



BỘ GIÁO DỤC VÀ ĐÀO TẠO  
TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT THÀNH PHỐ HỒ CHÍ MINH  
**60** NĂM XÂY DỰNG VÀ PHÁT TRIỂN

HUỲNH NGUYỄN CHÍNH (Chủ biên)  
NGUYỄN THỊ THANH VÂN

GIÁO TRÌNH

# MẠNG MÁY TÍNH CĂN BẢN

(Giáo trình dùng cho sinh viên ngành Công nghệ thông tin)



NHÀ XUẤT BẢN  
ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH

HUỲNH NGUYÊN CHÍNH (CHỦ BIÊN)

NGUYỄN THỊ THANH VÂN

GIÁO TRÌNH

# MẠNG MÁY TÍNH CĂN BẢN

(Giáo trình dùng cho sinh viên ngành Công nghệ thông tin)

NHÀ XUẤT BẢN ĐẠI HỌC QUỐC GIA  
THÀNH PHỐ HỒ CHÍ MINH - 2022



## LỜI NÓI ĐẦU

**Giáo trình Mạng máy tính căn bản** là tài liệu phục vụ cho sinh viên ngành Công nghệ thông tin và Kỹ thuật dữ liệu, thuộc chương trình đào tạo 150 tín chỉ của Trường Đại học Sư phạm Kỹ thuật Thành phố Hồ Chí Minh. Tài liệu được biên soạn nhằm cung cấp cho sinh viên các kiến thức cơ bản về mạng máy tính, các giao thức mạng, các thành phần cấu thành mạng LAN và cách quản trị hệ thống mạng. Ngoài ra, tài liệu cũng đề cập đến một số vấn đề an ninh mạng với các giải pháp phổ biến. Tài liệu không chỉ đề cập đến những cơ sở lý luận mà còn trình bày một số kỹ năng cần thiết để thiết kế, cài đặt và quản trị hệ thống mạng. Hy vọng tài liệu sẽ có ích cho các sinh viên và những người muốn xây dựng các hệ thống mạng, quản trị các mạng doanh nghiệp. Có thể còn thiếu sót trong trình bày, biên soạn, nhóm tác giả mong nhận được những đóng góp của độc giả để tài liệu được hoàn thiện hơn.



# MỤC LỤC

<b>MỤC LỤC .....</b>	5
<b>DANH MỤC TỪ VIẾT TẮT .....</b>	10
<b>DANH MỤC CÁC HÌNH ẢNH .....</b>	11
<b>DANH MỤC BẢNG BIỂU .....</b>	17
<b>CHƯƠNG 1: TỔNG QUAN VỀ MẠNG MÁY TÍNH.....</b>	19
<b>1.1. Giới thiệu.....</b>	19
1.1.1. Khái niệm .....	19
1.1.2. Các thành phần cơ bản .....	20
1.1.3. Phân loại mạng .....	21
1.1.4. Sơ đồ mạng.....	22
<b>1.2. Mô hình OSI và TCP/IP .....</b>	25
1.2.1. Mô hình tham chiếu OSI .....	25
1.2.2. Mô hình TCP/IP .....	27
<b>1.3. Quá trình vận chuyển dữ liệu qua mạng.....</b>	36
1.3.1. Quá trình đóng gói và mở gói dữ liệu .....	38
1.3.2. Phân tích quá trình vận chuyển dữ liệu.....	40
<b>1.4. Tổng kết chương.....</b>	47
<b>1.5. Câu hỏi và bài tập.....</b>	47
<b>CHƯƠNG 2: MẠNG LAN VÀ WLAN.....</b>	53
<b>2.1. Giới thiệu.....</b>	53
2.1.1. Một số khái niệm .....	53
2.1.2. Các thiết bị mạng.....	54
<b>2.2. Mạng LAN và chuẩn Ethernet .....</b>	58
2.2.1. Các hệ thống mạng LAN .....	58
2.2.2. Các chuẩn Ethernet .....	59
2.2.3. Các loại cáp thường dùng .....	62

2.2.4. Gửi dữ liệu trong mạng Ethernet .....	64
2.2.5. Một số công cụ kiểm tra kết nối .....	65
<b>2.3. Mạng WLAN .....</b>	<b>67</b>
2.3.1. Giới thiệu .....	67
2.3.2. Các chuẩn mạng không dây .....	67
2.3.3. Các mô hình triển khai mạng Wifi .....	68
2.3.4. Nguyên tắc hoạt động .....	72
2.3.5. Bảo mật trong WLAN.....	72
<b>2.4. Tổng kết chương.....</b>	<b>73</b>
<b>2.5. Câu hỏi Chương 2 .....</b>	<b>73</b>
 <b>CHƯƠNG 3: ĐỊA CHỈ IP .....</b>	<b>78</b>
<b>3.1. Giới thiệu.....</b>	<b>78</b>
<b>3.2. Địa chỉ IPv4.....</b>	<b>78</b>
3.2.1. Giới thiệu .....	78
3.2.2. Phân lớp địa chỉ .....	79
3.2.3. IP Public và IP Private .....	82
3.2.4. Subnet Mask .....	82
3.2.5. Kỹ thuật chia mạng con (IP Subnetting) .....	82
3.2.6. Kỹ thuật VLSM .....	87
3.2.7. Kỹ thuật CIDR.....	92
<b>3.3. Địa chỉ IPv6.....</b>	<b>93</b>
3.3.1. Giới thiệu .....	93
3.3.2. Các loại địa chỉ IPv6.....	94
3.3.3. Chia mạng con trong IPv6 .....	97
3.3.4. Địa chỉ EUI-64.....	98
3.3.5. Gán địa chỉ cho Card mạng.....	98
3.3.6. Các kỹ thuật chuyển đổi IPv4 và IPv6 .....	100
<b>3.4. Tổng kết chương.....</b>	<b>101</b>
<b>3.5. Câu hỏi và bài tập.....</b>	<b>101</b>
 <b>CHƯƠNG 4: KỸ THUẬT TRÊN HẠ TẦNG MẠNG.....</b>	<b>107</b>
<b>4.1. Định tuyến .....</b>	<b>107</b>

4.1.1. Giới thiệu .....	107
4.1.2. Phân loại định tuyến .....	108
4.1.3. Cấu hình định tuyến tĩnh.....	111
4.1.4. Cấu hình định tuyến động .....	113
<b>4.2. Kỹ thuật trên Switch .....</b>	<b>128</b>
4.2.1. VLAN .....	128
4.2.2. VTP .....	134
4.2.3. Giao thức STP .....	138
4.2.4. Định tuyến giữa các VLAN .....	142
<b>4.3. Tổng kết chương.....</b>	<b>147</b>
<b>4.4. Câu hỏi và bài tập.....</b>	<b>148</b>
 <b>CHƯƠNG 5: DỊCH VỤ MẠNG .....</b>	<b>155</b>
<b>5.1. Tổng quan .....</b>	<b>155</b>
<b>5.2. Dịch vụ DHCP .....</b>	<b>155</b>
5.2.1. Giới thiệu .....	155
5.2.2. Nguyên tắc hoạt động .....	156
5.2.3. Cấu hình cấp phát IP động.....	159
5.2.4. Tân công DHCP và giải pháp .....	164
<b>5.3. Dịch vụ DNS.....</b>	<b>165</b>
5.3.1. Giới thiệu .....	165
5.3.2. Các thành phần của hệ thống DNS .....	166
5.3.3. Truy vấn tên miền .....	167
5.3.4. Cấu hình DNS.....	168
<b>5.4. Dịch vụ WEB .....</b>	<b>171</b>
5.4.1. Giới thiệu .....	171
5.4.2. Các thành phần trong dịch vụ Web .....	171
5.4.3. Triển khai nhiều Website trên 1 Web Server.....	174
<b>5.5. Dịch vụ FTP .....</b>	<b>176</b>
5.5.1. Giới thiệu .....	176
5.5.2. Các thành phần của dịch vụ FTP .....	176
5.5.3. Phân loại Active FTP và Passive FTP.....	176
5.5.4. Triển khai dịch vụ FTP .....	178

<b>5.6. Dịch vụ E-MAIL .....</b>	180
5.6.1. Giới thiệu .....	180
5.6.2. Các thành phần của dịch vụ E-mail .....	181
5.6.3. Một số giao thức trong dịch vụ E-mail .....	181
5.6.4. Triển khai dịch vụ E-mail .....	182
<b>5.7. Tổng kết chương .....</b>	182
<b>5.8. Câu hỏi và bài tập .....</b>	183

## **CHƯƠNG 6: CÁC MÔ HÌNH QUẢN TRỊ HỆ THỐNG .....** 189

<b>6.1. Giới thiệu .....</b>	189
<b>6.2. Mô hình quản trị không sử dụng Domain .....</b>	189
<b>6.3. Mô hình quản trị sử dụng Domain .....</b>	191
6.3.1. Các thành phần trong Domain .....	191
6.3.2. Kiến trúc Active Directory .....	194
6.3.3. Các thành phần trong AD .....	197
6.3.4. Quy tắc viết tên đối tượng trên Active Directory .....	197
6.3.5. Cài đặt Domain Controller trên Windows Server .....	199
6.3.6. Quản trị User, Group trên Windows Server .....	204
<b>6.4. Quản trị truy xuất dùng NTFS .....</b>	209
6.4.1. Giới thiệu .....	209
6.4.2. Các quyền truy xuất NTFS .....	210
6.4.3. Các quy tắc phân quyền NTFS .....	212
<b>6.5. Chia sẻ dữ liệu trên mạng .....</b>	216
6.5.1. Đặc điểm của chia sẻ dữ liệu .....	216
6.5.2. Các quy tắc khi chia sẻ thư mục .....	217
6.5.3. Thư mục chia sẻ mặc định .....	219
6.5.4. Thực hiện chia sẻ thư mục .....	219
6.5.5. Truy xuất dữ liệu chia sẻ .....	220
6.5.6. Kiểm soát dữ liệu chia sẻ .....	221
<b>6.6. Kết hợp quyền thư mục được chia sẻ và quyền NTFS .....</b>	221
<b>6.7. Thiết lập các chính sách quản trị (GPO) .....</b>	222
<b>6.8. Tổng kết chương .....</b>	222
<b>6.9. Câu hỏi và bài tập .....</b>	225

<b>CHƯƠNG 7: AN NINH MẠNG .....</b>	230
<b>7.1. Giới thiệu .....</b>	230
<b>7.2. Phân loại lỗ hổng mạng .....</b>	233
<b>7.3. Các dạng tấn công mạng .....</b>	233
<b>7.4. Một số tấn công mạng phổ biến .....</b>	234
7.4.1. Tấn công vào các trang Web .....	234
7.4.2. Tấn công từ chối dịch vụ .....	234
7.4.3. Tấn công bằng mã độc .....	235
<b>7.5. Các hệ thống an ninh mạng .....</b>	235
7.5.1. Firewall .....	236
7.5.2. IDS/IPS .....	237
7.5.3. SIEM .....	238
7.5.4. Một số giải pháp nâng cao hiệu quả bảo mật .....	239
<b>7.6. Hệ thống giám sát mạng .....</b>	239
7.6.1. Giới thiệu .....	239
7.6.2. Các giao thức của hệ thống giám sát .....	240
7.6.3. Các hoạt động giám sát .....	241
<b>7.7. SDN, KDN và xu hướng quản trị .....</b>	242
7.7.1. Một số khái niệm .....	242
7.7.2. Controller .....	244
7.7.3. SDN .....	245
7.7.4. KDN .....	245
<b>7.8. Tổng kết chương .....</b>	245
<b>7.9. Câu hỏi và bài tập .....</b>	245
<b>TÀI LIỆU THAM KHẢO .....</b>	251

## DANH MỤC TỪ VIẾT TẮT

Viết tắt	Nội dung	Viết tắt	Nội dung
OSI	Open Systems Interconnection Reference	EUI-64	Extended Unique Identifier
ARP	Address Resolution Protocol	RIP	Routing Information Protocol
RARP	Reverse ARP	OSPF	Open Shortest Path First
MAC	Media Access Control	VLAN	Virtual Local Area Network
TCP	Transmission Control Protocol	EIGRP	Enhanced Interior Gateway Routing Protocol
UDP	User Datagram Protocol	STP	Spanning Tree Protocol
IP	Internet Protocol	NAT	Network Address Translation
HTTP	Hypertext Transfer Protocol	VTP	VLAN Trunking Protocol
FTP	File Transfer Protocol	FAT	File Allocation Table
DHCP	Dynamic Host Configuration Protocol	NTFS	New Technology File System
DNS	Domain Name System	EFS	Encrypted File Service
SMTP	Simple Mail Transfer Protocol	SNMP	Simple Network Management Protocol
POP	Post Office Protocol	ACL	Access Control List
UTP	Unshielded Twisted Pair	AD	Active Directory
RJ45	Registered Jack 45	DC	Domain controller
CSMA	Carrier Sense Multiple Access	GPO	Group Policy Object
CSMA/ CD	Collision Detection	SDN	Software Defined Network
CSMA/ CA	Collision Avoidance	KDN	Knowledge Defined Network
BSS	Basic Service Sets	IDS	Intrusion Detection System
AP	Access Point	DoS	Denial of Service
SSID	Service Set Identifier	DDoS	Distributed Dos
IBSS	Independent Basic Service Set	SIEM	Security Information and Event Management
ESS	Extended Service Set	IPS	Intrusion Prevention Systems
VLSM	Variable Length Subnet Masking	CIDR	Classless Inter Domain Routing

## DANH MỤC CÁC HÌNH ẢNH

<b>Hình 1.1:</b> Mô hình hệ thống mạng .....	20
<b>Hình 1.2:</b> Sơ đồ vật lý .....	22
<b>Hình 1.3:</b> Sơ đồ logic .....	23
<b>Hình 1.4:</b> Sơ đồ vật lý và logic .....	23
<b>Hình 1.5:</b> Sơ đồ luận lý .....	24
<b>Hình 1.6:</b> Ví dụ về sơ đồ vật lý .....	24
<b>Hình 1.7:</b> Mô hình tham chiếu OSI .....	26
<b>Hình 1.8:</b> Mô hình TCP/IP .....	27
<b>Hình 1.9:</b> Mối tương quan các tầng của mô hình OSI và TCP/IP .....	27
<b>Hình 1.10:</b> Đơn vị dữ liệu ở các tầng .....	29
<b>Hình 1.11:</b> Quá trình 3 bước bắt tay .....	30
<b>Hình 1.12:</b> Mô tả dữ liệu ở các tầng trong mô hình OSI .....	31
<b>Hình 1.13:</b> TCP Header .....	32
<b>Hình 1.14:</b> UDP Header .....	32
<b>Hình 1.15:</b> Máy gửi gửi một lượng dữ liệu lớn .....	33
<b>Hình 1.16:</b> Nhiều máy cùng gửi dữ liệu đến một máy .....	33
<b>Hình 1.17:</b> Điều khiển luồng .....	34
<b>Hình 1.18:</b> Window Size = 1 .....	35
<b>Hình 1.19:</b> Window Size = 3 .....	35
<b>Hình 1.20:</b> Giá trị Window Size được điều chỉnh khi có nghẽn .....	36
<b>Hình 1.21:</b> Truyền dữ liệu - kiểu truyền Unicast .....	37
<b>Hình 1.22:</b> Truyền dữ liệu - kiểu truyền Multicast .....	37
<b>Hình 1.23:</b> Truyền dữ liệu - kiểu truyền Broadcast .....	38
<b>Hình 1.24:</b> Quá trình đóng gói dữ liệu .....	38
<b>Hình 1.25:</b> Quá trình mở gói dữ liệu .....	39
<b>Hình 1.26:</b> Quá trình vận chuyển dữ liệu qua mạng .....	40
<b>Hình 1.27:</b> Hai máy kết nối qua Hub .....	40
<b>Hình 1.28:</b> Hoạt động của giao thức ARP .....	41
<b>Hình 1.29:</b> Gói tin ARP Request .....	41
<b>Hình 1.30:</b> Gói tin ARP Reply .....	42

<b>Hình 1.31:</b> Hai máy kết nối qua Switch .....	42
<b>Hình 1.32:</b> Swich học địa chỉ MAC từ gói tin ARP Request .....	43
<b>Hình 1.33:</b> Swich học địa chỉ MAC từ gói tin ARP Reply .....	44
<b>Hình 1.34:</b> Hai máy kết nối qua Router .....	44
<b>Hình 1.35:</b> Các thông số ARP Request và ARP Reply ở máy gửi .....	46
<b>Hình 1.36:</b> Các thông số ARP Request và ARP Reply ở máy nhận.....	47
<b>Hình 2.1:</b> Truyền dữ liệu qua Hub .....	55
<b>Hình 2.2:</b> Bảng địa chỉ MAC trên Switch.....	56
<b>Hình 2.3:</b> Bảng địa chỉ MAC trên Cisco Switch.....	57
<b>Hình 2.4:</b> Kết nối hệ thống mạng sử dụng Router .....	57
<b>Hình 2.5:</b> Sơ đồ mạng cơ bản của mạng SOHO .....	58
<b>Hình 2.6:</b> Sơ đồ của một hệ thống mạng tổ chức trong một tòa nhà ....	58
<b>Hình 2.7:</b> Quá trình phát triển các chuẩn Ethernet.....	59
<b>Hình 2.8:</b> Cấu trúc của Frame Ethernet.....	61
<b>Hình 2.9:</b> Cấu trúc địa chỉ MAC .....	62
<b>Hình 2.10:</b> Đầu nối RJ-45 .....	62
<b>Hình 2.11:</b> Chuẩn T568-A và T568-B .....	63
<b>Hình 2.12:</b> Cáp thẳng .....	63
<b>Hình 2.13:</b> Cáp chéo.....	63
<b>Hình 2.14:</b> Switch và Module quang .....	64
<b>Hình 2.15:</b> Thực hiện lệnh PING trên hệ điều hành Window .....	66
<b>Hình 2.16:</b> Telnet qua chế độ dòng lệnh trên hệ điều hành Window ....	66
<b>Hình 2.17:</b> Phần mềm PuTTy .....	67
<b>Hình 2.18:</b> Mô hình mạng Wifi với 1 AP .....	68
<b>Hình 2.19:</b> Mạng Wifi kết nối với mạng có dây .....	69
<b>Hình 2.20:</b> Mô hình ESS .....	70
<b>Hình 2.21:</b> Mô hình mạng Ad-Hoc .....	70
<b>Hình 2.22:</b> Mô hình Wifi - Repeater .....	71
<b>Hình 2.23:</b> Mô hình mạng Wifi - Outdoor Bridge.....	71
<b>Hình 2.24:</b> Mô hình mạng Wifi - Mesh .....	72
<b>Hình 2.25:</b> Chứng thực với Radius Server .....	73
<b>Hình 3.1:</b> Cấu trúc tổng quát của địa chỉ IP .....	78

<b>Hình 3.2:</b> IPv4 Header .....	79
<b>Hình 3.3:</b> Hoạch định IP cho một công ty.....	88
<b>Hình 3.4:</b> Kết quả hoạch định IP cho một công ty .....	92
<b>Hình 3.5:</b> IPv6 Header .....	93
<b>Hình 3.6:</b> Cấu trúc địa chỉ IPv6.....	94
<b>Hình 3.7:</b> Địa chỉ Unique Local IPv6 .....	95
<b>Hình 3.8:</b> Địa chỉ IPv6 Multicast .....	95
<b>Hình 3.9:</b> Địa chỉ IPv6 Link Local.....	96
<b>Hình 3.10:</b> Chia mạng con trong IPv6 .....	97
<b>Hình 3.11:</b> Ví dụ về hoạch định IP cho các mạng IPv6 .....	98
<b>Hình 3.12:</b> Thành lập địa chỉ dạng EUI-64.....	98
<b>Hình 3.13:</b> Địa chỉ EUI-64.....	98
<b>Hình 3.14:</b> Cấu hình IPv6 cho Card mạng trên hệ điều hành Windows .....	99
<b>Hình 3.15:</b> Cấu hình IPv6 tự động cho Host dạng Stateless .....	99
<b>Hình 3.16:</b> Kỹ thuật chuyển đổi Dual Stack .....	100
<b>Hình 3.17:</b> Kỹ thuật chuyển đổi NAT-TP.....	100
<b>Hình 3.18:</b> Kỹ thuật chuyển đổi Tunnel.....	101
<b>Hình 4.1:</b> Mô hình hệ thống mạng .....	107
<b>Hình 4.2:</b> Bảng định tuyến trên Router.....	108
<b>Hình 4.3:</b> Trao đổi thông tin định tuyến dạng Distance Vector.....	109
<b>Hình 4.4:</b> Trao đổi thông tin định tuyến dạng Link State .....	109
<b>Hình 4.5:</b> Mô hình ví dụ cho cấu hình định tuyến tĩnh .....	112
<b>Hình 4.6:</b> Cấu hình Default Route .....	113
<b>Hình 4.7:</b> Mạng không liên tục .....	114
<b>Hình 4.8:</b> Sơ đồ ví dụ cho cấu hình RIP.....	115
<b>Hình 4.9:</b> Ví dụ cấu hình chứng thực Plain Text trong RIPv2 .....	116
<b>Hình 4.10:</b> Sơ đồ ví dụ về cấu hình OSPF Single Area .....	120
<b>Hình 4.11:</b> Sơ đồ ví dụ về cấu hình OSPF Multi Area.....	120
<b>Hình 4.12:</b> Sơ đồ ví dụ cho cấu hình chứng thực trong OSPF .....	121
<b>Hình 4.13:</b> Sơ đồ mạng cấu hình định tuyến OSPF Multi Area.....	123
<b>Hình 4.14:</b> Sơ đồ mạng cấu hình định tuyến EIGRP AS 100 .....	126

<b>Hình 4.15:</b> Sơ đồ mạng ví dụ cấu hình chứng thực trong EIGRP.....	127
<b>Hình 4.16:</b> Chia VLAN trên Switch.....	128
<b>Hình 4.17:</b> VLAN tĩnh .....	129
<b>Hình 4.18:</b> VLAN động .....	129
<b>Hình 4.19:</b> Cấu hình VLAN trên Switch.....	131
<b>Hình 4.20:</b> Sử dụng mỗi kết nối cho từng VLAN.....	132
<b>Hình 4.21:</b> Kết nối Trunk cho các VLAN.....	133
<b>Hình 4.22:</b> Frame được đóng gói theo kiểu 802.1Q .....	134
<b>Hình 4.23:</b> Hoạt động của VTP .....	135
<b>Hình 4.24:</b> Các Mode của VTP .....	135
<b>Hình 4.25:</b> Sơ đồ mạng cấu hình VTP .....	136
<b>Hình 4.26:</b> Sơ đồ kết nối các Switch.....	139
<b>Hình 4.27:</b> Ví dụ về STP .....	140
<b>Hình 4.28:</b> STP cho từng VLAN (PVSTP+).....	140
<b>Hình 4.29:</b> Các tham số trong Bridge ID .....	141
<b>Hình 4.30:</b> Thiết lập Root trên các Switch khu vực Distribution.....	141
<b>Hình 4.31:</b> Định tuyến giữa các VLAN .....	142
<b>Hình 4.32:</b> Định tuyến VLAN dùng Sub Interface trên Router .....	143
<b>Hình 4.33:</b> Định tuyến cho các VLAN sử dụng MultiLayer Switch ..	145
<b>Hình 5.1:</b> DHCP Server và Client cùng miền quảng bá.....	156
<b>Hình 5.2:</b> DHCP Server và Client khác miền quảng bá.....	157
<b>Hình 5.3:</b> Mô hình cài đặt thử nghiệm DHCP Server .....	159
<b>Hình 5.4:</b> Giao diện cấu hình DHCP Server trên Window Server .....	160
<b>Hình 5.5:</b> Đặt tên cho Scope .....	160
<b>Hình 5.6:</b> Đặt dãy địa chỉ IP cho Scope và Subnet Mask .....	160
<b>Hình 5.7:</b> Thiết lập thời gian cho thuê IP .....	161
<b>Hình 5.8:</b> Thiết lập địa chỉ Default Gateway cho Scope.....	161
<b>Hình 5.9:</b> Thiết lập địa chỉ DNS .....	162
<b>Hình 5.10:</b> Kết quả cấu hình cho một Scope.....	162
<b>Hình 5.11:</b> Kiểm tra kết quả xin cấp phát IP từ máy Client .....	163
<b>Hình 5.12:</b> Tổ chức không gian tên miền Internet .....	166
<b>Hình 5.13:</b> DNS Server và Zone .....	167

<b>Hình 5.14:</b> Cấu hình phân giải thuận trên Windows Server.....	168
<b>Hình 5.15:</b> Cấu hình phân giải nghịch trên Windows Server.....	168
<b>Hình 5.16:</b> Kiểm tra kết quả phân giải với NsLookup .....	169
<b>Hình 5.17:</b> Điều chỉnh địa chỉ của DNS Server và các tham số .....	169
<b>Hình 5.18:</b> Các thành phần trong dịch vụ Web .....	171
<b>Hình 5.19:</b> Tên miền với Port mặc định.....	172
<b>Hình 5.20:</b> Tên miền với Port đã được điều chỉnh thành 8080 .....	172
<b>Hình 5.21:</b> Mô hình triển khai dịch vụ Web.....	172
<b>Hình 5.22:</b> Cấu hình Site Binding.....	173
<b>Hình 5.23:</b> Cấu hình đường dẫn thư mục chứa mã nguồn Web .....	173
<b>Hình 5.24:</b> Cấu hình cho Website baigiang.org .....	174
<b>Hình 5.25:</b> Cấu hình cho Website example.org.....	175
<b>Hình 5.26:</b> Thông tin cấu hình các Website .....	175
<b>Hình 5.27:</b> Mô hình dịch vụ FTP .....	176
<b>Hình 5.28:</b> Hoạt động của Active FTP .....	177
<b>Hình 5.29:</b> Hoạt động của Passive FTP .....	177
<b>Hình 5.30:</b> Cửa sổ cấu hình FTP Server.....	178
<b>Hình 5.31:</b> Cấu hình chứng thực .....	179
<b>Hình 5.32:</b> Cấu hình quyền truy cập .....	179
<b>Hình 5.33:</b> Đăng nhập sử dụng dịch vụ .....	180
<b>Hình 5.34:</b> Kết quả truy cập FTP Server.....	180
<b>Hình 5.35:</b> Hệ thống E-mail .....	181
<b>Hình 6.1:</b> Mô hình quản trị Workgroup .....	190
<b>Hình 6.2:</b> Thiết lập tên cho Workgroup.....	190
<b>Hình 6.3:</b> Máy chủ quản lý tập trung bên trong mạng .....	191
<b>Hình 6.4:</b> Các thành phần trong AD .....	192
<b>Hình 6.5:</b> Kiến trúc logic của Active Directory .....	194
<b>Hình 6.6:</b> Domain Tree.....	195
<b>Hình 6.7:</b> Kết nối giữa các Site .....	196
<b>Hình 6.8:</b> Sơ đồ tên tương đối DN .....	198
<b>Hình 6.9:</b> Cài đặt dịch vụ AD .....	199
<b>Hình 6.10:</b> Quá trình cài đặt AD .....	200

<b>Hình 6.11:</b> Giao diện cấu hình AD .....	200
<b>Hình 6.12:</b> Đặt tên cho Domain .....	201
<b>Hình 6.13:</b> Cấu hình Password cho Mode Restore .....	202
<b>Hình 6.14:</b> Máy Client gia nhập vào Domain .....	202
<b>Hình 6.15:</b> Công cụ quản trị trên Domain.....	203
<b>Hình 6.16:</b> Các Group mặc định trên Domain .....	206
<b>Hình 6.17:</b> Các Object trên Domain.....	207
<b>Hình 6.18:</b> Phân quyền truy cập.....	212
<b>Hình 6.19:</b> Phủ nhận quyền truy cập dữ liệu.....	213
<b>Hình 6.20:</b> Quyền truy cập khi Copy dữ liệu.....	214
<b>Hình 6.21:</b> Quyền truy cập khi di chuyển dữ liệu.....	215
<b>Hình 6.22:</b> Cấu hình thay đổi quyền truy cập .....	215
<b>Hình 6.23:</b> Một số chức năng cấu hình phân quyền nâng cao .....	216
<b>Hình 6.24:</b> Quyền trên thư mục chia sẻ .....	217
<b>Hình 6.25:</b> Phủ nhận quyền trên thư mục chia sẻ .....	218
<b>Hình 6.26:</b> Các thư mục chia sẻ mặc định .....	219
<b>Hình 6.27:</b> Chia sẻ thư mục và gán quyền truy cập .....	220
<b>Hình 6.28:</b> Ánh xạ ổ đĩa mạng .....	220
<b>Hình 6.29:</b> Kiểm tra các thư mục chia sẻ trên máy tính.....	221
<b>Hình 6.30:</b> Kết hợp quyền NTFS và quyền chia sẻ.....	222
<b>Hình 6.31:</b> Giao diện cấu hình các chính sách quản trị (GPO) .....	223
<b>Hình 6.32:</b> Giao diện chọn chức năng cấu hình GPO .....	224
<b>Hình 6.33:</b> Tạo mới một GPO .....	224
<b>Hình 7.1:</b> Ba giai đoạn trong bảo vệ hệ thống .....	231
<b>Hình 7.2:</b> Bảo mật theo chiều sâu .....	232
<b>Hình 7.3:</b> Tấn công DoS và DDoS.....	235
<b>Hình 7.4:</b> Bảo vệ mạng LAN với Firewall.....	236
<b>Hình 7.5:</b> Một số thiết bị an ninh trong hệ thống mạng .....	237
<b>Hình 7.6:</b> Các gói tin cơ bản trong SNMP .....	241
<b>Hình 7.7:</b> Mặt phẳng điều khiển và mặt phẳng dữ liệu.....	243
<b>Hình 7.8:</b> Quản lý tập trung với Controller.....	244
<b>Hình 7.9:</b> Mặt phẳng và quy trình hoạt động của KDN .....	245

## DANH MỤC BẢNG BIỂU

<b>Bảng 1.1:</b> Một số thiết bị mạng và giao thức phổ biến .....	29
<b>Bảng 1.2:</b> Các cơ chế truyền ở tầng Transport .....	30
<b>Bảng 1.3:</b> Mối liên hệ giữa tầng Application và Transport .....	32
<b>Bảng 2.1:</b> Một số chuẩn Ethernet phổ biến .....	60
<b>Bảng 4.1:</b> So sánh giữa RIPv1 và RIPv2 .....	114
<b>Bảng 4.2:</b> Bảng quy đổi STP Cost dựa vào tốc độ cổng vật lý .....	140



# **CHƯƠNG 1**

## **TỔNG QUAN VỀ MẠNG MÁY TÍNH**

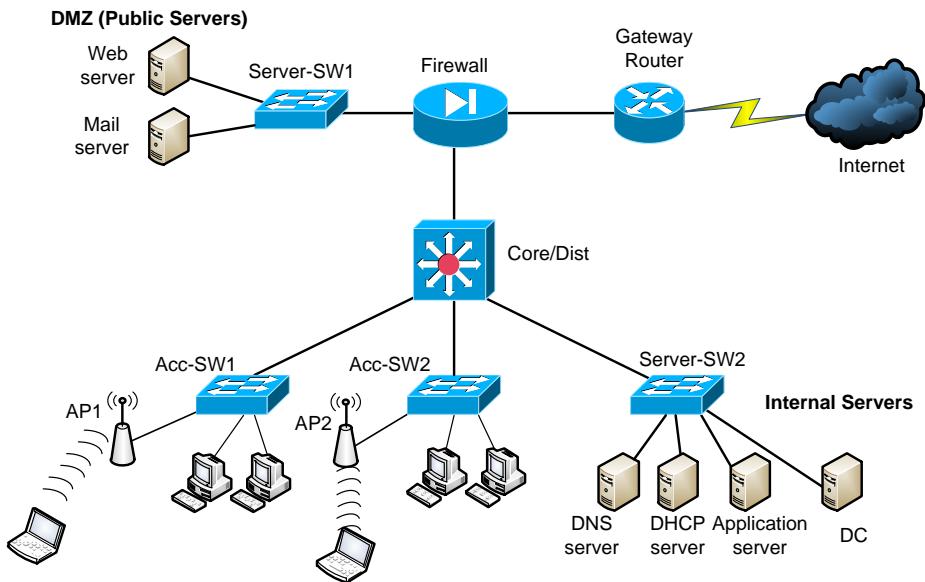
Chương này trình bày một số khái niệm về mạng máy tính, phân loại mạng máy tính, đặc điểm của mô hình tham chiếu OSI và mô hình TCP/IP, quá trình trao đổi dữ liệu qua mạng. Học xong chương này, người học có khả năng:

- Trình bày được khái niệm, các thành phần chính trong mạng máy tính.
- Phân biệt được đặc điểm của mô hình tham chiếu OSI và TCP/IP.
- Phân biệt được các loại mạng: LAN, WAN, MAN, SAN, Internet.
- Trình bày được quá trình trao đổi dữ liệu qua mạng.
- Phân tích được các thành phần cơ bản trong gói tin gửi qua mạng.

### **1.1. Giới thiệu**

#### **1.1.1. Khái niệm**

Có nhiều khái niệm về mạng máy tính được đưa ra. Nhìn chung, các khái niệm đều có những điểm chung tập trung vào: thiết bị đầu cuối, thiết bị mạng, môi trường kết nối và các giao thức. Chúng ta có thể hiểu mạng máy tính là một hệ thống gồm các thiết bị đầu cuối kết nối với nhau qua các thiết bị mạng để trao đổi dữ liệu giữa chúng thông qua một môi trường truyền dẫn nào đó. Để các thiết bị có thể trao đổi thông tin trên mạng, các giao thức mạng được sử dụng. Nó như các nguyên tắc, quy luật, ngôn ngữ được chuẩn hóa và cài đặt trên các đối tượng sử dụng.



**Hình 1.1: Mô hình hệ thống mạng**

Trong thời đại ngày nay, bên cạnh máy tính là thành phần chủ yếu, còn có nhiều thiết bị khác kết nối vào mạng máy tính như máy in, camera, điện thoại,... gọi chung là thiết bị đầu cuối. Môi trường kết nối gồm môi trường có dây và không dây; các thiết bị mạng thường dùng để kết nối các thiết bị đầu cuối như: Switch, Router, Access Point, Firewall,... Các giao thức được sử dụng để các thiết bị đầu cuối có thể giao tiếp được với nhau thông qua các ứng dụng/dịch vụ trên mạng.

### 1.1.2. Các thành phần cơ bản

Các thành phần cơ bản của mạng máy tính bao gồm:

- **Thiết bị đầu cuối:** Thông thường là các thiết bị làm việc trực tiếp với người dùng như máy tính, điện thoại thông minh, camera-ip, các thiết bị IoT,...
- **Thiết bị mạng:** Là các thiết bị trung gian có nhiệm vụ kết nối các thiết bị đầu cuối lại với nhau. **Switch** là thiết bị tập trung kết nối các thiết bị đầu cuối trong mạng có dây, **Access Point** là thiết bị tập trung kết nối các thiết bị đầu cuối trong mạng không dây, **Router** là thiết bị định tuyến dùng để kết nối giữa các mạng và thực hiện chức năng xác định đường đi cho các gói tin thông

qua hệ thống mạng. Bên cạnh đó còn có nhiều thiết bị khác như **Firewall, IDS/IPS, WAF, SIEM** làm chức năng bảo mật, giám sát hệ thống.

- **Môi trường kết nối:** Bao gồm môi trường có dây và không dây.
- **Các thiết bị kết nối:** Gồm Card mạng, đầu nối, dây cáp,...
- **Các Server** cung cấp ứng dụng/dịch vụ: Là một thành phần quan trọng trong hệ thống công nghệ thông tin (CNTT), có chức năng cung cấp các ứng dụng/dịch vụ cho hệ thống và cho người dùng. Các Server cung cấp ứng dụng/dịch vụ phổ biến như: Web Server, E-mail Server, DHCP Server, DNS Server,... Ngoài ra còn có các Server cung cấp ứng dụng phục vụ chuyên biệt cho nghiệp vụ của từng tổ chức, doanh nghiệp gọi là các Application Server.
- **Các giao thức mạng:** Là các nguyên tắc, quy luật, ngôn ngữ được chuẩn hóa, được tích hợp vào các ứng dụng dùng trong việc giao tiếp/sử dụng các ứng dụng/dịch vụ trên mạng như giao thức HTTP, HTTPS dùng trong ứng dụng **Web**; **SMTP, POP3, IMAP** dùng trong ứng dụng E-mail; **Telnet, SSH** dùng trong các ứng dụng hỗ trợ truy cập từ xa phục vụ cho công tác quản trị mạng,...

### 1.1.3. Phân loại mạng

Mạng máy tính được phân chia làm nhiều loại tùy vào mục đích nghiên cứu và mục đích sử dụng. Trong phần này giới thiệu một số loại mạng phổ biến: LAN, WAN, MAN, SAN và Internet.

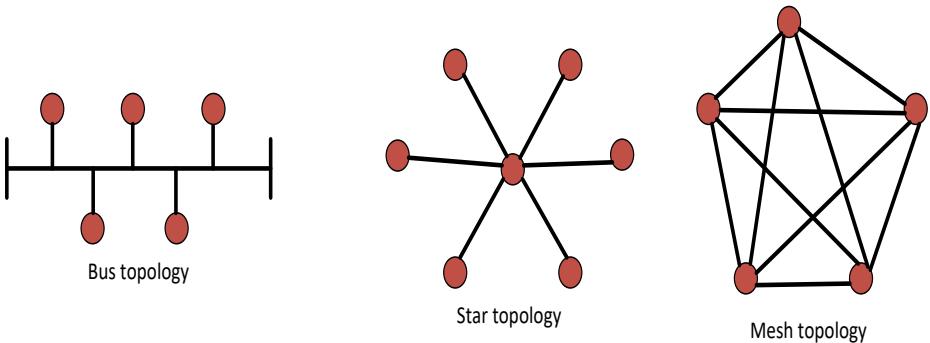
- **LAN (Local Area Network):** Mạng LAN là mạng cục bộ, được triển khai cho một tổ chức/doanh nghiệp trong một không gian địa lý nhỏ. Các thiết bị trong LAN có kết nối trực tiếp với nhau, tốc độ cao. Công nghệ mạng được sử dụng trong LAN phổ biến là **Ethernet (802.3)**.
- **WAN (Wide Area Network):** Mạng WAN là mạng diện rộng, là mạng của một tổ chức có nhiều chi nhánh kết nối với nhau thông qua môi trường Internet. Các công nghệ được sử dụng trong WAN phổ biến là: **MPLS, VPN,...**

- **MAN** (Metropolitan Area Network): Mạng MAN là mạng đô thị, các thành phố lớn thường tổ chức hệ thống mạng đường trực tốc độ cao để phục vụ cho các đơn vị quan trọng trong thành phố đó.
- **SAN** (Storage Area Network): Mạng SAN là mạng lưu trữ, nhằm thực hiện chức năng lưu trữ cho lượng dữ liệu lớn.
- **INTERNET**: Mạng Internet là mạng của các mạng, là hệ thống mạng toàn cầu.

#### 1.1.4. Sơ đồ mạng

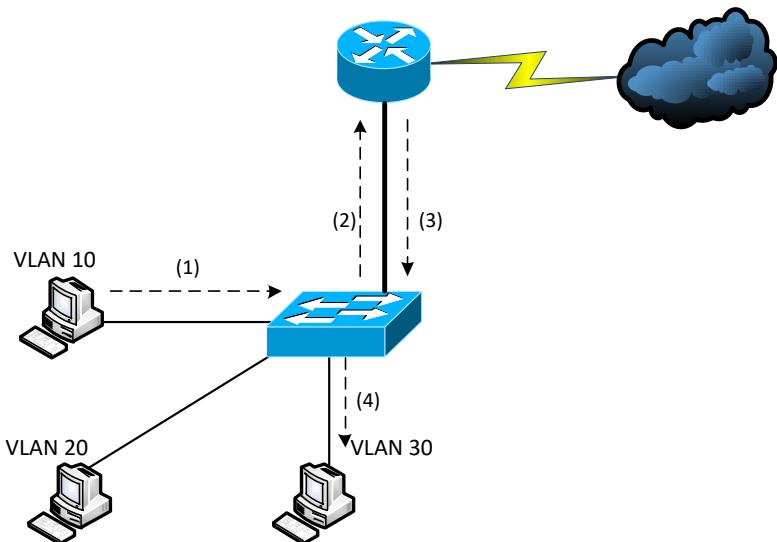
Sơ đồ mạng có ý nghĩa quan trọng trong việc phân tích, thiết kế, triển khai, vận hành và xử lý sự cố. Sơ đồ mạng được chia làm 2 loại là sơ đồ **vật lý** (physical topology) và **sơ đồ luận lý** (logical topology).

**Sơ đồ vật lý:** Mô tả về các thiết bị, cáp mạng, các kết nối vật lý. Trong một hệ thống CNTT, có thể có nhiều sơ đồ vật lý như: sơ đồ vật lý tổng quan, mô tả các thành phần chính của hệ thống và kết nối giữa chúng, hay sơ đồ chi tiết kết nối các thiết bị trong một phòng làm việc. Có 3 mô hình kết nối vật lý cơ bản là mô hình dạng Bus, Star và Mesh. Trong đó, mô hình kết nối dạng Bus là mô hình đã cũ, mô hình mạng **Star** là mô hình phổ biến nhất đang được sử dụng hiện nay. Mô hình mạng **Mesh** sử dụng trong những hệ thống cần thiết kế có tính dự phòng cao.



**Hình 1.2: Sơ đồ vật lý**

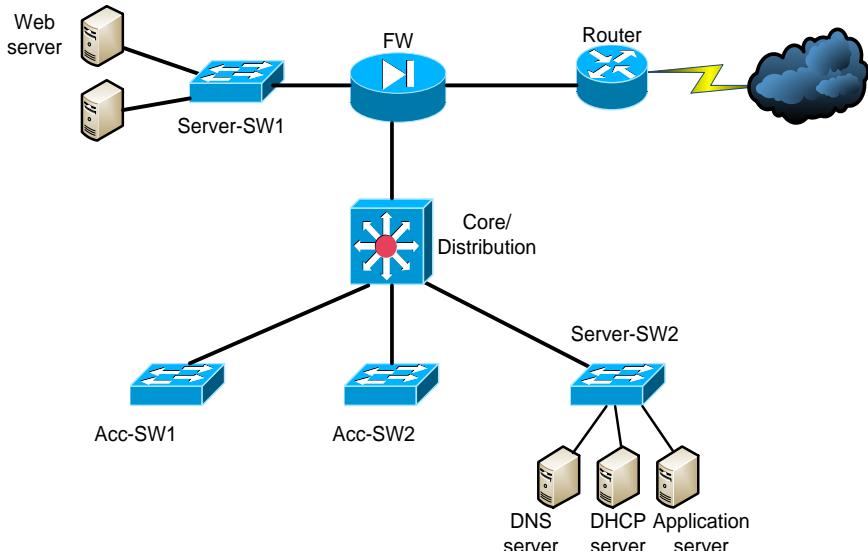
**Sơ đồ luận lý:** Mô tả các đường đi luận lý được sử dụng để truyền dữ liệu từ một điểm đến một điểm khác trong mạng.



**Hình 1.3:** Sơ đồ logic

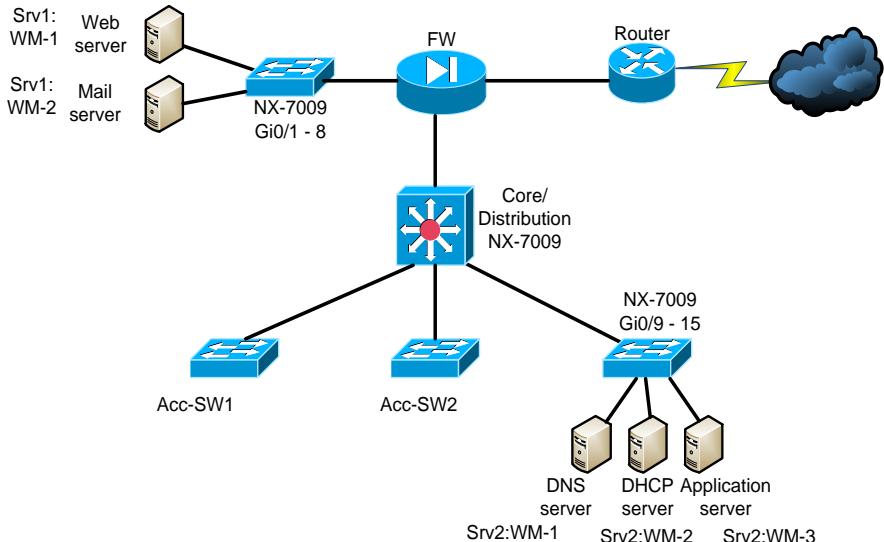
Sơ đồ vật lý và sơ đồ luận lý đôi khi khó phân biệt một cách rõ ràng. Trong một số trường hợp, hai sơ đồ này giống nhau. Trong một số trường hợp khác, hai sơ đồ này khác nhau. Chúng ta xem xét 2 ví dụ cụ thể sau đây.

**Ví dụ 1:** Sơ đồ vật lý và sơ đồ luận lý giống nhau trong trường hợp số lượng thiết bị được sử dụng là giống nhau như thể hiện trong Hình 1.4.

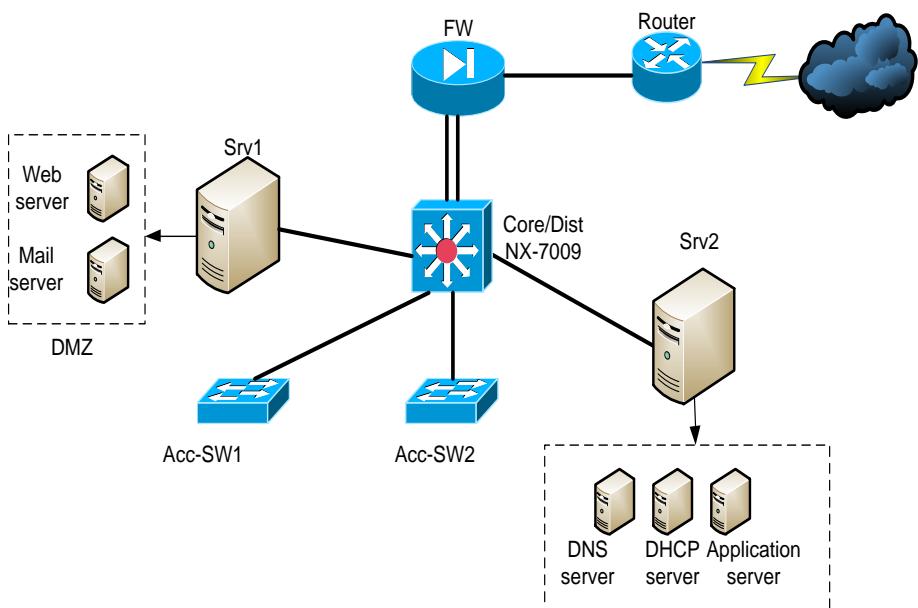


**Hình 1.4:** Sơ đồ vật lý và logic

**Ví dụ 2:** Sự khác nhau giữa sơ đồ vật lý và sơ đồ luân lý của cùng một hệ thống CNTT thể hiện ở Hình 1.5 và Hình 1.6. Trong trường hợp này, việc ảo hóa trên các máy chủ hay trên thiết bị mạng (tạo các VLAN trên Switch,...) đã làm giảm số lượng thiết bị vật lý. Do đó, ta thấy số lượng thiết bị mô tả trong sơ đồ luân lý nhiều hơn.



