

TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

VIỆN ĐIỆN TỬ - VIỄN THÔNG



ĐỒ ÁN

TỐT NGHIỆP ĐẠI HỌC

Đề tài:

**THIẾT KẾ PHẦN MỀM TRUYỀN THÔNG ĐA
PHƯƠNG TIỆN TRONG MẠNG LAN, WLAN**

Sinh viên thực hiện: NGUYỄN MINH THẢO
MSSV: 20112213
Lớp: ĐT3 – K56
Giảng viên hướng dẫn: TS. NGUYỄN VŨ THẮNG

Hà Nội, 6-2016

TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

VIỆN ĐIỆN TỬ - VIỄN THÔNG



ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC

Đề tài:

**THIẾT KẾ PHẦN MỀM TRUYỀN THÔNG ĐA
PHƯƠNG TIỆN TRONG MẠNG LAN, WLAN**

Sinh viên thực hiện: NGUYỄN MINH THẢO

MSSV: 20112213

Lớp ĐT3 – K56

Giảng viên hướng dẫn: TS. NGUYỄN VŨ THẮNG

Cán bộ phản biện:

Hà Nội, 6-2016

Đánh giá quyền đề án tốt nghiệp

(Dùng cho giảng viên hướng dẫn)

Giảng viên đánh giá:.....

Họ và tên Sinh viên:..... MSSV:.....

Tên đề án:

.....

.....

Chọn các mức điểm phù hợp cho sinh viên trình bày theo các tiêu chí dưới đây:

Rất kém (1); Kém (2); Đạt (3); Giỏi (4); Xuất sắc (5)

Có sự kết hợp giữa lý thuyết và thực hành (20)						
1	Nêu rõ tính cấp thiết và quan trọng của đề tài, các vấn đề và các giả thuyết (bao gồm mục đích và tính phù hợp) cũng như phạm vi ứng dụng của đề án	1	2	3	4	5
2	Cập nhật kết quả nghiên cứu gần đây nhất (trong nước/quốc tế)	1	2	3	4	5
3	Nêu rõ và chi tiết phương pháp nghiên cứu/giải quyết vấn đề	1	2	3	4	5
4	Có kết quả mô phỏng/thực nghiệm và trình bày rõ ràng kết quả đạt được	1	2	3	4	5
Có khả năng phân tích và đánh giá kết quả (15)						
5	Kế hoạch làm việc rõ ràng bao gồm mục tiêu và phương pháp thực hiện dựa trên kết quả nghiên cứu lý thuyết một cách có hệ thống	1	2	3	4	5

6	Kết quả được trình bày một cách logic và dễ hiểu, tất cả kết quả đều được phân tích và đánh giá thỏa đáng.	1	2	3	4	5
7	Trong phần kết luận, tác giả chỉ rõ sự khác biệt (nếu có) giữa kết quả đạt được và mục tiêu ban đầu đề ra đồng thời cung cấp lập luận để đề xuất hướng giải quyết có thể thực hiện trong tương lai.	1	2	3	4	5
Kỹ năng viết (10)						
8	Đồ án trình bày đúng mẫu quy định với cấu trúc các chương logic và đẹp mắt (bảng biểu, hình ảnh rõ ràng, có tiêu đề, được đánh số thứ tự và được giải thích hay đề cập đến trong đồ án, có căn lề, dấu cách sau dấu chấm, dấu phẩy v.v), có mở đầu chương và kết luận chương, có liệt kê tài liệu tham khảo và có trích dẫn đúng quy định	1	2	3	4	5
9	Kỹ năng viết xuất sắc (cấu trúc câu chuẩn, văn phong khoa học, lập luận logic và có cơ sở, từ vựng sử dụng phù hợp v.v.)	1	2	3	4	5
Thành tựu nghiên cứu khoa học (5) (chọn 1 trong 3 trường hợp)						
10a	Có bài báo khoa học được đăng hoặc chấp nhận đăng/đạt giải SVNC khoa học giải 3 cấp Viện trở lên/các giải thưởng khoa học (quốc tế/trong nước) từ giải 3 trở lên/ Có đăng ký bằng phát minh sáng chế	5				
10b	Được báo cáo tại hội đồng cấp Viện trong hội nghị sinh viên nghiên cứu khoa học nhưng không đạt giải từ giải 3 trở lên/Đạt giải khuyến khích trong các kỳ thi quốc gia và quốc tế khác về chuyên ngành như TI contest.	2				
10c	Không có thành tích về nghiên cứu khoa học	0S				

Điểm tổng	/50
Điểm tổng quy đổi về thang 10	

3. Nhận xét thêm của Thầy/Cô (giảng viên hướng dẫn nhận xét về thái độ và tinh thần làm việc của sinh viên)

.....

.....

.....

.....

.....

.....

.....

.....

.....

Ngày: / /2016

Người nhận xét

(Ký và ghi rõ họ tên)

Đánh giá quyền đề án tốt nghiệp

(Dùng cho cán bộ phản biện)

Giảng viên đánh giá:.....

Họ và tên Sinh viên:..... MSSV:.....

Tên đề án:

.....

.....

Chọn các mức điểm phù hợp cho sinh viên trình bày theo các tiêu chí dưới đây:

Rất kém (1); Kém (2); Đạt (3); Giỏi (4); Xuất sắc (5)

Có sự kết hợp giữa lý thuyết và thực hành (20)						
1	Nêu rõ tính cấp thiết và quan trọng của đề tài, các vấn đề và các giả thuyết (bao gồm mục đích và tính phù hợp) cũng như phạm vi ứng dụng của đề án	1	2	3	4	5
2	Cập nhật kết quả nghiên cứu gần đây nhất (trong nước/quốc tế)	1	2	3	4	5
3	Nêu rõ và chi tiết phương pháp nghiên cứu/giải quyết vấn đề	1	2	3	4	5
4	Có kết quả mô phỏng/thực nghiệm và trình bày rõ ràng kết quả đạt được	1	2	3	4	5
Có khả năng phân tích và đánh giá kết quả (15)						
5	Kế hoạch làm việc rõ ràng bao gồm mục tiêu và phương pháp thực hiện dựa trên kết quả nghiên cứu lý thuyết một cách có hệ thống	1	2	3	4	5

6	Kết quả được trình bày một cách logic và dễ hiểu, tất cả kết quả đều được phân tích và đánh giá thỏa đáng.	1	2	3	4	5
7	Trong phần kết luận, tác giả chỉ rõ sự khác biệt (nếu có) giữa kết quả đạt được và mục tiêu ban đầu đề ra đồng thời cung cấp lập luận để đề xuất hướng giải quyết có thể thực hiện trong tương lai.	1	2	3	4	5
Kỹ năng viết (10)						
8	Đồ án trình bày đúng mẫu quy định với cấu trúc các chương logic và đẹp mắt (bảng biểu, hình ảnh rõ ràng, có tiêu đề, được đánh số thứ tự và được giải thích hay đề cập đến trong đồ án, có căn lề, dấu cách sau dấu chấm, dấu phẩy v.v), có mở đầu chương và kết luận chương, có liệt kê tài liệu tham khảo và có trích dẫn đúng quy định	1	2	3	4	5
9	Kỹ năng viết xuất sắc (cấu trúc câu chuẩn, văn phong khoa học, lập luận logic và có cơ sở, từ vựng sử dụng phù hợp v.v.)	1	2	3	4	5
Thành tựu nghiên cứu khoa học (5) (chọn 1 trong 3 trường hợp)						
10a	Có bài báo khoa học được đăng hoặc chấp nhận đăng/đạt giải SVNC khoa học giải 3 cấp Viện trở lên/các giải thưởng khoa học (quốc tế/trong nước) từ giải 3 trở lên/ Có đăng ký bằng phát minh sáng chế	5				
10b	Được báo cáo tại hội đồng cấp Viện trong hội nghị sinh viên nghiên cứu khoa học nhưng không đạt giải từ giải 3 trở lên/Đạt giải khuyến khích trong các kỳ thi quốc gia và quốc tế khác về chuyên ngành như TI contest.	2				
10c	Không có thành tích về nghiên cứu khoa học	0				

Điểm tổng	/50
Điểm tổng quy đổi về thang 10	

3. Nhận xét thêm của Thầy/Cô

.....

.....

.....

.....

.....

.....

.....

.....

Ngày: / /20116

Người nhận xét

(Ký và ghi rõ họ tên)

Lời mở đầu

Hiện nay vấn đề toàn cầu hoá thông tin và tốc độ phát triển của khoa học công nghệ diễn ra một cách nhanh chóng, một kỷ nguyên mới được mở ra: kỷ nguyên của xã hội hóa thông tin. Công nghệ thông tin và truyền thông phát triển đã đưa thế giới chuyển sang thời đại mới thời đại của công nghệ. Việc nắm bắt và ứng dụng Công nghệ thông tin trong các lĩnh vực khoa học, kinh tế, xã hội đã đem lại cho các doanh nghiệp và các tổ chức những thành tựu và lợi ích to lớn.

Máy tính đã trở thành công cụ đắc lực và không thể thiếu của con người. Các tổ chức, công ty hay các cơ quan cần phải xây dựng hệ thống mạng máy tính cho riêng mình để trao đổi dữ liệu giữa các bộ phận. Dữ liệu được truyền đi trên mạng phải đảm bảo: dữ liệu được chuyển tới đích nhanh chóng và đúng đắn. Dữ liệu trao đổi có thể là File, text, audio streaming, video....

Hiểu được tầm quan trọng của việc trao đổi thông tin trong nội bộ các cơ quan tổ chức, nhất là những tổ chức có tính bảo mật cao. Em quyết định chọn đề tài viết phần mềm “*Truyền thông đa phương tiện trong mạng Lan, Wlan*” làm đề tài tốt nghiệp cho mình. Nội dung chính của đồ án bao gồm:

Chương 1. Giới thiệu một cách tổng quát nhất về Đa phương tiện cũng như truyền thông đa phương tiện.

Chương 2. Trình bày những kiến thức căn bản về mạng máy tính: định nghĩa, phân loại, các loại giao thức mạng, các mô hình hoạt động của mạng máy tính.

Chương 3. Lập trình socket trong java. Chương này đi sâu nghiên cứu các tính chất, khái niệm về socket, socket trong java và một số lớp trong lập trình java socket.

Chương 4. Trình bày về chữ ký điện tử, đây là một dạng dữ liệu đa phương tiện rất cần thiết trong thời buổi phát triển như hiện nay. Chương này đi sâu nghiên cứu về phương pháp tạo và giải mã chữ ký điện tử, thay cho việc ký tay truyền thống.

Chương 5. Chương này sẽ đi sâu phân tích thiết kế hệ thống phần mềm truyền thông đa phương tiện trong mạng Lan, Wlan. Kết quả chạy chương trình, ưu điểm, nhược điểm còn tồn tại.

Cuối cùng em xin được bày tỏ lòng biết ơn chân thành tới thầy giáo Ts. Nguyễn Vũ Thắng - Giảng viên khoa ĐTVT trường Đại học Bách Khoa Hà Nội, người thầy đã trực tiếp giảng dạy và tận tình giúp đỡ, chỉ bảo em trong suốt thời gian qua. Cảm ơn thầy đã luôn động viên, hướng dẫn, định hướng và truyền thụ cho em những kiến thức vô cùng quý báu để em có thể hoàn thành đồ án tốt nghiệp này.

Do tính thực tế và kiến thức còn hạn chế, vì vậy em rất mong nhận được sự chỉ bảo của các thầy cô giáo và sự tham gia đóng góp ý kiến của các bạn để em có thể hoàn thành tốt đề tài của mình.

Hà Nội, ngày....thángnăm 2016

Sinh viên

Mô tả đề tài

Tên đề tài: Thiết Kế Phần Mềm Truyền Thông Đa Phương Tiện Trong Mạng Lan, Wlan.

Tính cấp thiết của đề tài: Hiện nay, nhu cầu trao đổi thông tin giữa các nhân viên trong một tổ chức, một phòng ban hay thậm chí là của toàn bộ một công ty là hết sức cần thiết. Cụ thể đó là nhu cầu chat text, truyền file, video call, ký gửi... Nếu muốn thực hiện điều này, yêu cầu nhất thiết là công ty phải kết nối mạng Internet, nhưng cho dù có mạng Internet thì việc trao đổi cũng hết sức khó khăn vì phải tạo tài khoản và trao đổi với nhau trên các trang mạng xã hội như yahoo, facebook, email... Điều này tạo ra lỗ hổng bảo mật lớn trong công ty, nguy cơ về việc bị đánh cắp tài liệu, ăn cắp bản quyền, rò rỉ hợp đồng ra bên ngoài là hoàn toàn có thể xảy ra. Để đảm bảo về tính an toàn dữ liệu cho công ty, mỗi nhân viên khi muốn trao đổi thông tin, phải gặp nhau trực tiếp, khi muốn gửi file tài liệu cho nhau phải copy ra usb rồi gửi cho nhau, điều này làm mất rất nhiều thời gian và không tiện lợi. Hay khi một nhân viên muốn gửi một tài liệu cho giám đốc ký, nhân viên đó phải gặp trực tiếp giám đốc, đưa tài liệu tận tay cho giám đốc xem xét sau đó mới được ký. Một ngày có hàng trăm tài liệu cần ký, việc gặp giám đốc và chờ đợi được ký làm mất nhiều thời gian công sức, dẫn đến hiệu quả làm việc không được cao.

Hiểu được nhu cầu thiết yếu của việc trao đổi thông tin giữa các nhân viên trong một công ty, em quyết định chọn đề tài: *“Thiết kế phần mềm truyền thông đa phương tiện trong mạng Lan, Wlan”* để đáp ứng nhu cầu trên.

Kết quả mong muốn của đề tài: Thiết kế được phần mềm truyền thông đa phương tiện trong mạng Lan, Wlan có khả năng kết nối hàng trăm nhân viên trong một công ty vào một hệ thống duy nhất bằng tài khoản và mật khẩu được cấp. Phần mềm có hai phần, phía server chịu trách nhiệm quản lý tài khoản của nhân viên thông qua việc kết nối đến cơ sở dữ liệu SqlServer. Khi chạy hệ thống, thì server sẽ chạy trước và có nhiệm vụ lắng nghe, kiểm tra, chấp nhận việc đăng nhập vào hệ thống của nhân viên. Phía nhân viên hay còn gọi là phía clients, khi sử dụng phần mềm đó, sẽ có giao diện đăng nhập vào

server, sau đó các nhân viên có thể trao đổi thông tin cho nhau, họp nhóm, gửi file, gọi video cho nhau... đặc biệt là có thể tạo và thẩm định chữ ký điện tử, thay cho việc ký tay truyền thống.

Hướng giải quyết của đề tài: Để thực hiện được đề tài, trước tiên em tìm hiểu về đa phương tiện cũng như truyền thông đa phương tiện, để phục vụ cho việc viết code phần video call. Sau đó em tìm hiểu về phương pháp tạo và thẩm định chữ ký điện tử, đây là một chức năng quan trọng của phần mềm. Cuối cùng muốn truyền thông tin giữa các máy tính, em tìm hiểu về mạng máy tính cũng như lập trình mạng trong Java. Sở dĩ em chọn lập trình bằng ngôn ngữ Java vì nó có rất nhiều thư viện hỗ trợ, ví dụ như thư viện hỗ trợ việc get ảnh từ camera, thư viện get audio từ mic, thư viện mã hóa RSA....Hơn nữa việc lập trình giao diện với Swing trong Java khá dễ dàng, vì nó hỗ trợ kéo thả rất linh hoạt, tóm lại Java là ngôn ngữ lập trình rất mạnh, điều này giúp em có thể hoàn thành đồ án một cách dễ dàng hơn.

Tóm tắt đồ án

Tìm hiểu một cách tổng quát nhất về Đa phương tiện cũng như Truyền thông đa phương tiện. Nghiên cứu những kiến thức căn bản về mạng máy tính: Định nghĩa, phân loại, các loại giao thức mạng, các mô hình hoạt động của mạng máy tính. Lập trình socket trong java, đi sâu nghiên cứu các tính chất, khái niệm về socket, socket trong java và một số lớp trong lập trình java socket. Ngoài ra còn đi sâu nghiên cứu về phương pháp tạo và giải mã chữ ký điện tử, thay cho việc ký tay truyền thống, đây là một dạng dữ liệu đa phương tiện rất cần thiết trong thời buổi công nghệ phát triển không ngừng như hiện nay. Để từ đó thiết kế phần mềm truyền thông đa phương tiện trong mạng Lan, Wlan với mục đích: Giúp mọi người có thể kết nối được với nhau trong mạng nội bộ, trao đổi thông tin cho nhau, ký gửi, gọi điện thoại, gọi video với nhau, từ đó phát triển phục vụ việc hội thảo trực tuyến, dạy học trực tuyến qua mạng.

Learning multimedia as well as multimedia communications in the most general way. Research the basic knowledge of computer network: definition, classification, types of network protocol, the operating model of the computer network. Socket programming in java: study in depth the nature and concept of sockets, socket in java and some layers in the Java programming socket. Besides, methods of creating and decoding electronic signature replacing the traditional signing by hand also studied in depth. This is a form of multimedia data which is essential in times of progressive development of technology as today. Thence, software design of multimedia communication in LAN, WLAN with the aim of helping people to connect with each other in the local network, exchange information, deposit, and call or call video, thereby it is developed to service online seminars, online learning.

Mục lục

Lời mở đầu	1
Mô tả đề tài.....	3
Tóm tắt đồ án	5
Mục lục.....	6
Danh mục hình vẽ	9
Danh mục các từ viết tắt.....	11
CHƯƠNG 1. TỔNG QUAN VỀ TRUYỀN THÔNG ĐA PHƯƠNG TIỆN	12
1.1 Các khái niệm cơ bản.....	12
1.2 Các ứng dụng đa phương tiện	14
1.2.1 Xem phim theo yêu cầu	14
1.2.2 Thông tin theo yêu cầu (Information on Demand)	15
1.2.3 Giáo dục (Education)	15
1.2.4 Hệ thống thầy thuốc từ xa (Telemedicine).....	16
1.2.5 Điện thoại truyền hình và hội thảo truyền hình	16
1.3 Phân loại các hệ thống đa phương tiện	17
1.4 Kết luận	18
CHƯƠNG 2. TỔNG QUAN VỀ MẠNG MÁY TÍNH	19
2.1 Định nghĩa mạng máy tính.....	19
2.2 Phân loại mạng máy tính.....	20
2.3 Một số topo mạng thông dụng	22
2.4 Mô hình OSI.....	24
2.5 Mô hình TCP/IP	27

2.5.1 Tầng truy nhập mạng - Network Acces Layer	30
2.5.2 Tầng Internet – Internet Layer	30
2.5.3 Tầng giao vận - Transport Layer.....	30
2.5.4 Tầng ứng dụng – Application Layer	30
2.6 Kết luận	31
CHƯƠNG 3. LẬP TRÌNH SOCKET TRONG JAVA	32
3.1 Tổng quan về Socket.....	32
3.1.1 Các khái niệm cơ bản	32
3.1.2 Nguyên lý hoạt động	34
3.2 Socket trong Java	38
3.2.1 Các phương thức lớp ServerSocket trong Java	39
3.2.2 Các phương thức lớp Socket trong Java	40
3.2.3 Các phương thức lớp InetAddress trong Java	42
3.3. Kết luận	43
CHƯƠNG 4. CHỮ KÝ ĐIỆN TỬ	44
4.1 Tổng quan về chữ ký điện tử.....	44
4.1.1 Một số khái niệm quan trọng	44
4.1.2. Mô hình chữ ký điện tử RSA	45
4.2 Hàm băm SHA-1	47
4.2.1 Tổng quan về hàm băm.....	47
4.2.2 Hàm băm SHA-1	49
4.2.3 Cài đặt thuật toán băm SHA-1	50
4.3 Thuật toán RSA.....	53
4.3.1 Khái niệm.....	53

4.3.2 Sơ đồ thuật toán	54
4.4 Kết luận	55
CHƯƠNG 5. THIẾT KẾ PHẦN MỀM TRUYỀN THÔNG ĐA PHƯƠNG TIỆN.....	56
5.1 Sơ đồ khối tổng quát của hệ thống.....	56
5.1.1 Sơ đồ khối	56
5.1.2 Đặc tả Use Case	57
5.2 Phân tích thiết kế phía Server	58
5.2.1 Sơ đồ khối phía Server	58
5.2.2 Thiết kế chi tiết lớp phía Server	59
5.3 Phân tích thiết kế phía Client	60
5.3.1 Sơ đồ khối phía Client.....	60
5.3.2 Thiết kế chi tiết lớp phía Client.....	61
5.4 Kết quả chạy chương trình	65
5.5 Kết luận	71
Kết luận	72
Tài liệu tham khảo.....	73
Bảng đối chiếu thuật ngữ Anh Việt.....	75

Danh mục hình vẽ

Hình 1.1 Một mô hình các máy tính liên kết trong mạng	20
Hình 1.2 Mô hình mạng cục bộ LAN	21
Hình 1.3 Mô hình mạng diện rộng(WAN).....	22
Hình 1.4 Ring Topology	23
Hình 1.5 Bus Topology.....	23
Hình 1.6 Star Topology	23
Hình 3.1 Mô hình OSI	25
Hình 3.2 Mô hình TCP/IP	29
Hình 3.1 Mô hình OSI rút gọn	33
Hình 3.2 Mô hình Socket	33
Hình 3.4 Mô hình kết nối TCP	36
Hình 3.5 Mô hình kết nối UDP	37
Hình 4.1 Tạo chữ ký điện tử	45
Hình 4.2 Thẩm định chữ ký điện tử	46
Hình 4.3 Sơ đồ tổng quát thuật toán RSA	54
Hình 4.4 Sơ đồ tạo khóa	54
Hình 4.5 Sơ đồ mã hóa và giải mã	55
Hình 5.1 Sơ đồ khối tổng quát của hệ thống.....	56
Hình 5.2 Đặc tả Use case của hệ thống.....	57
Hình 5.3 Sơ đồ khối phía Server.....	58
Hình 5.4 Biểu đồ Class phía Server.....	59
Hình 5.5 Sơ đồ khối phía Client.....	60
Hình 5.6 Biểu đồ Class Main Packages.....	61
Hình 5.7 Biểu đồ Class File Packages.....	62
Hình 5.8 Biểu đồ Class RSA Packages	62
Hình 5.9 Biểu đồ class Video Call Packages.....	63
Hình 5.10 Biểu đồ Class Voice call Packages.....	64

<i>Hình 5.11 Giao diện phía Server</i>	<i>65</i>
<i>Hình 5.12 Giao diện phía Client.....</i>	<i>66</i>
<i>Hình 5.13 Giao diện chọn file để gửi.....</i>	<i>67</i>
<i>Hình 5.14 Giao diện tùy chọn có nhận file hay không.....</i>	<i>68</i>
<i>Hình 5.15 Giao diện bên ký.....</i>	<i>69</i>
<i>Hình 5.16 Giao diện bên thẩm định chữ ký</i>	<i>70</i>

Danh mục các từ viết tắt

Từ Viết Tắt	Nghĩa Tiếng Anh	Nghĩa Tiếng Việt
MOD	Movie On Demand	Dịch Vụ Video
IOD	Information On Demand	Thông Tin Theo Yêu Cầu
ITU	International Telecommunications Union	Hiệp Hội Viễn Thông Quốc Tế
LAN	Local Area Network	Mạng Cục Bộ
MAN	Metropolitan Area Network	Mạng Đô Thị
WAN	Wide Area Network	Mạng Diện Rộng
ISO	International Standard Organization	Tổ Chức Tiêu Chuẩn Quốc Tế
MAC	Media Access Control).	Điều Khiển Truy Nhập Phương Tiện
LLC	Logical Link Control	Điều Khiển Liên Kết Logic
IP	Internet Protocol	Giao thức mạng
TCP	Transmission Control Protocol	Giao Thức Điều Khiển Giao Vận
UDP	User Datagram Protocol	Giao Thức Vận Chuyển Gói

CHƯƠNG 1. TỔNG QUAN VỀ TRUYỀN THÔNG ĐA PHƯƠNG TIỆN

Chương này sẽ trình bày một cách tổng quát nhất về đa phương tiện cũng như truyền thông đa phương tiện bao gồm: Các khái niệm cơ bản, các ứng dụng đa phương tiện, phân loại các hệ thống đa phương tiện.

