Sau đó chúng ta sẽ xét cách mà các cổng dẫn đường chuyển các gói tin đến đích.

5.2 Kiến trúc của Internet và tính triết học

Một cách khái niệm, TCP/IP Internet cung cấp ba nhóm dịch vụ như được chỉ ra trong hình 5.1. Sự xếp đặt trong hình chỉ ra tính phụ thuộc giữa chúng. ở tầng thấp nhất, dịch vụ chuyển gói tin không liên kêt cung cấp cơ sở cho tất cả các dịch vụ khác. Tại tầng cao hơn, dịch vụ vận tải tin cậy cung cấp cơ sở cao hơn cho các dịch vụ.



Hình 5.1 Ba tầng khái niệm của dịch vụ Internet

Chúng ta có thể tạo quan hệ cho phần mềm giao thức với từng dịch vụ trong hình 5.1. Phần mềm Internet được thiết kế xung quanh ba dạng dịch vụ liên mạng có tính khái niệm trên; nhiều thành công đạt được từ kiến trúc đó vì kiến trúc này mạnh và có tính thích nghi. Một trong những ưu điểm quan trọng của sự phân chia có tính khái niệm này là có thể thay một dịch vụ mà không làm ảnh hưởng tới các dịch vụ khác.

5.3 Hệ thống chuyển không liên kết

Dịch vụ Internet cơ bản nhất là hệ thống chuyển gói tin. Một cách kỹ thuật, dịch vụ này được xác định là không chắc chắn, cố gắng nhất, là hệ thống chuyển gói tin không liên kết.

- Dịch vụ này được gọi là không chắc chắn vì nó không đảm bảo việc chuyển tới đích. Một gói tin có thể bị mất, lặp lại, chậm, hoặc chuyển không đúng thủ tục. Nhưng dịch vụ không phát hiện những điều đó, và không thông báo cho cả nơi gửi và nơi nhận.

- Dịch vụ này không liên kết vì mỗi gói tin được coi là độc lập với các gói tin khác. Một dãy các gói tin được chuyển từ máy này tới máy khác có thể đi theo nhiều đường, hoặc một số có thể bị mất trong khi các gói tin khác thì đến đích.
- Cuối cùng, dịch vụ được coi là chuyển cố gắng nhất vì phần mềm thực hiện cố gắng một cách xác định, nghiêm chỉnh để chuyển gói tin.

Như vậy Internet không hề loại bỏ gói tin một cách không báo trước, sự không chắc chắn chỉ xảy ra khi các tài nguyên trên mạng bị dùng hết hoặc phần cứng bên dưới bị hỏng.

5.4 Mục đích của giao thức Internet

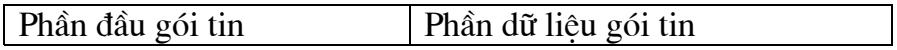
Giao thức xác định cơ cấu chuyển không chắc chắn, không liên kết là giao thức Internet và thường được gọi là Giao thức IP. Giao thức IP xác định ba định nghĩa quan trọng.

- Trước hết, nó xác định đơn vị cơ sở của truyền dữ liệu được sử dụng qua TCP/IP Internet. Tức là, nó xác định định dạng chính xác của tất cả dữ liệu khi chuyển qua TCP/IP Internet.
- Thứ hai, phần mềm IP thực hiện chức năng vạch đường, chọn đường đi mà dữ liệu sẽ được gửi.
- Thứ ba, giao thức IP bao gồm một tập các quy định chứa tư tưởng chuyển gói tin không chắc chắn. Những quy định này chỉ ra đặc tính các máy và cổng vạch đường nên xử lý gói tin như thế nào, khi nào thì tạo thông báo lỗi, và dưới điều kiện nào thì bỏ gói tin.

Giao thức IP là phần cơ bản của thiết kế Internet, do vậy đôi khi người ta gọi TCP/IP Internet là công nghệ dựa trên IP.

5.5 Gói tin Internet

Một gói tin là một khối dữ liệu cùng với thông tin cần thiết để truyền nó. Khái niệm này cũng tương đương như bức thư bưu điện, mỗi bức thư có nội dung và địa chỉ là thông tin cần thiết để chuyển bức thư tới đích. Mạng sử dụng thông tin địa chỉ cần thiết để chuyển gói tin từ mạng vật lý này tới mạng vật lý khác và dần dần tới đích. Mỗi gói tin di chuyển không phụ thuộc vào các gói tin khác. Hình 5.2 chỉ dạng tổng quát của gói tin:

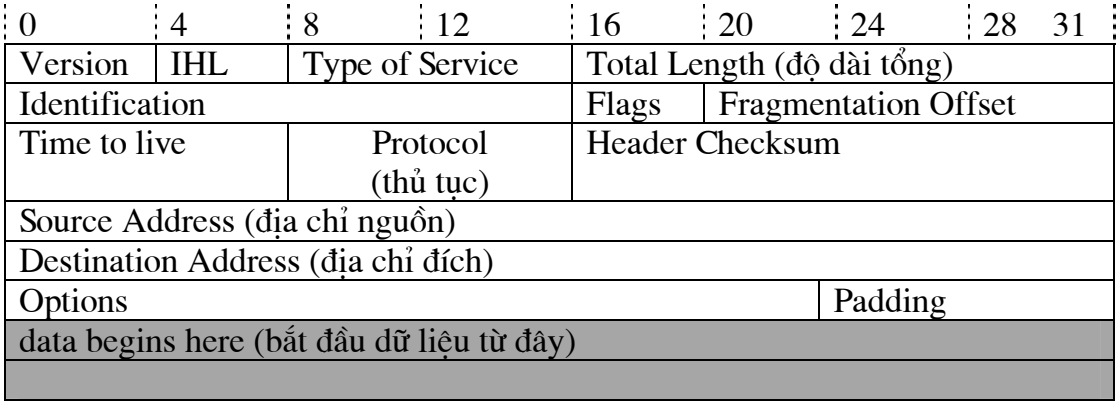


Hình 5.2 Dạng tổng quát của gói tin IP

Định dạng của gói tin

Hình 5.3 miêu tả các trường của gói tin IP. Gói tin định dạng bằng giao thức Internet được miêu tả trong hình 5.3. Năm hoặc sáu từ (mỗi từ gồm 32 bit) đầu tiên của mỗi gói tin là thông tin điều khiển còn gọi là đầu. Theo ngầm định đầu chứa năm từ 32 bit, trường hợp đầu có chứa sáu từ 32 bit là trường hợp tuỳ chọn. Bởi vì

độ dài của đầu không cố địnhnên trường có tên "độ dài đầu Internet" (Internet Header Length (IHL)) gồm 4 bit sẽ chỉ ra độ dài của đầu. Tất cả thông tin điều khiển cần thiết để truyền gói tin đến đích đều được chứa trong đầu. Trường độ dài tổng - Total Length chứa độ dài của gói tin IP được đo theo số byte, bao gồm cả số byte của đầu và dữ liệu. Do vậy, kích thước của dữ liệu có thể tính đượcbằng cách lấy độ dài tổng trừ đi độ dài đầu. Thủ tục IP truyền gói tin dựa trên địa chỉ đích được chứa trong từ thứ năm của đầu. Địa chỉ đích chính là dịa chỉ Internet 32 bit của đích. Nếu như địa chỉ đích là địa chỉ của máy cùng mạng với máy gửi thì gói tin được gửi trực tiếp đến đích. Nếu như địa chỉ đích không cùng mạng cục bộ với địa chỉ của máy gửi thì gói tin được gửi đến cổng dẫn đường (Gateway) để truyền. Cổng dẫn đường chính là những phương tiện kỹ thuật để chuyển gói tin giữa những mạng vật lý khác nhau. Để xác định gói tin được gửi đến cổng nào là nhờ đường dẫn. Thủ tục IP quyết định đường dẫn cho mỗi gói tin.



Hình 5.3 Định dạng gói tin của IP

5.6 Kích thước của gói tin, MTU mạng và phân đoạn

Khi xét đến kích thước của gói tin IP, câu hỏi đặt ra là:" gói tin có thể lớn bao nhiêu?" không giống như kích thước của gói dữ liệu của mạng vật lý do phần cứng công nhận, gói tin IP do phần mềm điều khiển. Độ dài của gói tin do các nhà thiết kế giao thức chọn. Chúng ta thấy rằng trong định dạng của gói tin, phần độ dài gói tin gồm 16 bit, do vậy gói tin có độ dài không được lớn hơn 65.535 byte. Tuy nhiên, giới hạn độ dài có thể thay đổi.

Trong trường hợp lý tưởng, toàn bộ một gói tin IP phù hợp với một gói dữ liệu vật lý, giúp cho việc truyền dọc theo mạng vật lý có hiệu quả. Trong công nghệ chuyển gói tin, có giới hạn trên cố định cho các gói dữ liệu vật lý. Ví dụ, trong mạng Ethernet giới hạn để chuyển mỗi gói dữ liệu là 1500 byte. Chúng ta gọi giới hạn đó là Đơn vị Truyền tin lớn nhất - Maximum Transfer Unit (MTU).

Khi các gói tin được di chuyển qua các mạng khác nhau, có khi các cổng phải chia gói tin thành các phần nhỏ hơn. Bởi vì một gói tin được nhận từ một mạng có thể quá lớn để chuyển như một gói trong mạng đó. Trường hợp này chỉ xảy ra khi cổng liên kết các mạng vật lý khác nhau.

Đối với TCP/IP, phần mềm chọn một kích thước gói tin thuận tiện và xếp đặt cách để chia các gói tin lớn thành nhuững phần nhỏ hơn khi gói tin cần truyền qua mạng có MTU nhỏ. Những phần nhỏ mà một gói tin bị chia gọi là các đoạn, quá trình chia một gói tin được biết là phân đoạn.

Giao thức IP không giới hạn kích thước nhỏ của gói tin, cũng không đảm bảo là các gói tin lớn sẽ được truyền mà không phân đoạn. Phần chương trình nguồn có thể chọn bất kỳ kích thước nào mà nó cho là phù hợp; việc phân đoạn và hợp lại xảy ra tự động. Chỉ dẫn IP nói rằng các cổng dẫn đường phải chấp nhận các gói tin có kích thước không lớn hơn MTU của mạng vật lý mà nó đang nối vào. Hơn nữa, các cổng dẫn đường phải luôn xử lý các gói tin lớn đến 576 byte.

Việc phân đoạn gói tin có nghĩa là chia gói tin thành nhiều gói tin nhỏ. Mỗi gói tin nhỏ có cùng định dạng như gói gốc. Và các gói tin được hợp lại tại máy đích. Từ thứ hai trong định dạng của gói tin IP (hình 5.3) xác định gói tin có bị chia hay không và chứa đủ thông tin liên kết lại gói tin đã bị chia. Trường "Identification" xác định gói tin nào bị chia và trường "Fragmentation Offset" xác định vị trí của gói tin con trong gói tin đã bị chia, còn trường "Flags" để chỉ rằng các gói tin đã được liên kết hết chưa.

5.7 Vạch đường dẫn trong Internet

Trong hệ thống chuyển gói tin, việc vạch đường dẫn là quá trình chọn đường để gửi gói tin, và bộ định tuyến (router) là một máy tính bất kỳ làm chức năng vạch đường dẫn.

Các cổng Internet dùng thủ tục IP để xác định đường dẫn cho các gói tin giữa các mạng. Trong truyền thống thuật ngữ của TCP/IP, chỉ có hai phương tiện kỹ thuật trong mạng là các cổng dẫn đường (gateways) và các máy tính chủ (hosts). Các cổng có nhiệm vụ truyền các gói tin giữa các mạng, còn các máy tính thì không có nhiệm vụ đó. Tuy nhiên, những máy tính được nối với hai mạng hay hơn thì chúng có thể truyền các gói tin giữa các mạng, và trong trường hợp này các máy tính đó có thể được gọi là cổng.

Trong lĩnh vực truyền dữ liệu, người ta phân biệt giữa cổng dẫn đường (gateway) và bộ định tuyến (router). Trong thuật ngữ ngày nay, cổng dùng để chuyển dữ liệu giữa các mạng có cấu trúc thủ tục khác nhau, còn bộ định tuyến để chuyển dữ liệu giữa các mạng khác nhau. Trong tài liệu này chúng ta không phân biệt hai thuật ngữ này.

Trong quá trình chuyển gói tin từ máy đầu đến máy cuối, các máy tính (máy cuối) xử lý các gói tin qua cả bốn lớp thủ tục, trong khi các cổng hay các hệ thống trung gian chỉ xử lý gói tin cho đến lớp Internet là nơi đường dẫn được vạch ra.

Thuật toán vạch đường dẫn IP thường khai thác bảng đường dẫn Internet (đôi khi gọi là bảng đường dẫn IP) trên mỗi máy, các máy này chứa thông tin về đích và làm thế nào tới được đích. Khi phần mềm IP trong máy hay cổng dẫn đường cần chuyển gói tin, nó hỏi bảng đường dẫn để quyết định gửi gói tin đi đâu.

Một cách tiêu biểu, một bảng đường dẫn chứa các cặp (N,G), với N là địa chỉ IP của mạng đích, còn G là địa chỉ IP của cổng dẫn đường "tiếp theo" trên đường tới mạng N. Như vậy bảng đường dẫn trong cổng dẫn đường chỉ vạch một bước dọc theo đường tới mạng đích. Cổng dẫn đường không biết toàn bộ đường tới đích.

Thuật toán để vạch đường dẫn IP có thể xem trong bảng 5.1

Thuật toán:

Vạch_đường_gói_tin_IP(gói_tin, bảng_đường_dẫn)

Lấy địa chỉ đích IP từ gói tin I_D
Tính địa chỉ IP của mạng đích, I_N
If (I_N=bất kỳ địa chỉ mạng nào nối trực tiếp)
    gửi gói tin đến đích qua mạng đó;
elsse if (I_D=đường dẫn đến máy riêng)
    gửi gói tin theo đường dẫn riêng trong bảng;
elsse if (I_N là đường dẫn trong bảng)
    gửi gói tin theo đường dẫn trong bảng;
elsse if (đường dẫn ngầm định đã được chỉ ra)
    gửi gói tin đến cổng ngầm định;
else thông báo lỗi;

Bảng 5.1 Thuật toán vạch đường dẫn

5.8 Cấu trúc vạch đường dẫn của Internet

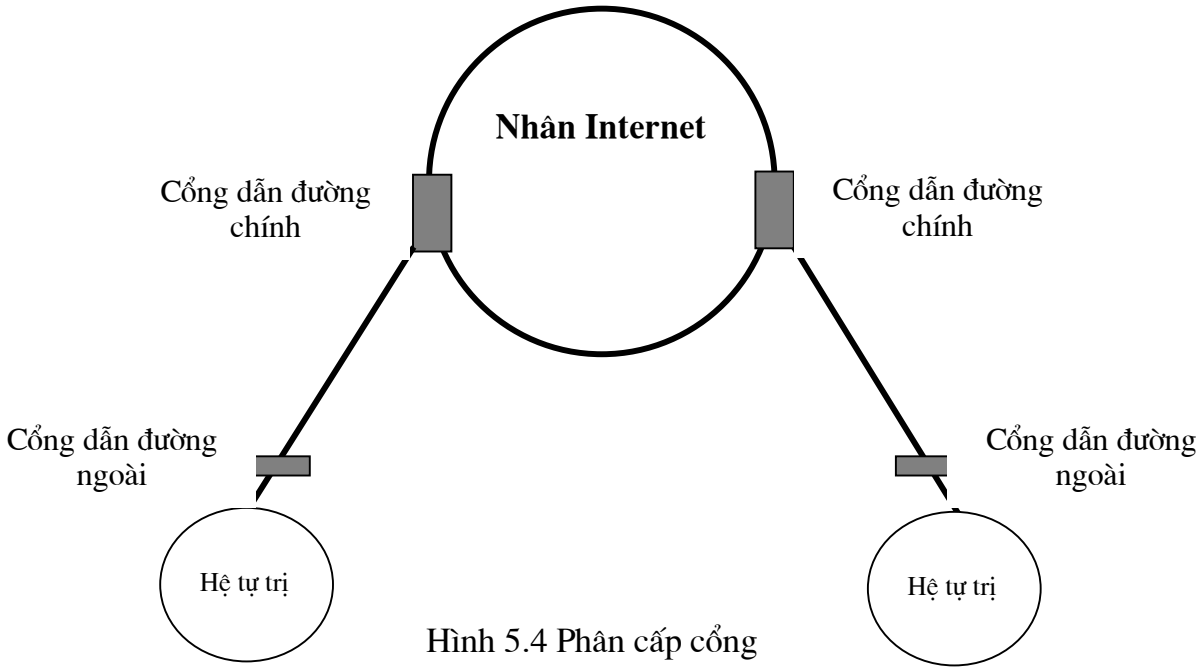
Trong cấu trúc truyền thống của Internet, có sự phân cấp của các cổng dẫn đường. Sự phân cấp này phản ánh lịch sử của Internet, vì Internet được xây dựng trên cơ sở của mạng ARPANET. Khi Internet được tạo ra, mạng ARPANET là xương sống của mạng Internet: đó chính là trung tâm truyền thông để truyền dữ liệu với khoảng cách xa. Hệ thống trung tâm đó được gọi là Nhân, và các cổng dẫn đường của Nhân được gọi là các cổng dẫn đường chính.

Khi cấu trúc phân cấp được sử dụng, thông tin dẫn đường về toàn bộ các mạng trong Internet được chuyển đến cho các cổng dẫn đường chính. Các cổng dẫn đường chính xử lý những thông tin này, và sau đó trao đổi thông tin này với nhau sử dụng thủ tục cổng tới cổng (Gateway to Gateway Protocol (GGP). Sau đó

những thông tin dẫn đường được chuyển lại cho các cổng ở ngoài. Do vậy không thể kích hoạt các thủ tục GGP trên các cổng cục bộ.

Ngoài Nhân của Internet là các nhóm của các mạng độc lập gọi là các hệ tự trị (Autonomous system (AS). Một hệ tự trị không chỉ đơn giản là một mạng độc lập, đó là tập các mạng và cổng dẫn đường với cấu trúc riêng bên trong để thu thập thông tin dẫn đường và có khả năng chuyênr thông tin đó cho các hệ mạng độc lập khác. Thông tin được chuyển đến hệ mạng khác được gọi là thông tin tới được. Thông tin tới được thông báo mạng nào có thể chuyển thông tin tới qua hệ tự trị. Thủ tục cổng ngoài (Exterior Gateway Protocol (EGP))đang được sử dụng nhiều nhất để chuyển thông tin giữa các hệ tự trị. (Xem hình 5.4).

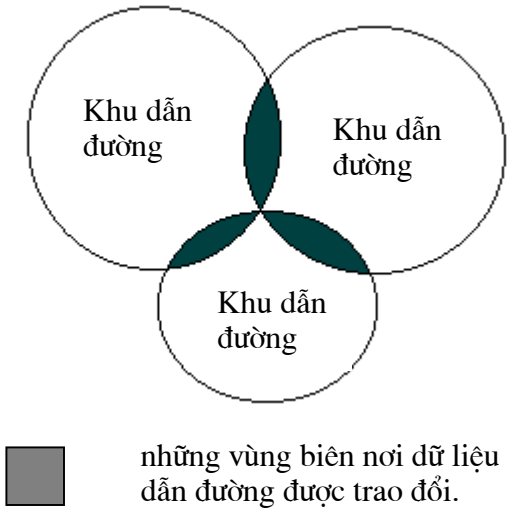
Mô hình phân cấp này có nhược điểm là mỗi đường đi phải được Nhân xử lý. Điều này làm cho Nhân của Internet phải xử lý rất nhiều thông tin, và khi Internet lớn lên, thì những thông tin mà Nhân phải xử lý cũng tăng nhanh chóng. Một mô hình mới ra đời.



Hình 5.4 Phân cấp cổng

Mô hình đường dẫn mới này dựa trên tập các hệ tự trị có quyền như nhau, được gọi là các khu dẫn đường. Các khu dẫn đường trao đổi thông tin dẫn đường với nhau nhờ thủ tục cổng biên (Border Gateway Protocol (BGP)). Mỗi khu dẫn đường xử lý thông tin nhận được từ khu dẫn đường khác. Không giống như mô hình phân cấp, mô hình này không phụ thuộc vào một hệ nhân riêng nào để chọn đường đi tốt nhất. Mỗi khu dẫn đường thực hiện việc xử lý thông tin cho chính nó; do vậy mô hình này có khả năng mở rộng. Hình 5.5 thể hiện mô hình này với ba vòng tròn, mỗi vòng tròn là một khu dẫn đường. Các vùng giao nhau là các vùng biên, ở đó các thông tin dẫn đường được dùng chung. Các khu dẫn đường dùng

chung thông tin, nhưng không dựa vào một hệ để cung cấp tất cả thông tin dẫn đường.



Hình 5.5 Các khu dẫn đường

5.9 Giải quyết các gói tin đến

Khi gói tin IP đến một máy, phần mềm giao diện mạng chuyển nó tới phần mềm IP để xử lý tiếp. Nếu như địa chỉ đích của gói tin phù hợp với địa chỉ IP của máy, phần mềm IP trên máy chấp nhận gói tin và chuyển nó tới phần mềm giao thức bậc cao (tầng vận tải) để tiếp tục xử lý. Nếu như địa chỉ IP không phù hợp, thì máy này phải bỏ gói tin (các máy tính bình thường không gửi gói tin tình cờ gửi đến chúng).

Khi lớp IP nhận được gói tin gửi cho chính máy chủ đó, nó phải gửi phần dữ liệu của gói tin đến thủ tục chính xác của lớp vận tải. Điều này có thể thực hiện được nhờ giá trị của trường số thủ tục "Protocol" trong từ thứ ba của gói tin IP (hình 5.3). Vì mỗi thủ tục trong lớp vận tải có một giá trị duy nhất, xác định đối với lớp IP.

Không giống như máy tính bình thường, các cổng dẫn đường thực hiện chuyển tiếp. Khi gói tin IP đến cổng dẫn đường, gói tin được chuyển đến phần mềm IP. Lúc này có hai trường hợp: gói tin có thể đã tới đích, hoặc nó cần phải chuyển tiếp. Cũng như trong trường hợp máy tính bình thường, nếu địa chỉ IP của gói tin phù hợp với địa chỉ của cổng, phần mềm IP chuyển gói tin lên cho phần mềm của giao thức bậc cao hơn để xử lý tiếp. Nếu như địa chỉ IP không phù hợp, phần mềm IP chuyển gói tin đi tiếp nhờ sử dụng thuật toán chuẩn và thông tin trong bảng đường dẫn.

CHƯƠNG 6. GIAO THỨC INTERNET: CÁC THÔNG BÁO ĐIỀU KHIỂN VÀ BÁO LỖI

6.1 Giới thiệu

Chúng ta đã thấy rằng Giao thức Internet cung cấp dịch vụ chuyển gói tin không chắc chắn và không liên kết, hơn nữa gói tin chuyển từ cổng dẫn đường tới cổng dẫn đường cho đến khi gói tin tới cổng cuối cùng để được chuyển thẳng tới đích cuối cùng. Nếu cổng dẫn đường không thể dẫn đường hoặc chuyển gói tin, hoặc nếu như cổng dẫn đường phát hiện ra các trường hợp không bình thường, như tắc mạng làm ảnh hưởng khả năng chuyển gói tin, cổng dẫn đường cần thông báo cho nguồn gửi biết để thực hiện hành động tương ứng nhằm tránh hoặc sửa vấn đề đang xảy ra. Chương này thảo luận cơ cấu mà các cổng và các máy sử dụng để trao đổi sự điều khiển hoặc thông báo lỗi.

6.2 Giao thức thông báo điều khiển Internet

Trong hệ thống không liên kết của giao thức IP, mỗi cổng dẫn đường hoạt động tự trị, dẫn đường hoặc chuyển gói tin mà không phối hợp với nơi gửi ban đầu. Hệ thống này làm việc tốt nếu như tất cả các máy hoạt động đúng, nhưng không có hệ thống nào luôn làm việc tốt. Ngoài hỏng đường truyền, giao thức IP không thể chuyển gói tin khi máy đích tạm thời không nối với mạng hoặc giao thông bị tắc nghẽn. Sự khác nhau quan trọng giữa việc có một mạng vật lý và mạng Internet dựa trên phần mềm là trong mạng vật lý thường có thể dựa vào phần cứng mạng để thông báo cho các máy khi các vấn đề như trên xảy ra. Trong Internet, không có một cơ cấu cứng nào, nơi gửi không thể nói khi nào thì việc chuyển bị hỏng do chức năng cục bộ bị hỏng, hoặc do máy ở xa không thực hiện được.

Để cho phép các công dẫn đường trong Internet báo các lỗi hoặc cung cấp thông tin về những trường hợp không đoán được trước, các nhà thiết kế thêm một cơ cấu thông báo đặc biệt cho bộ giao thức TCP/IP. Cơ cấu này được gọi là Giao thức Thông báo điều khiển Internet - Internet Control Message Protocol (ICMP). Giao thức này được coi là một phần của Giao thức Internet, và phải có trong mọi thực hiện của giao thức IP.

Cũng giống như mọi giao thức, các thông báo của ICMP chuyển dọc Internet trong phần dữ liệu của gói tin IP. Đích cuối cùng của một thông báo ICMP không phải là một chương trình ứng dụng hoặc người sử dụng trên máy đích, mà là phần mềm giao thức Internet trên máy đích. Có nghĩa là khi thông báo lỗi ICMP đến, modul phần mềm ICMP xử lý nó.

Giao thức Thông báo điều khiển Internet cho phép các cổng gửi thông báo lỗi hoặc thông báo điều khiển đéen các cổng khác hoặc đến các máy; giao thức ICMP cung cấp sự trao đổi giữa phần mềm giao thức Internet trên máy này với phần mềm giao thức Internet trên máy khác.

Tuy nhiên, giao thức ICMP không chỉ giới hạn cho các cổng, một máy có thể sử dụng ICMP có thể trao đổi với công hoặc máy khác.

6.3 Báo lỗi và sửa lỗi

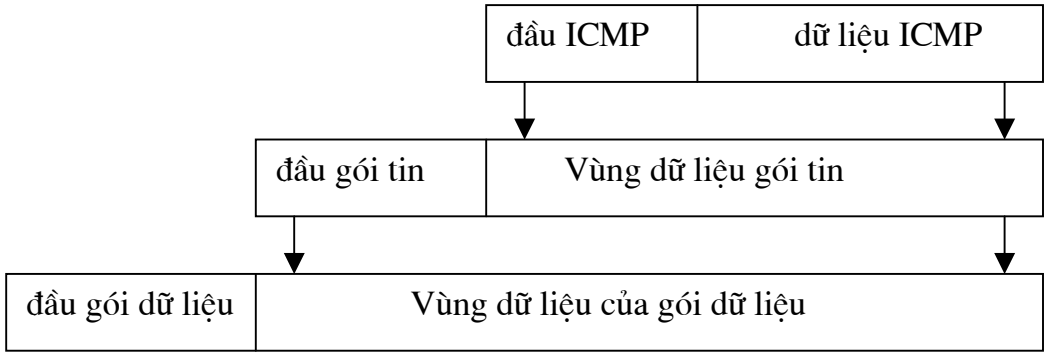
ICMP là cơ cấu báo lỗi. Giao thức này cung cấp cách để các cổng dẫn đường phát hiện ra lỗi và báo lỗi về cho nguồn ban đầu. ICMP chỉ báo lỗi cho nguồn ban đầu; nguồn phải hướng lỗi đến các chương trình ứng dụng riêng để thực hiện sửa lỗi.

Đa số các lỗi có nguồn gốc từ nguồn ban đầu, một số lỗi khác thì không do nguồn ban đầu sinh ra. Do vậy, ICMP không thể dùng để thông báo cho các cổng trung gian về các vấn đề. Ví dụ, cho rằng gói tin theo đường của một dãy các cổng dẫn đường G_1, G_2,..., G_k. Nếu G_k có thông tin dẫn đường không chính xác và gửi sai gói tin đến cổng dẫn đường G_E. G_E chỉ có thể báo lỗi về cho nguồn ban đầu của gói tin. Thật không may là nguồn ban đầu không chịu trách nhiệm gì về các vấn đề của các cổng trung gian. Thực ra, nguồn ban đầu cũng không có khả năng xác định cổng nào tạo ra lỗi.

Vì sao giao thức ICMP chỉ trao đổi với nguồn ban đầu? Điều này sinh ra dó định dạng của gói tin và cách vạch đường dẫn của IP. Gói tin chỉ chứa địa chỉ ban đầu và địa chỉ đích, gói tin không chứa toàn bộ đường đi. Hơn nữa các cổng có thể thiết lập và thay đổi các bảng dẫn đường, không có một thông tin tổng thể về toàn bộ các đường đi. Do vậy, khi cổng phát hiện một vấn đề, cổng không thể biết toàn bộ các máy trung gian đã xử lý gói tin, và cổng chỉ có thể sử dụng giao thức ICMP để báo cho nguồn ban đầu biết vấn đề đã xảy ra, và tin là người quản trị của máy sẽ hợp tác với các người quản trị mạng phát hiện và sửa lỗi.

6.4 Chuyển thông báo ICMP

Các thông báo ICMP yêu cầu hai tầng bao bọc dữ liệu như hình trong hình 6.1. Thông báo ICMP được bao bọc trong gói tin IP, đến lượt gói tin IP được bao bọc trong gói dữ liệu của mạng vật lý để truyền.

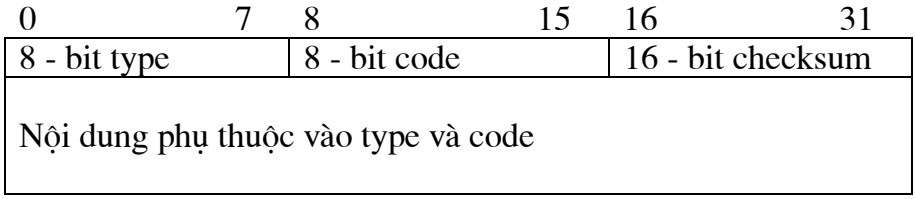


Hình 6.1 Hai tầng bao bọc dữ liệu của ICMP

Điều quan trọng phải chú ý là, mặc dù thông báo ICMP được bao bọc trong gói tin IP, giao thức ICMP không phải là giao thức tầng cao hơn giao thức IP, đó là một phần của giao thức IP. Lý do sử dụng IP để chuyển thông báo ICMP là các thông báo có thể phải truyền qua nhiều mạng vật lý để tới đích, do vậy chúng không thể chuyển chỉ bằng phần mạng vật lý.