**Hình 1.5: Sơ đồ luân lý**



**Hình 1.6: Ví dụ về sơ đồ vật lý**

Một số đặc trưng của mạng:

- **Tốc độ:** Là tốc độ truyền dữ liệu trên đường truyền.
- **Chi phí:** Mức độ đầu tư cho các thành phần mạng, chi phí cho quá trình cài đặt, vận hành, bảo trì và nâng cấp của một hệ thống mạng.
- **Bảo mật:** Sự bảo mật chỉ ra cách thức bảo vệ một mạng trước các nguy cơ xâm nhập và các tấn công mạng.
- **Tính sẵn sàng:** Là khả năng sẵn sàng đáp ứng được các yêu cầu của người dùng.
- **Khả năng mở rộng:** Là khả năng hệ thống mạng có thể được bổ sung thêm các ứng dụng, dịch vụ, chi nhánh mới,... mà không ảnh hưởng nhiều đến hệ thống mạng hiện tại.

## 1.2. Mô hình OSI và TCP/IP

Ngày nay mô hình mạng được sử dụng phổ biến là TCP/IP. Trước đó, các nhà sản xuất tạo ra các giao thức mạng chỉ hỗ trợ cho máy tính của họ. Do đó, chỉ có các máy tính của cùng một nhà sản xuất mới có thể giao tiếp được với nhau. Để có thể **giao tiếp giữa các máy tính khác nhà sản xuất** cần có mô hình trung gian hỗ trợ. Trong suốt những năm **1990**, hai mô hình OSI và TCP/IP là 2 mô hình được lựa chọn cho việc này. Đến **cuối những năm 1990**, TCP/IP trở thành lựa chọn phổ biến hơn.

Mô hình tham chiếu OSI và TCP/IP là hai mô hình cơ bản trong mạng máy tính. Trong đó, mô hình OSI gọi là mô hình tham chiếu, có thể hiểu đây là mô hình lý thuyết, được dùng cho mục đích học tập, nghiên cứu. Mô hình TCP/IP là mô hình được triển khai thực tế và dùng trong mạng Internet hiện nay. Cả hai mô hình được tổ chức theo dạng phân lớp, các lớp và chức năng của mỗi lớp ở mô hình TCP/IP có thể được ánh xạ tương đương với các lớp trong mô hình tham chiếu OSI.

### 1.2.1. Mô hình tham chiếu OSI

Mô hình tham chiếu OSI gồm 7 tầng (Layer) được mô tả ở Hình 1.7.

L7	Application
L6	Presentation
L5	Session
L4	Transport
L3	Network
L2	Data Link
L1	Physical

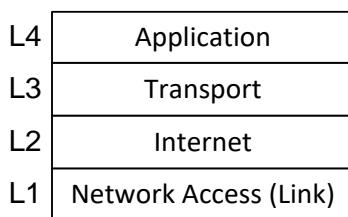
**Hình 1.7: Mô hình tham chiếu OSI**

- **Tầng 1 (Layer 1) - Physical:** Tầng *Vật lý* liên quan các đặc điểm về điện tử, cơ khí; xử lý dữ liệu dạng bit; thiết bị mạng phổ biến hoạt động ở tầng này là Hub.
- **Tầng 2 (Layer 2) - Data Link:** Tầng *Liên kết dữ liệu* liên quan đến việc định dạng dữ liệu theo các chuẩn, điều khiển cách thức truy xuất đến môi trường vật lý; xử lý dữ liệu dạng khung (**Frame**); liên quan đến địa chỉ vật lý (địa chỉ MAC); thiết bị mạng phổ biến hoạt động ở tầng này là Switch.
- **Tầng 3 (Layer 3) - Network:** Tầng *Mạng* thực hiện chức năng định tuyến cho các gói tin; xử lý dữ liệu dạng gói (**Packet**); liên quan đến địa chỉ luận lý (phổ biến là địa chỉ IP,...); thiết bị phổ biến hoạt động ở tầng này là Router.
- **Tầng 4 (Layer 4) - Transport:** Tầng *Vận chuyển* thực hiện chức năng đảm bảo việc vận chuyển dữ liệu từ nguồn đến đích thông qua hệ thống mạng. Thực hiện việc chia nhỏ dữ liệu cho **phù hợp** với kích thước tối đa của kênh truyền ở bên gửi và tái lập ở bên nhận.
- **Tầng 5 (Layer 5) - Session:** Tầng *Phiên* thực hiện việc thiết lập, quản lý và kết thúc các phiên làm việc của các chương trình ứng dụng.
- **Tầng 6 (Layer 6) - Presentation:** Tầng *Trình bày* thực hiện việc đảm bảo dữ liệu đọc được ở tầng *Ứng dụng*. Các **chức năng** của tầng này liên quan đến định dạng dữ liệu, cấu trúc dữ liệu, nén dữ liệu, mã hóa dữ liệu.
- **Tầng 7 (Layer 7) - Application:** Tầng *Ứng dụng* là tầng cao nhất trong mô hình OSI, liên quan đến các chương trình ứng dụng làm việc

trực tiếp với người dùng (như E-mail, FTP, Web,...) hoặc các dịch vụ hỗ trợ khác.

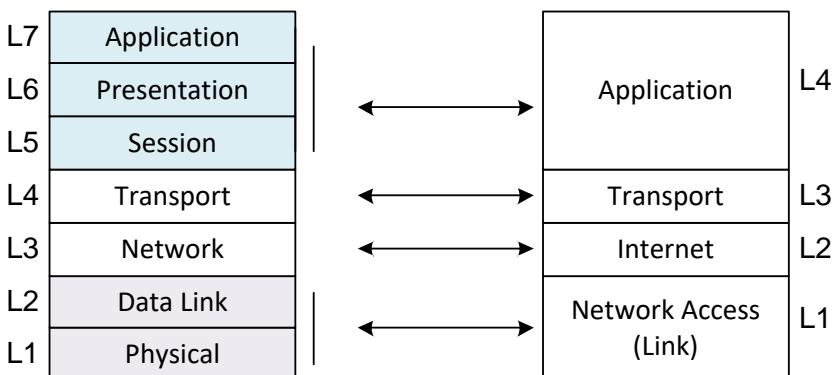
### 1.2.2. Mô hình TCP/IP

Mô hình TCP/IP gồm có 4 tầng được mô tả ở Hình 1.8. Đây là mô hình được sử dụng phổ biến ngày nay. Trong đó, hai giao thức quan trọng nhất được nhắc tới là TCP và IP.



*Hình 1.8: Mô hình TCP/IP*

Mối tương quan giữa 2 mô hình mạng:



*Hình 1.9: Mối tương quan các tầng của mô hình OSI và TCP/IP*

- **Tầng 1 - Network Access** (còn được gọi là tầng **Link** hay **Network Interface**): Bao gồm đặc điểm của 2 tầng thấp nhất của mô hình OSI là tầng Vật lý và tầng Liên kết dữ liệu. Tầng này mô tả về các **đặc điểm vật lý** của các kết nối, các cơ chế **điều khiển truy cập** và **định dạng dữ liệu** để truyền tải.
- **Tầng 2 - Internet**: **Cung cấp thông tin** về địa chỉ luận lý, tính năng định tuyến cho dữ liệu, di chuyển dữ liệu giữa tầng Link và tầng Transport. Giao thức IP được sử dụng chính ở tầng này. **Địa chỉ IP** là địa chỉ dùng để định danh cho các thiết bị trên mạng.

- **Tầng 3 - Transport:** Là tầng quan trọng trong kiến trúc TCP/IP. Tầng này **cung cấp** các dịch vụ truyền tải dữ liệu từ nguồn đến đích, liên quan đến quá trình xử lý của ứng dụng đang chạy trên mạng. Hai giao thức phổ biến được sử dụng là **TCP và UDP**.
- **Tầng 4 - Application:** **Cung cấp** các ứng dụng cho việc truyền tập tin, xử lý sự cố và các hoạt động Internet. Các giao thức tầng **Ứng dụng** cung cấp các dịch vụ cho các phần mềm ứng dụng. Ví dụ như giao thức HTTP định nghĩa cách thức làm thế nào để Web Browser có thể truy cập các nội dung của một trang Web từ một Web Server.

Như vậy, ta thấy rằng cả 2 mô hình đều được chia thành các tầng, mỗi tầng có một chức năng khác nhau, cùng phối hợp hoạt động với nhau. Một số ưu điểm quan trọng khi phân tầng ở các mô hình mạng:

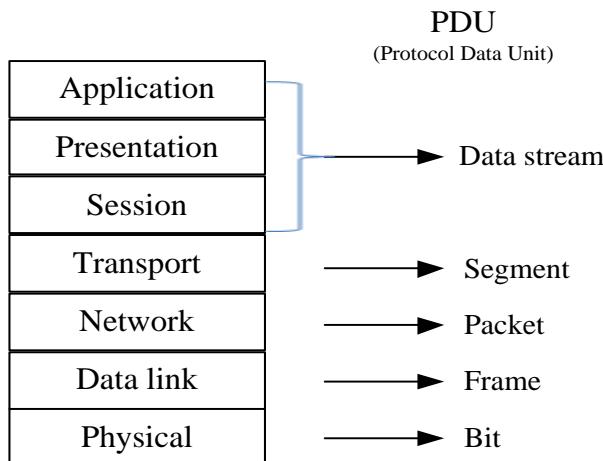
- **Giảm sự phức tạp:** Các chức năng mạng được chia nhỏ.
- **Các giao tiếp được chuẩn hóa:** Giữa mỗi tầng cho phép các nhà sản xuất tạo ra các sản phẩm có vai trò cụ thể.
- **Dễ học:** Người học có thể dễ dàng thảo luận và học về các chi tiết đặc thù của giao thức tương ứng trong các tầng của mô hình mạng.
- **Dễ phát triển:** Giảm sự phức tạp cho phép sự thay đổi chương trình dễ hơn và phát triển sản phẩm nhanh hơn.
- **Khả năng tương thích** với nhiều nhà sản xuất: Tạo ra các sản phẩm đáp ứng cùng tiêu chuẩn mạng cho phép các thiết bị từ các hãng sản xuất khác nhau có thể kết hợp hoạt động chung với nhau.
- **Module hóa:** Một nhà sản xuất có thể viết phần mềm để cài đặt cho các tầng cao (ví dụ: viết các Web Browser), các nhà sản xuất khác có thể viết phần mềm để cài đặt cho các tầng thấp hơn (ví dụ: Microsoft tích hợp TCP/IP vào hệ điều hành Windows).

**Bảng 1.1: Một số thiết bị mạng và giao thức phổ biến**

Tầng	Giao thức	Thiết bị
5-7	HTTP, FTP, SMTP, POP3, Telnet	Host, Firewall
4	TCP, UDP	Host, Firewall
3	IP	Router
2	Ethernet (IEEE 802.3)	LAN Switch, AP
1	Ethernet (IEEE 802.3), RJ45	Hub, Repeater, cáp

### Đơn vị dữ liệu ở mỗi tầng (PDU):

- Đơn vị dữ liệu ở mỗi tầng là tên gọi cho dữ liệu được xử lý ở tầng đó. Sử dụng các tên gọi này giúp cho việc diễn đạt phù hợp hơn.



**Hình 1.10: Đơn vị dữ liệu ở các tầng**

- Phản tiếp theo trình bày một số đặc điểm của tầng Transport, mối liên quan giữa tầng Application, tầng Network và tầng Transport. Nội dung này làm cơ sở để tìm hiểu kỹ hơn các nội dung khác trong chương trình học.

### Tầng Vận chuyển:

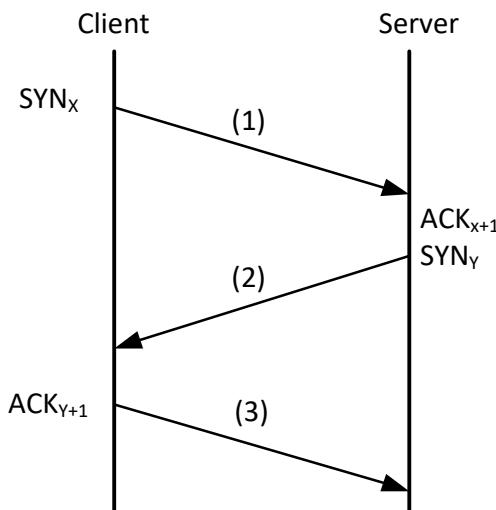
- Chức năng của tầng Vận chuyển là đảm bảo việc vận chuyển dữ liệu từ nguồn đến đích thông qua hệ thống mạng. Để thực hiện việc vận chuyển dữ liệu, ở tầng này hỗ trợ 2 cơ chế truyền dữ

liệu là **cơ chế truyền tin cậy** và **cơ chế truyền tốt nhất có thể**.  
 Bảng 1.2 trình bày một số đặc điểm để phân biệt hai cơ chế truyền này.

*Bảng 1.2: Các cơ chế truyền ở tầng Transport*

Cơ chế truyền	Tin cậy (Reliable)	Tốt nhất có thể (Best Effort)
Giao thức	TCP	UDP
Kiểu kết nối	Hướng kết nối (Connection Oriented)	Phi kết nối (Connectionless)
Gửi có báo nhận	Có	Không
Một số ứng dụng	<ul style="list-style-type: none"> <li>- E-mail</li> <li>- File Sharing</li> <li>- Downloading</li> </ul>	<ul style="list-style-type: none"> <li>- Void Streaming</li> <li>- Video Streaming</li> </ul>

- Trong cơ chế truyền tin cậy, kiểu kết nối được sử dụng là hướng kết nối, nghĩa là kênh truyền được thiết lập trước khi gửi dữ liệu đi. Thiết lập kênh truyền được thực hiện bằng kỹ thuật 3 bước bắt tay (Three Way Handshake). Hình 1.11 mô tả quá trình 3 bước bắt tay giữa Client và Server.



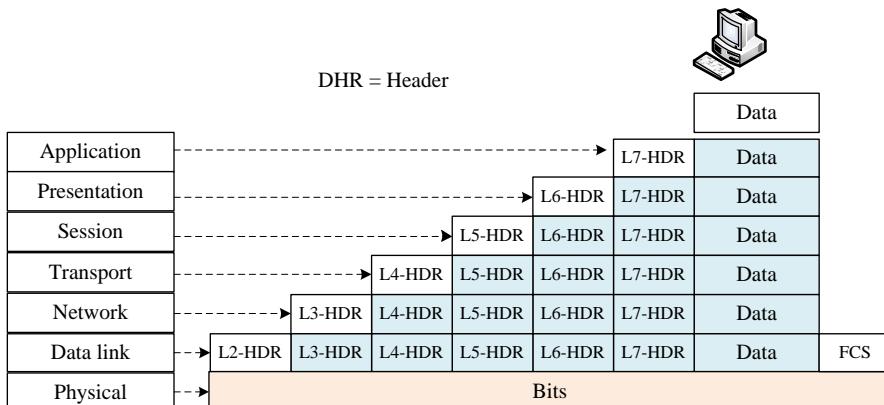
*Hình 1.11: Quá trình 3 bước bắt tay*

## Giao thức bắt tay gồm 3 bước:

- **Bước 1:** Client gửi gói tin  $SYN_X$  đến Server, với giá trị X được sinh ngẫu nhiên gọi là chỉ số tuần tự.
- **Bước 2:** Sau khi Server nhận được gói tin SYN từ Client, nó sẽ trả lời với gói  $SYN_Y + ACK_{X+1}$ . Trong đó, Y là giá trị ngẫu nhiên được sinh từ Server và giá trị X+1 của gói tin ACK là gói báo nhận cho gói SYN có giá trị ngẫu nhiên X nhận được từ Client.
- **Bước 3:** Client nhận được gói tin từ Server và gửi lại gói báo nhận ACK cho Server. Server nhận được và hoàn tất quá trình 3 bước bắt tay. Kênh truyền được thiết lập giữa Client và Server. Quá trình truyền dữ liệu bắt đầu diễn ra.

## Thông tin mô tả dữ liệu ở tầng Transport:

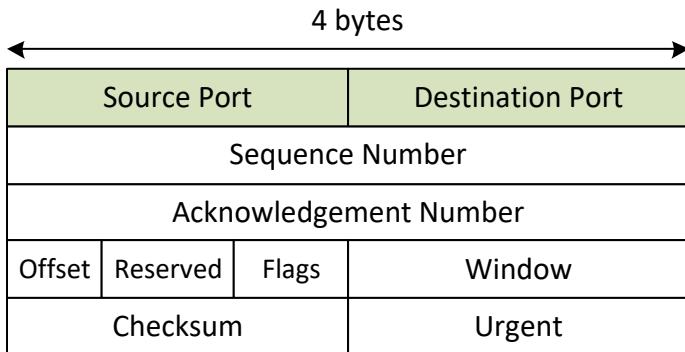
- Dữ liệu ở mỗi tầng đều chứa thông tin mô tả cho tầng đó, phần mô tả này được gọi là Header. Hiểu rõ cấu trúc tổ chức của các trường trong Header ở mỗi tầng có ý nghĩa quan trọng, giúp người học nắm vững kiến thức và vận dụng trong nhiều trường hợp như lập trình mạng hay phân tích gói tin,...



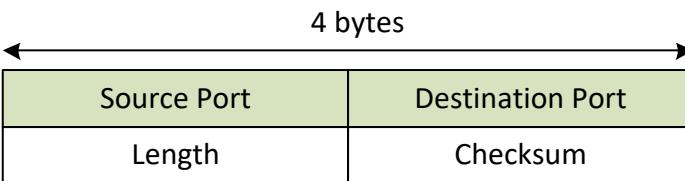
**Hình 1.12:** Mô tả dữ liệu ở các tầng trong mô hình OSI

- Trong bộ giao thức TCP/IP, tầng Transport hỗ trợ hai giao thức chính là TCP và UDP. Tương ứng cho hai giao thức này, ta có hai Header là TCP-Header và UDP-Header. Cấu trúc của TCP-

Header, UDP-Header được mô tả lần lượt trong Hình 1.13 và Hình 1.14.



**Hình 1.13: TCP Header**



**Hình 1.14: UDP Header**

- Mối liên quan giữa tầng Ứng dụng và tầng Vận chuyển thể hiện thông qua các cổng ở các ứng dụng và giao thức truyền ở tầng Vận chuyển. Một số ứng dụng quan trọng liên quan đến giao thức sử dụng ở tầng Vận chuyển cùng với cổng dịch vụ được thể hiện trong bảng sau.

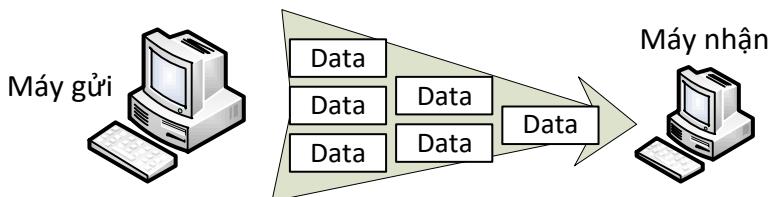
**Bảng 1.3: Mối liên hệ giữa tầng Application và Transport**

Giao thức tầng Ứng dụng	Giao thức tầng Vận chuyển	Cổng dịch vụ
HTTP	TCP	80
HTTPS	TCP	443
Telnet	TCP	23
SSH	TCP	22
SMTP	TCP	25
DHCP Server	UDP	67

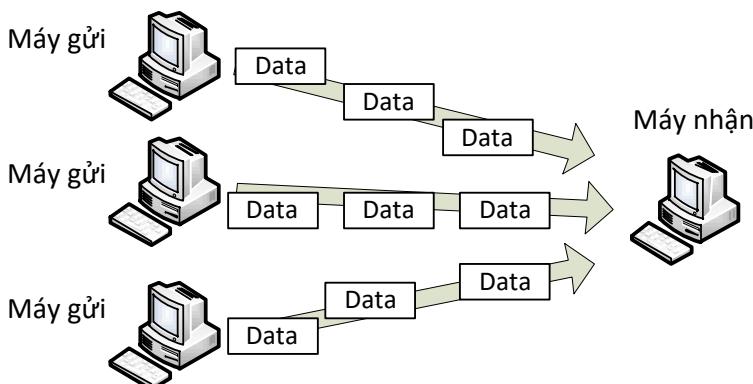
DHCP Client	UDP	68
SNMP	UDP	161
SSL	TCP	443
FTP	TCP	21
TFTP	UDP	69

### Điều khiển luồng (Flow Control):

- Trong quá trình truyền dữ liệu giữa các thiết bị trên mạng, nghẽn có thể xảy ra. Nghẽn xảy ra bởi một trong hai lý do cơ bản: (1) máy nhận có tài nguyên hạn chế, trong khi máy gửi có khả năng mạnh hơn có thể gửi một lượng lớn dữ liệu và (2) có nhiều máy gửi cùng lúc đến một máy nhận.



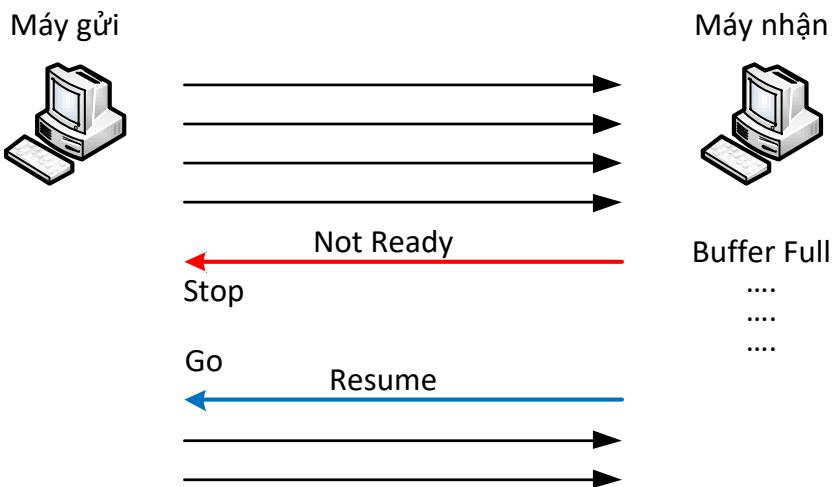
**Hình 1.15:** Máy gửi gửi một lượng dữ liệu lớn



**Hình 1.16:** Nhiều máy cùng gửi dữ liệu đến một máy

- Trong máy tính, mỗi máy đều có vùng nhớ đệm, đây là nơi khi dữ liệu nhận vào sẽ được lưu tạm trước khi xử lý. Nếu lưu lượng gửi đến nhiều, vùng nhớ đệm không còn khả năng lưu trữ, việc mất dữ liệu có thể xảy ra. Để tránh việc mất dữ liệu, trong cơ chế truyền tin cậy có hỗ trợ chức năng điều khiển luồng.

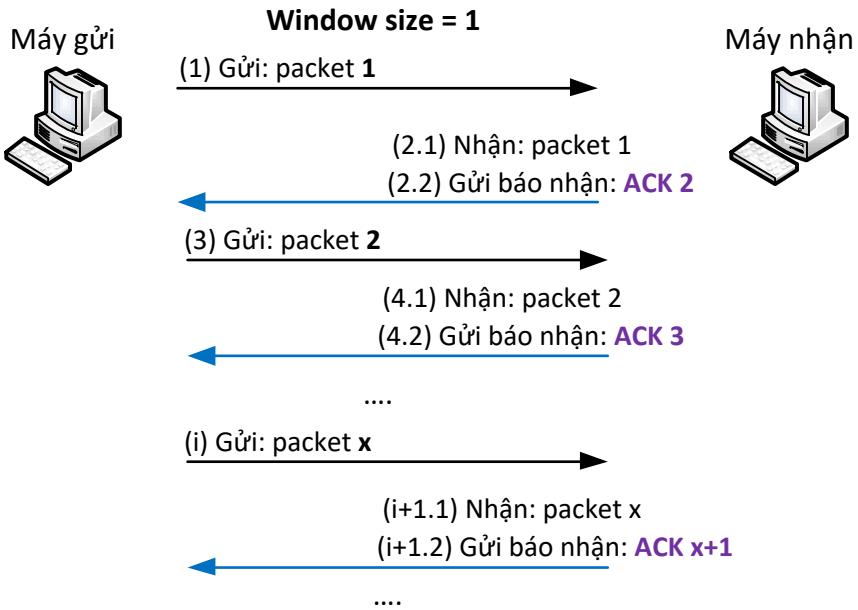
- Cơ chế này hoạt động như sau: khi vùng nhớ đệm đầy, máy nhận phát tín hiệu “Not Ready” báo hiệu dừng gửi dữ liệu. Trong lúc đó, nó sẽ tiếp tục xử lý dữ liệu trong vùng nhớ đệm. Khi vùng nhớ đệm có khả năng nhận, nó phát tín hiệu “Ready” để báo cho bên máy gửi tiếp tục gửi dữ liệu. Có thể tóm tắt quá trình này ở Hình 1.17.



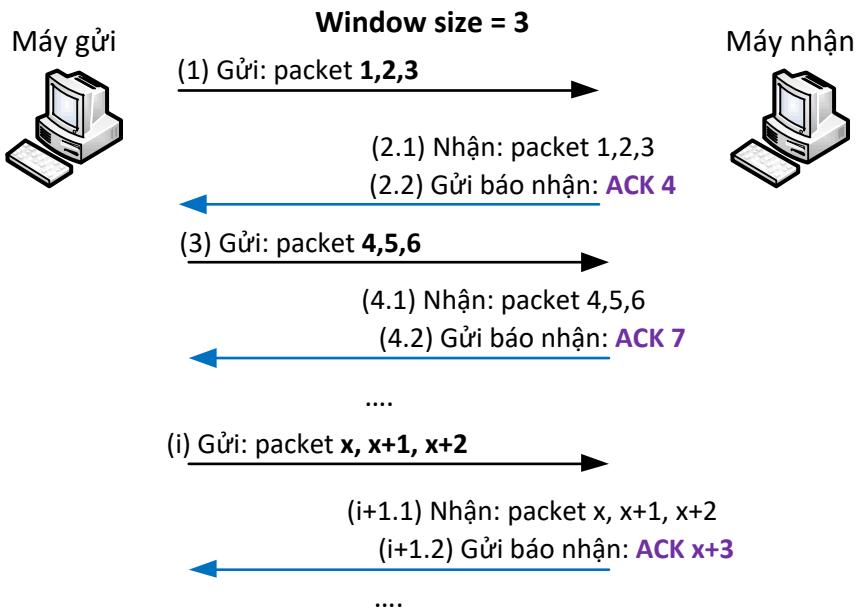
**Hình 1.17: Điều khiển luồng**

#### Window Size:

- Trong TCP Header, chúng ta thấy có trường Window Size. Trong cơ chế truyền tin cậy, các gói tin gửi đi sẽ chờ báo nhận gửi về từ máy nhận. Để việc truyền nhận đạt hiệu quả, thay vì cứ mỗi gói tin gửi đi lại chờ báo nhận gửi về, giá trị Window Size giúp xác định số lượng gói tin gửi đi trước khi chờ báo nhận gửi về.



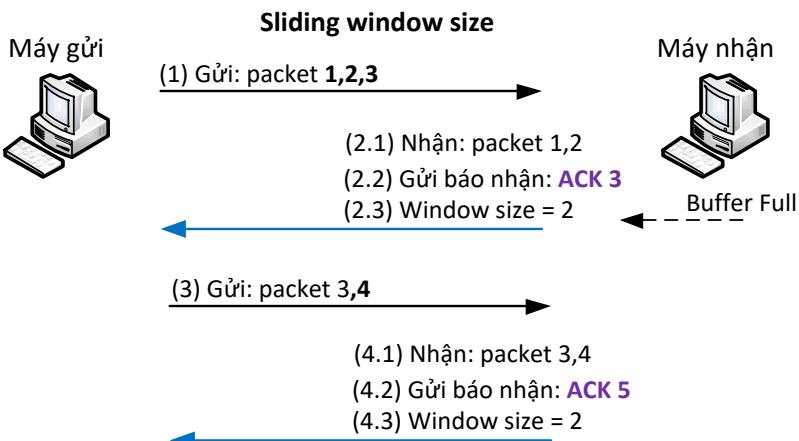
**Hình 1.18:** Window Size = 1



**Hình 1.19:** Window Size = 3

- Việc sử dụng giá trị Window Size cố định có thể gây ra nghẽn cho máy nhận vì có thể trong lúc đó máy nhận đang nhận dữ liệu

từ nhiều thiết bị khác. Để tránh tình trạng nghẽn có thể xảy ra, giá trị Window Size có thể được điều chỉnh trong suốt quá trình truyền dữ liệu giữa 2 máy.



**Hình 1.20:** Giá trị Window Size được điều chỉnh khi có nghẽn

#### Đánh số thứ tự vào các gói tin khi truyền và gói tin báo nhận:

- Trong TCP Header, trường Sequence có nhiệm vụ gắn số thứ tự vào các gói tin đối với các dữ liệu bị chia nhỏ cho phù hợp với kích thước cho phép truyền tối đa trên kênh truyền. Quá trình chia nhỏ dữ liệu diễn ra bên máy gửi. Quá trình ngược lại, gọi là quá trình tái hợp, diễn ra bên máy nhận. Quá trình tái hợp sẽ dựa vào giá trị được đánh số để lắp ghép đúng thứ tự cho luồng dữ liệu.
- Gói tin báo nhận (ACK) được sử dụng để máy nhận trả lời lại máy gửi, giá trị này được cộng thêm 1 vào số tuần tự trong trường Sequence của máy gửi, giả sử bên máy gửi có Seq = X thì gói báo nhận có giá trị X+1.

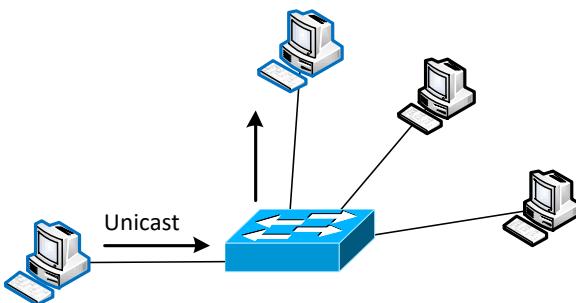
### 1.3. Quá trình vận chuyển dữ liệu qua mạng

Phân tích quá trình gói tin được vận chuyển qua mạng có ý nghĩa quan trọng trong việc hiểu được nguyên tắc hoạt động của các giao thức, các thiết bị hoạt động như thế nào. Nắm vững được vấn đề này là bước cơ bản, quan trọng đầu tiên tạo nền tảng cho việc học tập và nghiên cứu sâu hơn về lĩnh vực CNTT.

Trong phần này trình bày hai nội dung chính, thứ nhất là quá trình đóng gói bên máy gửi và mở gói bên máy nhận, thứ hai là phân tích quá trình truyền dữ liệu giữa hai máy qua mạng. Trong đó, phân tích tổng quát trình xử lý của gói tin ở thiết bị đầu cuối, qua các thiết bị mạng như Hub, Switch, Router. Các tham số được sử dụng trong phân tích được đề cập ở đây là địa chỉ IP của máy gửi ( $S_{IP}$ ), IP của máy nhận ( $D_{IP}$ ), địa chỉ MAC của máy gửi ( $S_{MAC}$ ), MAC của máy nhận ( $D_{MAC}$ ).

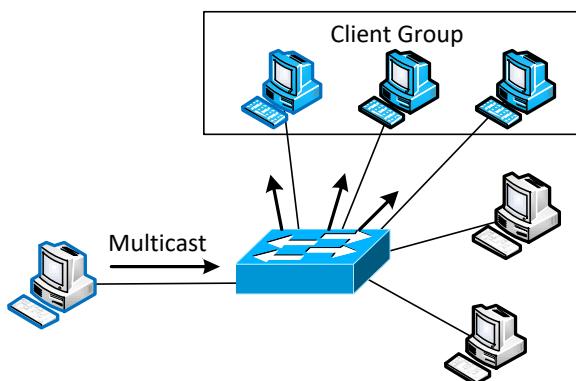
Trước tiên, chúng ta cần nắm vững về cơ chế của 3 cách truyền thông phổ biến trên mạng. Đó là truyền Unicast, Multicast và Broadcast.

- **Unicast:** Là kiểu giao tiếp trong đó dữ liệu được gửi trực tiếp từ một máy đến một máy đích (one - to - one).



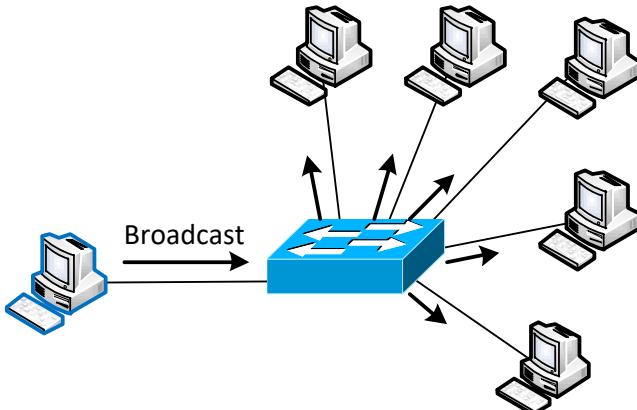
**Hình 1.21:** Truyền dữ liệu - kiểu truyền Unicast

- **Multicast:** Được thực hiện khi một máy muốn gửi gói tin cho một nhóm máy nhận (one - to - group). Trong truyền Multicast, các máy Client phải là thành viên của nhóm mới có thể nhận thông tin.



**Hình 1.22:** Truyền dữ liệu - kiểu truyền Multicast

- **Broadcast:** Là kiểu truyền trong đó gói tin được gửi từ một máy đến tất cả các máy khác trong mạng, các máy khác này nằm trong cùng miền quảng bá (one - to - all).



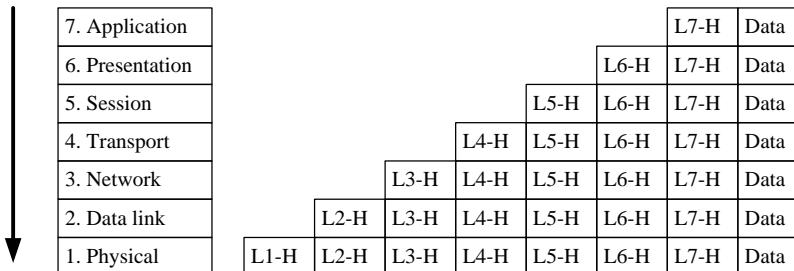
**Hình 1.23: Truyền dữ liệu - kiểu truyền Broadcast**

### 1.3.1. Quá trình đóng gói và mở gói dữ liệu

#### 1.3.1.1. Quá trình đóng gói dữ liệu

Quá trình đóng gói dữ liệu diễn ra bên máy gửi. Dữ liệu xuất phát từ tầng Úng dụng được đóng gói và chuyển xuống các tầng kế tiếp, đến mỗi tầng dữ liệu được **gắn thêm** thông tin mô tả của tầng tương ứng gọi là Header. Khi dữ liệu đến tầng Transport, tại đây diễn ra quá trình chia nhỏ gói tin nếu kích thước dữ liệu **lớn hơn** so với kích thước truyền tối đa cho phép. Khi dữ liệu đến tầng Network, mỗi gói tin sẽ **gắn thêm** thông tin tương ứng ở tầng này gọi là “IP Header”, trong đó chứa thông tin quan trọng là địa chỉ IP nguồn và IP đích, các địa chỉ này được sử dụng trong quá trình định tuyến. Dữ liệu đến tầng Data Link sẽ **gắn thêm** thông tin mô tả tầng này gọi là “Frame Header”, trong đó chứa thông tin về địa chỉ MAC nguồn và MAC đích. Trường hợp địa chỉ MAC đích chưa xác định được, máy tính sẽ dùng giao thức ARP để xác định giá trị này. Sau đó, dữ liệu được chuyển xuống tầng Physical, chuyển thành các tín hiệu nhị phân để truyền đi.

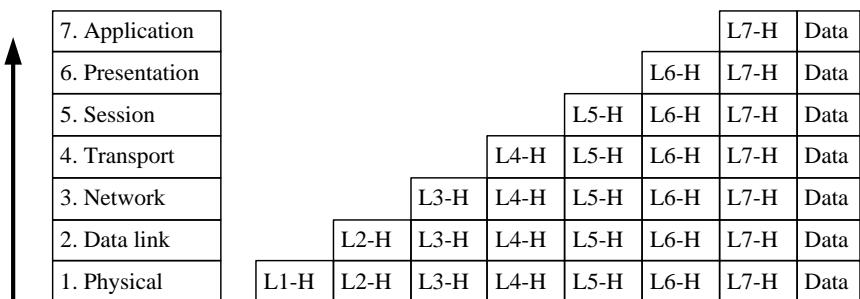
Máy gửi



**Hình 1.24:** Quá trình đóng gói dữ liệu

### 1.3.1.2. Quá trình mở gói dữ liệu

Máy nhận



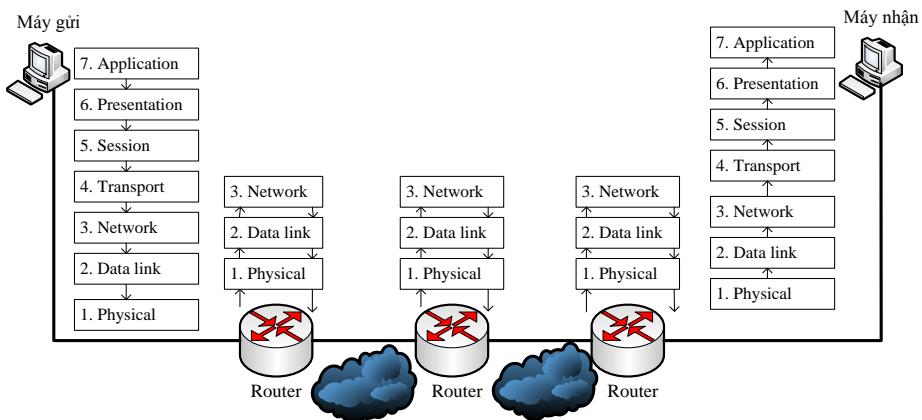
**Hình 1.25:** Quá trình mở gói dữ liệu

Quá trình mở gói dữ liệu diễn ra bên máy nhận. Nguyên tắc chung là các Header sẽ được mở và xử lý ở các tầng tương ứng. Khi máy đích nhận được một dãy các bit, dữ liệu được xử lý bởi quá trình mở gói như sau: tầng Physical nhận dữ liệu vào ở dạng các bit, các bit được cấu trúc lại ở dạng Frame ở **tầng Data Link**, kiểm tra Trailer (Trailer) để xem dữ liệu có bị lỗi hay không. Frame có thể bị loại bỏ hoặc yêu cầu để được truyền lại. Nếu dữ liệu không bị lỗi, tầng Data Link đọc và thông dịch thông tin điều khiển trong tầng 2. Tầng Data Link gỡ bỏ Header và Trailer, sau đó gửi phần dữ liệu còn lại lên tầng trên. Ở tầng Network, IP-Header được xử lý. Quá trình **tái hợp** dữ liệu được thực hiện ở tầng Transport. Cứ như

vậy, dữ liệu được chuyển lên, các Header được xử lý và gỡ bỏ ở các tầng tương ứng.

### 1.3.2. Phân tích quá trình vận chuyển dữ liệu

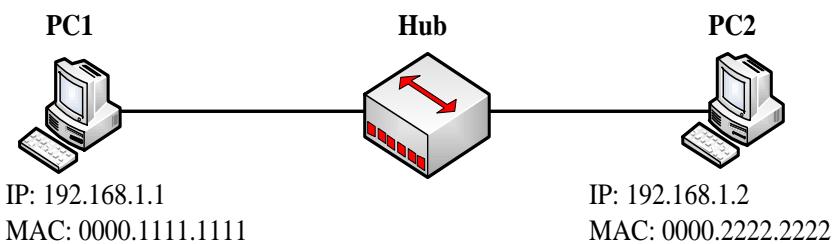
Chúng ta biết rằng địa chỉ IP là địa chỉ dùng để định danh cho các đối tượng (gọi là các Host) trên mạng. Do đó, để có thể trao đổi thông tin thì máy tính nguồn cần phải biết địa chỉ IP của máy tính đích.



**Hình 1.26:** Quá trình vận chuyển dữ liệu qua mạng

Để hiểu rõ hơn về cơ chế vận chuyển dữ liệu qua mạng giữa các thiết bị đầu cuối, trong phần này trình bày 3 trường hợp cơ bản và xét các thông tin địa chỉ từ tầng Network trở xuống.

**Trường hợp 1.** Hai máy tính kết nối trực tiếp hoặc kết nối qua Hub.



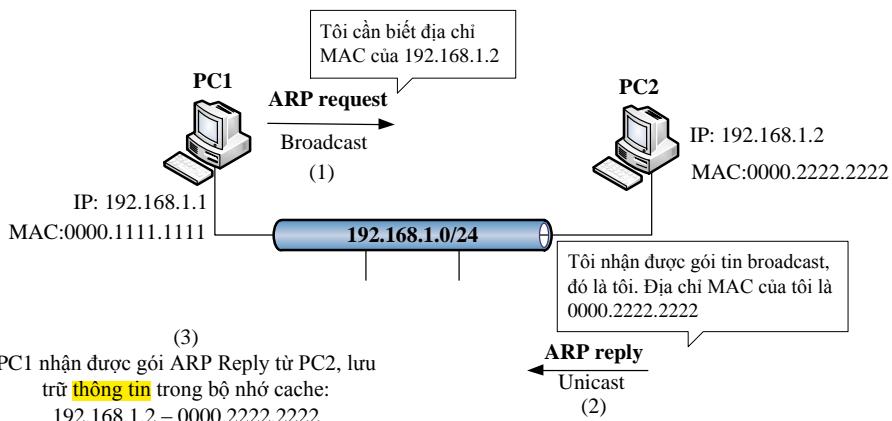
**Hình 1.27:** Hai máy kết nối qua Hub

Xem xét các thông số địa chỉ khi PC1 gửi dữ liệu cho PC2.

- L3:  $S_{IP} = 192.168.1.1$ ;  $D_{IP} = 192.168.1.2$
- L2:  $S_{MAC} = 0000.1111.1111$ ;  $D_{MAC} = ?$

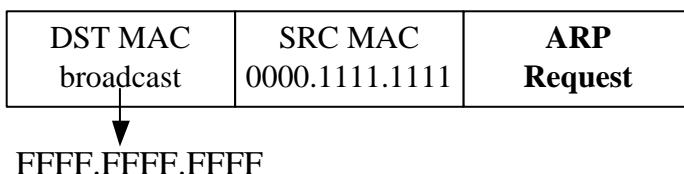
Vấn đề đặt ra: Xác định địa chỉ D<sub>MAC</sub> của PC2.

Trong trường hợp này, hai máy tính nằm cùng một miền quảng bá, giao thức được sử dụng để xác định địa chỉ MAC của PC2 là ARP. ARP là giao thức được sử dụng để ánh xạ địa chỉ MAC của một thiết bị khi biết IP của thiết bị đó trong một miền quảng bá. Hoạt động của giao thức ARP được mô tả trên Hình 1.28.



**Hình 1.28: Hoạt động của giao thức ARP**

Trở lại với trường hợp chúng ta đang xem xét, PC1 cần xác định địa chỉ MAC của PC2. PC1 sử dụng ARP Request để tìm MAC của PC2 có IP là 192.168.1.2. Đây là gói tin Broadcast, có nội dung là muốn xác định PC có IP: 192.168.1.2 có địa chỉ MAC là bao nhiêu. Cấu trúc của gói tin này được mô tả ở Hình 1.29.



**Hình 1.29: Gói tin ARP Request**

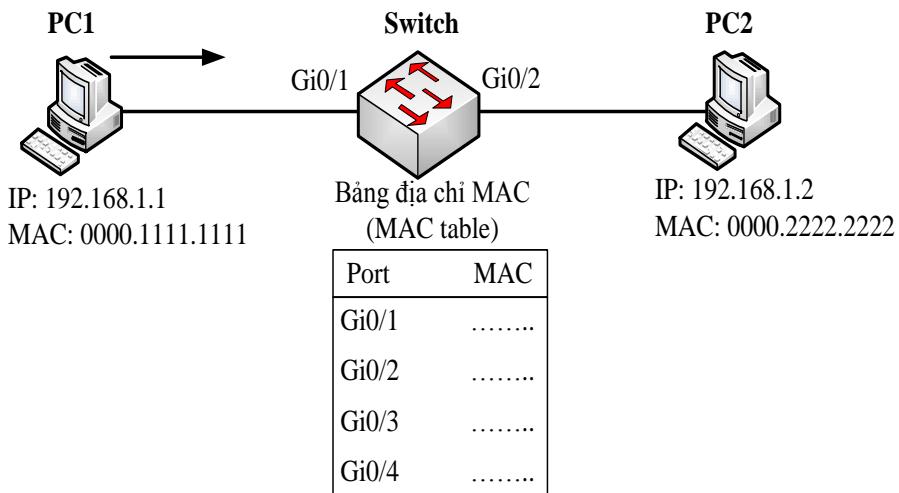
Gói tin ARP Request xuất phát từ PC1, đi đến Hub. Hub sẽ gửi ra tất cả các Port của nó. Tất cả các PC trong mạng đều nhận được Frame này. Chỉ PC2 mới xử lý và trả lời vì trong nội dung của Frame hỏi có chứa địa chỉ là IP của PC2. Gói tin trả lời ARP Reply từ PC2 có cấu trúc như ở Hình 1.30.

DST MAC	SRC MAC	ARP Reply
0000.1111.1111	0000.2222.2222	

**Hình 1.30:** Gói tin ARP Reply

Gói ARP Reply từ PC2 gửi đến Hub và Hub gửi ra tất cả các Port của nó, lúc này PC1 nhận được và lưu vào vùng nhớ đệm thông tin ánh xạ giữa IP: 192.168.1.2 và MAC: 0000.2222.2222 (gọi là **ARP Cache**).

**Trường hợp 2.** Hai máy tính kết nối qua Switch (thiết bị ở Layer 2).



**Hình 1.31:** Hai máy kết nối qua Switch

Xem xét các thông số địa chỉ khi PC1 gửi dữ liệu cho PC2.