1.1 Các khái niệm cơ bản

Trước khi định nghĩa truyền thông đa phương tiện, chúng ta tìm hiểu về các kiểu phương tiện truyền thông. Phương tiện (media) đề cập tới các kiểu thông tin hay các kiểu mang thông tin như dữ liệu chữ số, hình ảnh, âm thanh và video. Có nhiều cách để xếp loại phương tiện truyền thông. Nói chung, các cách xếp loại dựa trên các định dạng vật lý và các mối quan hệ của phương tiện truyền thông với thời gian. Với cách phân loại này, có 2 loại phương tiện truyền thông: phương tiện tĩnh (static media) và phương tiện động (dynamic media).

- Phương tiện tĩnh không có chiều thời gian, nội dung và ý nghĩa không phụ thuộc vào thời gian trình bày. Phương tiện tĩnh bao gồm chữ số (alphanumeric), đồ họa (graphics), hình ảnh tĩnh (still images).
- Phương tiện động (Dynamic media) có chiều thời gian, ý nghĩa và sự chính xác phụ thuộc vào tốc độ mà nó được trình bày. Phương tiện động bao gồm âm thanh (audio), hình ảnh động (animation), phim (video). Ví dụ: Để nhận biết sự chuyển động liên tục, video phải được phát lại 25/30 ảnh (frames) trong một giây. Tương tự như vậy, khi ta phát lại một tin nhắn thoại hoặc âm nhạc đã được ghi âm, chỉ với một tốc độ phát lại tự nhiên hoặc hợp lý. Phát lại ở tốc độ chậm hoặc nhanh hơn sẽ làm biến dạng ý nghĩa hay chất lượng của âm thanh. Vì phương tiện truyền thông này phải được phát lại một cách liên tục với một tốc độ cố định. Phương tiện động còn được gọi là phương tiện liên tục (continuous media) hoặc phương tiện đẳng thời (isochronous media).

Hệ thống đa phương tiện (Multimedia system): Không có định nghĩa đã được thừa nhận cho các hệ thống đa phương tiện. Theo quan điểm ngôn ngữ học, một hệ thống có khả năng thao tác nhiều hơn một phương tiện truyền thông được gọi là hệ thống đa phương tiện. Định nghĩa này làm cho hệ thống đa phương tiện hữu ích hơn, đầy thử thách, và thú vị. Vì vậy, khi chúng ta nói thông tin đa phương tiện (multimedia information), chúng có nghĩa là sự kết hợp của nhiều loại phương tiện truyền thông với ít nhất một phương tiện liên tục. Theo định nghĩa này, một hệ thống máy tính có khả năng thao tác dữ liệu chữ số và đồ họa có thể được gọi là hệ thống đa phương tiện. Trong môn học này, chúng ta định nghĩa hệ thống đa phương tiện là hệ thống có khả năng thao tác ít nhất một phương tiện truyền thông động dạng số (digital form) cũng như phương tiện truyền thông tĩnh. Do đó một hệ thống máy tính được sử dụng để điều khiển phát lại âm thanh hoặc video tương tự (analog) không thuộc hệ thống đa phương tiện theo định nghĩa của chúng ta. Chức năng chính của hệ thống đa phương tiện gồm: Thu / chụp (capture), tạo ra (generate), lưu trữ (store), tìm kiếm / truy xuất (retrieve), xử lý (process), truyền (transmit), trình bày (present). Ta phân biệt hai mặt của hệ thống đa phương tiện:

- Xử lý đa phương tiện (multimedia computing): Tập trung vào các chức năng xử lý thông tin đa phương tiện như tìm kiếm, nhận dạng (recognition) và làm nổi bật (enhancement).
- Truyền thông đa phương tiện (communication): Tập trung vào các chức năng truyền thông tin đa phương tiện như thu / chụp, truyền và trình bày.

Sự phân biệt này không rõ ràng vì có một số chức năng có thể có trong cả hai. Ví dụ như nén dữ liệu là chức năng của xử lý nhưng nó thường được dùng trong mục đích truyền thông tin. nó cũng có thể được lập luận rằng mục đích của tất cả các xử lý đa phương tiện là cho các hoạt động trình bày và truyền thông tin hiệu quả. Các hệ thống đa phương tiện tập trung giải quyết vấn đề: Làm sao truyền dữ liệu đa phương tiện từ một máy tính đến máy tính khác, làm sao để trình bày dữ liệu đến người sử dụng. Nó không cần phải xử lý dữ liệu đa phương tiện. Các hệ thống này được gọi là hệ thống đa phương tiện thể hệ thứ nhất. Trong lĩnh vực công nghệ tiên tiến, các quy trình xử lý như:

So sánh, tìm kiếm, tái tạo hình ảnh thời gian thực (real-time image restoration), nhận dạng âm thanh và hình ảnh (audio and image recognition), được sử dụng trong các hệ thống đa phương tiện. Các hệ thống này được gọi là hệ thống đa phương tiện thế hệ thứ hai. Vì vậy, các khía cạnh tính toán đa phương tiện sẽ được phát triển hơn nữa. Tương lai công nghệ đa phương tiện sẽ là sự tích hợp của xử lý và truyền thông.

1.2 Các ứng dụng đa phương tiện

1.2.1 Xem phim theo yêu cầu

Thông thường, ta xem các chương trình truyền hình và chiếu phim một cách thụ động (không thể tương tác và điều khiển thời gian để xem các chương trình đó). Dịch vụ Video / Movie on Demand (VOD / MOD) được phát triển để vượt qua các giới hạn nêu trên và cung cấp cho người dùng những tiện ích khác. Trong VOD, nhiều bộ sưu tập video được lưu trữ trên các máy chủ video (video server). Người sử dụng / khách hàng truy cập các video này thông qua mạng tốc độ cao.

Các ưu điểm của VOD:

- Có thể xem phim mà không cần đến rạp. Tivi được kết nối đến máy chủ video thông qua mạng. Chúng ta chỉ cần chọn phim thông qua một giao diện trên màn hình.
- Máy chủ video tập trung và cung cấp các dịch vụ cho nhiều người nên các bộ sưu tập của nó rất phong phú và luôn được cập nhật. Nhiều người có thể xem cùng một phim và không gặp phải vấn đề “Xin lỗi, hết chỗ” như khi đến rạp.
- Có thể xem phim mà mình yêu thích bất kỳ lúc nào.
- Có thể tạm dừng (pause), đi tới nhanh (fast-forward), quay lại (backward) hoặc tìm kiếm một cảnh đặc biệt trong phim.
- Phim được đảm bảo chất lượng cao vì được lưu trữ dưới dạng số. Chất lượng phim không bị giảm khi tăng số lượng người xem.

1.2.2 Thông tin theo yêu cầu (Information on Demand)

Là hệ thống giống như VOD, điểm khác biệt chính yếu là IOD lưu trữ nhiều kiểu khác nhau của thông tin làm cho người dùng có một thư viện đồ sộ và linh hoạt. Khi người dùng đưa ra một truy vấn thông tin thông qua một giao diện trên tivi thông minh (smart tivi) hoặc máy tính trạm, hệ thống sẽ tìm kiếm, lấy thông tin và trình bày thông tin tìm được cho người dùng. Khả năng quan trọng nhất của hệ thống là chỉ mục và tìm kiếm trong một khối lượng rất lớn các thông tin đa phương tiện.

Hệ thống IOD có nhiều ứng dụng:

- Hoạt động như một bộ tự điển bách khoa toàn thư về thông tin tổng quát.
- Dịch vụ cung cấp báo và tạp chí trực tuyến.
- Dịch vụ mua sắm tại nhà, xem sản phẩm và đặt hàng trên màn hình mà không cần ra khỏi nhà.
- Cung cấp thông tin đồng thời các thông tin dự báo thời tiết, lịch biểu của các phương tiện giao thông công cộng một cách trực tuyến.

World Wide Web có thể được xem là một hệ thống IOD sơ cấp. WWW có thể được phát triển xa hơn để hỗ trợ tìm kiếm, truyền và biểu diễn các thông tin đa phương tiện thời gian thực. Số lượng và chất lượng thông tin ngày càng phát triển.

1.2.3 Giáo dục (Education)

Một thế mạnh ứng dụng khác của các hệ thống đa phương tiện là giáo dục. Người ta có thể học nhiều hơn và nhanh hơn khi có thể nghe, nhìn và làm việc theo một quan niệm mới trong đó đa phương tiện là phương thức tự nhiên để đào tạo và giáo dục. Trước đây, hầu hết các bài giảng đa phương tiện trên các CDROM chạy một mình trên máy tính và không thể chia sẻ cho những người dùng khác. Nó được thay đổi khi có các máy chủ đa phương tiện trên mạng điện rộng, các máy chủ này sẽ cho các khách hàng chia sẻ bộ lưu trữ, bài giảng và các tài nguyên đa phương tiện khác. Thiết lập một hệ thống như vậy có nhiều điểm lợi, nó làm cho nhiều người cố gắng học tập.

Các điểm lợi:

- Trước tiên, các bài giảng được chia sẻ cho một số lượng lớn người học làm cho chi phí học tập rẻ hơn.
- Hai là, thuận tiện cho người học, họ có thể học bất kỳ ở đâu và bất kỳ lúc nào (học viên sử dụng thời gian di chuyển để học một vấn đề nào đó).
- Ba là, phương tiện học tập có thể được tổ chức một cách linh động để phù hợp với mọi học viên. Như vậy mỗi học viên có thể tự quyết định tốc độ học tập và cách học của chính họ.
- Bốn là, tương tác với thầy giáo có thể được thực hiện thông qua các giao tiếp bằng email, hoặc trực tiếp bằng âm thanh và video.

1.2.4 Hệ thống thầy thuốc từ xa (Telemedicine)

Hệ thống thầy thuốc từ xa là một ứng dụng quan trọng khác của đa phương tiện, nhất là các trường hợp cấp cứu được điều khiển từ xa. Trong hệ thống thầy thuốc từ xa, tất cả các bệnh án được lưu trữ bằng phương tiện điện tử. Các cơ quan y tế và thiết bị được kết nối thông qua một mạng đa phương tiện. Hệ thống y tế từ xa cung cấp các hoạt động sau đây:

- Tư vấn tức thì bởi các chuyên gia y tế từ xa thông qua việc sử dụng âm thanh và video chất lượng cao.
- Các nhân viên y tế có thể truy cập các bệnh án bất kỳ lúc nào, bất kỳ ở đâu trong trường hợp khẩn cấp.
- Truy cập toàn cầu các thông tin về một kiểu đặc biệt của nhóm máu hoặc bộ phận trong cơ thể.

1.2.5 Điện thoại truyền hình và hội thảo truyền hình

Hệ thống điện thoại truyền hình (video phone) và hội thảo truyền hình (video conference) làm gia tăng hiệu quả giao tiếp của con người ở các vị trí địa lý cách xa nhau. Hầu hết các hệ thống hội thảo truyền hình trước đây đều sử dụng các thiết bị

chuyên dùng và mạng chuyển mạch kênh, chúng rất đắt tiền và cũng không dễ dàng có được. Gần đây, các camera thu hình đã được trang bị và video có thể hiển thị trên màn hình máy tính, đồng thời truyền thông qua mạng tốc độ cao phát triển làm cho hội thảo truyền hình trở nên rẻ tiền và được sử dụng phổ biến. Điện thoại truyền hình sẽ được hợp nhất với điện thoại trong tương lai gần, khái niệm “talking” trong điện thoại được thay bằng “meet” khi sử dụng điện thoại có hình.

1.3 Phân loại các hệ thống đa phương tiện

Hệ thống đa phương tiện có thể được xếp vào hệ thống độc lập hoặc hệ thống phân phối. Hệ thống độc lập: Sử dụng tài nguyên chuyên dụng. Các thông tin đa phương tiện bị giới hạn và truyền thông đa không được hỗ trợ. Hệ thống phân phối: Chia sẻ cả hai tài nguyên hệ thống và tài nguyên thông tin và có thể được hỗ trợ truyền thông tin giữa những người sử dụng. Hiệp hội viễn thông quốc tế (ITU: International Telecommunications Union) định danh 4 loại cơ bản các dịch vụ và ứng dụng phân phối:

- Các dịch vụ đàm thoại (convesational services): Bao hàm sự tương tác giữa người sử dụng này và người khác hoặc với một hệ thống. Loại này bao gồm các dịch vụ giữa các cá nhân với nhau như điện thoại có hình (videophone) và hội thảo truyền hình (videoconference). Nó cũng bao gồm dịch vụ giám sát từ xa (telesurveillance) hay mua sắm từ xa (teleshopping).
- Các dịch vụ thông điệp (messaging services): Sự trao đổi không tức thì hoặc không đồng bộ các dữ liệu đa phương tiện thông qua các hộp thư điện tử.
- Các dịch vụ tìm kiếm thông tin (retrieval services): Bao gồm tất cả các kiểu truy cập đến các máy chủ thông tin đa phương tiện. Điển hình như, người dùng gửi một yêu cầu đến máy chủ và thông tin được yêu cầu được máy chủ gửi về cho người dùng một cách tức thì. Ví dụ: Truyền hình theo yêu cầu (Video On Demand) hoặc thông tin theo yêu cầu (Information On Demand).
- Các dịch vụ phân phát thông tin (distribution services): Bao gồm các dịch vụ phân phối thông tin chủ động của các máy chủ. Ví dụ: Truyền hình quảng bá.

1.4 Kết luận

Như vậy, trong chương này đã trình bày một cách khái quát về Đa phương tiện cũng như Truyền thông đa phương tiện, các dạng dữ liệu và ứng dụng quan trọng của đa phương tiện để từ đó làm cơ sở cho việc thiết kế cài đặt phần mềm truyền thông đa phương tiện ở các chương sau.

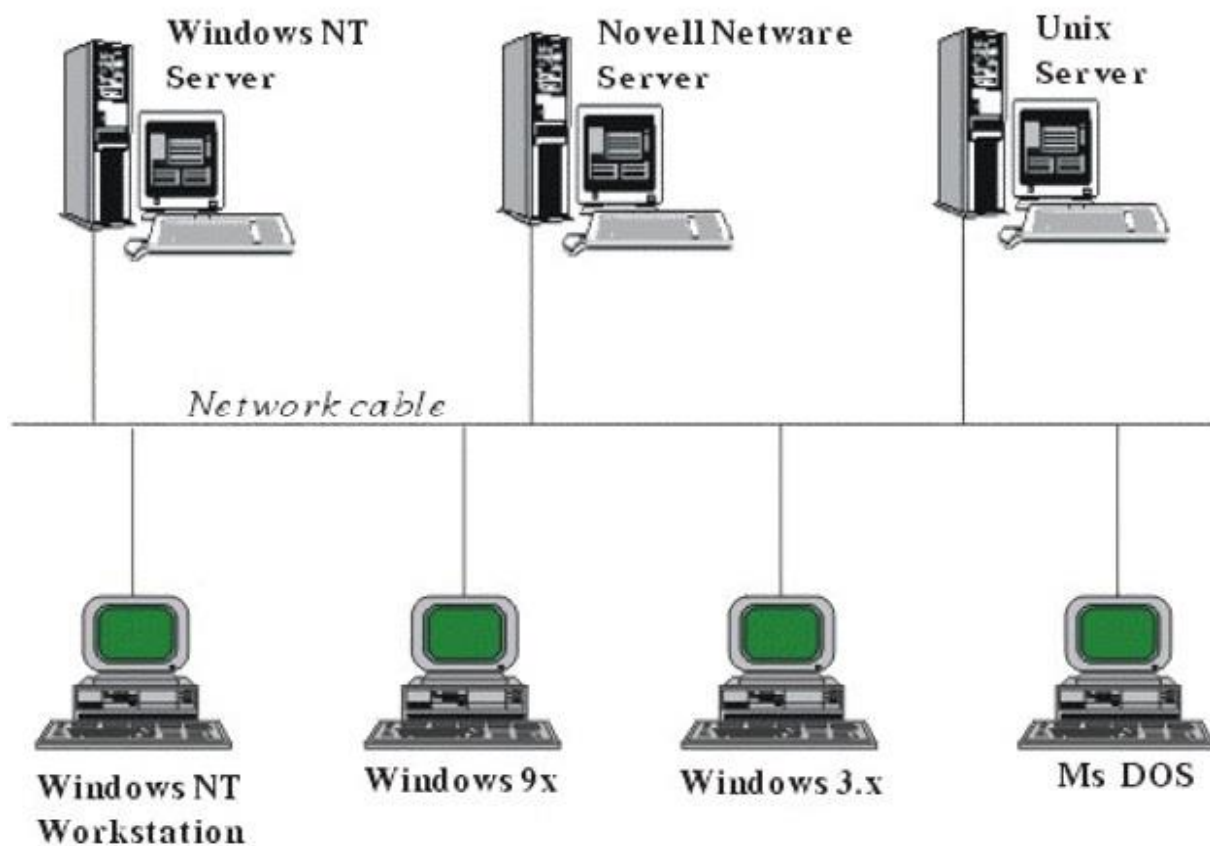
CHƯƠNG 2. TỔNG QUAN VỀ MẠNG MÁY TÍNH

Chương này sẽ trình bày những kiến thức căn bản về mạng máy tính: Định nghĩa, phân loại, các loại giao thức mạng, các mô hình hoạt động của mạng máy tính.

2.1 Định nghĩa mạng máy tính

Mạng máy tính là một tập hợp các máy tính được nối với nhau bởi đường truyền theo một cấu trúc nào đó và thông qua đó các máy tính trao đổi thông tin qua lại cho nhau.

Đường truyền là hệ thống các thiết bị truyền dẫn có dây hay không dây dùng để chuyển các tín hiệu điện tử từ máy tính này đến máy tính khác. Các tín hiệu điện tử đó biểu thị các giá trị dữ liệu dưới dạng các xung nhị phân (on - off). Tất cả các tín hiệu được truyền giữa các máy tính đều thuộc một dạng sóng điện từ. Tùy theo tần số của sóng điện từ có thể dùng các đường truyền vật lý khác nhau để truyền các tín hiệu. Ở đây đường truyền được kết nối có thể là dây cáp đồng trục, cáp xoắn, cáp quang, dây điện thoại, sóng vô tuyến ... Các đường truyền dữ liệu tạo nên cấu trúc của mạng. Hai khái niệm đường truyền và cấu trúc là những đặc trưng cơ bản của mạng máy tính.

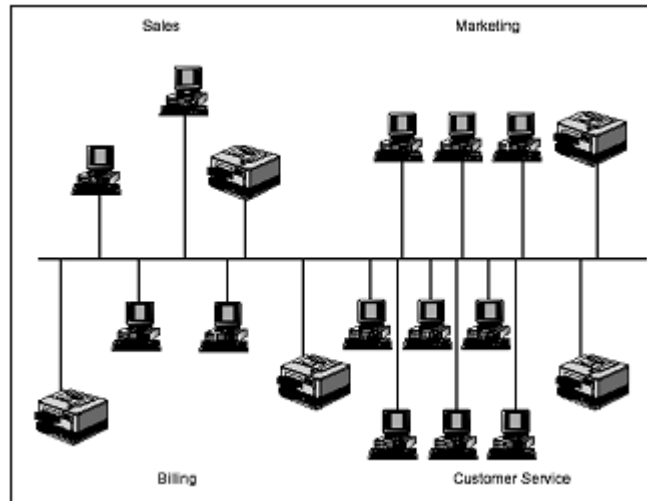


Hình 1.1 Một mô hình các máy tính liên kết trong mạng ^[4]

2.2 Phân loại mạng máy tính

Do hiện nay mạng máy tính được phát triển khắp nơi với những ứng dụng ngày càng đa dạng cho nên việc phân loại mạng máy tính là một việc rất phức tạp. Dựa theo phạm vi phân bố của mạng ta có thể phân ra các loại mạng như sau:

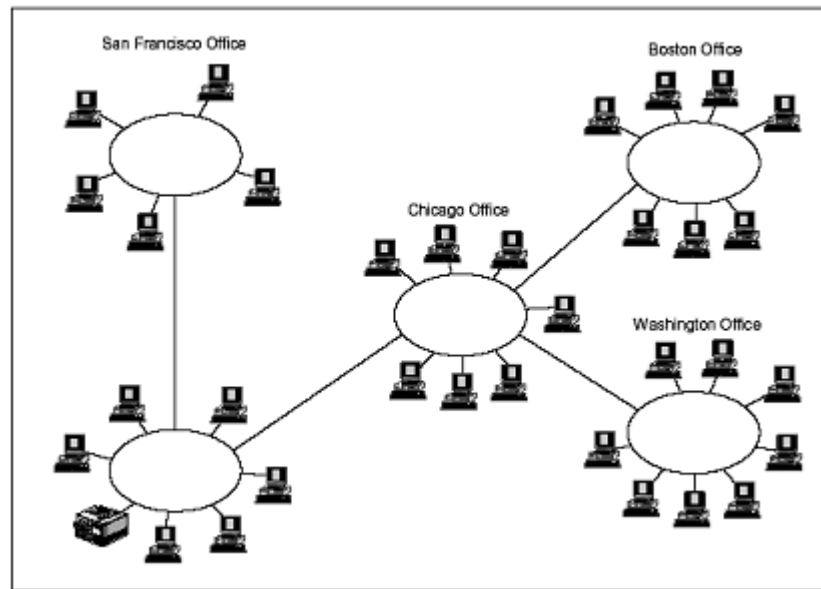
- *Mạng cục bộ LAN (Local Area Network)*: Mạng LAN là một nhóm máy tính và các thiết bị truyền thông mạng được nối kết với nhau trong một khu vực nhỏ như một tòa nhà cao ốc, khuôn viên trường đại học, khu giải trí... Các mạng LAN thường có đặc điểm sau: Băng thông lớn, có khả năng chạy các ứng dụng trực tuyến như xem phim, hội thảo qua mạng. Kích thước mạng bị giới hạn bởi các thiết bị. Chi phí các thiết bị mạng LAN tương đối rẻ, quản trị đơn giản



Hình 1.2 Mô hình mạng cục bộ LAN ^[4]

- *Mạng đô thị MAN (Metropolitan Area Network):* Mạng MAN gần giống như mạng LAN nhưng giới hạn của nó là một thành phố hay một quốc gia. Mạng MAN nối kết các mạng LAN lại với nhau thông qua các phương tiện truyền dẫn khác nhau (cáp quang, cáp đồng, sóng....) và các phương thức truyền thông khác nhau. Đặc điểm của mạng MAN: Băng thông mức trung bình, đủ để phục vụ các ứng dụng cấp thành phố hay quốc gia như chính phủ điện tử, thương mại điện tử, các ứng dụng của các ngân hàng...Do MAN nối kết nhiều LAN với nhau nên độ phức tạp cũng tăng đồng thời công tác quản trị sẽ khó khăn hơn. Chi phí các thiết bị mạng MAN tương đối đắt tiền.
- *Mạng diện rộng WAN (Wide Area Network):* Mạng WAN bao phủ vùng địa lý rộng lớn có thể là một quốc gia, một lục địa hay toàn cầu. Mạng WAN thường là mạng của các công ty đa quốc gia hay toàn cầu, điển hình là mạng internet. Do phạm vi rộng lớn của mạng WAN nên thông thường mạng WAN là tập hợp các mạng LAN, WAN nối lại với nhau bằng các phương tiện như: vệ tinh (satellites), sóng biva (microwave), cáp quang, cáp điện thoại. Đặc điểm của mạng WAN: Băng thông thấp, dễ mất kết nối, thường chỉ phù hợp với các ứng dụng offline như e-mail, web, ftp...Phạm vi hoạt động rộng lớn không giới hạn. Do kết nối của nhiều LAN, WAN lại với nhau nên mạng rất phức tạp và có tính toàn cầu nên

thường là có tổ chức quốc tế đứng ra quản trị. Chi phí cho các thiết bị và các công nghệ mạng WAN rất đắt tiền.