6.5 Định dạng của thông báo ICMP

Mặc dù mỗi thông báo ICMP có định dạng riêng, tất cả các thông báo đều bắt đầu bởi 3 trường (xem hình 6.2): Một số nguyên 8 bit xác định dang (TYPE) của thông báo, và một số nguyên 8 bit (CODE) xác định thông tin thêm về từng dạng, và một tổng kiểm tra (CHECKSUM) gồm 16 bit, ICMP tổng kiểm tra chỉ tính cho thông báo của ICMP. ICMP thông báo lỗi luôn chứa đầu và 64 bit dữ liệu đầu của gói tin đã sinh ra lỗi.



Hình 6.2 Định dạng của thông báo ICMP

Dựa trên các giá trị của TYPE và CODE mà thông báo ICMP báo các dạng thông báo và lỗi khác nhau, sau đây là một số chức năng chính của giao thức ICMP.

Điều khiển dòng thông tin:

Khi các gói thông tin được gửi đến quá nhanh không kịp xử lý thì máy đích hoặc cổng trung gian gưi một tin ICMP riêng để báo cho máy gửi tạm thời làm chậm tốc độ gửi tin.

Phát hiện không tới được máy đích:

Khi hệ thống phát hiện việc không tới được máy đích, thì hệ thống gửi tin ICMP "không tới được máy đích" cho máy gửi. Nếu như đích không tới được là một mạng hay máy chủ thì tin đó do cổng trung gian gửi đi, nếu như đích không tới được là cổng chương trình (Port) thì máy đích gửi tin đi. (Cổng chương trình sẽ được trình bày sau).

Chuyển đường:

Một cổng gửi tin ICMP chuyển đường đi đến máy nguồn để báo cho máy đó sử dụng cổng khác để gửi tin nếu như nó biết được chọn cổng khác là cách tốt hơn để gửi tin. Loại tin ICMP này chỉ có thể được gửi đi khi cả cổng và máy nguồn ở cùng trên một mạng.

Kiểm tra máy ở xa:

Một máy có thể gửi tin ICMP để biết xem một máy ở xa có đang hoạt động không và tin có tới được máy đó không. Vì khi máy đích nhận được laọi tin này nó bao giờ cũng gửi lại máy nguồn một tin để trả lời.

CHƯƠNG 7. GIAO THỨC GÓI TIN CỦA NGƯỜI SỬ DỤNG (UDP)

7.1 Giới thiệu

Chương 5 đã miêu tả khả năng của TCP/IP Internet truyền các gói tin IP giữa các máy tính, mỗi gói tin được chỉ đường trong Internet dựa trên địa chỉ đích IP. Tại tầng giao thức Internet, địa chỉ đích xác định máy, không có một sự phân biệt nào nữa để chỉ ra người sử dụng nào hoặc chương trình ứng dụng nào sẽ nhận gói tin đó. Chương này mở rộng bộ giao thức TCP/IP bằng cách thêm một cơ cấu phân biệt các đích khác nhau trong cùng một máy, điều này cho phép nhiều chương trình ứng dụng chạy trên cùng một máy gửi và nhận các gói tin một cách độc lập.

7.2 Giao thức gói tin người sử dụng

Trong bộ giao thức TCP/IP, Giao thức gói tin người sử dụng - User Datagram Protocol (UDP) cung cấp một cơ cấu để các chương trình ứng dụng sử dụng gửi các gói tin tới các chương trình ứng dụng khác. Giao thức UDP cung cấp các cổng chương trình của giao thức được sử dụng để phân biệt các chương trình đang chạy trên một máy. Có nghĩa là, ngoài dữ liệu gửi đi, mỗi gói tin Giao thức UDP chứa cả cổng chương trình đích (một số nguyên) và số là cổng chương trình nguồn. Các cổng này giúp cho phần mềm Giao thức gói tin người sử dụng trên máy đích chuyển gói tin tới đúng chương trình nhận và giúp cho chương trình nhận gửi trả lời.

Giao thức UDP sử dụng Giao thức Internet ở bên dưới để truyền gói tin từ máy này tới máy khác, và cung cấp cùng chức năng chuyển gói tin không chắc chắn, không liên kết như giao thức IP. Giao thức này không có gửi lại tin công nhận là đã nhận gói tin để đảm bảo là gói tin đã tới đích, giao thức cũng không sắp xếp trật tự các gói tin đến, và cũng không cung cấp những thông tin phản hồi để điều khiển tỷ lệ chuyển dòng thông tin giữa hai máy. Như vậy, các gói tin của giao thức UDP có thể bị mất, lặp lại, hoặc chuyển đến không theo trật tự. Hơn nữa, các gói tin có thể đến nhanh hơn khả năng nơi nhận xử lý.

Giao thức gói tin người sử dụng UDP cung cấp dịch vụ chuyển không liên kết và không chắc chắn, giao thức này sử dụng giao thức IP để truyền các gói tin giữa hai máy. Giao thức UDP thêm khả năng phân biệt các đích - các chương trình trên cùng một máy.

Chương trình ứng dụng sử dụng giao thức UDP chấp nhận toàn bộ trách nhiệm để giải quyết các vấn đề như tính chắc chắn, mất gói tin, lặp gói tin, chậm, các gói tin không theo trật tự và mất liên kết. Nhiều người lập trình ứng dụng thường quên những vấn đề này khi thiết kế phần mềm. Nhiều chương trình ứng dụng dựa vào giao thức UDP để hoạt động tốt trong môi trường cục bộ nhưng lại không làm việc tốt trong môi trường mạng lớn hơn.

7.3 Định dạng của gói tin UDP

Mỗi gói tin UDP còn được gọi là gói tin người dùng. Một cách khái niệm, mỗi gói tin người dùng gồm hai phần, phần đầu UDP và phần dữ liệu UDP. Như thấy trong hình 7.1, đầu gói tin được chia thành 4 trường 16 bit chỉ cổng chương trình nguồn - nơi gói tin được gửi đi, cổng chương trình đích - nơi gói tin được nhận, độ dài gói tin, và tổng kiểm tra của UDP.

0	16	31
Source Port (Cổng chương trình nguồn)	Destination Port (Cổng chương trình đích)	
Length (Độ dài)	Checksum (Tổng để kiểm tra)	
Data begin here (bắt đầu dữ liệu)		

Hình 7.1 Định dạng gói tin UDP

Các trường cổng chương trình nguồn và cổng chương trình đích chứa các số nguyên 16 bit là cổng chương trình của giao thức được sử dụng để phân biệt giữa các chương trình đang đợi nhận gói tin. Cổng chương trình nguồn là tuỳ chọn. Khi được sử dụng, nó chỉ ra cổng chương trình mà nơi nhận cần gửi thông tin trả lời đến, nếu không sử dụng, nó chứa các số không.

Trường độ dài chứa số các byte sử dụng trong gói tin UDP, bao gồm cả đầu gói tin UDP và dữ liệu người sử dụng. Như vậy, giá trị nhỏ nhất cho trường độ dài là 8, chỉ ra độ dài của đầu gói tin.

Tổng kiểm tra UDP là tuỳ chọn và không cần thiết phải sử dụng; Giá trị không của trường tổng kiểm tra có nghĩa là tổng kiểm tra chưa được tính. Các nhà thiết kế chọn tổng kiểm tra là tuỳ chọn để cho phép các ứng dụng hoạt động mà không phải tính toán nhiều khi sử dụng UDP trong một mạng cục bộ ổn định cao. Tuy nhiên, nhớ lại rằng giao thức IP không tính tổng kiểm tra trên phần dữ liệu của gói tin IP. Do vậy, tổng kiểm tra UDP cung cấp cách duy nhất để đảm bảo là dữ liệu được gửi đến còn nguyên.

7.4 Bao bọc dữ liệu của UDP và phân tầng giao thức

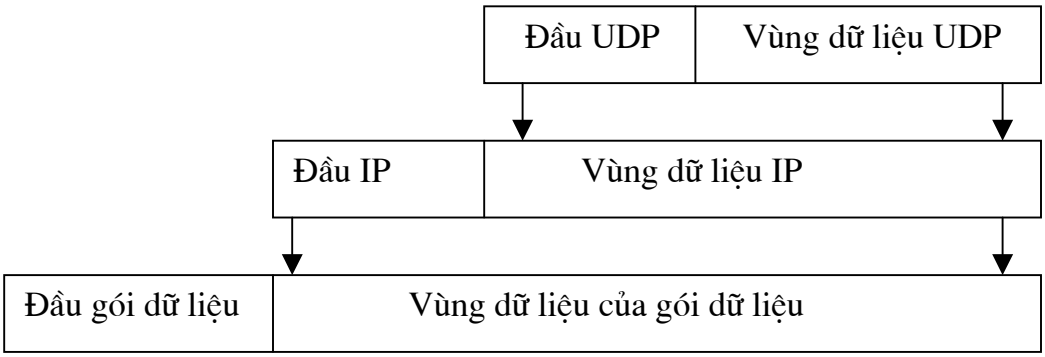
Giao thức UDP là ví dụ đầu tiên về giao thức của tầng vận tải. Trong mô hình TCP/IP, UDP nằm trên tầng giao thức Internet. Một cách khái niệm, các chương trình ứng dụng sử dụng UDP, còn giao thức UDP sử dụng giao thức IP để gửi và nhận các gói tin như trong hình 7.2.

Tầng ứng dụng
Giao thức UDP
Giao thức IP
Giao diện mạng

Hình 7.2 Tầng khái niệm của UDP giữa các chương trình ứng dụng và IP

Giao thức UDP nằm trên giao thức IP có nghĩa là toàn bộ gói tin UDP, bao gồm cả đầu và dữ liệu được bao bọc trong gói tin IP khi gói tin được truyền trong Internet như trong hình 7.3.

Đối với các giao thức, bao bọc có nghĩa là dữ liệu mà người dùng định gửi thì giao thức UDP coi là dữ liệu của mình và thêm đ ầu gói tin UDP vào, sau đó chuyển xuống cho giao thức IP. Giao thức IP coi toàn bộ gói tin UDP là dữ liệu của mình và thêm đầu IP vào, sau đó lại chuyển xuống cho tầng mạng ở phía dưới. Toàn bộ gói tin IP được tầng mạng vật lý ở dưới coi là dữ liệu của gói dữ liệu. Định dạng của gói dữ liệu phụ thuộc vào công nghệ mạng cụ thể ở dưới. Bình thường, các gói dữ liệu mạng thêm đầu dữ liệu vào cho phần dữ liệu mới.



Hình 7.3 Gói tin UDP được bao bọc trong gói tin IP để truyền trong Internet

Khi gói tin đến nơi nhận tại phần mềm mạng ở tầng dưới và được gửi dần lên cho các tầng trên. Mỗi tầng bỏ đi phần đầu tương ứng của gói tin trước khi chuyển lên cho tầng trên, sao cho tại tầng cao nhất dữ liệu được chuyển cho chương trình ứng dụng cần nhận và tất cả các thông tin đầu đều được loại bỏ. Khi quan sát việc loại bỏ thông tin đầu, phải chú ý đến nguyên tắc phân lớp. Gói tin UDP nhận từ tầng IP trên máy đích hoàn toàn giống với gói tin mà tầng UDP gửi cho tầng IP trên máy nguồn. Và dữ liệu mà giao thức UDP chuyển cho người dùng ở tầng ứng dụng trên máy đích sẽ giống hệt như dữ liệu mà người dùng chuyển cho giao thức UDP trên máy nguồn.

Tầng IP chỉ chịu trách nhiệm truyền dữ liệu giữa hai máy trong mạng Internet, còn tầng UDP chỉ chịu trách nhiệm phân biệt giữa các chương trình - các đích trong cùng một máy.

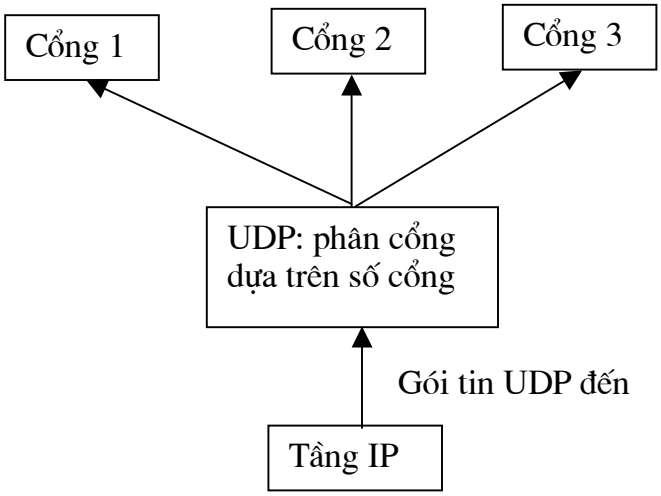
Như vậy, chỉ đầu IP xác định máy nguồn và máy đích; chỉ tầng UDP xác định các cổng chương trình nguồn hoặc các cổng chương trình đích trong một máy.

7.5 Phân cổng, hợp cổng của giao thức UDP

à cáGiao thức UDP chấp nhận các gói tin từ nhiều chương trình ứng dụng và chuyển chúng đến giao thức IP để truyền, và nó chấp nhận các gói tin UDP đến từ giao thức IP và chuyển chúng đến các chương trình ứng dụng thích hợp.

Một cách khái niệm, toàn bộ việc phân cổng và hợp cổng giữa phần mềm UDP vc chương trình ứng dụng xảy ra qua cơ chế cổng. Trong thực tế, mỗi chương trình ứng dụng phải thương lượng với hệ điều hành để lấy một số và gán số đó là cổng chương trình trước khi gửi gói tin UDP. Khi cổng chương trình đã được gán, mọi gói tin từ chương trình ứng dụng đó được gửi qua cổng sẽ có số là cổng chương trình trong trường source port (cổng chương trình nguồn) của gói tin.

Khi xử lý các đầu vào, giao thức UDP chấp nhận các gói tin đến từ phần mềm IP và phân cổng dựa vào cổng chương trình đichs của gói tin UDP, hình 7.4 miêu tả điều đó.



Hình 7.4 Ví dụ về phân cổng của giao thức UDP

Khi giao thức UDP nhận gói tin, nó kiểm tra xem số cổng chương trình đích có phù hợp với một trong những số các cổng đang được sử dụng. Nếu không, nó gửi một thông báo lỗi ICMP cổng không tới được - port unreachable và loại bỏ gói tin đó đi. Nếu như nó thấy sự phù hợp, giao thức UDP xếp hàng gói tin đến tại cổng, ở chỗ mà chương trình ứng dụng có thể truy cập được.

7.6 Các cổng UDP dự trữ và có sẵn

Một câu hỏi đặt ra là: các số cổng được gán như thế nào? Vấn đề này quan trọng vì hai máy tính cần phải thoả thuận với nhau về các số cổng trước khi chúng có thể hoạt động với nhau. Ví dụ, khi máy tính A muốn lấy một file từ máy tính B, nó cần phải biết cổng chương trình nào mà chương trình truyền file trên máy B đang sử dụng. Có hai phương pháp cơ bản để gán cổng. Cách thứ nhất, sử dụng cơ quan trung tâm. Mọi người đồng ý cho phép cơ quan trung tâm gán các số cổng như cần thiết và xuất bản danh sách các số cổng đã xếp đặt. Sau đó các phần mềm được xây dựng dựa trên danh sách. Phương pháp này thường được gọi là gán toàn bộ, và các cổng gán do cơ quan trung tâm chỉ ra là các cổng gán đã biết.

Phương pháp thứ hai để gán cổng sử dụng gán động. Trong phương pháp gán động, các cổng không được biết trên toàn cục. Thay vào đó, khi nào chương trình cần một cổng thì phần mềm mạng gán cho một số là cổng.

Các nhà thiết kế TCP/IP chấp nhận phương pháp xen kẽ cả hai phương pháp trên. Gán một số cổng trước, tuy nhiên để nhiều cổng có sẵn cho các chương trình ứng dụng hoặc cho địa phương sử dụng. Các cổng đã gán có giá trị thấp và tăng dần lên, để các số nguyên lớn cho gán động. Bảng 7.1 liệt kê một số cổng UDP đã gán cho các chương trình. Cột thứ hai là các từ khoá chuẩn của Internet, và cột thứ ba là các từ khoá hay dùng trong hệ UNIX.

Số cổng	Từ khoá trong Internet	Từ khoá trong UNIX	Miêu tả
0	-	-	Dự trữ
7	ECHO	echo	Đáp lại
9	DISCARD	discard	Bỏ đi
11	USERS	systat	Kích hoạt người dùng
13	DAYTIME	daytime	Thời gian ngày
15	-	netstat	Nestat
17	QUOTE	qotd	Trích dẫn của ngày
19	CHARGEN	chargen	Bộ sinh ký tự
37	TIME	time	Thời gian
42	NAMESERVER	name	Chương trình chủ tên máy
43	NICNAME	whois	Ai là
53	DOMAIN	nameserver	Chương trình chủ tên vùng
67	BOOTPS	bootps	Chương trình chủ giao thức bootstrap
68	BOOTPC	bootpc	Chương trình khách giao thức bootstrap
69	TFTP	tftp	Chuyển file đơn giản
111	SUNRPC	sunrpc	RPC của hãng Sun
123	NTP	ntp	Giao thức thời gian mạng
161	-	snmp	Theo dõi mạng của SNMP
162	-	snmp-trap	Traps của SNMP
512	-	biff	Comsat của UNIX
513	-	who	Daemon rwho của UNIX
514	-	syslog	System log
525	-	timed	Daemon thời gian

Bảng 7.1 Một số ví dụ về các cổng đã gán

7.7 Tóm tắt

UDP là một giao thức cho phép các chương trình ứng dụng truyền thông nhờ sử dụng dịch vụ chuyển gói tin không liên kết và không chắc chắn. Do vậy, các gói tin UDP có thể mất, lặp lại, chậm, hoặc chuyển đến không theo thủ tục; một chương trình ứng dụng sử dụng giao thức UDP phải giải quyết những vấn đề này.

Trong sơ dồ giao thức, UDP nằm trong tầng vận tải, trên giao thức Internet và dưới tầng ứng dụng. Một cách khái niệm, tầng vận tải độc lập với tầng Internet, nhưng trong thực tế chúng tương tác với nhau một cách mạnh mẽ. Tổng kiểm tra của UDP bao gồm các địa chỉ nguồn và đich IP, điều đó có nghĩa là phần mềm UDP phải tương tác với phần mềm IP để tìm các địa chỉ trước khi gửi các gói tin.

Giao thức gói tin người sử dụng UDP phân biệt các chương trình (hoặc quá trình) trong một máy nhờ cho phép nơi gửi và nơi nhận thêm một số nguyên 16 bit gọi là cổng chương trình vào mỗi gói tin UDP. Các số cổng xác định nguồn và đích. Một số cổng UDP quen biết đã được gán (ví dụ cổng 69 được giữ cho giao thức chuyển file đơn giản TFTP). Các cổng khác có sẵn để cho các chương trình ứng dụng tuỳ ý sử dụng.

CHƯƠNG 8. GIAO THỨC ĐIỀU KHIỂN TRUYỀN TIN

8.1 Giới thiệu

Các chương trước đã khai thác dịch vụ chuyển gói tin không liên kết và không chắc chắn, dịch vụ đó hình thành cơ sở cho toàn bộ truyền thông của Internet và giao thức IP xác định dịch vụ này. Chương này giới thiệu dịch vụ Internet quan trọng thứ hai, chuyển dòng tin một cách tin cậy, và Giao thức điều khiển truyền tin - Transmission Control Protocol (TCP) xác định dịch vụ này.

Tại tầng thấp nhất, các mạng máy tính truyền thông cung cấp việc chuyển gói tin không chắc chắn. Các gói tin có thể bị mất, hỏng khi những lỗi truyền tin tác động tới dữ liệu, khi phần cứng mạng không làm việc, hoặc khi mạng bị tắc nghẽn. Các mạng chỉ đường động cho các gói tin có thể chuyển chúng không theo quy tắc, chuyển bị chậm, hoặc lặp lại các gói tin. Hơn nữa các công nghệ mạng bên dưới có thể bắt tuân theo kích thước gói tin tối ưu hoặc đề ra các quy định ràng buộc khác để đạt được tỷ lệ truyền tin hiệu quả.

Tại tầng cao nhất, các chương trình ứng dụng thường cần phải một khối lượng lớn dữ liệutừ máy tính này tới máy tính khác. Sử dụng hệ thống chuyển gói tin không liên kết và không chắc chắn cho lượng lớn dữ liệu trở nên khó chịu, buồn tẻ, và đòi hỏi những người lập trình xây dựng việc phát hiện lỗi và khôi phục trong mỗi chương trình ứng dụng. Vì thiết kế, xây dựng, hoặc thay đổi phần mềm để cung cấp sự tin cậy là khá, chỉ có một số ít các nhà lập trình có đủ kiến thức cơ sở để làm được điều đó. Do vậy, một trong những mục đích của giao thức mạng là tìm một giải pháp chung để giải quyết vấn đề, cung cấp việc chuyển dòng tin tin cậy. Việc có một giao thức với mục đích chung giúp đỡ các chương trình ứng dụng không phải tìm hiểu chi tiết của mạng, làm cho việc xác định một giao diện cùng kiểu cho dịch vụ chuyển dòng tin.

8.2 Tính chất của dịch vụ chuyển tin cậy

Có thể nêu 5 đặc tính của giao diện giữa các chương trình ứng dụng và dịch vụ chuyển tin cậy TCP/IP:

- *Hướng đến dòng dữ liệu:* Khi hai chương trình ứng dụng (các quá trình của người dùng) chuyển những lượng dữ liệu lớn, chúng ta coi dữ liệu như dòng các bit, các dòng dữ liệu được chia thành các byte gồm 8 bit. Dịch vụ chuyển dòng dữ liệu đến máy đích để đến chương trình nhận dòng các byte như chương trình gửi chuyển qua từ máy nguồn.

- *Liên kết mạch ảo*. Thực hiện việc chuyển dòng dữ liệu cũng tương tự như gọi điện thoại. Trước khi có thể bắt đầu việc chuyển, cả chương trình ứng dụng của nơi gửi và nơi nhận tương tác với hệ điều hành riêng, báo cho hệ điều hành biết về mong muốn chuyển dòng dữ liệu. Các modul phần mềm trong hai hệ điều hành trao đổi với nhau nhờ các thông báo gửi qua Internet, kiểm tra việc

chuyển được uỷ quyền, và cả hai bên đều đã sẵn sàng. Khi tất cả các chi tiết đã được thiết lập, các modul giao thức thông báo cho các chương trình ứng dụng về sự liên kết đã được thiết lập và việc chuyển có thể bắt đầu. Trong qua trình truyền, phần mềm giao thức trên hai máy tiếp tục trao đổi để kiểm tra dữ liệu được nhận chính xác. Nếu như việc truyền hỏng do lý do nào đó (ví dụ, phần cứng mạng dọc theo đường truyền giữa các máy bị hỏng), cả hai máy phát hiện hỏng và báo cho các chương trình ứng dụng tương ứng. Chúng ta sử dụng mạng ảo để miêu tả những liên kết như vậy vì mặc dù các chương trình ứng dụng xem liên kết như là mạch phần cứng, sự tin cậy là một hình ảnh do dịch vụ chuyển dòng tin mang lại.

- *Truyền có phần đệm*. Các chương trình ứng dụng gửi dòng dữ liệu qua mạch ảo nhờ chuyển các byte dữ liệu lặp đi lặp lại đến phần mềm giao thức. Khi truyền dữ liệu, mỗi chương trình ứng dụng sử dụng kích thước bất kỳ nào mà nó cho là phù hợp, kích thước có thể chỉ là một byte. Tại nơi nhận, phần mềm giao thức kiểm tra và chuyển dữ liệu cho chương trình ứng dụng đúng trật tự như chúng đã được gửi. Phần mềm giao thức tự do chia dòng dữ liệu thành các gói tin không phụ thuộc vào các phần của chuương trình ứng dụng truyền. Để cho việc truyền hiệu quả hơn và giảm thiểu dòng thông tin trong mạng, những thực hiện ứng dụng thường thu đủ dữ liệu từ dòng dữ liệu để làm đầy gói tin đủ lớn trước khi truyền nó dọc theo Internet. Như vậy, ngay cả khi chương trình ứng dụng sinh dòng dữ liệu từng byte một, việc truyền dữ liệu qua Internet có thể vẫn hiệu quả. Tương tự, nếu như chương trình ứng dụng sinh những khối dữ liệu lớn, phần mềm giao thức có thể chia mỗi khối thành các phần nhỏ để truyền.

Đối với các chương trình ứng dụng mà dữ liệu nên chuyển ngay cả khi nó chưa làm đầy bộ đệm, dịch vụ dòng tin cung cấp cơ chế đẩy - push giúp chương trình ứng dụng sử dụng để bắt buộc phải truyền. Tại nơi gửi, đẩy bắt phần mềm giao thức truyền tất cả dữ liệu vừa sinh mà không đợi làm đầy bộ đệm. Khi dữ liệu đến nơi nhận, push làm cho TCP thực hiện để dữ liệu có sẵn cho chương trình ứng dụng mà không phải đợi.

- *Dòng dữ liệu không có cấu trúc*. Điều quan trọng nên hiểu là dịch vụ dòng dữ liệu TCP/IP không thực hiện các dòng dữ liệu có cấu trúc. ví dụ, không có cách nào cho chương trình bảng lương bảo dịch vụ dòng dữ liệu đánh dấu giữa các bản ghi người làm, hoặc xác định nội dung của dòng là dữ liệu bảng lương. Các chương trình ứng dụng sử dụng dịch vụ dòng dữ liệu phải hiểu nội dung dòng và đồng ý về định dạng trước khi chúng khởi đầu một liên kết.

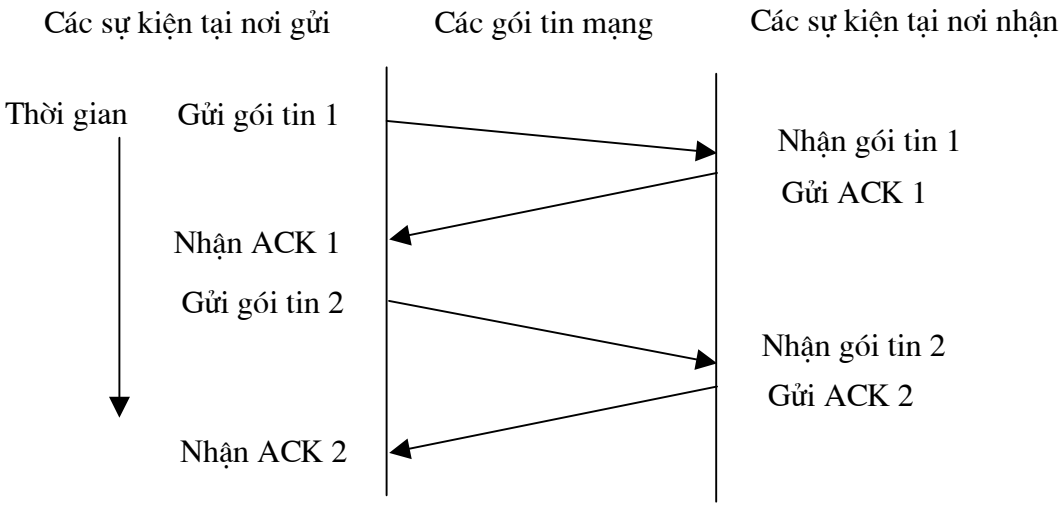
- *Liên kết hai chiều*. Những liên kết do dịch vụ dòng dữ liệu TCP/IP cung cấp cho phép truyền cùng một lúc cả hai chiều. Từ cách nhìn của qua trình ứng dụng, một liên kết đủ hai chiều bao gồm hai dòng dữ liệu độc lập theo các chiều ngược nhau, mà không có tương tác rõ ràng. Dịch vụ dòng dữ liệu cho phép quá trình ứng dụng dừng dòng dữ liệu trong một hướng trong khi dữ liệu

tiếp tục truyền trong hướng khác, làm cho liên kết trở thành một chiều. ưu điểm của liên kết hai chiều là phần mềm giao thức ở dưới có thể gửi thông tin điều khiển cho một dòng dữ liệu ngược trở về nguồn trong các gói tin mang dữ liệu theo hướng ngược lại.

8.3 Cung cấp sự tin cậy

Dịch vụ chuyển dòng dữ liệu tin cậy hay chắc chắn đảm bảo chuyển dòng dữ liệu từ máy này tới máy khác mà không bị mất hoặc lặp. Một câu hỏi đặt ra là:"làm cách nào phần mềm giao thức cung cấp việc truyền tin cậy nếu như hệ truyền thông ở dưới cung cấp việc chuyển gói tin không chắc chắn?". Câu trả lời khá phức tạp, nhưng đa số các giao thức tin cậy sử dụng một kỹ thuật cơ bản được biết là xác nhận dương với viẹec truyền lại. Kỹ thuật này yêu cầu nơi nhận trao đổi với nơi gửi, gửi lại một thông báo xác nhận khi nơi gửi nhận được dữ liệu. Nơi gửi giữ hồ sơ về mỗi gói tin mà nó gửi và đợi việc xác nhận trước khi gửi tiếp gói tin khác. Nơi gửi cũng bắt đầu ghi thời gian khi nó gửi gói tin và gửi lại gói tin nếu như sau một thời gian không nhận được sự xác nhận.

Hình 8.1 chỉ ra giao thức xác nhận dương đơn giản nhất truyền dữ liệu. Trong hình các sự kiện tại nơi gửi và nơi nhận chỉ ra ở bên trái và bên phải. Mỗi đường chéo qua phần giữa chỉ việc truyền của một gói tin quan trọng.

