TRƯỜNG ĐẠI HỌC PHAN THIẾT

GIÁO TRÌNH

LẬP TRÌNH MẠNG

LƯU HÀNH NỘI BỘ

MỤC LỤC

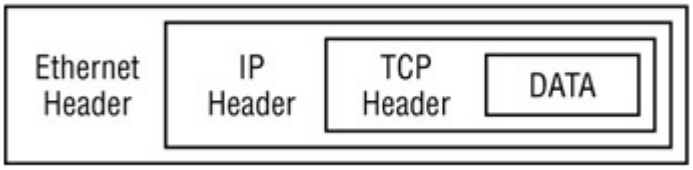
CHƯƠNG I: NHỮNG KIẾN THỨC CƠ BẢN VỀ LẬP TRÌNH MẠNG

I.1. Tổng quan

Internet Protocol (IP) là nền tảng của lập trình mạng. IP là phương tiện truyền tải dữ liệu giữa các hệ thống bất kể đó là hệ thống mạng cục bộ (LAN) hay hệ thống mạng diện rộng (WAN). Mặc dù lập trình viên mạng có thể chọn các giao thức khác để lập trình nhưng IP cung cấp các kỹ thuật mạnh nhất để gởi dữ liệu giữa các thiết bị, đặc biệt là thông qua mạng Internet.

Để hiểu rõ các khái niệm bên dưới lập trình mạng, chúng ta phải hiểu rõ giao thức IP, hiểu cách nó chuyển dữ liệu giữa các thiết bị mạng. Lập trình mạng dùng giao thức IP thường rất phức tạp. Có nhiều yếu tố cần quan tâm liên quan đến cách dữ liệu được gởi qua mạng: số lượng Client và Server, kiểu mạng, tắc nghẽn mạng, lỗi mạng,… Bởi vì các yếu tố này ảnh hưởng đến việc truyền dữ liệu từ thiết bị này đến thiết bị khác trên mạng do đó việc hiểu rõ chúng là vấn đề rất quan trọng để lập trình mạng được thành công.

Một gói dữ liệu mạng gồm nhiều tầng thông tin. Mỗi tầng thông tin chứa một dãy các byte được sắp đặt theo một trật tự đã được định sẵn. Hầu hết các gói dữ liệu dùng trong lập trình mạng đều chứa ba tầng thông tin cùng với dữ liệu được dùng để truyền tải giữa các thiết bị mạng. Hình sau mô tả hệ thống thứ bậc của một gói IP:

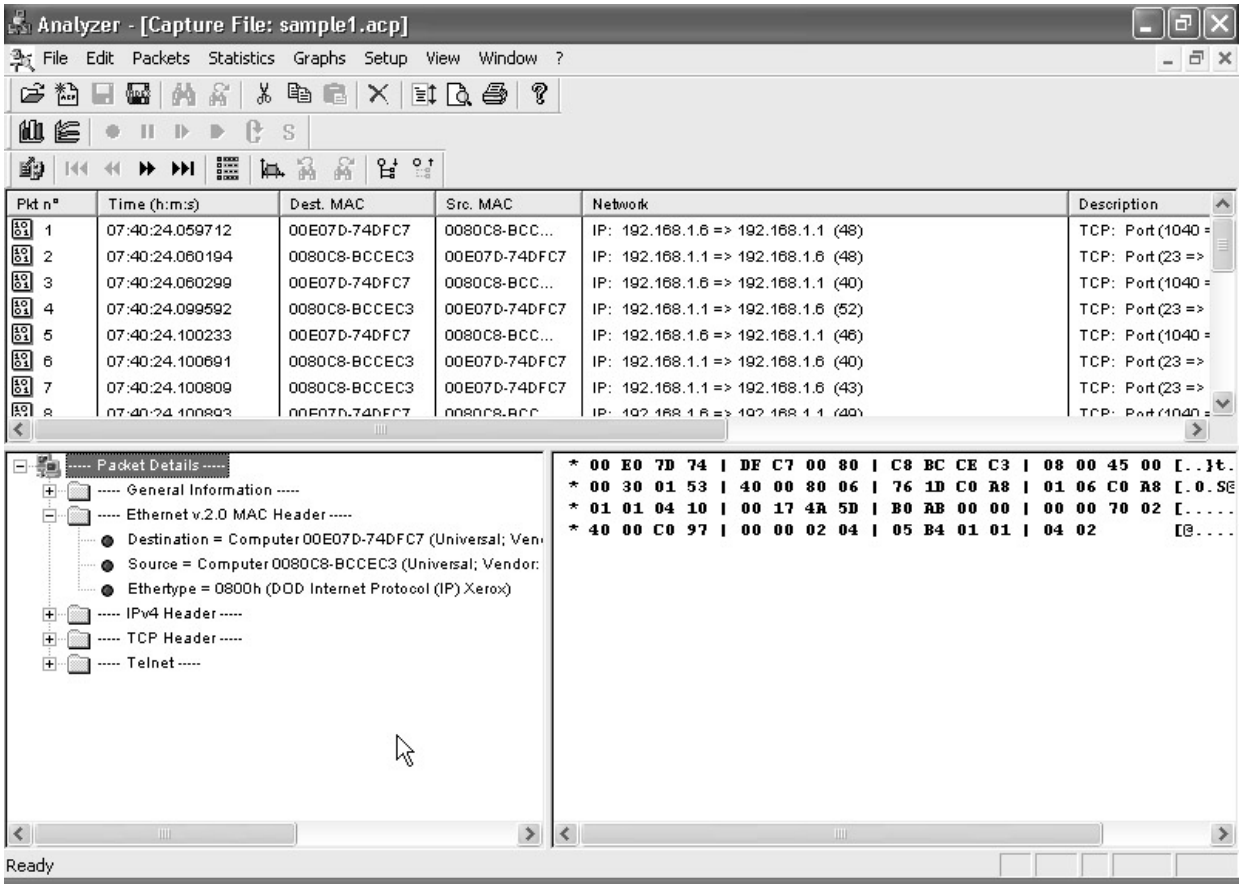


Hình I.1: Các tầng giao thức mạng trong các gói dữ liệu

I.1.1. Tầng Ethernet

Tầng đầu tiên của gói dữ liệu mạng được gọi là Ethernet Header, trong tầng này có ba gói giao thức Ethernet: Ethernet 802.2, Ethernet 802.3, và Ethernet phiên bản 2. Các giao thức Ethernet 802.2 và Ethernet 802.3 là các giao thức chuẩn của IEEE. Ethernet phiên bản 2 tuy không phải là giao thức chuẩn nhưng nó được sử dụng rộng

rãi trong mạng Ethernet. Hầu hết các thiết bị mạng kể cả hệ điều hành Windows mặc định dùng giao thức Ethernet phiên bản 2 để truyền tải các gói IP.



Hình I.2: Ethernet Header

Phần đầu của Ethernet phiên bản 2 là địa chỉ MAC (Media Access Card) dùng để xác định các thiết bị trên mạng cùng với số giao thức Ethernet xác định giao thức tầng tiếp theo chứa trong gói Ethernet. Mỗi gói Ethernet bao gồm:

- 6 byte địa chỉ MAC đích
- 6 byte địa chỉ MAC nguồn
- 2 byte xác định giao thức tầng kế tiếp
- Data payload từ 46 đến 1500 byte
- 4-byte checksum

I.1.2. Địa chỉ Ethernet

Địa chỉ Ethernet (địa chỉ MAC) là địa chỉ của các thiết bị, địa chỉ này được gán bởi các nhà sản xuất thiết bị mạng và nó không thay đổi được. Mỗi thiết bị trên mạng Ethernet phải có 1 địa chỉ MAC duy nhất. Địa chỉ MAC gồm 2 phần:

- 3 byte xác định nhà sản xuất
- 3 byte xác định số serial duy nhất của nhà sản xuất

Giản đồ địa chỉ Ethernet cho phép các địa chỉ broadcast và multicast. Đối với địa chỉ broadcast thì tất cả các bit của địa chỉ đích được gán bằng 1 (FFFFFFFFFFFF). Mỗi thiết bị mạng sẽ chấp nhận các gói có địa chỉ broadcast. Địa chỉ này hữu ích cho các giao thức phải gởi các gói truy vấn đến tất cả các thiết bị mạng. Địa chỉ multicast cũng là một loại địa chỉ đặc biệt của địa chỉ Ethernet, các địa chỉ multicast chỉ cho phép một số các thiết bị chấp nhận gói tin. Một số địa chỉ Ethernet multicast:

Địa Chỉ	**Mô Tả**
01-80-C2-00-00-00	Spanning tree (for bridges)
09-00-09-00-00-01	HP Probe
09-00-09-00-00-01	HP Probe
09-00-09-00-00-04	HP DTC
09-00-2B-00-00-00	DEC MUMPS
09-00-2B-00-00-01	DEC DSM/DTP
09-00-2B-00-00-02	DEC VAXELN
09-00-2B-00-00-03	DEC Lanbridge Traffic Monitor (LTM)
09-00-2B-00-00-04	DEC MAP End System Hello
09-00-2B-00-00-05	DEC MAP Intermediate System Hello
09-00-2B-00-00-06	DEC CSMA/CD Encryption
09-00-2B-00-00-07	DEC NetBios Emulator
09-00-2B-00-00-0F	DEC Local Area Transport (LAT)
09-00-2B-00-00-1x	DEC Experimental
09-00-2B-01-00-00	DEC LanBridge Copy packets (all bridges)
09-00-2B-02-00-00	DEC DNA Lev. 2 Routing Layer Routers
09-00-2B-02-01-00	DEC DNA Naming Service Advertisement
09-00-2B-02-01-01	DEC DNA Naming Service Solicitation
09-00-2B-02-01-02	DEC DNA Time Service
09-00-2B-03-xx-xx	DEC default filtering by bridges

Địa Chỉ	**Mô Tả**
09-00-2B-04-00-00	DEC Local Area System Transport (LAST)
09-00-2B-23-00-00	DEC Argonaut Console
09-00-4E-00-00-02	Novell IPX
09-00-77-00-00-01	Retix spanning tree bridges
09-00-7C-02-00-05	Vitalink diagnostics
09-00-7C-05-00-01	Vitalink gateway
0D-1E-15-BA-DD-06	HP
CF-00-00-00-00-00	Ethernet Configuration Test protocol (Loopback)