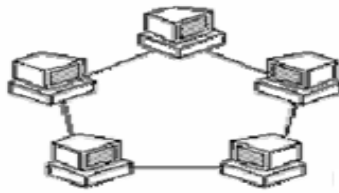
Hình 1.3 Mô hình mạng diện rộng(WAN) ^[4]

- *Mạng Internet*: Là trường hợp đặc biệt của mạng WAN, nó cung cấp các dịch vụ toàn cầu như mail, web, chat, ftp và phục vụ miễn phí cho mọi người.

2.3 Một số topo mạng thông dụng

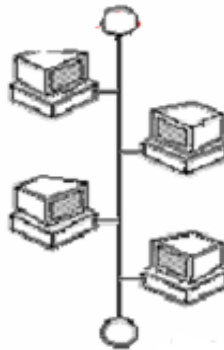
Theo định nghĩa về mạng máy tính, các máy tính được nối với nhau bởi các đường truyền vật lý theo một kiến trúc nào đó, các kiến trúc đó gọi là Topology. Thông thường mạng có ba loại kiến trúc đó là: mạng hình sao (Star Topology), mạng dạng tuyến (Bus Topology), mạng dạng vòng(Ring Topology).

- **Ring Topology**: Mạng được bố trí vòng tròn, đường dây cáp được thiết kế làm thành một vòng khép kín, tín hiệu chạy theo một chiều nào đó. Các nút truyền tín hiệu cho nhau tại một thời điểm được một nút mà thôi. Mạng dạng vòng có thuận lợi là có thể nối rộng ra xa nhưng đường dây phải khép kín, nếu bị ngắt ở một nơi nào đó thì toàn bộ hệ thống cũng bị ngưng.

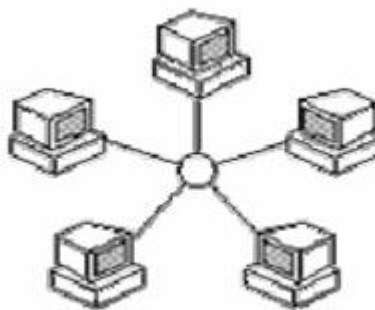


Hình 1.4 Ring Topology ^[4]

- Bus Topology: Ở dạng Bus tất cả các nút được phân chia một đường truyền chính (bus). Đường truyền này được giới hạn hai đầu bởi một loại đầu nối đặc biệt gọi là Terminator. Khi một nút truyền dữ liệu, tín hiệu được quảng bá trên hai chiều của bus, mọi nút còn lại đều được nhận tín hiệu trực tiếp. Loại mạng này dùng dây cáp ít, dễ lắp đặt. Tuy vậy cũng có những bất lợi đó là sẽ có sự ùn tắc giao thông khi di chuyển với lưu lượng lớn và khi có sự hỏng hóc ở đoạn nào đó thì rất khó phát hiện, nếu một nút ngừng hoạt động sẽ ảnh hưởng tới toàn bộ hệ thống.



Hình 1.5 Bus Topology ^[4]



Hình 1.6 Star Topology ^[4]

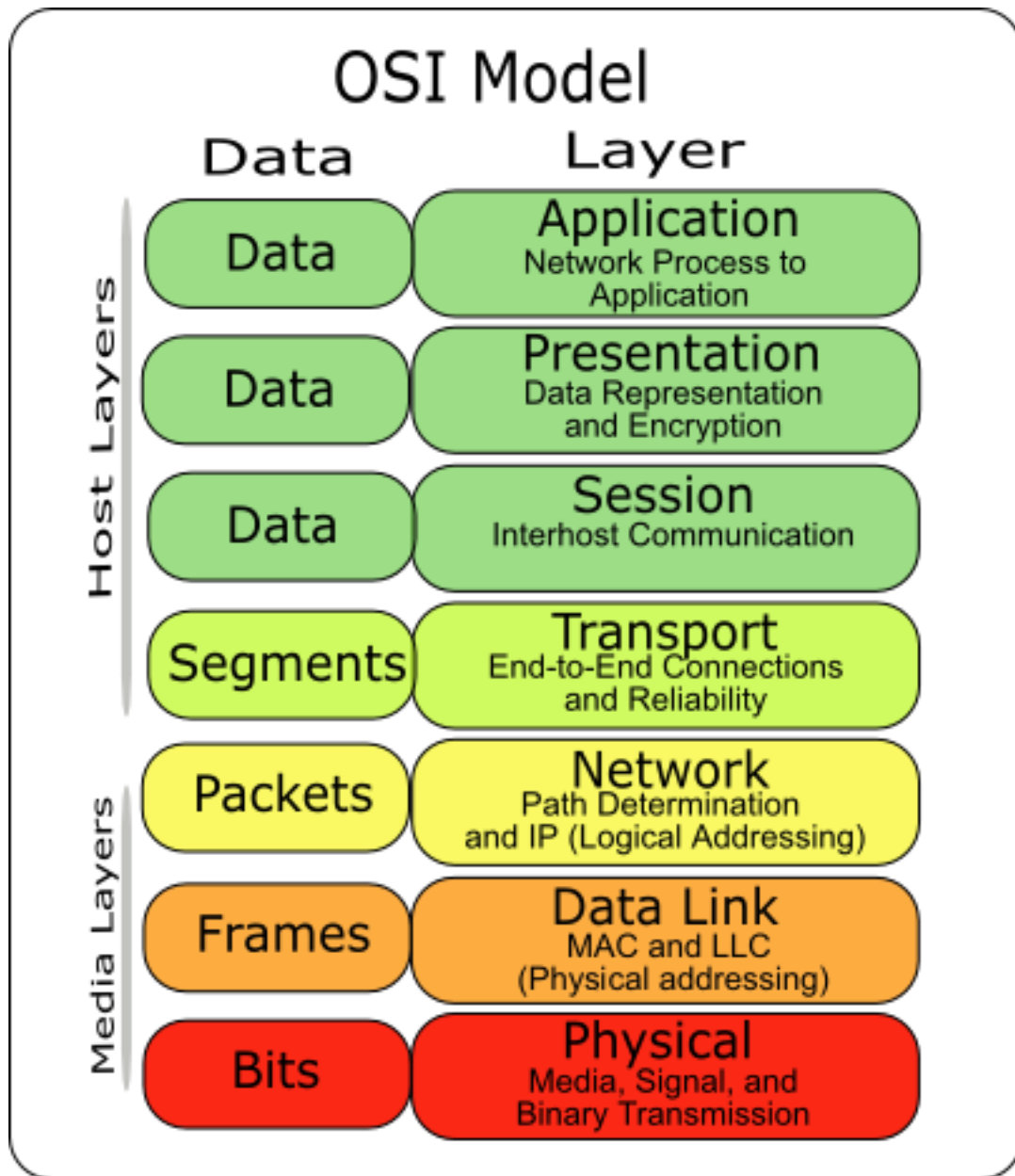
- Star Topology: Mạng hình sao bao gồm một bộ tập trung và các nút thông tin. Các nút thông tin có thể là các trạm cuối, các máy tính hay các thiết bị khác của mạng. Mạng hoạt động theo nguyên lý nối song song nên nếu có một nút bị hỏng mạng vẫn hoạt động bình thường. Mạng có thể mở rộng hoặc thu hẹp tùy theo yêu cầu của người sử dụng, tuy nhiên mở rộng phụ thuộc và khả năng của trung tâm.

2.4 Mô hình OSI

Để các máy tính và các thiết bị mạng có thể giao tiếp với nhau, ví dụ như truyền dữ liệu (FTP), truy cập trang web (HTTP) hay truy cập từ xa (Telnet),... chúng bắt buộc phải tuân theo những quy tắc chung gọi là giao thức (protocol). Từ những ngày đầu tiên của mạng máy tính, các tập đoàn lớn như IBM, Digital Equipment Corporation, Xerox,... đã cho ra các giao thức dành riêng cho thiết bị của do họ sản xuất. Kết quả của việc này là các thiết bị thuộc các hãng khác nhau không thể giao tiếp được với nhau, gây bất lợi lớn trong truyền thông.

Năm 1977, tổ chức Tiêu chuẩn quốc tế - ISO (International Standard Organization) đã đề xuất ra mô hình Hệ thống mở - OSI (Open System Interconnection) nhằm quy định thống nhất và chi tiết các hoạt động của máy tính và thiết bị mạng trong khi truyền thông, giúp các nhà sản xuất chế tạo ra các thiết bị tương thích với nhau. Đến năm 1984, mô hình tham chiếu OSI 7 lớp được công bố, mỗi lớp có một nhiệm vụ riêng biệt trong quá trình truyền thông. 7 lớp đó gồm: lớp Ứng dụng (Application), lớp Trình bày (Presentation), lớp Phiên (Session), lớp Giao vận (Transport), lớp Mạng (Network), lớp Liên kết dữ liệu (Data Link), và cuối cùng là lớp Vật lý (Physical).

Việc chia lớp của mô hình OSI có nhiều tác dụng, ví dụ như mô hình OSI giúp đơn giản hóa việc tìm hiểu và phân tích mạng, chuẩn hóa các thành phần mạng để cho phép phát triển mạng từ nhiều nhà sản xuất và ngăn chặn tình trạng thay đổi của một lớp làm ảnh hưởng đến lớp khác, giúp mỗi lớp có thể phát triển độc lập và nhanh chóng hơn.



Hình 3.1 Mô hình OSI ^[14]

Lớp Ứng dụng quy định giao diện giữa ứng dụng và mạng, các giao thức trong thuộc về lớp này rất nhiều, nhưng thường gặp nhất trên mạng là FTP, HTTP, HTTPs, SMTP, Telnet,... Lớp Ứng dụng sẽ đẩy dữ liệu xuống lớp tiếp theo ngay bên dưới là lớp Trình bày

Lớp Trình bày chịu trách nhiệm chính về phần mã hóa và định dạng dữ liệu. Ví dụ: để máy tính Linux có thể giao tiếp với máy tính Windows, lớp Trình bày phải định dạng dữ liệu sao cho phù hợp với các hệ điều hành. Các tên tập tin thường có phần đuôi mở rộng như .PICT, .MIDI, .MPEG, .RTF, ... phần đuôi này do chính lớp Trình bày thêm vào.

Lớp Phiên chịu trách nhiệm cung cấp và giải phóng các phiên làm việc thông qua việc cấp port cho các phiên này. Một máy tính trong mạng có thể vừa duyệt web, vừa gửi mail, vừa truyền file cho máy tính khác,... Các hoạt động trên diễn ra đồng thời và lớp Phiên phải phân biệt và cấp port cho các hoạt động này. Ví dụ: phiên truy cập web sẽ được cấp port là 80, phiên gửi mail được cấp port 25, phiên truyền file (FTP) được cấp port 20 và 21.

Lớp Vận chuyển đảm bảo truyền thông chính xác giữa các thiết bị. Các máy tính phải sử dụng kiểu truyền như thế nào cho phù hợp với môi trường truyền (môi trường ít lỗi hay nhiều lỗi), phải bắt tay kết nối trước khi truyền hay không,... đều do lớp Vận chuyển quy định. Dữ liệu từ lớp Session đưa xuống sẽ bị phân chia thành các đơn vị dữ liệu lớp Vận chuyển, gọi là segment, các segment được đánh số thứ tự để bên nhận có thể ghép dữ liệu lại một cách chính xác.

Lớp Mạng định ra địa chỉ logic cho các thiết bị trên mạng và quy định các nguyên tắc sử dụng địa chỉ logic này. Ví dụ: các giao thức như IP, IPX, Apple Talk có những cơ chế định địa chỉ cho máy tính và mạng máy tính trên mạng, các giao thức như RIP, OSPF, EIGRP, BGP chịu trách nhiệm định tuyến hay nói cách khác là tìm đường để dẫn gói tin đi đến đúng địa chỉ đích. Lớp Mạng sẽ đóng gói các segment do lớp Vận chuyển đẩy xuống thành các gói tin (packet).

Lớp Liên kết dữ liệu xác định địa chỉ vật lý của các thiết bị trên mạng và quy định cách thức mà dữ liệu sẽ được đưa xuống môi trường truyền. Đơn vị dữ liệu do lớp này quản lý gọi là frame. Lớp Liên kết dữ liệu bao gồm 2 lớp con là LLC (Logical Link Control) và MAC (Media Access Control). Lớp LLC liên kết với lớp Mạng để xác định

loại địa chỉ logic đang dùng là gì và sẽ đóng gói frame theo kiểu tương ứng. Lớp MAC lại kết hợp với lớp cuối cùng là lớp Vật lý để biết môi trường truyền dẫn bên dưới là gì để có cách thức sử dụng phù hợp. Ví dụ: nếu môi trường truyền dẫn là Ethernet, các frame sẽ đóng gói và định địa chỉ theo chuẩn 802.3, và quyết định có sử dụng cơ chế CSMA/CD hay không; nếu môi trường truyền dẫn là không dây thì đóng gói frame theo chuẩn 802.11 và sử dụng cơ chế CSMA/CA,...

Lớp Vật lý tìm cách biến đổi dữ liệu 0, 1 thành các tín hiệu điện và truyền ra môi trường.

Mô hình OSI đã chia nhỏ việc truyền thông phức tạp giữa các máy tính thành những tác vụ nhỏ hơn, rõ ràng hơn và dễ hiểu hơn. Các nhà nghiên cứu sẽ dựa vào những lớp con trong mô hình OSI để thiết kế ra các chuẩn mới cho mạng mà vẫn không gây ảnh hưởng lớn đến hoạt động của toàn hệ thống. Tuy nhiên, mô hình OSI chỉ là mô hình tham chiếu chứ không được đưa vào sử dụng trong thực tế. Các mô hình sử dụng trong thực tế như TCP/IP, NetBEUI (của Microsoft và IBM), IPX/SPX (của Novell), DECnet (của Digital Equipment Corporation) có biến đổi cho phù hợp hơn với thực tế nhưng vẫn dựa theo mô hình OSI này.

2.5 Mô hình TCP/IP

Mạng máy tính khổng lồ Internet hiện nay đang sử dụng mô hình TCP/IP để quản lý việc truyền thông. TCP/IP được xem là giản lược của mô hình OSI với bốn lớp sau: Ứng dụng (tích hợp 3 lớp trên cùng của mô hình OSI), Vận chuyển (tương đương với lớp Vận chuyển của OSI), Internet (tương đương với lớp Mạng nhưng chỉ sử dụng giao thức IP để định địa chỉ logic cho các máy tính) và Truy cập mạng (bao gồm 2 lớp dưới cùng của mô hình OSI).

Một số giao thức thường gặp trong mô hình TCP/IP: IP (Internet Protocol), ICMP (Internet Control Message Protocol), IGMP (Internet Group Message Protocol), TCP, UDP, Telnet, FTP, WWW, SMTP,...

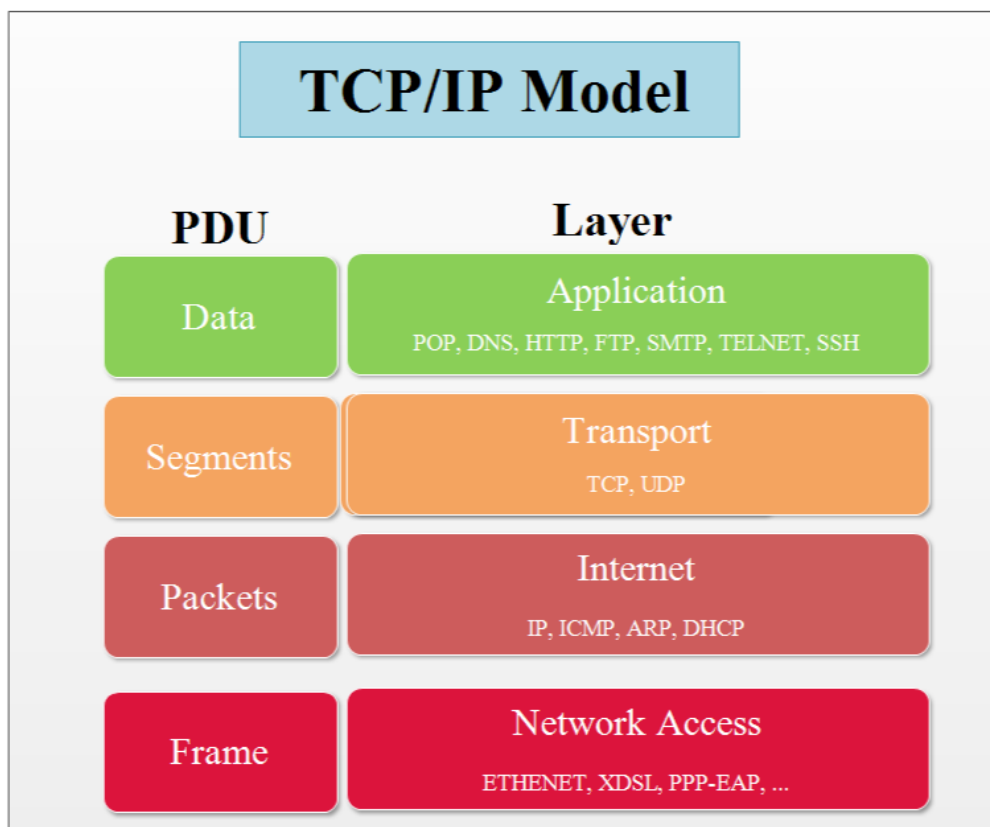
Mô hình TCP/IP gọn nhẹ hơn mô hình tham chiếu OSI, đồng thời có những biến đổi phù hợp thực tế hơn. Ví dụ: lớp Vận chuyển của mô hình OSI quy định việc truyền dữ liệu phải đảm bảo độ tin cậy hoàn toàn. Tuy nhiên, một số ứng dụng mới phát triển sau này như Voice over IP, Video Conference (hội nghị truyền hình),... đòi hỏi tốc độ cao và cho phép bỏ qua một số lỗi nhỏ. Nếu vẫn áp dụng mô hình OSI vào thì độ trễ trên mạng rất lớn và không đảm bảo chất lượng dịch vụ. Trong khi đó, mô hình TCP/IP, ngoài giao thức chính của lớp Vận chuyển là TCP (Transmission Control Protocol), còn cung cấp thêm giao thức UDP (User Datagram Protocol) để thích ứng với các ứng dụng cần tốc độ cao.

Giao thức quan trọng nhất trong mô hình TCP/IP là TCP và UDP. TCP đảm bảo độ tin cậy truyền thông bằng cách ép buộc máy nhận phải hồi báo cho máy gửi biết về những segment nào đã nhận được, segment nào bị lỗi,... để máy gửi tiếp tục truyền segment mới hay gửi lại segment bị lỗi. Các gói tin hồi báo này gọi tắt là ACK. Nếu đường truyền bị lỗi quá nặng, các gói tin hồi báo này không đến được máy gửi thì sau một khoảng thời gian quy định trước, segment sẽ được truyền lại, và nếu một segment được truyền lại quá nhiều lần, TCP sẽ ngắt kết nối với máy nhận và dừng việc truyền lại. UDP không có cơ chế tin cậy (hồi báo bằng ACK), nên việc kiểm soát độ tin cậy phải do lớp Application đảm trách. Tuy nhiên, đối với các ứng dụng yêu cầu tốc độ nhanh và chấp nhận tỷ lệ lỗi ở mức nào đó, sử dụng giao thức UDP là rất thích hợp do không phải hồi báo ACK nhiều lần. Việc linh động sử dụng giao thức TCP hay UDP trong các ứng dụng mạng phụ thuộc vào nhiều yếu tố như chất lượng đường truyền, độ quan trọng của thông tin cần truyền,...

Tuy nhiên, để hỗ trợ thêm tính tin cậy của UDP, năm 1998, các nhà nghiên cứu đã đề xuất cơ chế tránh nghẽn có tên là TCP – Friendly Rate Control, TFRC (chuẩn RFC 3448, năm 2003). Ý tưởng của cơ chế này là tìm cách báo hiệu cho máy gửi biết về tình trạng nghẽn ở máy nhận, từ đó máy gửi sẽ chủ động giảm tốc độ truyền xuống, các gói tin sẽ tới máy nhận chậm hơn một chút nhưng không đảm bảo không để gói tin bị đánh rơi do máy nhận xử lý không kịp. TCP – Friendly thích hợp cho các ứng dụng truyền

thoại, hội nghị truyền hình, xem phim qua mạng và một số ứng dụng khác yêu cầu tốc độ và tính trơn tru của dữ liệu.

Chuẩn mạng tính kỹ thuật và lịch sử của Internet là mô hình TCP/IP. Bộ quốc phòng Hoa Kỳ (DoD: Department of Defense) đã tạo ra mô hình DoD là tiền thân của mô hình TCP/IP, bởi họ muốn thiết kế một mạng có thể tồn tại dưới bất kỳ hoàn cảnh nào, ngay cả cuộc chiến tranh hạt nhân. Trong một thế giới được kết nối bằng các loại đường truyền khác nhau như cáp đồng trục, sóng vi ba, cáp sợi quang và các liên kết vệ tinh, DoD muốn truyền dẫn các gói vào mọi lúc dưới bất kỳ điều kiện nào. Bài toán thiết kế rất khác biệt này đã dẫn đến sự phát minh ra mô hình TCP/IP. Mô hình TCP/IP có bốn lớp sau: Lớp ứng dụng, Lớp vận chuyển, Lớp Internet, Lớp truy nhập mạng.