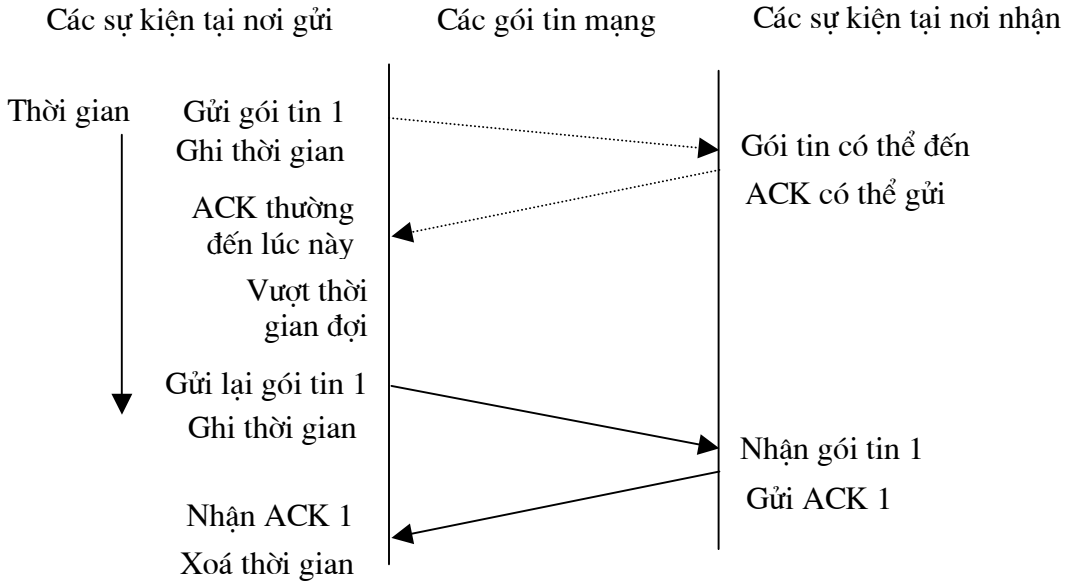


Hình 8.1 Một giao thức sử dụng xác nhận dương với việc truyền lại. Nơi gửi đợi một xác nhận cho mỗi gói tin đã gửi

Hình 8.2 sử dụng cùng sơ đồ như hình 8.1 để chỉ điều gì xảy ra khi một gói tin bị mất hay hỏng. Nơi gửi bắt đầu ghi thời gian sau khi truyền một gói tin. Khi thời gian đợi đã qua, nơi gửi cho là gói tin đã bị mất và gửi lại.

Vấn đề tin cậy xuất hiện khi hệ thống chuyển gói tin ở dưới lặp lại các gói tin. Việc lặp lại có thể cũng xảy ra khi nhiều sự chậm trễ lớn xảy ra trong mạng tạo ra việc truyền lại sớm. Giải quyết sự lặp lại yêu cầu suy nghĩ cẩn thận vì cả các gói

tin và việc xác nhận đều có thể bị lặp. Các giao thức tin cậy phát hiện các gói tin lặp lại nhờ gán mỗi gói tin một số và yêu cầu nơi nhận nhớ dãy các số đã nhận. Để tránh sự lẫn lộn sinh ra do chậm trễ hoặc xác nhận lặp lại, các giao thức xác nhận dương gửi các dãy số ngược trở lại trong xác nhận, do vậy nơi nhận có thể khôi phục lại những sự xác nhận liên quan với các gói tin.



Hình 8.2 Vượt thời gian đợi và truyền lại xảy ra khi một gói tin bị mất. Đường chấm chấm chỉ thời gian cần phải tính theo việc truyền và xác nhận của gói tin nếu gói tin không mất.

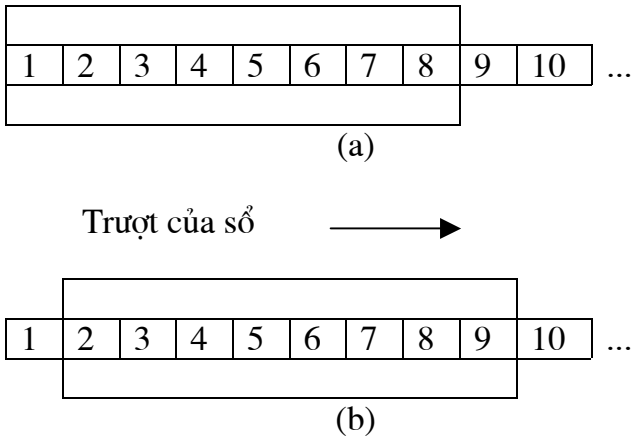
8.4 Tư tưởng đằng sau các cửa sổ trượt

Khái niệm cửa sổ trượt giúp cho việc truyền dòng dữ liệu hiệu quả. Để hiểu động cơ đối với các cửa sổ trượt, xem lại dòng các sự kiện mà hình 8.1 miêu tả. Để đạt được sự tin cậy, nơi gửi truyền một gói tin và sau đó đợi một sự xác nhận trước khi truyền gói tin khác. Như hình 8.1 chỉ ra, dữ liệu chỉ truyền giữa hai máy theo một hướng tại bất kỳ thời gian nào, ngay cả khi mạng có khả năng truyền thông đồng thời cả hai hướng. Mạng sẽ hoàn toàn không làm gì cả trong thời gian các máy làm chậm sự trả lời (có nghĩa là khi các máy đang tính đường đi hay tổng kiểm tra). Nếu chúng ta hình dung một mạng với việc truyền thông chậm, vấn đề sau trở nên rõ ràng:

Giao thức xác thực dương đơn giản làm lãng phí một lượng đáng kể dải tần của mạng vì mạng làm châmj việc gửi gói tin mới cho đến khi nó nhận được sự xác nhận đối với gói tin trước.

Kỹ thuật cửa sổ trượt là một dạng phức tạp hơn của xác nhận dương và truyền lại khi so với phương pháp đơn giản đã thảo luận trên. các giao thức cửa sổ trượt sử dụng dải tần của mạng tốt hơn vì chúng cho phép nơi gửi truyền nhiều gói

tin trước khi đợi sự xác nhận. Trong hình 8.3 miêu tả giao thức đặt một cửa sổ nhỏ trên dãy các gói tin và truyền tất cả các gói tin nằm trong cửa sổ.



Hình 8.3 (a) giao thức cửa sổ trượt với 8 gói tin trong cửa sổ, và (b) Cửa sổ trượt sao cho gói tin 9 có thể được gửi khi có xác nhận của gói tin 1. Chỉ những gói tin không có xác nhận mới phải truyền lại.

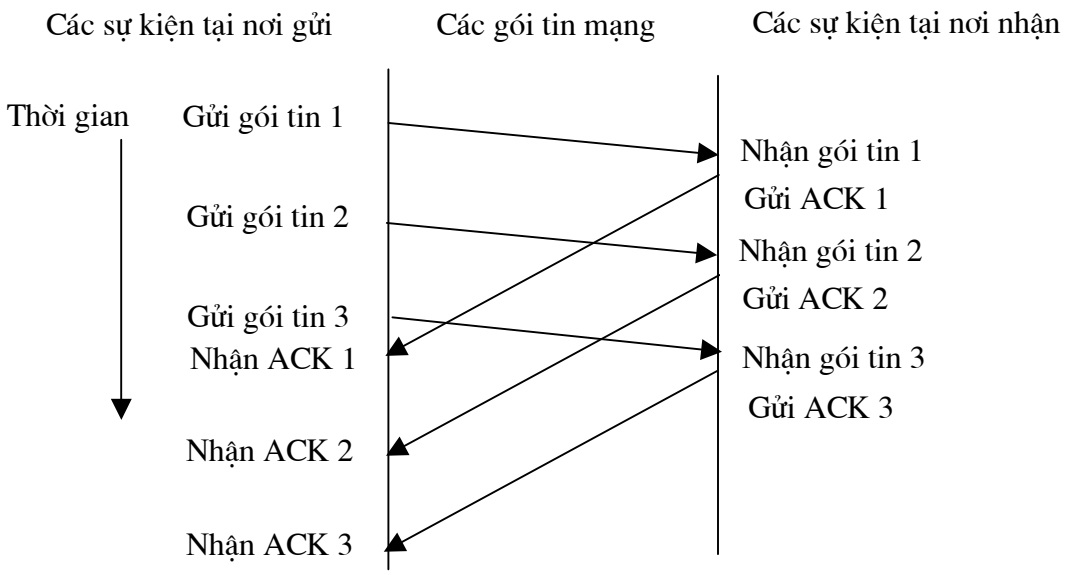
Một gói tin không xác nhận nếu như nó đã được truyền nhưng không nhận được sự xác nhận. Một cách kỹ thuật, số các gói tin có thể không được xác nhận tại một thời điểm bị chặn bởi kích thước của sổ. Ví dụ, trong giao thức cửa sổ trượt với kích thước cửa sổ là 8, nó gửi được cho phép truyền 8 gói tin trước khi nó nhận được một sự xác nhận.

Như hình 8.3 chỉ ra, khi nơi gửi nhận được sự xác nhận cho gói tin đầu tiên trong cửa sổ, nó "trượt" cửa sổ dọc theo dòng dữ liệu và gửi gói tin tiếp theo. Cửa sổ tiếp tục trượt chừng nào nhận được các xác nhận.

Sự thực hiện của các giao thức cửa sổ trượt phụ thuộc vào kích thước cửa sổ và tốc độ mạng nhận các gói tin. Hình 8.4 chỉ một ví dụ hoạt động của giao thức cửa sổ trượt khi gửi ba gói tin. Để ý rằng nơi gửi truyền cả ba gói tin trước khi nhận được một sự xác nhận.

Với cửa sổ kích thước là 1, giao thức cửa sổ trượt đúng như giao thức xác nhận dương đơn giản. Bằng việc nâng kích thước cửa sổ, có khả năng xoá bỏ thời gian không làm gì của mạng. Có nghĩa là, trong trạng thái đều đặn, nơi gửi có thể truyền các gói tin nhanh như mạng có thể chuyển chúng. Điểm cơ bản là:

Vì một giao thức cửa sổ trượt tốt giữ cho mạng bão hoà với các gói tin, mạng có được thông lượng cao hơn đáng kể so với giao thức xác nhận dương.



Hình 8.4 Một ví dụ về ba gói tin được truyền sử dụng giao thức cửa sổ trượt. Khái niệm chính là nơi gửi có thể truyền tất cả các gói tin trong cửa sổ mà không đợi một sự xác nhận.

Cửa sổ trượt chia dãy các gói tin thành ba nhóm: nhóm các gói tin ở bên trái cửa sổ đã được truyền, được nhận và được xác nhận; nhóm gói tin ở bên phải cửa sổ còn chưa được truyền; và nhóm gói tin ở trong cửa sổ đang được truyền. Gói tin có số thấp nhất trong cửa sổ là gói tin đầu tiên trong dãy dữ liệu chưa được xác nhận.

8.5 Giao thức điều khiển truyền tin (TCP)

Dịch vụ chuyển dòng dữ liệu một cách tin tưởng trong Internet do Giao thức Điều khiển truyền tin - Transmision Control Protocol (TCP) cung cấp. Điều quan trọng đầu tiên cần hiểu là: TCP là giao thức truyền thông, không phải là một chương trình phần mềm.

Sự khác biệt giữa giao thức và phần mềm thực hiện giao thức cũng tương tự như sự khác biệt giữa định nghĩa ngôn ngữ lập trình và chương trình biên dịch (compiler). Bình thường mọi người va chạm với phần mềm TCP hơn là va chạm với những chi tiết cụ thể của giao thức.

Vậy giao thức TCP cung cấp cụ thể những gì? TCP là một giao thức phức tạp, do vậy không có một trả lời đơn giản. Giao thức chỉ ra định dạng của dữ liệu và những xác nhận mà hai máy tính trao đổi để đạt được sự truyền tin cậy, và cũng chỉ ra những thủ tục mà các máy tính sử dụng để đảm bảo là dữ liệu đến nơi chính xác. Giao thức chỉ ra cách để phần mềm TCP phân biệt các đích trên cùng một

máy tính, và cách mà các máy trao đổi để khôi phục từ những lỗi như mất hoặc lặp các gói tin. Giao thức cũng chỉ ra cách hai máy tính khởi đầu việc truyền dòng dữ liệu và cách chúng đồng ý với nhau khi kết thúc.

Hiểu những gì mà giao thức TCP không có cũng quan trọng. Mặc dù những chỉ dẫn TCP miêu tả cách các chương trình ứng dụng sử dụng giao thức TCP theo nghĩa chung, giao thức không miêu tả chi tiết về giao diện giưa một chương trình ứng dụng và giao thức TCP. Điều này có nghĩa là, tài liệu của giao thức chỉ thảo luận những hoạt động mà giao thức TCP cung cấp, chứ không chỉ ra những thủ tục chính xác mà các chương trình ứng dụng cần gọi để truy cập các hoạt động. Lý do để phần giao diện của chương trình ứng dụng lại là do tính linh hoạt của TCP/IP. Các nhà lập trình thường thực hiện TCP trong một hệ điều hành cụ thể, họ cần khai thác giao diện mà hệ điều hành cung cấp.

Do giao thức TCP giả thiết một chút về hệ truyền thông ở dưới, giao thức TCP có thể được sử dụng với nhiều dạng hệ thống chuyển gói tin khác nhau, bao gồm cả dịch vụ chuyển gói tin IP. Ví dụ, giao thức TCP có thể được thực hiện trong các đường quay số điện thoại mạng cục bộ, mạng sợi quang tốc độ cao, hoặc mạng đường dài tốc độ thấp.

8.6 Các cổng chương trình, các đường liên kết và các điểm cuối

Cũng giống như giao thức UDP trong chương 7, giao thức TCP nằm trên tầng IP trong sơ đồ các tầng giao thức. Hình 8.5 chỉ tổ chức có tính khái niệm về các tầng. Giao thức TCP cho phép nhiều chương trình ứng dụng trong cùng một máy truyền thông cùng lúc, và giao thức phân luồng dữ liệu đến giữa các chương trình ứng dụng. Cũng như giao thức gói tin người sử dụng UDP, giao thức TCP sử dụng các số - cổng chương trình để xác định đích cuối cùng trong một máy tính. Mỗi cổng chương trình được gán một số nguyên nhỏ để xác định nó.

<table>
<tr><td colspan="2">Chương trình ứng dụng</td></tr>
<tr><td>Giao thức TCP</td><td>Giao thức UDP</td></tr>
<tr><td colspan="2">Internet (IP)</td></tr>
<tr><td colspan="2">Giao diện mạng</td></tr>
</table>

Hình 8.5 Tầng có khái niệm của giao thức UDP và TCP trên IP

Khi thảo luận về các cổng chương trình của UDP, chúng ta nghĩ về mỗi cổng như là một hàng đợi mà phần mềm giao thức đặt các gói tin đến vào. Các cổng chương trình giao thức TCP phức tạp hơn nhiều vì số của cổng không tương ứng với một đối tượng. Thay vào đó, giao thức TCP xây dựng liên kết trừu tượng, các đối tượng được xác định là liên kết mạch ảo, không phải là cổng chương trình riêng biệt.

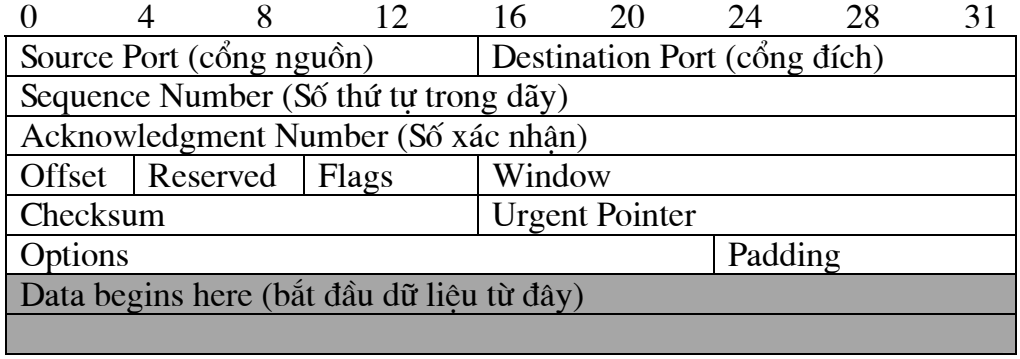
Vậy điểm cuối của mỗi đường liên kết là gì? Có thể cho chương trình ứng dụng là điểm cuối của mỗi đường liên kết không? Trong giao thức TCP điểm cuối là cặp số nguyên (host, port), với host là địa chỉ IP của máy, còn port là cổng chương trình. Ví dụ, điểm cuối (128.10.2.3, 25) và (128.10.2.3, 53) xác định một đường liên kết. Do giao thức TCP liên hệ những gói tin với đường liên kết chứ không phảicổng chương trình. Tư tưởng quan trọng cần nhớ là:

Vì giao thức TCP xác định một đường liên kết nhờ một cặp hai điểm cuối, một cổng của giao thức TCP có thể được dùng chung cho nhiều đường liên kết trên cùng một máy.

Từ cách nhìn của người lập trình, việc trừu tượng đường liên kết là khái niệm quan trọng. Điều này có nghĩa là người lập trình có thể thiết kế một chương trình ứng dụng cung cấp một dịch vụ đồng thời cho nhiều đường liên kết một lúc mà không cần phải xác định mỗi đường liên kết một cổng. Ví dụ, nhiều hệ thống cung cấp sự truy cập đồng thời đến chương trình chủ thư điện tử, cho phép nhiều máy tính gửi thư đến cùng một lúc. Vì chương trình sử dụng giao thức TCP ngay cả khi nó cho phép xử lý nhiều liên kết một lúc.

8.7 Định dạng của đoạn TCP

Đơn vị truyền giữa hai phần mềm TCP trên hai máy được gọi là đoạn. Các đoạn được trao đổi để thiết lập liên kết, truyền dữ liệu, gửi các xác nhận, thông báo kích thước cửa sổ, và dòng liên kết. Hình 8.6 chỉ định dạng của đoạn TCP.



Hình 8.6 Định dạng của đoạn TCP

Mỗi đoạn được chia thành hai phần, phần đầu và sau là phần dữ liệu. Phần đầu còn được biết là đầu TCP, mang sự nhận dạng và thông tin điều khiển. Trường SOURCE PORT và DESTINATION PORT chứa các số nguyên là cổng TCP để xác định chương trình ứng dụng tại cuối của mỗi liên kết. Trường SEQUENCE NUMBER xác định vị trí trong dòng byte dữ liệu của nơi gửi. Trường ACKNOWLEDGEMENT NUMBER xác định số các byte mà nguồn chờ nhận tiếp theo. Trường OFFSET chứa số nguyên chỉ độ dài của đầu của đoạn, trường này cần thiết vì trường tuỳ chọn OPTIONS không có độ dài cố định, phụ thuộc vào tuỳ chọn nào đang có.

Một số đoạn chỉ mang sự xác nhận còn một số đoạn khác mang dữ liệu. Các đoạn khác mang yêu cầu để thiết lập hoặc đóng liên kết. Phần mềm TCP sử dụng trường 6 bit FLAGS để xác định mục đích và nội dung của đoạn. Sáu bit này nói cách giải thích những trường khác trong đầu theo nghĩa bảng 8.1.

Bit (từ trái sang phải)	Có nghĩa khi bit = 1
URG	Trường Urgent Pointer hợp lệ
ACK	Trường Acknowledge Number hợp lệ
PSH	Nơi gửi cần chuyển nhanh dữ liệu này đến chương trình ứng dụng.
RST	Thiết lập lại đường liên kết
SYN	Đồng bộ (Synchro nize) sequence number để khởi đầu liên kết
FIN	Nơi gửi đã dừng dữ liệu

Bảng 8.1 Các bit của FLAGS trong đầu TCP

Phần mềm TCP thông báo bao nhiêu dữ liệu nữa mà nó con muốn nhận mỗi lần bằng cách nó gửi một đoạn chỉ kích thước của bộ đệm trong trường WINDOW. Trường này chứa một số nguyên không dấu 32 bit theo trật tự byte chuẩn trong mạng.

8.8 Một số đặc tính của giao thức TCP

Dữ liệu khẩn

Mặc dù TCP là giao thức hương đến dòng dữ liệu, đôi khi chương trình ở một đầu liên kết phải gửi dữ liệu "ngoài dải", mà không đợi chương trình ở đầu liên kết kia xử lý hết các dữ liệu đang có trong dòng dữ liệu. Ví dụ, khi giao thức TCP đang được sử dụng để thực hiện phiên liên lạc từ xa, người sử dụng có thể quyết định gửi dãy ký tự bàn phím để "ngắt" hoặc "kết thúc sớm" chương trình từ đầu kia của liên kết. Những tín hiệu như vậy thương cần thiết khi chương trình ở một máy từ xa hoạt động không chính xác. Tín hiệu cần phải được gửi mà không đợi chương trình đọc hết các byte đã đang có trong dòng TCP. Nếu không thì không có khả năng "kết thúc sớm" chương trình.

Cơ chế được sử dụng để đánh dấu dữ liệu khi truyền trong đoạn là bit URG được bật, và con trỏ khẩn cấp - urgent pointer chỉ vị trí kết thúc dữ liệu khẩn trong cửa sổ. Chi tiết cụ thể để giao thức TCP báo cho chương trình ứng dụng về dữ liệu khẩn phụ thuộc vào hệ điều hành của máy.

Chọn kích thước đoạn lớn nhất

Không phải tất cả các đoạn được gửi qua một liên kết đều có cùng kích thước. Tuy nhiên, cả hai đầu liên kết phải thoả thuận về đoan lớn nhất có thể truyền trong đường liên kết. Phần mềm TCP sử dụng trường tùy chọn - OPTIONS

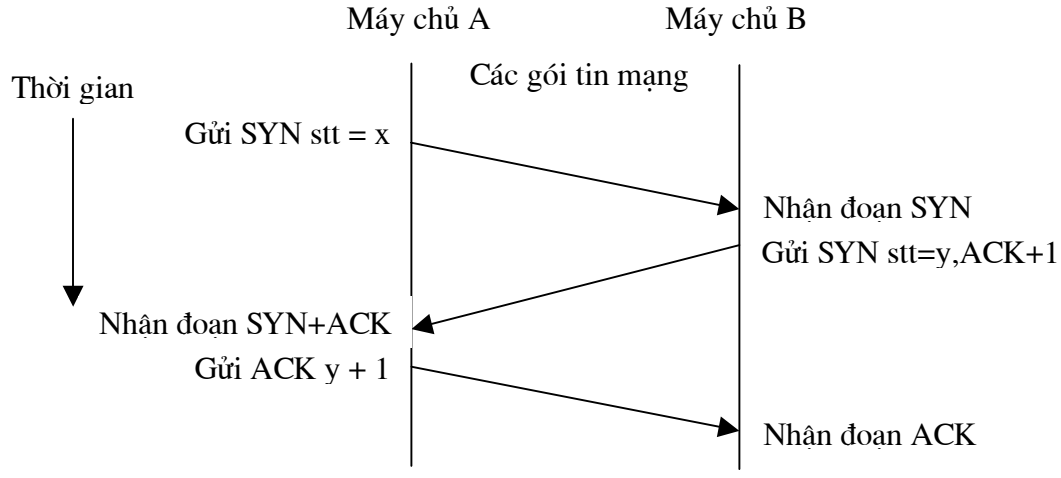
để thương lượng với phần mềm TCP ở đầu liên kết kia; một trong những tuỳ chọn cho phép phần mềm TCP chỉ kích thước đoạn lớn nhất mà nó sẵn sàng nhận. Bình thường, nếu hai điểm cuối nằm trên cùng mạng vật lý, giao thức TCP thường tính kích thước đoạn lớn nhất để gói tin IP phù hợp với MTU của mạng. Nếu hai điểm cuốikhông nằm trên cùng một mạng vật lý, chỉ dẫn hiện tại đề xuất sử dụng kích thước đoạn lớn nhất là 536 (kích thước ngầm định của gói tin IP là 576 trừ đi độ dài chuẩn của đầu IP và TCP). Hiện nay, trong thực tế không có một kích thước chuẩn.

Xác nhận và truyền lại

Do giao thức TCP gửi dữ liệu trong những đoạn không có độ dài cố định, và vì các đoạn truyền lại có thể có nhiều dữ liệu hơn là dữ liệu gốc, việc xác nhận không thể dễ dàng hướng đến các gói tin hay các đoạn. Thay vào đó, việc xác nhận sử dụng sequence number - số thứ tự trong dãy để hướng đến vị trí trong dòng dữ liệu. Nơi nhận thu thập các byte dữ liệu từ các đoạn đến và xây dựng lại bản sao chính xác của dòng dữ liệu vừa được gửi. Vì các đoạn truyền trong các gói tin IP, chúng có thể bị mất hoặc không theo trật tự, nơi nhận sử dụng các số thứ tự trong dãy để lập lại trật tự cho các đoạn. Do vậy nơi nhận luôn xác nhận số các byte liên tục dài nhất tính từ đầu của dòng dữ liệu đã nhận một cách chính xác. *Việc xác nhận luôn chỉ số thứ tự trong dãy của byte tiếp theo mà nơi nhận muốn chờ để nhận.*

Thiết lập một liên kết TCP

Để thiết lập một liên kết, giao thức TCP sử dụng three way handshake - cái bắt tay ba lần. Trong trường hợp đơn giản, bắt tay để bắt đầu thiết lập liên kết được chỉ ra trong hình 8.7.



Hình 8.7 Dãy các đoạn TCP trong cái bắt tay ba lần

Đoạn đầu tiên của cái bắt tay ba lần có thể được xác định vì nó có bit SYN được bật trong trường FLAGS. Đoạn thứ hai có cả bit SYN và bit ACK bật để chỉ rằng nó xác nhận đoạn SYN đầu tiên và tiếp tục bắt tay. Đoạn cuối cùng của bắt

tay chỉ xác nhận và chỉ để thông báo đích là cả hai bên đều đồng ý thiết lập liên kết.

Hai chương trình sử dụng TCP để trao đổi có thể kết thúc nhờ sử dụng hoạt động Close - đóng. TCP sử dụng một dạng bắt tay ba lần có biến đổi để đóng liên kết.

Các cổng chương trình TCP dự trữ

Cũng giống như UDP, giao thức TCP tổ hợp các công chương trình tĩnh và động, nhờ sử dụng một tập các cổng gán cho những chương trình chung (như thư điện tử), tuy nhiên để lại đa số các cổng cho hệ thống để phân phối cho các chương trình. Những chỉ dẫn nói rằng chỉ các cổng có số nhỏ hơn 256 sẽ được sử dụng là các cổng quen biết; những cổng còn lại đẻ sẵn cho các chương trình tuỳ ý khác. Bảng 8.2 liệt kê một số các cổng đang được sử dụng rộng rãi. Cần để ý rằng mặc dù các cổng TCP và UDP độc lập, các nhà thiết kế đã chọn sử dụng các có cùng số nguyên cho bất kỳ dịch vụ nào mà cả UDP và TCP truy nhập tới. Ví dụ, chương trình chủ tên vùng (domain name server) có thể truy cập bằng TCP hoặc UDP qua cổng 53.

Cổng số	Từ khoá	Từ khoá của UNIX	Miêu tả
0	TCPMUX		Dự trữ
1	RJE	-	TCP multiplexor
5	ECHO	-	Remote job entry
7	DISCARD	echo	Echo
9	USERS	discard	Loại bỏ
11	DAYTIME	systat	Kích hoạt người dùng
13	-	daytime	Daytime
15	QUOTE	netstat	Chương trình trạng thái mạng
17	CHARGEN	quotd	Trích dẫn trong ngày
19	FTP-DATA	chargen	Bộ sinh ký tự
20	FTP	ftp-data	Giao thức chuyển file (dữ liệu)
21	TELNET	ftp	Giao thức chuyển file
23	SMTP	telnet	Liên kết màn hình
25	TIME	smtp	Giao thức đơn giản vận tải thư
37	NAMESERV	time	Thời gian
42	ER	name	Chương trình chủ tên máy
43	NICNAME	whois	Là ai
53	DOMAIN	nameserver	Chương trình chủ tên vùng
.	.	.	.
.	.	.	.
.	.	.	.
160-223	dự trữ		

Bảng 8.2 Một số ví dụ về các cổng chương trình TCP.

8.9 Tóm tắt

Giao thức điều khiển truyền tin TCP, xác định một dịch vụ then chốt do Internet cung cấp, đó chính là dịch vụ dòng dữ liệu tin cậy, giao thức TCP cung cấp một liên kết hai chiều giữa hai máy, cho phép các máy trao đổi những lượng lớn dữ liệu một cách hiệu quả.

Vì giao thức sử dụng cửa sổ trượt, TCP có thể sử dụng hiệu quả cho Internet. Vì giao thức chỉ giả thiết một ít về hệ thống chuyển bên dưới, nên TCP đủ linh hoạt để hoạt động với nhiều hệ thống khác nhau. Do TCP cung cấp sự quản lý dòng dữ liệu, giao thức TCP cho phép nhiều hệ thống truyền thông với tốc độ thay đổi.

Đơn vị cơ sở dữ liệu mà TCP sử dụng để truyền là đoạn. Các đoạn được sử dụng để chuyển thông tin điều khiển (ví dụ, cho phép phần mềm TCP trên hai máy thiết lập liên kết hoặc dừng liên kết) hoặc dữ liệu. Định dạng của đoạn cho phép một máy xác nhận dữ liệu chuyển theo một hướng nhờ bao gồm xác nhận trong các đầu đoạn của dữ liệu truyền theo hướng ngược lại.

Giao thức TCP thực hiện điều khiển dòng dữ liệu nhờ nơi nhận thông báo số lượng dữ liệu nó sẵn sàng nhận. Giao thức cũng trợ giúp các thông báo khẩn nhờ sử dụng cờ dữ liệu khẩn - urgent data và bắt hệ thống chuyển đi với cơ chế đẩy - push.

CHƯƠNG 9. HỆ THỐNG TÊN VÙNG

9.1 Tên cho các máy tính

Cho đến nay chúng ta đã sử dụng các số nguyên 32 bit gọi là các địa chỉ giao thức Internet (hoặc địa chỉ IP) để xác định các máy tính nối vào Internet. Mặc dù những địa chỉ đó cung cấp sự thuận tiện, sự biểu diễn xúc tích để chi nguồn và đích trong các gói tin được gửi qua Internet, người dùng thích gán cho các máy những tên dễ nhớ, dễ đọc hơn.

Chương này xem xét một hệ thống để gán những tên bậc cao có nghĩa cho một tập lớn các máy, và thảo luận một cơ cấu để tương ứng giữa các tên máy bậc cao với các địa chỉ IP. Chúng ta sẽ xem xét cả việc dịch từ tên bậc cao thành địa chỉ IP và dịch từ các địa chỉ IP thành các tên bậc cao. Hệ thống tên này khá thú vị vì: nó đã được sử dụng để gán tên máy trong suốt quá trình nối mạng Internet, hơn nữa sự thực hiện cơ cấu tương ứng tên cung cấp một ví dụ về chủ đề client-server (khách-chủ).

Những hệ thống máy tính đầu tiên bị bắt buộc phải hiểu các địa chỉ số. Dần dần trong môi trường máy tính, mọi người sử dụng muốn những cái tên ký hiệu có ý nghĩa, để xác định máy.

