

BỘ CÔNG THƯƠNG
TRƯỜNG ĐẠI HỌC KINH TẾ - KỸ THUẬT CÔNG NGHIỆP
KHOA CÔNG NGHỆ THÔNG TIN

TÀI LIỆU HỌC TẬP
MẠNG MÁY TÍNH

Đối tượng: HSSV trình độ Đại học, Cao đẳng
Ngành đào tạo: Dùng chung cho Khối ngành Công nghệ

Lưu hành nội bộ

MỤC LỤC

MỤC LỤC	1
DANH MỤC HÌNH	6
DANH MỤC VIẾT TẮT	10
LỜI NÓI ĐẦU.....	13
CHƯƠNG 1. TỔNG QUAN VỀ MẠNG MÁY TÍNH	14
1.1. Sự hình thành và phát triển Mạng máy tính.	14
1.2. Các thành phần mạng máy tính.	16
1.2.1. Đường truyền vật lý	16
1.2.2. Kiến trúc mạng.	20
1.2.3. Giao thức mạng.	20
1.3. Phân loại mạng máy tính.	20
1.3.1 Phân loại mạng theo khoảng cách địa lý	20
1.3.2. Phân loại mạng theo topology	23
1.3.3. Phân loại mạng theo kỹ thuật chuyển mạch	25
1.4. Kiến trúc phân tầng và mô hình OSI.	28
1.4.1. Kiến trúc phân tầng	28
1.4.2. Các tổ chức tiêu chuẩn hóa mạng máy tính.....	29
1.4.3. Mô hình OSI	31
1.4.4. Mô hình TCP/IP	33
1.5. Xu hướng phát triển Mạng máy tính	34
CHƯƠNG 2. TẦNG VẬT LÝ	36
2.1. Vai trò chức năng tầng vật lý.....	36
2.2. Môi trường truyền thông	38
2.2.1. Kênh truyền hữu tuyến	38
2.2.2 Kênh truyền vô tuyến	40
2.2.3 Một số thiết bị cơ bản của lớp vật lý	40

2.3 Truyền tin tương tự.....	42
2.3.1. Hệ thống điện thoại	42
2.3.2. Modem.....	46
2.4. Truyền tín hiệu số.....	46
2.4.1. Điều chế xung mã -PCM (Pulse Code Modulation).....	47
2.4.2. Chuẩn X 21	47
Chương 3. TẦNG LIÊN KẾT DỮ LIỆU: CÁC LIÊN KẾT, TRUY CẬP MẠNG VÀ CÁC LAN	49
3.1 Giới thiệu về tầng Liên kết dữ liệu.....	49
3.1.1. Các dịch vụ tầng liên kết	51
3.1.2. Vị trí triển khai ở tầng liên kết	52
3.2. Kỹ thuật phát hiện và sửa lỗi.....	53
3.2.1. Kiểm tra Bit chẵn lẻ.....	53
3.2.2. Phương pháp kiểm tra (checksum).....	55
3.2.3. Phương pháp kiểm tra theo chu kỳ (CRC)	56
3.3. Đa liên kết truy cập và Các giao thức.....	56
3.3.1. Phương pháp chia kênh	57
3.3.2. Giao thức truy cập ngẫu nhiên.....	60
3.3.3. Phương pháp phân lượt truy cập đường truyền	65
3.4. Chuyển mạch trong LAN	70
3.4.1. Địa chỉ liên kết và ARP	71
3.4.2. Ethernet.....	74
3.4.3 Chuyển mạch trong LAN (LAN SWITCH)	76
3.4.4. Mạng LAN ảo VLAN.....	77
3.5. Liên kết ảo	79
Chương 4. TẦNG MẠNG	83
4.1. Giới thiệu về Tầng mạng	83
4.2. Mạch ảo và mạng gói dữ liệu	83

4.3. Các vấn đề về Định tuyến.....	85
4.4. Giao thức Internet: Chuyển tiếp và đánh địa chỉ trên Internet	87
4.4.1. Giao thức mạng IP (Internet Protocol)	87
4.4.2. Giao thức thông báo điều khiển mạng ICMP	92
4.4.3. Giao thức phân giải địa chỉ ARP	92
4.4.4. Giao thức phân giải địa chỉ ngược RARP	93
4.4.5. Giao thức IPv6 (Internet Protocol Version Number 6)	94
4.5. Các thuật toán định tuyến	98
4.5.1. Link state (định tuyến theo trạng thái đường liên kết)	98
4.5.2. Distance vector (định tuyến theo vector khoảng cách)	99
4.6. Định tuyến trên Internet.....	100
4.6.1. OSPF.....	100
4.6.2. Giao thức định tuyến RIP	116
4.7. Tổng kết và bài tập ứng dụng	125
4.7.1. Wireshark Lab : ICMP	125
4.7.2 Wireshark Lab : IP.....	129
Chương 5. TẦNG GIAO VẬN	136
5.1. Giới thiệu và các dịch vụ tầng Giao vận	136
5.1.1. Các giao thức chuẩn cho Tầng Vận chuyển	136
5.2. Các giao thức đa truy cập	137
5.2.1. Phương pháp chia kênh	137
5.2.2. Phương pháp truy cập đường truyền ngẫu nhiên	140
5.2.3. Phương pháp phân luợt truy cập đường truyền	145
5.3. Giao thức vận chuyển không liên kết: UDP	150
5.4. Nguyên tắc truyền dữ liệu tin cậy.....	151
5.5. Giao thức vận chuyển hướng kết nối:TCP	151
5.6. Nguyên tắc điều khiển xung đột.....	153
5.7. Tổng kết và bài tập ứng dụng	155

5.7.1. Wireshark Lab : TCP	155
5.7.2. Wireshark Lab : UDP	162
Chương 6. TẦNG ỨNG DỤNG.....	168
6.1. Nguyên tắc của các ứng dụng mạng	168
6.1.1. Mô hình khách/chủ	169
6.1.2. Mô hình ngang hàng (Peer to peer)	170
6.1.3. Mô hình lai (Hybrid)	170
6.2. Web và HTTP	170
6.2.2. Các thông điệp trả lời	172
6.2.3. Các kết nối TCP.....	173
6.2.4. Bộ lưu trữ đệm.....	174
6.3. Giao thức truyền file: FTP	174
6.3.1. Giao thức FTP	175
6.3.2. Các lệnh cơ bản	175
6.4. Thư điện tử trên Internet.....	176
6.4.1. Các thành phần của hệ thống email.....	176
6.4.2. Khuôn dạng của một email.....	177
6.4.3. Chuyển thư	179
6.4.4. Phân phát thư	181
6.5. Dịch vụ phân giải tên miền –DNS.....	184
6.5.1. Miền phân cấp	185
6.5.2. Các server phục vụ tên	185
6.5.3. Phương pháp phân tích tên	187
6.6. Ứng dụng mạng ngang hàng.....	189
6.7 Tổng kết và bài tập ứng dụng	191
6.7.1 Wireshark Lab : DNS	191
6.7.2 Wireshark Lab : HTTP	197
6.7.3 Wireshark Lab : DHCP	202
Chương 7. MẠNG KHÔNG DÂY VÀ MẠNG DI ĐỘNG	207

7.1. Mạng cục bộ không dây (WLAN - Wireless LAN)	207
7.1.1. Giới thiệu về WLAN	207
7.1.2. Lịch sử hình thành và phát triển	207
7.1.3. Cơ sở hạ tầng WLAN	209
7.1.4. Các mô hình WLAN.....	212
7.1.5. Các giải pháp bảo mật WLAN	214
7.2. Các Chuẩn không dây.....	221
7.2.1. IEEE 802.11b	223
7.2.2. IEEE 802.11a.....	223
7.2.3. IEEE 802.11g	224
7.2.4. IEEE 802.11n	227
7.3. Không dây dải tần rộng	227
7.3.1. Giới thiệu WiMax.....	227
7.3.2. Những vấn đề ở lớp Vật lý	228
7.3.3. Những vấn đề ở lớp MAC	229
7.4. Mạng Manet.....	229
7.5. Hệ thống GMS.....	231
7.6. Công nghệ 4G	234
7.7. Mobile IP	235
TÀI LIỆU THAM KHẢO.....	242

DANH MỤC HÌNH

Hình 1. 1 Mô hình mạng tổng quát.....	15
Hình 1. 2 Cấu trúc mạng LAN cơ bản.....	21
Hình 1. 3 Cấu trúc mạng MAN	22
Hình 1. 4 Cấu trúc mạng WAN	23
Hình 1. 5 Mạng hình sao	23
Hình 1. 6 Mạng tuyến tính.....	24
Hình 1. 7 Mạng vòng	25
Hình 1. 8 Mô hình chuyển mạch kênh	26
Hình 1. 9 Mô hình chuyển mạch thông báo	27
Hình 1. 10 Mô hình chuyển mạch gói	27
Hình 1. 11 Mô hình kiến trúc phân tầng.....	29
Hình 1. 12 Mô hình OSI	33
Hình 1. 13 Mô hình OSI và TCP/IP	34
Hình 2. 1 Môi trường thực của tầng vật lý	36
Hình 2. 2 Cáp xoắn đôi.....	38
Hình 2. 3 Cáp đồng trục	39
Hình 2. 4 Cấu trúc cáp quang	40
Hình 2. 5 Kênh truyền.....	40
Hình 2. 6 Thiết bị Repeater	41
Hình 2. 7 Bộ tập trung Hub	42
Hình 2. 8 (a) Mạng kết nối đầy đủ. (b) Công tắc tập trung. (c) Hệ thống phân cấp hai cấp.	43
Hình 2. 9 Một tuyến đường điển hình cho một cuộc gọi khoảng cách trung bình.....	45
Hình 2. 10 Bộ điều chế	46
Hình 3. 1 Sáu bước nhảy liên kết giữa máy chủ và thiết bị không dây.....	51
Hình 3. 2 Bộ điều phối	53
Hình 3. 3 Chắn lẻ một bit	54
Hình 3. 4 Bít chắn lẻ hai chiều	55
Hình 3. 5 Ví dụ về FDMA	57
Hình 3. 6 Ví dụ về Slotted ALOHA	61
Hình 3. 7 Ví dụ về Pure ALOHA	62
Hình 3. 8 Thời gian cần thiết để truyền một khung.....	64

Hình 3. 9 Mô tả các chu kỳ hoạt động của hệ thống thăm dò phân tán	66
Hình 3. 10 Mô hình hoạt động của mạng Token Ring	67
Hình 3. 11 Nhả Token Ring	68
Hình 3. 12 Sử dụng role	70
Hình 3. 13 Hệ thống kết nối mạng	71
Hình 3. 14 Địa chỉ MAC	72
Hình 3. 15 Giao thức ARP	74
Hình 3. 16 Các chuẩn Ethernet 100 Mbps.....	75
Hình 3. 17 Phân đoạn Mạng	76
Hình 3. 18 Mô hình mạng VLAN	78
Hình 3. 19 Tiêu đề MPLS.....	79
Hình 3. 20 VPN layer 3	80
Hình 4. 1 Mạng chuyển mạch gói	84
Hình 4. 2 Cấu trúc gói tin IP.....	88
Hình 4. 3 Cấu trúc các lớp địa chỉ IP	90
Hình 4. 4 Minh họa quá trình tìm địa chỉ MAC bằng ARP	93
Hình 4. 5 Minh họa quá trình tìm địa chỉ IP bằng giao thức RARP	94
Hình 4. 6 Bầu chọn router – id	101
Hình 4. 7 Bầu chọn router – id	102
Hình 4. 8 Các router gửi gói tin hello.....	104
Hình 4. 9 Kiến trúc phân vùng trong OSPF	105
Hình 4. 10 Trao đổi LSDB với kết nối point – to – point	107
Hình 4. 11 Broadcast MultiAccess	108
Hình 4. 12 Hoạt động trao đổi thông tin thông qua DR	108
Hình 4. 13 Đây là môi trường Multi – access dù chỉ có 02 router	109
Hình 4. 14 Sơ đồ ví dụ tính path – cost	111
Hình 4. 15 Tổng path – cost là 66 hay 129.....	111
Hình 4. 16 Các công tham gia vào tiến trình tính toán path – cost với OSPF	112
Hình 4. 17 Sơ đồ ví dụ cấu hình.....	112
Hình 4. 18 Sơ đồ ví dụ 1.....	117
Hình 4. 19 R3 gửi cho R2 bảng định tuyến của nó	118
Hình 4. 20 Bảng định tuyến của R2	118
Hình 4. 21 R2 gửi bảng định tuyến của nó cho R1	118

Hình 4. 22	Bảng định tuyến của R1	119
Hình 4. 23	Kết quả hội tụ cuối cùng của ví dụ 1	119
Hình 4. 24	Mạng 192.168.3.0/24 down.....	120
Hình 4. 25	Bảng định tuyến của R3	120
Hình 4. 26	Bảng định tuyến của R2	121
Hình 4. 27	Loop trong định tuyến	121
Hình 4. 28	R2 sẽ không gửi ngược thông tin nó học được từ R3 về cho R3	122
Hình 4. 29	Route poisoning và Poison reverse	122
Hình 4. 30	Sơ đồ ví dụ 2.....	123
Hình 4. 31	Mạng 192.168.3.0/24 down.....	124
Hình 4. 32	Sơ đồ xảy ra loop.....	124
Hình 5. 1	Ví dụ về FDMA	137
Hình 5. 2	Ví dụ về Slotted ALOHA	141
Hình 5. 3	Ví dụ về Pure ALOHA.....	142
Hình 5. 4	Thời gian cần thiết để truyền một khung.....	144
Hình 5. 5	Mô tả các chu kỳ hoạt động của hệ thống thăm dò phân tán	146
Hình 5. 6	Mô hình hoạt động của mạng Token Ring.....	147
Hình 5. 7	Nhả Token Ring	148
Hình 5. 8	Sử dụng role	149
Hình 5. 9	Cấu trúc gói tin UDP	150
Hình 5. 10	Cấu trúc gói tin TCP (TCP Segment).....	152
Hình 5. 11	Quá trình thiết lập và kết thúc liên kết TCP 3 bước	154
Hình 6. 1	<i>Trình duyệt Web Internet Explorer</i>	170
Hình 6. 2	<i>Truyền dữ liệu.....</i>	175
Hình 6. 3	<i>Hệ thống Email.....</i>	176
Hình 6. 4	Quá trình phân giải tên trong thực tế, các số 1 đến 8 chỉ ra trình tự thực hiện	189
Hình 7. 1	Cấu trúc cơ bản của WLAN	209
Hình 7. 2	Thiết bị Wireless accesspoint	210
Hình 7. 3	AP hoạt động ở root mode.....	210
Hình 7. 4	Chế độ cầu nối của AP	211
Hình 7. 5	Chế độ Repeater của AP	211
Hình 7. 6	Thiết bị Wireless Router.....	212
Hình 7. 7	Wireless NICs.....	212

Hình 7. 8 Mô hình mạng Ad-hoc.....	213
Hình 7. 9 Mô hình mạng BSS chuẩn	213
Hình 7. 10 Mô hình mạng ESS.....	214
Hình 7. 11 Mô hình WLAN VPN	215
Hình 7. 12 Mô hình hoạt động xác thực 802.1x.....	216
Hình 7. 13 Tiết trình xác thực MAC	219
Hình 7. 14 Lọc giao thức	220
Hình 7. 15 Escalating Security	221
Hình 7. 16 CCK và OFDM trong 802.11g; CCK – OFDM và PBCC	225
Hình 7. 17 Lược đồ điều biến 802.11g và tương ứng với tốc độ dữ liệu	226

DANH MỤC VIẾT TẮT

Tên viết tắt	Nội dung
IT (Information Technology)	Công nghệ về máy tính.
PC (Personal Computer)	Máy tính cá nhân.
ICT(Information Communication Technology)	Ngành công nghệ thông tin - truyền thông.
CPU (Central Processing Unit)	Đơn vị xử lý trung tâm trong máy tính.
OS (Operating System)	Hệ điều hành máy tính.
BPS (Bits Per Second)	Số bít truyền trên mỗi giây.
ROM (Read Only Memory)	Bộ nhớ chỉ đọc, không thể ghi - xóa.
RAM (Random Access Memory)	Bộ nhớ truy cập ngẫu nhiên.
HDD (Hard Disk Drive)	Ô Đĩa cứng - là phương tiện lưu trữ chính.
Modem (Modulator/Demodulator)	Điều chế và giải điều chế - chuyển đổi qua lại giữa tín hiệu Digital và Analog.
DAC (Digital to Analog Converted)	Bộ chuyển đổi từ tín hiệu số sang tín hiệu Analog.
NTFS (New Technology File System)	Hệ thống tập tin theo công nghệ mới - công nghệ bảo mật hơn dựa trên nền tảng là Windows NT.
FAT (File Allocation Table)	Một bảng hệ thống trên đĩa để cấp phát File.
SAM (Security Account Manager)	Noi quản lý và bảo mật các thông tin của tài khoản người dùng.
HT (Hyper Threading)	Công nghệ siêu phân luồng.
S/P (Supports)	Sự hỗ trợ.
PNP (Plug And Play)	Cắm và chạy.
IEEE (Institute of Electrical and Electronics Engineers)	Viện kỹ thuật Điện và Điện Tử.
OSI (Open System Interconnection)	Mô hình liên kết hệ thống mở - chuẩn hóa quốc tế.
Wi - Fi (Wireless Fidelity)	Kỹ thuật mạng không dây.

Tên viết tắt	Nội dung
LAN (Local Area Network)	Mạng máy tính cục bộ.
WAN (Wide Area Network)	Mạng máy tính diện rộng.
NIC (Network Interface Card)	Card giao tiếp mạng.
UTP (Unshielded Twisted Pair)	Cáp xoắn đôi - dùng để kết nối mạng thông qua đầu nối RJ45.
STP (Shielded Twisted Pair)	Cáp xoắn đôi có vỏ bọc.
BNC (British Naval Connector)	Đầu nối BNC dùng để nối cáp đồng trục.
ADSL (Asymmetric Digital Subscriber Line)	Đường thuê bao bát đối xứng - kết nối băng thông rộng.
TCP/IP (Transmission Control Protocol/Internet Protocol)	Giao thức điều khiển truyền/ giao thức Internet
IP (Internet Protocol)	Giao thức giao tiếp mạng Internet.
DHCP (Dynamic Host Configuration Protocol)	Hệ thống giao thức cấu hình IP động.
DNS (Domain Name System)	Hệ thống phân giải tên miền thành IP và ngược lại.
RIS (Remote Installation Service)	Dịch vụ cài đặt từ xa thông qua LAN.
ARP (Address Resolution Protocol)	Giao thức chuyển đổi từ địa chỉ Logic sang địa chỉ vật lý.
ICS (Internet Connection Sharing)	Chia sẻ kết nối Internet.
MAC (Media Access Control)	Khả năng kết nối ở tầng vật lý.
ISP (Internet Service Provider)	Nhà cung cấp dịch vụ Internet.
WWW (World Wide Web)	Hệ thống Web diện rộng toàn cầu.
HTTP (Hyper Text Transfer Protocol)	Giao thức truyền tải File dưới dạng siêu văn bản.
URL (Uniform Resource Locator)	Dùng để định nghĩa một Website, là đích của một liên kết.
FTP (File Transfer Protocol)	Giao thức truyền tải File.
E_Mail (Electronic Mail)	Hệ thống thư điện tử.
POP (Post Office Protocol)	Giao thức văn phòng, dùng để nhận Mail

Tên viết tắt	Nội dung
	từ Mail Server.
SMTP (Simple Mail Transfer Protocol)	Giao thức dùng để gửi Mail từ Mail Client đến Mail Server.
ISA Server (Internet Security & Acceleration Server)	Chương trình hỗ trợ quản lý và tăng tốc kết nối Internet dành cho Server.
SQL (Structured Query Language)	Ngôn ngữ truy vấn cấu trúc - kết nối đến CSDL.
IE (Internet Explorer)	Trình duyệt Web “Internet Explorer” của Microsoft.
CCNA (Cisco Certified Network Associate)	Là chứng chỉ mạng quốc tế do hãng sản xuất thiết bị mạng thế giới - Cisco – cấp, và được công nhận trên toàn thế giới.
CCNP (Cisco Certified Network Professional)	Là chứng chỉ mạng cao cấp của Cisco.
MCP (Microsoft Certified Professional)	Là chứng chỉ ở cấp độ đầu tiên của Microsoft.
MCSA (Microsoft Certified Systems Administrator)	Chứng chỉ dành cho người quản trị hệ điều hành mạng của Microsoft, được chính Bill Gate ký.
MCSE (Microsoft Certified Systems Engineer)	Là kỹ sư mạng được Microsoft chứng nhận
WLAN (wireless LAN)	Là mạng LAN không dây, kết nối các thiết bị với nhau bằng phương thức truyền theo dạng không dây
AC (Access Point)	Điểm truy cập dữ liệu không dây
VPN (Virtual Private Network)	Mạng riêng ảo
PDU (Protocol Data Unit)	Đơn vị dữ liệu giao thức

LỜI NÓI ĐẦU

Cùng với sự phát triển của khoa học và kỹ thuật, Công nghệ thông tin ở nước ta trong những năm gần đây phát triển rất mạnh. Mạng máy tính cũng đã phát triển một cách nhanh chóng và đa dạng cả về quy mô, hệ điều hành và ứng dụng. Do nhu cầu và trình độ cao, những người hoạt động chuyên ngành Công nghệ thông tin cần luôn phải nâng cao trình độ để đáp ứng. Tuy nhiên, các mạng máy tính cũng có cùng các điểm chung thông qua đó chúng ta có thể khảo sát, phân loại và đánh giá chúng.

Để đáp ứng với yêu cầu học tập của sinh viên chuyên ngành công nghệ thông tin, Trường Đại học Kinh tế - Kỹ thuật Công nghiệp tổ chức biên soạn Tài liệu học tập “Mạng máy tính”. Đây là một học phần cơ sở của sinh viên chuyên ngành Đại học và Cao đẳng Công nghệ thông tin. Học phần cung cấp cho sinh viên những kiến thức cơ bản và chuyên sâu về hệ thống mạng máy tính, trang bị cho sinh viên những kỹ năng thiết kế, cấu hình và quản trị hệ thống mạng. Đây có thể xem là những kiến thức nền tảng cho các quản trị viên về hệ thống mạng máy tính. Tài liệu học tập được biên soạn theo đúng chương trình đào tạo và các quy định về cách trình bày của Nhà trường.

Nội dung của bài giảng bao gồm 07 chương:

Chương 1: Tổng quan về mạng máy tính. Khái niệm cơ bản về kiến trúc và các giao thức mạng, các loại mạng máy tính và mục tiêu ứng dụng của nó.

Chương 2: Tầng vật lý. Tìm hiểu về các phương tiện điện, cơ, chức năng thủ tục để kích hoạt, duy trì và hủy bỏ kết nối Vật lý giữa các hệ thống.

Chương 3: Tầng liên kết dữ liệu. Tìm hiểu các liên kết, duy trì và hủy bỏ các liên kết dữ liệu. Kiểm soát lỗi và kiểm soát lưu lượng.

Chương 4: Tầng mạng. Hiểu về chọn đường và chuyển tiếp. Ngoài hai chức năng quan trọng trên tầng mạng cũng thực hiện một số chức năng khác như: Thiết lập, duy trì và giải phóng các liên kết logic, kiểm soát lỗi, kiểm soát luồng dữ liệu, dồn kenh/phân kenh, cắt/hợp dữ liệu.

Chương 5: Tầng giao vận. Tìm hiểu việc truyền dữ liệu giữa 2 đầu mút, kiểm soát lỗi, kiểm soát luồng dữ liệu giữa 2 đầu mút, việc ghép kenh/cắt/hợp dữ liệu nếu cần.

Chương 6: Tầng ứng dụng. Cung cấp các phương tiện để người sử dụng có thể truy cập được vào môi trường OSI, đồng thời cung cấp các dịch vụ thông tin phân tán.

Chương 7: Mạng không dây và mạng di động. Tìm hiểu về cơ chế và các chuẩn về mạng không dây

Mong rằng nội dung Tài liệu học tập sẽ giúp cho sinh viên những kiến thức cần thiết, làm cơ sở để có thể đi sâu vào thiết kế, làm chủ mạng máy tính.

Xin chân thành cảm ơn!

CHƯƠNG 1. TỔNG QUAN VỀ MẠNG MÁY TÍNH

Mục đích:

Ngày nay, nhu cầu sử dụng máy tính không ngừng được tăng lên về cả số lượng và ứng dụng, đặc biệt là sự phát triển hệ thống mạng máy tính, kết nối các máy tính lại với nhau thông qua môi trường truyền tin để cùng nhau chia sẻ tài nguyên trên mạng góp phần làm tăng hiệu quả của các ứng dụng trong tất cả các lĩnh vực khoa học kỹ thuật, kinh tế, quân sự, văn hóa.... Sự kết hợp của máy tính với hệ thống truyền thông (communication) đặc biệt là viễn thông (telecommunication) đã tạo ra một sự chuyển biến có tính cách mạng trong vấn đề tổ chức khai thác và sử dụng các hệ thống máy tính. Từ đó đã hình thành các môi trường trao đổi thông tin tập trung, phân tán, cho phép đồng thời nhiều người cùng trao đổi thông tin với nhau một cách nhanh chóng và hiệu quả từ những vị trí địa lý khác nhau. Các hệ thống như thế được gọi là mạng máy tính (computer networks).

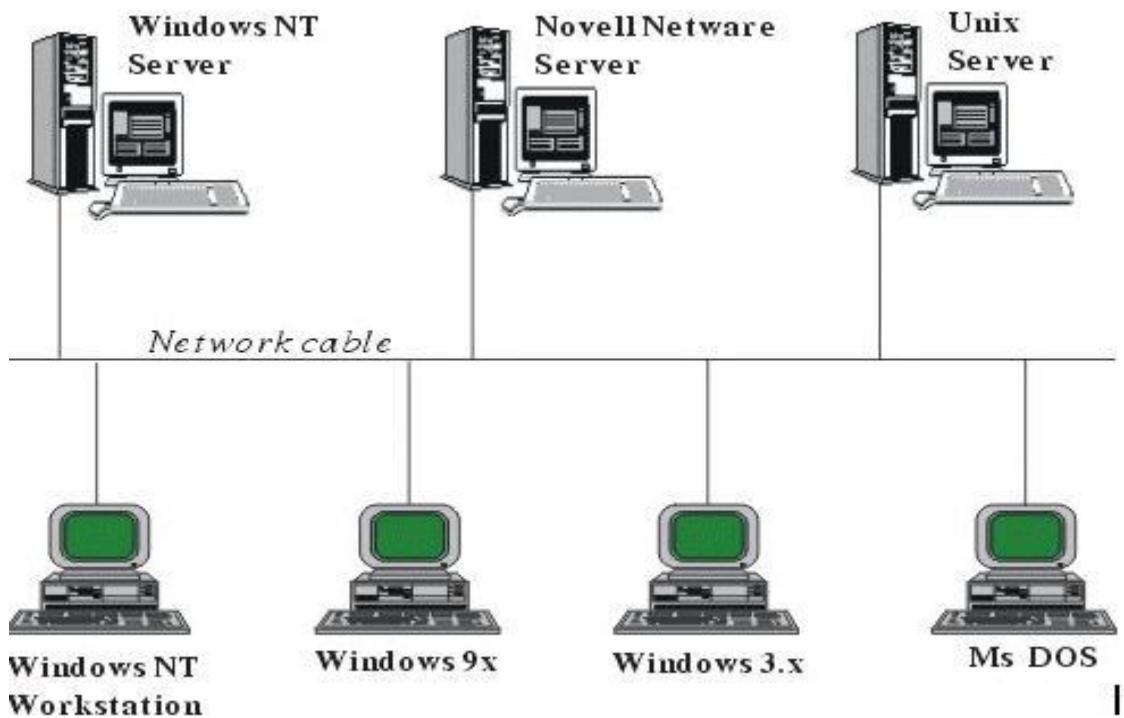
Mạng máy tính trở thành lĩnh vực nghiên cứu, phát triển rất quan trọng bảo đảm truyền tin đáng tin cậy, chính xác, phù hợp tốc độ và đảm bảo an toàn thông tin trên mạng.

1.1. Sự hình thành và phát triển Mạng máy tính.

Trước những năm 1970 đã bắt đầu hình thành các máy tính nối với nhau thành mạng và các thiết bị đầu cuối dữ liệu đã kết nối trực tiếp vào máy tính trung tâm để tận dụng tài nguyên chung, khai thác dữ liệu, giảm giá thành truyền số liệu, sử dụng tiện lợi và nhanh chóng hơn. Cùng với thời gian xuất hiện các máy tính Mini Computer và máy tính cá nhân (Personal Computer) đã tăng yêu cầu truyền số liệu giữa máy tính - trạm đầu cuối (Terminal) và ngược lại hình thành nhiều mạng cục bộ, mạng diện rộng trong phạm vi lớn. Do đó mạng máy tính ngày càng được phát triển để đáp ứng với nhu cầu của người sử dụng. Sự hình thành của mạng máy tính được mô tả như sau:

Ban đầu là sự kết nối các thiết bị đầu cuối trực tiếp đến máy tính lớn, tiếp theo do sự phát triển ngày càng nhiều các trạm nên chúng được kết nối thành từng nhóm qua bộ tập trung rồi nối đến máy chủ trung tâm. Trong giai đoạn này máy tính trung tâm có chức năng quản lý truyền tin qua các tám ghép nối điều khiển cứng đó để tăng sức mạnh quản lý toàn hệ thống trước khi dữ liệu được đưa đến máy tính trung tâm người ta thay thế các tám ghép nối, quản lý đường truyền bằng máy tính MINI. Bộ tiền xử lý gắn chặt với trung tâm, các xử lý ngoại vi đưa vào máy chủ trong những trạm đầu cuối thông minh.

Trong giai đoạn cuối đưa vào mạng truyền tin cho phép xây dựng mạng máy tính rộng lớn .



Hình 1. 1 Mô hình mạng tổng quát

Mạng truyền tin bao gồm các nút truyền tin và các đường dây truyền tin nối giữa các nút để đảm bảo vận chuyển tin. Các thiết bị đầu cuối, thiết bị tập trung, bộ tiền xử lý và các máy tính được ghép nối vào các nút mạng.

Trong giai đoạn này xuất hiện các trạm đầu cuối thông minh mà nó ngày càng liên kết với các máy Mini.

Chức năng của máy tính trung tâm:

- Xử lý các chương trình ứng dụng, phân chia tài nguyên và ứng dụng.
- Quản lý hàng đợi và các trạm đầu cuối.

Chức năng của bộ tiền xử lý :

- Điều khiển mạng truyền tin (Đường dây, cất giữ tập tin, trạm đầu cuối)
- Điều khiển chuyển ký tự lên đường dây, bổ sung hay bỏ đi những ký tự đồng bộ.

Chức năng của bộ tập trung: Quản lý truyền tin, các đầu cuối. Tiền xử lý, lưu trữ số liệu, điều khiển giao dịch.

Chức năng của thiết bị đầu cuối:

- Quản lý truyền tin, thủ tục truyền tin, ghép nối với người sử dụng.
- Điều khiển truy nhập số liệu và lưu trữ số liệu.

Do số lượng các trạm đầu cuối ngày càng tăng, nếu nối trực tiếp với máy tính trung tâm, tốn vật liệu nối ghép, quản lý nặng nề, không tương xứng với nhiệm vụ của máy tính, hiệu suất thấp nên đưa ra bộ tập trung để khắc phục những nhược điểm trên.

Tóm lại, việc kết nối các máy tính thành mạng nhằm vào các mục đích chính sau:

- Tận dụng tài nguyên chung, chinh phục khoảng cách.
- Tăng chất lượng hiệu quả khai thác, xử lý thông tin và độ tin cậy của hệ thống.

1.2. Các thành phần mạng máy tính.

1.2.1. Đường truyền vật lý

Đường truyền vật lý dùng để chuyển các tín hiệu điện tử giữa các máy tính. Tất cả các tín hiệu đó biểu thị các dữ liệu dưới dạng xung nhị phân.

Có hai loại đường truyền: Hữu tuyến (cable), vô tuyến (wireless) được sử dụng trong việc kết nối mạng. Đường truyền hữu tuyến gồm có cáp đồng trục, cáp xoắn đôi, cáp sợi quang, đường truyền vô tuyến gồm có: sóng Radio, sóng cực ngắn (viba), tia hồng ngoại (infrared).

Tất cả các tín hiệu truyền giữa các máy tính có dạng sóng điện từ và có tần số trải từ tần số cực ngắn đến tia hồng ngoại. Tùy theo tần số của sóng điện từ mà có thể dùng các đường truyền vật lý khác nhau để truyền. Đường truyền vật lý có những đặc trưng cơ bản sau: Giải thông, độ suy hao, độ nhiễu từ.

+ **Băng thông** (*bandwidth*) của đường truyền là độ đo phạm vi tần số mà nó có thể đáp ứng được. Băng thông của một đường truyền là miền tần số giới hạn thấp và tần số giới hạn cao, tức là miền tần số mà đường truyền đó có thể đáp ứng được. Ví dụ băng thông của cáp thoại từ 400 đến 4000 Hz, có nghĩa là nó có thể truyền các tín hiệu với tần số từ 400 đến 4000 chu kỳ/giây. Băng thông của cáp phụ thuộc vào chiều dài của cáp. Cáp ngắn băng thông cao và ngược lại. Vì vậy khi thiết kế lắp đặt cáp, chiều dài cáp sao cho không vượt qua giới hạn cho phép, vì có thể xảy ra lỗi trong quá trình truyền.

+ **Thông lượng** (*throughput*) Thông lượng của đường truyền là số lượng các bit (chuỗi bit) được truyền đi trong một giây. Hay nói cách khác là tốc độ của đường truyền dẫn. Ký hiệu là bit/s hoặc bps. Tốc độ của đường truyền phụ thuộc vào băng thông và độ dài của nó.

+ **Độ suy hao** (*Attenuation*) là độ đo độ suy yếu của tín hiệu trên đường truyền. Cáp càng dài thì độ suy hao càng lớn. Suy hao phụ thuộc vào độ dài của cáp, cáp càng dài thì suy hao càng cao. Khi thiết kế cáp cũng rất cần quan tâm đến giới hạn chiều dài cho phép của từng loại cáp.

+ **Độ nhiễu điện từ** làm nhiễu tín hiệu trên đường truyền.

1.2.1.1. Các loại cáp mạng

Cáp đồng trục (Coaxial cable): Là phương tiện truyền các tín hiệu có phô rộng và tốc độ cao. Băng thông của cáp đồng trục từ 2,5 Mbps (ARCnet) đến 10 Mbps (Ethernet). Thường sử dụng để lắp đặt mạng hình BUS (các loại mạng LAN cục bộ Thick Ethernet, Thin Ethernet) và mạng hình sao (mạng ARCnet).

Cáp đồng trục gồm: một dây dẫn trung tâm, một dây dẫn ngoài, tạo nên đường ống bao quanh trục, lớp cách điện giữa 2 dây dẫn và cáp vỏ bọc ngoài.

Các loại cáp đồng trục:

- Cáp RC-8 và RCA-11, 50 Ohm dùng cho mạng Thick Ethernet.
- Cáp RC-58 , 50 Ohm dùng cho mạng Thin Ethernet.
- Cáp RG-59 , 75 Ohm dùng cho truyền hình cáp.
- Cáp RC-62, 93 Ohm dùng cho mạng ARCnet.

Cáp xoắn đôi (Twisted Pair cable): Cáp xoắn đôi được sử dụng trong các mạng LAN cục bộ. Giá thành rẻ, dễ cài đặt, có vỏ bọc tránh nhiệt độ, độ ẩm và có loại có khả năng chống nhiễu STP (Shield Twisted Pair). Cáp cơ bản có 2 dây đồng xoắn vào nhau, giảm độ nhạy của cáp với EMI, giảm bức xạ âm nhiễu tần số radio gây nhiễu.

Các loại cáp xoắn:

- Cáp có màng chắn (STP): Loại cáp STP thường có tốc độ truyền vào khoảng 16 Mbps trong loại mạng Token Ring. Với chiều dài 100 m tốc độ đạt 155 Mbps (lý thuyết là 500 Mbps). Suy hao cho phép khoảng 100 m, đặc tính EMI cao. Giá thành cao hơn cáp Thin Ethernet, cáp xoắn trần, nhưng lại rẻ hơn giá thành loại cáp Thick Ethernet hay cáp sợi quang. Cài đặt đòi hỏi tay nghề và kỹ năng cao.

- Loại cáp không có vỏ bọc UTP (Unshielded Twisted Pair): Cáp trần không có khả năng chống nhiễu, tốc độ truyền khoảng 100 Mbps. Đặc tính suy hao như cáp đồng, giới hạn độ dài tối đa 100m. Do thiếu màng chắn nên rất nhạy cảm với EMI, không phù hợp với môi trường các nhà máy. Được dùng phổ biến cho các loại mạng, giá thành hạ, dễ lắp đặt.

Cáp sợi quang (Fiber Optic Cable): rất lý tưởng cho việc truyền dữ liệu, băng thông có thể đạt 2 Gbps, tránh nhiễu tốt, tốc độ truyền 100 Mbps trên đoạn cáp dài vài km. Cáp sợi quang gồm một hoặc nhiều sợi quang trung tâm được bao bọc bởi một lớp vỏ nhựa phản xạ các tín hiệu trở lại, vì vậy hạn chế sự suy hao, mất mát tín hiệu. Cáp sợi quang chỉ truyền các tín hiệu quang. Các tín hiệu dữ liệu được biến đổi thành các tín hiệu quang trên đường truyền và khi nhận, các tín hiệu quang chuyển thành các tín hiệu dữ liệu. Cáp sợi quang hoạt động một trong hai chế độ: chế độ đơn (Single Mode) và đa chế độ (Multi Mode). Cài đặt cáp sợi quang đòi hỏi phải có kỹ năng cao, quy trình khó và phức tạp.

1.2.1.2. Các phương tiện vô tuyến.

Radio: Quang phổ của điện từ nằm trong khoảng 10 KHz đến 1GHz. Có nhiều dải tần: Sóng ngắn (Short Wave), VHF (Very High Frequency)-Tivi & Radio FM và UHF (Ultra High Frequency)-Tivi.

Đặc tính truyền: tần số đơn, công suất thấp không hỗ trợ tốc độ dữ liệu các mạng cục bộ LAN yêu cầu. Tần số đơn, công suất cao dễ cài đặt, băng thông cao từ 1 - 10 Mbps, suy hao chậm. Khả năng nhiễu từ thấp, bảo mật kém. Giá thành cao trung bình.

Radio quang phô trai (Spread spectrum) độ tin cậy cao, bảo mật dữ liệu. Băng thông cao, tốc độ truyền có thể đạt theo yêu cầu của các mạng cục bộ.

Viba: Truyền thông viba có hai dạng: Viba mặt đất và vệ tinh. Viba mặt đất sử dụng các trạm thu và phát. Kỹ thuật truyền thông vệ tinh sử dụng các trạm thu mặt đất (các đĩa vệ tinh) và các vệ tinh. Tín hiệu đến vệ tinh và từ vệ tinh đến trạm thu một lượt đi hoặc về 23.000 dặm. Thời gian truyền một tín hiệu độc lập với khoảng cách. Thời gian truyền tín hiệu từ vệ tinh đến các trạm nằm vòng tròn 1/3 chu vi quả đất là như nhau, gọi là trễ lan truyền (Propagation Delay). Thông thường là 0,5-5 giây.

Tia hồng ngoại (Infrared system): Có 2 phương thức kết nối mạng Point - to - Point và Multi Point. Point – to - Point tiếp sóng các tín hiệu hồng ngoại từ thiết bị này sang thiết bị khác. Giải tần từ 100 GHz đến 1000 THz, tốc độ truyền khoảng 100 Kbps - 16 Mbps. Multi Point truyền đồng thời các tín hiệu hồng ngoại đến các thiết bị. Giải tần số từ 100 GHz đến 1000 THz, nhưng tốc độ truyền chỉ đạt tối đa 1 Mbps.

1.2.1.3. Các thiết bị kết nối

- Wireless Access Point là thiết bị kết nối mạng không dây được thiết kế theo chuẩn IEEE 802.11b, cho phép nối LAN to LAN, dùng cơ chế CSMA/CA để giải quyết tranh chấp, dùng cả hai kiến trúc kết nối mạng là Infrastructure và AdHoc, mã hóa theo 64/128 bit. Nó còn hỗ trợ tốc độ truyền không dây lên tới 11Mbps trên băng tần 2,4 GHz và dùng công nghệ radio DSSS (Direct Sequence Spectrum Spreading).

- Wireless Ethernet Bridge là thiết bị cho phép các thiết bị Ethernet kết nối vào mạng không dây. Ví dụ như thiết bị Linksys WET54G Wireless-G Ethernet Bridge. Nó hỗ trợ bất kỳ thiết bị Ethernet nào kết nối vào mạng không dây dù thiết bị Ethernet đó có thể là một thiết bị đơn hoặc một router kết nối đến nhiều thiết bị khác.

- Card mạng là một loại card mở rộng được gắn thêm trên máy tính, cung cấp giao tiếp vật lý và logic giữa máy tính với các thiết bị mạng, hệ thống mạng thông qua phương tiện truyền dẫn.

- Repeater đơn giản chỉ là một bộ khuếch đại tín hiệu giữa hai cổng của hai phân đoạn mạng. Repeater được dùng trong mô hình mạng Bus nhằm mở rộng khoảng cách tối đa trên một đường cáp. Có hai loại Repeater đang được sử dụng là Repeater điện và Repeater điện quang. Dùng để nối hai mạng có cùng giao thức truyền thông

- Hub là thiết bị có chức năng giống như Repeater nhưng nhiều cổng giao tiếp hơn cho phép nhiều thiết bị mạng kết nối tập trung với nhau tại một điểm. Hub thông thường có từ 4 đến 24 cổng giao tiếp, thường sử dụng trong những mạng Ethernet 10BaseT. Thật ra, Hub chỉ là Repeater nhiều cổng. Hub lặp lại bất kỳ tín hiệu nào nhận được từ một cổng bất kỳ và gửi tín hiệu đó đến tất cả các cổng còn lại trên nó. Hub hoạt động ở lớp vật lý của mô hình OSI và cũng không lọc được dữ liệu. Hub thường được dùng để nối mạng, thông qua những đầu cắm của nó người ta liên kết với các máy tính dưới dạng

hình sao. Hub được chia làm hai loại chính: Hub thụ động (Passive hub) và Hub chủ động (Active hub).

- Bridge là thiết bị cho phép nối kết hai nhánh mạng, có chức năng chuyển có chọn lọc các gói tin đến nhánh mạng chứa máy nhận gói tin. Để lọc các gói tin và biết được gói tin nào thuộc nhánh mạng nào thì Bridge phải chứa bảng địa chỉ MAC. Bảng địa chỉ này có thể được khởi tạo tự động hay phải cấu hình bằng tay. Do Bridge hiểu được địa chỉ MAC nên Bridge hoạt động ở tầng hai (tầng data link) trong mô hình OSI.

- Modem là thiết bị dùng để chuyển đổi dữ liệu định dạng số thành dữ liệu định dạng tương tự cho một quá trình truyền từ môi trường tín hiệu số qua môi trường tín hiệu tương tự và sau đó trở môi trường tín hiệu số ở phía nhận cuối cùng. Tên gọi Modem thật ra là từ viết tắt được ghép bởi những chữ cái đầu tiên của Modulator/DEModulator – Bộ điều biến/Bộ giải điều biến.

- Switch là sự kết hợp hài hòa về kỹ thuật giữa Bridge và Hub. Cơ chế hoạt động của Switch rất giống Hub bởi vì là thiết bị tập trung các kết nối mạng lại trên nó. Những cổng giao tiếp trên Switch là những Bridge thu nhỏ được xây dựng trên mỗi cổng giao tiếp tương ứng.

- Router là bộ định tuyến dùng để nối kết nhiều phân đoạn mạng, hay nhiều kiểu mạng (thường là không đồng nhất về kiến trúc và công nghệ) vào trong cùng một mạng tương tác. Thông thường có một bộ xử lý, bộ nhớ, và hai hay nhiều cổng giao tiếp ra/vào.

- Gateway là thiết bị trung gian dùng để nối kết những mạng khác nhau cả về kiến trúc lẫn môi trường mạng. Gateway được hiểu như cổng ra vào chính của một mạng nội bộ bên trong kết nối với mạng khác bên. Có thể đó là thiết bị phần cứng chuyên dụng nhưng thường là một server cung cấp kết nối cho các máy mà nó quản lý đi ra bên ngoài giao tiếp với một mạng khác.

- Máy chủ (Server)

Máy chủ (Server) là: một máy tính được kết nối với một mạng máy tính hoặc internet, có IP tĩnh, có năng lực xử lý cao và trên đó người ta cài đặt các phần mềm để phục vụ cho các máy tính khác truy cập để yêu cầu cung cấp các dịch vụ và tài nguyên.

- Máy trạm (Client)

Máy trạm có thể là bất cứ thiết bị gì thuộc nhóm máy tính cá nhân, máy tính xách tay, máy tính bảng, điện thoại thông minh có thể kết nối tới máy chủ thông qua mạng.

1.2.1.4. Các đơn vị đo.

- Bps (Bits per second-số bit trong một giây): đây là đơn vị cơ bản của băng thông.
- KBps (Kilobits per second): $1 \text{ KBps} = 103 \text{ bps} = 1000 \text{ Bps}$
- MBps (Megabits per second): $1 \text{ MBps} = 103 \text{ KBps}$
- GBps (Gigabits per second): $1 \text{ GBps} = 103 \text{ MBps}$

- TBps (Terabits per second): 1 TBps = 103 GBPS.

1.2.2. Kiến trúc mạng.

Kiến trúc mạng máy tính là thể hiện cách nối ghép các máy tính với nhau như thế nào và tập hợp các quy tắc, quy ước mà tất cả các thực thể tham gia truyền thông trên mạng phải tuân theo để đảm bảo mạng hoạt động tốt. Cách nối các máy tính được gọi là hình trạng (topology) của mạng.

*** Topo mạng:**

Có hai kiểu nối mạng chủ yếu là *điểm - điểm* (*point - to - point*) và *quảng bá* (*broadcast hay point - to - multipoint*).

Theo kiểu *điểm - điểm*, các đường truyền nối từng cặp nút với nhau và mỗi nút đều có trách nhiệm lưu trữ tạm thời sau đó chuyển tiếp dữ liệu đi cho tới đích. Do cách thức làm việc như thế nên mạng kiểu này còn được gọi là mạng “*Lưu và chuyển tiếp*” (*store and forward*).

Theo kiểu *quảng bá*, tất cả các nút phân chia chung một đường truyền vật lý. Dữ liệu được gửi đi từ một nút nào đó sẽ có thể được tiếp nhận bởi tất cả các nút còn lại, bởi vậy cần chỉ ra địa chỉ đích của dữ liệu để mỗi nút căn cứ vào đó kiểm tra xem dữ liệu có phải dành cho mình hay không.

1.2.3. Giao thức mạng.

Việc trao đổi thông tin, cho dù là đơn giản nhất, cũng đều phải tuân theo những quy tắc nhất định. Việc truyền tín hiệu trên mạng cần phải có những quy tắc, quy ước về nhiều mặt, từ khuôn dạng (cú pháp, ngữ nghĩa) của dữ liệu cho tới các thủ tục gửi, nhận dữ liệu, kiểm soát hiệu quả, chất lượng truyền tin và xử lý các lỗi. Yêu cầu về xử lý và trao đổi thông tin của người sử dụng càng cao thì các quy tắc càng nhiều và phức tạp hơn. Tập hợp tất cả những quy tắc, quy ước đó được gọi là giao thức (*Protocol*) của mạng. Rõ ràng là các mạng có thể sử dụng các giao thức khác nhau tùy sự lựa chọn của người thiết kế, tuy nhiên các tổ chức chuẩn quốc tế đã đưa ra một số giao thức chuẩn được dùng trong nhiều mạng khác nhau để thuận lợi cho việc kết nối chung.

1.3. Phân loại mạng máy tính.

Có nhiều cách phân loại mạng khác nhau tùy theo yếu tố chính được chọn để làm chỉ tiêu phân loại.

1.3.1 Phân loại mạng theo khoảng cách địa lý

Hiện nay, mạng máy tính được phát triển khắp nơi với những ứng dụng ngày càng đa dạng nên việc phân loại mạng máy tính là một việc rất phức tạp. Người ta có thể chia các mạng máy tính theo khoảng cách địa lý ra làm các loại mạng sau:

Mạng cục bộ LAN (Local Area Networks):

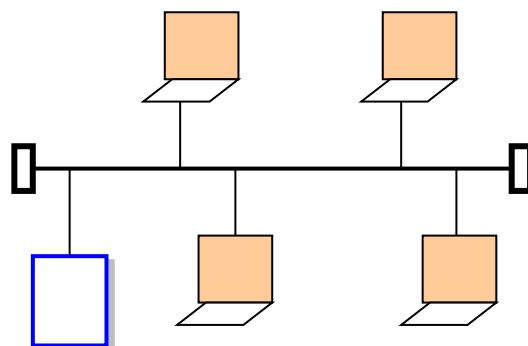
Mạng cục bộ LAN: kết nối các máy tính đơn lẻ thành mạng nội bộ, tạo khả năng trao đổi thông tin và chia sẻ tài nguyên trong cơ quan, xí nghiệp... Có hai loại

mạng LAN khác nhau: LAN nối dây (sử dụng các loại cáp) và LAN không dây (sử dụng sóng cao tần hay tia hồng ngoại). Đặc trưng cơ bản của mạng cục bộ:

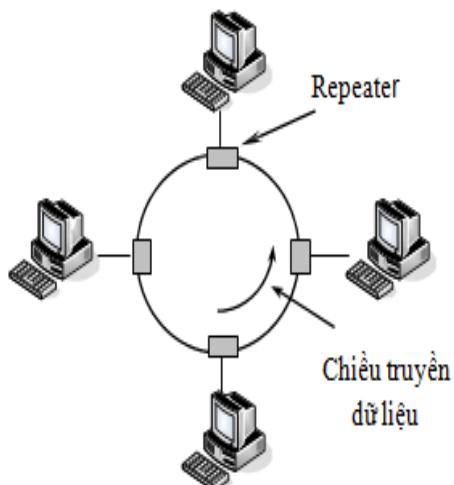
Quy mô của mạng nhỏ, phạm vi hoạt động vào khoảng vài km. Các máy trong một tòa nhà, một cơ quan hay xí nghiệp nối lại với nhau. Quản trị và bảo dưỡng mạng đơn giản.

Công nghệ truyền dẫn sử dụng trong mạng LAN thường là quảng bá (Broadcast), bao gồm một cáp đơn nối tất cả các máy. Tốc độ truyền dữ liệu cao, từ $10\text{--}100$ Mbps đến hàng trăm Gbps, thời gian trễ nhỏ (cỡ $10\mu\text{s}$), độ tin cậy cao, tỷ số lỗi bit từ 10^{-8} đến 10^{-11} .

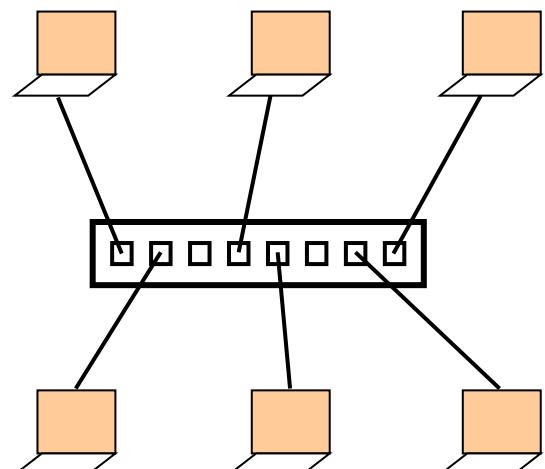
Cấu trúc tông của mạng đa dạng. Ví dụ Mạng hình BUS, mạng vòng (Ring), mạng hình sao (Star) và các loại mạng kết hợp, lai ghép....



a. Topology dạng Bus



b. Topology dạng Ring



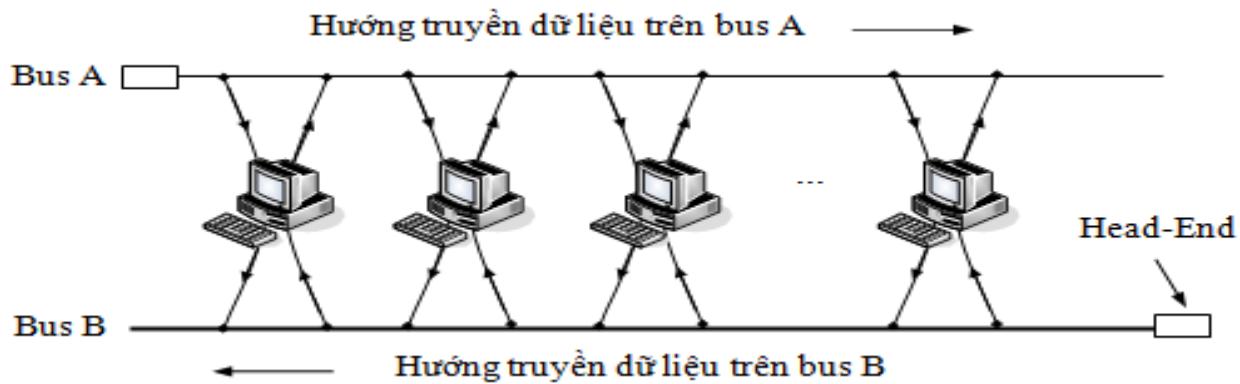
c. Topology dạng Star

Hình 1. 2 Cấu trúc mạng LAN cơ bản

Mạng đô thị MAN (Metropolitan Area Networks)

Mạng đô thị (Metropolitan Area Network – MAN): là mạng được cài đặt trong phạm vi một đô thị hoặc một trung tâm kinh tế - xã hội có bán kính khoảng 100km trở lại.

Mạng đô thị MAN hoạt động theo kiểu quảng bá, LAN to LAN. Mạng cung cấp các dịch vụ thoại và phi thoại và truyền hình cáp. Trong một mạng MAN, có thể sử dụng một hoặc hai đường truyền vật lý và không chứa thực thể chuyển mạch. Dựa trên tiêu chuẩn DQDB (Distributed Queue Dual Bus - IEEE 802.6) quy định 2 cáp đơn kết nối tất cả các máy tính lại với nhau, các máy bên trái liên lạc với các máy bên phải thông tin vận chuyển trên đường BUS trên. Các máy bên phải liên lạc với các máy bên trái, thông tin đi theo đường BUS dưới.



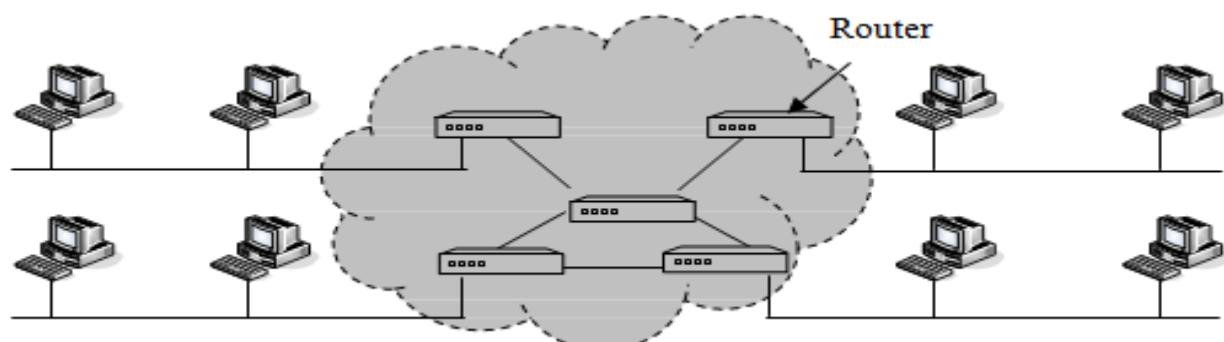
Hình 1. 3 Cấu trúc mạng MAN

Mạng diện rộng WAN (Wide Area Network).

Mạng diện rộng WAN (Wide Area Network): phạm vi của mạng có thể vượt qua biên giới quốc gia và thậm chí cả lục địa. Cáp truyền qua đại dương hoặc vệ tinh được dùng cho việc truyền dữ liệu trong mạng WAN.

Đặc trưng cơ bản của một mạng WAN:

- Hoạt động trên phạm vi một quốc gia hoặc trên toàn cầu.
- Tốc độ truyền dữ liệu thấp so với mạng cục bộ.
- Lỗi truyền cao.



Hình 1. 4 Cấu trúc mạng WAN

Mạng toàn cầu GAN (Global Area Network).

Mạng toàn cầu GAN (Global Area Network): phạm vi của mạng trải rộng toàn Trái đất. Việc kết nối các máy tính được thực hiện thông qua mạng viễn thông và vệ tinh.

Khoảng cách địa lý có tính chất tương đối đặc biệt trong thời đại ngày nay những tiến bộ và phát triển của công nghệ truyền dẫn và quản lý mạng nên ranh giới khoảng cách địa lý giữa các mạng là mờ nhạt.

Tuy nhiên về sau người ta thường quan niệm chung bằng cách đồng nhất 4 loại thành 2 loại sau:

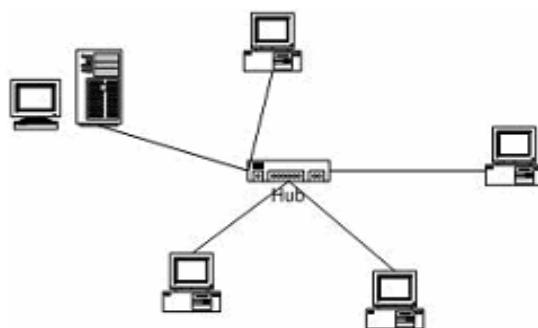
WAN là mạng lớn trên diện rộng, hệ mạng này có thể truyền thông và trao đổi dữ liệu với một phạm vi lớn có khoảng cách xa như trong một quốc gia hay quốc tế.

LAN là mạng cục bộ được bố trí trong phạm vi hẹp như một cơ quan, một Bộ, Ngành ... một số mạng LAN có thể nối lại với nhau để tạo thành một mạng LAN lớn hơn.

1.3.2. Phân loại mạng theo topology

Theo topology, mạng được chia làm các loại như mạng hình sao (Star topology), mạng tuyến tính (Bus topology), mạng vòng (Ring topology) và mạng kết hợp.

❖ Mạng hình sao (Star topology).



Hình 1. 5 Mạng hình sao

Mạng hình sao có tất cả các trạm được kết nối với một thiết bị trung tâm có nhiệm vụ nhận tín hiệu từ các trạm và chuyển đến trạm đích. Tùy theo yêu cầu truyền thông trên mạng mà thiết bị trung tâm có thể là hub, switch, router hay máy chủ trung tâm. Vai trò của thiết bị trung tâm là thiết lập các liên kết Point –to – Point.

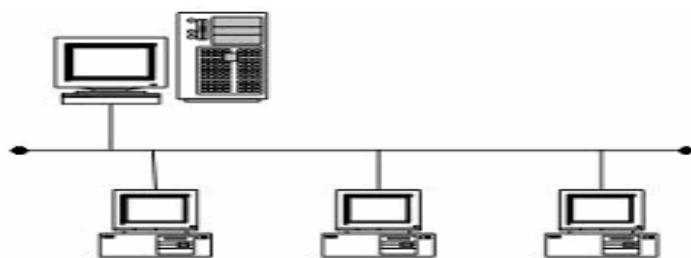
– **Ưu điểm:** Thiết lập mạng đơn giản, dễ dàng cấu hình lại mạng (thêm, bớt các trạm), dễ dàng kiểm soát và khắc phục sự cố, tận dụng được tối đa tốc độ truyền của đường truyền vật lý.

– **Khuyết điểm:** Độ dài đường truyền nối một trạm với thiết bị trung tâm bị hạn chế (bán kính khoảng 100m với công nghệ hiện nay).

❖ Mạng tuyến tính (Bus topology).

Tất cả các node truy nhập chung trên một đường truyền vật lý được giới hạn hai đầu bằng hai đầu nối đặc biệt gọi là terminator. Mỗi trạm được nối với trục chính (BUS) qua một đầu nối chữ T (T-connector) hoặc một thiết bị thu phát (transceiver). Chuẩn IEEE 802.3 được gọi là Ethernet, là một mạng hình BUS quảng bá với cơ chế điều khiển quảng bá động phân tán, trao đổi thông tin với tốc độ 10 Mbps hoặc 100 Mbps.

Phương thức truy nhập đường truyền được sử dụng trong mạng hình BUS hoặc TOKEN BUS, hoặc đa truy nhập sử dụng sóng mang với việc phát hiện xung đột thông tin trên đường truyền CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

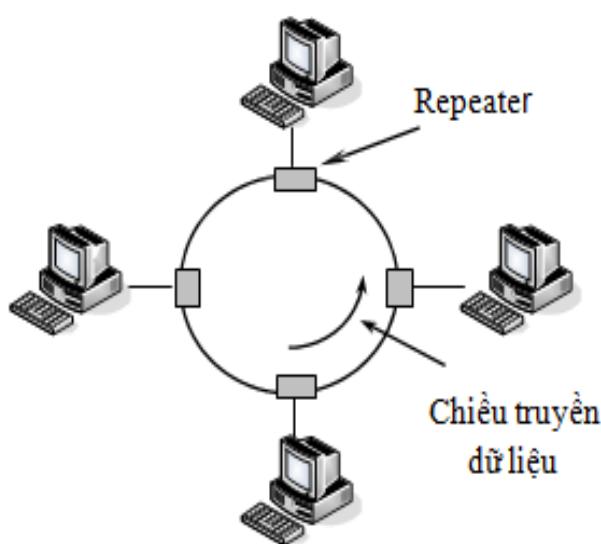


Hình 1. 6 Mạng tuyến tính

- **Ưu điểm:** Dễ thiết kế và chi phí thấp, nếu một nút mạng hỏng thì không ảnh hưởng đến hoạt động của toàn mạng.
- **Khuyết điểm:** Tính ổn định kém, dễ xảy ra xung đột thông tin trên đường truyền.

❖ Mạng vòng (Ring topology)

Với mạng vòng (Ring topology) tất cả các node cùng truy nhập chung trên một đường truyền vật lý. Tín hiệu được lưu chuyển trên vòng theo một chiều duy nhất, theo liên kết điểm - điểm. Dữ liệu được chuyển một cách tuần tự từng bit quanh vòng, qua các bộ chuyển tiếp. Bộ chuyển tiếp có ba chức năng: chèn, nhận và hủy bỏ thông tin. Các bộ chuyển tiếp sẽ kiểm tra địa chỉ đích trong các gói dữ liệu khi đi qua nó.



Hình 1. 7 Mạng vòng

- *Ưu điểm:* Với dạng kết nối này có ưu điểm là không tốn nhiều dây cáp, tốc độ truyền dữ liệu cao, không gây ách tắc.

- *Nhược điểm:* Các giao thức để truyền dữ liệu phức tạp và nếu có trục trặc trên một trạm thì cũng ảnh hưởng đến toàn mạng.

1.3.3. *Phân loại mạng theo kỹ thuật chuyển mạch*

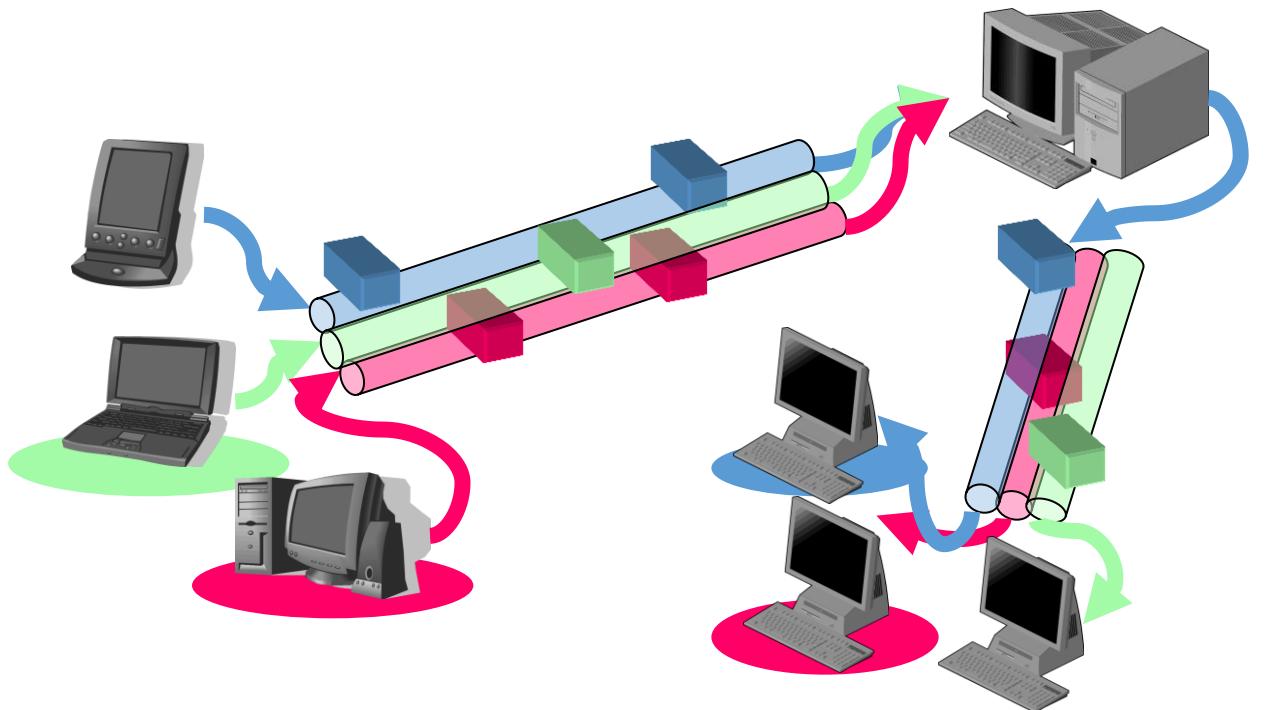
Nếu lấy kỹ thuật chuyển mạch so sánh thì có thể phân chia mạng ra thành: Mạng chuyển mạch kênh, mạng chuyển mạch thông báo, mạng chuyển mạch gói.

1.3.3.1 Mạng chuyển mạch kênh (Circuit - Switched - Network)

Đây là mạng giữa hai thực thể muốn liên lạc với nhau thì giữa chúng tạo ra một kênh cứng, cố định được duy trì liên tục cho đến khi một trong hai thực thể ngắt liên lạc như mạng điện thoại. Phương pháp chuyển mạch này có hai nhược điểm chính:

- + Hiệu xuất sử dụng đường truyền không cao vì có khi kênh bị bỏ không.
- + Tiêu tốn thời gian cho việc thiết lập kênh cố định giữa hai thực thể.

Mô tả chuyển mạch kênh:



Hình 1.8 Mô hình chuyển mạch kênh

1.3.3.2. Mạng chuyển mạch thông báo (Message - Switched - Network)

Các nút của mạng căn cứ vào địa chỉ đích của “*thông báo*” để chọn nút kế tiếp trên đường dẫn tới đích. Như vậy các nút cần lưu trữ tạm thời và đọc tin nhận được, quản lý việc chuyển tiếp thông báo đi. Tùy thuộc vào điều kiện mạng mà các thông báo khác nhau có thể được gửi trên các con đường khác nhau. Phương pháp chuyển mạch thông báo có những ưu điểm sau:

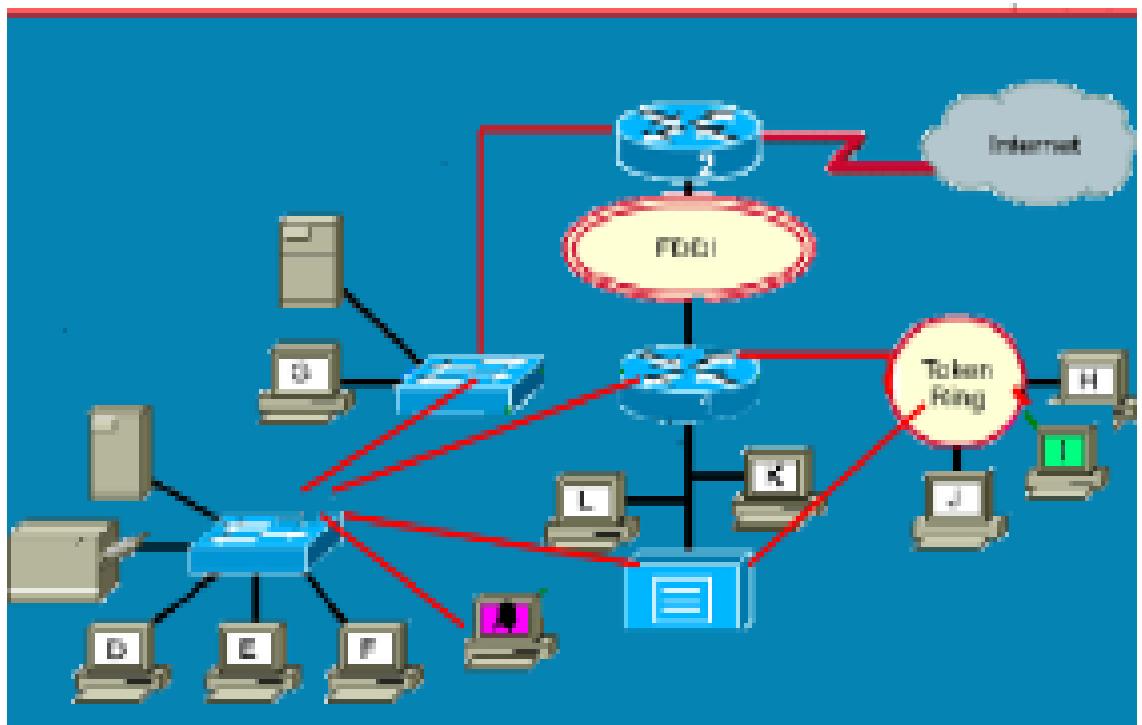
+ Hiệu suất sử dụng đường truyền cao vì không bị chiếm dụng độc quyền mà được phân chia giữa nhiều thực thể.

+ Mỗi nút mạng có thể lưu trữ thông báo cho tới khi kênh truyền rỗng mới chuyển thông báo đi, do đó giảm tình trạng tắc nghẽn trên mạng.

+ Có thể điều khiển truyền tin bằng cách sắp xếp mức độ ưu tiên của các thông báo. Trong mạng chuyển mạch thông báo ta có thể làm tăng hiệu suất sử dụng giải thông của mạng bằng cách gán địa chỉ quảng bá cho các thông báo để gửi nó đồng thời đến nhiều đích khác nhau.

Nhược điểm chủ yếu là trong trường hợp một thông báo dài bị lỗi, phải truyền thông báo này lại nên hiệu suất không cao. Phương pháp này thích hợp với phương pháp truyền thư tín điện tử (*Electronic mail*).

Mô tả chuyển mạch thông báo:



Hình 1. 9 Mô hình chuyển mạch thông báo

1.3.3.3 Mạng chuyển mạch gói (Packet - Switched - Network)

Trong trường hợp này một thông báo có thể chia ra thành nhiều gói tin (Packet) khác nhau, độ dài khoảng 256 byte, có khuôn dạng quy định. Các gói tin chứa thông tin điều khiển, trong đó có địa chỉ nguồn và địa chỉ đích. Các gói tin của một thông báo có thể gửi đi bằng nhiều đường khác nhau.

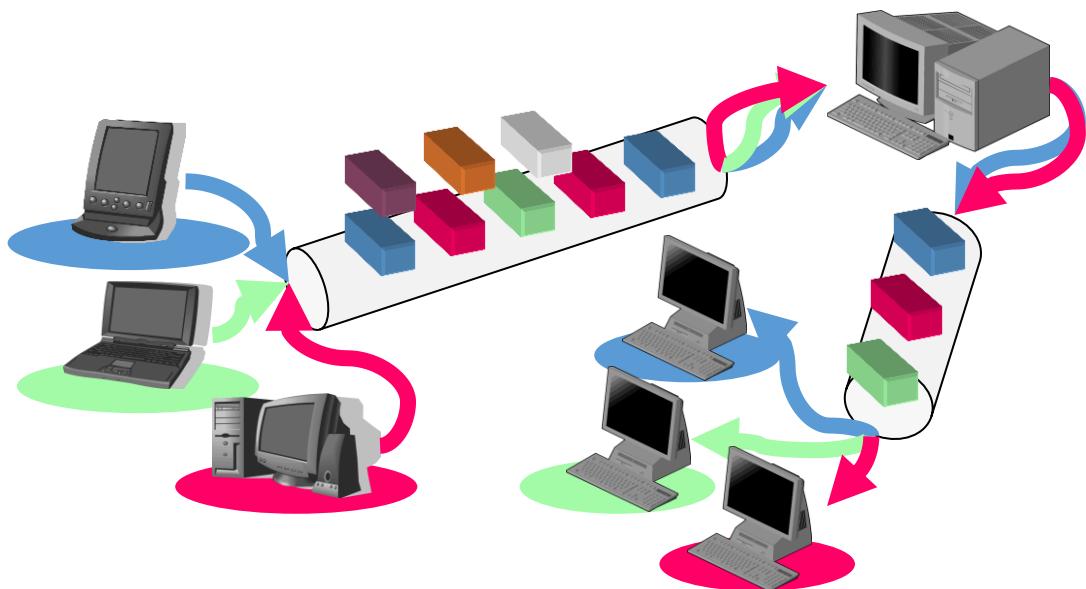
+ Mạng chuyển mạch gói có hiệu suất cao hơn mạng chuyển mạch thông báo vì kích thước của gói tin là hạn chế sao cho các nút mạng có thể xử lý toàn bộ gói tin trong bộ nhớ mà không cần lưu trữ tạm thời trên đĩa, do đó mạng chuyển các gói tin nhanh hơn.

+ Mỗi đường truyền chiếm thời gian rất ngắn vì có thể dùng bất kỳ đường nào để đi đến đích và khả năng đồng bộ bit rất cao.

+ Là thời gian truyền tin rất ngắn nên nếu thời gian chuyển mạch lớn thì tốc độ truyền không cao vì nó đòi hỏi thời gian chuyển mạch cực ngắn.

+ Việc tổ hợp các gói tin để tạo lại để thông báo là khó khăn, đặc biệt là trong trường hợp các gói được truyền đi theo nhiều đường khác nhau.

Mô tả chuyển mạch gói:



Hình 1. 10 Mô hình chuyển mạch gói

Do có nhiều ưu điểm là mềm dẻo và hiệu suất cao nên chuyển mạch gói được dùng phổ biến hiện nay. Việc tổ hợp hai kỹ thuật chuyển mạch kênh và chuyển mạch gói trong cùng một mạng thống nhất gọi tắt là **ISDN** (*Intergrated Service digital Network*) đang là xu hướng phát triển hiện nay, đó chính là mạng dịch vụ tích hợp số.

Ngoài ra, có thể phân loại theo cách Khai Thác Dữ Liệu

Nếu xem xét mạng theo góc độ logic (hay kiểu khai thác dữ liệu) thì mạng chia thành hai kiểu.

- Bình đẳng (peer to peer), trong kiểu này các máy tính được nối lại với nhau, máy này có thể sử dụng tài nguyên của các máy kia và ngược lại, không có máy nào được coi là máy chủ.

- Kiểu chủ/khách (server/client) ít nhất một máy gọi là máy chủ (server), đó là máy trên đó có cài đặt các phần mềm hệ điều hành mạng (NETWARE SYSTEM), máy này có chức năng điều khiển và phân chia việc khai thác tài nguyên theo yêu cầu của máy khác.

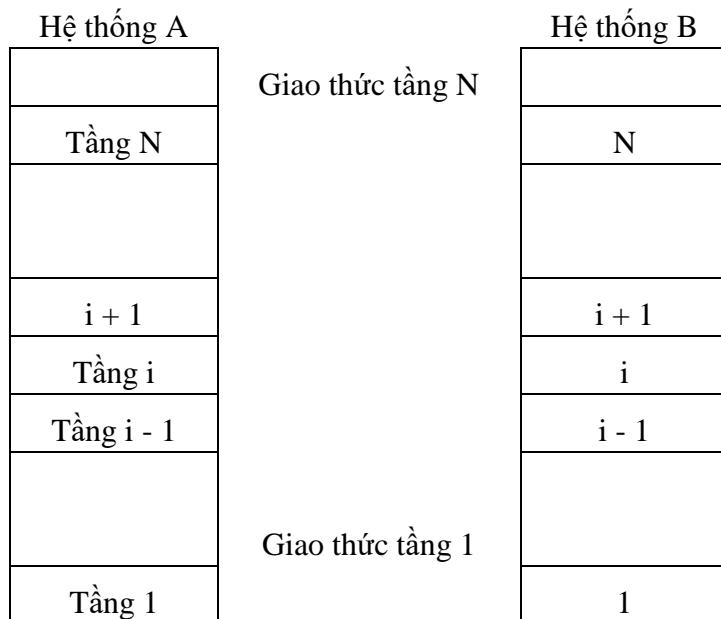
Thuật ngữ CLIENT được dùng để chỉ người khai thác hệ thống mạng. Mỗi người khai thác mạng phải sử dụng một máy tính nào đó có nối với máy chủ để khai thác mạng, người này gọi là client.

1.4. Kiến trúc phân tầng và mô hình OSI.

1.4.1. Kiến trúc phân tầng

Để giảm phức tạp của việc thiết kế và cài đặt mạng, hầu hết các mạng máy tính đều có phân tích, thiết kế theo quan điểm phân tầng (layering). Sự phân tầng giao thức rất quan trọng vì nó cung cấp sự hiểu biết sâu sắc về các thành phần giao thức khác nhau cần thiết cho mạng và thuận tiện cho việc thiết kế và cài đặt các phần mềm truyền thông. Mỗi tầng thực hiện một số chức năng xác định và cung cấp một số dịch vụ nhất định cho tầng cao hơn.

Kiến trúc phân tầng tổng quát:



Hình 1.11 Mô hình kiến trúc phân tầng

Mỗi hệ thống trong mạng đều có cấu trúc tầng dựa vào: Số lượng tầng, chức năng mỗi tầng và định nghĩa mối quan hệ giữa 2 tầng đồng mức, giữa 2 tầng kề nhau

Khi ta nghiên cứu hoạt động mạng gồm kết nối Vật lý, giao thức và ứng dụng ta có thể thấy những yếu tố mạng này từ một hệ thống phân cấp các ứng dụng ở trên đỉnh và kết nối ở dưới đáy. Những giao thức cung cấp một cầu nối giữa các ứng dụng và kết nối vật lý. Để hiểu hệ thống phân cấp giữa các yếu tố mạng ta cần một “tiêu chuẩn so sánh” hoặc mô hình xác định những chức năng này. Một mô hình phổ biến nhất là *mô hình OSI*. Một mô hình khác, *mô hình DoD* (Department of Defense), được thiết kế đặc biệt cho việc mô tả các giao thức TCP/IP.

1.4.2. Các tổ chức tiêu chuẩn hóa mạng máy tính.

Tình trạng không tương thích giữa các mạng, đặc biệt là mạng bán trên thị trường gây trở ngại cho những người sử dụng, tác động đến mức tiêu thụ các sản phẩm về mạng. Do đó, cần xây dựng các mô hình chuẩn làm căn cứ cho các nhà nghiên cứu và thiết kế mạng tạo ra các sản phẩm có tính chất mở về mạng, đưa tới dễ phổ cập, sản xuất và sử dụng **Hai tổ chức chuẩn chính là ISO và CCITT:**

ISO (International Organization for Standardization) thành lập năm 1946 dưới sự bảo trợ của liên hợp quốc, các thành viên là các cơ quan tiêu chuẩn của các quốc gia. ISO đã xây dựng hơn 500 chuẩn ở tất cả các lĩnh vực. ISO được chia thành các ủy ban kỹ thuật (*Technical Committee - TC*) TC97 đảm bảo lĩnh vực chuẩn hóa xử lý tin. Mỗi TC lại chia thành nhiều tiểu ban (*SubCommittee - SC*) và mỗi SC lại chia thành nhiều nhóm làm việc khác nhau, đảm nhiệm các nhiệm vụ khác nhau. Các chuẩn do hội đồng ISO ban hành như là các chuẩn quốc tế chính thức.

CCITT tổ chức tư vấn quốc tế về điện tín và điện thoại hoạt động dưới sự bảo trợ của liên hiệp quốc, các thành viên chủ yếu là các cơ quan bưu chính - viễn thông của các quốc gia và tư nhân. CCITT đã đưa ra các khuyến nghị loại V liên quan đến truyền dữ liệu, các khuyến nghị loại X liên quan đến mạng truyền dữ liệu công cộng và loại I dành cho các mạng ISDN.

Ngoài ISO, CCITT trên thế giới còn có các tổ chức khác như ECMA, ANSI, IEEE là những tổ chức đã có nhiều đóng góp trong chuẩn hóa mạng. Tổ chức ISO đã đưa ra một số các nguyên tắc chính để xây dựng mô hình 7 tầng là:

- Chỉ thiết lập một lớp khi cần đến 1 cấp độ trừu tượng khác nhau.
- Mỗi lớp phải thực hiện chức năng rõ ràng.
- Chức năng của mỗi lớp phải định rõ những giao thức theo đúng tiêu chuẩn quốc tế.
- Ranh giới các lớp phải giảm tối thiểu lưu lượng thông tin truyền qua giao diện lớp.
- Các chức năng khác nhau phải được xác định trong lớp riêng biệt, song số lượng lớp phải vừa đủ để cấu trúc không trở nên quá phức tạp.

Sự ghép nối giữa các mức:

- Khi máy A gửi tin đi, các đơn vị dữ liệu đi từ tầng trên xuống dưới. Qua môi trường nó được bổ sung thông tin điều khiển của môi trường.

- Khi nhận tin, thông tin từ dưới lên, qua mỗi tầng thông tin điều khiển được tách ra để xử lý gói. Cuối cùng máy nhân B được bản tin của máy phát A

* Các giao thức chuẩn ISO

Việc trao đổi thông tin, cho dù là đơn giản nhất, cũng đều phải tuân theo những qui tắc nhất định. Do vậy việc truyền tin trên mạng cần phải có những qui tắc, qui ước về nhiều mặt, từ khuôn dạng (cú pháp, ngữ nghĩa) của dữ liệu cho tới các thủ tục gửi, nhận dữ liệu kiểm soát hiệu quả và chất lượng truyền tin, xử lý các lỗi và sự cố. Các giao thức chuẩn ISO đưa tới cách xây dựng cho giao thức từng tầng.

Trong mạng chuyển mạch gói có thể truyền theo phương pháp:

- *Truyền có liên kết* (*connection*)
 - *Truyền không có liên kết* (*connectionless*)

Với các mạng có liên kết các dịch vụ và giao thức ở mỗi tầng trong mô hình OSI phải thực hiện 3 giai đoạn theo thứ tự thời gian:

- Thiết lập liên kết.
 - Truyền dữ liệu.
 - Hủy bỏ liên kết.

Với các mạng không liên kết thì chỉ có một giai đoạn truyền dữ liệu, các gói dữ liệu được truyền độc lập và theo một con đường xác định.

- Trong giai đoạn thiết lập liên kết hai thực thể cùng tầng ở hai đầu của liên kết sẽ thương lượng về tập các tham số sử dụng trong giai đoạn truyền dữ liệu và trong giai đoạn này các cơ chế kiểm soát bởi luồng dữ liệu, ghép kênh, cắt hợp dữ liệu được thực hiện để tăng cường độ tin cậy và hiệu suất.

Các giao thức chuẩn hóa của ISO được xây dựng trên cơ sở 4 hàm nguyên thủy

Ví dụ:	tương ứng
- Request (yêu cầu)	quay số
- Indication (chỉ báo)	chuông đồ
- Response (trả lời)	nhắc máy
- Confirm (xác nhận)	nối

Request được gửi bởi người sử dụng dịch vụ ở tầng N+1 trong hệ thống A để gọi thủ tục của giao thức ở tầng N. Yêu cầu cấu tạo dưới dạng 1 hoặc nhiều đối với dữ liệu của giao thức (PDU) (Protocol data unit) để gửi tới B.

B sẽ thông báo yêu cầu đó lên tầng N+1 bằng hàm indication. Sau đó response được gửi tới từ N+1 của B xuống N để gọi thủ tục giao thức tầng N để trả lời cho A.

* Các chuẩn hệ thống mở (Open System Standards)

Mô hình tham chiếu chỉ đơn giản là một mô hình cho cấu trúc của một hệ thống con thông tin, nó làm chỗ dựa cho các hoạt động chuẩn hóa liên quan đến từng lớp. Nó không có nghĩa là phải có một giao thức chuẩn cho mỗi lớp. Đúng hơn là mỗi lớp phải có một tập hợp các chuẩn, mỗi chuẩn cung ứng các mức chức năng khác nhau. Như vậy, đối với một môi trường kết nối các hệ thống nhất định, ta phải xác định một tập hợp các chuẩn có chọn lựa để tất cả các hệ thống trong môi trường đó sử dụng.

Ba tổ chức Quốc tế chính tích cực tạo ra các chuẩn cho thông tin máy tính là ISO, IEEE và CCITT. Về cơ bản, ISO và IEEE đưa ra các chuẩn để sử dụng cho các nhà sản xuất máy tính, trong khi đó CCITT định nghĩa các chuẩn dùng cho việc kết nối các thiết bị vào các kiểu mạng công cộng Quốc gia và Quốc tế khác nhau. Tuy nhiên, khi mức độ xen phủ lên nhau giữa công nghiệp máy tính và công nghiệp viễn thông tăng lên thì mức độ cộng tác và mức độ chung nhau giữa các chuẩn được đưa ra bởi các tổ chức này cũng tăng lên.

Ngoài ra, trước và song hành với các hoạt động chuẩn hóa của ISO, Bộ Quốc phòng Mỹ cũng đã nghiên cứu và kết nối mạng trong nhiều năm thông qua cơ quan DARPA (Defense Advanced Research Projects Agency). Kết quả là sự ra đời của mạng được phát triển bởi các tổ chức chính phủ khác. Liên mạng tổ hợp đó hiện nay được gọi đơn giản là Internet.

1.4.3. Mô hình OSI

Mô hình kết nối các hệ thống mở OSI là mô hình căn bản về các tiến trình truyền thông, thiết lập các tiêu chuẩn kiến trúc mạng ở mức Quốc tế, là cơ sở chung để các hệ thống khác nhau có thể liên kết và truyền thông được với nhau. Mô hình OSI tổ chức các giao thức truyền thông thành 7 lớp, mỗi một lớp giải quyết một phần hẹp của tiến trình truyền thông, chia tiến trình truyền thông thành nhiều lớp và trong mỗi lớp có thể có nhiều giao thức khác nhau thực hiện các nhu cầu truyền thông cụ thể.

- *Lớp vật lý*: Cung cấp phương tiện truyền tin, thủ tục khởi động, duy trì, hủy bỏ các liên kết vật lý cho phép truyền các dòng dữ liệu ở dòng bit. Nói cách khác ở mức Vật lý đảm bảo cho các yêu cầu về thiết bị như máy tính, thiết bị đầu cuối, bus truyền tin...

- *Lớp liên kết dữ liệu*: Thiết lập, duy trì, hủy bỏ các liên kết dữ liệu, kiểm soát luồng dữ liệu, khắc phục sai sót, cắt hợp dữ liệu.

Ví dụ: Giao thức BSC, SDLC, HDLC, LAPB, LAPD.

- *Lớp mạng*: Định rõ các thủ tục cho các chức năng như định tuyến, điều khiển độ lưu lượng, thiết lập cuộc gọi và kết thúc các thông tin người sử dụng mạng lưới, xây dựng dựa trên kiểu kết nối từ nút đến nút do lớp liên kết thông tin cung cấp.

Ví dụ: Giao thức IPX ,X.25PLP, IP

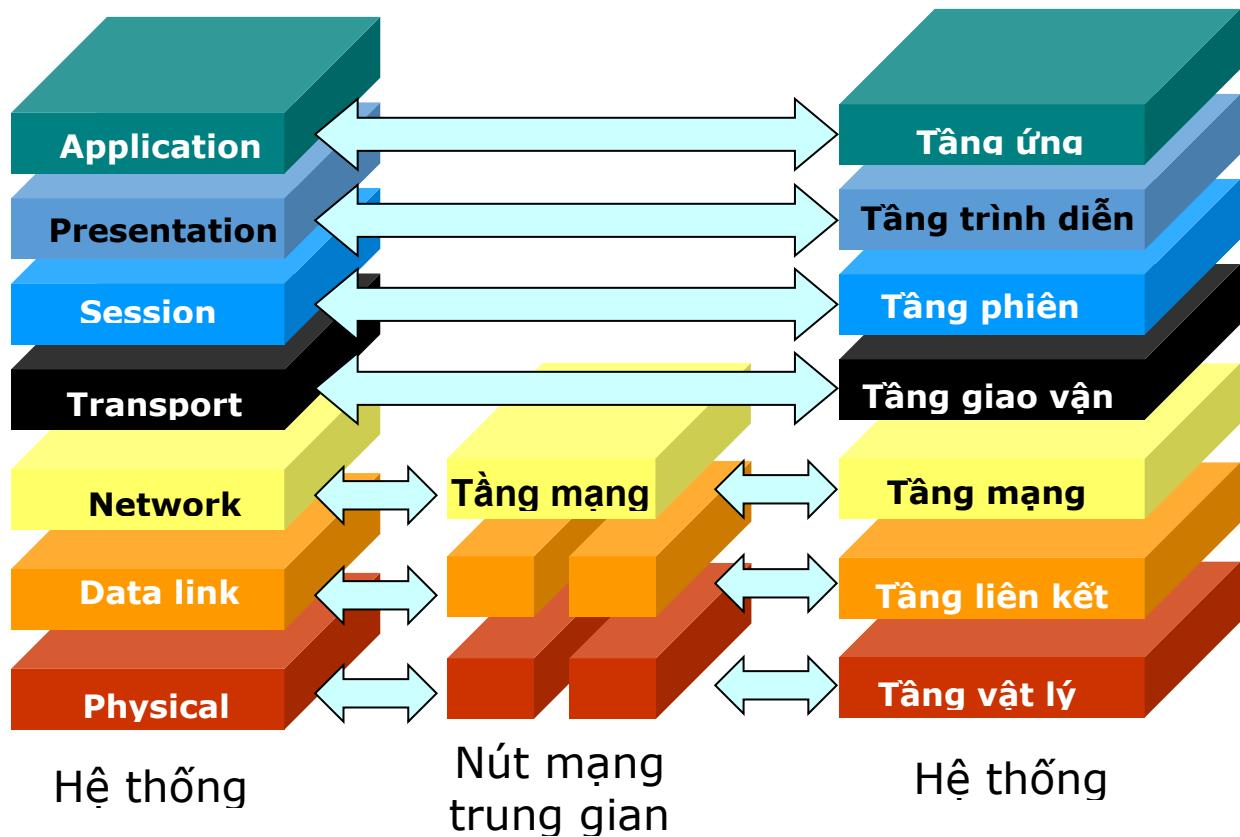
- *Lớp vận chuyển*: Định rõ giao thức và các cấp dịch vụ cho thông tin không lời giữa các HOST đi qua mạng con.

Ví dụ: Giao thức SPX, TCP, UDP.

- *Lớp phiên*: Định rõ thông tin từ quá trình này đến quá trình kia, khôi phục lỗi, đồng bộ phiên. Lớp phiên có nhiệm vụ thiết lập (và hủy bỏ) một kênh thông tin (đối thoại) giữa hai thực thể giao thức lớp ứng dụng đang thông tin trong một giao dịch mạng đầy đủ.

- *Lớp trình bày*: liên quan đến việc biểu diễn (cú pháp) của số liệu khi chuyển đi giữa hai tiến trình ứng dụng đang thông tin. Để có được một kết nối các hệ thống mở đúng nghĩa, một số dạng cú pháp số liệu trừu tượng phổ biến được định nghĩa để các tiến trình ứng dụng sử dụng cùng với những cú pháp chuyển số liệu có liên quan. Một chức năng khác của lớp trình bày liên quan đến vấn đề an toàn số liệu..

- *Lớp ứng dụng*: Là mức cao nhất của mô hình OSI, cung cấp phương tiện để người sử dụng có thể truy cập được vào môi trường OSI đồng thời cung cấp dịch vụ thông tin phân tán, thông thường là một chương trình/tiến trình ứng dụng - một loạt các dịch vụ thông tin phân tán trên khắp mạng. Các dịch vụ này bao gồm quản lý và truy cập việc chuyển file, các dịch vụ trao đổi thông báo và tài liệu chung như thư tín điện tử.



Hình 1. 12 Mô hình OSI

1.4.4. Mô hình TCP/IP

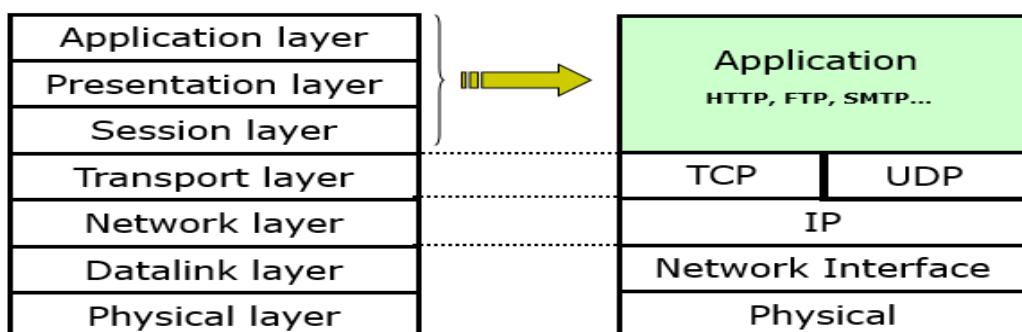
TCP/IP (Transmission Control Protocol/Internet Protocol) là chòng giao thức cùng hoạt động nhằm cung cấp các phương tiện truyền thông liên mạng. Năm 1981, TCP/IP phiên bản 4 (IPv4) được hoàn thành và sử dụng phổ biến trên máy tính sử dụng hệ điều hành UNIX, trở thành một trong những giao thức cơ bản của hệ điều hành Windows 9x. Năm 1994, một phiên bản mới IPv6 được hình thành trên cơ sở cải tiến những hạn chế của IPv4. TCP/IP bao gồm cả các giao thức định hướng mạng và các giao thức hỗ trợ ứng dụng. Bởi vì TCP/IP đang được sử dụng rộng rãi với một liên mạng đang tồn tại cho nên rất nhiều giao thức của TCP/IP đã được sử dụng rộng rãi bởi các tổ chức thương mại và các cơ quan Nhà nước để tạo ra các môi trường kết nối hệ thống mở.

Mặc dù có nhiều giao thức trong bộ giao thức truyền thông TCP/IP, hai giao thức quan trọng nhất được lấy tên đặt cho bộ giao thức này là TCP (Transmission Control Protocol) và IP (Internet Protocol). Mô hình TCP/IP được chia thành 4 tầng: tầng truy cập mạng (network access), tầng liên mạng (internet), tầng vận chuyển (transport) và tầng ứng dụng (application).