Hình 3.2 Mô hình TCP/IP ^[14]

2.5.1 Tầng truy nhập mạng - Network Acces Layer

Tầng truy nhập mạng bao gồm các giao thức mà nó cung cấp khả năng truy nhập đến một kết nối mạng. Tại tầng này, hệ thống giao tiếp với rất nhiều kiểu mạng khác nhau. Cung cấp các trình điều khiển để tương tác với các thiết bị phần cứng ví dụ như Token Ring, Ethernet, FDDI...

2.5.2 Tầng Internet – Internet Layer

Tầng Internet cung cấp chức năng dẫn đường các gói tin. Vì vậy tại tầng này bao gồm các thủ tục cần thiết giữa các hosts và gateways để di chuyển các gói giữa các mạng khác nhau. Một gateway kết nối hai mạng, và sử dụng kết nối mạng bao gồm IP (Internet Protocol), ICMP (Internet Control Message Protocol)

2.5.3 Tầng giao vận - Transport Layer

Tầng giao vận phân phát dữ liệu giữa hai tiến trình khác nhau trên các máy tính host. Một giao thức đầu vào tại đây cung cấp một kết nối logic giữa các thực thể cấp cao. Các dịch vụ có thể bao gồm việc điều khiển lỗi và điều khiển luồng. Tại tầng này bao gồm các giao thức Transmission Control Protocol (TCP) và User Datagram Protocol (UDP)

2.5.4 Tầng ứng dụng – Application Layer

Tầng này bao gồm các giao thức phục vụ cho việc chia sẻ tài nguyên và điều khiển từ xa (remote access). Tầng này bao gồm các giao thức cấp cao mà chúng được sử dụng để cung cấp các giao diện với người sử dụng hoặc các ứng dụng. Một số giao thức quan trọng như File Transfer Protocol (FTP) cho truyền thông, HyperText Transfer Protocol (HTTP) cho dịch vụ World Wide Web, và Simple Network Management Protocol (SNMP) cho điều khiển mạng. Ngoài ra còn có : Domain Naming Service (DNS), Simple Mail Transport Protocol (SMTP)

Post Office Protocol (POP). Internet Mail Access Protocol (IMAP), Internet Control Message Protocol (ICMP)....

2.6 Kết luận

Như vậy chương này đã trình bày đầy đủ về định nghĩa, phân loại, các loại giao thức mạng, các mô hình hoạt động của mạng máy tính từ đó làm cơ sở cho việc phân tích thiết kế phần mềm truyền thông đa phương tiện trong mạng Lan, Wlan ở các chương tiếp theo.

CHƯƠNG 3. LẬP TRÌNH SOCKET TRONG JAVA

Chương này sẽ trình bày về lập trình socket trong java, đi sâu nghiên cứu các tính chất, khái niệm về socket, socket trong java và một số lớp trong lập trình java socket.

3.1 Tổng quan về Socket

3.1.1 Các khái niệm cơ bản

- **Socket**

Socket là một công logic mà một chương trình sử dụng để kết nối với một chương trình khác chạy trên một máy tính khác trên Internet. Chương trình mạng có thể sử dụng nhiều Socket cùng một lúc, nhờ đó nhiều chương trình có thể sử dụng Internet cùng một lúc. Có 2 loại Socket:

- *Stream Socket*: Dựa trên giao thức TCP(Transmission Control Protocol) việc truyền dữ liệu chỉ thực hiện giữa 2 quá trình đã thiết lập kết nối. Giao thức này đảm bảo dữ liệu được truyền đến nơi nhận một cách đáng tin cậy, đúng thứ tự nhờ vào cơ chế quản lý luồng lưu thông trên mạng và cơ chế chống tắc nghẽn.

- *Datagram Socket*: Dựa trên giao thức UDP(User Datagram Protocol) việc truyền dữ liệu không yêu cầu có sự thiết lập kết nối giữa 2 quá trình. Ngược lại với giao thức TCP thì dữ liệu được truyền theo giao thức UDP không được tin cậy, có thể không đúng trình tự và lặp lại. Tuy nhiên vì nó không yêu cầu thiết lập kết nối không phải có những cơ chế phức tạp nên tốc độ nhanh...ứng dụng cho các ứng dụng truyền dữ liệu nhanh như chat, game.....

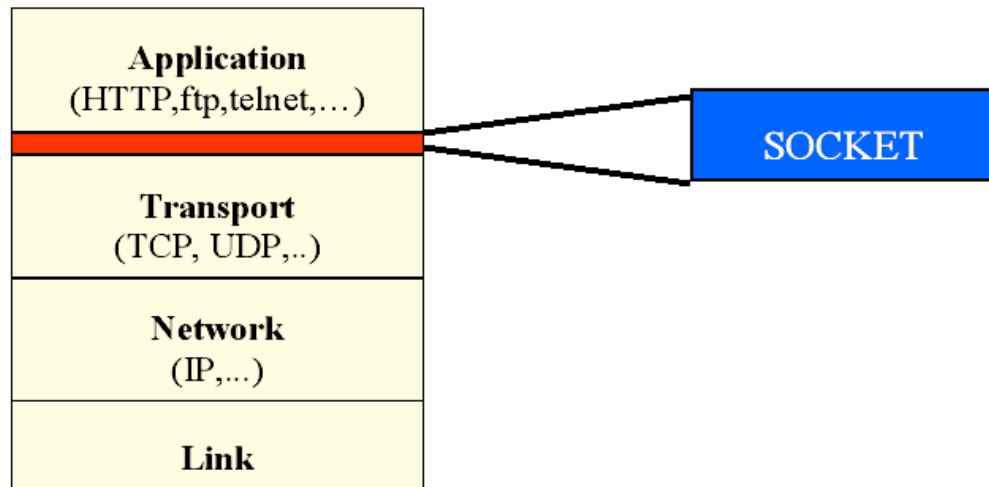
- **Port**

Port xác định duy nhất một quá trình (process) trên một máy trong mạng. Hay nói cách khác là cách mà phân biệt giữa các ứng dụng.

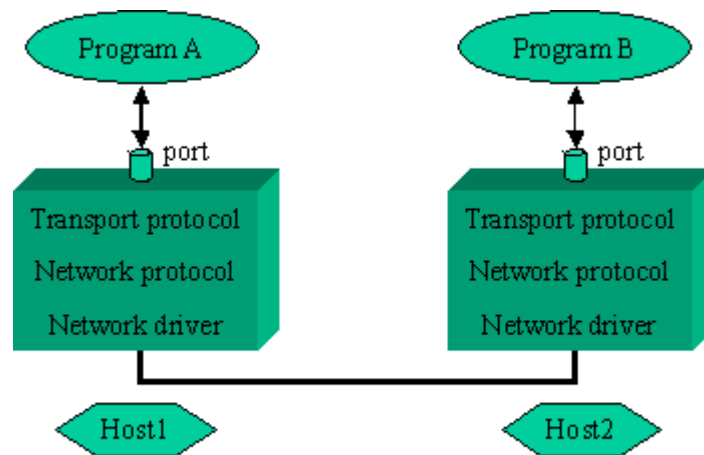
VD: Khi máy chạy nhiều ứng dụng mạng như Yahoo,Firefox, game online... .Ví dụ chương trình Yahoo sử dụng (port 5150 hay 5050) thì khi ai đó gửi tin nhắn đến cho bạn, lúc tin nhắn đến máy bạn nó sẽ dựa vào port để nhận biết đó là chương trình Yahoo (port

5150) chứ ko phải là chương trình khác. Sau đó thông tin sẽ đc xử lý và hiển thị tin nhắn lên.

Một TCP/IP Socket gồm một địa chỉ IP kết hợp với một port ? Xác định duy nhất một tiến trình (process) trên mạng. Hay nói cách khác Luồng thông tin trên mạng dựa vào IP là để xác định máy một máy trên mạng còn port xác định 1 tiến trình trên 1 máy.



Hình 3.1. Mô hình OSI rút gọn ^[3]



Hình 3.2 Mô hình Socket ^[3]

3.1.2 Nguyên lý hoạt động

Ta đã thấy khi hai ứng dụng muốn trao đổi dữ liệu qua mạng, chúng sẽ tạo ra ở mỗi phía một socket và trao đổi dữ liệu bằng cách đọc/ghi từ socket. Để hiểu rõ cách thức socket trao đổi dữ liệu chúng ta hãy xem xét nguyên lý hoạt động của chúng.

Trước hết chúng ta hãy xem xét làm thế nào các socket có thể xác định được nhau. Khi một chương trình tạo ra một socket, một định danh dạng số (định danh dạng số này còn được gọi là số hiệu cổng) sẽ được gán cho socket. Việc gán số hiệu cổng này cho socket có thể được thực hiện bởi chương trình hoặc hệ điều hành tùy theo cách socket được sử dụng như thế nào. Trong mỗi gói tin mà socket gửi đi có chứa hai thông tin để xác định đích đến của gói tin: Một địa chỉ mạng để xác định hệ thống sẽ nhận gói tin. Một số định danh cổng để nói cho hệ thống đích biết socket nào trên nó sẽ nhận dữ liệu. Nhờ hai thông tin này mà gói tin có thể đến được đúng máy tính chứa socket mà nó cần đến (nhờ địa chỉ mạng) và được phân phối đến đúng socket đích (nhờ địa chỉ cổng của socket đích).

Dưới góc độ lập trình các socket thường làm việc theo cặp, một socket đóng vai trò làm server còn các socket khác đóng vai trò như clients. Socket phía server xác định một cổng cho giao tiếp mạng, sau đó chờ nghe yêu cầu mà client gửi tới nó bằng client socket. Do đó các cổng cho server socket phải được biết bởi các chương trình client. Ví dụ server FTP sử dụng một socket để nghe tại cổng 21 do đó nếu một chương trình client muốn giao tiếp với server FTP nó cần phải kết nối đến socket có số hiệu cổng 21.

Như vậy số hiệu cổng của socket phía server được xác định bởi chương trình, ngược lại cổng cho client socket được xác định bởi hệ điều hành. Khi một socket phía client gửi một gói tin tới socket phía server thì trong gói tin đã có chứa thông tin về địa chỉ của hệ thống client và cổng của socket phía client nên server hoàn toàn có thể gửi thông tin phản hồi cho client.

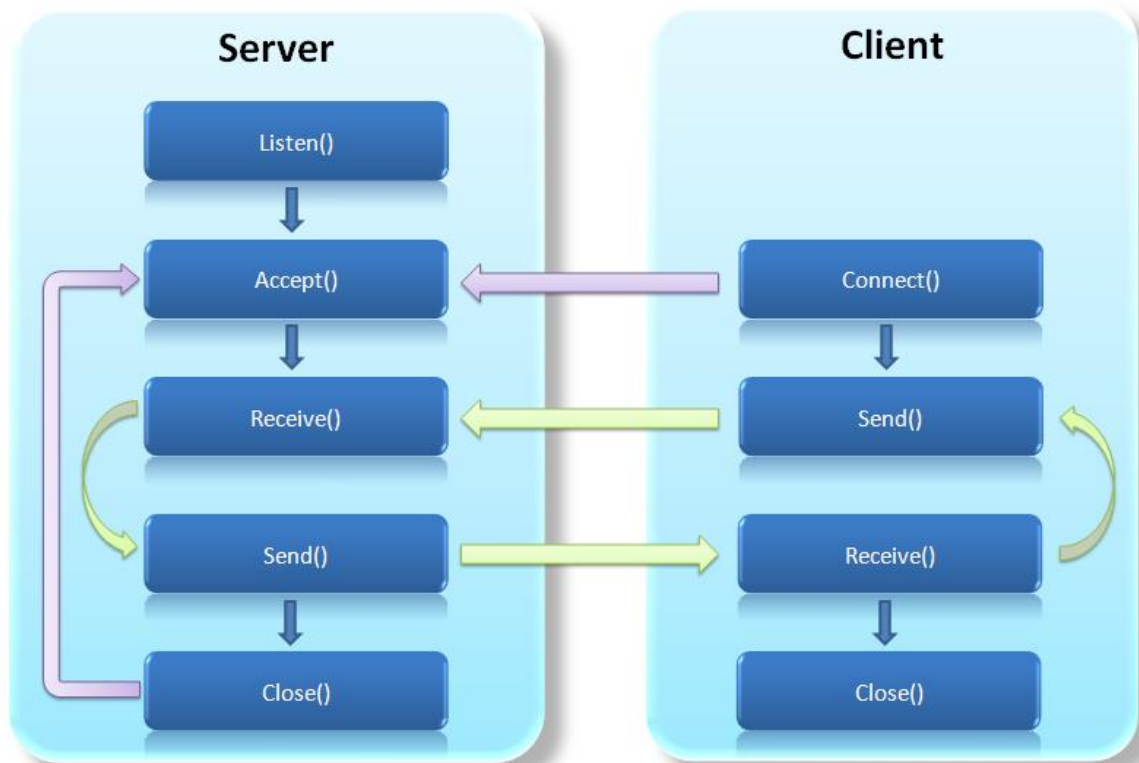
Chúng ta có thể khái quát quá trình trao đổi dữ liệu thông qua các socket như sau: Chương trình phía server tạo ra một socket, socket này được chương trình gán với một cổng trên server. Sau khi được tạo ra socket này (ta gọi là socket phía server) sẽ chờ

nghe yêu cầu từ phía clients. Khi chương trình phía clients cần kết nối với một server, nó cũng tạo ra một socket, socket này cũng được hệ điều hành gắn với một cổng. Chương trình client sẽ cung cấp cho socket của nó (ta gọi là socket phía client) địa chỉ mạng và cổng của socket phía server và yêu cầu thực hiện kết nối (nếu chương trình định sử dụng giao thức hướng kết nối) hoặc truyền dữ liệu (nếu chương trình sử dụng giao thức không hướng kết nối). Chương trình phía server và chương trình phía clients trao đổi dữ liệu với nhau bằng cách đọc từ socket hoặc ghi vào socket của mình. Các socket ở hai phía nhận dữ liệu từ ứng dụng và đóng gói để gửi đi hoặc nhận các dữ liệu được gửi đến và chuyển cho chương trình ứng dụng bởi socket ở cả hai phía đều biết được địa chỉ mạng và địa chỉ cổng của nhau.

Ở bước thứ hai chúng ta thấy chương trình ứng dụng phải lựa chọn giao thức mà nó định sử dụng để trao đổi dữ liệu. Tùy theo việc chúng ta sử dụng giao thức nào (TCP hay UDP) mà cách thức xử lý trước yêu cầu của clients có thể khác. Sau đây chúng ta sẽ xem xét chi tiết cách thức trao đổi dữ liệu của socket với từng loại giao thức.

- ***Socket hỗ trợ TCP***

Ở phía Server: Khi một ứng dụng trên server hoạt động nó sẽ tạo ra một socket và đăng ký với server một cổng ứng dụng và chờ đợi yêu cầu kết nối từ phía clients qua cổng này.



Hình 3.4 Mô hình kết nối TCP^[14]

Ở phía clients: Nó biết địa chỉ của máy trên đó server đang chạy vào cổng và server đang chờ nghe yêu cầu. Do đó khi muốn kết nối đến server, nó cũng tạo một socket chứa địa chỉ máy client và cổng của ứng dụng trên máy clients đồng thời clients sẽ cung cấp cho socket của nó địa chỉ và cổng của server mà nó cần kết nối và yêu cầu socket thực hiện kết nối.

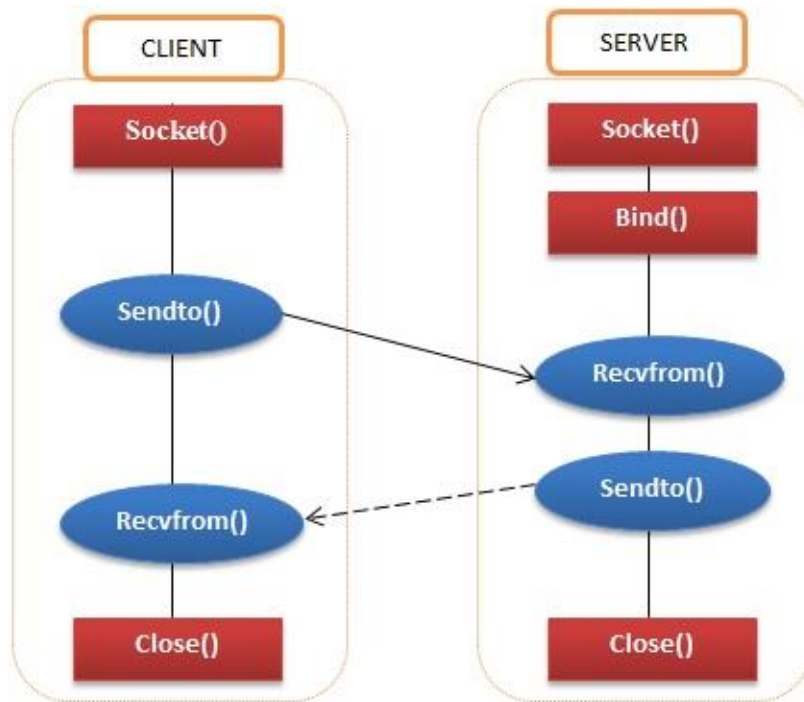
Khi server nhận được yêu cầu kết nối từ clients, nếu nó chấp nhận thì server sẽ sinh ra một socket mới được gắn với một cổng khác với cổng mà nó đang nghe yêu cầu. Sở dĩ server làm như vậy bởi nó cần cổng cũ để tiếp tục nghe yêu cầu từ phía clients trong khi vẫn cần một kết nối với clients. Sau đó chương trình ứng dụng phía server sẽ gửi thông báo chấp nhận kết nối cho clients cùng thông tin về địa chỉ cổng mới của socket mà nó dành cho clients.

Quay lại phía clients, nếu kết nối được chấp nhận nghĩa là socket của nó đã được tạo ra thành công và nó có thể sử dụng socket để giao tiếp với server bằng cách viết và ghi tới socket theo cách giao tiếp với một tài nguyên trên máy tính thông thường.

- **Socket hỗ trợ UDP**

Ở phía Server: Khi một ứng dụng trên server hoạt động nó sẽ tạo ra một socket và đăng ký với server một cổng ứng dụng và chờ đợi yêu cầu kết nối từ phía clients qua cổng này.

Ở phía Clients: Nó biết địa chỉ của máy trên đó server đang chạy vào cổng và server đang chờ nghe yêu cầu. Do đó khi muốn giao tiếp với server, nó cũng tạo ra một socket chứa địa chỉ máy clients và cổng của ứng dụng trên máy clients đồng thời clients sẽ cung cấp cho socket của nó địa chỉ và cổng của server mà nó cần kết nối. Khi clients muốn gửi tin để server nó sẽ chuyển dữ liệu cho socket của mình, socket này sẽ chuyển thẳng gói tin mà client muốn gửi tới server dưới dạng một datagram có chứa địa chỉ máy server và cổng mà server đang chờ nghe yêu cầu. Như vậy không hề có một kết nối nào được thực hiện giữa client với server và server cũng không cần tạo ra một socket khác để kết nối với clients thay vào đó server dùng ngay cổng ban đầu để trao đổi dữ liệu.



Hình 3.5 Mô hình kết nối UDP ^[14]

3.2 Socket trong Java

Các Socket cung cấp kỹ thuật giao tiếp giữa hai máy tính sử dụng TCP. Một chương trình Client tạo một socket trên đầu cuối của giao tiếp và cố gắng để kết nối socket đó tới một Server. Khi kết nối được tạo, Server tạo một đối tượng Socket trên đầu cuối của giao tiếp. Client và Server bây giờ có thể giao tiếp bằng việc đọc và ghi từ Socket. Lớp `java.net.Socket` biểu diễn một Socket, và lớp `java.net.ServerSocket` cung cấp một kỹ thuật cho chương trình Server để nghe thông tin từ các Client và thành lập các kết nối với chúng. Các bước sau xảy ra khi thành lập một kết nối TCP giữa hai máy tính sử dụng Socket:

- Server thuyết minh một đối tượng `ServerSocket`, biểu thị số hiệu cổng (port) nào để xuất hiện giao tiếp.
- Server gọi phương thức `accept()` của lớp `ServerSocket`. Phương thức này đợi tới khi một Client kết nối với Server trên cổng đã cho.
- Sau khi Server đang đợi, một Client khởi tạo một đối tượng Socket, xác định tên Server và số hiệu cổng để kết nối tới.
- Constructor của lớp `Socket` cố gắng để kết nối Client tới Server và số hiệu cổng đã xác định. Nếu giao tiếp được thành lập, bây giờ Client có một đối tượng Socket có khả năng giao tiếp với Server.
- Trên Server-side, phương thức `accept()` trả về một tham chiếu tới một socket mới trên Server mà được kết nối với socket của Client.

Sau khi các kết nối được thành lập, giao tiếp có thể xảy ra bởi sử dụng I/O stream. Mỗi Socket có cả một `OutputStream` và `InputStream`. `OutputStream` của Client được kết nối với `InputStream` của Server, và `InputStream` của Client được kết nối với `OutputStream` của Server.

TCP là một giao thức giao tiếp hai chiều, vì thế dữ liệu có thể được gửi qua cả hai luồng tại cùng một thời điểm. Các lớp hữu ích sau đây cung cấp đầy đủ các phương thức để triển khai các Socket.

3.2.1 Các phương thức lớp *ServerSocket* trong Java

Lớp **java.net.ServerSocket** trong Java được sử dụng bởi các ứng dụng Server để thu nhận một cổng và nghe các yêu cầu từ Client. Lớp *ServerSocket* có 4 constructor sau:

STT	Phương thức và miêu tả
1	public ServerSocket(int port) throws IOException Cố gắng để tạo một Server Socket giới hạn với số hiệu cổng đã xác định. Một exception xuất hiện nếu cổng này thuộc phạm vi của ứng dụng khác.
2	public ServerSocket(int port, int backlog) throws IOException Tương tự như constructor trước, tham số backlog xác định có bao nhiêu Client đang vào để lưu giữ trong một hàng đợi (wait queue)
3	public ServerSocket(int port, int backlog, InetAddress address) throws IOException Tương tự như constructor trước, tham số InetAddress xác định địa chỉ IP nội bộ để kết nối tới. InetAddress này được sử dụng cho các Server mà có thể có nhiều địa chỉ IP, cho phép Server xác định địa chỉ IP nào của nó để chấp nhận yêu cầu của Client
4	public ServerSocket() throws IOException Tạo một Server Socket không giới hạn. Khi sử dụng constructor này, sử dụng phương thức bind() khi bạn đã kết nối với Server Socket

Bảng dưới liệt kê các phương thức phổ biến của lớp ServerSocket trong Java:

STT	Phương thức và miêu tả
1	public int getLocalPort() Trả về cổng mà Server Socket đang nghe trên đó. Phương thức này hữu dụng nếu bạn truyền số hiệu cổng là 0 trong một constructor và để Server tìm một cổng cho bạn
2	public Socket accept() throws IOException Đợi cho một Client đang đến. Phương thức này block tới khi một Client kết nối tới Server trên cổng đã xác định hoặc Socket là trễ (timeout), giả sử rằng giá trị time-out đã được thiết lập với phương thức setSoTimeout(). Nếu không thì, phương thức này block vô hạn
3	public void setSoTimeout(int timeout) Thiết lập giá trị timeout cho Server Socket đợi một Client trong bao lâu, trong khi phương thức accept() gọi
4	public void bind(SocketAddress host, int backlog) Nối kết Socket tới Server và cổng đã xác định trong đối tượng SocketAddress. Sử dụng phương thức này nếu bạn đã thuyết minh đối tượng ServerSocket với constructor không có tham số

Khi ServerSocket gọi phương thức accept(), phương thức này không trả về giá trị tới khi một Client kết nối. Sau khi một Client kết nối, ServerSocket tạo một Socket mới trên một cổng chưa được xác định và trả về một tham chiếu tới Socket mới này. Bây giờ, một kết nối TCP tồn tại giữa Client và Server, và giao tiếp có thể bắt đầu.