I.1.3. Ethernet Protocol Type

Một phần khác rất quan trọng của Ethernet Header là trường Protocol Type, trường này có kích thước hai byte. Sự khác nhau giữa gói tin Ethernet phiên bản 2 và Ethernet 802.2 và 802.3 xảy ra ở trường này. Các gói tin Ethernet 802.2 và 802.3 sử dụng trường này để cho biết kích thước của một gói tin Ethernet. Ethernet phiên bản 2 dùng trường này để định nghĩa giao thức tầng kế tiếp trong gói tin Ethernet. Một số giá trị của trường này:

Giá Trị	**Giao Thức**
0800	IP
0806	ARP
0BAD	Banyan VINES
8005	HP Probe
8035	Reverse ARP
809B	AppleTalk
80D5	IBM SNA
8137	Novell
8138	Novell
814C	Raw SNMP
86DD	IPv6
876B	TCP/IP compression

I.1.4. Data payload

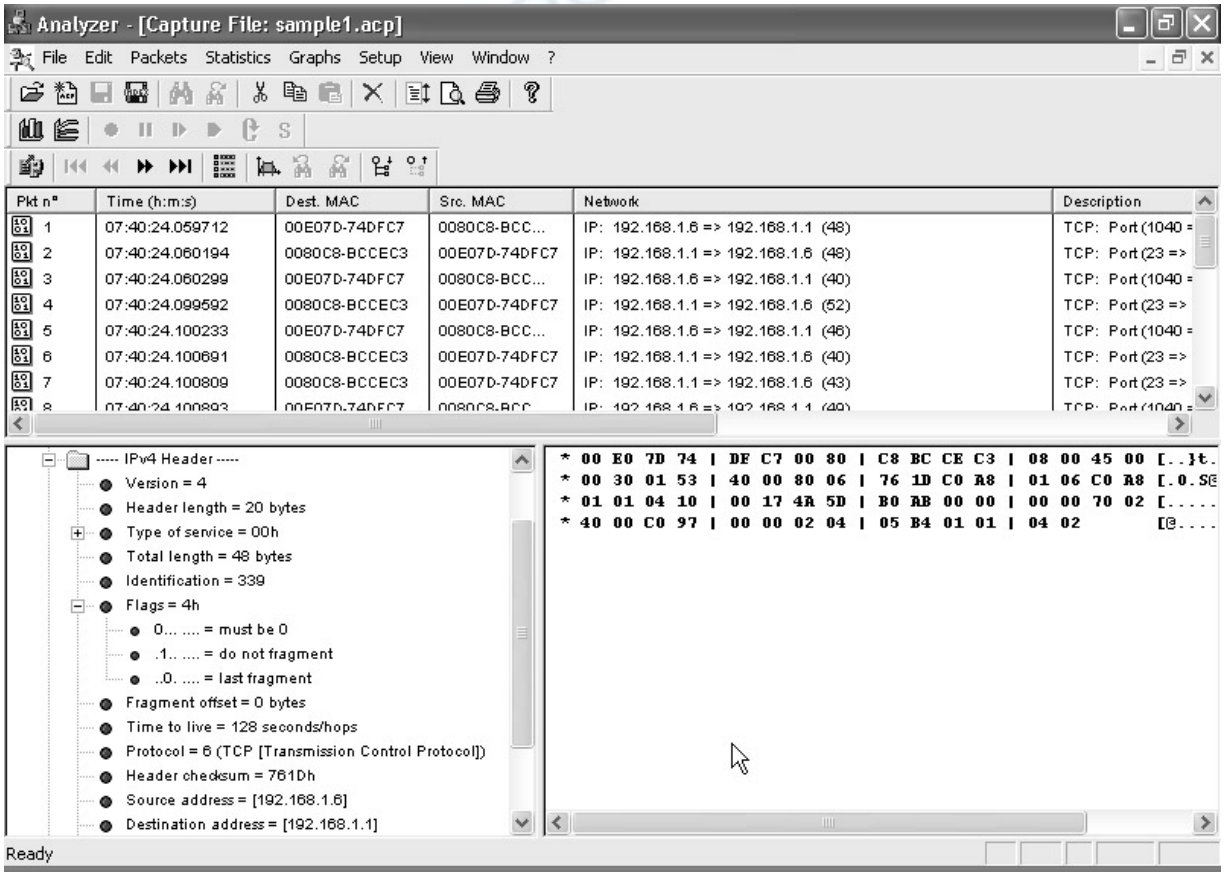
Data payload phải chứa tối thiểu 46 byte để đảm bảo gói Ethernet có chiều dài tối thiểu 64 byte. Nếu phần data chưa đủ 46 byte thì các ký tự đệm được thêm vào cho đủ. Kích thước của trường này từ 46 đến 1500 byte.

I.1.5. Checksum

Giá trị checksum cung cấp cơ chế kiểm tra lỗi cho dữ liệu, kích thước của trường này là 4 byte . Nếu gói tin bị hỏng trong lúc truyền, giá trị checksum sẽ bị tính toán sai và gói tin đó được đánh dấu là gói tin xấu.