- *Tầng ứng dụng (Application Layer)*: Ứng với các lớp Session, Presentation và Application trong mô hình OSI. Tầng ứng dụng hỗ trợ các ứng dụng cho các giao thức lớp Host to Host. Cung cấp giao diện cho người sử dụng mô hình TCP/IP. Các giao thức ứng dụng gồm TELNET (truy nhập từ xa), FTP (truyền File), SMTP (thư điện tử)

- *Tầng vận chuyển (Transport Layer)*: Ứng với tầng vận chuyển (Transport Layer) trong mô hình OSI, tầng vận chuyển thực hiện những kết nối giữa hai máy chủ trên mạng bằng 2 giao thức: giao thức điều khiển trao đổi dữ liệu TCP (Transmission Control Protocol) và giao thức dữ liệu người sử dụng UDP (User Datagram Protocol). Giao thức TCP là giao thức kết nối hướng liên kết (Connection - Oriented) chịu trách nhiệm đảm bảo tính chính xác và độ tin cậy cao trong việc trao đổi dữ liệu giữa các thành phần của mạng, tính đồng thời và kết nối song công (Full Duplex). Khái niệm tin độ cậy cao nghĩa là TCP kiểm soát lỗi bằng cách truyền lại các gói tin bị lỗi. Giao thức TCP cũng hỗ trợ những kết nối đồng thời. Nhiều kết nối TCP có thể được thiết lập tại một máy chủ và dữ liệu có thể được truyền đi một cách đồng thời và độc lập với nhau trên các kết nối khác nhau. TCP cung cấp kết nối song công (Full Duplex), dữ liệu có thể được trao đổi trên một kết nối đơn theo 2 chiều. Giao thức UDP được sử dụng cho những ứng dụng không đòi hỏi độ tin cậy cao.

- *Tầng mạng (Internet Layer)*: Ứng với lớp mạng (Network Layer) trong mô hình OSI, tầng mạng cung cấp một địa chỉ logic cho giao diện vật lý mạng. Giao thức thực



hiện của tầng mạng trong mô hình DOD là giao thức IP kết nối không liên kết (Connectionless), là hạt nhân hoạt động của Internet. Cùng với các giao thức định tuyến RIP, OSPF, BGP, lớp mạng IP cho phép kết nối một cách mềm dẻo và linh hoạt các loại mạng "vật lý" khác nhau như: Ethernet, Token Ring, X.25... Ngoài ra tầng này còn hỗ trợ các ánh xạ giữa địa chỉ vật lý (MAC) do lớp Network Access Layer cung cấp với địa chỉ logic bằng các giao thức phân giải địa chỉ ARP (Address Resolution Protocol) và phân giải địa chỉ đảo RARP (Reverse Address Resolution Protocol). Các vấn đề có liên quan đến chuẩn đoán lỗi và các tình huống bất thường liên quan đến IP được giao thức ICMP (Internet Control Message Protocol) thống kê và báo cáo. Tầng trên sử dụng các dịch vụ do tầng Liên mạng cung cấp.

Hình 1. 13 Mô hình OSI và TCP/IP

- *Tầng truy nhập mạng (Network Access Layer):* Tương ứng với tầng Vật lý và Liên kết dữ liệu trong mô hình OSI, tầng truy nhập mạng cung cấp các phương tiện kết nối vật lý cáp, bộ chuyển đổi (Transceiver), Card mạng, giao thức kết nối, giao thức truy nhập đường truyền như CSMA/CD, Token Ring, Token Bus..). Cung cấp các dịch vụ cho lớp Internet phân đoạn dữ liệu thành các khung.

1.5. Xu hướng phát triển Mạng máy tính

Ngày nay nhu cầu truyền các loại thông tin khác nhau như tiếng nói, hình ảnh, số liệu cùng một lúc trên mạng, nhu cầu truyền thông tin từ một điểm đến nhiều điểm, từ nhiều điểm tới nhiều điểm với tốc độ cao cùng tăng lên mạnh mẽ. Với mạng thông tin hiện tại không còn đáp ứng được các nhu cầu hướng tới truyền thông đa phương tiện (multimedia) bởi tính không mềm dẻo của chúng. Thông tin đa phương tiện vừa là ước mơ vừa là hiện thực của sự phát triển mạng thông tin hiện tại và tương lai. Từ đó ra đời mạng tổ hợp dịch vụ số băng rộng (Broadband Intergrated Server Digital Network: B-ISDN) có khả năng truyền các thông tin liên quan tới nhiều ứng dụng khác nhau như truyền hình số, truyền hình độ phân giải cao, điện thoại truyền hình với chất lượng cao, các dịch vụ hình ảnh, các dịch vụ truyền số liệu tốc độ cao với kiểu truyền không đồng bộ ATM (Asynchronous Transfer Mode).

TÓM TẮT NỘI DUNG CỐT LÕI.

- Sự hình thành và phát triển mạng máy tính.
- Các thành phần mạng máy tính.
- Phân loại mạng máy tính.
- Kiến trúc phân tầng và mô hình OSI.
- Xu hướng phát triển mạng máy tính.

BÀI TẬP ỦNG DỤNG, LIÊN HỆ THỰC TẾ.

Câu 1. Topo mạng cục bộ nào mà tất cả các trạm phân chia chung một đường truyền chính

- A. Star B. Tree C. Cả 3 đều đúng D. Bus

Câu 2. Hãy chọn cụm từ tương ứng để hoàn thiện khẳng định sau: Mục tiêu kết nối các máy tính thành mạng là cung cấp các đa dạng, chia sẻ tài nguyên chung và giảm bớt các chi phí về trang thiết bị

- A. Dịch vụ mạng B. Thiết bị mạng C. Mục tiêu mạng D. Tài nguyên mạng

Câu 3. Thiết bị mạng trung tâm dùng để kết nối các máy tính trong mạng hình sao (STAR)

- A. Router B. Repeater C. NIC D. Switch / Hub

Câu 4. Các trạm hoạt động trong một mạng vừa như máy phục vụ (server) vừa như máy khách (client) có thể tìm thấy trong mạng nào?

- A. Client / Server B. Ethernet C. LAN D. Peer to Peer

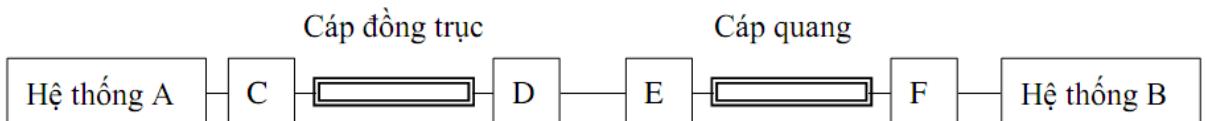
CHƯƠNG 2. TẦNG VẬT LÝ

Mục đích:

Tầng vật lý cung cấp các phương tiện điện, cơ, chức năng thủ tục để kích hoạt, duy trì và hủy bỏ kết nối Vật lý giữa các hệ thống. Phương tiện điện liên quan đến sự biểu diễn các bít (mức thể hiện) và tốc độ truyền các bít, đặc tính cơ liên quan đến các tính chất Vật lý của giao diện với một đường truyền (kích thước, cấu hình). Thuộc tính chức năng chỉ ra các chức năng được thực hiện bởi các phần tử của giao diện Vật lý, giữa một hệ thống đường truyền còn thủ tục liên quan đến giao thức điều khiển việc truyền các xâu bít qua đường truyền Vật lý.

2.1. Vai trò chức năng tầng vật lý

Tầng vật lý là tầng thấp nhất trong mô hình 7 lớp OSI. Các thực thể tầng giao tiếp với nhau qua một đường truyền vật lý. Tầng vật lý xác định các chức năng, thủ tục về điện, cơ, quang để kích hoạt, duy trì và giải phóng các kết nối vật lý giữa các hệ thống mạng. Cung cấp các cơ chế về điện, cơ hàm, thủ tục ... nhằm thực hiện việc kết nối các phần tử của mạng thành một hệ thống bằng các phương pháp vật lý. Đảm bảo cho các yêu cầu về chuyển mạch hoạt động nhằm tạo ra các đường truyền thực cho các



chuỗi bit thông tin.

Hình 2. 1 Môi trường thực của tầng vật lý

Trong hình trên, A và B là hai hệ thống mở được nối với nhau bằng một đoạn cáp đồng trực và một đoạn cáp quang. Modem C để chuyển đổi tín hiệu từ tín hiệu số sang tín hiệu tương tự để truyền trên cáp đồng, và modem D lại chuyển đổi tín hiệu từ tín hiệu tương tự sang tín hiệu số. Transducer E chuyển đổi từ xung điện thành xung ánh sáng để chuyển qua các quang. Cuối cùng Transducer F chuyển đổi thành xung điện để đi vào B.

Các chuẩn trong tầng vật lý là các chuẩn xác định giao diện người sử dụng và môi trường mạng. Các giao thức lớp vật lý có hai loại truyền dị bộ (Asynchronous) và truyền đồng bộ (Synchronous).

* Các chuẩn cho giao diện vật lý

Trước khi vào phần này hãy làm quen với hai thuật ngữ mới, đó là thiết bị cuối dữ liệu (Data Terminal Equipment – DTE) và thiết bị cuối kênh dữ liệu (Data Circuit Terminal Equipment – DCE).

DTE là một thuật ngữ chung để chỉ các máy của người sử dụng cuối (end-user), có thể là máy tính hoặc một trạm cuối (terminal). Tất cả các ứng dụng của người dùng đều

nằm ở DTE. Mục đích của việc nối mạng chính là để nối các DTE lại với nhau để chia sẻ tài nguyên, lưu trữ thông tin chung và trao đổi dữ liệu.

DCE là thuật ngữ chung chỉ các thiết bị làm nhiệm vụ kết nối các DTE với đường truyền. Nó có thể là một Modem, Transducer, Multiplexing. DCE có thể được cài đặt ngay bên trong DTE hoặc đứng riêng như một thiết bị độc lập. Chức năng chủ yếu của nó là chuyển đổi tín hiệu biểu diễn dữ liệu của người dùng thành tín hiệu chấp nhận được bởi đường truyền và ngược lại.

Trong hình 2.1 ở trên, các hệ thống mở A, B chính là các DTE, còn các Modem C, D và Transducer E, F đóng vai trò là các DCE.

Đa số các trường hợp kết nối mạng máy tính sử dụng cùng một kiểu giao diện vật lý để thuận tiện cho việc truyền thông trực tiếp giữa các sản phẩm khác loại, khỏi phải thực hiện việc chuyển đổi rắc rối. Các đặc tả về hoạt động của các DTE và DCE được đưa ra bởi nhiều tổ chức chuẩn hóa như CCITT, EIA và IEEE. ISO cũng đã công bố các đặc tả về các đầu nối cơ học kết nối giữa các DCE và DTE.

Việc truyền dữ liệu chủ yếu được thực hiện thông qua mang điện thoại, bởi thế các tổ chức trên đã đưa ra nhiều khuyến nghị về vấn đề này. Các khuyến nghị loại V và loại X của CCITT là một ví dụ điển hình. Chúng là các đặc tả ở lớp vật lý được sử dụng phổ biến nhất trên thế giới, đặc biệt là ở Tây Âu. Bên cạnh đó các chuẩn thuộc họ RS- (nay đã đổi thành EIA-) của EIA cũng đã được sử dụng rất phổ biến, đặc biệt là ở Bắc Mỹ. Dưới đây là một số chuẩn thông dụng nhất.

- V24/RS-232-C:

Là hai họ chuẩn tương ứng của CCITT và EIA nhằm định nghĩa giao diện vật lý giữa DTE và DCE (giữa máy tính và Modem chẳng hạn). Về phương diện cơ, các sản phẩm này sử dụng các đầu nối 25 chân (25-pin connector). Về điện, các chuẩn này quy định các tín hiệu số nhị phân 0 và 1 tương ứng với các thế hiệu nhỏ hơn -3V và lớn hơn +3V. Tốc độ tín hiệu không vượt quá 20 Kbps với khoảng cách tối đa là 15m.

Trong trường hợp đặc biệt, khi khoảng cách giữa các thiết bị quá gần đến mức cho phép hai DTE có thể truyền trực tiếp tín hiệu với nhau, lúc đó các mạch RS-232-C vẫn có thể được dùng nhưng không cần có mặt DCE nữa. Từ năm 1987, RS-232-C đã được sửa đổi và đặt tên lại là EIA-232-D.

- RS-449/422-A/423-A:

Nhược điểm chính của V24/RS-232-C là sự hạn chế về tốc độ và khoảng cách. Để cải thiện yếu điểm đó, EIA đã đưa ra một tập các chuẩn mới để thay thế, đó là RS-449, RS-422-A và RS-423-A. Mặc dù chuẩn RS-232-C vẫn được sử dụng nhiều nhất cho giao diện DTE/DCE, nhưng các chuẩn mới nói trên cũng đang ngày càng được sử dụng nhiều hơn. RS-449 định nghĩa các đặc trưng cơ, chức năng, còn RS-422-A và RS-423-A định nghĩa các đặc trưng về điện của chuẩn mới.

RS-449 tương tự như RS-232-C và có thể liên tác với chuẩn cũ. Về phương diện chức năng, RS-449 giữ lại toàn bộ các mạch của RS-232-C (trừ mạch AA), và thêm vào 10 mạch mới, trong đó có các mạch quan trọng là: IS, NS, SF, LL, RL, TM. Về phương diện cơ, RS-449 dùng đầu nối 37-chân cho giao diện cơ bản và dùng một đầu nối 9 chân riêng biệt cho kênh phụ. Song trong nhiều trường hợp, chỉ có một số chân được sử dụng.

Về phương diện thủ tục, RS-449 tương tự như RS-232-C. Mỗi mạch có chức năng riêng và việc truyền tin dựa trên các cặp “tác động-phản ứng”. Ví dụ DTE thực hiện Request to Send thì sau đó nó sẽ đợi DCE trả lời với Clear to Send.

Cải tiến chủ yếu của RS-449 so với RS-232-C là ở các đặc trưng về điện, và các chuẩn RS-422-A, RS-423-A định nghĩa các đặc trưng đó. Trong khi RS-232-C được thiết kế ở thời đại của các linh kiện điện tử rời rạc thì các chuẩn mới đã được tiếp nhận các ưu việt của công nghệ mạc tổ hợp (IC). RS-423-A sử dụng phương thức truyền thông không cân bằng, đạt tốc độ 3Kbps ở khoảng cách 1000m và 300 Kbps ở khoảng cách 10m.

Trong khi đó, RS-422-A sử dụng phương thức truyền thông cân bằng, đạt tốc độ 100Kbps ở khoảng cách 1200m và tới 10 Mbps ở khoảng cách 12m.

Ngoài các chuẩn trên EIA còn phát triển các chuẩn khác như EIA-530 để thay thế cho EIA-232 trong trường hợp các giao đổi hỏi tốc độ cao hơn 20Kbps, hay EIA-366 định nghĩa giao diện cho các thiết bị tự động, một modem và một DTE.

2.2. Môi trường truyền thông

2.2.1. Kênh truyền hữu tuyến

Cáp thuộc loại kênh truyền hữu tuyến được sử dụng để nối máy tính và các thành phần mạng lại với nhau. Hiện nay có 3 loại cáp được sử dụng phổ biến là: Cáp xoắn đôi (twisted pair), cáp đồng trục (coax) và cáp quang (fiber optic). Việc chọn lựa loại cáp sử dụng cho mạng tùy thuộc vào nhiều yếu tố như: giá thành, khoảng cách, số lượng máy tính, tốc độ yêu cầu, băng thông.

- Cáp xoắn đôi (Twisted Pair)

Cáp xoắn đôi có hai loại: Có vỏ bọc (Shielded Twisted Pair - STP) và không có vỏ bọc (Unshielded Twisted Pair - UTP). Cáp xoắn đôi có vỏ bọc sử dụng một vỏ bọc đặc biệt quấn xung quanh dây dẫn có tác dụng chống nhiễu. Cáp xoắn đôi trở thành loại cáp mạng được sử dụng nhiều nhất hiện nay.



Hình 2. 2 Cáp xoắn đôi

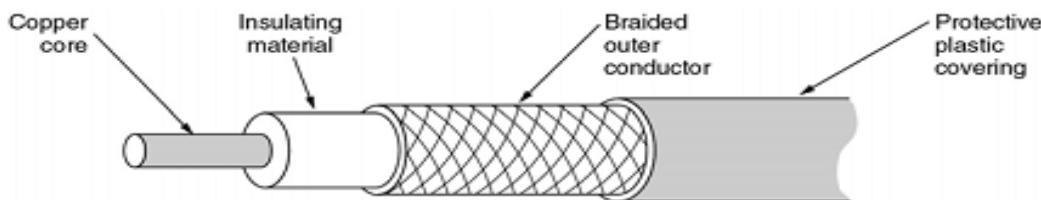
Nó hỗ trợ hầu hết các khoảng tốc độ và các cấu hình mạng khác nhau và được hỗ trợ bởi hầu hết các nhà sản xuất thiết bị mạng.

Các đặc tính cáp xoắn đôi:

- Được sử dụng trong mạng token ring (cáp loại 4 tốc độ 16Mbps), chuẩn mạng Ethernet 10BaseT (Tốc độ 10Mbps), hay chuẩn mạng 100BaseT (tốc độ 100Mbps)
- Giá cả chấp nhận được.
- UTP thường được sử dụng bên trong các tòa nhà vì nó ít có khả năng chống nhiễu hơn so với STP.
 - Cáp loại 2 có tốc độ đạt đến 1Mbps (cáp điện thoại).
 - Cáp loại 3 có tốc độ đạt đến 10Mbps (Dùng trong mạng Ethernet 10BaseT)
 - Cáp loại 5 có tốc độ đạt đến 100Mbps (dùng trong mạng 10BaseT và 100BaseT)
 - Cáp loại 5E và loại 6 có tốc độ đạt đến 1000 MBps (dùng trong mạng 1000 BaseT)

- Cáp đồng trục (Coaxial Cable).

Cáp đồng trục là loại cáp được chọn lựa cho các mạng nhỏ ít người dùng, giá thành thấp. Có cáp đồng trục gầy (thin coaxial cable) và cáp đồng trục béo (thick coaxial



cable).

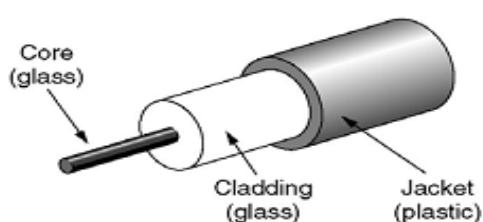
Hình 2. 3 Cáp đồng trục

Cáp đồng trục gầy, ký hiệu RG-58AU, được dùng trong chuẩn mạng Ethernet 10Base2.

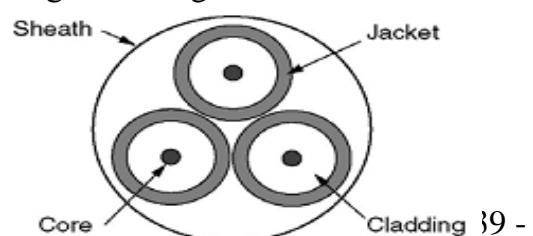
Cáp đồng trục béo, ký hiệu RG-11, được dùng trong chuẩn mạng 10Base5

- Cáp quang (Fiber Optic)

Cáp quang truyền tải các sóng điện từ dưới dạng ánh sáng. Thực tế, sự xuất hiện của một sóng ánh sáng tương ứng với bit “1” và sự mất ánh sáng tương ứng với bit “0”. Các tín hiệu điện tử được chuyển sang tín hiệu ánh sáng bởi bộ phát, sau đó các tín hiệu ánh sáng sẽ được chuyển thành các sóng điện tử bởi bộ nhận. Nguồn phát quang có thể là các đèn LED (Light Emitting Diode) cổ điển, hay các diod laser. Bộ dò ánh sáng có thể là các tế bào quang điện truyền thông hay các tế bào quang điện dạng khói.



a. Cáp Single mode



b. Cáp Multi mode

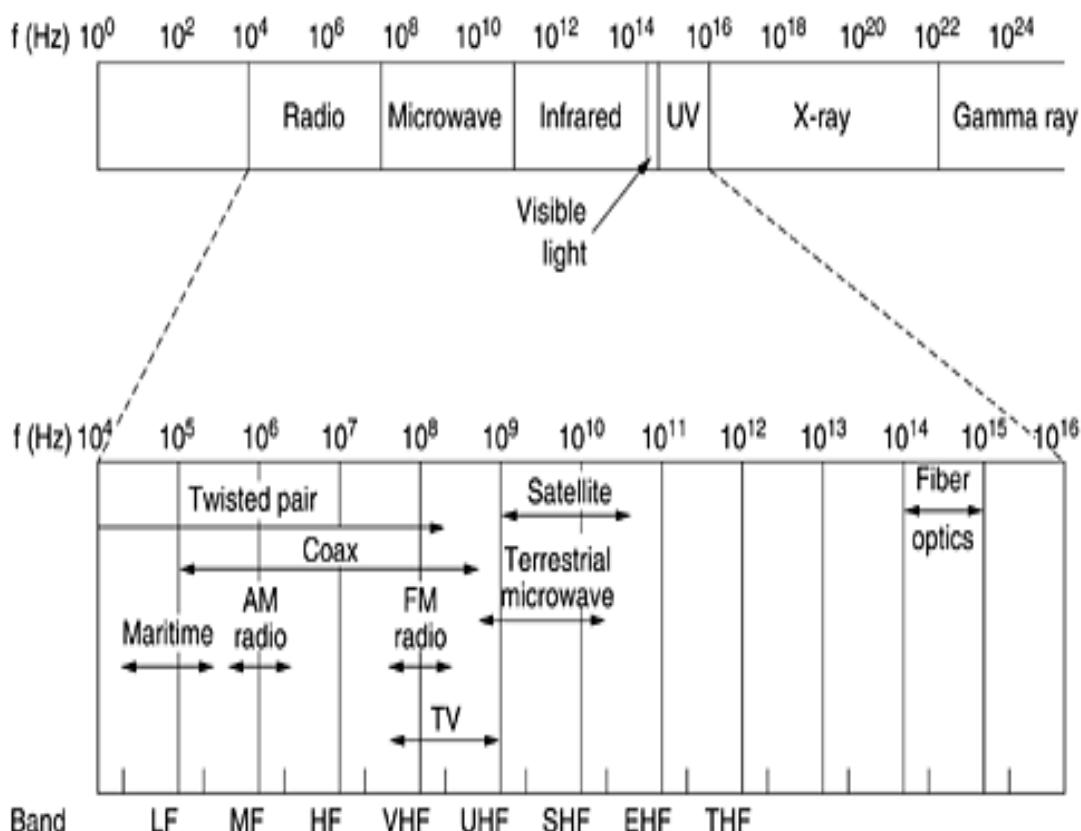
Hình 2. 4 Cấu trúc cáp quang

2.2.2 Kênh truyền vô tuyến

Kênh truyền vô tuyến thì thật sự tiện lợi, đặc biệt ở những địa hình mà kênh truyền hữu tuyến không thể thực hiện được hoặc phải tốn nhiều chi phí. Kênh truyền vô tuyến truyền tải thông tin ở tốc độ ánh sáng.

Gọi:

- f_c là tốc độ ánh sáng,
- f là tần số của tín hiệu sóng
- λ là độ dài sóng.



Hình 2. 5 Kênh truyền

Tín hiệu có độ dài sóng càng lớn thì khoảng cách truyền càng xa mà không bị suy giảm, ngược lại những tín hiệu có tần số càng cao thì có độ phát tán càng thấp.

2.2.3 Một số thiết bị cơ bản của lớp vật lý

* Bộ lặp – Repeater.

Repeater là loại thiết bị phần cứng đơn giản nhất trong các thiết bị liên kết mạng, nó được hoạt động trong lớp vật lý của mô hình hệ thống mở OSI. Repeater dùng để nối 2 mạng giống nhau hoặc các phần một mạng cùng có một nghi thức và một cấu hình. Khi Repeater nhận được một tín hiệu từ một phía của mạng thì nó sẽ phát tiếp vào phía kia của mạng.



Hình 2. 6 Thiết bị Repeater

Repeater không có xử lý tín hiệu mà nó chỉ loại bỏ các tín hiệu méo, nhiễu, khuếch đại tín hiệu đã bị suy hao (vì đã được phát với khoảng cách xa) và khôi phục lại tín hiệu ban đầu. Việc sử dụng Repeater đã làm tăng thêm chiều dài của mạng. Hiện nay có hai loại Repeater đang được sử dụng là Repeater điện và Repeater điện quang.

Repeater điện nối với đường dây điện ở cả hai phía của nó, nó nhận tín hiệu điện từ một phía và phát lại về phía kia. Khi một mạng sử dụng Repeater điện để nối các phần của mạng lại thì có thể làm tăng khoảng cách của mạng, nhưng khoảng cách đó luôn bị hạn chế bởi một khoảng cách tối đa do độ trễ của tín hiệu. Ví dụ với mạng sử dụng cáp đồng trục 50 thì khoảng cách tối đa là 2.8 km, khoảng cách đó không thể kéo thêm cho dù sử dụng thêm Repeater.

Repeater điện quang liên kết với một đầu cáp quang và một đầu là cáp điện, nó chuyển một tín hiệu điện từ cáp điện ra tín hiệu quang để phát trên cáp quang và ngược lại. Việc sử dụng Repeater điện quang cũng làm tăng thêm chiều dài của mạng.

Việc sử dụng Repeater không thay đổi nội dung các tín hiệu đi qua nên nó chỉ được dùng để nối hai mạng có cùng kiểu (như hai mạng Ethernet hay hai mạng Token ring) nhưng không thể nối hai mạng có giao thức truyền thông khác nhau (như một mạng Ethernet và một mạng Token ring). Thêm nữa Repeater không làm thay đổi khối lượng chuyển vận trên mạng nên việc sử dụng không tính toán nó trên mạng lớn sẽ hạn chế hiệu năng của mạng. Khi lựa chọn sử dụng Repeater cần chú ý lựa chọn loại có tốc độ chuyển vận phù hợp với tốc độ của mạng.

* Bộ tập trung – Hub.

Hub được coi là Repeater có nhiều cổng. Một Hub có từ 4 đến 24 cổng và có thể nhiều hơn.

Khi cấu hình mạng hình sao (Topo Star) thì Hub đóng vai trò là trung tâm của mạng. Với một Hub, thông tin đưa vào từ một cổng và sẽ được đưa đến tất cả các cổng khác.

Làm việc với lớp thứ nhất của mô hình OSI - lớp vật lý



Hình 2. 7 Bộ tập trung Hub

Phân biệt các Hub thành 3 loại như sau:

- *Hub bị động (Passive Hub)*: Hub bị động không chứa các linh kiện điện tử và cũng không xử lý các tín hiệu dữ liệu, nó có chức năng duy nhất là tổ hợp các tín hiệu từ một số đoạn cáp mạng. Khoảng cách giữa một máy tính và Hub không thể lớn hơn một nửa khoảng cách tối đa cho phép giữa 2 máy tính trên mạng (ví dụ khoảng cách tối đa cho phép giữa 2 máy tính của mạng là 200m thì khoảng cách tối đa giữa một máy tính và hub là 100m). Các mạng ARCnet thường dùng Hub bị động.

- *Hub chủ động (Active Hub)*: Hub chủ động có các linh kiện điện tử có thể khuếch đại và xử lý các tín hiệu điện tử truyền giữa các thiết bị của mạng. Quá trình xử lý tín hiệu được gọi là tái sinh tín hiệu, nó làm cho tín hiệu trở nên tốt hơn, ít nhạy cảm với lỗi do vậy khoảng cách giữa các thiết bị có thể tăng lên. Tuy nhiên những ưu điểm đó cũng kéo theo giá thành của Hub chủ động cao hơn nhiều so với Hub bị động. Các mạng Token ring có xu hướng dùng Hub chủ động.

- *Hub thông minh (Intelligent Hub)*: cũng là Hub chủ động nhưng có thêm các chức năng mới so với loại trước, nó có thể có bộ vi xử lý của mình và bộ nhớ mà qua đó nó không chỉ cho phép điều khiển hoạt động thông qua các chương trình quản trị mạng mà nó có thể hoạt động như bộ tìm đường hay một cầu nối. Nó có thể cho phép tìm đường cho gói tin rất nhanh trên các cổng của nó, thay vì phát lại gói tin trên mọi cổng thì nó có thể chuyển mạch để phát trên một cổng có thể nối tới trạm đích.

2.3 Truyền tin tương tự

2.3.1. Hệ thống điện thoại

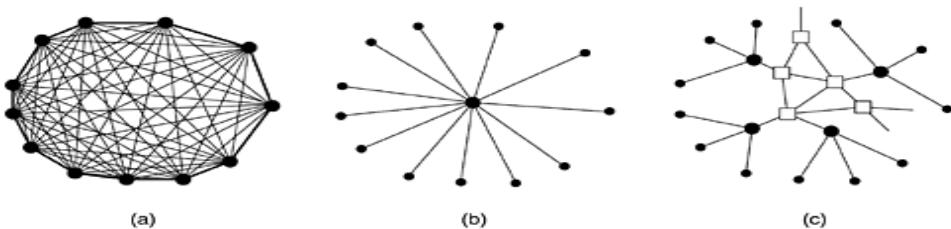
Để truyền số liệu có thể dùng mạng điện thoại hoặc đường truyền riêng có tốc độ cao. Dịch vụ truyền số liệu bằng điện thoại là một trong những dịch vụ đầu tiên về truyền số liệu.

Mạng điện thoại có thể nối đầy đủ, chuyển mạch tập trung hoặc phân cấp 2 mức. Khi 2 điện thoại cùng mắc vào một chuyển mạch địa phương thì chuyển mạch này sẽ nối 2 điện thoại này với nhau. Nếu hai điện thoại nối vào hai chuyển mạch địa phương khác nhau và hai chuyển mạch này cùng nối với một khu vực thì hai điện thoại được nối qua chuyển mạch địa phương và chuyển mạch khu vực, nếu ở xa nữa thì nó được nối qua chuyển mạch trung tâm. Phụ thuộc vào dung lượng cần truyền mà dùng đôi dây xoắn, cáp đồng trực, hay cáp quang.

Khi hai máy tính thuộc sở hữu của cùng một công ty hoặc tổ chức và nằm gần nhau cần liên lạc với nhau, việc chạy cáp giữa chúng thường dễ dàng nhất. Mô hình mạng LAN hoạt động theo cách này. Tuy nhiên, khi khoảng cách lớn hoặc có nhiều máy tính hoặc dây cáp phải đi qua đường công cộng hoặc đường truyền công cộng khác, chi phí chạy cáp riêng thường phức tạp. Do đó, các nhà thiết kế mạng phải dựa vào các cơ sở viễn thông hiện có. Các cơ sở này, đặc biệt là PSTN (Mạng điện thoại chuyển mạch công cộng - Public Switched Telephone Network), thường được thiết kế từ nhiều năm trước, với mục tiêu hoàn toàn khác. Nhưng tình hình đang thay đổi nhanh chóng với sự ra đời của cáp quang và công nghệ kỹ thuật số. Trong mọi trường hợp, hệ thống điện thoại được kết hợp chặt chẽ với các mạng máy tính (diện rộng), đáng để dành thời gian nghiên cứu về nó.

Cấu trúc hệ thống điện thoại công cộng

Ngay sau khi Alexander Graham Bell cấp bằng sáng chế cho điện thoại vào năm 1876 (chỉ vài giờ trước đối thủ của ông, Elisha Gray), đã có một nhu cầu rất lớn cho phát minh mới của ông. Thị trường ban đầu là để bán điện thoại, mà đi theo cặp. Tùy thuộc vào khách hàng để xâu một sợi dây giữa họ. Nếu một chủ sở hữu điện thoại muốn nói chuyện với n chủ sở hữu điện thoại khác, các dây riêng biệt phải được nối vào tất cả các nhà n. Trong vòng một năm, các thành phố được bao phủ bởi những sợi dây điện đi qua những ngôi nhà. Rõ ràng là mô hình kết nối mọi điện thoại với mọi điện thoại khác, như trong Hình 2-8 (a), sẽ không hoạt động.



Hình 2. 8 (a) Mạng kết nối đầy đủ. (b) Công tắc tập trung. (c) Hệ thống phân cấp hai cấp.

Với uy tín của mình, Bell đã nhìn thấy điều này và thành lập Công ty Điện thoại Bell, mở văn phòng chuyển mạch đầu tiên (ở New Haven, Connecticut) vào năm 1878. Công ty đã điều hành một dây đến từng nhà hoặc văn phòng của khách hàng. Để thực hiện cuộc gọi, khách hàng sẽ quay điện thoại để phát ra tiếng chuông trong văn phòng

công ty điện thoại để thu hút sự chú ý của một nhà điều hành, người sau đó sẽ kết nối thủ công người gọi với callee bằng cách sử dụng cáp nhảy. Mô hình của một văn phòng chuyển mạch đơn được minh họa trong Hình 2-8 (b).

Ngay sau đó, các văn phòng chuyển mạch của Hệ thống Bell đã mọc lên khắp nơi và mọi người muốn thực hiện các cuộc gọi đường dài giữa các thành phố, vì vậy hệ thống Bell bắt đầu kết nối các văn phòng chuyển mạch. Vấn đề là kết nối mọi văn phòng chuyển mạch với mọi văn phòng chuyển mạch khác bằng một sợi dây giữa chúng nhanh chóng trở nên không thể quản lý được, vì vậy các văn phòng chuyển mạch cấp hai đã được phát minh. Sau một thời gian, nhiều văn phòng cấp hai là cần thiết, như được minh họa trong Hình 2-8 (c). Cuối cùng, hệ thống phân cấp đã tăng lên năm cấp.

Đến năm 1890, ba bộ phận chính của hệ thống điện thoại đã được đưa ra: văn phòng chuyển mạch, dây nối giữa khách hàng và văn phòng chuyển mạch (bằng cách bây giờ là cặp cân bằng, cách điện, xoắn thay vì dây mờ với trở lại trái đất) và dài kết nối giữa các văn phòng chuyển mạch.

Trước khi AT&T chia tay năm 1984, hệ thống điện thoại được tổ chức theo hệ thống phân cấp rất đa dạng, dư thừa. Mô tả sau đây rất đơn giản nhưng vẫn mang lại hương vị thiết yếu. Mỗi điện thoại có hai dây đồng đi ra từ nó đi thẳng đến văn phòng cuối gần nhất của công ty điện thoại (còn gọi là văn phòng trung tâm địa phương). Khoảng cách thường là 1 đến 10 km, ở thành phố ngắn hơn ở nông thôn. Chỉ riêng ở Hoa Kỳ có khoảng 22.000 văn phòng cuối. Các kết nối hai dây giữa điện thoại của mỗi thuê bao và văn phòng cuối được gọi là giao dịch địa phương. Nếu các vòng địa phương trên thế giới được kéo dài từ đầu đến cuối, chúng sẽ kéo dài tới mặt trăng và quay lại 1000 lần.

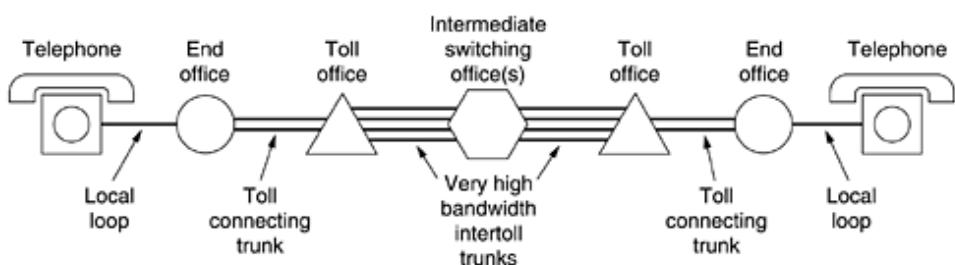
Đã có lúc, 80 phần trăm giá trị vốn của AT&T là đồng trong các vòng địa phương. AT&T sau đó, trên thực tế, là mỏ đồng lớn nhất thế giới. May mắn thay, thực tế này đã không được biết đến rộng rãi trong cộng đồng đầu tư. Nếu được biết, một số người đột kích của công ty có thể đã mua AT&T, chấm dứt tất cả các dịch vụ điện thoại ở Hoa Kỳ, xé tất cả dây và bán dây cho một nhà tinh chế đồng để được hoàn vốn nhanh chóng.

Nếu một thuê bao được gắn vào một văn phòng cuối cụ thể gọi một thuê bao khác được gắn vào cùng một văn phòng cuối, cơ chế chuyển mạch trong văn phòng sẽ thiết lập kết nối điện trực tiếp giữa hai vòng cục bộ. Kết nối này vẫn còn nguyên trong suốt thời gian của cuộc gọi.

Nếu điện thoại được gọi được gắn vào một văn phòng cuối khác, một quy trình khác phải được sử dụng. Mỗi văn phòng cuối có một số đường dây gửi đến một hoặc nhiều trung tâm chuyển mạch gần đó, được gọi là văn phòng thu phí (hoặc nếu chúng ở trong cùng một khu vực địa phương, văn phòng song song). Những dòng này được gọi là thân kết nối thu phí. Nếu cả hai văn phòng cuối của người gọi và callee đều có một trạm thu phí kết nối với cùng một văn phòng thu phí (có thể xảy ra nếu họ ở gần nhau), kết nối

có thể được thiết lập trong văn phòng thu phí. Một mạng điện thoại chỉ bao gồm điện thoại (các chấm nhỏ), văn phòng cuối (các chấm lớn) và văn phòng thu phí (các ô vuông) được hiển thị trong Hình 2-8 (c).

Nếu người gọi và callee không có văn phòng thu phí chung, đường dẫn sẽ phải được thiết lập ở đâu đó cao hơn trong hệ thống phân cấp. Các văn phòng chính, bộ phận và khu vực tạo thành một mạng lưới mà các văn phòng thu phí được kết nối. Các trao đổi thu phí, chính, mặt cắt và khu vực giao tiếp với nhau thông qua các đường trực xen kẽ băng thông cao (còn được gọi là các đường trực xen kẽ). Số lượng các loại trung tâm chuyển mạch khác nhau và cấu trúc liên kết của chúng (ví dụ: hai văn phòng có thể có kết



nối trực tiếp hoặc chúng phải đi qua một văn phòng khu vực?) Thay đổi tùy theo quốc gia tùy thuộc vào mật độ điện thoại của quốc gia. Hình 2-9 cho thấy cách kết nối khoảng cách trung bình có thể được định tuyến.

Hình 2. 9 Một tuyến đường điển hình cho một cuộc gọi khoảng cách trung bình.

Trước đây, việc truyền tải trên toàn hệ thống điện thoại là tương tự, với tín hiệu thoại thực tế được truyền dưới dạng điện áp từ nguồn đến đích. Với sự ra đời của cáp quang, thiết bị điện tử kỹ thuật số và máy tính, tất cả các thân và công tắc hiện là kỹ thuật số, để lại vòng lặp cục bộ là phần cuối cùng của công nghệ analog trong hệ thống. Truyền kỹ thuật số được ưa thích vì không cần thiết phải tái tạo chính xác một dạng sóng tương tự sau khi nó đã đi qua nhiều bộ khuếch đại trong một cuộc gọi dài. Có thể phân biệt chính xác 0 với 1 là đủ. Đặc tính này làm cho truyền dẫn kỹ thuật số đáng tin cậy hơn so với analog. Nó cũng rẻ hơn và dễ dàng hơn để duy trì.

Tóm lại, hệ thống điện thoại bao gồm ba thành phần chính:

- Các vòng lặp cục bộ (cặp xoắn tương tự đi vào nhà và doanh nghiệp).
- Trunks (sợi quang kỹ thuật số kết nối các văn phòng chuyển mạch).
- Chuyển văn phòng (nơi các cuộc gọi được chuyển từ một thân cây khác).

Hệ thống truyền dẫn trong mạng điện thoại

Là môi trường truyền dẫn tín hiệu trong mạng điện thoại đảm bảo độ suy hao cho phép và thỏa mãn các yêu cầu về:

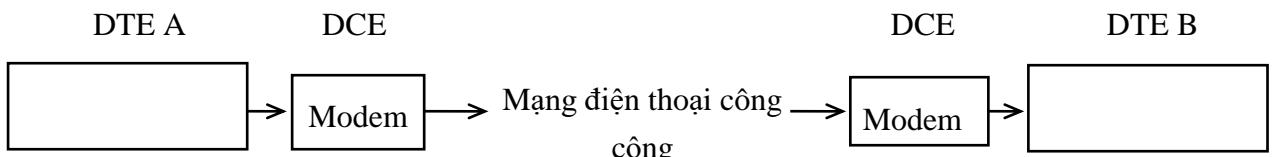
- Dung lượng thuê bao và tốc độ phát triển thuê bao
 - + Điều kiện địa lý, khí hậu thời tiết

- + Các yếu tố về quy hoạch đô thị
 - + Thuận tiện cho bảo dưỡng, sửa chữa
 - + Tiết kiệm chi phí
- Tùy theo số lượng thuê bao hay tốc độ phát triển thuê bao chia thành:
- + Mạng điện thoại không phân vùng
 - + Mạng điện thoại phân vùng

2.3.2. Modem

Là bộ điều chế và giải điều chế để biến đổi các tín hiệu số thành tín hiệu tương tự và ngược lại trên mạng thoại.

Sơ đồ đơn giản truyền tin giữa A và B:



Hình 2. 10 Bộ điều chế

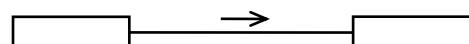
Tín hiệu số từ máy tính đến Modem, được Modem biến đổi thành tín hiệu tương tự để có thể đi qua mạng thoại. Tín hiệu này đến Modem ở điểm B được biến đổi ngược lại thành tín hiệu số đưa vào máy tính ở B.

Các kỹ thuật điều chế cơ bản:

- ✓ Điều chế biến đổi biên độ (Amplitude Modulation)
- ✓ Điều chế tần số (Frequency Modulation)
- ✓ Điều chế Pha (Phase Modulation)

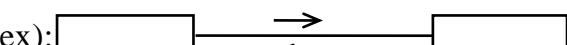
Các phương thức truyền giữa hai điểm có thể là:

- Đơn công (Simplex):



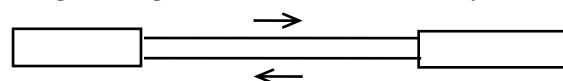
Chỉ cho phép truyền một hướng.

- Bán song công (Half - duplex):



Có thể truyền theo hai hướng nhưng mỗi thời điểm chỉ truyền một hướng.

- Song công (Duplex):



Có thể nhận hoặc phát cùng một lúc.

Các Modem hiện đại đều có kiểu hoạt động ở hai chế độ song công và bán song công.

2.4. Truyền tín hiệu số

Cùng với tiến bộ của máy tính và điện tử số, các chuyển mạch trung tâm dần dần chuyển sang dùng truyền số (Phát đi các Bit 0 và 1 thay thế các tín hiệu liên tục). Cho thấy những ưu việt của truyền số so với truyền tương tự:

Độ tin cậy cao vì chỉ có những giá trị 0 và 1, giảm được lỗi do suy giảm và nhiễu trên đường dây gây ra.

- ✓ Tốc độ truyền số liệu cao hơn.
- ✓ Thiết bị truyền số dùng cho cả điện thoại, số liệu, âm nhạc, hình ảnh.
- ✓ Giá máy tính và vi mạch rẻ, nên truyền số rẻ hơn truyền tương tự.

2.4.1. Điều chế xung mã -PCM (Pulse Code Modulation)

Khi có cuộc gọi qua chuyển mạch số (Digital End Office), tín hiệu phát ra là tín hiệu Analog. Tín hiệu này được số hóa ở End Office bởi Code, tạo nên số 7 hay 8 bit. Codec là ngược của Modem. Modem đổi dòng bit số thành tín hiệu Analog được điều chế, Codec đổi tín hiệu Analog thành dòng bit số.

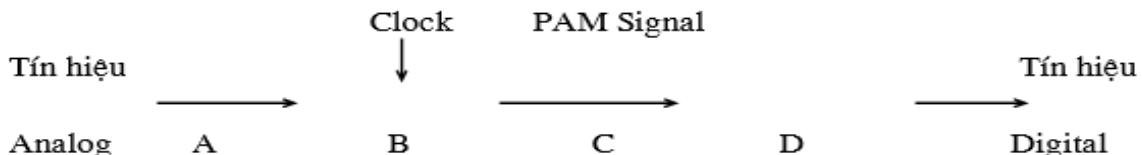
Nguyên lý làm việc của Codec:

Kỹ thuật này được gọi là PMC (Pulse Code Modulation) Codec làm 8000 mẫu/sec ứng với dải băng 4Khz.

Phương pháp đang được dùng rộng rãi là TRIBUNAL DESCONOMIE1 carrier của Bell System. T1 Carrier có thể quản lý 24 kênh thoại. Các tín hiệu tương tự được lấy mẫu qua Codec đầu ra là Digital Output.

Tốc độ truyền là 1,554 Mbps, Bell system có thêm các chuẩn T2, T3, T4 ở 6.312, 44.763, 565.148 Mbps.

Nguyên lý điều chế tín hiệu:



Áp dụng định lý Nyquist cho việc biến đổi tín hiệu Analog và Digital, tần số trích mẫu chỉ cần gấp đôi tần số của tín hiệu tương tự thì đã khôi phục được tín hiệu tương tự (Analog), (Giả sử kênh tiếng nói dải tần 4 KHz thì tần số lấy mẫu là 8 KHz).

Hãng Bell đưa ra đường truyền 24 kênh tiếng nói (T1) mỗi tín hiệu được mã hóa 8 bits.

Chuẩn T2 = 4.T1 = 96 kênh tiếng nói - tốc độ 6.312 Mbít/s.

T3 = 7.T2 = 672 kênh tiếng nói - tốc độ 44.736 Mbít/s

T4 = 6.T3 = 4032 kênh tiếng nói - tốc độ 274.176 Mbít/s.

2.4.2. Chuẩn X 21

Đây là chuẩn khuyến nghị loại X21 đặc tả một đầu nối 15 chân với các mạch được chỉ ra trong bảng. Giống như RS-232-C và R-449, nó có một mạch truyền theo cả hai chiều (T và R). Tuy vậy các mạch đó ở đây có thể cung cấp cả dữ liệu người sử dụng lẫn thông tin điều khiển và còn có thêm hai mạch khác (C và I) tương ứng cho mỗi chiều dành cho thông tin điều khiển và trạng thái. Chúng không mang các dữ liệu số mà có thể

trạng thái ON hoặc OFF. X-21 được định nghĩa chỉ cho chế độ truyền đồng bộ nên có một mạch đồng bộ bít.

X-21 chấp nhận các chế độ truyền cân bằng và không cân bằng như trong RS-422-A và RS-423-A, do vậy có cùng giới hạn tốc độ/khoảng cách.

Trong nhiều trường hợp chỉ có chế độ cân bằng được sử dụng trên tất cả các mạch. Hầu hết các thủ tục định nghĩa cho các mạch X-21 được thực hiện qua một mạng chuyền mạch kênh. X-21 thể hiện tính mềm dẻo, hiệu quả hơn so với RS-232-C và RS-449. Việc sử dụng các chuỗi ký tự điều khiển tạo ra một tập không giới hạn các khả năng tùy chọn dành cho các yêu cầu công nghệ mới.

TÓM TẮT NỘI DUNG CÓT LÕI.

- Vai trò chức năng tầng vật lý.
- Môi trường truyền thông.
- Truyền tin tương tự.
- Truyền tín hiệu số.

BÀI TẬP ÚNG DỤNG, LIÊN HỆ THỰC TẾ.

Câu 1. Cáp xoắn đôi UTP sử dụng đầu nối gì?

- A. RJ11 B.RJ45 C. BNC D. Tất cả đều đúng

Câu 2. Độ dài tối đa cho phép khi sử dụng dây cáp mạng UTP là bao nhiêu mét

- A.100 B. 185 C. 200 D. 500

Câu 3. Độ dài tối đa cho phép khi sử dụng dây cáp đồng trực mỏng là bao nhiêu mét

- A. 100 B.185 C. 200 D. 500

Câu 4. Độ dài tối đa cho phép khi sử dụng dây cáp đồng trực dày là bao nhiêu mét

- A. 100 B.185 C. 200 D.500

Câu 5. Phương tiện vật lý nào cho tỷ lệ lỗi ít nhất khi truyền thông tin

- A. Cáp đồng trực. B. Cáp xoắn đôi UTP
C.Cáp quang D. Truyền dẫn không dây (Wireless, Microware).

Chương 3. TẦNG LIÊN KẾT DỮ LIỆU: CÁC LIÊN KẾT, TRUY CẬP MẠNG VÀ CÁC LAN

Mục đích:

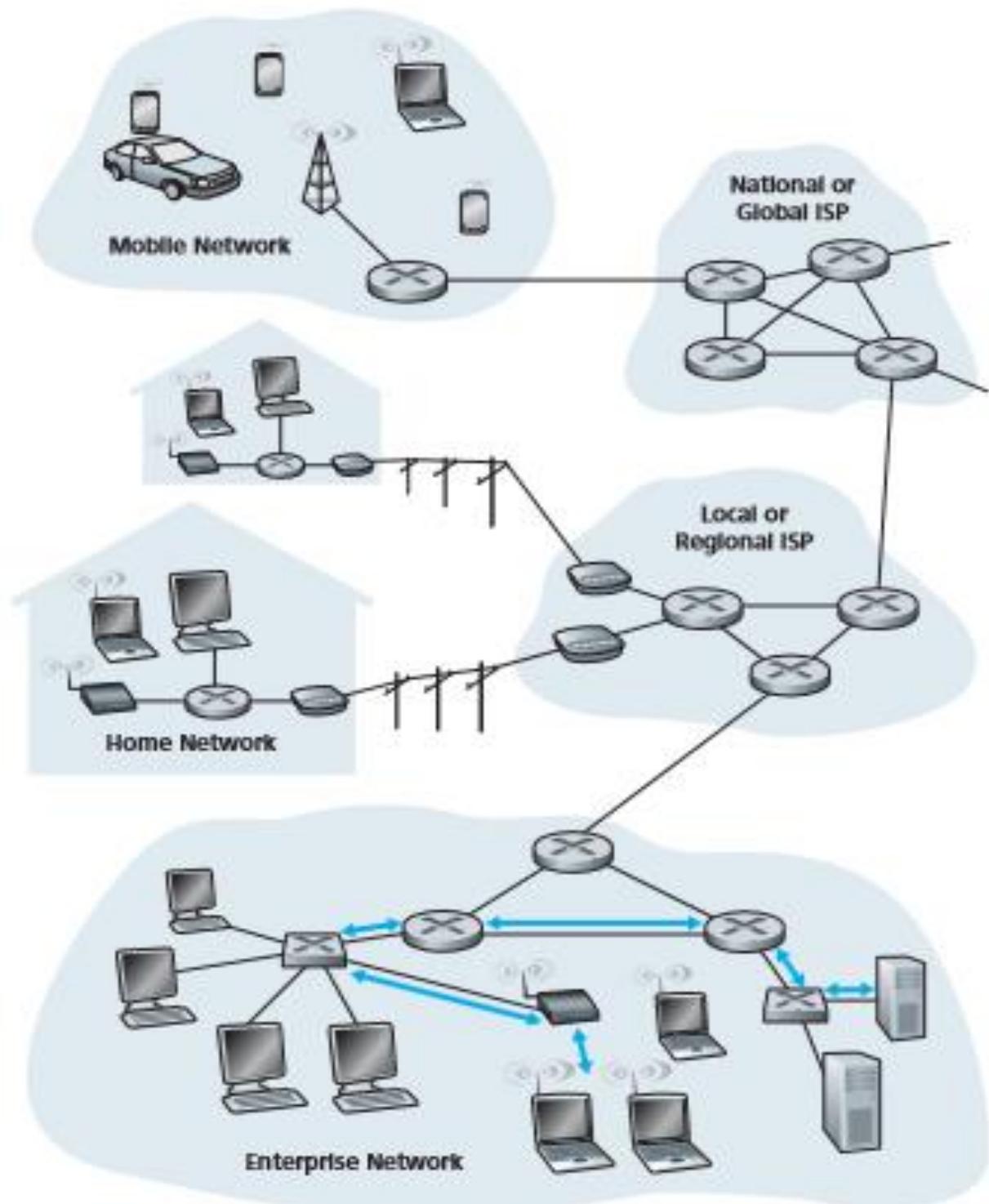
Việc xây dựng giao thức mạng chuẩn để so sánh đối chiếu các giao thức của các mạng rất quan trọng trong việc xác lập cấu hình, gỡ rối trong mạng và nâng cao chất lượng về mạng. Trên cơ sở của giao thức truyền tin để nắm được cách thức nhận biết gói tin, kiểm soát lỗi truyền tin và cơ chế kiểm soát thông lượng để giải quyết vấn đề tắc nghẽn thông tin trên mạng.

3.1 Giới thiệu về tầng Liên kết dữ liệu

Nhiệm vụ chủ yếu của tầng liên kết dữ liệu là thực hiện thiết lập các liên kết, duy trì và huỷ bỏ các liên kết dữ liệu. Kiểm soát lỗi và kiểm soát lưu lượng. Chia thông tin thành các khung thông tin (Frame), truyền các khung tuần tự và xử lý các thông điệp xác nhận (Acknowledgement Frame) từ bên máy thu gửi về. Tháo gỡ các khung thành chuỗi bít không cấu trúc chuyển xuống tầng vật lý. Tầng 2 bên thu, tái tạo chuỗi bít thành các khung thông tin. Đường truyền vật lý có thể gây lỗi, nên tầng liên kết dữ liệu phải giải quyết vấn đề kiểm soát lỗi, kiểm soát luồng, kiểm soát lưu lượng, ngăn không để nút nguồn gây “ngập lụt” dữ liệu cho bên thu có tốc độ thấp hơn. Trong các mạng quảng bá, lớp con MAC (Medium Acces Sublayer) điều khiển việc truy nhập đường truyền.

Để một datagram được chuyển từ máy chủ nguồn sang máy chủ đích, nó phải được di chuyển qua từng liên kết riêng lẻ trong đường dẫn từ đầu đến cuối. Ví dụ, trong mạng công ty được hiển thị ở cuối Hình 3.1, hãy xem xét việc gửi một datagram từ một trong các máy chủ không dây đến một trong các máy chủ. Datagram này thực sự sẽ đi qua sáu liên kết: liên kết WiFi giữa gửi máy chủ và điểm truy cập WiFi, liên kết Ethernet giữa điểm truy cập và chuyển đổi lớp liên kết; một liên kết giữa bộ chuyển đổi lớp liên kết và bộ định tuyến, một liên kết giữa hai bộ định tuyến; một liên kết Ethernet giữa bộ định tuyến và bộ chuyển mạch lớp liên kết; và cuối cùng là một liên kết Ethernet giữa bộ chuyển mạch và máy chủ. Qua một liên kết đã cho, một nút truy cập sẽ đóng gói datagram trong khung lớp liên kết và truyền khung vào liên kết. Để có được cái nhìn sâu sắc hơn nữa về tầng liên kết và cách nó liên quan đến tầng mạng. Hãy xem xét một đại lý du lịch đang lên kế hoạch cho một chuyến đi cho một khách du lịch từ Hà Nội, đến Phú Quốc. Đại lý du lịch quyết định rằng thuận tiện nhất cho khách du lịch là đi xe Ô tô từ Hà Nội đến sân bay Nội Bài, sau đó đi máy bay từ sân bay Nội Bài đến sân bay Tân Sơn Nhất, và cuối cùng là một chuyến Ô tô từ sân bay Tân Sơn Nhất di chuyển tới Phú Quốc. Khi đó đại lý du lịch thực hiện đặt phòng, trách nhiệm của công ty xe Ô tô là đưa khách du lịch từ Hà Nội đến sân bay Nội Bài; trách nhiệm của công ty hàng không là đưa khách du lịch từ sân bay Nội Bài đến sân bay Tân Sơn Nhất; và trách nhiệm của dịch vụ xe Ô tô ở sân bay Tân Sơn Nhất là đưa khách du lịch từ sân bay Tân Sơn Nhất đến Phú Quốc. Mỗi một

trong ba đoạn của chuyến đi là trực tiếp vào giữa hai địa điểm liền kề nhau. Lưu ý rằng ba phân khúc vận chuyển được quản lý bởi các công ty khác nhau và sử dụng các chế độ vận chuyển hoàn toàn khác nhau (xe Ô tô, máy bay). Mặc dù các chế độ vận chuyển là khác nhau, nhưng mỗi phương thức đều cung cấp dịch vụ cơ bản cho việc di chuyển hành khách từ một địa điểm đến một địa điểm lân cận. Tương tự vận trong chuyến này, khách du lịch là một datagram, mỗi phân đoạn vận chuyển là một liên kết, chế độ vận chuyển là



một giao thức lớp liên kết và tác nhân du lịch là một giao thức định tuyến.

Hình 3. 1 Sáu bước nhảy liên kết giữa máy chủ và thiết bị không dây

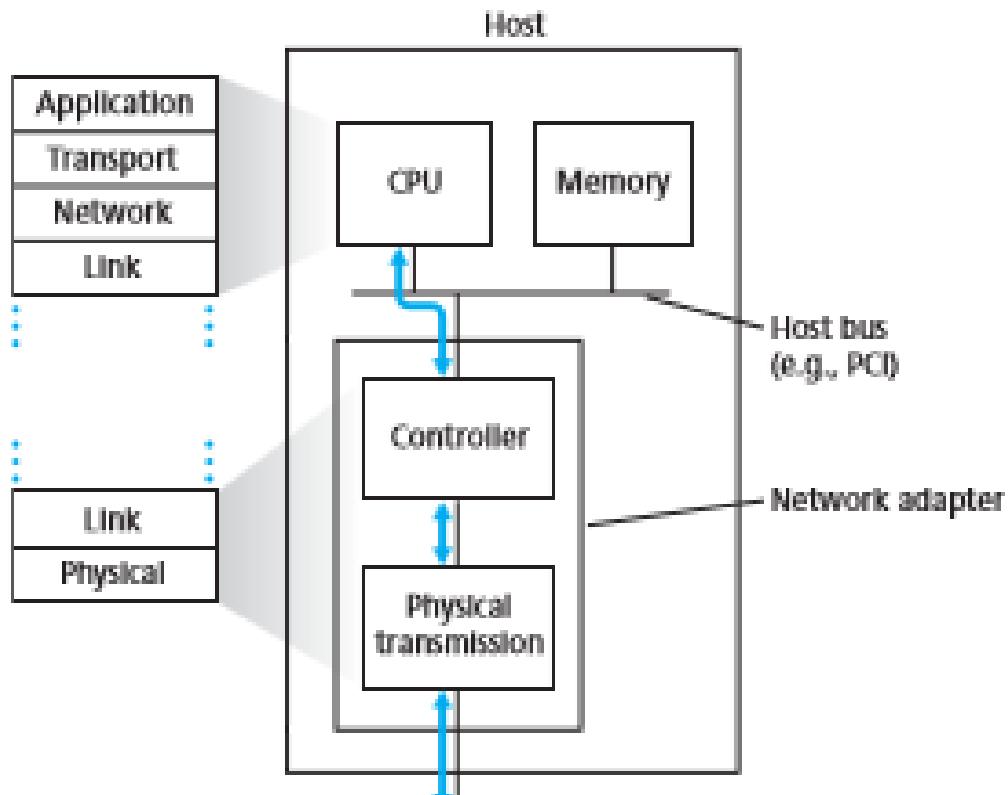
3.1.1. Các dịch vụ tầng liên kết

Mặc dù dịch vụ cơ bản của bất kỳ lớp liên kết nào là để di chuyển một datagram từ một nút sang một nút liền kề qua một liên kết giao tiếp duy nhất, các chi tiết của dịch vụ được cung cấp có thể thay đổi từ một giao thức lớp liên kết sang giao thức tiếp theo. Các giao thức tầng liên kết bao gồm:

- Đóng khung (framing). Hầu như tất cả các giao thức tầng liên kết đóng gói mỗi datagram tầng mạng trong khung tầng liên kết trước khi truyền qua liên kết. Một khung tin bao gồm một trường dữ liệu, trong đó datagram tầng mạng được chèn và một số trường tiêu đề. Cấu trúc của khung được chỉ định bởi giao thức tầng liên kết.
- Liên kết truy cập. Giao thức điều khiển truy cập (MAC) chỉ định các quy tắc mà khung được truyền lên liên kết. Đối với các liên kết điểm-điểm có một người gửi ở một đầu của liên kết và một người nhận ở đầu kia của liên kết, giao thức MAC rất đơn giản. Người gửi có thể gửi một khung bất cứ khi nào liên kết nhàn rỗi. Trường hợp khi nhiều nút chia sẻ một liên kết quảng bá duy nhất, hay còn được gọi là nhiều truy cập, giao thức MAC sẽ phục vụ cho việc phối hợp truyền các khung của nhiều nút.
- Giao hàng đáng tin cậy. Khi một giao thức lớp liên kết cung cấp dịch vụ phân phối đáng tin cậy, nó đảm bảo di chuyển từng datagram tầng mạng qua liên kết mà không gặp lỗi. Giao thức tầng vận chuyển nhất như TCP cũng cung cấp dịch vụ phân phối đáng tin cậy. Tương tự như dịch vụ giao hàng đáng tin cậy ở tầng vận chuyển, dịch vụ giao hàng đáng tin cậy ở tầng liên kết có thể đạt được bằng các xác nhận và truyền lại. Dịch vụ phân phối đáng tin cậy ở tầng liên kết thường được sử dụng cho các liên kết có tỷ lệ lỗi cao, chẳng hạn như liên kết không dây, với mục tiêu sửa lỗi cục bộ trên liên kết nơi xảy ra lỗi thay vì buộc phải truyền lại kết thúc của dữ liệu bằng giao thức tầng vận chuyển hoặc tầng ứng dụng. Tuy nhiên, phân phối đáng tin cậy ở tầng liên kết có thể được coi là chi phí không cần thiết cho các liên kết có lỗi bit thấp, bao gồm cáp đồng, cáp xoắn đôi. Vì lý do này, nhiều giao thức lớp liên kết có dây không cung cấp dịch vụ giao hàng đáng tin cậy.
- Phát hiện lỗi và sửa lỗi. Phần cứng tầng liên kết trong một nút nhận có thể quyết định không chính xác rằng một bit trong khung là 0 khi nó được truyền dưới dạng 1 và ngược lại. Lỗi bit như vậy được giới thiệu bởi sự suy giảm tín hiệu và nhiễu điện tử. Do không cần chuyển tiếp một datagram có lỗi, nhiều giao thức tầng liên kết cung cấp một cơ chế để phát hiện các lỗi bit như vậy. Điều này được thực hiện bằng cách có nút truyền bao gồm các bit phát hiện lỗi trong khung và có nút nhận thực hiện kiểm tra lỗi. Phát hiện lỗi trong tầng liên kết thường phức tạp hơn và được thực hiện trong phần cứng. Sửa lỗi tương tự như phát hiện lỗi, ngoại trừ việc người nhận không chỉ phát hiện khi xảy ra lỗi bit trong khung mà còn xác định chính xác vị trí xảy ra lỗi trong khung và sau đó sửa các lỗi này.

3.1.2. Vị trí triển khai ở tầng liên kết

Nơi lớp liên kết được thực hiện được tập trung vào một hệ thống cuối là một lớp liên kết máy chủ lưu trữ được thực hiện trong phần cứng hoặc phần mềm. Nó có thể được thực hiện trên một thẻ hoặc chip riêng biệt và nó giao tiếp với phần còn lại của một thành phần hệ điều hành và phần cứng máy chủ. Hình 3.2 cho thấy một kiến trúc máy chủ điển hình, tầng liên kết được triển khai trong bộ điều phối, đôi khi còn được gọi là thẻ giao diện mạng (NIC). Trung tâm của bộ điều phối là bộ điều khiển tầng liên kết, thường là chip đơn, mục đích là thực hiện nhiều dịch vụ của tầng liên kết (đóng khung, truy cập liên kết, phát hiện lỗi, v.v.). Do đó, phần lớn chức năng điều khiển tầng liên kết được thực hiện trong phần cứng. Ví dụ, bộ điều khiển Intel 8254x [Intel 2012] thực hiện các giao thức Ethernet. Bộ điều khiển Atheros AR5006 [Atheros 2012] thực hiện các giao thức WiFi 802.11. Cho đến cuối những năm 1990, hầu hết các bộ điều phối là các thẻ riêng biệt (như PCMCIA card hoặc thẻ cắm vào khớp với thẻ PCI của PC khe cắm) nhưng ngày càng nhiều hơn, các bộ điều phối đang được tích hợp vào bo mạch chủ của máy chủ, hay còn gọi là cầu hình LAN-on-bo mạch chủ. Về phía gửi, bộ điều khiển lấy một datagram đã được tạo và lưu trữ trong bộ nhớ máy chủ bởi các lớp cao hơn của ngăn xếp giao thức, đóng gói datagram trong khung lớp liên kết (điền vào các trường khác nhau của khung), sau đó truyền đóng khung vào liên kết truyền thông, theo giao thức truy cập liên kết. Về phía nhận, bộ điều khiển nhận toàn bộ khung và trích xuất datagram tầng



mạng. Nếu tầng liên kết thực hiện phát hiện lỗi, thì đó là bộ điều khiển gửi đặt các bit phát hiện lỗi trong tiêu đề khung và nó là bộ điều khiển nhận thực hiện phát hiện lỗi.

Hình 3. 2 Bộ điều phói

Hình 3.2 cho thấy bộ điều phói gắn với bus máy chủ (ví dụ: bus PCI hoặc PCI-X), trong đó nó trông giống như bất kỳ thiết bị I/O nào khác với các thành phần máy chủ khác. Hình 3.2 cũng cho thấy rằng trong khi hầu hết tầng liên kết được triển khai trong phần cứng, một phần của tầng liên kết được triển khai trong phần mềm chạy trên CPU máy chủ lưu trữ. Các thành phần phần mềm của tầng liên kết thực hiện chức năng liên kết cấp cao hơn như lắp ráp thông tin địa chỉ tầng liên kết và kích hoạt phần cứng bộ điều khiển. Về phía bên nhận, phần mềm tầng liên kết đáp ứng các ngắt của bộ điều khiển (ví dụ: do nhận được một hoặc nhiều khung), xử lý các điều kiện lỗi và chuyển một datagram lên tầng mạng. Do đó, tầng liên kết là sự kết hợp giữa phần cứng và phần mềm, vị trí trong ngăn xếp giao thức nơi phần mềm đáp ứng phần cứng.

3.2. Kỹ thuật phát hiện và sửa lỗi

Khi truyền đi một byte trong hệ thống máy tính thì khả năng xảy ra một lỗi do hỏng hóc ở phần nào đó hoặc do nhiễu gây nên là luôn có thể. Các kênh vào ra thường xảy ra lỗi, đặc biệt là ở truyền số liệu. Để kiểm tra lỗi ta có thể:

- + *Dùng Timer*, nghĩa là nếu quá thời gian qui định bên gửi không nhận được tín hiệu trả lời, xem như lỗi, phát lại gói tin hỏng.
- + *Đánh số Frame gửi đi*, nếu không nhận đúng thứ tự khung là lỗi, yêu cầu phát lại.
- + Để kiểm tra thu đúng gói tin gửi đi thường khi phát tin có kèm theo *trường kiểm tra lỗi* (*FCS*) bằng cách sử dụng các phương pháp sau:

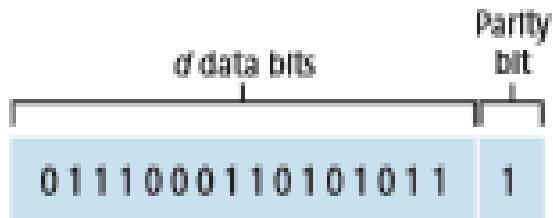
- Phương pháp bit chẵn lẻ.
- Phương pháp checksum.
- Phương pháp kiểm tra theo chu kỳ (CRC).

Khi điều khiển xử lý tiếp nhận cần phải thực hiện thủ tục điều khiển lỗi tự động bằng cách tính trường lỗi khung tin thu được so với trường lỗi truyền qua nếu đúng thì trả lời ACK, nếu sai trả lời NAK hoặc bên thu không nhận được tín hiệu ACK sau một thời gian để bên phát truyền lại khung hỏng.

3.2.1. Kiểm tra Bit chẵn lẻ

Hình thức phát hiện lỗi đơn giản nhất là sử dụng một bit chẵn lẻ. Giả sử rằng thông tin được gửi, D trong Hình 3.3, có d bit. Trong sơ đồ chẵn lẻ, người gửi chỉ cần thêm một bit bổ sung và chọn giá trị của nó sao cho tổng số 1s trong các bit $d + 1$ (thông tin ban đầu cộng với một bit chẵn lẻ) là chẵn. Đôi với các sơ đồ chẵn lẻ, giá trị bit chẵn lẻ được chọn sao cho có số lẻ là 1s. Hình 3.3 minh họa một sơ đồ chẵn lẻ, với bit chẵn lẻ được lưu trữ trong một trường riêng biệt. Hoạt động thu cũng đơn giản với một bit chẵn lẻ. Người

nhận chỉ cần đếm số lượng 1 giây trong các bit $d + 1$ nhận được. Nếu một số lẻ các bit được định giá 1 được tìm thấy với sơ đồ chẵn lẻ, người nhận biết rằng đã xảy ra ít nhất

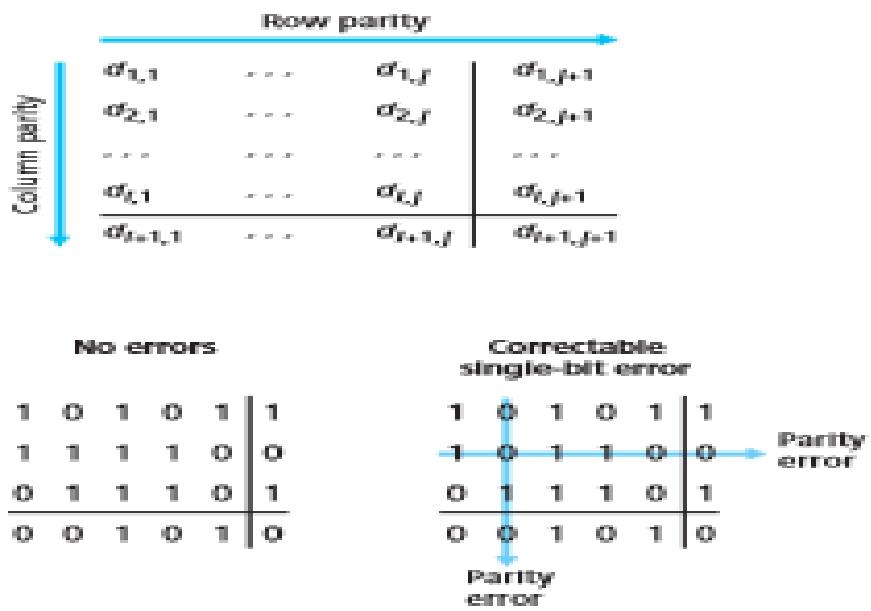


một lỗi bit. Chính xác hơn, nó biết rằng một số lỗi bit lẻ đã xảy ra. Nhưng điều gì xảy ra nếu một số bit chẵn xảy ra ? Điều này sẽ dẫn đến một lỗi không bị phát hiện. Nếu xác suất xảy ra lỗi bit là nhỏ và lỗi có thể được giả định xảy ra độc lập từ bit này sang bit khác, thì xác suất xảy ra lỗi nhiều bit trong một gói sẽ cực kỳ nhỏ.

Hình 3. 3 Chẵn lẻ một bit

Trong trường hợp này, một bit chẵn lẻ có thể đủ. Tuy nhiên, các phép đo đã chỉ ra rằng, thay vì xảy ra độc lập, các lỗi thường được nhóm lại với nhau trong các cụm. Trong điều kiện lỗi, xác suất xảy ra lỗi không được phát hiện trong khung được bảo vệ bởi tính chẵn lẻ bit có thể đạt tới 50%. Hình 3.4 cho thấy bit hai chiều của sơ đồ bit chẵn lẻ. Ở đây, các bit d trong D được chia thành i hàng và j cột. Một giá trị chẵn lẻ được tính cho mỗi hàng và cho mỗi cột. Kết quả là các bit chẵn lẻ $i, j, 1$ bao gồm các bit phát hiện lỗi của khung lớp liên kết.

Giả sử bây giờ xảy ra lỗi bit đơn trong d bit thông tin ban đầu. Với sơ đồ chẵn lẻ hai chiều này, tính chẵn lẻ của cả cột và hàng chứa bit sẽ bị lỗi. Do đó, người nhận không chỉ có thể phát hiện thực tế là đã xảy ra lỗi một bit, mà còn có thể sử dụng các chỉ số cột và hàng của cột và hàng có lỗi tương đương để thực sự xác định bit bị hỏng và sửa lỗi. Hình 3.4 cho thấy một ví dụ trong đó bit có giá trị 1 ở vị trí (2,2) bị hỏng và chuyển sang 0 0 lỗi một lỗi có thể phát hiện và sửa được tại máy thu.



Hình 3. 4 Bít chẵn lẻ hai chiều

Khả năng của người nhận để phát hiện và sửa lỗi được gọi là sửa lỗi chuyển tiếp **forward error correction** (FEC). Những kỹ thuật này thường được sử dụng trong các thiết bị lưu trữ và phát lại âm thanh như đĩa CD. Các kỹ thuật FEC có giá trị vì chúng có thể giảm số lần truyền lại của người gửi. Có lẽ quan trọng hơn, họ cho phép sửa lỗi ngay lập tức tại máy thu. Điều này tránh việc phải chờ độ trễ lan truyền khứ hồi cần thiết cho người gửi để nhận gói NAK và gói được truyền lại để truyền lại cho người nhận.

3.2.2. Phương pháp kiểm tra (checksum)

Trong các kỹ thuật kiểm tra, các bit d của dữ liệu trong Hình 3.3 được coi là một chuỗi các số nguyên k-bit. Một phương pháp kiểm tra đơn giản là chỉ cần tính tổng các số nguyên k-bit này và sử dụng tổng kết quả các bit phát hiện lỗi. Các byte dữ liệu được coi là số nguyên 16 bit và được tính tổng. Phần bù 1s của tổng này sau đó tạo thành tổng kiểm tra, người nhận kiểm tra bằng cách lấy phần bù 1s của tổng dữ liệu nhận được và kiểm tra xem kết quả có phải là tất cả 1 bit hay không. Nếu bất kỳ bit nào bằng 0, một lỗi được chỉ định (theo RFC 1071). Trong giao thức TCP và UDP, phương pháp kiểm tra được tính trên tất cả các trường (bao gồm các trường tiêu đề và dữ liệu). Trong IP, phương pháp kiểm tra được tính trên tiêu đề IP do phân đoạn UDP hoặc TCP có phần kiểm tra riêng. Phương pháp kiểm tra yêu cầu chi phí tương đối ít gói. Ví dụ, phương pháp kiểm tra trong TCP và UDP chỉ sử dụng 16 bit. Tuy nhiên, chúng cung cấp bảo vệ tương đối yếu trước các lỗi so với kiểm tra dự phòng theo chu kỳ.

3.2.3. Phương pháp kiểm tra chu kỳ (CRC)

Phương pháp này khai thác đặt trưng của các số nhị phân khi dùng phép toán modulo-2. Giả sử $M(x)$ là một số m bit cần truyền, $G(x)$ là đa thức sinh có bậc r (phần tử chia). Ta có các bước thực hiện như sau:

Bước 1: Thêm r bit 0 vào cuối xâu bit cần truyền. Xâu ghép có $m+r$ bits, tương ứng với đa thức $x^rM(x)$.

Bước 2: Chia modulo-2 xâu bit tương ứng với $x^rM(x)$ cho xâu bit tương ứng với $G(x)$.

Bước 3: Lấy số bị chia trong bước 2 trừ (modulo-2) cho số dư.

Kết quả sẽ là xâu bit được truyền đi (xâu gốc ghép với checksum).

Chú ý: Hiện nay có 3 đa thức sinh được xem là chuẩn quốc tế:

$$\text{CRC-12} = x^{12} + x^{11} + x^3 + x^2 + x + 1$$

$$\text{CRC-16} = x^{16} + x^{15} + x^2 + 1$$

$$\text{CRC-CCITT} = x^{16} + x^{12} + x^5 + 1$$

3.3. Đa liên kết truy cập và Các giao thức

Mạng LAN là mạng sử dụng truyền quảng bá và có nhiều giao thức truyền quảng bá của nó. Trong bất kỳ mạng dạng quảng bá nào, vấn đề then chốt luôn là cách thức quyết định ai có quyền truy cập kênh truyền tại một thời điểm.

Để làm rõ vấn đề hơn, hãy xem xét ví dụ sau: Có sáu người đang họp thông qua hệ thống điện thoại, mọi người đều được nối kết để có thể nghe và nói với những người khác. Khi một người ngừng nói mà có hai người hoặc nhiều hơn cùng phát biểu tiếp sẽ tạo ra tình trạng lộn xộn. Trong các cuộc họp dạng gặp mặt trực tiếp, tình trạng lộn xộn này có thể được giải quyết bằng cách đưa tay xin phát biểu. Nhưng trong hệ thống hội thảo thông qua điện thoại này, khi mà đường truyền rãnh, việc quyết định ai sẽ nói tiếp có vẻ khó làm hơn. Đã có nhiều giao thức dùng giải quyết vấn đề trên. Và chúng chính là nội dung trình bày của phần này. Nói một cách khác, các kênh truyền dạng quảng bá thỉnh thoảng còn được gọi là các kênh đa truy cập (multiaccess channels) hay là các kênh truy cập ngẫu nhiên (random access channels).

Các giao thức được sử dụng để quyết định ai có quyền truy cập đường truyền quảng bá trước được gom vào trong một lớp con của lớp liên kết dữ liệu gọi là lớp con MAC. Lớp con MAC là đặc biệt quan trọng trong mạng LAN, do nhiều mạng LAN sử dụng đường truyền dạng quảng bá như là phương tiện truyền thông nền tảng. Các mạng WAN, theo xu hướng ngược lại, lại dùng các nối kết dạng điểm-điểm (ngoại trừ các mạng dùng vệ tinh). Về cơ bản, có ba phương pháp điều khiển truy cập đường truyền: Chia kênh, truy cập ngẫu nhiên (Random Access) và phân lượt (“Taking-turns”).

3.3.1. Phương pháp chia kênh

Ý tưởng chung của phương pháp này là: đường truyền sẽ được chia thành nhiều kênh truyền, mỗi kênh truyền sẽ được cấp phát riêng cho một trạm. Có ba phương pháp chia kênh chính: FDMA, TDMA, CDMA.

3.3.1.1. Chia tần số (FDMA – Frequency Division Multiple Access).

Một phương thức truyền thống để chia sẻ một kênh truyền đơn cho nhiều người dùng cạnh tranh là Chia tần số (FDMA). Phổ của kênh truyền được chia thành nhiều băng tần (frequency bands) khác nhau. Mỗi trạm được gán cho một băng tần cố định. Những trạm nào được cấp băng tần mà không có dữ liệu để truyền thì ở trong trạng thái nhàn rỗi (idle).

Ví dụ: Một mạng LAN có sáu trạm, các trạm 1, 3, 4 có dữ liệu cần truyền, các trạm 2, 5, 6 nhàn rỗi.



Hình 3.5 Ví dụ về FDMA

Nhận xét:

Do mỗi người dùng được cấp một băng tần riêng, nên không có sự đụng độ xảy ra. Khi chỉ có số lượng người dùng nhỏ và ổn định, mỗi người dùng cần giao tiếp nhiều thì FDMA chính là cơ chế điều khiển truy cập đường truyền hiệu quả.

Tuy nhiên, khi mà lượng người gửi dữ liệu là lớn và liên tục thay đổi hoặc đường truyền vượt quá khả năng phục vụ thì FDMA bộc lộ một số vấn đề. Nếu phổ đường truyền được chia làm N vùng và có ít hơn N người dùng cần truy cập đường truyền, thì một phần lớn phổ đường truyền bị lãng phí. Ngược lại, có nhiều hơn N người dùng có nhu cầu truyền dữ liệu thì một số người dùng sẽ phải bị từ chối không có truy cập đường truyền vì thiếu băng thông. Tuy nhiên, nếu lại giả sử rằng số lượng người dùng bằng cách nào đó luôn được giữ ổn định ở con số N, thì việc chia kênh truyền thành những kênh truyền con như thế tự thân là không hiệu quả. Lý do cơ bản ở đây là: nếu có vài người dùng rỗi, không truyền dữ liệu thì những kênh truyền con cấp cho những người dùng này bị lãng phí.

f) Có thể dễ dàng thấy được hiệu năng nghèo nàn của FDMA từ một phép tính theo lý thuyết xếp hàng đơn giản. Đầu tiên là thời gian trì hoãn trung bình T trong một

kênh truyền có dung lượng C bps, với tỉ lệ đến trung bình là λ khung/giây, mỗi khung có chiều dài được chỉ ra từ hàm phân phối mũ với giá trị trung bình là $1/\mu$ bit/khung. Với các tham số trên sẽ có được tỉ lệ phục vụ là μC khung/giây.

$$\text{Tù lý thuyết xếp hàng ta có: } T = \frac{1}{\mu C - \lambda}$$

Ví dụ: nếu $C = 100$ Mbps, $1/\mu = 10000$ bits và $\lambda = 5000$ khung/giây thì $T = 200$ μ s. Bây giờ nếu chia kênh lớn này thành N kênh truyền nhỏ độc lập, mỗi kênh truyền nhỏ có dung lượng C/N bps. Tỉ lệ trung bình các khung đến các kênh truyền nhỏ bây giờ là λ/N . Tính toán lại T sẽ có:

$$T_{FDMA} = \frac{1}{\mu(C/N) - (\lambda/N)} = \frac{N}{\mu C - \lambda} = NT$$

Thời gian chờ đợi trung bình trong các kênh truyền con sử dụng FDMA là xấp xỉ hơn gấp N lần so với trường hợp ta sắp xếp cho các khung được truyền tuần tự trong một kênh lớn.

3.3.1.2. Chia thời gian (TDMA – Time Division Multiple Access)

Trong phương pháp này, các trạm sẽ xoay vòng (round) để truy cập đường truyền. Vòng ở đây có thể hiểu là vòng thời gian. Một vòng thời gian là khoảng thời gian đủ để cho tất cả các trạm trong LAN đều được quyền truyền dữ liệu. Qui tắc xoay vòng như sau: một vòng thời gian sẽ được chia đều thành các khe (slot) thời gian bằng nhau, mỗi trạm sẽ được cấp một khe thời gian – đủ để nó có thể truyền hết một gói tin. Những trạm nào tới lượt được cấp cho khe thời gian của mình mà không có dữ liệu để truyền thì vẫn chiếm lấy khe thời gian đó, và khoảng thời gian bị chiếm này được gọi là thời gian nhàn rỗi (idle time). Tập hợp tất cả các khe thời gian trong một vòng được gọi lại là khung (frame).

Như vậy với phương pháp này, nếu người dùng không sử dụng khe thời gian này để truyền dữ liệu thì thời gian sẽ bị lãng phí.

3.3.1.3. Kết hợp giữa FDMA và TDMA

Trong thực tế, hai kỹ thuật TDMA và FDMA thường được kết hợp sử dụng với nhau, ví dụ như trong các mạng điện thoại di động.

f Các điện thoại di động TDMA sử dụng các kênh 30 KHz, mỗi kênh lại được chia thành ba khe thời gian. Một thiết bị cầm tay sử dụng một khe thời gian cho việc gửi và một khe khác cho việc nhận dữ liệu. Chẳng hạn như các hệ thống: Cingular (Nokia 8265, TDMA 800/ 1900 MHz, AMPS 800 mHz), AT&T Wireless.

f Hệ thống GSM sử dụng các kênh 200 KHz được chia thành 8 khe thời gian. Một thiết bị cầm tay sẽ sử dụng một khe thời gian trong hai kênh khác nhau để gửi và nhận thông tin. Các hệ thống Cingular, T-Mobile, AT&T đang chuyển sang dùng kỹ thuật này.

3.3.1.4. Phân chia mã (CDMA – Code Division Multiple Access)

CDMA hoàn toàn khác với FDMA và TDMA. Thay vì chia một dãy tần số thành nhiều kênh truyền bằng thông hẹp, CDMA cho phép mỗi trạm có quyền phát dữ liệu lên toàn bộ phổ tần của đường truyền lớn tại mọi thời điểm. Các cuộc truy cập đường truyền xảy ra đồng thời sẽ được tách biệt với nhau bởi kỹ thuật mã hóa. CDMA cũng xóa tan lo lắng cho rằng những khung dữ liệu bị đụng độ trên đường truyền sẽ bị biến dạng. Thay vào đó CDMA chỉ ra rằng nhiều tín hiệu đồng thời sẽ được cộng lại một cách tuyến tính. Kỹ thuật CDMA thường được sử dụng trong các kênh truyền quảng bá không dây (mạng điện thoại di động, vệ tinh ...).

Trước khi đi vào mô tả giải thuật CDMA, hãy xem xét một ví dụ gần giống như sau: tại một phòng đợi trong sân bay có nhiều cặp hành khách đang chuyện trò. TDM có thể được so sánh với cảnh tượng: tất cả mọi người đều đứng giữa phòng, chờ đến lượt mình được phát biểu. FDM thì giống như cảnh tượng: mỗi một cặp được sắp vào một ô nói chuyện riêng. Còn CDMA lại giống như cảnh: mọi người đều đứng ngay trong phòng đợi, nói chuyện đồng thời, nhưng mỗi cặp chuyện trò sẽ sử dụng một ngôn ngữ riêng. Cặp nói tiếng Pháp chỉ nói với nhau bằng tiếng Pháp, bỏ qua mọi tiếng động không phải là tiếng Pháp và coi đó như là tiếng ồn. Vì thế, vấn đề then chốt trong CDMA là khả năng rút trích ra được tín hiệu mong muốn trong khi từ chối mọi thứ khác và coi đó là tiếng ồn ngẫu nhiên.

Trong CDMA, thời gian gửi một bit (bit time) lại được chia thành m khoảng nhỏ hơn, gọi là chip. Thông thường, có 64 hay 128 chip trên một bit, nhưng trong ví dụ phía dưới, chúng ta dùng 8 chip cho đơn giản.

Nhiều người dùng đều chia sẻ chung một băng tần, nhưng mỗi người dùng được cấp cho một mã duy nhất dài m bit gọi là chuỗi bit (chip sequence). Chuỗi bit này sẽ được dùng để mã hóa và giải mã dữ liệu của riêng người dùng này trong một kênh truyền chung đa người dùng. Ví dụ, sau đây là một chuỗi bit: (11110011). Để gửi bit 1, người dùng sẽ gửi đi chuỗi bit của mình. Còn để gửi đi bit 0, người dùng sẽ gửi đi phần bù của chuỗi bit của mình. Ví dụ với chuỗi bit trên, khi gửi bit 1, người dùng sẽ gửi 11110011; khi gửi bit 0 thì người dùng sẽ gửi 00001100.

Để tiện cho việc minh họa, chúng ta sẽ sử dụng các ký hiệu lưỡng cực sau: bit 0 được ký hiệu là -1, bit 1 được ký hiệu là +1.

Cũng cần phải đưa ra một định nghĩa mới: tích trong (inner product): Tích trong của hai mã S và T , ký hiệu là $S \cdot T$, được tính bằng trung bình tổng của tích các bit nội tại tương ứng của hai mã này.

$$S \cdot T = \frac{1}{m} \sum_{i=1}^m S_i T_i$$

Ví dụ: $S = +1+1+1-1-1+1+1-1$

$T = +1+1+1+1-1-1+1-1$

$$S \cdot T = \frac{+1+1+1+(-1)+1+(-1)+1+1}{8} = \frac{1}{2}$$

Bây giờ xem xét cách thức cấp phát chuỗi chip cho các trạm, sao cho không gây ra lẫn lộn thông tin giữa các trạm với nhau.

Định nghĩa:

Hai mã S và T có cùng chiều dài m bits được gọi là trực giao khi: $S \cdot T = 0$.

Ví dụ:

$$S = +1+1-1-1-1-1+1$$

$$T = -1-1+1-1-1+1+1$$

$$S \cdot T = \frac{(-1) + (-1) + (-1) + 1 + 1 + 1 + (-1) + 1}{8} = 0$$

Nếu người dùng trong hệ thống có các mã trực giao với nhau thì họ có thể cùng tồn tại và truyền dữ liệu một cách đồng thời với khả năng bị giao thoa dữ liệu là ít nhất.

Qui ước:

- f Gọi D_i là bit dữ liệu mà người dùng i muốn mã hóa để truyền trên mạng.
- f C_i là chuỗi chip (mã số) của người dùng i.

Sau đây là cách thức mã hóa tín hiệu để gửi lên đường truyền và giải mã để lấy dữ liệu đó ra:

Tín hiệu được mã của người dùng i: $Z_i = D_i \times C_i$

Tín hiệu tổng hợp được gửi trên đường truyền: $Z = \sum_{i=1}^n Z_i$ với n là tổng số người dùng gửi

tín hiệu lên đường truyền tại cùng thời điểm.

Giải mã:

Dữ liệu mà người dùng i lấy về từ tín hiệu tổng hợp chung: $D_i = Z \cdot C_i$. Nếu $D_i >$ “ngưỡng”, coi nó là 1, ngược lại coi nó là -1

3.3.2. Giao thức truy cập ngẫu nhiên

Trong phương pháp truy cập đường truyền ngẫu nhiên (Random Access), người ta để cho các trạm tự do tranh chấp đường truyền chung để truyền từng khung dữ liệu một. Nếu một trạm cần gửi một khung, nó sẽ gửi khung đó trên toàn bộ dải thông của kênh truyền. Sẽ không có sự phối hợp trình tự giữa các trạm. Nếu có hơn hai trạm phá cùng một lúc, “đụng độ” (collision) sẽ xảy ra, các khung bị đụng độ sẽ bị hư hại. Giao thức truy cập đường truyền ngẫu nhiên được dùng để xác định:

- f Làm thế nào để phát hiện đụng độ.
- f Làm thế nào để phục hồi sau đụng độ.

Ví dụ về các giao thức truy cập ngẫu nhiên: slotted ALOHA và pure ALOHA, CSMA, CSMA/CD và CSMA/CA.

3.3.2.1. ALOHA.

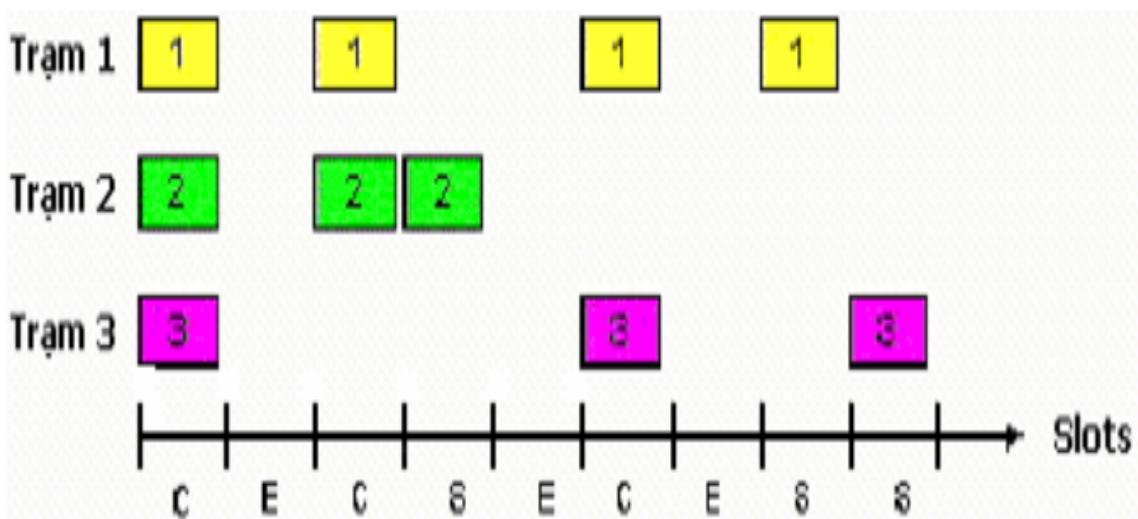
Vào những năm 1970, Norman Abramson cùng các đồng sự tại Đại học Hawaii đã phát minh ra một phương pháp mới ưu hạng dùng để giải quyết bài toán về cấp phát kênh truyền. Sau đó công việc của họ tiếp tục được mở rộng bởi nhiều nhà nghiên cứu khác. Mặc dù công trình của Abramson, được gọi là hệ thống ALOHA, sử dụng hệ thống truyền quảng bá trên sóng radio mặt đất, nhưng ý tưởng cơ sở của nó có thể áp dụng cho bất kỳ hệ thống nào trong đó những người dùng không có phôi hợp với nhau sẽ tranh chấp sử dụng đường truyền chung duy nhất.

Ở đây, chúng ta sẽ thảo luận về hai phiên bản của ALOHA: pure (thuần túy) và slotted (được chia khe).

a. Slotted ALOHA.

Thời gian được chia thành nhiều slot có kích cỡ bằng nhau (bằng thời gian truyền một khung). Một trạm muốn truyền một khung thì phải đợi đến đầu slot thời gian kế tiếp mới được truyền. Dĩ nhiên là sẽ xảy ra đụng độ và khung bị đụng độ sẽ bị hư. Tuy nhiên, dựa trên tính phản hồi của việc truyền quảng bá, trạm phát luôn có thể theo dõi xem khung của nó phát đi có bị hủy hoại hay không bằng cách lắng nghe kênh truyền. Những trạm khác cũng làm theo cách tương tự. Trong trường hợp vì lý do nào đó mà trạm không thể dùng cơ chế lắng nghe đường truyền, hệ thống cần yêu cầu bên nhận trả lời một khung báo nhận (acknowledgement) cho bên phát. Nếu phát sinh đụng độ, trạm phát sẽ gửi lại khung tại đầu slot kế tiếp với xác suất p cho đến khi thành công.

Ví dụ minh họa: Có 3 trạm đều muốn truyền một khung thông tin.



Hình 3. 6 Ví dụ về Slotted ALOHA

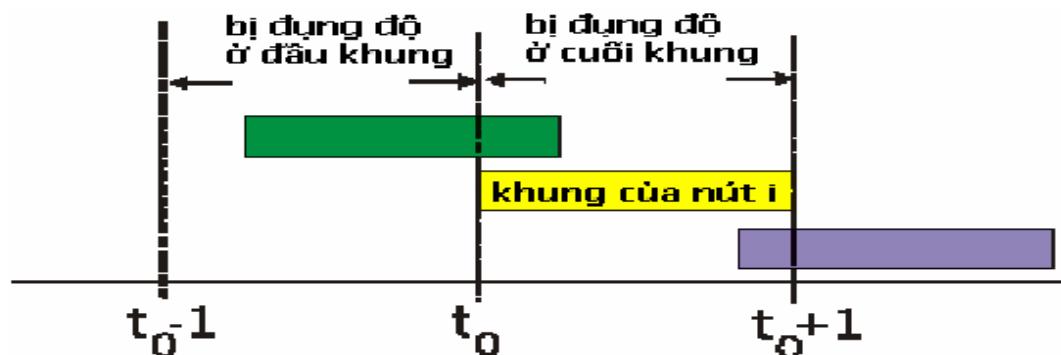
Do sẽ có đụng độ mà mất khung thông tin, một câu hỏi đặt ra là: đâu là tỉ suất truyền khung thành công của các trạm trong mạng?

Giả sử có N trạm muốn truyền dữ liệu, mỗi trạm truyền khung thông tin của mình trong một slot với xác suất p . Xác suất để một trạm trong N trạm truyền thành công $S(p)$ được tính như sau: $S(p) = Np(1-p)^{N-1}$

Khi $p = 1/N$ thì $S(p)$ sẽ đạt giá trị cực đại $(1-1/N)^{N-1}$

b. Pure ALOHA.