Các tên máy thể hiện môi trường nhỏ mà các máy đó đang ở. Hoàn toàn tự nhiên, trong các vùng người dùng chọn các têndựa trên mục đích của máy. Ví dụ, các máy thường có tên research - nghiên cứu, production - sản xuất, và development - phát triển. Người dùng thấy các tên này thích hơn là các địa chỉ số.

Mặc dù sự phân biệt tên và địa chỉ là trừu tượng, đây là sự nhân tạo. Tên chỉ xác định nhờ dãy các ký tự từ tập hữu hạn các chữ cái. Các tên chỉ có ích khi hệ thống có thể tương ứng một cách hiệu quả với các đối tượng mà tên thể hiện. Do vậy, chúng ta coi địa chỉ IP là các tên bậc thấp, còn người dùng thích các tên bậc cao.

9.2 Các tên phân cấp

Làm cách nào hệ thống tên có thể phủ được tập rất lớn các tên máy đang phát triển rất nhanh mà khoong cần một mạng trung tâm quản lý nó? Câu trả lời nằm ở phân cấp trung tâm cơ cấu tên nhờ bộ phận uỷ quyền đối với các phần của không gian tên và phân phối trách nhiệm đối với việc tương ứng các tên và các địa chỉ. Sự phân bổ vùng tên phải được xác định theo cách mà nó trợ giúp việc tương ứng tên hiệu quả và đảm bảo quản lý tự trị việc gán tên.

Hệ thống tên phân cấp hoạt động như sự quản lý của một tổ chức lớn. Không gian tên được chia từ bậc cao nhất, và uỷ quyền cho các tên trong các vùng nhỏ được chuyển cho tổ chức được chỉ định. Trong không gian tên, sự uỷ quyền có

thể tiếp tục được chia tiếp tại mỗi bậc. Tư tưởng là việc chia không gian tên được thực hiện sao cho mỗi bộ phận con đủ nhỏ để có thể quanr lý được.

Trong TCP/IP Internet, các tên máy đã phân cấp được gán theo cấu trúc của các tổ chức đạt được quyền đối với các phần của không gian tên, không cần thiết phù hợp với cấu trúc của các liên kết vật lý của mạng.

9.3 Các tên vùng TCP/IP Internet

Cơ cấu thực hiện việc phân cấp tên máy cho TCP/IP Internet được gọi là Domain Name System (DNS) - Hệ thống tên vùng. Hệ thống này có hai mặt khái niệm độc lập. Thứ nhất hệ thống chỉ cú pháp và các quy tắc cho tổ chức được chỉ định các tên. Thứ hai, hệ thống chỉ ra sự thực hiện của hệ máy tính phân tán có khả năng tương ứng một cách hiệu quả tên và địa chỉ.

Hệ thống tên vùng sử dụng sơ đồ đánh tên phân cấp gọi là các Domain name - tên vùng. Một tên vùng gồm một dãy các tên con phân cách bởi dấu chấm. Ví dụ, tên cs.purdue.edu chứa ba nhãn: cs, purdue và edu. cs là tên viết tắt của khoa máy tính - computer science, purdue là tên trường, và edu là tên viết tắt của môi trường giáo dục - education.

Bộ phận chuyên môn của Internet đã chọn cách phân các tên vùng từ trên xuống như liệt kê trong bảng 9.1. Các tên vùng không phân biệt chữ cái in hoa hay in thường. Bảng 9.2 chỉ một số ví dụ về mã của tên các nước.

Một cách khái niệm, các tên ở mức cao nhất cho phép hai hệ phân cấp tên khác nhau: theo địa lý và theo tổ chức. Hệ thống địa lý chia các tên máy theo nước. Còn các tổ chức lại thích đăng ký tên dưới các tên: COM, EDU, MIL, hoặc GOV.

Tên vùng - Domain Name	ý nghĩa
COM	Commercial organization - Các tổ chưc thương mại
EDU	Educational institutions - Các cơ quan giao dục
GOV	Government institutions - Các cơ quan của Chính phủ
MIL	Military Groups - Các nhóm quân sự
NET	Các trung tâm trợ giúp mạng (network) chính
ORG	Các tổ chức (organizations) không thuộc các nhóm trên
ARPA	Tên vùng ARPANET (đã lỗi thời)
Internet	International organizations - Các tổ chức quốc tế
Mã từng nước	Tên từng nước

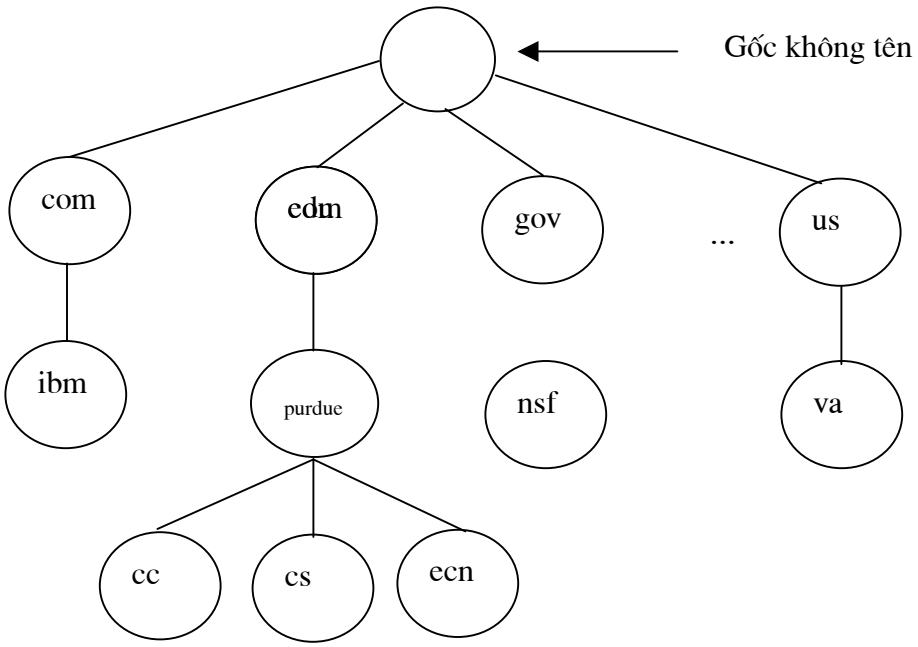
Bảng 9.1 Các tên vùng Internet mức cao nhất

AU	Australia
CA	Canada
CN	China

DE	Germany
DK	Denmark
FI	Finland
FR	France
HK	Hong Kong
KR	Korea (South)
MY	Malaysia
NZ	New Zealand
PH	Philippines
RU	Russian Federation
SG	Singapore
UK	United Kingdom
US	United States
VN	Vietnam

Bảng 9.2 Một số ví dụ về mã của các nước

Hình 9.1 minh hoạ một phần nhỏ của phân cấp tên vùng của Internet. Như trong hình chỉ ra, công ty kinh doanh máy tính quốc tế IBM ở Mỹ có tên: ibm.com. Một máy tính có tên xinu trong khoa máy tính (computer science) tại trường đại học Purdue trong môi trường giáo dục ở Mỹ có tên: xinu.cs.purdue.edu. Tên vùng của khoa máy tính (computer science) ở một trường đại học xxx ở Australia thường có tên cs.xxx.edu.au.



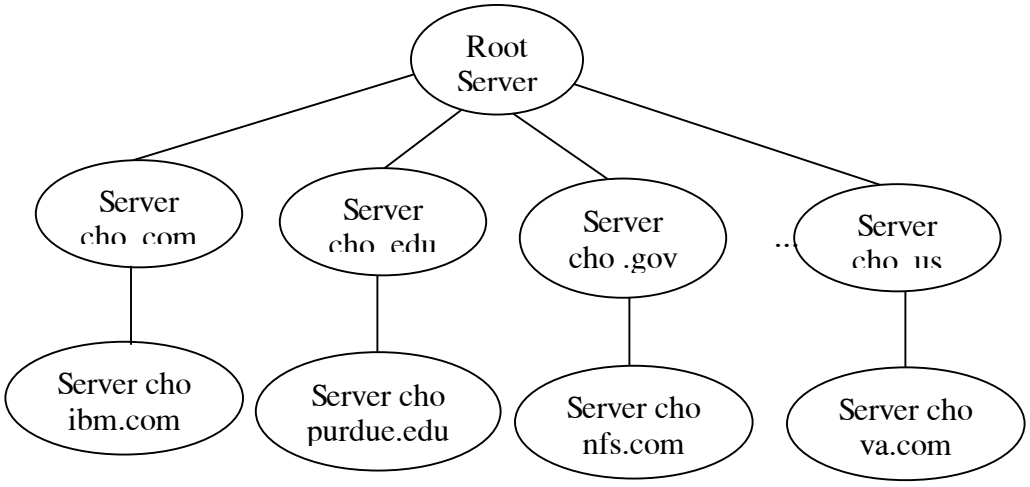
Hình 9.1 Một phần nhỏ của phân cấp (cây) tên vùng của Internet.

9.4 Tương ứng tên vùng và địa chỉ

Cùng với các quy tắc cho các cú pháp và các tổ chức uỷ quyền, hệ thống tên vùng bao gồm một hệ thống phân tán, tin cậy, hiệu quả, có mục đích chung để tương ứng tên với địa chỉ. Hệ thống này được phân tán theo nghĩa kỹ thuật, có nghĩa là một tập các chương trình chủ (servers) hoạt động ở nhiều vùng hợp tác để giải quyết vấn đề tương ứng địa chỉ. Trước hết nhận thấy rằng nhiều tên có thể tương ứng với địa chỉ trong vùng cục bộ; chỉ có một số tên yêu cầu trao đổi trong Internet; Hệ thông này tin cậy, vì một máybị hỏng không làm cho hệ thống hoạt động không chính xác.

Cơ cấu tên vùng để tương ứng các tên với các địa chỉ gồm các hệ thống hợp tác, độc lập gọi là các chương trình chủ cung cấp tên (name servers). Một chương trình cung cấp tên làm việc dịch tên - địa chỉ, tương ứng các tên vùng với các địa chỉ IP. Chương trình cung cấp tên chạy trên máy được gọi là máy cung cấp tên. Phần chương trình khách (client) gọi là chương trình giải quyết tên, mỗi chương trình khách sử dụng một hay nhiều các chương trình chủ cung cấp tên để dịch tên.

Cách dễ nhất để hiểu các chương trình tên vùng làm việc là hình dung chúng được xếp đặt trong một cấu trúc hình cây tương ứng với phân cấp tên như trong minh hoạ của hình 9.2. Gốc (root) của cây là một chương trình chủ nhận biết các vùng ở mức cao nhất và biết chương trinhf chủ giải quyết từng tên vùng. Đưa ra một tên vùng, chương trình chủ ở gốc có thể chọn đúng chương trình chủ ở mức thấp hơn giải quyết tên đó. Tại mức thấp hơn là một tập các chương trình chủ (như .edu) cung cấp lời giải cho tên vùng ở mức cao hơn và biết chương trình chủ nào có thể giải quyết tên vùng ở mức thấp hơn.



Hình 9.2 Sự xếp đặt khái niệm của các máy chủ tên vùng trong cây tương ứng với phân cấp tên vùng.

Sự liên kết của cây khái niệm không chỉ sự liên kết mạng vật lý. Đó chỉ là cây của các chương trình chủ trừu tượng sử dụng trong Internet để truyền thông. Các chương trình chủ có thể ở tại các vị trí tuỳ ý trong Internet.

Trong thực tế, mối quan hệ giữa phân cấp tên và cây của các chương trình chủ không đơn giản như mô hình. Cây của các chương trình chủ có vài mức vì một chương trình chủ có thể chứa tất cả các thông tin thuộc những phần lớn của phân cấp tên. Cụ thể, các tổ chức thương thu thập thông tin từ tất cả các vùng mức thấp hơn vào một chương trình chủ.

Làm cách nào các chương trình khách (chương trình giải quyết tên) tìm được một chương trình tên chủ để bắt đầu tim tương ứng tên? Làm cách nào một chương trình chủ khi không trả lời được câu hỏi của chương trình tìm được các chương trình chủ khác để có thể trả lời được câu hỏi. Câu trả lời khá đơn giản. Chương trình giải quyết tên phải biết cách liên lạc được với ít nhất một chương trình tên chủ. Chương trình tên chủ ở gốc (root) chứa thông tin về gốc và những tên vùng ở mức cao nhất. Mỗi chương trình tên chủ biết những chương trình tên chủ ở mức cao hơn và vị trí của chúng (theo địa chỉ IP). Hơn nữa, Internet yêu cầu mỗi vùng tên cung cấp và duy trì hai chương trình tên chủ; một chương trình tên chủ chính và một chương trình tên chủ phụ để thay thế khi chương trình tên chủ chính bị hỏng.

Các chương trình tên chủ sử dụng một cổng chương trình được biết cho tất cả mọi truyền thông, do vậy các chương trình giải quyết tên biết cách trao đổi với các chương trình tên chủ khi chúng biết địa chỉ IP của máy có chương trình tên chủ.

Các chương trình tên chủ Internet sử dụng nơi lưu trữ (cache) tên để tối ưu hoá quá trình tìm kiếm tên. Mỗi chương trình tên chủ lưu trữ (cache) những tên mới sử dụng và ghi lại nơi đã thấy thông tin tương ứng tên - địa chỉ. Khi một chương trình khách (giải quyết tên) hỏi chương trình tên chủ về một tên, chương trình chủ trước hết kiểm tra xem nó có quyền đối với tên đó không theo thủ tục chuẩn, nếu không chương trình tên chủ tìm trong nơi lưu trữ (cache) của nó để xem tên đó đã được giải quyết chưa. Do vậy, các chương trình khách có thể có được câu trả lời một cách nhanh chóng.

PHẦN II
GIẢI PHÁP BẢO MẬT
Ở CÁC TẦNG KHÁC NHAU

CHƯƠNG 10-AN TOÀN TẦNG MẠNG[1]

10.1 Giới thiệu

Ngày nay, các mạng máy tính hiện đại được đặc trưng bởi các kiến trúc giao thức phân tầng làm cho những thiết kế mạng phù hợp với các ứng dụng không hạn chế và các kỹ thuật kết nối. Giải pháp phân tầng này cho phép các giao thức trở nên modul hoá, nghĩa là được phát triển một cách độc lập và được gắn kết cùng với các giao thức khác theo một cách nào đó để tạo nên một giao thức hoàn chỉnh. Cơ sở đã biết về phân tầng giao thức là kiến trúc liên kết các hệ thống mở (OSI). Các chuẩn OSI thiết lập mô hình kiến trúc và định nghĩa các giao thức cụ thể phù hợp với mô hình bảy tầng này. Các giao thức ở mỗi tầng được nhóm lại với nhau thành một cụm tầng OSI xác định để thi hành các yêu cầu kết nối của một tiến trình ứng dụng.

Các chuẩn cũng cần hỗ trợ an toàn trong kiến trúc kết nối phân tầng OSI một cách thích đáng. Để vừa đảm bảo chức năng an toàn cần thiết, mà vẫn đảm bảo thực thi có hiệu quả đòi hỏi phải có một tập các chuẩn toàn diện, đồng bộ. Vì tính phức tạp và mềm dẻo của mô hình OSI, vấn đề an toàn phải được xem xét một cách cẩn thận để tránh tăng khả năng các chức năng bị lặp lại trên toàn kiến trúc và các chi tiết an toàn không tương hợp được sử dụng ở những bộ phận khác nhau của kiến trúc. Cũng có thể có trường hợp là những kỹ thuật an toàn khác nhau có khả năng mâu thuẫn nhau được sử dụng trong các ứng dụng hoặc tầng khác nhau, nơi mà một vài kỹ thuật sẽ cho những kết quả theo yêu cầu nhưng đỡ phức tạp và kinh tế hơn.

Các chuẩn an toàn đã được bổ sung vào kiến trúc OSI nhằm cung cấp một giải pháp toàn diện, chặt chẽ và đồng bộ cho chức năng an toàn. Các chuẩn an toàn có thể được nhóm thành các loại như sau: (1) chuẩn về kiến trúc và cơ cấu an toàn, (2) chuẩn về các kỹ thuật an toàn, (3) chuẩn về giao thức an toàn tầng, (4) chuẩn về an toàn ứng dụng-cụ thể và (5) chuẩn về quản lý an toàn. Ở đây chủ yếu tập trung vào an toàn tầng mạng là một bộ phận của họ các chuẩn về giao thức an toàn tầng. Tuy nhiên, do các chuẩn có liên quan chặt chẽ với nhau, nên cần có một sự khái quát ngắn gọn các chuẩn về kiến trúc và cơ cấu an toàn. Các chuẩn này như là cơ sở tham khảo để xây dựng các chuẩn thuộc những loại khác, trong đó có an toàn tầng mạng.

10.2 Cấu trúc, dịch vụ và giao thức an toàn tầng mạng

Tầng mạng trong mô hình OSI thích nghi với sự đa dạng của các công nghệ mạng con và các chiến lược kết nối, khiến cho nó là một tầng phức tạp nhất trong bảy tầng của mô hình. Tầng mạng phải đưa ra giao diện dịch vụ chung với tầng

[1] Network Layer Security, Steven F. Blanding, Chapter 8, Information Security Management Hanbook, 4th edition, Boca Raton-London- New York-Washington, editors Harold F.Tipton and Micki Krause

giao vận và điều phối giữa các mạng con có các công nghệ khác nhau. Góp phần đáng kể vào độ phức tạp này là hai kiểu hoạt động, có liên kết và không liên kết.

Có ba chuẩn OSI mô tả các dịch vụ tầng mạng, gồm: ISO/IEC 8648, ISO/IEC 8880 và ISO/IEC 8348. Tổ chức bên trong của tầng mạng được diễn giải bằng chuẩn ISO/IEC 8648. Các nguyên tắc chung, sự chuẩn bị và hỗ trợ các dịch vụ mạng theo kiểu liên kết và không liên kết được diễn giải bằng chuẩn ISO/IEC 8880. Định nghĩa dịch vụ mạng bao gồm phụ chương về kiểu liên kết và không liên kết, phụ chương về đánh địa chỉ được trình bày bằng chuẩn ISO/IEC 8348. Chuẩn này cũng mô tả các khái niệm về hệ thống cuối và hệ thống trung gian. Một hệ thống cuối mô hình hoá phần cứng thoả mãn mô hình kết nối bảy tầng OSI hoàn chỉnh, trong khi hệ thống trung gian được đặt ở tầng mạng chỉ có các chức năng thoả mãn ba tầng OSI thấp nhất. Các kết nối một hệ thống cuối với hệ thống cuối khác có thể thực hiện trực tiếp hoặc thông qua một vài hệ thống trung gian.

Các hệ thống trung gian cũng có thể bao hàm hoặc quy vào một mạng con thực sự, một đơn vị liên kết mạng kết nối hai hay nhiều mạng con thực sự, hoặc pha trộn cả hai một mạng con thực sự và một đơn vị liên kết mạng. Một tập hợp phần cứng và các liên kết vật lý kết nối các hệ thống thực sự được gọi là mạng con thực sự. Những ví dụ về các mạng con thực sự gồm các mạng cục bộ hoặc các mạng chuyển mạch gói công cộng. Trên cơ sở này có thể thiết lập nhiều giao thức tầng mạng khác nhau. Vì giao thức có thể tồn tại ở mức mạng con trong tầng mạng, nên không cần thiết kế chúng để hỗ trợ riêng chuẩn OSI. Như vậy, việc đáp ứng tất cả các chức năng mà dịch vụ tầng mạng yêu cầu không cần giao thức cơ sở của mạng con cung cấp. Để đạt được chức năng chuẩn OSI, có thể đưa ra các lớp giao thức nhỏ hơn nữa trên giao thức mạng con.

Bỏ qua kiểu liên kết thiết kế, giao thức tầng mạng thực thi một trong ba vai trò. Các vai trò này là giao thức hội tụ mạng con độc lập (SNICP- subnetwork-independent convergence protocol), giao thức hội tụ mạng con phụ thuộc (SNDCP-subnetwork-dependent convergence protocol) và giao thức truy nhập mạng con (SNAcP-subnetwork-access protocol). Vai trò SNICP đảm bảo các chức năng đáp ứng dịch vụ mạng OSI nhờ các khả năng cơ sở hoàn toàn xác định mà không dựa hẳn vào bất kỳ mạng con cụ thể nào. Nhiệm vụ là áp tải thông tin đánh địa chỉ và định tuyến qua các mạng đa liên kết và thông thường ghép vào giao thức liên kết được sử dụng. Vai trò SNDCP hoạt động nhờ một giao thức đáp ứng vai trò SNAcP nhằm bổ sung các khả năng mà giao thức SNICP yêu cầu hoặc cần thiết để cung cấp dịch vụ mạng OSI hoàn chỉnh. Vai trò SNAcP đảm bảo dịch vụ mạng con tại những điểm cuối của nó, đó là dịch vụ có thể hoặc không thể tương đương với dịch vụ mạng OSI. Giao thức này là một bộ phận vốn gắn liền với một kiểu mạng con cụ thể.

ISO/IEC 8473 xác định một giao thức khác rất quan trọng đối với tầng mạng - giao thức mạng không liên kết (CLNP-connectionless network protocol). Giao thức này cung cấp dịch vụ mạng kiểu không liên kết trong phạm vi vai trò SNICP.

Định nghĩa về hoạt động của giao thức này trên các mạng con chuyển mạch gói hoặc các mạng con LAN được bao hàm trong chuẩn ISO/IEC 8473.

10.3 Sắp đặt kiến trúc dịch vụ an toàn

Khi thiết kế an toàn, cần đưa ra các quyết định quan trọng về các lớp, nơi mà dữ liệu hoặc chế độ bảo vệ dựa vào kết nối nên áp dụng. Việc thực thi các dịch vụ an toàn trong kiến trúc truyền thông phân tầng có thể là một sự nỗ lực phức tạp và có thể nảy sinh các vấn đề nghiêm trọng. Khái niệm phân tầng giao thức ý nói các mục dữ liệu có thể được bao trong các mục dữ liệu và các kết nối có thể được bao trong các kết nối với khả năng nhiều tầng lồng nhau.

Sự chỉ đạo về vị trí các dịch vụ an toàn trong mô hình OSI được chỉ ra trong chuẩn ISO/IEC 7498-2. Như chuẩn hình thức đầu tiên viết về việc gán tầng cho các dịch vụ an toàn, chuẩn này bên cạnh việc cung cấp hướng dẫn về những tầng OSI nào được dành riêng cho các dịch vụ an toàn, còn cho phép nhiều lựa chọn. Yêu cầu an toàn phụ thuộc vào ứng dụng. Một số dịch vụ an toàn có thể phải cung cấp ở các tầng khác nhau trong những ngữ cảnh ứng dụng khác nhau, trong khi một số khác có thể cùng phải cung cấp ở nhiều tầng trong cùng ngữ cảnh. Có thể minh hoạ độ phức tạp của các dịch vụ an toàn này bằng việc truyền thông giữa một cặp hệ thống cuối qua một loạt các mạng con.

Một hệ thống cuối điển hình được định nghĩa như là một phần thiết bị riêng rẽ, hoặc một trạm làm việc PC, máy tính mini, máy tính mainframe. Một hệ thống cuối được mô tả chỉ có một chính sách tác nghiệp đối với các mục đích an toàn. Một mạng con là một bộ các phương tiện truyền thông áp dụng cùng một công nghệ truyền thông. Mạng cục bộ (LAN) hoặc mạng diện rộng (WAN) là một ví dụ về mạng con. Một mạng con được mô tả chỉ có một căn cứ giải quyết các mục đích an toàn. Tuy nhiên, mỗi mạng con về cơ bản có môi trường an toàn khác nhau, và vì vậy có thể sẽ có chính sách tác nghiệp khác nhau. Cũng như vậy, một hệ thống cuối và một mạng con kết nối với nó có thể có hoặc không có cùng chính sách tác nghiệp.

Một sự phức tạp khác thường thấy trong các hệ thống cuối là chúng thường phải đáp ứng cùng một lúc nhiều ứng dụng, chẳng hạn thư điện tử, truy nhập file và truy nhập thư mục của nhiều người dùng. Các ứng dụng này thường cần đáng kể các yêu cầu an toàn khác nhau. Các yêu cầu an toàn có thể không chỉ khác nhau trong các hệ thống cuối và đối với các mạng con, mà chúng cũng có thể khác nhau ngay trong một mạng con. Nói chung, các mạng con bao gồm nhiều liên kết kết nối các thành phần mạng con, và các liên kết khác nhau có thể đi qua các môi trường an toàn khác nhau. Kết quả là các liên kết đơn lẻ có khả năng cần được bảo vệ thông qua một cơ chế an toàn.

Để giảm độ phức tạp, có thể mô tả các dịch vụ an toàn một cách đơn giản hơn và hiệu quả hơn trong mô hình bốn mức. Bốn mức mà tại đó các yêu cầu an toàn là rõ ràng và phân biệt đối với các yếu tố giao thức an toàn bao gồm mức ứng dụng,

mức hệ thống cuối, mức mạng con và mức liên kết trực tiếp. Ở mức ứng dụng, các thành phần giao thức an toàn phụ thuộc vào ứng dụng. Ở mức hệ thống cuối, các thành phần giao thức an toàn đảm bảo sự bảo vệ trên cơ sở từ hệ thống cuối tới hệ thống cuối. Ở mức mạng con, các thành phần giao thức an toàn đáp ứng việc bảo vệ bên trong một mạng con, nơi được xem như ít tin cậy hơn các bộ phận khác của môi trường mạng. Ở mức liên kết trực tiếp, các thành phần giao thức an toàn cung cấp sự bảo vệ bên trong một mạng con trên một liên kết được xem là thiếu tin cậy hơn các bộ phận khác của môi trường mạng con.

Khi xác định nơi đặt các dịch vụ an toàn trong các tầng kiến trúc dựa vào bốn mức, thì trước hết phải kiểm tra một số thuộc tính chung khác nhau giữa các mức cao và thấp. Các thuộc tính chung này bao gồm hỗn hợp thông tin trao đổi, thông tin định tuyến, số các điểm bảo vệ, bảo vệ tiêu đề giao thức và liên kết nguồn/nơi gom.

Trafic mixing là một thuật ngữ được sử dụng để mô tả việc trộn dữ liệu qua lại giữa các mức cao và thấp của kiến trúc phân tầng OSI. Theo khái niệm dồn kênh, các mức thấp có khuynh hướng hướng tới các mục dữ liệu từ các ứng dụng và người dùng nguồn và đích khác nhau được trộn trong luồng dữ liệu nhiều hơn các mức cao. Kiểu chính sách an toàn có thể biến đổi đáng kể nhân tố này. Trong các trường hợp mà chính sách an toàn định để cho các ứng dụng hoặc người dùng cụ thể định ra yêu cầu bảo vệ dữ liệu, thì việc đặt các dịch vụ an toàn ở một mức cao là tốt hơn. Các ứng dụng hoặc người dùng đơn lẻ sẽ không có sự bảo vệ đầy đủ ở nơi mà an toàn được chỉ định ở các mức thấp. Thêm vào đó, một số dữ liệu cũng sẽ được bảo vệ một cách không cần thiết vì những đòi hỏi an toàn của dữ liệu khác phân chia luồng dữ liệu.

Thông tin định tuyến (route knowledge) cũng là một nhân tố quan trọng trong việc sắp đặt an toàn. Cái đó cho biết nhiều về các đặc trưng an toàn của các lộ trình và các liên kết ở những mức thấp hơn là ở những mức cao. Việc đặt an toàn ở các mức thấp có thể có hiệu lực và những lợi ích tiềm năng trong một môi trường mà các đặc trưng này khác nhau đáng kể. Có thể loại trừ các chi phí an toàn ở nơi không cần sự bảo vệ trên các mạng con hoặc các liên kết, trong khi đó các dịch vụ an toàn hướng đích được sử dụng theo cách đặc biệt với nghĩa dành riêng.

Số các điểm bảo vệ (number of protection points) có thể khác nhau đáng kể phụ thuộc vào nơi đặt bảo vệ an toàn. Nếu an toàn được đặt ở mức rất cao, chẳng hạn tầng ứng dụng, thì an toàn cũng cần đặt trong mỗi ứng dụng nhạy cảm ở mỗi hệ thống cuối. Nếu an toàn được đặt ở một mức rất thấp, chẳng hạn mức liên kết trực tiếp, thì an toàn cũng sẽ được đặt ở các điểm cuối của mọi liên kết mạng. Nếu an toàn được đặt gần giữa kiến trúc, thì số điểm cần đặt các chi tiết an toàn có chiều hướng ít hơn đáng kể.

Để có được sự bảo vệ đầy đủ tiêu đề giao thức, cần đặt các dịch vụ an toàn ở một mức thấp. Nếu các dịch vụ an toàn được đặt ở các mức cao, thì tiêu đề của giao thức mức thấp trong một số môi trường có thể là nhạy cảm sẽ không nhận được sự bảo vệ.

Liên kết nguồn là sự kết hợp dữ liệu với nguồn gốc của nó. Việc áp dụng xác thực nguồn gốc dữ liệu và các dịch vụ an toàn chống từ chối được thực thi phụ thuộc vào liên kết này. Các dịch vụ an toàn này hầu hết được thực hiện hiệu quả ở các mức cao, đặc biệt ở mức ứng dụng. Tuy nhiên, lệ thuộc vào các ràng buộc cụ thể, đôi khi có thể thực hiện nó ở các mức thấp.

10.4 An toàn mức hệ thống cuối

An toàn mức hệ thống cuối liên quan tới hoặc tầng giao vận hoặc các giao thức tầng mạng của mạng con độc lập. Các chuẩn đã được triển khai hỗ trợ cả hai lựa chọn, ISO/IEC 10736 cho tầng giao vận và ISO/IEC 11577 cho tầng mạng. Các loại yêu cầu an toàn tương ứng với giải pháp an toàn hệ thống cuối tập trung vào ba loại lớn. Loại thứ nhất bao gồm các yêu cầu liên quan tới các kết nối mạng không gắn với bất kỳ ứng dụng cụ thể nào. Loại thứ hai gồm các yêu cầu do người có thẩm quyền với hệ thống cuối chỉ định được áp đặt trên tất cả các cuộc truyền thông mà không để ý tới ứng dụng. Cuối cùng, loại thứ ba gồm các yêu cầu dựa vào giả thiết rằng các hệ thống cuối là đáng tin cậy, nhưng tất cả các mạng truyền thông bên dưới là không tin cậy.