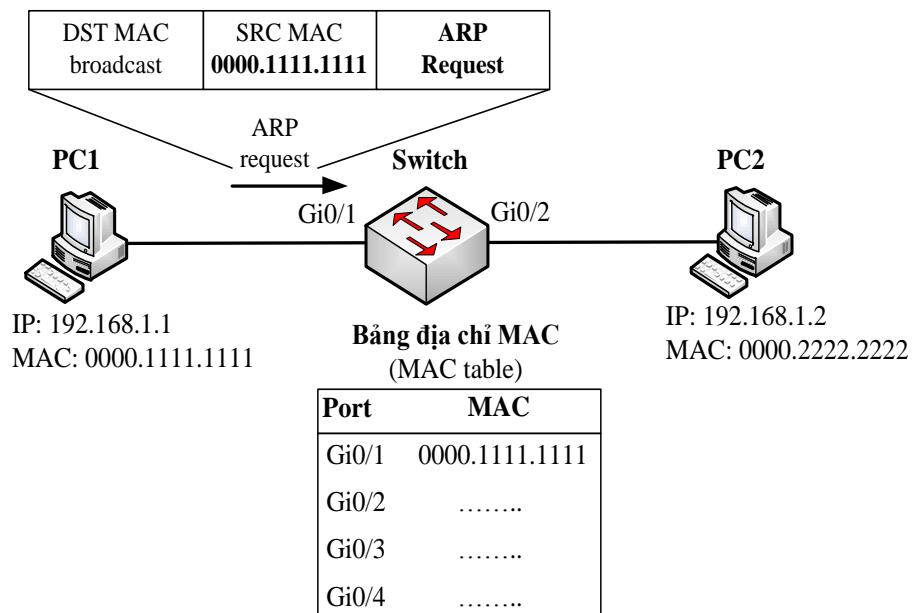
- L3:  $S_{IP} = 192.168.1.1$ ;  $D_{IP} = 192.168.1.2$
- L2:  $S_{MAC} = 0000.1111.1111$ ;  $D_{MAC} = ?$

Vấn đề đặt ra: Xác định địa chỉ  $D_{MAC}$  của PC2.

Trong trường hợp này, cả hai PC đều thuộc cùng một miền Broadcast (gọi là cùng mạng). Do đó, để xác định giá trị  $D_{MAC}$ , PC1 cũng sử dụng giao thức ARP tương tự như trường hợp 1. Tuy nhiên, ở đây chúng ta sẽ phân tích để nắm rõ thêm quá trình học để tạo bảng địa chỉ MAC của Switch.

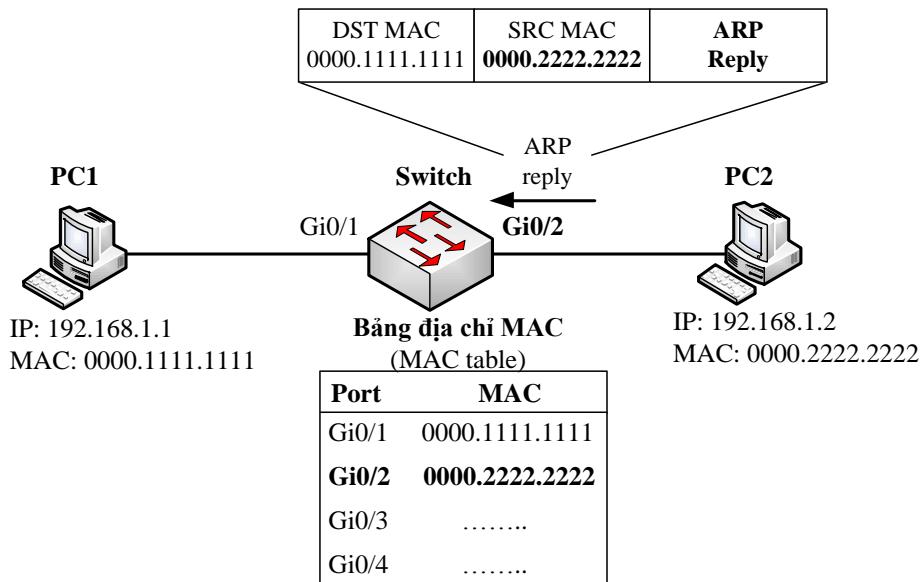
Nguyên tắc học địa chỉ MAC của Switch: Switch học địa chỉ  $S_{MAC}$  trong Frame gửi tới nó. Nghĩa là Switch **dựa vào** cổng nhận Frame và  $S_{MAC}$  trong Frame để lưu vào bảng địa chỉ MAC của nó.

Xét gói tin ARP Request xuất phát từ PC1 đến Switch, Switch nhận Frame này vào ở Port Gi0/1. Switch đọc  $S_{MAC}$  trong Frame này mà gán thông tin địa chỉ MAC này tương ứng với Port Gi0/1 trong bảng địa chỉ MAC.



**Hình 1.32:** Swich học địa chỉ MAC từ gói tin ARP Request

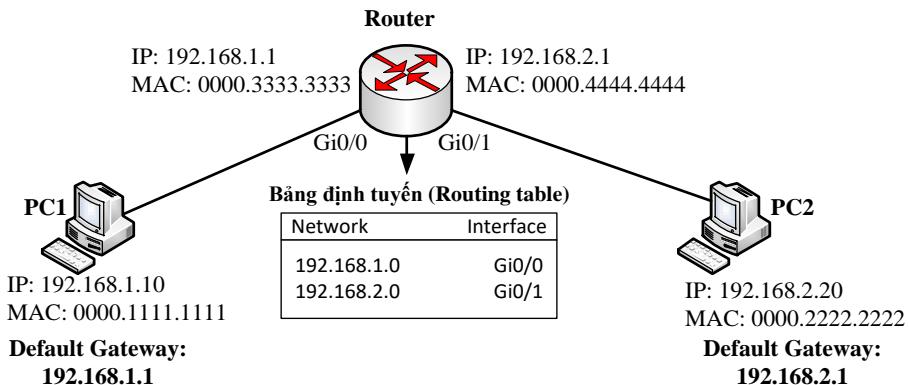
Switch nhận gói ARP Request và đọc địa chỉ  $D_{MAC}$  là địa chỉ Broadcast nên Switch sẽ gửi Frame này ra tất cả các cổng của nó trừ cổng nhận Frame này vào. Tương tự như trường hợp 1, chỉ có PC2 mới trả lời (ARP Reply). Switch nhận được gói tin ARP Reply ở Port Gi0/2, học địa chỉ MAC nguồn và điền thông tin tương ứng với Port Gi0/2 vào bảng địa chỉ MAC.



**Hình 1.33:** Swich học địa chỉ MAC từ gói tin ARP Reply

Dựa vào D<sub>MAC</sub> trong gói tin ARP Reply và bảng địa chỉ MAC, Switch chuyển tiếp gói tin ARP Reply qua cổng Gi0/1 để đến PC1. Khi đó, PC1 có được thông tin địa chỉ MAC của PC2 và lưu trữ thông tin ánh xạ giữa IP và MAC của PC2.

**Trường hợp 3.** Hai máy tính kết nối qua Router (thiết bị ở Layer 3).



**Hình 1.34:** Hai máy kết nối qua Router

Hai PC giao tiếp với nhau trong trường hợp này thuộc 2 miền Broadcast khác nhau (gọi là khac mạng) được kết nối qua Router. Router đóng vai trò là thiết bị định tuyến, giúp chuyển tiếp các gói tin. Router

dựa vào địa chỉ IP đích của gói tin nhận vào và bảng định tuyến để xác định đường đi và chuyển tiếp gói tin qua cổng tương ứng.

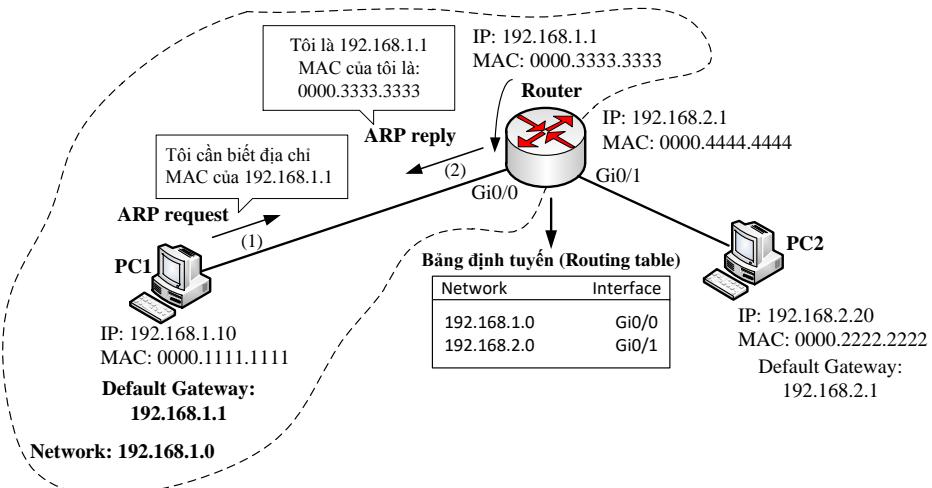
Trong trường hợp này, chúng ta chú ý rằng trong cấu hình tham số địa chỉ cho các PC cần xác định giá trị Default Gateway. Default Gateway ở đây là địa chỉ IP của cổng Router kết nối trực tiếp với mạng của PC đang xét. Máy tính nguồn có thể giao tiếp trực tiếp với máy tính đích nếu 2 máy tính cùng một mạng. Nếu 2 máy khác mạng, máy tính bên gửi phải gửi dữ liệu đến Router, thông qua giá trị được xác định là Default Gateway, làm nhiệm vụ chuyển tiếp dữ liệu đến đích. Chúng ta sẽ xem xét ý nghĩa và sự cần thiết của tham số này trong quá trình phân tích gói tin trao đổi giữa PC1 và PC2.

Tương tự các trường hợp 1 và 2, xét PC1 muốn gửi dữ liệu cho PC2. Các tham số địa chỉ khi PC1 gửi dữ liệu cho PC2 như sau:

- L3:  $S_{IP} = 192.168.1.10$ ;  $D_{IP} = 192.168.2.20$
- L2:  $S_{MAC} = 0000.1111.1111$ ;  $D_{MAC} = ?$

Vấn đề đặt ra: Xác định địa chỉ  $D_{MAC}$  của PC2.

Ta thấy rằng 2 PC ở khác miền Broadcast. Do đó, PC1 không thể sử dụng ARP Request để tìm địa chỉ MAC của PC2. Router là thiết bị ngăn các tín hiệu Broadcast, nên gói tin ARP Request từ PC1 sẽ bị Router ngăn không cho gửi vào vùng Broadcast của PC2. Để xác định thông tin  $D_{MAC}$  còn thiếu ở trên, PC1 sẽ kiểm tra giá trị của Default Gateway trong thông tin cấu hình Card mạng của nó. Nếu không có giá trị ở tham số này, PC1 sẽ không thể tiến hành các bước tiếp theo để gửi dữ liệu cho PC2. Trong trường hợp tham số Default Gateway đã được cấu hình, PC1 sẽ sử dụng ARP Request để lấy địa chỉ MAC của thiết bị có IP này và điền vào giá trị  $D_{MAC}$  còn thiếu ở trên.



**Hình 1.35:** Các thông số ARP Request và ARP Reply ở máy gửi

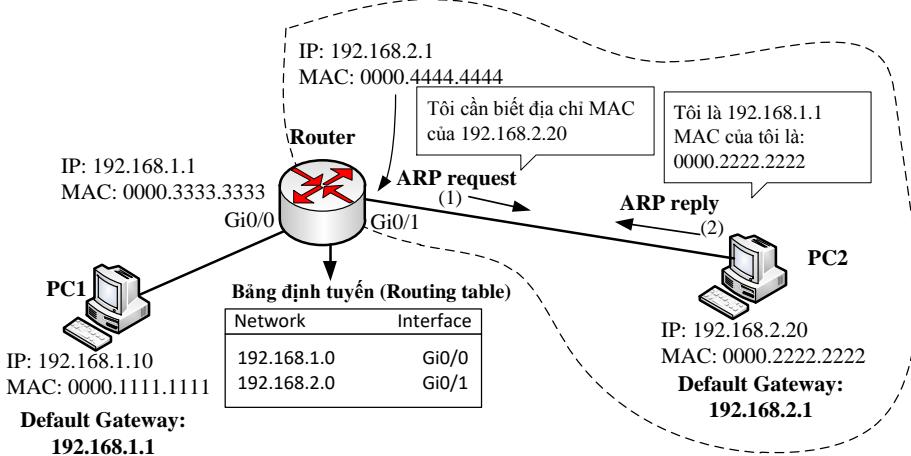
Lúc này, các thông số địa chỉ của PC1 như sau:

- L3:  $S_{IP} = 192.168.1.10; D_{IP} = 192.168.2.20$
- L2:  $S_{MAC} = 0000.1111.1111; D_{MAC} = 0000.3333.3333$

Khi gói tin ARP Request từ PC1 gửi ra, Router sẽ nhận được. Ở Layer 2, Router nhận thấy rằng địa chỉ MAC đích của Frame này là địa chỉ của nó. Nó tiếp tục đưa lên Layer 3 để mở gói và xử lý. Trong IP Header, Router thấy rằng địa chỉ IP đích của gói tin **không phải** của nó. Dựa vào địa chỉ IP đích này và bảng định tuyến, Router xác định gửi qua cổng Gi0/1 của nó để chuyển tiếp gói tin đi. Trước khi chuyển đi, Router tiến hành đóng gói dữ liệu, **chuyển gói tin xuống** Layer 2, thay đổi địa chỉ  $S_{MAC}$  và  $D_{MAC}$ . Các tham số địa chỉ bây giờ sẽ là:

- L3:  $S_{IP} = 192.168.1.10; D_{IP} = 192.168.2.20$
- L2:  $S_{MAC} = 0000.4444.4444; D_{MAC} = ?$

Router **xác định** được rằng địa chỉ IP đích và địa chỉ cổng Gi0/1 của nó cùng mạng (cùng miền Broadcast). Do đó, Router sử dụng giao thức ARP để tìm  $D_{MAC}$  của PC2. Lúc này Router biết được giá trị của  $D_{MAC} = 0000.2222.2222$  để điền thông tin và lưu trữ trong ARP Cache và chuyển tiếp gói tin đến PC2.



**Hình 1.36:** Các thông số ARP Request và ARP Reply ở máy nhận

## 1.4. Tổng kết chương

Trong chương này trình bày một số khái niệm cơ bản về mạng máy tính, phân loại các mạng máy tính phổ biến. Hai mô hình mạng quan trọng được trình bày là OSI và TCP/IP. Hai mô hình này có đặc điểm chung là phân chia thành các tầng, mỗi tầng đảm nhiệm các chức năng khác nhau. Đơn vị dữ liệu ở tầng Ứng dụng gọi là “Data”, ở tầng Vận chuyển gọi là “Segment”, ở tầng Mạng gọi là “Packet” và ở tầng Liên kết gọi là “Frame”.

Quá trình đóng gói dữ liệu diễn ra bên máy gửi và quá trình mở gói diễn ra bên máy nhận. Trong quá trình đóng gói, dữ liệu từ tầng Ứng dụng được chuyển xuống các tầng thấp hơn và thông tin ở mỗi tầng đó được thêm vào. Quá trình mở gói diễn ra ngược lại với quá trình đóng gói.

## 1.5. Câu hỏi và bài tập

- Câu nào sau đây mô tả thứ tự đúng của các tầng trong mô hình tham chiếu OSI?
  - Application, Transport, Session, Presentation, Network, Data Link, Physical.
  - Presentation, Application, Session, Transport, Network, Data Link, Physical.

- C. Application, Presentation, Session, Transport, Network, Data Link, Physical.
  - D. Application, Presentation, Transport, Network, Session, Data Link, Physical.
2. Trong mô hình OSI, “segment” là đơn vị dữ liệu (PDU) của tầng nào?
- A. Transport.
  - B. Network.
  - C. Application.
  - D. Data Link.
3. Thông tin nào sau đây được thêm vào bảng địa chỉ MAC khi Switch nhận được một Frame gửi tới?
- A. Địa chỉ MAC đích trong Frame và cổng nhận dữ liệu vào.
  - B. Địa chỉ MAC nguồn trong Frame và cổng nhận dữ liệu vào.
  - C. Địa chỉ MAC đích trong Frame và cổng chuyển dữ liệu ra.
  - D. Địa chỉ MAC nguồn trong Frame và cổng chuyển dữ liệu ra.
4. Câu nào sau đây là mô tả đúng khi Switch nhận vào gói tin ARP Request?
- A. Địa chỉ MAC nguồn trong Frame là FF-FF-FF-FF-FF-FF.
  - B. Địa chỉ MAC đích trong Frame là FF-FF-FF-FF-FF-FF.
  - C. Switch chỉ chuyển tiếp gói ARP Request đến cổng kết nối với máy đích.
  - D. Switch sẽ trực tiếp trả lời gói ARP Reply.
5. Hai tầng con (Sublayer) trong tầng Data Link của mô hình OSI là?
- A. Internet.
  - B. Physical.
  - C. LLC.
  - D. Transport.
  - E. MAC.
  - F. Network Access.

6. Câu nào sau đây mô tả về giá trị Default Gateway được thiết lập trên máy tính?
- A. Là địa chỉ IP của một cổng của Router cùng mạng với máy tính này.
  - B. Là địa chỉ MAC của cổng trên Switch kết nối với máy tính này.
  - C. Là địa chỉ MAC của cổng trên Router cùng mạng với máy tính này.
  - D. Là địa chỉ IP đặt trên cổng của Switch kết nối với Router.
7. Kiểu truyền dữ liệu nào gửi một thông điệp đến tất cả các thiết bị trong một mạng?
- A. Broadcast.
  - B. Multicast.
  - C. Unicast.
  - D. Allcast.
8. Kích thước nhỏ nhất của IPv4 Header là?
- A. 10 byte.
  - B. 16 byte.
  - C. 20 byte.
  - D. 32 byte.
9. Câu nào sau đây mô tả thứ tự đúng của dữ liệu được đóng gói?
- A. User Datagrams, Packets, Segments, Frames, Bits.
  - B. User Datagrams, Sessions, Segments, Packets, Frames, Bits.
  - C. User Datagrams, Segments, Packets, Frames, Bits.
  - D. Bits, Frames, Sessions, Packets, User Datagrams.
10. Dịch vụ HTTP ở tầng Ứng dụng sử dụng cơ chế truyền nào ở tầng Vận chuyển?
- A. Reliable.
  - B. Best Effort.
  - C. Half Duplex.
  - D. Full Duplex.

11. Những câu nào sau đây là mô tả đúng cho kiểu kết nối tin cậy trong quá trình truyền dữ liệu?
- A. Là quá trình gửi dữ liệu có báo nhận.
  - B. Khi buffer đầy, dữ liệu sẽ bị loại bỏ và không được truyền lại.
  - C. Giá trị Windows Size được sử dụng để điều khiển số lượng dữ liệu truyền đi trước khi chờ báo nhận gửi về.
  - D. Nếu hết thời gian chờ trong việc truyền gói tin thì máy gửi sẽ ngắt kết nối với máy nhận.
  - E. Máy nhận chờ gói tin báo nhận từ máy gửi trước khi yêu cầu dữ liệu gửi tiếp theo.
12. Địa chỉ MAC có bao nhiêu bit?
- A. 32 bit.
  - B. 48 bit.
  - C. 56 bit.
  - D. 64 bit.
13. Điều gì được yêu cầu phải thực hiện trước khi TCP bắt đầu gửi các segment?
- A. Three-way handshake.
  - B. Chỉ số Port được thống nhất trước giữa máy gửi và máy nhận.
  - C. Đánh số tuần tự vào các segment.
  - D. Chỉ số báo nhận của các segment.
14. Câu nào sau đây mô tả đúng nhất về chức năng của Switch Layer 2?
- A. Chuyển tiếp dữ liệu dựa vào địa chỉ IP.
  - B. Khuếch đại và tái sinh tín hiệu điện để gửi ra tất cả các Port của nó.
  - C. Học địa chỉ MAC bằng cách xem xét các địa chỉ MAC đích trong Frame gửi tới nó.
  - D. Xác định các Port để chuyển tiếp dữ liệu dựa vào địa chỉ MAC đích và bảng địa chỉ MAC của nó.

15. E-mail và FTP hoạt động ở Layer nào trong mô hình OSI?
- A. Layer 3.
  - B. Layer 4.
  - C. Layer 5.
  - D. Layer 7.
16. Các thiết bị mạng nào sau đây hoạt động ở Layer Data Link?
- A. Hub.
  - B. Switch.
  - C. Router.
  - D. Repeater.
17. Layer nào trong mô hình OSI đảm nhận vai trò nén (encryption) và giải nén (decryption) dữ liệu?
- A. Network.
  - B. Presentation.
  - C. Session.
  - D. Physical.
18. Layer nào trong mô hình OSI đảm nhận vai trò thiết lập các kết nối tin cậy?
- A. Network.
  - B. Session.
  - C. Transport.
  - D. Data Link.
19. Những thiết bị nào sau đây hoạt động ở Layer Network trong mô hình OSI?
- A. Router.
  - B. Repeater.
  - C. Hub.
  - D. Switch.

20. Điều nào sau đây là ưu điểm quan trọng nhất khi triển khai mô hình mạng dạng Full Mesh?
- A. Tăng băng thông cho hệ thống.
  - B. Tăng khả năng dự phòng cho hệ thống.
  - C. Giảm số lượng Switch cho toàn bộ hệ thống.
  - D. Tăng độ phức tạp cho hệ thống.
  - E. Tăng chi phí đầu tư cho hệ thống.

## CHƯƠNG 2

### MẠNG LAN VÀ WLAN

Chương này trình bày một số đặc điểm, các chuẩn, các giao thức phổ biến dùng trong LAN, WLAN. Học xong chương này, người học có khả năng:

- Trình bày được đặc điểm của mạng LAN, WLAN.
- Trình bày được đặc điểm của chuẩn Ethernet.
- Phân biệt được các chuẩn phổ biến trên mạng Wifi.
- Vận dụng các kiến thức về mạng LAN, WLAN trong việc phân tích các vấn đề căn bản xảy ra trong mạng nội bộ.

#### **2.1. Giới thiệu**

Mạng máy tính của các tổ chức, doanh nghiệp ngày nay thông thường được tổ chức thành 2 loại phổ biến là LAN và WAN. Mạng LAN kết nối các thiết bị gần nhau như các thiết bị trong cùng một phòng, cùng một tòa nhà hay giữa các tòa nhà của một tổ chức, doanh nghiệp ở một vị trí địa lý xác định nào đó. Mạng WAN kết nối các LAN của một tổ chức, doanh nghiệp lại với nhau. Các LAN này nằm ở các vị trí địa lý khác nhau. Hay nói cách khác, mạng WAN kết nối các chi nhánh của cùng một tổ chức, doanh nghiệp lại với nhau. Để kết nối mạng giữa các chi nhánh này phải thông qua môi trường mạng của các nhà cung cấp dịch vụ Internet (ISP).

Có nhiều loại mạng LAN, phổ biến ngày nay được đề cập đến là mạng Ethernet LAN và WLAN. Mạng Ethernet LAN sử dụng dây cáp để kết nối các thiết bị với nhau. Mạng WLAN không sử dụng dây cáp mà sử dụng sóng để kết nối các thiết bị với nhau. Mạng WLAN được xem như là sự mở rộng của mạng có dây trong hệ thống mạng nội bộ của một tổ chức, doanh nghiệp.

##### **2.1.1. Một số khái niệm**

###### **Miền đụng độ**

Đụng độ có khả năng xảy ra khi có hai hay nhiều máy truyền dữ liệu đồng thời trong một thời điểm trong môi trường mạng chia sẻ. Khi

đụng độ xảy ra, các gói tin đang được truyền đều bị phá hủy, các máy đang truyền sẽ dừng việc truyền dữ liệu và chờ một khoảng thời gian ngẫu nhiên theo quy luật của CSMA/CD đối với mạng có dây. Trong trường hợp mạng không dây, thuật toán CSMA/CA được sử dụng để tránh đụng độ xảy ra trong môi trường này. Nếu đụng độ xảy ra quá nhiều, mạng có thể không hoạt động được. Miền đụng độ (Collision Domain) là khu vực mà trong đó các thiết bị trao đổi thông tin có thể xảy ra đụng độ.

### **Miền quảng bá**

Miền quảng bá (Broadcast Domain) là khu vực bao gồm tất cả các thiết bị có thể nhận được gói tin quảng bá từ một thiết bị nào đó. Khi một thiết bị muốn gửi một gói quảng bá thì địa chỉ MAC đích của gói tin đó sẽ là FF:FF:FF:FF:FF:FF. Với địa chỉ như vậy, mọi thiết bị trong miền này đều nhận và xử lý gói tin này.

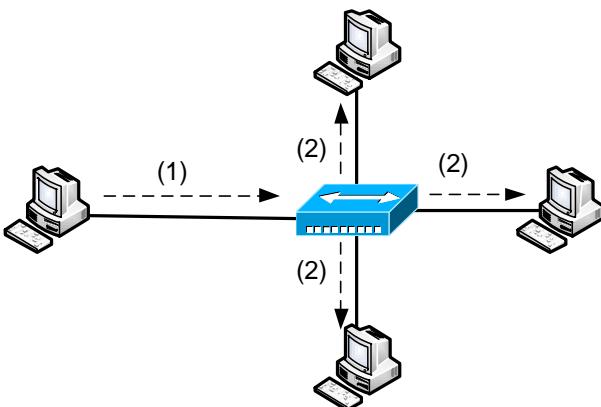
#### **2.1.2. Các thiết bị mạng**

Các thiết bị mạng thường dùng trong LAN, WLAN gồm: Hub, Switch, Router, Access Point. Ngoài ra, một số hệ thống còn trang bị các thiết bị bảo mật như Firewall, IPS, SIEM, WAF,... Trong phần này trình bày một số đặc điểm chính của 3 thiết bị phổ biến là Hub, Switch và Router.

##### **2.1.2.1. Hub**

Hub là thiết bị mạng hoạt động ở tầng Physical trong mô hình OSI, có vai trò là thiết bị tập trung trong mạng kết nối hình sao. Nhìn vào bề ngoài, ta thấy rằng giữa Hub và Switch có vẻ giống nhau và có vai trò như nhau. Cả hai thiết bị này đều được dùng phổ biến để kết nối các thiết bị trong mạng LAN.

Hub chuyển tiếp dữ liệu trong mạng ở tầng Vật lý. Do đó, Hub chỉ có thể xử lý các tín hiệu bit chứ không thể nhìn vào các giá trị S<sub>MAC</sub>, D<sub>MAC</sub> trong Frame ở Layer 2. Khi nhận được tín hiệu đầu vào từ một cổng, nó sẽ khuếch đại và tái sinh tín hiệu để truyền đi ra tất cả các cổng trừ cổng nhận tín hiệu vào. Hub được xem là Repeater có nhiều cổng.



**Hình 2.1: Truyền dữ liệu qua Hub**

Các thiết bị kết nối vào Hub nằm cùng một miền dung độ. Nghĩa là, nếu trong một thời điểm có 2 hoặc nhiều hơn các thiết bị cùng truyền dữ liệu một lúc thì dung độ xảy ra. Để giải quyết vấn đề dung độ các thiết bị sử dụng thuật toán CSMA/CD.

### 2.1.2.2. Switch

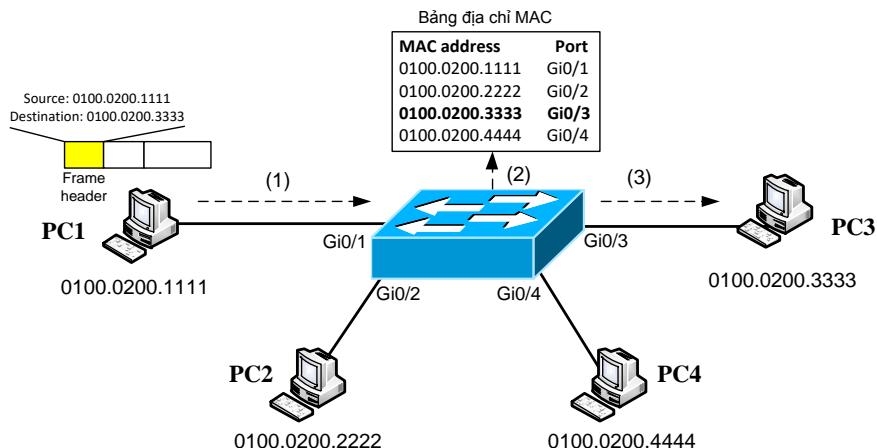
Switch là thiết bị hoạt động ở tầng Liên kết dữ liệu, xử lý dữ liệu dạng Frame. Môi trường trên Switch không xảy ra dung độ, mỗi cổng của nó là một miền dung độ. Khi Switch nhận được gói tin quảng bá thì nó sẽ gửi ra tất cả các cổng trừ cổng nhận gói tin vào. Mỗi thiết bị nhận được gói quảng bá đều phải xử lý thông tin nằm trong đó. Gói tin quảng bá được gửi bởi một thiết bị trong một miền quảng bá không được chuyển tiếp đến một miền quảng bá khác.

Các Switch ngày nay hỗ trợ nhiều tính năng rất hữu ích trong việc thiết lập, cấu hình và quản trị mạng LAN như VLAN, STP, Port Security,... Một số Switch có khả năng hoạt động ở các tầng cao hơn trong mô hình OSI, gọi là Switch Layer 3 hay MultiLayer Switch. Trong thiết kế cho hệ thống mạng LAN lớn, các Switch ở tầng Core/Distribution là các MultiLayer Switch, các Switch ở tầng Access là các L2-Switch.

#### Bảng địa chỉ MAC:

- Switch dùng bảng địa chỉ MAC để chuyển tiếp các Frame. Switch xây dựng bảng địa chỉ MAC dựa vào khả năng học địa

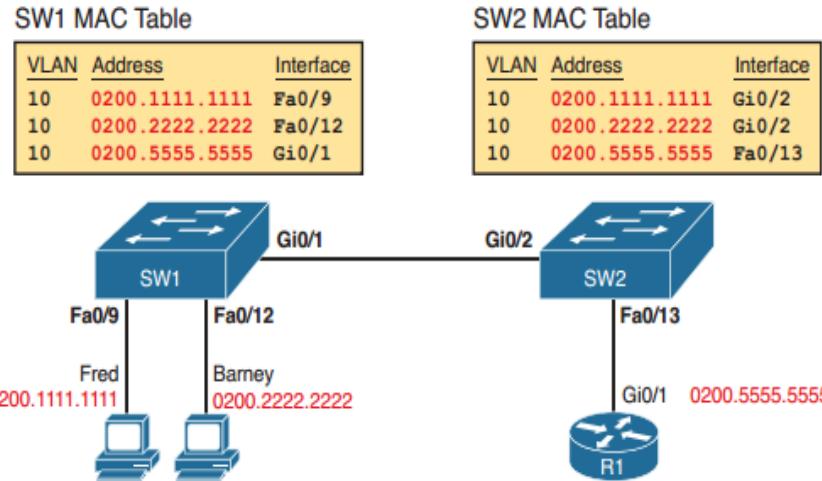
chỉ  $S_{MAC}$  trong Frame gửi tới nó. Quá trình chuyển tiếp Frame trên Switch được minh họa ở Hình 2.2. Ngoài tên gọi là bảng địa chỉ MAC còn có các tên gọi khác như bảng chuyển mạch (Switching Table, Bridging Table) hay bảng CAM (Content Addressable Memory Table).



**Hình 2.2: Bảng địa chỉ MAC trên Switch**

- + Frame được gửi từ PC1 đến cổng Gi0/1 của Switch.
- + Switch dựa vào địa chỉ MAC đích trong Frame ( $D_{MAC}$ ) và tra vào bảng địa chỉ MAC để xác định cổng sẽ chuyển Frame ra.
- + Frame được gửi ra cổng Gi0/3. Switch không gửi Frame ra các cổng khác.
- Trong trường hợp Switch được chia thành các VLAN, nghĩa là chia một Switch vật lý thành nhiều Switch ảo, mỗi Switch ảo này gọi là một VLAN. Các VLAN thông thường sẽ sử dụng một số cổng vật lý cho riêng mình. Khi đó, trong bảng địa chỉ MAC sẽ có thêm trường VLAN để nhận diện. Hình 2.3 minh họa bảng địa chỉ MAC ở SW1 và SW2. Trong trường hợp có nhiều VLAN trên Switch thông tin bảng địa chỉ MAC thể hiện như ví dụ sau:

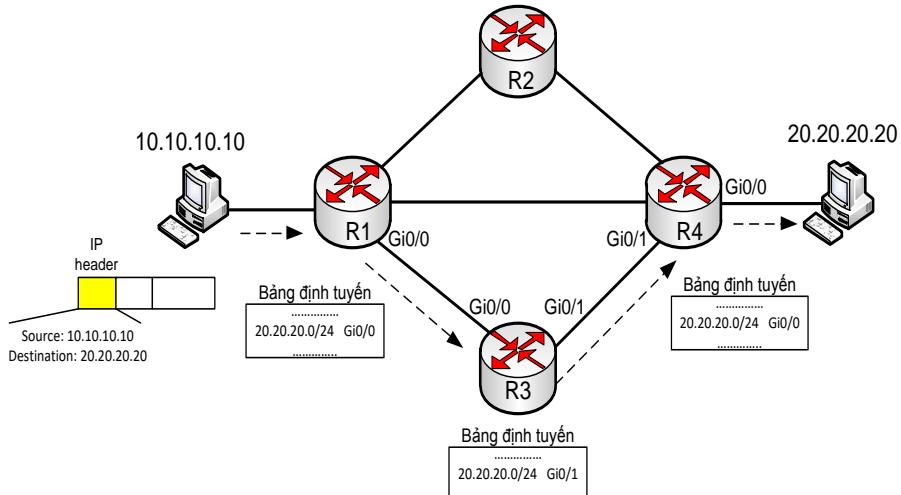
Vlan	Mac Address	Type	Ports
10	0004.9a6a.b5bc	DYNAMIC	Fa0/2
10	00e0.f949.0114	DYNAMIC	Fa0/1
20	0001.4252.c5de	DYNAMIC	Fa0/7
20	00e0.f73d.db56	DYNAMIC	Fa0/6



**Hình 2.3:** Bảng địa chỉ MAC trên Cisco Switch

### 2.1.2.3. Router

Router là thiết bị hoạt động ở tầng Network. Router được sử dụng để chia mạng thành nhiều miền quảng bá. Chức năng chính của Router là định tuyến, nghĩa là xác định đường đi cho các gói tin từ nguồn đến đích thông qua hệ thống mạng. Địa chỉ IP được sử dụng để định danh cho các thiết bị trên mạng. Router dựa vào thông tin địa chỉ IP đích trong gói tin mà nó nhận được và dựa vào bảng định tuyến để xác định đường đi cho các gói tin.

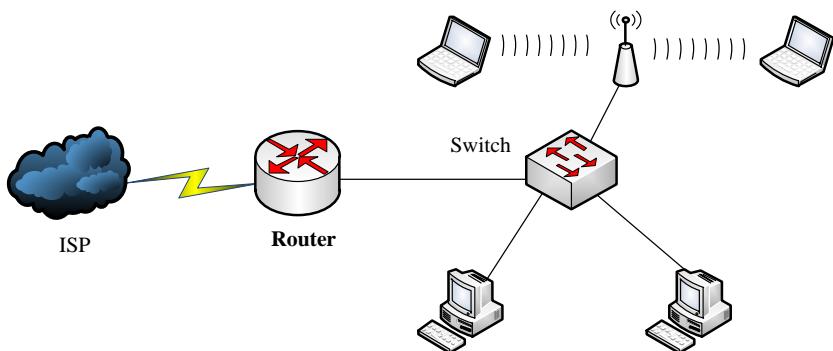


**Hình 2.4:** Kết nối hệ thống mạng sử dụng Router

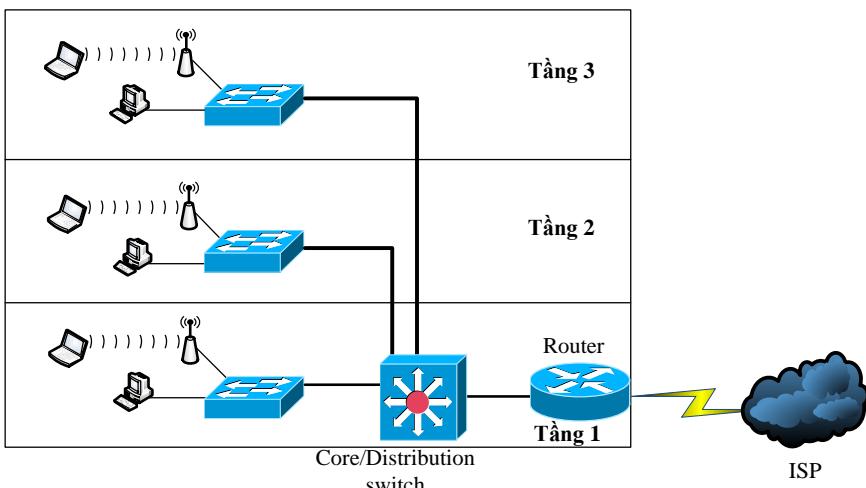
## 2.2. Mạng LAN và chuẩn Ethernet

### 2.2.1. Các hệ thống mạng LAN

Mạng LAN là mạng máy tính kết nối các thiết bị đầu cuối như máy tính, máy in, laptop, điện thoại thông minh, các thiết bị IoT lại với nhau để trao đổi thông tin. Các thiết bị trong LAN kết nối ở gần nhau như trong cùng một phòng, trong một tòa nhà hoặc kết nối các tòa nhà trong một vị trí địa lý của một tổ chức, doanh nghiệp,... Mạng LAN có thể phục vụ cho một đơn vị nhỏ như một văn phòng làm việc hay trong các hệ thống lớn như mạng của một trường đại học hay mạng của một tổ chức, doanh nghiệp bố trí trong một tòa nhà hoặc nhiều tòa nhà trong một khuôn viên địa lý.



Hình 2.5: Sơ đồ mạng cơ bản của mạng SOHO



Hình 2.6: Sơ đồ của một hệ thống mạng tổ chức trong một tòa nhà

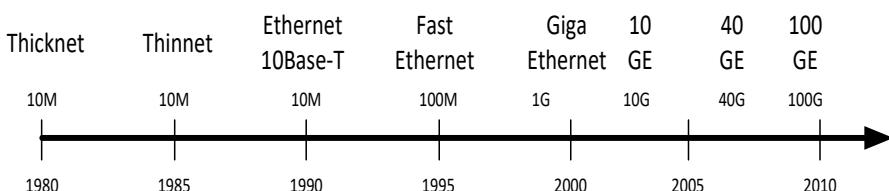
Trong mạng LAN, người quản trị có toàn quyền triển khai theo giải pháp thiết kế để kết nối hạ tầng cho các thiết bị trong LAN và quản trị các ứng dụng/dịch vụ. Kích cỡ mạng LAN có thể nhỏ như mạng của một gia đình hay văn phòng nhỏ, gọi là mạng SOHO (Small Office Home Office), hoặc có thể lớn như mạng của một tòa nhà hoặc nhiều tòa nhà trong một khuôn viên địa lý, gọi là mạng Campus hay Enterprise. Đối với các hệ thống mạng lớn, mạng LAN cần được thiết kế bài bản để đảm bảo các tính năng sẵn sàng, tính linh hoạt, khả năng mở rộng, tin cậy và bảo mật.

Chuẩn mạng trong LAN được nhắc đến nhiều nhất là chuẩn Ethernet, được định nghĩa bởi IEEE. Chuẩn này đưa ra các quy định về cáp, đầu nối, các giao thức,... Nói cách khác, nó định nghĩa một số đặc điểm ở các tầng Physical và tầng Data Link tạo nên một mạng Ethernet LAN. Ethernet LAN là công nghệ phổ biến nhất hiện nay được sử dụng trong mạng nội bộ.

## 2.2.2. Các chuẩn Ethernet

### 2.2.2.1. Giới thiệu

Từ khi ra đời đến nay, các chuẩn Ethernet luôn được phát triển theo hướng tốc độ ngày một cao hơn, hỗ trợ các loại cáp mạng khác nhau và tăng khoảng cách chiều dài cáp. Hình 2.7 giới thiệu một số chuẩn Ethernet cùng với tốc độ của nó phát triển theo thời gian.



**Hình 2.7: Quá trình phát triển các chuẩn Ethernet**

Chuẩn Ethernet định nghĩa nhiều loại cáp mạng và khoảng cách truyền giữa các thiết bị. Hai loại cáp phổ biến được sử dụng ngày nay là cáp đồng và cáp quang, có tốc độ từ 10 Mbps đến 100 Gbps. Các chuẩn Ethernet có nhiều cách gọi tên khác nhau, có tên bắt đầu bằng 802.3 và một số ký tự sau như 802.3ab, 802.3ae,... Hoặc có tên gọi ngắn gọn như 1000BASE-T, 10GBASE-X,... Hay có khi gọi là Gigabit Ethernet,

10 Gigabit Ethernet,... Bảng 2.1 trình bày một số chuẩn Ethernet với các tên gọi khác nhau của nó, cùng với ý nghĩa về tốc độ, loại cáp sử dụng và khoảng cách truyền.

Một số chuẩn Ethernet tầng Vật lý:

**Bảng 2.1: Một số chuẩn Ethernet phổ biến**

Chuẩn IEEE	Tên ngắn gọn	Tên thường gọi	Tốc độ	Loại cáp, khoảng cách truyền
802.3	10BASE-T	Ethernet	10 Mpbs	Cáp đồng, 100 m
802.3u	100BASE-T	FastEthernet	100 Mpbs	Cáp đồng, 100 m
802.3z	1000BASE-LX	Gigabit Ethernet	1 Gbps	Cáp quang, 5000 m
802.3ab	1000BASE-T	Gigabit Ethernet	1 Gbps	Cáp đồng, 100 m
802.3an	10GBASE-T	10 Gi Ethernet	10 Gpbs	Cáp đồng, 100 m
802.3ae	10GBASE-X	10 GigE	10 Gbps	Cáp quang
802.3ba	40GBASE-X	40 GigE	40 Gbps	Cáp quang
802.3ba	100GBASE-X	100 GigE	100 Gbps	Cáp quang

Ghi chú: Chữ “T”: cáp đồng, chữ “X”: cáp quang.

Dựa vào các chuẩn Ethernet, đặc biệt là các tham số về tốc độ, khoảng cách truyền dẫn, loại cáp hỗ trợ, người thiết kế và triển khai áp dụng trong bài toán thực tế như lựa chọn phương pháp kết nối mạng giữa các tòa nhà, kết nối giữa các tầng trong cùng một tòa nhà, kết nối các thiết bị trong cùng một tầng cho phù hợp.

### Tính nhất quán của chuẩn Ethernet ở tầng Data Link:

- Mặc dù có nhiều chuẩn ở tầng Vật lý, Ethernet hoạt động như một công nghệ LAN đơn thuần vì nó sử dụng cùng chuẩn ở tầng Data Link đối với tất cả các loại chuẩn Ethernet ở liên kết vật lý. Chuẩn này Ethernet ở tầng Data Link định nghĩa Ethernet Header và Trailer. **Bất kể** dữ liệu được truyền qua cáp đồng hay

cáp quang và tốc độ bao nhiêu, Header và Trailer sử dụng chung định dạng.

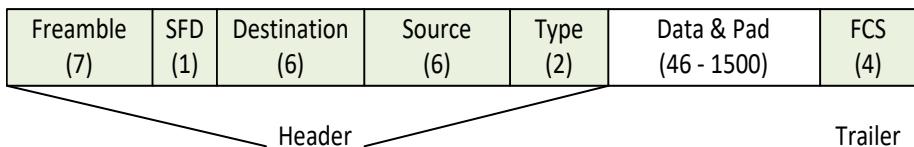
- Trong khi các tiêu chuẩn lớp vật lý tập trung vào việc gửi các tín hiệu bit qua cáp, các giao thức Ethernet tầng Data Link tập trung vào việc gửi một Frame từ nguồn đến đích. Thuật ngữ Frame đề cập đến Header và Trailer của một giao thức tầng Data Link.
- Như vậy có thể hiểu Ethernet LAN là sự **kết hợp** của các thiết bị người dùng, Switch và các loại cáp khác nhau. Mỗi kết nối có thể sử dụng các loại cáp khác nhau, ở tốc độ khác nhau. Tất cả chúng hoạt động cùng nhau để **vận chuyển** các Ethernet Frame từ một thiết bị trong mạng LAN đến các thiết bị khác.

### 2.2.2.2. Cấu trúc Frame Ethernet

Các bit được truyền qua mạng Ethernet LAN được tổ chức trong các Frame. Frame Ethernet là dữ liệu ở Layer 2 trong mô hình OSI.

Frame bao gồm thông tin về Header, Trailer và phần nội dung dữ liệu.

Cấu trúc của một Frame Ethernet được tổ chức như sau:



**Hình 2.8: Cấu trúc của Frame Ethernet**

Trong đó:

- Preamble: Bắt đầu một Frame.
- SFD: Đánh dấu kết thúc của Preamble.
- Destination: Địa chỉ MAC của máy gửi ( $D_{MAC}$ ).
- Source: Địa chỉ MAC của máy nhận ( $S_{MAC}$ ).
- Type: Mã xác định giao thức ở tầng trên.
- Data & Pad: Chứa dữ liệu nhận từ tầng Mạng trong quá trình đóng gói ở máy gửi. Nếu dữ liệu nhỏ hơn 46 byte, mỗi chuỗi các bit được bổ sung vào (gọi là Pad).
- FCS: Được sử dụng để kiểm tra lỗi xảy ra trên đường truyền, thiết bị nhận sẽ so sánh kết quả tính toán với giá trị trong FCS của thiết bị gửi để phát hiện ra có lỗi xảy ra cho Frame hay không.

### 2.2.2.3. Địa chỉ Ethernet

Các trường địa chỉ nguồn và đích có vai trò quan trọng để chỉ ra Ethernet LAN hoạt động như thế nào. Bên máy gửi sử dụng địa chỉ của nó đặt vào trường địa chỉ nguồn và đặt vào trường địa chỉ đích là địa chỉ của máy muốn gửi tới trong Frame Ethernet. Địa chỉ ở đây được gọi là địa chỉ MAC hay còn được gọi là địa chỉ vật lý. Địa chỉ MAC có 48 bit, được biểu diễn dưới dạng Hexa. Trong địa chỉ MAC, 48 được chia làm 2 phần, 24 bit đầu là mã định danh cho nhà sản xuất và 24 bit sau là mã định danh cho thiết bị. Địa chỉ MAC còn được gọi là địa chỉ Ethernet, địa chỉ LAN, địa chỉ vật lý. Các nhà sản xuất gán địa chỉ này cho các Card mạng (NIC).

Mã NSX (24 bit)	Mã thiết bị (24 bit)
--------------------	-------------------------

**Hình 2.9:** Cấu trúc địa chỉ MAC

Địa chỉ MAC có thể được biểu diễn ở nhiều định dạng tùy vào hệ thống. Ví dụ như 0000.1111.2e08; 00:00:11:11:2e:08; 00-00-11-11-2e-08. Các địa chỉ MAC của Card mạng có thể là các địa chỉ Unicast (đại diện cho 1 Card mạng). Ngoài ra, IEEE định nghĩa 2 loại địa chỉ ở Layer 2 để đại diện cho một nhóm là địa chỉ Broadcast và địa chỉ Multicast. Địa chỉ Broadcast: là địa chỉ đại diện cho tất cả các thiết bị trong LAN, có giá trị các bit đều là 1, FFFF.FFFF.FFFF. Địa chỉ Multicast: là địa chỉ đại diện cho một nhóm các thiết bị.

### 2.2.3. Các loại cáp thường dùng

#### Cáp UTP:



**Hình 2.10:** Đầu nối RJ-45

Cáp UTP là cáp rất thông dụng trong các mạng LAN hiện nay, sợi cáp UTP **gồm** 8 sợi, chia làm 4 đôi xoắn với nhau. Để kết nối các thiết bị, đầu nối RJ45 **được sử dụng** ở 2 đầu dây. Hai loại cáp được sử dụng phổ

biến để kết nối các thiết bị là cáp thẳng và cáp chéo. Hai chuẩn bấm cáp được sử dụng là T568-A và T568-B.