Kỹ thuật Pure ALOHA đơn giản hơn Slotted ALOHA do không có sự đồng bộ hóa giữa các trạm. Mỗi khi muốn truyền một khung thông tin, trạm sẽ truyền nó ngay mà không cần đợi đến đầu của slot thời gian kế tiếp. Vì thế xác xuất bị dụng độ tăng thêm. Nghĩa là khung thông tin được gửi tại thời điểm t sẽ đụng độ với những khung được gửi trong khoảng thời gian $[t_0 - 1, t_0 + 1]$.



Hình 3. 7 Ví dụ về Pure ALOHA

Gọi P là xác xuất của một sự kiện nào đó, ta có những phân tích sau:

$$P(\text{nút } i \text{ truyền thành công}) = P(\text{để nút } i \text{ truyền})$$

$$P(\text{không có nút nào khác truyền trong khoảng } [t_0 - 1, t_0])$$

$$P(\text{không có nút nào khác truyền trong khoảng } [t_0, t_0 + 1]) = p(1-p)^{N-1}(1-p)^{N-1}$$

$$S(p) = P(\text{một nút bất kỳ trong } N \text{ nút truyền thành công}) = Np(1-p)^{N-1}(1-p)^{N-1}$$

Những phân tích vừa nêu giả sử rằng luôn có thường trực N trạm trong mạng. Và trong trường hợp tối ưu, mỗi trạm thử truyền với xác suất $1/N$.

Trong thực tế, số lượng các trạm thường trực trong mạng luôn thay đổi. Giả sử chúng ta có tổng cộng m trạm làm việc. n trạm là thường trực trên mạng, mỗi trạm thường trực trên mạng sẽ cố gửi khung thông tin với xác suất cố định p . $m-n$ trạm còn lại là không thường trực, và chúng có thể gửi khung thông tin với xác suất p_a , với p_a có thể nhỏ hơn p .

3.3.2.2. CSMA – Carrier Sense Multiple Access.

a. Giao thức CSMA

Giao thức ALOHA mặc dù đã chạy được, nhưng một điều đáng ngạc nhiên là lại để cho các trạm làm việc tự do gửi thông tin lên đường truyền mà chẳng cần quan tâm đến việc tìm hiểu xem những trạm khác đang làm gì. Và điều đó dẫn đến rất nhiều vụ đụng độ tín hiệu. Tuy nhiên, trong mạng LAN, có thể thiết kế các trạm làm việc sao cho

chúng có thể điều tra xem các trạm khác đang làm gì và tự điều chỉnh hành vi của mình một cách tương ứng. Làm như vậy sẽ giúp cho hiệu năng mạng đạt được cao hơn. CSMA là một giao thức như vậy. Các giao thức mà trong đó các trạm làm việc lắng nghe đường truyền trước khi đưa ra quyết định mình phải làm gì tương ứng với trạng thái đường truyền đó được gọi là các giao thức có “cảm nhận” đường truyền (carrier sense protocol). Cách thức hoạt động của CSMA như sau: lắng nghe kênh truyền, nếu thấy kênh truyền rồi thì bắt đầu truyền khung, nếu thấy đường truyền bận thì trì hoãn lại việc gửi khung. Thế nhưng trì hoãn việc gửi khung cho đến khi nào?

Có ba giải pháp:

Theo dõi không kiên trì (Non-persistent CSMA): Nếu đường truyền bận, đợi trong một khoảng thời gian ngẫu nhiên rồi tiếp tục nghe lại đường truyền.

Theo dõi kiên trì (persistent CSMA): Nếu đường truyền bận, tiếp tục nghe đến khi đường truyền rồi rồi thì truyền gói tin với xác suất bằng 1.

Theo dõi kiên trì với xác suất p (P-persistent CSMA): Nếu đường truyền bận, tiếp tục nghe đến khi đường truyền rồi rồi thì truyền gói tin với xác suất bằng p.

Dễ thấy rằng giao thức CSMA cho dù là theo dõi đường truyền kiên trì hay không kiên trì thì khả năng tránh đụng độ vẫn tốt hơn là ALOHA. Tuy thế, đụng độ vẫn có thể xảy ra trong CSMA.

Tình huống phát sinh như sau: khi một trạm vừa phát xong thì một trạm khác cũng phát sinh yêu cầu phát khung và bắt đầu nghe đường truyền. Nếu tín hiệu của trạm thứ nhất chưa đến trạm thứ hai, trạm thứ hai sẽ cho rằng đường truyền đang rảnh và bắt đầu phát khung. Như vậy đụng độ sẽ xảy ra.

Hậu quả của đụng độ là: khung bị mất và toàn bộ thời gian từ lúc đụng độ xảy ra cho đến khi phát xong khung là lãng phí.

b. CSMA với cơ chế theo dõi đụng độ (CSMA/CD–CSMA with Collision Detection)

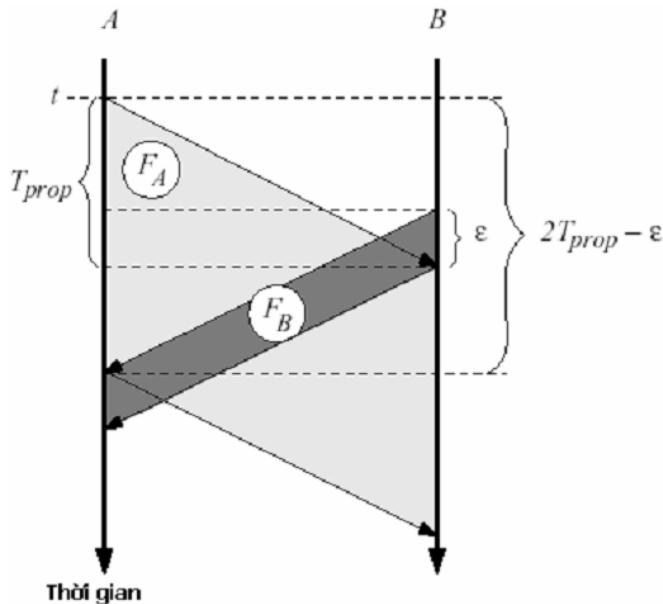
CSMA/CD về cơ bản là giống như CSMA: lắng nghe trước khi truyền. Tuy nhiên CSMA/CD có hai cải tiến quan trọng là: phát hiện đụng độ và làm lại sau đụng độ.

Phát hiện đụng độ: Trạm vừa truyền vừa tiếp tục dò xét đường truyền. Ngay sau khi đụng độ được phát hiện thì trạm ngưng truyền, phát thêm một dãy nhồi (dãy nhồi này có tác dụng làm tăng cường thêm sự va chạm tín hiệu, giúp cho tất cả các trạm khác trong mạng thấy được sự đụng độ), và bắt đầu làm lại sau đụng độ.

Tại thời điểm t_0 , một trạm đã phát xong khung của nó. Bất kỳ trạm nào khác có khung cần truyền bây giờ có thể có truyền thử. Nếu hai hoặc nhiều hơn các trạm làm như vậy cùng một lúc thì sẽ xảy ra đụng độ. Đụng độ có thể được phát hiện bằng cách theo dõi năng lượng hay độ rộng của xung của tín hiệu nhận được và đem so sánh với độ rộng của xung vừa truyền đi. Bây giờ ta đặt ra câu hỏi: Sau khi truyền xong khung (hết giai

đoạn truyền), trạm sẽ bỏ ra thời gian tối đa là bao lâu để biết được là khung của nó đã bị đụng độ hoặc nó đã truyền thành công? Gọi thời gian này là “cửa sổ va chạm” và ký hiệu nó là T_w . Phân tích sau đây sẽ cho ra câu trả lời.

Hình sau sẽ mô phỏng chi tiết về thời gian phát khung giữa hai trạm A và B ở hai đầu mút xa nhau nhất trên đường truyền tải.



Hình 3. 8 Thời gian cần thiết để truyền một khung

Đặt T_{prop} là thời gian lan truyền tín hiệu giữa hai đầu mút xa nhau nhất trên đường truyền tải.

Tại thời điểm t , A bắt đầu phát đi khung dữ liệu của nó.

Tại $t+T_{prop}-\varepsilon$, B phát hiện kênh truyền rảnh và phát đi khung dữ liệu của nó.

Tại $t+T_{prop}$, B phát hiện sự đụng độ.

Tại $t+2T_{prop}-\varepsilon$, A phát hiện sự đụng độ.

Theo phân tích trên, thì $T_w = 2T_{prop}$

Việc hủy bỏ truyền khung ngay khi phát hiện có đụng độ giúp tiết kiệm thời gian và băng thông, vì nếu cứ tiếp tục truyền khung đi nữa, khung đó vẫn hư và vẫn phải bị hủy bỏ.

Làm lại sau khi đụng độ: Sau khi bị đụng độ, trạm sẽ chạy một thuật toán gọi là back-off dùng để tính toán lại lượng thời gian nó phải chờ trước khi gửi lại khung. Lượng thời gian này phải là ngẫu nhiên để các trạm sau khi quay lại không bị đụng độ với nhau nữa.

Thuật toán back-off hoạt động như sau:

Rút ngẫu nhiên ra một con số nguyên M thỏa: $0 \leq M \leq 2^k$. Trong đó $k = \min(n, 10)$, với n là tổng số lần đụng độ mà trạm đã gánh chịu.

Kỳ hạn mà trạm phải chờ trước khi thử lại một lần truyền mới là M^*Tw .

Khi mà n đạt đến giá trị 16 thì hủy bỏ việc truyền khung. (Trạm đã chịu đựng quá nhiều vụ đụng độ rồi, và không thể chịu đựng hơn được nữa!)

Đánh giá hiệu suất của giao thức CSMA/CD:

Gọi:

- P là kích thước của khung, ví dụ như 1000 bits.
- C là dung lượng của đường truyền, ví dụ như 10 Mbps.

Ta có thời gian phát hết một khung thông tin là P/C giây.

Trung bình, chúng ta sẽ thử e lần trước khi truyền thành công một khung.

Vì vậy, với mỗi lần phát thành công một khung (tốn P/C giây), ta đã mất tổng cộng $2eT_{prop}$ ($\approx 5T_{prop}$) vì đụng độ. Thành thử hiệu năng của giao thức (tỉ lệ giữa thời gian hoạt động hữu ích trên tổng thời gian hoạt động) là:

$$\frac{\frac{P}{C}}{\frac{P}{C} + 5T_{prop}} = \frac{1}{1 + \frac{5T_{prop}}{\frac{P}{C}}} = \frac{1}{1 + 5a}$$

$$\text{với } a = \frac{T_{prop}C}{P}$$

Ta có thể thấy giá trị của a đóng vai trò rất quan trọng đến hiệu suất hoạt động của mạng kiểu CSMA/CD.

3.3.3. Phương pháp phân lượt truy cập đường truyền

Bây giờ thử nhìn lại hai phương pháp điều khiển truy cập đường truyền “chia kênh” và “truy cập ngẫu nhiên”, ta sẽ thấy chúng đều có những điểm hay và hạn chế:

f Trong các giao thức dạng chia kênh, kênh truyền được phân chia một cách hiệu quả và công bằng khi tải trọng đường truyền là lớn. Tuy nhiên chúng không hiệu quả khi tải trọng của đường truyền là nhỏ: có độ trì hoãn khi truy cập kênh truyền, chỉ $1/N$ băng thông được cấp cho người dùng ngay cả khi chỉ có duy nhất người dùng đó hiện diện trong hệ thống.

f Các giao thức dạng truy cập ngẫu nhiên thì lại hoạt động hiệu quả khi tải trọng của đường truyền thấp. Nhưng khi tải trọng đường truyền cao thì phải tốn nhiều chi phí cho việc xử lý đụng độ. Các giao thức dạng “phân lượt” sẽ để ý đến việc tận dụng những mặt mạnh của hai dạng nói trên.

Ý tưởng chính của các giao thức dạng “phân lượt” là không để cho đụng độ xảy ra bằng cách cho các trạm truy cập đường truyền một cách tuần tự.

Về cơ bản, có hai cách thức để “phân lượt” sử dụng đường truyền:

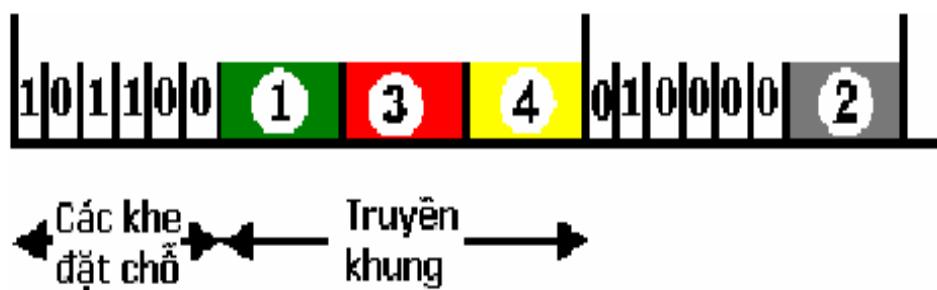
f *Thăm dò (polling)*: Trạm chủ (master) sẽ mời các trạm tớ (slave) truyền khi đến lượt. Lượt truyền được cấp phát cho trạm tớ có thể bằng cách: trạm chủ dành phần cho

trạm tớ hoặc trạm tớ yêu cầu và được trạm chủ đáp ứng. Tuy nhiên có thể thấy những vấn đề sẽ gặp phải của giải pháp này là: chi phí cho việc thăm dò, độ trễ do phải chờ được phân luợt truyền, hệ thống rối loạn khi trạm chủ gặp sự cố.

f) *Chuyển thẻ bài (token passing):* Thẻ bài điều khiển sẽ được chuyển lần lượt từ trạm này qua trạm kia. Trạm nào có trong tay thẻ bài sẽ được quyền truyền, truyền xong phải chuyển thẻ bài qua trạm kế tiếp. Những vấn đề cần phải quan tâm: chi phí quản lý thẻ bài, độ trễ khi phải chờ thẻ bài, khó khăn khi thẻ bài bị mất.

3.3.3.1. Ví dụ về phương pháp thăm dò phân tán

Trong phương pháp thăm dò phân tán (Distributed Polling), thời gian được chia thành những “khe” (slot). Giả sử hệ thống hiện có N trạm làm việc. Một chu kỳ hoạt động của hệ thống bắt đầu bằng N khe thời gian ngắn dùng để đặt chỗ (reservation slot).



Hình 3.9 Mô tả các chu kỳ hoạt động của hệ thống thăm dò phân tán

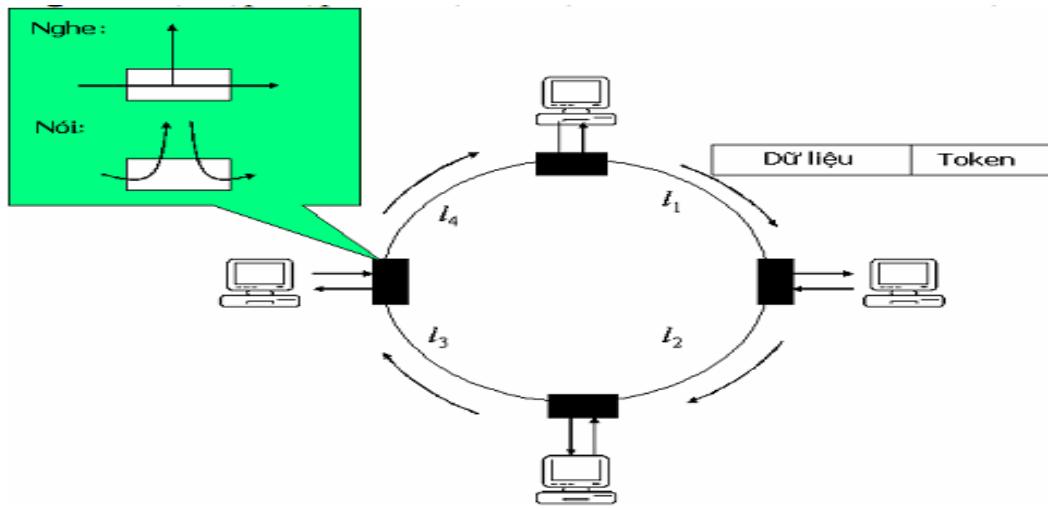
Khe thời gian dùng để đặt chỗ bằng với thời gian lan truyền tín hiệu giữa hai đầu mút xa nhất trên đường truyền. Tới khe đặt chỗ thứ i, trạm thứ i nếu muốn truyền dữ liệu sẽ phát tín hiệu đặt chỗ của mình lên kênh truyền, và tín hiệu này sẽ được nhìn thấy bởi tất cả các trạm khác trong mạng.

Sau thời gian đặt chỗ, các trạm bắt đầu việc truyền dữ liệu của mình theo đúng trình tự đã đăng ký.

3.3.3.2. Ví dụ về phương pháp chuyển thẻ bài: Token Ring

Giao thức này sử dụng mạng kiểu hình vòng, dùng thẻ bài để cấp quyền sử dụng đường truyền. Mạng token ring bao gồm một tập hợp các trạm được nối với nhau thành một vòng.

Dữ liệu luôn chạy theo một hướng vòng quanh vòng. Mỗi trạm nhận khung từ trạm phía trên của nó và rồi chuyển khung đến trạm phía dưới. Thẻ bài là công cụ để quyết định ai có quyền truyền tại một thời điểm.



Hình 3. 10 Mô hình hoạt động của mạng Token Ring

Cách thức hoạt động của mạng token ring như sau: một thẻ bài, thực chất chỉ là một dãy bit, sẽ chạy vòng quanh vòng; mỗi nút sẽ nhận thẻ bài rồi lại chuyển tiếp thẻ bài này đi. Khi một trạm có khung cần truyền và đúng lúc nó thấy có thẻ bài tới, nó liền lấy thẻ bài này ra khỏi vòng (nghĩa là không có chuyển tiếp chuỗi bit đặc biệt này lên vòng nữa), và thay vào đó, nó sẽ truyền khung dữ liệu của mình đi. Khi khung dữ liệu đi một vòng và quay lại, trạm phát sẽ rút khung của mình ra và chèn lại thẻ bài vào vòng. Hoạt động cứ xoay vòng như thế.

Card mạng dùng cho token ring sẽ có trên đó một bộ nhận, một bộ phát và một bộ đệm dùng chứa dữ liệu. Khi không có trạm nào trong vòng có dữ liệu để truyền, thẻ bài sẽ lưu chuyển vòng quanh. Nếu một trạm có dữ liệu cần truyền và có thẻ bài, nó có quyền truyền một hoặc nhiều khung dữ liệu tùy theo qui định của hệ thống.

Mỗi khung dữ liệu được phát đi sẽ có một phần thông tin chứa địa chỉ đích của trạm bên nhận; ngoài ra nó còn có thể chứa địa chỉ multicast hoặc broadcast tùy theo việc bên gửi muốn gửi khung cho một nhóm người nhận hay tất cả mọi người trong vòng. Khi khung thông tin chạy qua mỗi trạm trong vòng, trạm này sẽ nhìn vào địa chỉ đích trong khung đó để biết xem có phải nó là đích đến của khung không. Nếu phải, trạm sẽ chép nội dung của khung vào trong bộ đệm của nó, chỉ chép thôi chứ không được xóa khung ra khỏi vòng.

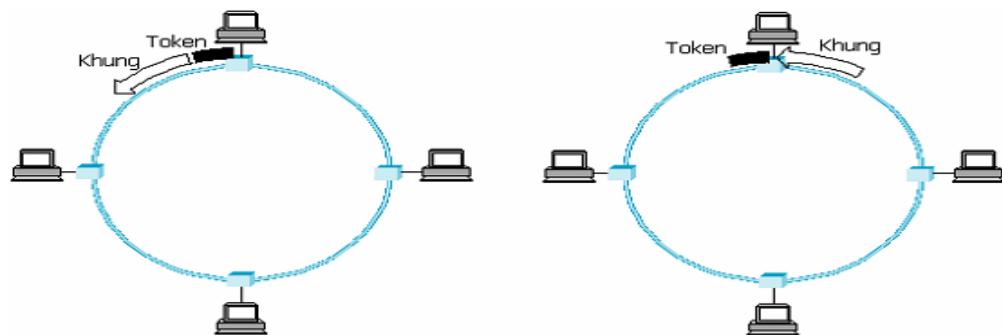
Một vấn đề cần phải quan tâm đến là một trạm đang giữ thẻ bài thì nó có quyền truyền bao nhiêu dữ liệu, hay nói cách khác là trạm được cho bao nhiêu thời gian để truyền dữ liệu? Chúng ta gọi thời gian này là thời gian giữ thẻ bài – THT (Token Holding Time). Trong trường hợp trong vòng chỉ có một trạm cần truyền dữ liệu và các trạm khác không có nhu cầu truyền, thì ta có thể cấp THT cho trạm có nhu cầu càng lâu càng tốt. Điều này sẽ làm tăng hiệu suất sử dụng hệ thống một cách đáng kể. Bởi vì sẽ thật là ngớ

ngắn nếu bắt trạm ngừng, chờ thẻ bài chạy hết một vòng, rồi lại truyền tiếp. Tuy nhiên, giải pháp trên sẽ không hoạt động tốt nếu có nhiều trạm trong vòng cần gửi dữ liệu. THT dài chỉ thích hợp cho những trạm cần truyền nhiều dữ liệu, nhưng lại không phù hợp với những trạm chỉ có ít thông điệp cần gửi đi ngay cả khi thông điệp này là tối quan trọng. Điều này cũng giống như tình huống mà bạn xếp hàng để sử dụng máy ATM ngay sau một anh chàng định rút ra 10 triệu đồng, trong khi bạn chỉ cần vào đây để kiểm tra tài khoản của mình còn bao nhiêu tiền. Trong các mạng 802.5, THT mặc định là 10 ms.

Từ thời gian giữ thẻ bài, chúng ta lại nghĩ ra một số đo quan trọng khác: Thời gian xoay vòng của thẻ bài – TRT (Token rotation time), nghĩa là lượng thời gian bỏ ra để thẻ bài đi hết đúng một vòng.

Dễ nhận thấy rằng: $TRT \leq Sô nút hoạt động \times THT + Độ trễ của vòng$

Với “Độ trễ của vòng” là tổng thời gian để thẻ bài đi hết một vòng khi trong vòng không có trạm nào cần truyền dữ liệu, “Số nút hoạt động” ám chỉ số trạm có dữ liệu cần truyền. Giao thức 802.5 cung cấp một phương thức truyền dữ liệu tin cậy bằng cách sử dụng hai bit A và C ở đuôi của khung dữ liệu. Hai bit này ban đầu nhận giá trị 0. Khi một trạm nhận ra nó là đích đến của một khung dữ liệu, nó sẽ đặt bit A trong khung này lên. Khi trạm chép khung vào trong bộ nhớ đệm của nó, nó sẽ đặt bit C lên. Khi trạm gửi thấy khung của nó quay lại với bit A vẫn là 0, nó biết là trạm đích bị hư hỏng hoặc không có mặt. Nếu bit A là 1, nhưng bit C là 0, điều này ám chỉ trạm đích có mặt nhưng vì lý do nào đó trạm đích không thể nhận khung (ví dụ như thiếu bộ đệm chẳng hạn). Vì thế khung này có thể sẽ được truyền lại sau đó với hy vọng là trạm đích có thể tiếp nhận nó. Chi tiết cuối cùng cần phải xem xét là: chính xác khi nào thì trạm sẽ nhả thẻ bài ra? Có hai đề nghị: a) nhả thẻ bài ra ngay sau khi trạm vừa truyền khung xong (RAT); b) nhả thẻ bài ra ngay sau khi trạm nhận lại khung vừa phát ra (RAR)



a. RAT b. RAR

Hình 3. 11 Nhả Token Ring

Quản lý hoạt động của mạng Token Ring:

Cần thiết phải đề cử ra một trạm làm nhiệm vụ quản lý mạng token ring gọi là monitor. Công việc của monitor là đảm bảo sức khỏe cho toàn bộ vòng. Bất kỳ trạm nào cũng có thể trở thành monitor. Thủ tục bầu chọn monitor diễn ra khi vòng vừa được tạo ra hoặc khi monitor của vòng bị sự cố. Một monitor mạnh khỏe sẽ định kỳ thông báo sự hiện diện của nó cho toàn vòng bằng một thông điệp đặc biệt. Nếu một trạm không nhận được thông báo hiện diện của monitor trong một khoảng thời gian nào đó, nó sẽ coi như monitor bị hỏng và sẽ cố trở thành monitor mới.

Khi một trạm quyết định rằng cần phải có một monitor mới, nó sẽ gửi một thông điệp thỉnh cầu, thông báo ý định trở thành monitor của mình. Nếu thông điệp này chạy một vòng và về lại được trạm, trạm sẽ cho rằng mọi người đồng ý vị trí monitor của nó. Còn nếu đồng thời có nhiều trạm cùng gửi thông điệp thỉnh cầu, chúng sẽ áp dụng một luật lựa chọn nào đó, chẳng hạn như “ai có địa chỉ cao nhất sẽ thắng cử”.

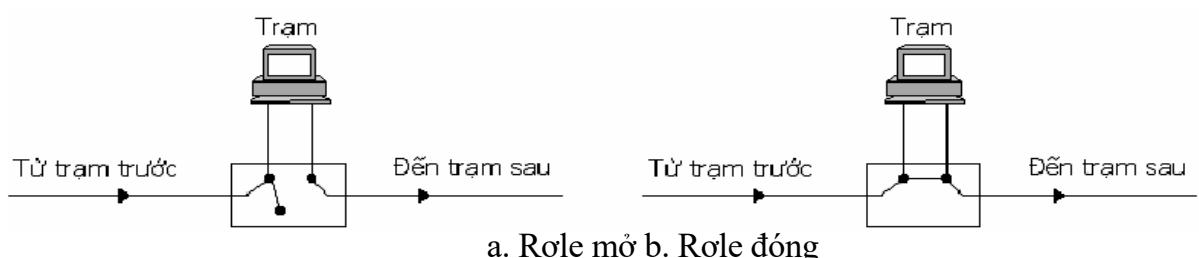
Nhiệm vụ đáng chú ý của monitor là phải đảm bảo luôn luôn có sự hiện diện của thẻ bài ở đâu đó trên vòng, có thể là đang di chuyển hay đang bị giữ bởi một trạm nào đó. Rõ ràng là thẻ bài có thể bị biến mất vì lý do nào đó chẳng hạn như lỗi bit, trạm đang giữ nó bị hư hỏng. Để phát hiện ra việc thẻ bài bị mất, khi thẻ bài chạy ngang qua monitor, nó sẽ bật một bộ đếm thời gian để tính giờ. Bộ đếm này có giá trị tối đa là:

$$\text{Số lượng trạm} \times \text{THT} + \text{Độ trễ của vòng}$$

Trong đó “Số lượng trạm” là số các trạm làm việc đang hiện diện trên vòng, “độ trễ của vòng” là tổng thời gian lan truyền tín hiệu trên vòng. Nếu bộ đếm đạt đến giá trị tối đa mà monitor vẫn không thấy thẻ bài chạy qua nó nữa thì nó sẽ tạo ra thẻ bài mới.

Monitor cũng phải kiểm tra xem có khung nào bị hỏng hoặc vô thừa nhận hay không. Một khung nếu có lỗi checksum hoặc khuôn dạng không hợp lệ sẽ chạy một cách vô định trên vòng. Monitor sẽ thu khung này lại trước khi chèn lại thẻ bài vào vòng. Một khung vô thừa nhận là khung mà đã được chèn thành công vào vòng, nhưng cha của nó bị chết, nghĩa là trạm gửi nó chỉ gửi nó lên vòng, nhưng chưa kịp thu nó lại thì đã bị chết (down). Những khung như vậy sẽ bị phát hiện bằng cách thêm vào một bit điều khiển gọi là monitor bit. Khi được phát lần đầu tiên, monitor bit trên khung sẽ nhận giá trị 0. Khi khung đi ngang qua monitor, monitor sẽ đặt monitor bit lên 1. Nếu monitor thấy khung này lại chạy qua nó với monitor bit là 1, nó sẽ rút khung này ra khỏi vòng.

Một chức năng quản lý vòng khác là phát hiện ra một trạm bị chết. Nếu một trạm trong vòng bị chết, nó sẽ làm đứt vòng. Để tránh tình trạng này người ta thêm vào trạm một ro-le điện tử (relay). Khi trạm còn mạnh khỏe, ro-le sẽ mở và trạm được nối với vành, khi trạm bị chết và ngưng không cung cấp năng lượng cho role, role sẽ tự động đóng mạch và bỏ qua trạm này.



Hình 3. 12 Sử dụng role

Khi monitor nghi ngờ một trạm bị chết, nó sẽ gửi đến trạm đó một khung đặc biệt gọi là khung beacon. Nếu không nhận được trả lời thích đáng, monitor sẽ coi trạm đó đã chết.

4.2.3.3. Ví dụ về phương pháp chuyển thẻ bài: Token BUS

Kỹ thuật Token Bus về bản chất là sử dụng mạng hình bus. Tuy nhiên người ta muốn thiết lập một vòng ảo trên đó để nó hoạt động giống như Token Ring. Nguyên tắc hoạt động như sau: trạm có nhu cầu truyền dữ liệu thì sẽ tham gia vào vòng ảo, ngược lại thì sẽ nằm ngoài và chỉ nghe thôi!

Giải thuật bổ sung một trạm vào vòng:

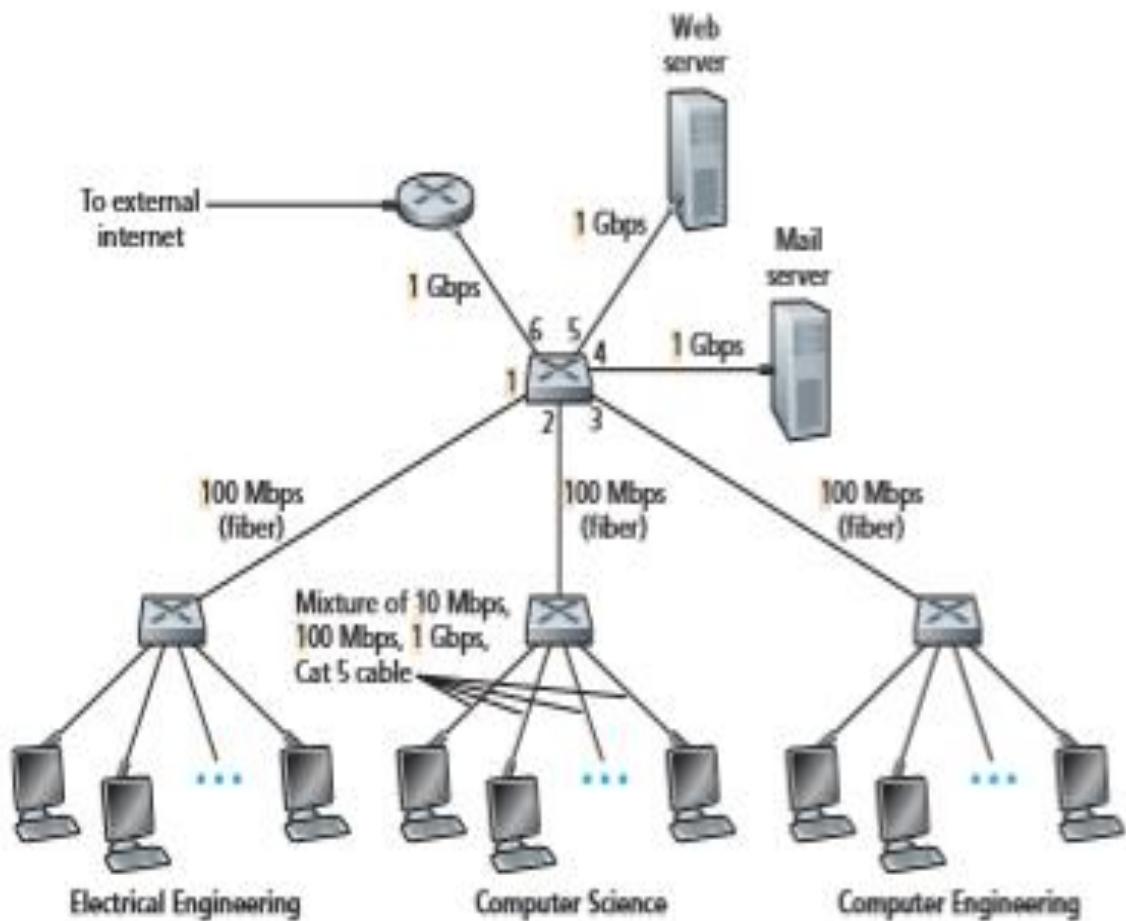
- ✓ Mỗi trạm trong vòng có trách nhiệm định kỳ tạo điều kiện cho các trạm khác tham gia vào vòng.
- ✓ Trước khi chuyển thẻ bài đi, trạm sẽ gửi thông báo “tìm trạm đứng sau” (có địa chỉ giữa nó và trạm đứng liền kề hiện tại).
- ✓ Nếu sau một thời gian xác định mà vẫn không có yêu cầu gia nhập nào, trạm sẽ chuyển thẻ bài đến trạm kế tiếp như thường lệ.
- ✓ Nếu có yêu cầu gia nhập vòng, thì trạm sẽ ghi nhận trạm mới yêu cầu là trạm kế tiếp của nó và sẽ chuyển thẻ bài tới trạm kế mới này.

Giải thuật rút lui ra khỏi vòng:

- ✓ Khi muốn rút ra khỏi vòng, trạm sẽ chờ đến khi nó có token, sau đó sẽ gửi yêu cầu “nối trạm đứng sau” tới trạm đứng trước nó, yêu cầu trạm đứng trước nối trực tiếp với trạm đứng liền sau nó.
- ✓ Ngoài ra còn phải quan tâm đến tình trạng mất thẻ bài, các trạm thành viên trong vòng bị hư hỏng.

3.4. Chuyển mạch trong LAN

Trong hình 3.13 cho thấy một mạng cục bộ được chuyển đổi kết nối ba phòng ban, hai máy chủ và bộ định tuyến với bốn thiết bị chuyển mạch. Vì các giao thức này hoạt động ở tầng liên kết, chúng chuyển đổi các khung tầng liên kết (chứ không phải các datagram tầng mạng), không nhận ra địa chỉ lớp mạng và không sử dụng các thuật toán định tuyến như RIP hoặc OSPF để xác định đường dẫn qua mạng của giao thức tầng 2. Thay vì sử dụng địa chỉ IP, mà sử dụng địa chỉ lớp liên kết để chuyển tiếp các khung liên kết thông qua mạng lưới các thiết bị chuyển mạch.



Hình 3. 13 Hệ thống kết nối mạng

3.4.1. Địa chỉ liên kết và ARP

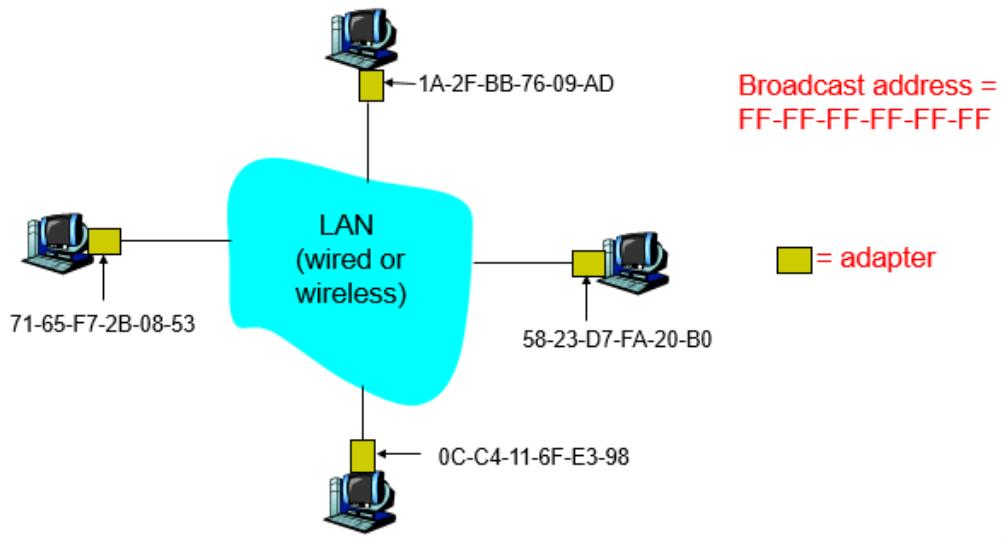
3.4.1.1. Địa chỉ MAC

Địa chỉ MAC (media access control: kiểm soát truy cập phương tiện truyền thông) của máy tính là một định danh duy nhất (unique identifier) được gán cho một bộ điều khiển giao diện mạng cho truyền thông tại tầng liên kết dữ liệu của một phân đoạn mạng. Địa chỉ MAC được sử dụng làm địa chỉ mạng cho hầu hết các công nghệ mạng IEEE 802, bao gồm Ethernet và Wi-Fi. Về mặt logic, các địa chỉ MAC được sử dụng trong tầng con của media access control của mô hình tham chiếu OSI.

Địa chỉ MAC thường được chỉ định bởi nhà sản xuất bộ điều khiển giao diện mạng (NIC) và được lưu trữ trong phần cứng, chẳng hạn như bộ nhớ chỉ đọc của card mạng hoặc một số cơ chế phần mềm khác. Nếu được chỉ định bởi nhà sản xuất, một địa chỉ MAC thường mã hóa số nhận dạng của nhà sản xuất đã đăng ký. Nó cũng có thể được biết đến như một địa chỉ phần cứng Ethernet (EHA), địa chỉ phần cứng hoặc địa chỉ vật lý (không nên nhầm lẫn với địa chỉ vật lý bộ nhớ). Điều này có thể tương phản với địa chỉ được lập trình, nơi thiết bị ban lệnh đến NIC sử dụng một địa chỉ nào đó.

Một nút mạng có thể có nhiều NIC và mỗi NIC phải có một địa chỉ MAC duy nhất. Các thiết bị mạng tinh vi như chuyển mạch multilayer hoặc router có thể đòi hỏi một hoặc nhiều địa chỉ MAC được gán vĩnh viễn.

Địa chỉ MAC được hình thành theo quy tắc của một trong ba không gian tên số do Viện Kỹ sư Điện và Điện tử (IEEE) quản lý: MAC-48, EUI-48 và EUI-64. IEEE tuyên bố nhãn hiệu với tên EUI-48 và EUI-64, trong đó EUI là chữ viết tắt từ Extended Identity Identifier.



Hình 3. 14 Địa chỉ MAC

3.4.1.2. Giao thức phân giải địa chỉ (ARP)

Trên thực tế, các card mạng (NIC) chỉ có thể kết nối với nhau theo địa chỉ MAC, địa chỉ cố định và duy nhất của phần cứng. Do vậy ta phải có một cơ chế để chuyển đổi các dạng địa chỉ này qua lại với nhau. Từ đó ta có giao thức phân giải địa chỉ: Address Resolution Protocol (ARP).

Nguyên tắc làm việc của ARP trong một mạng LAN

Khi một thiết bị mạng muốn biết địa chỉ MAC của một thiết bị mạng nào đó mà nó đã biết địa chỉ ở tầng network (IP, IPX...) nó sẽ gửi một ARP request bao gồm địa chỉ MAC address của nó và địa chỉ IP của thiết bị mà nó cần biết MAC address trên toàn bộ

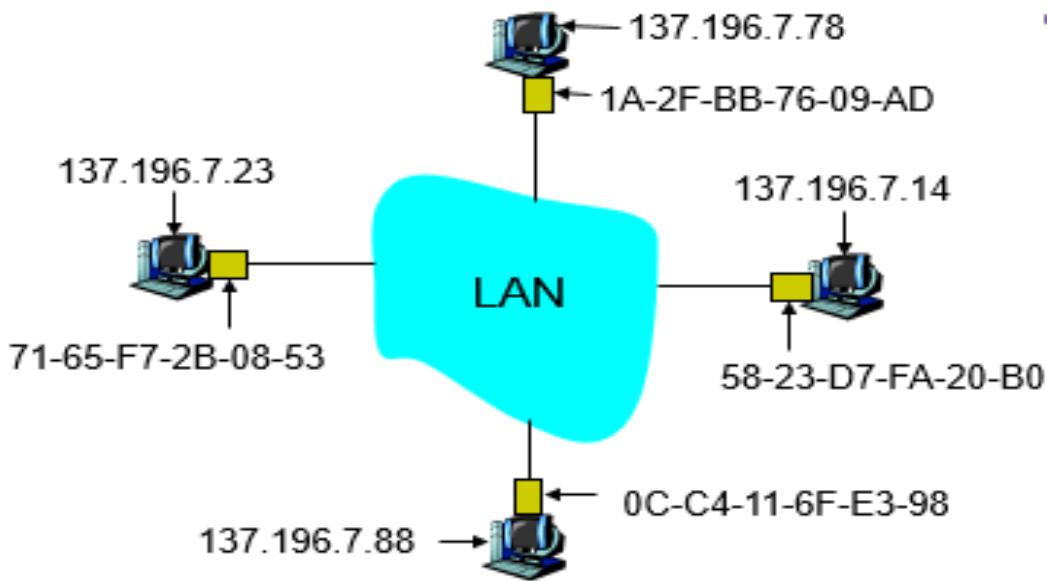
một miền broadcast. Mỗi một thiết bị nhận được request này sẽ so sánh địa chỉ IP trong request với địa chỉ tầng network của mình. Nếu trùng địa chỉ thì thiết bị đó phải gửi ngược lại cho thiết bị gửi ARP request một gói tin (trong đó có chứa địa chỉ MAC của mình). Trong một hệ thống mạng đơn giản, ví dụ như PC A muốn gửi gói tin đến PC B và nó chỉ biết được địa chỉ IP của PC B. Khi đó PC A sẽ phải gửi một ARP broadcast cho toàn mạng để hỏi xem "địa chỉ MAC của PC có địa chỉ IP này là gì?" Khi PC B nhận được broadcast này, nó sẽ so sánh địa chỉ IP trong gói tin này với địa chỉ IP của nó. Nhận thấy địa chỉ đó là địa chỉ của mình, PC B sẽ gửi lại một gói tin cho PC A trong đó có chứa địa chỉ MAC của B. Sau đó PC A mới bắt đầu truyền gói tin cho B.

Nguyên tắc hoạt động của ARP trong môi trường hệ thống mạng:

Hoạt động của ARP trong một môi trường phức tạp hơn đó là hai hệ thống mạng gắn với nhau thông qua một Router C. Máy A thuộc mạng A muốn gửi gói tin đến máy B thuộc mạng B. Do các broadcast không thể truyền qua Router nên khi đó máy A sẽ xem Router C như một cầu nối hay một trung gian (Agent) để truyền dữ liệu. Trước đó, máy A sẽ biết được địa chỉ IP của Router C (địa chỉ Gateway) và biết được rằng để truyền gói tin tới B phải đi qua C. Tất cả các thông tin như vậy sẽ được chứa trong một bảng gọi là bảng định tuyến (routing table). Bảng định tuyến theo cơ chế này được lưu giữ trong mỗi máy. Bảng định tuyến chứa thông tin về các Gateway để truy cập vào một hệ thống mạng nào đó. Ví dụ trong trường hợp trên trong bảng sẽ chỉ ra rằng để đi tới LAN B phải qua port X của Router C. Bảng định tuyến sẽ có chứa địa chỉ IP của port X. Quá trình truyền dữ liệu theo từng bước sau:

- Máy A gửi một ARP request (broadcast) để tìm địa chỉ MAC của port X.
- Router C trả lời, cung cấp cho máy A địa chỉ MAC của port X.
- Máy A truyền gói tin đến port X của Router.
- Router nhận được gói tin từ máy A, chuyển gói tin ra port Y của Router. Trong gói tin có chứa địa chỉ IP của máy B. Router sẽ gửi ARP request để tìm địa chỉ MAC của máy B.
- Máy B sẽ trả lời cho Router biết địa chỉ MAC của mình. Sau khi nhận được địa chỉ MAC của máy B, Router C gửi gói tin của A đến B.

Trên thực tế ngoài dạng bảng định tuyến này người ta còn dùng phương pháp proxyARP, trong đó có một thiết bị đảm nhận nhiệm vụ phân giải địa chỉ cho tất cả các thiết bị khác. Theo đó các máy trạm không cần giữ bảng định tuyến nữa Router C sẽ có nhiệm vụ thực hiện, trả lời tất cả các ARP request của tất cả các máy.



Hình 3. 15 Giao thức ARP

3.4.2. Ethernet

Ethernet là một họ lớn và đa dạng gồm các công nghệ mạng dựa khung dữ liệu (frame-based) dành cho mạng LAN. Tên Ethernet xuất phát từ khái niệm Éte trong ngành vật lý học. Ethernet định nghĩa một loạt các chuẩn nối dây và phát tín hiệu cho tầng vật lý, hai phương tiện để truy nhập mạng tại phần MAC (điều khiển truy nhập môi trường truyền dẫn) của tầng liên kết dữ liệu, và một định dạng chung cho việc đánh địa chỉ.

Ethernet đã được chuẩn hóa thành IEEE 802.3. Cấu trúc mạng hình sao, hình thức nối dây cáp xoắn (twisted pair) của Ethernet đã trở thành công nghệ LAN được sử dụng rộng rãi nhất từ thập kỷ 1990 cho tới nay, nó đã thay thế các chuẩn LAN cạnh tranh khác như Ethernet cáp đồng trục (coaxial cable), token ring, FDDI, và ARCNET. Trong những năm gần đây, Wi-Fi, dạng LAN không dây đã được chuẩn hóa bởi IEEE 802.11, đã được sử dụng bên cạnh hoặc thay thế cho Ethernet trong nhiều cấu hình mạng.

Mỗi host trong một mạng Ethernet (thật ra là tất cả các host trên thế giới) có một địa chỉ Ethernet duy nhất. Mô tả một cách kỹ thuật, địa chỉ được gắn vào card mạng chứ không phải máy tính; nó được ghi vào ROM trên card mạng. Các địa chỉ Ethernet thường được in theo thể thức mà con người có thể đọc được: một dãy gồm 6 bytes được viết dưới dạng thập lục phân, cách nhau bởi dấu hai chấm. Ví dụ 8:0:2b:e4:b1:2 là cách biểu diễn dễ đọc của địa chỉ Ethernet sau 00001000 00000000 00101011 11100100 10110001 00000010. Để đảm bảo rằng mọi card mạng được gán một địa chỉ duy nhất, mỗi nhà sản xuất thiết bị Ethernet được cấp cho một phần đầu địa chỉ (prefix) khác nhau. Ví dụ Advanced Micro Devices đã được cấp phần đầu dài 24 bit x08002 (hay 8:0:2). Nhà sản

xuất này sau đó phải đảm bảo phần đuôi (suffix) của các địa chỉ mà họ sản xuất ra là duy nhất.

Mỗi khung được phát ra Ethernet sẽ được nhận bởi tất cả các card mạng có nối với đường truyền. Mỗi card mạng sẽ so sánh địa chỉ đích trong khung với địa chỉ của nó, và chỉ cho vào máy tính những khung nào trùng địa chỉ. Địa chỉ duy nhất như vậy gọi là địa chỉ **unicast**. Ngoài ra còn có loại địa chỉ **broadcast** là loại địa chỉ quảng bá, có tất cả các bit đều mang giá trị 1. Mọi card mạng đều cho phép các khung thông tin có địa chỉ đích là **broadcast** đi đến host của nó. Cũng có một loại địa chỉ khác gọi là **multicast**, trong đó chỉ một vài bit đầu được đặt là 1. Một host có thể lập trình điều khiển card mạng của nó chấp nhận một số lớp địa chỉ **multicast**. Địa chỉ **multicast** được dùng để gửi thông điệp đến một tập con (subset) các host trong mạng Ethernet.

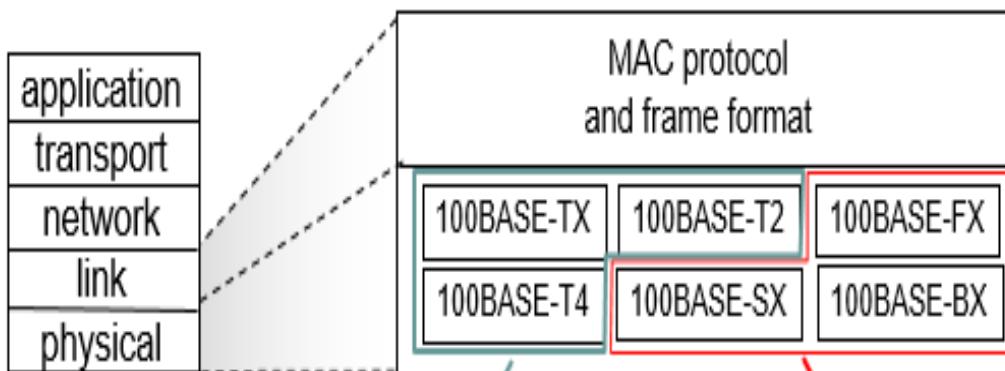
Các công nghệ Ethernet.

➤ 10 BASE 2

Mạng Ethernet 10BASE2 sử dụng cáp đồng trực gãy, hình thái bus. Trong trường hợp mạng có nhiều segments, các repeaters sẽ được sử dụng để nối kết các segments này lại.

➤ 10 BASE T và 100 BASE T

Mạng đạt tốc độ 10/100 Mbps, về sau được gọi là “fast Ethernet”. Chữ T viết tắt cho Twisted Pair: cáp xoắn đôi. Cách thức nối mạng được mô phỏng như sau: Các HUB được nối tới các SWITCH bằng cáp xoắn đôi. Với cách thức đấu nối như vậy, mạng được gọi là “hình sao”. Cơ chế CSMA/CD được cài đặt tại HUB.



Hình 3. 16 Các chuẩn Ethernet 100 Mbps

➤ GIGABIT ETHERNET

Gbit Ethernet sử dụng khuôn dạng khung chuẩn của Ethernet cho phép mạng hoạt động trên cả hai kiểu nối kết điểm-điểm và kênh quảng bá chia sẻ. Trong kiểu nối kết điểm-điểm, Gbit Ethernet sử dụng các switches thay cho các hub. Đường truyền được sử dụng theo kiểu hai chiều đồng thời với tốc độ 1 Gbps.

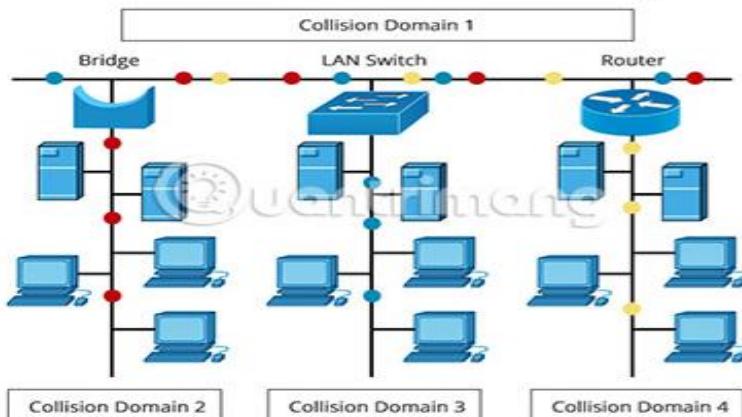
3.4.3 Chuyển mạch trong LAN (LAN SWITCH)

Một mạng doanh nghiệp thường bao gồm nhiều chi nhánh. Các thiết bị người dùng đầu cuối trong nội bộ một site như PC, laptop, smartphone, được kết nối với nhau thông qua hệ thống mạng nội bộ (Local Area Network – LAN). Tiếp theo đó, mỗi site lại sử dụng thiết bị router để kết nối mạng LAN vào đường truyền WAN (Wide Area Network) thuê từ các nhà cung cấp dịch vụ Internet. Với các router và các kết nối WAN, người dùng đầu cuối giữa các site có thể trao đổi dữ liệu với nhau và truy nhập được Internet.

Trong lịch sử phát triển, có rất nhiều kiến trúc LAN đã từng tồn tại như Token Ring, FDDI (Fiber Distributed Data Interface), Ethernet. Tuy nhiên, cuối cùng kiến trúc mạng LAN còn lại và được sử dụng rộng rãi ngày nay là Ethernet LAN. Do đó, khi nói đến, mạng LAN, người ta thường nghĩ ngay đến Ethernet LAN.

Chuyển mạch LAN là một hình thức chuyển mạch trong đó các gói dữ liệu được truyền từ máy tính này sang máy tính khác qua mạng LAN. Công nghệ chuyển mạch LAN rất quan trọng đối với thiết kế mạng, vì nó cho phép lưu lượng chỉ được gửi đến những nơi được yêu cầu. Chuyển mạch LAN chủ yếu bao gồm 3 loại phương thức chuyển đổi: Chuyển mạch Layer 2 bằng phần cứng dựa trên địa chỉ MAC, chuyển mạch Layer 3 dựa trên địa chỉ IP và chuyển mạch Layer 4 trong đó có thể xác định QoS (Quality of Service) cho mỗi người dùng. Trong số 3 phương thức này, chuyển mạch Layer 2 được sử dụng rộng rãi nhất cho phân đoạn mạng (network segmentation) trong mạng LAN. Như được minh họa bên dưới, LAN switch được kết nối giữa bridge và router để tạo thành 4 collision domain (miền xung đột). Nó cho phép một thiết kế mạng phẳng hơn với nhiều phân đoạn mạng hơn các mạng truyền thống (được tạo thành bởi

Collision Domains in LAN Switching



repeater, hub và router).

Hình 3.17 Phân đoạn Mạng

Một mạng LAN thông thường bao gồm một hoặc nhiều LAN switch có thể được kết nối với router, modem hoặc bridge để truy cập Internet. Các thiết bị mạng khác như tường lửa, trình cân bằng tải và trình phát hiện xâm nhập mạng cũng có thể được bao

gồm trong mạng LAN. Các mạng LAN nâng cao được đặc trưng bởi việc sử dụng các liên kết dự phòng với các LAN switch, bằng cách sử dụng giao thức Spanning Tree để ngăn chặn các vòng lặp, phân phối QoS và phân tách lưu lượng với Vlan.

LAN switch là thành phần thiết yếu được sử dụng trong các mạng LAN. LAN switch là một switch mạng kết nối hai hoặc nhiều mạng LAN và chuyển tiếp các gói giữa các mạng này. Tốc độ tối đa của LAN switch không quá con số Gigabit, thông thường ở mức 1000 megabit/giây. LAN switch sử dụng ba loại chuyển mạch LAN, đó là chuyển mạch Layer 2, Layer 3 và Layer 4 để định tuyến lưu lượng trong mạng LAN. Vì hầu hết các LAN switch hoạt động ở tầng Data Link (Layer 2), nên switch Layer 2 được sử dụng phổ biến nhất và có thể được tìm thấy trong gần như bất kỳ mạng LAN nào. Nó cung cấp một số lợi ích của cả bridge và router. Giống như bridge, LAN switch Layer 2 có thể chuyển tiếp lưu lượng dựa trên header Layer 2. Giống như router, nó phân vùng mạng thành các phân đoạn hợp lý, cung cấp khả năng quản trị, bảo mật và quản lý multicast traffic tốt hơn. Switch Layer 3 hoặc Layer 4 đòi hỏi công nghệ tiên tiến và đắt tiền hơn, do đó chúng thường được sử dụng nhiều hơn trong mạng LAN lớn hoặc trong môi trường mạng đặc biệt.

Phương thức định tuyến lưu lượng.

➤ Cut-through

Trong phương thức Cut-through, LAN switch có thể đọc địa chỉ MAC ngay khi nó phát hiện gói tin. Sau khi lưu trữ 6 byte tạo thành thông tin địa chỉ MAC, chúng ngay lập tức gửi gói đến node đích, ngay cả khi phần còn lại của gói vẫn đang tiếp tục truyền tới switch.

➤ Store-and-forward

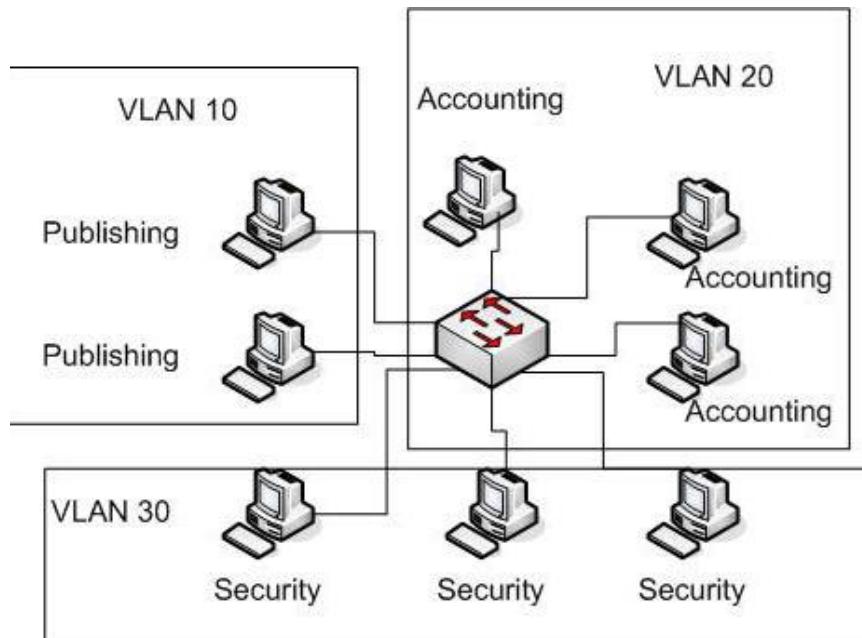
Phương thức Store-and-forward sẽ lưu toàn bộ gói vào bộ đệm và kiểm tra lỗi trước khi gửi đến node đích. Nếu gói có lỗi, nó sẽ bị loại bỏ. Nếu không, switch sẽ tra cứu địa chỉ MAC và gửi gói đến node đích. Nhiều LAN switch có thể kết hợp hai phương thức này, sử dụng Cut-through cho đến khi đạt đến một mức lỗi nhất định và sau đó thay đổi sang phương thức Store-and-forward.

➤ Fragment-free

Một phương pháp ít phổ biến hơn là Fragment-free. Nó hoạt động tương tự như phương thức Cut-through ngoại trừ việc lưu trữ 64 byte đầu tiên của gói trước khi gửi đi. Lý do là hầu hết các lỗi và xung đột xảy ra trong 64 byte đầu tiên của gói. Chuyển mạch LAN đi kèm với khả năng mở rộng cao, bảo mật và dễ quản lý. Hiện tại, LAN switch tốc độ tương đối thấp thường được sử dụng trong kiến trúc mạng vòng và Daisy-Chain, do phạm vi địa lý hạn chế của mạng LAN.

3.4.4. Mạng LAN ảo VLAN

VLAN là viết tắt của Virtual Local Area Network hay còn gọi là mạng LAN ảo. Một VLAN được định nghĩa là một nhóm logic các thiết bị mạng và được thiết lập dựa trên các yếu tố như chức năng, bộ phận, ứng dụng... của công ty. Về mặt kỹ thuật, VLAN là một miền quảng bá được tạo bởi các switch. Bình thường thì router đóng vai trò tạo ra miền quảng bá. Đối với VLAN, switch có thể tạo ra miền quảng bá. Việc này được thực hiện khi người quản trị đặt một số cổng switch trong VLAN ngoại trừ VLAN 1 - VLAN mặc định. Tất cả các cổng trong một mạng VLAN đơn đều thuộc một miền quảng bá duy nhất. Vì các switch có thể giao tiếp với nhau nên một số cổng trên switch A có thể nằm trong VLAN 10 và một số cổng trên switch B cũng có thể trong VLAN 10. Các bản tin quảng bá giữa những máy tính này sẽ không bị lộ trên các cổng thuộc bất kỳ VLAN nào ngoại trừ VLAN 10. Tuy nhiên, tất cả các máy tính này đều có thể giao tiếp với nhau vì chúng thuộc cùng một VLAN. Nếu không được cấu hình bổ sung, chúng sẽ không thể giao tiếp với các máy tính khác nằm ngoài VLAN này.



Hình 3. 18 Mô hình mạng VLAN

Lợi ích của VLAN

Tiết kiệm băng thông của hệ thống mạng: VLAN chia mạng LAN thành nhiều đoạn (segment) nhỏ, mỗi đoạn đó là một vùng quảng bá (broadcast domain). Khi có gói tin quảng bá (broadcast), nó sẽ được truyền duy nhất trong VLAN tương ứng. Do đó việc chia VLAN giúp tiết kiệm băng thông của hệ thống mạng.

Tăng khả năng bảo mật: Do các thiết bị ở các VLAN khác nhau không thể truy nhập vào nhau (trừ khi ta sử dụng router nối giữa các VLAN). Như trong ví dụ trên, các máy tính trong VLAN kế toán (Accounting) chỉ có thể liên lạc được với nhau. Máy ở VLAN kế toán không thể kết nối được với máy tính ở VLAN kỹ sư (Engineering).

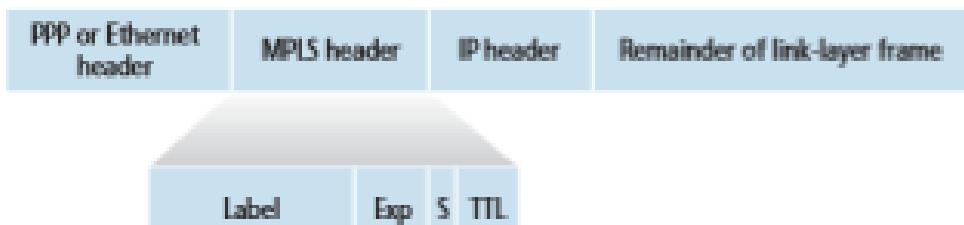
Dễ dàng thêm hay bớt máy tính vào VLAN: Việc thêm một máy tính vào VLAN rất đơn giản, chỉ cần cấu hình cổng cho máy đó vào VLAN mong muốn.

Giúp mạng có tính linh động cao: VLAN có thể dễ dàng di chuyển các thiết bị. Giả sử trong ví dụ trên, sau một thời gian sử dụng công ty quyết định để mỗi bộ phận ở một tầng riêng biệt. Với VLAN, ta chỉ cần cấu hình lại các cổng switch rồi đặt chúng vào các VLAN theo yêu cầu. VLAN có thể được cấu hình tĩnh hay động. Trong cấu hình tĩnh, người quản trị mạng phải cấu hình cho từng cổng của mỗi switch. Sau đó, gán cho nó vào một VLAN nào đó. Trong cấu hình động mỗi cổng của switch có thể tự cấu hình VLAN cho mình dựa vào địa chỉ MAC của thiết bị được kết nối vào.

3.5. Liên kết ảo

Trong phần này sẽ tìm hiểu mạng liên kết ảo MPLS. MPLS là thuật ngữ viết tắt cho Multi-Protocol Label Switching (chuyển mạch nhãn đa giao thức). Nguyên tắc cơ bản của MPLS là thay đổi các thiết bị tầng 2 trong mạng như các thiết bị chuyển mạch ATM thành các LSR (label-switching router-Bộ định tuyến chuyển mạch nhãn). LSR có thể được xem như một sự kết hợp giữa hệ thống chuyển mạch ATM với các bộ định tuyến truyền thông.

Trên đường truyền dữ liệu, LSR đầu tiên được gọi là Ingress LSR; LSR cuối cùng được gọi là Egress LSR; còn lại các LSR trung gian gọi là các Core LSR. Trong một mạng MPLS mỗi gói dữ liệu sẽ chứa một nhãn (label) dài 20 bit nằm trong tiêu đề MPLS (MPLS header) dài 32 bit. Đầu tiên, một nhãn sẽ được gán tại Ingress LSR để sau đó sẽ được chuyển tiếp qua mạng theo thông tin của bảng định tuyến. Khối chức năng điều khiển của mạng sẽ tạo ra và duy trì các bảng định tuyến này và đồng thời cũng có sự trao đổi về thông tin định tuyến với các nút (node) mạng khác.



Hình 3. 19 Tiêu đề MPLS

Việc chia tách riêng hai khối chức năng độc lập nhau là: chuyển tiếp và điều khiển là một trong các thuộc tính quan trọng của MPLS. Khối chức năng điều khiển sử dụng một giao thức định tuyến truyền thông (ví dụ: OSPF) để tạo ra và duy trì một bảng chuyển tiếp. Khi gói dữ liệu đến một LSR, chức năng chuyển tiếp sẽ sử dụng thông tin ghi trong tiêu đề để tìm kiếm bảng chuyển tiếp phù hợp và LSR đó sẽ gán một nhãn vào gói tin và chuyển nó đi theo tuyến LSP (label-switched path: tuyến chuyển mạch nhãn). Tất cả các gói có nhãn giống nhau sẽ đi theo cùng tuyến LSP từ điểm đầu đến điểm cuối.

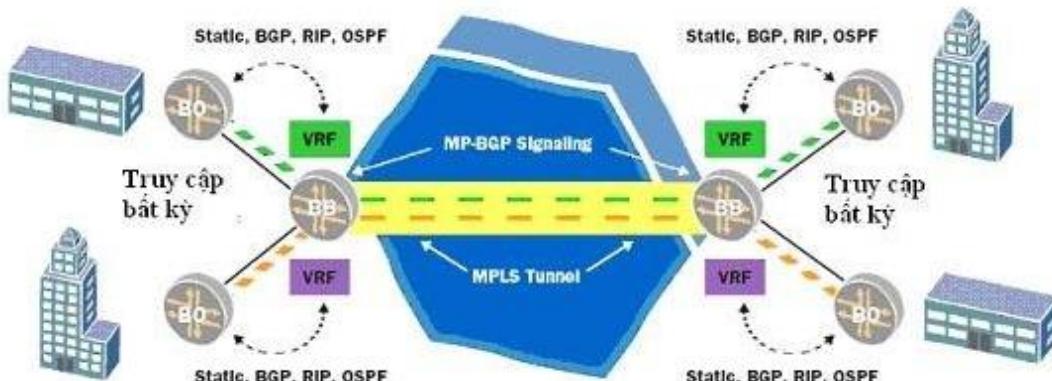
Đây là điểm khác với các giao thức định tuyến truyền thống (có thể có nhiều tuyến đường nối giữa hai điểm)

Các Core LSR sẽ bỏ qua phần tiêu đề lớp mạng của gói, khôi phục nhãn chuyển tiếp của những LSR này sử dụng số cổng vào (input port number) và nhãn để thực hiện việc tìm kiếm bảng chuyển tiếp phù hợp rồi sau đó thay thế nhãn mới và chuyển ra ngoài vào tuyến LSP.

Như vậy, Công nghệ MPLS là một dạng phiên bản của công nghệ IPoA (IP over ATM) truyền thông, nên MPLS có cả ưu điểm của ATM (tốc độ cao, QoS và điều khiển luồng) và của IP (độ mềm dẻo và khả năng mở rộng). Giải quyết được nhiều vấn đề của mạng hiện tại và hỗ trợ được nhiều chức năng mới, MPLS được cho là công nghệ mạng trực IP lý tưởng.

MPLS dùng trong VPN: Cấu hình một mạng riêng ảo dựa trên MPLS có thể triển khai trên tầng 3 hoặc tầng 2 như sau: **VPN/ MPLS tầng 3**

Thường được xây dựng dựa trên tiêu chuẩn IETF RFC 2547bis. Lớp này của VPN chuyển tải lưu lượng qua mạng thông qua sử dụng đường hầm MPLS và giao thức báo hiệu MP-BGP (Multiprotocol Border Gateway Protocol) như minh họa trong hình 3.20.



Hình 3. 20 VPN layer 3

Lợi ích của MPLS với doanh nghiệp, tổ chức

Với mạng sử dụng MPLS có rất nhiều các dịch vụ được cung cấp với chất lượng cao như:

1. Tải tin cho các mạng số liệu, Internet và thoại quốc gia. Lưu lượng thoại được chuyển dần sang mạng trực MPLS quốc gia. Mạng này sẽ thay thế dần mạng trực TDM quốc gia đang hoạt động.

2. Cung cấp dịch vụ truy nhập Internet tốc độ cao tại một số địa phương trọng điểm trên toàn quốc. Bước đầu hình thành mạng trực quốc gia trên cơ sở công nghệ gói.

3. Cung cấp dịch vụ truyền số liệu tốc độ cao cho các doanh nghiệp, tổ chức như Ngân hàng, các hãng thông tấn báo chí.

4. Cung cấp dịch vụ mạng riêng ảo VPN cho các công ty xuyên quốc gia và các doanh nghiệp, tổ chức lớn. Đây đang được coi như dịch vụ quan trọng nhất tác động đến việc thay đổi cơ cấu kinh doanh và tăng khả năng cạnh tranh của các nhà khai thác.

5. Cung cấp dịch vụ Video.

Đối với các doanh nghiệp, tổ chức, loại hình mạng riêng ảo trên mạng diện rộng đang là nhu cầu bức thiết nhất và thể hiện lợi ích rõ ràng với hoạt động của các đối tượng này. Để một công ty đạt được các mục tiêu kinh doanh, hạ tầng mạng riêng phải được tách rộn theo mọi hướng. Mạng MPLS có khả năng hỗ trợ hàng nghìn mạng riêng ảo chỉ trên một hạ tầng vật lý duy nhất nhờ đặc điểm phân chia nhiệm vụ đã giảm bớt yêu cầu kết nối ngang hàng hoàn toàn đầu- cuối qua mạng. Xét về khả năng hỗ trợ VPN, các hạ tầng mạng riêng ảo truyền thống dựa trên các công nghệ cũ như leased line, X25, ATM không thể đáp ứng được thực trạng đa dạng về yêu cầu, đa dạng về chất lượng dịch vụ của hàng loạt các đối tượng khách hàng như hiện nay. Đây sẽ là lý do khiến các nhà cung cấp dịch vụ này phải chuyển hướng sang một mô hình cung cấp khác hiệu quả hơn.

Như vậy, với mạng riêng dựa trên MPLS các doanh nghiệp, tổ chức hoàn toàn có thể đạt được các mục tiêu của mình như: điều khiển nhiều hơn trên hạ tầng mạng, có được dịch vụ hiệu năng và độ tin cậy tốt hơn, cung cấp đa lớp dịch vụ tới người sử dụng, mở rộng an toàn, đảm bảo hiệu năng đáp ứng theo yêu cầu của ứng dụng, hỗ trợ hội tụ đa công nghệ và đa kiểu lưu lượng trên cùng một mạng đơn. Tuy nhiên, các đơn vị này khi chọn lựa nhà cung cấp phần cứng cần phải cẩn thận và phải căn cứ trên nhiều góc độ và tiêu chí đánh giá khác nhau. Ví dụ có thể căn cứ các tài liệu đánh giá hiệu năng sản phẩm của các đơn vị truyền thông, bức tranh phát triển của nhà cung cấp đó cả về chiều rộng và chiều sâu. Nhờ ưu điểm vượt trội của chất lượng dịch vụ qua mạng IP và là phương án triển khai VPN mới khắc phục được nhiều vấn đề mà các công nghệ ra đời trước nó chưa giải quyết được, MPLS thực sự là một lựa chọn hiệu quả trong triển khai hạ tầng thông tin doanh nghiệp.

TÓM TẮT NỘI DUNG CỐT LÕI.

- Giới thiệu về tầng Liên kết giữ liệu.
- Kỹ thuật phát hiện và sửa lỗi.
- Đa liên kết truy cập và Các giao thức.
- Chuyển mạch trong LAN.
- Liên kết ảo.

BÀI TẬP ÚNG DỤNG, LIÊN HỆ THỰC TẾ.

Bài 1. Nếu tất cả các liên kết trong Internet là để cung cấp dịch vụ phân phối đáng tin cậy, liệu dịch vụ phân phối TCP đáng tin cậy có bị dư thừa không? Tại sao?

Bài 2. Một số dịch vụ có thể có mà giao thức lớp liên kết có thể cung cấp cho lớp mạng là gì? Những dịch vụ lớp liên kết nào có dịch vụ tương ứng trong IP? Trong TCP?

Bài 3. Trong CSMA / CD, sau lần va chạm thứ năm, xác suất mà một nút chọn $K = 4$ là bao nhiêu? Kết quả $K = 4$ tương ứng với độ trễ là bao nhiêu giây trên Ethernet 10 Mb / giây?

Bài 4. Tại sao giao thức Token-ring không hiệu quả nếu mạng LAN có chu vi rất lớn?

Bài 5. Không gian địa chỉ MAC lớn như thế nào? Không gian địa chỉ IPv4? Không gian địa chỉ IPv6?

Bài 6. Giả sử các nút A, B và C mỗi nút gắn vào cùng một mạng LAN quảng bá (thông qua bộ điều hợp của chúng). Nếu A gửi hàng ngàn IPdatagram tới B với mỗi khung đóng gói được gửi đến địa chỉ MAC của B, liệu C có phải là bộ điều hợp xử lý các khung này không? Nếu vậy, bộ điều hợp C có chuyển các IPdatagram trong các khung này sang lớp mạng C không? Câu trả lời của bạn sẽ thay đổi như thế nào nếu A gửi các khung có địa chỉ quảng bá MAC?

Bài 7. So sánh cấu trúc khung cho 10BASE-T, 100BASE-T và Gigabit Ethernet. Chúng khác nhau như thế nào?

Bài 8. Số lượng Vlan tối đa có thể được cấu hình trên một giao thức hỗ trợ 802.1Q là bao nhiêu? Tại sao?

Bài 9. Giả sử nội dung thông tin của gói là mẫu bit 1110 0110 1001 1101 và sơ đồ chẵn lẻ đang được sử dụng. Giá trị của trường chứa các bit chẵn lẻ sẽ là gì đối với trường hợp của sơ đồ chẵn lẻ hai chiều? Câu trả lời của bạn phải sao cho trường tổng kiểm tra có độ dài tối thiểu được sử dụng.

Chương 4. TẦNG MẠNG

Mục đích:

Các giao thức tầng mạng được nhiều chuyên gia đánh giá là phức tạp nhất trong các tầng của mô hình OSI. Tầng mạng cung cấp phương tiện để truyền các đơn vị dữ liệu qua mạng, đảm bảo truyền tin end-to-end, bởi vậy nó phải đáp ứng với nhiều kiểu mạng và nhiều dịch vụ cung cấp bởi các mạng khác nhau.

Hai chức năng chủ yếu của tầng mạng là chọn đường và chuyển tiếp. Ngoài hai chức năng quan trọng trên tầng mạng cũng thực hiện một số chức năng khác như:

Thiết lập, duy trì và giải phóng các liên kết logic, kiểm soát lỗi, kiểm soát luồng dữ liệu, dòn kênh/phân kênh, cắt/hợp dữ liệu v.v....

4.1. Giới thiệu về Tầng mạng

Các giao thức tầng mạng được nhiều chuyên gia đánh giá là phức tạp nhất trong các tầng của mô hình OSI. Tầng mạng cung cấp phương tiện để truyền các đơn vị dữ liệu qua mạng, đảm bảo truyền tin end-to-end, bởi vậy nó phải đáp ứng với nhiều kiểu mạng và nhiều dịch vụ cung cấp bởi các mạng khác nhau.

Hai chức năng chủ yếu của tầng mạng là chọn đường và chuyển tiếp. Ngoài hai chức năng quan trọng trên tầng mạng cũng thực hiện một số chức năng khác như:

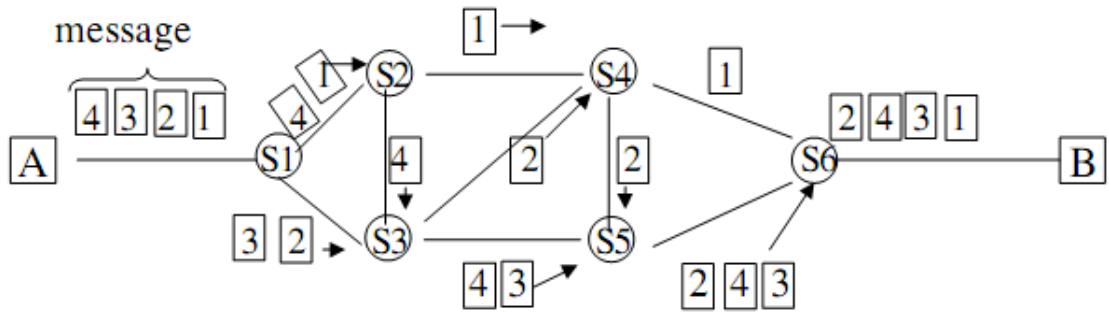
Thiết lập, duy trì và giải phóng các liên kết logic, kiểm soát lỗi, kiểm soát luồng dữ liệu, dòn kênh/phân kênh, cắt/hợp dữ liệu v.v....

4.2. Mạch ảo và mạng gói dữ liệu

Nguyên lý chuyển mạch gói: Thông điệp (Message) của người sử dụng được chia thành nhiều gói nhỏ (Packet) có độ dài quy định. Độ dài gói tin cực đại (Maximum Transfer Unit) MTU trong các mạng khác nhau là khác nhau. Các gói tin của một thông điệp có thể truyền độc lập trên nhiều tuyến hướng đích và các gói tin của nhiều thông điệp khác nhau có thể cùng truyền trên một tuyến liên mạng. Tại mỗi node, các gói tin được tiếp nhận, lưu trữ, xử lý tại bộ nhớ, không cần phải lưu trữ tạm thời trên bộ nhớ ngoài (như đĩa cứng) và được chuyển tiếp đến node kế tiếp. Định tuyến các gói tin qua mạng nhanh hơn và hiệu quả hơn.

Kỹ thuật chuyển mạch gói có nhiều ưu điểm hơn so với chuyển mạch kênh:

- Các gói tin lưu chuyển hướng đích độc lập, trên một đường có thể chia sẻ cho nhiều gói tin. Vì vậy hiệu suất đường truyền cao hơn.
- Các gói tin được xếp hàng và truyền qua tuyến kết nối.
- Hai thực thể có tốc độ dữ liệu khác nhau có thể trao đổi các gói với tốc độ phù hợp.
- Trong mạng chuyển mạch kênh, khi lưu lượng tăng thì mạng từ chối thêm các yêu cầu kết nối (do nghẽn) cho đến khi giảm xuống. Trong mạng chuyển mạch gói, các gói tin vẫn được chấp nhận, nhưng trễ phân phát gói tin có thể tăng lên.



Hình 4. 1 Mạng chuyển mạch gói

Các công nghệ chuyển mạch gói: Nếu một thực thể gửi một gói dữ liệu qua mạng có độ dài lớn hơn kích thước gói cực đại MTU, nó sẽ được chia thành các gói nhỏ có độ dài quy định và gửi lên mạng. Có hai kỹ thuật được sử dụng trong các mạng chuyển mạch gói là kỹ thuật *datagram* trong mạng không liên kết (Connectionless) và kỹ thuật *kênh ảo* cho mạng hướng liên kết (Connection- Oriented).

- *Phương thức datagram sử dụng trong mạng không liên kết:* Mỗi một gói tin được lưu chuyển và xử lý độc lập, không cần tham chiếu đến các gói tin đã gửi trước. Mỗi một gói tin được xem như là một datagram.

Ưu, nhược điểm của phương thức datagram: Giai đoạn thiết lập và giải phóng kết nối sẽ được bỏ qua. Phù hợp với yêu cầu truyền khối lượng dữ liệu không lớn trong thời gian ngắn. Phương thức linh hoạt hơn so với phương thức kênh ảo. Nếu xảy ra nghẽn thông tin, các datagram có thể được định tuyến ra khỏi vùng nghẽn. Và nếu có node bị hỏng, các gói tin tự tìm một tuyến khác để lưu chuyển hướng đích, việc phân phát các gói tin tin cậy hơn.

- *Phương thức kênh ảo VC (Virtual Circuit) sử dụng trong mạng hướng liên kết:* Trước khi trao đổi thông tin, hai thực thể tham gia truyền thông đàm phán với nhau về các tham số truyền thông như kích thước tối đa của gói tin, các cửa sổ, đường truyền.... Một kênh ảo đã được hình thành thông qua liên mạng và tồn tại cho đến khi các thực thể ngừng trao đổi với nhau. Tại một thời điểm, có thể có nhiều kênh ảo đi và đến từ nhiều hướng khác nhau. Các gói tin vẫn được đệm tại mỗi node và được xếp hàng đầu ra trên một đường truyền, các gói tin của các thông điệp khác trên kênh ảo khác có thể chia sẻ sử dụng đường truyền này.

Ưu, nhược điểm của phương pháp kênh ảo: Mạng có thể cung cấp các dịch vụ kênh ảo, bao gồm việc điều khiển lỗi và thứ tự các gói tin. Tất cả các gói tin đi trên cùng một tuyến sẽ đến theo thứ tự ban đầu. Điều khiển lỗi đảm bảo không chỉ các gói đến đích theo đúng thứ tự mà cho tất cả các gói không bị lỗi. Một ưu điểm khác là các gói tin lưu chuyển trên mạng sẽ nhanh hơn vì không cần phải định tuyến tại các node. Tuy nhiên sẽ khó khăn hơn việc thích ứng với nghẽn. Nếu có node bị hỏng thì tất cả các kênh ảo qua node đó sẽ bị mất, việc phân phát datagram càng khó khăn hơn, độ tin cậy không cao.

4.3. Các vấn đề về Định tuyến

a. Định tuyến (routing) là quá trình chọn lựa các đường đi trên một mạng máy tính để gửi dữ liệu qua đó. Việc định tuyến được thực hiện cho nhiều loại mạng, trong đó có mạng điện thoại, liên mạng, Internet, mạng giao thông.

Routing sẽ chỉ ra hướng, sự di chuyển của các gói (dữ liệu) được đánh địa chỉ từ mạng nguồn của chúng, hướng đến đích cuối thông qua các node trung gian; thiết bị phân cứng chuyên dùng được gọi là router (bộ định tuyến). Tiến trình định tuyến thường chỉ hướng đi dựa vào bảng định tuyến, đó là bảng chứa những lộ trình tốt nhất đến các đích khác nhau trên mạng. Vì vậy việc xây dựng bảng định tuyến, được tổ chức trong bộ nhớ của router, trở nên vô cùng quan trọng cho việc định tuyến hiệu quả.

Các mạng nhỏ có thể có các bảng định tuyến được cấu hình thủ công, còn những mạng lớn hơn có topo mạng phức tạp và thay đổi liên tục thì xây dựng thủ công các bảng định tuyến là vô cùng khó khăn. Tuy nhiên, hầu hết mạng điện thoại chung (public switched telephone network - PSTN) sử dụng bảng định tuyến được tính toán trước, với những tuyến dự trữ nếu các lộ trình trực tiếp đều bị nghẽn. Định tuyến động (dynamic routing) có gắng giải quyết vấn đề này bằng việc xây dựng bảng định tuyến một cách tự động, dựa vào những thông tin được giao thức định tuyến cung cấp, và cho phép mạng hành động gần như tự trị trong việc ngăn chặn mạng bị lỗi và nghẽn.

b. Các phương pháp định tuyến.

Định tuyến là quá trình mà Router thực hiện để chuyển gói dữ liệu tới mạng đích. Tất cả các Router đọc theo đường đi đều dựa vào địa chỉ IP đích của gói dữ liệu để chuyển gói theo đúng hướng đến đích cuối cùng. Để thực hiện được điều này, Router phải học thông tin về đường đi tới các mạng khác. Nếu Router chạy định tuyến động thì Router tự động học những thông tin này từ các Router khác. Còn nếu Router chạy định tuyến tĩnh thì người quản trị mạng phải cấu hình các thông tin đến các mạng khác cho Router.

Định tuyến tĩnh.

Đối với định tuyến tĩnh, các thông tin về đường đi phải do người quản trị mạng nhập cho Router. Khi cấu trúc mạng có bất kỳ thay đổi nào thì chính người quản trị mạng phải xóa hoặc thêm các thông tin về đường đi cho Router. Những loại đường đi như vậy gọi là đường cố định. Đối với hệ thống mạng lớn thì công việc bảo trì bảng định tuyến cho Router như trên tốn rất nhiều thời gian. Còn đối với hệ thống mạng nhỏ, ít có thay đổi thì công việc này đỡ mất công hơn. Chính vì định tuyến tĩnh đòi hỏi người quản trị mạng phải cấu hình mọi thông tin về đường đi cho Router nên nó không có được tính linh hoạt như định tuyến động. Trong những hệ thống mạng lớn, định tuyến tĩnh thường được sử dụng kết hợp với giao thức định tuyến động cho một số mục đích đặc biệt.

Ưu điểm của định tuyến tĩnh.

Ưu điểm lớn nhất của định tuyến tĩnh là sự thay đổi chậm, điều đó có nghĩa là tính chịu đàm hồi của mạng sẽ tốt hơn. Điều đó dẫn tới việc dự đoán hiệu năng mạng và sửa lỗi nhanh hơn. Các hệ thống sử dụng định tuyến tĩnh thường là các hệ thống kết cuối, việc chuyển thông tin vào mạng có thể chỉ có một tuyến đường duy nhất và thường được gọi là hướng ngầm định, các Router không cần trao đổi các thông tin tìm đường cũng như cơ sở dữ liệu định tuyến. Vì vậy, định tuyến tĩnh có một số ứng dụng hữu ích.

Định tuyến động có khuynh hướng truyền đạt tất cả thông tin về một liên mạng. Tuy nhiên, trong một số trường hợp, vì lý do an toàn chúng ta có thể muốn che dấu một số phần của liên mạng. Định tuyến tĩnh cho phép chúng ta che dấu thông tin không muốn tiết lộ.

Nhược điểm của định tuyến tĩnh.

- Quyết định định tuyến tĩnh không dựa trên sự đánh giá lưu lượng và Topo mạng hiện thời.
- Trong môi trường IP các Router không thể phát hiện ra các Router mới, chúng chỉ định tuyến gói tin tới các Router được chỉ định của nhà quản lý mạng.
- Trong định tuyến tĩnh, các tuyến được thiết lập thủ công, mỗi khi mạng có sự cố hoặc cấu hình mạng thay đổi thì người quản trị mạng phải thiết lập lại tuyến mới

Định tuyến động.

Định tuyến động có cơ chế hoạt động ngược lại so với định tuyến tĩnh. Sau khi người quản trị nhập các lệnh cấu hình để khởi tạo định tuyến động, thông tin về tuyến sẽ được cập nhật tự động mỗi khi nhận được một thông tin mới từ lớp mạng. Các thay đổi về Topo mạng được trao đổi giữa các Router.

Ưu điểm của định tuyến động

Định tuyến động lựa chọn tuyến dựa trên thông tin trạng thái hiện thời của mạng. Thông tin trạng thái có thể đo hoặc dự đoán và tuyến đường có thể thay đổi khi Topo mạng hoặc lưu lượng mạng thay đổi. Thông tin định tuyến cập nhật vào trong các bảng định tuyến của các node mạng trực tuyến, đáp ứng tình thời gian thực nhằm tránh tắc nghẽn cũng như tối ưu hiệu năng mạng.

Ưu điểm lớn nhất của định tuyến động là nó có thể thiết lập tuyến đường tới tất cả các thiết bị trong mạng, tự động thay đổi tuyến đường khi cấu hình mạng thay đổi. Nó rất thích hợp cho:

- Thêm thiết bị và địa chỉ mới vào mạng.
- Loại bỏ thiết bị và địa chỉ khỏi mạng.

Các giao thức định tuyến động cũng có thể chuyển lưu lượng từ cùng một phiên làm việc qua nhiều đường đi khác nhau trong mạng để có hiệu suất cao hơn. Tính chất này được gọi là chia tải (load sharing).

Nhược điểm của định tuyến động.

Trong mạng phức hợp sử dụng định tuyến động, một mạng có thể bị tái tạo lại cấu hình một cách liên tục vì sự khác nhau về thiết bị và chính sách của rất nhiều nhà khai thác cùng hoạt động. Điều đó có thể gây nên những tổn thất trên mạng về sử dụng tài nguyên hay nói cách khác việc sử dụng định tuyến động cũng sẽ tạo ra độ phức tạp cao.

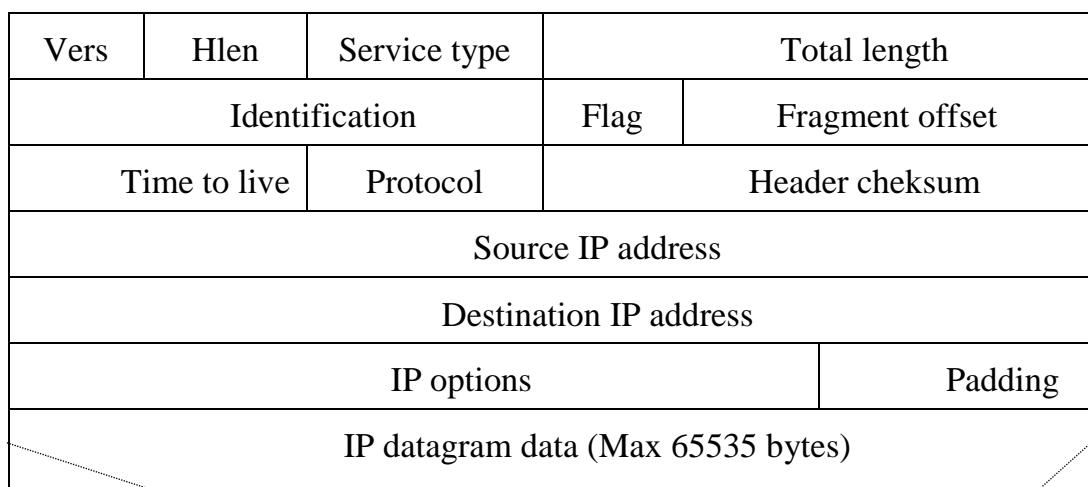
4.4. Giao thức Internet: Chuyển tiếp và đánh địa chỉ trên Internet

4.4.1. Giao thức mạng IP (Internet Protocol)

a. Các chức năng chính của IP: IP (Internet Protocol) là giao thức không liên kết. Chức năng chủ yếu của IP là cung cấp các dịch vụ Datagram và các khả năng kết nối các mạng con thành liên mạng để truyền dữ liệu với phương thức chuyển mạch gói IP Datagram, thực hiện tiến trình định địa chỉ và chọn đường. IP Header được thêm vào đầu các gói tin và được giao thức lớp thấp truyền theo dạng khung dữ liệu (Frame). IP định tuyến các gói tin thông qua liên mạng bằng cách sử dụng các bảng định tuyến động tham chiếu tại mỗi bước nhảy. Định tuyến được tiến hành bằng cách tham khảo thông tin thiết bị mạng vật lý và logic như ARP giao thức phân giải địa chỉ. IP thực hiện việc tháo rời và khôi phục các gói tin theo yêu cầu kích thước được định nghĩa cho các lớp vật lý và liên kết dữ liệu thực hiện. IP kiểm tra lỗi thông tin điều khiển, phần đầu IP bằng giá trị tổng CheckSum.

0

31



Destination Address	Source Address	Type field	IP data	CRC
---------------------	----------------	------------	---------	-----

Hình 4. 2 Cấu trúc gói tin IP

- VER (4 bits): Version hiện hành của IP được cài đặt.
- IHL (4 bits): Internet Header Length của Datagram, tính theo đơn vị word (32 bits).
- Type of service (8 bits): Thông tin về loại dịch vụ và mức ưu tiên của gói IP:
- Total Length (16 bits): Chỉ độ dài Datagram
- Identification (16bits): Định danh cho một Datagram trong thời gian sống của nó.
- Flags (3 bits): Liên quan đến sự phân đoạn (Fragment) các Datagram:
- Fragment Offset (13 bits): Chỉ vị trí của Fragment trong Datagram.
- Time To Live (TTL-8 bits): Thời gian sống của một gói dữ liệu.
- Protocol (8 bits): Chỉ giao thức sử dụng TCP hay UDP.
- Header Checksum (16 bits): Mã kiểm soát lỗi CRC (Cycle Redundancy Check).
- Source Address (32 bits): địa chỉ của trạm nguồn.
- Destination Address (32 bits): Địa chỉ của trạm đích.
- Option (có độ dài thay đổi): Sử dụng trong trường hợp bảo mật, định tuyến đặc biệt.
- Padding (độ dài thay đổi): Vùng đệm cho phần Header luôn kết thúc ở 32 bits
- Data (độ dài thay đổi): Độ dài dữ liệu tối đa là 65.535 bytes, tối thiểu là 8 bytes.

b. Phân mảnh và hợp nhất các gói IP:

Các gói IP được nhúng trong khung dữ liệu ở lớp liên kết dữ liệu tương ứng trước khi chuyển tiếp trong mạng. Một gói dữ liệu IP có độ dài tối đa 65.536 byte, trong khi hầu hết các lớp liên kết dữ liệu chỉ hỗ trợ các khung dữ liệu nhỏ hơn độ lớn tối đa của gói dữ liệu IP nhiều lần (ví dụ độ dài lớn nhất của một khung dữ liệu Ethernet là 1500 byte). Vì vậy cần thiết phải có cơ chế phân mảnh khi phát và hợp nhất khi nhận đối với các gói dữ liệu IP.

Độ dài tối đa của một gói liên kết dữ liệu là MTU (Maximum Transmit Unit). Khi cần chuyển một gói dữ liệu IP có độ dài lớn hơn MTU của một mạng cụ thể, cần phải chia gói số liệu IP đó thành những gói IP nhỏ hơn để độ dài của nó nhỏ hơn hoặc bằng MTU gọi là mảnh (Fragment). Trong phần tiêu đề của gói dữ liệu IP có thông tin về phân mảnh và xác định các mảnh có quan hệ phụ thuộc để hợp thành sau này.

Quá trình hợp nhất diễn ra ngược lại với quá trình phân mảnh. Khi IP nhận được một gói phân mảnh, nó giữ phân mảnh đó trong vùng đệm, cho đến khi nhận được hết các gói IP trong chuỗi phân mảnh có cùng trường định danh. Khi phân mảnh đầu tiên được nhận, IP khởi động một bộ đếm thời gian (giá trị ngầm định là 15s). IP phải nhận hết các phân mảnh kế tiếp trước khi đồng hồ tắt. Nếu không IP phải huỷ tất cả các phân mảnh trong hàng đợi

hiện thời có cùng trường định danh. Khi IP nhận được hết các phân mảnh, nó thực hiện hợp nhất các gói phân mảnh thành các gói IP gốc và sau đó xử lý nó như một gói IP bình thường. IP thường chỉ thực hiện hợp nhất các gói tại hệ thống đích của gói.

c. Địa chỉ IP (Internet Protocol-IPv4).

Mỗi một trạm (Host) được gán một địa chỉ duy nhất gọi là địa chỉ IP. Mỗi địa chỉ IP có độ dài 32 bit được tách thành 4 vùng (mỗi vùng 1 byte), có thể được biểu diễn dưới dạng thập phân, bát phân, thập lục phân hoặc nhị phân. Cách viết phổ biến nhất là dưới dạng thập phân có dấu chấm để tách giữa các vùng.

Địa chỉ IP được chia thành 5 lớp ký hiệu là A, B, C, D, E với cấu trúc mỗi lớp được xác định. Các bit đầu tiên của byte đầu tiên được dùng để định danh lớp địa chỉ (0 - lớp A, 10 - lớp B, 110 - lớp C, 1110 - lớp D, 11110 - lớp E).

Cấu trúc chung địa chỉ các lớp:

Class bit	NetId	HostId
-----------	-------	--------

Trong đó:

- ✓ Class bit: Bit nhận định danh lớp địa chỉ
- ✓ NetId: Địa chỉ của mạng.
- ✓ HostId: Địa chỉ của máy.

- Lớp A cho phép định danh tối đa 126 mạng (byte đầu tiên), với tối đa 16 triệu Host (3 byte còn lại) cho mỗi mạng. Lớp này được dùng cho các mạng có số trạm cực lớn.

0	7	8	31
0	NetId		HostId

- Lớp B cho phép định danh tới 16384 mạng con, với tối đa 65535 Host trên mỗi mạng. Dạng địa chỉ của lớp B:

0	15	16	31
1	0	NetId	HostId

- Lớp C cho phép định danh tới 2.097.150 mạng và tối đa 254 Host cho mỗi mạng.