Trong sự lựa chọn giữa tầng giao vận hay tầng mạng để đặt bảo vệ an toàn mức hệ thống cuối, các nhân tố thiên về giải pháp tầng mạng bao gồm: (1) sự dễ dàng chèn vào các thiết bị an toàn tại những điểm khớp nối vật lý chuẩn, (2) khả năng đáp ứng một kiến trúc tầng trên nào đó gồm ISO, Internet và kiến trúc độc quyền, (3) khả năng sử dụng cùng một giải pháp ở các mức hệ thống cuối và mạng con.

10.5 An toàn mức mạng con

An toàn mức mạng con cung cấp sự bảo vệ qua một hoặc nhiều mạng con cụ thể. Cần phân biệt an toàn mức mạng con với an toàn mức hệ thống cuối do hai lý do quan trọng. Thứ nhất, thiết bị và chi phí điều hành cho các giải pháp an toàn mức mạng con có thể thấp hơn nhiều so với mức hệ thống cuối vì số lượng hệ thống cuối thường vượt xa số cổng mạng con. Thứ hai, các mạng con gắn với các hệ thống cuối có cùng độ tin cậy như bản thân các hệ thống cuối vì chúng có cùng các tiền đề và được quản lý dưới cùng các điều kiện. Do vậy, giữa an toàn mức mạng con và an toàn mức hệ thống cuối nên thường xuyên xem xét chọn lựa an toàn mức mạng con đến khả năng có thể. Trong kiến trúc OSI an toàn mức mạng con ánh xạ tới tầng mạng.

10.6 Giao thức an toàn tầng mạng

Tầng mạng là một trong số các tầng phức tạp của mô hình OSI. Cho nên, đòi

hỏi có một vài chuẩn OSI để mô tả các chức năng truyền, định tuyến và liên kết mạng cho tầng này. Chuẩn ISO/IEC 8880 mô tả tổng quan về tầng mạng. Hai chuẩn khác là ISO/IEC 8348 và 8648 định nghĩa dịch vụ mạng và mô tả tổ chức bên trong của tầng mạng. Chuẩn phát hành gần đây nhất là ISO/IEC 11577 mô tả giao thức an toàn tầng mạng (NLSP- network-layer security protocol).

Các tầng con khác nhau tạo nên tầng mạng, mỗi tầng con thực hiện các vai trò khác nhau, chẳng hạn giao thức truy nhập mạng con (SNAcP) và giao thức hội tụ mạng con phụ thuộc (SNDCP). NLSP có thể được đặt ở một vị trí nào đó trong số một vài vị trí khác nhau trong tầng mạng có chức năng như là một tầng con. Trên tầng cao nhất của nó là tầng giao vận, hoặc có thể là bộ định tuyến có chức năng chuyển tiếp hoặc chọn đường.

Trong giao thức an toàn tầng mạng có hai giao diện dịch vụ: giao diện dịch vụ NLSP và giao diện dịch vụ mạng bên dưới (UN- underlaying network). Dịch vụ NLSP là giao diện biểu diễn một thực thể hoặc tầng con bên trên, dịch vụ UN là giao diện với một tầng con bên dưới. Các giao diện dịch vụ này được mô tả theo cách để có vẻ giống như dịch vụ mạng đã định nghĩa trong ISO/IEC 8348. Giao thức an toàn tầng mạng cũng có thể định nghĩa theo hai dạng hoặc biến thể, có liên kết và không liên kết. Trong NLSP có liên kết, dịch vụ NLSP và dịch vụ UN là có liên kết, ngược lại trong dịch vụ NLSP không liên kết, các dịch vụ này là không liên kết. Tính mềm dẻo của kiến trúc này dẫn tới khả năng NLSP đáp ứng cả hai dịch vụ an toàn mức hệ thống cuối hay mức mạng con.

Ví dụ, trong NLSP có liên kết, giả sử chúng ta xác định X.25 là công nghệ mạng con bên dưới. Ở cấu hình này, NLSP được đặt ở đỉnh tầng mạng (chỉ bên dưới tầng giao vận và ngay trên mạng con X.25), cho phép dịch vụ NLSP ngang hàng với phiên bản an toàn của dịch vụ mạng OSI. Theo ví dụ này, giao thức X.25 không nhận thấy an toàn được cung cấp từ bên trên.

NLSP cũng có thể cung cấp an toàn mức mạng con. Trong các trường hợp mạng con không tin cậy, NLSP tăng cường an toàn cần thiết, nó có thể ngang hàng với hoặc dịch vụ mạng OSI trong hệ thống cuối hoặc dịch vụ tầng bên trong mạng (NILS) trong hệ thống chuyển tiếp. Trong các trường hợp không liên kết, có thể có một vài cấu hình với các ứng dụng thực tế, chẳng hạn các tiêu đề giao thức mạng không liên kết (CLNP) không mã hoá hoàn toàn, các địa chỉ CLNP mã hoá với các phần tiêu đề không mã hoá, hoặc các tiêu đề CLNP mã hoá hoàn toàn.

10.7 Truyền dữ liệu an toàn

Việc đóng gói là một chức năng an toàn sử dụng để bảo vệ dữ liệu người dùng và các tham số nhạy cảm. Trong cả hai NLSP có liên kết và không liên kết, chức năng cơ bản là cung cấp sự bảo vệ bắt nguồn từ các nguyên thuỷ hỏi hoặc đáp đưa ra ở dịch vụ NLSP. Hàm đóng gói gắn với an toàn này sinh ra các giá trị dữ liệu tương ứng với các nguyên thuỷ hỏi hoặc đáp đưa ra ở dịch vụ UN, sau đó

chúng được đảo ngược lại tại điểm nhận cuối. Điều này rất giống với tiến trình sử dụng trong TLSP (transport layer security protocol), nơi sinh ra và xử lý PDU (protocol data unit) đóng gói an toàn.

Các hàm đóng gói khác nhau khả dụng đối với các môi trường khác nhau trong NLSP. Khả năng này bao gồm hàm đóng gói cơ bản rất giống với hàm đóng gói định nghĩa trong TLSP. NLSP cũng có một số chi tiết bổ sung vào hàm cơ bản. Mỗi xâu octet được bảo vệ chứa một dãy các trường gồm: (1) các tham số địa chỉ yêu cầu bảo vệ, (2) các tham số chất lượng dịch vụ cần bảo vệ, (3) một chỉ báo về kiểu nguyên thuỷ (ví dụ, kết nối hỏi, kết nối đáp, không kết nối,...), (4) dữ liệu người dùng cần bảo vệ, (5) dữ liệu kiểm tra để sử dụng trong việc kiểm tra hoạt động của hệ thống mã hoá và (6) nhãn an toàn.

Nếu so sánh với TLSP thì tiến trình bảo vệ là như nhau ngoại trừ hai trường bổ sung bao hàm trong PDU được sinh ra. Đó là số thứ tự toàn vẹn (ISN-integrity sequence number) và một trường thông tin đệm. Số thứ tự toàn vẹn được sử dụng để hỗ trợ toàn vẹn thứ tự. Vì các số thứ tự giao thức vận tải có thể phục vụ mục đích này trong TLSP, nên chi tiết này không được yêu cầu ở tầng đó. Trường thông tin đệm được sử dụng để hỗ trợ dịch vụ bảo mật luồng thông tin là một đòi hỏi của NLSP, nhưng không cần ở TLSP.

Hàm đóng gói có thể bao hàm một tiến trình tiêu đề rõ hoặc khi chọn hàm đóng gói cơ bản là một tiến trình không có tiêu đề. Trong trường hợp tiêu đề rõ, thì một tiêu đề rõ được thêm vào đầu xâu octet bảo vệ thu được để sinh ra một PDU truyền dữ liệu an toàn NLSP chứa định danh liên kết an toàn. Trường hợp đóng gói không tiêu đề cũng khả dụng đối với lựa chọn chỉ sử dụng NLSP có liên kết. Có thể sử dụng tùy chọn không tiêu đề nếu chỉ áp dụng cơ chế an toàn là mã hoá và khi tiến trình mã hoá - giải mã không làm thay đổi độ dài dữ liệu. Khi lựa chọn không tiêu đề, PDU truyền dữ liệu an toàn được thay thế bằng một phiên bản mã hoá của dữ liệu yêu cầu bảo vệ. Điều này cho phép chèn NLSP vào tầng mạng một cách trong suốt. Các đặc tính của dữ liệu của các dịch vụ bên dưới, chẳng hạn tỉ suất dữ liệu, kích thước gói và dải thông không bị ảnh hưởng. Vì vậy, các hàm an toàn có thể dễ dàng bổ sung vào các dịch vụ đang tồn tại mà không làm thay đổi kiến trúc mạng. Tuy nhiên, phạm vi các dịch vụ có thể được hỗ trợ bị giảm đi nhiều vì có thể không sử dụng đến ICV (integrity check-value), ISN, đệm và các nhãn an toàn. Các dịch vụ toàn vẹn vẫn được duy trì ở nơi dữ liệu có khả năng chắc chắn dư thừa và nếu mã hoá kiểu chuỗi (chaining) được sử dụng.

Việc ánh xạ cùng kiểu các gốc dịch vụ NLSP với các gốc dịch vụ UN, ngoại trừ thiết lập và giải phóng kết nối, đó là cách hoạt động của NLSP. Nếu các trường không yêu cầu bảo vệ thì chúng được sao trực tiếp từ một gốc dịch vụ tới gốc dịch vụ khác. Các trường của NLSP này yêu cầu bảo vệ thì được xử lý bằng hàm đóng gói. Kết quả đóng gói, hoặc PDU truyền dữ liệu bảo mật được ánh xạ vào tham số dữ liệu người dùng của gốc dịch vụ UN. Việc áp dụng hàm bọc có thể gây ra dãn tin, điều này dẫn đến phải phân đoạn.

10.8 Thiết lập và giải phóng kết nối

Như đã lưu ý trước đây, để thực hiện thiết lập kết nối với NLSP có liên kết đòi hỏi các thủ tục đặc biệt. NLSP tương tự TLSP không chỉ hỗ trợ giao thức an toàn bên trong, mà còn hỗ trợ các liên kết an toàn do phương tiện khác quản lý. Việc sử dụng các thủ tục đặc biệt phụ thuộc vào có hay không thiết lập liên kết an toàn cần thiết để kết hợp với thiết lập kết nối.

Ngay cả khi liên kết an toàn phù hợp tồn tại (nói cách khác, trường hợp không dính dáng đến thiết lập liên kết an toàn), thì vẫn có một yêu cầu đối với việc trao đổi NLSP cụ thể tại thời diểm thiết lập kết nối. Đó là cần thực hiện xác thực thực thể ngang hàng, mã hoá cụ thể và các khoá toàn vẹn để sử dụng trong khi kết nối và khởi đầu các số thứ tự toàn vẹn. Trong trường hợp này, PDU điều khiển an toàn kết nối được định nghĩa trong NLSP để truyền thông tin này. Tại thời điểm thiết lập kết nối, diễn ra trao đổi hai chiều các PDU này. Kiểu cơ chế xác thực kết nối được mô tả đối với liên kết an toàn cụ thể xác định mức độ biến đổi nội dung rõ của PDU. Các trường của PDU sẽ gồm một nhãn an toàn, thông tin tham chiếu khoá hoặc nguồn gốc khoá và các phiên bản mã hoá của hai số thứ tự toàn vẹn, mỗi số cho một hướng truyền. Việc giải mã trường số thứ tự toàn vẹn thành công có thể cùng một lúc đảm bảo bảo vệ chống lặp lại.

Ở nơi mà việc thiết lập tổ hợp an toàn diễn ra đồng thời với thiết lập kết nối, những cuộc trao đổi dữ liệu có thể phức tạp hơn nhiều. Độ phức tạp tăng lên về cơ bản do phải định nghĩa PDU tổ hợp an toàn riêng rẽ. Khi có nhiều hơn một cuộc trao đổi hai chiều, sử dụng PDU tách riêng này để giải quyết nhu cầu của các mục tiêu xác thực và tìm ra nguồn gốc khoá, cũng như thoả thuận thuộc tính tiếp theo. Một lần nữa, giống với TLSP, NLSP không đòi hỏi kỹ thuật thiết tổ hợp an toàn cụ thể. Thay vào đó là một kỹ thuật phù hợp dựa vào mô tả trao đổi xác thực Diffie-Hellman.

Cuối cùng trong phần này mô tả những trao đổi giao thức thiết lập liên kết NLSP ánh xạ lên dịch vụ UN như thế nào. Việc ánh xạ trực tiếp lên các gốc thiết lập kết nối UN sẽ là tình huống lý tưởng. Tuy nhiên, trong thực tế những trao đổi giao thức NLSP làm tăng tổng chi phí thực tế và cản trở khả năng này. Không thể có khoảng trống trong các PDU thiết lập kết nối UN đối với tất cả dữ liệu cần truyền vì các trường dữ liệu người dùng của các giao thức mạng thông thường bị giới hạn về độ dài. Thêm vào đó, có thể cần trao đổi giao thức nhiều chiều để thiết lập liên kết an toàn.

Những điều kiện này đòi hỏi lựa chọn một trong hai ánh xạ cơ bản. Một thiết lập kết nối NLSP có thể ánh xạ trực tiếp tới thiết lập kết nối UN, nơi chỉ cần một trao đổi hai chiều và tất cả dữ liệu yêu cầu có thể vừa khít trong các trường dữ liệu người dùng của các nguyên thuỷ kết nối UN. Nếu những điều kiện này không tồn tại, thì các cuộc truyền dữ liệu yêu cầu ánh xạ tới những trao đổi dữ liệu UN theo sau thiết lập kết nối UN. Độ phức tạp có thể tăng lên khi mà các cuộc truyền dữ

liệu ánh xạ tới các trao đổi dữ liệu UN. Có khả năng thông lượng, kích thước cửa sổ, chất lượng dịch vụ và các tham số dịch vụ khác đã đặt cuối cùng không hợp với các đặc trưng của kết nối UN. Khi điều này xảy ra, một kết nối UN mới được thiết lập với những đặc trưng yêu cầu hiện có và kết nối UN ban đầu bị giải phóng.

Những vấn đề ánh xạ cũng có thể xảy ra ở nơi mà với việc giải phóng kết nối NLSP, dữ liệu người dùng khi ngắt kết nối cần được bảo vệ bằng hàm đóng gói và PDU thu được không thể vừa khít với tham số dữ liệu người dùng của ngắt UN. PDU NLSP phải ánh xạ tới trao đổi dữ liệu người dùng trước khi ngắt UN trong ngữ cảnh này. NLSP là một giao thức mạnh và phức tạp vì lượng ánh xạ có thể có rất lớn.

10.9 Tóm tắt

Tổng quát, các giao thức an toàn tầng thấp đáp ứng các dịch vụ an toàn mức hệ thống cuối, mức liên kết trực tiếp và mức mạng con. Các dịch vụ an toàn ở các mức mạng con và mức hệ thống cuối hỗ trợ bảo mật, toàn vẹn, điều khiển truy nhập và các dịch vụ xác thực. Các dịch vụ an toàn ở mức liên kết trực tiếp chỉ hỗ trợ bảo mật. Các dịch vụ này khác nhau ở chỗ môi trường là có liên kết hay không liên kết.

Trên khắp các tầng thấp, những khái niệm về bảo vệ chất lượng dịch vụ và tổ hợp an toàn được sử dụng. Để thông báo các yêu cầu bảo vệ qua các biên tầng và thoả thuận các yêu cầu giữa hai điểm cuối, chất lượng dịch vụ bảo vệ được sử dụng. Để cung cấp một kiểu bảo vệ vững chắc cho thứ tự của dữ liệu được truyền giữa hai hệ thống, tổ hợp an toàn được sử dụng để mô hình hoá tập hợp thông tin về thuộc tính liên quan duy trì giữa các hệ thống này. Một tổ hợp an toàn có thể thiết lập thông qua các trao đổi giao thức tầng ứng dụng, các trao đổi giao thức tầng thấp hơn trong cùng tầng, hoặc thông qua các phương pháp phi chuẩn.

NLSP là rất mềm dẻo, có chức năng hoặc ở mức hệ thống cuối hoặc ở mức mạng con. Có thể đặt NLSP ở một vị trí nào đó trong một vài vị trí trong tầng mạng, có chức năng như một tầng con. NLSP có thể che giấu thông tin về giao thức mạng con tin cậy trong khi thông tin này truyền qua một mạng con không tin cậy, phụ thuộc vào việc đặt vị trí của nó trong tầng mạng. Những biến thể của NLSP gồm có liên kết và không liên kết. Biến thể có liên kết làm việc kết hợp với các giao thức cùng loại như X.25, và biến thể không liên kết làm việc cùng với giao thức mạng không liên kết (CLNP). Quá trình bọc gói rất giống với với TLSP được dùng bởi NLSP. Để đảm bảo thiết lập các tổ hợp an toàn, hỗ trợ giao thức tuỳ chọn được sử dụng.

CHƯƠNG 11-AN TOÀN TẦNG GIAO VẬN[2]

11.1 Giới thiệu

Tầng giao vận của mô hình OSI bảo đảm khả năng truyền dữ liệu điểm tới điểm tin cậy theo tiêu chuẩn mà tầng phiên đòi hỏi, không tính đến loại mạng sẽ truyền dữ liệu bên dưới. Ở đây sẽ khảo sát các dịch vụ cung cấp cho những người dùng dịch vụ giao vận và sự an toàn kết hợp với tầng giao vận.

Các chuẩn tầng giao vận cơ bản được tìm thấy trong định nghĩa dịch vụ vận chuyển ISO (International Organization for Standardization) /IEC (International Electrotechnical Commision) 8072, đặc tả giao thức vận tải có liên kết ISO/IEC 8602. Những văn bản này được xuất bản lần đầu tiên vào năm 1986 và 1987. Tiếp theo những xuất bản phẩm này, chức năng tiện ích an toàn đã được bổ sung vào tầng giao vận với việc hoàn thiện chuẩn giao thức an toàn tầng giao vận (TLSP), ISO/IEC 10736 năm 1993. Dự án của chính phủ Mỹ do Uỷ ban an ninh quốc gia (NSA) khởi xướng SDNS (Secure Data Network System) đã đưa ra đặc tả giao thức an toàn 4 (SP4) mà sau này trở thành nguồn cơ bản cho sự phát triển của TLSP. SP4 là một sản phẩm của cả ngành kinh doanh và chính phủ, nó mô tả các dịch vụ, cơ chế và giao thức an toàn để bảo vệ dữ liệu người dùng trong các mạng dựa vào mô hình OSI. TLSP, ngay kể cả những phần đóng góp bổ sung tạo ra theo nó, vẫn hầu như dựa vào SP4.

Trước khi trình bày giao thức an toàn tầng giao vận, cần có sự khái quát về tầng giao vận để người đọc có kiến thức cơ bản cần thiết để hiểu kiến trúc an toàn.

11.2 Khái quát về tầng giao vận

Dịch vụ giao vận được định nghĩa trong văn bản định nghĩa dịch vụ OSI 8072. Bất cứ khi nào dịch vụ giao vận cũng ở một trong ba giai đoạn: (1) thiết lập liên kết giao vận (TC-transport connection), (2) truyền dữ liệu, hoặc (3) giải phóng liên kết giao vận. Trong giai đoạn thiết lập TC, một liên kết được thiết lập giữa những người dùng TS ngang hàng (các thực thể tầng phiên). Thực thể tầng phiên khởi đầu TC đặc tả chất lượng dịch vụ mà liên kết yêu cầu dưới dạng độ tin cậy và các khía cạnh khác của dịch vụ. Một khi TC được thiết lập, các thực thể tầng phiên có thể trao đổi các đơn vị dịch vụ giao vận (TSDU-Transport Service Data Unit) một cách trong suốt ngang qua liên kết. Trong giai đoạn giải phóng, mỗi người dùng dịch vụ giao vận giải phóng TC vô điều kiện.

Việc truyền dữ liệu điểm tới điểm tin cậy do phần tử dịch vụ T-DATA cung cấp và dữ liệu expedited do phần tử dịch vụ T-EXPEDITED-DATA cung cấp. Mức

[2] Transport Layer Security, Steven F. Blanding, Chapter 9, Information Security Management Hanbook, 4th edition, Boca Raton-London- New York-Washington, editors Harold F.Tipton and Micki Krause

dịch vụ mà TC yêu cầu được thông báo cho thực thể giao vận khởi đầu trong tham số chất lượng dịch vụ (QoS) của yêu cầu T-CONNECT. Điều này được sử dụng như là cơ sở để thoả thuận QoS có thể chấp nhận và có được giữa các hệ thống cuối trong quá trình thiết lập TC. Sau đó trong suốt thời gian tồn tại liên kết, nhà cung cấp TS phải duy trì QoS đã thoả thuận này.

Các tham số kết hợp với mỗi dịch vụ giao vận nguyên thuỷ bao gồm địa chỉ đã gọi, địa chỉ đang gọi, quyền lựa chọn dữ liệu expedited, chất lượng dịch vụ, dữ liệu người dùng TS, địa chỉ đáp, điều kiện ngắt. Địa chỉ bị gọi và địa chỉ gọi là các địa chỉ TSAP (Transport Service Address Protocol), định danh người dùng TS khởi đầu TC và nơi đáp được hướng tới. Địa chỉ đáp chuyên chở TSAP như địa chỉ bị gọi, chỉ khác nó khi địa chỉ đó đã được người dùng TS đầu tiên cung cấp theo một số dạng tổng quát. Một dạng như thế dẫn đến sự lựa chọn một địa chỉ TSAP cụ thể của hệ thống cuối đáp dựa vào dạng tổng quát được cung cấp. Lựa chọn này là tham số được trả lại. Tham số quyền lựa chọn dữ liệu expedited được sử dụng để thoả thuận về hiệu lực của dịch vụ vận chuyển dữ liệu expedited trên TC. Nếu người dùng TS gọi hoặc nhà cung cấp TS không đưa ra dịch vụ này được thể hiện trong dấu hiệu T-CONNECT, thì người dùng TS bị gọi không thể cố tình đòi nó bằng việc bao hàm nó trong lời đáp.

Dữ liệu người dùng TS là tham số mà trong trường hợp T-DATA và T-EXPEDITED-DATA là cơ chế bảo đảm trao đổi TSDU trong suốt, tin cậy qua TC giữa những người dùng TS ngang hàng. Đối với các dịch vụ khác, tham số này cho phép giới hạn số lượng dữ liệu người dùng hợp pháp được truyền giữa những người dùng TS có khả năng định chất lượng các dịch vụ khi cần. Dữ liệu người dùng TS bị hạn chế về độ dài theo kiểu phần tử dịch vụ: tối đa 32 octets cho T-CONNECT, 64 octets cho T-DISCONNECT, 16 octets cho T-EXPEDITED-DATA và không hạn chế đối với T-DATA.

Kích thước không giới hạn của TSDUs dữ liệu chuẩn tắc thường không áp dụng trong thực tế. Các ràng buộc trong quá trình thực thi hoặc trong môi trường điều hành thực thể giao vận, chẳng hạn kích thước bộ nhớ đệm khả dụng, dẫn đến một giới hạn gắn với TSDUs. Một giới hạn như thế có những tác động trở lại ở các tầng cao hơn, nhưng những điều này có thể vượt qua bằng cách phân đoạn nhờ các thực thể tầng phiên. Phân đoạn là phương tiện mà nhờ nó người dùng dữ liệu dịch vụ tầng phiên (SSDU), như một đối tượng yêu cầu dữ liệu, có thể truyền được giữa các thực thể tầng phiên ngang hàng không phải theo một đơn vị dữ liệu giao thức tầng phiên đơn lẻ (SPDU) mà theo các đoạn, nghĩa là theo một vài SPDU liên tiếp.

Tham số chất lượng dịch vụ tự bản thân nó là một "danh sách" các tham số. Theo yêu cầu T-CONNECT, nó là một chỉ thị của người dùng khởi đầu TS liên quan tới mức dịch vụ mà nó đòi hỏi ở TC, cho đến khi đó chưa được thiết lập. Nó liên quan tới những thứ như là các mức độ lỗi và thông lượng dữ liệu tối thiểu chấp nhận được. Cả hai thực thể giao vận gọi và bị gọi có thể thay đổi QoS thành một mức mà xem như có thể khả thi, đưa ra thông báo về các khía cạnh của mạng mà

người dùng khởi đầu TS không cần thấy. Trong quá trình thiết lập liên kết, QOS được truyền tới người dùng TS đáp trong chỉ báo. Việc chấp nhận liên kết có được trong xác nhận T-CONNECT mang QOS sau cùng. Nếu điều này bị thay đổi thành một mức không chấp nhận được, thì người dùng khởi đầu TS có lựa chọn ngắt liên kết đã thiết lập bằng cách đưa ra yêu cầu T-DISCONNECT với một giá trị tham số điều kiện thích hợp và đồng thời hạn chế dữ liệu người dùng, chẳng hạn "QOS đổi thành mức không chấp nhận được".

Tham số điều kiện của chỉ báo T-DISCONNECT đưa ra nguyên nhân giải phóng TC. Nó chỉ ra giải phóng người dùng hay nhà cung cấp khởi đầu, có thể bao gồm các giá trị có thể có "chất lượng dịch vụ ở dưới mức cho phép đối với TC", "tắc nghẽn hoặc lỗi của nhà cung cấp TS địa phương hoặc từ xa", "lý do không biết", "địa chỉ TSAP bị gọi không có hiệu lực", hoặc "địa chỉ TSAP bị gọi không khả dụng".

11.3 Độ tin cậy của mạng con

Các lỗi bắt nguồn trong một mạng con và do vậy bị tầng giao vận theo dõi thuộc hai kiểu, lỗi tín hiệu và lỗi dư thừa. Lỗi tín hiệu là lỗi do tầng mạng phát hiện nhưng trong tầng đó không có bước nào được đưa ra để khôi phục. Sự kiện này chỉ báo hiệu cho tầng giao vận khôi phục. Hai ví dụ là ngắt mạng (kết nối mạng bị mất) và khởi động lại mạng (thiết lập lại liên kết mạng theo trạng thái đã biết, có thể bị mất dữ liệu đang truyền, nhưng kết nối giữ nguyên tính khả dụng).

Các lỗi dư thừa là các lỗi khác hẳn các lỗi tín hiệu. Theo tầm ảnh hưởng, tầng mạng không phát hiện ra chúng. Những ví dụ là mất, làm sai lạc, lặp lại và phá vỡ thứ tự của các TSDU.

Các mạng con được phân tích theo hai kiểu lỗi này được phân loại như sau hoặc (1) mạng con có mức độ lỗi ở cả hai kiểu chấp nhận được, (2) mạng con có mức độ lỗi dư thừa chấp nhận được nhưng lỗi tín hiệu thì không, hoặc (3) mạng con có mức độ lỗi dư thừa không chấp nhận được. Một liên kết mạng diễn ra trên một số mạng con có các loại lỗi khác nhau nên dự tính một mức dịch vụ là mức kém nhất trong các mức dịch vụ của các mạng con mà nó hoạt động trên đó.

Về phần thiết lập liên kết giao vận, các thực thể giao vận ngang hàng phải thiết lập mức dịch vụ mạng nâng cao để đảm nhận được việc cung cấp QOS cho phép đối với liên kết này. Điều này liên quan tới sự lựa chọn tập các thủ tục sẽ được sử dụng trong suốt thời gian kết nối. Sự lựa chọn này được thực hiện như là một phần của thủ tục thiết lập liên kết song song với thoả thuận về QOS.

11.4 Các lớp giao vận

Có một tập năm mức cơ sở hay lớp nâng cao dịch vụ mạng khả dụng ở tầng giao vận. Theo một số giả thuyết, mỗi lớp liên quan tới ba loại mạng con đã đưa ra ở trên. Các thực thể giao vận trong quá trình thiết lập TC thực hiện dàn xếp thủ tục

được mô tả ở trên bằng việc thoả thuận một giao vận được dùng trên mạng đối với TC cụ thể này. Việc lựa chọn lớp vốn gắn liền với tập các thủ tục giao vận liên đới.

Lớp 0, lớp đơn giản, với tổng chi phí ít nhất đảm bảo một liên kết giao vận được thiết kế để sử dụng với dịch vụ mạng có mức độ lỗi ở cả hai kiểu có thể chấp nhận được. Kết quả là kiểu dịch vụ mạng này bảo đảm truyền dữ liệu tin cậy, chỉ yêu cầu mức hoạt động giao vận cơ bản. Lớp 1, lớp khôi phục lỗi cơ bản, với tổng chi phí ít nhất đảm bảo một liên kết giao vận cơ bản được thiết kế để sử dụng với các dịch vụ mạng có mức độ lỗi dư thừa chấp nhận được, nhưng lỗi tín hiệu thì không. Nó xử lý các lỗi tín hiệu, như ngắt kết nối mạng, không làm ảnh hưởng tới người dùng TS. Lớp 2, lớp dồn kênh, như lớp 0, nhưng có các cơ chế bổ sung để hỗ trợ dồn kênh các liên kết giao vận thành các liên kết mạng đơn lẻ. Lớp 3, lớp phát hiện và khôi phục lỗi, như lớp 1, nhưng có bổ sung các cơ chế dồn kênh. Lớp 4, lớp phát hiện và khôi phục lỗi thoả mãn tất cả khả năng của lớp 3 cùng với các cơ chế cần thiết để phát hiện và khôi phục từ các lỗi không được nhà cung cấp NS báo hiệu. Lớp này cũng bảo đảm tăng thông lượng và tăng cường khả năng phục hồi chống lại lỗi từ nhà cung cấp NS. Nó được thiết kế để sử dụng trên loại mạng có mức độ lỗi dư thừa không chấp nhận được.

11.5 Các thủ tục giao vận

Giao thức vận tải được định nghĩa như một tập các thủ tục, mỗi thủ tục liên quan tới một hành động cụ thể. Ẩn trong lớp giao vận thoả thuận cuối cùng là sự lựa chọn một tập con các thủ tục này, đó là các thủ tục cần thiết để đảm bảo chức năng tiện ích của lớp đó. Nghiên cứu các thủ tục này sẽ thấy rằng nhiều thủ tục là cơ sở để cung cấp dịch vụ giao vận cơ bản. Những thủ tục này hình thành một tập các thủ tục phổ biến với tất cả các lớp giao vận. Các thủ tục này bao gồm (nhưng không hạn chế) như sau: gán liên kết mạng; truyền TPDU; phân đoạn và ráp lại; ghép nối và tách; thiết lập liên kết; từ chối kết nối; giải phóng chuẩn; huỷ lỗi; kết hợp TPDUs với các liên kết giao vận; đánh số TPDU; truyền dữ liệu expedited; gán lại sau lỗi; lưu trước khi báo nhận TPDUs; tái đồng bộ; dồn kênh và tách kênh; điều khiển luồng thông tin rõ; tổng kiểm tra; cố định tham trỏ; tái truyền vào thời gian chết; sắp lại thứ tự; điều khiển dừng; xử lý lỗi giao thức; tách và tổ hợp lại.