I.2. Tầng IP

Tầng IP định nghĩa thêm nhiều trường thông tin của của giao thức Ethernet



Hình I.3: Thông tin tầng IP

Các trường trong tầng IP:

Trường	**Bit**	**Mô Tả**
Version	4	Phiên bản IP header (phiên bản hiện tại là 4)
Header Length	4	Chiều dài phần header của gói IP

Trường	**Bit**	**Mô Tả**
Type of Service	8	Kiểu chất lượng dịch vụ QoS (Quality of Service)
Total Length	16	Chiều dài của gói IP
Identification	16	Giá trị ID duy nhất xác định các gói IP
Flags	3	Cho biết gói IP có bị phân đoạn hay không hay còn các phân đoạn khác
Fragment offset	13	Vị trí của phân đoạn trong gói IP
Time to Live (TTL)	8	Thời gian tối đa gói tin được phép ở lại trên mạng (được tính bằng giây)
Protocol	8	Kiểu giao thức của tầng dữ liệu kế tiếp
Header Checksum	16	Checksum của dữ liệu gói IP header
Source Address	32	Địa chỉ IP của thiết bị gởi
Destination Address	32	Địa chỉ IP của thiết bị nhận
Options		Định nghĩa các đặc điểm của gói IP trong tươnglai

I.2.1. Trường địa chỉ

Địa chỉ Ethernet dùng để xác định các thiết bị trên mạng LAN nhưng nó không thể dùng để xác định địa chỉ của các thiết bị trên mạng ở xa. Để xác định các thiết bị trên các mạng khác nhau, địa chỉ IP được dùng. Một địa chỉ IP là một số 32 bit và địa chỉ IP được chia thành 4 lớp sau:

Lớp A	0.x.x.x–127.x.x.x
Lớp B	128.x.x.x–191.x.x.x
Lớp C	192.x.x.x–223.x.x.x
Lớp D	224.x.x.x–254.x.x.x

I.2.2. Các cờ phân đoạn

Một trong những phức tạp, rắc rối của gói IP là kích thước của chúng. Kích thước tối đa của gói IP có thể lên đến 65,536 byte. Đây là một lượng rất lớn dữ liệu cho một gói tin. Thực tế hầu hết các truyền tải dữ liệu ở cấp thấp như Ethernet không thể hỗ trợ một gói IP lớn (phần dữ liệu của Ethernet chỉ có thể tối đa 1500 byte). Để giải quyết vấn đề này, các gói IP dùng fragmentation (phân đoạn) để chia các gói IP thành các phần nhỏ hơn để truyền tải tới đích. Khi các mảnh được truyền tải tới đích, phần mềm của thiết bị nhận phải có cách để nhận ra các phân đoạn của gói tin và ráp chúng lại thành thành 1 gói IP.

Sự phân đoạn được thành lập nhờ vào việc sử dụng 3 trường của gói IP: fragmentation flags, fragment offset, và trường identification. Cờ phân đoạn bao gồm ba cờ một bit sau:

- Cờ reserved: giá trị zero
- Cờ Don't Fragment: cho biết gói IP không bị phân đoạn
- Cờ More Fragment: cho biết gói tin bị phân đoạn và còn các phân đoạn khác nữa

Trường IP Indentification xác định duy nhất định danh mỗi gói IP. Tất cả các phân đoạn của bất kỳ gói IP nào cũng đều có cùng số indentification. Số identification giúp cho phần mềm máy nhận biết được các phân đoạn nào thuộc gói IP nào và ráp lại cho đúng.

Trường fragment offset cho biết vị trí của phân đoạn trong gói tin ban đầu.

I.2.3. Trường Type of Service

Trường Type of Service xác định kiểu chất lượng dịch vụ QoS (Quality of Service) cho gói IP. Trường này được dùng để đánh dấu một gói IP có một độ ưu tiên nào đó chẳng hạn như được dùng để tăng độ ưu tiên của các dữ liệu cần thời gian thực như Video, Audio.

Trong hầu hết các truyền tải mạng, trường này được được thiết lập giá trị zero, cho biết đây là dữ liệu bình thường, tuy nhiên với các ứng dụng cần thời gian thực như Video hay Audio thì trường này sẽ được sử dụng để tăng độ ưu tiên cho gói dữ liệu. Trường này gồm tám bit và ý nghĩa các bit như sau:

- 3 bit được dùng làm trường ưu tiên
- 1 bit cho biết thời gian trễ là bình thường hay thấp
- 1 bit cho biết thông lượng bình thường hay cao
- 1 bit cho biết độ tin cậy bình thường hay cao
- 2 bit được dùng trong tương lai

I.2.4. Trường Protocol

Được dùng để xác định giao thức tầng tiếp theo trong gói IP, IANA định nghĩa 135 giá trị cho trường này có thể dùng trong gói IP nhưng chỉ có một số giá trị hay được dùng trong bảng sau:

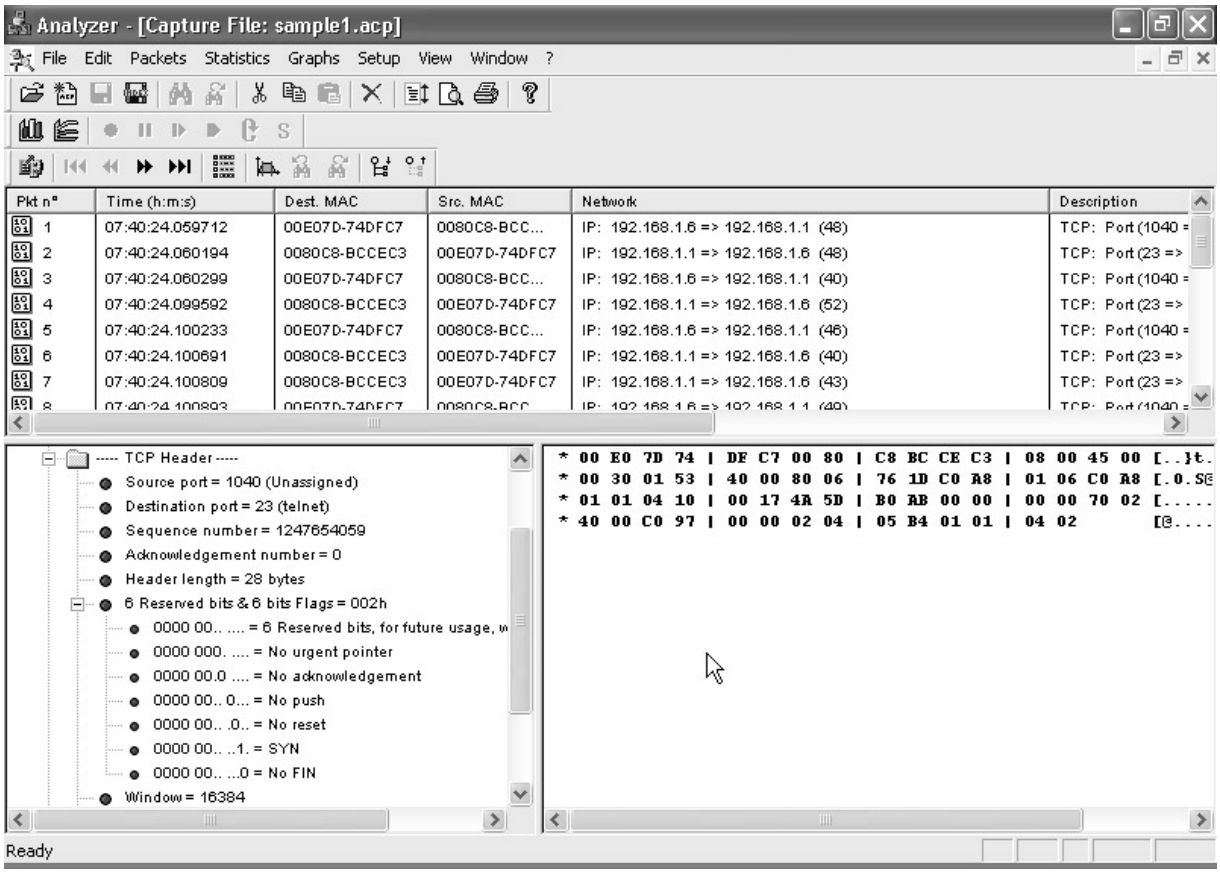
Giá Trị	**Giao Thức**
1	Internet Control Message (ICMP)
2	Internet Group Message (IGP)
6	Transmission Control (TCP)
8	Exterior Gateway (EGP)
9	Interior Gateway (Cisco IGP)
17	User Datagram (UDP)
88	Cisco EIGRP

Hai giao thức được dùng nhiều nhất trong lập trình mạng là TCP và UDP

I.3. Tầng TCP

Giao thức TCP (Transmission Control Protocol) là giao thức hướng kết nối, nó cho phép tạo ra kết nối điểm tới điểm giữa hai thiết bị mạng, thiết lập một đường nhất quán để truyền tải dữ liệu. TCP đảm bảo dữ liệu sẽ được chuyển tới thiết bị đích, nếu dữ liệu không tới được thiết bị đích thì thiết bị gởi sẽ nhận được thông báo lỗi.

Các nhà lập trình mạng phải hiểu cách hoạt động cơ bản của TCP và đặc biệt là phải hiểu cách TCP truyền tải dữ liệu giữ các thiết bị mạng. Hình sau cho thấy những trường của TCP Header. Những trường này chứa các thông tin cần thiết cho việc thực thi kết nối và truyền tải dữ liệu một cách tin tưởng.