0	23	24	31
1	1	0	NetId

- Lớp D dùng để gửi IP Datagram tới một nhóm các Host trên một mạng. Tất cả các số lớn hơn 233 trong trường đầu là thuộc lớp D.

- Lớp E dự phòng để dùng trong tương lai.

Lớp	Bit định danh lớp	Số lượng mạng	Số lượng Host	Biểu diễn bằng số thập phân
-----	-------------------	---------------	---------------	-----------------------------

A	0	127	16.777.214	0.1.0.0- 126.255.255.255
B	10	16.383	65.534	128.1.0.0 - 191.255.255.255
C	110	2.097.151	254	192.1.0.0 - 223.255.255.255
D	1110			223.0.0.0 - 239.255.255.255
E	11110			240.0.0.0 - 247.255.255.255

Hình 4. 3 Cấu trúc các lớp địa chỉ IP

Các địa chỉ IP dành riêng:

- Net ID và classbit toàn bit 0: cho biết địa chỉ máy
- Net ID và classbit toàn bit 1: địa chỉ mặt nạ mạng con
- Host ID toàn là bit 0: địa chỉ mạng - được sử dụng để định danh cho chính mạng đó
- Host ID toàn bit 1: địa chỉ Broadcast - được sử dụng để quảng bá gói tin đến tất cả các thiết bị trên mạng
- 0.0.0.0: RIP protocol
- 127.x.x.x: Loopback address - gói tin trả ngược trở lại khi gửi ICMP - Một thông điệp được đánh địa chỉ loopback được gửi bởi phần mềm TCP/IP cục bộ đến chính nó. Địa chỉ loopback được dùng để kiểm tra xem phần mềm TCP/IP có hoạt động không. Địa chỉ loopback 127.0.0.1 thường được sử dụng nhất.
- InterNIC và IANA đã đưa ra một số dải địa chỉ IP - gọi là private address dùng để thiết lập cho các mạng cục bộ không kết nối với Internet. Đó là các địa chỉ:
 - 10.0.0.0 – 10.255.255.255
 - 172.16.0.0 – 172.31.255.255
 - 192.168.0.0 – 192.168.255.255
- IP có dạng 169.254.x.x thì nghĩa là DHCP Server đã bị ngắt không cấp phát IP.

Địa chỉ mạng con của Internet (IP subnetting).

Một mạng khi gia nhập Internet được Trung tâm thông tin mạng Internet (NIC) phân cho một số địa chỉ vừa đủ dùng với yêu cầu lúc đó, sau này nếu mạng phát triển thêm lại phải xin NIC thêm, đó là điều không thuận tiện cho các nhà khai thác mạng.

Hơn nữa các lớp địa chỉ của Internet không phải hoàn toàn phù hợp với yêu cầu thực tế, địa chỉ lớp B chẳng hạn, mỗi một địa chỉ mạng có thể cấp cho 65534 máy, Thực tế có mạng nhỏ chỉ có vài chục máy chủ thì sẽ lãng phí rất nhiều địa chỉ còn lại mà không ai dùng được. Để khắc phục vấn đề này và tận dụng tối đa địa chỉ được NIC phân, bắt đầu từ năm 1985 người ta nghĩ đến Địa chỉ mạng con.

Như vậy phân địa chỉ mạng con là mở rộng địa chỉ cho nhiều mạng trên cơ sở một địa chỉ mạng mà NIC phân cho, phù hợp với số lượng thực tế máy có trên từng mạng.

Phương pháp phân địa chỉ mạng con.

Trước khi nghiên cứu phần này chúng ta cần phải hiểu qua một số khái niệm liên quan tới việc phân địa chỉ các mạng con.

Default Mask: (Giá trị mặt nạ mặc định nhận địa chỉ mạng) được định nghĩa trước cho từng lớp địa chỉ A, B, C. Thực chất là giá trị thập phân cao nhất (khi tất cả 8 bit đều bằng 1) trong các Octet dành cho địa chỉ mạng - NetId.

Default Mask (không sử dụng làm subnet):

Lớp A 255.0.0.0

Lớp B 255.255.0.0

Lớp C 255.255.255.0

Subnet Mask: (giá trị mặt nạ của từng mạng con)

Subnet Mask là kết hợp của Default Mask với giá trị thập phân cao nhất của các bit lấy từ các Octet của địa chỉ máy chủ sang phần địa chỉ mạng để tạo địa chỉ mạng con.

Subnet Mask bao giờ cũng đi kèm với địa chỉ mạng tiêu chuẩn để cho người đọc biết địa chỉ mạng tiêu chuẩn này dùng cả cho 254 máy hay chia ra thành các mạng con. Mặt khác nó còn giúp Router trong việc định tuyến cuộc gọi.

Nguyên tắc chung:

Lấy bớt một số bit của phần địa chỉ máy để tạo địa chỉ mạng con.

Lấy đi bao nhiêu bit phụ thuộc vào số mạng con cần thiết (Subnet mask) mà nhà khai thác mạng quyết định sẽ tạo ra.

Tính toán số lượng các subnet, host:

- Số lượng subnet trong network: $2^{\text{số bit subnet}} - 2$

- Số lượng host trong 1 subnet: $2^{\text{số bit host}} - 2$

* Tính toán Network number (số mạng).

- Sử dụng hàm AND giữa địa chỉ IP và Subnetmask ta sẽ được địa chỉ mạng.

- Địa chỉ Host đầu tiên trong một Subnet có thể sử dụng bằng địa chỉ Subnet cộng 1.

- Địa chỉ Broadcast bằng địa chỉ Subnet kế tiếp trừ 1.

- Địa chỉ cuối trong Subnet có thể sử dụng bằng địa chỉ Broadcast trừ 1.

Ví dụ 1: Cho địa chỉ lớp C: 202.168.15.0 Hãy chia mạng trên thành các mạng con sao cho mỗi mạng con có 30 Host.

Bài làm

- Subnet mặc định của lớp C là 255.255.255.0. số bit sử dụng cho host là 8 bit.

- Mỗi mạng con có 30 host, do vậy phải sử dụng 5 bit cho các host (vì số host = $2^5 - 2 = 30$).

- Số bit còn lại dùng để chia mạng con là $8-5=3$ bit.

- Số subnet (mạng con) được chia là: $2^3 - 2 = 6$ subnet.

Do đó Subnet mask mặc định sẽ là: 255.255.255.224

Ta có bảng địa chỉ như sau:

Số thứ tự Subnet	Địa chỉ Subnet	Địa chỉ Broadcast	Khoảng địa chỉ các Host trong từng Subnet
1	202.168.15.32	202.168.15.63	202.168.15.33 - 202.168.15.62
2	202.168.15.64	202.168.15.95	202.168.15.65 - 202.168.15.94
3	202.168.15.96	202.168.15.127	202.168.15.97 - 202.168.15.126
4	202.168.15.128	202.168.15.159	202.168.15.129 - 202.168.15.158
5	202.168.15.160	202.168.15.191	202.168.15.161 - 202.168.15.190
6	202.168.15.192	202.168.15.223	202.168.15.193 - 202.168.15.222

4.4.2. Giao thức thông báo điều khiển mạng ICMP

Giao thức IP không có cơ chế kiểm soát lỗi và kiểm soát luồng dữ liệu. Các nút mạng cần biết tình trạng các nút khác, các gói dữ liệu phát đi có tới đích hay không...

Các chức năng chính: ICMP (Internet Control Message Protocol) là giao thức điều khiển của lớp IP, sử dụng để trao đổi các thông tin điều khiển dòng dữ liệu, thông báo lỗi và các thông tin trạng thái khác của bộ giao thức TCP/IP.

- Điều khiển lưu lượng (Flow Control): Khi các gói dữ liệu đến quá nhanh, thiết bị đích hoặc thiết bị định tuyến ở giữa sẽ gửi một thông điệp ICMP trả lại thiết bị gửi, yêu cầu thiết bị gửi tạm thời ngừng việc gửi dữ liệu.

- Thông báo lỗi: Trong trường hợp không tới được địa chỉ đích thì hệ thống sẽ gửi một thông báo lỗi "Destination Unreachable".

- Định hướng lại các tuyến (Redirect Router): Một Router gửi một thông điệp ICMP cho một trạm thông báo nên sử dụng Router khác. Thông điệp này có thể chỉ được dùng khi trạm nguồn ở trên cùng một mạng với hai thiết bị định tuyến.

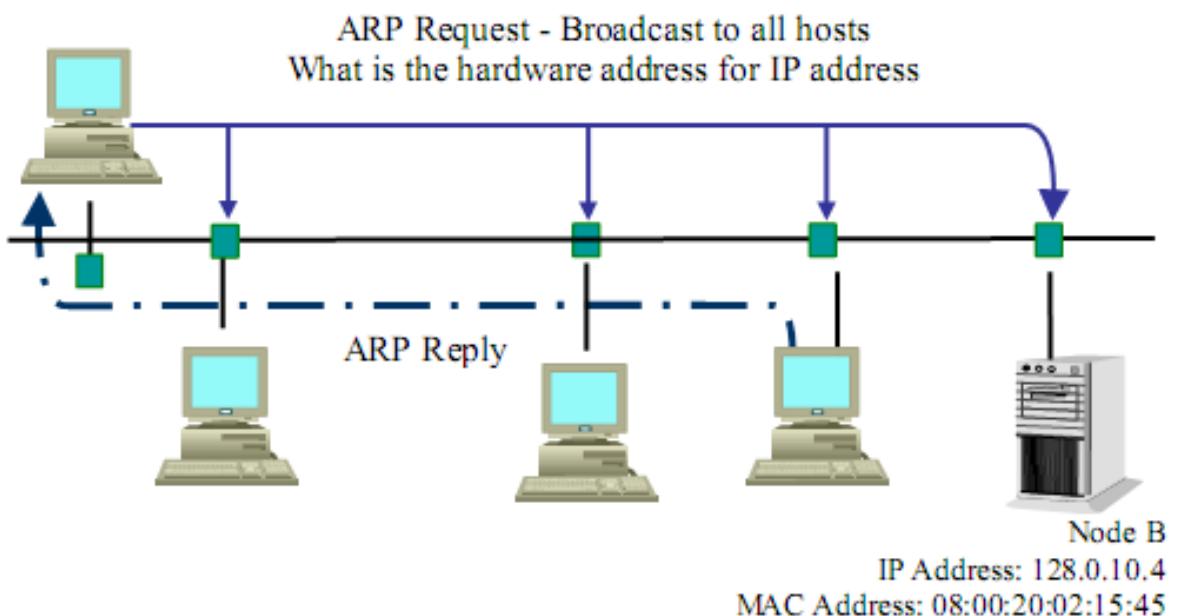
- Kiểm tra các trạm ở xa: Một trạm có thể gửi một thông điệp ICMP "Echo" để kiểm tra trạm có hoạt động hay không.

4.4.3. Giao thức phân giải địa chỉ ARP

Giao thức TCP/IP sử dụng ARP (Address Resolution Protocol) để tìm địa chỉ vật lý của trạm đích. Ví dụ khi cần gửi một gói dữ liệu IP cho một hệ thống khác trên cùng một mạng vật lý Ethernet, hệ thống gửi cần biết địa chỉ Ethernet của hệ thống đích để lớp liên

kết dữ liệu xây dựng khung gói dữ liệu. Thông thường, mỗi hệ thống lưu giữ và cập nhật bảng thích ứng địa chỉ IP-MAC tại chỗ (còn được gọi là bảng ARP Cache). Bảng thích ứng địa chỉ được cập nhật bởi người quản trị hệ thống hoặc tự động bởi giao thức ARP sau mỗi lần ánh xạ được một địa chỉ tương ứng mới.

Trước khi trao đổi thông tin với nhau, node nguồn cần phải xác định địa chỉ vật lý MAC của node đích bằng cách tìm kiếm trong bảng địa chỉ IP. Nếu không tìm thấy, node nguồn gửi quảng bá(Broadcast) một gói yêu cầu ARP(ARP Request) có chứa địa chỉ IP nguồn, địa chỉ IP đích cho tất cả các máy trên mạng. Các máy nhận, đọc, phân tích và so sánh địa chỉ IP của nó với địa chỉ IP của gói. Nếu cùng địa chỉ IP, nghĩa là node đích tìm trong bảng thích ứng địa chỉ IP- MAC của nó và trả lời bằng một gói ARP Rely có chứa địa chỉ MAC cho node nguồn. Nếu không cùng địa chỉ IP, nó chuyển tiếp gói yêu cầu nhận được dưới dạng quảng bá cho tất cả các trạm trên mạng.



Hình 4. 4 Minh họa quá trình tìm địa chỉ MAC bằng ARP

Tóm lại, tiến trình của ARP được mô tả như sau:

- IP yêu cầu địa chỉ MAC.
- Tìm kiếm trong bảng ARP.
- Nếu tìm thấy sẽ trả lại địa chỉ MAC.
- Nếu không tìm thấy, tạo gói ARP yêu cầu và gửi tới tất cả các trạm.
- Tuỳ theo gói tin trả lời, ARP cập nhật vào bảng ARP và gửi địa chỉ MAC cho IP.

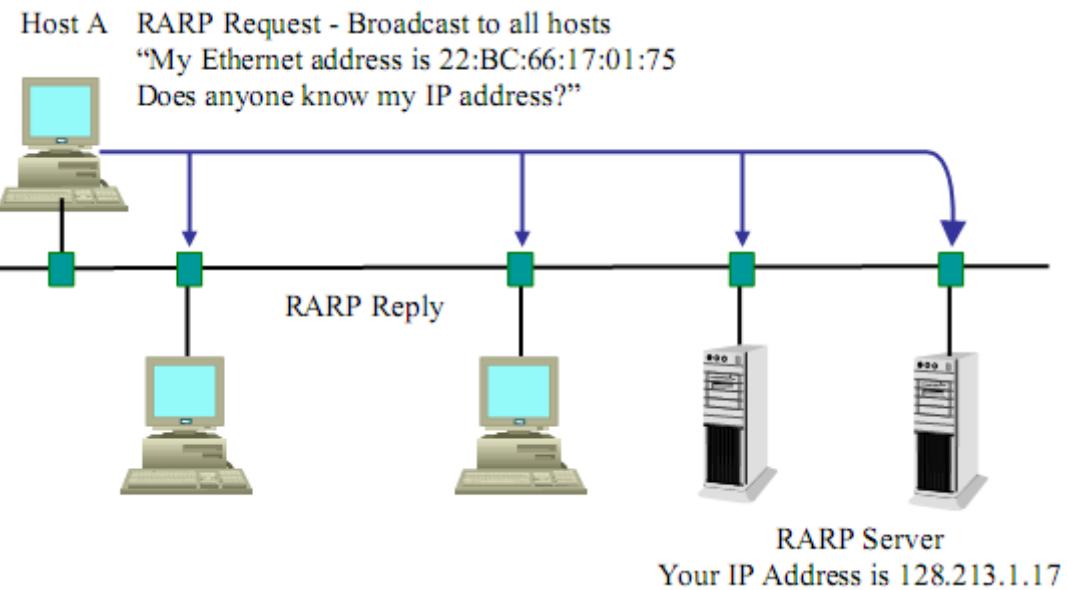
4.4.4. Giao thức phân giải địa chỉ ngược RARP

RARP (Reverse Address Resolution Protocol) là giao thức phân giải địa chỉ ngược. Quá trình này ngược lại với quá trình ARP ở trên, nghĩa là cho trước địa chỉ mức liên kết, tìm địa chỉ IP tương ứng. Như vậy RARP được sử dụng để phát hiện địa chỉ IP, khi

biết địa chỉ vật lý MAC. Và cũng được sử dụng trong trường hợp trạm làm việc không có đĩa.

Khuôn dạng gói tin RARP tương tự như khuôn dạng gói ARP đã trình bày, chỉ khác là trường Opcode có giá trị 0x0003 cho mã lệnh yêu cầu (RARP Request) và có giá trị 0x0004 cho mã lệnh trả lời (RARP Reply).

Nguyên tắc hoạt động của RARP ngược với ARP, nghĩa là máy đã biết trước địa chỉ vật lý MAC tìm địa chỉ IP tương ứng của nó. Hình 3.12 minh họa hoạt động của giao thức RARP. Máy A cần biết địa IP của nó, nó gửi gói tin RARP Request chứa địa chỉ MAC cho tất cả các máy trong mạng LAN. Mọi máy trong mạng đều có thể nhận gói



tin này nhưng chỉ có Server mới trả lại RARP Reply chứa địa chỉ IP của nó.

Hình 4. 5 Minh họa quá trình tìm địa chỉ IP bằng giao thức RARP

4.4.5. Giao thức IPv6 (Internet Protocol Version 6)

Giao thức IPng (Next General Internet Protocol) là phiên bản mới của giao thức IP được IETF (Internet Engineering Task Force) đề xướng và năm 1994, IESG (Internet Engineering SteeringGroup) phê chuẩn với tên chính thức là IPv6. IPv6 là phiên bản kế thừa phát triển từ IPv4.

4.4.5.1. Nguyên nhân ra đời của IPv6

- Internet phát triển mạnh, nhu cầu sử dụng địa chỉ IP tăng dần đến không gian địa chỉ ngày càng bị thu hẹp và tình trạng thiếu hụt địa chỉ tắt yếu sẽ xảy ra trong vài năm tới.
- Việc phát triển quá nhanh của mạng Internet dẫn đến kích thước các bảng định tuyến trên mạng ngày càng lớn.
- Cài đặt IPv4 bằng thủ công hoặc bằng giao thức cấu hình địa chỉ trạng thái DHCP (Dynamic Host Configuration Protocol), khi mà nhiều máy tính và các thiết bị kết

nối vào mạng thì cần thiết phải có một phương thức cấu hình địa chỉ tự động và đơn giản hơn.

- Trong quá trình hoạt động IPv4 đã phát sinh một số vấn đề về bảo mật và QoS. Khi kết nối thành mạng Intranet cần nhiều địa chỉ khác nhau và truyền thông qua môi trường công cộng. Vì vậy đòi hỏi phải có các dịch vụ bảo mật để bảo vệ dữ liệu ở mức IP.

- Mặc dù có các chuẩn đảm bảo chất lượng dịch vụ QoS trong IPv4 trường IPv4 TOS (Type of Service), nhưng hạn chế về mặt chức năng, cần thiết hỗ trợ tốt hơn cho các ứng dụng thời gian thực.

Vì vậy việc cần thiết phải thay thế giao thức IPv4 là tất yếu. Thiết kế IPv6 nhằm mục đích tối thiểu hóa ảnh hưởng qua lại giữa các giao thức lớp trên và lớp dưới bằng cách tránh việc bổ sung một cách ngẫu nhiên các chức năng mới.

4.4.5.2. Các đặc trưng của IPv6

IPv6 được chọn thay thế cho giao thức IPv4 không chỉ do IPv4 không còn phù hợp với yêu cầu phát triển hiện tại của mạng Internet mà còn vì những ưu điểm của giao thức IPv6:

- Đơn giản hóa Header: Một số trường trong Header của IPv4 bị bỏ hoặc chuyển thành các trường tùy chọn. Giảm thời gian xử lý và tăng thời gian truyền.

- Không gian địa chỉ lớn: Độ dài địa chỉ IPv6 là 128 bit, gấp 4 lần độ dài địa chỉ IPv4. Không gian địa chỉ IPv6 không bị thiếu hụt trong tương lai.

- Khả năng địa chỉ hóa và chọn đường linh hoạt: IPv6 cho phép nhiều lớp địa chỉ với số lượng các node. Cho phép các mạng đa mức và phân chia địa chỉ thành các mạng con riêng lẻ. Có khả năng tự động trong việc đánh địa chỉ. Mở rộng khả năng chọn đường bằng cách thêm trường “Scop” vào địa chỉ quảng bá (Multicast).

- Tự động cấu hình địa chỉ: Khả năng tự cấu hình của IPv6 được gọi là khả năng cắm và chạy (Plug and Play). Tính năng này cho phép tự cấu hình địa chỉ cho giao diện mà không cần sử dụng các giao thức DHCP.

- Khả năng bảo mật: IPsec bảo vệ và xác nhận các gói tin IP:

+ Mã hóa dữ liệu: Phía gửi sẽ tiến hành mã hóa gói tin trước khi gửi.

+ Toàn vẹn dữ liệu: Phía nhận có thể xác nhận gói tin nhận được để đảm bảo rằng dữ liệu không bị thay đổi trong quá trình truyền.

+ Xác nhận nguồn gốc dữ liệu: Phía nhận có thể biết được phía gửi gói tin. Dịch vụ này phụ thuộc vào dịch vụ toàn vẹn dữ liệu.

+ Antireplay: Phía nhận có thể phát hiện và từ chối gói tin gửi lại.

- Chất lượng dịch vụ QoS (Quanlity of Service): Chất lượng dịch vụ QoS trong IPv4 không cao. Trong Header IPv4 chứa địa chỉ nguồn và địa chỉ đích, truyền có độ tin cậy không cao. IPv6 Header có thêm một số trường mới để xử lý và xác định lưu lượng trên

mạng. Do cơ chế xác nhận gói tin ngay trong Header nên việc hỗ trợ QoS có thể thực hiện được ngay cả khi gói tin được mã hóa qua IPsec.

- Giao thức phát hiện lân cận NDP (Neighbor Discovery Protocol) của IPv6 là một dãy các thông báo ICMPv6 cho phép quản lý tương tác giữa các node lân cận, thay thế ARP trong IPv4. Các thông báo ICMPv4 Router Discovery và ICMPv4 Redirect được thay bởi các thông báo Multicast, Unicast Neighbor Discovery.

- Khả năng mở rộng: Thêm vào trường Header mở rộng tiếp ngay sau Header, IPv6 có thể được mở rộng thêm các tính năng mới một cách dễ dàng.

- Tính di động: IPv4 không hỗ trợ cho tính di động, IPv6 cho phép nhiều thiết bị di động kết nối vào Internet theo chuẩn của PCMCIA (Personal Computer Memory Card International Association) qua mạng công cộng nhờ sóng vô tuyến.

4.4.5.3. So sánh đặc điểm Ipv4 và Ipv6

IPv4	IPv6
Độ dài địa chỉ là 32 bit (4 byte)	Độ dài địa chỉ là 128 bit (16 byte)
IPsec chỉ là tùy chọn	IPsec được gắn liền với IPv6.
Header của địa chỉ IPv4 không có trường xác định luồng dữ liệu của gói tin cho các Router để xử lý QoS.	Trường Flow Label cho phép xác định luồng gói tin để các Router có thể đảm bảo chất lượng dịch vụ QoS
Việc phân đoạn được thực hiện bởi cả Router và máy chủ gửi gói tin	Việc phân đoạn chỉ được thực hiện bởi máy chủ phía gửi mà không có sự tham gia của Router
Header có chứa trường Checksum	Không có trường Checksum trong IPv6 Header
Header có chứa nhiều tùy chọn	Tất cả các tùy chọn có trong Header mở rộng
Giao thức ARP sử dụng ARP Request quảng bá để xác định địa chỉ vật lý.	Khung ARP Request được thay thế bởi các thông báo Multicast Neighbor Solicitation.
Sử dụng giao thức IGMP để quản lý thành viên các nhóm mạng con cục bộ	Giao thức IGMP được thay thế bởi các thông báo MLD (Multicast Listener Discovery)
Sử dụng ICMP Router Discovery để xác định địa chỉ cổng Gateway mặc định phù hợp nhất, là tùy chọn.	Sử dụng thông báo quảng cáo Router (Router Advertisement) và ICMP Router Solicitation thay cho

	ICMP Router Discovery, là bắt buộc
Địa chỉ quảng bá truyền thông tin đến tất cả các node trong một mạng con	Trong IPv6 không tồn tại địa chỉ quảng bá, thay vào đó là địa chỉ Multicast
Thiết lập cấu hình bằng thủ công hoặc sử dụng DHCP	Cho phép cấu hình tự động, không sử dụng nhân công hay cấu hình qua DHCP
Địa chỉ máy chủ được lưu trong DNS với mục đích ánh xạ sang địa chỉ IPv4	Địa chỉ máy chủ được lưu trong DNS với mục đích ánh xạ sang địa chỉ IPv6
Con trỏ địa chỉ được lưu trong IN – ADDR ARPA DNS để ánh xạ địa chỉ IPv4 sang tên máy chủ	Con trỏ địa chỉ được lưu trong Ipv6 – INT DNS để ánh xạ địa chỉ từ IPv4 sang tên máy chủ
Hỗ trợ gói tin kích thước 576 bytes (có thể phân đoạn)	Hỗ trợ gói tin kích thước 1280 bytes (không cần phân đoạn)

4.4.5.4. Phương pháp biểu diễn địa chỉ IPv6

Địa chỉ IPv6 được biểu diễn bằng chuỗi số Hexa, được chia thành các nhóm 16 bit tương ứng với bốn chữ số Hexa, ngăn cách nhau bởi dấu “:”

Ví dụ: 4021: 0000: 240E: 0000: 0000: 0AC0: 3428: 121C.

Trong cách biểu diễn địa chỉ Ipv6 có thể thu gọn bằng cách thay các nhóm 0 liên tiếp bằng kí hiệu “::” nhiều nhất 1 lần.

Ví dụ 12AB: 0000: 0000: CD30: 0000: 0000: 0000 /60 có thể viết là
12AB : 0 : 0 : CD30 : 0 : 0 : 0 : 0 /60 hoặc 12AB :: CD30 : 0 : 0 : 0 : 0 /60 hoặc
12AB : 0 : 0 : CD30 :: /60 . Không được viết 12AB :: CD30 /60 hay 12AB :: CD30 :: /60.

4.4.5.5. Phân loại địa chỉ IPv6

Trong IPv6, được chia làm 3 loại địa chỉ khác nhau:

- *Địa chỉ Unicast*: Là địa chỉ của một giao diện. Một gói tin được chuyển đến địa chỉ Unicast sẽ chỉ được định tuyến đến giao diện gắn với địa chỉ đó

- *Địa chỉ Anycast*: Là địa chỉ của một tập giao diện thuộc của nhiều node khác nhau. Mỗi gói tin tới địa chỉ Anycast được chuyển tới chỉ một trong tập giao diện gắn với địa chỉ đó (là giao diện gần node gửi nhất và có Metrics nhỏ nhất).

- *Địa chỉ Multicast*: Địa chỉ của tập các giao diện thuộc về nhiều node khác nhau. Một gói tin gửi tới địa chỉ Multicast sẽ được gửi tất cả các giao diện trong nhóm.

4.4.5.6. So sánh cách đánh địa chỉ IPv4 và địa chỉ IPv6

Địa chỉ IPv6 và IPv4 có một số điểm chung như cùng sử dụng một số loại địa chỉ với một số chức năng tương tự, nhưng trong IPv6 có một số thay đổi thể hiện trong bảng sau:

IPv4 Address	IPv6 Address
Phân lớp địa chỉ (Lớp A, B, C và D)	Không phân lớp địa chỉ. Cấp phát theo tiền tố
Lớp D là Multicast (224.0.0.0/4)	Địa chỉ multicast có tiền tố FF00::/8
Sử dụng địa chỉ Broadcast	Không có Broadcast, thay bằng Anycast
Địa chỉ unspecified là 0.0.0.0	Địa chỉ Unspecified là ::
Địa chỉ Loopback 127.0.0.1	Địa chỉ Loopback là ::1
Sử dụng địa chỉ Public	Tương ứng là địa chỉ Unicast toàn cầu
Địa chỉ IP riêng (10.0.0.0/8, 172.16.0.0/12, và 192.168.0.0/16)	Địa chỉ Site-Local (FEC0::/48)
Địa chỉ tự cấu hình (169.254.0.0/16)	Địa chỉ Link-Local (FE80::/64)
Dạng biểu diễn: chuỗi số thập phân cách nhau bởi dấu chấm	Dạng biểu diễn: chuỗi số Hexa cách nhau bởi dấu hai chấm; có thể nhóm chuỗi số 0 liền nhau vào một kí tự
Sử dụng mặt nạ mạng con	Chỉ sử dụng kí hiệu tiền tố để chỉ mạng
Phân giải tên miền DNS: bản ghi tài nguyên địa chỉ máy chủ IPv4 (A)	Phân giải tên miền DNS: bản ghi tài nguyên địa chỉ máy chủ IPv6 (AAAA)
Tên miền ngược: IN-ADDR.ARPA	Tên miền ngược: IP6.INT domain

4.5. Các thuật toán định tuyến

4.5.1. Link state (định tuyến theo trạng thái đường liên kết)

Định tuyến theo trạng thái đường liên kết là chọn đường ngắn nhất dựa trên cấu trúc của toàn bộ hệ thống mạng.

Thuật toán này là thuật toán Dijkstras hay còn được gọi là thuật toán SPF (Shortest Path First – tìm đường ngắn nhất). Thuật toán định tuyến theo trạng thái đường liên kết thực hiện việc xây dựng và bảo trì một cơ sở dữ liệu đầy đủ về cấu trúc của toàn bộ hệ thống mạng.

Định tuyến theo trạng thái đường liên kết sử dụng các công cụ sau:

- Thông điệp thông báo trạng thái đường liên kết: (LSA – Link State Advertisement): LSA là một gói dữ liệu nhỏ mạng thông tin định tuyến được truyền đi giữa các Router.
- Cơ sở dữ liệu về cấu trúc mạng: được xây dựng từ thông tin thu thập được từ các LSA

- Thuật toán SPF: dựa trên cơ sở dữ liệu về cấu trúc mạng, thuật toán SPF sẽ tính toán để tìm đường ngắn nhất.
- Bảng định tuyến: chứa danh sách các đường đi đã được chọn lựa.

Quá trình thu thập thông tin mạng để thực hiện định tuyến theo trạng thái đường liên kết:

Mỗi Router bắt đầu trao đổi LSA với tất cả các Router khác, trong đó LSA mang thông tin về các mạng kết nối trực tiếp của từng Router. Từ đó, các Router xây dựng cơ sở dữ liệu dựa trên thông tin của các LSA.

Mỗi Router tiến hành xây dựng lại cấu trúc mạng theo dạng hình cây với bản thân nó là gốc, từ đó Router vẽ ra tất cả các đường đi tới tất cả các mạng trong hệ thống. Sau đó thuật toán SPF chọn đường ngắn nhất để đưa vào bảng định tuyến. Trên bảng định tuyến sẽ chứa thông tin về các đường đi đã được chọn với công thức tương ứng. Bên cạnh đó, Router vẫn tiếp tục duy trì cơ sở dữ liệu về cấu trúc hệ thống mạng và trạng thái của các đường liên kết.

Router nào phát hiện cấu trúc mạng thay đổi đầu tiên sẽ phát thông tin cập nhật cho tất cả các Router khác. Router phát gói LSA, trong đó có thông tin về Router mới, các thay đổi về trạng thái đường liên kết. Gói LSA này được phát đi cho tất cả các Router khác.

Khi Router nhận được gói LSA thì nó sẽ cập nhật lại cơ sở dữ liệu của nó với thông tin mới vừa nhận được. Sau đó SPF sẽ tính lại để chọn đường lại và cập nhật lại cho bảng định tuyến.

Ưu điểm của giao thức:

- Tốc độ hội tụ nhanh
- Ít bị lặp vòng
- Có khả năng mở rộng
- Đảm bảo băng thông mạng

Nhược điểm của giao thức:

- Bộ xử lý trung tâm của Router phải tính toán nhiều.
- Độ dài đường lượng bộ nhớ lớn.
- Chiếm dụng băng thông đường truyền.

4.5.2. Distance vector (định tuyến theo vector khoảng cách)

Định tuyến theo vector khoảng cách là chọn đường theo hướng và khoảng cách tới đích.

Định tuyến theo vector khoảng cách thực hiện truyền bá sao của bảng định tuyến từ Router này sang Router khác theo định kỳ. Việc cập nhật định kỳ giữa các Router giúp trao đổi thông tin khi cấu trúc mạng thay đổi. Thuật toán định tuyến theo vector khoảng

cách còn được gọi là thuật toán Bellman – Ford. Mỗi Router nhận được bảng định tuyến của những Router láng giềng kết nối trực tiếp với nó.

Router thu thập thông tin về khoảng cách đến các mạng khác, từ đó nó xây dựng và bảo trì một cơ sở dữ liệu về thông tin định tuyến trong mạng. Tuy nhiên, hoạt động theo thuật toán vector khoảng cách như vậy thì Router sẽ không biết được chính xác cấu trúc của toàn bộ hệ thống mạng mà chỉ biết được các Router láng giềng kết nối trực tiếp với nó mà thôi.

Khi sử dụng định tuyến theo vector khoảng cách, bước đầu tiên là Router phải xác định các Router láng giềng với nó. Các mạng kết nối trực tiếp vào cổng giao tiếp của Router sẽ có khoảng cách là 0. Còn đường đi tới các mạng không kết nối trực tiếp vào Router thì Router sẽ chọn đường tốt nhất dựa trên các thông tin mà nó nhận được từ các Router láng giềng.

Bảng định tuyến được cập nhật theo chu kỳ hoặc khi cấu trúc mạng có sự thay đổi. Quá trình cập nhật này cũng diễn ra từng bước một từ Router này đến Router khác. Khi cập nhật, mỗi Router gửi đi toàn bộ bảng định tuyến của nó cho các Router láng giềng. Trong bảng định tuyến có thông tin về đường đi tới từng mạng đích: tổng chi phí cho đường đi, địa chỉ của Router kế tiếp.

Ưu điểm của định tuyến theo vector khoảng cách là tốn ít tài nguyên của hệ thống

Những hạn chế của định tuyến theo vector khoảng cách:

- Hội tụ chậm, do mỗi lần thay đổi cấu trúc mạng thì phải sửa đổi lại bảng định tuyến bằng việc truyền các bản tin lần lượt từ Router này sang Router khác, làm cho quá trình cập nhật diễn ra rất chậm. Dẫn đến dễ bị lặp vòng.
- Lưu lượng cập nhật lớn, việc phát các broadcast bản tin cập nhật định kỳ giữa các Router có thể dẫn đến hao phí băng thông mạng một cách không cần thiết.
- Các metric bị giới hạn.

4.6. Định tuyến trên Internet

4.6.1. OSPF

OSPF – Open Shortest Path First, là một giao thức định tuyến link – state điển hình. Đây là một giao thức được sử dụng rộng rãi trong các mạng doanh nghiệp có kích thước lớn. Trong chương trình CCNA, đây cũng là một chủ đề chính được đề cập nhiều. Do đó, nắm vững những nguyên tắc hoạt động của OSPF sẽ giúp các bạn đang theo học chương trình CCNA hoàn thành tốt kỳ thi lấy chứng chỉ quốc tế CCNA cũng như đáp ứng tốt nhu cầu công việc trong thực tế.

Một số đặc điểm chính của giao thức OSPF:

1. OSPF là một giao thức link – state điển hình. Mỗi router khi chạy giao thức sẽ gửi các trạng thái đường link của nó cho tất cả các router trong vùng (area). Sau một thời gian trao đổi, các router sẽ đồng nhất được bảng cơ sở dữ liệu trạng thái

đường link (Link State Database – LSDB) với nhau, mỗi router đều có được “bản đồ mạng” của cả vùng. Từ đó mỗi router sẽ chạy giải thuật Dijkstra tính toán ra một cây đường đi ngắn nhất (Shortest Path Tree) và dựa vào cây này để xây dựng nên bảng định tuyến.

2. OSPF có AD = 110.
3. Metric của OSPF còn gọi là cost, được tính theo bandwidth trên cổng chạy OSPF.
4. OSPF chạy trực tiếp trên nền IP, có protocol – id là 89.
5. OSPF là một giao thức chuẩn quốc tế, được định nghĩa trong RFC – 2328.

Ta cùng review hoạt động của OSPF thông qua các bước hoạt động như sau:

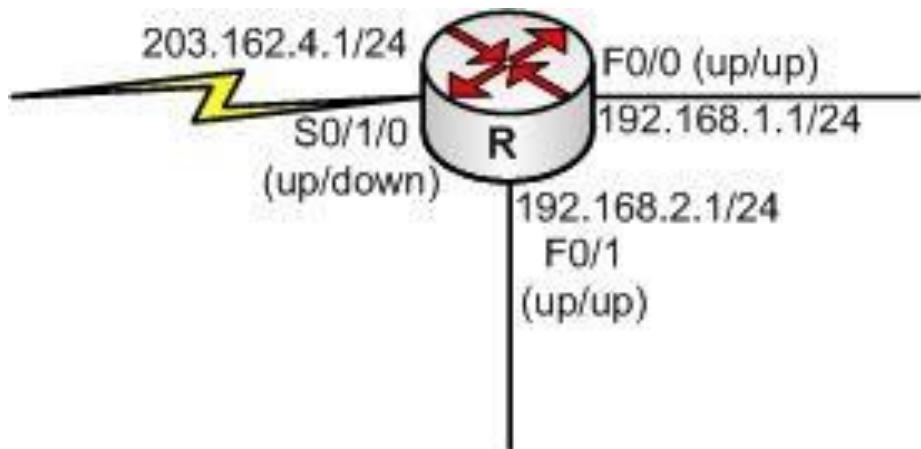
1. Bầu chọn Router – id.
2. Thiết lập quan hệ láng giềng (neighbor).
3. Trao đổi LSDB.
4. Tính toán xây dựng bảng định tuyến.

Router – id:

Đầu tiên, khi một router chạy OSPF, nó phải chỉ ra một giá trị dùng để định danh duy nhất cho nó trong cộng đồng các router chạy OSPF. Giá trị này được gọi là Router – id.

Router – id trên router chạy OSPF có định dạng của một địa chỉ IP. Mặc định, tiến trình OSPF trên mỗi router sẽ tự động bầu chọn giá trị router – id là địa chỉ IP cao nhất trong các interface đang active, ưu tiên cổng loopback.

Ta cùng làm rõ ý này thông qua ví dụ:

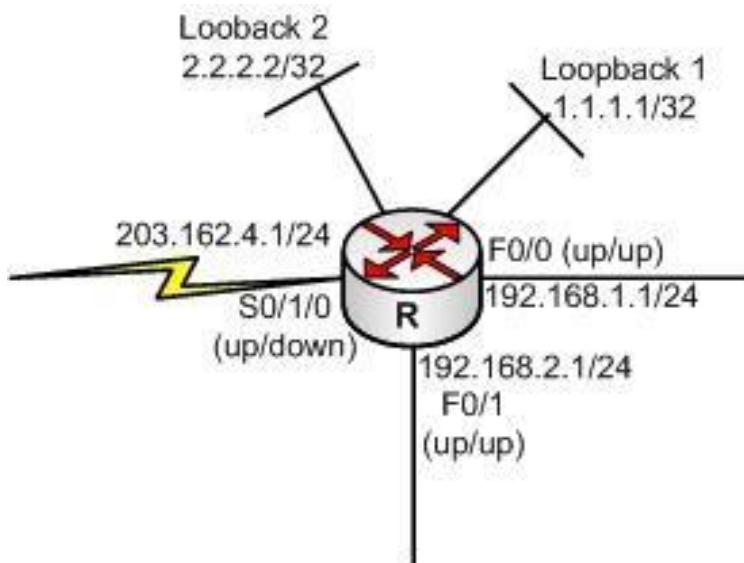


Hình 4. 6 Bầu chọn router – id

Khi cho router R tham gia OSPF (xem hình 1), router R phải bầu chọn ra một ‘nick name’ để định danh R khi R chạy OSPF. Vì ‘nick name’ này có định dạng của một địa chỉ IP nên R sẽ lấy một trong các địa chỉ IP trên nó để làm Router – id. Như đã nói ở trên, chỉ địa chỉ của các interface đang active, tức là ở trạng thái *up/up* (status *up*, line protocol *up*) mới được tham gia bầu chọn. Ta thấy trên hình 4.6, chỉ có hai cổng F0/0 và F0/1 của R là *up/up* nên router R sẽ chỉ xem xét hai địa chỉ trên hai cổng này là 192.168.1.1 và 192.168.2.1. Để xác định trong hai địa chỉ này, địa chỉ nào là cao hơn, R tiến hành so sánh hai địa chỉ này theo từng octet từ trái sang phải, địa chỉ nào có octet đầu tiên lớn hơn được xem là lớn hơn. Ta thấy, với cách so sánh này, địa chỉ 192.168.2.1 được xem là lớn hơn địa chỉ 192.168.1.1 nên nó sẽ được sử dụng để làm router – id. Vậy R sẽ tham gia OSPF với giá trị ‘nick name’ – router id là 192.168.2.1.

Ta cũng thấy trong 03 địa chỉ xuất hiện ở trên hình 1, địa chỉ 203.162.4.1 của cổng serial S0/1/0 trên router R là lớn nhất nhưng vì cổng này down nên không được tham gia bầu chọn.

Cũng ví dụ trên nhưng lần này trên router R có thêm các interface loopback:



Hình 4. 7 Bầu chọn router – id

Khi ta bật OSPF trên router R, R xúc tiến việc bầu chọn router – id. Vì lần này có các interface loopback nên R sẽ bỏ qua, không xem xét các địa chỉ của các interface vật lý. Hai địa chỉ của hai interface loopback 1 và 2 sẽ được so sánh để chọn ra router – id cho router R, và ta thấy rõ ràng $2.2.2.2 > 1.1.1.1$ nên router R sẽ chọn 2.2.2.2 làm router – id khi tham gia OSPF. Từ hình 4.7, ta thấy, 2.2.2.2 không phải là địa chỉ IP cao nhất nhưng vì tiến trình ưu tiên cổng loopback nên các địa chỉ trên các cổng loopback sẽ được xem xét trước. Điều này được giải thích là sẽ đem lại sự ổn định cho tiến trình OSPF vì interface loopback là loại interface luận lý không bao giờ down trừ khi người quản trị shutdown interface này.

Thực chất, việc up/down của các interface không ảnh hưởng nhiều lắm đến router – id của các router chạy OSPF. Thật vậy, giả sử trong ví dụ trên, router R đã chọn xong router – id là 192.168.2.1 là IP của cổng F0/1 (xét trường hợp chưa có các interface loopback) và tham gia vào OSPF với router – id 192.168.2.1. Lúc này, nếu ta có bổ sung thêm các interface loopback trên router thì router cũng sẽ không đổi lại router – id thành IP của các interface loopback. Hơn nữa, cho dù lúc này cổng F0/1 có down, thì router vẫn giữ giá trị router – id mà nó đã chọn. Có nghĩa là, router – id đơn thuần chỉ là một cái tên. Khi tên đã được chọn thì tiến trình OSPF sẽ làm việc với cái tên này và không thay đổi lại nữa. Cổng có IP được trích xuất làm tên của router lúc này có up/down cũng không ảnh hưởng gì cả. Vậy nếu chúng ta muốn đổi lại router – id của tiến trình thì sao? Ta phải thực hiện khởi động lại router hoặc gỡ bỏ tiến trình OSPF rồi cấu hình lại, khi đó tiến trình bầu chọn router – id sẽ được thực hiện lại với các interface đang hiện hữu trên router.

Và như vậy, ta thấy việc ưu tiên sử dụng IP trên loopback mang nhiều ý nghĩa về mặt quản trị hơn là tính ổn định của tiến trình. Nó cho phép người quản trị kiểm soát hiệu quả hơn các router – id của các router.

Có một cách khác để thiết lập lại giá trị router – id cho router mà không cần phải khởi động lại router hoặc cấu hình lại OSPF là sử dụng câu lệnh ‘router-id’ để thiết lập bằng tay giá trị này trên router:

```
Router(config)#router ospf 1
Router(config-router)#router-id A.B.C.D
```

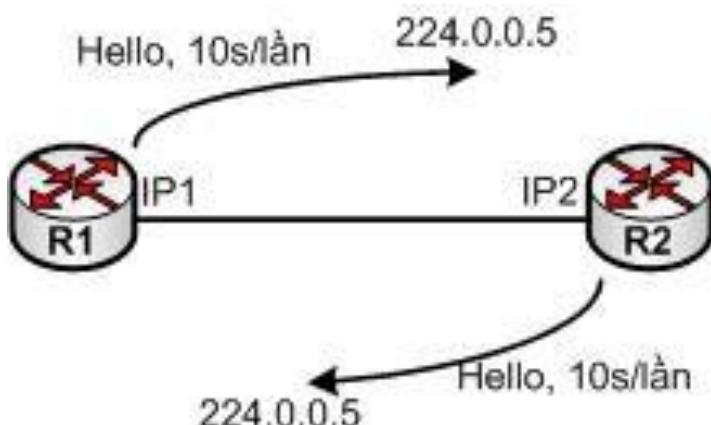
Lúc này giá trị của router – id có thể không cần phải là một địa chỉ IP có sẵn trên router. Bên cạnh đó, nếu tiến trình OSPF đã chạy và router – id đã được thiết lập trước đó, ta phải khởi động lại tiến trình OSPF thì mới áp dụng được giá trị router – id mới được chỉ ra trong câu lệnh ‘router – id’. Câu lệnh khởi động lại tiến trình OSPF:

```
Router#clear ip ospf process
Reset ALL OSPF processes? [no]: yes <- Ta chọn ‘Yes’
```

Sau khi đã chọn xong router – id để hoạt động, router chạy OSPF sẽ chuyển qua bước tiếp theo là thiết lập quan hệ láng giềng với các router kết nối trực tiếp với nó.

Thiết lập quan hệ láng giềng

Bước tiếp theo, sau khi đã chọn xong router – id, router chạy OSPF sẽ gửi ra tất cả các cổng chạy OSPF một loại gói tin được gọi là gói tin hello. Gói tin này được gửi đến



địa chỉ multicast dành riêng cho OSPF là 224.0.0.5, đến tất cả các router chạy OSPF khác trên cùng phân đoạn mạng. Mục đích của gói tin hello là giúp cho router tìm kiếm láng giềng, thiết lập và duy trì mối quan hệ này. Gói tin hello được gửi theo định kỳ mặc định 10s/lần.

Hình 4. 8 Các router gửi gói tin hello

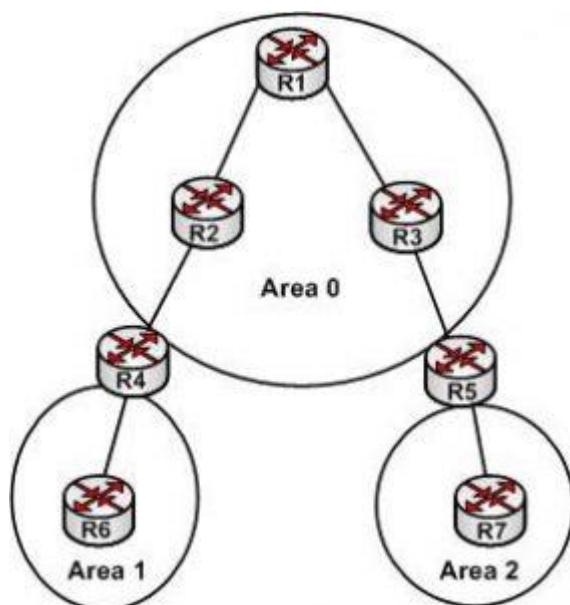
Có nhiều thông tin được hai router kết nối trực tiếp trao đổi với nhau qua gói tin hello. Trong các loại thông tin được trao đổi, có năm loại thông tin sau bắt buộc phải match với nhau trên hai router để chúng có thể thiết lập được quan hệ láng giềng với nhau:

1. Area – id.
2. Hello timer và Dead timer.
3. Hai địa chỉ IP đầu nối phải cùng subnet (một vài trường hợp còn yêu cầu cùng cả subnet – mask).
4. Thỏa mãn các điều kiện xác thực.
5. Cùng bật hoặc cùng tắt cờ stub.

Ta cùng phân tích từng thông số đã nêu ở trên.

Area – id

Nguyên tắc hoạt động của OSPF là mỗi router phải ghi nhớ bảng cơ sở dữ liệu trạng thái đường link của toàn bộ hệ thống mạng chạy OSPF rồi từ đó thực hiện tính toán định tuyến dựa trên bảng cơ sở dữ liệu này. Để giảm tải bộ nhớ cũng như tải tính toán cho mỗi router và giảm thiểu lượng thông tin định tuyến cần trao đổi, các router chạy OSPF được chia thành nhiều vùng (area), mỗi router lúc này chỉ cần phải ghi nhớ thông tin cho một vùng mà nó ở trong đó (hình 4.9).



Hình 4. 9 Kiến trúc phân vùng trong OSPF

Cách tổ chức như vậy rõ ràng tiết kiệm tài nguyên mạng và tài nguyên trên mỗi router. Ngoài ra, cách tổ chức này còn cô lập được những bất ổn vào trong một vùng: khi có một link nào đó trên một router up/down, sự kiện này chỉ lan truyền trong nội bộ một vùng và gây ra sự tính toán lại định tuyến của các router trong vùng ấy chứ không ảnh hưởng đến các router thuộc vùng khác.

Mỗi vùng được chỉ ra sẽ có một giá trị định danh cho vùng gọi là Area – id. Area – id có thể được hiển thị dưới dạng một số tự nhiên hoặc dưới dạng của một địa chỉ IP. Ví dụ Area 0 có thể được biểu diễn là Area 0.0.0.0. Một nguyên tắc bắt buộc trong phân vùng OSPF là nếu chia thành nhiều vùng thì bắt buộc phải tồn tại một vùng mang số hiệu 0 – Area 0, Area 0 còn được gọi là Backbone Area và mọi vùng khác bắt buộc phải có kết nối với vùng 0.

Khi thực hiện cấu hình phân vùng cho router, ta không gán cả router vào một vùng mà thực hiện gán link trên router vào một vùng. Area – id được gán cho link của router chứ không phải gán cho bản thân router. Ví dụ: trên hình 4, ta thấy toàn bộ router R2 nằm trong vùng 0 là vì khi cấu hình ta đã gán hai link trên R2 vào vùng 0. Những router mà có tất cả các link đều được gán vào một vùng thì sẽ lọt hẳn vào vùng đó và được gọi là các Internal router, các Internal router chỉ phải ghi nhớ trạng thái đường link của vùng mà nó nằm bên trong. Ta cũng xét tiếp router R4. Router này có một link thuộc vùng 0, lại có một link thuộc vùng 1, như vậy nó thuộc về cả hai vùng và phải ghi nhớ trạng thái đường link của cả hai vùng. Những router như vậy được gọi là các router ABR – Area Border Router – router biên giới giữa hai vùng.

Khi hai router langoing giềng kết nối với nhau qua một link, chúng phải thống nhất với nhau về area – id của link này. Cả hai router phải gán cùng một số area – id cho link kết nối giữa chúng với nhau. Nếu điều này bị vi phạm, chúng sẽ không thể thiết lập được quan hệ langoing giềng thông qua link này và do đó không bao giờ có thể trao đổi được thông tin định tuyến qua link. Đó là điều kiện thứ nhất trong việc thiết lập quan hệ langoing giềng: thống nhất về area – id trên link kết nối.

Chương trình CCNA không đề cập đến OSPF đa vùng mà chỉ nói về OSPF đơn vùng, trong đó mọi router đều được gán vào một vùng. Kiến trúc đa vùng và các vấn đề chi tiết của nó sẽ được đề cập chi tiết trong course Route của chương trình CCNP.

Hello timer và Dead timer

Hello timer là khoảng thời gian định kỳ gửi gói tin hello ra khỏi một cổng chạy OSPF. Khi một router nhận được hello từ langoing giềng, nó sẽ khởi động *Dead timer*. Nếu sau khoảng thời gian được chỉ ra trong *Dead timer* mà router không nhận được gói tin hello từ langoing giềng, nó sẽ coi như langoing giềng này không còn và sẽ xóa mọi thông tin mà nó học được từ langoing giềng. Ngược lại, cứ mỗi lần nhận được gói tin hello từ langoing

giềng, *Dead timer* lại được reset. Giá trị mặc định của *hello – timer* và *dead – timer* là 10s và 40s. Ta có thể hiệu chỉnh các giá trị này trên cổng chạy OSPF bằng cách sử dụng câu lệnh:

```
R(config-if)#ip ospf {hello-interval | dead-interval} seconds
```

Để hai router thiết lập được quan hệ láng giềng với nhau, cặp giá trị này bắt buộc phải khớp nhau trên hai router ở hai đầu của đường link.

Cùng subnet

Hai địa chỉ IP1 và IP2 đầu nối nhau giữa hai router bắt buộc phải cùng subnet thì hai router này mới có thể thiết lập quan hệ láng giềng với nhau (xem hình 3). Một số trường hợp còn bắt buộc hai địa chỉ này phải cùng cả subnet – mask để có thể thiết lập neighbor.

Thỏa mãn authentication

Trong trường hợp để tăng cường tính bảo mật của hoạt động trao đổi thông tin định tuyến, chúng ta thực hiện cài đặt các password trên hai router hai đầu đường link. Yêu cầu bắt buộc là hai password này phải khớp nhau ở hai đầu để hai router có thể thiết lập neighbor (tất nhiên!). Cấu hình xác thực sai có thể dẫn đến không thiết lập neighbor được giữa hai router từ đó dẫn đến không trao đổi được thông tin định tuyến.

Cờ stub

Trong kiến trúc đa vùng của OSPF có một loại vùng gọi là vùng stub. Vùng stub là vùng không tiếp nhận LSA type – 5. Khi ta đã cho một link của một router thuộc vùng stub thì bắt buộc đầu kia của link cũng phải gán link này thuộc vùng stub. Khi đó các gói tin định tuyến trao đổi nhau giữa hai đầu sẽ có cờ stub được bật lên. Chi tiết về vùng stub được đề cập cụ thể trong course Route của chương trình CCNP, chương trình CCNA không cover vấn đề này.

Sau khi cả 05 điều kiện nêu trên đã được thỏa mãn, hai router thiết lập với nhau một mối quan hệ gọi là quan hệ láng giềng và được ký hiệu là 2 – WAY. Khi các router đã thiết lập được quan hệ 2 – WAY với nhau, chúng bắt đầu thực hiện trao đổi bằng cơ sở dữ liệu trạng thái đường link (LSDB – Link State Database) cho nhau. Việc trao đổi này được lan ra toàn mạng và cuối cùng mỗi router đều có được trạng thái đường link của mọi router trong mạng, từ đó chúng thực hiện tính toán trên cơ sở dữ liệu trạng thái đường link này và xây dựng bảng định tuyến.

Trao đổi LSDB

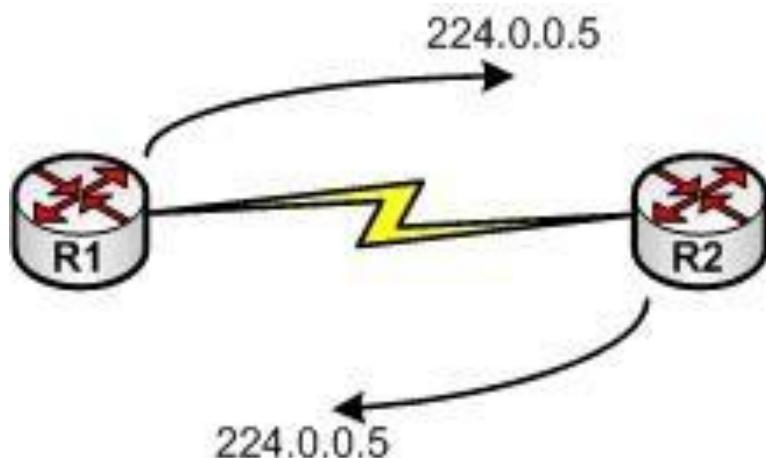
LSDB – Link State Database – Bảng cơ sở dữ liệu trạng thái đường link là một bảng trên router ghi nhớ mọi trạng thái đường link của mọi router trong vùng. Ta có thể coi LSDB là một “tấm bản đồ mạng” mà router sẽ căn cứ vào đó để tính toán định tuyến. LSDB phải hoàn toàn giống nhau giữa các router cùng vùng. Các router sẽ không trao đổi với nhau cả một bảng LSDB mà sẽ trao đổi với nhau từng đơn vị thông tin gọi là LSA –

Link State Advertisement. Các đơn vị thông tin này lại được chứa trong các gói tin cụ thể gọi là LSU – Link State Update mà các router thực sự trao đổi với nhau. Lưu ý: LSA không phải là một loại *gói tin* mà chỉ là một *bản tin*. LSU mới thực sự là gói tin và nó chứa đựng các bản tin này.

Việc trao đổi thông tin diễn ra rất khác nhau tùy theo từng loại network – type gán cho link giữa hai router. Trong khuôn khổ chương trình CCNA, chúng ta chỉ xét đến hai loại network – type là *Point – to – Point* và *Broadcast Multiaccess*.

Point – to – point

Loại link point – to – point điển hình là kết nối serial điểm – điểm chạy giao thức HDLC hoặc PPP nối giữa hai router (hình 4.10).

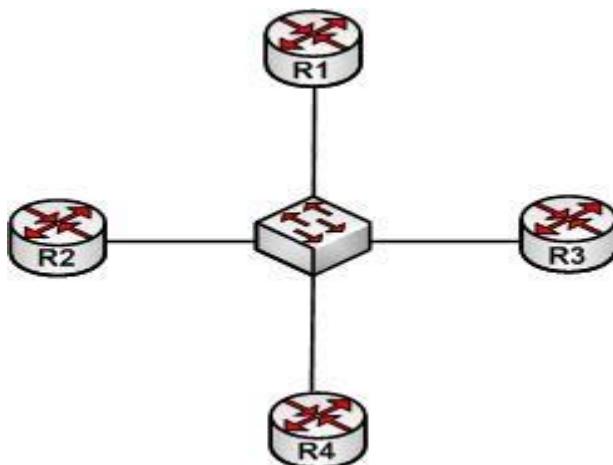


Hình 4. 10 Trao đổi LSDB với kết nối point – to – point

Trong trường hợp này, hai router lóng giềng sẽ ngay lập tức gửi toàn bộ bảng LSDB cho nhau qua kết nối point – to – point và chuyển trạng thái quan hệ từ 2 – WAY sang một mức độ mới gọi là quan hệ dạng FULL. Quan hệ Full qua một kết nối serial point – to – point được ký hiệu là FULL/ –

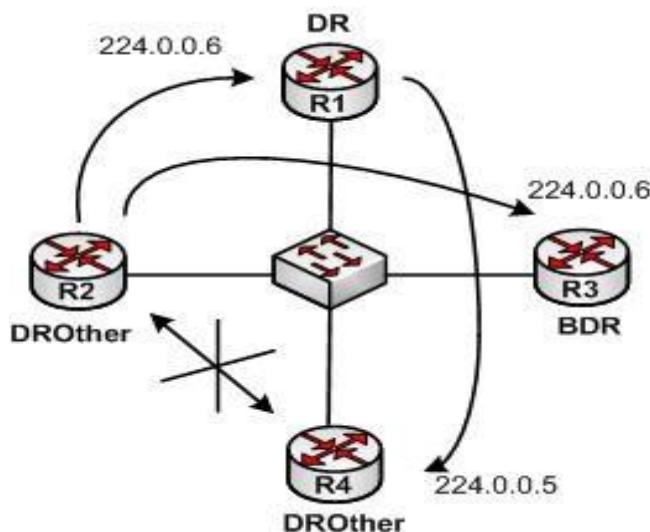
Broadcast Multiaccess

Môi trường Broadcast Multiaccess điển hình chính là môi trường Ethernet LAN (hình 6).



Hình 4. 11 Broadcast MultiAccess

Việc trao đổi LSDB diễn ra hoàn toàn khác trong môi trường này. Với môi trường này, mỗi router đều kết nối trực tiếp với nhau và đều thiết lập quan hệ 2 – WAY với nhau. Tuy nhiên, các router sẽ không trao đổi trực tiếp với nhau mà sẽ tiến hành trao đổi thông tin thông qua một router đầu mối gọi là DR – Designated Router. Trên mỗi kết nối Multi – access, một DR router được bầu ra. Một router khác sẽ được bầu làm Backup DR (BDR) để dự phòng cho DR trong trường hợp DR down. Các router còn lại đóng vai trò là DROther. Nguyên tắc đặt ra như sau: các router DROther khi trao đổi thông tin định tuyến sẽ không gửi trực tiếp cho nhau mà sẽ gửi lên cho DR và BDR. Sau đó router DR này sẽ forward lại thông tin xuống cho các router DROther khác. Khi các router gửi thông tin lên cho DR và BDR, chúng sẽ sử dụng địa chỉ multicast 224.0.0.6 còn khi DR



forward lại thông tin xuống các router khác, nó sử dụng địa chỉ 224.0.0.5. Nhắc lại, các DROther không trao đổi trực tiếp với nhau.

Hình 4. 12 Hoạt động trao đổi thông tin thông qua DR

Về quan hệ giữa các cặp router lúc này, ta thấy như sau:

- Các DROther không bao giờ trao đổi thông tin với nhau nên quan hệ giữa chúng mãi mãi chỉ dừng lại ở mức độ 2 – WAY. Thực hiện show bảng neighbor trên các router DROther sẽ thấy rằng các router này hiển thị tình trạng quan hệ với nhau là 2-WAY/DROther.
- Các DROther có trao đổi dữ liệu với DR và BDR nên trong bảng neighbor của các router DROther, các router DR và BDR sẽ hiện ra với quan hệ dạng full: FULL/DR và FULL/BDR. Ngược lại, các router DR và BDR cũng thấy tình trạng quan hệ của các router DROther với chúng là FULL/DROther.

Như vậy, router DR đóng một vai trò rất quan trọng trên môi trường Multiaccess: đó là router điều phối thông tin trên môi trường này. Vậy router nào sẽ được chọn làm DR? Ta có nguyên tắc bầu chọn DR và BDR cho một môi trường multi – access như sau:

- Trên mỗi cổng đấu nối multi – access của mỗi router đều có một giá trị gọi là priority. Giá trị priority này nằm trong dải từ 0 đến 255 và được trao đổi giữa các router trong các gói tin hello. Router nào nắm giữ giá trị priority cao nhất sẽ được bầu chọn làm DR, priority cao nhì làm BDR, còn lại sẽ là DROther. Giá trị priority mặc định trên các cổng router là bằng 1. Lưu ý rằng nếu router mang giá trị priority bằng 0 sẽ không tham gia vào tiến trình bầu chọn DR và BDR, nó luôn luôn đảm nhận vai trò là DROther.

- Trong trường hợp giá trị priority bằng nhau (ví dụ để mặc định bằng 1 hết, không cấu hình gì thêm), router nào có Router – id cao nhất sẽ làm DR, Router – id cao nhì sẽ làm BDR, còn lại làm DROther. Ta nói Router – id là tie – breaker của Priority.

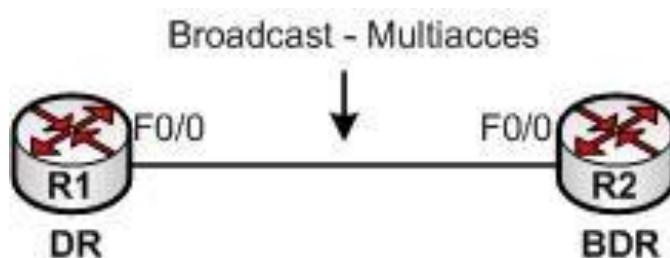
Có một số lưu ý cho việc bầu chọn DR và BDR như sau:

- Nếu ta cấu hình một router nhận giá trị priority bằng 0, router này sẽ không tham gia vào tiến trình bầu chọn DR và BDR, nó luôn luôn là DROther. Chúng ta phải lưu ý điều này vì nếu chúng ta cấu hình cho tất cả các router đấu nối vào môi trường multi – access giá trị priority = 0 thì sẽ không có router nào chịu làm DR cho môi trường này! Lỗi này dẫn đến lỗi hỏng trong việc trao đổi thông tin định tuyến.

- Luật bầu chọn DR là non – preempt: khi một DR đã được bầu chọn xong, nếu router mới tham gia vào môi trường multi – access có priority hay router – id cao hơn router DR nó cũng không thể chiếm quyền của DR hiện tại. Chỉ khi nào DR hiện tại down, router khác mới có cơ hội tranh quyền DR.

- Một router có thể đóng nhiều vai trò khác nhau trên nhiều cổng multi – access khác nhau. Ví dụ: nó có thể là DR trên môi trường Multi – access đấu nối vào cổng F0/0 nhưng lại là DROther trên môi trường Multi – access đấu nối vào cổng F0/1.

- Chúng ta không được nhầm lẫn kết nối Ethernet nối 02 router là một kết nối point – to – point, kết nối này vẫn được xem là Multi – access. Trong trường hợp này, một router sẽ làm DR, một làm BDR, không có DROther (hình 8).



Hình 4. 13 Đây là môi trường Multi – access dù chỉ có 02 router

Sau khi hoàn thành xong thao tác trao đổi LSDB, mỗi router trong vùng đều đã có được bảng cơ sở dữ liệu trạng thái đường link của mọi router trong vùng, hay nói một cách khác, mỗi router đã có được “tấm bản đồ mạng” của cả vùng. Dựa trên LSDB này, các router sẽ chạy thuật toán Dijkstra để xây dựng một cây đường đi ngắn nhất đến mọi đích đến trong mạng với gốc cây chính là router ấy. Từ cây này, router xây dựng lên bảng định tuyến của mình. Chi tiết về giải thuật Dijkstra xin không đề cập ở đây. Các bạn quan tâm có thể tìm hiểu thông qua các giáo trình về Toán rời rạc hoặc Lý thuyết đồ thị của các trường Đại học. Bài viết này sẽ giới thiệu cách OSPF tính toán metric cho các đường đi và cách người quản trị nhìn vào sơ đồ mạng để xác định đường đi mà OSPF đã chọn mà không phải “chạy” thuật toán Dijkstra trong đầu ^^:

Tính toán metric với OSPF

Metric trong OSPF được gọi là cost, được xác định dựa vào bandwidth danh định của đường truyền theo công thức như sau:

$$\text{Metric} = \text{cost} = 10^8 / \text{Bandwidth} \text{ (đơn vị bps)}.$$

Ta phân biệt giữa bandwidth danh định trên cổng và tốc độ thật của cổng ấy. Hai giá trị này không nhất thiết phải trùng nhau và giá trị danh định mới chính là giá trị được tham gia vào tính toán định tuyến. Giá trị danh định được thiết lập trên cổng bằng câu lệnh:

`R(config-if)#bandwidth BW(đơn vị là kbps)`

Ta phải chỉnh giá trị danh định này trùng với tốc độ thật của cổng để tránh việc tính toán sai lầm trong định tuyến. Ví dụ: một đường leased – line kết nối vào cổng serial chỉ có tốc độ thật là 512kbps nhưng giá trị bandwidth danh định trên cổng serial luôn là 1.544Mbps ở mặc định. Điều đó dẫn đến OSPF xem một cổng 512 kbps như một cổng 1.544 Mbps! Ta phải chỉnh lại băng thông danh định trên cổng trong trường hợp này để phản ánh đúng tốc độ thật:

`R(config-if)#bandwidth 512`

Dựa vào công thức metric đã nêu ở trên, ta có giá trị cost default của một số loại cổng:

Ethernet (BW = 10Mbps) -> cost = 10.

Fast Ethernet (BW = 100Mbps) -> cost = 1.

Serial (BW = 1.544Mbps) -> cost = 64 (chặt bỏ phần thập phân trong phép chia).

Ta cùng xem xét một ví dụ để khảo sát cách tính toán path – cost cho một đường đi:



Hình 4. 14 Sơ đồ ví dụ tính path – cost

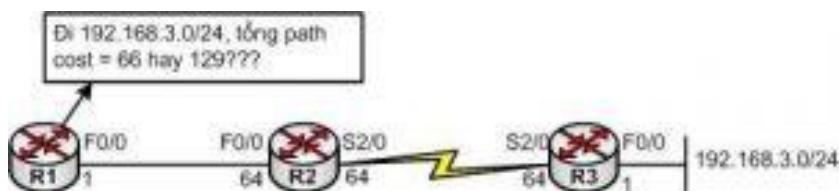
Yêu cầu đặt ra với sơ đồ hình 9 là tính path – cost (metric) cho đường đi từ R1 đến mạng 192.168.3.0/24 của R3.

Ta thấy một cách dễ dàng: từ R1 đi đến mạng 192.168.3.0/24 của R3 sẽ đi qua các đường link Fast Ethernet có cost = 1, serial có cost là 64 và link Fast Ethernet có cost bằng 1. Vậy tổng cost tích lũy sẽ là $1 + 64 + 1$ là 66. Metric từ R1 đến mạng 192.168.3.0/24 là 66.

Tuy nhiên việc tính toán sẽ trở nên phức tạp hơn nếu hai cổng router ở hai đầu link không đồng nhất về giá trị cost. Ví dụ, ta vào cổng F0/0 của R2 đổi lại giá trị cost thành 64 bằng cách đánh lệnh sau đây trên cổng F0/0 của R2:

```
R2(config)#interface f0/0
R2(config-if)#ip ospf cost 64
```

Vậy câu hỏi đặt ra là với link Fast Ethernet nối giữa R1 và R2 ta chọn cost của link này là 1 hay 64? Nếu chọn là 1, tổng cost toàn tuyến vẫn giữ giá trị như cũ là 66, nhưng nếu chọn là 64, tổng cost toàn tuyến sẽ là $64 + 64 + 1$ là 129, hai giá trị rất khác



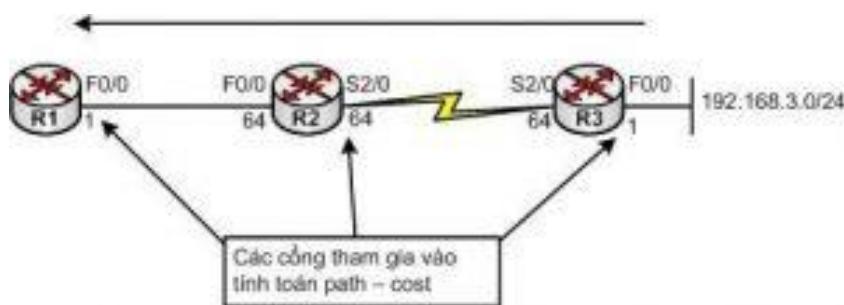
nhau!

Hình 4. 15 Tổng path – cost là 66 hay 129

Để trả lời được câu hỏi này, ta cần nắm nguyên tắc sau đây trong việc tính tổng cost với OSPF:

Để tính tổng cost từ một router đến một mạng đích theo một đường (path) nào đó, ta thực hiện lần ngược từ đích lần về và cộng dồn cost theo quy tắc đi vào thì cộng, đi ra thì không cộng.

Áp dụng quy tắc này cho ví dụ ở hình 10: để tính tổng cost từ R1 đến mạng 192.168.3.0/24, ta đi ngược từ mạng 192.168.3.0/24 đi về. Khi đi về ta đi vào cổng F0/0 của R3, cộng giá trị cổng này (tổng cost lúc này là 1); đi ra khỏi cổng S2/0 của R3, bỏ qua không cộng (tổng cost vẫn là 1); đi tiếp vào cổng S2/0 của R2, cộng giá trị cổng này (lúc này tổng cost là $1 + 64 = 65$); đi ra khỏi cổng F0/0 của R2, bỏ qua không cộng (tổng cost vẫn là 65); đi tiếp vào cổng F0/0 của R1, cộng giá trị cổng này (tổng cost là $65 + 1 = 66$), kết thúc hành trình. Vậy tổng cost vẫn là 66, việc thay đổi giá trị cost trên cổng F0/0 không ảnh hưởng gì đến path – cost từ R1 đi đến 192.168.3.0/24.



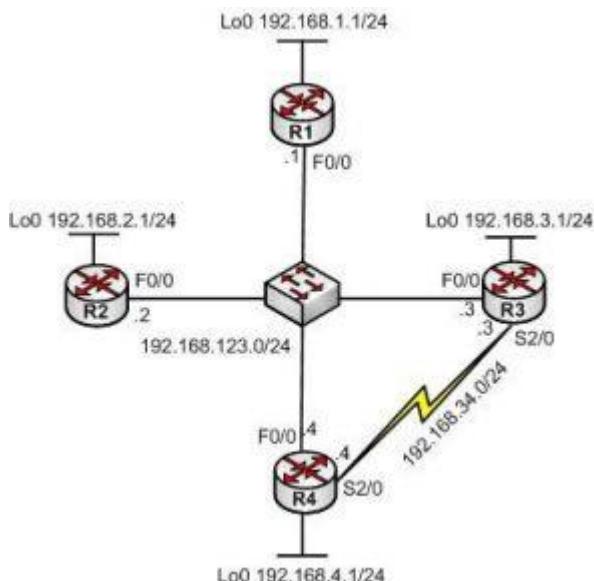
Hình 4. 16 Các cổng tham gia vào tiến trình tính toán path – cost với OSPF

Như vậy với OSPF, để đánh giá đúng được cost của đường đi và có thể hiệu chỉnh cost trên cổng để bé đường đi của gói tin theo ý muốn, ta cần phải cẩn thận trong việc xác định xem cổng nào trên đường đi sẽ tham gia vào tính toán để hiệu chỉnh đúng cổng vì hiệu chỉnh không đúng cổng sẽ không mang lại bất kỳ thay đổi gì.

Trên đây, chúng ta đã cùng nhau review một số nét chính trong hoạt động của OSPF đơn vùng thông qua các bước hoạt động của tiến trình OSPF: chọn Router – id, thiết lập quan hệ láng giềng, trao đổi LSDB và tính toán xây dựng bảng định tuyến.

Tiếp theo chúng ta cùng review lại cách thức cấu hình OSPF thông qua ví dụ được trình bày dưới đây.

Cấu hình



Hình 4. 17 Sơ đồ ví dụ cấu hình.

Trên hình 4.17 là 4 router đại diện cho bốn chi nhánh khác nhau của một doanh nghiệp: R1 cho chi nhánh 1, R2 cho chi nhánh 2, R3 cho chi nhánh 3 và R4 cho chi nhánh 4. Các interface loopback trên các router đại diện cho các mạng nội bộ của mỗi chi nhánh, sử dụng các subnet trên R1, R2, R3 và R4 lần lượt là 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24 và 192.168.4.0/24. Bốn router này đều nối với nhau thông qua một kết nối multi – access (đại diện bằng một Ethernet Switch), sử dụng subnet là 192.168.123.0/24 (trên thực tế, đây có thể là một môi trường Metro net đấu nối giữa các chi nhánh). Router R3 và R4 còn thực hiện đấu nối riêng với nhau bằng một đường leased – line thông qua các cổng serial, sử dụng subnet 192.168.34.0/24.

Yêu cầu đặt ra là chạy định tuyến OSPF đảm bảo mọi địa chỉ trên sơ đồ này thấy nhau.

Để thực hiện chạy OSPF trên các router, chúng ta sử dụng câu lệnh sau:

```
R(config)#router ospf process-id
```

```
R(config-router)#network địa chỉ IP wildcard-mask area area-id
```

Trong đó:

Process – id: số hiệu của tiến trình OSPF chạy trên router, chỉ có ý nghĩa local trên router

Để cho một cổng tham gia OSPF, ta thực hiện network địa chỉ mạng của cổng đó. Với OSPF ta phải sử dụng thêm wildcard – mask để lấy chính xác subnet tham gia định tuyến. Ta cũng phải chỉ ra link thuộc area nào bằng tham số “area”.

Cấu hình trên các router:

Trên router R1:

```
R1(config)#router ospf 1
```

```
R1(config-router)#network 192.168.123.0 0.0.0.255 area 0
```

```
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
```

Trên router R2:

```
R2(config)#router ospf 1
```

```
R2(config-router)#network 192.168.123.0 0.0.0.255 area 0
```

```
R2(config-router)#network 192.168.2.0 0.0.0.255 area 0
```

Trên router R3:

```
R3(config)#router ospf 1
```

```
R3(config-router)#network 192.168.123.0 0.0.0.255 area 0
```

```
R3(config-router)#network 192.168.34.0 0.0.0.255 area 0
```

```
R3(config-router)#network 192.168.3.0 0.0.0.255 area 0
```

Trên router R4:

```
R4(config)#router ospf 1
```

```
R4(config-router)#network 192.168.123.0 0.0.0.255 area 0
```

```
R4(config-router)#network 192.168.34.0 0.0.0.255 area 0
```

```
R4(config-router)#network 192.168.4.0 0.0.0.255 area 0
```

Ta thấy khi muốn cho cổng F0/0 trên router tham gia OSPF, ta “network” mạng 192.168.123.0/24 trên cổng này. Giá trị wildcard – mask được tính cho /24 sẽ là 0.0.0.255 (để tính được giá trị wildcard mask, ta lấy giá trị 255.255.255.255 trừ đi giá trị subnet – mask 255.255.255.0 từng octet một sẽ được kết quả cần tìm. Cách tính này chỉ đúng cho một dải IP liên tiếp, không phải đúng cho mọi trường hợp. Về wildcard – mask sẽ có một bài viết khác để cập chi tiết cho vấn đề này). Tương tự với các cổng khác của các router.

Kiểm tra bằng cách hiển thị bảng định tuyến của các router:

Trên R1:

R1#sh ip route ospf

192.168.4.0/32 is subnetted, 1 subnets

O 192.168.4.1 [110/2] via 192.168.123.4, 00:00:29, FastEthernet0/0

O 192.168.34.0/24 [110/65] via 192.168.123.4, 00:00:29, FastEthernet0/0
[110/65] via 192.168.123.3, 00:00:29, FastEthernet0/0

192.168.2.0/32 is subnetted, 1 subnets

O 192.168.2.1 [110/2] via 192.168.123.2, 00:00:29, FastEthernet0/0

192.168.3.0/32 is subnetted, 1 subnets

O 192.168.3.1 [110/2] via 192.168.123.3, 00:00:29, FastEthernet0/0

Trên R2:

R2#show ip route ospf

192.168.4.0/32 is subnetted, 1 subnets

O 192.168.4.1 [110/2] via 192.168.123.4, 00:01:20, FastEthernet0/0

O 192.168.34.0/24 [110/65] via 192.168.123.4, 00:01:20, FastEthernet0/0
[110/65] via 192.168.123.3, 00:01:20, FastEthernet0/0

192.168.1.0/32 is subnetted, 1 subnets

O 192.168.1.1 [110/2] via 192.168.123.1, 00:01:20, FastEthernet0/0

192.168.3.0/32 is subnetted, 1 subnets

O 192.168.3.1 [110/2] via 192.168.123.3, 00:01:20, FastEthernet0/0

Trên R3:

R3#show ip route ospf

192.168.4.0/32 is subnetted, 1 subnets

O 192.168.4.1 [110/2] via 192.168.123.4, 00:02:07, FastEthernet0/0

192.168.1.0/32 is subnetted, 1 subnets

O 192.168.1.1 [110/2] via 192.168.123.1, 00:02:07, FastEthernet0/0

192.168.2.0/32 is subnetted, 1 subnets

O 192.168.2.1 [110/2] via 192.168.123.2, 00:02:07, FastEthernet0/0

Trên R4:

R4#show ip route ospf

192.168.1.0/32 is subnetted, 1 subnets

O 192.168.1.1 [110/2] via 192.168.123.1, 00:21:57, FastEthernet0/0

192.168.2.0/32 is subnetted, 1 subnets

O 192.168.2.1 [110/2] via 192.168.123.2, 00:21:57, FastEthernet0/0

192.168.3.0/32 is subnetted, 1 subnets

O 192.168.3.1 [110/2] via 192.168.123.3, 00:21:57, FastEthernet0/0

Ta thấy rằng các subnet ở xa đã được học thông qua OSPF (các route OSPF được ký hiệu bằng ký tự “O”).

Một điểm đặc đáo chúng ta để ý là các mạng loopback khi hiển thị trong bảng định tuyến của các router đều được OSPF chuyển thành /32. Đây là một nét trong hoạt động của giao thức OSPF, một loại giao thức cung cấp cho mỗi router một cái nhìn tổng quan toàn mạng chứ không phải chỉ dựa vào “tin đồn được lan truyền” như với Distance – vector. Với cái nhìn như vậy, mỗi router xác định được mạng loopback nằm trên một cổng không đấu nối đi đâu cả và chỉ có một địa chỉ của cả một mạng được sử dụng. /32 được sử dụng để phản ánh điều này. Để khắc phục hiện tượng này và khiến cho các subnet loopback được hiển thị đúng giá trị prefix – length, ta thay đổi kiểu network – type trên interface loopback thành kiểu “point – to – point” bằng câu lệnh:

```
R(config)#interface loopback 0
```

```
R(config-if)#ip ospf network point-to-point
```

Chi tiết về các “network – type” được sử dụng trong OSPF sẽ được đề cập trong các bài viết khác trong khuôn khổ của chương trình CCNP.

Ta cùng khảo sát bảng neighbor trên các router:

Trên R4:

```
R4#show ip ospf neighbor
```

Neighbor ID Pri State Dead Time Address Interface

192.168.3.1 0 FULL/ – 00:00:34 192.168.34.3 Serial2/0

192.168.1.1 1 FULL/DROther 00:00:32 192.168.123.1 FastEthernet0/0

192.168.2.1 1 FULL/DROther 00:00:34 192.168.123.2 FastEthernet0/0

192.168.3.1 1 FULL/BDR 00:00:37 192.168.123.3 FastEthernet0/0

Ta thấy, R4 đã thiết lập quan hệ láng giềng với các router còn lại. Qua cổng F0/0, nó thấy 03 router láng giềng có router – id là 192.168.1.1, 192.168.2.1, 192.168.3.1. Tình trạng quan hệ cũng chỉ rõ quan hệ là dạng FULL và vai trò của các router láng giềng trong môi trường multi – access. Từ kết quả show ở trên, ta thấy rất rõ ràng router R1 (192.168.1.1), R2 (192.168.2.1) là các DROther router, R3 (192.168.3.1) là BDR router và dĩ nhiên, ta có thể suy ra được R4 chính là DR router. DR thiết lập quan hệ dạng FULL với tất cả các router trong môi trường multi – access.

Ta cũng thấy rằng R4 cũng thiết lập quan hệ láng giềng dạng FULL với R3 qua cổng serial 2/0. Vì đây là cổng point – to – point nên các router không bầu chọn DR và BDR và quan hệ giữa hai router được ký hiệu là FULL/-.

Trên R1:

R1#show ip ospf neighbor

Neighbor ID Pri State Dead Time Address Interface

192.168.2.1 1 2WAY/DROther 00:00:30 192.168.123.2 FastEthernet0/0

192.168.3.1 1 FULL/BDR 00:00:32 192.168.123.3 FastEthernet0/0

192.168.4.1 1 FULL/DR 00:00:31 192.168.123.4 FastEthernet0/0

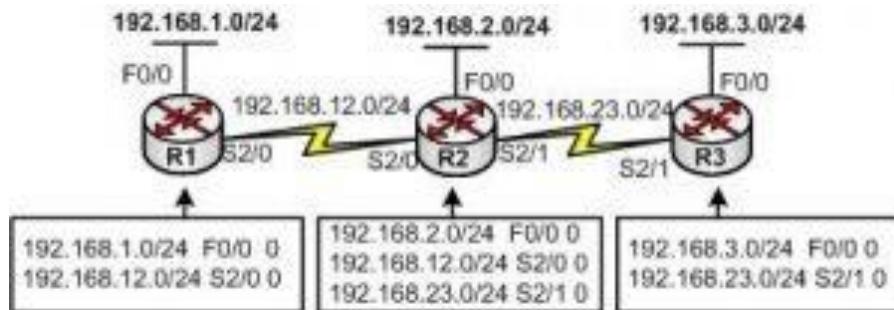
Trên kết quả show của R1, ta cũng thấy các láng giềng R2 (192.168.2.1), R3(192.168.3.1) và R4 (192.168.4.1) và vai trò của từng con router trong môi trường multi – access. Ta để ý rằng R1 chỉ duy trì quan hệ ở mức 2WAY với R2, cũng là một DROther giống nó. Hai DROther không bao giờ trao đổi trực tiếp thông tin định tuyến với nhau nên không bao giờ thiết lập được quan hệ dạng FULL.

Thực hiện kiểm tra tương tự với các router R2 và R3.

4.6.2. Giao thức định tuyến RIP

1. RIP là một giao thức distance – vector điển hình. Mỗi router sẽ gửi toàn bộ bảng định tuyến của nó cho router láng giềng theo định kỳ 30s/lần. Thông tin này lại tiếp tục được láng giềng lan truyền tiếp cho các láng giềng khác và cứ thế lan truyền ra mọi router trên toàn mạng. Kiểu trao đổi thông tin như thế còn được gọi là “lan truyền theo tin đòn”. (Ở đây, ta có thể hiểu router láng giềng là router kết nối trực tiếp với router đang xét).
2. Metric trong RIP được tính theo hop count – số node lớp 3 (router) phải đi qua trên đường đi để đến đích. Với RIP, giá trị metric tối đa là 15, giá trị metric = 16 được gọi là infinity metric (“metric vô hạn”), có nghĩa là một mạng chỉ được phép cách nguồn tin 15 router là tối đa, nếu nó cách nguồn tin từ 16 router trở lên, nó không thể nhận được nguồn tin này và được nguồn tin xem là không thể đi đến được.
3. RIP chạy trên nền UDP – port 520.
4. RIPv2 là một giao thức classless còn RIPv1 lại là một giao thức classful.
5. Cách hoạt động của RIP có thể dẫn đến loop nên một số quy tắc chống loop và một số timer được đưa ra. Các quy tắc và các timer này có thể làm giảm tốc độ hội tụ của RIP.
6. AD của RIP là 120.

Ta cùng khảo sát hoạt động “lan truyền theo tin đồn” của RIP bằng một ví dụ như sau:



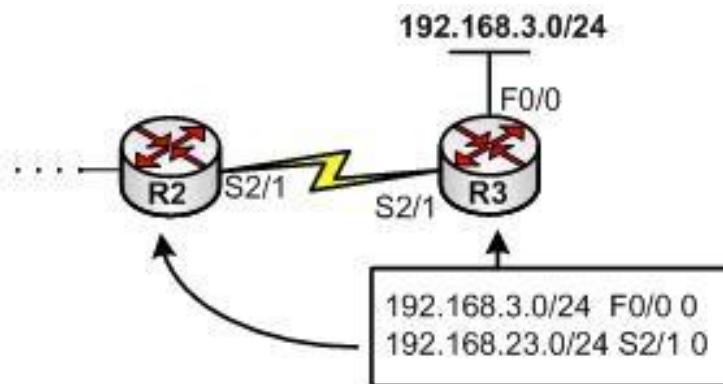
Hình 4.18 Sơ đồ ví dụ 1

Trên hình 4.18 là sơ đồ kết nối của 03 router R1, R2 và R3. Các router này được kết nối với nhau bằng các đường serial point – to – point mô tả các kết nối leased – line. Bản thân mỗi router lại đấu nối xuống các mạng LAN bằng các cổng F0/0 của chúng. Quy hoạch IP cho các phân đoạn mạng được mô tả chi tiết trên sơ đồ.

Như đã thảo luận trong bài viết trước, khi chưa chạy định tuyến mỗi router chỉ biết các mạng kết nối trực tiếp trên các cổng đầu nối của mình và đưa các subnet này vào bảng định tuyến. Trên hình 1 cũng hiển thị bảng định tuyến của mỗi router tại thời điểm đầu tiên khi chưa chạy định tuyến. Các giá trị “0” bên cạnh phản ánh rằng metric để đi đến các mạng này bằng 0 theo quan điểm metric của RIP (các mạng này đều kết nối trực tiếp nên để đi đến chúng không phải bước qua router nào cả).

Tiếp theo, để các router có thể lấy được thông tin của nhau, ta thực hiện chạy định tuyến RIP trên các router để chúng quảng bá thông tin cho nhau bằng cách vào các router bật RIP trên các cổng thích hợp. Câu lệnh để bật RIP sẽ được đề cập đến sau trong bài viết. Ở bước này, ta chỉ khảo sát hoạt động của RIP.

Như đã nói, RIP hoạt động theo kiểu Distance – vector, mỗi router sẽ gửi toàn bộ bảng định tuyến của mình cho các router láng giềng theo định kỳ. Không mất tính tổng quát, ta giả sử R3 sẽ gửi cho R2 trước tiên bảng định tuyến của mình.



Hình 4. 19 R3 gửi cho R2 bảng định tuyến của nó

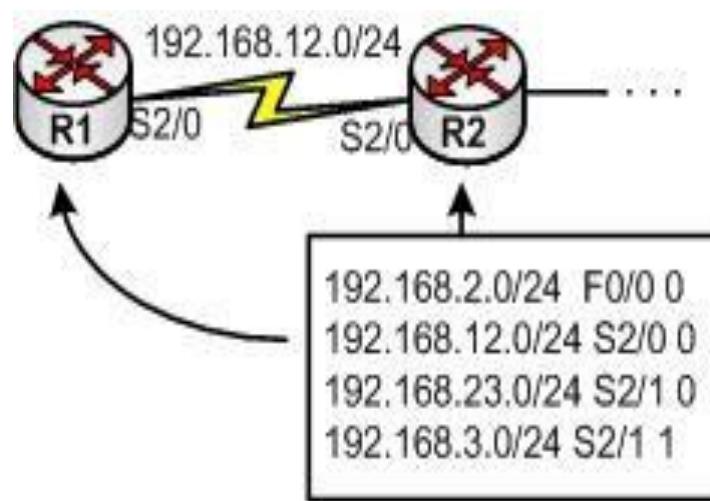
Khi R2 nhận bảng định tuyến này, nó sẽ kiểm tra thông tin và tiếp nhận những route nó chưa có. Có một route 192.168.3.0/24 mà R2 chưa có trong bảng định tuyến, nó sẽ tiếp nhận route này vào bảng định tuyến của nó. Sau khi đã tiếp nhận xong thông tin từ R3, bảng định tuyến từ R2 sẽ là:

192.168.2.0/24	F0/0 0
192.168.12.0/24	S2/0 0
192.168.23.0/24	S2/1 0
192.168.3.0/24	S2/1 1

Hình 4. 20 Bảng định tuyến của R2

Ta thấy route mới được cập nhật chỉ cồng ra là S2/1 vì route này được cập nhật từ phía cổng S2/1, và nó chỉ ra rằng để đi đến được mạng 192.168.3.0/24, gói tin từ R2 phải được đẩy ra cổng S2/1. Thêm nữa, ta cũng thấy metric của route này được tăng thêm 1 đơn vị khi lan truyền qua thêm một router. Quan sát trên hình 1, ta cũng thấy rõ ràng rằng từ R2 muốn đi đến được mạng 192.168.3.0/24, ta phải bước qua một con router (R3) trên đường đi.

Tiếp theo, đến lượt router R2 lại đem toàn bộ bảng định tuyến của mình gửi cho R1:



Hình 4. 21 R2 gửi bảng định tuyến của nó cho R1

Khi R1 nhận bảng định tuyến này, nó sẽ kiểm tra thông tin và tiếp nhận những route nó chưa có. Có hai route là 192.168.23.0/24 và 192.168.3.0/24 mà R1 chưa có trong

bảng định tuyến, nó sẽ tiếp nhận các route này vào bảng định tuyến. Sau khi đã tiếp nhận xong thông tin từ R2, bảng định tuyến từ R1 sẽ là:

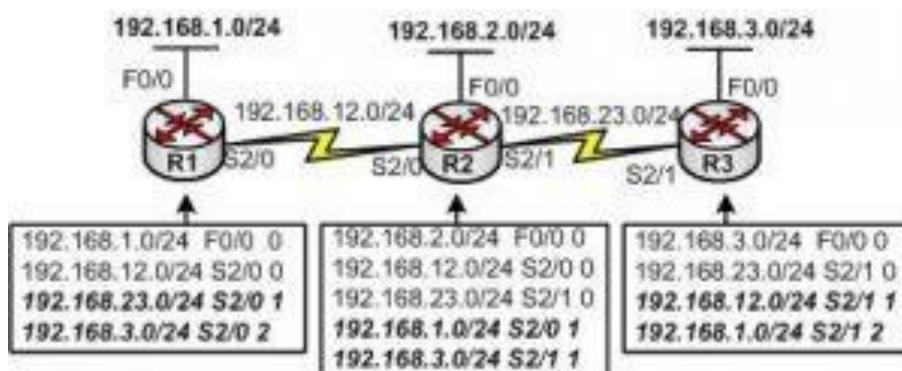
192.168.1.0/24 F0/0 0
192.168.12.0/24 S2/0 0
192.168.23.0/24 S2/0 1
192.168.3.0/24 S2/0 2

Hình 4. 22 Bảng định tuyến của R1

Bảng định tuyến của R1 có thêm các route mới học được: 192.168.23.0/24, cảng ra là S2/0, metric = 1 và 192.168.3.0/24, cảng ra S2/0 với metric = 2. Quan sát lại trên sơ đồ mạng ở hình 1, ta thấy các thông tin này đã được cập nhật hoàn toàn đúng đắn.

Như vậy sau một lượt lan truyền thông tin định tuyến từ R3 đến R1, các subnet phía R3 đã được học trên toàn mạng. Quá trình học này bắt đầu từ láng giềng R2 của R3, sau đó lan từ R2 sang R1. Kiểu lan truyền này được gọi một cách形象 ảnh là “lan truyền theo tin đòn”: R3 “đòn” thông tin của nó sang R2, R2 lại “đòn” tiếp thông tin sang R1. Chúng ta cần nắm vững nguyên tắc hoạt động này của Distance – vector vì các giao thức thuộc trường phái link – state như OSPF lại hoạt động hoàn toàn khác: thông tin định tuyến được gửi đi không phải là các route trong bảng định tuyến mà là các “trạng thái đường link” trong bảng cơ sở dữ liệu trạng thái đường link, và được gửi đi đến mọi router trong vùng chứ không phải là chỉ gửi đi cho láng giềng như đối với Distance – vector.

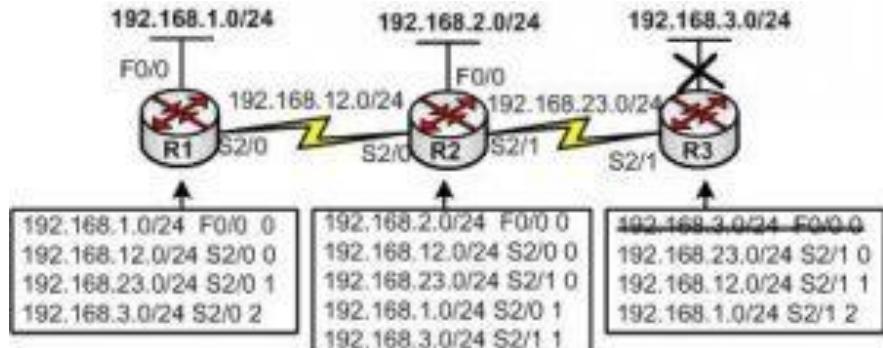
Cuối cùng, sau một vài lượt “lan truyền theo tin đòn” như đã mô tả ở trên, kết quả hội tụ cuối cùng của các bảng định tuyến trên các router sẽ là:



Hình 4. 23 Kết quả hội tụ cuối cùng của ví dụ 1

Các router đều đã học được các subnet ở xa không kết nối trực tiếp thông qua chạy giao thức định tuyến, đảm bảo đi đến được mọi nơi trong hệ thống mạng.