Gán liên kết mạng là một thủ tục chung ở tất cả các lớp. Không thể thiết lập một liên kết lớp giao vận trước khi thực hiện một phép gán. Phép gán là sự kết hợp TC với liên kết mạng NC. Trong quá trình thiết lập TC , không thể tiến hành thiết lập cho đến khi một phép gán được thực hiện. Tuy nhiên, một khi phép gán đã thực hiện và TC được thiết lập, thì TC có thể vẫn được nhớ lại và gán với một NC khác. Trong mỗi trường hợp, thực thể giao vận có thể lựa chọn thiết lập một NC mới hoặc sử dụng NC đang tồn tại tương ứng.

Thủ tục *truyền TPDU* điều phối việc truyền các TPDU giữa các thực thể giao vận ngang hàng. Nó sử dụng các phần tử dịch vụ dữ liệu expedited chuẩn N-DATA và N-EXPEDITED-DATA. Thủ tục này chung cho tất cả các lớp giao vận. Trong

các PDU dữ liệu giao vận, dữ liệu (DT-DaTa) và dữ liệu expedited (ED-Expedited Data), cấu trúc sau này ám chỉ phần điều khiển PDU, thông tin điều khiển giao thức (PCI-protocol control information) gồm một định danh cùng với tham số độ dài chỉ độ dài của PCI trong PDU. Tuy nhiên, không có chỉ báo độ dài đối với trường dữ liệu và PDU. Toàn bộ được chuyển tới nhà cung cấp NS như NSDU, và xuất phát từ độ dài tổng thể của NSDU này, mà thực thể giao vận nhận có thể xác định kích thước của trường dữ liệu được tính bằng độ dài NSDU trừ đi độ dài PCI.

Phân đoạn và ráp lại cũng có thể thực hiện trong tầng giao vận. Một TSDU do người dùng TS yêu cầu truyền có thể vượt quá giới hạn đã đặt dựa vào số lượng dữ liệu có thể truyền được giữa các thực thể giao vận ngang hàng trong một TPDU dữ liệu đơn lẻ. Một giới hạn như thế phản ánh các ràng buộc trong dịch vụ mạng trên NSDUs liên kết với phần tử dịch vụ N-DATA. Trong trường hợp này, phân đoạn được đề cập tới để cắt TSDU thành nhiều DT TPDU có kích thước thích hợp. Khi thực thể giao vận ngang hàng nhận được, thứ tự của các TPDU DT ứng với TSDU đã phân đoạn sẽ được ráp lại trong TSDU đơn lẻ. Một chỉ báo dịch vụ dữ liệu sẽ được đưa ra cho người dùng TS cuối cùng khi nhận được TSDU hoàn chỉnh này. Tham số kết thúc giao vận (EOT- End of Transport) trong mỗi DT TPDU chỉ được đặt vào lúc một TSDU hoàn chỉnh đã được truyền xong, và được dùng để thực thể giao vận tiếp nhận nhận biết TSDU bị phân đoạn. Ở đâu TSDUs được chứa trọn vẹn trong DT (Data Transport) TPDUs thì EOT được đặt trên mỗi DT TPDU.

Tầng giao vận cũng đảm bảo việc *ghép nối và tách* TPDUs. Có thể ghép nối một số TPDUs trong một NSDU đơn lẻ để thực thể giao vận tiếp nhận truyền và tách khi nhận được. Nếu một TPDU là một nhóm TPDUs ghép nối thì nó phải là TPDU cuối cùng của quá trình ghép nối, và như vậy có thể là TPDU duy nhất.

Thủ tục *thiết lập liên kết* có ở tất cả các lớp giao vận để thiết lập TC sau phép gán với một liên kết mạng thành công. Một liên kết giao vận được thiết lập với sự thoả thuận giữa các thực thể ngang hàng qua trao đổi PDUs thích hợp được truyền đi bằng cách sử dụng dữ liệu mạng chuẩn, N-DATA. Nhờ kết quả thoả thuận, mà xác định được QOS được duy trì và lớp giao vận được sử dụng trên mạng. Có các thủ tục tuỳ chọn phụ thuộc vào các lớp cụ thể mà bản thân chúng không buộc phải có trong lớp, và vì thế sự thoả thuận về các tính năng tuỳ chọn cũng được thực hiện vào thời gian này. Ví dụ, "truyền dữ liệu expedited" và "ghi nhớ trước khi báo nhận TPDU" là hai tính năng tuỳ chọn ở lớp 1.

Từ chối liên kết là một thủ tục được khởi đầu bằng thực thể giao vận đáp khi trả lời hoặc một yêu cầu T-DISCONNECT từ người dùng TS đáp, hoặc không có khả năng tuân theo các yêu cầu của thực thể giao vận khởi đầu truyền theo CR TPDU. Từ chối liên kết được thực hiện bằng cách gửi một TPDU yêu cầu ngắt (DR-disconnect request) tới bộ khởi đầu sử dụng dữ liệu mạng chuẩn.

Có hai kiểu *thủ tục giải phóng* - giải phóng chuẩn và giải phóng lỗi. Có thể mô tả giải phóng chuẩn thông qua hai dạng - ẩn (không tường minh) và hiện (tường minh). Ở lớp 0, dạng ẩn của giải phóng chuẩn được thực hiện bằng việc ngắt liên kết mạng (NC-network connection) sử dụng yêu cầu N-DISCONNECT, kết quả nhận được bao hàm cả giải phóng TC liên đới. Dạng tường minh của giải phóng chuẩn được kết hợp với tất cả các lớp khác. Dưới dạng tường minh, TC được giải phóng do hành động xác nhận liên quan tới sự trao đổi giữa các thực thể ngang hàng theo yêu cầu ngắt (DR) và TPDUs xác nhận ngắt (DC) sử dụng dữ liệu mạng chuẩn. Giải phóng lỗi chỉ được dùng ở lớp 0 và 2. Thủ tục này dùng để giải phóng liên kết giao vận sau khi nhận được lỗi tín hiệu từ nhà cung cấp NS. Người dùng TS được thông báo giải phóng nhờ chỉ báo T-DISCONNECT.

Tổ hợp của các TPDUs với các liên kết giao vận là một thủ tục dùng trong tất cả các lớp trong khi truyền dữ liệu. Có ba hành động kèm theo khi một thực thể giao vận truyền NSDU từ nhà cung cấp dịch vụ mạng. Thứ nhất, kiểm tra để xác định rằng có thể giải mã NSDU thành một hoặc nhiều dãy ghép TPDUs. Thứ hai, nếu phát hiện dãy ghép thì gọi thủ tục tách. Cuối cùng, ở đâu có nhiều TCs được liên kết với NC qua cái mà NSDU nhận được, thì bảo đảm TPDUs được gắn với liên kết giao vận thích hợp.

Đánh số TPDU là một tính năng được yêu cầu để đảm bảo thực hiện thành công các thủ tục nào đó. Đây là một số thứ tự được định danh là một tham số trong PCI và được đưa vào mỗi DT TPDU. Các thủ tục này bao gồm điều khiển luồng thông tin, sắp lại thứ tự, khôi phục.

Thủ tục *truyền dữ liệu expedited* đặt dữ liệu người dùng dịch vụ giao vận do yêu cầu T-EXPEDITED-DATA cung cấp thành một trường của TPDU dữ liệu expedited (ED). Mặc dầu không cần xác nhận dịch vụ vận chuyển dữ liệu expedited, nhưng giao thức vận tải đòi hỏi xác nhận thủ tục thực thể ngang hàng, nên mỗi ED TPDU phải được báo nhận vào lúc tiếp nhận thực thể giao vận ngang hàng bằng cách dùng TPDU nhận biết dữ liệu expedited (EA). Tại một thời điểm bất kỳ, đối với mỗi hướng luồng dữ liệu của TC không thể có quá một ED TPDU báo nhận tồn tại.

Thủ tục *gán lại sau lỗi* được gọi khi nhận được một lỗi tín hiệu mạng, báo mất liên kết mạng được gán cho liên kết giao vận. Kết quả là liên kết giao vận được gán cho liên kết mạng khác, hoặc đang tồn tại hoặc do thực thể giao vận sở hữu hoặc tạo mới theo mục đích. Thủ tục tái đồng bộ được gọi khi thực hiện gán lại; tuy nhiên, không nên tiến hành gán lại, TC sẽ được xem như đã giải phóng và cố định tham trỏ giao vận. Thủ tục *cố định tham trỏ* (mô tả ở bên dưới trong đoạn cố định các tham trỏ) được sử dụng sau đó để đảm bảo rằng một tham trỏ không bị gán lại cho một TC khác sau khi được cố định.

Ghi nhớ trước khi có báo nhận TPDUs bảo đảm các cơ chế mà nhờ đó thực thể giao vận đang truyền có thể duy trì "các bản sao" của TPDUs cho đến khi nhận được một báo nhận tường minh từ thực thể ngang hàng. Có thể không có báo nhận sau một khoảng thời gian trôi qua, hoặc có thể xảy ra lỗi tín hiệu, khi đó TPDUs có thể bị truyền lại. Việc mất TPDUs liên tục sẽ dẫn tới QOS xuống thấp dưới mức chấp nhận cho phép và liên kết giao vận bị ngắt.

Tái đồng bộ là một thủ tục dùng để phục hồi liên kết giao vận trở lại bình thường sau khi gán lại TC sau lỗi liên kết mạng hoặc sau khi nhà cung cấp dịch vụ mạng chỉ báo có vấn đề trong kết nối mạng. Mục đích của việc tái đồng bộ thực thể giao vận là hồi phục hoạt động trên kết nối giao vận đang tồn tại tại thời điểm biến cố bắt đầu. Tái đồng bộ chỉ có được nhờ thực thể giao vận khởi đầu. Thực thể ngang hàng chỉ đóng vai trò bị động trong quá trình tái đồng bộ. Vì cả hai thực thể đều cần thiết cho việc tái đồng bộ, nên một trong các thực thể giao vận ngang hàng phải đóng vai trò bị động, nếu không tái đồng bộ bằng cả hai thực thể ngang hàng sẽ dẫn đến các giải pháp giải quyết xung đột biến cố không cần thiết. Thực thể bị động đáp lại bằng việc chọn thời gian nhận TPDUs liên quan tới tái đồng bộ từ bên khởi xướng liên kết giao vận. Nếu tái đồng bộ không xảy ra, thời gian đã chọn hết hiệu lực và thực thể xem như liên kết giao vận đã giải phóng và cố định tham trỏ.

Các thủ tục dồn kênh và tách kênh khả dụng với các lớp 2, 3 và 4. Quá trình này cho phép nhiều liên kết giao vận dùng chung một NC đơn lẻ. Dồn kênh đưa ra vị trí mà một thực thể giao vận truyền hoặc nhận TPDUs thuộc liên kết giao vận khác nhau trên cùng liên kết mạng. Thực thể giao vận nhận TPDUs phải thực hiện tách kênh. Tách kênh được thực hiện bằng việc gọi thủ tục liên kết TPDUs ở nơi xác định liên kết giao vận với cái có liên quan tới các TPDUs tách rời. Các hiệu suất mạng có được ở nơi sử dụng đồng thời cả hai thủ tục dồn kênh và ghép nối, và truyền một NSDU đơn lẻ chứa các TPDU ghép nối của các liên kết giao vận khác nhau.

Điều khiển luồng tường minh là một thủ tục khả dụng với các lớp 2, 3 và 4. Ở lớp 2 điều khiển luồng tường minh là tuỳ chọn, nhưng ở lớp 3 và 4 nó là bắt buộc. Thủ tục này điều chỉnh luồng DT TPDUs giữa các thực thể giao vận ngang hàng trên một liên kết giao vận trong tầng giao vận và hành động một cách độc lập với điều khiển luồng sẵn có trong mạng.

Tổng kiểm tra là một thủ tục tuỳ chọn chỉ dùng ở lớp 4. Tổng kiểm tra là một giá trị tính toán theo thuật toán định nghĩa trong đặc tả giao thức có các octet bao gồm TPDU với cái liên kết với nó xem như các đối của nó. Sau khi truyền trên mạng, giá trị tổng kiểm tra được tính toán lại và so sánh với giá trị trong tham số TPDU. Sẽ có sai lạc nếu các giá trị này khác nhau. Trong trường hợp này, TPDU bị bỏ qua, không chấp nhận gửi đi, cuộc truyền thực thể giao vận tái truyền TPDU.

Cố định các tham trỏ được các lớp 1, 3 và 4 sử dụng . Chúng được dùng để đảm bảo rằng một tham trỏ không bị gán lại cho một TC khác sau khi bị cố định. Các tham trỏ là thông tin liên quan tới định danh của TC. Tái truyền vào thời gian chết là một thủ tục dùng để bảo đảm rằng bên gửi TPDUs tái truyền chúng khi xuất hiện khả năng mất chúng. Trong trường hợp này, cuộc truyền thực thể giao vận phát hiện TPDUs bị thất lạc khi nó không được thừa nhận trong một khoảng thời gian cố định và khi những cái đã được công nhận đang tồn tại. Khi điều này xảy ra, tái truyền TPDU đầu tiên theo thứ tự của các TPDU không được thừa nhận, đồng hồ được khởi động lại và bắt đầu có hiệu lực. Sau một vài cuộc tái truyền ngoài ý muốn, thực thể giao vận đang gửi sẽ gọi thủ tục giải phóng và thông báo cho người dùng TS về lỗi. Chỉ lớp 4 sử dụng thủ tục này.

Thủ tục *sắp lại thứ tự* dùng để sắp xếp các DT TPDU bị mất thứ tự do nhà cung cấp dịch vụ mạng thực hiện. Thủ tục này bảo đảm các octet có thứ tự đúng được phân phối tới người dùng dịch vụ giao vận vì mỗi TPDU bất chấp tính không nhất quán của mạng có thể dẫn tới các TPDU ngoài thứ tự. Mất thứ tự có thể xảy ra khi thực thể giao vận cắt một TPDU thành nhiều TPDU và ở nơi tách các kết quả trong các TPDU đang di chuyển giữa các hệ thống cuối trải trên một số liên kết mạng.

Thủ tục xác định ngắt liên kết mạng không báo trước là thủ tục *điều khiển tính bất hoạt (inactivity control)*. Thủ tục này chỉ sử dụng ở lớp 4, được gọi khi đồng hồ bấm giờ bất hoạt do thực thể giao vận duy trì hết hiệu lực. Nó tính khoảng thời gian không nhận được TPDU nào. Thủ tục điều khiển tính bất hoạt hết hiệu lực sau một khoảng thời gian thực sự dài và sau đó gọi thủ tục giải phóng chuẩn. Để bảo vệ chống lại sự kết thúc do sự bất hoạt dẫn đến tắc nghẽn giao vận thì khoảng thời gian phải đủ dài để không bỏ qua thời gian có một liên kết tốt.

Thủ tục *xử lý các lỗi giao thức* được dùng khi nhận được một TPDU không thể diễn dịch theo các quy tắc của chuẩn, khi không nhận được lỗi nào và không có các lỗi tổng kiểm tra. Có thể có một vài hành động cụ thể khác nhau phụ thuộc vào các chi tiết vận hành của các lỗi. Thủ tục này được dùng ở tất cả các lớp.

Liên kết giao vận có thể tạo khả năng sử dụng nhiều liên kết mạng thông qua thủ tục *tách và tái tổ hợp*. Kết quả của thủ tục này có thể là thông lượng tăng lên hoặc khả năng phục hồi đề phòng lỗi lớn hơn trong các mạng thực sự không tin cậy. Một khi, một liên kết tồn tại giữa một liên kết giao vận và nhiều liên kết mạng, thì các TPDU của liên kết giao vận đó có thể được truyền trên bất kỳ liên kết mạng nào trong các liên kết mạng. Vì thế, các TPDU có thể đến thực thể giao vận ngang hàng không theo thứ tự. Thủ tục này chỉ khả dụng với lớp 4.

11.6 Dữ liệu expedited

Dữ liệu expedited là dạng đặc biệt của dữ liệu truyền, dữ liệu đó được đảm bảo đến bên nhận trước bất kỳ dữ liệu nào được truyền sau đó bằng cách gọi một

dịch vụ dữ liệu nào đó. Lưu ý rằng dữ liệu được truyền nhờ sử dụng dữ liệu expedited sẽ đến trước dữ liệu thông thường đã sẵn sàng để truyền nhưng do người dùng mà đến lúc này vẫn chưa được truyền; tuy nhiên, nó sẽ không đến trước bất kỳ dữ liệu expedited nào đưa ra trước đó nhưng chưa cấp phát. Ở tầng giao vận có thể thấy phương pháp tạo ra dữ liệu expedited, trong khi đó nó thường chỉ được nhận biết ở các tầng cao của mô hình OSI.

Dữ liệu expedited phụ thuộc lớp. Điều đó có nghĩa là dữ liệu expedited được cung cấp trọn vẹn trong các lớp 2, 3 và 4 nhưng không được cung cấp ở lớp 0. Ở các lớp này, các TPDU expedited được gửi với tư cách ED TPDUs trên dịch vụ mạng dữ liệu thông thường. Ở lớp 1, hiệu quả expedited được đảm bảo nhờ cơ chế expedited trong tầng giao vận cùng với việc sử dụng dịch vụ mạng dữ liệu expedited để truyền ED TPDUs. Nếu dịch vụ mạng này không sẵn sàng thì sử dụng dịch vụ mạng dữ liệu thông thường.

11.7 Chất lượng dịch vụ

Một ứng dụng dùng khái niệm chất lượng dịch vụ (QOS) để đưa ra những yêu cầu truyền thông với các tầng thấp hơn nó. Quá trình chuyển tín hiệu này diễn ra qua tham số QOS đi kèm với yêu cầu thiết lập liên kết hoặc mục dữ liệu không liên kết truyền từ tầng cao tới tầng thấp ngang qua ranh giới dịch vụ tầng giao vận. Tầng giao vận sử dụng tham số QOS tương tự trong yêu cầu thiết lập liên kết hoặc mục dữ liệu không liên kết mà nó chuyển tới tầng mạng. Nếu tầng mạng không đảm bảo một QOS thoả đáng thì tầng giao vận nên nâng cấp QOS đã có lên mức cần thiết bằng cách bổ sung giá trị vào giao thức riêng của nó. Thực hiện điều này bằng việc lựa chọn loại giao thức vận tải thích hợp và các tuỳ chọn.

Tham số QOS có thể truyền một lượng thông tin lớn bao gồm các yêu cầu như thông lượng, mức độ lỗi dư thừa và khả năng mất liên kết. QOS có thể được biểu diễn như một tập tiêu chuẩn thực thi. Nói chung chúng nằm trong hai nhóm: tốc độ và độ chính xác/ độ tin cậy. Tiêu chuẩn của giai đoạn thiết lập liên kết gồm các tham số QOS về khả năng trì hoãn thiết lập và không thiết lập được. Tiêu chuẩn ở giai đoạn giải phóng liên kết gồm các tham số QOS về khả năng trì hoãn giải phóng và không giải phóng được. Tiêu chuẩn ở giai đoạn truyền dữ liệu gồm các tham số QOS về thông lượng, độ trễ truyền, mức độ lỗi dư thừa, khả năng phục hồi liên kết và khả năng không truyền được.

Thành phần của QOS liên quan tới an toàn được gọi là QOS bảo vệ. Nó được dùng để thông báo các dịch vụ an toàn cần gọi và năng lực của cơ chế cần dùng để hỗ trợ dịch vụ an toàn. TLSP và NLSP định nghĩa QOS bảo vệ gồm một thành phần đối với mỗi dịch vụ an toàn liên quan. Với mỗi thành phần, nó có khả năng định rõ một giá trị nguyên chỉ mức yêu cầu đối với dịch vụ đó. Phạm vi của các số nguyên có sẵn, ý nghĩa của các giá trị cụ thể chưa được định rõ trong chuẩn. Chúng được bao hàm trong tập các quy tắc an toàn được thoả thuận cụ thể cho liên kết an toàn

khi sử dụng. Việc dùng các số nguyên bao hàm một quan hệ về thứ tự giữa các mức, với mức cao hơn ý nói tới một cơ chế mạnh hơn.

Có thể bổ sung giải pháp dựa vào mức với QOS bảo vệ bằng cách truyền một nhãn an toàn giữa các tầng, chẳng hạn giữa các tầng dịch vụ vận tải và mạng. Nhãn này dùng như một chỉ báo về QOS yêu cầu. Các nhãn an toàn dùng cho mục đích này có thể giống hệt các nhãn dùng để hỗ trợ điều khiển truy nhập, nhưng chúng sẽ có ý nghĩa khác. Ví dụ, nhãn "không được xếp nhóm chỉ tính nhạy cảm" có thể bao hàm ý sử dụng cơ chế bảo mật mức thương mại dựa vào mã DES, nơi có nhãn "bí mật" ý nói sử dụng cơ chế bảo mật với thuật toán mã hoá loại cao hơn.

Ở tầng giao vận hoặc tầng mạng, việc thiết lập QOS cho một liên kết đòi hỏi phải có sự thoả thuận giữa hai thực thể ngang hàng, với mục đích là các yêu cầu QOS tương xứng nhất giữa hai người dùng dịch vụ cùng với những khả năng của hai nhà cung cấp dịch vụ. Liên quan đến QOS bảo vệ, một phần tử khác được đưa vào. Ở mức nhà cung cấp dịch vụ, mỗi thực thể ngang hàng có thể xen những ràng buộc QOS bảo vệ quyền phân phối. Các ràng buộc này là các yêu cầu an toàn tối thiểu do nơi quản trị hệ thống đặt ra để thoả mãn chính sách an toàn hệ thống cục bộ. Ví dụ, một ứng dụng của người dùng có thể đòi hỏi một liên kết hoàn toàn không có bảo vệ an toàn nhưng phụ thuộc vào các hoàn cảnh, mà nơi quản trị hệ thống cục bộ tại một trong hai thực thể ngang hàng có thể nâng cấp QOS yêu câù để có sự bảo mật ở mức bắt buộc nào đó. Việc thoả thuận QOS bảo vệ có thể thực hiện một phần khi thiết lập liên kết an toàn và một phần khi trao đổi các tham số QOS thường xuyên trong giao thức thiết lập liên kết.

11.8 Kiến trúc an toàn

Giao thức an toàn tầng giao vận (TLSP) được đặt hoàn toàn trong tầng giao vận. Trừ việc truyền các tham số QOS bảo vệ, sự tồn tại và hoạt động của TLSP hoàn toàn trong suốt với cả các tầng bên trên và tầng mạng bên dưới. TLSP được thiết kế để bổ sung vào các giao thức tầng giao vận thông thường mà không phải để thay đổi chúng. TLSP làm việc kết hợp với đơn vị dữ liệu giao thức vận tải (TPDU) và các thủ tục xử lý kèm theo sự bổ sung một tầng giao thức con khác. Các TPDU chuẩn tắc được bảo vệ bằng việc đóng gói trong TLSP PDUs tại nơi gửi trước khi truyền tới tầng mạng. Sự đóng gói được gỡ bỏ ở nơi nhận để sản sinh TPDU chuẩn tắc mà sau đó tiếp tục chịu xử lý của giao thức chuẩn.Các thủ tục xử lý được diễn giải trong ISO/IEC 8073 với tiến trình xử lý có liên kết và trong ISO/IEC 8602 với tiến trình xử lý không liên kết. Bảo vệ tất cả các PDU chuẩn tắc kết hợp với một liên kết vận tải bị chi phối bởi một liên kết an toàn trong trường hợp có liên kết. Nói cách khác, cùng một dạng bảo vệ được áp dụng cho tất cả các PDU. Tuy nhiên, lược đồ bảo vệ có thể trở nên phức tạp hơn ở nơi mà bộ dồn kênh tầng giao vận đặt thấp hơn TLSP. Trong tình huống này, các liên kết vận tải khác nhau hay các TPDU không liên kết khác nhau được cung cấp các kiểu bảo vệ khác nhau, dù rằng các PDU được dồn kênh trên một liên kết mạng giữa hai hệ thống cuối. Nơi nào sử dụng các thủ tục ghép nối tầng giao vận thì cùng một liên kết an

toàn phải bảo vệ tất cả các PDU được ghép nối. Các thủ tục ghép nối được đặt bên trên TLSP. Thứ tự ghép nối của các TPDU được TLSP xử lý tương tự với một TPDU đơn lẻ không ghép nối.

11.9 Các cơ chế an toàn

Hàm đóng gói của TLSP hỗ trợ việc cung cấp một vài dịch vụ an toàn và có thể kéo theo tổ hợp các cơ chế an toàn nào đó được yêu cầu. Các cơ chế này là nhãn an toàn, con trỏ hướng, giá trị kiểm tra toàn vẹn (ICV), đệm mã hoá (padding) và mã hoá.

Nhãn an toàn được được thêm vào đầu TPDU để hỗ trợ cung cấp dịch vụ điều khiển truy nhập. Các trường được cung cấp để định nghĩa một định danh hợp pháp xác định duy nhất cùng với giá trị nhãn theo một khuôn dạng do tác quyền xác định điều khiển. OSI không định nghĩa khuôn dạng nhãn cụ thể. *Trỏ hướng* là một tiền tố của trường cờ gồm một bit chỉ hướng truyền TPDU. Tiền tố này chứa tham trỏ tới khởi đầu đoán nhận/ quan hệ đáp xác định khi thiết lập liên kết an toàn và được sử dụng để chống những tấn công có chủ định. *ICV* là một giá trị được tính toán và gắn thêm, đòi hỏi một tiến trình phải bổ sung các octets vào dữ liệu trước khi tính ICV. ICV là một cơ chế cơ bản cho việc cung cấp cả hai dịch vụ toàn vẹn liên kết và toàn vẹn không liên kết. *Đệm mã hoá* là đệm các octets vào dữ liệu ở nơi nó được yêu cầu theo thuật toán mã hoá hoặc vì các mục tiêu ẩn độ dài của các PDU cần bảo vệ. Mã hoá là cơ chế đáp ứng bảo mật liên kết hoặc không liên kết và cung cấp sự bảo vệ thông tin cần thiết phát sinh từ các cơ chế an toàn khác.

Đối với trường hợp có liên kết, một số dịch vụ an toàn được cung cấp thông qua cách xử lý phối hợp của hàm đóng gói TLSP và các thủ tục chuẩn của tầng giao vận. Toàn vẹn thứ tự được thực hiện nhờ các số thứ tự do giao thức vận tải lớp 2, 3 hoặc 4 cùng với toàn vẹn liên kết cung cấp. Các hệ thống đánh số thứ tự riêng rẽ được duy trì đối với các luồng dữ liệu chuẩn và dữ liệu expedited. Khôi phục toàn vẹn được thực hiện nhờ các thủ tục khôi phục giao thức vận tải lớp 4 cùng với toàn vẹn liên kết. Toàn vẹn thứ tự không thể dùng với giao thức vận tải lớp 0 hoặc lớp 1.

Xác nhận thực thể thực chất là một tiến trình hai giai đoạn. Giai đoạn thứ nhất là thiết lập liên kết an toàn dẫn đến trong mỗi thực thể vận tải nhận một khoá có thể dùng để thẩm tra thực thể khác về định danh của nó. Ngay sau khi thiết lập liên kết an toàn hoàn thành, giai đoạn thứ hai là xác nhận thực thể khi thiết lập liên kết. Điều này được thực hiện thông qua việc mỗi thực thể xác nhận thông tin về khoá được gắn vào bằng cách dùng khoá đó để sinh ra ICV mã hoá khi đóng gói TPDU yêu cầu liên kết. Với sự bảo vệ chống lặp lại, các TPDU yêu cầu liên kết và xác nhận liên kết sử dụng các giá trị tham trỏ liên kết, trong thời gian khoá có hiệu lực các giá trị này phải duy nhất. Điều này thực hiện dễ dàng nhất khi có một thành

phần về thứ tự trong các tham trỏ liên kết. Sau đó hệ thống sẽ tăng thành phần này đối với mỗi thiết lập liên kết mới có liên quan.

Ở trường hợp không liên kết cũng sử dụng một tiến trình hai giai đoạn cơ bản giống để xác thực dữ liệu gốc. Sử dụng khoá dùng trong tiến trình đóng gói để có xác nhận yêu cầu về TPDU không liên kết nhờ thông tin xác thực khoá đó. Cùng với khoá dùng cho các mục đích xác thực, các địa chỉ ngang hàng trong thiết lập liên kết hoặc các TPDU không liên kết cũng được yêu cầu để kiểm tra tính nhất quán khi cần bảo vệ chặt hơn chống các nguy cơ giả mạo.

11.10 Các thuộc tính liên kết an toàn

TLSP cũng kết hợp chặt chẽ các tính năng bao gồm cả các thuộc tính tổ hợp an toàn và tập các quy tắc an toàn thoả thuận (ASSR-agreed set of security rules). Thuật ngữ tổ hợp an toàn dùng để mô hình hoá các tập thông tin liên quan lưu giữ ở hai hay nhiều hệ thống nhằm các mục đích bảo đảm có cùng kiểu bảo vệ thứ tự đối với các cuộc truyền dữ liệu khác nhau. Các mục thông tin lưu trong một tổ hợp an toàn được hiểu như là các thuộc tính của tổ hợp an toàn đó. Những định danh tổ hợp an toàn gồm định danh cục bộ và định danh từ xa, đó là các xâu octets có độ dài do ASSR xác định.