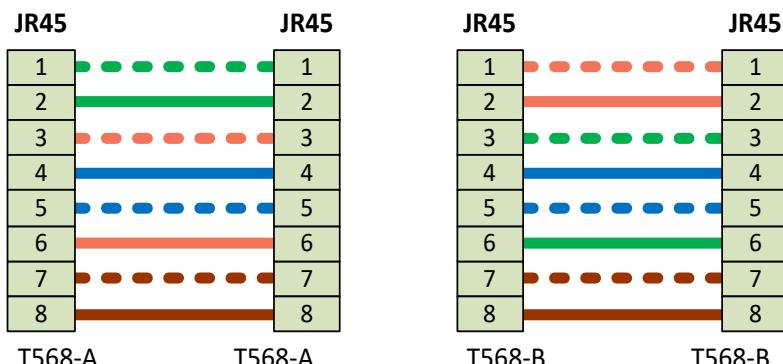
1	White green	1	White orange
2	Green	2	Orange
3	White orange	3	White green
4	Blue	4	Blue
5	White blue	5	White blue
6	Orange	6	Green
7	White brown	7	White brown
8	Brown	8	Brown

T568-A

T568-B

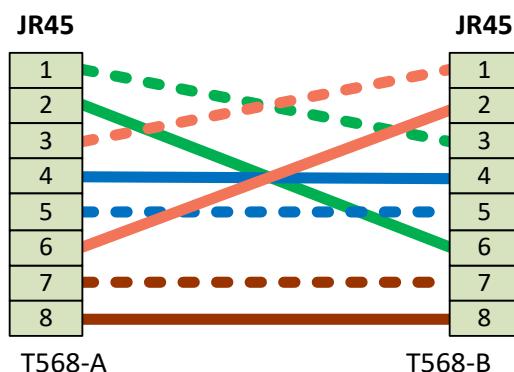
**Hình 2.11:** Chuẩn T568-A và T568-B

- **Cáp thẳng:** Hai đầu cáp bấm cùng chuẩn T568-A hoặc T568-B.



**Hình 2.12:** Cáp thẳng

- **Cáp chéo:** Một đầu cáp bấm theo chuẩn T568-A và đầu còn lại bấm theo chuẩn T568-B.



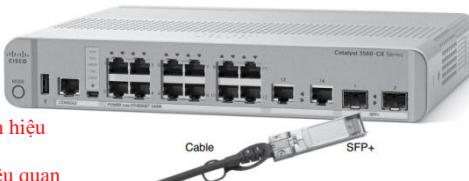
**Hình 2.13:** Cáp chéo

Cáp chéo thường kết nối trực tiếp giữa 2 máy tính, giữa 2 Switch hoặc giữa 2 Router. Một số thiết bị hiện nay có thể sử dụng cả cáp thẳng hoặc cáp chéo đều chạy được.

Cáp quang: Gồm 2 loại cơ bản là Multi Mode và Single Mode.

Cáp Single Mode có khoảng cách truyền xa hơn và tốc độ truyền cao hơn cáp Multi Mode. Điểm khác biệt về mặt vật lý là ở kích thước của phần lõi. Để sử dụng truyền dẫn quang, chúng ta phải sử dụng **Switch** có hỗ trợ Port quang, module quang và cáp quang và đầu nối quang.

port quang :cổng kết nối để sử dụng tín hiệu  
quang học  
module quang: tín hiệu điện-> tín hiệu quang  
cáp quang : dẫn truyền tín hiệu quang



**Hình 2.14:** Switch và Module quang

#### 2.2.4. Gửi dữ liệu trong mạng Ethernet

Gửi Ethernet Frame sử dụng Hub và Switch.

Có 2 chế độ truyền cơ bản trên các thiết bị chuyển mạch được sử dụng là Half Duplex và Full Duplex. Điểm khác biệt cơ bản của 2 chế độ này là: đối với chế độ Half Duplex, nó không thể thực hiện việc truyền và nhận đồng thời; ngược lại, ở chế độ Full Duplex, nó có thể thực hiện việc truyền và nhận cùng một lúc.

Hub và Switch là 2 thiết bị phổ biến được dùng trong mạng LAN, các hệ thống mạng ngày nay đa phần chuyển sang dùng Switch thay thế cho Hub. Ưu điểm của Switch là hoạt động nhanh hơn và cung cấp nhiều chức năng hiệu quả khác mà Hub không có được. Mặc dù cả Hub và Switch đều là các thiết bị tập trung trong mô hình hình sao, nhưng cách chuyển tiếp lưu lượng không giống nhau. Hub hoạt động ở tầng Vật lý, xử lý các tín hiệu bit để truyền dữ liệu. Switch hoạt động ở Layer 2, xử lý các Frame và đọc được các địa chỉ MAC nguồn, MAC đích,... để chuyển tiếp dữ liệu.

Hub chuyển tiếp dữ liệu dựa vào các chuẩn ở tầng Vật lý. Do đó, chúng ta có thể xem cách thức chuyển dữ liệu qua Layer 1 như đã trình bày ở Chương 1. Khi một tín hiệu điện được nhận vào từ một Port của

Hub, Hub sẽ khuếch đại tín hiệu và gửi ra tất cả các Port của nó, trừ Port nhận tín hiệu vào. Vấn đề có thể xảy ra trong việc truyền dữ liệu với Hub là trong trường hợp có hai hoặc nhiều thiết bị đến Hub cùng một lúc thì dung độ xảy ra. Để tránh sự dung độ này, Hub sử dụng chế độ truyền Half Duplex giữa Port của nó với thiết bị đầu cuối. Ở chế độ này, Hub sẽ báo cho các máy kết nối vào nó biết được có máy nào đang truyền hay không, nếu có thì phải chờ trước khi gửi lên.

Các thiết bị sử dụng chế độ truyền Half Duplex thực ra là sử dụng một thuật toán giải quyết dung độ với tên gọi là CSMA/CD:

- B1: Các thiết bị trước khi muốn truyền dữ liệu sẽ lắng nghe đường truyền có đang rảnh hay không.
- B2: Nếu đường truyền rảnh thì tiến hành truyền dữ liệu.
- B3: Các thiết bị khi gửi sẽ lắng nghe xem có dung độ xảy ra hay không. Nếu có dung độ xảy ra thì thực hiện như sau:
  - + Gửi tín hiệu báo có dung độ đến các thiết bị trong miền dung độ.
  - + Tự động thiết lập ngẫu nhiên thời gian truyền lại.
  - + Thực hiện lại bước (1).

Các hệ thống mạng LAN hiện đại thường không dùng Hub mà thay thế bằng Switch. Do đó, việc dung độ sẽ không xảy ra.

### 2.2.5. Một số công cụ kiểm tra kết nối

#### 2.2.5.1. Ipconfig

Lệnh **Ipconfig** sử dụng trên môi trường Microsoft Windows, hiển thị các thông tin cấu hình mạng TCP/IP. Lệnh Ipconfig chỉ hiển thị IP Address, Subnet Mask, Default Gateway cho tất cả các Card mạng.

Cú pháp: **ipconfig [/all] [/renew] [/release]**

Ý nghĩa của các tham số:

- **/all:** Hiển thị đầy đủ các thông tin cấu hình TCP/IP tất cả các Card mạng. Ngoài các thông tin cơ bản như ở lệnh Ipconfig, tham số này hiển thị thêm các thông tin về cổng vật lý và logic, các thông tin về DHCP, DNS,...
- **/renew:** Dùng trong trường hợp Card mạng cấu hình xin IP tự động từ DHCP Server.

- **/release:** Gửi thông điệp cho DHCP Server để loại bỏ các thông tin cấu hình IP.

### 2.2.5.2. Lệnh Ping

Ping là công cụ giúp kiểm tra kết nối giữa các thiết bị trên mạng. Ping sử dụng giao thức ở Layer 3 (ICMP) với 2 gói tin ICMP Echo Request và ICMP Echo Reply. Nếu một thiết bị nhận một ICMP Echo Request, nó sẽ trả lời lại gói ICMP Echo Reply. Trong mỗi gói tin gửi đi, lệnh Ping tính toán thời gian nhận gói trả lời. Ở mỗi gói tin nhận được, nó hiển thị thời gian từ khi gói yêu cầu được gửi đi và khi gói trả lời được nhận về.

```
C:\Users\Admin>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=82ms TTL=59
Reply from 8.8.8.8: bytes=32 time=264ms TTL=59
Reply from 8.8.8.8: bytes=32 time=40ms TTL=59
Reply from 8.8.8.8: bytes=32 time=65ms TTL=59

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 40ms, Maximum = 264ms, Average = 112ms
```

**Hình 2.15:** Thực hiện lệnh PING trên hệ điều hành Window

### 2.2.5.3. Telnet và SSH

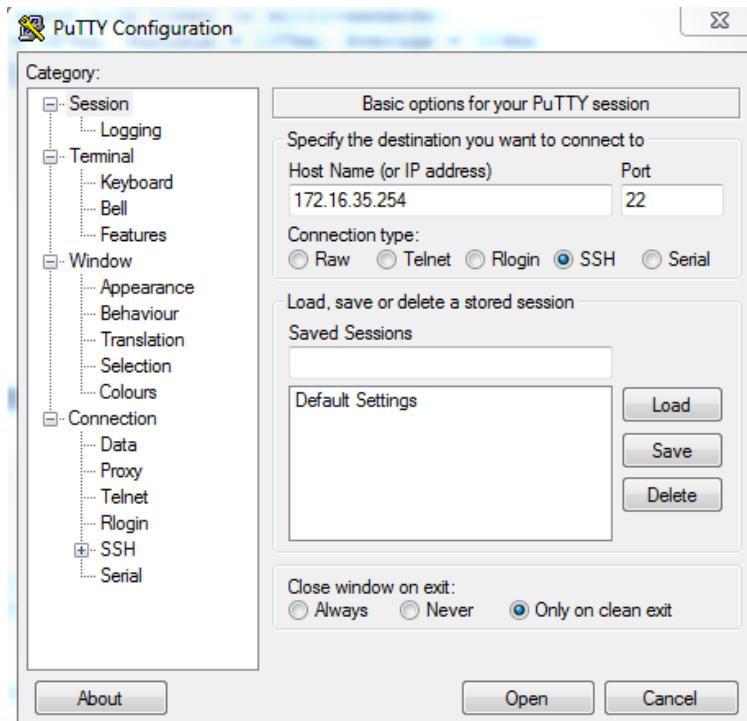
Telnet và SSH được sử dụng cho mục đích quản trị hệ thống từ xa. Người quản trị không cần đến trực tiếp thiết bị để quản trị mà thông qua môi trường mạng có thể kết nối từ xa để cấu hình và theo dõi hệ thống. Hai công cụ này hỗ trợ cấu hình ở chế độ dòng lệnh. Điểm khác biệt chính giữa hai công cụ này là SSH hỗ trợ việc mã hóa dữ liệu khi truyền còn Telnet thì không. Để cấu hình từ xa qua giao diện có thể sử dụng những cách khác như qua giao diện Web hay Remote Desktop.

```
C:\>telnet 192.168.60.1
Trying 192.168.60.1 ...Open

User Access Verification

Password: |
```

**Hình 2.16:** Telnet qua chế độ dòng lệnh trên hệ điều hành Window



**Hình 2.17: Phần mềm PuTTY**

## 2.3. Mạng WLAN

### 2.3.1. Giới thiệu

Mạng không dây có nhiều loại như WPAN, WLAN, WMAN, WWAN. Trong phần này, chúng ta xem xét mạng không dây trong LAN gọi là WLAN. Mạng WLAN được hiểu là sự mở rộng mạng LAN đối với việc sử dụng các thiết bị không dây như laptop, Ipad, điện thoại thông minh, các thiết bị IoT,... Mạng WLAN, còn gọi là mạng Wifi, ngày càng có vai trò quan trọng vì lý do tiện dụng của nó.

### 2.3.2. Các chuẩn mạng không dây

Chuẩn IEEE Wifi trong WLAN là 802.11 có nhiều phiên bản khác nhau như 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax,... Sơ lược lịch sử phát triển của các chuẩn Wifi phổ biến và các đặc trưng cơ bản như sau:

- **802.11a:** Ra đời năm 1999, tốc độ tối đa 54 Mbps, hoạt động ở dải tần số 5 GHz.

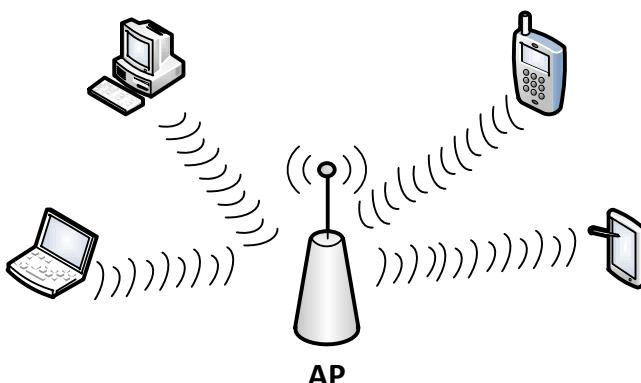
- **802.11b**: Ra đời năm 1999, tốc độ tối đa 11 Mbps, hoạt động ở dải tần số 2,4 GHz.
- **802.11g**: Ra đời năm 2003, tốc độ tối đa 54 Mbps, hoạt động ở dải tần số 2,4 GHz.
- **802.11n (Wifi 4)**: Ra đời năm 2009, tốc độ tối đa 600 Mbps, hoạt động ở vùng tần số 2,4 GHz và 5 GHz.
- **802.11ac (Wifi 5)**: Ra đời năm 2013, tốc độ tối đa 1,3 Gbps, hoạt động ở vùng tần số 5 GHz.
- **802.11ax (Wifi 6)**: Ra đời năm 2019, tốc độ tối đa 14 Gbps, hỗ trợ hoạt động ở vùng tần số 2,4 GHz và 5 GHz.

### 2.3.3. Các mô hình triển khai mạng Wifi

#### 2.3.3.1. Mô hình BSS

Trong mô hình này, một thiết bị tập trung (AP) được sử dụng để kết nối tín hiệu cho các thiết bị kết nối vào mạng Wifi. AP phục vụ như một điểm liên lạc duy nhất cho mọi thiết bị muốn sử dụng BSS. Nó quảng bá sự tồn tại của BSS để các thiết bị có thể tìm thấy nó và kết nối vào. Để làm điều đó, AP sử dụng một mã định danh BSS (BSSID) duy nhất dựa trên địa chỉ MAC Radio của AP.

AP quảng bá mạng không dây bằng mã định danh SSID, đây là một chuỗi văn bản chứa tên do người quản trị tự đặt. Một thiết bị phải gửi yêu cầu kết hợp và AP chấp nhận hoặc từ chối yêu cầu. Sau khi liên kết, một thiết bị trở thành máy khách của BSS.

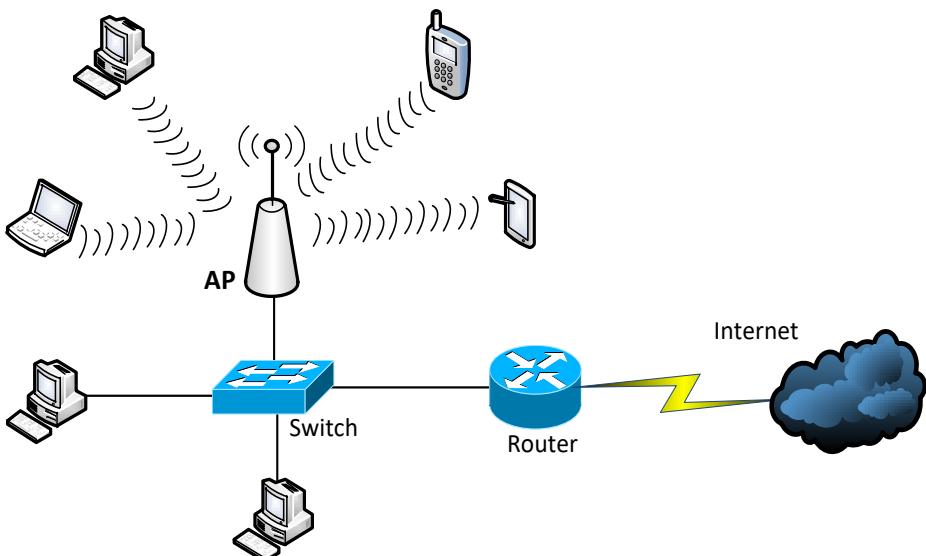


**Hình 2.18:** Mô hình mạng Wifi với 1 AP

Hầu hết các giao tiếp đến và từ máy khách phải truyền qua AP, như được chỉ ra trong Hình 2.18. Bằng cách sử dụng BSSID làm địa chỉ nguồn hoặc địa chỉ đích, các Frame dữ liệu có thể được chuyển tiếp đến hoặc từ AP.

### 2.3.3.2. Hệ thống phân phối

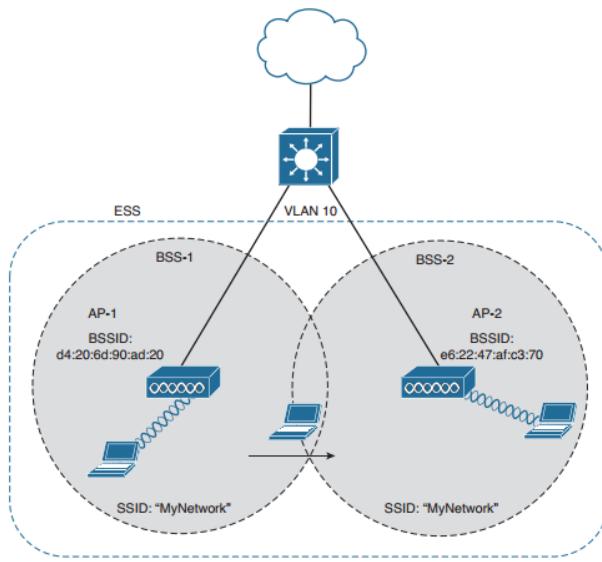
Các Client trong mạng Wifi cần giao tiếp với các thiết bị khác ngoài BSS, khi đó hệ thống mạng AP kết nối với mạng LAN có dây. Khi xây dựng mạng Ethernet LAN có dây, mạng WLAN được xem như một thành phần hay là sự mở rộng của mạng có dây.



*Hình 2.19: Mạng WiFi kết nối với mạng có dây*

### 2.3.3.3. Mô hình ESS

Trong một hệ thống mạng ngày nay, một AP không thể phủ sóng hết được khu vực phục vụ người dùng. Vì vậy, nhiều AP được lắp đặt và cung cấp dịch vụ kết nối cho người dùng. Khi các AP được đặt tại các vị trí khác nhau, tất cả chúng có thể kết nối với nhau thông qua hạ tầng các Switch. Chuẩn 802.11 gọi đây là bộ dịch vụ mở rộng (ESS) như thể hiện trong hình sau.

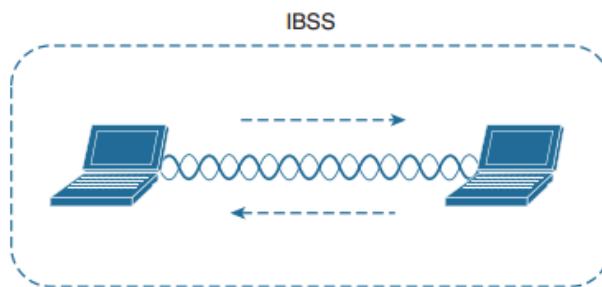


**Hình 2.20: Mô hình ESS**

Trong ESS, một máy khách không dây có thể liên kết với một AP trong khi nó nằm ở vị trí gần AP đó. Nếu khách hàng sau đó chuyển đến một vị trí khác, nó có thể liên kết với một địa điểm khác gần đó AP tự động. Chuyển từ AP này sang AP khác được gọi là chuyển vùng (roaming).

#### 2.3.3.4. IBSS (Ad-Hoc)

Mô hình mạng Ad-Hoc không cần có AP, các máy Client tự thiết lập kết nối Wifi với nhau. Trong đó, một Client tự thiết lập các tham số như tên định danh và lựa chọn chế độ bảo mật. Máy Client khác sẽ dò tên và thực hiện kết nối vào mạng Ad-Hoc.

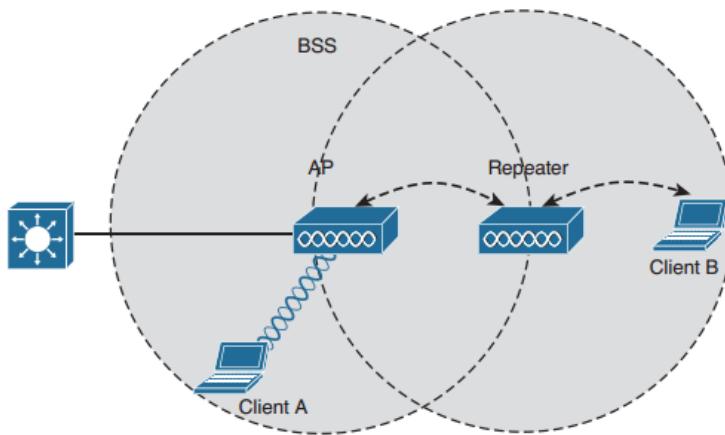


**Hình 2.21: Mô hình mạng Ad-Hoc**

### 2.3.3.5. Các mô hình khác

#### Repeater:

Thông thường, mỗi AP trong mạng không dây đều có kết nối có dây trở lại cơ sở hạ tầng mạng có dây thông qua các Switch như trong mô hình mạng phân phối. Để mở rộng vùng phủ sóng không dây, các AP được bổ sung vào và các kết nối có dây của chúng được thêm vào. Trong một số trường hợp, không thể chạy kết nối có dây với AP mới vì khoảng cách cáp quá xa để hỗ trợ truyền thông Ethernet. Trong trường hợp này, có thể thêm AP làm cầu hình ở chế độ Repeater. Khi đó, nó là điểm tiếp nhận và khuếch đại tín hiệu.



**Hình 2.22: Mô hình WiFi - Repeater**

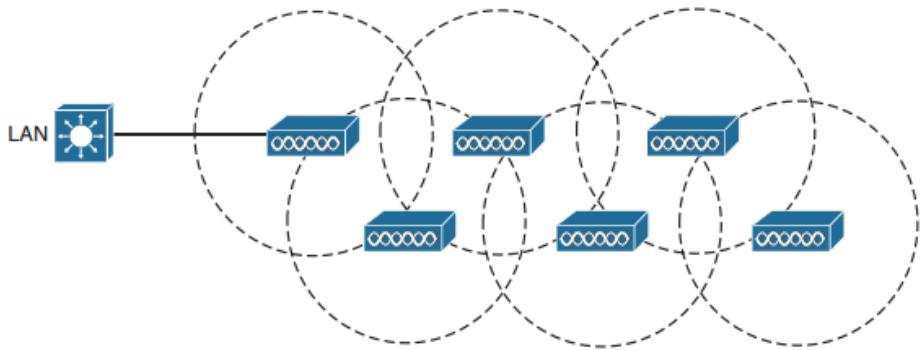
#### Outdoor Bridge:

Một AP có thể được cấu hình để hoạt động như một Bridge để thực hiện kết nối từ một mạng LAN đến một mạng khác qua khoảng cách xa. Anten định hướng thường được sử dụng trong trường hợp này.



**Hình 2.23: Mô hình mạng WiFi - Outdoor Bridge**

## Mạng Mesh:



**Hình 2.24: Mô hình mạng WiFi - Mesh**

Để cung cấp mạng WiFi trong một vùng rộng lớn, thay vì phải nối cáp đến các AP, các AP có thể cấu hình với chế độ Mesh để tạo mạng WiFi Mesh. Để quản trị tập trung mạng WiFi Mesh này, các Controller được sử dụng để cấu hình quản lý thiết bị và thiết lập các SSID đồng nhất trong toàn hệ thống. Các SSID có thể được thiết lập riêng cùng với các chính sách điều khiển truy cập, QoS khác nhau.

### 2.3.4. Nguyên tắc hoạt động

Trong mạng WLAN, SSID là một tên đại diện cho mạng và thông thường được quảng bá trong phạm vi phủ sóng. Các thiết bị có thể dò và kết nối vào. Tùy vào cấu hình mà hệ thống có yêu cầu người dùng chứng thực hay không. Để đảm bảo tính bảo mật, các hệ thống mạng WLAN ngày nay yêu cầu chứng thực trước khi sử dụng.

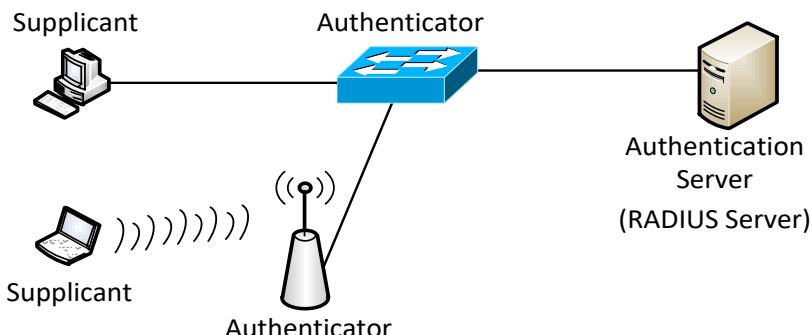
Mạng không dây IEEE 802.11 cũng dựa vào các địa chỉ MAC. Mỗi Card không dây của Client có địa chỉ MAC để có thể gửi và nhận Frame. Để chuyển Frame qua AP, AP cũng có địa chỉ MAC của nó. Wireless Client biết địa chỉ MAC của AP (gọi là BSSID) và gửi kèm nó trong Frame gửi tới AP.

### 2.3.5. Bảo mật trong WLAN

Việc triển khai mạng WiFi hiện nay được xem như một thành phần tất yếu trong các mạng LAN. Mạng WiFi mang lại sự tiện dụng cho người dùng trong việc kết nối các thiết bị vào mạng như điện thoại thông minh, máy tính bảng, máy tính xách tay,... và là một nền tảng trong kết nối các

thiết bị IoT. Do đó, việc triển khai mạng Wifi sẽ làm gia tăng các tấn công bênh mặt cho hệ thống. Đảm bảo an toàn trong mạng Wifi trở thành mối quan tâm lớn trong các hệ thống mạng. Một số phương pháp thường dùng để bảo mật mạng Wifi như sau:

- Lọc địa chỉ MAC.
- WPA2, WPA3.
- Chứng thực người dùng RADIUS Server (802.1X).



**Hình 2.25: Chứng thực với Radius Server**

## 2.4. Tổng kết chương

Chương này đã trình bày về các thiết bị, kỹ thuật dùng trong mạng LAN, WLAN. Các chuẩn mạng phổ biến Ethernet với các thông số kỹ thuật và thiết bị tương ứng sẽ giúp việc triển khai hệ thống mạng đạt hiệu quả cao. Ngoài ra, các chuẩn mạng không dây và các mô hình của nó sẽ giúp việc triển khai dễ dàng. Để tránh các tấn công trong mạng WLAN, vấn đề bảo mật được nghiên cứu thông qua các kỹ thuật WPA2, WPA3, chứng thực qua Radius Server.

## 2.5. Câu hỏi Chương 2

1. Chuẩn cáp mạng nào sau đây hỗ trợ tốc độ lên tới 1Gb/s sử dụng 4 cặp cáp của CAT5e?
  - A. 1000BASE-T.
  - B. 1000BASE-SX.
  - C. 1000BASE-LX.
  - D. 1000BASE-X.

2. Câu nào sau đây là đúng khi thay thế các Hub bằng các Switch?

- A. Làm tăng số lượng miền đụng độ.
- B. Làm giảm số lượng miền đụng độ.
- C. Làm tăng số lượng miền quảng bá.
- D. Làm giảm số lượng miền quảng bá.

3. Lý do nào sau đây mà giao thức Ethernet sử dụng địa chỉ vật lý?

- A. Nó tạo ra sự khác biệt giữa các cách truyền thông ở Layer 2 và Layer 3.
- B. Nó định nghĩa mô hình địa chỉ luận lý cho các thiết bị.
- C. Nó dùng để định danh duy nhất cho các thiết bị ở Layer 2.
- D. Nó cho phép một máy tính xác định là ở xa hay trong mạng cục bộ.

4. Trường nào trong IP Header được dùng để tránh trường hợp một gói tin tồn tại mãi trên mạng?

- A. Checksum.
- B. Flags.
- C. TTL.
- D. Header Length.

5. Trong Frame, trường nào được dùng để phát hiện lỗi?

- A. MTU.
- B. MAC.
- C. PDU.
- D. FCS.
- E. ERR.
- F. Flag.

6. Các chuẩn nào sau đây không phải là chuẩn của Wifi?

- A. 802.11g.
- B. 802.11n.
- C. 802.1Q.

- D. 802.11ac.
  - E. 802.1d.
  - F. 802.11ax.
7. Câu nào sau đây là đúng khi nói về địa chỉ MAC?
- A. Phần OUI tạo ra sự duy nhất cho một địa chỉ MAC.
  - B. 24 bit đầu của địa chỉ MAC được nhà sản xuất gán cho thiết bị để định danh cho thiết bị.
  - C. Hub sử dụng địa chỉ MAC để chuyển mạch cho các Frame.
  - D. Nếu bit I/G có giá trị 1 thì Frame chứa địa chỉ này được nhận điện là Broadcast hoặc Multicast.
8. Thành phần nào sau đây trong mạng Wifi cho phép người dùng chuyển vùng giữa các AP mà vẫn giữ nguyên việc chứng thực?
- A. BSS.
  - B. ESS.
  - C. WLAN controller.
  - D. SSID.
9. Chuẩn Ethernet là:
- A. IEEE 802.1.
  - B. IEEE 802.11.
  - C. IEEE 802.3.
  - D. IEEE 802.5.
10. Switch sẽ xử lý như thế nào khi nhận vào một gói tin mà trong đó, địa chỉ MAC đích không có trong bảng địa chỉ MAC của nó?
- A. Switch sẽ hủy gói tin đó.
  - B. Switch sẽ trả gói tin đó lại cho máy gửi.
  - C. Switch sẽ học địa chỉ MAC đó.
  - D. Switch sẽ chuyển gói tin đó ra tất cả các cổng của nó, trừ cổng nhận gói tin vào.
11. Trong mạng Wifi, thuật toán nào được sử dụng để xử lý khi đụng độ xảy ra?
- A. CSMA/CA.
  - B. CSMA/CD.

- C. CSMA/DA.
  - D. 802.1X.
12. Thuật toán nào được sử dụng để xử lý đụng độ trong môi trường mạng có dây, khi sử dụng chế độ Half Duplex?
- A. CSMA/CD.
  - B. CSMA/CA.
  - C. CSMA/MD.
  - D. CSMA/DA.
13. Địa chỉ nào sau đây không phải là cách biểu diễn đúng của một địa chỉ MAC?
- A. 00.11.22.33.44.55.
  - B. 1111.2222.3333.
  - C. 12-34-56-78-AX-MH.
  - D. 0C-9F-00-1C-AB-98.
14. Tại sao Switch không bao giờ học địa chỉ MAC là địa chỉ Broadcast?
- A. Vì địa chỉ Broadcast không bao giờ là địa chỉ nguồn trong gói tin.
  - B. Vì địa chỉ Broadcast là địa chỉ đại diện cho tất cả các máy trong miền Broadcast.
  - C. Vì địa chỉ Broadcast dễ bị tấn công.
  - D. Vì địa chỉ Broadcast không thể xác định được máy tính nào trong mạng.
15. Có 2 chuẩn bấm cáp đồng là?
- A. T568-A.
  - B. T567-A.
  - C. T586-A.
  - D. T568-B.
  - E. T586-B.
16. Bấm cáp thẳng là?
- A. Bấm hai đầu cáp theo hai chuẩn khác nhau.
  - B. Bấm hai đầu cáp theo cùng một chuẩn.
  - C. Bấm một đầu theo chuẩn T568-A và một đầu theo chuẩn T865-A.
  - D. Bấm một đầu theo chuẩn T568-A và một đầu theo chuẩn T568-B.

17. Thiết bị mạng nào sau đây có thể chia mạng thành nhiều miền quảng bá (Broadcast Domain)?
- A. Hub & Switch.
  - B. Switch & Router.
  - C. Hub & Router.
  - D. Repeater & Bridge.
18. Cấu hình bảo mật cho mạng Wifi với WPA2 có 2 chế độ có thể dùng là?
- A. WPA2 - Personal.
  - B. WPA2 - Enterprise.
  - C. WPA2 - AES.
  - D. WPA2 - Pre Shared Key.
19. Trong mô hình chứng thực cho mạng có dây và không dây với 802.1X, có 3 thành phần chính bao gồm những cái nào sau đây?
- A. Supplicant.
  - B. Authentication Server.
  - C. Application Server.
  - D. Web Browser.
  - E. Authenticator.
20. Telnet và SSH là 2 công cụ hỗ trợ truy cập từ xa, 2 công cụ này hoạt động ở các Port theo thứ tự là?
- A. 22, 25.
  - B. 23, 22.
  - C. 23, 80.
  - D. 22, 21.
  - E. 22, 53.

## CHƯƠNG 3

# ĐỊA CHỈ IP

Chương này trình bày về địa chỉ IP, là địa chỉ dùng để định danh cho các thiết bị trên mạng. Học xong chương này, người học có khả năng:

- Trình bày được vai trò, cấu trúc của địa chỉ IP trong mạng.
- Trình bày được sự phân lớp địa chỉ IPv4.
- Trình bày và vận dụng được các kỹ thuật chia mạng con IP Subneting, VLSM.
- Phân biệt được địa chỉ IPv4 và IPv6.
- Hoạch định được địa chỉ IP cho một sơ đồ mạng.

### 3.1. Giới thiệu

Địa chỉ IP là địa chỉ được dùng để định danh cho một đối tượng trên mạng. Các đối tượng này có thể là máy tính, máy in, camera, điện thoại thông minh, các thiết bị IoT,... gọi chung là các thiết bị người dùng cuối hay là các “Host”.



*Hình 3.1: Cấu trúc tổng quát của địa chỉ IP*

Cấu trúc địa chỉ IP gồm 2 phần là NETWORK và HOST, có khi người ta gọi là Net\_ID và Host\_ID, nghĩa là phần định danh cho phần Network và phần định danh cho Host. Các địa chỉ IP có cùng phần Network gọi là cùng mạng. Các địa chỉ IP trên một mạng là duy nhất. Hai loại địa chỉ IP được trình bày trong chương này là IPv4 và IPv6.

### 3.2. Địa chỉ IPv4

#### 3.2.1. Giới thiệu

Trong IPv4 Header có chứa địa chỉ của máy gửi ( $S_{IP}$ ) và máy nhận ( $D_{IP}$ ), dựa vào thông tin địa chỉ này, các thiết bị định tuyến sẽ

xác định đường đi cho các gói tin và chuyển tiếp chúng qua mạng để đến máy nhận.

Ver	IHL	Service Type	Service Type	
Identification		Flag		Flag. Offset
Time to Live		Protocol		Header Checksum
Source Address				
Destination Address				
Options			Padding	

**Hình 3.2: IPv4 Header**

Địa chỉ IPv4 có 32 bit, được chia thành 4 phần (Octet), được biểu diễn dưới dạng nhị phân hoặc thập phân, các phần ngăn cách nhau bởi dấu “.”. Ví dụ: 192.168.10.1

Trong thiết kế và vận hành một hệ thống mạng, nhất là trong các hệ thống mạng lớn, vấn đề hoạch định địa chỉ IP có vai trò và ý nghĩa quan trọng. Từ đó, triển khai các kỹ thuật định tuyến đạt hiệu quả.

### 3.2.2. Phân lớp địa chỉ

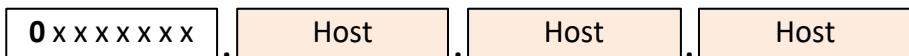
Địa chỉ IPv4 được chia thành 5 lớp: A, B, C, D, E.

Trong đó:

- Các lớp A, B, C được dùng để gán cho các Host.
- Lớp D là lớp địa chỉ Multicast.
- Lớp E không dùng.

#### Đặc điểm của các lớp:

- **Lớp A (Class A):**



- + Octet đầu tiên làm phần Network, 3 Octet còn lại làm phần Host.
- + Bit đầu tiên của Octet đầu tiên phải là bit 0.
- + Một mạng lớp A có thể được sử dụng để cho  $2^{24} - 2 = 16.777.214$  (\*) Host.

**Như vậy:** Octet đầu tiên có giá trị là:

- + **00000000 → 01111111** (viết dưới dạng nhị phân).
- + Hay từ 0 đến 127 (viết dưới dạng thập phân).

**Lưu ý:**

- + Giá trị đầu tiên 00000000 không dùng.
- + Giá trị cuối: 01111111 (127) được dùng làm địa chỉ Loopback (127.0.0.1).

**Kết luận:** Địa chỉ lớp A có Octet đầu tiên mang giá trị **00000001** đến **01111110** (hay từ 1 đến 126).

Ví dụ: **10.10.10.1**

**00001010.00001010.00001010.00000001**

- **Lớp B (Class B):**



- + 2 Octet đầu tiên làm phần Network, 2 Octet còn lại làm phần Host.
- + 2 bit đầu tiên của Octet đầu tiên phải là bit 10.
- + Một mạng lớp B có thể được sử dụng để gán cho  $2^{16} - 2 = 65.534$  (\*) Host.

**Như vậy:** Octet đầu tiên có giá trị:

- + **10000000** đến **10111111** (viết dưới dạng nhị phân).
- + Hay từ 128 đến 191 (viết dưới dạng thập phân).

Ví dụ: **172.16.10.1**

**10101100.00010000.00001010.00000001**

- **Lớp C (Class C):**



- + 3 Octet đầu tiên làm phần Network, 1 Octet còn lại làm phần Host.

- + 3 bit đầu tiên của Octet đầu tiên phải là bit 110.
- + Một mạng lớp C có thể được sử dụng để gán cho  $2^8 - 2 = 254$  (\*) Host.

Như vậy: Octet đầu tiên có giá trị:

- + **11000000** đến **11011111** (viết dưới dạng nhị phân).
- + Hay từ 192 đến 223 (viết dưới dạng thập phân).

Ví dụ: **192.168.1.1**

**11000000.10101000.00000001.00000001**

- **Lớp D (Class D): Địa chỉ lớp D là địa chỉ Multicast.**

- + 4 bit đầu tiên của Octet đầu tiên phải là bit 1110.

Như vậy: Octet đầu tiên có giá trị là:

- + **11100000** đến **11101111** (viết dưới dạng nhị phân).
- + Hay từ 224 đến 239 (viết dưới dạng thập phân).

Ví dụ: **224.0.0.5**

**1110000.00000000.00000000.00000101**

- **Lớp E (Class E): Còn lại, chưa sử dụng.**

5 bit đầu tiên của Octet đầu tiên phải là 11110.

### **Hai địa chỉ đặc biệt:**

Trong mỗi mạng có 2 địa chỉ đặc biệt không dùng để gán cho các thiết bị, đó là địa chỉ mạng (network address) và địa chỉ quảng bá (Broadcast Address).

- **Địa chỉ mạng (Network Address):** Là địa chỉ đại diện cho một mạng, tất cả các bit ở phần HOST trong địa chỉ IP đều là bit 0.

Ví dụ: **192.168.1.0**

- **Địa chỉ quảng bá (Broadcast Address):** Là địa chỉ tất cả các bit ở phần HOST đều là bit 1.

Ví dụ: **192.168.1.255**

### **3.2.3. IP Public và IP Private**

IP Private hay IP Local là các địa chỉ dùng triển khai trong các mạng nội bộ. Mục tiêu của việc phân chia này là một trong các giải pháp giúp tiết kiệm và quản lý địa chỉ IP trên mạng. Các địa chỉ IP Public (hay IP Global) được quản lý bởi cơ quan có thẩm quyền và phân chia cho các ISP để cấp phát cho khách hàng.

- Dãy địa chỉ IP Private (RFC 1918):
    - + **10.x.x.x**
    - + **172.16.x.x → 172.31.x.x**
    - + **192.168.0.x → 192.168.255.x**
  - IP Public: Các IP còn lại.

### 3.2.4. Subnet Mask

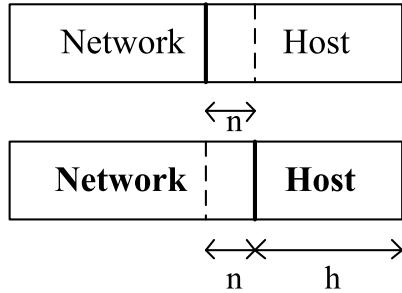
Subnet Mask có chiều dài bit bằng với địa chỉ IP được dùng để chỉ ra trong một địa chỉ IP những bit nào thuộc phần Network và những bit nào thuộc phần Host. Trong đó, các bit 1 chỉ ra tương ứng các bit thuộc phần Network và các bit 0 chỉ ra tương ứng các bit thuộc phần Host.

Subnet Mask được biểu diễn dưới dạng: (1) 4 Octet giống như địa chỉ IP hoặc (2) /n với n là số bit làm phần Network. Subnet Mask mặc định (Default Subnet Mask) cho các lớp địa chỉ IP như sau:

- Class A: 255.0.0.0 hoặc /8
  - Class B: 255.255.0.0 hoặc /16
  - Class C: 255.255.255.0 hoặc /24

### 3.2.5. Kỹ thuật chia mạng con (IP Subnetting)

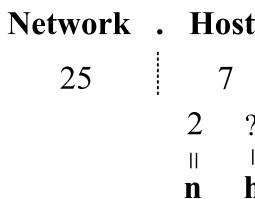
Kỹ thuật chia mạng con là một kỹ thuật cho phép tạo ra nhiều mạng con từ một mạng ban đầu. Kỹ thuật này tạo ra nhiều mạng con với số lượng IP ít hơn, phù hợp cho nhu cầu sử dụng và tối ưu cho hệ thống. Các mạng con sinh ra có kích thước bằng nhau. Để thực hiện điều này, người ta mượn một số bit ở phần Host tham gia vào phần Network.



Ta có một số tính chất cần lưu ý như sau:

- Gọi  $n$  là số bit mượn ở phần Host thì số mạng con (Subnet) có thể chia là  $2^n$ .
- Gọi  $h$  là số bit còn lại của phần Host thì số Host cho mỗi mạng con là  $2^h - 2$ .

**Ví dụ:** Cho một mạng có địa chỉ 192.168.1.0/25, mượn 2 bit. Xác định địa chỉ của các mạng con sinh ra.

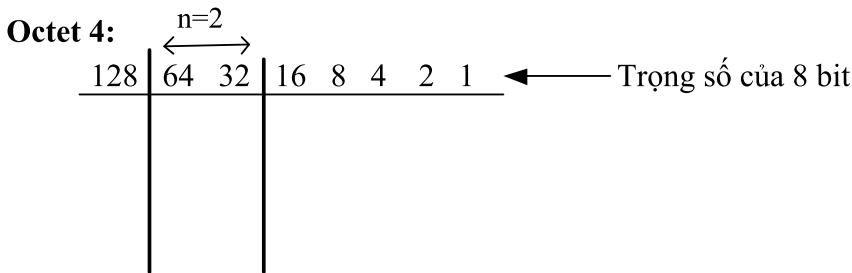


Mượn 2 bit  $\rightarrow n = 2$  và  $h = 5$ . Do đó, số mạng con sinh ra là  $2^n = 2^2 = 4$  và số lượng IP của mỗi mạng con là  $2^h - 2 = 2^5 - 2 = 30$ .

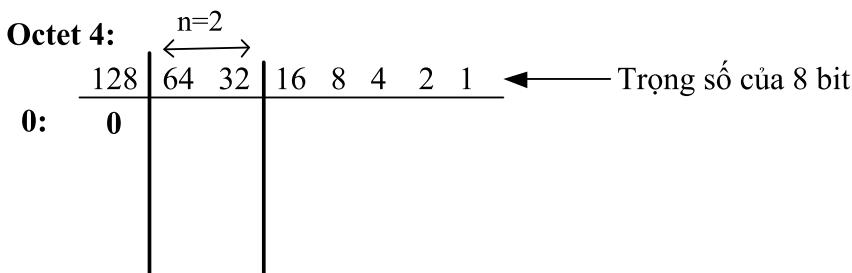
Các bước để xác định địa chỉ các mạng con sinh ra:

- **Bước 1.** Xác định đường ranh giới của  $n$  bit mượn dựa vào Subnet Mask và  $n$  bit mượn.
- **Bước 2.** Xác định giá trị của Octet chưa đường ranh giới.
- **Bước 3.** Tỏ hợp của  $n$  bit  $\rightarrow$  suy ra được  $2^n$  giá trị  $\rightarrow 2^n$  địa chỉ mạng con.

Tiếp tục với ví dụ trên, ta có thể xác định đường ranh giới của  $n$  bit mượn thuộc Octet 4.



Octet chứa đường ranh giới là Octet 4, giá trị của Octet này ở địa chỉ IP là 0. Do đó, phần thể hiện giá trị này dạng nhị phân ở Octet 4 như sau:



Tổ hợp của 2 bit, ta được 4 giá trị. Từ đó, suy ra được các mạng con tương ứng.

**Octet 4:**

128	64	32	16	8	4	2	1
-----	----	----	----	---	---	---	---

$\longleftrightarrow^{n=2}$

← Trọng số của 8 bit

<b>0</b>	0	0	→ 192.168.1.0/27				
	0	1	→ 192.168.1.32/27				
	1	0	→ 192.168.1.64/27				
	1	1	→ 192.168.1.96/27				

### Một số dạng bài tập IP:

#### Dạng 1. Xác định địa chỉ mạng của một địa chỉ IP cho trước

Trong phần này trình bày hai cách có thể sử dụng để xác định địa chỉ mạng (Network Address) của một IP cho trước.

#### Cách 1: Sử dụng công thức sau:

$$\text{Network Address} = \text{IP-Address AND Subnet Mask}$$

Để có thể tính nhanh kết quả, chúng ta có thể nhớ lại tính chất sau của phép AND.

Với  $X = \{0,1\}$ , thì  $X \text{ AND } 0 = 0$  và  $X \text{ AND } 1 = X$ .

**Ví dụ:** Cho một PC có IP: 192.168.1.158 và Subnet Mask: 255.255.255.240. Xác định địa chỉ mạng của PC trên.

AND	192.168.1.158
	255.255.255.240
Kq	192.168.1.?

**Nhận xét:** 3 Octet đầu của Subnet Mask đều có các bit là bit 1. Do đó, phần kết quả của phép AND của 3 Octet đầu chỉ cần ghi nhận lại giá trị của 3 Octet của IP (áp dụng  $X \text{ AND } 1 = X$ ). Bây giờ chỉ cần thực hiện phép AND giữa 158 và 240 ở Octet thứ 4.