Hình I.4: Các trường của TCP Header

Mỗi trường của TCP Header kết hợp với một chức năng đặc biệt của một phiên làm việc TCP. Có một số chức năng quan trọng sau:

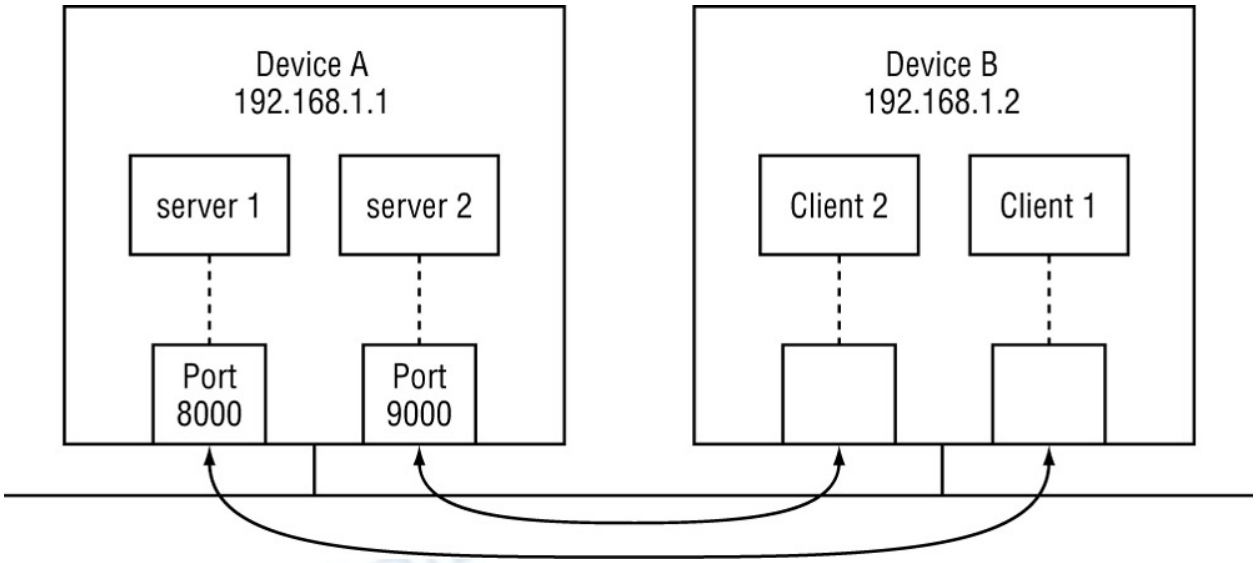
- Source port và Destination port: theo dõi các kết nối giữa các thiết bị
- Sequence và Acknowledgement number: theo dõi thứ tự các gói tin và truyền tải lại các gói tin bị mất
- Flag: mở và đóng kết nối giữa các thiết bị để truyền tải dữ liệu

I.3.1. TCP port

TCP sử dụng các port để xác định các kết nối TCP trên một thiết bị mạng. Để liên lạc với một ứng dụng chạy trên một thiết bị mạng ở xa ta cần phải biết hai thông tin :

- Địa chỉ IP của thiết bị ở xa
- TCP port được gán cho thiết bị ở xa

Để kết nối TCP được thành lập, thiết bị ở xa phải chấp nhận các gói tin truyền đến port đã được gán. Bởi vì có nhiều ứng dụng chạy trên một thiết bị sử dụng TCP do đó thiết bị phải cấp phát các cổng khác nhau cho các ứng dụng khác nhau.



Hình I.5: Kết nối TCP đơn giản

Trong hình trên thì thiết bị A đang chạy hai ứng dụng Server, hai ứng dụng này đang chờ các gói tin từ Client. Một ứng dụng được gán port 8000 và một ứng dụng được gán port 9000. Thiết bị mạng B muốn kết nối đến thiết bị mạng A thì nó phải được gán một TCP port còn trống từ hệ điều hành và port này sẽ được mở trong suốt phiên làm việc. Các port ở Client thường không quan trọng và có thể gán bất kỳ một port nào hợp lệ trên thiết bị.

Tổ hợp của một địa chỉ IP và một port là một IP endpoint. Một phiên làm việc TCP được định nghĩa là một sự kết hợp của một IP endpoint cục bộ và một IP endpoint ở xa. Một ứng dụng mạng có thể sử dụng cùng một IP endpoint cục bộ nhưng mỗi thiết bị ở xa phải sử dụng một địa chỉ IP hay port riêng.

IANA định nghĩa một danh sách các port TCP tiêu chuẩn được gán cho các ứng dụng đặc biệt:

Port	**Mô Tả**
7	Echo
13	Daytime
17	Quote of the day
20	FTP (data channel)
21	FTP (control channel)

Port	**Mô Tả**
22	SSH
23	Telnet
25	SMTP
37	Time
80	HTTP
110	POP3
119	NNTP
123	Network Time Protocol (NTP)
137	NETBIOS name service
138	NETBIOS datagram service
143	Internet Message Access Protocol (IMAP)
389	Lightweight Directory Access Protocol (LDAP)
443	Secure HTTP (HTTPS)
993	Secure IMAP
995	Secure POP3

Các port từ 0->1023 được gán cho các ứng dụng thông dụng do đó với các ứng dụng mà các lập trình viên tạo ra thì các port được gán phải từ 1024->65535.

I.3.2. Cơ chế đảm bảo độ tin cậy truyền tải các gói tin

Trường tiếp theo trong TCP Header sau port là số sequence và acknowledgement. Những giá trị này cho phép TCP theo dõi các gói tin và đảm bảo nó được nhận theo đúng thứ tự. Nếu bất kỳ gói tin nào bị lỗi, TCP sẽ yêu cầu truyền tải lại các gói tin bị lỗi và ráp chúng lại trước khi gởi gói tin cho ứng dụng.