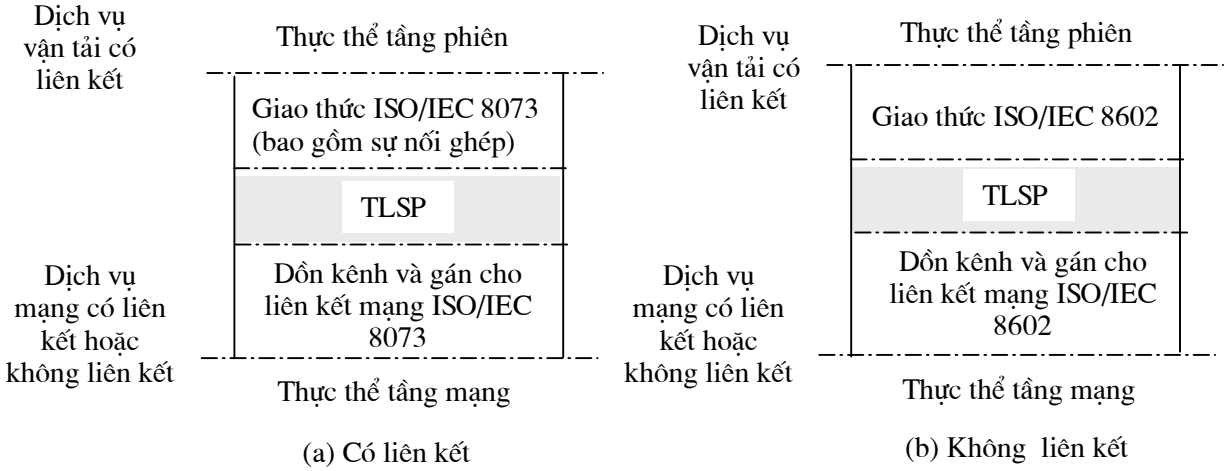
Thuật ngữ ASSR dùng để mô tả sự thoả thuận giữa hai hay nhiều hệ thống có sử dụng các cơ chế an toàn và các giá trị hệ thống được đưa vào các tham số của các cơ chế này. Điều này ngăn ngừa việc dàn xếp các chi tiết kỹ thuật với mỗi thiết lập liên kết an toàn bằng cách dùng tập các quy tắc an toàn thoả thuận trong gói thông tin kỹ thuật an toàn xác định trước. Các quy tắc an toàn này được đăng ký và gán một định danh duy nhất để sau đó tất cả những người dùng đến nhận biết.

Các thuộc tính kết hợp an toàn khác do thực thể TLSP nắm giữ gồm số thứ tự toàn vẹn, cơ cấu ICV, kỹ thuật mã hoá, con trỏ khởi đầu/ đáp, QOS bảo vệ, cơ cấu nhãnvà địa chỉ thực thể TLSP ngang hàng. Những số thứ tự cuối cùng gửi hoặc nhận của các luồng dữ liệu chuẩn và expedited là các thuộc tính thứ tự toàn vẹn. Thuộc tính cơ cấu ICV và kỹ thuật mã hoá gồm thuật toán, mức độ modul hoá khoá, tham trỏ khoá và kích thước khối để xác định phần đệm cần thiết. Khi lựa chọn hướng thì con trỏ khởi đầu/đáp chỉ ra thực thể TLSP nào đóng vai trò khởi đầu và thực thể TLSP nào đóng vai trò đáp. Như đã đề cập trước đây, con trỏ QOS bảo vệ được định nghĩa là một nhãn QOS cộng với một giá trị mức nguyên với mỗi dịch vụ tồn tại. ASSR xác định phạm vi các giá trị nguyên và định dạng của nhãn QOS. Tập các nhãn an toàn cho phép đối với liên kết an toàn được nói đến chính là các thuộc tính về cơ cấu nhãn. Các thuộc tính về cơ chế an toàn chỉ các cơ chế an toàn nào được sử dụng (ví dụ, xác nhận thực thể, các nhãn an toàn, các giá trị kiểm tra toàn vẹn, các số thứ tự toàn vẹn và mã hoá). Cuối cùng, địa chỉ thực thể TLSP là tham trỏ kết nối được lưu giữ nếu liên kết an toàn bị ràng buộc với một kết nối giao vận cụ thể.

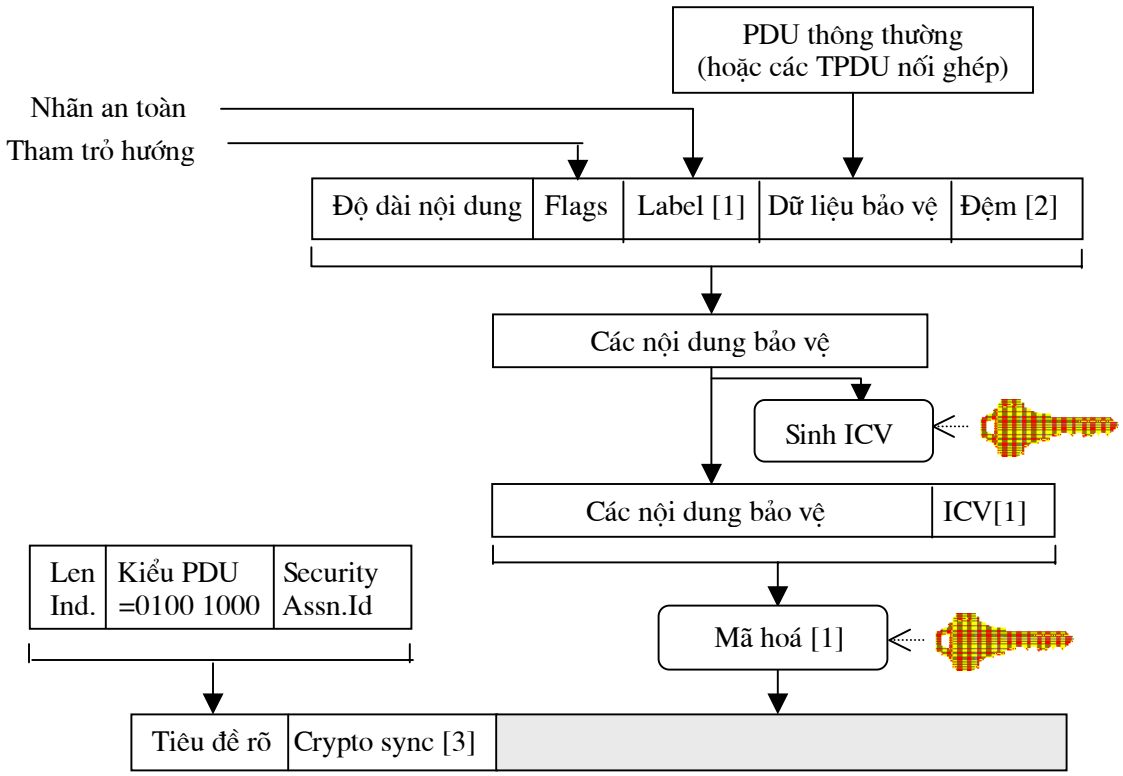
11.11 Giao thức tổ hợp an toàn

Một tổ hợp an toàn có thể được thiết lập thông qua các trao đổi giao thức tầng ứng dụng (mặc dù trao đổi an toàn do giao thức tầng thấp hơn sử dụng), hoặc thông qua các trao đổi giao thức ở cùng tầng kiến trúc sử dụng trao đổi an toàn, hoặc thông qua cách thức không định rõ (có thể hoặc không thể kéo theo các cuộc truyền thông dữ liệu trực tuyến). Một giao thức tổ hợp an toàn tuỳ chọn dùng để điều tiết các trao đổi giao thức sử dụng giao thức an toàn ở cùng tầng kiến trúc.

Các khuôn dạng PDU có khả năng hỗ trợ việc thiết lập tổ hợp an toàn, giải phóng tổ hợp an toàn và thiết lập khoá dữ liệu mới (đặt lại khoá) trong tổ hợp an toàn đang hoạt động được định nghĩa bởi giao thức tổ hợp an toàn. Việc thiết lập các khoá và giá trị dữ liệu khởi đầu đối với tất cả các thuộc tính tổ hợp an toàn là chức năng của việc thiết lập tổ hợp an toàn.



Sắp đặt kiến trúc của TLSP



Chú ý: [1] Nhãn an toàn, ICV, và/hoặc mã hoá có thể bỏ qua, tuỳ theo các yêu cầu liên kết an toàn.

[2] Các trường đệm tách biệt có thể được bao hàm theo tuỳ chọn nhằm thoả mãn nhu cầu sinh ICV và mã hoá

[3] Trường *crypto sync* là tuỳ chọn; nó có thể mang dữ liệu thuật toán cụ thể

CHƯƠNG 12-CÁC GIAO THỨC AN TOÀN TẦNG ỨNG DỤNG CỦA CÁC MẠNG[3]

12.1 Sự cần thiết của các giao thức an toàn tầng ứng dụng

Sự tăng trưởng nhanh chóng về khả năng sử dụng Internet đã làm thay đổi những giao dịch công tác hàng ngày từ máy fax và điện thoại tới thư điện tử và thương mại điện tử. Sự thay đổi này có thể là do mối liên kết kinh tế rộng rãi của Internet cũng như năng lực của Internet đối với các kiểu giao dịch phức tạp hơn. Các chuyên gia an toàn phải hiểu các vấn đề và rủi ro đi liền với các giao dịch này nếu họ muốn cung cấp các giải pháp an toàn để giao dịch Internet có khả năng tồn tại và phát triển.

Sự phân bố trên Internet tạo cho nó khả năng điều khiển các giao dịch quốc tế, đa nhóm, đa địa điểm không tính đến sự khác nhau về thời gian hay ngôn ngữ. Tuy nhiên, mức độ liên kết này đã tạo ra tình thế khó xử nghiêm trọng về an toàn đối với các tổ chức thương mại. Làm thế nào một công ty có thể duy trì khả năng giao dịch tương thích với hàng nghìn hệ thống khác nhau mà vẫn bảo đảm bí mật của các giao dịch này? Biện pháp an toàn trước kia được cho rằng phù hợp với các cuộc truyền tệp và thông báo bằng văn bản dường như hoàn toàn không tương xứng với các cuộc truyền thông đa phương tiện và thương mại điện tử phức tạp. Để thấy được độ phức tạp của các giao dịch này thì ngay cả các giao thức chuẩn như IPEC cũng không cung cấp đầy đủ.

Phần này bao gồm ba lĩnh vực có mối quan tâm đặc biệt: gửi thông báo điện tử, các giao dịch WWW và trao đổi tiền tệ. Tất cả lệ thuộc vào khả năng rủi ro về những tổn thất tài chính cũng như những khả năng vi phạm nghiêm trọng các quan hệ hợp pháp và công khai. Các giao dịch này đòi hỏi độ an toàn tốt đến mức vượt ra khỏi năng lực của hầu hết các giao thức an toàn tầng thấp. Chúng yêu cầu an toàn tầng ứng dụng.

12.2 Nhìn từng tầng ở góc độ an toàn

Trước khi đi vào các vấn đề cụ thể về an toàn căn cứ vào ứng dụng, vấn đề đặt ra có thể giúp nhìn nhận xem an toàn toàn được thực thi như thế nào ở các tầng ISO khác nhau. Hình sau mô tả mô hình ISO được chia thành các giao thức tầng cao (các giao thức này gắn với ứng dụng về dữ liệu) và các giao thức tầng thấp (các giao thức này gắn với việc truyền dữ liệu). Phía bên phải liệt kê các ví dụ về một số giao thức an toàn ở mỗi tầng. Bây giờ hãy cùng bắt đầu với từng tầng.

---

[3] Application- Layer Security Protocols for Network, Bill Stackpole, Chapter 10, Information Security Management Hanbook, 4th edition, Boca Raton-London- New York-Washington, editors Harold F.Tipton and Micki Krause

Mô hình bảy tầng ISO

7	Tầng ứng dụng	PEM, S-HTTP, SET
6	Tầng trình diễn	
5	Tầng phiên	SSL
4	Tầng giao vận	IPSEC
3	Tầng mạng	PPTP, swIPe
2	Tầng liên kết dữ liệu	VPDN, L2F, L2TP
1	Tầng vật lý	Fiber Optics

Có một số biện pháp phổ biến để bảo đảm an toàn ở tầng vật lý:

- Bảo vệ những ống dẫn cáp - bọc chúng trong bêtông
- Bảo vệ chống phát xạ không đúng lúc - giông tố
- Sử dụng môi trường khó mắc trộm - cáp quang

Bên cạnh hiệu quả, các biện pháp này bị hạn chế bởi những thứ nằm trong phạm vi điều khiển vật lý của bạn.

Các chuẩn tầng 2 phổ biến gồm lọc và điều chỉnh địa chỉ vật lý (ví dụ, L2F, L2TP). Có thể sử dụng các chuẩn này để điều khiển truy nhập và đảm bảo bí mật trên bất kỳ kiểu kết nối nào nếu không bị giới hạn bởi các phân đoạn ở các điểm cuối mà người cài đặt an toàn biết rõ. Các chuẩn tầng 3 bảo đảm các kỹ thuật lọc và điều chỉnh phức tạp hơn (ví dụ, PPTP). Những cài đặt đã chuẩn hoá như IPSEC có thể đáp ứng mức độ an toàn cao trên nhiều nền hệ thống. Tuy nhiên các giao thức tầng 3 kém phù hợp với các cài đặt ở nhiều địa điểm vì chúng bị hạn chế trong một mạng đơn lẻ. Các giao thức dựa vào giao vận tầng 4 vượt qua hạn chế mạng đơn lẻ nhưng vẫn thiếu sự tinh vi mà các giao dịch đa nhóm đòi hỏi. Giống như tất cả các giao thức tầng thấp, các giao thức giao vận không tương tác với dữ liệu chứa trong tải trọng, nên chúng không thể bảo vệ chống lại việc ngắt tải trọng hay những tấn công vào nội dung.

12.3 An toàn tầng ứng dụng - ALS (application layer security)

Điều này hoàn toàn là lợi thế của các giao thức tầng cao. An toàn dựa vào ứng dụng có khả năng diễn dịch và tương tác với thông tin chứa trong phần tải trọng của một gói dữ liệu. Ví dụ, các proxy ứng dụng sử dụng ở hầu hết các filewall đối với các cuộc truyền FTP. Các proxy này có khả năng hạn chế việc sử dụng một số lệnh nào đó cho dù các lệnh này được lưu trong phần trọng tải của gói dữ liệu. Khi khởi đầu một cuộc truyền FTP, một kết nối được thiết lập để truyền các lệnh tới server. Các lệnh mà bạn gõ (ví dụ, LIST, GET, PASV) được gửi tới server trong phần trọng tải của gói lệnh như minh hoạ ở hình sau. Do được căn cứ

vào ứng dụng nên filewall proxy có khả năng kiểm soát các lệnh này và vì thế hạn chế việc sử dụng chúng.

ETHERNET HEADER	IP HEADER	TCP HEADER	PAYLOAD
0040A0...40020A	10.1.2.1...10.2.1.2	FTP (Command)	List...

Giao thức truyền file - Lệnh - Gói

Các giao thức an toàn tầng thấp như IPSEC không có khả năng này. Chúng có thể mã hoá các lệnh nhằm bảo mật và xác thực, nhưng không thể hạn chế sử dụng chúng.

Nhưng an toàn tầng ứng dụng chính xác là cái gì? Như tên đã bao hàm, nó là sự an toàn do bản thân chương trình ứng dụng cung cấp. Ví dụ, kho dữ liệu dùng các danh sách điều khiển truy nhập được lưu giữ bên trong để hạn chế người dùng truy nhập tới các file, bản ghi hoặc các file đang thực thi an toàn theo ứng dụng. Áp dụng an toàn ở mức ứng dụng tạo cho nó có thể thực hiện một số yêu cầu an toàn phức tạp nào đó và điều tiết các yêu cầu bổ sung khi chúng xảy đến. Ngữ cảnh này làm việc đặc biệt tốt khi tất cả các ứng dụng của bạn được lưu trên một máy chủ đơn lẻ hoặc intranet an toàn, nhưng nó trở nên khó hiểu khi bạn cố gắng mở rộng chức năng tiện ích của nó qua Internet tới hàng nghìn hệ thống và ứng dụng khác nhau. Theo cách truyền thống, an toàn trong các môi trường này được xác định theo kiểu riêng trong chính các ứng dụng, nhưng điều này đang thay đổi nhanh chóng. Trạng thái phân bố tự nhiên của các ứng dụng trên Internet đã đưa đến việc thiết kế một vài giải pháp chuẩn hoá để thay thế các cơ chế an toàn theo nhà sản suất cụ thể, không dự tính trước.

12.4 Khả năng tương tác - Chìa khoá đưa tới thành công của ALS

Khả năng tương tác gắn chặt với sự thành công của bất kỳ giao thức nào trên Internet. Sự tôn trọng triệt để các chuẩn quyết định khả năng tương tác. Mặc dù các giao thức ALS đề cập trong chương này bao trùm ba lĩnh vực khác biệt, nhưng tất cả chúng đều dựa vào một tập các chuẩn chung và cung cấp các dịch vụ an toàn như nhau. Phần này giới thiệu một số phần tử chung này. Ở đây không phải chỉ kể đến tất cả các phần tử chung, mà bao gồm cả các phần tử được tìm thấy trong mọi cài đặt ALS bảo đảm có sự tương đồng thích đáng.

Mã hoá là thành phần chủ yếu của tất cả các giao thức an toàn hiện đại. Tuy nhiên, trong quá khứ quản lý khoá mã là một trở ngại chính cho việc sử dụng nó trong các môi trường mở như Internet. Với sự ra đời các chuẩn chứng nhận số và quản lý khoá công khai thì trở ngại này đã được vượt qua phần lớn. Các chuẩn như cấu trúc hạ tầng khoá công khai Internet X.509 (pkix) và cấu trúc hạ tầng khoá công khai đơn giản (spki) cung cấp các cơ chế cần thiết để thực thi, quản lý và phê chuẩn các khoá mã qua nhiều vùng và nền hệ thống. Tất cả các giao thức đề cập trong chương này đều hỗ trợ sử dụng cấu trúc hạ tầng khoá công khai.

Các dịch vụ an toàn chuẩn - Bảo vệ thông báo tối đa

Tất cả các giao thức ALS nói đến trong chương này đều cung cấp bốn dịch vụ an toàn chuẩn sau:

- *Bảo mật* - Đảm bảo rằng chỉ người nhận định trước mới có thể đọc được những nội dung thông tin gửi cho họ.
- *Toàn vẹn* - Đảm bảo rằng thông tin nhận được hoàn toàn giống thông tin đã được gửi.
- *Xác thực* - Đảm bảo rằng người gửi thông báo hoặc truyền đúng là người mà họ xác nhận được.
- *Không từ chối* - Chứng minh rằng một thông báo do người khởi tạo nó đã gửi đi ngay cả khi người này không chịu thừa nhận nó.

Mỗi dịch vụ này dựa vào một dạng mã hoá theo chức năng tiện ích của nó. Mặc dầu các cài đặt dịch vụ có thể khác nhau, nhưng tất cả đều sử dụng một tập thuật toán khá chuẩn.

Các thuật toán đã được thử nghiệm và đúng đắn

Sức mạnh của một thuật toán mã hoá có thể được đo bằng sự trường tồn của nó. Các thuật toán tốt tiếp tục chứng tỏ mức độ mã hoá cao sau nhiều năm phân tích và tấn công. Các giao thức ALS đề cập ở đây đáp ứng ba kiểu mã hoá - đối xứng, không đối xứng và hàm băm - dùng các thuật toán đã được kiểm chứng qua thời gian.

Mã đối xứng (còn gọi là khoá bí mật) chủ yếu dùng cho các chức năng bảo mật vì nó có mức độ mã hoá cao và có thể xử lý nhanh chóng một lượng dữ liệu lớn. Trong các cài đặt ALS, DES là thuật toán đối xứng được dùng phổ biến nhất. *Mã không đối xứng* hay *mã khoá công khai* được dùng phổ biến nhất trong các ứng dụng ALS để bảo đảm tính bảo mật trong thời gian khởi đầu hoặc thiết lập một giao dịch. Các khoá công khai và các xác nhận số được dùng để xác thực các nhóm tham gia với một nhóm khác và trao đổi các khoá đối xứng dùng cho thời gian còn lại của giao dịch. RSA là thuật toán không đối xứng được dùng phổ biến nhất trong các cài đặt ALS.

Kỹ thuật băm mật mã được dùng để đảm bảo tính toàn vẹn và xác thực trong các cài đặt ALS. Khi sử dụng riêng rẽ, xác thực xác nhận người gửi và tính toàn vẹn của thông báo, nhưng khi dùng chúng kết hợp với nhau đảm bảo chứng minh rằng thông báo đã không bị giả mạo và vì thế không thể bị từ chối (không thừa nhận). Ba hàm băm được dùng phổ biến nhất trong các cài đặt ALS là MD2, MD5 và SHA. Bổ sung vào tập các thuật toán chung, các hệ thống muốn hoạt động trong một môi trường mở phải có khả năng vượt qua và công nhận tập các tham số an toàn chung. Phần tiếp theo giới thiệu một số chuẩn dùng để định nghĩa và phê chuẩn các tham số này.

Các chuẩn

Để trao đổi thông tin hiệu quả các ứng dụng phải thoả thuận trên cơ sở một định dạng chung đối với thông tin đó. Nếu các dịch vụ an toàn là đáng tin cậy thì chúng đòi hỏi tất cả các nhóm thực hiện chức năng theo một sự nhất trí. Các tham số truyền thông phải được thiết lập, các dịch vụ an toàn, các mô hình và thuật toán được thoả thuận trước, các khoá mật mã được trao đổi và phê chuẩn. Để thuận tiện cho các tiến trình này, các giao thức ALS nói đến ở đây đáp ứng các chuẩn định dạng sau:

- X.509 - Chuẩn X.509 định nghĩa dạng chứng nhận số mà những người có thẩm quyền xác nhận dùng để phê chuẩn các khoá mã công khai.
- PKCS - Chuẩn mật mã khoá công khai định nghĩa các tham số cơ bản (các định danh đối tượng) dùng để thực hiện các phép biến đổi mật mã và phê chuẩn dữ liệu khoá.
- CMS (Cryptographic Message Syntax)- Cú pháp thông báo mật mã định nghĩa các định dạng truyền và các kiểu nội dung mã hoá mà các dịch vụ an toàn sử dụng. CMS định nghĩa sáu kiểu mã hoá gồm từ không mã hoá tới gồm cả mã hoá và ký. Chúng là: Data, signedData, envelopedData, signedAndEnvelopedData, digestData, encryptedData.
- MOSS - Các dịch vụ an toàn đối tượng MIME định nghĩa hai kiểu nội dung mã hoá bổ sung cho các đối tượng multipart MIME có thể được dùng đơn lẻ hoặc phối hợp với nhau. Chúng là: multipart-signed và multipart-encrypted.

Mã hoá cần thiết cho sự bảo đảm tính bí mật và toàn vẹn giao dịch trên các mạng mở, và kiến trúc Public Key/Certification Authority cung cấp cấu trúc hạ tầng cần thiết để quản lý việc phân phối và phê chuẩn các khoá mã. Hiện nay các cơ chế an toàn tại tất cả các mức có một biện pháp chuẩn để khởi đầu các giao dịch an toàn, vì thế không cần có các giải pháp riêng khi thực hiện các giao dịch đa nhóm, đa cổng hay quốc tế. Giao thức giao dịch thẻ tín dụng SET mới là một ví dụ.

12.5 Cài đặt ví dụ - giao thức giao dịch điện tử an toàn của Visa

SET (giao dịch điện tử an toàn) là một giao thức an toàn căn cứ vào ứng dụng do Visa và MasterCard cùng nhau phát triển. Nó được tạo ra để đảm bảo các giao dịch thẻ thanh toán an toàn trên các mạng mở. SET là tương đương theo nghĩa điện tử chỉ một giao dịch mặt đối mặt hoặc thẻ tín dụng đặt hàng. Nó bảo đảm bí mật và toàn vẹn cho các cuộc trao đổi thanh toán và xác thực tất cả các nhóm liên quan tới giao dịch. Hãy khảo sát một giao dịch SET để thấy giao thức tầng ứng dụng này thực hiện một giao dịch tài chính đa nhóm phức tạp như thế nào.

Một giao dịch SET liên quan tới năm thành phần tham dự khác nhau: *cardholder* (người giữ thẻ), *issuer* (người phát hành thẻ thanh toán), *merchant* (thương gia), *acquirer* (người giữ tài khoản của thương gia) và một *payment gateway* (cổng thanh toán) tiến hành các giao dịch thanh toán thay mặt acquirer. Các chính sách chỉ đạo việc điều khiển các giao dịch như thế nào do nhóm thứ sáu

brand (nhãn hiệu) (ví dụ Visa) thiết lập, nhưng chúng không tham gia vào các giao dịch thanh toán.

Một giao dịch SET đòi hỏi hai cặp khoá mã không đối xứng và hai chứng nhận số; một cho trao đổi thông tin và một cho các chữ ký số. Các khoá và chứng nhận này có thể được lưu trong một thẻ tín dụng "thông minh" hoặc gắn vào một ứng dụng cho phép SET (ví dụ Web browser). Các khoá và xác nhận được phát ra từ cardholder nhờ quyền xác thực (CA) nhân danh issuer. Các khoá và xác thực số của merchant được phát ra từ họ theo quyền xác nhận nhân danh acquirer. Chúng đảm bảo rằng merchant có tài khoản được acquirer phê chuẩn. Các xác nhận của cardholder và merchant được ký hiệu bằng số theo cơ quan tài chính phát hành nhằm đảm bảo xác thực chúng và ngăn chặn chúng khỏi bị sửa đổi bất hợp pháp. Một chi tiết thú vị của sự sắp đặt này là xác nhận của cardholder không chứa số tài khoản của anh ta hay ngày mãn hạn. Thông tin đó được mã hoá bằng một khoá bí mật chỉ được cung cấp tới payment gateway trong thời gian cấp phép thanh toán. Đến đây chúng ta đã làm quen với tất cả các vai. Hãy cùng bắt đầu.

Bước 1

Cardholder đi mua sắm, lựa chọn hàng hoá của anh ta và gửi một đơn đặt hàng tới merchant yêu cầu một loại thanh toán SET. (Đặc tả SET không định nghĩa việc mua sắm được hoàn thành như thế nào vì nó không liên quan đến phần này của giao dịch). Nếu cardholder và merchant không sẵn sàng, thì họ xác thực lẫn nhau bằng việc trao đổi xác nhận và chữ ký số. Trong quá trình trao đổi này merchant cũng cung cấp thông tin xác nhận và chữ ký số của cổng thanh toán tới cardholder. Sau đây bạn sẽ thấy điều này sẽ được sử dụng như thế nào. Trong trao đổi này cũng thiết lập một cặp khoá đối xứng được sinh ra một cách ngẫu nhiên sẽ được dùng để mã hoá các cuộc trao đổi giữa cardholder - merchant còn lại.

Bước 2

Một khi các trao đổi ở trên đã hoàn thành, merchant liên lạc với cổng thanh toán. Một phần trao đổi này bao hàm thông tin lựa chọn ngôn ngữ để bảo đảm khả năng tương tác quốc tế. Một lần nữa thông tin xác nhận và chữ ký số được dùng để xác thực merchant với gateway và thiết lập các khoá đối xứng ngẫu nhiên. Sau đó thông tin thanh toán (PI-payment information) được gửi tới gateway để cấp phép thanh toán. Lưu ý rằng chỉ thông tin thanh toán được gửi tới. Điều này được thực hiện nhằm thoả mãn các yêu cầu điều chỉnh đối với việc sử dụng mã hoá triệt để. Nhìn chung, việc dùng mã hoá triệt để của các cơ quan tài chính không bị hạn chế nếu các giao dịch chỉ chứa các giá trị tiền tệ.

Bước 3

Dựa vào PI nhận được, payment gateway xác thực cardholder. Lưu ý rằng cardholder được xác thực mà không phải liên lạc trực tiếp với cổng mua. Điều này được thực hiện thông qua một tiến trình gọi là chữ ký số kép. Thông tin do cổng mua yêu cầu để xác thực cardholder được gửi tới merchant với một chữ ký số khác

với chữ ký số dùng cho các trao đổi merchant-cardholder. Có khả năng thực hiện điều này vì merchant đã gửi xác nhận về cổng mua tới cardholder trong trao đổi trước đó! Merchant thường gửi thông tin này tới payment gateway như một phần của yêu cầu cấp phép thanh toán. Một mẩu thông tin khác gửi qua trao đổi này là khoá bí mật mà gateway cần để giải mã số tài khoản và ngày mãn hạn của cardholder.

Bước 4

Gateway tái định dạng thông tin thanh toán và gửi nó qua một mạch riêng tới issuer để cấp phép. Khi issuer cấp phép cho giao dịch thì payment gateway thông báo cho merchant, merchant thông báo cho cardholder và giao dịch được hoàn thành.

Bước 5

Merchant kết thúc giao dịch bằng việc đưa ra yêu cầu nhận thanh toán với payment gateway dẫn đến tài khoản của cardholder bị ghi nợ và số lượng giao dịch được ghi vào tài khoản của merchant.

Một giao dịch SET đơn lẻ như giao dịch được phác thảo ở trên phức tạp đến không ngờ, để có được thành công nó đòi hỏi trên 59 hành động khác nhau. Độ phức tạp như thế đòi hỏi công nghệ tầng ứng dụng được quản lý hiệu quả. Tuy nhiên, cái hay của SET chính là khả năng thực thi theo cách an toàn và phổ biến của nó. Các giao thức khác đang đạt được thành công tương tự trong các phạm vi ứng dụng khác nhau.

12.6 Từ những bưu thiếp tới những lá thư - Thư tín điện tử an toàn

Thông báo điện tử là một thế giới bưu thiếp. Khi các thông báo di chuyển từ nguồn tới đích, chúng có thể dùng được một cách công khai (như ghi vào bưu thiếp) để những người tạo ra chúng đọc được. Nếu bưu thiếp không phù hợp với các cuộc truyền thông thương mại, thì trên một mạng mở thư điện tử cũng không phù hợp. Các cuộc truyền thông thương mại chuẩn đòi hỏi bí mật và các cuộc truyền thông khác có tính nhạy cảm hơn đòi hỏi tăng cường bảo vệ như chứng thực cấp phát hay xác minh người gửi, những tính năng không sẵn trong các giao thức thư Internet được dùng phổ biến. Điều này dẫn tới việc phát triển một vài giao thức truyền thông báo nâng cao an toàn. PEM là một giao thức như thế.

Hệ thư tăng cường bảo mật (PEM- Privacy Enhanced Mail) là một giao thức an toàn tầng ứng dụng do IETF phát triển nhằm bổ sung các dịch vụ bảo mật và xác thực cho các thông báo điện tử trên Internet. Mục đích là tạo ra một chuẩn có thể được cài đặt trên bất kỳ máy chủ nào, có khả năng tương thích với các hệ thư đang tồn tại, hỗ trợ các lược đồ quản lý khoá chuẩn, bảo vệ cả thư gửi đơn lẻ và thư gửi theo danh sách và không dính líu tới việc cấp phát thư không an toàn. Khi chuẩn được hoàn thành vào năm 1993, nó đã thành công trên mọi phương diện đã tính toán. PEM đáp ứng cả bốn dịch vụ an toàn chuẩn, mặc dầu không phải tất cả

các dịch vụ là bộ phận cần thiết của mọi thông báo. Các thông báo PEM có thể là các thông báo MIC-CLEAR chỉ bảo đảm toàn vẹn và xác thực; các thông báo MIC-ONLY đảm bảo toàn vẹn và xác thực với sự hỗ trợ của các cài đặt cổng nào đó hoặc các thông báo ENDCRYTED bảo đảm toàn vẹn, xác thực và bảo mật.