Octet 4:

	128	64	32	16	8	4	2	1	← Trọng số của 8 bit
158:	1	0	0	1	1	1	1	0	
AND	1	1	1	1	0	0	0	0	
240:	1	1	1	1	0	0	0	0	→ 144

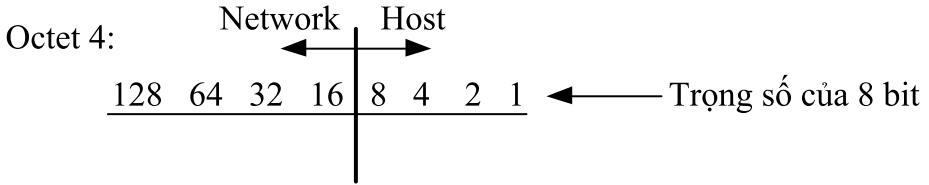
Vậy địa chỉ mạng cần tìm là: 192.168.1.144/28

**Cách 2:** Sử dụng tính chất sau: “Địa chỉ mạng là địa chỉ có các bit phần Host đều là bit 0”. Để xác định địa chỉ mạng, có thể thực hiện theo các bước sau:

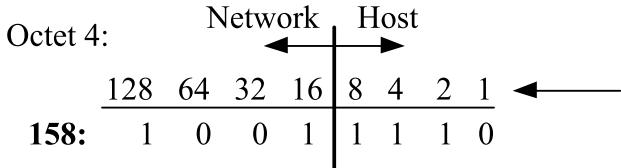
- B1. Xác định đường ranh giới giữa phần Network và Host dựa vào Subnet Mask.
- B2. Xác định giá trị của Octet chứa đường ranh giới.
- B3. Cho các bit thuộc phần Host → 0. Từ đó xác định địa chỉ mạng.

Sử dụng lại ví dụ ở cách 1, các bước xác định địa chỉ mạng như sau:

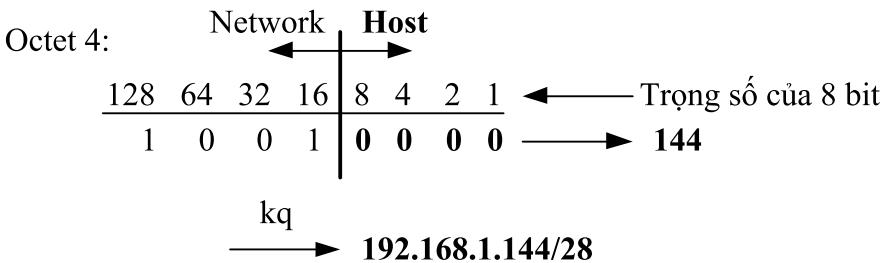
Từ địa chỉ Subnet Mask: 255.255.255.240, suy ra đường ranh giới giữa phần Network và Host nằm ở Octet 4.



Giá trị của Octet 4 ở địa chỉ IP là 158.



Cho tất cả các bit phần Host → 0.



Các Octet đầu ghi lại giá trị, kết hợp với giá trị vừa tính được ở Octet thứ 4, ta có được kết quả cần tìm.

## Dạng 2. Xác định dãy địa chỉ IP của một mạng

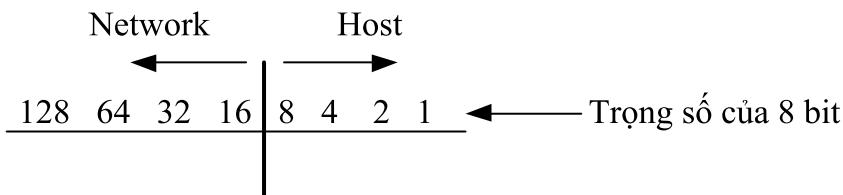
Xác định dãy địa chỉ IP của một mạng là xác định địa chỉ bắt đầu và địa chỉ cuối, dãy địa chỉ này được dùng để gán cho các thiết bị trên mạng. Nên lưu ý rằng, hai địa chỉ đặc biệt của một mạng không được dùng để gán cho các thiết bị đó là địa chỉ mạng và địa chỉ Broadcast.

### Hướng dẫn:

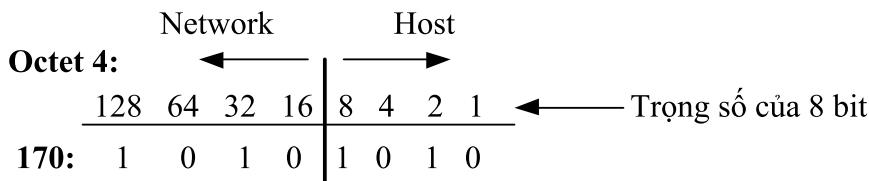
- Bước 1. Xác định đường ranh giới giữa phần Network và Host dựa vào Subnet Mask.
- Bước 2. Xác định giá trị của Octet chứa đường ranh giới.
- Bước 3. Xác định giá trị đầu tiên và giá trị cuối cùng của dãy dựa vào các bit phần Host.

**Ví dụ:** Một PC có địa chỉ IP là 192.168.1.170 và Subnet Mask là 255.255.255.240. Xác định dãy địa chỉ IP (IP Range) của mạng chứa IP trên.

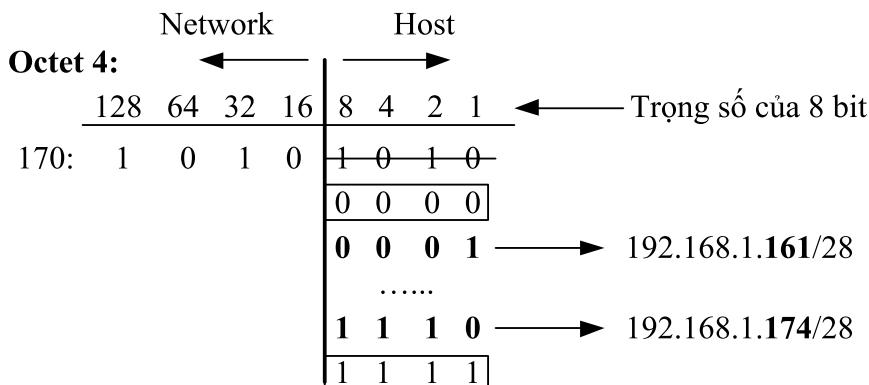
- Dựa vào giá trị của Subnet Mask, có thể xác định đường ranh giới giữa phần Network và Host nằm ở Octet 4.



- Octet chứa đường ranh giới là Octet 4, có giá trị trong địa chỉ IP là 170 được biểu diễn ở dạng nhị phân như sau:



- Xác định địa chỉ đầu tiên và cuối cùng của dãy dựa vào các bit phần Host.



Vậy dãy IP của mạng chứa IP: 192.168.1.170/28 là 192.168.1.161/28 – 192.168.1.174/28.

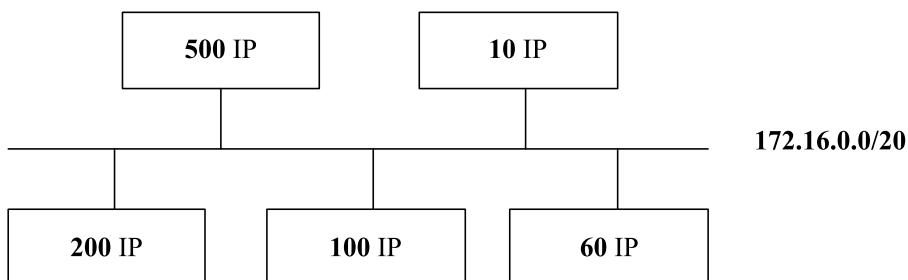
### 3.2.6. Kỹ thuật VLSM

Kỹ thuật chia mạng con có đặc điểm là các mạng con sinh ra có kích thước giống nhau. Trong một số hệ thống mạng, các đơn vị phòng

ban có thể được hoạch định số lượng IP có kích thước khác nhau. Đối với các hệ thống như vậy, việc sử dụng kỹ thuật IP Subnetting sẽ gây lãng phí IP, không được tối ưu, ít hiệu quả. Vì khi đó, có đơn vị phòng ban sẽ thừa nhiều IP.

Kỹ thuật VLSM (Variable Length Subnet Masking) giúp cho việc hoạch định IP tối ưu hơn. Kỹ thuật này xem xét thực hiện việc chia IP cho từng mạng riêng biệt. Chiến lược được sử dụng là chia mạng cho lần lượt các mạng có kích thước từ lớn đến nhỏ. Chúng ta sẽ tìm hiểu chi tiết kỹ thuật này thông qua một ví dụ cụ thể.

**Ví dụ:** Một công ty tổ chức thành 5 phòng ban, số lượng IP cần thiết cho các thiết bị tối đa cho mỗi phòng ban được thể hiện là giá trị ghi trong các ô hình chữ nhật (mỗi ô hình chữ nhật đại diện cho một phòng ban của công ty). Sử dụng địa chỉ mạng 172.16.0.0/20, hãy chia mạng con cho các phòng ban, sao cho tiết kiệm địa chỉ IP nhất có thể.



**Hình 3.3: Hoạch định IP cho một công ty**

Chiến lược để thực hiện việc hoạch định IP theo VLSM được tiến hành cho phòng ban có nhiều IP nhất. Ở ví dụ này, phòng ban có nhiều IP nhất là 500.

- **Phòng ban 500 IP:**

Sử dụng mạng ban đầu là 172.16.0.0/20. Dựa vào giá trị Subnet Mask, ta có số lượng các bit thuộc phần NETWORK và phần HOST như sau:

Network	.	Host
20		12
	n	h

Gọi  $n$  là số bit mượn phần HOST và  $h$  là số bit phần Host còn lại. Để có thể hỗ trợ cho phòng ban 500 IP thì  $2^h - 2 \geq 500$ , để chia tiết kiệm IP thì ta cần tìm  $h_{\min}$ . Từ bất đẳng thức trên ta suy ra  $h_{\min} = 9$ .

### Network . Host

20	12
3	9
$\parallel$	$\parallel$
<b>n</b>	<b><math>h_{\min}</math></b>

Ta suy ra  $n = 3$ . Với  $n = 3$ , số lượng mạng con sinh ra là  $2^n = 2^3 = 8$ . Từ giá trị của  $n$ , áp dụng dạng bài tập 2 để xác định địa chỉ các mạng con sinh ra (Subnet).

Octet 3:	Network				Host		
	128	64	32	16	8	4	2
	0	0	0	0	0	0	0
					0	0	1
					0	1	0
					0	1	1
							.....

←  $n=3$

← Trọng số của 8 bit

→ 172.16.0.0/23 (1)

→ 172.16.2.0/23 (2)

→ 172.16.4.0/23 (3)

→ 172.16.6.0/23 (4)

Chọn 1 trong 8 mạng con sinh ra để gán cho phòng ban 500 IP, giả sử chọn mạng 172.16.0.0/23 (1). Phòng ban kế tiếp để tiếp tục hoạch định IP là phòng 200 IP.

#### - Phòng ban 200 IP:

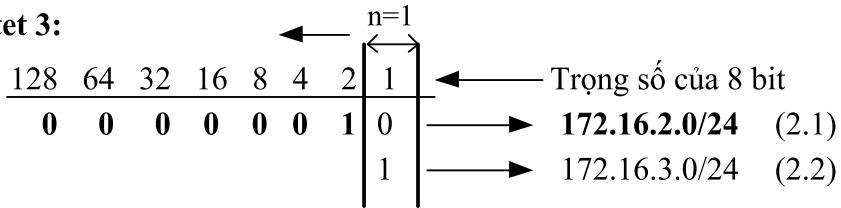
Sử dụng 1 trong 7 mạng con còn lại ở bước trên để chia IP. Giả sử chọn (2) có IP là 172.16.2.0/23. Với các bước làm tương tự, để hỗ trợ được cho mạng này và tiết kiệm số lượng IP thì ta xác định  $h_{\min}$  trong bất đẳng thức  $2^h - 2 \geq 200$ . Từ đó suy ra  $h_{\min} = 8$  và  $n = 1$ .

### Network . Host

23	9
1	8
$\parallel$	$\parallel$
<b>n</b>	<b><math>h_{\min}</math></b>

Xác định địa chỉ của  $2^n = 2^1 = 2$  mạng con sinh ra.

**Octet 3:**

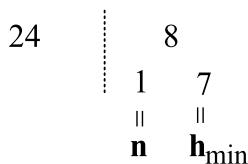


Chọn 1 trong 2 mạng con sinh ra để gán cho phòng ban 200 IP, giả sử chọn mạng 172.16.2.0/24. Phòng ban kế tiếp được xem xét là phòng ban 100 IP.

#### - Phòng ban 100 IP:

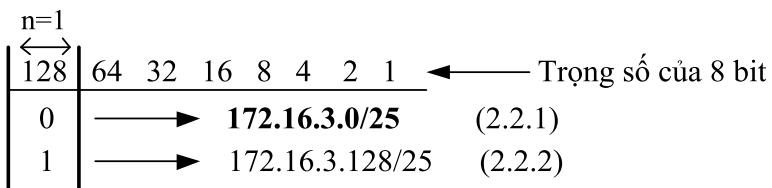
Sử dụng mạng (2.2) hoặc các mạng (3) – (8) để chia IP cho mạng 100 IP, giả sử chọn mạng (2.2) với địa chỉ 172.16.3.0/24. Với các bước làm tương tự, để hỗ trợ được cho mạng này và tiết kiệm số lượng IP thì ta xác định  $h_{\min}$  trong bất đẳng thức  $2^h - 2 \geq 100$ . Từ đó suy ra  $h_{\min} = 7$  và  $n = 1$ .

**Network . Host**



Xác định địa chỉ của  $2^n = 2^1 = 2$  mạng con sinh ra.

**Octet 4:**



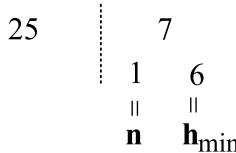
Chọn 1 trong 2 mạng con sinh ra để gán cho phòng ban 100 IP, giả sử chọn mạng 172.16.3.0/25. Phòng ban kế tiếp được xem xét là phòng ban 60 IP.

#### - Phòng ban 60 IP:

Sử dụng mạng (2.2.2) hoặc các mạng (3) – (8) để chia IP cho mạng 60 IP, giả sử chọn mạng (2.2.2) với địa chỉ 172.16.3.128/25. Với các

bước làm tương tự, để hỗ trợ được cho mạng này và tiết kiệm số lượng IP thì ta xác định  $h_{\min}$  trong bất đẳng thức  $2^h - 2 \geq 60$ . Từ đó suy ra  $h_{\min} = 6$  và  $n = 1$ .

### Network . Host



Xác định địa chỉ của  $2^n = 2^1 = 2$  mạng con sinh ra.

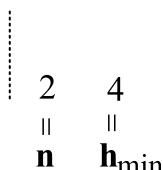
Octet 4:	$\frac{n=1}{128 \quad 64 \quad 32 \quad 16 \quad 8 \quad 4 \quad 2 \quad 1}$								Trọng số của 8 bit
	1	0	1	→ 172.16.3.128/26 (2.2.2.1)	→ 172.16.3.192/26 (2.2.2.2)				

Chọn 1 trong 2 mạng con sinh ra để gán cho phòng ban 60 IP, giả sử chọn mạng 172.16.3.128/25. Phòng ban kế tiếp được xem xét là phòng ban 10 IP.

#### - Phòng ban 10 IP:

Sử dụng mạng (2.2.2.2) hoặc các mạng (3) – (8) để chia IP cho mạng 10 IP, giả sử chọn mạng (2.2.2.2) với địa chỉ 172.16.3.192/26. Với các bước làm tương tự, để hỗ trợ được cho mạng này và tiết kiệm số lượng IP thì ta xác định  $h_{\min}$  trong bất đẳng thức  $2^h - 2 \geq 10$ . Từ đó suy ra  $h_{\min} = 4$  và  $n = 2$ .

### Network . Host

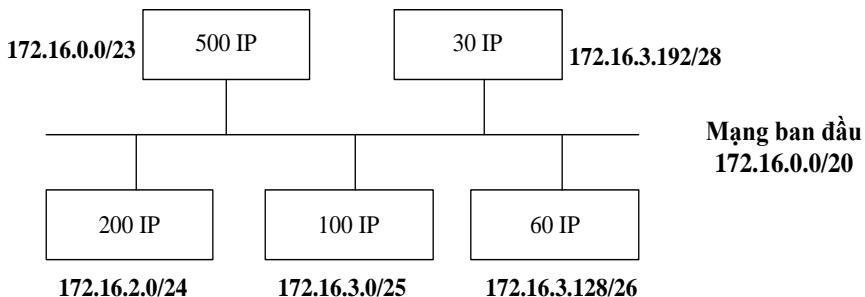


Xác định địa chỉ của  $2^n = 2^2 = 4$  mạng con sinh ra.

**Octet 4:**

		n=2					
128	64	32	16	8	4	2	1
1	1	0	0	→	172.16.3.192/28		
		0	1	→	172.16.3.208/28		
		1	0	→	172.16.3.224/28		
		1	1	→	172.16.3.249/28		

Chọn 1 trong 4 mạng con sinh ra để gán cho phòng ban 10 IP, giả sử chọn mạng 172.16.3.192/28.

**Kết quả chia IP bằng kỹ thuật VLSM:**

**Hình 3.4:** Kết quả hoạch định IP cho một công ty

**Như vậy:** VLSM là kỹ thuật hoạch định địa chỉ IP cho một hệ thống mạng, trong đó các mạng con của cùng một mạng ban đầu sau khi chia có chiều dài Subnet Mask (số bit thuộc phần NETWORK) khác nhau.

**3.2.7. Kỹ thuật CIDR**

CIDR (Classless Inter Domain Routing) là một kỹ thuật hoạch định IP giúp cải thiện việc phân bổ địa chỉ IP. CIDR mở rộng so với hệ thống cũ các lớp A, B và C. CIDR khác VLSM ở chỗ gộp các mạng ở phân lớp chuẩn thành mạng lớn hơn, do đó nó là một cải tiến cho việc thu thập định tuyến.

Địa chỉ IP CIDR bao gồm hai bộ giá trị. Địa chỉ mạng được viết dưới dạng tiền tố, ví dụ: 192.255.255.255; phần thứ hai là hậu tố cho biết có bao nhiêu bit trong toàn bộ địa chỉ dùng làm phần Network, ví dụ: /12. Đặt 2 phần này lại với nhau, một địa chỉ IP CIDR sẽ như sau: 192.255.255.255/12.

Cơ chế đánh địa chỉ này được xem là cấp phát hiệu quả hơn: cơ chế ít lãng phí và linh hoạt hơn, làm tăng hiệu quả và tính mở rộng cho IPv4, là một cải tiến cho việc thu thập định tuyến vì số lượng entry trong bảng định tuyến của Router giảm xuống và tăng số lượng Host được cấp phát trong Network, giảm kích thước các bảng lưu trữ của Router và tăng tốc quá trình tìm kiếm.

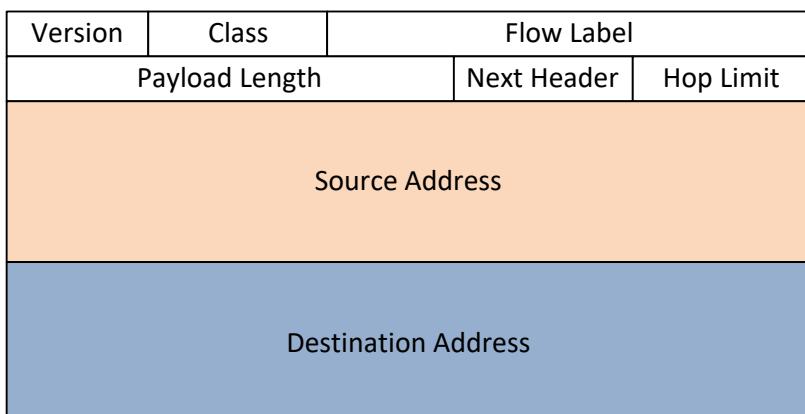
Ví dụ, cho địa chỉ IP CIDR: 192.168.54.0/23. Network address là 192.168.54.0, prefix là /23, do đó 9 bit còn lại có thể được dùng để đánh địa chỉ Host:  $2^9 - 2 = 510$ .

Nếu công ty muốn có yêu cầu gán địa chỉ IP cho nhiều hơn 510 Host, thì ta có thể bớt bit ở NetID, ví dụ /22, tức ta sẽ có:  $2^{10} - 2 = 1022$  Host, thay vì phung phí toàn bộ cả địa chỉ lớp B, hỗ trợ đến 65.534 Host ( $2^{16} - 2$ ).

### 3.3. Địa chỉ IPv6

#### 3.3.1. Giới thiệu

IPv4 là một giao thức cốt lõi và hữu ích cho sự phát triển của TCP/IP và Internet. Sự phát triển của Internet tạo nên một vấn đề lớn đối với IPv4. IPv4 tồn tại một số hạn chế, đặc biệt là không gian địa chỉ không đáp ứng đủ cho số lượng rất lớn các thiết bị cần dùng. Do đó cần thiết phải sử dụng một giao thức thay thế. IPv6 là một phiên bản IP mới, các chức năng cơ bản cũng tương tự như IPv4 như định nghĩa các loại địa chỉ, chia mạng con,... Tuy nhiên, IPv6 có một số khác biệt, như không gian địa chỉ lớn hơn, biểu diễn địa chỉ dưới dạng Hexa,...



**Hình 3.5: IPv6 Header**

Giống như IPv4, IPv6 cũng định nghĩa Header tương ứng. So với IPv4, IPv6 Header có một số thay đổi như đơn giản hơn (số trường ít hơn), có kích thước cố định là 40 byte.

### **Định dạng của địa chỉ IPv6:**

- Cấu trúc tổng quát của một địa chỉ IPv6 cũng gồm 2 phần: phần Prefix có ý nghĩa giống như phần NETWORK trong IPv6 và phần HOST.

Prefix	Host (Interface ID)
--------	---------------------

### **Hình 3.6: Cấu trúc địa chỉ IPv6**

- Địa chỉ IPv6 có 128 bit, được chia thành 8 phần, ngăn cách nhau bởi dấu “:”. Địa chỉ IPv6 được biểu diễn dưới dạng nhị phân hoặc thập lục phân.

Ví dụ: 09A6:0000:0000:31C3:0000:0000:0000:0871

**Nguyên tắc rút gọn địa chỉ IPv6:** Sử dụng 2 luật sau đây để viết tắt địa chỉ IPv6:

- Bỏ 0 ở đầu mỗi phần.
- Thay thế một dãy liên tiếp các phần 0 (2 trở lên) bằng ký hiệu “::” và chỉ được sử dụng một lần trong một địa chỉ IPv6.

Với một địa chỉ IPv6 như trong ví dụ trên, áp dụng luật đầu tiên, thì địa chỉ trên có thể viết thành 9A6:0:0:31C3:0:0:871. Áp dụng luật thứ hai, thì địa chỉ IP trên có thể viết thành 9A6::31C3:0:0:871 hay 9A6:0:0:31C3::871.

### **Biểu diễn Prefix Length trong IPv6:**

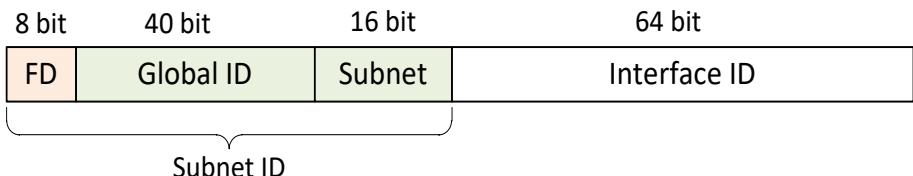
Giống như Subnet Mask trong IPv4, trong IPv6 sử dụng giá trị này với tên gọi là Prefix Length. Nó được biểu diễn dạng /n, với n là một giá trị thập phân (từ 0 đến 128) để xác định Prefix Length giống như xác định Subnet ID trong IPv4.

Ví dụ: 2003::1/64

### **3.3.2. Các loại địa chỉ IPv6**

IPv6 có 3 loại địa chỉ là: Unicast, Multicast và Anycast.

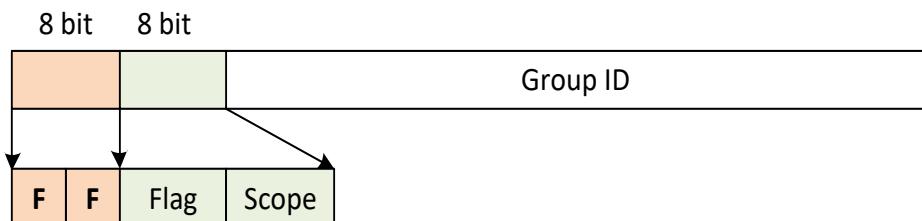
- **Địa chỉ Unicast:** Là địa chỉ được đặt để định danh cho một thiết bị.
  - + Địa chỉ Global Unicast IPv6: Đây là loại địa chỉ có ý nghĩa giống như IP Public trong IPv4.
  - + Địa chỉ Unique Local IPv6:



**Hình 3.7: Địa chỉ Unique Local IPv6**

Địa chỉ Unique Local bắt đầu với 2 giá trị (hex) đầu là FD, loại địa chỉ này có ý nghĩa giống như địa chỉ IP Private trong IPv4. 40 bit tiếp theo được lựa chọn làm Global-ID. Như vậy, ta được 48 bit đầu làm prefix. 16 bit kế tiếp là Subnet và 64 bit còn lại làm phần định danh cho một Host trên mạng.

- **Địa chỉ Multicast:** Là địa chỉ đại diện cho một nhóm các Host. Trong kiểu truyền Multicast có dạng One To Group, nghĩa là lưu lượng sẽ được truyền hết cho các thành viên trong nhóm. Cũng giống như địa chỉ Multicast trong IPv4, IPv6 nó được dùng trong nhiều ứng dụng Multicast. Địa chỉ Multicast được bắt đầu với giá trị FF::/8.



**Hình 3.8: Địa chỉ IPv6 Multicast**

- **Địa chỉ Anycast:** Là địa chỉ đại diện cho một nhóm. Trong kiểu truyền Anycast có dạng One To Nearest, nghĩa là truyền cho địa chỉ gần nhất trong nhóm. Trong đó, Router quyết định thiết bị nào là gần nhất trong nhóm.

Giả sử rằng các Router cần thu thập để cài đặt một số dịch vụ. Thay vì chỉ có một Router cung cấp dịch vụ đó, dịch vụ đó hoạt động tốt khi được cài đặt trên nhiều Router. Nhưng các Host sử dụng dịch vụ này chỉ cần liên lạc đến Router gần nhất, hệ thống mạng sẽ ẩn các chi tiết đối với các Host. Các Host chỉ cần gửi một gói tin và Router sẽ chuyển tiếp gói tin đến Router gần nhất có hỗ trợ dịch vụ này.

Địa chỉ Anycast không sử dụng một dãy IP dành riêng, mà nó sử dụng từ không gian địa chỉ Unicast. Thông thường, nó được cấu hình với prefix /128, Router sẽ quảng bá các Host Route này. Ví dụ cấu hình địa chỉ Anycast trên Cisco Router như sau:

```
R1#config terminal
R1(config)#interface gigabitEthernet 0/0
R1(config)#ipv6 address 2001:1:1:1::1/64
R1(config)#ipv6 address 2001:1:1:2::99/128
anycast
```

Một số loại địa chỉ IPv6:

Loại địa chỉ	Giá trị nhận diện (các giá trị đầu - Hex)
Unique Local	FD
Multicast	FF
Link Local	FE80
Loopback	::1
Unknown	::

### Địa chỉ Link Local:

IPv6 sử dụng địa chỉ Link Local để gửi và nhận dữ liệu trong cùng một mạng. Nó được sử dụng trong một số trường hợp như: dùng làm địa chỉ nguồn trong các gói tin RS và SA để phát hiện các Router, được sử dụng trong giao thức NDP (giống chức năng của ARP trong IPv4) và có thể sử dụng để cấu hình Next Hop trong định tuyến.

10 bit	54 bit	64 bit
FE80/10	000...000	Interface ID

**Hình 3.9: Địa chỉ IPv6 Link Local**

Mỗi Card mạng có thêm một địa chỉ gọi là Link Local. Các gói tin được gửi đến một địa chỉ Link Local bị Router chặn lại, nghĩa là nó chỉ tồn tại trong một mạng mà không thể chuyển tiếp đến một mạng khác. Một số giao thức chỉ cần gửi thông điệp trong cùng mạng (Subnet), khi đó có thể sử dụng địa chỉ Link Local. Ví dụ như giao thức NDP, có chức năng hoạt động giống như ARP trong IPv4, sử dụng địa chỉ Link Local. Địa chỉ Link Local có dạng FE80::/10.

#### **Hoạt động của giao thức NDP:**

- Giống với giao thức ARP trong IPv4, giao thức NDP được sử dụng trong IPv6 để ánh xạ giữa địa chỉ IPv6 của một Host với địa chỉ MAC của nó. Khi một Host hay Router muốn gửi dữ liệu cho một Host hay Router khác trong cùng LAN, Host/Router đầu tiên tìm kiếm trong cơ sở dữ liệu của nó (Neighbor Database). Cơ sở dữ liệu này chứa danh sách các địa chỉ IPv6 và các địa chỉ MAC tương ứng. Nếu không tìm thấy, Host/Router sử dụng giao thức NDP để tự động tìm kiếm địa chỉ MAC.
- PC1 gửi gói NS (Neighbor Solicitation) ICMP dạng Multicast, yêu cầu R1 trả lời với địa chỉ MAC của R1. R1 gửi gói NA (Neighbor Advertisement) ICMP dạng Unicast lại cho PC1 với thông tin địa chỉ MAC của R1. R1 bây giờ địa chỉ MAC đích trong Frame là địa chỉ MAC của R1.

#### **3.3.3. Chia mạng con trong IPv6**

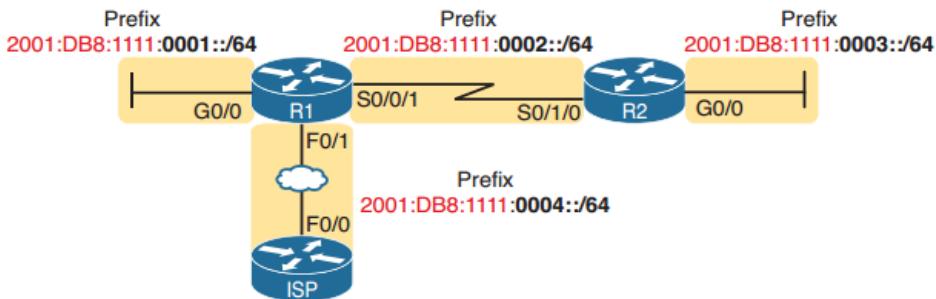
Tương tự như địa chỉ IPv4, địa chỉ IPv6 cũng hỗ trợ việc hoạch định IP cho phù hợp với kích thước của mạng cần sử dụng. Các bit thuộc phần Subnet ở hình dưới được sử dụng để chia mạng con.

P bit	S bit	I bit
Global Routing Prefix	Subnet	Interface ID

$P + S + I = 128$

**Hình 3.10: Chia mạng con trong IPv6**

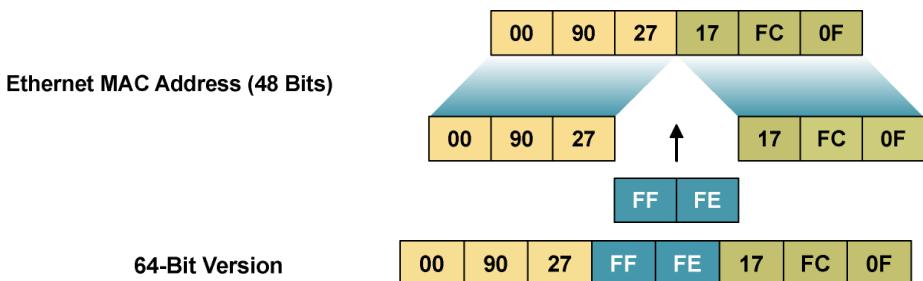
Ví dụ:



**Hình 3.11:** Ví dụ về hoạch định IP cho các mạng IPv6

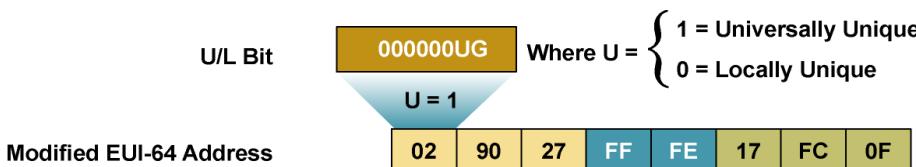
### 3.3.4. Địa chỉ EUI-64

Cách thiết lập địa chỉ IPv6, với 64 bit phần Host được xác định dựa vào địa chỉ MAC của Card mạng. Các bước thiết lập như sau: địa chỉ MAC (48 bit) được chia làm 2 phần, sau đó chèn FFFE vào giữa.



**Hình 3.12:** Thành lập địa chỉ dạng EUI-64

Bit thứ 7 (bit U) được chuyển thành “1”. Từ đó có được 64 bit phần Host. 64 bit này sẽ kết hợp với 64 bit phần Prefix tạo thành 1 địa chỉ IPv6 cho Card mạng.

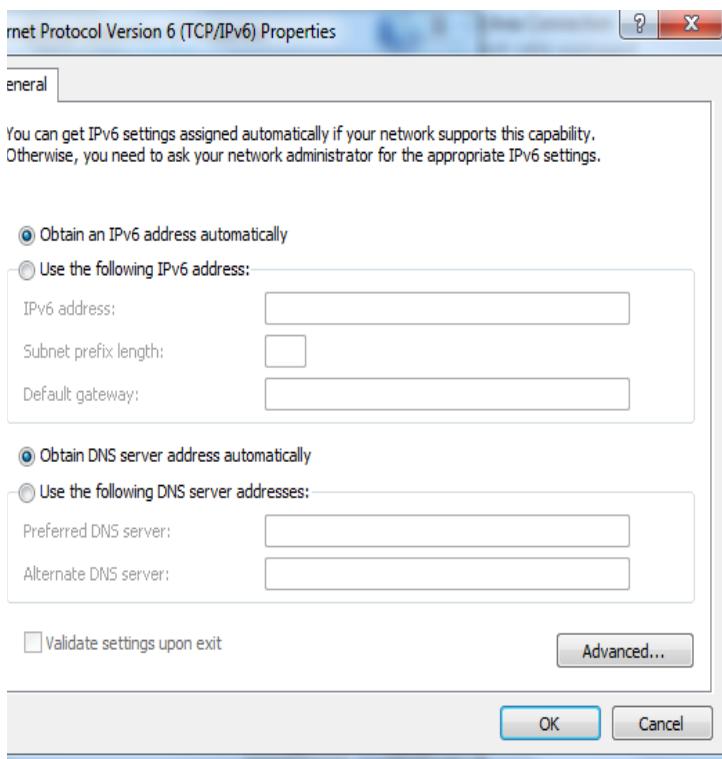


**Hình 3.13:** Địa chỉ EUI-64

### 3.3.5. Gán địa chỉ cho Card mạng

Tương tự như IPv4, để gán địa chỉ IPv6 cho Card mạng có thể gán tĩnh hoặc gán động.

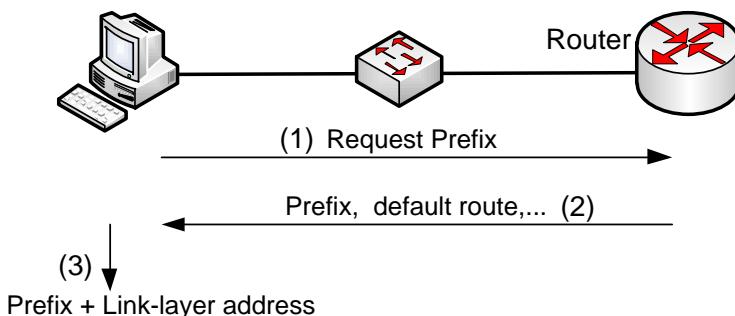
- Đặt địa chỉ IPv6 tĩnh: Ở các hệ điều hành phổ biến hiện tại đều hỗ trợ cấu hình Card mạng sử dụng địa chỉ IPv6.



**Hình 3.14:** Cấu hình IPv6 cho Card mạng trên hệ điều hành Windows

- Gán IP động: Có 2 trường hợp là: (1) thiết bị tự động cấu hình, và (2) sử dụng DHCP Server để cấp phát.

Trường hợp 1: Thiết bị tự động cấu hình (Stateless Autoconfiguration).



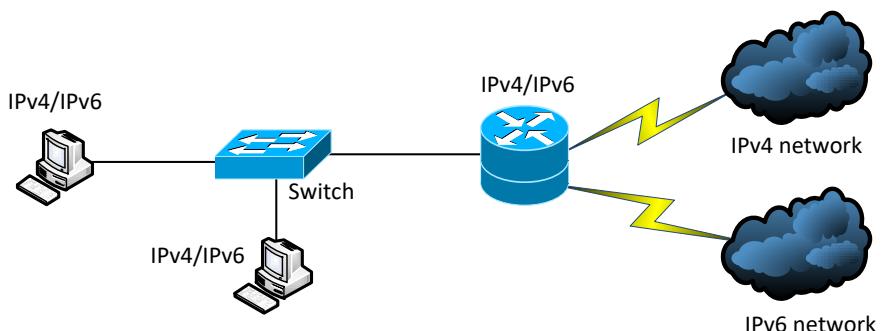
**Hình 3.15.** Cấu hình IPv6 tự động cho Host dạng Stateless

Trường hợp 2: Sử dụng DHCP Server để cấp phát.

### 3.3.6. Các kỹ thuật chuyển đổi IPv4 và IPv6

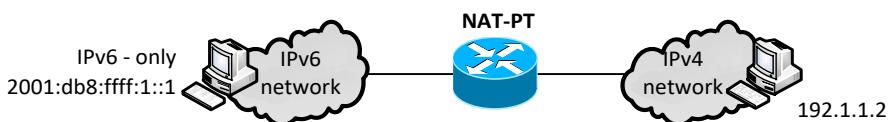
Trong quá trình triển khai thế hệ địa chỉ IPv6 trên mạng Internet, khi đó hai thế hệ mạng IPv4 và IPv6 sẽ cùng tồn tại trong một thời gian rất dài. Trong quá trình phát triển, các kết nối IPv6 sẽ tận dụng cơ sở hạ tầng sẵn có của IPv4. Do vậy cần có những công nghệ phục vụ cho việc chuyển đổi từ địa chỉ IPv4 sang địa chỉ IPv6 và đảm bảo không phá vỡ cấu trúc Internet cũng như làm gián đoạn hoạt động của mạng Internet. Những công nghệ chuyển đổi này, cơ bản có thể phân thành ba loại như sau:

- **Dual Stack:** Cho phép IPv4 và IPv6 cùng tồn tại trong cùng một thiết bị mạng.



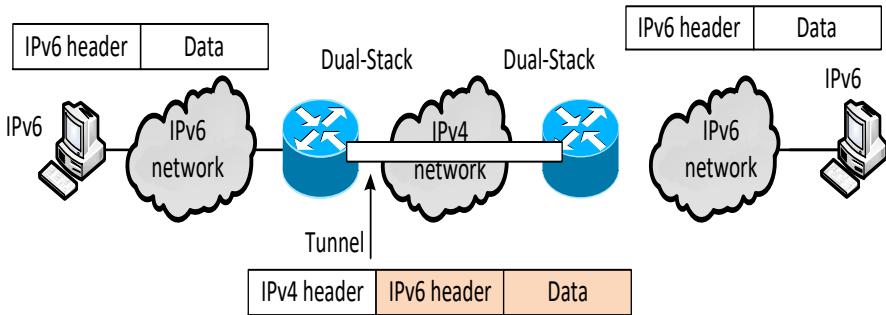
**Hình 3.16:** Kỹ thuật chuyển đổi Dual Stack

- Công nghệ biên dịch: Thực chất là một dạng thức của kỹ thuật NAT, cho phép thiết bị chỉ hỗ trợ IPv6 có thể giao tiếp với thiết bị chỉ hỗ trợ IPv4.



**Hình 3.17:** Kỹ thuật chuyển đổi NAT-TP

- Công nghệ đường hầm (Tunnel): Công nghệ sử dụng cơ sở hạ tầng mạng IPv4 để truyền tải gói tin IPv6, phục vụ cho kết nối IPv6.



*Hình 3.18: Kỹ thuật chuyển đổi Tunnel*

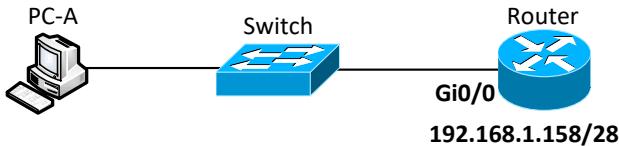
### 3.4. Tổng kết chương

Địa chỉ IP là định danh quan trọng mà những thiết bị điện tử hiện nay đang sử dụng để nhận diện và liên lạc với nhau trên mạng máy tính bằng cách sử dụng giao thức Internet. Hiểu được về cấu trúc thành phần, chia lớp của địa IP sẽ giúp chúng ta tự mình khắc phục các vấn đề về kết nối mạng, biết cách lưu trữ hoặc lấy dữ liệu từ máy tính này sang máy tính khác, cài đặt một Server lưu trữ dữ liệu dùng chung. Với một người quản trị mạng, nắm được kiến thức về địa chỉ IP sẽ giúp cho việc quản lý vận hành các thiết bị và dịch vụ mạng thuận tiện hơn.

### 3.5. Câu hỏi và bài tập

1. Địa chỉ IP nào sau đây là địa chỉ thuộc lớp B (Class B)?
  - A. 10.10.10.1.
  - B. 100.128.254.1.
  - C. 190.162.41.1.
  - D. 192.168.12.1.
2. Địa chỉ IP nào sau đây là địa chỉ dạng Private?
  - A. 11.11.11.11.
  - B. 172.30.150.1.
  - C. 172.50.30.1.
  - D. 193.120.56.1.
3. Số lượng địa chỉ IP có thể gán cho các thiết bị cùng mạng nhiều nhất là bao nhiêu khi sử dụng giá trị Subnet Mask là 255.255.255.224?

- A. 14.
  - B. 15.
  - C. 16.
  - D. 30.
  - E. 31.
4. Địa chỉ nào sau đây là địa chỉ Broadcast của mạng chứa máy tính có IP là 192.168.190.55/27?
- A. 255.255.190.55.
  - B. 192.168.190.59.
  - C. 192.168.190.63.
  - D. 192.168.190.0.
5. Cho sơ đồ mạng:

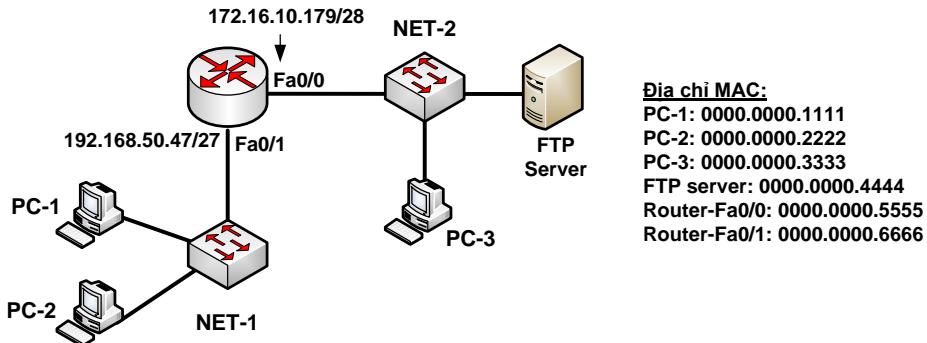


Địa chỉ IP nào sau đây có thể được gán cho PC-A?

- A. 192.168.1.143/28.
  - B. 192.168.1.144/28.
  - C. 192.168.1.145/28.
  - D. 192.168.1.159/28.
  - E. 192.168.1.160/28.
6. Những địa chỉ IP nào sau đây là địa chỉ Public?
- A. 10.172.13.65.
  - B. 172.16.223.125.
  - C. 172.64.12.29.
  - D. 192.168.23.252.
  - E. 198.234.12.95.
  - F. 212.193.48.254.

7. Bạn đang tạo dãy địa chỉ DHCP cho mạng con (Subnet) 192.168.1.32/28. Mạng con gồm các máy Windows 2019, Windows 10, và 2 máy Linux. Hai máy Linux được gán địa chỉ IP tĩnh lớn nhất thuộc mạng con này. Gateway được gán địa chỉ IP tĩnh nhỏ nhất của mạng con này. Xác định dãy địa chỉ IP nào mà bạn sẽ tạo trên DHCP Server?

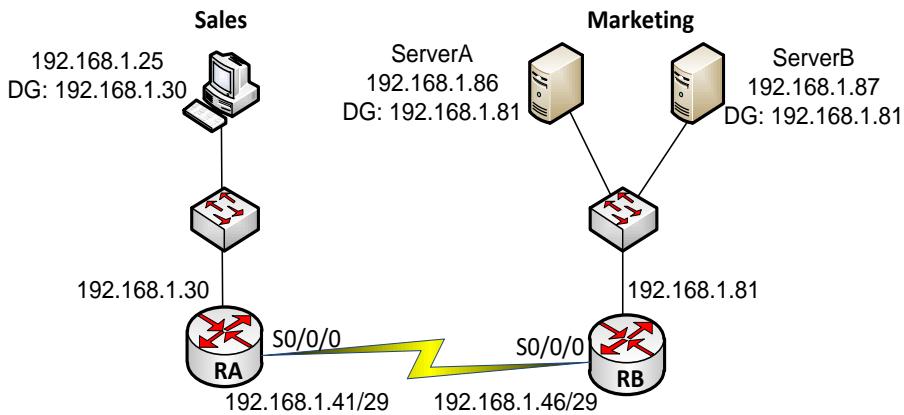
8. Cho sơ đồ mạng:



- Địa chỉ PC-1 và PC-2 lần lượt là địa chỉ IP đầu tiên và cuối cùng trong mạng NET-1.
- Địa chỉ của PC-3 và FTP-Server có địa chỉ IP đầu tiên và cuối cùng trong mạng NET-2.

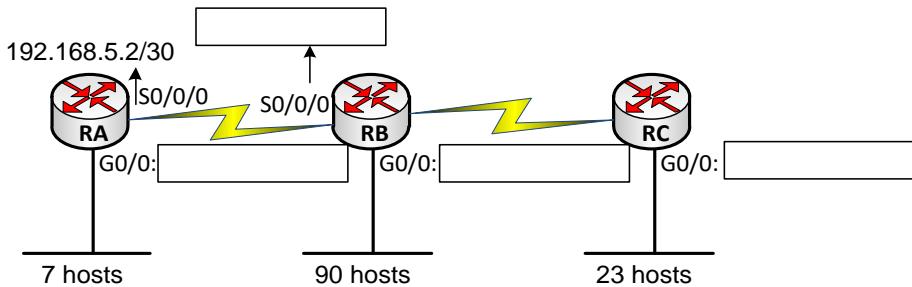
- A. Xác định địa chỉ IP cho PC-1, PC-2, PC-3, FTP-Server?
- B. PC-1 đang Ping tới FTP Server. Xác định các địa chỉ MAC nguồn, MAC đích và IP nguồn và IP đích trong Frame mà FTP Server nhận được?
9. Địa chỉ nào sau đây là Prefix của địa chỉ  
2000:0000:0000:0005:6000:0700:0080:0009/64?
- A. 2000::5:/64.
  - B. 2000::5:0:0:0:0/64.
  - C. 2000:0:0:5:/64.
  - D. 2000:0:0:5:0:0:0:0/64.
10. Những địa chỉ nào sau đây là địa chỉ Host cho mạng có địa chỉ 192.168.15.19/28? (Chọn 2).