Mỗi gói tin có một số duy nhất sequence cho một phiên làm việc TCP. Một số ngẫu nhiên được chọn cho gói tin đầu tiên được gởi đi trong phiên làm việc. Mỗi gói tin tiếp theo được gởi sẽ tăng số sequence bằng số byte dữ liệu TCP trong gói tin trước đó. Điều này đảm bảo mỗi gói tin được xác định duy nhất trong luồng dữ liệu TCP.

Thiết bị nhận sử dụng trường acknowledgement để hồi báo số sequence cuối cùng được nhận từ thiết bị gởi. Thiết bị nhận có thể nhận nhiều gói tin trước khi gởi lại một hồi báo. Số acknowledgement được trả về là số sequence cao nhất liền sau của dữ liệu được nhận. Kỹ thuật này được gọi là cửa sổ trượt. Các gói tin được nhận ngoài thứ

tự có thể được giữ trong bộ đệm và được đặt vào đúng thứ tự khi các gói tin khác đã được nhận thành công. Nếu một gói tin bị mất, thiết bị nhận sẽ thấy được số sequence bị lỗi và gởi một số acknowledgement thấp hơn để yêu cầu các gói tin bị lỗi. Nếu không có cửa sổ trượt mỗi gói tin sẽ phải hồi báo lại, làm tăng băng thông và độ trễ mạng.

I.3.3. Quá trình thành lập một phiên làm việc TCP

Quá trình làm thành lập một phiên làm việc TCP được thực hiện nhờ vào việc sử dụng các cờ (Flag):

Flag	**Mô Tả**
6 bit dành riêng	Dành riêng để sử dụng trong tương lai, giá trị luôn luôn là zero
1-bit URG flag	Đánh dấu gói tin là dữ liệu khẩn cấp
1-bit ACK flag	Hồi báo nhận một gói tin
1-bit PUSH flag	Cho biết dữ liệu được đẩy vào ứng dụng ngay lập tức
1-bit RESET flag	Thiết lập lại tình trạng khởi đầu kết nối TCP
1-bit SYN flag	Bắt đầu một phiên làm việc
1-bit FIN flag	Kết thúc một phiên làm việc

TCP sử dụng các tình trạng kết nối để quyết định tình trạng kết nối giữa các thiết bị. Một giao thức bắt tay đặc biệt được dùng để thành lập những kết nối này và theo dõi tình trạng kết nối trong suốt phiên làm việc. Một phiên làm việc TCP gồm ba pha sau:

- Mở bắt tay
- Duy trì phiên làm việc
- Đóng bắt tay

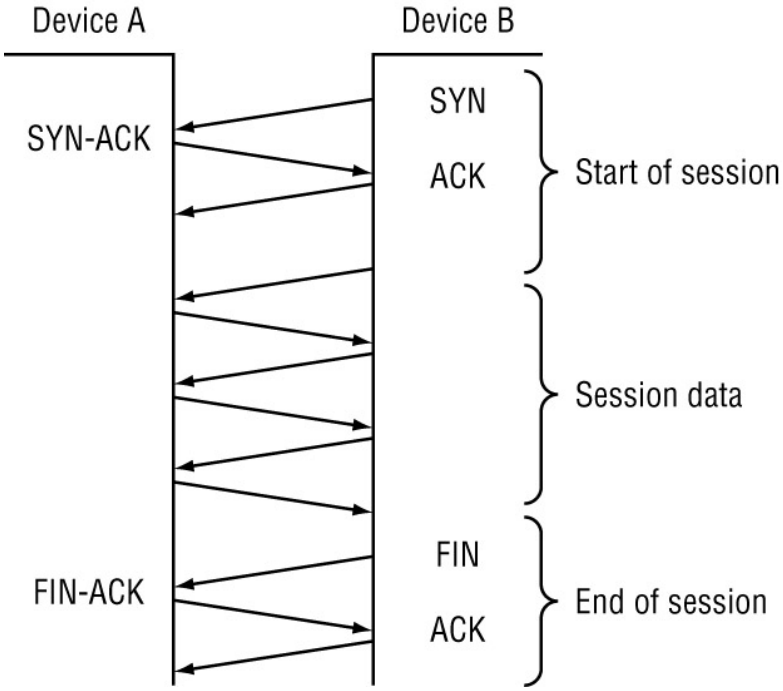
Mỗi pha yêu cầu các bit cờ được thiết lập trong một thứ tự nào đó. Quá trình mở bắt tay thường được gọi là ba cái bắt tay và nó yêu cầu ba bước để thành lập kết nối.

- Thiết bị gởi gởi cờ SYN cho biết bắt đầu phiên làm việc
- Thiết bị nhận gởi cả cờ SYN và cờ ACK trong cùng một gói tin cho biết nó chấp nhận bắt đầu phiên làm việc

- Thiết bị gởi gởi cờ ACK cho biết phiên làm việc đã mở và đã sẵng sàng cho việc gởi và nhận các gói tin.