Một số tính năng chủ yếu của PEM là:

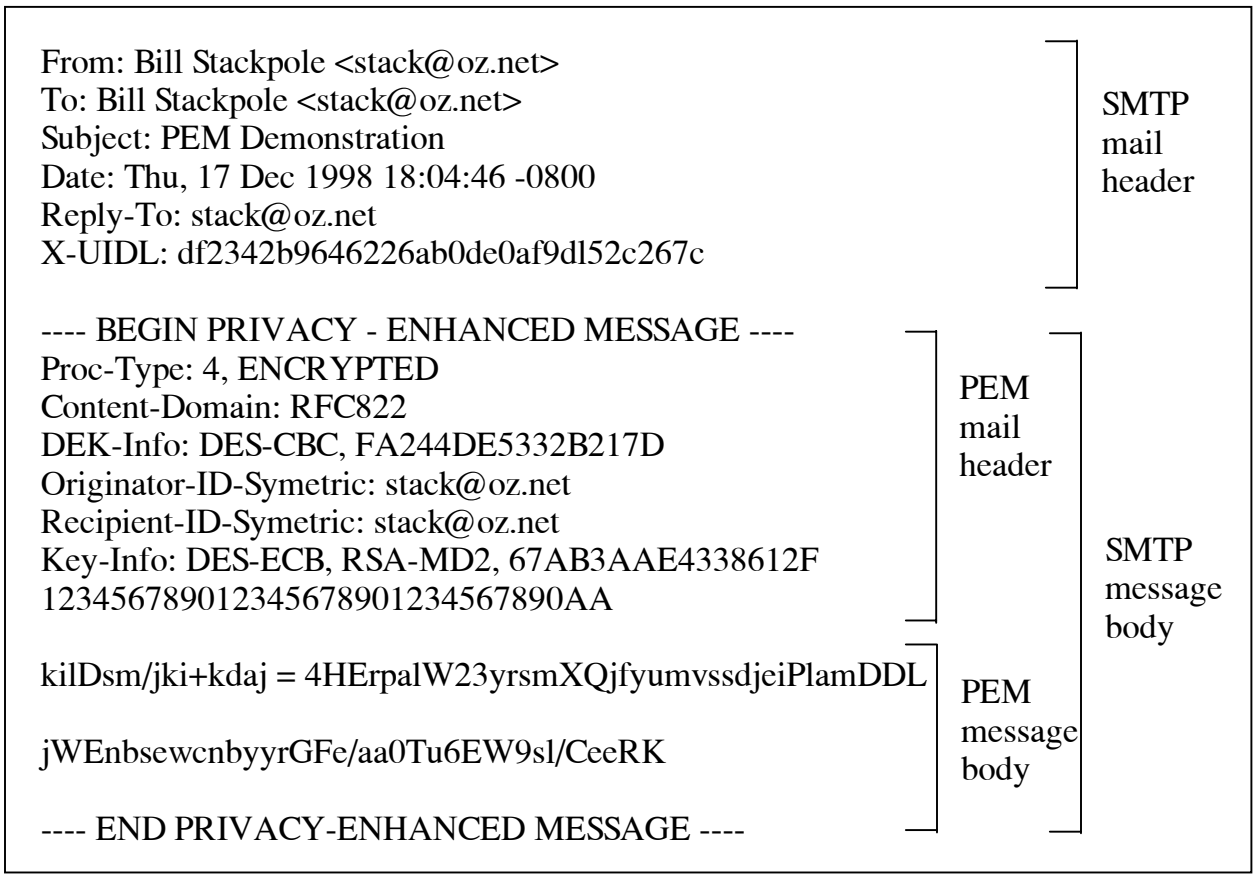
- *Bảo mật điểm tới điểm* - Các thông báo được bảo vệ chống bị lộ từ khi chúng rời hệ thống của người gửi cho tới lúc người nhận đọc được chúng.
- *Xác thực người gửi và người chuyển tiếp* - Các chữ ký số PEM xác thực những người gửi và những người chuyển tiếp, đảm bảo toàn vẹn thông báo. PEM dùng một tham số kiểm tra toàn vẹn cho phép các thông báo được nhận theo một thứ tự nào đó và vẫn được kiểm soát - một tính năng quan trọng trong các môi trường như Internet, nơi mà các thông báo có thể bị phân đoạn trong quá trình truyền.
- *Không từ chối người khởi tạo* - Tính năng này xác thực người khởi tạo thông báo PEM. Nó đặc biệt có lợi đối với các thông báo được chuyển tiếp vì chữ ký số PEM chỉ xác thực người gửi sau cùng. Không từ chối kiểm chứng lại người khởi tạo nếu không có vấn đề gì sau một khoảng thời gian thì thông báo được chuyển tiếp.
- *Độc lập về thuật toán* - PEM được thiết kế để dễ dàng tương thích với các lược đồ mã hoá và quản lý khoá mới. Hiện tại PEM đáp ứng các thuật toán phổ biến trong bốn lĩnh vực: DES cho mã hoá dữ liệu, DES và RSA cho quản lý khoá, RSA cho toàn vẹn thông báo và RSA cho các chữ ký số.
- *Hỗ trợ PKIX* - PEM đáp ứng đầy đủ sự tương tác trên các mạng mở dùng cấu trúc hạ tầng khoá công khai Internet X.509.
- *Độc lập với hệ thống cấp phát* - PEM có được sự độc lập với hệ thống cấp phát vì các hàm của nó được chứa trong chính các thông báo chuẩn và sử dụng một tập ký tự chuẩn như minh hoạ ở hình 10.3.
- *Hỗ trợ đặt tên phân biệt X.500* - PEM dùng tính năng đặt tên phân biệt (DN) của chuẩn thư mục X.500 để nhận biết những người gửi và người nhận. Tính năng này tách thư khỏi những cá nhân cụ thể cho phép các tổ chức, các bản kê khai và các hệ thống gửi và nhận các thông báo PEM.

RIPEM (Riordan's Internet PEM) là một cài đặt công khai của giao thức PEM, tuy nhiên không phải tất cả các chức năng. Khi tác giả Mark Riordan đã đặt mã lệnh công khai, nó đã được chuyển tới một số lớn các hệ điều hành. Có thể có chương trình nguồn và các bản nhị phân qua FTP từ các công dân Mỹ và Canada tới ripem.msu.edu. Hãy đọc file GETTING_ACCESS trong thư mục /pub/crypt trước khi thử tải xuống.

Các hệ thư Internet an toàn/đa mục tiêu mở rộng (**S/MIME**) là một giao thức tầng ứng dụng khác cung cấp cả bốn dịch vụ an toàn chuẩn cho các thông báo điện tử. Đặc tả S/MIME ban đầu do RSA Data Security thiết kế, nhưng hiện tại lại do IETF S/MIME Working Group quản lý. Mặc dù S/MIME không phải là một chuẩn

IETF, nhưng nó sẵn có sự hỗ trợ của nhà sản xuất có thế lực dự tính trước, trên quy mô lớn vì nó dựa vào các chuẩn đã được thử thách nhiều đảm bảo mức độ tương tác cao. Đương nhiên, đáng chú ý nhất vẫn là chuẩn MIME nổi tiếng và sử dụng rộng rãi, nhưng S/MIME cũng tận dụng các chuẩn CMS, PKCS và X.509. Cũng như PEM, S/MIME tương thích với hầu hết các hệ thư Internet đang tồn tại và không gây trở ngại cho việc truyền thông báo không an toàn. Tuy nhiên, S/MIME có một cái lợi nữa khi làm việc cùng với các giao vận MIME khác (ví dụ HTTP) và có thể hoạt động bình đẳng trong các môi trường giao vận hỗn hợp. Điều này khiến cho nó đặc biệt hấp dẫn khi dùng với các cuộc truyền tự động như EDI và Internet FAX.

Có hai kiểu thông báo S/MIME: signed và signed & enveloped. Các thông báo được ký đảm bảo toàn vẹn và xác thực người gửi, trong khi các thông báo được ký và bọc đảm bảo toàn vẹn, xác thực và bảo mật. Các tính năng còn lại của S/MIME rất giống với PEM và không nhắc lại ở đây.



Một danh sách các sản phẩm S/MIME thương mại đã hoàn thành tốt đẹp cuộc kiểm tra tính tương tác, S/MIME sẵn có trên trang web của RSA Data Security tại: www.rsa.com/smime/html/interop_center.html. Phiên bản vùng công khai của

S/MIME do Ralph Levien viết trong PERL có tại: www.c2.org/ ~raph/premail.html.

Open Pretty Good Privacy (**OpenPGP**), đôi khi gọi là PGP/MIME, một giao thức ALS nổi bật khác tiếp tục trở thành một chuẩn IETF. Nó dựa vào PGP, một chương trình an toàn thông báo được triển khai rộng rãi nhất trên Internet. Về các tính năng và chức năng tiện ích OpenPGP rất giống với S/MIME, nhưng có hai điểm không thể tương tác vì chúng dùng hai thuật toán mã hoá và hàm đóng gói MIME khác nhau rõ rệt. Một danh sách các cài đặt PGP và thông tin khác về OpenPGP có tại: http://www.ns.rutgers.edu/ ~mione/openpgp/. Các cài đặt miễn phí của OpenPGP có tại North American Cryptographiy Archives (**www.cryptography.org)**.

12.7 Chế ngự HTTP - An toàn ứng dụng WEB

Các ứng dụng dựa vào WEB nhanh chóng trở thành chuẩn cho tất cả các giao dịch điện tử vì chúng dễ sử dụng và có khả năng tương tác cao. Các tính năng này cũng là sự thiếu an toàn chính yếu của chúng. Các giao dịch WEB ngang qua mạng theo các định dạng quen thuộc và dễ bị chặn lại, khiến chúng không mấy phù hợp với hầu hết các giao dịch thương mại. Phần này sẽ đề cập một số cơ chế dùng để vượt qua các vấn đề an toàn WEB này.

Giao thức truyền siêu văn bản an toàn (S/HTTP) là một giao thức an toàn theo thông báo được thiết kế để cung cấp các dịch vụ bảo mật, toàn vẹn, xác thực và không từ chối từ điểm tới điểm cho các client và server HTTP. Nó được Enterprise Integration Technologies (nay là Verifone, Inc.) triển khai lần đầu vào năm 1995. Theo văn bản này, S/HTTP vẫn là một chuẩn IETF thô, nhưng nó đã được dùng rộng rãi trong các ứng dụng WEB. Thành công của nó có thể là do thiết kế mềm dẻo bắt nguồn từ các chuẩn đã thiết lập. Tất nhiên, chuẩn nổi tiếng là HTTP, song giao thức vẫn dùng chuẩn chữ ký số NIST, các chuẩn CMS, MOSS và X.509. Sự tôn trọng triệt để mô hình truyền thông báo HTTP của S/HTTP bảo đảm tính độc lập với hệ thống cấp phát và làm cho nó dễ dàng tích hợp các hàm S/HTTP vào các ứng dụng HTTP chuẩn. Sự độc lập về thuật toán và khả năng thoả thuận các tuỳ chọn an toàn giữa các nhóm tham gia bảo đảm khả năng tương tác của S/HTTP trong những năm tới. Các mô hình hoạt động của HTTP an toàn gồm bảo vệ thông báo, quản lý khoá và cơ chế tái tạo giao dịch.

Các tính năng bảo vệ an toàn HTTP gồm:

- *Hỗ trợ cho MOSS và CMS* - Cung cấp sự bảo vệ ở cả hai vùng nội dung dùng kiểu nội dung CMS "ứng dụng/s-http" hoặc tiêu đề MOSS "đa lớp-có dấu" hay "đa lớp- mã hoá".
- *Khả năng tương thích cú pháp* - Các tham số bảo vệ được đặc tả bằng việc mở rộng phạm vi tiêu đề thông báo HTTP, tạo thông báo S/HTTP giống các thông báo HTTP chuẩn về cú pháp, ngoại trừ phạm vi của các tiêu đề là khác nhau và thân thường được mã hoá.

- *Các biện pháp bảo vệ đệ quy* - Những biện pháp bảo vệ có thể được dùng đơn lẻ hoặc áp vào một tầng sau khi một tầng khác đạt được mức bảo vệ cao hơn. Phân tầng bảo vệ giúp cho hệ thống nhận dễ dàng hơn khi phân tích cú pháp chúng. Thông báo thường phân tích một tham số bảo vệ trong một thời gian cho đến khi nó thoả mãn một kiểu nội dung HTTP chuẩn.
- *Độc lập thuật toán* - Cấu trúc thông báo S/HTTP có thể dễ dàng hợp nhất với các cài đặt mật mã mới. Đặc tả hiện tại đòi hỏi hỗ trợ MD5 cho các phân loại thông báo, MD5-HMAC cho xác thực, DES-CBC cho mã đối xứng và NIST-DSS cho việc sinh và thẩm tra chữ ký.
- *Tính năng tái tạo* - S/HTTP dùng một hỏi-đáp đơn giản để bảo đảm rằng dữ liệu được trả lại server là "tươi". Trong các môi trường như HTTP, nơi mà có các khoảng thời gian dài trôi qua giữa các thông báo, nên khó theo dõi trạng thái của một giao dịch. Để khắc phục vấn đề này, người khởi tạo thông báo HTTP gửi một giá trị mới (trong trường hợp này) tới nơi nhận cùng với dữ liệu giao dịch. Nơi nhận trả lại giá trị này cùng với lời đáp. Nếu các giá trị này tương xứng thì dữ liệu là mới và giao dịch có thể tiếp tục. Dữ liệu cũ đưa ra một điều kiện lỗi.
- *Trao đổi thủ công* - Những bí mật dùng chung được trao đổi thông qua một cơ chế mật khẩu đơn giản như PAP. Server thường gửi cho client một hộp thoại yêu cầu định danh người dùng (userID) và mật khẩu, sau đó xác thực câu trả lời dựa vào danh sách những người dùng hợp pháp đang tồn tại.
- *Trao đổi khoá công khai* - Các khoá được trao đổi lợi dụng cấu trúc hạ tầng khoá công khai Internet với sự hỗ trợ xác nhận đầy đủ của X.509. Để hỗ trợ Diffie-Hellman đối với các trao đổi khoá, trong vùng yêu cầu có các cài đặt S/HTTP.
- *Trao đổi khoá ngoài vùng* - Các khoá đối xứng có thể được đặt trước thông qua một số môi trường khác (ví dụ thư chậm). Tính năng này chỉ có với S/HTTP, cho phép các nhóm không có các khoá công khai đã thiết lập tham gia vào các giao dịch an toàn.
- *Trao đổi khoá đối xứng trong vùng* - S/HTTP có thể dùng mã hoá khoá công khai để trao đổi các khoá đối xứng ngẫu nhiên trong những tình huống mà giao dịch sẽ tận dụng được hiệu suất mã đối xứng cao hơn.

Nhiều bộ duyệt và server WEB thương mại cài đặt giao thức S/HTTP, nhưng tác giả không thể tìm thấy bất kỳ cài đặt vùng công khai nào. Cài đặt S/HTTP đầy đủ bao gồm mã nguồn C có trong SecureWeb Toolkit™ từ Terisa (www.spyrus.com). Bộ này cũng chứa mã nguồn của SSL.

Tầng socket an toàn (**SSL**) là một giao thức client-server do Netscape thiết kế đảm bảo truyền thông an toàn cho các sản phẩm duyệt Web và server của họ. Nó nhanh chóng được các nhà sản xuất khác chấp nhận và trở thành chuẩn không chính thức cho các giao dịch Web an toàn. Tuy nhiên, SSL không hạn chế với các

dịch vụ Web; nó có thể cung cấp các dịch vụ bảo mật, toàn vẹn xác thực và không từ chối giữa bất kỳ cặp ứng dụng đang truyền thông nào. Phiên bản hiện nay của SSL (SSL 3.0) đang tiến tới trở thành một chuẩn IETF. Trong khi ở đây nó chỉ được nói đến như một giao thức tầng ứng dụng thì trong thực tế SSL được thiết kế để thực hiện chức năng ở các tầng phiên và ứng dụng. Giao thức SSL Record cung cấp các dịch vụ an toàn ở tầng phiên - điểm mà ở đó ứng dụng ghép nối các socket giao vận TCP/IP. Nó được dùng để đóng gói các giao thức và dữ liệu tầng cao để nén và truyền. Giao thức SSL Handshake là một dịch vụ theo ứng dụng thường dùng để xác thực client và server với nhau và thoả thuận các tham số an toàn đối với mỗi phiên truyền thông.

Giao thức SSL Handshake dùng mã hoá khoá công khai cùng với phê chuẩn xác nhận X.509 để thoả thuận các tham số mã đối xứng dùng cho mỗi phiên giao dịch client-server. SSL là một giao thức hoàn toàn hình thức. Nó chuyển tiếp qua một vài trạng thái khác nhau trong thời gian kết nối và hoạt động của phiên. Giao thức handshake được dùng để phối hợp và duy trì các trạng thái này.

Một phiên SSL có thể gồm nhiều kết nối và các nhóm tham gia có thể có nhiều phiên diễn ra cùng lúc. Trạng thái phiên duy trì thông tin xác nhận ngang hàng, các tham số nén, các tham số mã và khoá mã đối xứng. Trạng thái kết nối duy trì MAC và các khoá không đối xứng cho client và server cũng như các vector (nếu yêu cầu) để khởi đầu mã đối xứng. SSL được thiết kế để hoàn toàn có khả năng mở rộng và có thể hỗ trợ nhiều lược đồ mã hoá. Phiên bản hiện nay yêu cầu hỗ trợ các lược đồ sau:

- DES, RC2, RC4 và IDEA để bảo mật
- RSA và DSS để xác thực ngang hàng
- SHA và MD5 để toàn vẹn thông báo
- Các xác nhận X.509 và FORTEZZA để phê chuẩn khoá
- RSA, Diffie-Hellman và FORTEZZA để trao đổi khoá.

SSL cũng hỗ trợ các tham số NULL đối với các giao dịch không dấu và không mã hoá. Điều này cho phép người cài đặt áp dụng mức độ an toàn thích hợp cho ứng dụng của họ. Hỗ trợ cho hệ thống mã hoá phần cứng FORTEZZA được đồng nhất với SSL khi có yêu cầu nén dữ liệu. SSL dùng cơ chế lưu trữ phiên để thoả mãn việc thiết lập nhiều phiên giữa các client và server và hồi phục lại các phiên bị phá vỡ.

Có một cài đặt vùng công khai ngoại lệ của SSL do Eric Young và Tim Hudson của Úc tạo ra, được gọi là SSLeay. Nó bao gồm cài đặt đầy đủ phiên bản SSL 2 của Netscape cùng với các phần ráp nối với Telnet, FTP, Mosaic và một vài server Web. Phiên bản hiện tại có thể có từ Web site SSLeay www.ssleay.org. Site này gồm một vài trang trắng SSL và một tài liệu tham khảo tuyệt vời cho người lập trình.

12.8 Đừng cho tôi thấy tiền - An toàn giao dịch tiền tệ

Thành công của thương mại trên Internet phụ thuộc vào khả năng quản lý các giao dịch tiền tệ an toàn của nó. Mặc dù việc mua bán dường như có ảnh hưởng lớn tới lĩnh vực này, nhưng thanh toán hoá đơn, các cuộc chuyển tiền và phương tiện và EDI là những nghiên cứu quan trọng. Việc thiếu các chuẩn cho hoạt động thanh toán điện tử đã khuyến khích vô số các giải pháp độc quyền gồm những đề xuất phổ biến Cybercash (Cybercoln), Digital (Millicent) và Digicash. Tuy nhiên, các giải pháp độc quyền không thể có được thành công rộng rãi trong môi trường hỗn tạp như Internet. Phần này sẽ tập trung vào các giải pháp chuẩn hoá. Vì giao thức SET đã được đề cập ở một số chi tiết, nên ở đây chỉ đề cập tới các cài đặt SET.

Thanh toán an toàn (**S/PAY**) là bộ công cụ của nhà phát triển dựa vào giao thức SET. Nó được RSA Data Security phát triển, mặc dù các quyền marketing hiện nay thuộc về Trintech Group (www,trintech.com). Thư viện S/Pay cài đặt đầy đủ các hàm SET v1.0 cardholder, merchant và acquier và các hàm mã hoá và quản lý xác nhận bên dưới đối với nền hệ thống là Windows95/NT và UNIX. Bao hàm trong mã là sự hỗ trợ phương tiện mã phần cứng, thiết bị card thông minh và kho lưu trữ khoá cá nhân thời gian dài. Trintech cũng đề xuất các cài đặt đầy đủ phần mềm SET cardholder, merchant và acquier. Phần này bao gồm sản phẩm Pay-Ware Net-POS của họ, sản phẩm này hỗ trợ một vài tổ hợp của các công nghệ SSL và SET nhằm dễ dàng truyền từ các giao dịch Web SSL tới các giao dịch SET được cài đặt đầy đủ.

Trao đổi tiền tệ mở (OFX-**Open Financial Exchange**) là một giao thức tầng ứng dụng do Checkfree, Intuit và Microsoft tạo ra để hỗ trợ phạm vi khách hàng rộng rãi và các dịch vụ ngân hàng thương mại nhỏ trên Internet. OFX là một đặc tả mở khả dụng với bất kỳ cơ quan tài chính hay nhà sản xuất nào có nhu cầu cài đặt các dịch vụ OFX. OFX sử dụng SSL với sự hỗ trợ xác nhận số nhằm cung cấp các dịch vụ bảo mật, toàn vẹn và xác thực cho các giao dịch của nó. Giao thức này đã giành được sự ủng hộ to lớn trong kỹ nghệ ngân hàng và đầu tư vì nó đáp ứng hầu như mọi giao dịch tiền tệ có thể có. Hiện nay, uỷ ban OFX đang tìm cách mở rộng biểu diễn của OFX thông qua các khả năng hợp tác với IBM và các nhà sản xuất khác. Các bản sao đặc tả OFX có được từ Web site OFX (www.ofx.net).

Micro Payment Transfer Protocol (MPTP) là một phần của World Wide Web Consortium (W3C) Joint Electronic Payment Initiative. Hiên nay, MPTP là bản phác thảo hoạt động của W3C. Đặc tả này dựa vào các biến thể của Rivest and Shamir's Pay-Word, Digital's Millicent và các đề xuất Bellare's iKP. MPTP là giao thức rất mềm dẻo có thể được phân tầng căn cứ vào các giao vận đang tồn tại như HTTP hay MIME để cung cấp phạm vi giao dịch rộng lớn. Nó có dung sai các độ trễ truyền cao cho phép nhiều xử lý giao dịch tiến hành gián tiếp. MPTP được thiết kế để đảm bảo các thanh toán thông qua các dịch vụ của người môi giới nhóm thứ ba. Trong phiên bản hiện này, người môi giới phải là quen thuộc với cả khách hàng và nhà sản xuất, mặc dù các cuộc truyền của người môi giới trung gian được dự

kiến cho các cài đặt trong tương lai. Điều này là cần thiết nếu MPTP sẽ cân bằng có hiệu quả để thoả mãn các đòi hỏi của Internet.

Các khách hàng thiết lập một tài khoản với người môi giới. Khi đã thiết lập, họ tự do mua bán với bất kỳ nhà sản xuất nào quen thuộc với người môi giới của họ. Thiết kế MPTP đưa vào xem xét phần lớn những rủi ro đi liền với thanh toán điện tử và cung cấp các cơ chế làm giảm bớt các rủi ro này, nhưng nó cũng không cài đặt một chính sách an toàn cụ thể. Những người môi giới tự do hoạch định chính sách phù hợp nhất với các nhu cầu buôn bán của họ.

MPTP dựa vào công nghệ S/key dùng các thuật toán MD5 hay SHA để cấp phép thanh toán. MPTP cho phép đánh dấu các thông báo nhằm xác thực, toàn vẹn và không từ chối sử dụng mật mã khoá công khai hay bí mật và đáp ứng đầy đủ các xác nhận X.509. Mặc dù MPTP vẫn còn ở giai đoạn thô, nhưng với thiết kế đặc biệt, độ mềm dẻo và hiệu suất cao của nó, MPTP được cho là đối thủ hàng đầu trong lĩnh vực thanh toán điện tử.

Java Electronic Commerce Framework (JECF) là mục được đề cập cuối cùng của chúng ta. JECF không phải là một giao thức ứng dụng. Nó là bộ khung cho việc cài đặt xử lý thanh toán điện tử dùng công nghệ nội dung động. Công nghệ nội dung chủ động sử dụng một máy (ví dụ máy ảo Java) cài đặt trên client để thực hiện các phần chương trình (ví dụ applets) từ server gửi tới nó. Các thành phần nội dung động JECF hiện nay bao gồm các thông báo Java thương mại, mô hình an toàn gateway, các nhân Java thương mại và client Java thương mại (JCC).

JEFC căn cứ quanh khái niệm sổ tay (wallet) điện tử. Wallet là khả năng kỹ thuật phía client có thể mở rộng hỗ trợ một số lương các giao dịch thương mại điện tử nào đó. Các nhà sản xuất tạo các ứng dụng Java bao gồm các module dịch vụ (applets) gọi là Commerce JavaBeans cắm vào wallet. Các applet này thực hiện các thao tác và giao thức cần thiết để quản lý các giao dịch với nhà sản xuất. Có một vài ưu điểm cơ bản của kiến trúc này như sau:

- Các nhà sản xuất không bị ràng buộc với các chính sách cụ thể đối với các giao dịch của họ. Họ tự do tạo các module chứa các chính sách và thủ tục phù hợp nhất với công việc của họ.
- Các client không đòi hỏi có các ứng dụng cụ thể. Vì các applet JavaBean có nội dung động, chúng có thể được cấp phát và tải một cách linh hoạt trên hệ thống của khách hàng khi giao dịch xảy ra.
- Các ứng dụng có thể được cập nhật linh hoạt. Các applet giao dịch có thể được cập nhật hay thay đổi để hiệu chỉnh các vấn đề hoặc thoả mãn các nhu cầu công việc gia tăng mà không phải gửi những cập nhật tới tất cả client. Các module mới sẽ được tải trên module cũ trong giao dịch tiếp theo của chúng.
- Các module có thể được tải hoặc ngừng tải trên đường truyền để điều tiết các yêu cầu thanh toán, mã hoá hay ngôn ngữ khác nhau. Các module

OFX có thể được tải cho các giao dịch ngân hàng và sau đó ngừng tải khi khách hàng yêu cầu các module tạo cuộc mua bán thẻ tín dụng.

- Các module JavaBean chạy trên bất kỳ hệ điều hành, bộ duyệt hay ứng dụng nào hỗ trợ Java. Điều này cho phép nhà sản xuất truy nhập tức thời tới cơ sở khách hàng lớn nhất có thể.

Tính mềm dẻo, dễ di chuyển và cơ sở người dùng Java lớn khiến cho JECF là một giải pháp thương mại điện tử rất hấp dẫn. Nó chắc chắn sẽ đóng vai trò chính trong lĩnh vực thương mại điện tử.

12.9 Nếu bây giờ nó không được mã hoá....

Internet đã làm thay đổi đột ngột cách làm việc của chúng ta, nhưng cũng phải trả giá. Sự thiếu an toàn ghê gớm đối với các giao dịch Internet và truyền thông báo dẫn đến nhiều cái mà chúng ta đang làm trên Internet như một cuốn sách mở để tất cả cùng đọc. Điều này không thể tiếp tục. Có các giải pháp bất chấp độ phức tạp của các vấn đề mà chúng ta phải đối mặt. Các công nghệ đưa ra trong chương này cung cấp các giải pháp thực sự nhằm giảm bớt những rủi ro của giao dịch Internet. Chúng ta có thể bảo vệ các thông báo, các ứng dụng web và các trao đổi tiền tệ của chúng ta. Phải thừa nhận một số ứng dụng này không tinh tế như chúng ta mong muốn, nhưng dù sao chúng cũng hiệu quả và hầu như chắc chắn là một bước đi đúng.

Một ngày nào đó tất cả các giao dịch công tác của chúng ta trên Internet sẽ được mã hoá, đánh dấu, cất giấu và cấp phát, nhưng tôi không tin rằng chúng ta có thể đợi tới ngày đó. Các giao dịch công tác trên Internet ngày càng tăng và sẽ lại tìm thấy những lợi ích giao dịch mới của Internet. Việc chờ đợi những thứ tốt hơn sẽ chỉ đẩy chúng ta vào chỗ quanh co. ALS ngay bây giờ!

Tài liệu tham khảo

Crocker, S., Freed, N., Galvan, J., and Murphy, S., RFC 1848 – MIME object security services, IETF, October 1995.

Dusse, Steve and Matthews, Tim, S/MIME: anatomy of a secure e-mail standard, *Messaging Magazine*, 1988.

Freier, Alan O., Karlton, Philip, and Kocher, Paul C., "INTERNET-DRAFT- The SSL Protocol Version 3.0", November 18, 1996.

Hallam-Baker, Phillip, "Micro Payment Transfer Protocol (MPTP) Version 1.0", Joint Electronic Payment Initiative – W3C, November 1995.

Hirsch, Frederick, Introducing SSL and certificates using SSLeay, the Open Group Research Institute, *World Wide Web Journal*, Summer 1997.

Hudson, T.J. and Young, E.A., *SSL Programmers Reference*, July 1, 1995.

Lundblade, Laurence, *A Review of E-mail Security Standards*, Qualcomm Inc., 1998.

Pearah, David, *Micropayments*, Massachusetts Institute of Technology, April 23, 1997.

PKCS#7: *Cryptographic Message Syntax Standard*, RSA Laboratories Technical Note Version 1.5, RSA Laboratories, November 1, 1993.
Ramsdell, Blake, "INTERNET-DRAF- S/MIME Version3 Message Specification", Worldtalk Inc., August 6, 1998.
Resorla, E. and Schiffman, A., "INTERNET-DRAFT – The Secure HyperText Transfer Protocol", Terisa Systems, Inc., June 1998.
Schneier, Bruce, E-Mail Security: How to Keep Your Electronic Messages Private, John Wiley & Sons, 1995.
SET *Secure Electronic Transaction Specification, Book 1: Business Description*, Setco, Inc., May 31, 1997.