Với kiểu hoạt động này, mỗi router đều phải tin tưởng tuyệt đối vào thông tin định tuyến nhận được từ người láng giềng của mình, từ đó dẫn đến có thể xảy ra hiện tượng loop trên sơ đồ chạy Distance – vector. Để hiểu rõ vấn đề, ta cùng quan sát tiếp ví dụ đã



nêu ở trên trong trường hợp mạng 192.168.3.0/24 bị down:

Hình 4. 24 Mạng 192.168.3.0/24 down

Như mô tả trên hình 7, khi mạng 192.168.3.0/24 down, R3 loại bỏ mạng này ra khỏi bảng định tuyến và xem như không biết thông tin gì về mạng này. Một thời gian ngắn sau, khi đến hạn, R2 lại gửi toàn bộ bảng định tuyến của nó qua cho R3. R3 tiếp nhận thông tin định tuyến mới và thấy rằng trong khôi thông tin mà R2 chuyển sang cho nó có mạng 192.168.3.0/24 mà nó không biết, R3 cập nhật thông tin này vào bảng định

192.168.3.0/24 S2/1 2
192.168.23.0/24 S2/1 0
192.168.12.0/24 S2/1 1
192.168.1.0/24 S2/1 2

tuyến của mình:

Hình 4. 25 Bảng định tuyến của R3

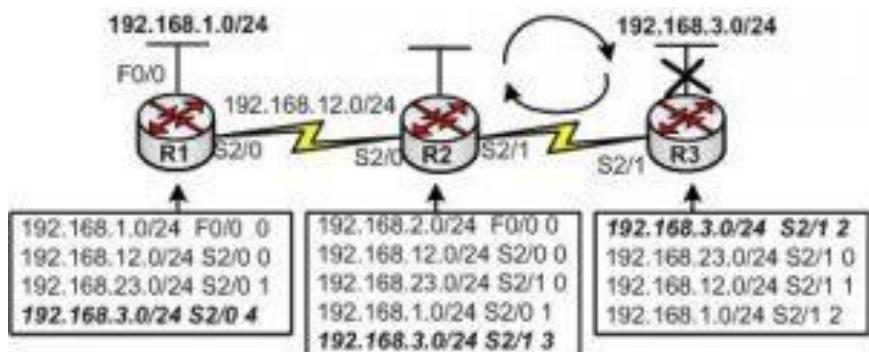
Ta thấy R3 đã cập nhật thông tin định tuyến một cách sai lầm và chỉ một đường hoàn toàn sai đến mạng 192.168.3.0/24 không còn tồn tại nữa! Chưa dừng lại ở đó, khi đến hạn, R3 lại tiếp tục gửi bảng định tuyến của nó sang cho R2. Khi R2 tiếp nhận thông tin từ R3, R2 thấy rằng thông tin mạng 192.168.3.0/24 mà nó học từ R3 trước đó đã có sự thay đổi về metric và nó cập nhật lại thông tin metric này:

192.168.2.0/24 F0/0 0
192.168.12.0/24 S2/0 0
192.168.23.0/24 S2/1 0
192.168.1.0/24 S2/0 1
192.168.3.0/24 S2/1 3

Hình 4. 26 Bảng định tuyến của R2

Cứ như thế R2 và R3 trao đổi thông tin định tuyến cho nhau và thông tin về metric của route 192.168.3.0/24 ngày một sai lệch – tăng lên sau mỗi lần trao đổi.

Khi một gói tin định đi đến mạng 192.168.3.0/24 đi đến R2, R2 sẽ tra bảng định tuyến rồi đẩy nó sang R3 theo cổng ra là S2/1 (xem hình 10). R3 khi tiếp nhận gói tin này lại tra bảng định tuyến rồi đẩy ngược lại R2, R2 khi nhận được lại đẩy trở lại về R3... Từ đó tạo nên một vòng loop trong vận chuyển gói tin.



Hình 4. 27 Loop trong định tuyến

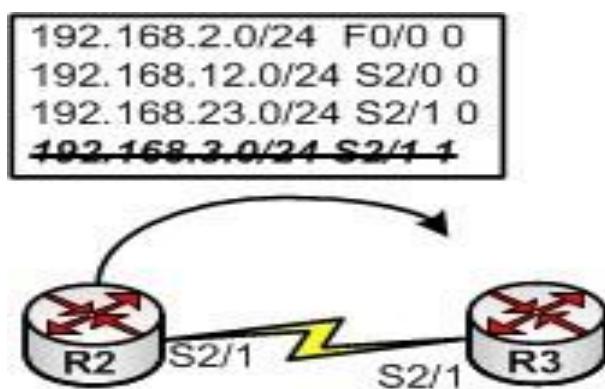
Các quy tắc chống loop

Để khắc phục hiện tượng này, RIP sử dụng một quy tắc chống loop gọi là quy tắc **Split – horizon**.

Luật Split – horizon:

Khi router nhận được cập nhật định tuyến của một mạng từ phía cổng nào thì nó không gửi ngược lại cập nhật cho mạng áy về phía cổng mà nó nhận được nữa.

Theo cách này, trở lại ví dụ trên, khi R2 đã nhận cập nhật định tuyến cho mạng 192.168.3.0/24 từ cổng S2/1 thì trong những lần gửi cập nhật định tuyến về phía cổng S2/1, nó sẽ loại ra không gửi thông tin 192.168.3.0/24 đi nữa. Từ đó R3 sẽ không nhận được thông tin định tuyến sai lệch khi mạng 192.168.3.0/24 của nó bị down.



Hình 4. 28 R2 sẽ không gửi ngược thông tin nó học được từ R3 về cho R3

Ngoài ra, khi xảy ra các sự cố down mạng như trên, RIP còn sử dụng thêm các quy tắc sau để thúc đẩy nhanh hơn tiến trình cập nhật định tuyến và hỗ trợ cho tiến trình chống loop:

Route – poisoning:

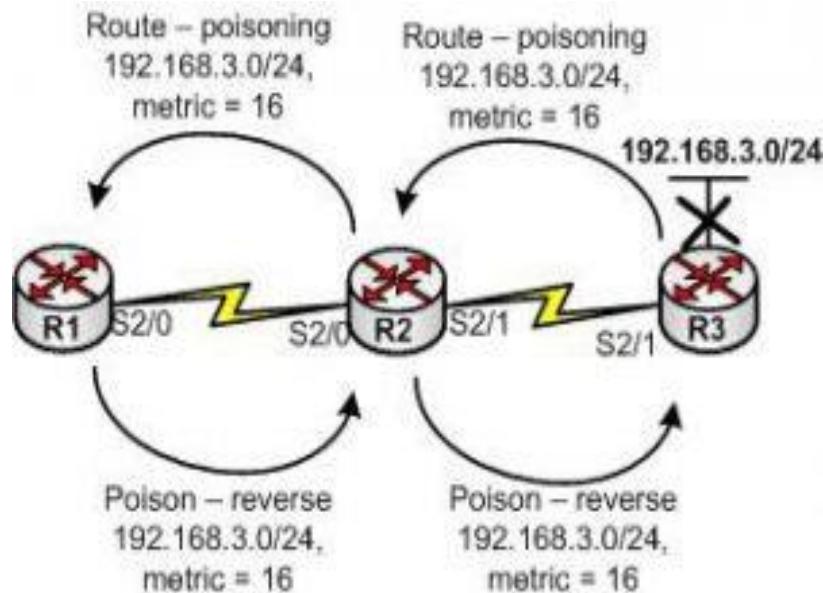
Khi một subnet kết nối trực tiếp chuyển sang down, router sẽ gửi đi một bản tin cập nhật cho subnet này có metric = 16 (infinity metric) cho láng giềng của nó. Router láng giềng khi nhận được bản tin này sẽ cập nhật được rằng subnet đã không còn nữa, đến lượt nó, nó lại tiếp tục phát ra một cập nhật định tuyến cho subnet này với metric = 16 cho láng giềng tiếp theo, cứ thế cả mạng sẽ nhanh chóng biết được subnet này không còn nữa. Việc phát ra bản tin cập nhật cho subnet down được thực hiện ngay lập tức mà không cần phải chờ tới hạn định kỳ (ta gọi việc này là *trigger update*).

Poison – reverse:

Khi router láng giềng nhận được bản tin update cho một subnet down có metric = 16 (infinity metric), nó cũng phải ngay lập tức hồi đáp về cho láng giềng một bản tin cập nhật cho subnet ấy cũng với metric = 16. Hoạt động này được gọi là *poison – reverse*.

Trigger – update:

Việc phát ra các bản tin Route – poisoning và Poison – reverse phải được thực hiện ngay lập tức mà không cần chờ tới hạn định kỳ gửi cập nhật định tuyến được gọi là hoạt động *trigger update*.

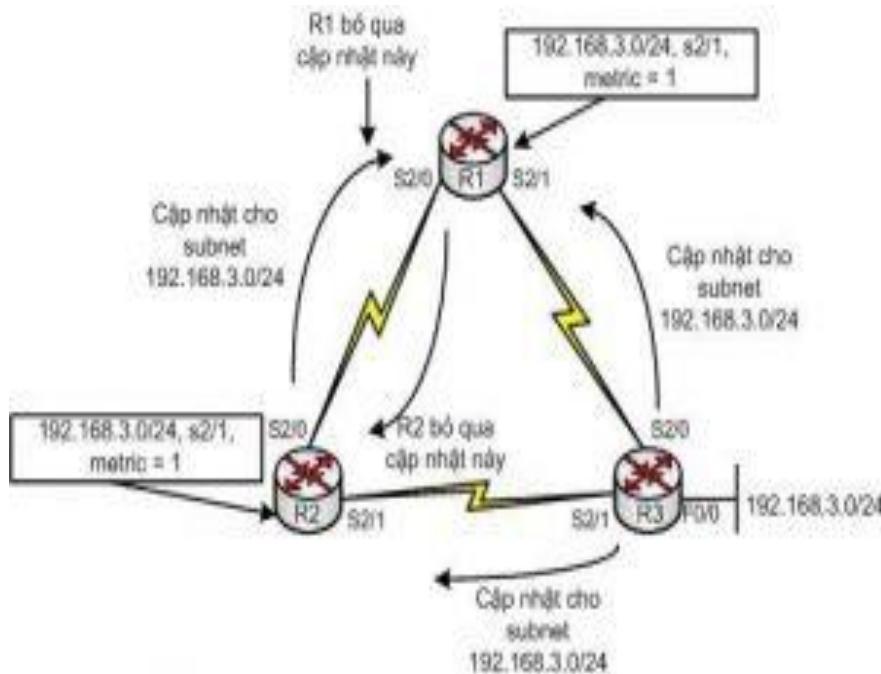


Hình 4. 29 Route poisoning và Poison reverse

Ngoài ra, để chống loop, RIP còn sử dụng một tiến trình đó là tiến trình holddown, sử dụng một bộ định thời gọi là holddown – timer.

Holddown timer:

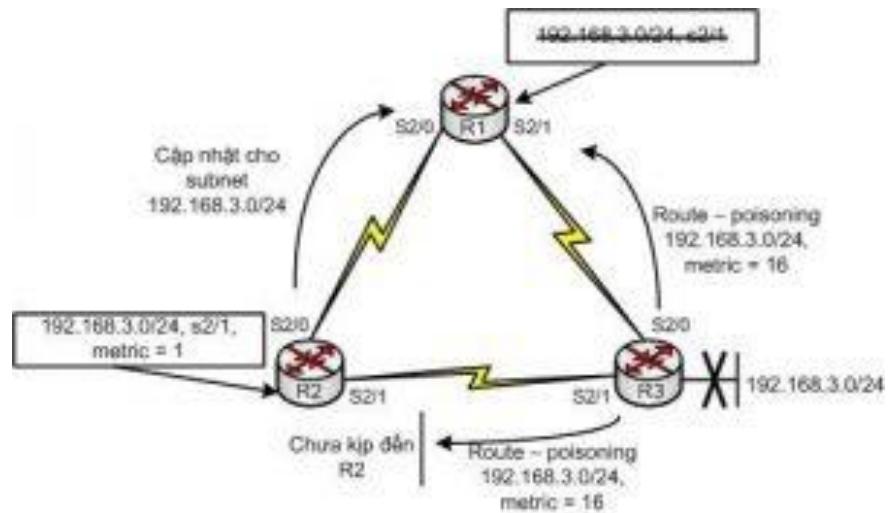
Ta cùng xem xét một trường hợp cho thấy rằng ngay cả khi *split – horizon* đã được bật, vẫn có thể xảy ra loop và lỗi tăng metric đến infinity. Sơ đồ ví dụ:



Hình 4. 30 Sơ đồ ví dụ 2

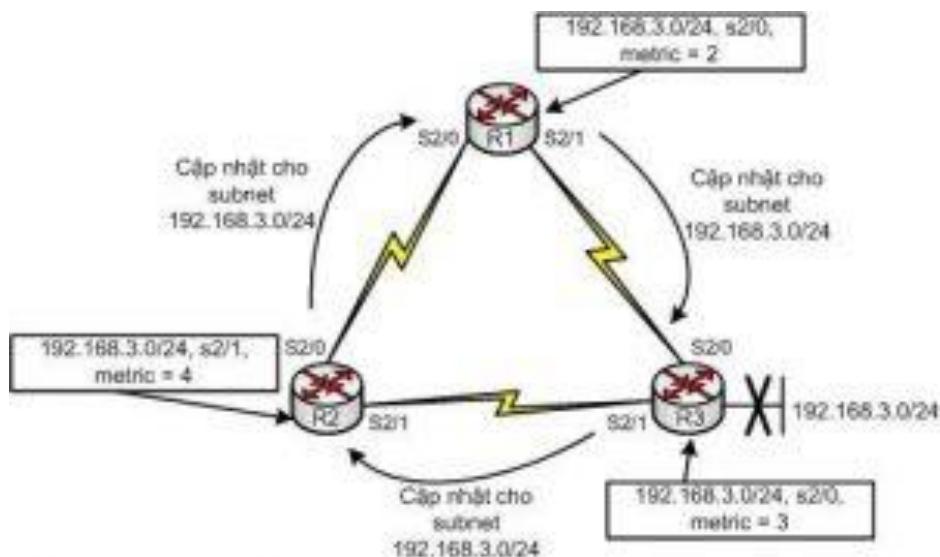
Như đã thảo luận trong ví dụ trước, trong trường hợp bình thường, khi bật RIP trên các router R1, R2 và R3, R3 sẽ gửi thông tin về mạng 192.168.3.0/24 của mình ra khỏi các cổng serial đầu nối đến R1 và R2 để R1 và R2 cập nhật thông tin về mạng 192.168.3.0/24 vào bảng định tuyến của mình như hình 13. Tuy nhiên, R1 và R2 đến lượt chúng cũng lại tiếp tục gửi cập nhật ra các cổng serial còn lại sang nhau nhưng R1 và R2 đều bỏ qua các cập nhật mạng 192.168.3.0/24 nhận được từ nhau vì metric của các cập nhật này lớn hơn metric trong cập nhật nhận được trực tiếp từ R3.

Khi mạng 192.168.3.0/24 trên cổng F0/0 của R3 chuyển sang down, như đã trình bày, R3 sẽ gửi các bản tin route – poisoning đến R1 và R2 với nội dung “192.168.3.0/24, metric = 16”. R1 và R2 sẽ cập nhật và biết được mạng 192.168.3.0/24 đã down, sau đó chúng tiếp tục gửi bản tin này cho láng giềng khác (gửi cho nhau). Tuy nhiên, một trường hợp có thể xảy ra đó là khi bản tin route – poisoning đã đi đến được R1, R1 kết luận mạng 192.168.3.0/24 down, nhưng bản tin này chưa đến kịp R2 (có thể do trễ) và đúng vào lúc đó R2 gửi cho R1 bản tin cập nhật như thường lệ về mạng 192.168.3.0/24 (R2 lúc này chưa biết mạng này đã down) (xem hình 4.31).



Hình 4. 31 Mạng 192.168.3.0/24 down

R1 khi nhận được bản tin cập nhật từ R2 lập tức cập nhật mạng 192.168.3.0/24 vào bảng định tuyến của nó vì lúc này nó đang ở trạng thái không biết mạng 192.168.3.0/24. Đến lượt nó, nó lại gửi tiếp cập nhật 192.168.3.0/24 cho R3, R3 lúc này cũng không biết mạng 192.168.3.0/24 nên lại cập nhật vào bảng định tuyến chỉ đường về R1. Sau đó R3 tiếp tục gửi cập nhật đi cho R2 và R2 lại cập nhật lại mạng 192.168.3.0/24 vào bảng định tuyến của nó chỉ đường đi về R3... Cứ như vậy, loop lại xảy ra (xem hình 4.32).



Hình 4. 32 Sơ đồ xảy ra loop

Các giao thức Distance – vector sử dụng holddown – timer để ngăn chặn việc xảy ra loop trong trường hợp như thế này.

Luật **Holddown timer**: Sau khi nhận được một poisoned route, router sẽ khởi động bộ định thời holddown – timer cho route này. Trước khi bộ timer này hết hạn, không tin

tưởng bất kỳ thông tin định tuyến nào về route down này, ngoại trừ thông tin đến từ chính lảng giềng đã cập nhật cho mình route này đầu tiên. Giá trị default của holddown – timer là 180s.

Như vậy theo luật này, khi R1 nhận được cập nhật route – poisoning từ R3 cho mạng 192.168.3.0/24 và kết luận rằng route này down, R1 sẽ không chấp nhận bất kỳ thông tin nào đến từ nguồn tin khác ngoại trừ R3 trong suốt khoảng thời gian holddown – timer. Nhờ đó thông tin route – poisoning cho mạng 192.168.3.0/24 được cập nhật kịp thời đến R2 và không còn gây ra loop nữa.

Các bộ timer

Bên cạnh các quy tắc chống loop đã đề cập ở trên, RIP còn sử dụng một số timer cho hoạt động của mình:

Update timer: khoảng thời gian định kỳ gửi bản tin cập nhật định tuyến ra khỏi các cổng chạy RIP, giá trị default là 30s.

Invalid timer: khi router đã nhận được cập nhật về một subnet nào đó mà sau khoảng thời gian *invalid timer* vẫn không nhận lại cập nhật về mạng này (mà đúng ra là phải nhận được 30s/lần), router sẽ coi route đi đến subnet này là invalid nhưng vẫn chưa xóa route này khỏi bảng định tuyến. Giá trị default của timer này là 180s.

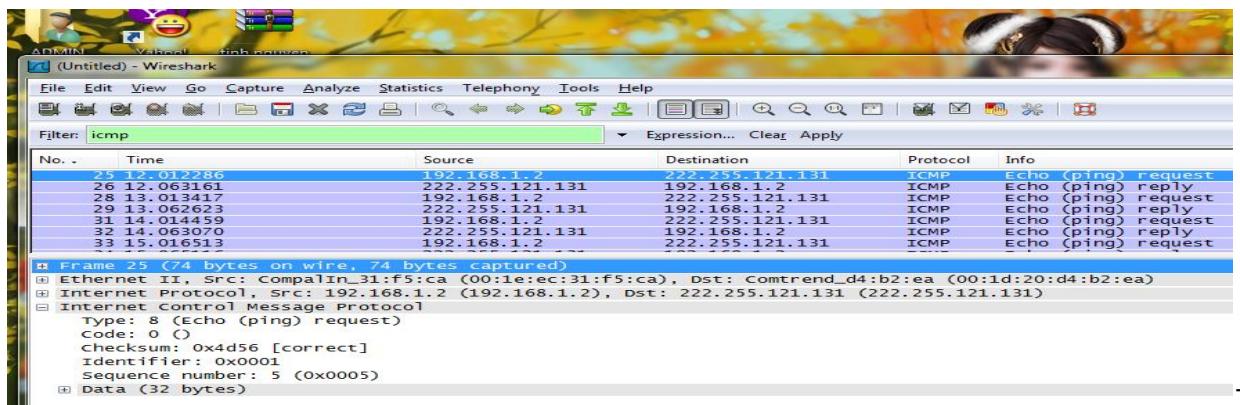
Flush timer: khi router đã nhận được cập nhật về một subnet nào đó mà sau khoảng thời gian *flush timer* vẫn không nhận lại cập nhật về mạng này (mà đúng ra là phải nhận được 30s/lần), router sẽ xóa bỏ hẳn route này khỏi bảng định tuyến. Giá trị default của timer này là 240s.

Như vậy, khi một route cho một subnet nào đó xuất hiện trong bảng định tuyến, router kỳ vọng rằng cứ 30s một lần route này phải được lảng giềng gửi lại cập nhật để “refresh”. Nếu sau 30s, route không được “refresh”, nó sẽ được theo dõi tiếp cho đến hết giây thứ 180 và bị đánh dấu invalid. Khi invalid, route vẫn còn được duy trì trong bảng định tuyến thêm 60s nữa (đến hết giây thứ 240) mới bị xóa hoàn toàn khỏi bảng định tuyến.

4.7. Tổng kết và bài tập ứng dụng

4.7.1. Wireshark Lab : ICMP

1. Địa chỉ IP của máy bạn ? Địa chỉ IP của máy đích ?



Địa chỉ IP máy trạm của tôi : 192.168.1.2
Địa chỉ IP máy trạm đích: 222.255.121.131

2. Tại sao 1 ICMP packet không có số hiệu cổng nguồn, đích?

ICMP là giao thức lớp 3 trong khi port number lại được sử dụng ở lớp 4

3. Khảo sát một gói tin yêu cầu được gửi trên máy của bạn. Cho biết giá trị của 2 thuộc tính Type và Code của gói tin ICMP? Và các thuộc tính khác như Checksum, sequence và identifier

Type 8

Code 0

Checksum: 0x4d56

Identifier: 0x0001

Sequence number: 5 (0x0005)

4. Khảo sát một gói tin reply yêu cầu. Cho biết giá trị của 2 thuộc tính Type và Code của gói tin ICMP? Và các thuộc tính khác như Checksum, sequence và identifier

Time	Source	Destination	Protocol	Info
25 12.012286	192.168.1.2	222.255.121.131	ICMP	Echo (ping) request
26 12.063161	222.255.121.131	192.168.1.2	ICMP	Echo (ping) reply
28 13.013417	192.168.1.2	222.255.121.131	ICMP	Echo (ping) request
29 13.062623	222.255.121.131	192.168.1.2	ICMP	Echo (ping) reply
31 14.014459	192.168.1.2	222.255.121.131	ICMP	Echo (ping) request
32 14.063070	222.255.121.131	192.168.1.2	ICMP	Echo (ping) reply
33 15.016513	192.168.1.2	222.255.121.131	ICMP	Echo (ping) request

Frame 26 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: Comtrend_d4:b2:ea (00:1d:20:d4:b2:ea), Dst: Compaq_31:f5:ca (00:1e:ec:31:f5:ca)
Internet Protocol, Src: 222.255.121.131 (222.255.121.131), Dst: 192.168.1.2 (192.168.1.2)
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0 ()
Checksum: 0x5556 [correct]
Identifier: 0x0001
Sequence number: 5 (0x0005)
Data (32 bytes)

Type : 0

Code: 0 ()

Cheksum: 0x5556

Identifier: 0x0001

Sequence number: 5

5. What is the IP address of your host? What is the IP address of the target destination host?

IP address of your host 192.168.1.2

the IP address of the target destination host 222.255.121.131

6. Nếu ICMP gửi gói tin UDP thay thế (as in Unix/Linux), thì IP protocol number có còn là 01 đối với các gói tin ko? Nếu ko thì nó sẽ là bao nhiêu?

Không, ICMP sẽ gửi packet có port 0x01(17)

7. Khảo sát ICMP echo packet trên máy của bạn. Có gì khác biệt giữa các thành phần so với ICMP ping query packets ở nửa đầu bài lab ko? Nếu có thì khác ở điểm nào?

Không có gì khác biệt

8. Khảo sát gói tin ICMP error. Nó có thêm thuộc tính nào so với gói tin ICMP echo. Nó bao gồm những thuộc tính gì?

```
Frame 19 (134 bytes on wire, 134 bytes captured)
Ethernet II, Src: Comtrend_d4:b2:ea (00:1d:20:d4:b2:ea), Dst: CompaIn_31:f5:ca (00:1e:ec:31:f5:ca)
Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.2 (192.168.1.2)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0xc0 (DSCP 0x30: class selector 6; ECN: 0x00)
        Total Length: 120
        Identification: 0x3299 (12953)
    Flags: 0x00
        Fragment offset: 0
        Time to live: 64
        Protocol: ICMP (0x01)
    Header checksum: 0xc3d8 [correct]
        Source: 192.168.1.1 (192.168.1.1)
        Destination: 192.168.1.2 (192.168.1.2)
Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ff [correct]
Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 222.255.121.131 (222.255.121.131)
Internet Control Message Protocol

0000  00 1e ec 31 f5 ca 00 1d 20 d4 b2 ea 08 00 45 c0  .1.....E.
0010  00 78 32 99 00 00 40 01 c3 d8 c0 a8 01 01 c0 a8  .x2...@. .....
0020  01 02 0b 00 f4 ff 00 00 00 00 45 00 00 5c 6a f3  .....E..\\j.
0030  00 00 01 01 34 81 c0 a8 01 02 de ff 79 83 08 00  ....4....y...
0040  f7 ef 00 01 00 0f 00 00 00 00 00 00 00 00 00 00 00  ......

0000  00 1e ec 31 f5 ca 00 1d 20 d4 b2 ea 08 00 45 c0  .1.....E.
0010  00 78 32 99 00 00 40 01 c3 d8 c0 a8 01 01 c0 a8  .x2...@. .....
0020  01 02 0b 00 f4 ff 00 00 00 00 45 00 00 5c 6a f3  .....E..\\j.
0030  00 00 01 01 34 81 c0 a8 01 02 de ff 79 83 08 00  ....4....y...
0040  f7 ef 00 01 00 0f 00 00 00 00 00 00 00 00 00 00 00  .....
```

Điểm khác biệt là

Type: 11

Code: 0

Ko có thuộc tính Identifier

9. Khảo sát gói tin ICMP error. Nó có thêm thuộc tính nào so với gói tin ICMP echo. Nó bao gồm những thuộc tính gì?

```
Frame 19 (134 bytes on wire, 134 bytes captured)
Ethernet II, Src: Comtrend_d4:b2:ea (00:1d:20:d4:b2:ea), Dst: CompaIn_31:f5:ca (00:1e:ec:31:f5:ca)
Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.2 (192.168.1.2)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0xc0 (DSCP 0x30: class selector 6; ECN: 0x00)
        Total Length: 120
        Identification: 0x3299 (12953)
    Flags: 0x00
        Fragment offset: 0
        Time to live: 64
        Protocol: ICMP (0x01)
    Header checksum: 0xc3d8 [correct]
        Source: 192.168.1.1 (192.168.1.1)
        Destination: 192.168.1.2 (192.168.1.2)
Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ff [correct]
Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 222.255.121.131 (222.255.121.131)
Internet Control Message Protocol

0000  00 1e ec 31 f5 ca 00 1d 20 d4 b2 ea 08 00 45 c0  .1.....E.
0010  00 78 32 99 00 00 40 01 c3 d8 c0 a8 01 01 c0 a8  .x2...@. .....
0020  01 02 0b 00 f4 ff 00 00 00 00 45 00 00 5c 6a f3  .....E..\\j.
0030  00 00 01 01 34 81 c0 a8 01 02 de ff 79 83 08 00  ....4....y...
0040  f7 ef 00 01 00 0f 00 00 00 00 00 00 00 00 00 00 00  ......

0000  00 1e ec 31 f5 ca 00 1d 20 d4 b2 ea 08 00 45 c0  .1.....E.
0010  00 78 32 99 00 00 40 01 c3 d8 c0 a8 01 01 c0 a8  .x2...@. .....
0020  01 02 0b 00 f4 ff 00 00 00 00 45 00 00 5c 6a f3  .....E..\\j.
0030  00 00 01 01 34 81 c0 a8 01 02 de ff 79 83 08 00  ....4....y...
0040  f7 ef 00 01 00 0f 00 00 00 00 00 00 00 00 00 00 00  .....
```

Điểm khác biệt là

Type: 11

Code: 0

Ko có thuộc tính Identifier

Khảo sát 3 gói tin ICMP cuối cùng nhận được bởi host nguồn. Những gói tin này có gì khác biệt so với gói tin ICMP error? Tại sao chúng lại khác nhau?

1171 58.744827	192.168.1.2	222.255.121.131	ICMP	Echo (ping) request
1172 58.794535	203.162.185.218	192.168.1.2	ICMP	Time-to-live exceeded (1)
1219 64.247857	192.168.1.2	222.255.121.131	ICMP	Echo (ping) request
1220 64.296635	222.255.121.131	192.168.1.2	ICMP	Echo (ping) reply
1221 64.297551	192.168.1.2	222.255.121.131	ICMP	Echo (ping) request
1222 64.346337	222.255.121.131	192.168.1.2	ICMP	Echo (ping) reply
1223 64.347246	192.168.1.2	222.255.121.131	ICMP	Echo (ping) request
1224 64.395142	222.255.121.131	192.168.1.2	ICMP	Echo (ping) reply

Frame 19 (134 bytes on wire, 134 bytes captured)
Ethernet II. Src: Comtrend d4:b2:ea (00:1d:20:d4:b2:ea). Dst: CombalIn 31:f5:ca (00:1e:ec:31:f5:ca)

0000 00 1e ec 31 f5 ca 00 1d 20 d4 b2 ea 08 00 45 c0 ..1....E.
0010 00 78 32 99 00 00 40 01 c3 d8 c0 a8 01 01 c0 a8 .x2...@.
0020 01 02 0b 00 f4 ff 00 00 00 00 45 00 00 5c 6a f3E..\\j.
0030 00 00 01 01 34 81 c0 a8 01 02 de ff 79 83 08 004....y....
0040 f7 ef 00 01 00 0f 00 00 00 00 00 00 00 00 00 00
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Đó là 3 gói tin ICMP reply

10. Khi thực hiện lệnh tracert ta thấy có 1 số link có độ trễ lớn hơn các link khác, cho biết đó là link nào? Dự đoán xem nguyên nhân là tại sao?

Ví dụ như khi ta thực hiện lệnh tracert www.inria.fr có kết quả như sau:

```
Administrator: C:\Windows\system32\cmd.exe
 12  401 ms   393 ms   396 ms  ae-64-64.csw1.Washington1.Level3.net [4.69.134.1]
 78] 
 13  381 ms   383 ms   384 ms  ae-62-62.ebr2.Washington1.Level3.net [4.69.134.1]
45] 
 14    *      416 ms   414 ms  ae-42-42.ebr2.Frankfurt1.Level3.net [4.69.137.53]
] 
 15    *      432 ms   407 ms  ae-82-82.csw3.Frankfurt1.Level3.net [4.69.140.26]
] 
 16  398 ms   417 ms   424 ms  ae-81-81.ebr1.Frankfurt1.Level3.net [4.69.140.91]
 17  474 ms   476 ms   487 ms  ae-47-47.ebr2.Paris1.Level3.net [4.69.143.142]
 18  482 ms   477 ms   481 ms  ae-2-52.edge5.Paris1.Level3.net [4.69.139.235]
 19  493 ms   489 ms   489 ms  RENATER.edge5.Paris1.Level3.net [212.73.207.174]
 20  497 ms   493 ms   495 ms  te1-1-marseille-rtr-021.noc.renater.fr [193.51.1
89.18]
 21  486 ms   475 ms   475 ms  te1-2-nice-rtr-021.noc.renater.fr [193.51.189.26]
] 
 22  484 ms   485 ms   484 ms  inria-gi8-2-nice-rtr-021.noc.renater.fr [193.51.
181.137]
 23  500 ms   496 ms   505 ms  www.inria.fr [138.96.146.2]

Trace complete.

C:\Users\ADMIN>
```

Để trả lời câu hỏi 10 ta sẽ xem lại 1 số quy tắc đọc kết quả từ lệnh tracert

Dòng 1: là dòng kết nối giữa modem và máy tính, độ trễ tốt nhất là 1ms 1ms 1ms! Nếu cao hơn hoặc xuất hiện dấu * hay Request timed out thì kết nối modem và máy có vấn đề!

Dòng 2: là kết nối giữa modem và mạng của ISP (nhà cung cấp mạng), độ trễ tốt nhất nằm trong khoảng 10-40 ms! Cao hơn khoảng này hoặc xuất hiện dấu * hay Request timed out thì kết nối modem và mạng ISP có vấn đề !

Dòng 3 trả đi tới trace complete: là kết nối trong mạng giữa các ISP với nhau , nếu xuất hiện dấu * hay Request timed out thì kết nối trong mạng ISP có vấn đề !

Dựa vào đó ta thấy từ hop thứ 13 đến 23 độ trễ tăng rất cao đặc biệt co hop còn bị request timed out, nguyên nhân có thể là do kết nối trong mạng giữa các ISP với nhau, hoặc do số lượng truy cập quá đông, đứt cáp, nhiệt độ hay khí hậu (lưu ý là từ dòng thứ 3 trả đi ta không thể có cách khắc phục độ trễ)

4.7.2 Wireshark Lab : IP

1. Địa chỉ IP máy tính của bạn là gì ?
Địa chỉ IP máy tính của tôi là : 192.168.1.4
2. Trong gói IP packet header, trường giá trị nào thuộc về giao thức lớp trên?
Đó là trường : ICMP(0x01)
3. Kích cỡ của IP header ? Kích cỡ của IP datagram ở trong payload ? Giải thích tại sao lại xác định được những giá trị đó?
$$\text{IP header} = \text{Total Length} - \text{Header Length} = 56 - 20 = 36$$
.
payload of the IP datagram is 0 bytes bởi vì trường Flags : 0x00 .
4. IP datagram có bị phân mảnh ko ? Giải thích tại sao lại ?
IP datagram ko bị phân mảnh . Vì flags=0 và offset=0;
5. Những trường giá trị nào luôn thay đổi trong IP datagram...?

Trả lời:

1. Identification
 2. Time to live (TTL)
 3. Checksum
6. Những giá trị nào là hằng số ? Những giá trị nào phải thay đổi ? Tại sao

Những trường giá trị là hằng số:

1. Version
 2. Header length
 3. Flag
 4. Fragment offset
 5. Protocol
 6. Source
 7. Destination Checksum phải thay đổi vì checksum phụ thuộc vào TTL và ID.
7. Giới thiệu qua về những gì bạn nhìn thấy ở trường identification của IP datagram
Identification : unique IP datagram value. Có độ dài là 16 bits

8. Giá trị của Identification và TTL?

Trả lời:

Identification: 0x117b(4475)

Time to live: 1

9. Giá trị ICMP TTL-exceeded replies gửi tới máy nguồn từ các router gần nhất (first hop) có thay đổi được ko? Vì sao?

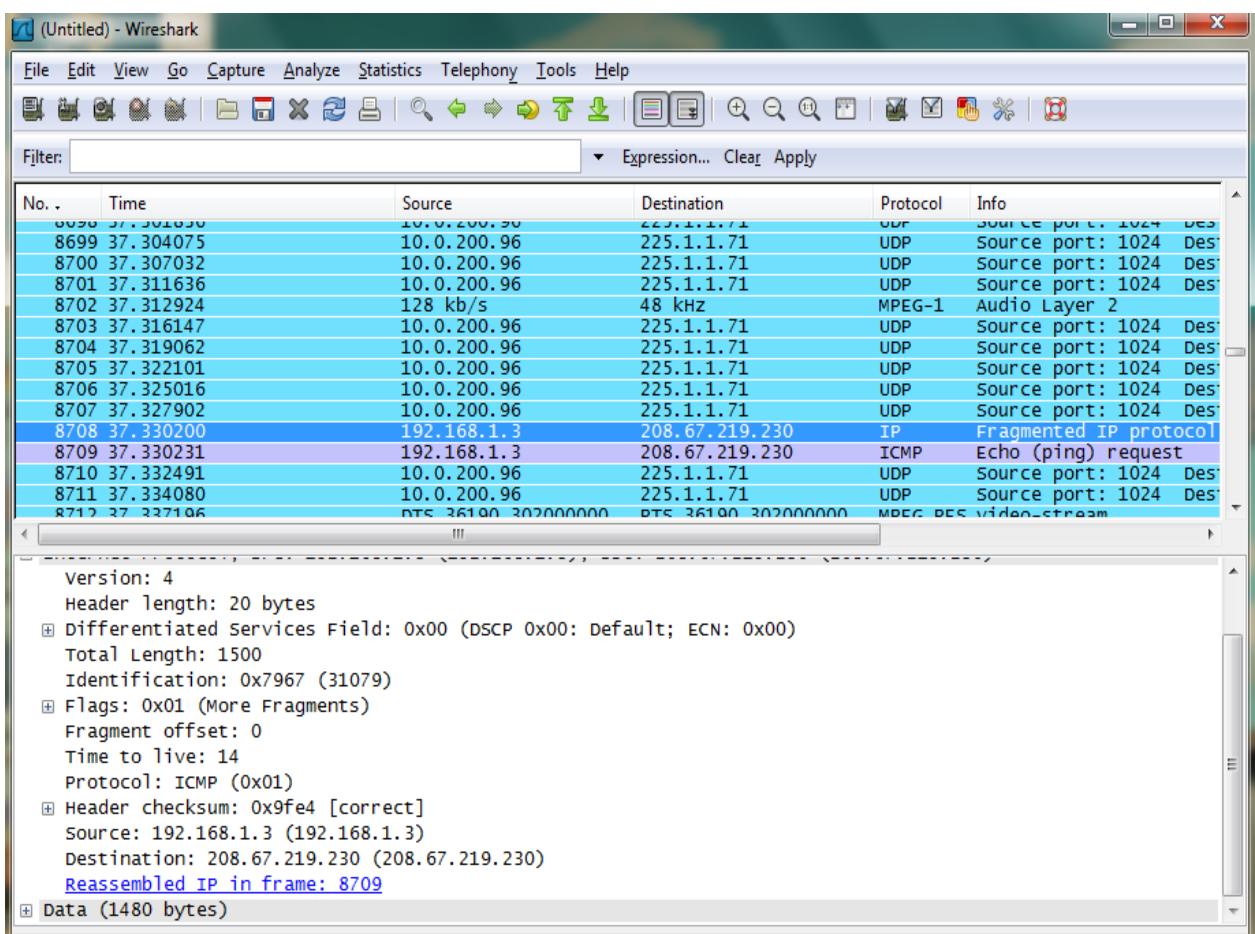
Trả lời:

Giá trị ICMP TTL-exceeded replies gửi tới máy nguồn từ các router gần nhất (first hop) ko được thay đổi vì giá trị TTL đối với router ở hop đầu tiên là duy nhất. TTL phụ thuộc vào hệ điều hành và số lượng các hop.

10. Tìm đến gói tin request echo ICMP đầu tiên sau khi bạn thay đổi giá trị của Packet trong chương trình pinglotter lên 2000. Gói tin này có bị phân mảnh thành nhiều IP datagram ko?

Trả lời:

Theo hình vẽ gói tin có bị phân mảnh thành các IP datagram.



11. Trường thông tin nào ở trong IP header cho thấy rằng gói dữ liệu có bị phân mảnh hay ko? Và trường thông tin nào cho thấy đó có phải là fragment đầu tiên hay ko? Kích cỡ của IP datagram?

8707 37.327902	10.0.200.96	225.1.1.71
8708 37.330200	192.168.1.3	208.67.219.230
8709 37.330231	192.168.1.3	208.67.219.230
8710 37.332491	10.0.200.96	225.1.1.71
8711 37.334080	10.0.200.96	225.1.1.71
8712 37.337196	DTS 36190 3020000000	DTS 36190 3020000000

Header Length: 20 bytes

- + Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
- + Total Length: 1500
- + Identification: 0x7967 (31079)
- Flags: 0x01 (More Fragments)
 - 0.. = Reserved bit: Not Set
 - .0. = Don't fragment: Not Set
 - .1 = More fragments: Set
- + Fragment offset: 0
- + Time to live: 14
- + Protocol: ICMP (0x01)
- + Header checksum: 0x9fe4 [correct]
- + Source: 192.168.1.3 (192.168.1.3)
- + Destination: 208.67.219.230 (208.67.219.230)

Giá trị flags chứng tỏ rằng gói dữ liệu được phân mảnh. Nếu đó là fragment đầu tiên thì fegment offset thiết lập bằng 0. kích cỡ của gói dữ liệu IP là 1500 (bytes)

12. Thông tin nào ở trong IP header cho thấy đó ko phải là datagram fragment đầu tiên? Nó có bị phân mảnh nữa ko? Giải thích?

The Fragment offset = 1480 vì thế nó không phải datagram fragment đầu tiên. Nó sẽ ko phân mảnh nữa vì Flags = 0x00

- 0..= Reserved bit: Not set
- .0. = Don't fragment: Not set
- .0 = More fragments: Not set

8707 37.327902	10.0.200.96	225.1.1.71
8708 37.330200	192.168.1.3	208.67.219.230
8709 37.330231	192.168.1.3	208.67.219.230
8710 37.332491	10.0.200.96	225.1.1.71
8711 37.334080	10.0.200.96	225.1.1.71
8712 37.337196	DTS 36190 3020000000	DTS 36190 3020000000

Header Length: 20 bytes

- Flags: 0x00
 - 0.. = Reserved bit: Not Set
 - .0. = Don't fragment: Not Set
 - .0 = More fragments: Not Set
- + Fragment offset: 1480
- + Time to live: 14
- + Protocol: ICMP (0x01)
- + Header checksum: 0xc2ff [correct]
- + Source: 192.168.1.3 (192.168.1.3)
- + Destination: 208.67.219.230 (208.67.219.230)
- [IP Fragments (1980 bytes): #8708(1480), #8709(500)]
 - [Frame: 8708, payload: 0-1479 (1480 bytes)]
 - [Frame: 8709, payload: 1480-1979 (500 bytes)]

+ Internet Control Message Protocol

0000 00 1d 20 d4 b2 ea 00 1e ec 31 f5 ca 08 00 45 00 1....E.
0010 02 08 79 67 00 b9 0e 01 c2 ff c0 a8 01 03 d0 43	:yg.....C
0020 db e6 6e 64 61 72 64 33 2e 33 30 2e 31 73 30 45	ndard3 .30.is0E

Frame (534 bytes) Reassembled IPv4 (1980 bytes)

Frame (frame), 534 bytes Packets:

13. Giá trị nào thay đổi trong IP header giữa fragment đầu tiên và thứ hai ?

Trả lời

- 1.Total length
- 2.Flag
- 3.Fragment offset
- 4.Checksum

14. Có bao nhiêu fragments được tạo ra từ datagram đầu tiên ?

Quan sát wireshark ta thấy có 3 gói tin có fragment offset =0

=> Có 3 gói packet được tạo từ datagram gốc

393 26.361402	192.168.1.3	70.85.12.146	TCP	60802 > http [ACK] Seq
394 26.366714	192.168.1.3	208.67.219.230	IP	Fragmented IP protocol
395 26.366715	192.168.1.3	208.67.219.230	IP	Fragmented IP protocol
396 26.366751	192.168.1.3	208.67.219.230	IP	Fragmented IP protocol
397 26.366755	192.168.1.3	208.67.219.230	IP	Fragmented IP protocol
398 26.366771	192.168.1.3	208.67.219.230	ICMP	Echo (ping) request
399 26.366792	192.168.1.3	208.67.219.230	ICMP	Echo (ping) request
400 26.366941	192.168.1.3	208.67.219.230	IP	Fragmented IP protocol
401 26.366961	192.168.1.3	208.67.219.230	IP	Fragmented IP protocol
402 26.366976	192.168.1.3	208.67.219.230	ICMP	Echo (ping) request
403 26.367113	192.168.1.3	208.67.219.230	IP	Fragmented IP protocol
404 26.367134	192.168.1.3	208.67.219.230	IP	Fragmented IP protocol
405 26.367147	192.168.1.3	208.67.219.230	ICMP	Echo (ping) request

Frame 394 (1514 bytes on wire, 1514 bytes captured)

Ethernet II, Src: CompaqIn_31:f5:ca (00:1e:ec:31:f5:ca), Dst: Comtrend_d4:b2:ea (00:1d:20:d4:b2:ea)

Internet Protocol, Src: 192.168.1.3 (192.168.1.3), Dst: 208.67.219.230 (208.67.219.230)

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

Total Length: 1500

Identification: 0x31b5 (12725)

Flags: 0x01 (More Fragments)

- 0.. = Reserved bit: Not Set
- .0. = Don't fragment: Not Set
- ..1 = More fragments: Set

Fragment offset: 0

Time to live: 2

394	26.366/14	192.168.1.3
395	26.366/15	192.168.1.3
396	26.366/151	192.168.1.3
397	26.366/155	192.168.1.3
398	26.366/171	192.168.1.3
399	26.366/192	192.168.1.3
400	26.366/941	192.168.1.3
401	26.366/961	192.168.1.3
402	26.366/976	192.168.1.3
403	26.367/113	192.168.1.3
404	26.367/134	192.168.1.3
405	26.367/147	192.168.1.3

◀
▶

☰

[+] Frame 395 (1514 bytes on wire, 1514 bytes captured)
[+] Ethernet II, Src: CompaqIn_31:f5:ca (00:1e:ec:31:f5:c)
[+] Internet Protocol, Src: 192.168.1.3 (192.168.1.3), Ds
 Version: 4
 Header Length: 20 bytes
[+] Differentiated Services Field: 0x00 (DSCP 0x00: Def
 Total Length: 1500
 Identification: 0x31b4 (12724)
[+] Flags: 0x01 (More Fragments)
 0.. = Reserved bit: Not Set
 .0. = Don't fragment: Not Set
 ..1 = More fragments: Set
 Fragment offset: 0
[+] Time to live: 2

394	26.366714	192.168.1.3
395	26.366715	192.168.1.3
396	26.366751	192.168.1.3
397	26.366755	192.168.1.3
398	26.366771	192.168.1.3
399	26.366792	192.168.1.3
400	26.366941	192.168.1.3
401	26.366961	192.168.1.3
402	26.366976	192.168.1.3
403	26.367113	192.168.1.3
404	26.367134	192.168.1.3
405	26.367147	192.168.1.3

Frame 400 (1514 bytes on wire, 1514 bytes captured)
 Ethernet II, Src: CompaqIn_31:f5:ca (00:1e:ec:31:f5:ca)
 Internet Protocol, Src: 192.168.1.3 (192.168.1.3), Dst:
 Version: 4
 Header length: 20 bytes
 Differentiated Services Field: 0x00 (DSCP 0x00: Default)
 Total Length: 1500
 Identification: 0x31b6 (12726)
 Flags: 0x01 (More Fragments)
 0.. = Reserved bit: Not Set
 .0. = Don't fragment: Not Set
 ..1 = More fragments: Set
 Fragment offset: 0
 Time to live: 1
 Protocol: TCP (0x06)
 Source: 192.168.1.3
 Destination: 192.168.1.3
 0000 00 1d 20 d4 b2 ea 00 1e ec 31 f5 ca 08 00 45 00 .
 0010 05 dc 31 b6 20 00 01 01 f4 95 c0 a8 01 03 d0 43 .

15. Những giá trị nào thay đổi trong IP header giữa các fragment ?

Trả lời:

- 1.Total length
- 2.Flag
- 3.Fragment offset
- 4.Checksum

TÓM TẮT NỘI DUNG CỐT LÕI.

- Vai trò chúc năng tầng mạng.
- Dịch vụ cung cấp cho tầng mạng.
- Tổ chức các kênh truyền tin trong mạng.
- Các kỹ thuật định tuyến.
- Vấn đề tắc nghẽn mạng.

BÀI TẬP ÚNG DỤNG:

Câu 1. Byte đầu tiên của một địa chỉ IP có dạng: 11000001. Vậy nó thuộc lớp nào

- A. Lớp A B. Lớp B C. Lớp C D. B Lớp D

Câu 2. Cấu trúc khuôn dạng của IP lớp B là

- A. Bit 1-2: 10, bit 3 - 16: NetID, bit 17-32: HostID
- B. Bit 1-2: 11, bit 3-16: NetID, bit 17-32: HostID
- C. Bit 1: 0, bit 2-16: NetID, bit 17-32: HostID
- D. Bit 1-2: 11, bit 3-8: NetID, 9-32: HostID

Câu 3. Mạng Internet là

- A. Mạng máy tính toàn cầu
- B. Mạng của các máy tính toàn cầu kết nối lại với nhau theo giao thức TCP/IP
- C. Mạng diện rộng
- D. Mạng của các mạng con kết nối lại với nhau

Câu 4. Địa chỉ IP nào dưới đây là hợp lệ

- A. 192.168.10.132
- B. 192.0.0.0
- C. 192.255.255.255
- D. Tất cả đều sai

Câu 5. Địa chỉ IP nào sau đây là địa chỉ quảng bá cho một mạng bất kỳ

- A. 10.255.255.255
- B. 172.16.255.255
- C. 255.255.255.255
- D. 230.20.30.255

Câu 6. Xác định subnet mask để 2 IP 172.16.1.2 và 172.16.3.1 cùng mạng

- A. 255.255.240.0
- B. 255.255.0.0
- C. 255.255.255.0
- D. 255.255.254.0

Câu 7. Một mạng con lớp A cần chứa tối thiểu 255 host sử dụng subnet mask nào sau đây

- A. 255.255.255.240
- B. 255.255.255.192
- C. 255.255.254.0
- D. 255.0.0.255

Câu 8. Địa chỉ ip 169.254.0.0 với subnet mask 255.255.0.0 được gọi là

- A. Địa chỉ mạng
- B. Không phải là địa chỉ IP
- C. Địa chỉ broadcast
- D. Địa chỉ host

Câu 9. Địa chỉ 129.219.255.255 là địa chỉ gì

- A. Broadcast lớp A
- B. Broadcast lớp B
- C. Host lớp A
- D. Host lớp B

Câu 10. Địa chỉ 29.219.255.255 là địa chỉ gì

- A. Host lớp A
- B. Host lớp B
- C. Broadcast lớp A
- D. Broadcast lớp B

Chương 5. TẦNG GIAO VẬN

Mục tiêu:

- Hiểu về vai trò chức năng tầng giao vận
- Hiểu về các dịch vụ cung cấp cho tầng Session
- Đảm bảo chất lượng dịch vụ đường truyền dữ liệu
- Các lớp giao thức của tầng giao vận.
- So sánh chế độ truyền đồng bộ và không đồng bộ.

5.1. Giới thiệu và các dịch vụ tầng Giao vận

Vai trò & chức năng.

Là lớp cao nhất có liên quan đến các giao thức trao đổi dữ liệu giữa các hệ thống mở, kiểm soát việc truyền dữ liệu từ Host tới Host (End-to-End). Thủ tục trong 3 lớp dưới (vật lý, liên kết dữ liệu và mạng) chỉ phục vụ việc truyền dữ liệu giữa các lớp kề nhau trong cùng hệ thống. Các thực thể đồng lớp hội thoại, thương lượng với nhau trong quá trình truyền dữ liệu.

Tầng Vận chuyển thực hiện việc chia các gói tin lớn thành các gói tin nhỏ hơn trước khi gửi đi và đánh số các gói tin và đảm bảo chúng chuyển theo đúng thứ tự. Là lớp cuối cùng chịu trách nhiệm về mức độ an toàn trong truyền dữ liệu nên giao thức Tầng Vận chuyển phụ thuộc nhiều vào bản chất của lớp mạng. Tầng Vận chuyển có thể thực hiện việc ghép kênh (multiplex) một vài liên kết vào cùng một liên kết nối để giảm giá thành.

5.1.1. Các giao thức chuẩn cho Tầng Vận chuyển

Trên cơ sở loại giao thức lớp mạng chúng ta có 5 lớp giao thức Tầng Vận chuyển đó là:

- Giao thức lớp 0 (Simple Class - lớp đơn giản): cung cấp các khả năng rất đơn giản để thiết lập liên kết, truyền dữ liệu và hủy bỏ liên kết trên mạng "có liên kết" loại A. Nó có khả năng phát hiện và báo hiệu các lỗi nhưng không có khả năng phục hồi.
- Giao thức lớp 1 (Basic Error Recovery Class - Lớp phục hồi lỗi cơ bản) dùng với các loại mạng B, ở đây các gói tin (TPDU) được đánh số. Ngoài ra giao thức còn có khả năng báo nhận cho nơi gửi và truyền dữ liệu khẩn. So với giao thức lớp 0 giao thức lớp 1 có thêm khả năng phục hồi lỗi.
- Giao thức lớp 2 (Multiplexing Class - lớp dồn kênh) là một cải tiến của lớp 0 cho phép dồn một số liên kết chuyển vận vào một liên kết mạng duy nhất, đồng thời có thể kiểm soát luồng dữ liệu để tránh tắc nghẽn. Giao thức lớp 2 không có khả năng phát hiện và phục hồi lỗi. Do vậy nó cần đặt trên một lớp mạng loại A.
- Giao thức lớp 3 (Error Recovery and Multiplexing Class - lớp phục hồi lỗi cơ bản và dồn kênh) là sự mở rộng giao thức lớp 2 với khả năng phát hiện và phục hồi lỗi, nó cần đặt trên một lớp mạng loại B.

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

5.2. Các giao thức đa truy cập

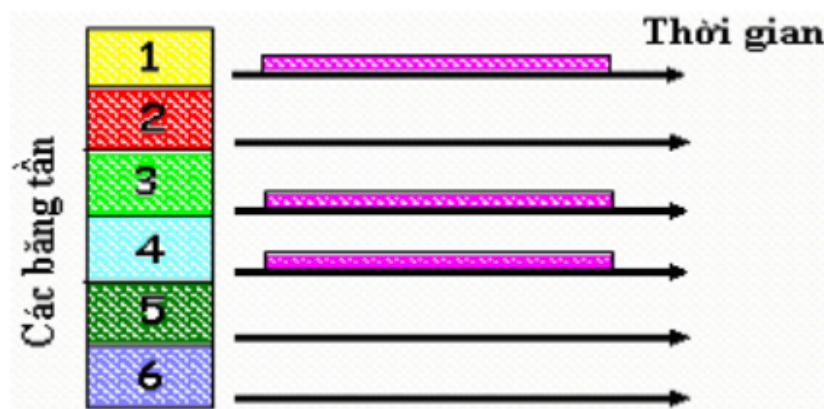
5.2.1. Phương pháp chia kênh

Ý tưởng chung của phương pháp này là: đường truyền sẽ được chia thành nhiều kênh truyền, mỗi kênh truyền sẽ được cấp phát riêng cho một trạm. Có ba phương pháp chia kênh chính: FDMA, TDMA, CDMA.

5.2.1.1 Chia tần số (FDMA – Frequency Division Multiple Access)

Một phương thức truyền thống để chia sẻ một kênh truyền đơn cho nhiều người dùng cạnh tranh là Chia tần số (FDMA). Phổ của kênh truyền được chia thành nhiều băng tần (frequency bands) khác nhau. Mỗi trạm được gán cho một băng tần cố định. Những trạm nào được cấp băng tần mà không có dữ liệu để truyền thì ở trong trạng thái nhàn rỗi (idle).

Ví dụ: Một mạng LAN có sáu trạm, các trạm 1, 3, 4 có dữ liệu cần truyền, các trạm 2, 5, 6 nhàn rỗi.



Hình 5.1 Ví dụ về FDMA

Nhận xét:

Do mỗi người dùng được cấp một băng tần riêng, nên không có sự đụng độ xảy ra. Khi chỉ có số lượng người dùng nhỏ và ổn định, mỗi người dùng cần giao tiếp nhiều thì FDMA chính là cơ chế điều khiển truy cập đường truyền hiệu quả.

Tuy nhiên, khi mà lượng người gửi dữ liệu là lớn và liên tục thay đổi hoặc đường truyền vượt quá khả năng phục vụ thì FDMA bộc lộ một số vấn đề. Nếu phổ đường truyền được chia làm N vùng và có ít hơn N người dùng cần truy cập đường truyền, thì một phần lớn phổ đường truyền bị lãng phí. Ngược lại, có nhiều hơn N người dùng có nhu cầu truyền dữ liệu thì một số người dùng sẽ phải bị từ chối không có truy cập đường truyền vì thiếu băng thông. Tuy nhiên, nếu lại giả sử rằng số lượng người dùng bằng cách nào đó luôn được giữ ổn định ở con số N, thì việc chia kênh truyền thành những kênh

truyền con như thế tự thân là không hiệu quả. Lý do cơ bản ở đây là: nếu có vài người dùng rồi, không truyền dữ liệu thì những kênh truyền con cấp cho những người dùng này bị lãng phí.

Có thể dễ dàng thấy được hiệu năng nghèo nàn của FDMA từ một phép tính theo lý thuyết xếp hàng đơn giản. Bắt đầu là thời gian trì hoãn trung bình T trong một kênh truyền có dung lượng C bps, với tỉ lệ đến trung bình là λ khung/giây, mỗi khung có chiều dài được chỉ ra từ hàm phân phối mũ với giá trị trung bình là $1/\mu$ bit/khung. Với các tham số trên ta có được tỉ lệ phục vụ là μC khung/giây.

$$\text{Từ lý thuyết xếp hàng ta có: } T = \frac{1}{\mu C - \lambda}$$

Ví dụ: nếu $C = 100 \text{ Mbps}$, $1/\mu = 10000 \text{ bits}$ và $\lambda = 5000 \text{ khung/giây}$ thì $T = 200 \mu\text{s}$. Nay nếu ta chia kênh lớn này thành N kênh truyền nhỏ độc lập, mỗi kênh truyền nhỏ có dung lượng C/N bps. Tỉ lệ trung bình các khung đến các kênh truyền nhỏ bây giờ là λ/N . Tính toán lại T chúng ta có:

$$T_{\text{FDMA}} = \frac{1}{\mu(C/N) - (\lambda/N)} = \frac{N}{\mu C - \lambda} = NT$$

Thời gian chờ đợi trung bình trong các kênh truyền con sử dụng FDMA là xấp xỉ hơn gấp N lần so với trường hợp ta sắp xếp cho các khung được truyền tuần tự trong một kênh lớn.

5.2.1.2 Chia thời gian (TDMA – Time Division Multiple Access)

Trong phương pháp này, các trạm sẽ xoay vòng (round) để truy cập đường truyền. Vòng ở đây có thể hiểu là vòng thời gian. Một vòng thời gian là khoảng thời gian đủ để cho tất cả các trạm trong LAN đều được quyền truyền dữ liệu. Qui tắc xoay vòng như sau: một vòng thời gian sẽ được chia đều thành các khe (slot) thời gian bằng nhau, mỗi trạm sẽ được cấp một khe thời gian – đủ để nó có thể truyền hết một gói tin. Những trạm nào tới lượt được cấp cho khe thời gian của mình mà không có dữ liệu để truyền thì vẫn chiếm lấy khe thời gian đó, và khoảng thời gian bị chiếm này được gọi là thời gian nhàn rỗi (idle time). Tập hợp tất cả các khe thời gian trong một vòng được gọi lại là khung (frame).

Như vậy với phương pháp này, nếu người dùng không sử dụng khe thời gian này để truyền dữ liệu thì thời gian sẽ bị lãng phí.

5.2.1.3. Kết hợp giữa FDMA và TDMA

Trong thực tế, hai kỹ thuật TDMA và FDMA thường được kết hợp sử dụng với nhau, ví dụ như trong các mạng điện thoại di động.

Các điện thoại di động TDMA sử dụng các kênh 30 KHz, mỗi kênh lại được chia thành ba khe thời gian. Một thiết bị cầm tay sử dụng một khe thời gian cho việc gửi và

một khe khác cho việc nhận dữ liệu. Chẳng hạn như các hệ thống: Cingular (Nokia 8265, TDMA 800/ 1900 MHz, AMPS 800 mHz), AT&T Wireless.

Hệ thống GSM sử dụng các kênh 200 KHz được chia thành 8 khe thời gian. Một thiết bị cầm tay sẽ sử dụng một khe thời gian trong hai kênh khác nhau để gửi và nhận thông tin. Các hệ thống Cingular, T-Mobile, AT&T đang chuyển sang dùng kỹ thuật này.

5.2.1.4. Phân chia mã (CDMA – Code Division Multiple Access)

CDMA hoàn toàn khác với FDMA và TDMA. Thay vì chia một dãy tần số thành nhiều kênh truyền băng thông hẹp, CDMA cho phép mỗi trạm có quyền phát dữ liệu lên toàn bộ phổ tần của đường truyền lớn tại mọi thời điểm. Các cuộc truy cập đường truyền xảy ra đồng thời sẽ được tách biệt với nhau bởi kỹ thuật mã hóa. CDMA cũng xóa tan lo lắng cho rằng những khung dữ liệu bị đụng độ trên đường truyền sẽ bị biến dạng. Thay vào đó CDMA chỉ ra rằng nhiều tín hiệu đồng thời sẽ được cộng lại một cách tuyến tính! Kỹ thuật CDMA thường được sử dụng trong các kênh truyền quảng bá không dây (mạng điện thoại di động, vệ tinh ...).

Trước khi đi vào mô tả giải thuật CDMA, hãy xem xét một ví dụ gần giống như sau: tại một phòng đợi trong sân bay có nhiều cặp hành khách đang chuyện trò. TDM có thể được so sánh với cảnh tượng: tất cả mọi người đều đứng giữa phòng, chờ đến lượt mình được phát biểu. FDM thì giống như cảnh tượng: mỗi một cặp được sắp vào một ô nói chuyện riêng. Còn CDMA lại giống như cảnh: mọi người đều đứng ngay trong phòng đợi, nói chuyện đồng thời, nhưng mỗi cặp chuyện trò sẽ sử dụng một ngôn ngữ riêng. Cặp nói tiếng Pháp chỉ nói với nhau bằng tiếng Pháp, bỏ qua mọi tiếng động không phải là tiếng Pháp và coi đó như là tiếng ồn. Vì thế, vấn đề then chốt trong CDMA là khả năng rút trích ra được tín hiệu mong muốn trong khi từ chối mọi thứ khác và coi đó là tiếng ồn ngẫu nhiên.

Trong CDMA, thời gian gửi một bit (bit time) lại được chia thành m khoảng nhỏ hơn, gọi là chip. Thông thường, có 64 hay 128 chip trên một bit, nhưng trong ví dụ phía dưới, chúng ta dùng 8 chip cho đơn giản.

Nhiều người dùng đều chia sẻ chung một băng tần, nhưng mỗi người dùng được cấp cho một mã duy nhất dài m bit gọi là chuỗi bit (chip sequence). Chuỗi bit này sẽ được dùng để mã hóa và giải mã dữ liệu của riêng người dùng này trong một kênh truyền chung đa người dùng. Ví dụ, sau đây là một chuỗi bit: (11110011). Để gửi bit 1, người dùng sẽ gửi đi chuỗi bit của mình. Còn để gửi đi bit 0, người dùng sẽ gửi đi phần bù của chuỗi bit của mình. Ví dụ với chuỗi bit trên, khi gửi bit 1, người dùng sẽ gửi 11110011; khi gửi bit 0 thì người dùng sẽ gửi 00001100.

Để tiện cho việc minh họa, chúng ta sẽ sử dụng các ký hiệu lưỡng cực sau: bit 0 được ký hiệu là -1, bit 1 được ký hiệu là +1.

Cũng cần phải đưa ra một định nghĩa mới: tích trong (inner product): Tích trong của hai mã S và T, ký hiệu là $S \cdot T$, được tính bằng trung bình tổng của tích các bit nội tại tương ứng của hai mã này.

$$S \cdot T = \frac{1}{m} \sum_{i=1}^m S_i T_i$$

Ví dụ: $S = +1+1+1-1-1+1+1-1$

$T = +1+1+1+1-1-1+1-1$

$$S \cdot T = \frac{+1+1+1+(-1)+1+(-1)+1+1}{8} = \frac{1}{2}$$

Bây giờ ta xem xét cách thức cấp phát chuỗi chip cho các trạm, sao cho không gây ra lẫn lộn thông tin giữa các trạm với nhau.

Định nghĩa:

Hai mã S và T có cùng chiều dài m bits được gọi là trực giao khi: $S \cdot T = 0$.

Ví dụ:

$S = +1+1-1-1-1-1+1$

$T = -1-1+1-1-1-1+1+1$

$$S \cdot T = \frac{(-1)+(-1)+(-1)+1+1+1+(-1)+1}{8} = 0$$

Nếu các người dùng trong hệ thống có các mã trực giao với nhau thì họ có thể cùng tồn tại và truyền dữ liệu một cách đồng thời với khả năng bị giao thoa dữ liệu là ít nhất.

Qui ước:

Gọi D_i là bit dữ liệu mà người dùng i muốn mã hóa để truyền trên mạng.

C_i là chuỗi chip (mã số) của người dùng i.

Sau đây là cách thức mã hóa tín hiệu để gửi lên đường truyền và giải mã để lấy dữ liệu đó ra:

- Tín hiệu được mã của người dùng i: $Z_i = D_i \times C_i$
- Tín hiệu tổng hợp được gửi trên đường truyền: $Z = \sum_{i=1}^n Z_i$ với n là tổng số người dùng gửi tín hiệu lên đường truyền tại cùng thời điểm.
- Giải mã:

Dữ liệu mà người dùng i lấy về từ tín hiệu tổng hợp chung: $D_i = Z \cdot C_i$. Nếu $D_i > "ngưỡng"$, coi nó là 1, ngược lại coi nó là -1

5.2.2. Phương pháp truy cập đường truyền ngẫu nhiên

Trong phương pháp truy cập đường truyền ngẫu nhiên (Random Access), người ta để cho các trạm tự do tranh chấp đường truyền chung để truyền từng khung dữ liệu một. Nếu một trạm cần gửi một khung, nó sẽ gửi khung đó trên toàn bộ dải thông của kênh

truyền. Sẽ không có sự phối hợp trình tự giữa các trạm. Nếu có hơn hai trạm phá cùng một lúc, “đụng độ” (collision) sẽ xảy ra, các khung bị đụng độ sẽ bị hư hại. Giao thức truy cập đường truyền ngẫu nhiên được dùng để xác định:

- Làm thế nào để phát hiện dung độ.
 - Làm thế nào để phục hồi sau dung độ.

Ví dụ về các giao thức truy cập ngẫu nhiên: slotted ALOHA và pure ALOHA, CSMA, CSMA/CD và CSMA/CA.

5.2.2.1. ALOHA

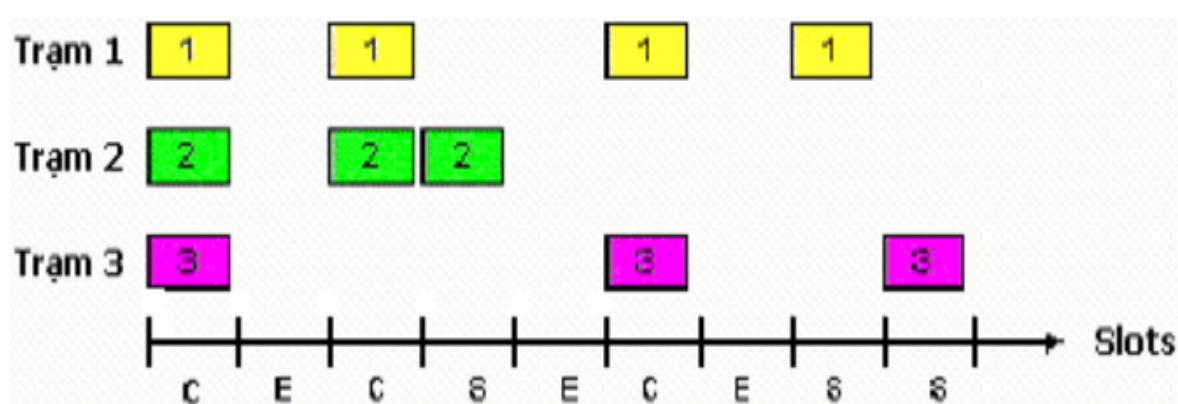
Vào những năm 1970, Norman Abramson cùng các đồng sự tại Đại học Hawaii đã phát minh ra một phương pháp mới ưu hạng dùng để giải quyết bài toán về cấp phát kênh truyền. Sau đó công việc của họ tiếp tục được mở rộng bởi nhiều nhà nghiên cứu khác. Mặc dù công trình của Abramson, được gọi là hệ thống ALOHA, sử dụng hệ thống truyền quảng bá trên sóng radio mặt đất, nhưng ý tưởng cơ sở của nó có thể áp dụng cho bất kỳ hệ thống nào trong đó những người dùng không có phôi hợp với nhau sẽ tranh chấp sử dụng đường truyền chung duy nhất.

Ở đây, chúng ta sẽ thảo luận về hai phiên bản của ALOHA: pure (thuần túy) và slotted (được chia khe).

a. Slotted ALOHA.

Thời gian được chia thành nhiều slot có kích cỡ bằng nhau (bằng thời gian truyền một khung). Một trạm muốn truyền một khung thì phải đợi đến đầu slot thời gian kế tiếp mới được truyền. Dĩ nhiên là sẽ xảy ra đụng độ và khung bị đụng độ sẽ bị hư. Tuy nhiên, dựa trên tính phản hồi của việc truyền quảng bá, trạm phát luôn có thể theo dõi xem khung của nó phát đi có bị hủy hoại hay không bằng cách lắng nghe kênh truyền. Những trạm khác cũng làm theo cách tương tự. Trong trường hợp vì lý do nào đó mà trạm không thể dùng cơ chế lắng nghe đường truyền, hệ thống cần yêu cầu bên nhận trả lời một khung báo nhận (acknowledgement) cho bên phát. Nếu phát sinh đụng độ, trạm phát sẽ gửi lại khung tại đầu slot kế tiếp với xác suất p cho đến khi thành công.

Ví dụ minh họa: Có 3 trạm đều muốn truyền một khung thông tin.



Hình 5.2 Ví dụ về Slotted ALOHA

Do sẽ có dung độ mà mất khung thông tin, một câu hỏi đặt ra là: đâu là tỉ suất truyền khung thành công của các trạm trong mạng?

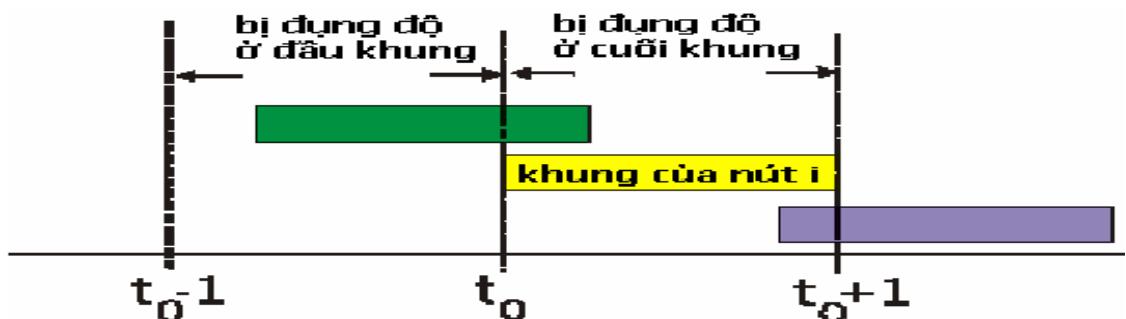
Giả sử có N trạm muốn truyền dữ liệu, mỗi trạm truyền khung thông tin của mình trong một slot với xác suất p. Xác suất để một trạm trong N trạm truyền thành công S(p) được tính như sau: $S(p) = Np(1-p)^{N-1}$

Khi $p = 1/N$ thì $S(p)$ sẽ đạt giá trị cực đại $(1-1/N)^{N-1}$

b. Pure ALOHA.

Kỹ thuật Pure ALOHA đơn giản hơn Slotted ALOHA do không có sự đồng bộ hóa giữa các trạm.

Mỗi khi muốn truyền một khung thông tin, trạm sẽ truyền nó ngay mà không cần đợi đến đầu của slot thời gian kế tiếp. Vì thế xác xuất bị dụng độ tăng thêm! Nghĩa là khung thông tin được gửi tại thời điểm t sẽ dung độ với những khung được gửi trong khoảng thời gian $[t_0 - 1, t_0 + 1]$.



Hình 5. 3 Ví dụ về Pure ALOHA

Gọi P là xác xuất của một sự kiện nào đó, ta có những phân tích sau:

$$P(\text{nút } i \text{ truyền thành công}) = P(\text{để nút } i \text{ truyền})$$

$$P(\text{không có nút nào khác truyền trong khoảng } [t_0-1, t_0])$$

$$P(\text{không có nút nào khác truyền trong khoảng } [t_0, t_0 + 1]) = p(1-p)^{N-1}(1-p)^{N-1}$$

$$S(p) = P(\text{một nút bất kỳ trong } N \text{ nút truyền thành công}) = Np(1-p)^{N-1}(1-p)^{N-1}$$

Những phân tích vừa nêu giả sử rằng luôn có thường trực N trạm trong mạng. Và trong trường hợp tối ưu, mỗi trạm thử truyền với xác suất 1/N.

Trong thực tế, số lượng các trạm thường trực trong mạng luôn thay đổi. Giả sử chúng ta có tổng cộng m trạm làm việc. n trạm là thường trực trên mạng, mỗi trạm thường trực trên mạng sẽ cố gửi khung thông tin với xác suất cố định p. m-n trạm còn lại là không thường trực, và chúng có thể gửi khung thông tin với xác suất pa, với pa có thể nhỏ hơn p.

5.2.2.2. CSMA – Carrier Sense Multiple Access

a. Giao thức CSMA

Giao thức ALOHA mặc dù đã chạy được, nhưng một điều đáng ngạc nhiên là người ta lại để cho các trạm làm việc tự do gửi thông tin lên đường truyền mà chẳng cần quan tâm đến việc tìm hiểu xem những trạm khác đang làm gì. Và điều đó dẫn đến rất nhiều vụ đụng độ tín hiệu. Tuy nhiên, trong mạng LAN, người ta có thể thiết kế các trạm làm việc sao cho chúng có thể điều tra xem các trạm khác đang làm gì và tự điều chỉnh hành vi của mình một cách tương ứng. Làm như vậy sẽ giúp cho hiệu năng mạng đạt được cao hơn. CSMA là một giao thức như vậy! Các giao thức mà trong đó các trạm làm việc lắng nghe đường truyền trước khi đưa ra quyết định mình phải làm gì tương ứng với trạng thái đường truyền đó được gọi là các giao thức có “cảm nhận” đường truyền (carrier sense protocol). Cách thức hoạt động của CSMA như sau: lắng nghe kênh truyền, nếu thấy kênh truyền rỗi thì bắt đầu truyền khung, nếu thấy đường truyền bận thì trì hoãn lại việc gửi khung. Thế nhưng trì hoãn việc gửi khung cho đến khi nào?

Có ba giải pháp:

Theo dõi không kiên trì (Non-persistent CSMA): Nếu đường truyền bận, đợi trong một khoảng thời gian ngắn rồi tiếp tục nghe lại đường truyền.

Theo dõi kiên trì (persistent CSMA): Nếu đường truyền bận, tiếp tục nghe đến khi đường truyền rỗi rồi thì truyền gói tin với xác suất bằng 1.

Theo dõi kiên trì với xác suất p (P-persistent CSMA): Nếu đường truyền bận, tiếp tục nghe đến khi đường truyền rỗi rồi thì truyền gói tin với xác suất bằng p .

Dễ thấy rằng giao thức CSMA cho dù là theo dõi đường truyền kiên trì hay không kiên trì thì khả năng tránh đụng độ vẫn tốt hơn là ALOHA. Tuy thế, đụng độ vẫn có thể xảy ra trong CSMA!

Tình huống phát sinh như sau: khi một trạm vừa phát xong thì một trạm khác cũng phát sinh yêu cầu phát khung và bắt đầu nghe đường truyền. Nếu tín hiệu của trạm thứ nhất chưa đến trạm thứ hai, trạm thứ hai sẽ cho rằng đường truyền đang rảnh và bắt đầu phát khung. Như vậy đụng độ sẽ xảy ra.

Hậu quả của đụng độ là: khung bị mất và toàn bộ thời gian từ lúc đụng độ xảy ra cho đến khi phát xong khung là lãng phí!

b. CSMA với cơ chế theo dõi đụng độ (CSMA/CD–CSMA with Collision Detection)

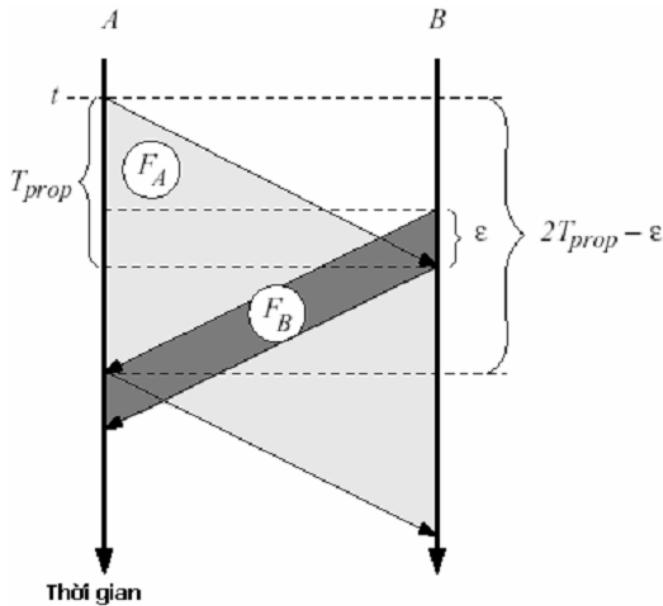
CSMA/CD về cơ bản là giống như CSMA: lắng nghe trước khi truyền. Tuy nhiên CSMA/CD có hai cải tiến quan trọng là: phát hiện đụng độ và làm lại sau đụng độ.

Phát hiện đụng độ: Trạm vừa truyền vừa tiếp tục dò xét đường truyền. Ngay sau khi đụng độ được phát hiện thì trạm ngưng truyền, phát thêm một dãy nhồi (dãy nhồi này có tác dụng làm tăng cường thêm sự va chạm tín hiệu, giúp cho tất cả các trạm khác trong mạng thấy được sự đụng độ), và bắt đầu làm lại sau đụng độ.

Tại thời điểm t_0 , một trạm đã phát xong khung của nó. Bất kỳ trạm nào khác có khung cần truyền bây giờ có thể cố truyền thử. Nếu hai hoặc nhiều hơn các trạm làm như

vậy cùng một lúc thì sẽ xảy ra đụng độ. Đụng độ có thể được phát hiện bằng cách theo dõi năng lượng hay độ rộng của xung của tín hiệu nhận được và đem so sánh với độ rộng của xung vừa truyền đi. Nay giờ ta đặt ra câu hỏi: Sau khi truyền xong khung (hết giai đoạn truyền), trạm sẽ bỏ ra thời gian tối đa là bao lâu để biết được là khung của nó đã bị đụng độ hoặc nó đã truyền thành công? Gọi thời gian này là “cửa sổ va chạm” và ký hiệu nó là T_w . Phân tích sau đây sẽ cho ra câu trả lời.

Hình sau sẽ mô phỏng chi tiết về thời gian phát khung giữa hai trạm A và B ở hai đầu mút xa nhau nhất trên đường truyền tải.



Hình 5.4 Thời gian cần thiết để truyền một khung

Đặt T_{prop} là thời gian lan truyền tín hiệu giữa hai đầu mút xa nhau nhất trên đường truyền tải.

- Tại thời điểm t , A bắt đầu phát đi khung dữ liệu của nó.
- Tại $t+T_{prop}-\epsilon$, B phát hiện kênh truyền rảnh và phát đi khung dữ liệu của nó.
- Tại $t+T_{prop}$, B phát hiện sự đụng độ.
- Tại $t+2T_{prop}-\epsilon$, A phát hiện sự đụng độ.

Theo phân tích trên, thì $T_w = 2T_{prop}$

Việc hủy bỏ truyền khung ngay khi phát hiện có đụng độ giúp tiết kiệm thời gian và băng thông, vì nếu cứ tiếp tục truyền khung đi nữa, khung đó vẫn hư và vẫn phải bị hủy bỏ.

Làm lại sau khi đụng độ: Sau khi bị đụng độ, trạm sẽ chạy một thuật toán gọi là back-off dùng để tính toán lại lượng thời gian nó phải chờ trước khi gửi lại khung. Lượng thời gian này phải là ngẫu nhiên để các trạm sau khi quay lại không bị đụng độ với nhau nữa.

Thuật toán back-off hoạt động như sau:

- Rút ngẫu nhiên ra một con số nguyên M thỏa: $0 \leq M \leq 2^k$. Trong đó $k = \min(n, 10)$, với n là tổng số lần đụng độ mà trạm đã gánh chịu.
- Kỳ hạn mà trạm phải chờ trước khi thử lại một lần truyền mới là M^*T_w .
- Khi mà n đạt đến giá trị 16 thì hủy bỏ việc truyền khung. (Trạm đã chịu đựng quá nhiều vụ đụng độ rồi, và không thể chịu đựng hơn được nữa!)

Đánh giá hiệu suất của giao thức CSMA/CD:

Gọi:

- P là kích thước của khung, ví dụ như 1000 bits.
- C là dung lượng của đường truyền, ví dụ như 10 Mbps.

Ta có thời gian phát hết một khung thông tin là P/C giây.

Trung bình, chúng ta sẽ thử e lần trước khi truyền thành công một khung.

Vì vậy, với mỗi lần phát thành công một khung (tốn P/C giây), ta đã mất tổng cộng $2eT_{prop}$ ($\approx 5T_{prop}$) vì đụng độ. Thành thử hiệu năng của giao thức (tỉ lệ giữa thời gian hoạt động hữu ích trên tổng thời gian hoạt động) là:

$$\frac{\frac{P}{C}}{\frac{P}{C} + 5T_{prop}} = \frac{1}{1 + \frac{5T_{prop}}{\frac{P}{C}}} = \frac{1}{1 + 5a}$$

$$\text{với } a = \frac{T_{prop}C}{P}$$

Ta có thể thấy giá trị của a đóng vai trò rất quan trọng đến hiệu suất hoạt động của mạng kiểu CSMA/CD.

5.2.3. Phương pháp phân lượt truy cập đường truyền

Bây giờ thử nhìn lại hai phương pháp điều khiển truy cập đường truyền “chia kênh” và “truy cập ngẫu nhiên”, ta sẽ thấy chúng đều có những điểm hay và hạn chế:

Trong các giao thức dạng chia kênh, kênh truyền được phân chia một cách hiệu quả và công bằng khi tải trọng đường truyền là lớn. Tuy nhiên chúng không hiệu quả khi tải trọng của đường truyền là nhỏ: có độ trì hoãn khi truy cập kênh truyền, chỉ $1/N$ băng thông được cấp cho người dùng ngay cả khi chỉ có duy nhất người dùng đó hiện diện trong hệ thống.

Các giao thức dạng truy cập ngẫu nhiên thì lại hoạt động hiệu quả khi tải trọng của đường truyền thấp. Nhưng khi tải trọng đường truyền cao thì phải tốn nhiều chi phí cho việc xử lý đụng độ. Các giao thức dạng “phân lượt” sẽ để ý đến việc tận dụng những mặt mạnh của hai dạng nói trên.

Ý tưởng chính của các giao thức dạng “phân lượt” là không để cho đụng độ xảy ra bằng cách cho các trạm truy cập đường truyền một cách tuần tự.

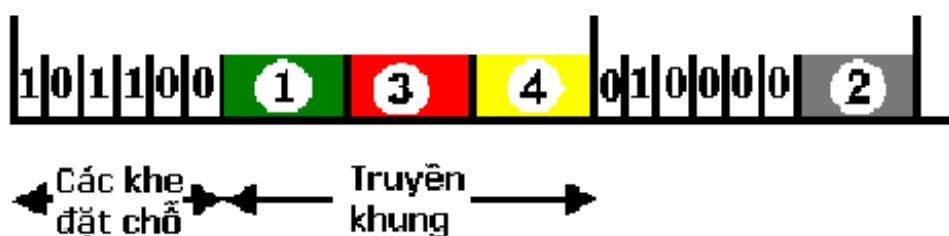
Về cơ bản, có hai cách thức để “phân lượt” sử dụng đường truyền:

Thăm dò (polling): Trạm chủ (master) sẽ mời các trạm tớ (slave) truyền khi đến lượt. Lượt truyền được cấp phát cho trạm tớ có thể bằng cách: trạm chủ dành phần cho trạm tớ hoặc trạm tớ yêu cầu và được trạm chủ đáp ứng. Tuy nhiên có thể thấy những vấn đề sẽ gặp phải của giải pháp này là: chi phí cho việc thăm dò, độ trễ do phải chờ được phân luợt truyền, hệ thống rối loạn khi trạm chủ gặp sự cố.

Chuyển thẻ bài (token passing): Thẻ bài điều khiển sẽ được chuyển lần lượt từ trạm này qua trạm kia. Trạm nào có trong tay thẻ bài sẽ được quyền truyền, truyền xong phải chuyển thẻ bài qua trạm kế tiếp. Những vấn đề cần phải quan tâm: chi phí quản lý thẻ bài, độ trễ khi phải chờ thẻ bài, khó khăn khi thẻ bài bị mất.

5.2.3.1. Ví dụ về phương pháp thăm dò phân tán

Trong phương pháp thăm dò phân tán (Distributed Polling), thời gian được chia thành những “khe” (slot). Giả sử hệ thống hiện có N trạm làm việc. Một chu kỳ hoạt động của hệ thống bắt đầu bằng N khe thời gian ngắn dùng để đặt chỗ (reservation slot).



Hình 5.5 Mô tả các chu kỳ hoạt động của hệ thống thăm dò phân tán

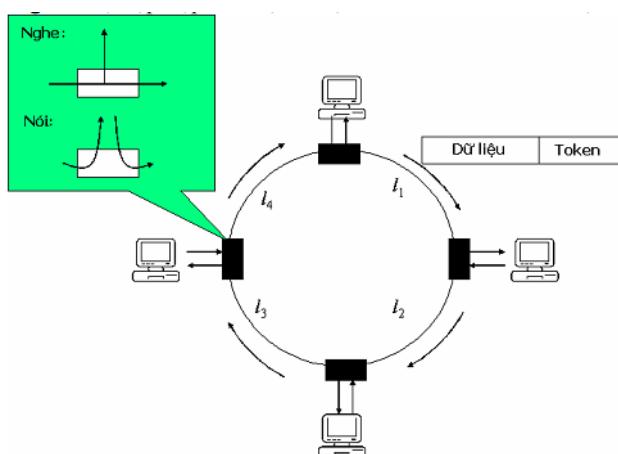
Khe thời gian dùng để đặt chỗ bằng với thời gian lan truyền tín hiệu giữa hai đầu mút xa nhất trên đường truyền. Tới khe đặt chỗ thứ i, trạm thứ i nếu muốn truyền dữ liệu sẽ phát tín hiệu đặt chỗ của mình lên kênh truyền, và tín hiệu này sẽ được nhìn thấy bởi tất cả các trạm khác trong mạng.

Sau thời gian đặt chỗ, các trạm bắt đầu việc truyền dữ liệu của mình theo đúng trình tự đã đăng ký.

5.2.3.2. Ví dụ về phương pháp chuyển thẻ bài: Token Ring

Giao thức này sử dụng mạng kiểu hình vòng, dùng thẻ bài để cấp quyền sử dụng đường truyền. Mạng token ring bao gồm một tập hợp các trạm được nối với nhau thành một vòng.

Dữ liệu luôn chạy theo một hướng vòng quanh vòng. Mỗi trạm nhận khung từ trạm



phía trên của nó và rồi chuyển khung đến trạm phía dưới. Thẻ bài là công cụ để quyết định ai có quyền truyền tại một thời điểm.

Hình 5. 6 Mô hình hoạt động của mạng Token Ring

Cách thức hoạt động của mạng token ring như sau: một thẻ bài, thực chất chỉ là một dãy bit, sẽ chạy vòng quanh vòng; mỗi nút sẽ nhận thẻ bài rồi lại chuyển tiếp thẻ bài này đi. Khi một trạm có khung cần truyền và đúng lúc nó thấy có thẻ bài tới, nó liền lấy thẻ bài này ra khỏi vòng (nghĩa là không có chuyển tiếp chuỗi bit đặc biệt này lên vòng nữa), và thay vào đó, nó sẽ truyền khung dữ liệu của mình đi. Khi khung dữ liệu đi một vòng và quay lại, trạm phát sẽ rút khung của mình ra và chèn lại thẻ bài vào vòng. Hoạt động cứ xoay vòng như thế.

Card mạng dùng cho token ring sẽ có trên đó một bộ nhận, một bộ phát và một bộ đệm dùng chứa dữ liệu. Khi không có trạm nào trong vòng có dữ liệu để truyền, thẻ bài sẽ lưu chuyển vòng quanh. Nếu một trạm có dữ liệu cần truyền và có thẻ bài, nó có quyền truyền một hoặc nhiều khung dữ liệu tùy theo qui định của hệ thống.

Mỗi khung dữ liệu được phát đi sẽ có một phần thông tin chứa địa chỉ đích của trạm bên nhận; ngoài ra nó còn có thể chứa địa chỉ multicast hoặc broadcast tùy theo việc bên gửi muốn gửi khung cho một nhóm người nhận hay tất cả mọi người trong vòng. Khi khung thông tin chạy qua mỗi trạm trong vòng, trạm này sẽ nhìn vào địa chỉ đích trong khung đó để biết xem có phải nó là đích đến của khung không. Nếu phải, trạm sẽ chép nội dung của khung vào trong bộ đệm của nó, chỉ chép thôi chứ không được xóa khung ra khỏi vòng.

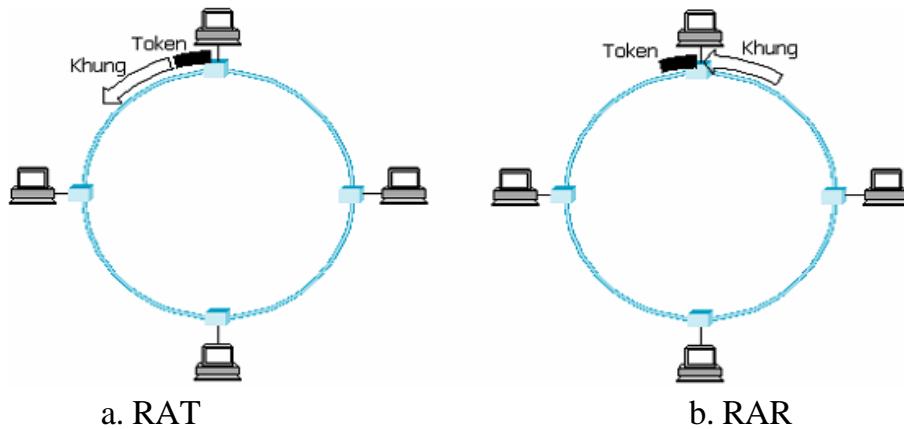
Một vấn đề cần phải quan tâm đến là một trạm đang giữ thẻ bài thì nó có quyền truyền bao nhiêu dữ liệu, hay nói cách khác là trạm được cho bao nhiêu thời gian để truyền dữ liệu? Chúng ta gọi thời gian này là thời gian giữ thẻ bài – THT (Token Holding Time). Trong trường hợp trong vòng chỉ có một trạm cần truyền dữ liệu và các trạm khác không có nhu cầu truyền, thì ta có thể cấp THT cho trạm có nhu cầu càng lâu càng tốt. Điều này sẽ làm tăng hiệu suất sử dụng hệ thống một cách đáng kể. Bởi vì sẽ thật là ngớ ngẩn nếu bắt trạm ngừng, chờ thẻ bài chạy hết một vòng, rồi lại truyền tiếp. Tuy nhiên, giải pháp trên sẽ không hoạt động tốt nếu có nhiều trạm trong vòng cần gửi dữ liệu. THT dài chỉ thích hợp cho những trạm cần truyền nhiều dữ liệu, nhưng lại không phù hợp với những trạm chỉ có ít thông điệp cần gửi đi ngay cả khi thông điệp này là tối quan trọng. Điều này cũng giống như tình huống mà bạn xếp hàng để sử dụng máy ATM ngay sau một anh chàng định rút ra 10 triệu đồng, trong khi bạn chỉ cần vào đây để kiểm tra tài khoản của mình còn bao nhiêu tiền! Trong các mạng 802.5, THT mặc định là 10 ms.

Từ thời gian giữ thẻ bài, chúng ta lại nghĩ ra một số đo quan trọng khác: Thời gian xoay vòng của thẻ bài – TRT (Token rotation time), nghĩa là lượng thời gian bỏ ra để thẻ bài đi hết đúng một vòng.

Dễ nhận thấy rằng: $TRT \leq Số nút hoạt động \times THT + Độ trễ của vòng$

Với “Độ trễ của vòng” là tổng thời gian để thẻ bài đi hết một vòng khi trong vòng không có trạm nào cần truyền dữ liệu, “Số nút hoạt động” ám chỉ số trạm có dữ liệu cần truyền. Giao thức 802.5 cung cấp một phương thức truyền dữ liệu tin cậy bằng cách sử dụng hai bit A và C ở đuôi của khung dữ liệu. Hai bit bày ban đầu nhận giá trị 0. Khi một trạm nhận ra nó là đích đến của một khung dữ liệu, nó sẽ đặt bit A trong khung này lên. Khi trạm chép khung vào bộ nhớ đệm của nó, nó sẽ đặt bit C lên. Khi trạm gửi thấy khung của nó quay lại với bit A vẫn là 0, nó biết là trạm đích bị hư hỏng hoặc không có mặt. Nếu bit A là 1, nhưng bit C là 0, điều này ám chỉ trạm đích có mặt nhưng vì lý do nào đó trạm đích không thể nhận khung (ví dụ như thiếu bộ đệm chằng hạn). Vì thế khung này có thể sẽ được truyền lại sau đó với hy vọng là trạm đích có thể tiếp nhận nó.

Chi tiết cuối cùng cần phải xem xét là: chính xác khi nào thì trạm sẽ nhả thẻ bài ra? Có hai đề nghị: a) nhả thẻ bài ra ngay sau khi trạm vừa truyền khung xong (RAT); b) nhả thẻ bài ra ngay sau khi trạm nhận lại khung vừa phát ra (RAR).



Hình 5.7 Nhả Token Ring

Quản lý hoạt động của mạng Token Ring:

Cần thiết phải đề cử ra một trạm làm nhiệm vụ quản lý mạng token ring gọi là monitor. Công việc của monitor là đảm bảo sức khỏe cho toàn bộ vòng. Bất kỳ trạm nào cũng có thể trở thành monitor. Thủ tục bầu chọn monitor diễn ra khi vòng vừa được tạo ra hoặc khi monitor của vòng bị sự cố. Một monitor mạnh khỏe sẽ định kỳ thông báo sự hiện diện của nó cho toàn vòng biết bằng một thông điệp đặc biệt. Nếu một trạm không nhận được thông báo hiện diện của monitor trong một khoảng thời gian nào đó, nó sẽ coi như monitor bị hỏng và sẽ cố trở thành monitor mới.

Khi một trạm quyết định rằng cần phải có một monitor mới, nó sẽ gửi một thông điệp thỉnh cầu, thông báo ý định trở thành monitor của mình. Nếu thông điệp này chạy một vòng và về lại được trạm, trạm sẽ cho rằng mọi người đồng ý vị trí monitor của nó. Còn nếu đồng thời có nhiều trạm cùng gửi thông điệp thỉnh cầu, chúng sẽ phải áp dụng một luật lựa chọn nào đó, chẳng hạn như “ai có địa chỉ cao nhất sẽ thắng cử”.