- A. 192.168.15.17.
  - B. 192.168.15.14.
  - C. 192.168.15.29.
  - D. 192.168.15.16.
11. Một mạng được hỗ trợ bởi kỹ thuật VLSM. Để giảm sự lãng phí địa chỉ IP trong các kết nối WAN dạng điểm, số bit của Subnet Mask được dùng là:
- A. /35.
  - B. /30.
  - C. /27.
  - D. /23.
12. Máy của Sales không liên lạc được với Server B. Những địa chỉ IP nào bị đánh sai?



- A. 192.168.1.25.
- B. 192.168.1.30.
- C. 192.168.1.81.
- D. 192.168.1.86.
- E. 192.168.1.87.
- F. 192.168.1.41.
- G. 192.168.1.42.

13. Đánh địa chỉ IP phù hợp vào các ô trống trên hình vẽ:



- A. 192.168.55.57/27.
  - B. 192.168.55.29/28.
  - C. 192.168.55.1/30.
  - D. 192.168.55.132/25.
  - E. 192.168.55.0/30.
  - F. 192.168.55.127/26.
14. Bạn đang quản trị mạng công ty A, mạng này được cung cấp địa chỉ là 165.100.27.0/24. Cho biết mạng này được chia ra bao nhiêu mạng con, và bao nhiêu Host được dùng trong mỗi mạng con?
- A. Một mạng, với 254 IP.
  - B. 254 mạng, với 254 IP/mạng.
  - C. 65.534 mạng, với 255 IP/mạng.
  - D. 30 mạng, với 64 mạng.
  - E. 254 mạng, với 65.534/mạng.
15. Những địa chỉ IP nào dưới đây thuộc khối địa chỉ CIDR của mạng 215.64.4.0/22?
- A. 215.64.8.32.
  - B. 215.64.3.255.
  - C. 215.64.6.255.
  - D. 215.64.7.64.
  - E. 215.64.5.128.
  - F. 215.64.12.128.

16. Một mạng con lớp B mượn 5 bit để chia Subnet thì Subnet Mask sẽ là:
- 255.255.248.0.
  - 255.255.255.1.
  - 255.255.255.248.
  - 255.255.255.128.
17. Mạng có Subnet Mask 255.255.255.192 có thể đánh địa chỉ cho bao nhiêu máy:
- 192.
  - 124.
  - 64.
  - 62.
18. Địa chỉ IPv6 nào dưới đây tương đương với địa chỉ Loopback của IPv4 127.0.0.1?
- ::1.
  - 0::/10.
  - ::.
  - 2000::/3.
19. Địa chỉ nào biểu diễn địa chỉ Link Local của IPv6?
- FE81::280f.512b:e14f:3d69.
  - FE80::380e:611a:e14f:3d69.
  - FE08::280e:611:a:f14f.3d69.
  - FEFE:0345:5f1b::e14d:3d69.
20. Những kỹ thuật nào sau đây dùng để triển khai mạng IPv6 qua môi trường IPv4?
- NAT-PT.
  - Dual Stack.
  - Ánh xạ tĩnh giữa IPv4 và IPv6.
  - Cấu hình trực tiếp IPv6.
  - Dùng DHCPv6 để ánh xạ IPv4 sang IPv6.
  - Dùng phương pháp đường hầm (Tunnel).

## CHƯƠNG 4

# KỸ THUẬT TRÊN HẠ TẦNG MẠNG

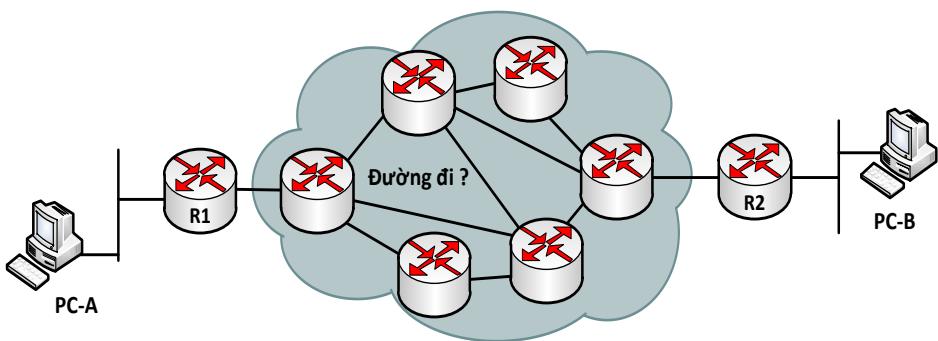
Chương này trình bày đặc điểm cơ bản của một kỹ thuật được sử dụng phổ biến trên hạ tầng mạng như kỹ thuật định tuyến trên Router và một số kỹ thuật trên Switch như VLAN, STP,... Học xong chương này, người học có khả năng:

- Xác định được vai trò và đặc điểm của chức năng định tuyến trong hệ thống mạng.
- Phân biệt được các loại định tuyến.
- Trình bày được khái niệm và đặc điểm của VLAN, VTP, STP.
- Cấu hình VLAN, VTP, STP trên Switch.
- Cấu hình định tuyến giữa các VLAN.

### 4.1. Định tuyến

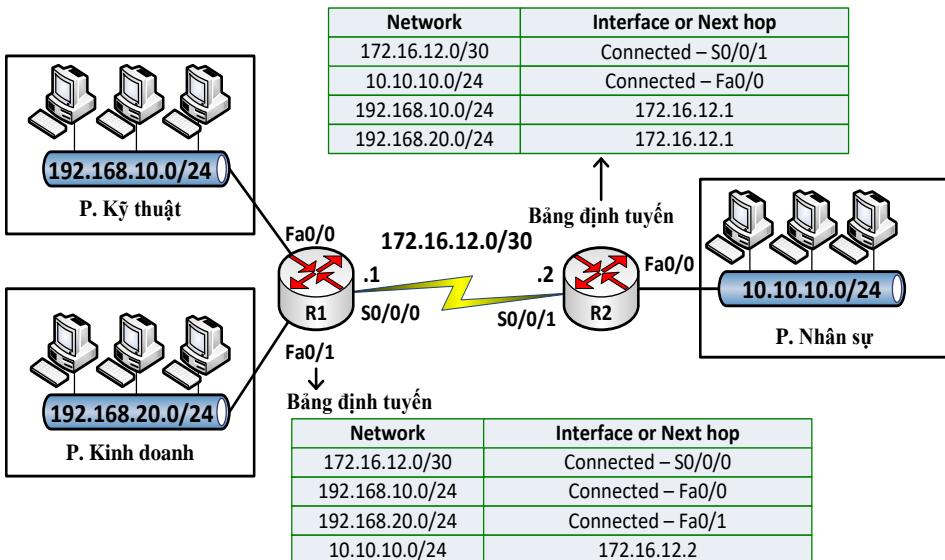
#### 4.1.1. Giới thiệu

Định tuyến là chức năng của Router giúp xác định đường đi cho các gói tin từ nguồn tới đích thông qua hệ thống mạng.



**Hình 4.1: Mô hình hệ thống mạng**

Router dựa vào địa chỉ IP đích (Destination IP) trong các gói tin và sử dụng bảng định tuyến (Routing Table) để xác định đường đi cho chúng.



**Hình 4.2: Bảng định tuyến trên Router**

Trong bảng định tuyến, mỗi mạng mà Router có thể chuyển đi (mạng đích) thể hiện bằng một dòng. Mỗi mạng này có được có thể do chúng đang kết nối trực tiếp với Router đang xét hay Router học được thông qua việc cấu hình định tuyến.

#### 4.1.2. Phân loại định tuyến

Có hai loại định tuyến: định tuyến tĩnh và định tuyến động.

##### + Định tuyến tĩnh:

Định tuyến tĩnh là loại định tuyến mà trong đó Router sử dụng các tuyến đường đi tĩnh để vận chuyển dữ liệu đi. Các tuyến đường đi tĩnh này có được do người quản trị cấu hình thủ công vào các Router.

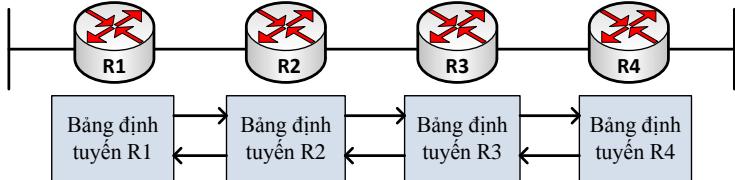
##### + Định tuyến động:

Định tuyến động là loại định tuyến mà trong đó Router sử dụng các tuyến đường đi động để vận chuyển dữ liệu đi. Các tuyến đường đi động này có được do các Router sử dụng các giao thức định tuyến động trao đổi thông tin định tuyến với nhau tạo ra.

Một số giao thức định tuyến động phổ biến: RIP, OSPF, BGP,...

Trong định tuyến động, người ta chia ra thành 2 loại: Distance Vector và Link State.

- **Distance Vector:**



**Hình 4.3:** Trao đổi thông tin định tuyến dạng Distance Vector

Các Router định tuyến loại “Distance Vector” thực hiện gửi định kỳ toàn bộ bảng định tuyến của mình và chỉ gửi cho các Router láng giềng kết nối trực tiếp với mình.

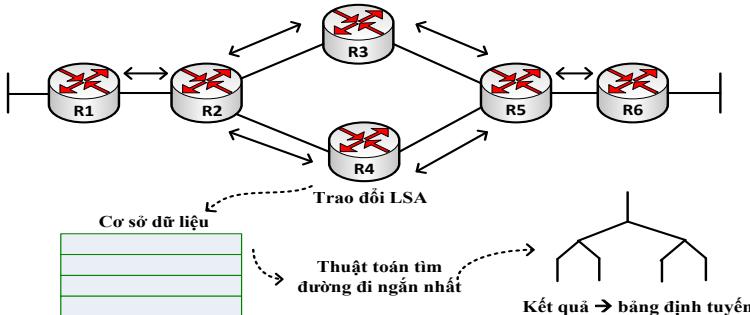
Các Router định tuyến theo dạng này không biết được đường đi đến đích một cách cụ thể, không biết về các Router trung gian trên đường đi và cấu trúc kết nối giữa chúng.

Bảng định tuyến là nơi lưu kết quả chọn đường tốt nhất của mỗi Router. Do đó, khi chúng trao đổi bảng định tuyến với nhau, các Router chọn đường dựa trên kết quả đã chọn của Router láng giềng. Mỗi Router nhìn hệ thống theo sự chi phối của các Router láng giềng.

Các Router định tuyến theo “Distance Vector” thực hiện cập nhật thông tin định tuyến theo định kỳ nên tồn tại nhiều băng thông đường truyền. Khi có sự thay đổi xảy ra, Router nào nhận biết sự thay đổi đầu tiên sẽ cập nhật bảng định tuyến của mình trước rồi chuyển bảng định tuyến cập nhật cho các Router láng giềng.

Giao thức định tuyến thuộc loại này: RIP.

- **Link State:**



**Hình 4.4:** Trao đổi thông tin định tuyến dạng Link State

Trong các giao thức định tuyến loại Link State, các Router sẽ trao đổi các LSA (Link State Advertisement) với nhau để xây dựng và duy trì cơ sở dữ liệu về trạng thái các đường liên kết hay còn gọi là cơ sở dữ liệu về cấu trúc mạng (Topology Database). Các thông tin trao đổi được gửi dưới dạng Multicast.

Như vậy mỗi Router đều có một cái nhìn đầy đủ và cụ thể về cấu trúc của hệ thống mạng. Từ đó mỗi Router sẽ dùng thuật toán tìm đường đi ngắn nhất (SPF - Shortest Path First) để tính toán chọn đường đi tốt nhất đến từng mạng đích.

Khi các Router định tuyến theo Link State đã hội tụ xong, nó không thực hiện cập nhật định tuyến định kỳ mà chỉ cập nhật khi nào có sự thay đổi xảy ra. Do đó, thời gian hội tụ nhanh và ít tốn băng thông.

Giao thức định tuyến theo Link State có hỗ trợ CIDR, VLSM nên chúng là một chọn lựa tốt cho các mạng lớn và phức tạp. Nhưng đồng thời nó đòi hỏi dung lượng bộ nhớ lớn và khả năng xử lý mạnh của CPU trên các Router.

Để đảm bảo cho các cơ sở dữ liệu cập nhật thông tin mới, trong các LSA này được đánh thêm chỉ số tuần tự “Sequence”. Chỉ số “Sequence” được bắt đầu từ giá trị Initial đến giá trị Max Age. Khi một Router nào đó tạo ra một LSA, nó sẽ đặt giá trị Sequence bằng Initial. Mỗi khi Router gửi ra một phiên bản LSA, nó sẽ tăng giá trị đó lên 1. Như vậy, giá trị Sequence càng cao thì thông tin LSA càng mới. Nếu giá trị Sequence này đạt đến Max Age, Router sẽ gửi LSA ra cho tất cả các Router còn lại, sau đó Router đó sẽ đặt lại giá trị Sequence về Initial.

Một số giao thức định tuyến thuộc loại này: OSPF, IS-IS.

Ngoài cách phân loại như trên, người ta còn chia giao thức định tuyến động theo 2 dạng: “Classful Routing Protocol” và “Classless Routing Protocol”.

#### - Giao thức định tuyến dạng Classfull

Các giao thức định tuyến nhóm Classfull không quảng bá Subnet Mask cùng với địa chỉ mạng quảng bá trong các gói tin cập nhật định tuyến. Do đó, khi Router nhận được các cập nhật này, Router phải lấy giá trị Network Mask mặc định có cùng với địa chỉ lớp mạng của địa chỉ

dích. Nếu địa chỉ mạng đó được kết nối trực tiếp với Router, Network Mask được lấy cùng với Network Mask được cấu hình trên cổng kết nối đến mạng đó. Nếu địa chỉ mạng đích không nối trực tiếp, Router sẽ lấy địa chỉ Subnet Mask mặc định của địa chỉ mạng đích.

Các giao thức thuộc loại này không hỗ trợ mạng VLSM, tóm tắt các tuyến tự động. Giao thức định tuyến dạng này: RIPv1.

- **Giao thức định tuyến dạng Classless**

Các giao thức định tuyến thuộc nhóm Classless sẽ quảng bá thông tin “Subnet Mask” cùng với địa chỉ mạng quảng bá trong các gói tin cập nhật định tuyến, hỗ trợ VLSM, cho phép tóm tắt các tuyến một cách thủ công.

Các giao thức định tuyến thuộc dạng này: RIPv2, OSPF, EIGRP.

### **Hai tham số dùng trong định tuyến: Metric và AD.**

- **Metric:**

Là tham số được sử dụng để chọn đường tốt nhất cho việc định tuyến. Đây là giá trị mà bất kỳ giao thức định tuyến nào cũng phải dùng để tính toán đường đi đến mạng đích.

Trong trường hợp có nhiều đường đi đến một mạng đích thì đường đi nào có Metric thấp nhất sẽ được lựa chọn để đưa vào bảng định tuyến. Mỗi giao thức định tuyến có một kiểu Metric khác nhau.

- **AD:**

AD (Administrative Distance) là giá trị quy ước dùng để chỉ độ tin cậy của các giao thức định tuyến, giao thức nào có AD nhỏ hơn sẽ được xem là đáng tin cậy hơn. Trong trường hợp Router học được một mạng đích thông qua nhiều giao thức định tuyến khác nhau, thì tuyến của giao thức định tuyến nào có AD nhỏ nhất thì sẽ được lựa chọn và đưa vào bảng định tuyến.

#### **4.1.3. Cấu hình định tuyến tĩnh**

Trong cấu hình định tuyến tĩnh, người quản trị phải cấu hình thủ công chỉ ra đường đi đến tất cả các mạng đích trên các Router trong hệ thống. Định tuyến tĩnh không có hoạt động gửi thông tin cập nhật như các giao thức định tuyến động.

Lưu ý: Mặc định Router sẽ biết được đường đi đến các mạng đích đang kết nối trực tiếp với nó.

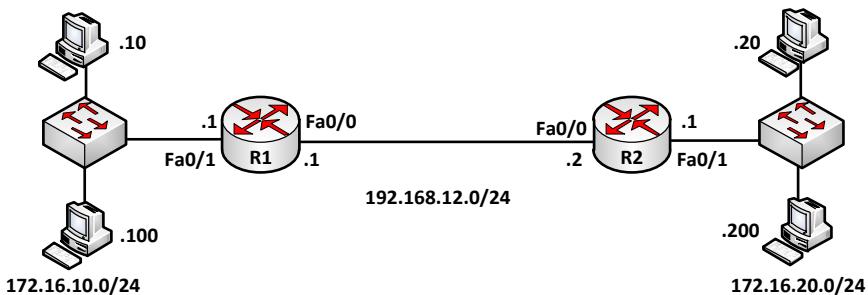
Để cấu hình định tuyến tĩnh, chúng ta sử dụng cú pháp sau:

```
Router(config)#ip route <destination> <subnet-mask> {Next-hop  
|Outgoing -interface>}
```

Trong đó:

- Destination Network: Là địa chỉ mạng đích cần đi tới.
- Subnet Mask: Subnet Mask của Destination Network.
- Next Hop Address: Địa chỉ IP của cổng trên Router kế tiếp có kết nối trực tiếp với Router đang xét.
- Out Bound Interface: Cổng của Router sẽ gửi dữ liệu ra.
- Distance: Thay đổi giá trị AD cho tuyến này. Mặc định các tuyến tĩnh có AD = 1.

Ví dụ: Cấu hình định tuyến tĩnh cho mô hình mạng sau:



**Hình 4.5:** Mô hình ví dụ cho cấu hình định tuyến tĩnh

**Nhận xét:** Trong mô hình mạng đã cho có 3 mạng: 172.16.10.0/24, 192.168.12.0/24 và 172.16.20.0/24. Để hệ thống mạng liên thông với nhau thì trong bảng định tuyến của các Router R1 và R2 phải có đường đi đến tất cả các mạng này. Do mặc định các Router biết được đường đi đến các mạng đang kết nối trực tiếp với nó nên:

- + Router R1: Đã biết được đường đi đến 2 mạng đang kết nối trực tiếp là 172.16.10.0/24 và 192.168.12.0/24. Đối với mạng 172.16.20.0/24, chúng ta cấu hình định tuyến tĩnh như sau:

```
R1 (config) #ip route 172.16.20.0 255.255.255.0 fa0/0
```

Hoặc:

```
R1(config)#ip route 172.16.20.0 255.255.255.0  
192.168.12.2
```

- + Router R2: Tương tự Router R1, mặc định R2 biết được đường đi đến 2 mạng đang kết nối trực tiếp với nó là 192.168.12.0/24 và 172.16.20.0/24. Chúng ta cần chỉ ra đường đi đến mạng 172.16.10.0/24 bằng định tuyến tĩnh như sau:

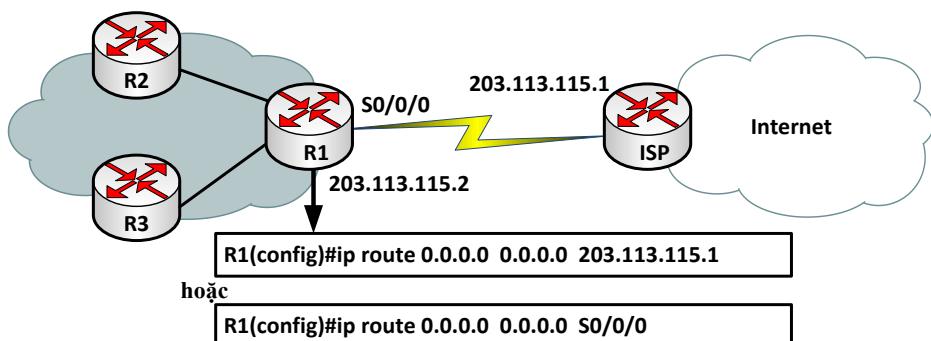
```
R2(config)#ip route 172.16.10.0 255.255.255.0 fa0/0
```

Hoặc:

```
R2(config)#ip route 172.16.10.0 255.255.255.0  
192.168.12.1
```

### Default Route:

Default Route nằm ở cuối bảng định tuyến và được sử dụng để gửi các gói tin đi trong trường hợp mạng đích không tìm thấy trong bảng định tuyến. Nó rất hữu dụng trong các mạng dạng “stub network” như kết nối từ mạng nội bộ ra ngoài Internet.



*Hình 4.6: Cấu hình Default Route*

#### 4.1.4. Cấu hình định tuyến động

##### 4.1.4.1. RIP

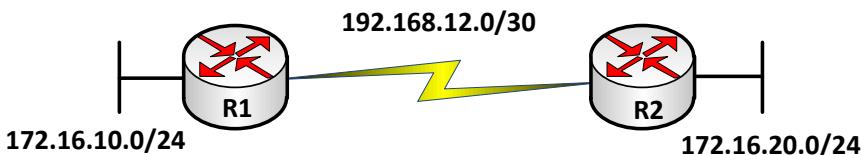
RIP là một giao thức định tuyến theo kiểu “Distance Vector”. “Hop Count” được sử dụng làm Metric cho việc chọn đường. Nếu có nhiều đường đến cùng một đích thì RIP sẽ chọn đường nào có số Hop Count (số Router đi qua) ít nhất. RIP hỗ trợ tính năng chia tải (Load Balancing) mặc định là 4 đường, tối đa 16 đường.

Nếu Hop Count lớn hơn 15 thì các gói tin sẽ bị loại bỏ. Mặc định thời gian cập nhật định tuyến là 30 giây. Giá trị AD mặc định của RIP là 120. RIP có hai phiên bản là RIPv1 và RIPv2.

**Bảng 4.1:** So sánh giữa RIPv1 và RIPv2

Đặc điểm	RIPv1	RIPv2
Loại định tuyến	Classful	Classless
Hỗ trợ VLSM và mạng không liên tục	Không	Có
Gửi kèm Subnet Mask trong bản tin cập nhật định tuyến	Không	Có
Quảng bá thông tin định tuyến	Broadcast	Multicast
Hỗ trợ tóm tắt các tuyến thủ công	Không	Có
Hỗ trợ chứng thực	Không	Có
Định nghĩa trong RFC	RFC 1058	RFC 1721, 1722, 2453

Mạng không liên tục (Discontiguous Network): Là mạng mà trong đó các mạng con (Subnet) của cùng một mạng lớn (Major Network: là mạng theo đúng lớp) bị ngăn cách bởi “Major Network” khác.



**Hình 4.7:** Mạng không liên tục

Hai mạng con của cùng một “Major Network” là 172.16.0.0 bị ngăn cách bởi một “Major Network” khác là 192.168.12.0 tạo nên mạng không liên tục.

- **Cấu hình:**

- + Khởi tạo tiến trình định tuyến RIP:

```
Router(config)#router rip
```

- + Bật chế độ RIPv2:

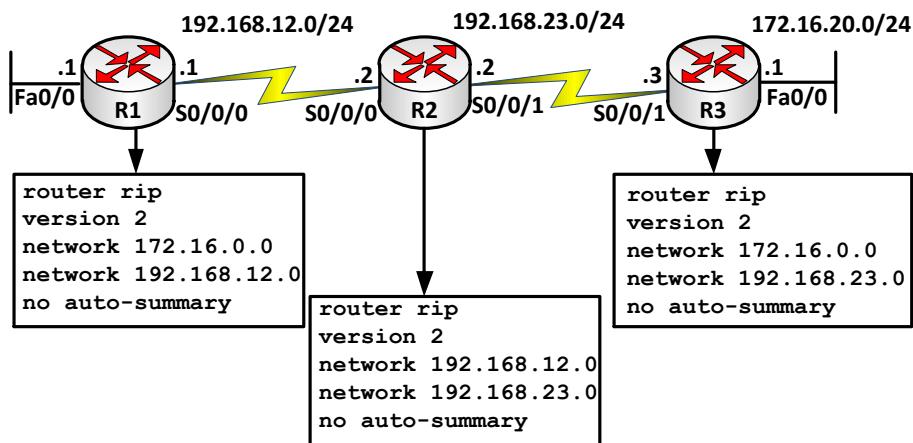
```
Router(config-router)#version 2 //sử dụng cho RIPv2
```

- + Chọn cổng tham gia vào quá trình trao đổi thông tin định tuyến:  

```
Router(config-router) #network <major-classful-network>
```
- + Tắt tính năng tự động tóm tắt các tuyến:  

```
Router(config-router) #no auto-summary //sử dụng cho RIPv2
```

- **Ví dụ:**



**Hình 4.8: Sơ đồ ví dụ cho cấu hình RIP**

- **Chứng thực trong RIPv2:**

Chứng thực trong định tuyến là cách thức bảo mật trong việc trao đổi thông tin định tuyến giữa các Router. Nếu có cấu hình chứng thực thì các Router phải vượt qua quá trình này trước khi các thông tin trao đổi định tuyến được thực hiện. RIPv2 hỗ trợ hai kiểu chứng thực là: “Plain Text” và “MD5”.

+ **Chứng thực dạng “Plain Text”:** còn gọi là “Clear Text”.

Quá trình chứng thực chỉ đơn giản là các Router được cấu hình một khóa (Password) và trao đổi chúng để so khớp. Các khóa này được gửi dưới dạng không mã hóa trên đường truyền.

### Các bước cấu hình:

Bước 1. Tạo bộ khóa:

```
Router(config) #key chain <name>
```

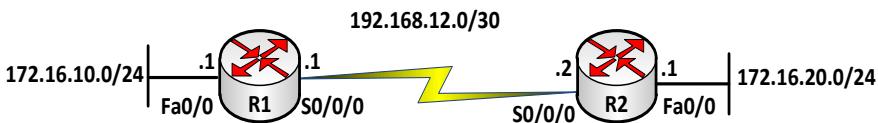
Bước 2. Tạo các khóa:

```
Router(config-keychain) #key <key-id>  
Router(config-keychain-key) #key-string <password>
```

### Bước 3. Áp đặt vào cổng gửi chứng thực:

```
Router(config) #interface <interface>  
Router(config-if) #ip rip authentication key-chain  
<name>
```

**Ví dụ:** Cấu hình chứng thực trong định tuyến RIPv2 dạng “Plain Text”:



**Hình 4.9:** Ví dụ cấu hình chứng thực Plain Text trong RIPv2

```
R1(config) #key chain newstar  
R1(config-keychain) #key 1  
R1(config-keychain-key) #key-string ccna  
R1(config) #interface S0/0/0  
R1(config-if) #ip rip authentication key-chain newstar  
R2(config) #key chain newstar2  
R2(config-keychain) #key 1  
R2(config-keychain-key) #key-string ccna  
R2(config) #interface S0/0/0  
R2(config-if) #ip rip authentication key-chain newstar2
```

### + Chứng thực dạng MD5:

Dạng chứng thực này sẽ gửi thông tin về khóa đã được mã hóa giúp các thông tin trao đổi được an toàn hơn. Các bước cấu hình tương tự như dạng “Plain Text”, chỉ có khác ở bước 3 phải thêm 1 lệnh sau:

```
Router(config-if) #ip rip authentication mode md5
```

**Ví dụ:** Sử dụng lại mô hình mạng trong ví dụ chứng thực dạng “Plain Text”, chúng ta sẽ cấu hình chứng thực định tuyến RIPv2 bằng MD5 với tên bộ khóa là “spkt” và mật khẩu là “123456” trên R1 và tên bộ khóa là “cntt” và mật khẩu là “123456” trên R2.

```
R1(config)#key chain spkt
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string 123456
R1(config)#interface S0/0/0
R1(config-if)#ip rip authentication mode md5
R1(config-if)#ip rip authentication key-chain spkt
```

```
R2(config)#key chain cntt
R2(config-keychain)#key 1
R2(config-keychain-key)#key-string 123456
R2(config)#interface S0/0/0
R2(config-if)#ip rip authentication mode md5
R2(config-if)#ip rip authentication key-chain cntt
```

### Các lệnh kiểm tra cấu hình:

```
R#debug ip rip
R#show ip route
```

#### 4.1.4.2. OSPF

OSPF (Open Shortest Path First) là một giao thức định tuyến dạng Link State, sử dụng thuật toán Dijkstra để xây dựng bảng định tuyến.

OSPF mang những đặc điểm của giao thức Link State. Nó có ưu điểm là hội tụ nhanh, hỗ trợ được mạng có kích thước lớn và không xảy ra “Routing Loop”. OSPF đồng thời là giao thức định tuyến dạng Classless nên hỗ trợ VLSM và mạng không liên tục. OSPF sử dụng địa chỉ Multicast 224.0.0.5 và 224.0.0.6 (DR và BDR Router) để gửi các thông điệp Hello và Update trong quá trình cập nhật định tuyến.

Bên cạnh đó OSPF còn được thiết kế theo dạng phân cấp, sử dụng các Area để giảm yêu cầu về CPU, bộ nhớ của Router. OSPF hỗ trợ chứng thực dạng Plain Text và dạng MD5.

### Metric của OSPF:

- OSPF sử dụng Metric là Cost. Cost của toàn tuyến được tính theo cách cộng dồn Cost dọc theo tuyến đường đi của Packet. Cách tính Cost được IETF đưa ra trong RFC 2328.

- Cost được tính dựa trên băng thông sao cho tốc độ kết nối của đường kết nối càng cao thì Cost càng thấp dựa trên công thức  $10^8/\text{Bandwidth}$  với giá trị Bandwidth được cấu hình trên mỗi cổng của Router và đơn vị tính là bps.
- Tuy nhiên, chúng ta có thể thay đổi giá trị Cost. Nếu Router có nhiều đường đến đích mà chi phí bằng nhau thì Router sẽ cân bằng tải trên các đường đó, mặc định trên 4 đường, tối đa là 16 đường. Những tham số bắt buộc phải giống nhau trong các Router chạy OSPF trong một hệ thống mạng, đó là Hello/Dead Interval, Area ID, Authentication Password (nếu có), Stub Area Flag.

### **Các loại môi trường OSPF:**

- Multiple Access (Ethernet).
- Point To Point.
- NBMA (Non Broadcast Multiple Access).

### **Quá trình xây dựng bảng định tuyến của OSPF:**

- Các OSPF gửi các gói Hello định kỳ để thiết lập quan hệ láng giềng. Gói tin Hello mang các thông tin thương lượng với các Router láng giềng trước khi thiết lập quan hệ Adjacency. Trong mạng đa truy cập, giao thức Hello sẽ bầu ra DR và BDR. DR và BDR sẽ thiết lập mối quan hệ Adjacency với tất cả các Router khác và những Router này chỉ trao đổi thông tin với DR và BDR. Trong mạng Point To Point không cần chọn DR và BDR.
- Mỗi Router nhận một LSA từ láng giềng với cơ sở dữ liệu về trạng thái các đường liên kết (Link State Database) của láng giềng đó và gửi một bản sao của LSA tới tất cả các láng giềng khác của nó.
- Bằng cách gửi các LSA cho toàn bộ một Area, tất cả Router sẽ xây dựng chính xác cơ sở dữ liệu về trạng thái liên kết. Khi cơ sở dữ liệu được hoàn tất, mỗi Router sử dụng thuật toán SPF để xây dựng nên cây SPF.

- Mỗi Router sẽ xây dựng nên bảng định tuyến từ cây SPF. Kết quả là mỗi Router sẽ có thông tin về đường đến tất cả các mạng đích trong hệ thống mạng.

### **Quá trình bầu chọn DR và BDR:**

- Quá trình bầu chọn liên quan đến 2 tham số: độ ưu tiên (Priority) và Router-ID. Tham số Priority được chọn trước tiên, giá trị priority nằm trong khoảng từ 0 đến 255. Nếu Priority đặt là 0 thì Router này sẽ không tham gia vào quá trình bầu chọn DR/BDR. Router nào có độ ưu tiên cao nhất sẽ được chọn là DR, cao thứ hai sẽ là BDR. Mặc định giá trị Priority OSPF là 1. Khi giá trị Priority đều bằng nhau thì OSPF sẽ bầu chọn DR dựa vào tham số thứ hai là Router-ID.
- Trong hệ thống mạng dùng OSPF không cấu hình cổng Loopback thì giá trị Router-ID được chọn là giá trị địa chỉ IP lớn nhất của các cổng đang hoạt động trên Router. Nếu có cổng Loopback thì cổng Loopback được chọn, trường hợp có nhiều cổng Loopback thì chọn cổng Loopback nào có địa chỉ IP cao nhất.

### **Cấu hình OSPF:**

- Khởi tạo tiến trình định tuyến OSPF:

```
Router(config)#router ospf <process-id>
```

- Chọn cổng tham gia vào quá trình trao đổi thông tin định tuyến:

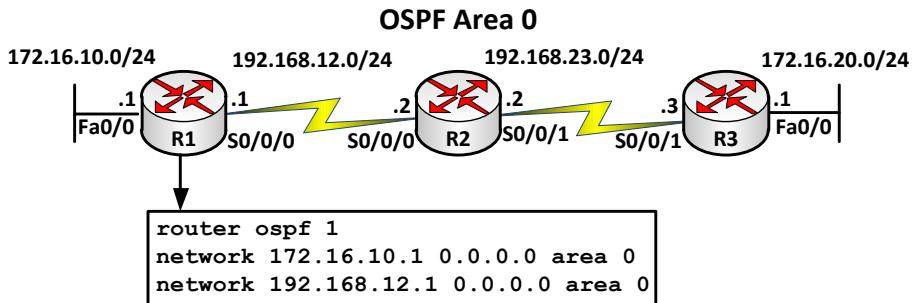
```
Router(config-router)#network <address> <wildcard>
area <area-id>
```

Trong đó:

- Process-ID: Chỉ số tiến trình của OSPF, mang tính chất cục bộ, có giá trị 1 đến 65535.
- Address: Địa chỉ cổng tham gia định tuyến.
- Wildcard: Điều kiện kiểm tra giữa địa chỉ cấu hình trong Address và địa chỉ các cổng trên Router, tương ứng bit 0 - phải kiểm tra khớp với nhau, bit 1 - không cần kiểm tra.

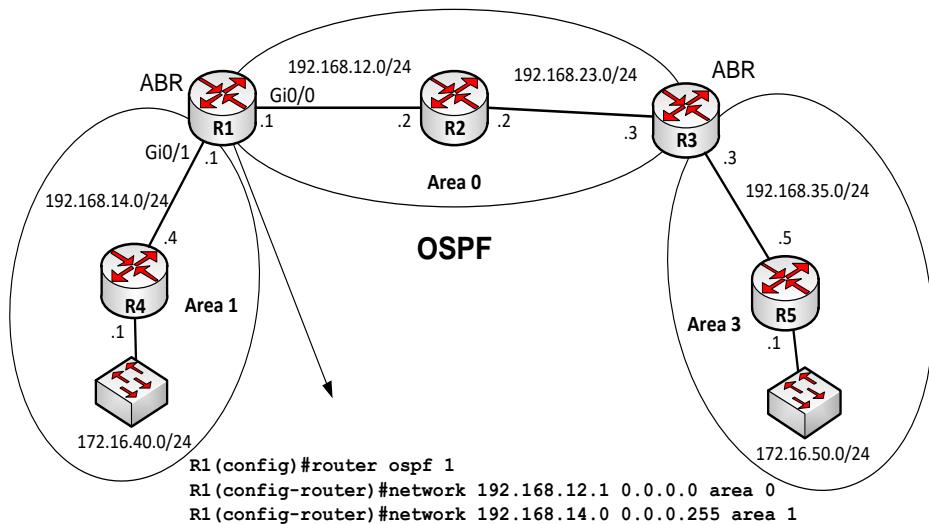
- Area ID: Vùng mà công ty ứng ứng thuộc về trong kiến trúc OSPF.

Ví dụ 1: OSPF Single Area.



**Hình 4.10:** Sơ đồ ví dụ về cấu hình OSPF Single Area

Ví dụ 2: OSPF Multi Area.



**Hình 4.11:** Sơ đồ ví dụ về cấu hình OSPF Multi Area

Các câu lệnh kiểm tra cấu hình OSPF:

```
Router#show ip protocol
Router#show ip route
Router#show ip ospf interface
Router#show ip ospf neighbor
Router#debug ip ospf events
Router#debug ip ospf packet
```

## Chứng thực trong OSPF:

Giao thức OSPF hỗ trợ hai dạng chứng thực là: “Plain Text” và MD5.

- Chứng thực bằng “Plain Text”:

Cấu hình giữa hai cổng của 2 Router nối trực tiếp với nhau để chứng thực giữa chúng trước khi trao đổi thông tin định tuyến. Mật khẩu gửi chứng thực không được mã hóa.

```
R(config)#interface <interface>
R(config-if)#ip ospf authentication
R(config-if)#ip ospf authentication-key <password>
```

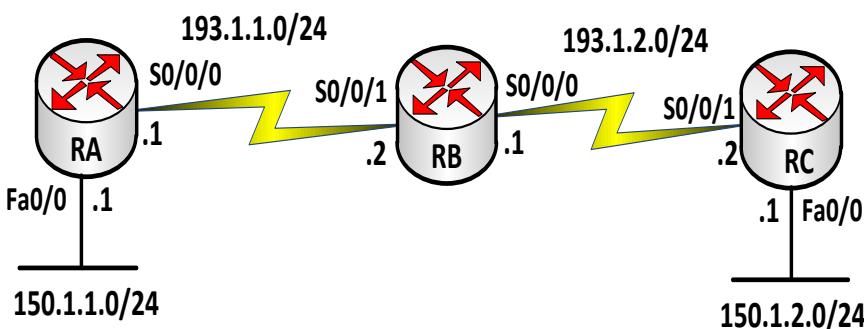
- Chứng thực bằng MD5:

Trên cổng của Router gửi thông tin chứng thực cấu hình lệnh sau:

```
R(config)#interface <interface>
R(config-if)#ip ospf authentication message-digest
R(config-if)#ip ospf messages-digest-key 1 md5
<password>
```

**Ví dụ 1:** Cho mô hình mạng sau.

Yêu cầu: Cấu hình OSPF cho các Router RA, RB và RC (Area 0) trong mô hình mạng sau để quảng bá các thông tin định tuyến. Cấu hình chứng thực dạng “Plain Text” và MD5 giữa 2 Router: RA và RB với mật khẩu là “cisco”.



**Hình 4.12:** Sơ đồ ví dụ cho cấu hình chứng thực trong OSPF

**Hướng dẫn cấu hình:**

Bước 1: Cấu hình cơ bản (đặt Hostname, địa chỉ IP cho các cổng: Serial, FastEthernet).

## Bước 2: Cấu hình giao thức định tuyến OSPF trên mỗi Router.

```
RA(config) #router ospf 1
RA(config-router) #network 150.1.1.0 0.0.0.255 area 0
RA(config-router) #network 193.1.1.0 0.0.0.255 area 0

RB(config) #router ospf 1
RB(config-router) #network 193.1.1.0 0.0.0.255 area 0
RB(config-router) #network 193.1.2.0 0.0.0.255 area 0

RC(config) #router ospf 1
RC(config-router) #network 150.1.2.0 0.0.0.255 area 0
RC(config-router) #network 193.1.2.0 0.0.0.255 area 0
```

### Bước 3.1. Cấu hình chứng thực dạng “Plain Text” giữa 2 Router: RA và RB.

```
RA(config) #int S0/0/0
RA(config-if)#ip ospf authentication
RA(config-if)#ip ospf authentication-key cisco

RB(config) #int S0/0/1
RB(config-if)#ip ospf authentication
RB(config-if)#ip ospf authentication-key cisco
```

### Bước 3.2. Cấu hình chứng thực dạng MD5 giữa 2 Router: RA và RB.

```
RA(config) #int S0/0/0
RA(config-if)#ip ospf authentication message-digest
RA(config-if)#ip ospf messages-digest-key 1 md5 cisco

RB(config) #int S0/0/1
RB(config-if)#ip ospf authentication message-digest
RB(config-if)#ip ospf messages-digest-key 1 md5 cisco
```

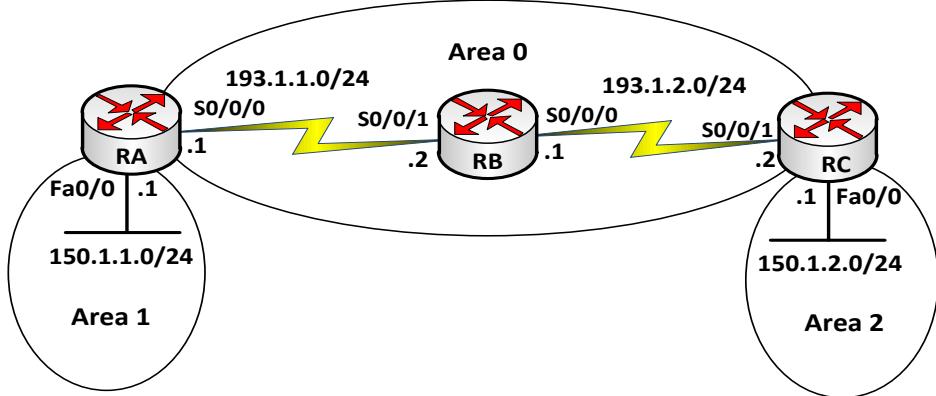
## Bước 4. Kiểm tra cấu hình.

Thực hiện các câu lệnh sau để kiểm tra cấu hình:

R#show ip route: Xem bảng định tuyến.

R#debug ip ospf event: Xem quá trình cập nhật định tuyến của OSPF.

**Ví dụ 2:** Định tuyến động – OSPF.



**Hình 4.13:** Sơ đồ mạng cấu hình định tuyến OSPF Multi Area

### Mô tả:

- RA, RB, RC sử dụng OSPF để quảng bá thông tin định tuyến.
- Các Router cấu hình OSPF và quảng bá tất cả các mạng nội trực tiếp. Từ Router RA, RB và RC ta Ping được hết các địa chỉ trong mạng.

### Các bước thực hiện:

- Đặt Hostname, địa chỉ IP cho các cổng trên Router.
  - **Cấu hình giao thức định tuyến RIP trên mỗi Router.**
- ```

RA(config)#router ospf 1
RA(config-router)#network 150.1.1.0 0.0.0.255 area 1
RA(config-router)#network 193.1.1.0 0.0.0.255 area 0
RB(config)#router ospf 1
RB(config-router)#network 193.1.1.0 0.0.0.255 area 0
RB(config-router)#network 193.1.2.0 0.0.0.255 area 0
RC(config)#router ospf 1
RC(config-router)#network 150.1.2.0 0.0.0.255 area 2
RC(config-router)#network 193.1.2.0 0.0.0.255 area 0

```

### Kiểm tra cấu hình:

Thực hiện các câu lệnh sau để kiểm tra cấu hình:

Router#show ip route: Xem bảng định tuyến.

Router#ping: Kiểm tra kết nối.

#### 4.1.4.3. EIGRP

EIGRP (Enhanced Interior Gateway Routing Protocol) là giao thức định tuyến do Cisco tạo ra, chỉ hoạt động trên các thiết bị của Cisco. EIGRP là một giao thức định tuyến lai, nó vừa mang những đặc điểm của “Distance Vector” vừa mang một số đặc điểm của ”Link State”. EIGRP là dạng định tuyến “Classless”.

EIGRP hỗ trợ VLSM và CIDR nên sử dụng hiệu quả không gian địa chỉ, sử dụng địa chỉ Multicast (224.0.0.10) để trao đổi thông tin cập nhật định tuyến.

Cách tính Metric của EIGRP:

$$\text{metric}_{EIGRP} = \left[ K1 * BW + \frac{K2 * BW}{(256 - \text{load})} + K3 * \text{Delay} \right] * \frac{K5}{(\text{reliability} + K4)}$$

Với K1, K2, K3, K4, K5 là hằng số.

Mặc định: K1 = 1, K2 = 0, K3 = 1, K4 = 0, K5 = 0.

Do đó, ta có:

$$\text{metric} = \text{bandwidth} + \text{delay}$$

Những xử lý cơ bản của EIGRP trong việc học các mạng đích:

- Các Router phát hiện các láng giềng của nó, danh sách các láng giềng được lưu giữ trong “**Neighbor Table**”.
- Mỗi Router sẽ trao đổi các thông tin về cấu trúc mạng với các láng giềng của nó.
- Router đặt những thông tin về cấu trúc hệ thống mạng học được vào cơ sở dữ liệu về cấu trúc mạng (Topology Table).
- Router chạy thuật toán DUAL với cơ sở dữ liệu đã thu thập được ở bước trên để tính toán tìm ra đường đi tốt nhất đến mỗi một mạng trong cơ sở dữ liệu.
- Router đặt các đường đi tốt nhất đến mỗi mạng đích vào bảng định tuyến.
- Trong EIGRP có hai tuyến ta cần quan tâm là “Successor Route” và “Fossible Successor Route”.

- + **Successor Route:** Là tuyến đường đi chính được sử dụng để chuyển dữ liệu đến đích, được lưu trong bảng định tuyến. EIGRP cho phép chia tài tối đa trên 16 đường (mặc định là 4 đường) đến mỗi mạng đích.
- + **Fossible Successor Route:** Là đường đi dự phòng cho đường đi chính và được lưu trong bảng cấu trúc mạng (Topology Table).

### **EIGRP chống “Routing Loop”:**

“Routing Loop” là một trở ngại rất lớn trong các giao thức định tuyến dạng “Distance Vector”. Các giao thức định tuyến dạng “Link State” vượt qua vấn đề này bằng cách mỗi Router đều nắm giữ toàn bộ cấu trúc mạng. Trong giao thức EIGRP, khi tuyến đường đi chính gặp sự cố, Router có thể kịp thời đặt đường đi dự phòng vào bảng định tuyến đóng vai trò như đường đi chính.

Trường hợp không có đường đi dự phòng, EIGRP sử dụng thuật toán DUAL cho phép Router gửi các yêu cầu và tính toán lại các đường đi đến đích.

### **Cấu hình EIGRP:**

- **Bước 1.** Kích hoạt giao thức định tuyến EIGRP.

```
Router(config)#router eigrp <autonomous-system>
```

Trong đó, autonomous-system có giá trị từ 1 đến 65535, giá trị này phải giống nhau ở tất cả các Router trong hệ thống chạy EIGRP.

- **Bước 2.** Chọn cổng tham gia vào quá trình trao đổi thông tin định tuyến.

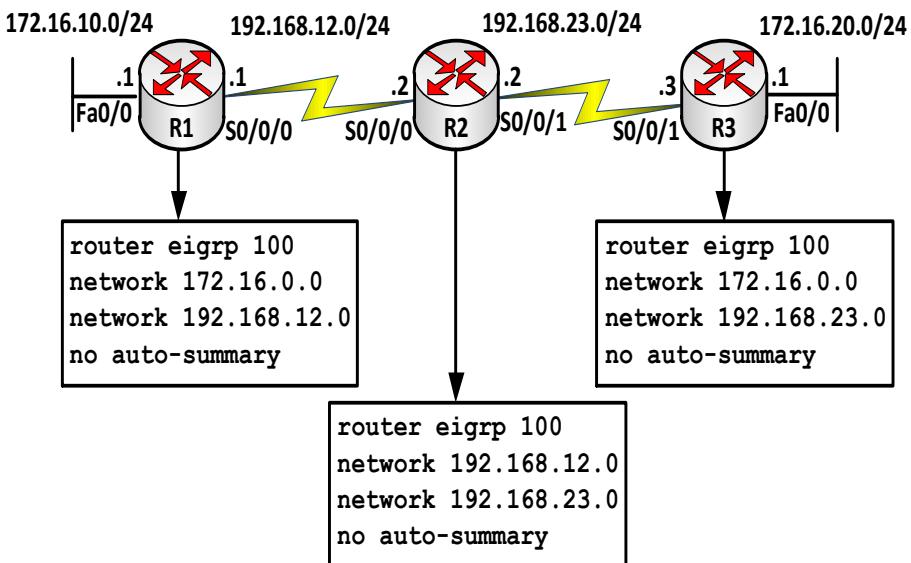
```
Router(config-router)#network <network-number>
```

Trong đó, Network Number là địa chỉ cổng theo đúng lớp mạng của nó.