3.2.2 Các phương thức lớp Socket trong Java

Lớp **java.net.Socket** biểu diễn socket mà cả Client và Server sử dụng để kết nối với nhau. Client thu nhận một đối tượng Socket bằng việc thuyết minh nó, trong khi Server thu nhận một đối tượng Socket từ giá trị trả về của phương thức accept().

Lớp Socket có 5 constructor mà một Client sử dụng để kết nối tới một Server:

STT	Phương thức và Miêu tả
1	public Socket(String host, int port) throws UnknownHostException, IOException. Phương thức này cố gắng kết nối tới Server đã xác định tại cổng đã xác định. Nếu constructor này không ném một exception, kết nối là thành công và Client được kết nối tới Server
2	public Socket(InetAddress host, int port) throws IOException Phương thức này tương tự constructor trước, ngoại trừ host được biểu thị bởi một đối tượng InetAddress
3	public Socket(String host, int port, InetAddress localAddress, int localPort) throws IOException. Kết nối tới host và cổng đã xác định, tạo một Socket trên host nội bộ tại địa chỉ và cổng đã xác định
4	public Socket(InetAddress host, int port, InetAddress localAddress, int localPort) throws IOException. Phương thức này tương tự constructor trước, ngoại trừ host được biểu thị bởi một đối tượng InetAddress thay vì một String
5	public Socket() Tạo một Socket rời rạc. Sử dụng phương thức connect() để kết nối Socket này tới một Server

Khi Socket constructor trả về giá trị, nó không đơn giản chỉ khởi tạo một đối tượng Socket mà nó còn thực sự cố gắng kết nối tới Server và cổng đã xác định. Một số phương thức của lớp Socket đáng quan tâm được liệt kê dưới đây. Chú ý rằng, cả Server và Client đều có một đối tượng Socket, vì thế những phương thức này có thể được gọi bởi cả Client và Server.

STT	Phương thức và Miêu tả
1	public void connect(SocketAddress host, int timeout) throws IOException Phương thức này kết nối Socket tới host đã xác định. Phương thức này chỉ cần thiết khi bạn đã thuyết minh Socket bởi sử dụng constructor không có tham số
2	public InetAddress getInetAddress() Phương thức này trả về địa chỉ của máy tính khác mà Socket này được kết nối tới
3	public int getPort() Trả về cổng mà Socket được kết nối trên thiết bị từ xa
4	public int getLocalPort() Trả về cổng mà Socket được kết nối trên thiết bị nội bộ
5	public SocketAddress getRemoteSocketAddress() Trả về địa chỉ của Socket từ xa
6	public InputStream getInputStream() throws IOException Trả về input stream của Socket. Input stream được kết nối tới output stream của Socket từ xa
7	public OutputStream getOutputStream() throws IOException Trả về output stream của Socket. Output stream được kết nối tới input stream của Socket từ xa

3.2.3 Các phương thức lớp *InetAddress* trong Java

Lớp này biểu diễn một địa chỉ Internet Protocol (IP). Dưới đây liệt kê một số phương thức hữu ích mà bạn sẽ cần trong khi lập trình Socket.

STT	Phương thức và Miêu tả
1	static InetAddress getByAddress(byte[] addr) Trả về một đối tượng InetAddress đã cung cấp địa chỉ IP thô
2	static InetAddress getByAddress(String host, byte[] addr) Tạo một InetAddress dựa trên tên host và địa chỉ IP đã cung cấp

3	static InetAddress getByName(String host) Xác định địa chỉ IP của một host, đã cung cấp tên host
4	String getHostAddress() Trả về chuỗi địa chỉ IP dạng biểu diễn nguyên văn
5	String getHostName() Nhận tên host cho địa chỉ IP này
6	static InetAddress InetAddress getLocalHost() Trả về host nội bộ
7	String toString() Biến đổi địa chỉ IP này thành một String

3.3. Kết luận

Như vậy trong chương này đã trình bày đầy đủ về lập trình socket trong java, đi sâu nghiên cứu các tính chất, khái niệm về socket, socket trong java và một số lớp trong lập trình java socket. Để từ đó làm cơ sở cho việc cài đặt triển khai phần mềm truyền thông đa phương tiện ở các chương tiếp theo.

CHƯƠNG 4. CHỮ KÝ ĐIỆN TỬ

Chương này trình bày về chữ ký điện tử, đây là một dạng dữ liệu đa phương tiện rất cần thiết trong thời buổi phát triển như hiện nay. Trong chương này, chúng ta đi sâu nghiên cứu về phương pháp tạo và giải mã chữ ký điện tử, thay cho việc ký tay truyền thống.

4.1 Tổng quan về chữ ký điện tử

4.1.1 Một số khái niệm quan trọng

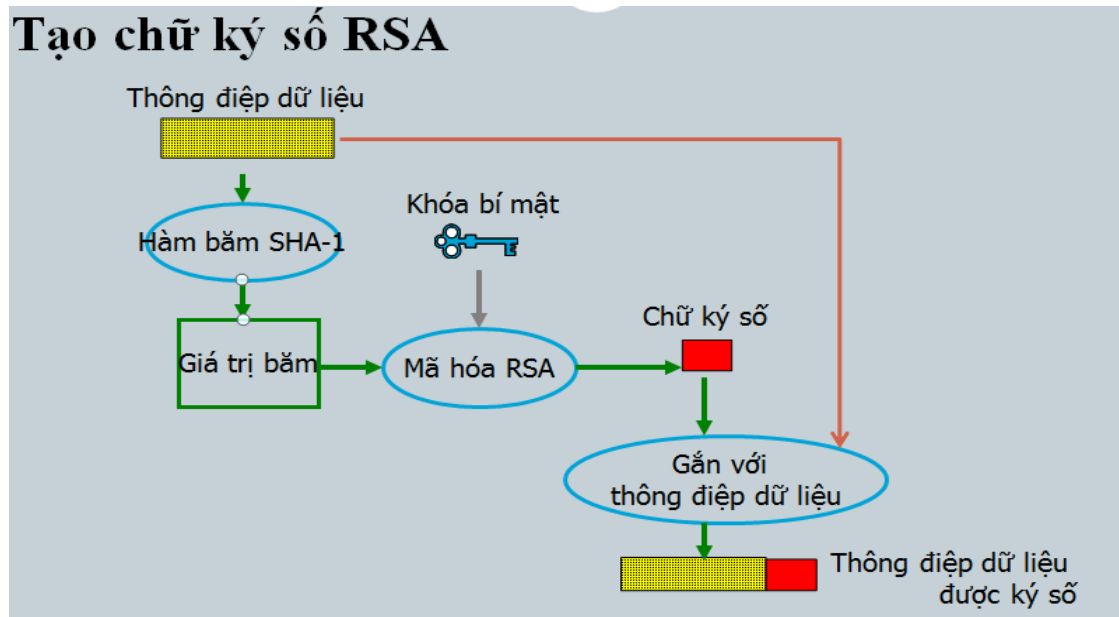
- Chữ kí số (Digital Signature) là một chuỗi dữ liệu liên kết với một thông điệp (message) và thực thể tạo ra thông điệp.
- Giải thuật tạo ra chữ ký số (Digital Signature generation algorithm) là một phương pháp sinh chữ ký số.
- Giải thuật kiểm tra chữ ký số (Digital Signature verification algorithm) là một phương pháp xác minh tính xác thực của chữ ký số, có nghĩa là nó thực sự được tạo ra bởi 1 bên chỉ định.
- Một hệ chữ ký số (Digital Signature Scheme) bao gồm giải thuật tạo chữ số và giải thuật kiểm tra chữ ký số.
- Quá trình tạo chữ ký số (Digital Signature signing process) bao gồm:
 - Giải thuật tạo chữ ký số.
 - Phương pháp chuyển dữ liệu thông điệp thành dạng có thể ký được
- Quá trình kiểm tra chữ ký số (Digital signature verification process) bao gồm:
 - Giải thuật kiểm tra chữ ký số
 - Phương pháp khôi phục dữ liệu từ thông điệp
- Lược đồ chữ ký số RSA.

Trong phần này mô tả lược đồ chữ ký RSA. Độ an toàn của lược đồ chữ ký RSA dựa vào độ an toàn của hệ mã RSA. Lược đồ bao gồm cả chữ ký số kèm theo bản rõ và tự khôi phục thông điệp từ chữ ký số.

- Thuật toán sinh khóa cho lược đồ chữ ký RSA
- Thuật toán sinh chữ ký RSA
- Thuật toán chứng thực chữ ký RSA

4.1.2. Mô hình chữ ký điện tử RSA

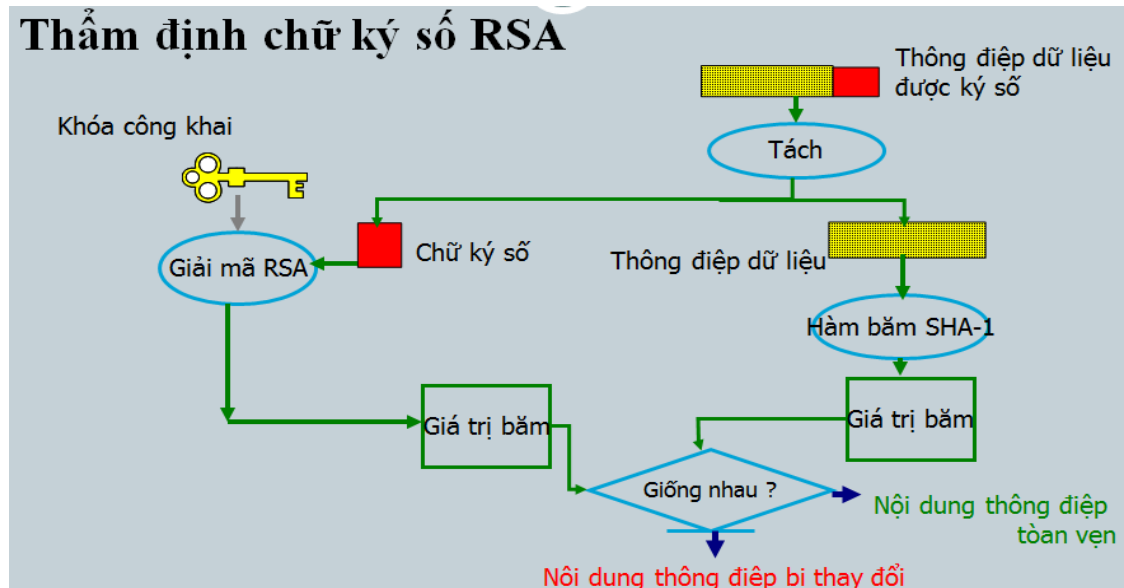
- Bên gửi



Hình 4.1 Tạo chữ ký điện tử^[13]

- Tính toán chuỗi đại diện (message digest/ hash value) của thông điệp sử dụng một giải thuật băm (Hashing algorithm) SHA-1
- Chuỗi đại diện được ký sử dụng khóa riêng (Private key) của người gửi và giải thuật tạo chữ ký (Signature/ Encryption algorithm) RSA. Kết quả chữ ký số (Digital signature) của thông điệp hay còn gọi là chuỗi đại diện được mã hóa bởi giải thuật RSA (Encrypted message digest)
- Thông điệp ban đầu (message) được ghép với chữ ký số (Digital signature) tạo thành thông điệp đã được ký (Signed message)
- Thông điệp đã được ký (Signed message) được gửi cho người nhận

- Bên nhận



Hình 4.2 Thẩm định chữ ký điện tử^[13]

- Tách chữ ký số RSA và thông điệp gốc khỏi thông điệp đã ký để xử lý riêng
- Tính toán chuỗi đại diện MD1 (message digest) của thông điệp gốc sử dụng giải thuật băm (là giải thuật sử dụng trong quá trình ký là SHA-1)
- Sử dụng khóa công khai (Public key) của người gửi để giải mã chữ ký số RSA- > chuỗi đại diện thông điệp MD2
- So sánh MD1 và MD2:
 - + Nếu MD1 = MD2 -> chữ ký kiểm tra thành công. Thông điệp đảm bảo tính toàn vẹn và thực sự xuất phát từ người gửi (do khóa công khai được chứng thực).
 - + Nếu MD1 <> MD2 -> chữ ký không hợp lệ. Thông điệp có thể đã bị sửa đổi hoặc không thực sự xuất phát từ người gửi.

4.2 Hàm băm SHA-1

4.2.1 Tổng quan về hàm băm

Hàm băm (Hash Function) là hàm toán học chuyển đổi thông điệp (message) có độ dài bất kỳ (hữu hạn) thành một dãy bit có độ dài cố định (tùy thuộc vào thuật toán băm). Dãy bit này được gọi là thông điệp rút gọn (message digest) hay giá trị băm (hash value), đại diện cho thông điệp ban đầu.

Chỉ tới khi đụng vào hàm băm mật mã, thuật ngữ “băm” mới cho thấy ý nghĩa đầy đủ. Một ứng dụng của hàm băm mật mã là băm mật khẩu, lưu trữ mã băm sẽ an toàn hơn lưu trữ nguyên mật khẩu gốc dạng văn bản rõ (cleartext). Mã băm phải đảm bảo, từ mã băm rất khó để tìm ra được mật khẩu gốc. Muốn vậy thì hàm băm mật mã phải thực hiện băm thật kỹ, băm đi băm lại dữ liệu theo cách thức sao cho mã băm đầu ra, hiểu đơn giản là không còn dấu vết của dữ liệu đầu vào. Thực tế mật khẩu còn thường được cho thêm muối trước khi băm.

Để dữ liệu đầu vào có thể được cắt ra thành những khúc có kích thước nhất định trước khi băm, thuật toán băm thực hiện nhồi thêm các bits vào dữ liệu gốc, giống như chúng ta độn thêm bột hay phụ gia vào thực phẩm vậy. Ví dụ đối với hàm băm sử dụng khúc dữ liệu cỡ 512 bits, dữ liệu đầu vào (thông điệp) được gắn thêm bit 1, sau đó không thêm hoặc thêm một số bit 0 sao cho tổng chiều dài dữ liệu chia cho 512 dư 448. Cuối cùng thêm 64 bits biểu diễn chiều dài thông điệp. Chiều dài tổng thể của dữ liệu như thế là bội của 512 và dữ liệu bao gồm các khúc 512 bits.

Quá trình băm thực hiện trên từng khúc dữ liệu, mỗi khúc được băm một số vòng (số vòng lặp đang sử dụng hiện nay là 64 vòng hoặc 80 vòng). Thuật toán duy trì các biến tương ứng với các từ của mã băm, mỗi từ 32 bits hoặc 64 bits, và mỗi vòng thực hiện tính toán các biến trên cơ sở khúc dữ liệu và các thao tác khác. Khúc dữ liệu, tùy theo loại hàm băm có thể được sơ chế hoặc không, được chia thành các mảnh nhỏ cỡ 32 bits hoặc 64 bits và được “trộn” dần vào các vòng băm. Trong mỗi vòng băm, “gia vị” được bổ sung là hằng số, đối với đa số hàm băm hằng số được lấy từ một hay hai mảng cho

trước, trong đó có mảng các giá trị của một hàm phi tuyến hoặc mảng của các số nguyên tố đầu tiên. Dữ liệu được “băm” sử dụng kết hợp các phép toán trên bit. Cuối một vòng, thuật toán thực hiện “nháo” dữ liệu bằng cách gán một số biến đầu ra bằng với một số biến đầu vào nhưng hoán vị. Các biến với giá trị mới lại trở thành biến đầu vào cho vòng tiếp theo. Chúng ta thấy rằng dữ liệu được băm là dữ liệu hỗn hợp, nhưng mô tả rõ hơn thì, thuật toán thực hiện băm các biến trong khi thả mảnh dữ liệu và gia vị vào, rồi nháo các biến, tính toán, khởi tạo các biến cho vòng sau, rồi lại băm tiếp. Khi kết thúc tất cả các vòng băm của một khúc, khúc dữ liệu coi như được nén vào các biến.

Việc tính toán được bắt đầu với một giá trị hash khởi tạo, coi như mã băm hiện hành của khúc dữ liệu đầu tiên. Ở đầu chu kỳ của một khúc, các biến được gán với các từ tương ứng của mã băm hiện hành. Sau khi đi qua hết các vòng băm, các biến kết quả được cộng tương ứng vào các từ của mã băm hiện hành để tạo ra mã băm mới. Quá trình băm thực hiện băm đi băm lại trên từng khúc dữ liệu, mã băm mới của chu kỳ này được dùng làm mã băm hiện hành của chu kỳ tiếp theo, cho tới khúc cuối cùng. Giá trị nối các từ của mã băm sau cùng là mã kết quả của hàm băm.

Hàm băm mật mã ứng dụng nhiều trong an ninh thông tin, điển hình là kiểm tra tính toàn vẹn của dữ liệu, mã hóa mật khẩu, xác minh tệp tin, chứng thực thông điệp, chữ ký kỹ thuật số, và các dạng ứng dụng hệ quả khác mà chứa hàm băm mật mã bên trong. Hàm băm mật mã còn được sử dụng như hàm băm thường, phục vụ cho bảng băm như chúng ta đã biết. Vì mã băm của một đối tượng là duy nhất, nó có thể được dùng như dấu vân tay để nhận dạng đối tượng. Ví dụ để chỉ ra một người sử dụng, cách tốt nhất là sử dụng dấu vân tay là mã băm mật mã dành cho người đó, trong khi mã nhận dạng kiểu khác có thể không rõ ràng và bị trùng lặp.

Hàm băm mật mã phải có khả năng chống cự các loại tấn công mật mã, tối thiểu phải đảm bảo có 3 tính chất sau:

- Kháng tiền ảnh (Pre-image resistance): Với một mã băm h bất kỳ, khó tìm được một thông điệp m nào mà $h = \text{hash}(m)$. Điều này làm chúng ta liên tưởng tới tính

một chiều của hàm số. Trong góc độ hàm số toán học, mã băm là ảnh còn thông điệp là tạo ảnh của mã băm, hay gọi là tiền ảnh. Sức kháng cự tấn công từ ảnh ngược về tiền ảnh gọi là kháng tiền ảnh. Một hàm băm có kháng tiền ảnh yếu là lỗ hổng cho các cuộc tấn công tiền ảnh.

- Kháng tiền ảnh thứ hai (Second pre-image resistance): Với một thông điệp m_1 bất kỳ, khó tìm được một thông điệp thứ hai m_2 sao cho $m_1 \neq m_2$ và $\text{hash}(m_1) = \text{hash}(m_2)$. Xác suất xảy ra biến cố có thông điệp m_2 như thế tương tự biến cố “Cùng ngày sinh như bạn”. Một hàm băm có kháng tiền ảnh thứ hai yếu là lỗ hổng cho các cuộc tấn công tiền ảnh thứ hai.
- Kháng xung đột (Collision resistance): Khó tìm được một cặp thông điệp m_1 và m_2 sao cho $m_1 \neq m_2$ và $\text{hash}(m_1) = \text{hash}(m_2)$. Cặp như thế được gọi là xung đột băm mật mã. Tính chất này đôi khi còn được gọi là kháng xung đột mạnh. Nó yêu cầu chiều dài băm ít nhất phải dài hơn hai lần so với yêu cầu của kháng tiền ảnh, nếu không xung đột có thể xảy ra bởi một cuộc tấn công Ngày sinh.

4.2.2 Hàm băm SHA-1

- Hàm băm SHA-1: Thuật toán SHA-1 nhận thông điệp ở đầu vào có chiều dài $k < 2^{64}$ bit, thực hiện xử lý và đưa ra thông điệp thu gọn (message digest) có chiều dài cố định 160 bits. Quá trình tính toán cũng thực hiện theo từng khối 512bits, nhưng bộ đệm xử lý dùng 5 thanh ghi 32-bits. Thuật toán này chạy tốt với các bộ vi xử lý có cấu trúc 32 bits.
- SHA-1 là 1 phần trong các ứng dụng bảo mật được sử dụng rộng rãi trong các giao thức như: TLS và SSL, PGP, SSH và IPSEC..
- Các SHA-1 có thể được sử dụng với các DSA trong thư điện tử, chuyển tiền điện tử, phân phối phần mềm, lưu trữ dữ liệu, và các ứng dụng khác cần đảm bảo tính toàn vẹn DL và xác thực nguồn gốc DL. Các SHA-1 cũng có thể sử dụng bất cứ khi nào nó là cần thiết để tạo ra 1 phiên bản đặc của tin nhắn
- Hàm SHA-1 còn được sử dụng trên Wii của Nintendo để xác minh chữ ký thời gian khởi động

- SHA-1 và SHA-2 là những thuật toán băm an toàn theo yêu cầu của pháp luật để sử dụng trong một số ứng dụng của Chính Phủ Hoa Kỳ, bao gồm cả sử dụng trong các thuật toán mã hóa khác và các giao thức, để bảo vệ thông tin mật nhạy cảm. Nhưng hiện nay thì Chính Phủ không còn sử dụng SHA-1 nữa nhưng thay vào đó là SHA-2
- Các hàm băm SHA được dùng làm cơ sở cho mã khối SHACAL.
- Nếu không có sự giới hạn về bộ nhớ: có thể xây dựng bảng băm với mỗi khóa ứng với một địa chỉ với mong muốn thời gian truy xuất tức thời.
- Nếu dung lượng bộ nhớ có giới hạn: tổ chức một số khóa có cùng địa chỉ, tốc độ truy xuất giảm.
- Các phép toán trên bảng băm hạn chế số lần so sánh, giảm được thời gian truy xuất.

4.2.3 Cài đặt thuật toán băm SHA-1

- Đầu vào: thông điệp với độ dài tối đa 264 bits
- Đầu ra: giá băm (message digest) có độ dài 160 bits
- Giải thuật gồm 5 bước thao tác trên các khối 512 bits
- **Nhồi dữ liệu:**
 - Thông điệp được nhồi thêm các bit sao cho độ dài $L \bmod 512$ luôn đồng dư là 448.
 - Thông điệp luôn luôn được nhồi thêm các bit.
 - Số bit nhồi thêm phải nằm trong khoảng [1-512].
 - Phần thêm vào cuối dữ liệu gồm 1 bit 1 và theo sau là các bit 0.
- **Thêm độ dài**
 - Độ dài của khối dữ liệu ban đầu sẽ được biểu diễn dưới dạng nhị phân 64 bit và được thêm vào cuối chuỗi nhị phân mà ta thu được của bước 1.
 - Độ dài được biểu diễn dưới dạng nhị phân 64 bit không dấu.