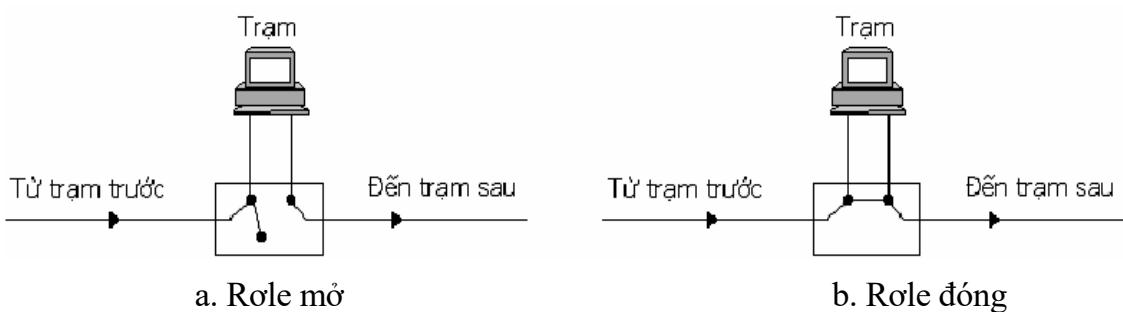
Nhiệm vụ đáng chú ý của monitor là phải đảm bảo rằng luôn luôn có sự hiện diện của thẻ bài ở đâu đó trên vòng, có thể là đang di chuyển hay đang bị giữ bởi một trạm nào đó. Rõ ràng là thẻ bài có thể bị biến mất vì lý do nào đó chẳng hạn như lỗi bit, trạm đang giữ nó bị hư hỏng. Để phát hiện ra việc thẻ bài bị mất, khi thẻ bài chạy ngang qua monitor, nó sẽ bật một bộ đếm thời gian để tính giờ. Bộ đếm này có giá trị tối đa là:

$$\text{Số lượng trạm} \times \text{THT} + \text{Độ trễ của vòng}$$

Trong đó “Số lượng trạm” là số các trạm làm việc đang hiện diện trên vòng, “độ trễ của vòng” là tổng thời gian lan truyền tín hiệu trên vòng. Nếu bộ đếm đạt đến giá trị tối đa mà monitor vẫn không thấy thẻ bài chạy qua nó nữa thì nó sẽ tạo ra thẻ bài mới.

Monitor cũng phải kiểm tra xem có khung nào bị hỏng hoặc vô thừa nhận hay không. Một khung nếu có lỗi checksum hoặc khuôn dạng không hợp lệ sẽ chạy một cách vô định trên vòng. Monitor sẽ thu khung này lại trước khi chèn lại thẻ bài vào vòng. Một khung vô thừa nhận là khung mà đã được chèn thành công vào vòng, nhưng cha của nó bị chết, nghĩa là trạm gửi nó chỉ gửi nó lên vòng, nhưng chưa kịp thu nó lại thì đã bị chết (down). Những khung như vậy sẽ bị phát hiện bằng cách thêm vào một bit điều khiển gọi là monitor bit. Khi được phát lần đầu tiên, monitor bit trên khung sẽ nhận giá trị 0. Khi khung đi ngang qua monitor, monitor sẽ đặt monitor bit lên 1. Nếu monitor thấy khung này lại chạy qua nó với monitor bit là 1, nó sẽ rút khung này ra khỏi vòng.

Một chức năng quản lý vòng khác là phát hiện ra một trạm bị chết. Nếu một trạm trong vòng bị chết, nó sẽ làm đứt vòng. Để tránh tình trạng này người ta thêm vào trạm một rờ-le điện tử (relay). Khi trạm còn mạnh khỏe, rờ-le sẽ mở và trạm được nối với vành, khi trạm bị chết và ngưng không cung cấp năng lượng cho rờ-le, rờ-le sẽ tự động đóng mạch và bỏ qua trạm này.



Hình 5. 8 Sử dụng rôle

Khi monitor nghi ngờ một trạm bị chết, nó sẽ gửi đến trạm đó một khung đặc biệt gọi là khung beacon. Nếu không nhận được trả lời thích đáng, monitor sẽ coi trạm đó đã chết.

5.2.3.3. Ví dụ về phương pháp chuyển thẻ bài: Token BUS

Kỹ thuật Token Bus về bản chất là sử dụng mạng hình bus. Tuy nhiên người ta muốn thiết lập một vòng ảo trên đó để nó hoạt động giống như Token Ring. Nguyên tắc

hoạt động như sau: trạm có nhu cầu truyền dữ liệu thì sẽ tham gia vào vòng ảo, ngược lại thì sẽ nằm ngoài và chỉ nghe thôi!

Giải thuật bổ sung một trạm vào vòng:

- Mỗi trạm trong vòng có trách nhiệm định kỳ tạo điều kiện cho các trạm khác tham gia vào vòng.
- Trước khi chuyển thẻ bài đi, trạm sẽ gửi thông báo “tìm trạm đứng sau” (có địa chỉ giữa nó và trạm đứng liền kề hiện tại).
- Nếu sau một thời gian xác định mà vẫn không có yêu cầu gia nhập nào, trạm sẽ chuyển thẻ bài đến trạm kế tiếp như thường lệ.
- Nếu có yêu cầu gia nhập vòng, thì trạm sẽ ghi nhận trạm mới yêu cầu là trạm kế tiếp của nó và sẽ chuyển thẻ bài tới trạm kế mới này.

Giải thuật rút lui ra khỏi vòng:

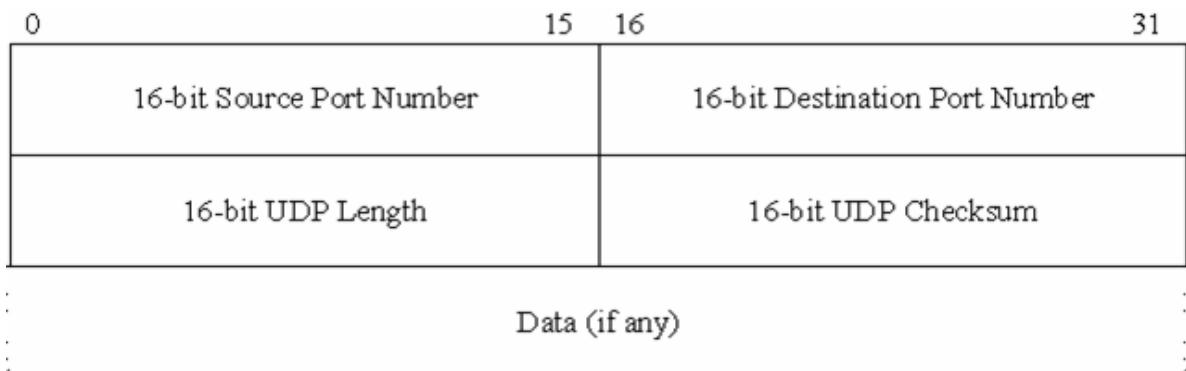
- Khi muốn rút ra khỏi vòng, trạm sẽ chờ đến khi nó có token, sau đó sẽ gửi yêu cầu “nối trạm đứng sau” tới trạm đứng trước nó, yêu cầu trạm đứng trước nối trực tiếp với trạm đứng liền sau nó.

Ngoài ra còn phải quan tâm đến tình trạng mất thẻ bài, các trạm thành viên trong vòng bị hư hỏng.

5.3. Giao thức vận chuyện không liên kết: UDP

Giao thức gói tin người sử dụng UDP.

UDP (User Datagram Protocol) là giao thức không liên kết (Connectionless). UDP sử dụng cho các tiến trình không yêu cầu về độ tin cậy cao, không có cơ chế xác nhận ACK, không đảm bảo chuyển giao các gói dữ liệu đến đích và theo đúng thứ tự và không thực hiện loại bỏ các gói tin trùng lặp. Nó cung cấp cơ chế gán và quản lý các số hiệu cổng để định danh duy nhất cho các ứng dụng chạy trên một Client của mạng và thực hiện việc ghép kênh. UDP thường sử dụng kết hợp với các giao thức khác, phù hợp cho các ứng dụng yêu cầu xử lý nhanh như các giao thức SNMP và VoIP.



Hình 5. 9 Cấu trúc gói tin UDP

Các thành phần trong gói tin UDP:

- + Source Port: port nguồn.

- + Destination Port: port đích.
- + UDP Length: chiều dài của gói tin.
- + UDP Checksum: dùng để kiểm tra gói tin có bị sai lệch hay không
- + Data: dữ liệu đi kèm trong gói tin (nếu có).

Khái niệm Port:

Trong cùng một thời điểm, một máy tính có thể có nhiều chương trình đang chạy. Vậy làm sao để xác định một gói tin sẽ được chương trình nào sử dụng?

Khái niệm Port ra đời để giải quyết chuyện đó. Mỗi chương trình ứng dụng mạng đều có một Port xác định. Để gửi gói tin đến một chương trình tại máy tính A, ta chỉ cần gửi gói tin đến địa chỉ IP của máy A, và Port mà chương trình đó đang sử dụng.

TCP hoặc UDP dùng port hoặc socket, nó là con số mà thông qua đó thông tin được truyền lên các lớp cao hơn. Các con số port được dùng trong việc lưu vết các cuộc hội thoại khác nhau trên mạng xảy ra trong cùng một thời điểm. Port là một loại địa chỉ logic trên một máy tính, là con số 2 byte. Các port có giá trị nhỏ hơn 1024 được dùng làm các port chuẩn. Các ứng dụng dùng port riêng có giá trị lớn hơn 1024. Các giá trị port được chứa trong phần địa chỉ nguồn và đích của mỗi segment TCP.

Một ứng dụng có thể sử dụng port riêng trong miền cho mình để giao dịch trên mạng nhưng chú ý là không được trùng với các port chuẩn.

Ví dụ một số port chuẩn mà các phần mềm sử dụng

- | | |
|--------------------------|-------------------------|
| + HTTP: Port number 80 | + SMTP: Port number 25 |
| + FTP: Port number 21 | + TFTP: Port number 69 |
| + DNS: Port number 53 | + SNMP: Port number 161 |
| + Telnet: Port number 23 | + RIP: Port number 52 |

5.4. Nguyên tắc truyền dữ liệu tin cậy

5.5. Giao thức vận chuyển hướng kết nối:TCP

TCP (Transmission Control Protocol) là một giao thức hướng liên kết (Connection Oriented), tức là trước khi truyền dữ liệu, thực thể TCP phát và thực thể TCP thu thương lượng để thiết lập một kết nối logic tạm thời, tồn tại trong quá trình truyền số liệu. TCP nhận thông tin từ lớp trên, chia dữ liệu thành nhiều gói theo độ dài quy định và chuyển giao các gói tin xuống cho các giao thức lớp mạng (Lớp IP) để định tuyến. Bộ xử lý TCP xác nhận từng gói, nếu không có xác nhận gói dữ liệu sẽ được truyền lại. Thực thể TCP bên nhận sẽ khôi phục lại thông tin ban đầu dựa trên thứ tự gói và chuyển dữ liệu lên lớp trên.

TCP cung cấp khả năng truyền dữ liệu một cách an toàn giữa các thành trong liên mạng. Cung cấp các chức năng kiểm tra tính chính xác của dữ liệu khi đến đích và truyền lại dữ liệu khi có lỗi xảy ra.

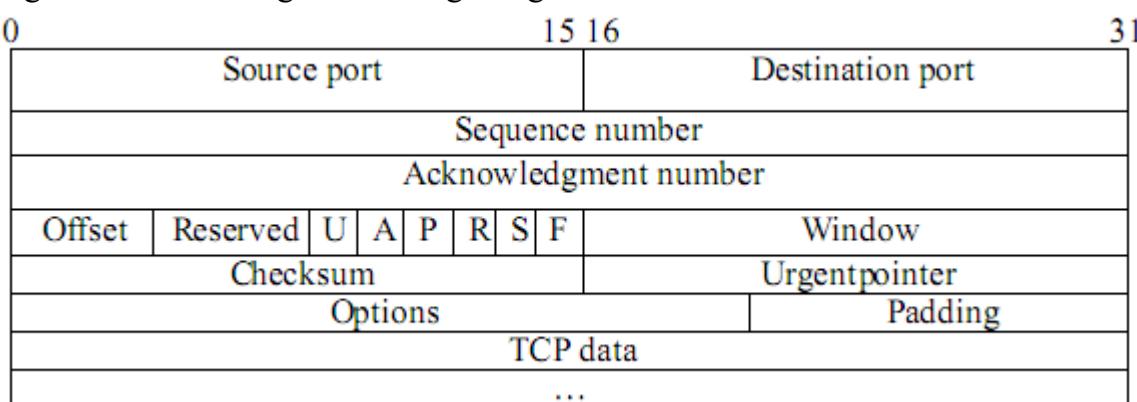
TCP cung cấp các chức năng chính sau:

- Thiết lập, duy trì, giải phóng liên kết giữa hai thực thể TCP.
- Phân phát gói tin một cách tin cậy.
- Tạo số thứ tự (Sequencing) các gói dữ liệu.
- Điều khiển lỗi.
- Cung cấp khả năng đa kết nối cho các quá trình khác nhau giữa thực thể nguồn và thực thể đích thông qua việc sử dụng số hiệu cổng.
- Truyền dữ liệu theo chế độ song công (Full Duplex).

TCP có những đặc điểm sau:

- Hai thực thể liên kết với nhau phải trao đổi, đàm phán với nhau về các thông tin liên kết. Hội thoại, đàm phán nhằm ngăn chặn sự tràn lụt và mất dữ liệu khi truyền.
- Hệ thống nhận phải gửi xác nhận cho hệ thống phát biết rằng nó đã nhận gói dữ liệu.
- Các Datagram IP có thể đến đích không đúng theo thứ tự, TCP nhận sắp xếp lại.
- Hệ thống chỉ phát lại gói tin bị lỗi, không loại bỏ toàn bộ dòng dữ liệu.

Cấu trúc gói tin TCP: Đơn vị dữ liệu sử dụng trong giao thức TCP được gọi là Segment. Khuôn dạng và nội dung của gói tin TCP được biểu diễn như sau:



Hình 5. 10 Cấu trúc gói tin TCP (TCP Segment)

- Cổng nguồn (Source Port): 16 bit, số hiệu cổng nguồn.
- Cổng đích (Destination Port): Độ dài 16 bit, chứa số hiệu cổng đích.
- Sequence Number: 32 bits, số thứ tự của gói số liệu khi phát.
- Acknowledgment Number (32 bits), Bên thu xác nhận thu được dữ liệu đúng.
- Offset (4 bits): Độ dài Header gói tin TCP.
- Reserved (6 bit) lưu lại: Lấp đầy bằng 0 để dành cho tương lai.

- Control bits: Các bits điều khiển

URG: Vùng con trả khẩn có hiệu lực.

ACK: Vùng báo nhận (ACK number) có hiệu lực.

PSH: Chức năng PUSH.

RST: Khởi động lại (reset) liên kết.

SYN: Đồng bộ các số liệu tuần tự (sequence number).

FIN: Không còn dữ liệu từ trạm nguồn.

- Window (16bits): Số lượng các Byte dữ liệu trong vùng cửa sổ bên phát.

- Checksum (16bits): Mã kiểm soát lỗi (theo phương pháp CRC).

- Urgent Pointer (16 bits): Số thứ tự của Byte dữ liệu khẩn, khi URG được thiết lập.

- Option (độ dài thay đổi): Khai báo độ dài tối đa của TCP Data trong một Segment.

- Padding (độ dài thay đổi): Phần chèn thêm vào Header.

Việc kết hợp địa chỉ IP của một máy trạm và số cổng được sử dụng tạo thành một Socket. Các máy gửi và nhận đều có Socket riêng. Số Socket là duy nhất trên mạng.

5.6. Nguyên tắc điều khiển xung đột

Điều khiển lưu lượng và điều khiển tắc nghẽn:

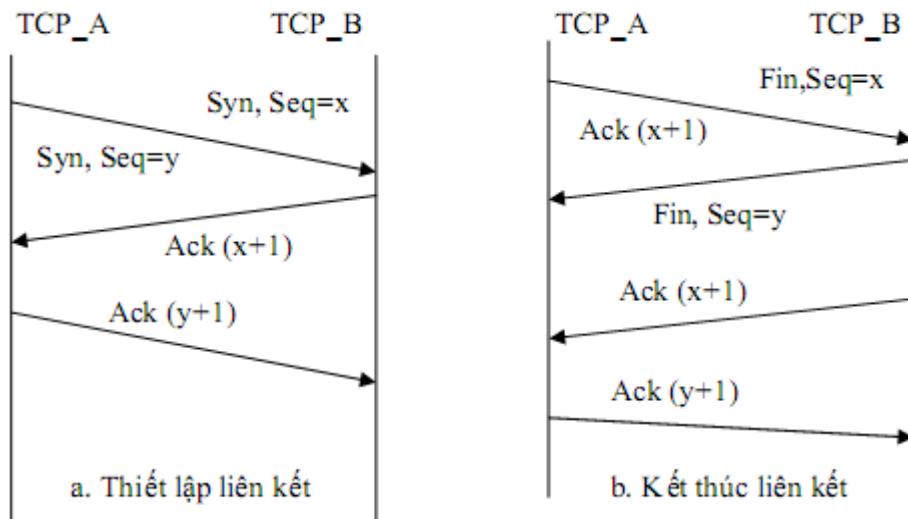
Cơ chế cửa sổ động: là một trong các phương pháp điều khiển thông tin trong mạng máy tính. Độ lớn của cửa sổ bằng số lượng các gói dữ liệu được gửi liên tục mà không cần chờ thông báo trả lời về kết quả nhận từng gói dữ liệu đó. Độ lớn cửa sổ quyết định hiệu suất trao đổi dữ liệu trong mạng. Nếu chọn độ lớn của sổ cao thì có thể gửi được nhiều dữ liệu trong cùng một đơn vị thời gian. Nếu truyền bị lỗi, dữ liệu phải gửi lại lớn thì hiệu quả sử dụng đường truyền thấp. Giao thức TCP cho phép thay đổi độ lớn của sổ một cách động, phụ thuộc vào độ lớn bộ đệm thu của thực thể TCP nhận.

Cơ chế phát lại thích nghi: Để đảm bảo kiểm tra và khắc phục lỗi trong việc trao đổi dữ liệu qua liên mạng, TCP phải có cơ chế đồng hồ kiểm tra phát (Time Out) và cơ chế phát lại (Retransmission) mềm dẻo, phụ thuộc vào thời gian trễ thực của môi trường truyền dẫn cụ thể. Thời gian trễ toàn phần RTT (Round Trip Time) được xác định bắt đầu từ thời điểm phát gói dữ liệu cho đến khi nhận được xác nhận của thực thể đối tác, là yếu tố quyết định giá trị của đồng hồ kiểm tra phát Tout. Như vậy Tout phải lớn hơn hoặc bằng RTT.

Cơ chế điều khiển tắc nghẽn: Hiện tượng tắc nghẽn dữ liệu thể hiện ở việc gia tăng thời gian trễ của dữ liệu khi chuyển qua mạng. Để hạn chế khả năng dẫn đến tắc nghẽn dữ liệu trong mạng, điều khiển lưu lượng dựa trên việc thay đổi độ lớn của sổ phát.

Thiết lập và huỷ bỏ liên kết: TCP là một giao thức hướng liên kết, tức là cần phải thiết lập một liên kết giữa một cặp thực TCP trước khi truyền dữ liệu. Sau khi liên kết được thiết lập, những giá trị cổng (Port) hoạt động như một nhận dạng logic được sử dụng nhận dạng mạch ảo (Virtual Circuit). Trên kênh ảo dữ liệu được truyền song công (Full Duplex). Liên kết TCP được duy trì trong thời gian truyền dữ liệu. Kết thúc truyền, liên kết TCP được giải phóng, các tài nguyên như bộ nhớ, các bảng trạng thái.. cũng được giải phóng.

Thiết lập liên kết TCP: Được thực hiện trên cơ sở phương thức bắt tay ba bước (Three - Way Handshake):



Hình 5. 11 Quá trình thiết lập và kết thúc liên kết TCP 3 bước

Bước 1: Như hình 2.9 yêu cầu liên kết luôn được trạm nguồn khởi tạo tiến trình bằng cách gửi một gói TCP với cờ SYN=1 và chứa giá trị khởi tạo số tuần tự ISN của Client. Giá trị ISN này là một số 4 byte không dấu và được tăng mỗi khi liên kết được yêu cầu (giá trị này quay về 0 khi nó tới giá trị 232). Trong thông điệp SYN này còn chứa số hiệu cổng TCP của phần mềm dịch vụ mà tiến trình trạm muốn liên kết.

Mỗi thực thể liên kết TCP đều có một giá trị ISN mới, số này được tăng theo thời gian. Vì một liên kết TCP có cùng số hiệu cổng và cùng địa chỉ IP được dùng lại nhiều lần, do đó việc thay đổi giá trị ISN ngăn không cho các liên kết dùng lại các dữ liệu đã cũ (Stale) vẫn còn được truyền từ một liên kết cũ và có cùng một địa chỉ liên kết.

Bước 2: Khi thực thể TCP của phần mềm dịch vụ nhận được thông điệp SYN, nó gửi lại gói SYN cùng giá trị ISN của nó và đặt cờ ACK=1 trong trường hợp sẵn sàng

nhận liên kết. Thông điệp này còn chứa giá trị ISN của tiến trình trạm trong trường hợp số tuần tự nhận để báo rằng thực thể dịch vụ đã nhận được giá trị ISN của tiến trình trạm.

Bước 3: Tiến trình trạm trả lời lại gói SYN của thực thể dịch vụ bằng một thông báo trả lời ACK. Bằng cách này, các thực thể TCP trao đổi một cách tin cậy các giá trị ISN của nhau và có thể bắt đầu trao đổi dữ liệu. Không có thông điệp nào trong ba bước trên chứa bất kỳ dữ liệu gì, tất cả thông tin trao đổi đều nằm trong phần Header của thông điệp TCP.

Kết thúc liên kết: Khi có nhu cầu kết thúc liên kết TCP, ví dụ A gửi yêu cầu kết thúc liên kết với FIN=1. Vì liên kết TCP là song công (Full-Duplex) nên mặc dù nhận được yêu cầu kết thúc liên kết của A, thực thể B vẫn có thể tiếp tục truyền cho đến khi B không còn số liệu để gửi và thông báo cho A bằng yêu cầu kết thúc liên kết với FIN=1. Khi thực thể TCP đã nhận được thông điệp FIN và sau khi đã gửi thông điệp FIN của mình, liên kết TCP thực sự kết thúc. Như vậy cả hai trạm phải đồng ý giải phóng liên kết TCP bằng cách gửi cờ FIN=1 trước khi chấm dứt liên kết xảy ra, việc này bảo đảm dữ liệu không bị thất lạc do đơn phương đột ngột chấm dứt liên lạc.

Truyền và nhận dữ liệu: Sau khi liên kết được thiết lập giữa một cặp thực thể TCP, các thực thể truyền dữ liệu. Liên kết TCP dữ liệu có thể được truyền theo hai hướng. Khi nhận một khối dữ liệu cần chuyển đi từ người sử dụng, TCP sẽ lưu trữ tại bộ đệm. Nếu cờ PUST được xác lập thì toàn bộ dữ liệu trong bộ đệm sẽ được gửi đi dưới dạng TCP Segment. Nếu PUST không được xác lập thì dữ liệu trong bộ đệm vẫn chờ gửi đi khi có cơ hội thích hợp.

Bên nhận, dữ liệu sẽ được gửi vào bộ đệm. Nếu dữ liệu trong bộ đệm được đánh dấu bởi cờ PUST thì toàn bộ dữ liệu trong bộ đệm sẽ được gửi lên cho người sử dụng. Ngược lại, dữ liệu vẫn được lưu trong bộ đệm. Nếu dữ liệu khẩn cần phải chuyển gấp thì cờ URGENT được xác lập và đánh dấu dữ liệu bằng bit URG để báo dữ liệu khẩn cần được chuyển gấp.

5.7. Tổng kết và bài tập ứng dụng

5.7.1. Wireshark Lab : TCP

1. Hỏi Số hiệu cổng TCP và địa chỉ IP được sử dụng bởi máy tính client (nguồn) là gì, tức thứ đang truyền file tới gaia.cs.umass.edu?

Trả lời:

Số hiệu cổng TCP: 49695 Địa chỉ IP: 192. 168. 1. 35

```

+ Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (0x06)
+ Header checksum: 0x68e2 [correct]
  Source: 192.168.1.35 (192.168.1.35)
  Destination: 128.119.245.12 (128.119.245.12)
  Transmission Control Protocol, Src Port: 49695 (49695), Dst Port: http (80), Seq: 1, Ack: 1, Len: 1452
  Source port: 49695 (49695)
  Destination port: http (80)
  [Stream index: 0]
  Sequence number: 1 (relative sequence number)

```

2. Hỏi địa chỉ IP của gaia.cs.umass.edu là gì? Số hiệu của cổng nó đang gửi và nhận các phần TCP cho kết nối này là gì?

Trả lời:

Địa chỉ IP: 128.119.245.12 Số hiệu cổng: 80

3. Số hiệu cổng TCP và địa chỉ IP được sử dụng bởi máy tính client của bạn (nguồn) để trao đổi file tới gaia.cs.umass.edu là gì?

Trả lời:

Số hiệu cổng TCP: 49695 Địa chỉ IP: 192.168.1.35

4. Số hiệu các chuỗi của phần TCP SYN được sử dụng để khởi tạo kết nối TCP giữa máy tính client và gaia.cs.umass.edu là gì? Nó là gì trong các phần đó, thứ định danh các phần như 1 phần SYN?

Trả lời:

Số hiệu chuỗi: 0 Bit cờ trường SYN: 1

```

  Transmission Control Protocol, Src Port: http (80), Dst Port: 49695 (49695), Seq: 0, Ack: 1, Len: 0
  Source port: http (80)
  Destination port: 49695 (49695)
  [Stream index: 0]
  Sequence number: 0 (relative sequence number)
  Acknowledgement number: 1 (relative ack number)
  Header length: 32 bytes
  Flags: 0x12 (SYN, ACK)
    0... .... = Congestion Window Reduced (CWR): Not set
    .0... .... = ECN-Echo: Not set
    ..0.... = Urgent: Not set
    ...1.... = Acknowledgement: Set
    ....0... = Push: Not set
    .....0.. = Reset: Not set
    + .... .1. = Syn: Set
    .... ..0 = Fin: Not set
  Window size: 5840

```

5. Số hiệu chuỗi của phần SYNACK gửi bởi gaia.cs.umass.edu tới máy tính client để phản hồi SYN là gì? Giá trị của trường ACKnowledgement trong phần SYNACK là gì? gaia.cs.umass.edu xác định giá trị đó như thế nào? Nó là gì trong phần mà dùng để định danh phần như 1 phần SYSACK?

Trả lời:

Số hiệu chuỗi của phần SYNACK gửi bởi gaia.cs.umass.edu tới máy tính client để phản hồi SYN : 0

Giá trị của trường ACKnowledgement trong phần SYNACK: 1

Bit cờ của trường ACK = 1 và bit cờ trường SYN: 1, chúng được định danh phần nhứ 1 phần SYNACK.

No.	Time	Source	Destination	Protocol	Info
19	15.238799	192.168.1.35	128.119.245.12	TCP	49695 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
20	15.554274	128.119.245.12	192.168.1.35	TCP	http > 49695 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1452 WS=2
21	15.554467	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=1 Ack=1 Win=66792 Len=0
22	15.554769	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=1 Ack=1 Win=66792 Len=1452
23	15.554792	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=1453 Ack=1 Win=66792 Len=1452
24	15.893731	128.119.245.12	192.168.1.35	TCP	http > 49695 [ACK] Seq=1 Ack=1453 Win=8760 Len=0
25	15.893882	192.168.1.35	128.119.245.12	TCP	49695 > http [PSH, ACK] Seq=2905 Ack=1 Win=66792 Len=1452
26	15.893900	128.119.245.12	192.168.1.35	TCP	49695 > http [ACK] Seq=2905 Ack=1453 Win=66792 Len=1452

internet Protocol, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.35 (192.168.1.35)

Transmission Control Protocol, Src Port: http (80), Dst Port: 49695 (49695), Seq: 0, Ack: 1, Len: 0

Source port: http (80)
 Destination port: 49695 (49695)
 [Stream index: 0]

Sequence number: 0 (relative sequence number)
 Acknowledgement number: 1 (relative ack number)
 Header length: 32 bytes

Flags: 0x12 (SYN, ACK)

- 0 = Congestion Window Reduced (CWR): Not set
- = ECN-Echo: Not set
- ..0 = Urgent: Not set
- ...1 = Acknowledgement: Set
- 0... = Push: Not set
-0.. = Reset: Not set

.... .1. = Syn: Set
0 = Fin: Not set

Window size: 5840

0000 00 1f 29 90 03 8f 00 02 cf 7e 13 de 08 00 45 00 ..)..... ~....E.
 0010 00 34 00 00 40 00 2b 06 18 75 80 77 f5 0c c0 a8 .4..@.+..U.W....

6. Số hiệu chuỗi của phần TCP chứa lệnh HTTP POST là gì?

Trả lời:

Số hiệu chuỗi của phần TCP chứa lệnh HTTP POST : 1

No.	Time	Source	Destination	Protocol	Info
19	15.238799	192.168.1.35	128.119.245.12	TCP	49695 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
20	15.554274	128.119.245.12	192.168.1.35	TCP	http > 49695 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1452 WS=2
21	15.554467	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=1 Ack=1 Win=66792 Len=0
22	15.554769	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=1 Ack=1 Win=56/92 Len=1452
23	15.554792	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=1453 Ack=1 Win=66792 Len=1452
24	15.893731	128.119.245.12	192.168.1.35	TCP	http > 49695 [ACK] Seq=1 Ack=1453 Win=8760 Len=0
25	15.893882	192.168.1.35	128.119.245.12	TCP	49695 > http [PSH, ACK] Seq=2905 Ack=1 Win=66792 Len=1452
26	15.893903	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=2906 Ack=1 Win=66792 Len=1452

④ Ethernet II, Src: Hewlett_P_90:03:8f (00:1f:29:90:03:8f), Dst: ZygateCo_7e:13:de (00:02:cf:7e:13:de)

⑤ Internet Protocol, Src: 192.168.1.35 (192.168.1.35), Dst: 128.119.245.12 (128.119.245.12)

Transmission Control Protocol, Src Port: 49695 (49695), Dst Port: http (80), Seq: 1, Ack: 1, Len: 1452

Source port: 49695 (49695)
 Destination port: http (80)
 [Stream index: 0]
 Sequence number: 1 (relative sequence number)
 [Next Sequence number: 1453 (relative sequence number)]
 Acknowledgement number: 1 (relative ack number)
 Header length: 20 bytes

Flags: 0x10 (ACK)
 0.... = Congestion Window Reduced (CWR): Not set
 .0.... = ECN-Echo: Not set
 ..0.... = Urgent: Not set
 ...1.... = Acknowledgement: Set
0.... = Push: Not set
0.. = Reset: Not set
0..0 = Syn: Not set
0..0 = Fin: Not set
 window size: 66707 (scaled)

7. Xem xét phần TCP chứa HTTP POST như là phần đầu tiên trong kết nối TCP. Các Số hiệu chuỗi của 6 phần đầu tiên trong kết nối TCP (bao gồm cả phần chứa HTTP POST) là gì? Thời gian mỗi phần gửi là bao lâu? Khi nào ACK cho mỗi phần được nhận? Đưa sự khác biệt giữ mỗi phần TCP được gửi, và khi acknowledgement của nó được nhận, giá trị RTT cho mỗi một trong 6 phần đó là bao nhiêu? Giá trị EstimatedRTT (xem trang 249 trong tài liệu) sau khi nhận mỗi ACK là bao nhiêu? Cho rằng giá trị của EstimatedRTT là bằng với giá trị RTT đo được trong segment đầu tiên, và sau đó được tính toán sử dụng đẳng thức EstimatedRTT trong trang 249 cho các segment đến sau. Chú ý: Wireshark có 1 tính chất tốt là cho phép bạn vẽ đồ thị RTT cho mỗi các phần TCP được gửi. Chọn TCP segment trong cửa sổ “listing of captured packets”, tức thứ được gửi từ client tới server gaia.cs.umass.edu . Sau đó chọn Statistics->TCP Stream Graph->Round Trip Time Graph.

Trả lời:

Các số hiệu của 6 phần đầu tiên trong kết nối TCP:

- 1: số hiệu chuỗi phần 1
- 2: số hiệu chuỗi phần 1453
- 3: số hiệu chuỗi phần 2905
- 4: số hiệu chuỗi phần 4357
- 5: số hiệu chuỗi phần 5809
- 6: số hiệu chuỗi phần 7261

HTTP POST segment có các số thứ tự: 22, 23, 25, 26, 28, 29

20 0.315475	128.119.245.12	192.168.1.35	TCP	http > 49695 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1452 WS=2
21 0.315668	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=1 Ack=1 Win=66792 Len=0
22 0.315970	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=1 Ack=1 Win=66792 Len=1452
23 0.315993	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=1453 Ack=1 Win=66792 Len=1452
24 0.654932	128.119.245.12	192.168.1.35	TCP	http > 49695 [ACK] Seq=1 Ack=1453 Win=8760 Len=0
25 0.655083	192.168.1.35	128.119.245.12	TCP	49695 > http [PSH, ACK] Seq=2905 Ack=1 Win=66792 Len=1452
26 0.655103	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=4357 Ack=1 Win=66792 Len=1452
27 0.681107	128.119.245.12	192.168.1.35	TCP	http > 49695 [ACK] Seq=1 Ack=2905 Win=11680 Len=0
28 0.681228	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=5809 Ack=1 Win=66792 Len=1452
29 0.681251	192.168.1.35	128.119.245.12	TCP	49695 > http [PSH, ACK] Seq=7261 Ack=1 Win=66792 Len=1452
30 1.005242	128.119.245.12	192.168.1.35	TCP	http > 49695 [ACK] Seq=1 Ack=4357 Win=14600 Len=0
31 1.005382	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=8713 Ack=1 Win=66792 Len=1452
32 1.005403	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=10165 Ack=1 Win=66792 Len=1452
33 1.047355	128.119.245.12	192.168.1.35	TCP	http > 49695 [ACK] Seq=1 Ack=5809 Win=17520 Len=0
34 1.047458	192.168.1.35	128.119.245.12	TCP	49695 > http [PSH, ACK] Seq=11617 Ack=1 Win=66792 Len=1452
35 1.047478	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=13069 Ack=1 Win=66792 Len=1452
36 1.063670	128.119.245.12	192.168.1.35	TCP	http > 49695 [ACK] Seq=1 Ack=7261 Win=20440 Len=0
37 1.063756	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=14521 Ack=1 Win=66792 Len=1452
38 1.063774	192.168.1.35	128.119.245.12	TCP	49695 > http [PSH, ACK] Seq=15973 Ack=1 Win=66792 Len=1452
39 1.106774	128.119.245.12	192.168.1.35	TCP	http > 49695 [ACK] Seq=1 Ack=8713 Win=23360 Len=0
40 1.106900	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=17425 Ack=1 Win=66792 Len=1452
41 1.106921	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=18877 Ack=1 Win=66792 Len=1452

ACK segment có các số thứ tự: 24, 27, 30, 33, 36, 39

21 0.315668	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=1 Ack=1 Win=66792 Len=0
22 0.315970	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=1 Ack=1 Win=66792 Len=1452
23 0.315993	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=1453 Ack=1 Win=66792 Len=1452
24 0.654932	128.119.245.12	192.168.1.35	TCP	http > 49695 [ACK] Seq=1 Ack=1453 Win=8760 Len=0
25 0.655083	192.168.1.35	128.119.245.12	TCP	49695 > http [PSH, ACK] Seq=2905 Ack=1 Win=66792 Len=1452
26 0.655103	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=4357 Ack=1 Win=66792 Len=1452
27 0.681107	128.119.245.12	192.168.1.35	TCP	http > 49695 [ACK] Seq=1 Ack=2905 Win=11680 Len=0
28 0.681228	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=5809 Ack=1 Win=66792 Len=1452
29 0.681251	192.168.1.35	128.119.245.12	TCP	49695 > http [PSH, ACK] Seq=7261 Ack=1 Win=66792 Len=1452
30 1.005242	128.119.245.12	192.168.1.35	TCP	http > 49695 [ACK] Seq=1 Ack=4357 Win=14600 Len=0
31 1.005382	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=8713 Ack=1 Win=66792 Len=1452
32 1.005403	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=10165 Ack=1 Win=66792 Len=1452
33 1.047355	128.119.245.12	192.168.1.35	TCP	http > 49695 [ACK] Seq=1 Ack=5809 Win=17520 Len=0
34 1.047458	192.168.1.35	128.119.245.12	TCP	49695 > http [PSH, ACK] Seq=11617 Ack=1 Win=66792 Len=1452
35 1.047478	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=13069 Ack=1 Win=66792 Len=1452
36 1.063670	128.119.245.12	192.168.1.35	TCP	http > 49695 [ACK] Seq=1 Ack=7261 Win=20440 Len=0
37 1.063756	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=14521 Ack=1 Win=66792 Len=1452
38 1.063774	192.168.1.35	128.119.245.12	TCP	49695 > http [PSH, ACK] Seq=15973 Ack=1 Win=66792 Len=1452
39 1.106774	128.119.245.12	192.168.1.35	TCP	http > 49695 [ACK] Seq=1 Ack=8713 Win=23360 Len=0
40 1.106900	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=17425 Ack=1 Win=66792 Len=1452
41 1.106921	192.168.1.35	128.119.245.12	TCP	49695 > http [ACK] Seq=18877 Ack=1 Win=66792 Len=1452
43 1.346214	128.119.245.12	192.168.1.35	TCP	http > 49695 [ACK] Seq=1 Ack=10165 Win=26280 Len=0
44 1.346329	192.168.1.35	128.119.245.12	TCP	49695 > http [PSH, ACK] Seq=20329 Ack=1 Win=66792 Len=1452

	Thời gian gửi	ACK	RTT
Segment 1	0,315970	0,654932	0,338962
Segment 2	0,315993	0,681107	0,365114
Segment 3	0,655083	1,005242	0,350159
Segment 4	0,655103	1,047355	0,392252
Segment 5	0,681228	1,063670	0,382442
Segment 6	0,681251	1,106774	0,425523

Tính toán giá trị EstimatedRTT :

$$\text{EstimatedRTT} = 0.875 * \text{EstimatedRTT} + 0.125 * \text{SampleRTT}$$

$$\text{EstimatedRTT of Segment 1} = 0.338962$$

$$\text{EstimatedRTT of Segment 2} = 0.875 * 0.338962 + 0.125 * 0.365114 = 0.342231$$

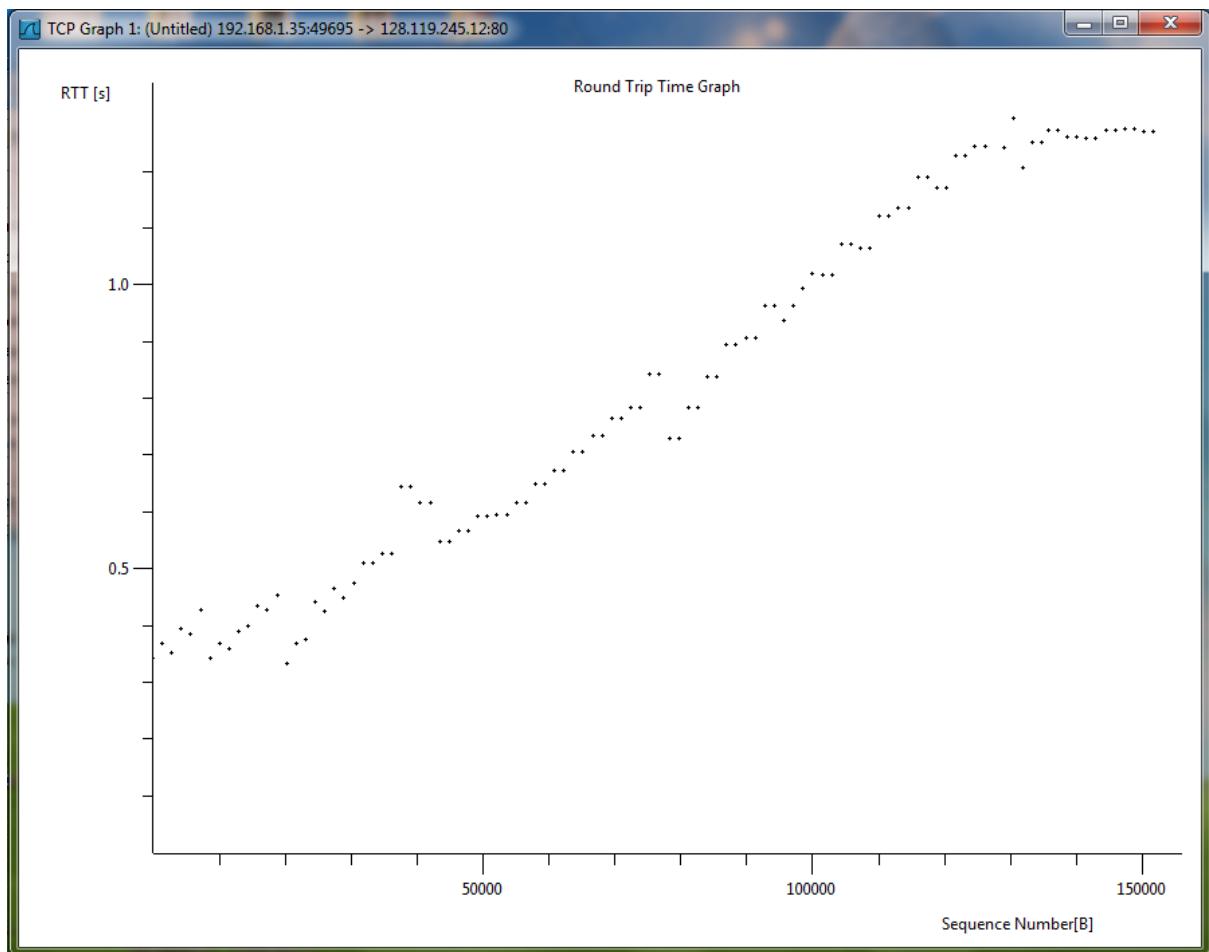
$$\text{EstimatedRTT of Segment 3} = 0.875 * 0.342231 + 0.125 * 0.350159 = 0.343222$$

$$\text{EstimatedRTT of Segment 4} = 0.875 * 0.343222 + 0.125 * 0.392252 = 0.349351$$

$$\text{EstimatedRTT of Segment 5} = 0.875 * 0.349351 + 0.125 * 0.382442 = 0.353487$$

$$\text{EstimatedRTT of Segment 6} = 0.875 * 0.353487 + 0.125 * 0.425523 = 0.362492$$

- Round Trip Time Graph



8. Độ rộng của mỗi một trong số 6 TCP segment đầu tiên là bao nhiêu?

Trả lời:

Độ rộng của segment thứ nhất là: 1452 bytes

Độ rộng của segment thứ hai là: 1452 bytes

Độ rộng của segment thứ ba là: 1452 bytes

Độ rộng của segment thứ tư là: 1452 bytes

Độ rộng của segment thứ năm là: 1452 bytes

Độ rộng của segment thứ sáu là: 1452 bytes

9. Giá trị nhỏ nhất của không gian đệm có thể ở phần nhận cho toàn bộ trace? Có thể xảy ra sự thiếu không gian đệm vùng nhận khi tắc nghẽn đường gửi không?

Trả lời:

Giá trị nhỏ nhất của không gian đệm có thể ở phần nhận cho toàn bộ trace là 66792 bytes (kích thước của window trong khởi tạo kết nối đầu tiên). Không xảy ra hiện tượng thiếu không gian đệm vùng nhận khi tắc nghẽn đường gửi .

10. Các segment có được tái truyền đi trong file trace? Bạn kiểm tra cái gì (trong trace) để trả lời câu hỏi này?

Trả lời:

Các segment có thể được tái truyền đi trong file trace. Có thể kiểm tra là 1 số số hiệu chuỗi được gửi đi hai lần hoặc nhiều hơn.

11. Bao nhiêu dữ liệu receiver báo nhận trong ACK? Bạn có thể nhận ra các trường hợp nơi mà receiver đang báo nhận mỗi khi segment khác được nhận không?

	Acknowledged sequence number	Acknowledged data
Ack 1	1	1452
Ack 2	1453	1452
Ack 3	2905	1452
Ack 4	4357	1452
Ack 5	5809	1452
Ack 6	7261	1452
Ack 7	8713	1452
...

12. Lưu lượng (số byte trao đổi mỗi đơn vị thời gian) cho kết nối TCP này là bao nhiêu? Giải thích bạn tính toán giá trị này như thế nào ?

Trả lời:

Lưu lượng trung bình của 1 kết nối = $(0,75*W)/RTT$

W: window size (bytes)

RTT : round trip time hiện tại (seconds)

Ví dụ: Sử dụng các số liệu ở bài 7, ta có lưu lượng trung bình của kết nối TCP đầu tiên:

$$W = 66792 \text{ bytes}$$

$$RTT = 0,338962 \text{ seconds}$$

$$\text{Lưu lượng trung bình của kết nối TCP} = (0,75*66792)/0,338962 = 147786,477 \text{ (bytes/sec)}$$

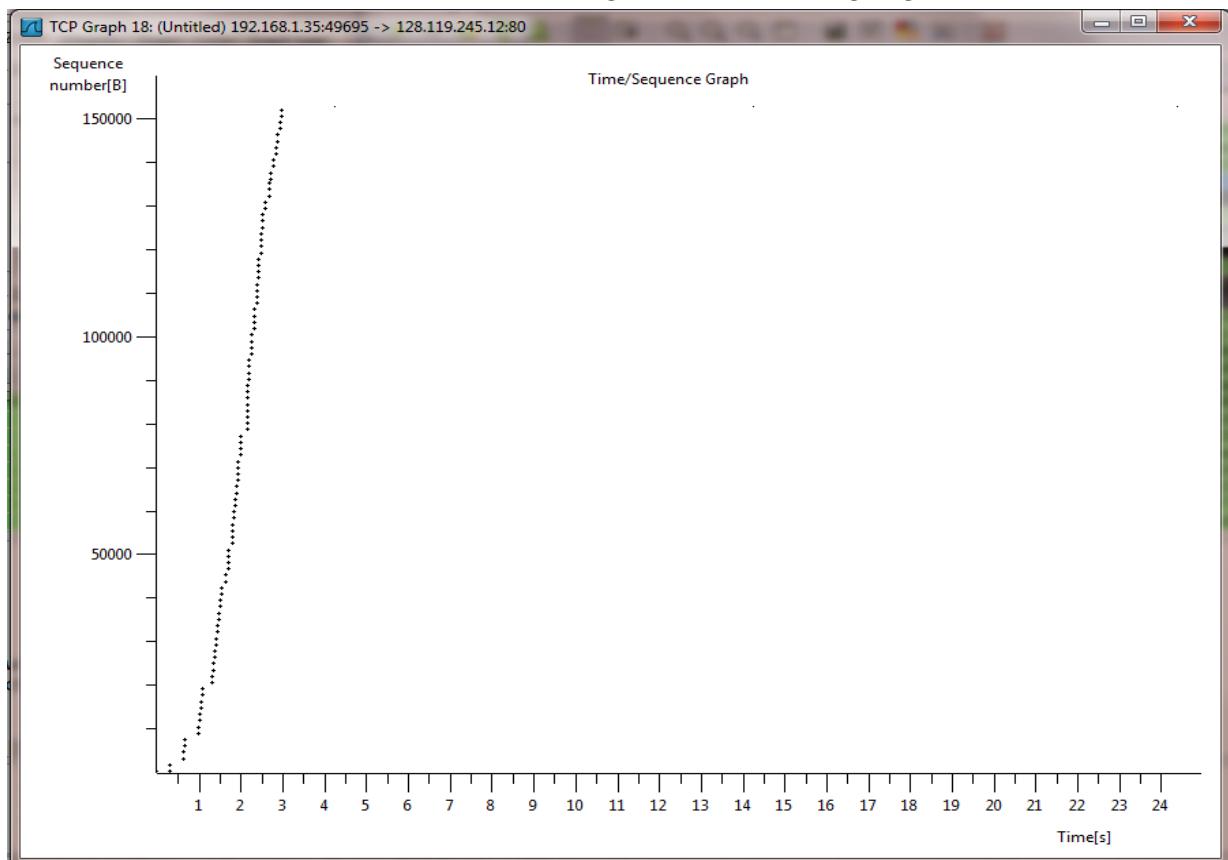
13. Sử dụng công cụ vẽ đồ thị Time-Sequence-Graph (Stevens) để xem số chuỗi trên thời gian vẽ của các segment đang gửi từ client tới server gaia.cs.umass.edu server. Bạn có thể nhận ra đoạn TCP bắt đầu chậm từ lúc nào tới lúc nào, và nơi nào sự trễ tắc

nghẽn đạt được? Dẫn giải con đường mà ở đó dữ liệu được đo khác với hành vi được lý tưởng hóa của TCP, tức thứ mà chúng ta được học trong tài liệu.

Trả lời:

Qua đồ thị Time-Sequence-Graph (Stevens) ta có thể nhận ra đợt TCP bắt đầu chậm và nơi có thể tránh tắc nghẽn. Vì đồ thị chỉ ra sơ đồ trên mạng, những điểm tắc nghẽn có thể xảy ra.

Khi TCP kết nối được giữa Sender và Reciever, nó có 1 giá trị duy nhất(chính là windows size), nó cho biết kích thước thông tin có thể được gửi giữa Sender và Receiver.

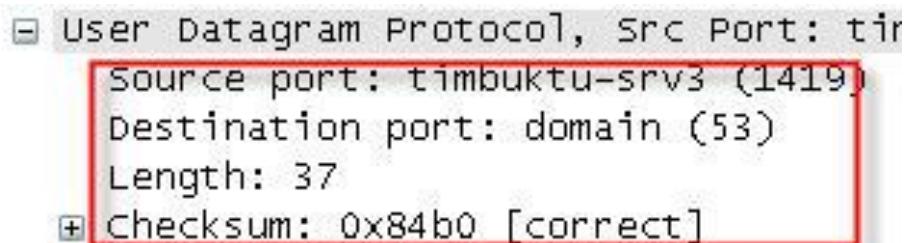


5.7.2. Wireshark Lab : UDP

1. Chọn 1 packet. Từ packet này, xác định có bao nhiêu trường trong UDP header.

Trả lời:

4 fields in UDP header. that is Source Port, Destination Port, Length, CheckSum.

A screenshot of the Wireshark interface showing the details of a User Datagram Protocol (UDP) header. The fields listed are: Source port: timbuktu-srv3 (1419), Destination port: domain (53), Length: 37, and Checksum: 0x84b0 [correct]. The last three fields are highlighted with a red border.

2. Từ trường nội dung packet, xác định độ rộng (byte) của mỗi trường UDP header.

Trả lời:

UDP gồm 4 trường, kích thước của mỗi trường:

- Source port number: 2 bytes
- Destination port number: 2 bytes
- Datagram size(Length) : 2 bytes
- Checksum : 2 bytes

3. Giá trị trong trường Length là độ dài của cái gì? Xác thực khăng định của bạn với gói UDP đã bắt.

Trả lời:

Trường Length xác định độ dài của toàn bộ datagram: header và data. Độ dài của trường Length trong trường hợp trên là 37 .

4. Giá trị tối đa các byte có thể bao gồm trong 1 phần tải có ích UDP là bao nhiêu?

Trả lời:

Kích thước tối đa của khối dữ liệu môi trường hệ thay đổi phụ thuộc vào điều hành.

Với trường kích thước 2bytes, kích thước tối đa theo lý thuyết của khối dữ liệu là 65535 ($= 2^{16}-1$) bytes.

5. Số hiệu cổng nguồn lớn nhất có thể là bao nhiêu?

Trả lời:

Số hiệu cổng nguồn lớn nhất có thể là 65535($= 2^{16}-1$).

6. Số hiệu giao thức cho UDP là bao nhiêu? Đưa câu trả lời của bạn trong cả hệ 16 và 10.

Trả lời:

Số hiệu giao thức cho UDP là: 0x11(hệ 16), 17(hệ 10).

```

Time to live: 128
Protocol: UDP (0x11)
⊕ Header checksum: 0xf178 [correct]
Source: ppp-58-10-77-186.revip2.asianet.co.th (58.10.77.186)
Destination: dns2.asianet.co.th (203.144.207.49)
User Datagram Protocol, Src Port: timbuktu-srv3 (1419), Dst Po
Source port: timbuktu-srv3 (1419)
Destination port: domain (53)
Length: 37
⊖ Checksum: 0x84b0 [correct]

```

8. Tìm “UDP” trên Google và xác định các trường trong tính toán UDP checksum.

Trả lời

Pseudo Header Field (trường header giả) được sử dụng trong tính toán UDP checksum, nó bao gồm các trường: the source address, the destination address, the protocol, and the UDP length. Thủ tục checksum cũng tương tự như trong TCP.

9. Khảo sát 1 cặp packet UDP mà ở đó packet đầu được gửi bởi host của bạn và packet sau là phản hồi tới packet đầu. Biểu diễn mối quan hệ giữa số hiệu cổng trong 2 packet đó.

Trả lời:

Packet thứ nhất: source port: 1801, Destination port: 53.

Packet thứ hai: source port: 53, Destination port is 1801.

10. Câu hỏi thêm:

Bắt 1 gói UDP nhỏ. Xác thực bằng tay checksum trong gói này. Chỉ ra công việc và giải thích tất cả các bước.

- UDP sender:

IP Source Address = 192. 168. 1. 35

Chuyển sang dạng 16 bit = 11000000.10101000.00000001.**00100011**

IP Destination Address = 192. 168. 1. 1

Chuyển sang dạng 16 bit = 11000000.10101000.00000001.**00000001**

Protocol: UDP (0x4c9b) = 0100110010011011

UDP Length: 40 = 010000000

Calculated checksum :

11000000 1010100

+

<u>00000001</u>	<u>00100011</u>
11000001 11001011	

+

<u>11000000</u>	<u>10101000</u>
110000010 01110011	

+

<u>00000001</u>	<u>00000001</u>
110000011 01110100	

+

<u>01001100</u>	<u>10011011</u>
111010000 00001111	

+

<u>111010000 01001111</u>	<u>00000000</u>
→ Lấy phần bù	

000101111 10110000 : UDP Sender

- UDP Receiver
IP Source Address = 192. 168. 1. 1

Chuyển sang dạng 16 bit = 11000000.10101000.00000001.00000001

IP Destination Address = 192. 168. 1. 35

seperate into 16 bit = 11000000.10101000.00000001.00100011

Protocol: UDP (0x4c9b) = 0100110010011011

UDP Length: 40 = 01000000

Calculated checksum :

11000000 10101000

+

<u>00000001</u>	<u>00000001</u>
11000001 10101001	

<u>11000000</u>	<u>10101000</u>
110000010 01010001	
	+
<u>00000001</u>	<u>00100011</u>
110000011 01110100	
	+
<u>01001100</u>	<u>10011011</u>
111010000 00001111	
	+
<u>00000000</u>	<u>01000000</u>
111010000 01001111 : kết quả Receiver	
	+
<u>000101111 01110000</u>	<u>: kết quả Sender</u>
1111111111111111	: Không có lỗi !

TÓM TẮT NỘI DUNG CÓT LÕI.

- Vai trò chức năng tầng giao vận
 - Các dịch vụ cung cấp cho tầng phiên
 - Chất lượng dịch vụ
 - Các lớp giao thức cho tầng giao vận
 - Chất lượng dịch vụ

BÀI TẬP ÚNG DỤNG:

1. Một kênh 4kHz không nhiễu được lấy mẫu cách 1 ms. Tốc độ dữ liệu tối đa là bao nhiêu?
 2. Các kênh truyền hình rộng 6Mhz. Có thể gửi được bao nhiêu bit/giây nếu các tín hiệu số 4 cấp được sử dụng? Giả sử kênh truyền không nhiễu.
 3. Nếu một tín hiệu nhị phân được gửi trên một kênh 3kHz có tỷ số tín hiệu/ồn là 20dB, tốc độ dữ liệu tối đa có thể đạt được là bao nhiêu?
 4. Cần đến tỉ số tín hiệu/tiếng ồn nào để đặt một sóng mang T1 trên một đường dây 50kHz?

5. Có bao nhiêu băng thông trong 0,1 micron phô với bước sóng 1 micron?
6. Một gói lớp phía trên được tách thành 10 frame, từng frame có khả năng đến không bị hỏng là 80%. Nếu việc kiểm soát không được thực hiện bởi giao thức liên kết dữ liệu, thông báo phải được gửi trung bình bao nhiêu lần để hoàn tất mọi thứ?
7. Một kênh 8kHz không nhiều được lấy mẫu cách 1 ms. Tốc độ dữ liệu tối đa là bao nhiêu?
8. Các kênh truyền hình rộng 8Mhz. Có thể gửi được bao nhiêu bit/giây nếu các tín hiệu số 4 cấp được sử dụng? Giả sử kênh truyền không nhiễu.
9. Cần đến tỉ số tín hiệu/tiếng ồn nào để đặt một sóng mang T1 trên một đường dây 100kHz 10. Nếu một tín hiệu nhị phân được gửi trên một kênh 6kHz có tỷ số tín hiệu/ồn là 20dB, tốc độ dữ liệu tối đa có thể đạt được là bao nhiêu?

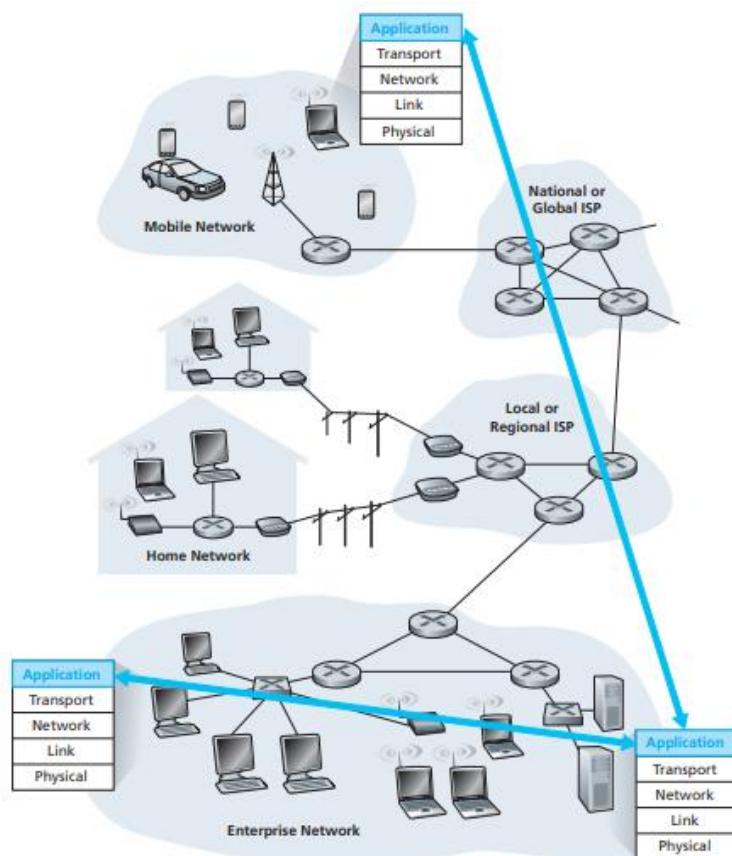
Chương 6. TẦNG ỨNG DỤNG

Mục tiêu:

- Chương này sẽ tìm hiểu một số ứng dụng mạng phổ biến hiện nay, chủ yếu tập trung vào giao thức hoạt động của chúng.
- Ví dụ đầu tiên được xem xét là dịch vụ tên phân tán, dịch vụ đầu tiên được cài đặt trong một mạng máy tính. Về thực chất dịch vụ tên là cái mà các ứng dụng khác phải phụ thuộc vào. Một server phục vụ tên thường được sử dụng bởi các ứng dụng khác hơn là bởi con người. Sau đó, các ứng dụng mạng truyền thống và phổ biến sẽ được giới thiệu, bao gồm các dịch vụ MAIL, WEB và FTP
- Cũng cần nói trước rằng, những dịch vụ mạng vừa nói sẽ dựa trên hai giao thức vận chuyển đã được đề cập trong chương trước là TCP và UDP.

6.1. Nguyên tắc của các ứng dụng mạng

Cốt lõi của phát triển ứng dụng mạng là viết các chương trình chạy trên các hệ thống đầu cuối khác nhau và liên lạc với nhau qua mạng. Ví dụ, trong ứng dụng Web có hai chương trình riêng biệt giao tiếp với nhau: chương trình duyệt đang chạy trong máy của người dùng (máy tính để bàn, máy tính xách tay, máy tính bảng, điện thoại thông minh, v.v.); và chương trình máy chủ Web đang chạy trong máy chủ Web. Một ví dụ khác, trong một hệ thống chia sẻ tệp P2P có một chương trình trong mỗi máy tham gia vào quá trình chia sẻ tệp tin.



Theo mô hình xử lý dữ liệu thì mạng máy tính được chia làm các loại mạng khác nhau như mạng ngang hàng (Peer to peer), mạng khách - chủ (Client – Server) và mạng theo mô hình lai (*Hybrid*).

6.1.1. Mô hình khách/chủ

Mô hình Client/Server mô tả các dịch vụ mạng và các ứng dụng được sử dụng để truy nhập các dịch vụ. Là mô hình phân chia các thao tác thành hai phần: phía Client cung cấp cho người sử dụng một giao diện để yêu cầu dịch vụ từ mạng và phía Server tiếp nhận các yêu cầu từ phía Client và cung cấp các dịch vụ một cách thông suốt cho người sử dụng.

Chương trình Server được khởi động trên một máy chủ và ở trạng thái sẵn sàng nhận các yêu cầu từ phía Client. Chương trình Client cũng được khởi động một cách độc lập với chương trình Server. Yêu cầu dịch vụ được chương trình Client gửi đến máy chủ cung cấp dịch vụ và chương trình Server trên máy chủ sẽ đáp ứng các yêu cầu của Client. Sau khi thực hiện các yêu cầu từ phía Client, Server sẽ trở về trạng thái chờ các yêu cầu khác.

Trong mô hình Client/Server nhiều lớp, quá trình xử lý được phân tán trên 3 lớp khác nhau với các chức năng riêng biệt. Mô hình này thích hợp cho việc tổ chức hệ thống thông tin trên mạng Internet/ Intranet. Phát triển mô hình 3 lớp sẽ khắc phục được một số hạn chế của mô hình 2 lớp. Các hệ cơ sở dữ liệu được cài đặt trên các máy chủ Web Server và có thể được truy nhập không hạn chế các ứng dụng và số lượng người dùng.

Lớp khách (Clients) cung cấp dịch vụ trình bày (Presentation Services), giao tiếp người sử dụng với lớp giao dịch thông qua trình duyệt Browser hay trình ứng dụng để thao tác và xử lý dữ liệu. Giao diện người sử dụng là trình duyệt Internet Explorer hay Netscape.

Lớp giao dịch (Business) cung cấp các dịch vụ quản trị, tổ chức và khai thác cơ sở dữ liệu. Các component trước đây được cài đặt trên lớp khách, nay được cài đặt trên lớp giao dịch. Ví dụ, một người sử dụng trên máy khách đặt mua hàng, lớp giao dịch kiểm tra mã mặt hàng để quyết định tiếp tục bán hay không bán. Thành phần của lớp giao dịch trong mô hình Internet là Web Server và COM+/MTS. Công nghệ của Microsoft với Web Server là IIS (Internet Information Services) sử dụng ASP để kết nối Client với COM. Web Server giao tiếp với COM+/MTS component qua COM. COM+/MTS component điều khiển tất cả giao tiếp với lớp dữ liệu nguồn thông qua ODBC hoặc OLE - DB.

Lớp nguồn dữ liệu (Data Source) cung cấp các dịch vụ tổ chức và lưu trữ các hệ cơ sở dữ liệu quan hệ. Sẵn sàng cung cấp dữ liệu cho lớp giao dịch. Đặc trưng của lớp này là ngôn ngữ tìm kiếm, truy vấn dữ liệu SQL.

6.1.2. Mô hình ngang hàng (Peer to peer)

Trong mô hình ngang hàng tất cả các máy đều là máy chủ đồng thời cũng là máy khách. Các máy trên mạng chia sẻ tài nguyên không phụ thuộc vào nhau. Mạng ngang hàng thường được tổ chức thành các nhóm làm việc Workgroup. Mô hình này không có quá trình đăng nhập tập trung, nếu đã đăng nhập vào mạng có thể sử dụng tất cả tài nguyên trên mạng. Truy cập vào các tài nguyên phụ thuộc vào người đã chia sẻ các tài nguyên đó, vì vậy có thể phải biết mật khẩu để có thể truy nhập được tới các tài nguyên được chia sẻ.

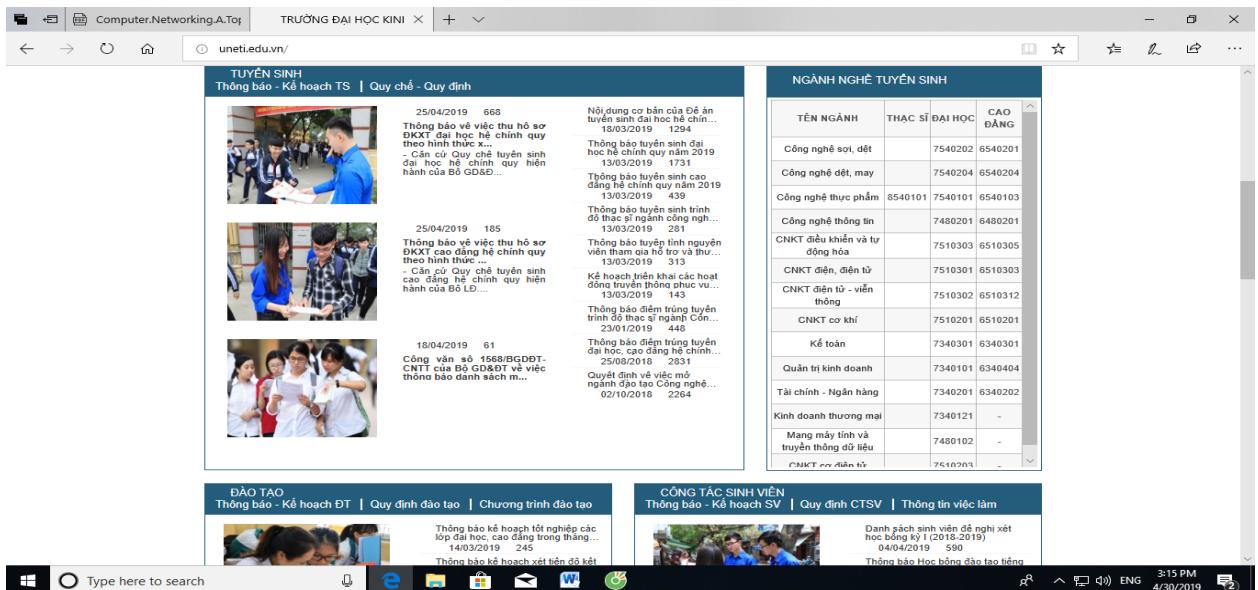
6.1.3. Mô hình lai (Hybrid)

Đây là mô hình kết hợp giữa Client-Server và Peer-to-Peer. Phần lớn các mạng máy tính trên thực tế thuộc mô hình này.

6.2. Web và HTTP

World Wide Web

Ứng dụng Web đã rất thành công, giúp cho nhiều người có thể truy cập Internet đến nỗi Web được hiểu đồng nghĩa với Internet! Có thể hiểu Web như là một tập các client và server hợp tác với nhau và cùng nói chung một ngôn ngữ: HTTP (Hyper Text Transfer Protocol). Đa phần người dùng tiếp xúc với Web thông qua chương trình client có giao diện đồ họa, hay còn gọi là trình duyệt Web (Web browser). Các trình duyệt Web thường được sử dụng nhất là Netscape Navigator (của Netscape) và Internet Explorer (của Microsoft). Hình bên dưới thể hiện trình duyệt Explorer đang trình bày trang chủ của Khoa Công Nghệ Thông Tin - Đại Học Uneti:



Hình 6. 1 Trình duyệt Web Internet Explorer

Bất kỳ trình duyệt Web nào cũng có chức năng cho phép người dùng “mở một URL”. Các URL (Uniform Resource Locators) cung cấp thông tin về vị trí của các đối tượng trên Internet; chúng thường trông giống như sau:

<http://www.Uneti.edu.vn/index.html>

Nếu người dùng mở URL trên, trình duyệt Web sẽ thiết lập một kết nối TCP đến Web Server tại địa chỉ www.Uneti.edu.vn và ngay lập tức tải tập tin index.html về và hiển thị nó. Hầu hết các tập tin trên Web chứa văn bản và hình ảnh, một số còn chứa audio và video clips. Chúng còn có thể chứa các liên kết đến các tập tin khác - được gọi là các liên kết siêu văn bản (hypertext links). Khi người dùng yêu cầu trình duyệt Web mở ra một liên kết siêu văn bản (bằng cách trỏ chuột và click lên liên kết đó), trình duyệt sẽ mở một nối kết mới, tải về và hiển thị một tập tin mới. Vì thế, rất dễ để duyệt từ server này đến server khác trên khắp thế giới để có được hết những thông tin mà người dùng cần.

Khi người dùng chọn xem một trang Web, trình duyệt Web sẽ nạp trang Web đó từ Web server về sử dụng giao thức HTTP chạy trên TCP. Giống như SMTP, HTTP là giao thức hướng ký tự. Về cốt lõi, một thông điệp HTTP có khuôn dạng tổng quát sau:

START_LINE <CRLF>

ME S S AGE_HE ADER <CRLF>

<CRLF>

MESSAGE_BODY <CRLF>

Hàng đầu tiên chỉ ra đây là thông điệp yêu cầu hay trả lời. Nó sẽ chỉ ra “thủ tục cần được thực hiện từ xa” (trong tình huống là thông điệp yêu cầu) hoặc là “trạng thái trả về” (trong tình huống là thông điệp trả lời). Tập hợp các hàng kế tiếp chỉ ra các tùy chọn hoặc tham số nhằm xác định cụ thể tính chất của yêu cầu hoặc trả lời. Phần MESSAGE_HEADER có thể không có hoặc có một vài hàng tham số và được kết thúc bằng một hàng trống. HTTP định nghĩa nhiều kiểu header, một số liên quan đến các thông điệp yêu cầu, một số liên quan đến các thông điệp trả lời và một số lại liên quan đến phần dữ liệu trong thông điệp. Ở đây chỉ giới thiệu một số kiểu thường dùng. Cuối cùng, sau hàng trống là phần nội dung của thông điệp trả lời (MESSAGE_BODY), phần này thường là rỗng trong thông điệp yêu cầu.

6.2.1. Các thông điệp yêu cầu

Hành động	Mô tả
OPTIONS	Yêu cầu thông tin về các tùy chọn hiện có.
GET	Lấy về tài liệu được xác định trong URL
HEAD	Lấy về thông tin thô về tài liệu được xác định trong URL
POST	Cung cấp thông tin cho server
PUT	Tải tài liệu lên server và đặt ở vị trí được xác định trong URL
DELETE	Xóa tài liệu nằm ở vị trí URL trên server
TRACE	Phản hồi lại thông điệp yêu cầu

Hàng đầu tiên của một thông điệp yêu cầu HTTP sẽ chỉ ra 3 thứ: thao tác cần được thực thi, trang Web mà thao tác đó sẽ áp lên và phiên bản HTTP được sử dụng. Bảng sau sẽ giới thiệu một số thao tác phổ biến.

Hai thao tác thường được sử dụng nhiều nhất là GET (lấy một trang Web về) và HEAD (lấy về thông tin của một trang Web). GET thường được sử dụng khi trình duyệt muốn tải một trang Web về và hiển thị nó cho người dùng. HEAD thường được sử dụng để kiểm tra tính hợp lệ của một liên kết siêu văn bản hoặc để xem một trang nào đó có bị thay đổi gì không kể từ lần tải về trước đó.

Ví dụ, dòng START_LINE

GET <http://www.Uneti.edu.vn/index.html> HTTP/1.1

nói rằng: người dùng muốn tải về trên server www.Uneti.edu.vn trang Web có tên index.html và hiển thị nó. Ví dụ trên dùng URL tuyệt đối. Ta cũng có thể sử dụng URL tương đối như sau:

GET /index.html HTTP/1.1 Host: www.Uneti.edu.vn

Ở đây, Host là một trong các trường trong MESSAGE_HEADER.

6.2.2. Các thông điệp trả lời

Giống như các thông điệp yêu cầu, các thông điệp trả lời bắt đầu bằng một hàng START_LINE. Trong trường hợp này, dòng START_LINE sẽ chỉ ra phiên bản HTTP đang được sử dụng, một mã 3 ký số xác định yêu cầu là thành công hay thất bại và một chuỗi ký tự chỉ ra lý do của câu trả lời này. Ví dụ:

START_LINE	
HTTP/1.1	202
Accepted	

chỉ ra server đã có thể thỏa mãn yêu cầu của người dùng.

Còn dòng

HTTP/1.1 404 Not Found

chỉ ra rằng server đã không thể tìm thấy tài liệu như được yêu cầu.

Có năm loại mã trả lời tổng quát với ký số đầu tiên xác định loại mã.

Mã	Loại	Lý do
1xx	Thông tin	Đã nhận được yêu cầu, đang tiếp tục xử lý
2xx	Thành công	Thao tác đã được tiếp nhận, hiểu được và chấp nhận được
3xx	Chuyển hướng	Cần thực hiện thêm thao tác để hoàn tất yêu cầu được đặt ra
4xx	Lỗi client	Yêu cầu có cú pháp sai hoặc không thể được đáp ứng
5xx	Lỗi server	Server thất bại trong việc đáp ứng một yêu cầu hợp lệ

Cũng giống như các thông điệp yêu cầu, các thông điệp trả lời có thể chứa một hoặc nhiều dòng trong phần MESSAGE_HEADER. Những dòng này cung cấp thêm thông tin cho client. Ví dụ, dòng header Location chỉ ra rằng URL được yêu cầu đang có ở vị trí khác. Vì thế, nếu trang Web của Khoa Công Nghệ Thông Tin được di chuyển từ địa chỉ <http://www.Uneti.edu.vn/index.html> sang địa chỉ <http://www.daotao.uneti.edu.vn/index.html> mà người dùng lại truy cập vào URL cũ, thì Web server sẽ trả lời như sau HTTP/1.1 301 Moved Permanently Location: <http://www.uneti.edu.vn/index.html>

Trong tình huống chung nhất, thông điệp trả lời cũng sẽ mang theo nội dung trang Web được yêu cầu. Trang này là một tài liệu HTML, nhưng vì nó có thể chứa dữ liệu không phải dạng văn bản (ví dụ như ảnh GIF), dữ liệu này có thể được mã hóa theo dạng MIME. Một số hàng trong phần MESSAGE_HEADER cung cấp thêm thông tin về nội dung của trang Web, bao gồm Content-Length (số bytes trong phần nội dung), Expires (thời điểm mà nội dung trang Web được xem như lỗi thời), và Last-Modified (thời điểm được sửa đổi lần cuối cùng).

6.2.3. Các kết nối TCP

Nguyên tắc chung của giao thức HTTP là client nối kết đến cổng TCP số 80 tại server, server luôn lắng nghe trên cổng này để sẵn sàng phục vụ client. Phiên bản đầu tiên (HTTP/1.0) sẽ thiết lập một nối kết riêng cho mỗi hạng mục dữ liệu cần tải về từ server. Không khó để thấy rằng đây là cơ chế không mấy hiệu quả: Các thông điệp dùng để thiết lập và giải phóng nối kết sẽ phải được trao đổi qua lại giữa client và server và khi mà tất cả client muốn lấy thông tin mới nhất của một trang Web, server sẽ bị quá tải.

Cải tiến quan trọng nhất trong phiên bản HTTP/1.1 là nó cho phép các kết nối lâu dài - client và server sẽ trao đổi nhiều thông điệp yêu cầu/trả lời trên cùng một kết nối TCP. Kết nối lâu dài có hai cái lợi. Thứ nhất, nó làm giảm thiểu chi phí cho việc thiết lập/giải phóng nối kết. Thứ hai, do client gửi nhiều thông điệp yêu cầu qua một kết nối TCP, cơ chế điều khiển tắc nghẽn của TCP sẽ hoạt động hiệu quả hơn.

Tuy nhiên, kết nối lâu dài cũng có cái giá phải trả. Vấn đề phát sinh ở chỗ: không ai trong client và server biết được kết nối đó sẽ kéo dài bao lâu. Điều này thực sự gây khó khăn cho phía server bởi vì tại mỗi thời điểm, nó phải đảm bảo duy trì kết nối đến cả ngàn client. Giải pháp cho vấn đề này là: server sẽ mãn kỳ và cắt nối kết nếu nó không

nhận được một yêu cầu cụ thể nào từ phía client trong một khoảng thời gian định trước. Ngoài ra, cả client và server phải theo dõi xem phía bên kia có chủ động cắt nối kết hay không và lấy đó làm cơ sở để tự cắt nối kết của mình. (Nhắc lại rằng, cả hai bên phải cắt nối kết thì nối kết TCP mới thực sự kết thúc).

6.2.4. Bộ lưu trữ đệm

Một trong những lĩnh vực nghiên cứu tích cực nhất hiện nay về Internet là làm sao để trữ tạm các trang Web một cách hiệu quả. Việc trữ tạm mang lại nhiều lợi ích. Từ phía client, việc nạp và hiển thị một trang Web từ bộ đệm gần đây là nhanh hơn rất nhiều so với từ một server nào đó ở nửa vòng trái đất. Đối với server, có thêm một bộ đệm để can thiệp vào và phục vụ giúp yêu cầu của người dùng sẽ giảm bớt tải trên server.

Việc trữ đệm có thể được cài đặt tại nhiều nơi khác nhau. Ví dụ, trình duyệt Web có thể trữ tạm những trang Web mới được nạp về gần đây, để khi người dùng duyệt lại những trang Web đó, trình duyệt sẽ không phải nối kết ra Internet để lấy chúng về mà dùng bản trữ sẵn. Ví dụ khác, một khu vực làm việc (site) có thể để cử một máy làm nhiệm vụ trữ tạm các trang Web, để những người dùng sau có thể sử dụng các bản trữ sẵn của những người dùng trước. Yêu cầu của hệ thống này là mọi người dùng trong site phải biết địa chỉ của máy tính làm nhiệm vụ bộ trữ tạm, và họ chỉ đơn giản là liên hệ với máy tính này để tải các trang Web về theo yêu cầu. Người ta thường gọi máy tính làm nhiệm vụ trữ tạm các trang Web cho một site là *proxy*. Vị trí trữ đệm có thể di chuyển gần hơn đến phần lõi của Internet là các ISP. Trong tình huống này, các site nối kết tới ISP thường không hay biết gì về việc trữ tạm ở đây. Khi các yêu cầu HTTP từ các site được chuyển phát đến router của ISP, router liền kiểm tra xem URL được yêu cầu có giống với các URL được trữ sẵn hay không. Nếu có, router sẽ trả lời ngay. Nếu không, router sẽ chuyển yêu cầu đến server thật sự và cũng không quên lưu vào bộ đệm của mình thông điệp trả lời từ phía server đó. Việc trữ tạm là đơn giản. Tuy nhiên bộ đệm phải đảm bảo những thông tin trữ đệm trong đó không quá cũ. Để làm được việc này, các Web server phải gán “ngày hết hạn” (tức là trường Expires trong header) cho mọi trang Web mà nó phục vụ cho client. Nhân đó, các bộ đệm cũng lưu lại thông tin này. Và từ đó, các bộ đệm sẽ không cần phải kiểm tra tính cập nhật của trang Web đó cho đến khi ngày hết hạn đến. Tại thời điểm một trang Web hết hạn, bộ đệm sẽ dùng lệnh HEAD hoặc lệnh GET có điều kiện (GET với trường If-Modified-Since trong phần header được đặt) để kiểm tra rằng nó có một phiên bản mới nhất của trang Web kia. Tổng quát hơn, cần phải có “các chỉ thị hướng dẫn” cho việc trữ đệm và các chỉ thị này phải được tuân thủ tại mọi bộ đệm. Các chỉ thị sẽ chỉ ra có nên trữ đệm một tài liệu hay không, trữ nó bao lâu, một tài liệu phải tươi như thế nào và vân vân.

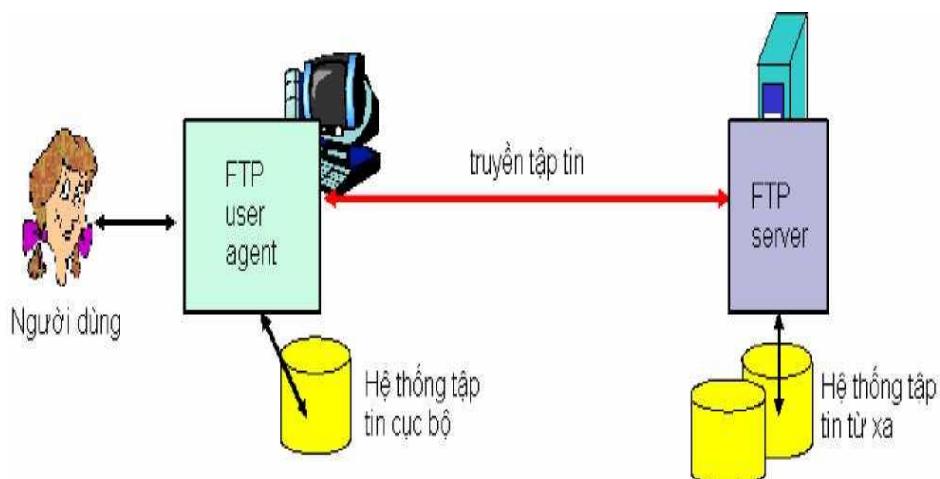
6.3. Giao thức truyền file: FTP

Truyền dữ liệu Đa phương tiện

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

Mục tiêu của dịch vụ FTP là:

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



Hình 6. 2 Truyền dữ liệu

6.3.1. Giao thức FTP

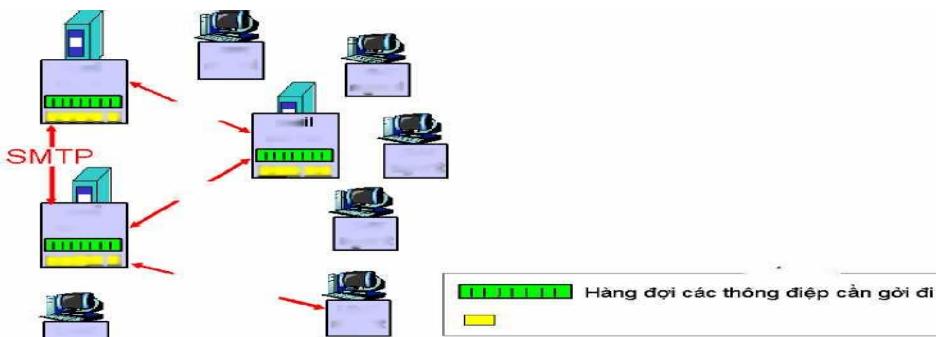
Đầu tiên, user agent thiết lập một kết nối điều khiển trên cổng 21 tới FTP server. Sau khi đã thỏa thuận các tham số truyền nhận, hai bên sẽ thiết lập một kênh dữ liệu chạy trên cổng 20. Dữ liệu của các tập tin được trao đổi qua lại giữa user agent và server sẽ chạy trên kênh dữ liệu này. Kênh dữ liệu là kênh hoạt động theo phuong thức hai chiều và không nhất thiết phải luôn tồn tại.

6.3.2. Các lệnh cơ bản

Sau đây là các lệnh cơ bản mà người dùng có thể sử dụng để thao tác lên hệ thống FTP

Lệnh	Tham số	Ý nghĩa
FTP	host-name	Nối kết đến FTP server có địa chỉ host-name
USER	user-name	Cung cấp tên người dùng cho FTP server để thực

ASCII		Chỉ định kiểu dữ liệu truyền nhận là ký tự
BINARY		Chỉ định kiểu dữ liệu truyền nhận là nhị phân
LS		Xem nội dung thư mục từ xa
CD	remote-dir	Chuyển đến thư mục khác trong hệ thống tập tin từ xa
GET	remote-file local-file	Tải tập tin remote-file trên FTP server về hệ thống
PUT	local-file remote-file	Nạp tập tin cục bộ local-file lên server và đặt tên là
MKDIR	dir-name	Tạo một thư mục có tên dir-name trên hệ thống tập
RMDIR	dir-name	Xóa thư mục có tên dir-name trên hệ thống tập tin từ
QUIT		Đóng kết nối FTP và thoát khỏi chương trình FTP



6.4. Thư điện tử trên Internet

Email là một trong những ứng dụng mạng lâu đời nhất nhưng lại phổ dụng nhất. Thủ nghĩ khi bạn muốn gửi thông điệp đến một người bạn ở đầu kia của thế giới, bạn muốn mang thư chạy bộ qua đó hay chỉ đơn giản lên máy tính gõ ít hàng và nhấn nút Send? Thực ra, những bậc tiền bối của mạng ARPANET đã không tiên đoán được email sẽ là ứng dụng then chốt chạy trên mạng này, mục tiêu chính của họ là thiết kế hệ thống cho phép truy cập tài nguyên từ xa. Hệ thống email ra đời không mấy nổi bật, để bây giờ lại được sử dụng hàng ngày bởi hàng triệu người trên thế giới. Mục tiêu của phần này là chỉ ra những nhân vật hoạt động trong hệ thống email, vai trò của họ, giao thức mà họ sử dụng và khuôn dạng thông điệp mà họ trao đổi với nhau.

Hình 6. 3 Hệ thống Email

6.4.1. Các thành phần của hệ thống email

Một hệ thống email thường có 3 thành phần chính: Bộ phận trợ giúp người dùng (User Agent), Mail Server và các giao thức mà các thành phần này dùng để giao tiếp với nhau.

Người ta phân loại các giao thức như sau:

- Giao thức giữa các mail servers bao gồm:

SMTP (Simple Mail Transfer Protocol): được các server dùng để chuyển thư qua lại với nhau. Ví dụ nôm na, nó giống như cách thức mà các trạm bưu điện dùng để chuyển các thùng thư của khách hàng cho nhau. Thông tin chi tiết về giao thức này được mô tả trong tài liệu RFC 822.

- Giao thức giữa mail server và user agent bao gồm:

POP3 (Post Office Protocol version 3 [RFC 1939]): được user agent sử dụng để lấy thư về từ hộp thư của nó trên server.
o SMTP: được user agent sử dụng để gửi thư ra server.

IMAP: (Internet Mail Access Protocol [RFC 1730]): Có nhiều tính năng vượt trội hơn POP3. Ngoài ra IMAP còn cho phép gửi mail.

6.4.2. Khuôn dạng của một email

RFC 822 định nghĩa một email gồm có hai phần: phần tiêu đề (header) và phần thân (body). Cả hai phần đều được thể hiện dưới dạng ký tự ASCII. Lúc đầu, phần thân được qui định có khuôn dạng văn bản đơn giản. Sau này người ta đề nghị một chuẩn mới gọi là MIME, có thể cho phép phần thân của email chứa bất kỳ loại dữ liệu nào.

Phần tiêu đề bao gồm nhiều dòng thông tin, mỗi dòng kết thúc bằng hai ký tự <CRLF>. Phần tiêu đề được chia khỏi phần thân bởi một hàng rỗng. Mỗi một hàng tiêu đề chứa một cặp “tên” và “giá trị”, cách nhau bởi dấu hai chấm (:). Người dùng có thể rất quen với nhiều hàng tiêu đề vì họ thường phải điền thông tin vào đây. Ví dụ

Tên	Giá trị
<i>Fro</i>	Địa chỉ người gửi
<i>To:</i>	Địa chỉ của người nhận
<i>Sub</i>	Chủ đề thư
<i>Dat</i>	Ngày gửi

RFC 822 được mở rộng năm 1993 (và được cập nhật lại năm 1996) để cho phép email mang được nhiều loại dữ liệu: audio, video, hình ảnh, tài liệu Word, ... MIME (Multipurpose Internet Mail Extensions) về cơ bản có ba phần. Phần đầu tiên là tập các dòng header dùng để bổ túc cho phần header cũ của RFC 822. Theo nhiều cách, những dòng header này mô tả dữ liệu chứa trong phần thân. Cụ thể như sau:

Phần thứ hai là các định nghĩa cho một tập các kiểu nội dung (và kiểu con nếu có). Ví dụ một số kiểu mà MIME định nghĩa:

Kiểu	Ý nghĩa
image/gif	Ảnh dạng gif
image/jpeg	Ảnh dạng jpeg

text/plain	Văn bản đơn giản
text/richtext	Văn bản mở rộng (có đặt font chữ, được định dạng đậm, nghiêng hoặc gạch dưới ...)
application	Dữ liệu trong thư được xuất ra từ một ứng dụng nào đó. Chẳng hạn: application/postscript : tài liệu Postscript (.ps) application/msword :

MIME cũng định nghĩa kiểu multipart để chỉ ra cách mà phần thân của thư mang nhiều loại dữ liệu khác nhau như thế nào. Chỉ có một kiểu con của multipart là mixed với ý nói rằng trong phần thân của thư có nhiều mảnh dữ liệu khác nhau, độc lập với nhau và được sắp xếp theo một trình tự cụ thể. Mỗi mảnh dữ liệu sẽ có phần tiêu đề riêng để mô tả kiểu dữ liệu của mảnh đó.

Tên	Giá trị
MIME-Version:	Phiên bản MIME đang sử dụng
Content-Description:	Mô tả trong thư đang có dữ liệu gì
Content-Type:	Mô tả kiểu dữ liệu đang nằm trong thư
Content-Transfer-Encoding:	Mô tả cách thức mã hóa dữ liệu trong thư

Phần thứ ba mô tả cách thức mã hóa các kiểu dữ liệu nói trên để có thể truyền chúng dưới dạng ASCII. Lý do để mọi bức thư phải chứa các ký tự ASCII là vì để đi được đến đích, bức thư đó có thể phải trung chuyển qua nhiều gateway, mà các gateway này đều coi mọi bức thư dưới dạng ASCII. Nếu trong thư chứa bất kỳ ký tự nào khác ASCII thì thư sẽ bị đứt gãy nội dung. MIME sử dụng phương pháp mã hóa trực tiếp dữ liệu nhị phân thành các ký tự nhị phân, gọi là base64. Ý tưởng của base64 là ánh xạ 3 bytes dữ liệu nhị phân nguyên thủy thành 4 ký tự ASCII. Giải thuật đơn giản như sau: tập hợp 3 bytes dữ liệu nhị phân lại thành 24 bits, sau đó chia 24 bits này thành 4 cụm, một cụm 6 bits. Một cụm 6 bits được ánh xạ vào một trong 64 ký tự ASCII hợp lệ; ví dụ 0 ánh xạ thành A, 1 ánh xạ thành B... Nếu nhìn vào bức thư đã được mã hóa dạng base64, người dùng sẽ thấy chỉ có 52 chữ cái cả hoa lẫn thường, 10 chữ số từ 0 đến 9 và các ký tự đặc biệt + và /. Đối với những người dùng chỉ sử dụng trình đọc thư hỗ trợ duy nhất kiểu ký tự thì việc đọc những bức thư có kiểu base64 sẽ rất là đau khổ. Vì lý do nhân đạo, MIME còn hỗ trợ kiểu mã hóa ký tự thường được gọi là 7-bit. 7-bit sẽ giữ nguyên dạng ký tự mà người ta nhập vào.

Tổng hợp lại, ví dụ một bức thư có 2 loại dữ liệu: văn bản thường, một ảnh JPEG, sẽ có hình.

From: ptphi@cit.ctu.edu.vn To: TH27@cit.ctu.edu.vn Subject:

Picture of students.

MIME-Version: 1.0

Content-Type: multipart/mixed; boundary="—98766789" --98766789

Content-Transfer-Encoding: 7bit Content-Type:

text/plain

Hi,

Please find a picture of you.

--98766789

Content-Transfer-Encoding: base64 Content-Type:

image/jpeg

base64 encoded data

6.4.3. Chuyển thư

Chúng ta sẽ xem xét giao thức SMTP - giao thức được dùng để chuyển thư từ máy này đến máy kia. Để đặt SMTP vào đúng ngữ cảnh, chúng ta nên nhắc lại các nhân vật then chốt trong hệ thống email. Đầu tiên, người dùng tương tác với trình đọc thư (hay còn gọi là user agent) để soạn, lưu, tìm kiếm và đọc thư của họ. Hiện trên thị trường có nhiều phần mềm đọc thư, cũng giống như hiện cũng đang có nhiều loại trình duyệt Web vậy. Thứ hai, có trình xử lý thư (hay còn gọi là mail server) chạy trên một máy nào đó trong mạng nội bộ của người dùng. Có thể xem mail server như một bưu điện: Người dùng trao cho mail server các bức thư mà họ muốn gửi cho người dùng khác, mail server sử dụng giao thức SMTP trên TCP để chuyển bức thư này đến mail server bên đích. Mail server bên đích nhận các thư đến và đặt chúng vào hộp thư của người dùng bên đích. Do SMTP là giao thức mà rất nhiều người có thể tự cài đặt, vì thế sẽ có rất nhiều sản phẩm mail server hiện có trên thị trường. Sản phẩm mail server thường được sử dụng nhất là sendmail, ban đầu được cài đặt trong hệ điều hành Berkeley Unix. Tất nhiên mail server bên máy gửi có thể kết nối SMTP/TCP trực tiếp tới mail server bên máy nhận, nhưng trong thực tế, một bức thư có thể đi ngang qua vài mail gateways trước khi đến đích. Cũng giống như máy đích, mỗi mail gateway cũng chạy một mail server. Không phải ngẫu nhiên mà các nút chuyển thư trung gian được gọi là mail gateway. Công việc của chúng cũng giống như các IP gateway là lưu tạm và chuyển phát tiếp các bức thư của người dùng. Điểm khác nhau duy nhất giữa chúng là, mail gateway trữ tạm các bức thư trong đĩa, trong khi các IP gateway trữ tạm các gói tin IP trong bộ nhớ.

Câu hỏi đặt ra : tại sao lại cần đến các mail gateways? Tại sao không dùng phương pháp nối kết SMTP/TCP trực tiếp từ bên gửi sang bên nhận? Lý do thứ nhất, người gửi không muốn kèm trong thư địa chỉ của máy đích. Ví dụ, riêng việc nhập vào trong thư địa chỉ đích ptphi@Uneti.edu.vn đã mất công rồi, không ai thấy thoải mái khi phải nhập thêm địa chỉ máy đích là machine-of-phi.Uneti.edu.vn. Thứ hai, không chắc lúc bên gửi thiết lập nối kết đến bên nhận, người dùng bên nhận đã bật sẵn máy! Thành thử chỉ cần địa chỉ

thư bên nhận là đủ. Khi bức thư đến được mail gateway của Khoa Công Nghệ Thông Tin - Đại học KTKTCN, nếu người dùng ptphi đang mở máy, mail gateway sẽ chuyển thư cho anh ta ngay, nếu không mail gateway sẽ trữ tạm thư trên đĩa của nó đến khi ptphi bật máy lên và kiểm tra thư..Dù có bao nhiêu mail gateways trung gian trên đường đến đích vẫn không đáng lo lắng, bởi vì mỗi mail gateway trung gian sẽ nỗ lực sử dụng một kết nối SMTP độc lập đến gateway kế tiếp trên đường đi nhằm chuyển thư càng ngày càng đến gần người nhận.

```
S: 220 ctu.edu.vn C: HELO uneti.edu.vn  
S: 250 ctu.edu.vn says hello to cit.ctu.edu.vn C: MAIL FROM:  
<ptphi@uneti.edu.vn>  
S: 250 Sender ok  
C: RCPT TO: <Ihly@yale.edu>  
S: 250 Recipient ok C: DATA  
S: 354 Enter mail, end with "." on a line by itself C: Subject: It's  
Xmas!  
C: So I hope you a merry Xmas and a happy new year! C: .  
S: 250 Message accepted for delivery C: QUIT  
S: 221 Bye-Bye
```

SMTP là một giao thức đơn giản dùng các ký tự ASCII. Sau khi thiết lập kết TCP đến cổng 25 của máy đích (được coi là server), máy nguồn (được coi là client) chờ nhận kết quả trả về từ server. Server khởi đầu cuộc đối thoại bằng cách gửi một dòng văn bản đến client thông báo danh tính của nó và khả năng tiếp nhận thư. Nếu server không có khả năng nhận thư tại thời điểm hiện tại, client sẽ hủy bỏ kết và thử thiết lập lại kết nối sau.