Để quảng bá các mạng con và hỗ trợ mạng không liên tục, chúng ta phải sử dụng lệnh sau:

```
Router(config-router)#no auto-summary
```

**Ví dụ:** Cấu hình định tuyến EIGRP cho mô hình mạng sau:



**Hình 4.14:** Sơ đồ mạng cấu hình định tuyến EIGRP AS 100

Các câu lệnh kiểm tra cấu hình EIGRP:

```

Router#show ip eigrp neighbors
Router#show ip eigrp topology
Router#show ip route eigrp
Router#show ip protocols
Router#show ip eigrp traffic
    
```

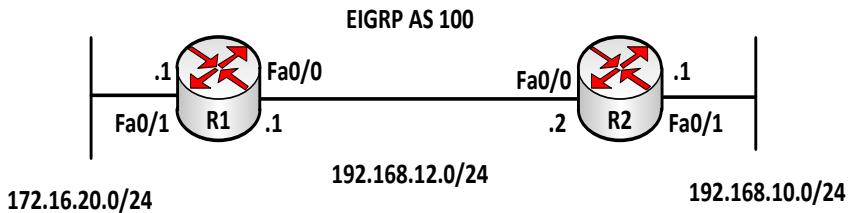
Chứng thực trong EIGRP: EIGRP chỉ hỗ trợ một dạng chứng thực là MD5.

Trên cổng của Router gửi thông tin chứng thực cấu hình lệnh sau:

```

R(config)#key chain <keychain>
R(config-keychain)#key <key-id>
R(config-keychain-key)#key-string <password>
R(config)#interface <interface>
R(config-if)#ip authentication mode eigrp <AS> md5
R(config-if)#ip authentication key-chain eigrp <AS> <keychain>
    
```

**Ví dụ:** Cấu hình chứng thực cho giao thức định tuyến EIGRP giữa hai Router R1 và R2.



**Hình 4.15:** Sơ đồ mạng ví dụ cấu hình chứng thực trong EIGRP

### Hướng dẫn cấu hình:

- Cấu hình cơ bản: Hostname, địa chỉ IP cho các cổng trên các Router.
- Cấu hình định tuyến EIGRP AS 100:

```
R1(config)#router eigrp 100
R1(config-if)#network 192.168.12.0
R1(config-if)#network 172.16.0.0
R1(config-if)#no auto-summary

R2(config)#router eigrp 100
R2(config-if)#network 192.168.12.0
R2(config-if)#network 192.168.10.0
R2(config-if)#no auto-summary
```

- Cấu hình chứng thực:

```
R1(config)#key chain my_keychain1
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string cisco

R1(config)#interface fa0/0
R1(config-if)#ip authentication mode eigrp 100 md5
R1(config-if)#ip authentication key-chain eigrp
100 my_keychain1

R2(config)#key chain my_keychain2
R2(config-keychain)#key 1
R2(config-keychain-key)#key-string cisco

R2(config)#interface fa0/0
R2(config-if)#ip authentication mode eigrp 100 md5
R2(config-if)#ip authentication key-chain eigrp
100 my_keychain2
```

### Kiểm tra cấu hình: Dùng các lệnh sau:

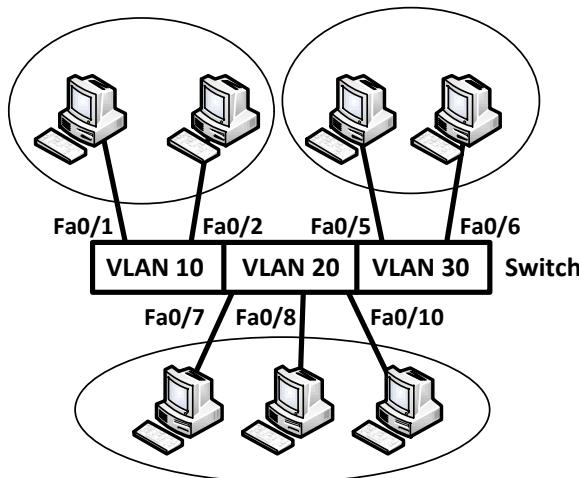
```
show ip eigrp neighbors
show ip eigrp interfaces details
show key chain
```

## 4.2. Kỹ thuật trên Switch

### 4.2.1. VLAN

#### 4.2.1.1. Khái niệm

VLAN (Virtual LAN) là kỹ thuật được sử dụng trên Switch, dùng để chia một Switch vật lý thành nhiều Switch luận lý. Mỗi một Switch luận lý gọi là một VLAN hoặc có thể hiểu VLAN là một tập hợp của các cổng trên Switch nằm trong cùng một miền quảng bá. Các cổng trên Switch có thể được nhóm vào các VLAN khác nhau trên một Switch hoặc được triển khai trên nhiều Switch.



**Hình 4.16:** Chia VLAN trên Switch

Khi có một gói tin quảng bá được gửi bởi một thiết bị nằm trong một VLAN sẽ được chuyển đến các thiết bị khác nằm trong cùng VLAN đó, gói tin quảng bá sẽ không được chuyển tiếp đến các thiết bị thuộc VLAN khác.

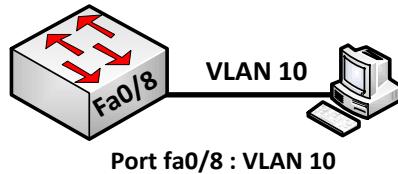
VLAN cho phép người quản trị tổ chức mạng theo luận lý chứ không theo vật lý. Sử dụng VLAN có ưu điểm là:

- Tăng khả năng bảo mật.
- Thay đổi cấu hình LAN dễ dàng.
- Di chuyển máy trạm trong LAN dễ dàng.
- Thêm máy trạm vào LAN dễ dàng.

**VLAN = broadcast domain = logical network**

#### 4.2.1.2. Phân loại

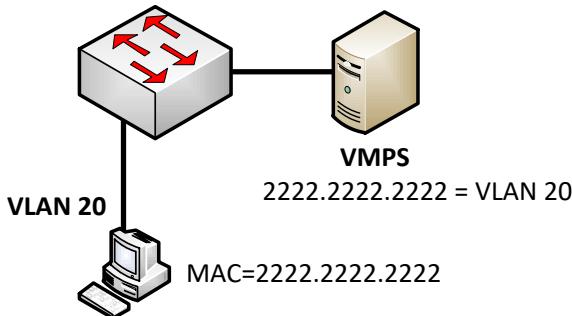
VLAN tĩnh (Static VLAN):



**Hình 4.17: VLAN tĩnh**

Đối với loại này, các cổng của Switch được cấu hình thuộc về một VLAN nào đó, các thiết bị gắn vào cổng đó sẽ thuộc về VLAN đã định trước. Đây là loại VLAN dùng phổ biến.

VLAN động (Dynamic VLAN):



**Hình 4.18: VLAN động**

Loại VLAN này sử dụng một Server lưu trữ địa chỉ MAC của các thiết bị và quy định VLAN mà thiết bị đó thuộc về, khi một thiết bị gắn vào Switch, Switch sẽ lấy địa chỉ MAC của thiết bị và gửi cho Server kiểm tra và cho vào VLAN định trước.

#### 4.2.1.3. Cấu hình VLAN

**Bước 1. Tạo VLAN.**

```
Switch(config)#vlan <vlan-id>
Switch(config-vlan)#name <vlan-name>
```

Ví dụ:

```
Switch(config)#vlan 10
```

```
Switch(config-if) #name P.KyThuat
```

## Bước 2. Gán các cổng cho VLAN.

- Trường hợp 1: Gán 1 cổng vào LAN.

```
Switch(config)#interface <interface>
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan <vlan-id>
```

Ví dụ:

```
Switch(config)#interface fa0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
```

- Trường hợp 2: Gán 1 dãy các cổng liên tiếp.

```
Switch(config)#interface range <start>-<end-intf>
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan
<vlan-id>
```

Ví dụ:

```
Switch(config)#interface fa0/10 - 20
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
```

- Trường hợp 3: Gán nhiều cổng không liên tiếp.

```
Sw(config)#int range <int1, int2,...>
Sw(config-if-range)#switchport mode access
Sw(config-if-range)#switchport access vlan <vlan-
id>
```

Ví dụ:

```
Switch(config)#interface fa0/7, fa0/9, fa0/2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
```

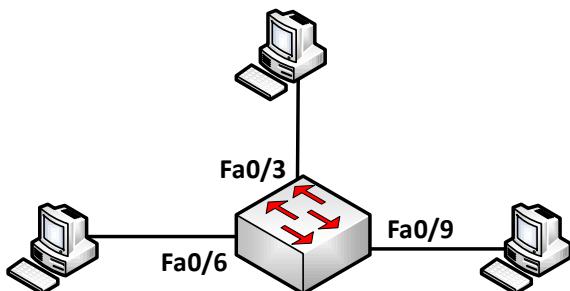
**Xóa VLAN:** Xóa một VLAN trên Switch bằng cách sử dụng lệnh “no” trước câu lệnh tạo VLAN.

## Lệnh kiểm tra cấu hình VLAN:

```
Switch#show vlan [brief]
```

Lệnh này cho phép hiển thị các VLAN-ID (số hiệu VLAN), tên VLAN, trạng thái VLAN và các cổng được gán cho VLAN trên Switch.

**Ví dụ:**



**Hình 4.19: Cấu hình VLAN trên Switch**

**Mô tả yêu cầu:**

- Cấu hình VLAN trên Switch.
- Tạo 3 VLAN: VLAN 10, VLAN 20, VLAN 30.
- Fa0/1 - Fa0/6: VLAN 10, Fa0/7 - Fa0/9: VLAN 20, Fa0/10 - Fa0/12: VLAN 30.

**Các bước thực hiện:**

**- Tạo VLAN:**

```
Switch(config)#vlan 10  
Switch(config)#vlan 20  
Switch(config)#vlan 30
```

**- Gán các cổng vào VLAN:**

```
Switch(config)#interface range f0/1 - 6  
Switch(config-if-range)#switchport mode access  
Switch(config-if-range)#switchport access vlan 10  
Switch(config)#interface range f0/7 - 9  
Switch(config-if-range)#switchport mode access  
Switch(config-if-range)#switchport access vlan 20  
Switch(config)#interface range f0/10 - 12  
Switch(config-if-range)#switchport mode access  
Switch(config-if-range)#switchport access vlan 30
```

- **Kiểm tra cấu hình:**

Thực hiện các câu lệnh sau để kiểm tra cấu hình:

```
Switch#show run
```

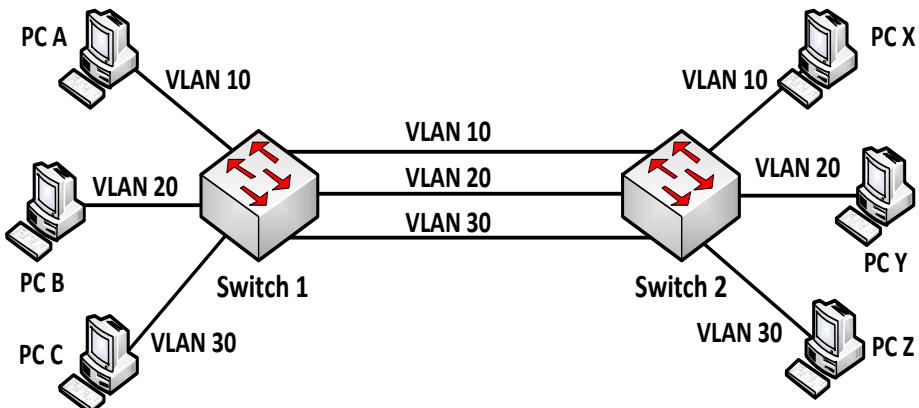
```
Switch#show vlan [brief]
```

Gắn PC vào các cổng như trên sơ đồ, đặt IP cho các PC và dùng lệnh “Ping” để kiểm tra kết nối.

#### 4.2.1.4. Đường Trunk

VLAN tổ chức trên nhiều Switch như vậy làm sao các thiết bị thuộc cùng một VLAN nhưng nằm ở những Switch khác nhau có thể liên lạc với nhau? Chúng ta có hai cách để giải quyết vấn đề này:

- Dùng mỗi kết nối cho từng VLAN:



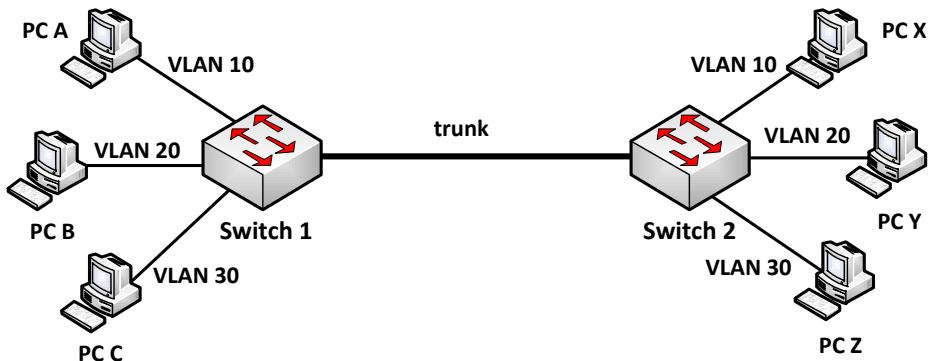
**Hình 4.20:** Sử dụng mỗi kết nối cho từng VLAN

Có nghĩa là mỗi VLAN ở trên các Switch sẽ được kết nối lại bằng một đường kết nối riêng. Theo mô hình trên ta thấy: nếu PC A trong VLAN 10 ở Switch 1 muốn liên lạc với PC X trong VLAN 10 ở Switch 2, ta phải có một kết nối vật lý nối Switch 1 với Switch 2 và hai cổng kết nối này phải thuộc cùng VLAN 10.

Tương tự đối với VLAN 2 và VLAN 3, ta cần hai kết nối vật lý. Như vậy, với n VLAN được tạo ra tổng cộng ta phải dùng đến n dây nối để các thành viên trong cùng VLAN có thể giao tiếp được với nhau. Điều này gây ra lãng phí.

- Kết nối Trunk (đường Trunk):

Một kỹ thuật khác để giải quyết vấn đề trên là dùng chỉ một kết nối cho phép dữ liệu của các VLAN có thể cùng lưu thông qua đường này. Người ta gọi kết nối này là đường **Trunk**.



**Hình 4.21:** Kết nối Trunk cho các VLAN

Theo như mô hình trên chúng ta chỉ dùng một dây nối Switch 1 với Switch 2, các thành viên trong cùng VLAN ở các Switch khác nhau vẫn có thể giao tiếp với nhau. Đường dây như thế gọi là liên kết Trunk lớp 2.

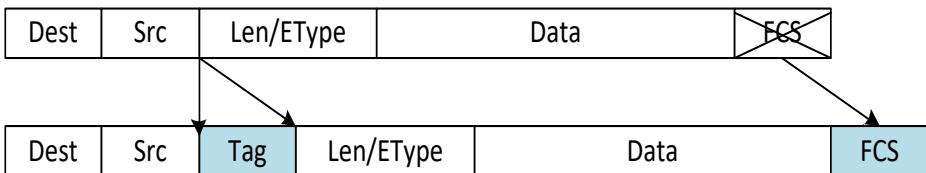
Mỗi thành viên trong cùng VLAN chỉ có thể thấy thành viên khác trong cùng VLAN với nó. Để PC A có thể giao tiếp với PC B hoặc C (không thuộc cùng VLAN), cần phải sử dụng thiết bị ở lớp 3 như Router hay Switch lớp 3 (MultiLayer Switch hay Switch Layer 3).

Kết nối “Trunk” là liên kết Point To Point giữa các cổng trên Switch với Router hoặc với Switch khác. Kết nối “Trunk” sẽ vận chuyển dữ liệu của nhiều VLAN thông qua một liên kết đơn và cho phép mở rộng VLAN trên hệ thống mạng.

Vì kỹ thuật này cho phép dùng chung một kết nối vật lý cho dữ liệu của các VLAN đi qua nên để phân biệt được chúng là dữ liệu của VLAN nào, người ta gắn vào các gói tin một dấu hiệu gọi là “Tagging”. Hay nói cách khác là dùng một kiểu đóng gói riêng cho các gói tin di chuyển qua đường “Trunk” này. Giao thức được sử dụng là 802.1Q (dot1q).

### Giao thức 802.1Q:

Đây là giao thức chuẩn của IEEE để dành cho việc nhận dạng các VLAN bằng cách thêm vào “Frame Header” đặc điểm của một VLAN. Phương thức này còn được gọi là gắn thẻ cho VLAN (Frame Tagging).



**Hình 4.22:** Frame được đóng gói theo kiểu 802.1Q

### Native VLAN:

Native VLAN là VLAN trong được gán nhãn, thông thường VLAN 1 mặc định là Native VLAN trong các Switch.

### Cấu hình VLAN Trunking:

Để cấu hình đường “Trunk”, chúng ta cấu hình 2 cổng “Trunk” như sau:

```
switch(config)#interface <interface>
switch(config-if)#switchport mode trunk
switch(config-if)#switchport trunk encapsulation dot1q
```

Lệnh cuối cùng là mặc định ở một số dòng Switch.

### 4.2.2. VTP

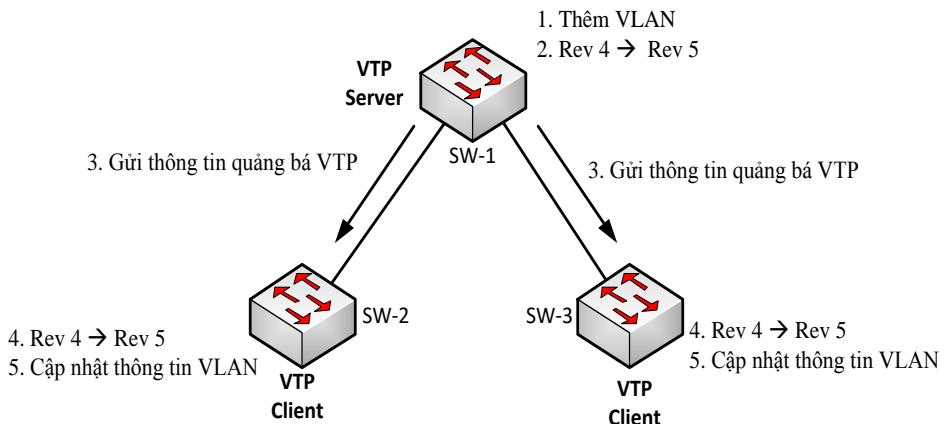
VTP là giao thức hoạt động ở tầng Liên kết dữ liệu trong mô hình OSI. VTP giúp cho việc cấu hình VLAN luôn đồng nhất khi thêm, xóa, sửa thông tin về VLAN trong hệ thống mạng.

#### Hoạt động của VTP:

VTP gửi thông điệp quảng bá qua “VTP Domain” mỗi 5 phút một lần, hoặc khi có sự thay đổi xảy ra trong cấu hình VLAN. Một thông điệp VTP bao gồm “Revision Number”, tên VLAN (VLAN Name), số hiệu VLAN (VLAN Number), và thông tin về các Switch có cổng gắn với mỗi VLAN. Bằng sự cấu hình VTP Server và việc quảng bá thông tin VTP, tất cả các Switch đều đồng bộ về tên VLAN và số hiệu VLAN của tất cả các VLAN.

Một trong những thành phần quan trọng trong các thông tin quảng bá VTP là tham số “Revision Number”. Mỗi lần VTP Server điều chỉnh thông tin VLAN, nó tăng “Revision Number” lên 1, rồi sau đó VTP Server mới gửi thông tin quảng bá VTP đi. Khi một Switch nhận một

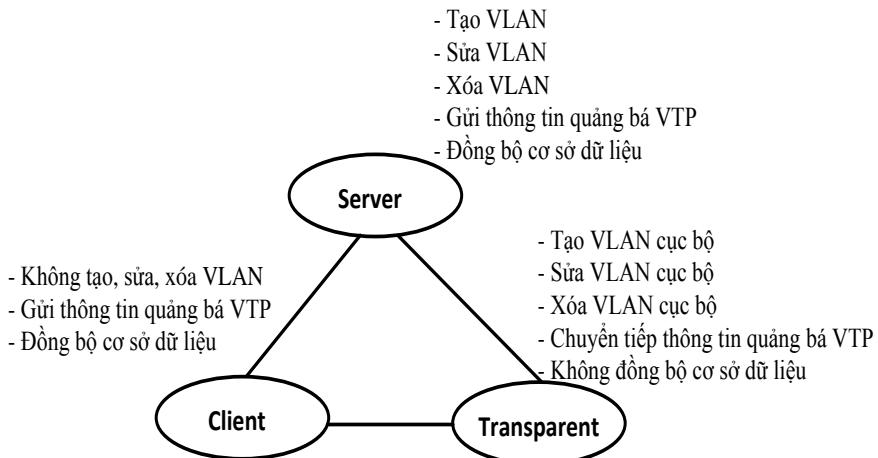
thông điệp VTP với “Revision Number” lớn hơn, nó sẽ cập nhật cấu hình VLAN.



**Hình 4.23: Hoạt động của VTP**

#### VTP hoạt động ở một trong ba chế độ:

- Server.
- Client.
- Transparent.



**Hình 4.24: Các Mode của VTP**

Switch ở chế độ VTP Server có thể tạo, chỉnh sửa và xóa VLAN. VTP Server lưu cấu hình VLAN trong NVRAM của nó. VTP Server gửi thông điệp ra tất cả các cổng “Trunk”.

Switch ở chế độ VTP Client không tạo, sửa và xóa thông tin VLAN. VTP Client có chức năng đáp ứng theo mọi sự thay đổi của VLAN từ Server và gửi thông điệp ra tất cả các cổng “Trunk” của nó. VTP Client đồng bộ cấu hình VLAN trong hệ thống.

Switch ở chế độ Transparent sẽ nhận và chuyển tiếp các thông điệp quảng bá VTP do các Switch khác gửi đến mà không quan tâm đến nội dung của các thông điệp này. Nếu “Transparent Switch” nhận được thông tin cập nhật VTP nó cũng không cập nhật vào cơ sở dữ liệu của nó; đồng thời nếu cấu hình VLAN của nó có gì thay đổi, nó cũng không gửi thông tin cập nhật cho các Switch khác. Trên “Transparent Switch” chỉ có một việc duy nhất là chuyển tiếp thông điệp VTP. Switch hoạt động ở “Transparent-mode” chỉ có thể tạo ra các VLAN cục bộ. Các VLAN này sẽ không được quảng bá đến các Switch khác.

### Cấu hình VTP:

- Cấu hình VTP Domain:

```
Switch(config)#vtp domain <domain_name>
```

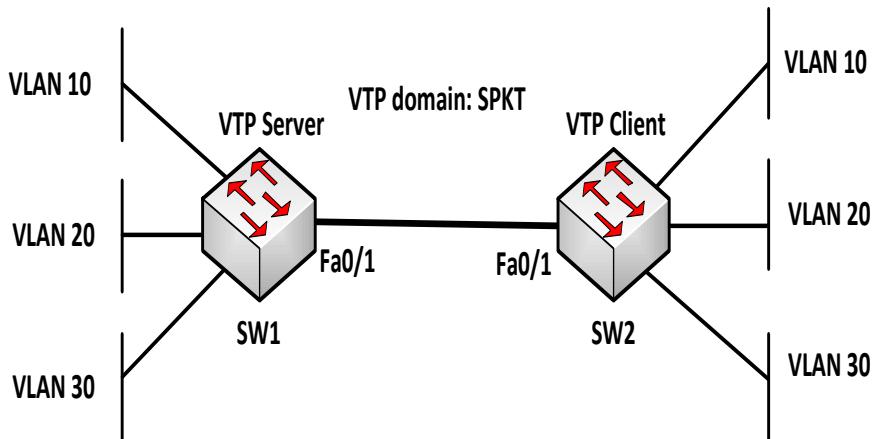
- Cấu hình VTP Mode:

```
Switch(config)#vtp [client| transparent| server]
```

- Lệnh xem cấu hình VTP:

```
Switch#show vtp status
```

**Ví dụ:** Cho sơ đồ mạng:



**Hình 4.25:** Sơ đồ mạng cấu hình VTP

## **Mô tả:**

- Hai Switch kết nối với nhau qua đường “Trunk”.
- Tạo 3 VLAN: VLAN 10, VLAN 20, VLAN 30 trên SW1.
- Cấu hình VTP để các thông tin các VLAN trên SW1 cập nhật cho SW2.
- Trên SW1: VLAN 10 (Fa0/2 - Fa0/4), VLAN 20 (Fa0/5 - Fa0/7), VLAN 30 (Fa0/8 - Fa0/10).
- Trên SW2: VLAN 10 (Fa0/4 - Fa0/6), VLAN 20 (Fa0/7 - Fa0/9), VLAN 30 (Fa0/10 - Fa0/12).

## **Các bước cấu hình:**

### **a. Cấu hình SW1 làm VTP Server**

- Thiết lập VTP Domain: SPKT, VTP Mode Server, và tạo các VLAN:

```
sw1#config terminal  
sw1(config)#vtp mode server  
sw1(config)#vtp domain SPKT  
sw1(config)#vlan 10  
sw1(config-vlan)#name CNTT  
sw1(config)#vlan 20  
sw1(config-vlan)#name TTTH  
sw1(config)#vlan 30  
sw1(config-vlan)#name TTCLC
```

- Cấu hình đường Trunk và cho phép tất cả các VLAN qua đường Trunk:

```
sw1(config)#interface f0/1  
sw1(config-if)#switchport mode trunk  
sw1(config-if)#switchport trunk encapsulation dot1q
```

- Gán các Port vào các VLAN:

```
sw1(config)#int range f0/2 - 4  
sw1(config-if-range)#switchport mode access  
sw1(config-if-range)#switchport access vlan 10  
sw1(config-if)#int range f0/5 - 7  
sw1(config-if-range)#switchport mode access  
sw1(config-if-range)#switchport access vlan 20
```

```
sw1(config-if)#int range f0/8 - 10  
sw1(config-if-range)#switchport mode access  
sw1(config-if-range)#switchport access vlan 30
```

- **Kiểm tra cấu hình.** Sử dụng các lệnh:

```
switch#show vlan  
switch# show vtp status
```

### b. Cấu hình SW2 làm VTP Client

- **Cấu hình VTP Domain:** SPKT, VTP Mode Client.

```
SW2(config)#vtp domain SPKT  
SW2(config)#vtp mode client
```

- **Cấu hình Trunking trên cổng f0/1 của SW2:**

```
SW2(config)#int f0/1  
SW2(config-if)#switchport mode trunk  
SW2(config-if)#switchport trunk encapsulation dot1q
```

### c. Gán các Port vào các VLAN:

```
sw2(config)#int range f0/4 - 6  
sw2(config-if-range)#switchport mode access  
sw2(config-if-range)#switchport access vlan 10  
sw2(config)#int range f0/7 - 9  
sw2(config-if-range)#switchport mode access  
sw2(config-if-range)#switchport access vlan 20  
sw2(config)#int range f0/10 - 12  
sw2(config-if-range)#switchport mode access  
sw2(config-if-range)#switchport access vlan 30
```

### c. Kiểm tra. Sử dụng các câu lệnh sau:

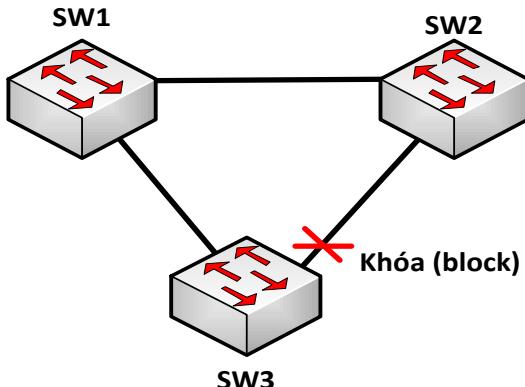
```
switch#show vlan  
switch#show int interface  
switch#show vtp status  
switch#show vtp counters → kiểm tra số lần gửi và nhận  
thông tin Trunking.
```

#### 4.2.3. Giao thức STP

Trong thiết kế mạng, việc tạo ra các kết nối dư thừa là cần thiết nhằm tạo khả năng dự phòng cho hệ thống. Tuy nhiên, khi thiết kế dự phòng trên Switch thì có 3 vấn đề cần xem xét là: bão quảng bá, nhiều gói tin được nhận giống nhau và bảng địa chỉ MAC trên các

Switch không ổn định. Có thể gọi chung trường hợp này là “Switching Loop”.

Giao thức STP được sử dụng để giải quyết vấn đề này bằng cách khóa tạm thời một hoặc một số cổng để tránh tình trạng như trên.



**Hình 4.26:** Sơ đồ kết nối các Switch

Hoạt động của STP qua các bước sau:

- Đầu chọn 1 Switch làm “Root Switch”, còn gọi là “Root Bridge”.
- Chọn “Root Port” trên các Switch còn lại.
- Chọn “Designated Port” trên mỗi phân đoạn (Segment) mạng.
- Cổng còn lại gọi là “Nondesignated Port” sẽ bị khóa.

Quá trình bầu chọn “Root Switch”:

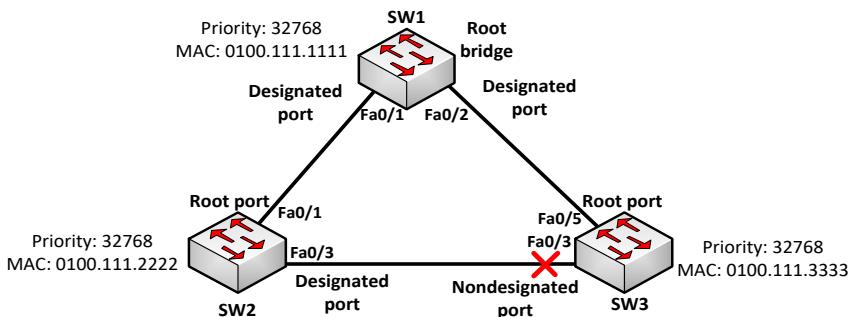
Mỗi Switch có một giá trị “Bridge-ID” gồm 2 trường là “Bridge Priority” và “MAC Address” và được đặt vào trong BPDU và gửi quảng bá cho các Switch khác mỗi 2 giây. Switch được chọn làm “Root Switch” là Switch có giá trị “Bridge-ID” nhỏ nhất. Để so sánh, giá trị “Bridge Priority” được dùng để so sánh trước, nếu tất cả các Switch đều có giá trị này bằng nhau thì tham số thứ 2 là “MAC Address” sẽ được dùng để so sánh.

Các loại cổng khác “Root Port”, “Designated Port” sẽ lần lượt được bầu chọn dựa vào chi phí nhỏ nhất tính từ nó đến “Root Switch”. Dựa vào bảng sau để tính chi phí cho mỗi chặng.

**Bảng 4.2: Bảng quy đổi STP Cost dựa vào tốc độ cổng vật lý**

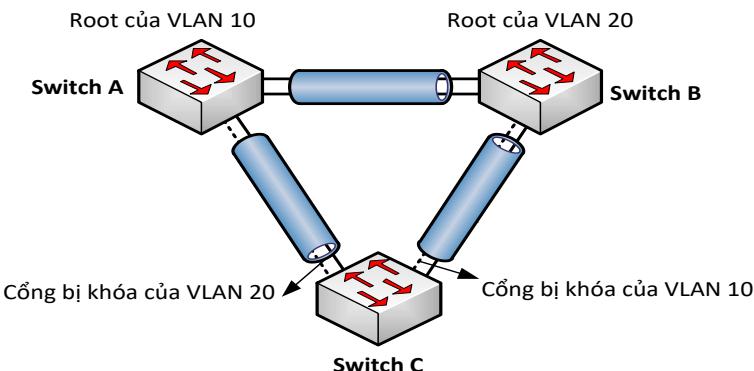
| Tốc độ cổng<br>(Ethernet Speed) | Chi phí<br>(IEEE Cost: 1998) | Chi phí<br>(IEEE Cost: 2004) |
|---------------------------------|------------------------------|------------------------------|
| 1 Tb/s                          | N/A                          | 20                           |
| 100 Gb/s                        | N/A                          | 200                          |
| 10 Gb/s                         | 2                            | 2.000                        |
| 1 Gb/s                          | 4                            | 20.000                       |
| 100 Mb/s                        | 19                           | 200.000                      |
| 10 Mb/s                         | 100                          | 2.000.000                    |

**Ví dụ:**



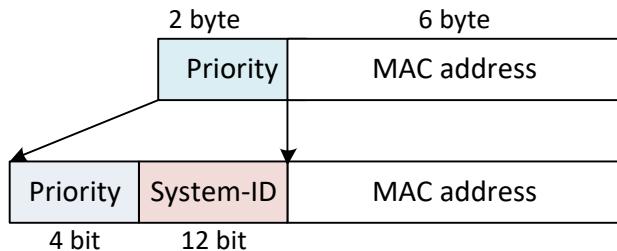
**Hình 4.27: Ví dụ về STP**

Một số dạng STP được cải tiến như: PVSTP+ (Per VLAN Spanning Tree Plus) dùng tạo cho mỗi VLAN một STP riêng.



**Hình 4.28: STP cho từng VLAN (PVSTP+)**

Trong PVSTP+, Bridge-ID có thêm trường System-ID (VLAN-ID) để phân biệt cho từng VLAN.



**Hình 4.29:** Các tham số trong Bridge ID

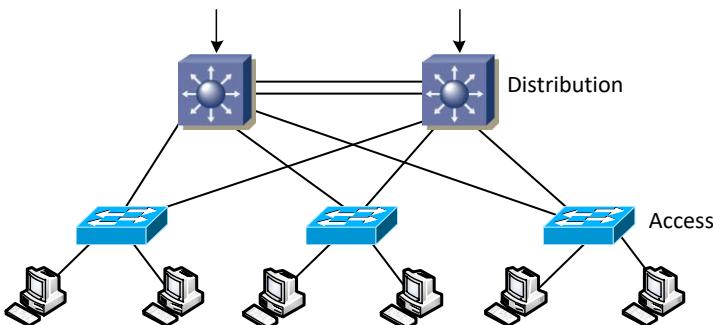
Một số lệnh cấu hình để điều chỉnh giá trị “Bridge Priority” mặc định của Switch. Chọn Switch làm “Root Switch” bằng lệnh sau:

```
Switch(config)#spanning-tree vlan <vlan-id> root  
primary
```

Hoặc:

```
Switch(config)#spanning-tree vlan <vlan-id> priority  
<priority>
```

Trong thiết kế mạng, các Switch ở tầng Distribution là lựa chọn tốt để làm vai trò của Root Switch. Do đó, sử dụng các lệnh thay đổi giá trị Bridge Priority là cần thiết để hệ thống mạng hoạt động có hiệu quả.



**Hình 4.30:** Thiết lập Root trên các Switch khu vực Distribution

Quá trình chuyển trạng thái cổng trên Switch trải qua các pha như sau: tổng thời gian từ trạng thái đầu đến trạng thái cuối mất khoảng 50 giây.

Blocking → Listening → Learning → Forwarding

#### 4.2.4. Định tuyến giữa các VLAN

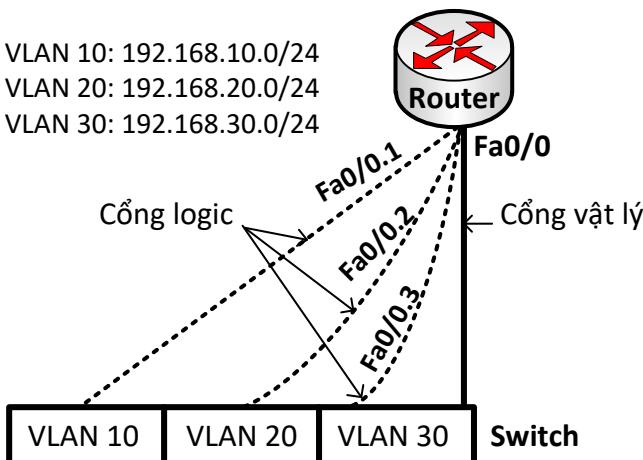
Mỗi VLAN là một miền quảng bá. Do đó, mặc định mỗi thiết bị trong VLAN chỉ liên lạc được với các thiết bị khác trong cùng một VLAN. Nếu một máy tính trong một VLAN muốn liên lạc với một máy tính thuộc một VLAN khác thì nó phải thông qua thiết bị định tuyến như là Router.

Router trong cấu trúc VLAN thực hiện ngăn chặn quảng bá, bảo mật và quản lý các lưu lượng mạng. Switch Layer 2 không thể chuyển dữ liệu giữa các VLAN với nhau. Dữ liệu trao đổi giữa các VLAN phải được định tuyến qua thiết bị hoạt động ở tầng Mạng như Router, Switch Layer 3.

Giả sử trên Switch tạo 3 VLAN, nếu ta dùng 3 cổng của Router để định tuyến cho 3 VLAN này thì quá cồng kềnh và không tiết kiệm. Ta chỉ cần sử dụng 1 cổng trên Router kết nối với một cổng trên Switch và cấu hình đường này làm đường Trunk (Trunk Layer 3) để định tuyến cho các VLAN.

Đường kết nối cho phép mang lưu lượng của nhiều VLAN gọi là kết nối Trunk lớp 3. Nó không phải là của riêng VLAN nào. Ta có thể cấu hình một đường Trunk để vận chuyển lưu thông cho tất cả VLAN hoặc một số VLAN cụ thể nào đó được chỉ ra trong cấu hình. Trunking Layer 3 đòi hỏi cổng trên VLAN phải có thể hoạt động ở tốc độ FastEthernet trở lên.

##### Cổng vật lý và cổng logic:



**Hình 4.31: Định tuyến giữa các VLAN**

Đường “Trunk” có ưu điểm là làm giảm số lượng cổng cần sử dụng của Router và Switch. Điều này không chỉ tiết kiệm chi phí mà còn giúp cho cấu hình bớt phức tạp. Kết nối “Trunk” trên Router có khả năng mở rộng với số lượng lớn VLAN. Nếu mỗi VLAN phải có một kết nối vật lý thì không thể đáp ứng được khi số lượng VLAN lớn.

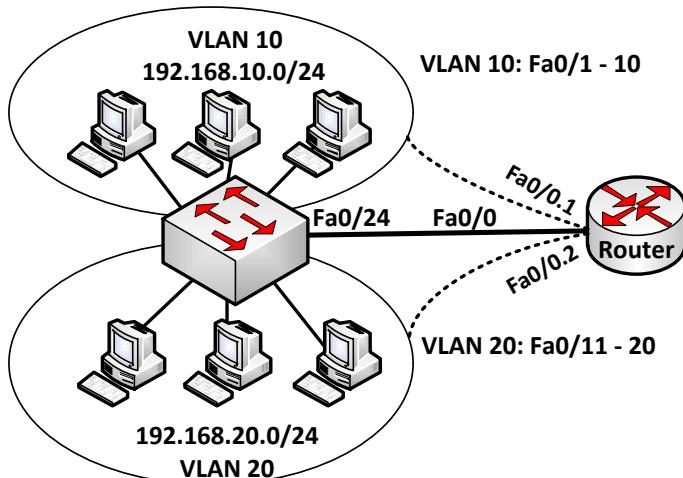
Một cổng vật lý có thể được chia thành nhiều cổng luận lý. Mỗi cổng luận lý tương ứng với một VLAN và được đặt một địa chỉ IP của VLAN đó. Mỗi VLAN là một mạng riêng, do đó cổng luận lý thuộc VLAN nào thì có địa chỉ IP thuộc mạng của VLAN đó.

Cấu hình định tuyến cho các VLAN dùng Router:

Sử dụng các cổng luận lý được chia từ một cổng vật lý để cấu hình định tuyến giữa các VLAN, các câu lệnh được sử dụng như sau:

```
R(config) #interface <port-number.subintf-number>  
R(config-if) #encapsulation dot1q <vlan-id>  
R(config-if) #ip address <address> <subnet-mask>
```

**Ví dụ:** Cấu hình định tuyến giữa các VLAN.



**Hình 4.32:** Định tuyến VLAN dùng Sub Interface trên Router

**Yêu cầu:**

- Tạo 2 VLAN: **VLAN 10** (P.KinhDoanh) và **VLAN 20** (P.KeToan).

- Các cổng Fa0/1 - Fa0/10 thuộc VLAN 10, các cổng Fa0/11 - Fa0/20 thuộc VLAN 20.
- Cấu hình định tuyến cho phép hai VLAN này có thể liên lạc được với nhau.

### Các bước thực hiện:

#### Cấu hình trên Switch:

- + Tạo VLAN:

```
switch(config)#vlan 10
switch(config-vlan)#name P.KinhDoanh
switch(vlan)#vlan 20
switch(config-vlan)#name P.KeToan
```

- + Gán các Port vào VLAN:

```
switch(config)#interface range fa0/1 - 10
switch(config-if-range)#switchport mode access
switch(config-if-range)#switchport access vlan 10
switch(config)#int fa0/11 - 20
switch(config-if-range)#switchport mode access
switch(config-if-range)#switchport access vlan 20
```

- + Cấu hình đường Trunk:

```
switch(config)#int fa0/24
switch(config-if)#switchport mode trunk
switch(config-if)#switchport trunk encapsulation
dot1q
```

**Lưu ý:** Lệnh cuối là mặc định trên một số dòng Switch.

#### Cấu hình trên Router:

- + Chọn cổng fa0/0 để cấu hình Trunk:

```
router(config)#interface fa0/0
router(config-if)#no shutdown
```

- + Kích hoạt Trunk trên Sub Interface fa0/0.1 và đóng gói bằng dot1q:

```
router(config)#int fa0/0.1
router(config-if)#encapsulation dot1q 10
```

- + Cấu hình thông tin lớp 3 cho Sub Interface **fa0/0.1**:

```
router(config-subif)#ip address 192.168.10.1  
255.255.255.0
```

- + Kích hoạt “Trunk” trên Sub Interface **fa0/0.2** và đóng gói bằng **dot1q**:

```
router(config)#int fa0/0.2  
router(config-subif)#encapsulation dot1q 20
```

- + Cấu hình thông tin lớp 3 cho Sub Interface **fa0/0.2**:

```
router(config-subif)#ip address 192.168.20.1  
255.255.255.0
```

- + Lưu cấu hình:

```
router#copy run start
```

- **Kiểm tra cấu hình:**

Trên Switch dùng các lệnh sau:

```
Switch#show interface interface
```

```
Switch#show vlan
```

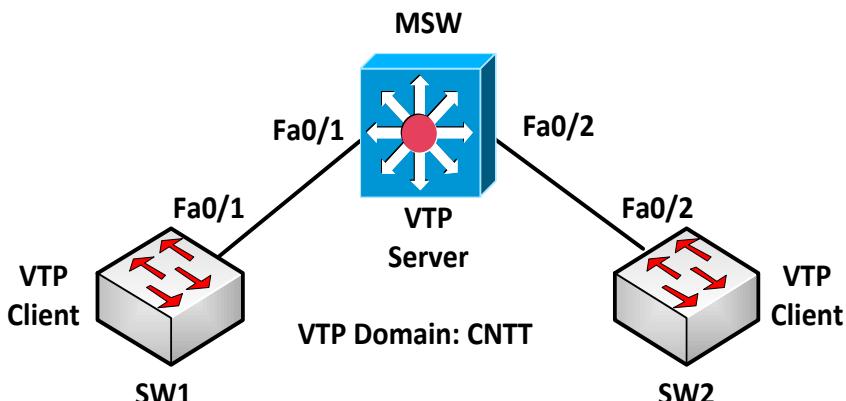
```
Switch#show vtp status
```

Trên Router dùng các lệnh sau:

Router#show vlan: Thông tin Layer 2 và Layer 3 cấu hình cho mỗi VLAN.

```
Router#show interfaces <interface>
```

Định tuyến cho các VLAN dùng Switch Layer 3 (MSW):



**Hình 4.33: Định tuyến cho các VLAN sử dụng MultiLayer Switch**

VLAN10: 192.168.10.0/24.

VLAN20: 192.168.20.0/24.

VLAN30: 192.168.30.0/24.

VLAN40: 192.168.40.0/24.

### **Yêu cầu:**

- Cấu hình đường Trunk.
- Cấu hình VTP, VLAN: VTP Domain: CNTT; MSW: VTP Server; SW1, SW2: VTP Client.
- Cấu hình MSW để định tuyến cho 4 VLAN.

### **Hướng dẫn cấu hình:**

#### Cấu hình đường Trunk:

```
SW1(config)#interface fa0/1
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk encapsulation dot1q
SW2(config)#interface fa0/2
SW2(config-if)#switchport mode trunk
SW2(config-if)#switchport trunk encapsulation dot1q
MSW(config)#interface fa0/1
MSW(config-if)#switchport mode trunk
MSW(config-if)#switchport trunk encapsulation dot1q
MSW(config)#interface fa0/2
MSW(config-if)#switchport mode trunk
MSW(config-if)#switchport trunk encapsulation dot1q
```

#### Cấu hình VTP, VLAN:

```
MSW(config)#vtp domain CNTT
MSW(config)#vtp mode server
SW1(config)#vtp domain CNTT
SW1(config)#vtp mode client
SW2(config)#vtp domain CNTT
SW2(config)#vtp mode client
MSW(config)#vlan 10
```

```
MSW(config)#vlan 20  
MSW(config)#vlan 30  
MSW(config)#vlan 40
```

Cấu hình MSW để Routing giữa 4 VLAN:

```
MSW(config)#ip routing  
MSW(config)#interface vlan 10  
MSW(config-if)#ip address 192.168.10.1 255.255.255.0  
MSW(config)#interface vlan 20  
MSW(config-if)#ip address 192.168.20.1 255.255.255.0  
MSW(config)#interface vlan 30  
MSW(config-if)#ip address 192.168.30.1 255.255.255.0  
MSW(config)#interface vlan 40  
MSW(config-if)#ip address 192.168.40.1 255.255.255.0
```

Kiểm tra cấu hình:

```
show interface trunk  
show vtp status  
show vlan brief  
show ip route
```

### 4.3. Tổng kết chương

Trong môi trường Ethernet LAN, tập hợp các thiết bị cùng nhận một gói quảng bá bởi bất kỳ một thiết bị còn lại được gọi là một “Broadcast Domain”. Trên các Switch không hỗ trợ VLAN, Switch sẽ gửi tất cả các gói tin quảng bá ra tất cả các cổng, ngoại trừ cổng mà nó nhận gói tin vào. Kết quả là trên các cổng của loại Switch này là cùng một “Broadcast Domain”. Nếu Switch này kết nối đến các Switch và các Hub khác, các cổng trên Switch này sẽ cùng “Broadcast Domain”.

VLAN cho phép kết hợp các cổng trên Switch thành các nhóm để giảm lưu lượng Broadcast. VLAN là một LAN theo logic dựa trên chức năng, ứng dụng của một tổ chức chứ không phụ thuộc vào vị trí vật lý hay kết nối vật lý trong mạng. Một VLAN là một miền quảng bá được tạo nên bởi một hay nhiều Switch.