- Kết quả thu được từ 2 bước là 1 khối dữ liệu có độ dài là bội số của 512.(với cứ 512 bit là 1 khối dữ liệu)

- **Khởi tạo bộ đệm MD (MD Buffer)**

Một bộ đệm 160-bit được dùng lưu trữ các giá trị băm trung gian và kết quả. Bộ đệm được biểu diễn bằng 5 thanh ghi 32-bit với các giá trị khởi tạo ở dạng big-endian (byte có trọng số lớn nhất trong từ nằm ở địa chỉ thấp nhất) và có 2 bộ đệm. 5 thanh ghi của bộ đệm đầu tiên được đánh đặt tên là A,B,C,D,E và tương tự cho bộ đệm thứ 2 là H₀,H₁,H₂,H₃,H₄. Có giá trị như sau (theo dạng Hex):

H₀=67452301

H₁=EFCDAB89

H₂=98BADCFE

H₃=10325476

H₄=C3D2E1F0

- **Xử lý các khối dữ liệu 512 bit**

- Trọng tâm của giải thuật bao gồm 4 vòng lặp thực hiện tất cả 80 bước.
- 4 vòng lặp có cấu trúc như nhau, chỉ khác nhau ở các hàm logic f_t.

Bước	Hàm	Giá trị
(0 ≤ t ≤ 19)	f _t = f(B,C,D)	(B AND C) OR ((NOT B) AND D)
(20 ≤ t ≤ 39)	f _t = f(B,C,D)	B XOR C XOR D
(40 ≤ t ≤ 59)	f _t = f(B,C,D)	(B AND C) OR (B AND D) OR (C AND D)
(60 ≤ t ≤ 79)	f _t = f(B,C,D)	B XOR C XOR D

- Mỗi vòng có đầu vào gồm khối 512-bit hiện thời và một bộ đệm 160-bit A,B,C,D,E. Các thao tác sẽ cập nhật giá trị bộ đệm .

- Chia khối dữ liệu đã nhồi thêm (cuối bước 2) thành 16 nhóm (mỗi nhóm gồm 32 bit) và đặt theo thứ tự là: W_0, W_1, \dots, W_{15} .

- Mở rộng từ 16 nhóm 32 bit lên 80 nhóm 32 bit bằng vòng lặp:

For $t = 16$ to 79 let

$$W_t = S^1(W_{t-3} \text{ XOR } W_{t-8} \text{ XOR } W_{t-14} \text{ XOR } W_{t-16}).$$

- Gán $A = H_0, B = H_1, C = H_2, D = H_3, E = H_4$.

- Mỗi vòng lặp sử dụng theo công thức chung với một hằng số K_t ($0 \leq t \leq 79$) như sau:

For $t = 0$ to 79 do

$$\text{TEMP} = S^5(A) + f_t(B, C, D) + E + W_t + K_t;$$

$$E = D; D = C; C = S^{30}(B); B = A; A = \text{TEMP};$$

Với:

$$K_t = 5A827999 \quad (0 \leq t \leq 19)$$

$$K_t = 6ED9EBA1 \quad (20 \leq t \leq 39)$$

$$K_t = 8F1BBCDC \quad (40 \leq t \leq 59)$$

$$K_t = CA62C1D6 \quad (60 \leq t \leq 79)$$

- Đầu ra của 4 vòng (bước 80) được cộng với giá trị của bộ đệm để tạo ra 1 chuỗi kết quả dài 160 bit.

$$H_0 = H_0 + A$$

$$H_1 = H_1 + B$$

$$H_2 = H_2 + C$$

$$H_3 = H_3 + D$$

$$H_4 = H_4 + E.$$

• Xuất kết quả

Sau khi thao tác trên toàn bộ N khối dữ liệu (blocks). Kết quả của khối thứ N là chuỗi băm 160-bit: $H = H_0 \parallel H_1 \parallel H_2 \parallel H_3 \parallel H_4$

4.3 Thuật toán RSA

4.3.1 Khái niệm

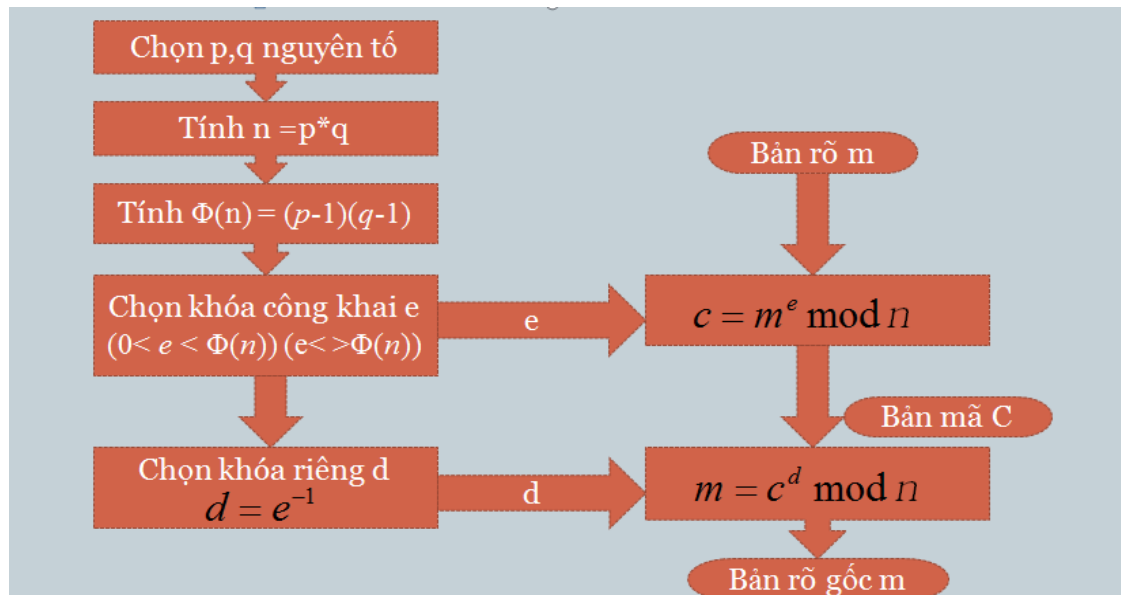
Trong mật mã học, RSA là một thuật toán mật mã hóa khóa công khai. Đây là thuật toán đầu tiên phù hợp với việc tạo ra chữ ký điện tử đồng thời với việc mã hóa. Nó đánh dấu một sự tiến bộ vượt bậc của lĩnh vực mật mã học trong việc sử dụng khóa công cộng. RSA đang được sử dụng phổ biến trong thương mại điện tử và được cho là đảm bảo an toàn với điều kiện độ dài khóa đủ lớn.

Thuật toán RSA có hai khóa: khóa công khai (hay khóa công cộng) và khóa bí mật (hay khóa cá nhân). Mỗi khóa là những số cố định sử dụng trong quá trình mã hóa và giải mã. Khóa công khai được công bố rộng rãi cho mọi người và được dùng để mã hóa. Những thông tin được mã hóa bằng khóa công khai chỉ có thể được giải mã bằng khóa bí mật tương ứng. Nói cách khác, mọi người đều có thể mã hóa nhưng chỉ có người biết khóa cá nhân (bí mật) mới có thể giải mã được.

Ta có thể mô phỏng trực quan một hệ mật mã khoá công khai như sau: Bob muốn gửi cho Alice một thông tin mật mà Bob muốn duy nhất Alice có thể đọc được. Để làm được điều này, Alice gửi cho Bob một chiếc hộp có khóa đã mở sẵn và giữ lại chìa khóa. Bob nhận chiếc hộp, cho vào đó một tờ giấy viết thư bình thường và khóa lại (như loại khoá thông thường chỉ cần sập chốt lại, sau khi sập chốt khóa ngay cả Bob cũng không thể mở lại được-không đọc lại hay sửa thông tin trong thư được nữa). Sau đó Bob gửi chiếc hộp lại cho Alice. Alice mở hộp với chìa khóa của mình và đọc thông tin trong thư. Trong ví dụ này, chiếc hộp với khóa mở đóng vai trò khóa công khai, chiếc chìa khóa chính là khóa bí mật.

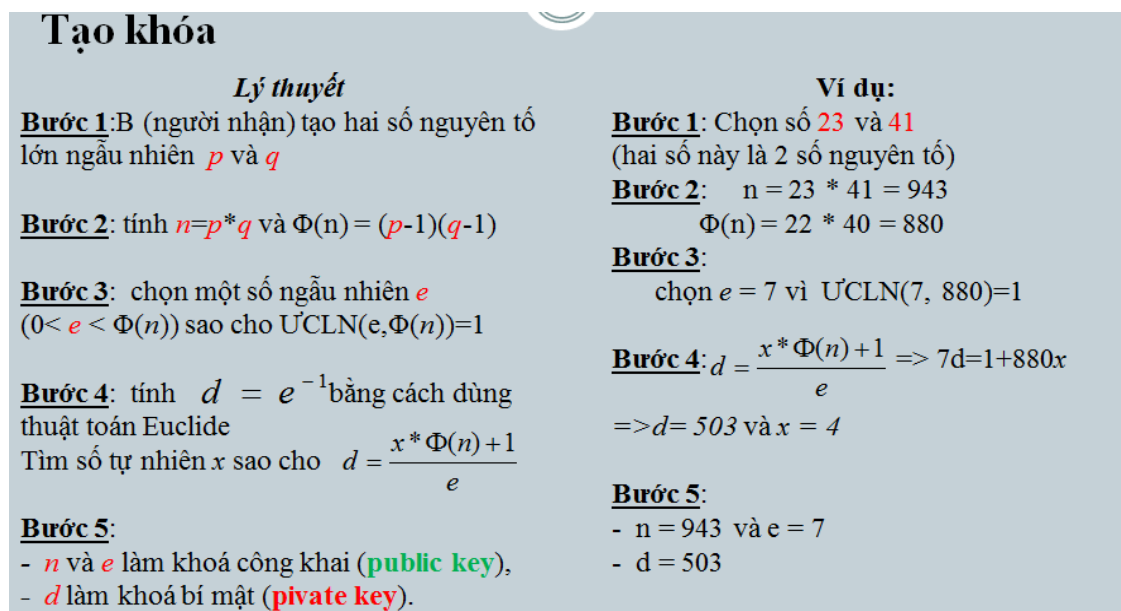
4.3.2 Sơ đồ thuật toán

- Sơ đồ tổng quát



Hình 4.3 Sơ đồ tổng quát thuật toán RSA ^[13]

- Sơ đồ tạo khóa



Hình 4.4 Sơ đồ tạo khóa ^[13]

- Sơ đồ mã hóa và giải mã

Mã hoá và giải mã	
<i>Lý thuyết</i>	Ví dụ:
Bước 1: A nhận khoá công khai của B.	Bước 1: A nhận khoá công khai $n = 943$ và $e = 7$
Bước 2: A biểu diễn thông tin cần gửi thành số m ($0 \leq m \leq n-1$)	Bước 2: Thông tin cần gửi $m = 35$
Bước 3: Tính $c = m^e \bmod n$	Bước 3: $c = 35^7 \bmod 943$
Bước 4: Gửi c cho B	Bước 4: $c = 545$
Bước 5: Giải mã tính $m = c^d \bmod n$ $\Rightarrow m$ là thông tin nhận được.	Bước 5: Giải mã $m = 545^{503} \bmod 943$ $\Rightarrow m = 35$

Hình 4.5 Sơ đồ mã hóa và giải mã ^[13]

4.4 Kết luận

Sự xuất hiện của chữ ký số và chức năng tiền định của nó, đặc biệt là vai trò của nó như là một công cụ trong việc xác định tính nguyên gốc, xác định tác giả, bảo đảm tính toàn vẹn của tài liệu số, đã đóng một vai trò vô cùng quan trọng trong việc xác định địa vị pháp lý của tài liệu số trong giao dịch số. Việc sử dụng chữ ký số trong phần lớn trường hợp là cơ sở khẳng định giá trị pháp lý của những văn bản điện tử tương đương với tài liệu giấy. Hiện nay, chữ ký số là phương tiện duy nhất để xác nhận giá trị pháp lý của tài liệu điện tử.

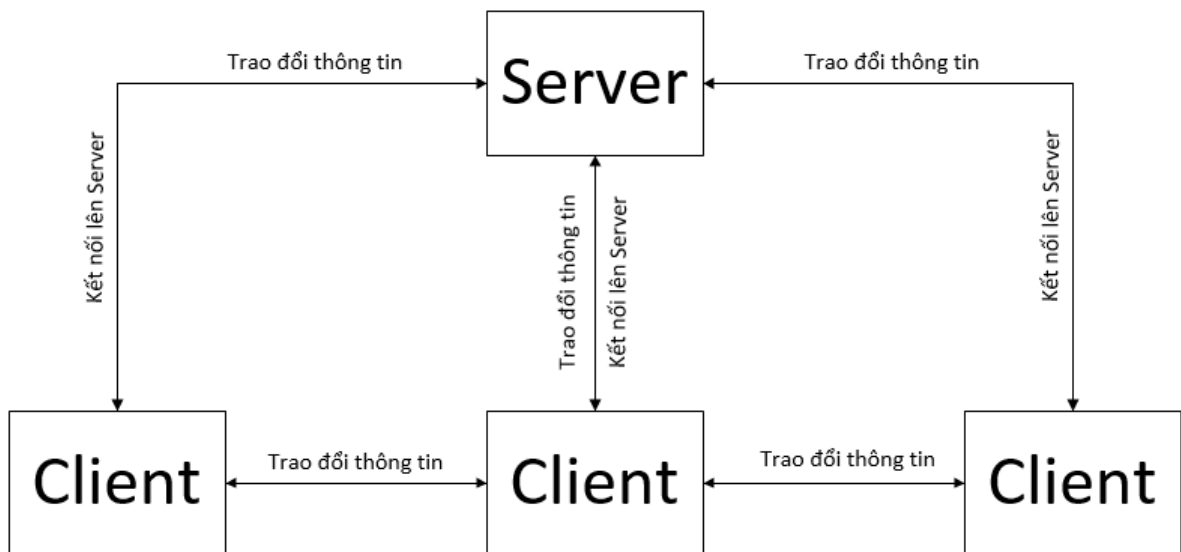
Như vậy, trong chương này đã trình bày được phương pháp tạo và kiểm tra chữ ký điện tử, từ đó cài đặt thuật toán phục vụ cho việc thiết kế phần mềm truyền thông đa phương tiện trong chương sau.

CHƯƠNG 5. THIẾT KẾ PHẦN MỀM TRUYỀN THÔNG ĐA PHƯƠNG TIỆN

Chương này sẽ đi sâu phân tích, thiết kế, triển khai hệ thống phần mềm truyền thông đa phương tiện trong mạng Lan, Wlan. Kết quả chạy chương trình, ưu điểm, nhược điểm còn tồn tại.

5.1 Sơ đồ khối tổng quát của hệ thống

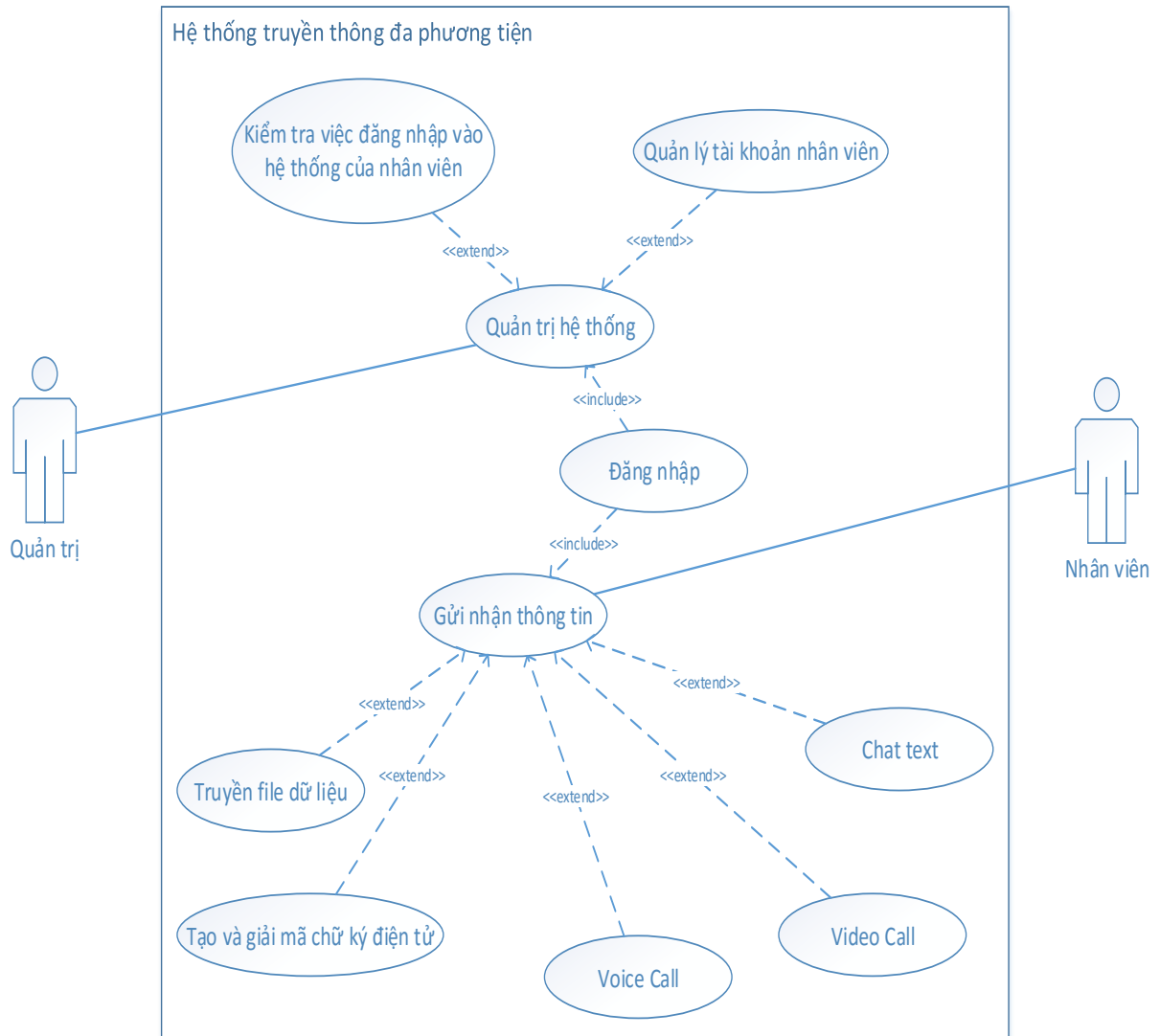
5.1.1 Sơ đồ khối



Hình 5.1 Sơ đồ khối tổng quát của hệ thống

Hệ thống có một Server kết nối cơ sở dữ liệu SqlServer, chứa thông tin tài khoản của nhân viên. Mỗi nhân viên sẽ được cấp một tài khoản đăng nhập vào hệ thống để trao đổi thông tin.

5.1.2 Đặc tả Use Case

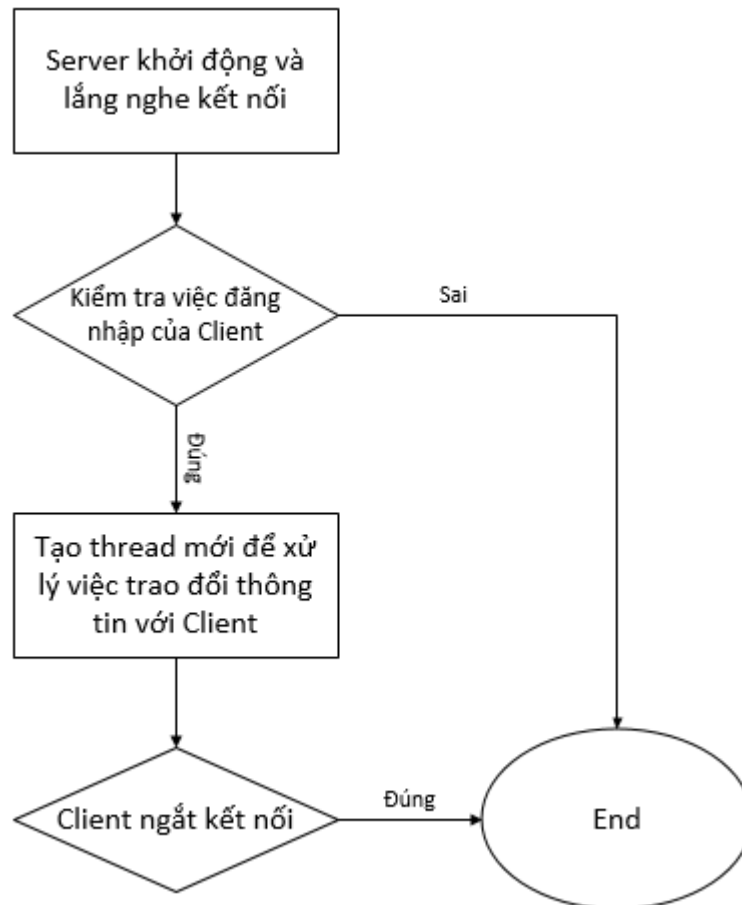


Hình 5.2 Đặc tả Use case của hệ thống

Hệ thống có hai đối tượng sử dụng đó là người quản trị và nhân viên. Người quản trị hệ thống là người khởi động Server đồng thời quản lý thông tin tài khoản của toàn bộ nhân viên, toàn bộ thông tin đó sẽ được lưu trong cơ sở dữ liệu SqlServer để phục vụ cho việc kiểm tra đăng nhập của nhân viên. Nhân viên mỗi khi muốn sử dụng hệ thống, phải đăng nhập bằng tài khoản vào mật khẩu được cấp vào hệ thống, nếu tài khoản đúng, nhân viên sẽ được chuyển đến giao diện chính của phần mềm, bao gồm các chức năng như chat text, truyền file, video call, chữ ký điện tử....