Nếu server sẵn sàng nhận thư, client sẽ thông báo lá thư đó từ đâu đến và ai sẽ là người nhận. Nếu người nhận đó tồn tại, server sẽ thông báo cho client tiếp tục gửi thư. Sau đó client gửi thư và server báo nhận cho thư đó. Sau khi cả hai bên hoàn tất phiên truyền nhận, kết nối sẽ được đóng lại.

Ví dụ một phiên truyền nhận được cho ngay dưới đây. Những dòng bắt đầu bằng C: là của phía client gửi đi; bằng S: là các câu trả lời của server.

LỆNH CỦA CLIENT	
Lệnh	Ý nghĩa
HELO	Câu chào và xưng danh của client
MAIL FROM	Địa chỉ email của người gửi
RCPT TO	Địa chỉ email của người nhận
DATA	Bắt đầu truyền nội dung của thư
QUIT	Hủy nối kết
TRẢ LỜI CỦA SERVER	
Trả lời	Ý nghĩa
250	Yêu cầu hợp lệ
550	Yêu cầu không hợp lệ, không tồn tại hộp thư như client đã chỉ ra.
354	Cho phép bắt đầu nhập thư vào. Kết thúc thư bằng <CRLF>.<CRLF>
221	Server đang đóng kết nối TCP

Vẫn còn nhiều lệnh và mã trả lời chưa được trình bày, xin tham khảo tài liệu RFC 822 để có được đầy đủ thông tin.

6.4.4. Phân phát thư

Khi đứng về góc độ người dùng thư, họ sẽ dùng user agent để gửi và nhận thư cho họ. User agent dùng giao thức SMTP để gửi thư đi, dùng giao thức POP3 hoặc IMAP để nhận thư về.

6.4.4.1. POP3

Một phiên làm việc theo giao thức POP3 bắt đầu tại user agent. User agent khởi động một nối kết TCP đến cổng 110 của mail server. Khi kết nối thực hiện xong, phiên làm việc POP3 sẽ trải qua theo thứ tự ba kỳ:

- ✓ Chứng thực.
- ✓ Giao dịch dữ liệu.
- ✓ Cập nhật.

Kỳ chứng thực buộc người dùng thực hiện thủ tục đăng nhập bằng cách nhập vào hai lệnh sau:

Lệnh	Ý nghĩa
USER < <i>tên người dùng</i> >	Khai báo tên người dùng.
PASS < <i>mật khẩu</i> >	Khai báo mật khẩu.

Báo trả của mail server sẽ là một trong hai câu sau:

Trả lời	Ý nghĩa
+OK < <i>chú thích</i> >	Khai báo của người dùng là đúng.
+ERR < <i>chú thích</i> >	Khai báo của người dùng là sai và lời giải thích.

Các trả lời của server có thể là các số liệu mà client yêu cầu hoặc các thông báo +OK, -ERR như trong phần đăng nhập.

Sau đây là dàn cảnh một phiên làm việc ví dụ giữa người dùng ptphi khi anh ta đăng nhập và làm việc trên hộp thư của mình tại server có địa chỉ mail.uneti.edu.vn.

Trong kỳ giao dịch, người dùng có thể xem danh sách thư chưa nhận về, nhận thư về và xóa thư trong hộp thư của mình khi cần thiết. Các lệnh mà người dùng thường sử dụng để giao dịch với server là:

Lệnh	Ý nghĩa
LIST [<50 <i>thứ tự thư</i> >]	Nếu dùng LIST không tham số, server sẽ trả về toàn bộ danh sách các thư chưa nhận. Nếu có tham số là số thứ tự thư cụ
RETR <50 <i>thứ tự thư</i> >	Tải lá thư có số thứ tự <50 <i>thứ tự thư</i> > về.
DELE <50 <i>thứ tự thư</i> >	Xóa lá thứ số <50 <i>thứ tự thư</i> > khỏi hộp thư.
QUIT	Hoàn tất giai đoạn giao dịch và hủy nối kết TCP

+OK	Hộp thư của ptphi còn hai thư chưa nhận
1 1024	thư thứ nhất có kích thước 1024 bytes, thư
2 2550	thứ hai có kích thước 2550 bytes
RET	ptphi tải thư thứ nhất về
+OK	server gửi thư thứ 1 cho ptphi
DEL	ptphi xóa thư thứ nhất trong hộp thư
+OK	server xoá thư thứ 1 thành công
QUI	ptphi hủy nối kết
+OK Bve-Bve	server hủy nối kết

6.4.4.2 IMAP

Tính năng	POP3	IMAP
Giao thức được định nghĩa ở đâu?	RFC 1939	RFC 2060
Cổng TCP được dùng	110	143
Email được lưu ở đâu	PC của người dùng	Server
Email được đọc ở đâu	Off-line	On-line
Thời gian nối kết	Ít	Nhiều
Sử dụng tài nguyên của server	Tối thiểu	Nhiều hơn
Nhiều hộp thư	Không	Đúng
Ai lưu phòng hờ các hộp thư	Người dùng	ISP
Tốt cho người dùng di động	Không	Có
Kiểm soát của người dùng đối với việc tải thư về	Ít	Tốt
Tải một phần thư	Không	Có
Quota đĩa có là vấn đề không?	Không	Thỉnh thoảng
Dễ cài đặt	Có	Không
Được hỗ trợ rộng rãi	Có	Đang phát triển

Với những người dùng có một tài khoản email trên một ISP và người dùng này thường truy cập email trên một PC thì giao thức POP3 hoạt động tốt. Tuy nhiên, một sự thật trong ngành công nghệ máy tính, khi một thứ gì đó đã hoạt động tốt, người ta lập tức đòi hỏi thêm nhiều tính năng mới (và tự chuốc lấy nhiều phiền nhiễu). Điều đó cũng xảy ra đối với hệ thống email. Ví dụ, người ta chỉ có một tài khoản email, nhưng họ lại muốn ngồi đâu cũng truy cập được nó. POP3 cũng làm được chuyện này bằng cách đơn giản tải hết các email xuống máy PC mà người dùng này đang ngồi làm việc. Và dĩ nhiên là thư từ của người dùng này nằm rải rác khắp nơi.

Sự bất tiện này khơi mào cho sự ra đời của giao thức phân phối thư mới, IMAP (Internet Message Access Protocol), được định nghĩa trong RFC 2060. Không giống như POP2, IMAP coi các thông điệp mặc nhiên nằm trên server vô hạn và trên nhiều hộp thư.

IMAP còn đưa ra cơ chế cho phép đọc các thông điệp hoặc một phần của thông điệp, một tính năng hữu ích khi người dùng kết nối đến server bằng đường truyền tốc độ chậm như điện thoại nhưng lại đọc các email có âm thanh, hình ảnh... Với quan niệm cho rằng người dùng không cần tải thư về lưu trên PC, IMAP cung cấp các cơ chế cho phép tạo, xóa và sửa đổi nhiều hộp thư trên server.

Cung cách làm việc của IMAP cũng giống như POP3, ngoài trừ trong IMAP có rất nhiều lệnh. IMAP server sẽ lắng nghe trên cổng 143. Cũng nên chú ý rằng, không phải mọi ISP đều hỗ trợ cả hai giao thức POP3 và IMAP.

6.5. Dịch vụ phân giải tên miền –DNS

Cho đến bây giờ, chúng ta vẫn dùng địa chỉ để định danh các host. Trong khi rất thuận tiện cho việc xử lý của các router, các địa chỉ số không thân thiện với người dùng lắm. Vì lý do này, các host thường được gán cho một cái tên thân thiện và dịch vụ tên được sử dụng để ánh xạ từ cái tên thân thiện với người dùng này sang địa chỉ số vốn rất thân thiện với các router. Dịch vụ như vậy thường là ứng dụng đầu tiên được cài đặt trong một mạng máy tính do nó cho phép các ứng dụng khác tự do định danh các host bằng tên thay vì bằng địa chỉ. Dịch vụ tên thường được gọi là phần trung gian (middleware) vì nó lấp đầy khoảng cách giữa các ứng dụng khác và lớp mạng phía dưới.

Tên host và địa chỉ host khác nhau ở hai điểm quan trọng. Thứ nhất, tên host thường có độ dài thay đổi và dễ gợi nhớ, vì thế nó giúp người dùng dễ nhớ hơn. Thứ hai, tên thường không chứa thông tin gì để giúp mạng định vị (chuyển các gói tin đến) host. Địa chỉ, ngược lại, lại hàm chứa thông tin vạch đường trong đó.

Trước khi đi vào chi tiết cách thức đặt tên cho các host trong mạng như thế nào, chúng ta đi định nghĩa một số thuật ngữ trước:

Không gian tên (name space) định nghĩa tập các tên có thể có. Một không gian tên có thể là phẳng (flat) - một tên không thể được chia thành các thành phần nhỏ hơn, hoặc phân cấp.

Hệ thống tên duy trì một **tập các ánh xạ** (collection of bindings) từ tên sang giá trị. Giá trị có thể là bất cứ thứ gì chúng ta muốn hệ thống tên trả về khi ta cấp cho nó một tên để ánh xạ; trong nhiều trường hợp giá trị chính là địa chỉ host.

Một **cơ chế phân giải** (resolution mechanism) là một thủ tục mà khi được gọi với tham số là một tên, sẽ trả về một giá trị tương ứng.

Một **server tên** (name server) là một kết quả cài đặt cụ thể của một cơ chế phân giải luôn sẵn dùng trên mạng và có thể được truy vấn bằng cách gởi đến nó một thông điệp.

Mạng Internet đã có sẵn một hệ thống đặt tên được phát triển tốt, gọi là **hệ thống tên miền** (domain name system - DNS). Vì thế chúng ta sẽ dùng DNS làm cơ sở để thảo luận về vấn đề đặt tên cho các host.

Khi người dùng đưa một tên host đến một ứng dụng (có thể tên host đó là một phần của một tên hỗn hợp như địa chỉ email chẳng hạn), ứng dụng này sẽ liên hệ với hệ thống tên để dịch tên host sang địa chỉ host. Sau đó ứng dụng liền tạo một nối kết đến host đó thông qua giao thức TCP chẳng hạn. Hiện trạng được mô tả trong hình dưới đây.

6.5.1. Miền phân cấp

DNS cài đặt không gian tên phân cấp dùng cho các đối tượng trên Internet. Các tên DNS được xử lý từ phải sang trái, sử dụng các dấu chấm (.) làm ký tự ngăn cách. (Mặc dù các tên DNS được xử lý từ phải qua trái, người dùng thường đọc chúng từ trái sang phải). Ví dụ tên miền của một host là **mail.Uneti.edu.vn**. Chú ý rằng các tên miền được sử dụng để đặt tên các đối tượng trên Internet, không phải chỉ được dùng để đặt tên máy. Ta có thể mường tượng cấu trúc phân cấp của DNS

Có thể thấy rằng, cây phân cấp không quá rộng ở mức đầu tiên. Mỗi quốc gia có một tên miền, ngoài ra còn có 6 miền lớn khác gồm: edu, com, gov, mil, org và net. Sáu miền lớn này nằm ở Mỹ. Những tên miền không chỉ ra tên nước một cách tường minh thì mặc nhiên là nằm ở Mỹ.

6.5.2. Các server phục vụ tên

Một cấu trúc tên miền phân cấp hoàn chỉnh chỉ tồn tại trong ý niệm. Vậy thì trong thực tế cấu trúc phân cấp này được cài đặt như thế nào? Bước đầu tiên là chia cấu trúc này thành các cây con gọi là các **vùng** (zone).

Mỗi một vùng có thể được xem là đơn vị quản lý một bộ phận của toàn hệ thống phân cấp. Ví dụ, vùng cao nhất của hệ thống phân cấp được quản lý bởi NIC (Network Information Center), vùng cao nhất được quản lý bởi Trường Đại Học Uneti.

Một vùng luôn có mối liên hệ đến các đơn vị cài đặt cơ bản trong DNS - các server tên. Thông tin chứa trong một vùng được thiết lập tại hai hoặc nhiều server tên. Mỗi server tên có thể truy xuất được qua mạng Internet. Client gửi yêu cầu đến server tên, server tên sẽ trả lời cho yêu cầu đó. Câu trả lời đôi khi chứa thông tin cuối cùng mà client cần, đôi khi lại chứa chỉ điểm đến một server tên khác mà client nên gửi câu hỏi đến đó. Vì thế, theo cách nhìn thiêng về cài đặt, người ta có thể nghĩ về DNS được cài đặt bằng cấu trúc phân cấp các server tên hơn là bằng cấu trúc phân cấp các miền.

Để ý rằng mỗi vùng được cài đặt trong hai hoặc nhiều server tên với lý do dự phòng; nghĩa là nếu một server bị chết sẽ còn các server khác thay thế. Mặt khác, một server tên cũng có thể được dùng để cài đặt nhiều hơn một vùng.

Mỗi server tên quản lý thông tin về một vùng dưới dạng một tập các mẫu tin tài nguyên (resource record). Mỗi mẫu tin tài nguyên là một ánh xạ từ tên sang giá trị (name to value binding), cụ thể hơn là một mẫu tin gồm 5 trường:

(Tên, Giá trị, Kiểu, Lớp, TTL) Các trường Tên và Giá trị là những gì chúng ta muốn có, ngoài ra trường Kiểu chỉ ra cách thức mà Giá trị được thông dịch. Chẳng hạn,

trường Kiểu = A chỉ ra rằng Giá trị là một địa chỉ IP. Vì thế các mẫu tin kiểu A sẽ cài đặt kiểu ánh xạ từ tên miền sang địa chỉ IP. Ví dụ như mẫu tin: (ns.uneti.edu.vn, 203.162.41.166, A, IN) chỉ ra rằng địa chỉ IP của host có tên ns.ctu.edu.vn là 203.162.41.166.

Ngoài ra còn có những kiểu khác:

- NS: Trường Giá trị chỉ ra tên miền của máy tính đang chạy dịch vụ tên, và dịch vụ đó có khả năng thông dịch các tên trong một miền cụ thể.

Ví dụ mẫu tin: (ctu.edu.vn, ns.uneti.edu.vn, NS, IN) chỉ ra rằng server tên của miền ctu.edu.vn có tên là ns.uneti.edu.vn.

- CNAME: Trường Giá trị chỉ ra một cái tên giả của một host nào đó. Kiểu này được dùng để đặt thêm bí danh cho các host trong miền.
- MX: Trường Giá trị chỉ ra tên miền của host đang chạy chương trình mail server mà server đó có khả năng tiếp nhận những thông điệp thuộc một miền cụ thể.

Ví dụ mẫu tin (uneti.edu.vn, mail.uneti.edu.vn, MX, IN) chỉ ra rằng host có tên mail.uneti.edu.vn là mail server của miền uneti.edu.vn.

Trường Lớp được sử dụng nhằm cho phép thêm vào những thực thể mạng không do NIC quản lý. Ngày nay, lớp được sử dụng rộng rãi nhất là loại được Internet sử dụng; nó được ký hiệu là IN. Cuối cùng trường TTL chỉ ra mẫu tin tài nguyên này sẽ hợp lệ trong bao lâu. Trường này được sử dụng bởi những server đang trữ tạm các mẫu tin của server khác; khi trường TTL hết hạn, các mẫu tin chứa trường TTL hết hạn đó sẽ bị các server xóa khỏi cache của mình.

Để hiểu rõ hơn cách thức các mẫu tin tài nguyên được thể hiện trong cấu trúc phân cấp, hãy xem ví dụ được vẽ trong hình. Để đơn giản hóa vấn đề, chúng ta bỏ qua trường TTL và cung cấp thông tin tương ứng cho một server tên làm nhiệm vụ quản lý cho một vùng.

Đầu tiên, server tên gốc (root name server) sẽ chứa một mẫu tin NS cho mỗi server cấp hai. Nó cũng chứa một mẫu tin A để thông dịch từ một tên server cấp hai sang địa chỉ IP của nó. Khi được ghép với nhau, hai mẫu tin này cài đặt một cách hiệu quả một con trỏ từ server gốc đến mỗi server cấp hai của nó.

(edu.vn, dns1.vnnic.net.vn, NS, IN); thông tin về miền con edu.vn lưu ở máy dns1.vnnic.net.vn

(dns1.vnnic.net.vn, 203.162.57.105, A, IN); máy dns1.vnnic.net.vn có địa chỉ 203.162.57.105 (cisco.com, ns1.cisco.com, NS, IN)

Ké tiếp, miền edu.vn có một server tên hiện hữu tại máy dns1.vnnic.net.vn và server này lại chứa các mẫu tin sau:

(uneti.edu.vn, ns.uneti.edu.vn, NS, IN)

(it.uneti.edu.vn, ns.it.uneti.edu.vn, NS, IN)
(ns.it.uneti.edu.vn, 203.162.36.144, A, IN)
(uneti.edu.vn, mail.uneti.edu.vn, MX, IN)
(mail.uneti.edu.vn, 203.162.139.21, A, IN)
www.uneti.edu.vn, mail.uneti.edu.vn, CNAME, IN)

(ns.uneti.edu.vn, 203.162.41.166, A, IN)

Cuối cùng server ns.uneti.edu.vn lại chứa thông tin về các máy tính của trường Đại Học Uneti cũng như các miền con của Trường Đại Học Uneti. Chú ý rằng trên lý thuyết các mẫu tin có thể được dùng để định nghĩa bất kỳ kiểu đối tượng nào, DNS lại thường được sử dụng để định danh các host và site. DNS không được dùng để định danh cá nhân con người hoặc các đối tượng khác như tập tin hay thư mục, việc định danh này được thực hiện trong các hệ thống phục vụ tên khác. Ví dụ X.500 là hệ thống định danh của ISO được dùng để định danh con người bằng cách cung cấp thông tin về tên, chức vụ, số điện thoại, địa chỉ, và vân vân. X.500 đã chứng tỏ là quá phức tạp nên không được hỗ trợ bởi các search engine nổi tiếng hiện nay. Tuy nhiên nó lại là nguồn gốc phát sinh ra chuẩn LDAP (Lightweight Directory Access Protocol). LDAP vốn là thành phần con của X.500 được thiết kế để làm phần front-end cho X.500. Ngày nay LDAP đang trở nên phổ biến nhất là ở cấp độ công ty, tổ chức lớn, đóng vai trò là hệ thống học và quản lý thông tin về người dùng của nó.

6.5.3. Phương pháp phân tích tên

Với một hệ thống phân cấp các server tên đã trình bày, bây giờ chúng ta đi tìm hiểu cách thức một khách hàng giao tiếp với các server này để phân tích cho được một tên miền thành địa chỉ. Giả sử một khách hàng muốn phân tích tên miền www.uneti.edu.vn, đầu tiên khách hàng này sẽ gửi yêu cầu chứa tên này đến server tên gốc. Server gốc không thể so khớp tên theo yêu cầu với các tên mà nó chứa, liền trả lời cho khách hàng một mẫu tin kiểu NS chứa edu.vn. Server gốc cũng trả về tất cả các mẫu tin có liên quan đến mẫu tin NS vừa nói, trong đó có mẫu tin kiểu A chứa địa chỉ của dns1.vnnic.vnn.vn. Khách hàng chưa có thông tin cuối cùng mà nó muốn, tiếp tục gửi yêu cầu đến server tên tại địa chỉ 203.162.57.105. Server tên thứ hai này lại không thể so khớp tên theo yêu cầu với các tên mà nó chứa, tiếp tục trả lời cho khách hàng một mẫu tin loại NS chứa tên ctu.edu.vn cùng với mẫu tin kiểu A tương ứng với tên server là

ns.uneti.edu.vn. Khách hàng lại tiếp tục gửi yêu cầu đến server tên tại địa chỉ 203.162.41.166 và lần này nhận được câu trả lời cuối cùng có kiểu A cho tên www.uneti.edu.vn.

Ví dụ trên chắc chắn sẽ để lại nhiều câu hỏi về quá trình phân giải tên. Câu hỏi thường được đặt ra là: Lúc khởi đầu, làm sao khách hàng có thể định vị được server gốc? Đây là bài toán cơ bản đặt ra cho mọi hệ thống phục vụ tên và câu trả lời là: hệ thống phải tự thân vận động để có được thông tin về các server gốc! Trong tình huống của hệ thống DNS, ánh xạ từ tên sang địa chỉ của một hay nhiều server gốc được phổ biến cho mọi người, nghĩa là ánh xạ đó được loan báo thông qua các phương tiện truyền thông khác nằm ngoài hệ thống tên.

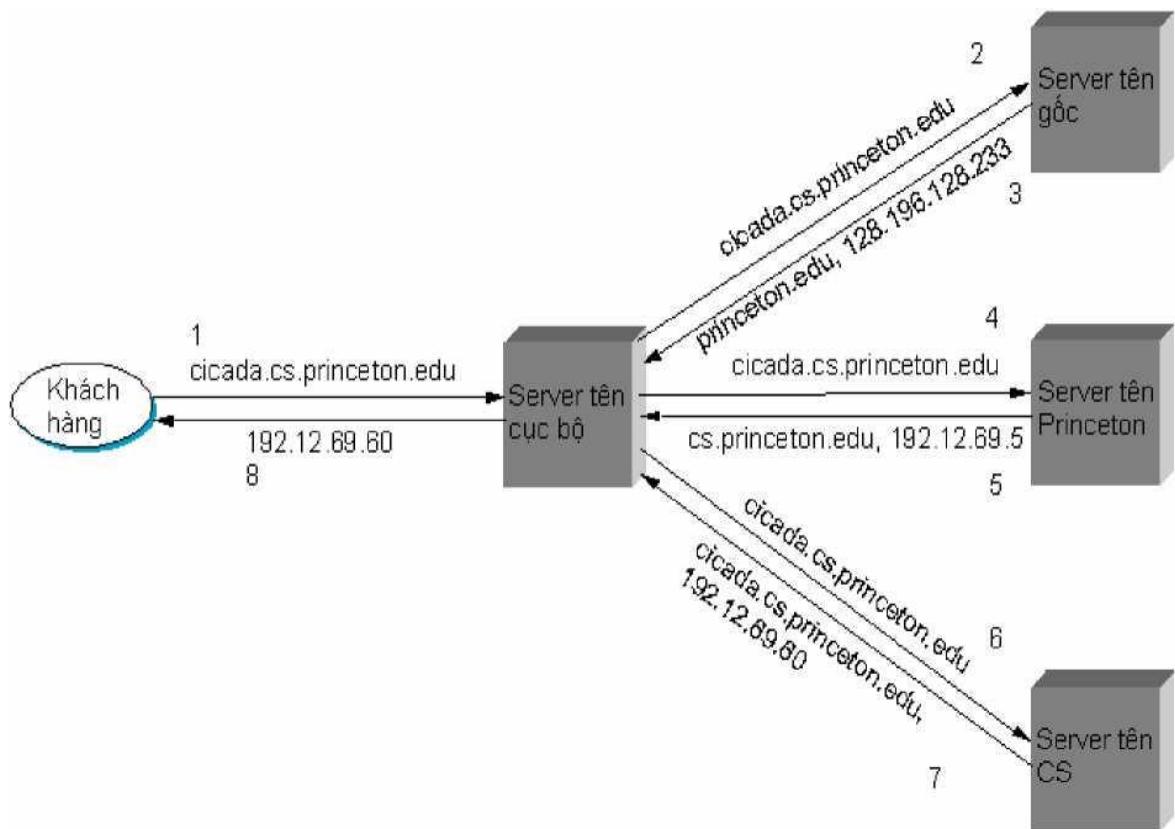
Tuy nhiên, trong thực tế không phải tất cả khách hàng đều biết về các server gốc. Thay vào đó, chương trình khách hàng chạy trên mỗi host trong Internet được khởi động với các địa chỉ lấy từ server tên cục bộ. Ví dụ, tất cả các host trong Khoa Công Nghệ Thông Tin của Trường Đại Học Uneti đều biết server tên nội bộ đang chạy trên máy ns.Uneti.edu.vn. Đến lượt server tên cục bộ này lại chứa các mẩu tin tài nguyên cho một hoặc nhiều server gốc của nó, ví dụ:

(. , a.root-servers.net, NS, IN)

(a.root-server.net, 198.41.0.4, A, IN)

Trong ví dụ trên, server tên cục bộ có thông tin về một server tên gốc của nó (chú ý miền gốc được ký hiệu bằng dấu chấm) là a.root-servers.net, địa chỉ IP tương ứng của server gốc này là 198.41.0.4.

Từ đó, việc phân giải một tên miền bắt đầu từ câu truy vấn của khách hàng đến server cục bộ. Nếu server cục bộ không có sẵn câu trả lời, nó sẽ gửi câu hỏi đến server từ xa dùm cho khách hàng. Chuỗi hành động trên có thể được mô tả trong hình H7.5



Hình 6.4 Quá trình phân giải tên trong thực tế, các số 1 đến 8 chỉ ra trình tự thực hiện

6.6. Ứng dụng mạng ngang hàng

Mạng ngang hàng ([tiếng Anh](#): peer-to-peer network), còn gọi là mạng ngang hàng, là một [mạng máy tính](#) trong đó hoạt động của mạng chủ yếu dựa vào khả năng tính toán và [băng thông](#) của các máy tham gia chứ không tập trung vào một số nhỏ các [máy chủ trung tâm](#) như các mạng thông thường. Mạng ngang hàng thường được sử dụng để kết nối các máy thông qua một lượng kết nối dạng [ad hoc](#). Mạng ngang hàng có nhiều ứng dụng. Ứng dụng thường xuyên gấp nhất là chia sẻ tệp tin, tất cả các dạng như âm thanh, hình ảnh, dữ liệu,... hoặc để truyền dữ liệu thời gian thực như điện thoại [VoIP](#).

Một mạng ngang hàng đúng nghĩa không có khái niệm [máy chủ](#) và [máy khách](#), nói cách khác, tất cả các máy tham gia đều bình đẳng và được gọi là peer, là một nút mạng đóng vai trò đồng thời là máy khách và máy chủ đối với các máy khác trong mạng.

Phân loại mạng ngang hàng

Ta có thể phân loại các mạng ngang hàng hiện nay theo tiêu chí về mức độ tập trung của chúng như sau:

Mạng ngang hàng thuần túy:

- Các máy trạm có vai trò vừa là máy chủ vừa là máy khách
- Không có máy chủ trung tâm quản lý mạng

- Không có máy định tuyến (bộ định tuyến) trung tâm, các máy trạm có khả năng tự định tuyến

Mạng ngang hàng lai:

- Có một máy chủ trung tâm dùng để lưu trữ thông tin của các máy trạm và trả lời các truy vấn thông tin này.
- Các máy trạm có vai trò lưu trữ thông tin, tài nguyên được chia sẻ, cung cấp các thông tin về chia sẻ tài nguyên của nó cho máy chủ.
- Sử dụng các trạm định tuyến để xác định địa chỉ IP của các máy trạm.

Ưu điểm mạng ngang hàng:

Một mục đích quan trọng của mạng ngang hàng là trong mạng tất cả các máy tham gia đều đóng góp tài nguyên, bao gồm băng thông, lưu trữ, và khả năng tính toán. Do đó khi càng có nhiều máy tham gia mạng thì khả năng tổng thể của hệ thống mạng càng lớn. Ngược lại, trong cấu trúc máy chủ-máy khách, nếu số lượng máy chủ là cố định, thì khi số lượng máy khách tăng lên khả năng chuyển dữ liệu cho mỗi máy khách sẽ giảm xuống.

Tính chất phân tán của mạng ngang hàng cũng giúp cho mạng hoạt động tốt khi một số máy gặp sự cố. Đối với cấu trúc tập trung, chỉ cần máy chủ gặp sự cố thì cả hệ thống sẽ ngưng trệ.

Mạng ngang hàng có cấu trúc và không cấu trúc:

Mạng phủ đồng đẳng bao gồm tất cả các nút mạng đại diện cho các máy tham gia và các liên kết giữa các nút mạng này. Một liên kết tồn tại giữa hai nút mạng khi một nút mạng biết vị trí của nút mạng kia. Dựa vào cấu trúc liên kết giữa các nút mạng trong mạng phủ ta có thể phân loại mạng ngang hàng thành hai loại: có cấu trúc hay không cấu trúc.

Một mạng ngang hàng không cấu trúc khi các liên kết giữa các nút mạng trong mạng phủ được thiết lập ngẫu nhiên (tức là không theo quy luật nào). Những mạng như thế này dễ dàng được xây dựng vì một máy mới khi muốn tham gia mạng có thể lấy các liên kết có sẵn của một máy khác đang ở trong mạng và sau đó dần dần tự bản thân nó sẽ thêm vào các liên kết mới của riêng mình. Khi một máy muốn tìm một dữ liệu trong mạng ngang hàng không cấu trúc, yêu cầu tìm kiếm sẽ được truyền trên cả mạng để tìm ra càng nhiều máy chia sẻ càng tốt. Hệ thống này thể hiện rõ nhược điểm: không có gì đảm bảo tìm kiếm sẽ thành công. Đối với tìm kiếm các dữ liệu phổ biến được chia sẻ trên nhiều máy, tỉ lệ thành công là khá cao, ngược lại, nếu dữ liệu chỉ được chia sẻ trên một vài máy thì xác suất tìm thấy là khá nhỏ. Tính chất này là hiển nhiên vì trong mạng ngang hàng không cấu trúc, không có bất kỳ mối tương quan nào giữa một máy và dữ liệu nó quản lý trong mạng, do đó yêu cầu tìm kiếm được chuyển một cách ngẫu nhiên đến một

số máy trong mạng. Số lượng máy trong mạng càng lớn thì khả năng tìm thấy thông tin càng nhỏ.

Một nhược điểm khác của hệ thống này là do không có định hướng, một yêu cầu tìm kiếm thường được chuyển cho một số lượng lớn máy trong mạng làm tiêu tốn một lượng lớn băng thông của mạng, dẫn đến hiệu quả tìm kiếm chung của mạng thấp.

Mạng ngang hàng có cấu trúc khắc phục nhược điểm của mạng không cấu trúc bằng cách sử dụng hệ thống [DHT](#) (Bảng Băm Phân Tán, tiếng Anh: Distributed Hash Table). Hệ thống này định nghĩa liên kết giữa các nút mạng trong mạng phủ theo một thuật toán cụ thể, đồng thời xác định chặt chẽ mỗi nút mạng sẽ chịu trách nhiệm đối với một phần dữ liệu chia sẻ trong mạng. Với cấu trúc này, khi một máy cần tìm một dữ liệu, nó chỉ cần áp dụng một giao thức chung để xác định nút mạng nào chịu trách nhiệm cho dữ liệu đó và sau đó liên lạc trực tiếp đến nút mạng đó để lấy kết quả.

6.7 Tổng kết và bài tập ứng dụng

6.7.1 Wireshark Lab : DNS

- Chạy nslookup để lấy địa chỉ IP của web server Asia

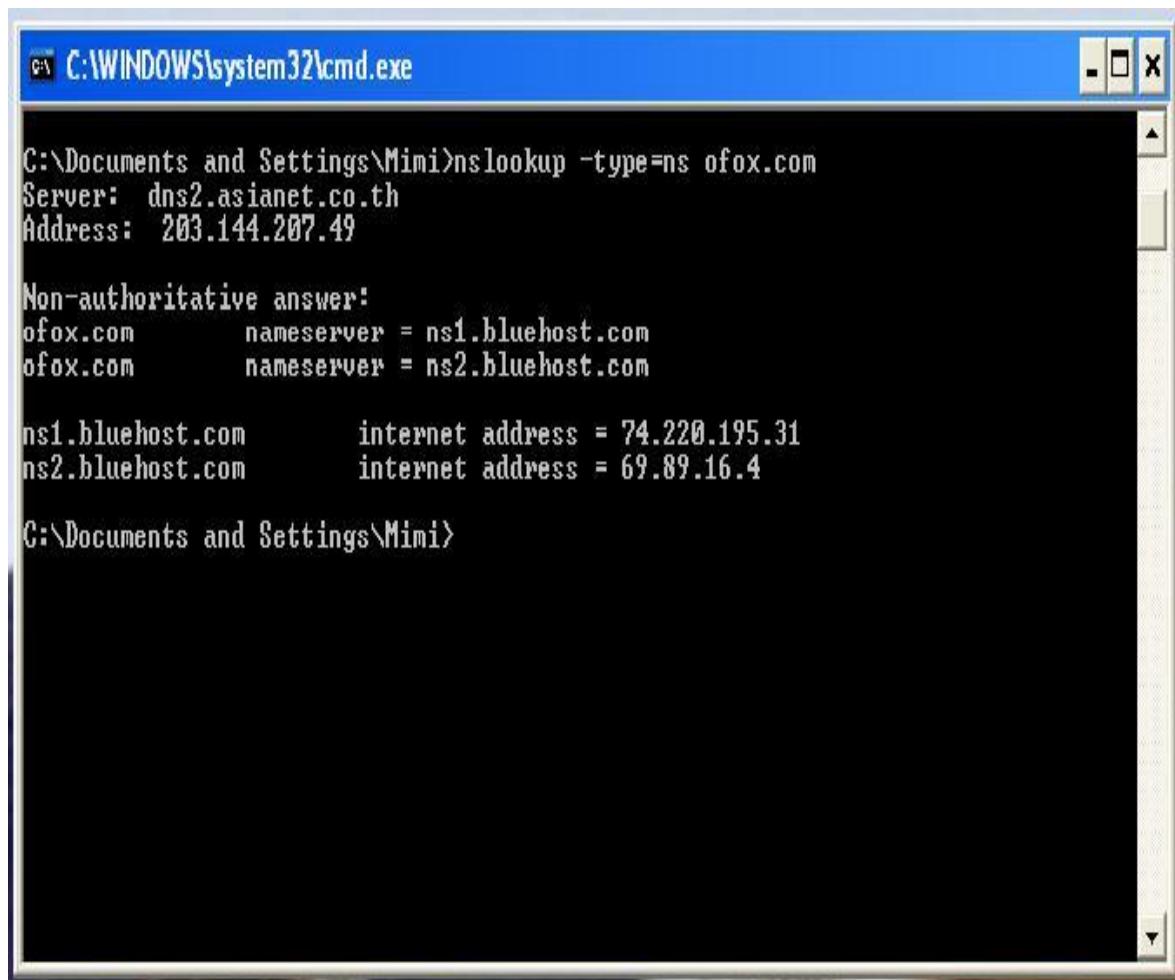
```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Mimi>nslookup www.kmitl.ac.th
Server: dns2.asianet.co.th
Address: 203.144.207.49

Non-authoritative answer:
Name: Chaokhun.cs.kmitl.ac.th
Address: 161.246.34.11
Aliases: www.kmitl.ac.th

C:\Documents and Settings\Mimi>_
```

- Chạy nslookup để xác định DNS server chủ của một trường đại học ở Châu Âu nào đó



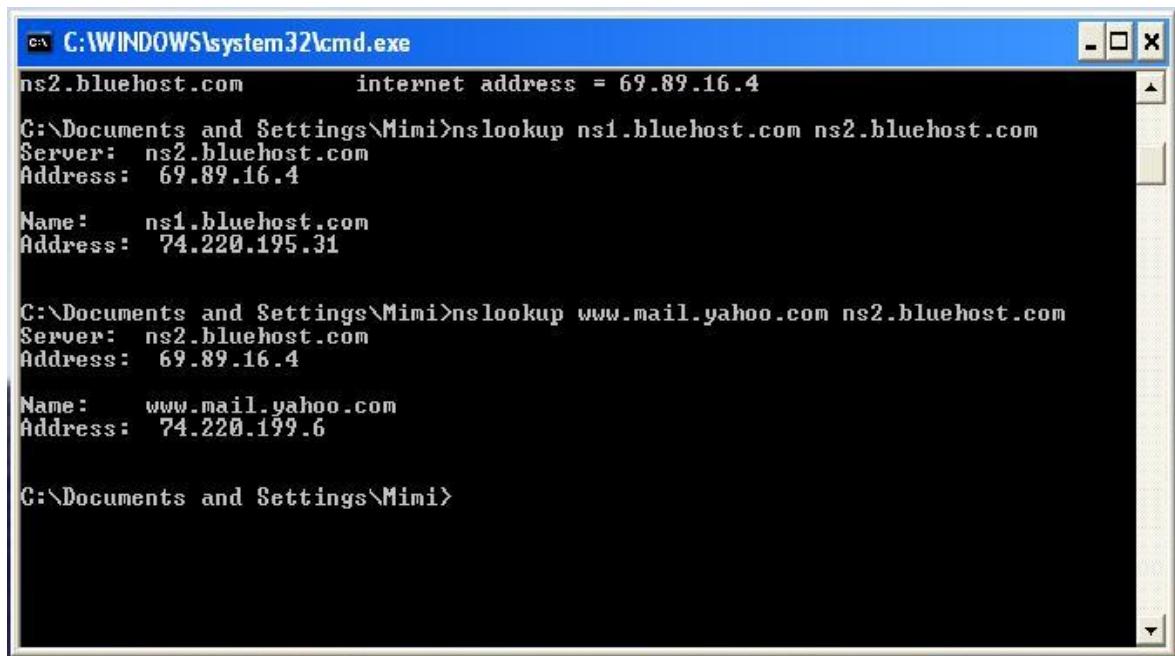
```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Mimi>nslookup -type=ns ofox.com
Server: dns2.asianet.co.th
Address: 203.144.207.49

Non-authoritative answer:
ofox.com      nameserver = ns1.bluehost.com
ofox.com      nameserver = ns2.bluehost.com

ns1.bluehost.com    internet address = 74.220.195.31
ns2.bluehost.com    internet address = 69.89.16.4

C:\Documents and Settings\Mimi>
```

3. Chạy nslookup như một trong các DNS server trong Question 2 là truy vấn đến mail server của yahoo mail



```
C:\WINDOWS\system32\cmd.exe
ns2.bluehost.com      internet address = 69.89.16.4
C:\Documents and Settings\Mimi>nslookup ns1.bluehost.com ns2.bluehost.com
Server: ns2.bluehost.com
Address: 69.89.16.4

Name: ns1.bluehost.com
Address: 74.220.195.31

C:\Documents and Settings\Mimi>nslookup www.mail.yahoo.com ns2.bluehost.com
Server: ns2.bluehost.com
Address: 69.89.16.4

Name: www.mail.yahoo.com
Address: 74.220.199.6

C:\Documents and Settings\Mimi>
```

4. Xác định thông điệp truy vấn DNS và đáp trả DNS. Chúng được gửi qua giao thức UDP hay TCP?

Giao thức: UDP

DNS query	DNS respond
<ul style="list-style-type: none">❑ queries<ul style="list-style-type: none">❑ www.ietf.org: type A, class IN<ul style="list-style-type: none">Name: www.ietf.orgType: A (Host address)Class: IN (0x0001)❑ Answers<ul style="list-style-type: none">❑ www.ietf.org: type A, class IN, addr 64.170.98.32<ul style="list-style-type: none">Name: www.ietf.orgType: A (Host address)Class: IN (0x0001)Time to live: 10 minutes, 36 secondsData length: 4Addr: 64.170.98.32	<ul style="list-style-type: none">Questions: 1Answer RRs: 0Authority RRs: 0Additional RRs: 0❑ Queries<ul style="list-style-type: none">❑ www.ietf.org: type A, class IN<ul style="list-style-type: none">Name: www.ietf.orgType: A (Host address)Class: IN (0x0001)

5. Cổng đích của thông điệp truy vấn DNS là bao nhiêu? Cổng nguồn là bao nhiêu?

Cổng nguồn : 192.168.1.108

Cổng đích : 8.8.8.8

6. Thông điệp truy vấn DNS gửi với địa chỉ IP là gì? Dùng *ipconfig* để xác định địa chỉ IP cho DNS server của bạn. 2 địa chỉ IP này có giống nhau không?

192.168.1.108

2 địa chỉ IP này giống nhau

7. Xét thông điệp truy vấn DNS. Truy vấn DNS này thuộc loại gì? Nó có chứa “answers” nào không?

type:A

không chứa answers nào

8. Xét thông điệp đáp trả. Có bao nhiêu loại “answers”? giải thích cụ thể từng loại?

Có 1 Answer

❑ Answers

❑ www.ietf.org: type A, class IN, addr 64.170.98.32

Name: www.ietf.org

Type: A (Host address)

Class: IN (0x0001)

Time to live: 10 minutes, 36 seconds

Data length: 4

Addr: 64.170.98.32

9. Xem xét gói TCP SYN gửi từ host của bạn. Có phải địa chỉ IP đích của gói SYN phù hợp với bất cứ địa chỉ IP được cung cấp trong thông điệp đáp trả DNS?

IP SYN: 64.170.98.32

IP của DNS respond:192.168.1.1

10. Trang web này bao gồm cả ảnh. Trước khi lấy về một ảnh thì host của bạn sẽ phát ra một truy vấn DNS mới chăng?

Không

11. Cổng đích của thông điệp truy vấn DNS là gì? Cổng nguồn của DNS respond là gì?
Dst port: 53(domain)

12. Thông điệp truy vấn DNS gửi bằng địa chỉ IP? Nó có phải là địa chỉ IP của DNS server cục bộ mặc định không?

IP của DNS query: 192.168.1.36

Yes!

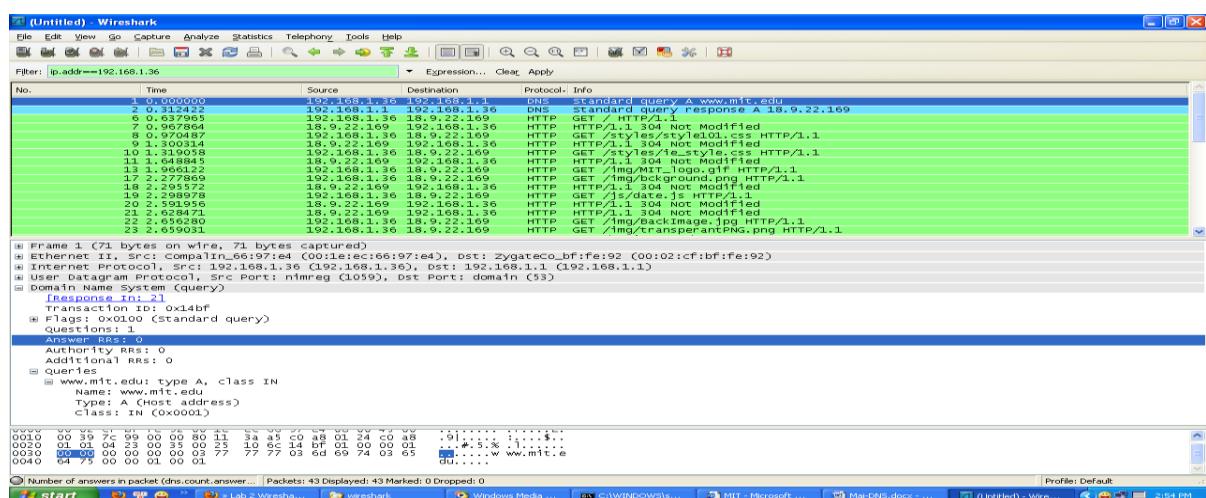
13. Xét thông điệp truy vấn DNS. Nó thuộc loại nào? Có chứa bất kỳ “answers” nào không?
type:A
không chứa answers nào

14. Xét thông điệp hồi đáp DNS. Thông điệp DNS này thuộc loại gì? Nó có chứa bất kỳ một “answer” nào không?

Type: A(host address)

```
questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
Answers
www.mit.edu: type A, class IN, addr 18.9.22.169
    Name: www.mit.edu
    Type: A (Host address)
    Class: IN (0x0001)
    Time to live: 1 minute
    Data length: 4
    Addr: 18.9.22.169
```

15. Đưa ra kết quả



16. Thông điệp truy vấn DNS gửi bằng địa chỉ IP nào? Nó có phải là địa chỉ IP của DNS server cục bộ mặc định không?

IP DNS query: 192.168.1.36

Yes

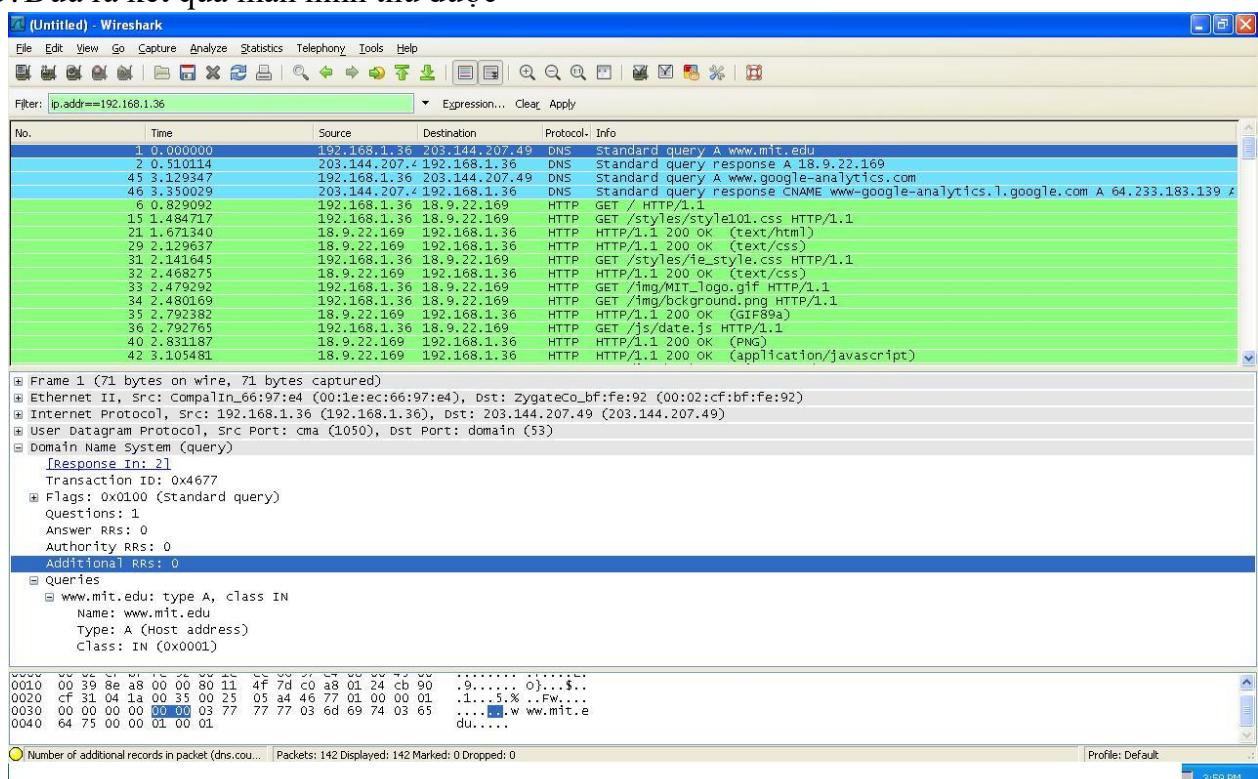
17. Xét thông điệp truy vấn DNS. Nó thuộc loại nào? Có chứa bất kỳ “answers” nào không?

```
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.mit.edu: type A, class IN
Name: www.mit.edu
Type: A (Host address)
Class: IN (0x0001)
```

18. Xét thông điệp hồi đáp. Tên server của MIT trả lời hồi đáp là gì? Thông điệp hồi đáp cũng chứa địa chỉ IP của server đó đúng ko?

```
Questions: 1
Answer RRs: 1
Authority RRs: 3
Additional RRs: 0
Queries
Answers
Authoritative nameservers
mit.edu: type NS, class IN, ns BITSY.mit.edu
mit.edu: type NS, class IN, ns W2ONS.mit.edu
mit.edu: type NS, class IN, ns STRAWB.mit.edu
```

19. Đưa ra kết quả màn hình thu được



20. Thông điệp truy vấn DNS gửi đi bằng địa chỉ IP nào? Nó có phải là địa chỉ IP của DNS server cục bộ mặc định không? Nếu không thì địa chỉ IP đó là gì?

IP của DNS query: 192.168.1.36

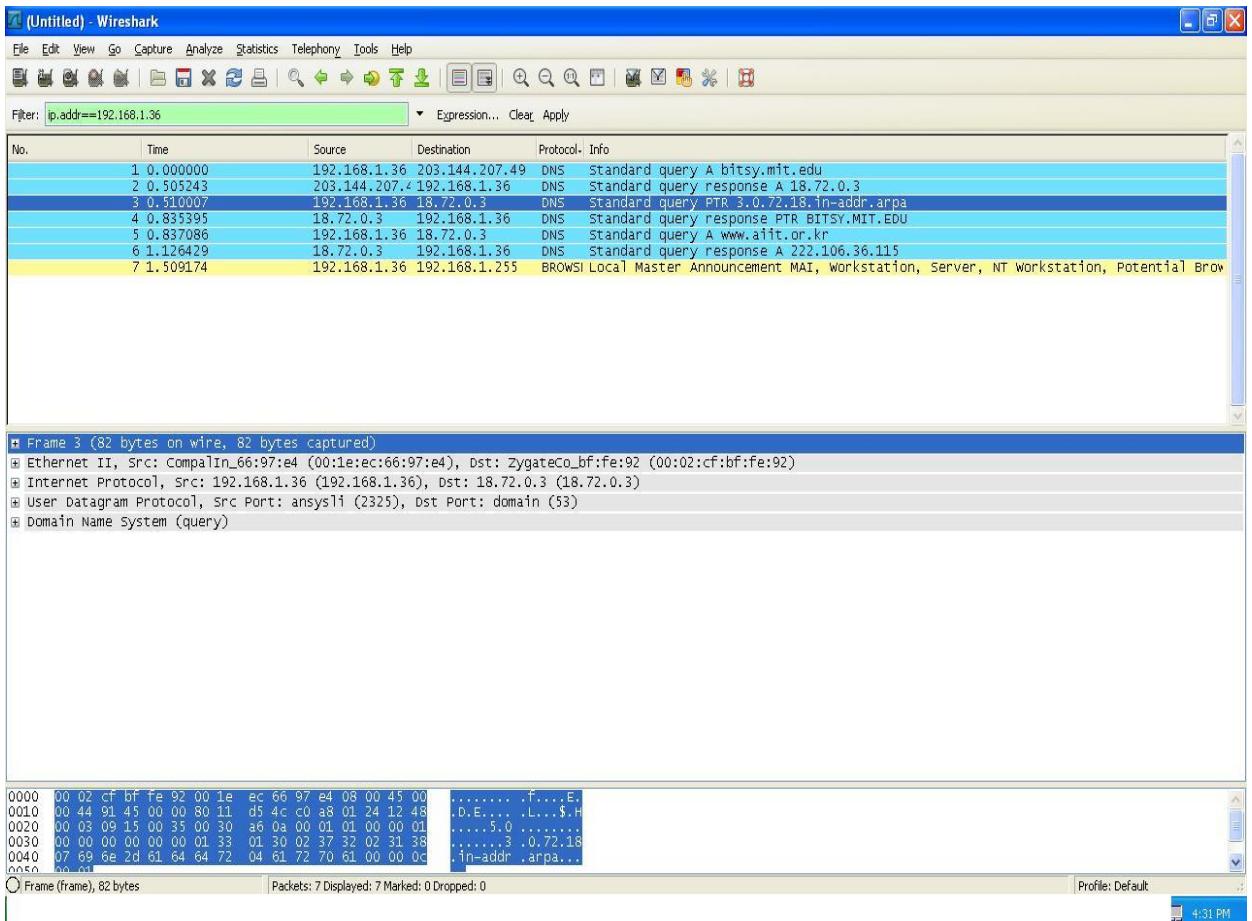
Yes

21. Xét thông điệp truy vấn DNS. Nó thuộc loại nào? Có chứa bất kỳ “answers” nào không?

```
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
  bitsy.mit.edu: type A, class IN
    Name: bitsy.mit.edu
    Type: A (Host address)
    Class: IN (0x0001)
```

22. Xét thông điệp đáp trả. Có bao nhiêu loại “answers”? giải thích cụ thể từng loại:

```
Questions: 1
Answer RRs: 1
Authority RRs: 3
Additional RRs: 3
Queries
  3.0.72.18.in-addr.arpa: type PTR, class IN
    Name: 3.0.72.18.in-addr.arpa
    Type: PTR (Domain name pointer)
    Class: IN (0x0001)
Answers
  3.0.72.18.in-addr.arpa: type PTR, class IN, BITSY/MIT.EDU
Authoritative nameservers
  18.in-addr.arpa: type NS, class IN, ns W20NS/MIT.EDU
  18.in-addr.arpa: type NS, class IN, ns BITSY/MIT.EDU
  18.in-addr.arpa: type NS, class IN, ns STRAWB/MIT.EDU
Additional records
  W20NS/MIT.EDU: type A, class IN, addr 18.70.0.160
  BITSY/MIT.EDU: type A, class IN, addr 18.72.0.3
  STRAWB/MIT.EDU: type A, class IN, addr 18.71.0.151
```



23. Đưa ra kết quả màn hình thu được

6.7.2 Wireshark Lab : HTTP

- Trình duyệt của bạn chạy HTTP phiên bản 1.0 hay 1.1? Phiên bản của HTTP được server chạy?

Trả lời:

Cả trình duyệt và server đều chạy phiên bản HTTP 1.1

```

HTTP/1.1 200 OK
Date: Tue, 23 Sep 2003 05:29:50 GMT
Server: Apache/2.0.40 (Red Hat Linux)
Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 12345
Connection: close
Vary: Accept-Encoding
Keep-Alive: timeout=10, max=100
X-Powered-By: PHP/4.3.10-1

```

- Ngôn ngữ mà trình duyệt web của bạn chỉ ra nó có thể chấp nhận server

Trả lời:

Ngôn ngữ trình duyệt chấp nhận là tiếng anh.

```
☒ Hypertext Transfer Protocol
☒ GET /ethereal-labs/lab2-1.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2)\r\n
  Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9
  Accept-Language: en-us,en;q=0.50\r\n
  Accept-Encoding: deflate, compress;q=0.8\r\n
```

3. Địa chỉ IP address của máy bạn và gaia.cs.umass.edu server?

Trả lời:

Địa chỉ IP máy nguồn là : 192.168.1.102

Địa chỉ IP của server là : 128.119.245.12

4. Mã trạng thái được trả về từ server cho trình duyệt của bạn.

Trả lời:

Mã trạng thái được trả về từ server cho trình duyệt là : 200 OK

Mã này báo yêu cầu thành công và đối tượng được yêu cầu ở sau trong thông điệp này.

5. Thời điểm file HTML mà bạn đang nhận được chỉnh sửa lần cuối ở server?

Trả lời:

Thời điểm file HTML được chỉnh sửa lần cuối ở server là :

```
Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n
```

6. Có bao nhiêu byte trong nội dung được trả về cho trình duyệt của bạn?

Trả lời:

Số byte nội dung trả về cho trình duyệt là 73

```
☒ Content-Length: 73\r\n
  [Content Length: 73]
  Keep-Alive: timeout=10, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=ISO-8859-1\r\n
```

7. Bằng cách xem xét dữ liệu thô trong cửa sổ nội dung packet, bạn thấy hay không bất kỳ các header bên trong dữ liệu, thứ không được hiển thị trong cửa sổ packet-listing? Nếu có, gọi tên 1 trong số đó.

Trả lời:

Không phải tất cả các header đều hiển thị trong cửa sổ packet-listing.

Ví dụ : Ethernet II hay Internet Protocol

Frame	Source IP	Destination IP	Port	Protocol	Request/Response	Content
12	4.718993	128.119.245.12	192.168.1.102	HTTP	HTTP/1.1 200 OK (text/html)	
13	4.724332	192.168.1.102	128.119.245.12	HTTP	GET /favicon.ico HTTP/1.1	
14	4.750366	128.119.245.12	192.168.1.102	HTTP	HTTP/1.1 404 Not Found (text/html)	

```

Frame 12 (439 bytes on wire, 439 bytes captured)
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: DellComp_4f:36:23 (00:08:74:4f:36:23)
Internet Protocol, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.102 (192.168.1.102)
Transmission Control Protocol, Src Port: http (80), Dst Port: unikeypro (4127), Seq: 1, Ack: 502, Len: 385
Hypertext Transfer Protocol
Line-based text data: text/html

```

8. Kiểm tra nội dung của yêu cầu HTTP GET đầu tiên từ trình duyệt của bạn tới server. Bạn có thấy 1 dòng “IF-MODIFIED-SINCE” trong HTTP GET?

Trả lời:

Không tôi không thấy dòng “IF-MODIFIED-SINCE” trong HTTP GET

9. Kiểm tra các nội dung của phản hồi server. Server có trả về rõ ràng các nội dung của file? Bạn có thể nói thế nào?

Trả lời:

Có, nó được hiển thị trong trường “Line-based text data”

Line-based text data: text/html

```

\n
<html>\n
\n
Congratulations again! Now you've downloaded the file lab2-2.html. <br>\n
This file's last modification date will not change. <p>\n
Thus if you download this multiple times on your browser, a complete copy <br>\n
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
field in your browser's HTTP GET request to the server.\n
\n
</html>\n

```

10. Bây giờ kiểm tra các nội dung của yêu cầu HTTP GET thứ 2 từ trình duyệt của bạn tới server. Bạn có thấy 1 dòng “IF-MODIFIED-SINCE” trong HTTP GET? Nếu có, Có thông tin gì sau “IF-MODIFIED-SINCE:” header?

Có, Thông tin sau dòng đó là :

If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT\r\n

11. Code trạng thái HTTP được trả về từ server trong phản hồi lại HTTP GET thứ hai? Server có trả về rõ ràng nội dung của các file? giải thích.

Trả lời:

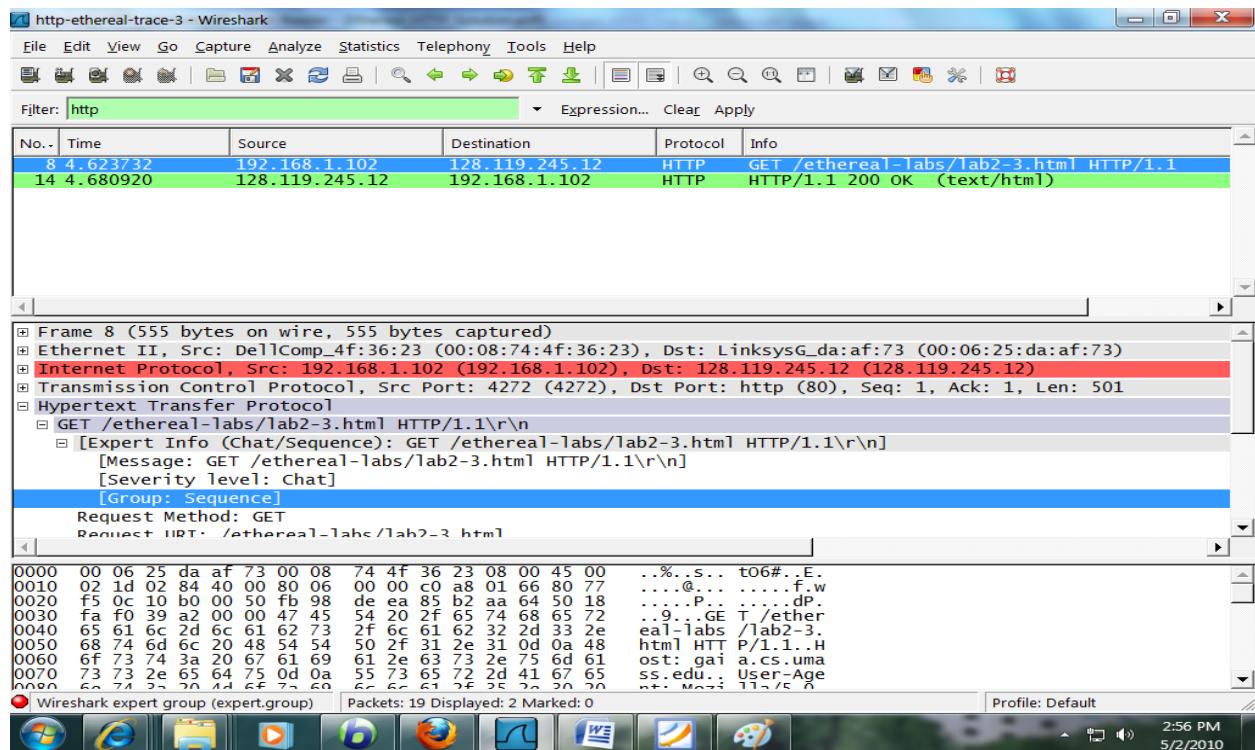
Code trạng thái HTTP được trả về là : HTTP/1.1 304 Not Modified

Server này không trả lại nội dung của file bởi vì file này không được chỉnh sửa và nó được hiển thị ra từ cache chứ không tải lại trên mạng.

12. Có bao nhiêu thông điệp yêu cầu HTTP GET được gửi bởi trình duyệt của bạn ?

Trả lời:

Chỉ có 1 yêu cầu HTTP được gửi bởi trình duyệt



13. Có bao nhiêu TCP segment chứa dữ liệu là cần thiết để mang 1 HTTP response đơn?

Có tổng cộng 4 TCP segment cần thiết để mang 1 HTTP response đơn gồm :

1460, 1460, 1460 và 436 byte tổng cộng là 4816 byte.

[Reassembled TCP Segments (4816 bytes): #10(1460), #11(1460), #13(1460), #14(436)]
[Frame: 10, payload: 0-1459 (1460 bytes)]
[Frame: 11, payload: 1460-2919 (1460 bytes)]
[Frame: 13, payload: 2920-4379 (1460 bytes)]
[Frame: 14, payload: 4380-4815 (436 bytes)]

14. Phần và code trạng thái liên kết với sự phản hồi cho yêu cầu HTTP GET là gì?

Code trạng thái phản hồi là : 200 OK

15. Có không bất kỳ dòng trạng thái HTTP nào trong dữ liệu được truyền liên quan đến 1 TCP được cảm ứng tiếp tục

Trả lời:

Không có bất kỳ dòng trạng thái HTTP nào trong dữ liệu được truyền mà lại liên quan đến 1 TCP được cảm ứng tiếp tục.

16. Có bao nhiêu thông điệp yêu cầu HTTP GET được gửi bởi trình duyệt của bạn? các địa chỉ Internet nào được các yêu cầu GET gửi tới?

No..	Time	Source	Destination	Protocol	Info
10	7.236929	192.168.1.102	128.119.245.12	HTTP	GET /ethereal-labs/lab2-4.html HTTP/1.1
12	7.260813	128.119.245.12	192.168.1.102	HTTP	HTTP/1.1 200 OK (text/html)
17	7.305485	192.168.1.102	165.193.123.218	HTTP	GET /catalog/images/pearson-logo-footer.gif
20	7.308803	192.168.1.102	134.241.6.82	HTTP	GET ~/kurose/cover.jpg HTTP/1.1
25	7.333054	165.193.123.218	192.168.1.102	HTTP	HTTP/1.1 200 OK (GIF89a)
54	7.589877	134.241.6.82	192.168.1.102	HTTP	HTTP/1.0 200 Document follows (JPEG JFIF in

Có 3 thông điệp yêu cầu HTTP GET được gửi bởi trình duyệt, các địa chỉ được yêu cầu GET gửi tới là :

- * 128.119.245.12
- * 165.193.123.218
- * 134.241.6.82

17. Bạn có thể nói có hay không trình duyệt của bạn download 2 ảnh tuần tự hay chúng được download từ 2 trang web song song? Giải thích

Trả lời:

Ở đây 2 ảnh được download tuần tự. Ta có thể thấy qua thời gian download frame đó về

```
☒ Frame 54 (1096 bytes on wire, 1096 bytes captured)
    Arrival Time: Sep 23, 2003 12:38:42.040490000
☒ Frame 25 (912 bytes on wire, 912 bytes captured)
    Arrival Time: Sep 23, 2003 12:38:41.783667000
```

18. Hồi phản hồi gì của server (phần và code trạng thái) tới thông điệp HTTP GET ban đầu từ trình duyệt của bạn?

Trả lời:

Mã phản hồi là : 401

Phrase : Authorization Required

Hex	Dec	ASCII	Comments
0000	48 54 54 50 2f 31 2e 31 20 34 30 31 20 41 75 74	HTTP/1.1 401 Aut	
0010	68 6f 72 69 7a 61 74 69 6f 6e 20 52 65 71 75 69	horizati on Requi	
0020	72 65 64 0d 0a 44 61 74 65 3a 20 54 75 65 2c 20	red..Dat e: Tue,	

19. Khi trình duyệt của bạn gửi thông điệp HTTP GET trong lần 2, trường nào mới bao gồm trong thông điệp HTTP GET?

Trả lời:

Có 1 trường mới là trường Authorization

The screenshot shows a Wireshark capture window. At the top, there is a status bar with the text "Connection: keep-alive\r\n". Below it, a blue-highlighted section contains the "Authorization" header field: "Authorization: Basic ZXRoLXN0dWRLbnRzOm5ldHdvcmtz\r\n". Underneath this, the "Credentials" field is shown as "eth-students:networks". The main pane displays a list of bytes for several network frames, starting from frame 0200. The bytes for the highlighted Authorization header are: 0a 41 75 74 68 6f 72 69. To the right of these bytes, the ASCII representation is partially visible: "0.66, *; q=0.66.. Keep-Ali ve: 300. .Connect ion: kee p-alive. .Authori zation: Basic ZX RoLXN0dW RLbnRzOm 5ldHdvcm tz...".

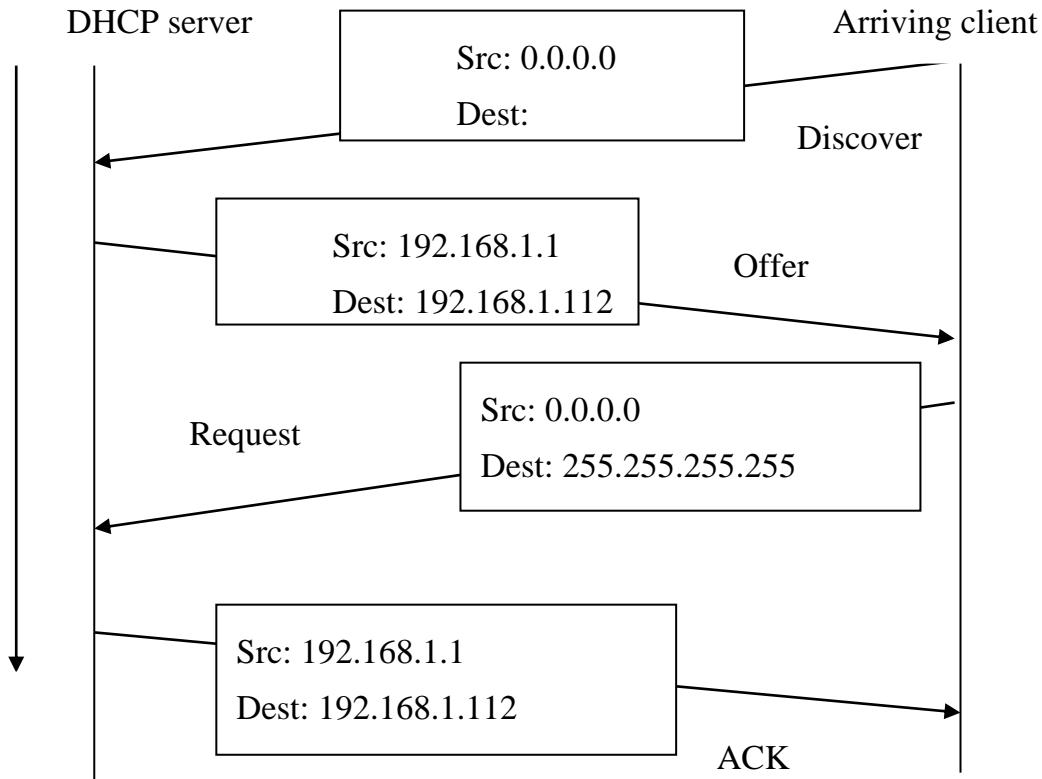
6.7.3 Wireshark Lab : DHCP

- Thông điệp DHCP được gửi qua UDP hay TCP?

Trả lời:

Thông điệp DHCP được gửi qua UDP

- Vẽ một datagram minh họa trình tự thời gian của 4 gói đầu tiên Discover/Offer/Request/ACK DHCP trao đổi giữa client và server. Mỗi gói sẽ chỉ ra số cổng nguồn và cổng đích. Số cổng trong ví dụ đưa ra và trong phòng lab có giống nhau không?



3. Địa chỉ link-layer của máy bạn là gì?

Trả lời:

Địa chỉ link-layer là : 00:1e:ec:66:97:e4

4. Giá trị nào của DHCP *discover message* phân biệt với DHCP *request message*

Trả lời:

Là giá trị Option

5. Giá trị của Transaction-ID trong từng thông điệp trong 4 thông điệp đầu tiên của DHCP (Discover/Offer/Request/ACK) bằng bao nhiêu? Chức năng của trường Transaction-ID ?

1. 0xd38t2330

2. 0x92c3653c

Transaction-ID là một số ngẫu nhiên được tạo ra bởi client. Mục đích của nó được sử dụng cung cấp cho client và DHCP server có thể được xác định qua sự quan hệ giữa các thông điệp DHCP gửi đi và nhận.

6. Host dùng DHCP để chia sẻ địa chỉ IP, nhưng địa chỉ IP của host không chấp nhận cho đến khi kết thúc việc trao đổi của 4 thông điệp. Nếu địa chỉ IP không được xác định cho đến khi kết thúc việc trao đổi của 4 thông điệp, sau đó giá trị nào là được dùng trong gói dữ liệu ngăn IP trong 4 thông điệp khi trao đổi??? Với mỗi 4 thông điệp

DHCP(Discover, Offer, Request, ACK) cho biết địa chỉ IP nguồn và đích được thực hiện trong lúc gói dữ liệu IP đóng gói.

Src: 0.0.0.0

Dst:

7. Địa chỉ IP của DHCP server của bạn là gì?

Trả lời:

192.168.1.36

8. Trên DHCP thì địa chỉ IP nào chỉ host của bạn trong *DHCP Offer message*. Chỉ rõ thông điệp DHCP nào chứa địa chỉ DHCP

Trả lời:

```
Bootp flags: 0x0000 (unicast)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 192.168.1.112 (192.168.1.112)
Next server IP address: 192.168.1.1 (192.168.1.1)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: CompaqIn_66:97:e4 (00:1e:ec:66:97:e4)
Client hardware address padding: 000000000000000000000000
Server host name: TP-LINK
Boot file name not given
```

9. Trong ví dụ trên ko có tác nhân relay nào giữa host và DHCP server. Giá trị nào của trace cho thấy không có khả năng nào cho một tác nhân relay? Có tác nhân relay nào bạn đã gặp phải? và địa chỉ IP của nó là gì?

Trả lời:

relay agent chịu trách nhiệm để kiểm soát quá trình gửi thông điệp DHCP từ bên này đến các mạng subnet khác. Trong thí nghiệm này ko có relay agent nào vì

ID: 0.0.0.0

10. Giải thích chức năng của router và mặt nạ supnet trong *DHCP offer message*

Trả lời:

Router được dùng để lấy địa chỉ IP của router qua client., Subnet mask Chúng được sử dụng để phân chia một mạng lớn thành các mạng nhỏ hơn

11. Trong ví dụ, host yêu cầu một địa chỉ IP trong *DHCP Request message*. Bạn đã làm gì?

Trả lời:

Host yêu cầu đề nghị với địa chỉ IP trong thông điệp DHCP request

12. Giải thích chức năng của lease time. Bạn đã làm lease time trong bao lâu?

Trả lời:

Lease time là thời gian mà nó nói lên cho biết thời gian mà địa chỉ IP dùng. Trong lab này, thời gian lease time là 3 ngày

```

    + Option: (t=53,l=1) DHCP Message Type = DHCP Offer
    + Option: (t=1,l=4) Subnet Mask = 255.255.255.0
    + Option: (t=15,l=1) Domain Name =
    + Option: (t=3,l=4) Router = 192.168.1.1
    + Option: (t=6,l=4) Domain Name Server = 192.168.1.1
    + Option: (t=58,l=4) Renewal Time value = 1 day, 12 hours
    + Option: (t=59,l=4) Rebinding Time value = 2 days, 15 hours
    + Option: (t=51,l=4) IP Address Lease Time = 3 days
    + Option: (t=54,l=4) DHCP Server Identifier = 192.168.1.1
    End Option
    Padding

```

13. Chức năng của *DHCP release message* là gì? DHCP server đưa ra thông báo xác nhận yêu cầu của DHCP của client. Chuyện gì sẽ xảy ra nếu thông điệp từ DHCP của client bị mất?

Trả lời:

Thông điệp DHCP release được dùng để cho biết DHCP server mà client đã sẵn sàng được dùng cho địa chỉ IP. Nếu thông điệp DHCP release bị mất thì sau đó địa chỉ IP sẽ được dùng cho đến khi hết hạn thời gian.

14. Làm sáng tỏ bootp filter trong cửa sổ wireshark. Bất kỳ gói ARP nào cũng được gửi hoặc nhận trong quá trình trao đổi các gói

Trả lời:

ARP (address solution protocol) là giao thức mà nó dùng cho việc đánh dấu giữa địa chỉ IP và địa chỉ MAC.

TÓM TẮT NỘI DUNG CỐT LÕI.

- Các máy chủ phục vụ tên miền
- Thư điện tử
- World Wide Web
- Truyền dữ liệu đa phương tiện
- Dịch vụ FTP
- Các lệnh cơ bản

BÀI TẬP ÚNG DỤNG:

Câu 1: Trình bày kiến trúc các server phục vụ tên miền.

Câu 2: Trình bày các thành phần hệ thống email và xây dựng mô hình email nội bộ cho doanh nghiệp.

Câu 3: Trình bày quy trình kết nối TCP trong dịch vụ World Wide Web

Câu 4: Trình bày kiến trúc giao thức FTP và xây dựng hệ thống FTP mô phỏng.

Câu 5: Xây dựng mô hình hệ thống máy chủ phục vụ tên cho danh nghiệp.

Câu 6: Xây dựng mô hình hệ thống máy chủ quản lý thư điện tử nội bộ.

Câu 7: Xây dựng mô hình máy chủ Web cho danh nghiệp

Câu 8: Xây dựng mô hình máy chủ truyền dữ liệu đa phương tiện dựa trên giao thức FTP.

Chương 7. MẠNG KHÔNG DÂY VÀ MẠNG DI ĐỘNG

Mục tiêu:

- Hiểu về cơ sở hạ tầng và các mô hình mạng cục bộ không dây.
- Hiểu cơ bản về các giải pháp bảo mật mạng không dây.
- Hiểu về các chuẩn không dây họ IEEE 802.
- Hiểu về mạng không dây dài tầm rộng.

7.1. Mạng cục bộ không dây (WLAN - Wireless LAN)

7.1.1. Giới thiệu về WLAN

Mạng LAN không dây viết tắt là **WLAN** (Wireless Local Area Network) hay WIFI (Wireless Fidelity), là một mạng dùng để kết nối hai hay nhiều máy tính với nhau mà không sử dụng dây dẫn. **WLAN** dùng công nghệ trai phô, sử dụng sóng vô tuyến cho phép truyền thông giữa các thiết bị trong một vùng nào đó gọi là Basic Service Set.

Đây là một giải pháp có rất nhiều ưu điểm so với kết nối mạng có dây (wireline) truyền thống. Người dùng vẫn duy trì kết nối với mạng khi di chuyển trong vùng phủ sóng.

7.1.2. Lịch sử hình thành và phát triển

Năm 1990, công nghệ **WLAN** lần đầu tiên xuất hiện, khi những nhà sản xuất giới thiệu những sản phẩm hoạt động ở băng tần 900 Mhz. Các giải pháp này (không có sự thống nhất của các nhà sản xuất) cung cấp tốc độ truyền dữ liệu 1Mbs, thấp hơn rất nhiều so với tốc độ 10 Mbs của hầu hết các mạng sử dụng cáp lúc đó.

Năm 1992, các nhà sản xuất bắt đầu bán những sản phẩm **WLAN** sử dụng băng tần 2.4GHz. Mặc dù những sản phẩm này có tốc độ truyền cao hơn nhưng chúng vẫn chỉ là những giải pháp riêng của mỗi nhà sản xuất và không được công bố rộng rãi. Sự cần thiết cho việc thống nhất hoạt động giữa các thiết bị ở những dãy tần số khác nhau dẫn đến một số tổ chức bắt đầu phát triển ra những chuẩn **mạng không dây**.

Năm 1997, IEEE (Institute of Electrical and Electronics Engineers) đã thông qua sự ra đời của chuẩn 802.11, và được biết đến với tên WIFI (Wireless Fidelity) cho các mạng **WLAN**.

Năm 1999, IEEE thông qua sự bổ sung cho chuẩn 802.11 là chuẩn 802.11a và 802.11b (định nghĩa ra những phương pháp truyền tín hiệu). Và các thiết bị **WLAN** dựa trên chuẩn 802.11b đã nhanh chóng trở thành công nghệ không dây nổi trội.

Năm 2003, IEEE công bố thêm sự cải tiến là chuẩn 802.11g, chuẩn này có gắng tích hợp tốt nhất các chuẩn 802.11a, 802.11b và 802.11g. Sử dụng băng tần 2.4Ghz cho phạm vi phủ sóng lớn hơn.

Năm 2009, IEEE cuối cùng thông qua chuẩn WIFI thế hệ mới 802.11n sau 6 năm thử nghiệm. Chuẩn 802.11n có khả năng truyền dữ liệu ở tốc độ 300Mbps hay thậm chí cao hơn.

7.1.2.1. *Ưu điểm của WLAN*

Sự tiện lợi: mạng không dây cung cấp giải pháp cho phép người sử dụng truy cập tài nguyên trên mạng ở bất kì nơi đâu trong khu vực WLAN được triển khai (khách sạn, trường học, thư viện...). Với sự bùng nổ của máy tính xách tay và các thiết bị di động hỗ trợ wifi như hiện nay, điều đó thật sự rất tiện lợi.

Khả năng di động: Với sự phát triển vô cùng mạnh mẽ của viễn thông di động, người sử dụng có thể truy cập internet ở bất cứ đâu. Như: Quán cafe, thư viện, trường học và thậm chí là ở các công viên hay vỉa hè. Người sử dụng đều có thể truy cập internet miễn phí.

Hiệu quả: Người sử dụng có thể duy trì kết nối mạng khi họ đi từ nơi này đến nơi khác.

Triển khai: Rất dễ dàng cho việc triển khai mạng không dây, chúng ta chỉ cần một đường truyền ADSL và một AP là được một mạng WLAN đơn giản. Với việc sử dụng cáp, sẽ rất tốn kém và khó khăn trong việc triển khai ở nhiều nơi trong tòa nhà.

Khả năng mở rộng: Mở rộng dễ dàng và có thể đáp ứng tức thì khi có sự gia tăng lớn về số lượng người truy cập.

7.1.2.2. *Nhược điểm*

Bên cạnh những thuận lợi mà mạng không dây mang lại cho chúng ta thì nó cũng mắc phải những nhược điểm. Đây là sự hạn chế của các công nghệ nói chung.

- **Bảo mật:** Đây có thể nói là nhược điểm lớn nhất của mạng WLAN, bởi vì phương tiện truyền tín hiệu là sóng và môi trường truyền tín hiệu là không khí nên khả năng một mạng không dây bị tấn công là rất lớn

- **Phạm vi:** Như ta đã biết chuẩn IEEE 802.11n mới nhất hiện nay cũng chỉ có thể hoạt động ở phạm vi tối đa là 150m, nên mạng không dây chỉ phù hợp cho một không gian hẹp.

- **Độ tin cậy:** Do phương tiện truyền tín hiệu là sóng vô tuyến nên việc bị nhiễu, suy giảm... là điều không thể tránh khỏi. Điều này gây ảnh hưởng đến hiệu quả hoạt động của mạng.

- **Tốc độ:** Tốc độ cao nhất hiện nay của WLAN có thể lên đến 600Mbps nhưng vẫn chậm hơn rất nhiều so với các mạng cáp thông thường (có thể lên đến hàng Gbps)

7.1.3. Cơ sở hạ tầng WLAN

7.1.3.1. Cấu trúc cơ bản của WLAN

Distribution System (Hệ thống phân phối): Đây là một thành phần logic sử dụng để điều phối thông tin đến các station đích. Chuẩn 802.11 không đặc tả chính xác kỹ thuật cho DS.

Access Point: chức năng chính của AP là mở rộng mạng. Nó có khả năng chuyển đổi các frame dữ liệu trong 802.11 thành các frame thông dụng để có thể sử dụng trong mạng khác.

Wireless Medium (tầng liên lạc vô tuyến): Chuẩn 802.11 sử dụng tần số liên lạc vô tuyến để chuyển đổi các frame dữ liệu giữa các máy trạm với nhau.

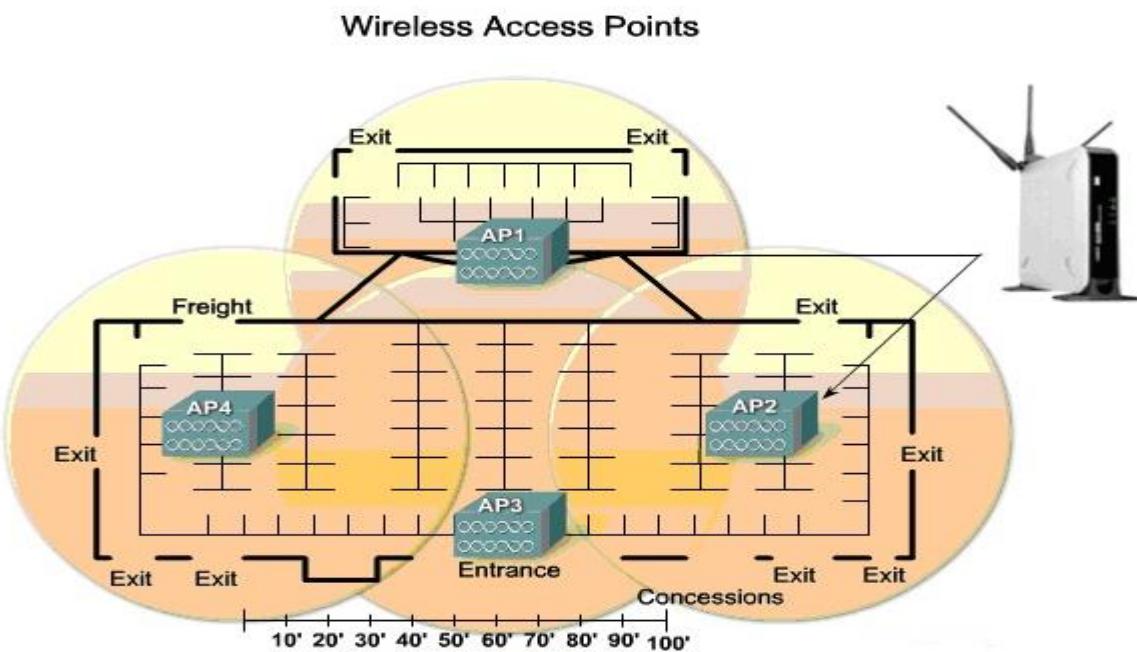
Station (các máy trạm): Đây là các thiết bị ngoại vi có hỗ trợ kết nối vô tuyến như: laptop, PDA, Palm...



Hình 7. 1 Cấu trúc cơ bản của WLAN

7.1.3.2. Thiết bị dành cho WLAN

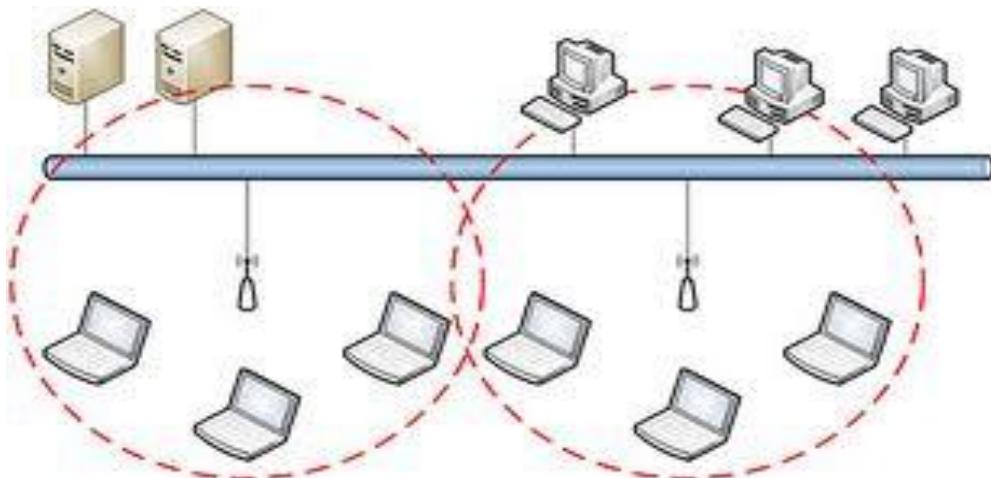
Wireless access point(AP): Là thiết bị có nhiệm vụ cung cấp cho máy khách (client) một điểm truy cập vào mạng.



Hình 7. 2 Thiết bị Wireless accesspoint

Các chế độ hoạt động của AP: AP có ba chế độ hoạt động chính.

Chế độ gốc (root mode): Root mode được sử dụng khi AP kết nối với mạng backbone có dây thông qua giao diện có dây (thường là Ethernet) của nó. Hầu hết các AP đều hoạt động ở chế độ mặc định là root mode.



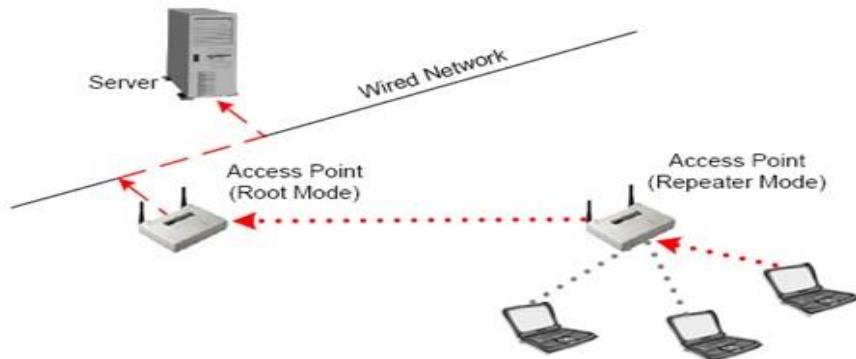
Hình 7. 3AP hoạt động ở root mode

Chế độ cầu nối(bridge mode): Trong bridge mode, AP hoạt động hoàn toàn như cầu nối không dây. Với chế độ này, máy khách (client) sẽ không kết nối trực tiếp với AP, nhưng thay vào đó, AP dùng để nối hai hay nhiều đoạn mạng có dây lại với nhau. Hiện nay, hầu hết các thiết bị AP đều hỗ trợ chế độ bridge.



Hình 7. 4 Chế độ cầu nối của AP

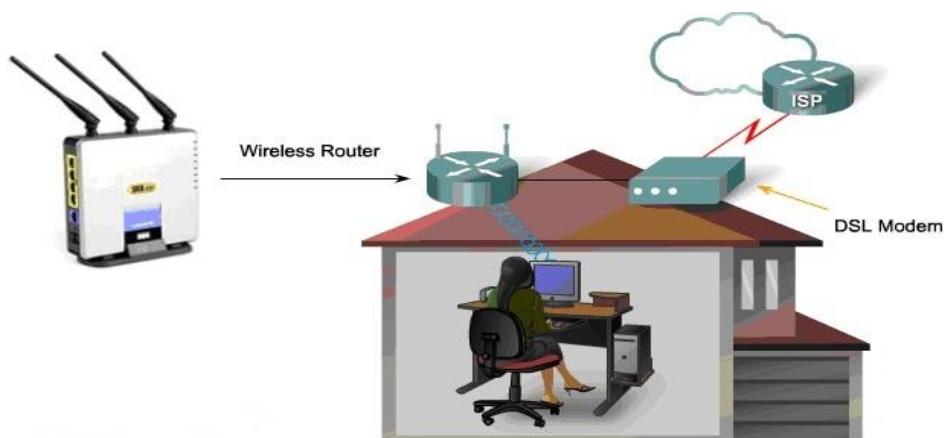
Chế độ lặp (Repeater mode): Ở chế độ Repeater, sẽ có ít nhất hai thiết bị AP, một root AP và một AP hoạt động như một Repeater không dây. AP trong Repeater mode hoạt động như một máy khách khi kết nối với root AP và hoạt động như một AP khi kết nối với máy khách.



Hình 7. 5 Chế độ Repeater của AP

Wireless Router

Ngày nay, với sự tiến bộ của công nghệ và kỹ thuật, sự ra đời của thiết bị đa năng Wireless Router với sự kết hợp chức năng của ba thiết bị là Wireless accesspoint, Ethernet Switch và Router.



Hình 7. 6 Thiết bị Wireless Router

Wireless NICs:

Là các thiết bị được máy khách dùng để kết nối vào AP.



Hình 7. 7 Wireless NICs

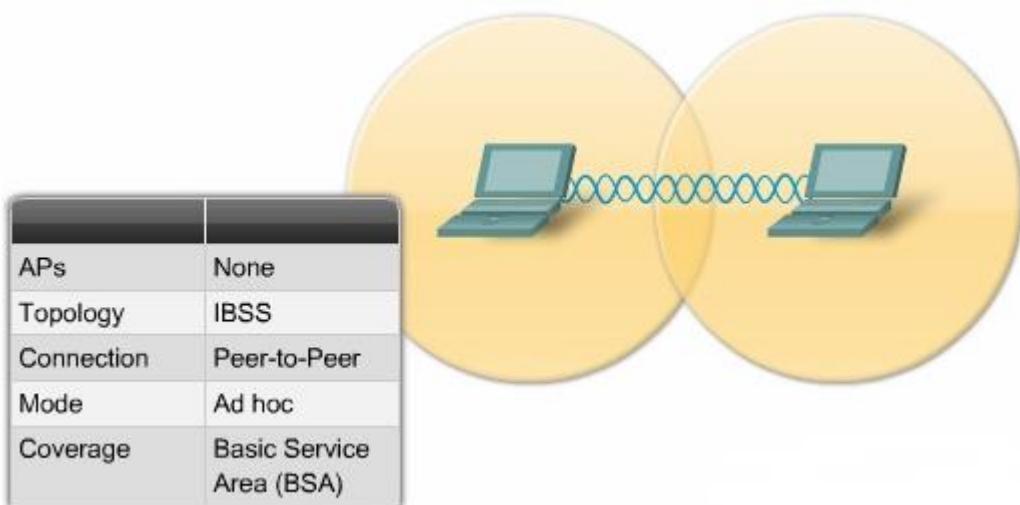
7.1.4. Các mô hình WLAN

Mạng 802.11 rất linh hoạt về thiết kế, bao gồm 3 mô hình cơ bản sau

- ✓ Mô hình mạng độc lập (IBSSs) hay còn gọi là mạng Ad-hoc.
- ✓ Mô hình mạng cơ sở (BSSs).
- ✓ Mô hình mạng mở rộng (ESSs).

7.1.4.1 Mô hình mạng độc lập

Mạng IBSSs (Independent Basic Service Set) hay còn gọi là mạng ad-hoc, trong mô hình mạng ad-hoc các client liên lạc trực tiếp với nhau mà không cần thông qua AP nhưng phải ở trong phạm vi cho phép. Mô hình mạng nhỏ nhất trong chuẩn 802.11 là 2 máy client liên lạc trực tiếp với nhau. Thông thường mô hình này được thiết lập bao gồm một số client được cài đặt dùng chung mục đích cụ thể trong khoảng thời gian ngắn .Khi mà sự liên lạc kết thúc thì mô hình IBSS này cũng được giải phóng.

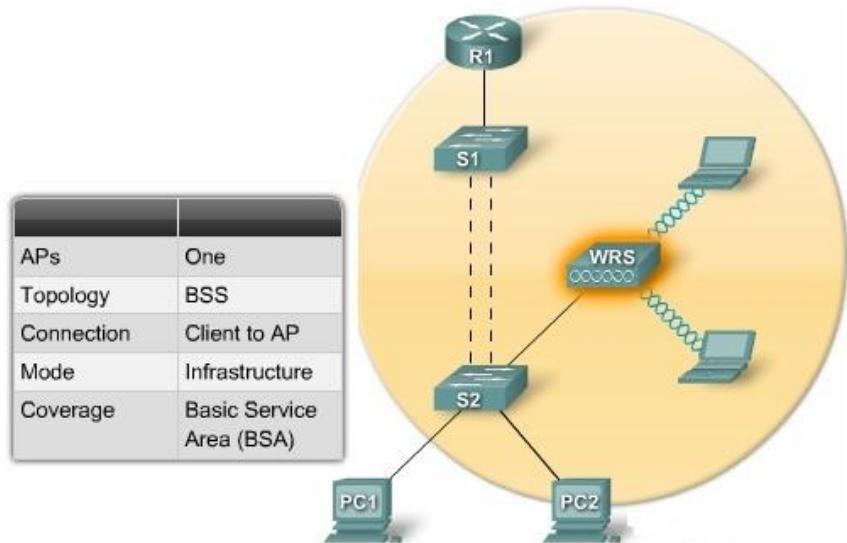


Hình 7.8 Mô hình mạng Ad-hoc.

7.1.4.2. Mô hình mạng cơ sở (BSSs)

The Basic Service Sets (BSS) là một topology nền tảng của mạng 802.11. Các thiết bị giao tiếp tạo nên một BSS với một AP duy nhất với một hoặc nhiều client. Các máy trạm kết nối với sóng wireless của AP và bắt đầu giao tiếp thông qua AP. Các máy trạm là thành viên của BSS được gọi là “có liên kết”.

Thông thường các AP được kết nối với một hệ thống phân phối trung bình (DSM), nhưng đó không phải là một yêu cầu cần thiết của một BSS. Nếu một AP phục vụ như là



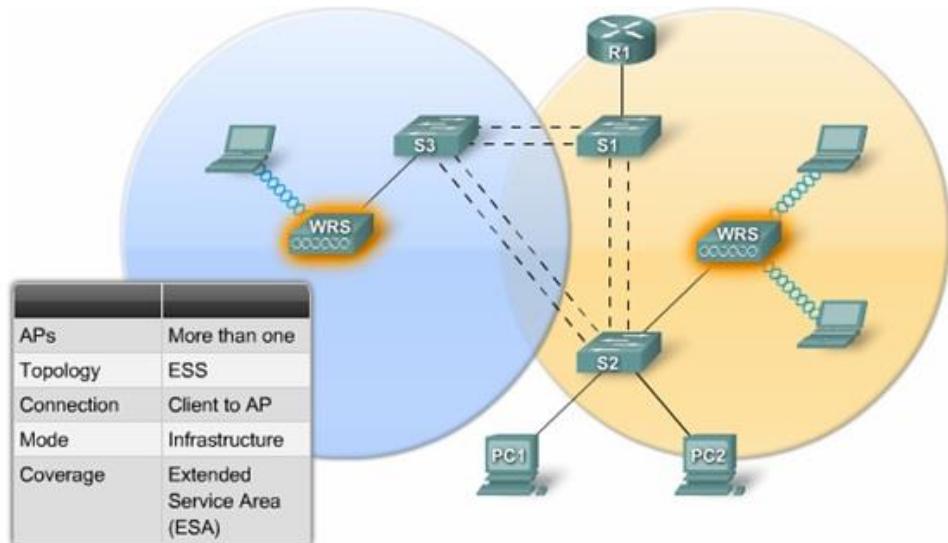
cổng để vào dịch vụ phân phối, các máy trạm có thể giao tiếp, thông qua AP, với nguồn tài nguyên mạng ở tại hệ thống phân phối trung bình. Nó cũng cần lưu ý là nếu các máy client muốn giao tiếp với nhau, chúng phải chuyển tiếp dữ liệu thông qua các AP. Các client không thể truyền thông trực tiếp với nhau, trừ khi thông qua các AP. Hình sau mô tả mô hình một BSS chuẩn.