Sau khi phiên làm việc được thành lập, cờ ACK sẽ được thiết lập trong các gói tin. Để đóng phiên làm việc, một quá trình bắt tay khác được thực hiện dùng cờ FIN:

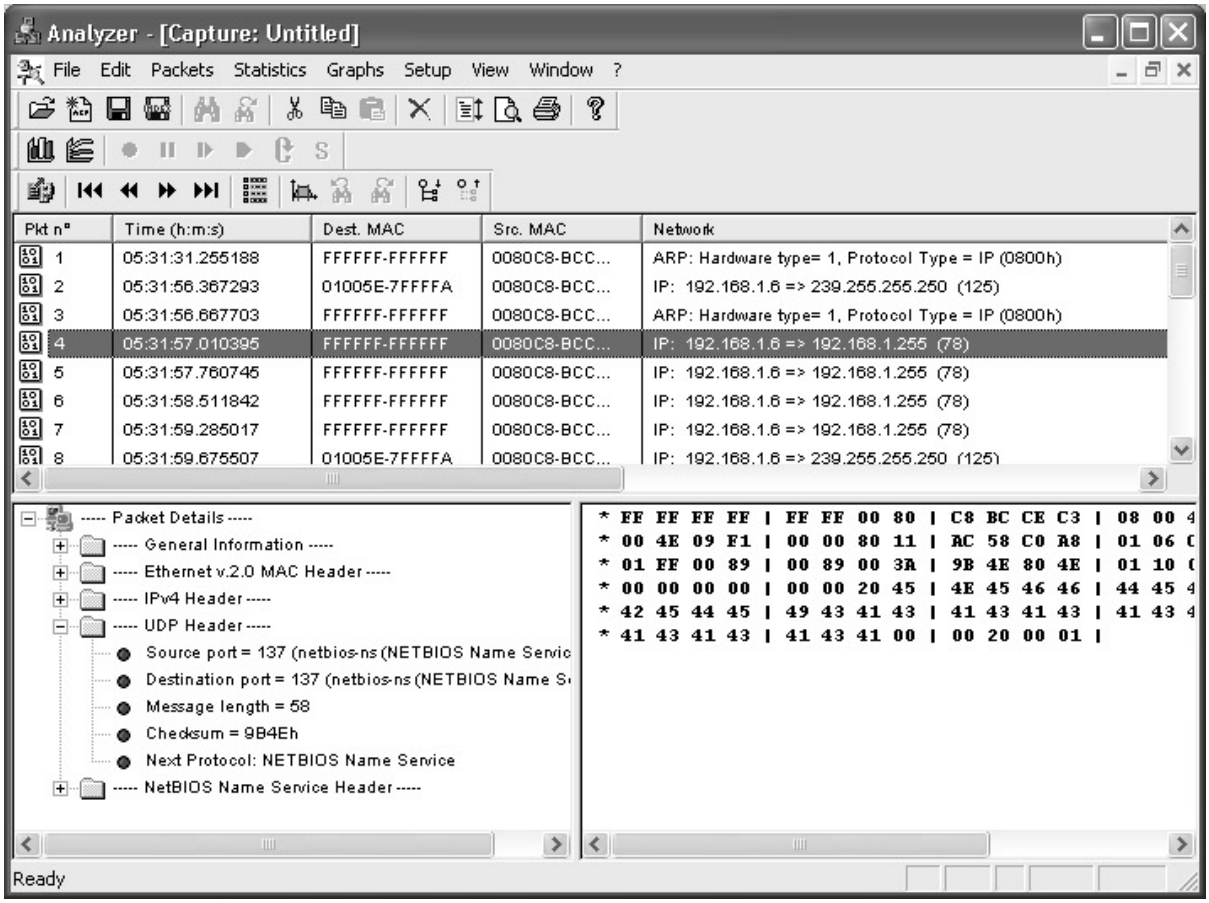
- Thiết bị khởi đầu đóng kết nối gởi cờ FIN
- Thiết bị bên kia gởi cờ FIN và ACK trong cùng một gói tin cho biết nó chấp nhận đóng kết nối
- Thiết bị khởi đầu đóng kết nối gởi cờ ACK để đóng kết nối



Hình I.6: Các bước bắt tay của giao thức TCP

I.4. Tầng UDP

User Datagram Protocol (UDP) là một giao thức phổ biến khác được dùng trong việc truyền tải dữ liệu của các gói IP. Không giống như TCP, UDP là giao thức phi nối kết. Mỗi phiên làm việc UDP không gì khác hơn là truyền tải một gói tin theo một hướng. Hình sau sẽ mô tả cấu trúc của một gói tin UDP



Hình I.7: UDP Header

UDP header gồm những trường sau:

- Source Port
- Destination Port
- Message Length
- Checksum
- Next Level Protocol

Cũng giống như TCP, UDP theo dõi các kết nối bằng cách sử dụng các port từ 1024->65536, các port UDP từ 0->1023 là các port dành riêng cho các ứng dụng phổ biến, một số dùng phổ biến như:

Port	**Mô Tả**
53	Domain Name System
69	Trivial File Transfer Protocol
111	Remote Procedure Call
137	NetBIOS name service
138	NetBIOS datagram

Port	**Mô Tả**
161	Simple Network Management Protocol