5.2 Phân tích thiết kế phía Server

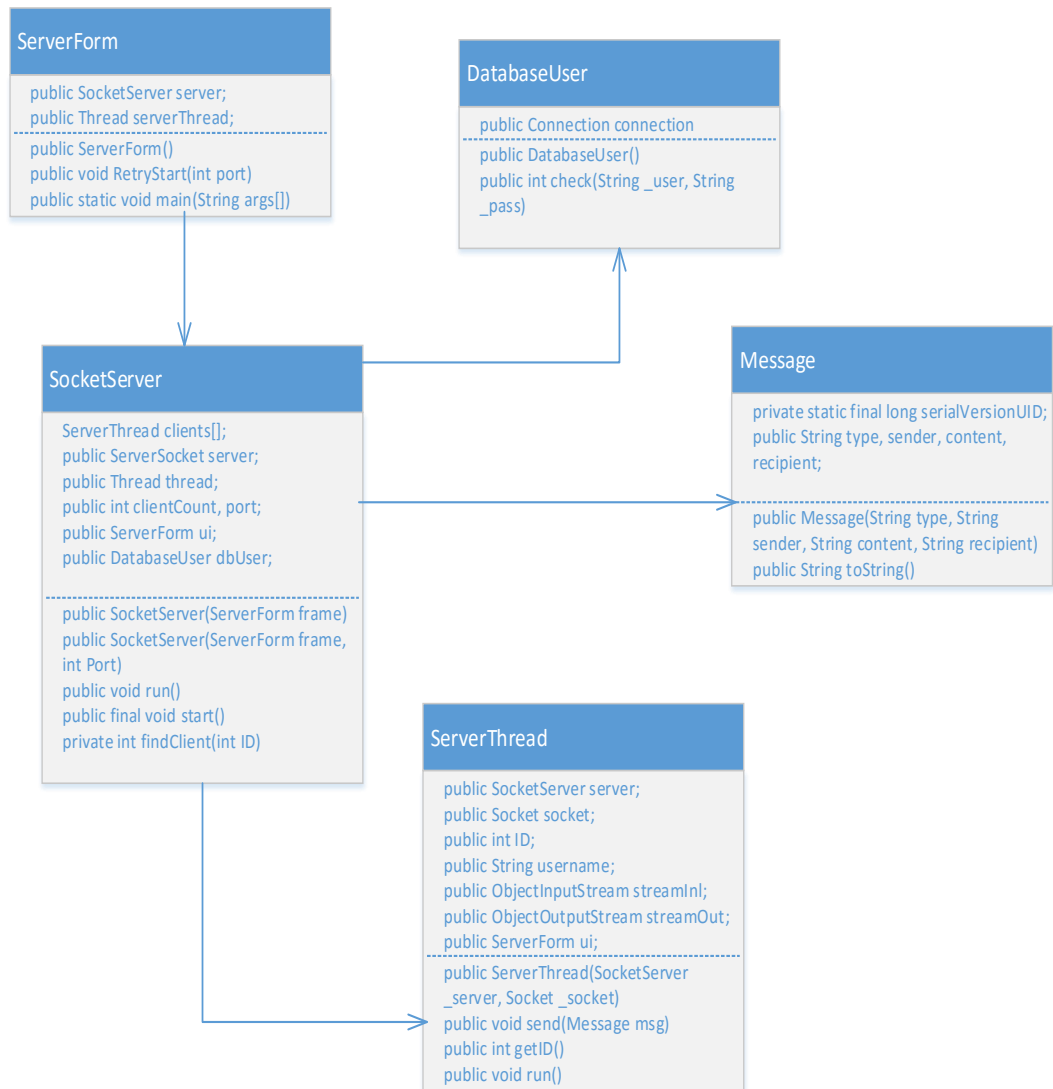
5.2.1 Sơ đồ khối phía Server



Hình 5.3 Sơ đồ khối phía Server

- Bước 1: Khởi động server và kết nối với cơ sở dữ liệu chứa thông tin nhân viên. Server có nhiệm vụ lắng nghe và chấp nhận các kết nối hợp lệ từ Client.
- Bước 2: Khi có tín hiệu kết nối từ Client, server kiểm tra xem thông tin tài khoản và mật khẩu đúng chưa, nếu đúng, server tạo ra một thread mới để tiến hành trao đổi thông tin và xử lý client đó.
- Bước 3: Nếu có tín hiệu ngắt kết nối từ client, server sẽ tiến hành ngắt kết nối và giải phóng thread phục vụ client đó.

5.2.2 Thiết kế chi tiết lớp phía Server



Hình 5.4 Biểu đồ Class phía Server

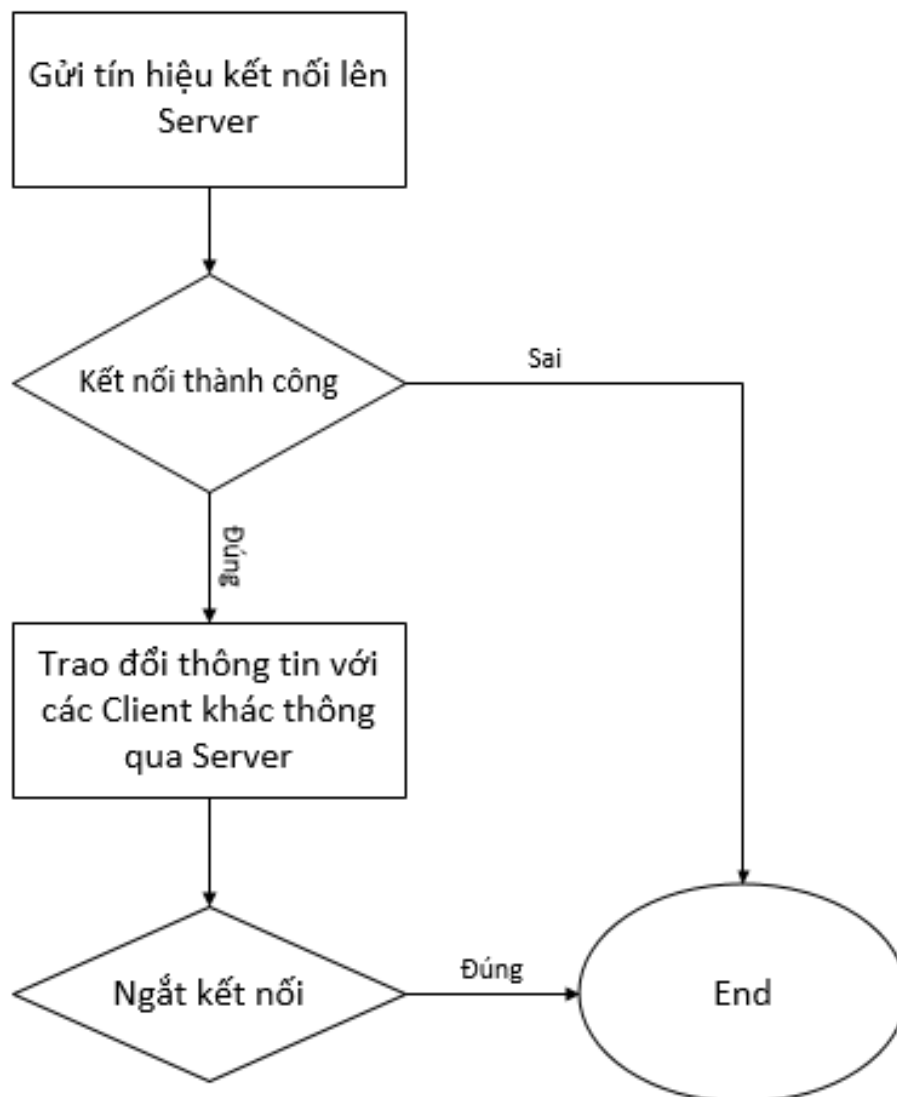
Phần cài đặt chương trình phía server sẽ gồm 5 lớp chính:

- Lớp Server form: có chức năng hiển thị giao diện chương trình, hiển thị địa chỉ IP và port của server, hiển thị danh sách và tình trạng kết nối của tất cả các client.
- Lớp Database user: thực hiện việc kết nối cơ sở dữ liệu và kiểm tra tính đúng đắn của việc đăng nhập phía client.

- Lớp Socket Server: lớp thực hiện việc lắng nghe kết nối và xử lý tất cả các Client kết nối đến.
- Lớp Server Thread: lớp này chính là tiến trình con thực hiện xử lý từng client riêng biệt
- Lớp Message: định dạng chuỗi thông điệp gửi nhận của server.

5.3 Phân tích thiết kế phía Client

5.3.1 Sơ đồ khối phía Client

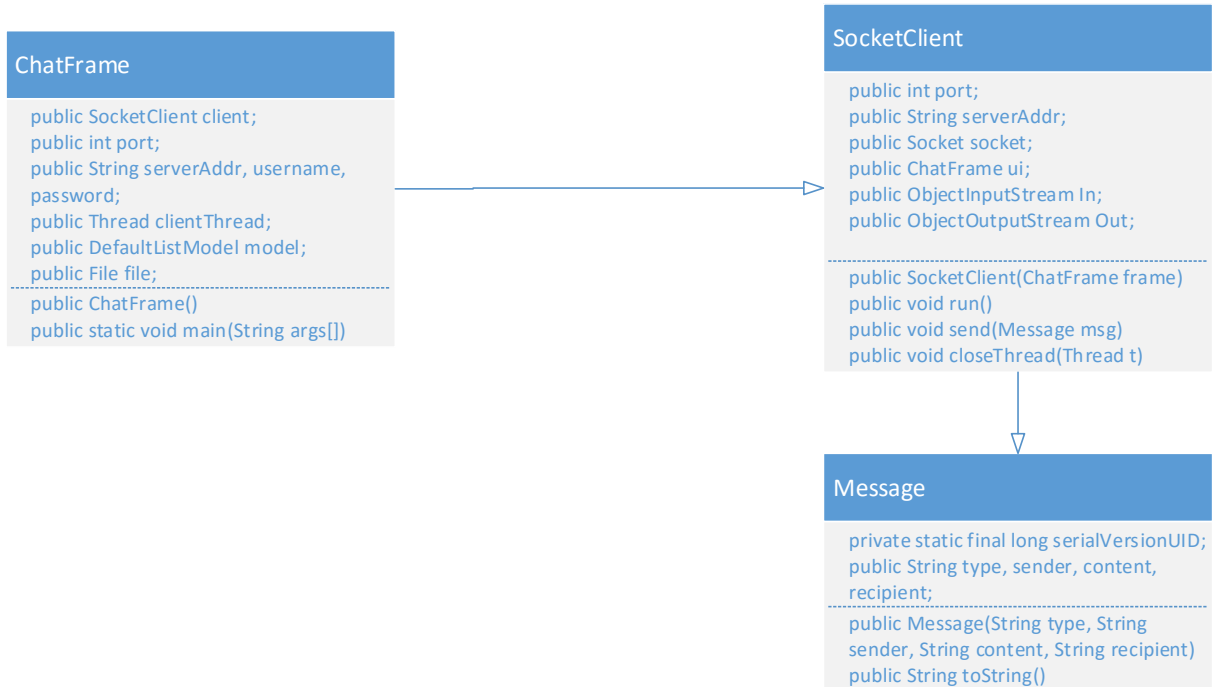


Hình 5.5 Sơ đồ khối phía Client

Trước tiên, client gửi tín hiệu kết nối lên server bằng việc đăng nhập đúng tên và tài khoản được cấp. Nếu đăng nhập đúng, client sẽ được kết nối vào hệ thống duy nhất. Tại đó, các client bắt đầu trao đổi thông tin cho nhau như chat text, video call, gửi file...

5.3.2 Thiết kế chi tiết lớp phía Client

- Main Packages

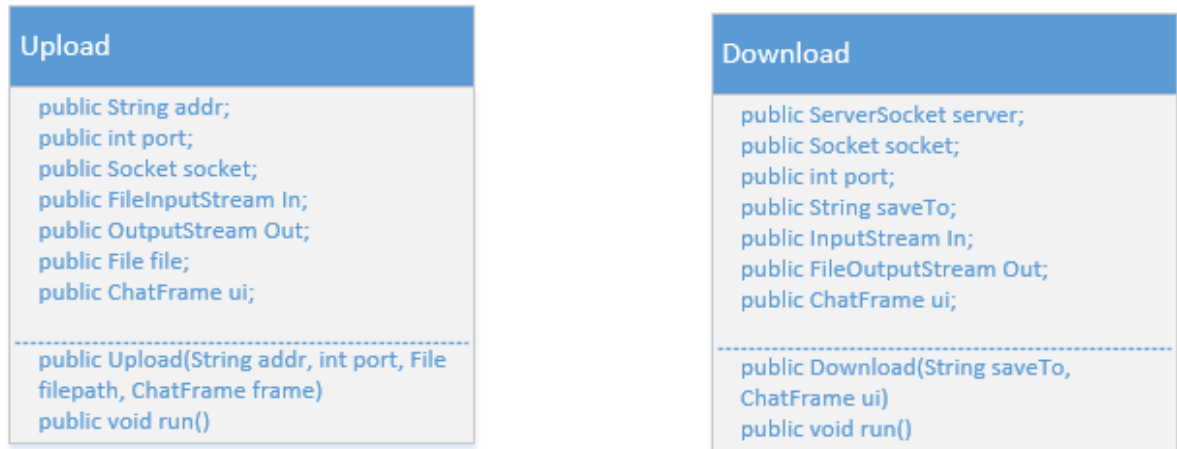


Hình 5.6 Biểu đồ Class Main Packages

Main Packages gồm có 3 lớp chính:

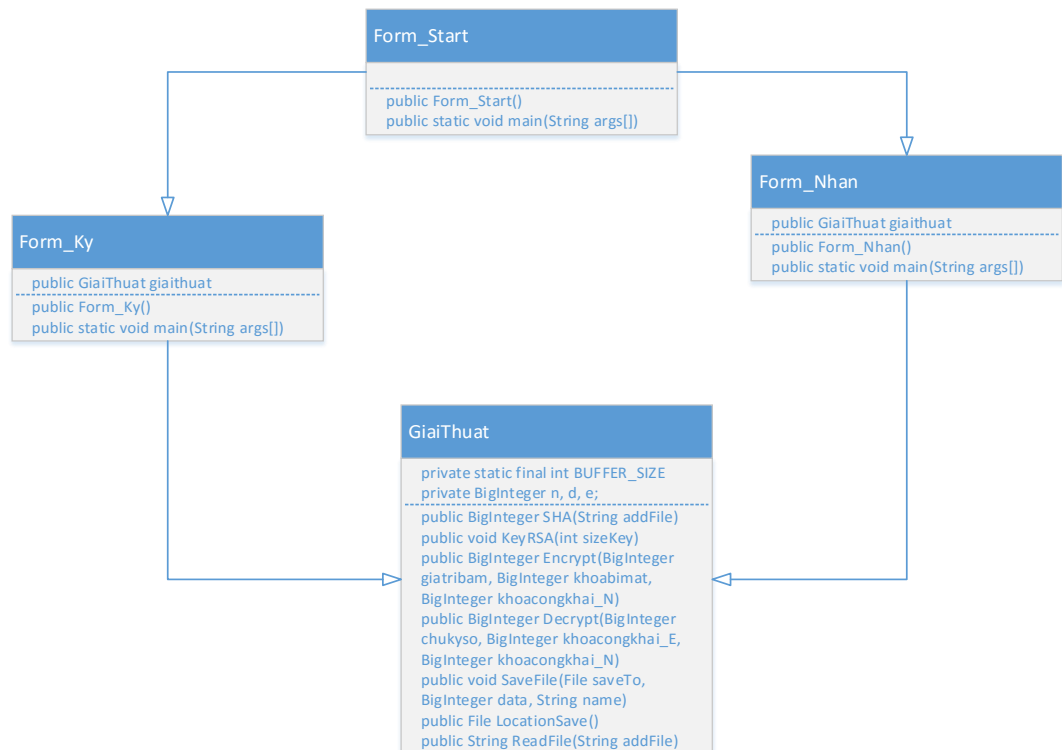
- Lớp Chat Frame: có nhiệm vụ hiển thị giao diện để người dùng thao tác.
- Lớp Message: định nghĩa khuôn dạng của thông điệp cần gửi nhận.
- Lớp Socket Client: thực hiện việc kết nối mạng lên server, trao đổi thông tin với server và các client khác.

- File Packages



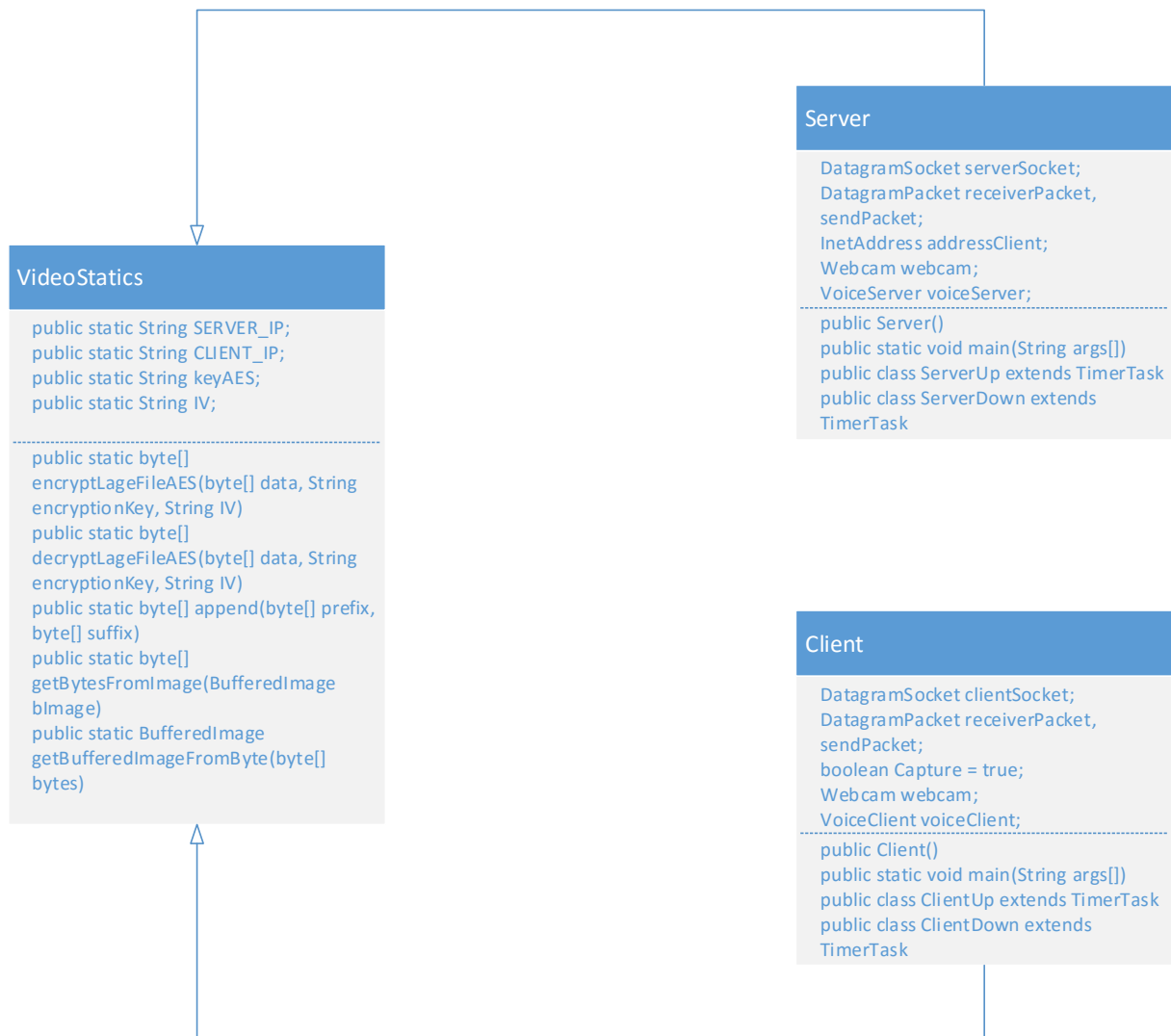
Hình 5.7 Biểu đồ Class File Packages

- RSA Packages



Hình 5.8 Biểu đồ Class RSA Packages

- Video Call Packages

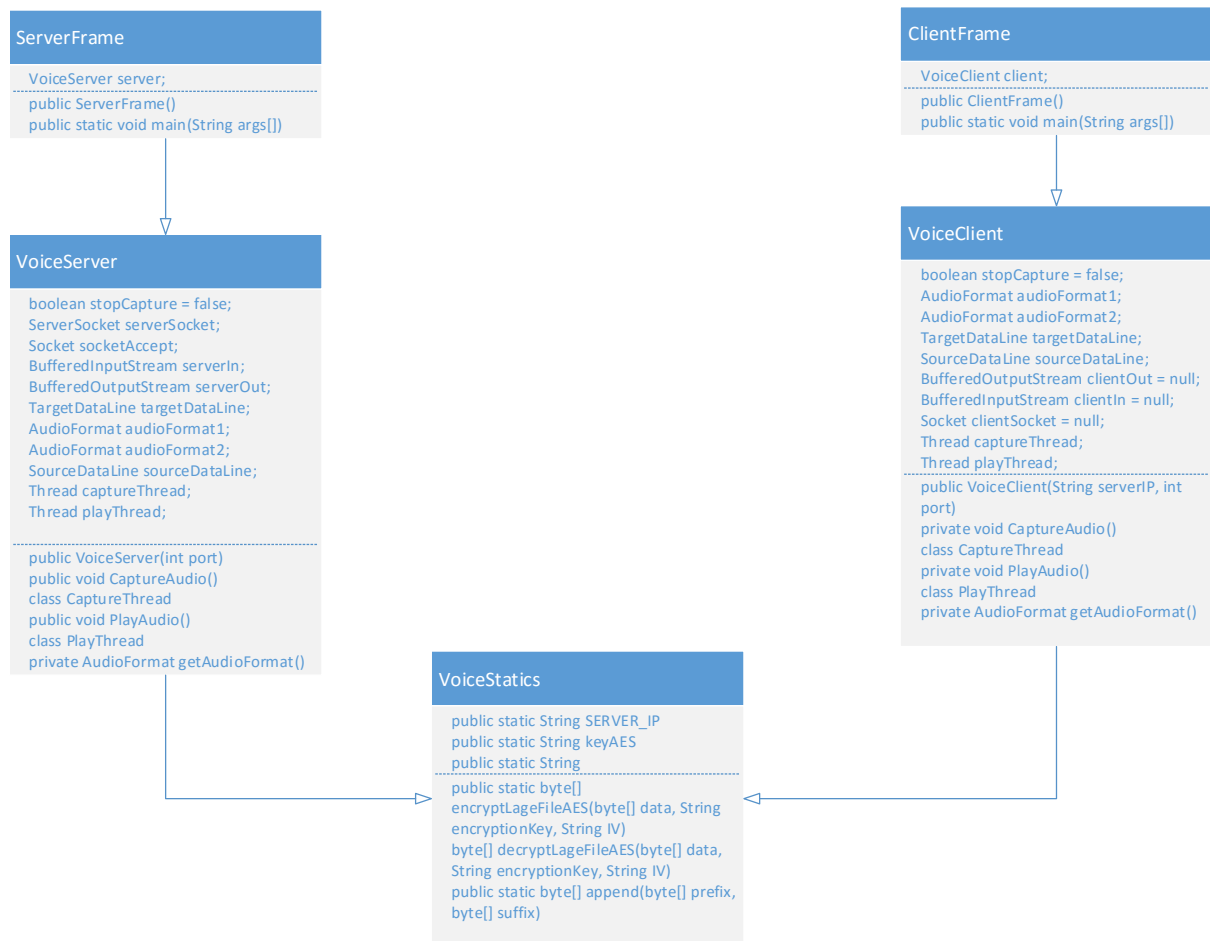


Hình 5.9 Biểu đồ class Video Call Packages

Video Call Packages gồm 3 lớp chính:

- Lớp server: thực hiện việc khởi động server để gọi video.
- Lớp Client: kết nối lên server để gửi nhận tín hiệu video.
- Lớp Video static: chứa các phương thức và thuộc tính cần thiết cho lớp server và client.