Hình 7.9 Mô hình mạng BSS chuẩn

7.1.4.3. Mô hình mạng mở rộng (ESSs)

Trong khi một BSS được coi là nền tảng của mạng 802.11, một mô hình mạng mở rộng ESS (extended service set) của mạng 802.11 sẽ tương tự như là một tòa nhà được xây dựng bằng đá. Một ESS là hai hoặc nhiều BSS kết nối với nhau thông qua hệ thống phân phối. Một ESS là một sự hội tụ nhiều điểm truy cập và sự liên kết các máy trạm của chúng. Tất cả chỉ bằng một DS. Một ví dụ phổ biến của một ESS có các AP với mức độ một phần các tế bào chồng chéo lên nhau. Mục đích đằng sau của việc này là để cung cấp sự chuyển vùng liên tục cho các client. Hầu hết các nhà cung cấp dịch vụ đề nghị các tế

bào chòng lên nhau khoảng 10%-15% để đạt được thành công trong quá trình chuyển vùng.



Hình 7. 10 Mô hình mạng ESS

7.1.5. Các giải pháp bảo mật WLAN

Với các hình thức tấn công được nêu trên, hacker có thể lợi dụng bất cứ điểm yếu và tấn công vào hệ thống v WLAN bất cứ lúc nào. Vì vậy, để ra các biện pháp bảo mật WLAN là điều cấp thiết. Dưới đây là các biện pháp bảo mật WLAN qua các thời kỳ. Có một số biện pháp đã bị hacker qua mặt như mã hóa WEB... Bài viết sau Viet-cntt.com sẽ trình bày các giải pháp bảo mật WLAN để biết rõ được ưu điểm, nhược điểm của các giải pháp bảo mật. Từ đó lựa chọn các giải pháp bảo mật phù hợp với từng mô hình của mạng WLAN

7.1.5.1. WEP

Wep (Wired Equivalen Privacy) có nghĩa là bảo mật không dây tương đương với có dây. Thực ra, WEP đã đưa cả xác thực người dùng và đảm bảo an toàn dữ liệu vào cùng một phương thức không an toàn. WEP sử dụng một khóa mã hóa không thay đổi có độ dài 64 bit hoặc 128 bit, (nhưng trừ đi 24 bit sử dụng cho vector khởi tạo khóa mã hóa, nên độ dài khóa chỉ còn 40 bit hoặc 104 bit) được sử dụng để xác thực các thiết bị được phép truy cập vào mạng và cũng được sử dụng để mã hóa truyền dữ liệu.

Rất đơn giản, các khóa mã hóa này dễ dàng được “bẻ gãy” bởi thuật toán brute-force và kiểu tấn công thử lỗi (trial-and-error). Các phần mềm miễn phí như Aircrack-ng, Airsnort, hoặc WEP crack sẽ cho phép hacker có thể phá vỡ khóa mã hóa nếu họ thu thập từ 5 đến 10 triệu gói tin trên một mạng không dây. Với những khóa mã hóa 128 bit cũng không khác biệt: 24 bit cho khởi tạo mã hóa nên chỉ có 104 bit được sử dụng.

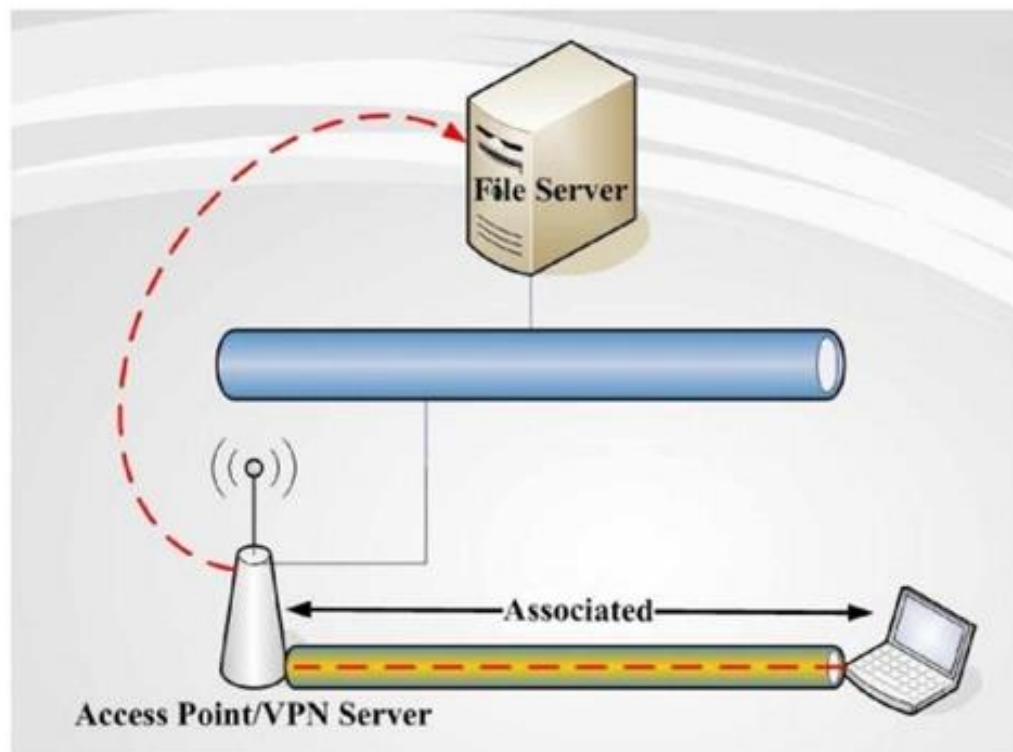
Dụng để mã hóa và cách thức cũng giống như mã hóa có độ dài 64 bit nên mã hóa 128 bit cũng dễ dàng bị bẻ khóa. Ngoài ra, những điểm yếu trong những vector khởi tạo

khóa mã hoá giúp cho hacker có thể tìm ra mật khẩu nhanh hơn với ít gói thông tin hơn rất nhiều.

Không dự đoán được những lỗi trong khóa mã hóa. WEP có thể được tạo ra cách bảo mật mạnh mẽ hơn nếu sử dụng một giao thức xác thực mà cung cấp mỗi khóa mã hóa mới cho mỗi phiên làm việc. Khóa mã hóa sẽ thay đổi trên mỗi phiên làm việc. Điều này sẽ gây khó khăn hơn cho hacker thu thập đủ các gói dữ liệu cần thiết để có thể bẻ gãy khóa bảo mật.

7.1.5.2. WLAN VPN

Mạng riêng VPN bảo vệ mạng WLAN bằng cách tạo ra một kênh che chằng dữ liệu khỏi các truy cập trái phép. VPN tạo ra một tin cậy cao thông qua việc sử dụng một cơ chế bảo mật như Ipsec (internetProtocol Security). IPsec để mã hóa dữ liệu và dùng các thuật toán khác để các thực gói dữ liệu. Ipsec cũng sử dụng thẻ xác nhận số để xác nhận khóa mã (public key). Khi được sử dụng trên mạng WLAN, công kết của VPN đảm bảo xác thực, đóng gói và mã hóa



Hình 7.11 Mô hình WLAN VPN

7.1.5.3. TKIP (Temporal Key Integrity Protocol)

Là giải pháp của IEEE được phát triển năm 2004. Là một nâng cấp cho WEP nhằm vành đai bảo mật trong cài đặt mã dòng RC4 trong WEP. TKIP dùng hàm băm (hashing) IV để chống lại việc MIC (message integrity check) để đảm bảo tính chính xác của gói tin TKIP và sử dụng khóa động bằng cách đặt cho mỗi frame một chuỗi sóng lại dạng tấn công giả mạo.

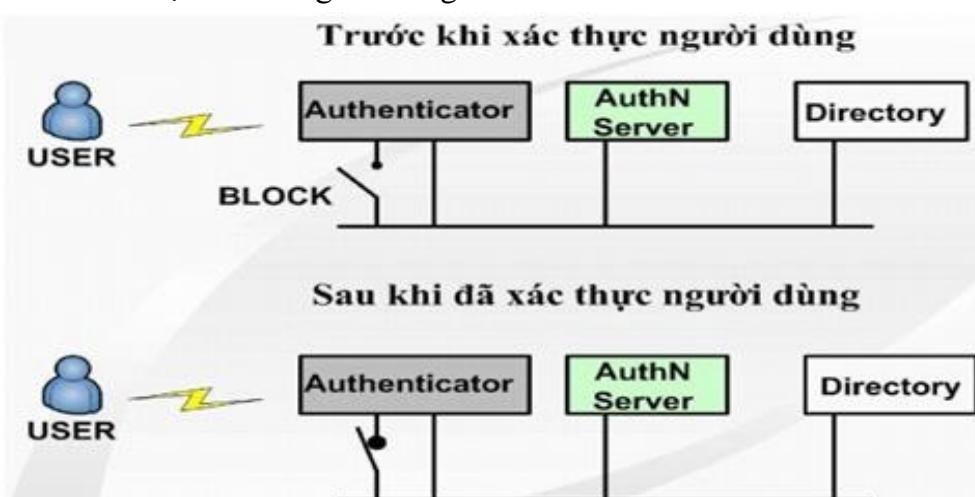
7.1.5.4. AES

Trong mật mã học AES (viết tắt của từ tiếng Anh: Advanced Encryption Standard, hay Tiêu chuẩn mã hóa tiên tiến) là một thuật toán mã hóa khối được chính phủ Hoa Kỳ áp dụng làm tiêu chuẩn mã hóa. Giống như tiêu chuẩn tiền nhiệm DES, AES được kỳ vọng áp dụng trên phạm vi thế giới và đã được nghiên cứu rất kỹ lưỡng. AES được chấp nhận làm tiêu chuẩn liên bang bởi viện tiêu chuẩn và công nghệ quốc gia Hoa Kỳ (NIST) sau một quá trình tiêu chuẩn hóa kéo dài 5 năm.

Thuật toán được thiết kế bởi 2 nhà mật mã học người Bỉ: Joan Daemen và Vincent Rijmen (lấy tên chung là Rijndael khi tham gia cuộc thi thiết kế AES). Rijndael được phát âm là “Rhine dahl” (theo phiên âm quốc tế).

7.1.5.5 802.1X và EAP

802.1x là chuẩn đặc tả cho việc truy cập dựa trên cổng (port-based) được định nghĩa bởi IEEE. Hoạt động trên cả môi trường có dây truyền thống và không dây. Việc điều khiển truy cập được thực hiện bằng cách: Khi một người dùng cố gắng kết nối vào hệ thống mạng, kết nối của người dùng sẽ được đặt ở trạng thái bị chặn (blocking) và chờ cho việc kiểm tra định danh người dùng hoàn tất.



Hình 7. 12 Mô hình hoạt động xác thực 802.1x

EAP là phương thức xác thực bao gồm yêu cầu định danh người dùng (password, certificate,...), giao thức được sử dụng (MD5, TLI_Transport Layer Security, OTP_One Time Password,...) hỗ trợ tự động sinh khóa và xác thực lẫn nhau.

v Quá trình chứng thực 802.1x-EAP như sau:

Wireless client muốn liên kết với một AP trong mạng.

1. AP sẽ chặn lại tất cả các thông tin của client cho tới khi client log on vào mạng. Khi đó client yêu cầu liên kết với AP.

2. AP đáp lại yêu cầu liên kết với một yêu cầu nhận dạng EAP.

3. Client gửi đáp lại yêu cầu nhận dạng EAP cho AP.

4. Thông tin đáp lại yêu cầu nhận dạng EAP của client được chuyển tới Server chứng thực.

5. Server chứng thực gửi một yêu cầu cho phép AP.

6. AP chuyển yêu cầu cho phép tới client.

7. Client gửi trả lời sự cấp phép EAP tới AP.

8. AP chuyển sự trả lời đó tới Server chứng thực.

9. Server chứng thực gửi một thông báo thành công EAP tới AP.

10. AP chuyển thông báo thành công tới client và đặt cổng của client trong chế độ forward.

7.1.5.6 WPA (WI-FI Protected access)

WEP được xây dựng để bảo vệ một mạng không dây tránh bị nghe trộm. Nhưng nhanh chóng sau đó người ta phát hiện ra nhiều lỗ hổng công nghệ này. Do đó công nghệ mới có tên gọi WPA (Wi-Fi Protected access) ra đời, khắc phục được nhiều nhược điểm của WEP.

Trong những cải tiến quan trọng nhất của WPA là sử dụng hàm thay đổi khóa TKIP. WPA cũng sử dụng thuật toán RC4 như WEP, nhưng mã hóa đầy đủ 128 bit. Và một đặc điểm khác là WPA thay đổi khóa cho mỗi gói tin. Các công cụ thu thập các gói tin để khóa phá mã hóa đều không thể thực hiện được với WPA. Bởi WPA thay đổi khóa liên tục nên hacker không bao giờ thu thập đủ dữ liệu mẫu để tìm ra mật khẩu.

Không những thế WPA còn bao gồm cả tính toàn vẹn của thông tin (Message Integrity check). Vì vậy, dữ liệu không thể bị thay đổi trong khi đang ở trên đường truyền. WPA có sẵn 2 lựa chọn: WPA Personal và WPA Enterprise. Cả 2 lựa chọn đều sử dụng giáo thức TKIP, và sự khác biệt chỉ là khóa khởi tạo mã hóa lúc đầu. WPA Personal thích hợp cho gia đình và mạng văn phòng nhỏ, khóa khởi tạo sẽ được sử dụng tại các điểm truy cập và thiết bị máy trạm. Trong khi đó, WPA cho doanh nghiệp cần một máy chủ xác thực và 802.1x để cung cấp các khóa khởi tạo cho mỗi phiên làm việc.

Lưu ý:

Có một lỗ hổng trong WPA và lỗi này chỉ xảy ra với WPA Personal. Khi mà sử dụng hàm thay đổi khóa TKIP được sử dụng để tạo ra các khóa mã hóa chưa phát hiện, nếu hacker có thể đoán được khóa khởi tạo hoặc một phần của mật khẩu, họ có thể xác định được toàn bộ mật khẩu, do đó có thể giải mã được dữ liệu. tuy nhiên, lỗ hổng này cũng sẽ được loại bỏ bằng cách sử dụng những khóa khởi tạo không dễ đoán (dùng sử dụng những từ như “P@SSWORD” để làm mật khẩu).

Điều này cũng có nghĩa rằng thủ thuật TKIP của WPA chỉ là giải pháp tạm thời, chưa cung cấp một phương thức bảo mật cao nhất. WPA chỉ thích hợp với những công ty mà không truyền dữ liệu “mật” về những thương mại hay các thông tin nhạy

cảm... WPA cũng thích hợp với những hoạt động hằng ngày và mang tính thử nghiệm công nghệ.

7.1.5.7. WPA2

Một giải pháp về lâu dài là sử dụng 802.11i tương đương với WPA2, được chứng nhận bởi Wi-Fi Alliance. Chuẩn này sử dụng thuật toán mã hóa mạnh mẽ và được gọi là Chuẩn mã hóa nâng cao AES. AES sử dụng thuật toán mã hóa đối xứng theo khối Rijndael, sử dụng khối mã hóa 128 bit, và 192 bit hoặc 256 bit. Để đánh giá chuẩn mã hóa này, Việc nghiên cứu quốc gia về Chuẩn và Công nghệ của Mỹ, NIST (National Institute of Standards and Technology), đã thông qua thuật toán mã hóa đối xứng này.

Lưu ý: Chuẩn mã hóa này được sử dụng cho các cơ quan chính phủ Mỹ để bảo vệ các thông tin nhạy cảm.

Trong khi AES được xem như là bảo mật tốt hơn rất nhiều so với WEP 128 bit hoặc 168 bit DES (Digital Encryption standard). Để đảm bảo về mặt hiệu năng, quá trình mã hóa cần thực hiện trong các thiết bị phần cứng như tích hợp vào chip. Tuy nhiên, rất ít người sử dụng mạng không dây quan tâm tới vấn đề này. Hơn nữa, hầu hết các thiết bị cầm tay WI-FI và máy quét mã vạch đều không tương thích với chuẩn 802.11i.

7.1.5.8. Lọc (Filtering)

Lọc là cơ chế bảo mật cơ bản có thể sử dụng cùng với WEP. Lọc hoạt động giống access list trên router, cấm những cái không mong muốn và cho phép những cái mong muốn. Có 3 kiểu lọc cơ bản có thể sử dụng trong wireless lan:

Lọc SSID

Lọc địa chỉ MAC

Lọc giao thức

Lọc SSID là phương thức cơ bản của lọc và chỉ nên được sử dụng trong việc điều khiển truy cập cơ bản.

SSID của client phải khớp với SSID của AP để có thể xác thực và kết nối với tập dịch vụ. SSID được quảng bá mà không được mã hóa trong các Beacon nên rất dễ bị phát hiện bằng cách sử dụng các phần mềm. Một số sai lầm mà người sử dụng WLAN mắc phải trong quản lý SSID gồm:

Sử dụng giá trị SSID mặc định tạo điều kiện cho hacker dò tìm địa chỉ MAC của AP.

Sử dụng SSID có liên qua đến công ty.

Sử dụng SSID như là phương thức bảo mật của công ty.

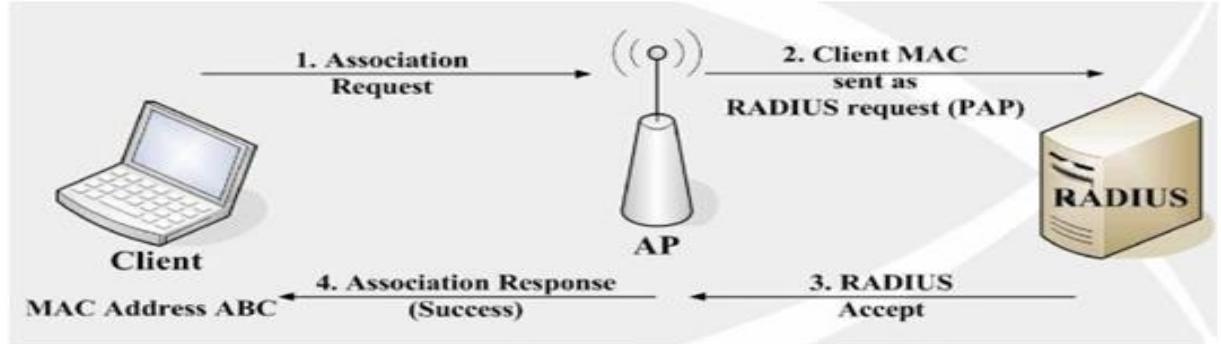
Quảng bá SSID một cách không cần thiết.

Lọc địa chỉ MAC: Hầu hết các AP đều có chức năng lọc địa chỉ MAC. Người quản trị xây dựng danh sách các địa chỉ MAC được cho phép.

Nếu client có địa chỉ MAC không nằm trong danh sách lọc địa chỉ MAC của AP thì AP sẽ ngăn chặn không cho phép client đó kết nối vào mạng.

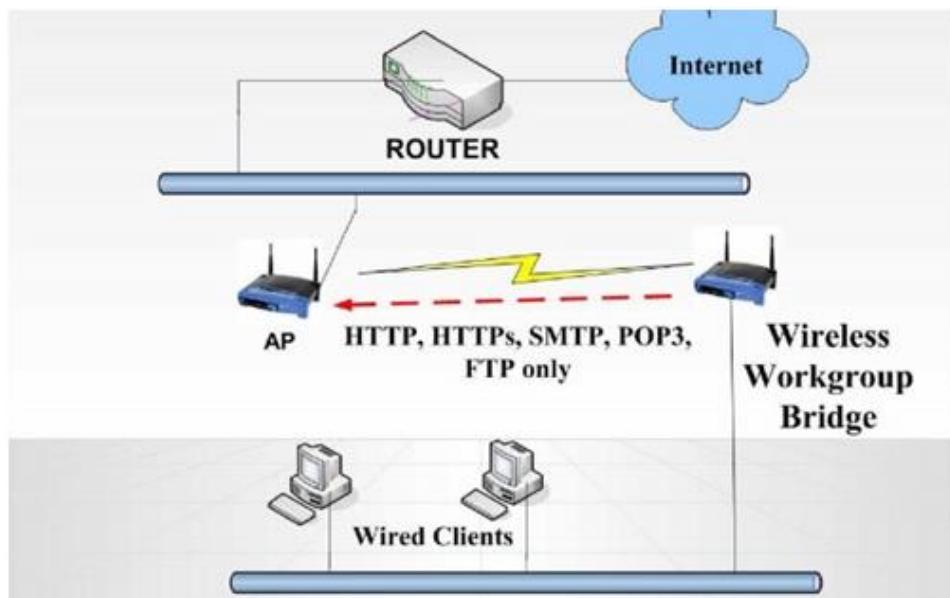
Nếu công ty có nhiều client thì có thể xây dựng máy chủ RADIUS có chức năng lọc địa chỉ MAC thay vì AP. Cấu hình lọc địa chỉ MAC là giải pháp bảo mật có tính mở rộng cao.

Lọc giao thức: Mạng Lan không dây có thể lọc các gói đi qua mạng dựa trên các giao thức từ lớp 2 đến lớp 7. Trong nhiều trường hợp người quản trị nên cài đặt lọc giao thức trong môi trường dùng chung,



Hình 7. 13 Tiến trình xác thực MAC

- Có một nhóm cầu nối không dây được đặt trên một Remote building trong một mạng WLAN của một trường đại học mà kết nối lại tới AP của tòa nhà kỹ thuật trung tâm.
- Vì tất cả những người sử dụng trong Remote builing chia sẻ băng thông 5Mbs giữa những tòa nhà này, nên một số lượng đáng kể các điều khiển trên các sử dụng này phải được thực hiện.
- Nếu các kết nối này được cài đặt với mục đích đặc biệt của sự truy nhập internet của người sử dụng, thì booj lọc giao thức sẽ loại trừ tất cả các giao thức, ngoại trừ HTTP, SMTP, HTTPS, FTP...



Hình 7.14 Lọc giao thức

Kết luận

Qua các hình thức tấn công cũng như các giải pháp bảo mật WLAN trên, người thiết kế mạng cũng như bảo mật mạng phải nắm được cụ thể các hình thức tấn công nào có thể xảy ra đối với mô hình mạng mình thiết kế. Từ đó có được các giải pháp bảo mật phù hợp với từng mô hình. Đảm bảo tính bảo mật nhưng cũng đảm bảo tính tiện dụng, không gây khó khăn cho người dùng. Sau đây là một số kiểu bảo mật áp dụng cho các mô hình mạng khác nhau.

Cho các điểm truy cập tự động (hotspots), việc mã hóa không cần thiết, chỉ cần người dùng xác thực mà thôi.

Với người dùng sử dụng mạng WLAN cho gia đình, một phương thức bảo mật với WPA passphrase hay preshared key được khuyến cáo sử dụng.

Với giải pháp doanh nghiệp, để tối ưu quá trình bảo mật với 802.1x EAP làm phương thức xác thực và TKIP hay AES làm phương thức mã hóa. Được dựa theo chuẩn WPA hay WPA2 và 802.11i security. Với các doanh nghiệp đòi hỏi bảo mật, quản lý người dùng chắc chắn và tập trung, một giải pháp tối ưu được đặt ra đó là sử dụng dịch vụ chứng thực RADIUS kết hợp với WPA2. Với dịch vụ chứng thực này, người dùng không dùng chung một “share key” mà có tên đăng nhập và mật khẩu riêng, được quản lý bởi server AAA. Cụ thể về dịch vụ xác thực sẽ được trình bày trong chương sau.

Open Access	Basic Security	Enhanced Security	Remote Access
<ul style="list-style-type: none"> - No encryption - Basic authentication - Public "hotspots" 	<ul style="list-style-type: none"> - WPA Passphase - WEP Encryption - Home use 	<ul style="list-style-type: none"> - 802.1x EAP - Mutual Authentication - TKIP Encryption - WPA/WPA2 - 802.11i Security - Enterprise 	<ul style="list-style-type: none"> - Virtual Private Network (VPN) - Business Traveler - Telecommuter

Hình 7. 15 Escalating Security

7.2. Các Chuẩn không dây

IEEE 802 là họ các chuẩn IEEE dành cho các mạng LAN và mạng MAN (metropolitan area network). Cụ thể hơn, các chuẩn IEEE 802 được giới hạn cho các mạng mang các gói tin có kích thước đa dạng. (Khác với các mạng này, dữ liệu trong các mạng cell-based được truyền theo các đơn vị nhỏ có cùng kích thước được gọi là cell. Các mạng Isochronous, nơi dữ liệu được truyền theo một dòng liên tục các octet, hoặc nhóm các octet, tại các khoảng thời gian đều đặn, cũng nằm ngoài phạm vi của chuẩn này.) Con số 802 chỉ đơn giản là con số còn trống tiếp theo mà IEEE có thể dùng, đôi khi "802" còn được liên hệ với ngày mà cuộc họp đầu tiên được tổ chức - tháng 2 năm 1980.

Các dịch vụ và giao thức được đặc tả trong IEEE 802 ánh xạ tới hai tầng thấp (tầng liên kết dữ liệu và tầng vật lý của mô hình 7 tầng OSI. Thực tế, IEEE 802 chia tầng liên kết dữ liệu OSI thành hai tầng con LLC (điều khiển liên kết lôgic) và MAC (điều khiển truy nhập môi trường truyền), do đó các tầng này có thể được liệt kê như sau:

Tầng liên kết dữ liệu

Tầng con LLC

Tầng con MAC

Tầng vật lý

Họ chuẩn IEEE 802 được bảo trì bởi Ban Tiêu chuẩn LAN/MAN IEEE 802 (IEEE 802 LAN/MAN Standards Committee (LMSC)). Các chuẩn được dùng rộng rãi nhất là dành cho họ Ethernet, Token Ring, mạng LAN không dây, các mạng LAN dùng bridge và bridge ảo (Bridging and Virtual Bridged LANs). Mỗi lĩnh vực có một Working Group tập trung nghiên cứu.

Các Working Group:

IEEE 802.1 Các giao thức LAN tầng cao

IEEE 802.2 điều khiển liên kết lôgic

IEEE 802.3 Ethernet

IEEE 802.4 Token bus (đã giải tán)

IEEE 802.5 Token Ring

IEEE 802.6 Metropolitan Area Network (đã giải tán)

IEEE 802.7 Broadband LAN using Coaxial Cable (đã giải tán)

IEEE 802.8 Fiber Optic TAG (đã giải tán)

IEEE 802.9 Integrated Services LAN (đã giải tán)

IEEE 802.10 Interoperable LAN Security (đã giải tán)

IEEE 802.11 Wireless LAN (Wi-Fi certification)

IEEE 802.12 công nghệ 100 Mbit/s plus

IEEE 802.13 (không sử dụng)

IEEE 802.14 modem cáp (đã giải tán)

IEEE 802.15 Wireless PAN

IEEE 802.15.1 (Bluetooth certification)

IEEE 802.15.4 (ZigBee certification)

IEEE 802.16 Broadband Wireless Access (WiMAX certification)

IEEE 802.16e (Mobile) Broadband Wireless Access

IEEE 802.17 Resilient packet ring

IEEE 802.18 Radio Regulatory TAG

IEEE 802.19 Coexistence TAG

IEEE 802.20 Mobile Broadband Wireless Access

IEEE 802.21 Media Independent Handoff

IEEE 802.22 Wireless Regional Area Network

Nỗ lực đầu tiên để định nghĩa một chuẩn được thực hiện vào cuối những năm 1980 bởi nhóm làm việc IEEE 802.4, chịu trách nhiệm về sự phát triển của phương pháp truy cập thông qua thẻ bus. Nhóm quyết định thẻ bài là một phương thức không hiệu quả để kiểm soát một mạng không dây và đề nghị sự phát triển của một chuẩn thay thế. Kết quả là, ban chấp hành của dự án IEEE 802 quyết định thành lập nhóm IEEE 802.11 được chịu trách nhiệm kể từ đó định nghĩa của các chuẩn phân tầng vật lý và MAC cho các mạng WLAN. Chuẩn 802.11 đầu tiên ra đời vào năm 1997 và được phát triển bằng cách xem xét khả năng nghiên cứu và các sản phẩm thị trường có sẵn, trong một khả năng để giải quyết cả hai kỹ thuật và các vấn đề thị trường. Nó cung cấp tốc độ dữ liệu lên đến 2Mbps sử dụng điều chế trai phỏ lây lan tại các băng tầnISM. Vào tháng 9 năm 1999, 2 bổ sung vào các tiêu chuẩn ban đầu được phê duyệt bởi hội đồng quản trị IEEE. Chuẩn đầu tiên 802.11b mở rộng hiệu năng của lớp vật lý 2.4 GHz đang tồn tại với tốc độ dữ liệu có thể lên đến 11Mbps. Tiếp theo là chuẩn 802.11a, cung cấp một tốc độ dữ liệu mới cao hơn từ 20 đến 54Mbps tầng vật lý trong băng tần 5MHz. 802.11b

7.2.1. IEEE 802.11b

Kỹ thuật mã hoá cho chuẩn 802.11 cung cấp tốc độ từ 1-2Mbps, thấp hơn tốc độ của chuẩn 802.3. Kỹ thuật duy nhất có khả năng cung cấp tốc độ cao hơn là DSSS(Direct sequence spread spectrum - Trải phổ chuỗi trực tiếp), được lựa chọn như là một chuẩn vật lý hỗ trợ tốc độ 1-2 Mbps và hai tốc độ mới là 5.5 và 11Mbps.

Để tăng tốc độ truyền lên cho chuẩn 802.11b, vào năm 1998, Lucent và Harris đề xuất cho IEEE một chuẩn được gọi là Complementary Code Keying(CCK). CCK sử dụng một tập 64 word các mã 8 bit, do đó 6 bit có thể được đại diện bởi bất kỳ code word nào. Vì là một tập hợp những code word này có các đặc tính toán học duy nhất cho phép chúng được nhận ra một cách chính xác với các kỹ thuật khác, ngay cả khi có sự hiện diện của nhiễu.

Với tốc độ 5.5 Mbps sử dụng CCK để mã hoá 4 bit mỗi sóng mang, và với tốc độ 11 Mbps mã hoá 8 bit mỗi sóng mang. Cả hai tốc độ đều sử dụng QPSK (Quadrature Phase-shift keying) làm kỹ thuật điều chế và tín hiệu ở 1.375 Mbps. Vì FCC điều chỉnh năng lượng đầu ra thành 1watt Effective Isotropic Radiated Power(EIRP). Do đó với những thiết bị 802.11, khi bạn di chuyển ra khỏi sóng radio, radio có thể thích nghi và sử dụng kỹ thuật mã hoá ít phức tạp hơn để gửi dữ liệu và kết quả là tốc độ chậm hơn.

Chuẩn này có tốc độ truyền thấp nhất nhưng lại được dùng phổ biến trong môi trường kinh doanh, sản xuất dịch vụ do chi phí mua linh kiện thấp, tốc độ truyền dẫn đủ đáp ứng các nhu cầu trao đổi thông tin trên internet như: duyệt web, chat, email, nhắn tin.

7.2.2. IEEE 802.11a

Không giống 802.11b, 802.11a được thiết kế để hoạt động ở băng tần 5 GHz Unlicensed National Information Infrastructure (UNII). Không giống như băng tần ISM (khoảng 83 MHz trong phổ 2.4 GHz), 802.11a sử dụng gấp 4 lần băng tần ISM vì UNII sử dụng phổ không nhiều 300MHz, 802.11a sử dụng kỹ thuật điều chế FDM (frequency-division multiplexing).

Ích lợi đầu tiên của 802.11a so với 802.11b là chuẩn hoạt động ở phổ 5.4 GHz, cho phép nó có hiệu suất tốt hơn vì có tần số cao hơn. Nhưng vì chuyển từ phổ 2.4GHz lên 5GHz nên khoảng cách truyền sẽ ngắn hơn và yêu cầu nhiều năng lượng hơn. Đó là lý do tại sao chuẩn 802.11a tăng EIRP (Effective Isotropic Radiated Power) đến tối đa của 50 mW. Phổ 5.4 GHz được chia thành 3 vùng hoạt động và mỗi vùng có giới hạn cho năng lượng tối đa.

Ích lợi thứ hai dựa trên kỹ thuật mã hoá sử dụng bởi 802.11a. 802.11a sử dụng một phương thức mã hoá được gọi là FDM (COFDM hay OFDM). Mỗi kênh phụ trong sự thực thi COFDM có độ rộng khoảng 300 kHz. COFDM hoạt động bằng cách chia nhỏ kênh truyền dữ liệu tốc độ cao thành nhiều kênh truyền phụ có tốc độ thấp hơn, và sau đó sẽ được truyền song song. Mỗi kênh truyền tốc độ cao có độ rộng là 20MHz và được chia

nhỏ thành 52 kênh phụ, mỗi cái có độ rộng khoảng 300 kHz. COFDM sử dụng 48 kênh phụ cho việc truyền dữ liệu, và 4 kênh còn lại được sử dụng cho sửa lỗi.

COFDM có tốc độ truyền cao hơn và có khả năng phục hồi lỗi tốt hơn, nhờ vào kỹ thuật mã hoá và sửa lỗi của nó. Mỗi kênh phụ có độ rộng khoảng 300 kHz. Để mã hoá 125 kbps thì BPSK được sử dụng cho tốc độ khoảng 6000 kbps. Sử dụng QPSK thì có khả năng mã hoá 16n tới 250 kbps mỗi kênh, cho tốc độ khoảng 12Mbps. Bằng cách sử dụng QAM (Quadrature Amplitude Modulation là một kỹ thuật line-code) 16 mức mã hoá 4bit/Hertz, và đạt được tốc độ 24 Mbps. Tốc độ 54 Mbps đạt được bằng cách sử dụng 64 QAM, cho phép từ 8-10 bit cho mỗi vòng, và tổng cộng lên đến 1.125 Mbps cho mỗi kênh 300 kHz. Với 48 kênh cho tốc độ 54 Mbps, tuy nhiên, tốc độ tối đa theo lý thuyết của COFDM là 108 Mbps.

Do tần số hoạt động cao nhất, băng thông lớn nên chứa được nhiều kênh thông tin hơn so với chuẩn 802.11b và 802.11g. Và cũng do tần số hoạt động cao hơn tần số hoạt động của các thiết bị viễn thông thông dụng như điện thoại mẹ bòng con, Bluetooth,...nên hệ thống mạng không dây sử dụng chuẩn 802.11a ít bị ảnh hưởng do nhiễu sóng. Nhưng đây cũng chính là nguyên nhân làm cho hệ thống dùng chuẩn này không tương thích với các hệ thống sử dụng 2 chuẩn còn lại.

Ưu điểm của 802.11a: tốc độ nhanh; tránh xuyên nhiễu bởi các thiết bị khác. Nhược điểm của 802.11a là giá thành cao; tầm phủ sóng ngắn hơn và dễ bị che khuất.

802.11g

Năm 2002 và 2003, các sản phẩm WLAN hỗ trợ chuẩn mới hơn được gọi là 802.11g nổi lên trên thị trường; chuẩn này có gắng kết hợp tốt nhất 802.11a và 802.11b. 802.11g hỗ trợ băng thông 54Mbps và sử dụng tần số 2,4GHz cho phạm vi phủ sóng lớn hơn. 802.11g tương thích ngược với 802.11b, nghĩa là các điểm truy cập (access point – AP) 802.11g sẽ làm việc với card mạng Wi-Fi chuẩn 802.11b...

7.2.3. IEEE 802.11g

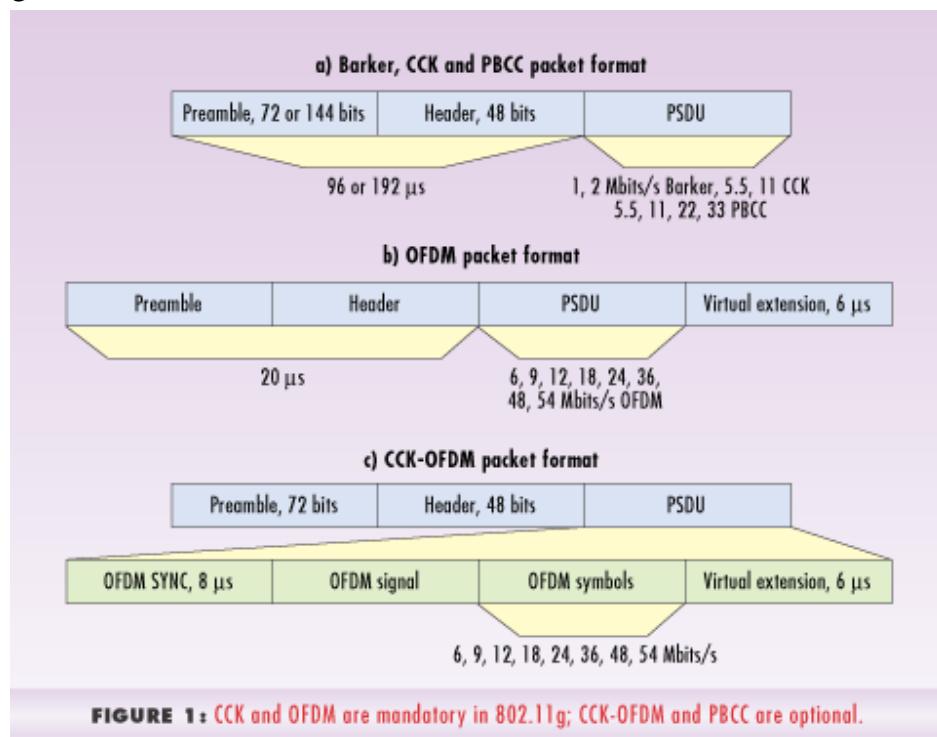
802.11g là một mở rộng của 802.11b, nó mở rộng tốc độ lên 54 Mbps bằng cách sử dụng kỹ thuật OFDM như 802.11a trong giải tần 2.4 GHz. 802.11g hoạt động ở giải tần 2.4 GHz, đó là giải băng tần S cho công nghiệp, khoa học và y học cho tín hiệu được truyền sử dụng khoảng 30 MHz (1/3 của băng tần). Chuẩn này có tốc độ truyền dẫn cao thích hợp cho hệ thống mạng có lưu lượng trao đổi dữ liệu cao. Dữ liệu luân chuyển trong hệ thống là những tập tin đồ họa, âm thanh, phim ảnh có dung lượng lớn. Chi phí trang bị cho hệ thống sử dụng kết nối không dây chuẩn 802.11g cao hơn 30% so với chuẩn 802.11b.

Vào năm 2000, nhóm phận sự G của IEEE 802.11 đưa ra nhiệm vụ phải phát triển một tốc độ cao hơn nữa, mở rộng lớp vật lý (PHY) tương thích với các phiên bản cũ. Xuất phát từ những thành công của chuẩn IEEE 802.11b, đã thúc đẩy cho ý tưởng này. Phần bổ sung mới này, đã định rõ IEEE 802.11g, tương thích được với lớp điều khiển

truy nhập môi trường truyền thông 802.11 (MAC). Thực thi tất cả những phần bắt buộc của của chuẩn IEEE 802.11b hiện tại bảo đảm tính tương thích và thao tác giữa các phần, và gồm cả tốc độ dữ liệu lớn nhất ít nhất cũng phải bằng 20 Mbps.

Gần như là chỉ một năm sau, nhóm 802.11g đã đưa ra được vài đề xuất, nhóm cho phép sự thông qua của bản phác thảo chuẩn IEEE 802.11g đầu tiên vào cuối tháng 10. Nhóm phận sự bổ sung thêm kỹ thuật tiến bộ hơn trong phiên làm việc vào đầu tháng giêng năm 2001 và hoàn thành chuẩn IEEE 802.11g vào năm 2003.

Bản phác thảo chuẩn IEEE 802.11g đã đạt tốc độ mở rộng tốc độ dữ liệu trên băng tần 2.4 GHz lên đến 54 Mbps. Tốc độ bắt buộc thấp nhất của chuẩn 802.11b là 1 và 2 Mbps đối với mã Barker (code), 5.5 đến 11 Mbps đối với điều chế khoá mã bù (CCK - Complementary Code Keying), và Long Preamble (192 microseconds) được quy định bên trong chuẩn IEEE 802.11g. Trong phần thêm vào, IEEE 802.11g cho Short Preamble (96 microseconds), đó là tùy chọn trong IEEE 802.11b, cho phép thông lượng gia tăng nhất là cho các Short Packet. Các tùy chọn 5.5 đến 11 Mbps cho mã xoắn gói nhị phân (packet binary convolutional coding (PBCC)) của IEEE 802.11b được mở rộng trong chuẩn IEEE 802.11g từ 22 đến 33 Mbps. Định dạng gói cho chế độ của Short Preamble và Long Preamble tốt như là Barker, CCK, PBCC được chỉ ra ở hình dưới đây:



Hình 7. 16 CCK và OFDM trong 802.11g; CCK – OFDM và PBCC

Đạt được tốc độ lên tới 54 Mbps, chuẩn IEEE 802.11g kế thừa từ chuẩn IEEE 802.11a. Chuẩn đó sử dụng tần số trực giao orthogonal frequency-division multiplexing (OFDM) trong dải tần 5 GHz đạt được tốc độ dữ liệu 6, 9, 12, 18, 24, 36, 48, 54 Mbps. IEEE 802.11g sử dụng định dạng mã hoá giống như trong giải tần 2.5 GHz đạt được tốc

độ giống như vậy, chế độ OFDM cho tốc độ 6, 12, và 24 Mbps. Chế độ khuôn dạng gói của OFDM được chỉ ra trong hình 7.16 b.

Chế độ tùy chọn thêm vào, CCK-OFDM trong chuẩn IEEE 802.11g sử dụng mã hoá Barker Preamble của 802.11b cùng với trường tải OFDM. CCK-OFDM phối hợp cũng được hỗ trợ tốc độ trường tải là 6, 9, 18, 14, 36, 48 và 54 Mbps. Khuôn dạng gói của CCK-OFDM được chỉ ra trong hình 7.16 c. Một trong những khía cạnh quan trọng của chuẩn IEEE 802.11g là tương thích với chuẩn IEEE 802.11b. Bằng cách duy trì tính tương thích, những nhà thiết kế bổ sung chuẩn IEEE 802.11g để nó trở nên phổ biến khắp nơi, sự thông qua chuẩn quốc tế của IEEE 802.11b trong sản xuất từ Laptops đến PDAs. Tương thích cũng ngăn ngừa sự phức tạp trên thị trường các thiết bị và cho phép giải quyết dễ dàng bởi nhà cung cấp dịch vụ và bởi những IT chuyên nghiệp. Họ lưu ý nâng cấp và hoàn thiện để việc xử lý được thực hiện nhanh hơn.

Tốc độ dữ liệu đã tăng lên đáng kể do sự mở rộng của phân lớp MAC chuẩn IEEE 802.11g. Trong khi đó chế độ 11 Mbps của IEEE 802.11b đạt được thông lượng truyền đồng đẳng trong lớp MAC vào khoảng 7.1 Mbps cho 1,500 – Byte packets, chế độ OFDM 54 Mbps sẽ cho phép thông lượng vượt quá giới hạn của 24.3 Mbps. Trong khi rất nhiều các nghiên cứu chỉ để mang lại một sự thống nhất của chuẩn WLAN trong dải băng tần 5 GHz, ví dụ như IEEE 802.11a và ETSI's HiperLAN 2, IEEE 802.11g có vẻ tỏ ra hoà hợp giữa dải băng tần 2.4 – 5 GHz. Khi lược đồ mã hoá OFDM của IEEE 802.11g và IEEE 802.11a là y hệt nhau, một thiết bị chuẩn 802.11g có nhiều quy định về mặt chức năng cho chuẩn 802.11a đã được xây dựng. Thực tế có xuất hiện nhiều cuộc tranh luận mở của nhiều nhà sản xuất kết hợp mà bao gồm cả IEEE 802.11g và IEEE 802.11a.

Ví dụ là IEEE 802.11g cũng là thiết bị kết hợp được chỉ ra như là thiết bị “IEEE 802.11abg”. Dự thảo đầu tiên của chuẩn IEEE 802.11g là “b+a=g”.

Vào năm 2001, FCC thông báo sự thành công mới đã mong đợi cho phép sự phát triển xa hơn của sự điều biến tín hiệu số trong giải băng tần 2.4 GHz đưa ra kỹ thuật trai phỏ, trong khi đó vẫn duy trì thủ tục hợp lệ cho ký tự truyền. FCC bây giờ cho phép rõ ràng sử dụng sự điều biến trong IEEE 802.11g ở dải tần 2.4 GHz.

IEEE 802.11g mode	Throughput with 1,500B packets using DCF (Mbps)
1 Barker	0.9
2 Barker	1.8
5.5 CCK or PBCC	4.5
11 CCK or PBCC	7.9
22 PBCC	12.5
24 OFDM	15.3
36 OFDM	19.8
54 OFDM	24.3

FIGURE 2: 802.11g modulation schemes and corresponding data rates.

Hình 7. 17 Lược đồ điều biến 802.11g và tương ứng với tốc độ dữ liệu

7.2.4. IEEE 802.11n

Chuẩn Wi-Fi mới nhất trong danh mục Wi-Fi là 802.11n. 802.11n được thiết kế để cải thiện tính năng của 802.11g về tổng băng thông được hỗ trợ bằng cách tận dụng nhiều tín hiệu không dây và anten (gọi là công nghệ MIMO-multiple-input and multiple-output). Khi chuẩn này hoàn thành, 802.11n sẽ hỗ trợ tốc độ lên đến 100Mbps. 802.11n cũng cho tầm phủ sóng tốt hơn các chuẩn Wi-Fi trước đó nhờ tăng cường độ tín hiệu. Các thiết bị 802.11n sẽ tương thích ngược với 802.11g.

Ưu điểm của 802.11n: tốc độ nhanh nhất, vùng phủ sóng tốt nhất; trở kháng lớn hơn để chống nhiễu từ các tác động của môi trường. Nhược điểm của 802.11n là chưa được phê chuẩn cuối cùng; giá cao hơn 802.11g; sử dụng nhiều luồng tín hiệu có thể gây nhiễu với các thiết bị 802.11b/g kế cận.

7.3. Không dây dải tần rộng

7.3.1. Giới thiệu WiMax

WiMAX (Worldwide Interoperability for Microwave Access) là viết tắt của sự tương tác mạng diện rộng bằng sóng vô tuyến. WiMAX tạo điều kiện thuận lợi cho việc trao đổi dữ liệu tốc độ cao qua mạng không dây ở các đô thị (WMANs). Với những lợi thế như triển khai nhanh, tính chuyển đổi cao, chi phí nâng cấp thấp, Wimax góp phần giải quyết vấn đề nghẽn cỏ chai. IEEE 802.16 là tiêu chuẩn, khuyến cáo hỗ trợ sự phát triển và triển khai công nghệ Wimax.

Tiêu chuẩn IEEE 802.16-2001 [1], xuất bản vào năm 2002. Định nghĩa điểm-đa điểm (PMP) kiểm tra sự truy cập mạng không dây giữa trạm gốc (BS) và các trạm thu bao (SSs). IEEE 802.16-2001 dải tầng hoạt động là 10–66 GHz, ta có thể gọi đó là tầm nhìn thẳng (LOS) viễn thông. Tiêu chuẩn 802.16-2004 được xuất bản năm 2004 mở rộng các đặc điểm kỹ thuật của WiMAX ở dải tầng số 2–11 GHz, ta có thể gọi là tầm nhìn không thẳng (NLOS) viễn thông. 802.16-2004 mô tả hồ sơ hệ thống WiMAX và sự phù hợp tiêu chuẩn đến môi trường mạng không dây tự động, giới thiệu về kiểu mắt lướt. IEEE 802.16-2004 là khả năng truyền từ node tới các node xung quanh. Tiêu chuẩn mới nhất IEEE 802.16-2005, được xuất bản tháng 12 năm 2005. Quy định về phân chia đa tầng số (SOFDM), IEEE 802.16-2005 cung cấp đầy đủ hỗ trợ hình ảnh lưu thông cho cả được phép và không được phép. Những tiêu chuẩn WiMAX đã được nêu trên là những công cụ cho sự truy cập bằng thông rộng nó như là một chiếc cầu cho dải thông không thích ứng và tới người sử dụng.

Những tiêu chuẩn của WiMAX xác định cấu trúc ở cả lớp điều khiển môi trường truy nhập (MAC) và lớp vật lý (PHY). PHY hỗ trợ các thao tác qua mạng diện rộng linh động qua một phạm vi phân bổ tần số (từ 2 đến 66 GHz), bao gồm sự thay đổi kênh trong dải thông, chia đôi tần số, và chia đôi thời gian. Lớp MAC là những quy định đặc tính chung cho sự đa dạng ở thiết bị ở lớp vật lý. Chức năng chính của MAC là sắp xếp ban

đầu, entry mạng, yêu cầu về băng thông, quản lý hướng kết nối, cũng như bảo mật trong môi trường kết nối WiMAX.

Truyền thông trong WiMAX là hướng kết nối. Tất cả dịch vụ từ lớp nghi thức lên WiMAX MAC, bao gồm những kết nối dịch vụ, là những bản đồ kết nối giữa SS và BS trong lớp MAC. Một SS có thể có nhiều kết nối đến BS với mục đích cung cấp nhiều dịch vụ đến người sử dụng. Kết nối được xác định bằng 16-bit (CIDs). Như tạo điều kiện thuận lợi dài thông cho kết nối nền và sự giúp đỡ QoS trong môi trường kết nối không dây tự động. Như vậy lớp MAC quy định về hướng kết nối dịch vụ.

Trong số ba lớp con của lớp MAC, lớp dịch vụ (CS) kết nối lớp MAC với các lớp trên. Sau đó phân loại các dịch vụ (SDUs) từ các giao thức lớp trên, lớp CS liên kết các SDUs phù hợp với định luồng (SFID) MAC và CID. Với những giao thức khác, như ATM, Ethernet, và IP, lớp CS định nghĩa các thông số phù hợp. Do đó, những phần chung của lớp con MAC (CPS) không cần hiểu định dạng của nó hay phân tích bất kỳ thông tin nào đến từ CS payload. Lớp CPS của WiMAX MAC chịu trách nhiệm về cung cấp chức năng, bao gồm truy nhập, định vị dài thông, và thiết lập kết nối WiMAX và bảo trì. Trao đổi, MAC SDUs (MSDUs) với các CSs khác.

Bảo mật ở lớp con bắt đầu từ khóa role trong chứng thực, khóa thiết lập, cũng như thông tin mã hóa. Trao đổi đơn vị dữ liệu giao thức MAC (MPDUs) với PHY trực tiếp. Vào cuối xử lý môi trường tự động không dây, WiMAX chỉ định một bộ bảo mật và cơ chế quản lý khóa. Hai thành phần ở lớp bảo mật là giao thức đóng gói và giao thức quản lý khóa riêng (PKM). Giao thức đóng gói mã hóa dữ liệu qua BWA, trong khi giao thức (PKM) đảm bảo phân phối khóa chủ và cho phép truy cập giữa SS và BS. Bảo vệ đến tốc độ truy nhập băng thông linh động, lớp bảo vệ cung cấp SS riêng và bảo vệ BS khỏi tấn công.

7.3.2. *Những vấn đề ở lớp Vật lý*

Hai tín hiệu gây nhiễu chính ở lớp PHY là jamming và scrambling. Jamming có được khi nhiễu mạnh nhiều hơn so với công suất kênh WiMAX. Các thông tin và thiết bị cần để thực hiện gây nhiễu dễ dàng có được. Khả năng phục hồi tín hiệu khi bị Jamming được tăng lên bằng cách tăng công suất tín hiệu hay làm tăng băng thông của tín hiệu thông qua các kỹ thuật truyền như nhảy tần hoặc trai phổ chuỗi trực tiếp. Trên thực tế, người ta chọn một máy phát có công suất lớn, anten phát có độ lợi cao, hoặc anten thu có độ lợi cao. Tín hiệu jamming rất dễ dò thu phát bởi thiết bị nhận. Luật cưỡng chế cũng giúp ngăn chặn thiết bị làm nhiễu. Jamming dễ dàng phát hiện và dò địa chỉ, do đó nó không gây ra một tác động đáng kể lên cả người dùng WiMAX và hệ thống.

Scrambling thường bị kích hoạt trong khoảng thời gian ngắn và mục tiêu là các frames hoặc các phần frames của WiMAX. Scrambling có thể được loại bỏ bằng bộ lọc điều khiển Scrambling hoặc gói tin quản lý với mục đích là thao tác mạng bình thường. Những khe của luồng dữ liệu nhắm đến SSs có thể chọn lọc scrambling, ép nó

phát lại. Attacker, giả làm một SS qua đó làm giảm băng thông của người bị tấn công. Tức là, khác SSs và tăng tốc độ xử lý dữ liệu của chính họ bằng cách chọn lọc Scrambling bởi những đường uplink của SSs khác. Không giống như trạng thái ngẫu nhiên của WiMAX jammer, scrambler cần thông tin điều khiển phiên dịch WiMAX đúng và để phát sinh nhiễu đúng khoảng thời gian. Tấn công từ scrambling là làm gián đoạn, và làm tăng dữ liệu dò tìm. Theo dõi sự bất thường ở xa theo định dạng là dò tìm scrambling and scramblers.

7.3.3. *Những vấn đề ở lớp MAC*

MPDU là dữ liệu được truyền trong lớp WiMAX MAC. MPDU sử dụng những mẫu khác nhau để mang những thông tin khác nhau. Mẫu chung của MPDU nằm ở MAC header, service data, và CRC (cyclic redundancy check). Không có trờ ngại chung ở cấu trúc chứa MAC header chứa thông tin mã. Mã hóa là đặt vào MAC PDU payload.

Tất cả các thông báo quản lý MAC được gửi mà không cần mã hóa để tạo điều kiện cho cài đặt, sắp xếp, và thao tác MAC. Các gói tin quản lý mang theo MPDU như hình 2. WiMAX sẽ không mã hóa MAC headers và gói tin quản lý MAC, nhằm mục đích là thao tác với những hệ thống khác nhau ở lớp MAC. Bởi vậy, hacker có thể nghe lén kênh WiMAX, và khôi phục lại các thông tin từ những gói tin quản lý MAC không được mã hóa. Nghe trộm những gói tin không được quản lý này giúp tin tặc biết được topo mạng, tấn công SSs cũng như hệ thống WiMAX. WiMAX cần sự chứng thực cao hơn. Ý tưởng là sử dụng thiết bị RSA (Rivest-Shamir-Adleman)/X.509 chứng nhận số. Chứng nhận số được sử dụng cho xác thực và dò tìm quản lý. Thiết bị không nhận thực khóa nghe trộm từ mạng.

Đánh cắp căn cước đe dọa đến những dịch vụ của WiMAX. Thiết bị giả có thể sử dụng địa chỉ phần cứng giả để đăng ký thiết bị bằng cách chia những gói tin quản lý ra ngoài. Một lần thành công hacker có thể giả làm BS, làm cho SSs liên hệ đến BS giả cuối cùng các dịch vụ được cung cấp bởi BS giả, kết quả chất lượng dịch vụ bị giảm sút hay không thể đáp ứng được dịch vụ.

WiMAX sử dụng đa truy cập phân chia theo thời gian (TDMA). Để trộm căn cước attacker phải truyền trong khi BS thật là phát. Tín hiệu của attacker phải nhầm đến đúng SSs và phải mạnh hơn tín hiệu BS thật trong giải nền. Từ đó dữ liệu truyền được chia ra những time slots, attacker đóng vai trò là một phiên dịch time slots được cấp đến hợp pháp hóa BS một cách thành công, và dò tín hiệu BS chính xác. Xác thực lẫn nhau làm giảm khả năng ăn trộm căn cước.

7.4. Mạng Manet

Lịch sử phát triển của mạng MANET

- Mobile Ad-hoc Network – MANET trước đây còn được gọi là mạng vô tuyến gói, và được

tài trợ, phát triển bởi DARPA trong đầu thập niên 1970

- Sau đó một mạng mới: SUSAN (Adaptive Survivable Network) đã được đề xuất bởi DARPA vào năm 1983 để hỗ trợ một mạng quy mô lớn hơn, mạnh mẽ hơn. Thời gian này, Ad-hoc đã được sử dụng để mô tả 1 loại mạng như tiêu chuẩn IEEE802.11
- Mobile Ad-hoc Network đã được định nghĩa bởi IETF

Các đặc điểm chính của mạng MANET.

- Thiết bị tự trị đầu cuối (Autonomous terminal): Trong Manet, mỗi thiết bị di động đầu cuối là một nút tự trị.
- Phân chia hoạt động (Distributed operation): Vì không có hệ thống mạng nền tảng cho trung tâm kiểm soát hoạt động của mạng nên việc kiểm soát và quản lý hoạt động của mạng được chia cho các thiết bị đầu cuối. Các nút trong MANET đòi hỏi phải có sự phối hợp với nhau. Khi cần thiết các nút hoạt động như một relay để thực hiện chức năng của mình.
- Định tuyến đa đường: Thuật toán định tuyến không dây cơ bản có thể định tuyến một chặng và nhiều chặng dựa vào các thuộc tính liên kết khác nhau và giao thức định tuyến
 - Cấu hình động (dynamic network topology): Vì các nút là di động, nên cấu trúc mạng có thể thay đổi nhanh và không thể biết trước, các kết nối giữa các thiết bị đầu cuối có thể thay đổi theo thời gian
 - Dao động về dung lượng liên kết (Fluctuating link capacity): Bản chất tỉ lệ bit lỗi cao của kết nối không dây cần quan tâm trong mạng MANET. Từ đầu cuối này đến đầu cuối kia có thể được chia sẻ qua một vài chặng. Kênh giao tiếp ở đầu cuối chịu ảnh hưởng của nhiễu, hiệu ứng đa đường, sự giao thoa và băng thông của nó ít hơn so với mạng có dây.
 - Tối ưu hóa cho thiết bị đầu cuối (light-weight terminals): Trong hầu hết các trường hợp các nút trong mạng MANET là thiết bị với tốc độ xử lý của CPU thấp, bộ nhớ ít và lưu trữ điện năng ít. Vì vậy cần phải tối ưu hóa các thuật toán và cơ chế

Khái niệm cơ bản về mạng MANET

- Khái niệm: MANET (mobile ad-hoc network) là một tập hợp của những nút mạng không dây, những nút này có thể được thiết lập tại bất kỳ thời điểm và tại bất cứ nơi nào. Mạng MANET không dùng bất kỳ cơ sở hạ tầng nào. Nó là một hệ thống tự trị mà máy chủ di động được kết nối bằng đường vô tuyến và có thể di chuyển tự do, thường hoạt động như một router.

Ứng dụng điển hình của mạng MANET trong các lĩnh vực.

- Quân sự: Hoạt động phi tập trung của mạng MANET và không phụ thuộc

vào cơ sở hạ tầng mạng là một yếu tố thiết yếu đối với lĩnh vực quân sự, nhất là trong các trường hợp chiến đấu khốc liệt, các cơ sở hạ tầng mạng bị phá hủy. Lúc này mạng MANET là lựa chọn số một để các thiết bị truyền thông liên lạc với nhau một cách nhanh chóng.

- Trường học: thiết lập các mạng MANET trong trường học, lớp học, thư viện, sân trường,... để kết nối các thiết bị di động (laptop, smartphone) lại với nhau, giúp sinh viên, thầy cô giáo có thể trao đổi bài một cách nhanh chóng thông qua mạng ad-hoc vừa tạo.
- Gia đình: tạo nhanh mạng MANET để kết nối các thiết bị di động của bạn với nhau, có thể di chuyển tự do mà vẫn đảm bảo kết nối truyền tải dữ liệu.
- Kết nối các thiết bị điện tử với nhau: Trong những năm tới khi mà các thiết bị điện tử đều được gắn các giao tiếp không dây, giúp chúng có thể trao đổi giao tiếp với nhau thì mạng MANET sẽ rất phù hợp để tạo nên một hệ thống thông minh có khả năng liên kết với nhau.

7.5. Hệ thống GMS

- Hệ thống thông tin di động toàn cầu ([tiếng Anh](#): Global System for Mobile Communications) là một công nghệ dùng cho [mạng thông tin di động](#). Dịch vụ GSM được sử dụng bởi hơn 2 tỷ người trên 212 quốc gia và vùng lãnh thổ. Các mạng thông tin di động GSM cho phép có thể [roaming](#) với nhau do đó những máy điện thoại di động GSM của các mạng GSM khác nhau ở có thể sử dụng được nhiều nơi trên thế giới. GSM là chuẩn phổ biến nhất cho [điện thoại di động](#) (ĐTDĐ) trên thế giới
- Trình bày giao diện vô tuyến của hệ thống GSM.
- GSM là mạng điện thoại di động thiết kế gồm nhiều tế bào do đó các máy điện thoại di động kết nối với mạng bằng cách tìm kiếm các cell gần nó nhất
- Các mạng di động GSM hoạt động trên 4 băng tần. Hầu hết thì hoạt động ở băng 900 MHz và 1800 MHz. Vài nước ở [Châu Mỹ](#) thì sử dụng băng 850 MHz và 1900 MHz do băng 900 MHz và 1800 MHz ở nơi này đã bị sử dụng trước.
- Các mạng sử dụng băng tần 900 MHz thì đường lên (từ thuê bao di động đến trạm truyền dẫn uplink) sử dụng tần số trong dải 890–915 MHz và đường xuống downlink sử dụng tần số trong dải 935–960 MHz. Và chia các băng tần này thành 124 kênh với độ rộng băng thông 25 MHz, mỗi kênh cách nhau 1 khoảng 200 kHz. Khoảng cách song công (đường lên & xuống cho 1 thuê bao) là 45 MHz

- Ở một số nước, băng tần chuẩn GSM900 được mở rộng thành E-GSM, nhằm đạt được dài tần rộng hơn. E-GSM dùng 880–915 MHz cho đường lên và 925–960 MHz cho đường xuống. Như vậy, đã thêm được 50 kênh (đánh số 975 đến 1023 và 0) so với băng GSM-900 ban đầu

Công nghệ 3G

- Nêu những đặc điểm chính và kể tên các tiêu chuẩn công nghệ của hệ thống thông tin di động thế hệ thứ 3 (3G).
- Nêu những đặc điểm chính của hệ thống thông tin di động thế hệ thứ 3 (3G).
- Tính linh hoạt: cung cấp hệ thống có tính linh hoạt cao, có khả năng hỗ trợ hàng loạt các dịch vụ và ứng dụng cao cấp. IMT-2000 hợp nhất 5 kỹ thuật (IMT-DS, IMT-MC, TMT-TC, IMT-SC, IMT-FT) về giao tiếp sóng dựa trên ba công nghệ truy cập khác nhau (FDMA - Đa truy nhập phân chia theo tần số, TDMA - Đa truy nhập phân chia theo thời gian và CDMA - Đa truy nhập phân chia theo mã).
- Tính kinh tế: Sự hợp nhất giữa các ngành công nghiệp 3G là bước quan trọng quyết định gia tăng số lượng người dùng và các nhà khai thác.
- Tính tương thích: Các dịch vụ trên IMT-2000 có khả năng tương thích với các hệ thống hiện có.
- Thiết kế theo modul: Chiến lược của IMT-2000 là phải có khả năng mở rộng dễ dàng để phát triển số lượng người dùng, vùng phủ sóng, dịch vụ mới với khoản đầu tư ban đầu thấp nhất.
- Phân loại các dịch vụ của IMT-2000

<ul style="list-style-type: none"> - 	<ul style="list-style-type: none"> - Phân loại 	<ul style="list-style-type: none"> - Dịch vụ chi tiết
<ul style="list-style-type: none"> - 	<ul style="list-style-type: none"> - Dịch vụ di động 	<ul style="list-style-type: none"> - Di động đầu cuối/di động cá nhân/di động dịch vụ

	<ul style="list-style-type: none"> - Dịch vụ thông tin định vị 	<ul style="list-style-type: none"> - Theo dõi di động/theo dõi di động thông minh
-	<ul style="list-style-type: none"> - Dịch vụ âm thanh 	<ul style="list-style-type: none"> - Dịch vụ âm thanh chất lượng cao(16 – 64 kbit/s) - Dịch vụ âm thanh AM (32 –64 kbit/s) - Dịch vụ truyền thanh FM (64 – 384kbit/s)
	<ul style="list-style-type: none"> - Dịch vụ số liệu 	<ul style="list-style-type: none"> - Dịch vụ số liệu tốc độ trung bình (64 – 144 kbit/s) - Dịch vụ số liệu tốc độ tương đối cao (144 – 2 Mbit/s) - Dịch vụ số liệu tốc độ cao (\geq 2Mbit/s)
	<ul style="list-style-type: none"> - Dịch vụ đa phương tiện 	<ul style="list-style-type: none"> - Dịch vụ Video (384kbit/s) - Dịch vụ hình chuyển động (384kbit/s - 2Mbit/s) - Dịch vụ hình chuyển động thời gian thực (\geq 2Mbit/s)
-	<ul style="list-style-type: none"> - Dịch vụ Internet đơn gian 	<ul style="list-style-type: none"> - Dịch vụ truy nhập Web (384kbit/s - 2Mbit/s)
	<ul style="list-style-type: none"> - Dịch vụ Internet thời gian thực 	<ul style="list-style-type: none"> - Dịch vụ Internet (384kbit/s - 2Mbit/s)

	<ul style="list-style-type: none"> - Dịch vụ internet - đa phương tiện 	<ul style="list-style-type: none"> - - Dịch vụ Website đa phương tiện thời gian thực ($\geq 2\text{Mbit/s}$)
--	--	--

Các tiêu chuẩn công nghệ của hệ thống thông tin di động thế hệ thứ 3 (3G).

- IMT-2000 CDMA Direct Spread (trải phổ trực tiếp), thường được biết dưới tên WCDMA.
- IMT-2000 CDMA Multi-Carrier (nhiều sóng mang), đây là phiên bản 3G của hệ thống IS-95 (hiện nay gọi là CDMA One)
- IMT-2000 CDMA TDD: hệ thống CDMA sử dụng phương pháp song công phân chia theo thời gian (Time-division duplex)
- IMT-2000 TDMA Single-Carrier (một sóng mang), các hệ thống thuộc nhóm này được phát triển từ các hệ thống GSM hiện có lên GSM 2+ (được gọi là EDGE).
- IMT-2000 FDMA/TDMA (thời gian tần số), đây là hệ thống các thiết bị kéo dài thuê bao số ở châu Âu.
- IMT-2000 OFDMA TDD WMAN (thường được biết dưới tên WiMAX di động).

7.6. Công nghệ 4G

Nêu những yêu cầu về cấu trúc của hệ thống thông tin di động thế hệ thứ 4 (4G). Giải thích thuật ngữ MIMO được sử dụng trong các mạng 4G.

Nêu những yêu cầu về cấu trúc của hệ thống thông tin di động thế hệ thứ 4 (4G).

- Mạng 4G phải đáp ứng được yêu cầu tích hợp được các mạng khác như các mạng di động thế hệ 2, thế hệ 3, thế hệ 3,5G,... và WLAN, WiMAX, và các mạng không dây khác.
- Mạng có tính mở: Cấu trúc mở của mạng 4G cho phép cài đặt các thành phần mới với các giao diện mới giữa các cấu trúc khác nhau trên các lớp
- Đảm bảo chất lượng dịch vụ cho các ứng dụng đa phương tiện trên nền IP: Để đảm bảo chất lượng dịch vụ, cần sự kết hợp chặt chẽ giữa các lớp truy nhập, truyền tải và các dịch vụ Internet. Đặc biệt đối với các vấn đề về độ trễ

mạng, băng thông dịch vụ...vv

- Đảm bảo tính an toàn, bảo mật thông tin: Tính an toàn của hệ thống được đánh giá qua khả năng bảo mật trong truyền thông, tính đúng đắn và riêng tư của các dữ liệu người sử dụng cũng như khả năng quản lý, giám sát hệ thống
- Mạng đảm bảo tính di động: Một trong những vấn đề quan trọng của 4G đó là cách để truy nhập nhiều mạng di động và không dây khác nhau.
- Mạng phải đảm bảo về tốc độ: Mạng mới ra đời phải có tốc độ truyền dữ liệu cao, đáp ứng được yêu cầu của người sử dụng. Tốc độ truyền dữ liệu trong mạng mới có thể lên đến 100Mbps và 160Mbps khi sử dụng MIMO (Nhiều đầu vào – Nhiều đầu ra)

Giải thích thuật ngữ MIMO được sử dụng trong các mạng 4G.

MIMO: Multi Input Multi Output, nghĩa là nhiều đầu vào và nhiều đầu ra.

Trong các mạng 4G hiện nay người ta sử dụng thuật ngữ này để chỉ các hệ thống sử dụng nhiều anten phía đầu phát và nhiều anten phía đầu thu để tạo ra độ lợi phân tách, nâng cao tốc độ và chất lượng tín hiệu truyền.

7.7. Mobile IP

IP di động (Mobile IP) là một chuẩn do nhóm chuyên trách kỹ thuật Internet (Internet Engineering Task Force - IETF) đề xuất và được trình bày cụ thể trong tài liệu RFC 3344 và RFC 5944 (RFC 5944 mới được công bố vào tháng 11/2010). IP di động được xây dựng nhằm mục đích cho phép người dùng với thiết bị di động của mình có thể di chuyển từ mạng này sang mạng khác mà vẫn tiếp tục duy trì các dòng thông tin đang diễn ra. Cùng với sự phát triển của công nghệ mạng 4G, Mobile IP vẫn đang được nghiên cứu và cải tiến nhằm đảm bảo tính di động của thiết bị trong thế hệ mạng tương lai. Nội dung bài này sẽ giúp các bạn nắm bắt được nguyên lý hoạt động và một số vấn đề cơ bản của mobile IP.

Trong thiết kế của giao thức IP, mỗi thiết bị khi nối kết vào mạng sẽ được gắn kết với một địa chỉ IP nhất định. Đây được xem như điểm nối vật lý của thiết bị với mạng internet. Khi trao đổi dữ liệu trên mạng các thiết bị được giả định là không thay đổi địa chỉ IP. Nếu một nút liên lạc CN (Correspondent Node) gửi gói tin đến nút di động MN (*Mobile Node*) thì trước tiên gói tin sẽ được định tuyến đến mạng thường trú HN (*Home Network*) của MN mà không phụ thuộc vào vị trí hiện tại của MN. Sau đó, IP di động đảm nhiệm việc chuyển tiếp gói tin này đến cho MN để duy trì dòng thông tin không bị gián đoạn giữa hai thiết bị.

Để hiểu rõ về nguyên lý hoạt động của IP Mobile, chúng ta cần phải làm quen với một số thuật ngữ chính:

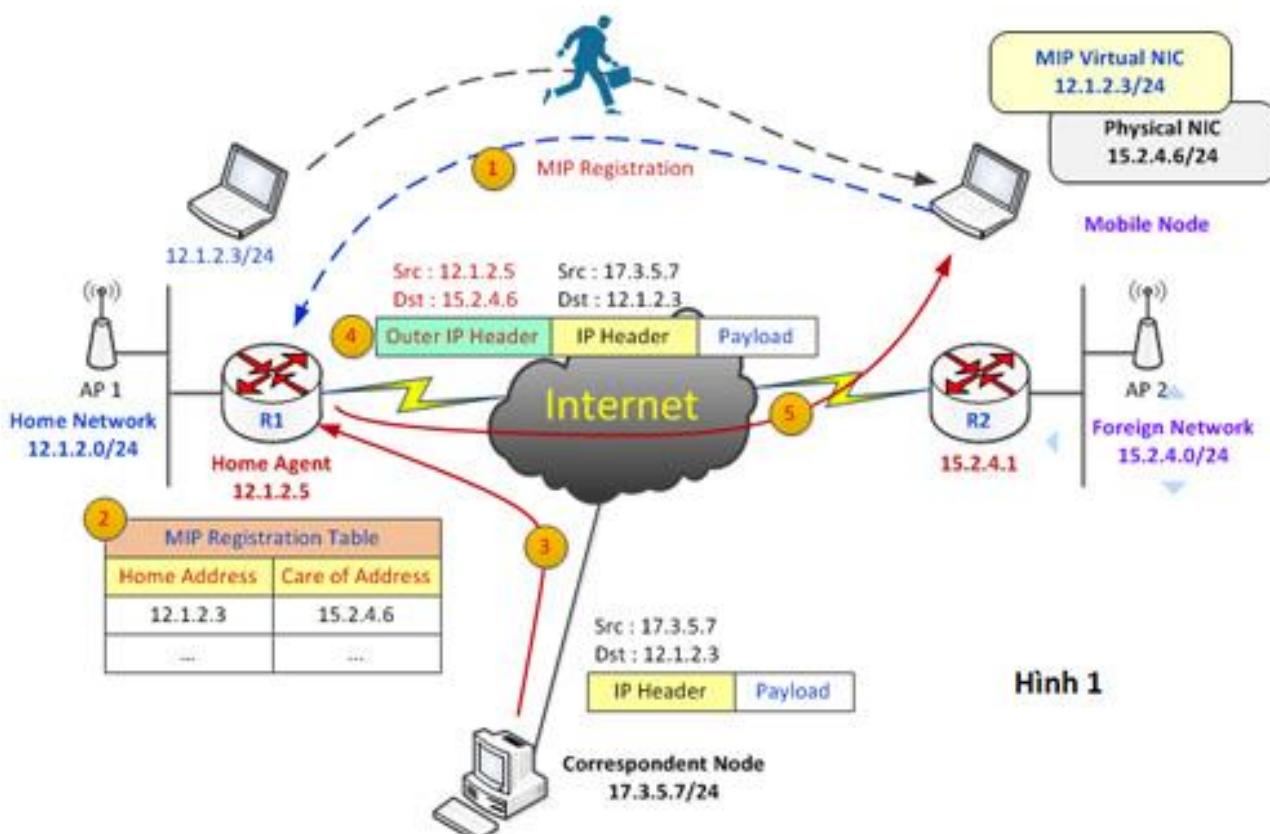
- Nút di động MN: là thiết bị có cài đặt phần mềm Mobile IP client. MN luôn được gán với một IP cố định gọi là địa chỉ thường trú HA (Home Address). Trong hình minh họa số 1 bên dưới thì địa chỉ thường trú của MN sẽ là 12.1.2.3/24. Khi MN đang trong mạng thường trú, quá trình liên lạc diễn ra bình thường, nút di động tiến hành gửi và nhận các gói tin như một thiết bị thông thường.

- Nếu MN di chuyển ra khỏi mạng thường trú, thì MN cần có một đại diện thường trú HA (Home Agent) thay mặt cho thiết bị. Vai trò của HA là nhận thông tin gửi đến MN và tiếp tục chuyển tiếp đến địa chỉ mới của MN.

- Khi MN chuyển từ mạng thường trú đến mạng tạm trú FN (Foreign Network), nó sẽ được cung cấp một địa chỉ tạm trú gọi là CoA (Care of Address). MN có nhiệm vụ đăng ký với HA địa chỉ CoA mới này. MN có thể nhận địa chỉ này từ máy chủ DHCP hoặc sử dụng IP của đại diện tạm trú FA (Foreign Agent).

Chắc hẳn các bạn sẽ thắc mắc làm thế nào để MN xác định nó đã di chuyển khỏi mạng thường trú hay chưa cũng như tìm kiếm FA mới ở mạng tạm trú. Vấn đề này sẽ được HA và FA giải quyết bằng cách định kỳ gửi thông điệp quảng bá trên các mạng cục bộ của chúng, MN tiếp nhận các gói tin này và xác định được những thông tin cần thiết. Quá trình này được biết đến với tên là Agent Discovery.

Vậy thì cách thức mà Mobile IP thực hiện để duy trì được dòng dữ liệu liên tục khi thiết bị di chuyển đến mạng khác với địa chỉ IP mới như thế nào. Để trả lời câu hỏi này, chúng ta phải xem cách thức gửi gói tin đến MN khi chúng ở mạng tạm trú trong hình minh họa số 1 bên dưới:

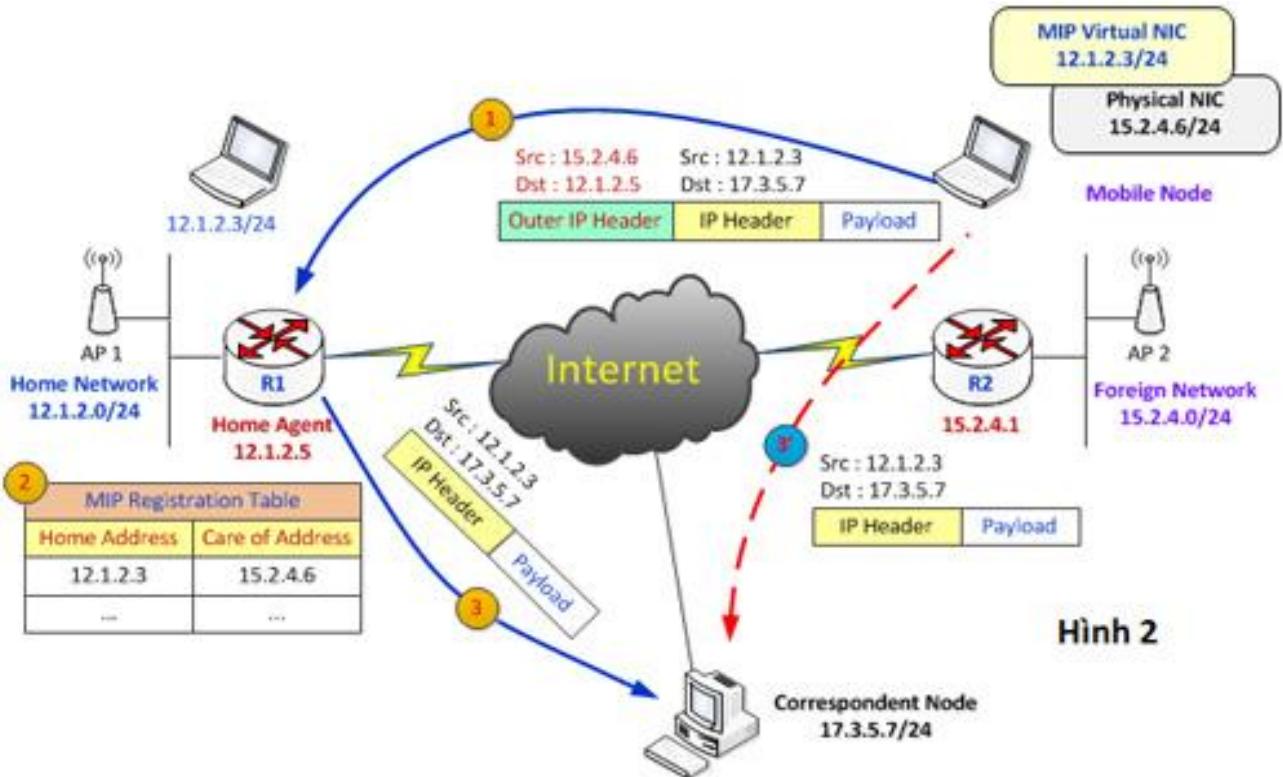


Hình 1

Phân tích:

1. Trong minh họa số 1 này, router R1 đóng vai trò như một HA cho nút di động. Khi MN di chuyển sang mạng tạm trú, nó sẽ thực hiện việc đăng ký địa chỉ CoA bằng cách gửi gói tin “MIP registration” đến cho đại diện thường trú HA.
 2. HA sử dụng địa chỉ CoA nhận được ở bước 1 để tiến hành cập nhật bảng đăng ký (MIP Registration Table). Bảng đăng ký này lưu trữ ánh xạ giữa địa chỉ thường trú, tạm trú và một số thông tin liên quan như thời hạn đăng ký.
 3. Khi gói tin được gửi từ CN đến địa chỉ thường trú của MN, đại diện thường trú HA sẽ đứng ra làm trung gian tiếp nhận gói tin này sau đó chuyển hướng chúng đến vị trí hiện tại của MN.
 4. HA dùng phương pháp "đóng gói" gói để chuyển thông tin cho MN bằng cách dùng thêm phần mào đầu IP bên ngoài (Outer IP header) vào gói tin gốc và chuyển theo đường hầm (IP-in-IP tunelling) đến địa chỉ CoA mà MN đã đăng ký. Trong ví dụ minh họa đường hầm được hình thành giữa HA và MN.
 5. Card mạng vật lý (Physical NIC) thực hiện tháo bỏ IP header ngoài để khôi phục gói tin gốc và chuyển giao cho card mạng ảo (Virtual NIC). Các ứng dụng đang thực thi trên MN vốn chỉ gắn kết với địa chỉ thường trú trên card mạng ảo, do vậy việc thay đổi của CoA của thiết bị sẽ không làm gián đoạn luồng thông tin giữa hai thiết bị.
- Quá trình tiếp diễn cho đến khi hết thời hạn đã đăng ký (hoặc MN chuyển đến vị trí mới). Khi điều này xảy ra, MN sẽ tiến hành đăng ký lại với HA. Khi MN trở về mạng thường trú, nó không cần di động nữa, vì thế MN sẽ gửi một yêu cầu hủy bỏ đăng ký lưu động đến HA, nói rõ rằng nó đang "ở nhà" để HA không thực hiện đường hầm và dọn bỏ các địa chỉ tạm trú trong bảng đăng ký trước đó.
- Như vậy, chúng ta vừa tìm hiểu nguyên lý hoạt động cơ bản của Mobile IP. Nếu để ý, chúng ta sẽ thấy rằng giao thức này có một nhược điểm là thời gian trễ (delay) lớn (do gói tin phải chuyển qua HA trước rồi mới đến MN) vì thế nó sẽ ảnh hưởng đến các ứng dụng thời gian thực (real-time application). Chính vì vậy, đã có nhiều cải tiến được đưa vào Mobile IP để tăng tính hiệu quả và giảm delay.
- Phản tiếp theo chúng ta sẽ tìm hiểu một số vấn đề liên quan đến Mobile IP.

7.7.1. Định tuyến tam giác TR (Triangular Routing):

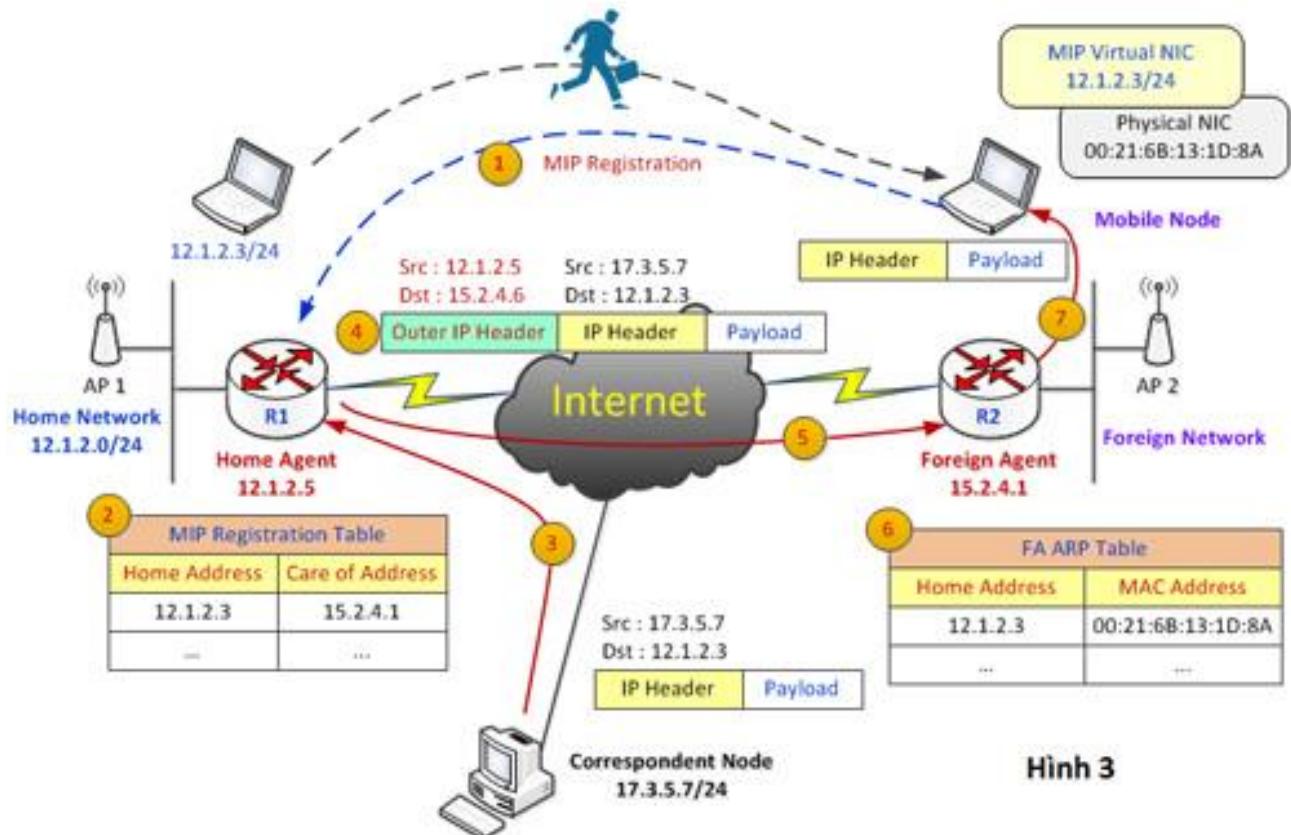


MN sau khi nhận được gói tin gốc sẽ biết được chính xác địa chỉ IP của CN. Vì thế, MN có thể gửi các gói tin trực tiếp đến CN hoặc thông qua đường hầm đến HA nhờ chuyển giúp. Việc gửi trực tiếp gói tin đến CN sẽ là giải pháp tối ưu giúp giảm thiểu delay khi gửi/nhận thông tin giữa MN và CN. Quá trình này được gọi là định tuyến tam giác. Tuy nhiên, thực tế một số router và firewall thường được cấu hình với chức năng "ingress filtering" nhằm mục đích ngăn chặn các cuộc tấn công giả mạo địa chỉ. Chức năng này sẽ chặn các gói tin có địa chỉ IP nguồn không thuộc subnet mạng cục bộ. Trong hình minh họa số 2 thì gói tin gửi từ MN đến CN sẽ có IP source là 12.1.2.3, không thuộc về subnet 15.2.4.0/24, do đó nó sẽ bị loại bỏ. Để giải quyết vấn đề này IP di động đưa ra giải pháp đường hầm nghịch (Reverse Tunneling). Theo đó MN sẽ chuyển gói tin thông qua đường hầm đến HA trước khi HA chuyển tiếp chúng cho CN (xem các bước 1, 2, 3 trong hình minh họa số 2).

Để cải thiện hiệu quả định tuyến, người ta đưa ra giải pháp cho phép MN sau khi xác định được địa chỉ IP của CN thì MN sẽ gửi trực tiếp thông tin CoA hiện hành đến CN. CN sẽ duy trì ánh xạ liên kết giữa địa chỉ thường trú và CoA của MN (tương tự như HA) trong một khoảng thời gian nhất định. Nếu ánh xạ này vẫn còn hợp lệ thì CN và MN sẽ trao đổi dữ liệu trực tiếp với nhau mà không cần qua HA. Nếu ánh xạ không tồn tại hoặc bị expired thì CN sẽ tiến hành gửi các gói tin đến HA, rồi từ HA sẽ chuyển đến MN như bình thường, sau đó MN có thể gửi lại CoA cho CN.

7.7.2. Đại diện tạm trú FA (Foreign Agents)

Việc sử dụng địa chỉ IP thật (Public IP) để đăng ký như minh họa trên sẽ dẫn buộc các mạng tạm trú dành trước một số IP thật cho các thiết bị di động. Nếu số lượng các MN di chuyển đến mạng tạm trú quá nhiều sẽ dẫn đến tình trạng không còn đủ IP để cung cấp cho MN mới. Để giải quyết vấn đề này IP di động đã bổ sung thêm khái niệm đại diện tạm trú FA (Foreign Agents). Khi có sự hiện diện của FA thì các MN sẽ dùng chung IP của FA để làm CoA của mình. Trong hình minh họa số 3 bên dưới CoA của MN sẽ là IP của router R2 15.2.4.1/24.



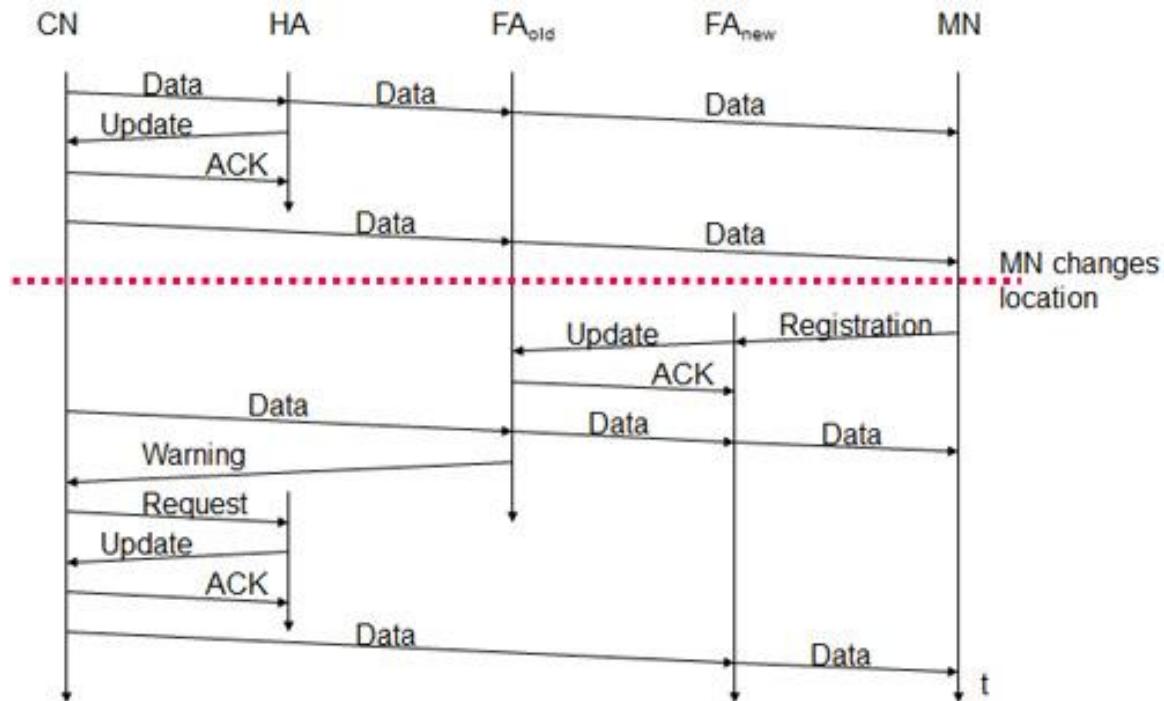
Hình 3

Các bước thực hiện từ 1 đến 4 tương tự như hình minh họa số 1. Tuy nhiên, đường hầm được hình thành giữa HA và FA chứ không phải là giữa HA và MN. Tại FA, gói tin gốc sẽ được khôi phục bằng cách tháo bỏ IP header bên ngoài. Sau đó, FA căn cứ vào thông tin địa chỉ MAC có bảng ARP của nó để gửi thông tin đến vị trí hiện hữu của MN một cách chính xác.

7.7.3. NAT và IP di động, Forwarding

Khi MN ở sau một thiết bị NAT thì đường hầm IP-in-IP giữa HA và MN sẽ không thể thực hiện được, bởi vì địa chỉ CoA không thể truy cập một cách trực tiếp từ mạng ngoài. Để giải quyết vấn đề này, IP di động thực hiện đóng gói “IP packet” trong “UDP segment” và sử dụng đường hầm IP-in-UDP để gửi thông tin (xem chi tiết về IP-in-UDP tunneling trong RFC 3519).

Nếu MN di chuyển từ mạng tạm trú này sang một mạng tạm trú khác, tức sẽ chuyển từ FA cũ (FAold) sang một FA mới (FAnew) thì trong quá trình chuyển từ FAold sang FANew, thông tin gói sẽ vẫn tiếp tục được chuyển đến FAold. Và để giảm số packet bị mất do vấn đề này thì người ta đã cải tiến tính năng forwarding để cho phép FAold sẽ chuyển tiếp thông tin nó nhận được đến FAnew.



Kết luận

Trên đây chúng ta đã tìm hiểu cơ bản về Mobile IP giao thức quản lý di động hoạt động ở lớp mạng (Network layer). Mobile IP được thiết kế bởi IETF nhằm giải quyết bài toán Internet di động. Từ sau sự ra đời của MIPv4 (Mobile IP version 4) đã có rất nhiều nghiên cứu cải tiến nhằm giảm thời gian từ lúc MN di chuyển đến lúc HA nhận được thông tin CoA của MN. Và hiện nay, MIPv6 (Mobile IP version 6) cũng đang được tiếp tục nghiên cứu và hoàn thiện.

TÓM TẮT NỘI DUNG CỐT LÕI.

- Mạng cục bộ không dây
- Các chuẩn mạng không dây
- Không dây dài tầm rộng
- Những vấn đề lớp vật lý
- Những vấn đề ở lớp MAC

BÀI TẬP ÚNG DỤNG, LIÊN HỆ THỰC TẾ:

1. Các LAN không dây mà chúng ta đã nghiên cứu sử dụng những giao thức, chẳng hạn như MACA thay vì sử dụng CSMA/CD. Trong những tình huống nào nếu có thể sử dụng CSMA/CD thay vì đó hay không?
2. Các giao thức truy cập kênh WDMA và GSM có chung những đặc tính gì?
3. Sáu trạm từ A đến F giao tiếp bằng giao thức MACA. 2 cuộc truyền có thể xảy ra cùng 1 lúc không? Giải thích?
4. Tám trạm từ A đến F giao tiếp bằng giao thức MACA. 2 cuộc truyền có thể xảy ra cùng 1 lúc không? Giải thích?
5. Một văn phòng tòa nhà 6 lầu có 15 văn phòng kề nhau trên mỗi lầu. Mỗi phòng chứa một ổ cắm tường cho một thiết bị đầu cuối trong tường phía trước, do ổ cắm hình thành một lối hỉnh chữ nhật trong mặt phẳng thẳng đứng với sự tách biệt 4mm giữa các ổ cắm theo cả chiều ngang và chiều dọc. Giả sử có thể chạy một cáp thẳng giữa bất kỳ cặp ổ cắm theo chiều ngang, chiều dọc hoặc theo đường chéo, cần đến bao nhiêu mét cáp để nối tất cả ổ cắm bằng cách sử dụng:

- 1 cấu hình sao với 1 router ở giữa
- 1 LAN 802.3
6. Trình bày các mô hình mạng WLAN cơ bản.
7. So sánh các chuẩn không dây họ IEEE 802
8. Trình bày một số vấn đề trong mạng không dây dài tầm rộng.

TÀI LIỆU THAM KHẢO

1. Hồ Đắc Phương (2014), Giáo trình Mạng máy tính, Nxb Giáo dục, Hà Nội.
2. TS. Phạm Thế Quê, *Giáo trình Mạng máy tính*, NXB Thông tin - Truyền thông, 2008.
3. Computer Networks, Fifth Edition, By Andrew, S. Tanenbaum Prentice Hall, March 17, 2007.
4. Computer Networking Top-and-Down Aproad, Sixth edition, James F. Kurose, Keith W. Ross, PEARSON, 2012