- Voice call Packages



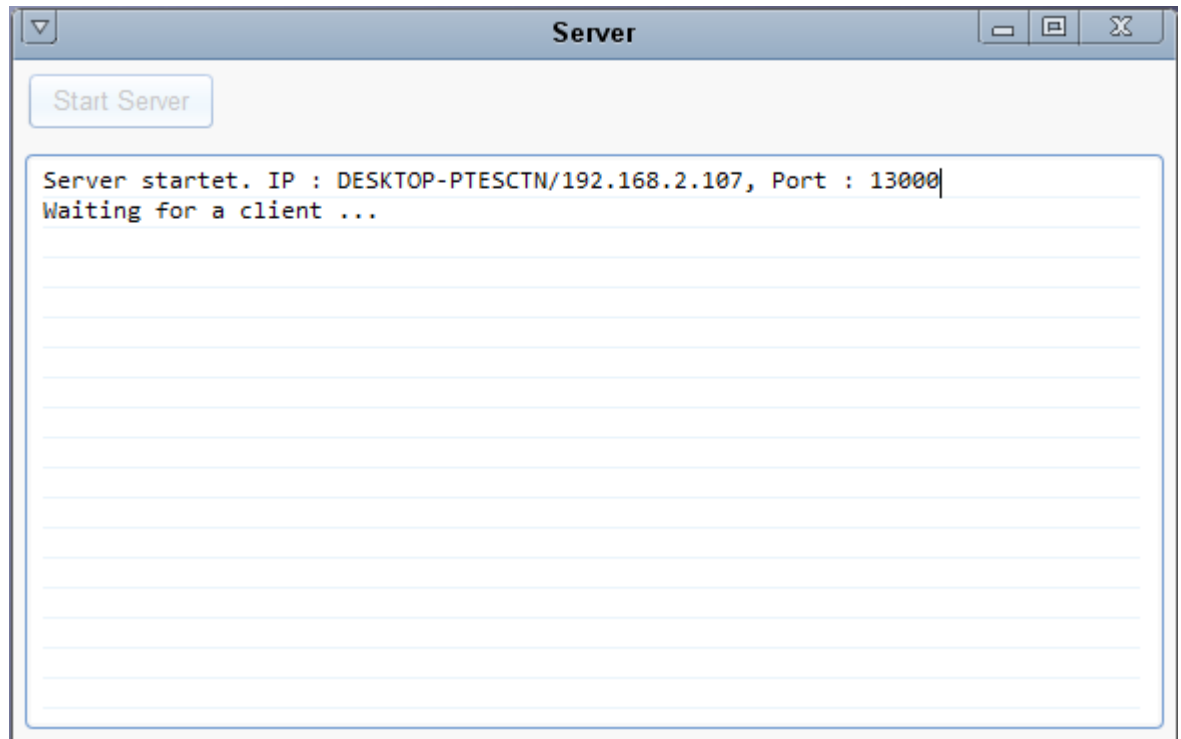
Hình 5.10 Biểu đồ Class Voice call Packages

Voice Call Packages gồm 3 lớp chính:

- Lớp Voice server: thực hiện việc khởi động server để gọi âm thanh.
- Lớp Voice Client: kết nối lên server để gửi nhận tín hiệu âm thanh.
- Lớp Voice static: chứa các phương thức và thuộc tính cần thiết cho lớp server và client.

5.4 Kết quả chạy chương trình

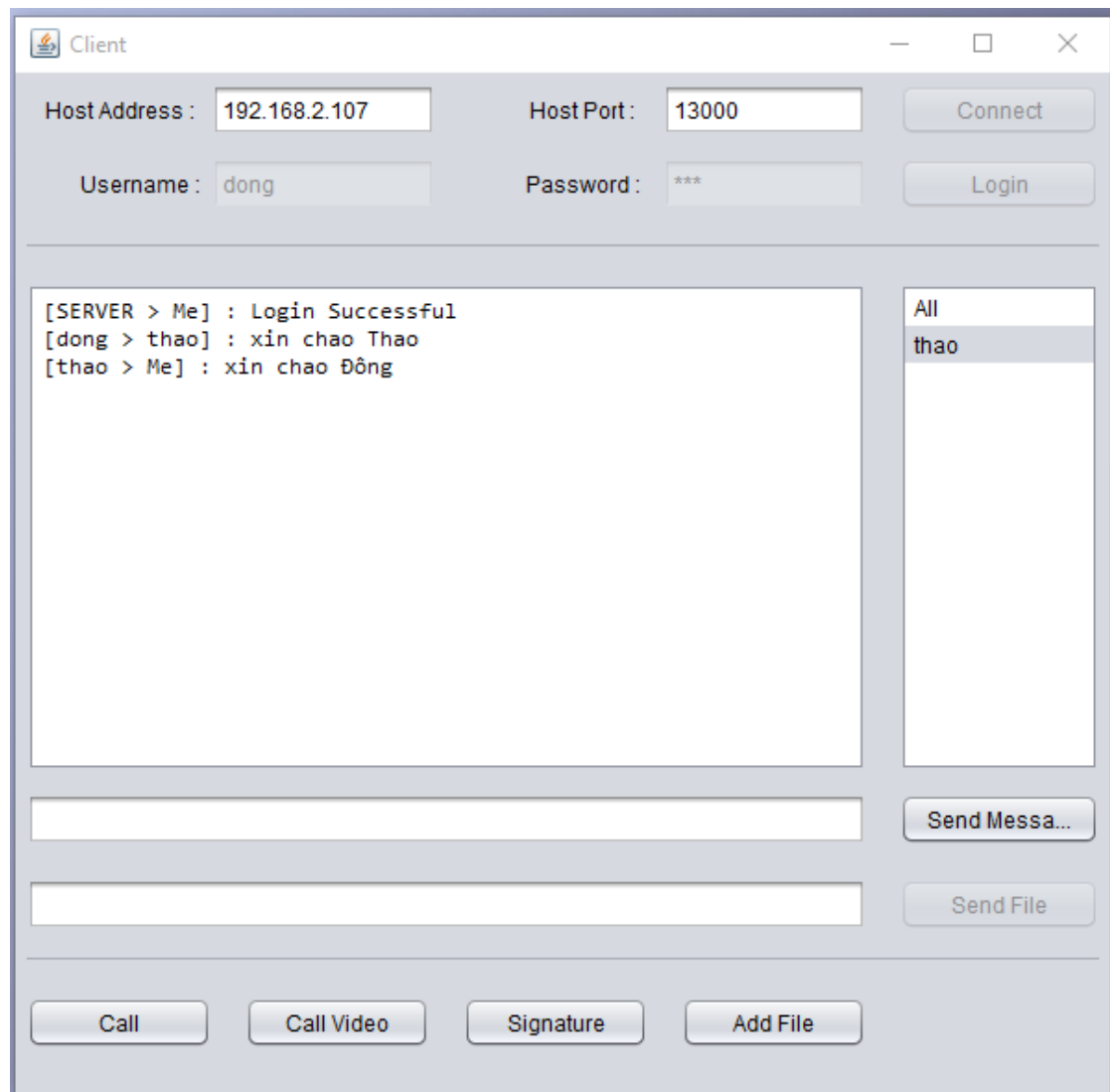
- Kết quả chạy phía Server



Hình 5.11 Giao diện phía Server

Chương trình phía server chạy thành công với giao diện diện gồm một nút Start để bắt đầu khởi động Server, một ô TextBox hiển thị thông tin Server như địa chỉ IP server, port server, số hiệu các tiến trình con kết nối lên server và ngắt kết nối khỏi server.

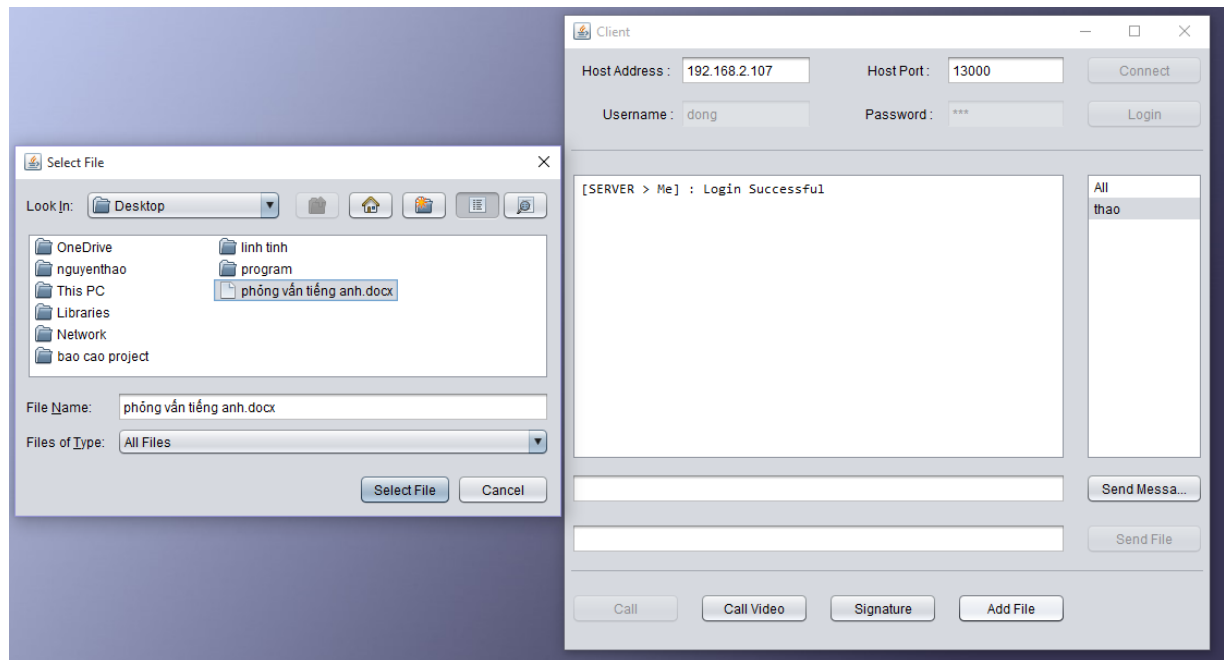
- Kết quả chạy phía Client



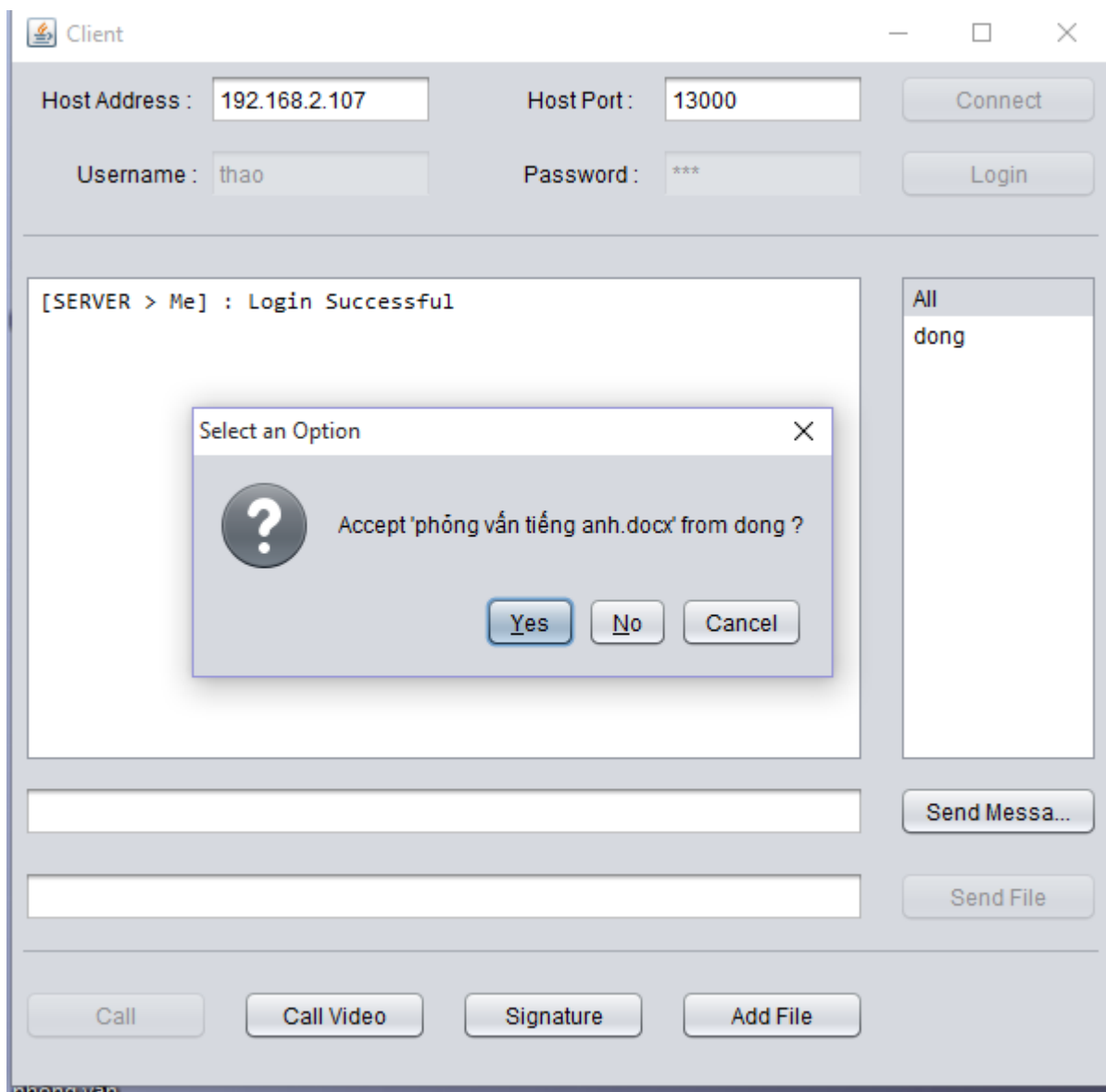
Hình 5.12 Giao diện phía Client

Chương trình phía client chạy thành công với giao diện gồm 3 phần, phần trên cùng chứa các edittext như Host Address, Host Port, User name, Password. Đây là những thông tin cần thiết cho việc đăng nhập kết nối lên Server. Phần giữa gồm một ô Textbox hiển thị thông tin cuộc trò chuyện giữa các Client, một ô Listview hiển thị danh sách các thành viên kết nối lên Server. Cuối cùng là phần chứa các button Call, Call Video, Signature, Add File thực hiện các chức năng đúng như tên gọi của chúng. Cụ thể như sau:

- Chức năng gửi file: thực hiện tốt, người dùng kích vào tên người nhận file, sau đó kích vào button add file để chọn file cần gửi. Người nhận sẽ nhận được thông báo tùy chọn có muốn nhận file hay không. Nếu chọn có nhận, sẽ hiển thị giao diện để chọn thư mục lưu file, nếu chọn không nhận, thì chương trình sẽ hủy việc gửi nhận file.



Hình 5.13 Giao diện chọn file để gửi




Hình 5.14 Giao diện tùy chọn có nhận file hay không


- Chức năng tạo và thẩm định chữ ký điện tử: thực hiện tốt. Khi người dùng muốn thực hiện chức năng này, sẽ kích vào button Signature, giao diện hiện ra với tùy chọn là bên ký hay bên nhận.


Bên Ký


Kích Thước Khóa: 256


File Gửi: 


Tạo Khóa **Tạo Chữ Ký**

Khóa Bí Mật 

Khóa Công Khai_E 

Khóa Công Khai_N 

Băm SHA-1 

Chữ Ký Số 

Reset

Hình 5.15 Giao diện bên ký

The screenshot shows a web application window titled "Bên Nhận" (Receiver). It contains the following elements:

- Four input fields, each preceded by a folder icon with a green arrow pointing up:
 - Khóa E (Public Key)
 - Khóa N (Modulus)
 - Chữ Ký Số (Signature)
 - Thông Điệp (Message)
- A section labeled "Băm SHA-1" (SHA-1 Hash) with a large multi-line text input area.
- A section labeled "Giải Mã Chữ Ký" (Decode Signature) with another large multi-line text input area.
- At the bottom, two buttons: "Kiểm Tra" (Check) on the left and "Reset" on the right.

Hình 5.16 Giao diện bên thẩm định chữ ký

- Chức năng Video Call: thực hiện tốt, âm thanh rõ nét, tuy nhiên chất lượng hình ảnh chưa được cao, thỉnh thoảng hay bị treo máy. Nguyên nhân là do tốc độ get ảnh từ camera nhanh hơn tốc độ gửi đi.

5.5 Kết luận

Về cơ bản, chương này đã trình bày đầy đủ các bước phân tích thiết kế hệ thống như sơ đồ khối, sơ đồ lớp, đặc tả use case. Bằng việc kết hợp lắp ghép các kiến thức về mặt lý thuyết ở các chương trước, đã xây dựng một phần mềm hoàn chỉnh với chức năng chính là trao đổi thông tin qua mạng nội bộ. Chương trình chạy tốt với các chức năng đề ra như gửi file, chat text, audio streaming, video streaming, tạo và thẩm định chữ ký điện tử....Tuy nhiên thì cũng có một vài mặt hạn chế, đó là giao diện chưa được đẹp, nhiều lúc chương trình bị treo.

Kết luận

Truyền thông qua mạng là một trong những ứng dụng phổ biến trên mạng LAN và Internet như: Tải xuống các file từ một máy chủ file ở xa, gửi/nhận thư điện tử, ... Truyền thông qua mạng dựa trên Socket TCP là một phương pháp truyền thông có độ tin cậy cao bởi vì trước khi truyền nó cần thiết lập thành công kênh truyền dữ liệu.

Không phải là phương pháp thay thế hoàn toàn những phương pháp truyền thông khác mà ta đã từng sử dụng. Bản chất của phương pháp truyền thông dựa vào Socket TCP là nhằm tăng thêm hiệu suất làm việc. Đề tài “*Truyền thông đa phương tiện trong mạng Lan, Wlan*” đã đạt được kết quả nhất định.

Về cơ sở lý thuyết, đồ án đã trình bày được các nội dung về Đa phương tiện, Mạng máy tính, Sơ lược về ngôn ngữ Java, Lập trình Socket TCP nói chung và lập trình Socket TCP trong Java nói riêng, Chữ ký điện tử và các nội dung liên quan đến truyền thông qua mạng.

Về ứng dụng đồ án đã phân tích một cách khá chi tiết cơ chế hoạt động của chương trình ở phía clients, phía server và đã cài đặt thành công chương trình. Java là một ngôn ngữ mạnh mẽ, tính bảo mật cao và độc lập với nền, do đó chương trình ứng dụng của đồ án có thể dễ dàng chạy trên các hệ thống khác nhau mà không phải lập trình lại.

Tuy nhiên, do hạn chế về thời gian và trình độ nên nhiều tính năng của chương trình chưa được hoàn thiện. Trong thời gian tới, chương trình sẽ được hoàn thiện theo hướng bổ sung các chức năng cho phù hợp yêu cầu đặc thù của việc truyền thông qua mạng, có thể áp dụng vào thực tế cuộc sống.

Tài liệu tham khảo

- [1]. <http://123doc.org/document/2270886-giao-trinh-truyen-thong-va-da-phuong-tien.htm> ,truy cập cuối cùng ngày 25/3/2016.
- [2]. <https://voer.edu.vn/c/socket-duoi-ngon-ngu-java/761b0302/4f8ba8e9> , truy cập cuối cùng ngày 10/04/2016.
- [3]. http://vietjack.com/java/lap_trinh_mang_trong_java.jsp ,truy cập cuối cùng ngày 15/4/2016.
- [4]. <http://luanvan.co/luan-van/do-an-tim-hieu-lap-trinh-socket-tcp-trong-java-va-ung-dung-truyen-file-qua-mang-34168/> , truy cập cuối ngày 16/4/2016.
- [5]. <http://www.javaworld.com/article/2077322/core-java/core-java-sockets-programming-in-java-a-tutorial.html>, truy cập cuối ngày 16/4/2016.
- [6]. <http://www.javatpoint.com/socket-programming> , truy cập cuối ngày 8/3/2016.
- [7]. <https://www.daniweb.com/programming/software-development/threads/429713/video-chatting-application-in-java>, truy cập cuối ngày 10/3/2016.
- [8]. <https://github.com/robelsharma/VideoConference>, truy cập cuối ngày 15/3/2016.
- [9]. <http://stackoverflow.com/questions/31312621/voice-chat-or-audio-call-using-socket-in-java>, truy cập cuối ngày 20/3/2016.
- [10]. <http://stackoverflow.com/questions/11623185/java-voice-chat-mixdown-incoming-data-for-single-output>, truy cập cuối ngày 22/3/2016.
- [11]. <http://stackoverflow.com/questions/10257591/how-to-build-a-video-chat-program-in-java-without-jmf>, truy cập cuối ngày 22/3/2016.
- [12]. <http://congdongjava.com/forum/threads/why-voice-chat.20627/>, truy cập cuối ngày 25/3/2016.

- [13]. https://www.academia.edu/16461804/_Nh%C3%B3m_6-ATBMHTTT-D12PM-HT-01_Gi%E1%BA%A3i_thu%E1%BA%ADt_t%E1%BA%A1o_ch%E1%BB%AF_k%C3%BD_s%E1%BB%91_s%E1%BB%AD_d%E1%BB%A5ng_RSA, truy cập cuối ngày 20/3/2016.
- [14]. <http://www.vnpro.vn/mo-hinh-tham-chieu-he-thong-mo-osi/>, truy cập cuối ngày 28/3/2016

Bảng đối chiếu thuật ngữ Anh Việt

TỪ TIẾNG ANH	NGHĨA TIẾNG VIỆT
Media	Phương Tiện
Static Media	Phương Tiện Tĩnh
Dynamic Media	Phương Tiện Động
Multimedia System	Hệ Thống Đa Phương Tiện
Process	Xử Lý
Multimedia Computing	Xử Lý Đa Phương Tiện
Communication	Truyền Thông Đa Phương Tiện
Education	Giáo Dục
Telemedicine	Hệ Thống Thầy Thuốc Từ Xa
Video Phone	Hệ Thống Điện Thoại Truyền Hình
Convesational Services	Các Dịch Vụ Đàm Thoại
Videoconference	Hội Thảo Truyền Hình
Telesurveillance	Dịch Vụ Giám Sát Từ Xa
Teleshopping	Mua Sắm Từ Xa
Messaging Services	Các Dịch Vụ Thông Điệp
Retrieval Services	Các Dịch Vụ Tìm Kiếm Thông Tin
Socket	Số Hiệu Cổng
Server	Máy Chủ
Digital Signature	Chữ Ký Số
Digital Signature Generation Algorithm	Giải Thuật Tạo Ra Chữ Ký Số
Digital Signature Verification Algorithm	Giải Thuật Kiểm Tra Chữ Ký Số