Giao thức VTP có vai trò duy trì cấu hình của VLAN và đồng nhất trên toàn mạng. VTP là giao thức sử dụng đường Trunk để quản lý sự thêm, xóa, sửa các VLAN trên toàn mạng từ Switch trung tâm được đặt trong Server Mode. VTP hoạt động chủ yếu là đồng nhất các thông tin VLAN trong cùng một VTP Domain giúp giảm đi sự cấu hình giống nhau trong các Switch.

Kết nối Trunk là liên kết Point To Point giữa các cổng trên Switch với Router hoặc với Switch khác. Kết nối Trunk sẽ vận chuyển thông tin của nhiều VLAN thông qua một liên kết đơn và cho phép mở rộng VLAN trên hệ thống mạng. Các VLAN được định tuyến sử dụng thiết bị ở tầng 3 như Router hay “Switch Layer 3”.

Giao thức STP được dùng trong trường hợp hệ thống mạng thiết kế các kết nối dự phòng trên Switch. STP chống tình trạng “Switching Loop” bằng cách khóa tạm một số cổng trong mạng. Một số phiên bản cải tiến từ STP truyền thống như PVSTP+, RSTP,...

#### 4.4. Câu hỏi và bài tập

1. Router xác định đường đi của các gói tin dựa vào đâu?

- A. Dựa vào địa chỉ IP nguồn trong gói tin gửi tới nó và bảng định tuyến.
- B. Dựa vào địa chỉ IP đích trong gói tin gửi tới nó và bảng định tuyến.
- C. Dựa vào địa chỉ MAC nguồn trong gói tin gửi tới nó và bảng định tuyến.
- D. Dựa vào địa chỉ MAC đích trong gói tin gửi tới nó và bảng định tuyến.
- E. Dựa vào địa chỉ MAC đích và bảng địa chỉ MAC.

2. Câu nào sau đây mô tả đúng nhất ưu điểm của loại định tuyến tĩnh?

- A. Phù hợp cho các hệ thống mạng lớn vì các sự thay đổi sẽ không ảnh hưởng đến việc định tuyến.
- B. Nó cho phép những người quản trị có thể cấu hình dễ dàng.
- C. Phù hợp trong các mô hình mạng lớn cần sự linh động khi cần sự thay đổi đường đi xảy ra.

- D. Phù hợp trong mô hình mạng nhỏ, cần sự kiểm soát chặt chẽ và giảm lưu lượng trao đổi giữa các Router.
3. Đường đi mặc định (Default Route) là đường đi có đặc điểm gì?
- A. Nằm ở cuối bảng định tuyến, được sử dụng khi không có tuyến đường đi nào cụ thể được chỉ ra trong bảng định tuyến.
  - B. Nằm ở cuối bảng định tuyến, được sử dụng khi không có giao thức định tuyến động nào được cấu hình.
  - C. Được sử dụng để gửi dữ liệu đến cho nhà cung cấp dịch vụ.
  - D. Được sử dụng để tăng tốc trong quá trình định tuyến.
4. Câu nào sau đây mô tả đúng nhất ý nghĩa của tham số AD (Administrative Distance) sử dụng trong định tuyến?
- A. AD được dùng để xác định các chuẩn giao thức.
  - B. AD được dùng xác định mức độ tin cậy của các giao thức định tuyến.
  - C. AD được dùng để đo khoảng cách ngắn nhất của các đường đi trong định tuyến.
  - D. AD được xác định bởi người quản trị cho việc chọn đường đi.
5. Những câu nào sau đây mô tả đặc trưng của giao thức thuộc loại Link-State?
- A. Cung cấp cái nhìn toàn diện về Topology mạng cho mỗi Router.
  - B. Trao đổi toàn bộ bảng định tuyến với Router láng giềng.
  - C. Tính toán đường đi ngắn nhất.
  - D. Sử dụng cơ chế cập nhật định tuyến chỉ khi có sự thay đổi về Topology mạng xảy ra (Triggered Updates).
  - E. Sử dụng cơ chế cập nhật định tuyến định thời (Periodic Updates).
6. Đặc điểm nào sau đây là của giao thức định tuyến Distance Vector?
- A. Router định thời trao đổi toàn bộ bảng định tuyến của mình với Router láng giềng.
  - B. Router chỉ trao đổi các thông tin thay đổi về đường đi trong quá trình cập nhật thông tin định tuyến.
  - C. Router trao đổi toàn bộ bảng định tuyến của mình với Router láng giềng ở lần trao đổi đầu tiên. Sau khi đạt đến trạng thái hội

tụ, các Router sẽ trao đổi với nhau nếu có sự thay đổi về đường đi xảy ra.

D. Router trao đổi các gói tin LSA với nhau và chạy thuật toán tìm đường đi ngắn nhất dựa trên cơ sở dữ liệu LSA này.

7. Giá trị AD (Administrative Distance) mặc định của OSPF là?

A. 90.

B. 110.

C. 120.

D. 150.

8. Giá trị AD (Administrative Distance) mặc định của RIP là?

A. 90.

B. 110.

C. 120.

D. 150.

9. Giá trị AD (Administrative Distance) mặc định của Static Routing là?

A. 90.

B. 110.

C. 120.

D. 1.

10. Một VLAN là một tập các thiết bị nằm cùng miền \_\_\_\_\_.

A. Autonomous System.

B. Broadcast Domain.

C. Bandwidth Domain.

D. Collision Domain.

11. Thiết bị nào sau đây được dùng để kết nối các VLAN?

A. Switch.

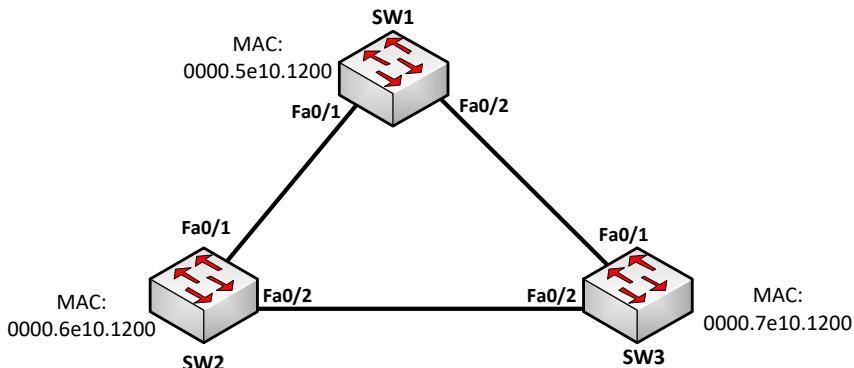
B. Bridge.

C. Router.

D. Hub.

12. Giao thức nào sau đây được dùng để phân phối thông tin về cấu hình VLAN đến các Switch khác trong mạng?
- A. STP.
  - B. VTP.
  - C. EIGRP.
  - D. SNMP.
  - E. CDP.
13. Giao thức STP dùng để làm gì?
- A. Dùng để cập nhật định tuyến trong môi trường Switch.
  - B. Dùng để chống “Routing Loop” trong mạng.
  - C. Dùng để tránh “Switching Loop” trong mạng.
  - D. Dùng để quản lý việc thêm, xóa, sửa thông tin VLAN trong hệ thống có nhiều Switch.
  - E. Dùng để phân hoạch mạng thành nhiều miền dung độ.
14. Để kiểm tra Interface fa0/5 có được gán cho VLAN Sales không, thì ta sử dụng lệnh nào sau đây?
- A. Show vlan.
  - B. Show mac-address-table.
  - C. Show vtp status.
  - D. Show spanning-tree root.
15. Show ip interface brief. Tại sao Switch không bao giờ học một địa chỉ “Broadcast”?
- A. Frame Broadcast không bao giờ được gửi tới Switch.
  - B. Địa chỉ Broadcast sử dụng định dạng không đúng trong bảng chuyển mạch trên Switch.
  - C. Địa chỉ Broadcast không bao giờ là địa chỉ nguồn trong một Frame.
  - D. Địa chỉ Broadcast chỉ dùng trong Layer 3.
  - E. Switch không bao giờ chuyển tiếp các gói tin Broadcast.

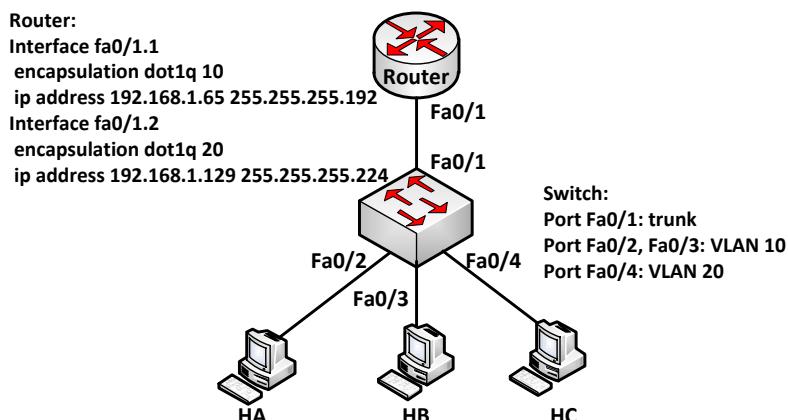
16. Cho mô hình mạng:



Tất cả các Switches được cấu hình STP mặc định và tất cả các kết nối qua Port FastEthernet. Port nào sẽ chuyển vào trạng thái “Blocking”?

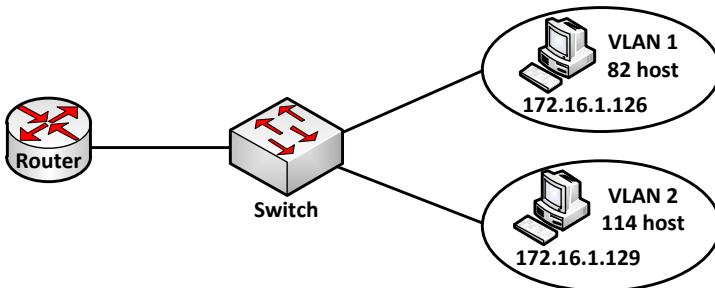
- A. Switch SW1 - Port Fa0/1.
- B. Switch SW1 - Port Fa0/2.
- C. Switch SW2 - Port Fa0/2.
- D. Switch SW2 - Port Fa0/1.
- E. Switch SW3 - Port Fa0/1.
- F. Switch SW3 - Port Fa0/2.

17. Cho mô hình mạng:

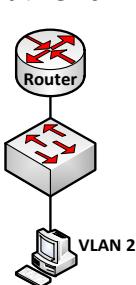


Những thông tin cấu hình nào sau đây là đúng cho các Host trong mô hình trên?

- A. Địa chỉ IP của HA: 192.1.1.65.
  - B. Subnet Mask của HA: 255.255.255.224.
  - C. Địa chỉ IP của HB: 192.1.1.125.
  - D. Default Gateway của HB: 192.1.1.65.
  - E. Địa chỉ IP của HC: 192.1.1.66.
  - F. Subnet Mask của HC: 255.255.255.224.
18. Cho mô hình mạng:



- Những phát biểu nào sau đây là đúng trong mô hình mạng trên?
- A. Subnet Mask được sử dụng là 255.255.255.192.
  - B. Subnet Mask được sử dụng là 255.255.255.128.
  - C. Địa chỉ IP 172.16.1.25 có thể được gán cho các Host thuộc VLAN 1.
  - D. Địa chỉ IP 172.16.1.205 có thể được gán cho các Host thuộc VLAN 1.
  - E. Cổng LAN trên Router được cấu hình với một địa chỉ IP.
  - F. Cổng LAN trên Router được cấu hình với nhiều địa chỉ IP.
19. Cho mô hình mạng:



```
R(config)#interface fastethernet 0/1.1
R(config-if)#encapsulation dot1q 1
R(config-if)#ip address 192.168.1.1 255.255.255.0
R(config)#interface fastethernet 0/1.2
R(config-if)#encapsulation dot1q 2
R(config-if)#ip address 192.168.2.1 255.255.255.0
R(config)#interface fastethernet 0/1.3
R(config-if)#encapsulation dot1q 3
R(config-if)#ip address 192.168.3.1 255.255.255.0
```

Router trong mô hình mạng được cấu hình như trên. Switch kết nối với Router qua đường Trunk. Trên Switch cấu hình 3 VLAN: VLAN 1, VLAN 2, và VLAN 3. Một máy tính A kết nối vào VLAN 2. Hỏi địa chỉ **Default Gateway** phải đặt cho máy tính này là địa chỉ nào sau đây?

- A. 192.168.1.1.
  - B. 192.168.1.2.
  - C. 192.168.2.1.
  - D. 192.168.2.2.
  - E. 192.168.3.1.
  - F. 192.168.3.2.
20. Hai tham số được STP sử dụng để bầu chọn “Root Bridge”?
- A. Bridge Priority.
  - B. Địa chỉ IP.
  - C. Địa chỉ MAC.
  - D. Phiên bản IOS.
  - E. Tốc độ kết nối.

# **CHƯƠNG 5**

## **DỊCH VỤ MẠNG**

Chương này trình bày đặc điểm và nguyên tắc hoạt động của một số dịch vụ phổ biến dùng trong hệ thống mạng như DHCP, DNS, Web, FTP, E-mail. Học xong chương này, người học có khả năng:

- Trình bày được vai trò, đặc điểm và nguyên tắc hoạt động của một số dịch vụ mạng phổ biến như DHCP, DNS, Web, FTP, E-mail.
- Cấu hình được các dịch vụ DHCP, DNS, Web, FTP, E-mail.
- Thiết kế được các loại ứng dụng trong một hệ thống mạng cụ thể.

### **5.1. Tổng quan**

Mỗi dịch vụ mạng cung cấp các chức năng giúp người dùng tương tác với các ứng dụng trên mạng. Xét ở góc độ quản trị hệ thống, việc hiểu rõ về nguyên tắc hoạt động, cài đặt và cấu hình các dịch vụ này rất quan trọng để vận hành tốt hệ thống mạng. Một số dịch vụ mạng phổ biến được trình bày trong chương này gồm:

- Dịch vụ DHCP: Là dịch vụ cấp phát địa chỉ IP tự động cho các người dùng trong hệ thống mạng.
- Dịch vụ DNS: Dịch vụ phân giải tên miền.
- Dịch vụ Web: Dịch vụ cung cấp trang Web cho người sử dụng truy cập.
- Dịch vụ FTP: Dịch vụ truyền tập tin trên mạng.
- Dịch vụ E-mail: Dịch vụ thư điện tử.

### **5.2. Dịch vụ DHCP**

#### **5.2.1. Giới thiệu**

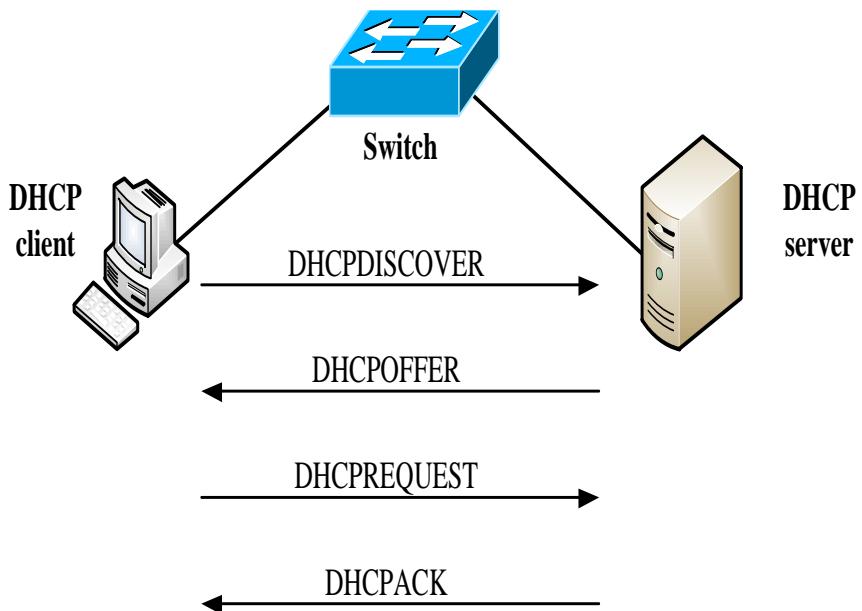
Dịch vụ DHCP cung cấp địa chỉ IP tự động cho các thiết bị trong mạng. Đây là một dịch vụ được sử dụng phổ biến đơn giản hóa trong việc cấu hình, quản lý địa chỉ trong mạng.

DHCP hoạt động theo dạng Client/Server. Máy chủ đóng vai trò DHCP Server được cấu hình các tham số để cấp phát. Các tham số gồm: tên, địa chỉ mạng, dãy địa chỉ cấp phát, Default Gateway, địa chỉ DNS, thời gian người dùng sử dụng địa chỉ IP này.

### 5.2.2. Nguyên tắc hoạt động

#### Trường hợp 1:

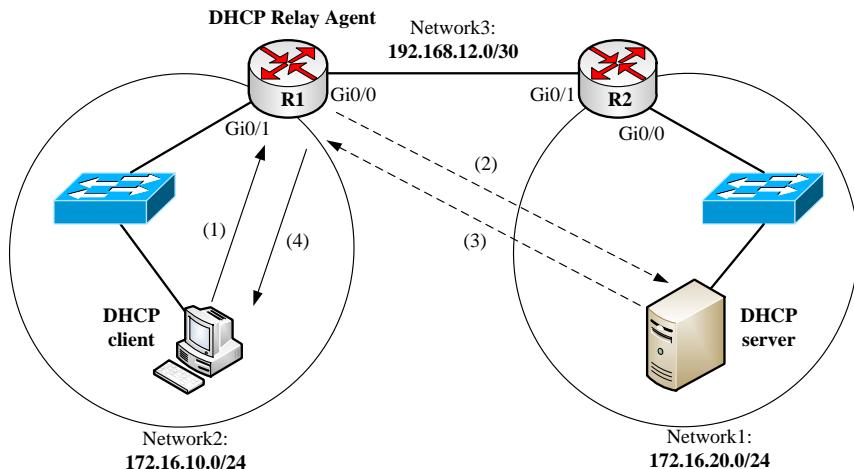
Quá trình trao đổi thông tin giữa DHCP Server và DHCP Client trong trường hợp chúng nằm cùng miền quảng bá diễn ra như sau:



**Hình 5.1: DHCP Server và Client cùng miền quảng bá**

- Bước 1: DHCP Client gửi gói tin **DHCPDISCOVER** dạng Broadcast đến DHCP Server.
- Bước 2: DHCP Server gửi lại gói **DHCPOFFER** dạng Broadcast cho DHCP Client.
- Bước 3: DHCP Client gửi gói **DHCPREQUEST** dạng Broadcast cho DHCP Server.
- Bước 4: DHCP Server gửi gói **DHCPACK** dạng Broadcast cho DHCP Client.

## Trường hợp 2: DHCP Client và DHCP Server nằm khác miền quảng bá (khác mạng).



**Hình 5.2: DHCP Server và Client khác miền quảng bá**

Trong trường hợp DHCP Server và DHCP Client nằm khác miền quảng bá, thì cần thiết phải sử dụng một thiết bị trung gian (gọi là DHCP Relay Agent hay DHCP Helper) để chuyển tiếp yêu cầu từ DHCP Client đến DHCP Server. Bởi vì, trong trường hợp này các gói tin (Local) Broadcast từ Client bị Router chặn nên sẽ không đến được DHCP Server.

Trong hình trên, Router R1 đóng vai trò là thiết bị trung gian giữ vai trò chuyển tiếp các gói tin xin IP của các Client trong Network 2 đến DHCP Server đang ở Network 1. Chi tiết quá trình này diễn ra như sau:

- Bước 1: DHCP Client gửi gói tin DHCPDISCOVER dạng Broadcast.
- Bước 2: DHCP Relay Agent (R1) nhận được gói tin DHCPDISCOVER và chuyển tiếp gói tin này (dạng Unicast) đến DHCP Server.
- Bước 3: DHCP Server gửi lại gói DHCPOFFER (Unicast) trả lời cho R1.
- Bước 4: R1 phát lại gói DHCPOFFER (dạng Broadcast) cho DHCP Client.
- Bước 5: DHCP Client gửi gói DHCPREQUEST dạng Broadcast.

- Bước 6: R1 chuyển tiếp gói DHCPREQUEST cho DHCP Server.
- Bước 7: DHCP Server gửi gói DHCPACK (Unicast) trả lời cho R1.
- Bước 8: R1 phát gói DHCPACK (dạng Broadcast) cho DHCP Client.

Trong quá trình Client thuê IP từ DHCP Server, khi đến 50% thời gian thuê, Client gửi gói tin DHCPREQUEST để kiểm tra DHCP Server có còn tồn tại trên hệ thống không. Nếu DHCP Server không trả lời bằng gói tin DHCPACK thì đến 87,5% thời gian thuê, Client sẽ gửi thêm lần nữa. Nếu không nhận tín hiệu trả lời từ DHCP Server thì Client sẽ phát gói tin DHCPDISCOVER để tìm kiếm và xin IP từ các DHCP Server trên mạng.

Trong quá trình liên lạc giữa DHCP Client và DHCP Server, DHCP Server lắng nghe các thông tin yêu cầu cấp phát IP ở Port 67 (UDP) và Client sử dụng Port 68 (UDP) để trao đổi với DHCP Server.

Ví dụ về các thông số địa chỉ của các gói tin trao đổi giữa DHCP Client và DHCP Server.

|                         |                                                                                                                                                                                       |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gói tin<br>DHCPDISCOVER | $S_{Mac}$ = Địa chỉ MAC của máy gửi (Client)<br>$D_{Mac}$ = FF:FF:FF:FF:FF:FF<br>$S_{IP}$ = 0.0.0.0, $D_{IP}$ = 255.255.255.255<br>$S_{port}$ = 68, $D_{port}$ = 67                   |
| Gói tin DHCPOFFER       | $S_{Mac}$ = Địa chỉ MAC của máy gửi (Server)<br>$D_{Mac}$ = địa chỉ MAC của Client<br>$S_{IP}$ = IP của Server, $D_{IP}$ = 255.255.255.255<br>$S_{port}$ = 67, $D_{port}$ = 68        |
| Gói tin<br>DHCPREQUEST  | $S_{Mac}$ = Địa chỉ MAC của máy gửi (Client)<br>$D_{Mac}$ = FF:FF:FF:FF:FF:FF<br>$S_{IP}$ = 0.0.0.0, $D_{IP}$ = 255.255.255.255<br>$S_{port}$ = 68, $D_{port}$ = 67                   |
| Gói tin DHCPACK         | $S_{Mac}$ = Địa chỉ MAC của máy gửi (Server)<br>$D_{Mac}$ = địa chỉ MAC của Client<br>$S_{IP}$ = IP của Server, $D_{IP}$ = IP được cấp cho Client<br>$S_{port}$ = 67, $D_{port}$ = 68 |

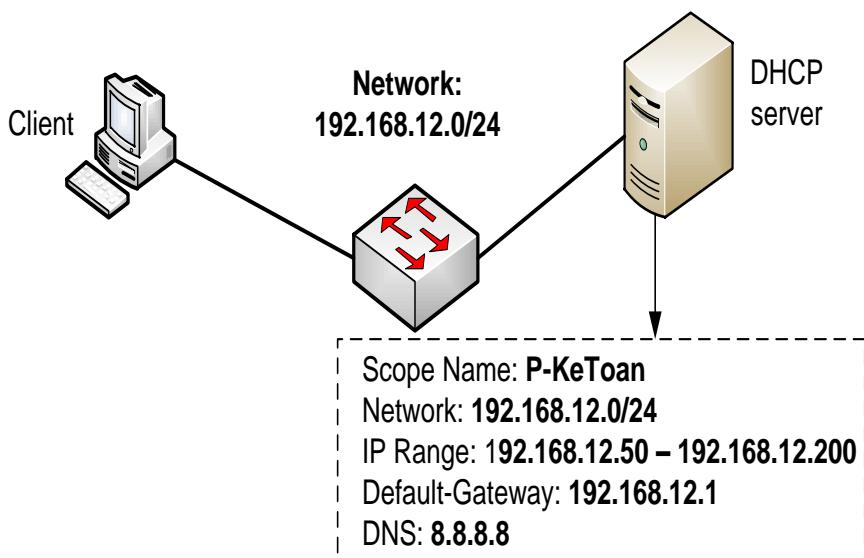
### 5.2.3. Cấu hình cấp phát IP động

Trên DHCP Server thiết lập cấp phát IP động cho một mạng gọi là Scope, các tham số cấu hình cho mỗi Scope gồm:

- Scope Name (Pool): Tên mô tả cho mạng cần cấp phát.
- Network: Địa chỉ mạng.
- IP Range: Xác định dãy địa chỉ IP sẽ cấp phát (xác định địa chỉ đầu và địa chỉ cuối, hoặc xác định địa chỉ đầu và số lượng IP cần cấp phát).
- Lease Duration: Thời gian thuê IP.
- DNS Server: IP của DNS Server để phân giải tên miền.
- Default Gateway: Địa chỉ Default Gateway là địa chỉ IP của Router.
- Reservation: IP dành riêng một thiết bị.

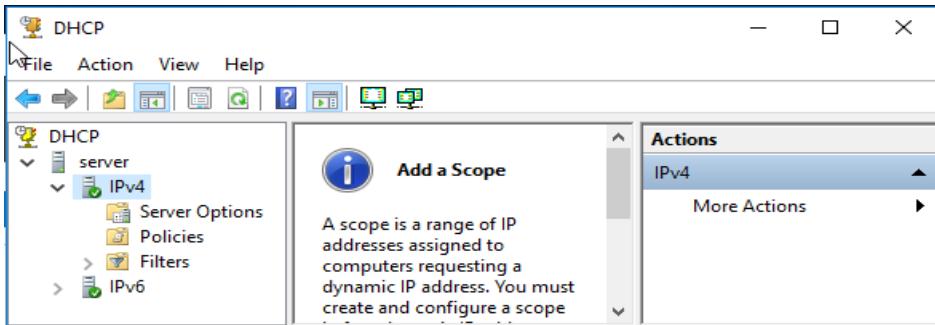
Hai tham số DNS và Default Gateway là các giá trị chọn lựa, không bắt buộc, tùy vào mô hình mạng mà người quản trị có sử dụng hay không.

#### 5.2.3.1. Cấu hình DHCP trên Windows Server



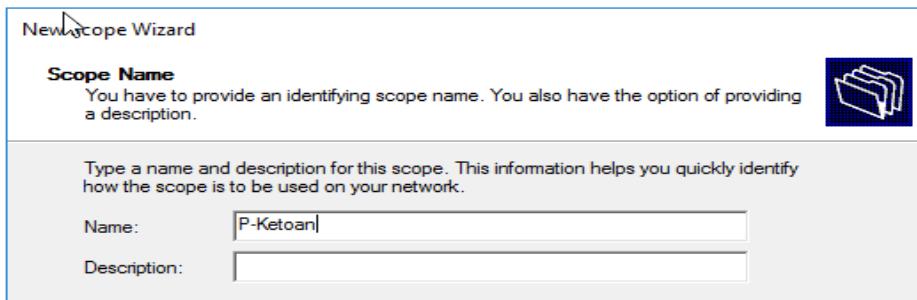
**Hình 5.3:** Mô hình cài đặt thử nghiệm DHCP Server

Cửa sổ cấu hình trên Windows Server:

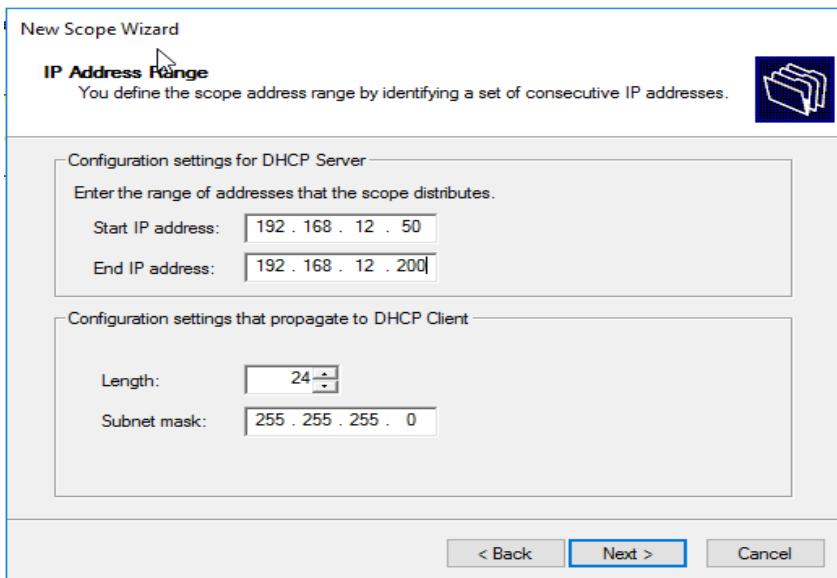


**Hình 5.4:** Giao diện cấu hình DHCP Server trên Window Server

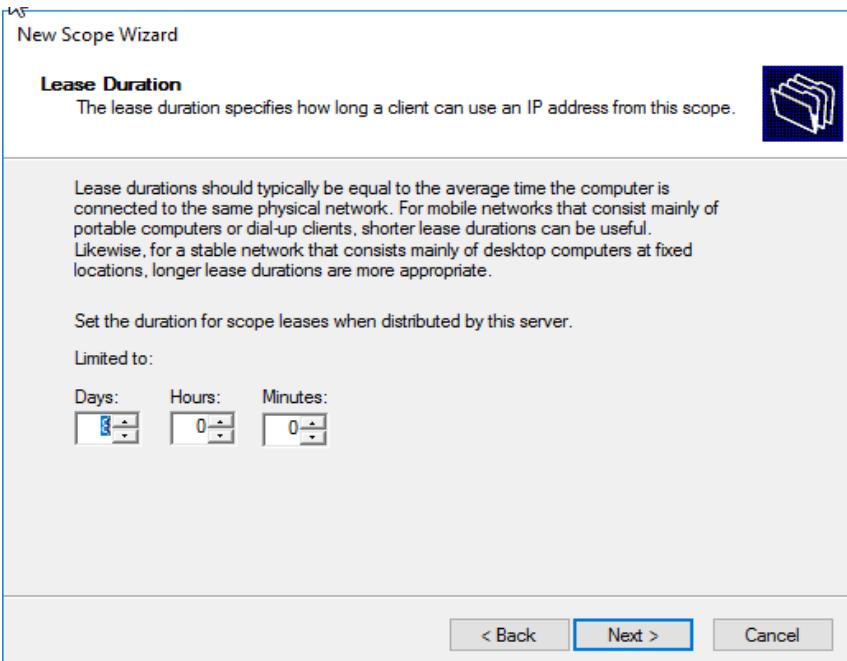
Click chuột phải vào **IPv4**, chọn **New Scope**.



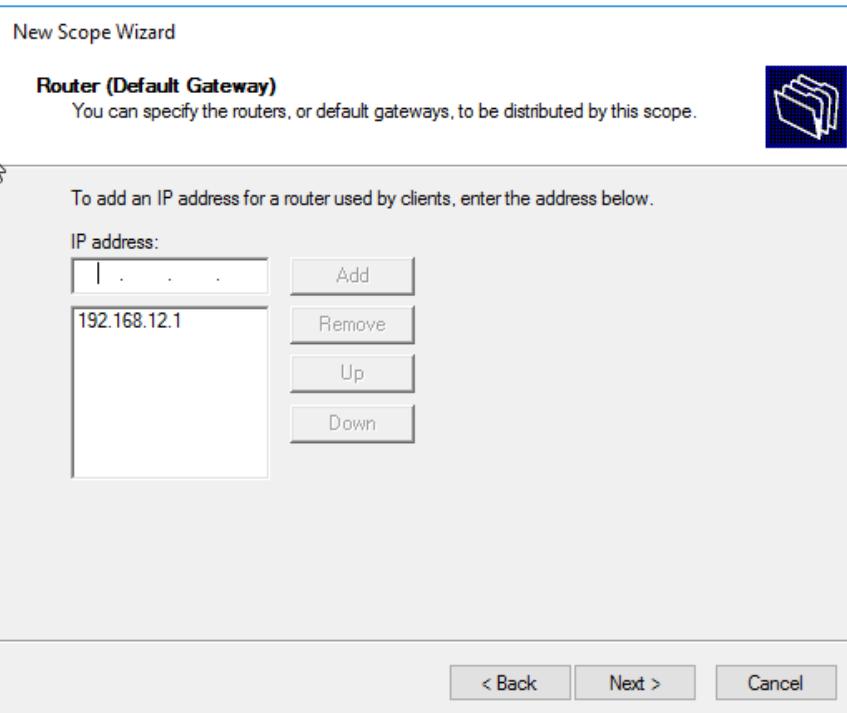
**Hình 5.5:** Đặt tên cho Scope



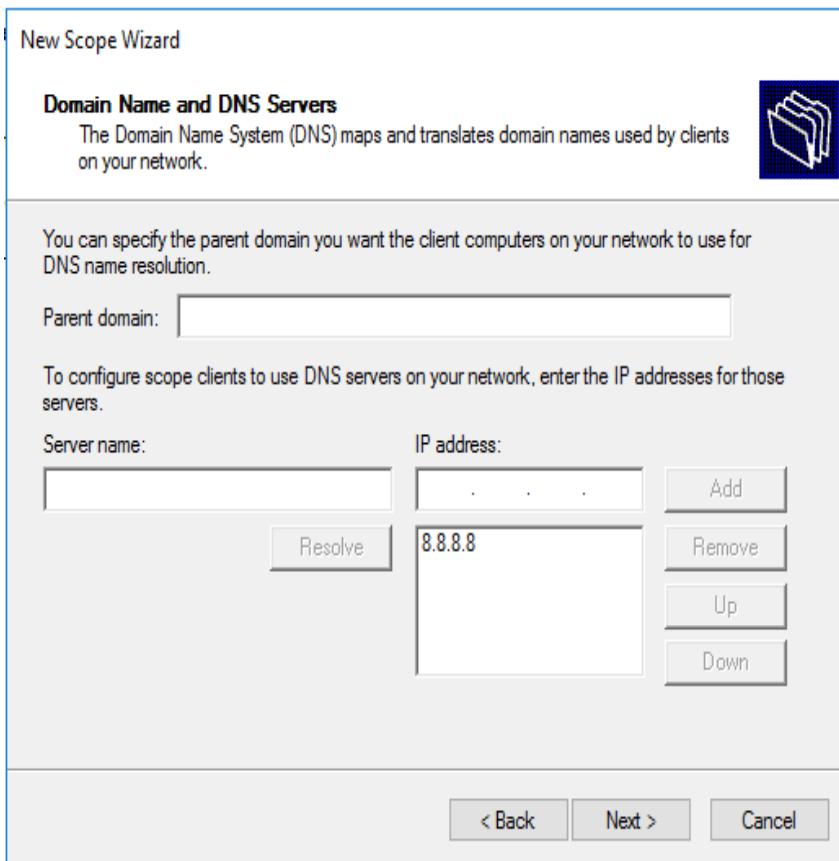
**Hình 5.6:** Đặt dãy địa chỉ IP cho Scope và Subnet Mask



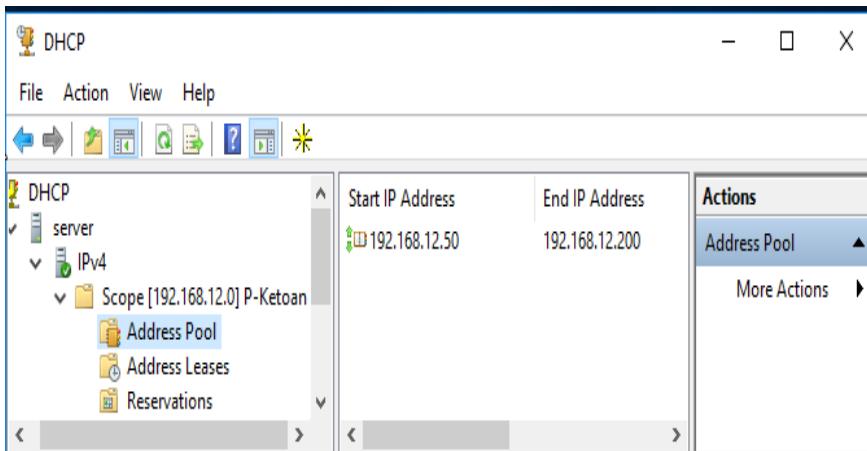
**Hình 5.7:** Thiết lập thời gian cho thuê IP



**Hình 5.8:** Thiết lập địa chỉ Default Gateway cho Scope

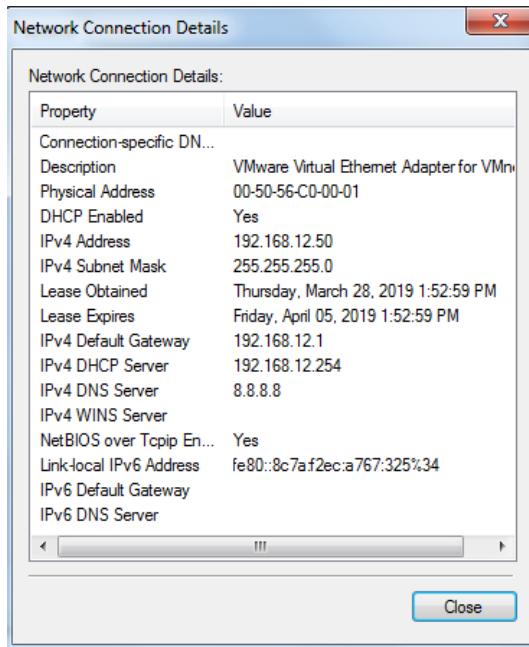


**Hình 5.9:** Thiết lập địa chỉ DNS



**Hình 5.10:** Kết quả cấu hình cho một Scope

- Kiểm tra trên máy Client:



**Hình 5.11:** Kiểm tra kết quả xin cấp phát IP từ máy Client

### 5.2.3.2. Cấu hình trên Linux

Để cấu hình DHCP Server trên Linux, chúng ta cài đặt dịch vụ `dhcp*` và thực hiện cấu hình bằng cách chỉnh sửa các nội dung trong tập tin: `/etc/dhcpd.conf`. Một số tham số cấu hình mẫu sau đây:

```
#vi /etc/dhcp/dhcpd.conf
subnet 192.168.12.0 netmask 255.255.255.0{
    option routers 192.168.12.1;
    option subnet-mask 255.255.255.0;
    option domain-name-servers 8.8.8.8;
    range 192.168.12.50 192.168.12.200;
    default-lease-time 21600;
    max-lease-time 43200; }
```

### Khả năng dự phòng DHCP Server trong hệ thống:

Các thiết bị trên mạng cần IP để cho thiết bị của mình có thể liên lạc được với các thiết bị khác trên mạng. Do đó, việc thiết lập khả năng dự phòng cho DHCP Server là cần thiết để tránh tình trạng DHCP Server bị hư hỏng không cấp được IP cho các Client trên mạng. Việc thiết lập

này có thể dùng thêm Server và cấp phát cho IP với các dãy địa chỉ lặp nhau, khi đó tránh được khả năng cấp phát trùng lặp và tạo khả năng dự phòng cho hệ thống.

#### **5.2.4. Tân công DHCP và giải pháp**

- Điểm yếu của DHCP Server.

Dịch vụ DHCP là dịch vụ mạng phổ biến, các thiết bị có khả năng làm chức năng cấp phát IP động (DHCP Server) tồn tại rất nhiều trên mạng như các Access Point, các Router,... Để kiểm soát việc cấp phát IP động cho các thiết bị trong mạng là vấn đề quản trị quan trọng cần lưu ý. Bất kỳ một thiết bị nào nếu kích hoạt tính năng cấp phát IP động (DHCP Server) đều có khả năng cấp phát cho các thiết bị trong mạng. Do đó, khi một thiết bị nhận IP từ một DHCP không được cấu hình đúng (vô tình hay cố ý) đều có khả năng không thể truy cập bình thường vì các thông số cấu hình khác với IP được hoạch định cho mạng hiện tại.

Một số công cụ tấn công DHCP Server bằng cách làm cho DHCP Server không còn IP trống đã khai báo để cấp phát cho người dùng. Việc tấn công này thực hiện và sau đó, kẻ tấn công có thể tự thiết lập DHCP Server giả để cấp phát và tiến hành các công cụ nghe trộm hay đánh cắp thông tin như kiểu tấn công Man-In-The-Middle.

- Một số giải pháp:

##### **Chống giả DHCP Server:**

Việc giả mạo các DHCP Server để cấp phát cho các người dùng trong mạng và nghe trộm thông tin như trên rất nguy hiểm, gây ảnh hưởng cho người dùng, có thể gián đoạn các hoạt động của người dùng. Hơn nữa, các thiết bị có khả năng cấp phát IP động có rất nhiều như các Access Point cấp phát Wifi là tình trạng phổ biến. Nhiều đơn vị tự mua và gắn vào hệ thống mạng hiện hữu để có thể sử dụng các thiết bị không dây như điện thoại di động, máy tính bảng,... mà không báo cáo hay nhờ sự hỗ trợ kỹ thuật từ bộ phận quản trị mạng. Điều này cũng gây nhiều phiền toái trong một hệ thống mạng. Khi đó, có thể phân đoạn mạng đó được AP cấp phát IP động và không có khả năng truy cập vào các hệ thống bình thường của đơn vị.

Từ những vấn đề trên cho thấy rằng dù vô hình hay có ý, kiểm soát các DHCP Server tồn tại trong hệ thống là vô cùng quan trọng. Các giải pháp chống giả DHCP Server có thể sử dụng như: giải pháp trên Switch có hỗ trợ chứng năng DHCP Snooping hay giải pháp trên môi trường Domain Controller hỗ trợ chứng thực, cấp phép cho các DHCP Server hoạt động trong hệ thống mạng.

## 5.3. Dịch vụ DNS

### 5.3.1. Giới thiệu

Mỗi thiết bị trên mạng có địa chỉ IP dùng để định danh trong các hoạt động trao đổi dữ liệu giữa chúng. Tuy nhiên, việc sử dụng các địa chỉ ít mang tính gợi nhớ, con người thường dễ nhớ hơn thông qua tên như www.microsoft.com hay www.google.com. Do đó, với mỗi tên miền, máy tính cần tìm địa chỉ IP tương ứng trước khi nó có thể giao tiếp với máy tính đó. Quá trình chuyển đổi từ tên ra địa chỉ IP và ngược lại là chứng năng chính của DNS.

Tập tin HOST.TXT giúp cho người dùng đỡ khó khăn hơn bằng cách ánh xạ giữa địa chỉ IP và tên của đối tượng cần truy cập. Qua quá trình phát triển mạnh mẽ của hệ thống mạng cho thấy sự không phù hợp của việc sử dụng tập tin này. Sự không phù hợp này thể hiện ở khả năng mở rộng, độ rộng tên miền, sự nhất quán. Điều này dẫn đến việc ra đời một dịch vụ mới để thực thi công việc này, đó là dịch vụ DNS. Năm 1984, Paul Mockapetris cho ra đời phiên bản đầu tiên và không ngừng được cập nhật, cải tiến sau này.

Dịch vụ DNS là dịch vụ phân giải tên miền, là thành phần thiết yếu của Internet. Để dễ hiểu về dịch vụ này, người ta hay liên tưởng đến danh bạ điện thoại mà mọi người vẫn hay sử dụng hàng ngày trong việc tìm kiếm số điện thoại để liên lạc thông qua tên được lưu tương ứng. DNS cũng hoạt động như cuốn danh bạ trên Internet. Do đó, các máy tính có thể tìm kiếm các địa chỉ IP tương ứng từ các tên miền.

Dịch vụ DNS hoạt động theo cơ chế Client/Server. Phần Server gọi là DNS Server hay Name Server chứa các thông tin cơ sở dữ liệu của DNS. Phần DNS Client hay còn gọi là Resolver là các hàm thư viện dùng

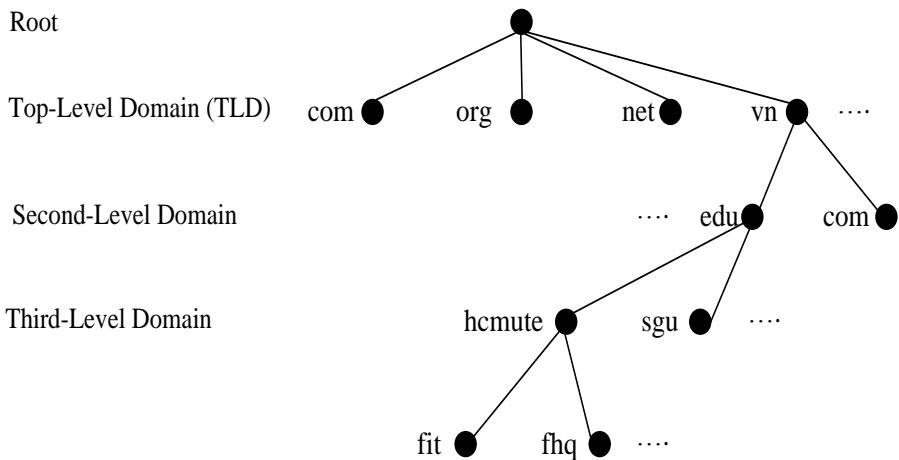
để tạo các truy vấn và gửi đến các DNS Server. Cơ sở dữ liệu của DNS là cơ sở dữ liệu phân tán, cung cấp khả năng mở rộng và có độ tin cậy cao.

DNS sử dụng giao thức TCP và UDP ở tầng Transport, hoạt động ở Port 53. DNS liên quan đến 3 thành phần chính: tổ chức không gian tên miền, các DNS Server và DNS Client hay còn gọi là Resolver.

### 5.3.2. Các thành phần của hệ thống DNS

Sơ đồ tổ chức của DNS:

DNS được tổ chức theo cấu trúc hình cây đảo ngược, mỗi Node trên cây là một miền (Domain) hoặc miền con (Sub Domain)



**Hình 5.12: Tổ chức không gian tên miền Internet**

#### DNS Zone:

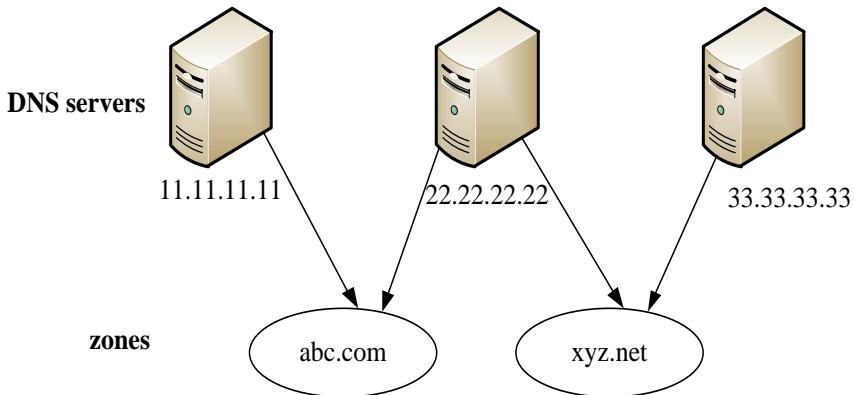
Hệ thống tên miền được quản lý theo các Zone (DNS Zone). Một Zone là một nhóm các Domain hay Sub Domain và được gán sự quản lý cho một cơ quan có thẩm quyền. Một Domain có thể được quản lý bởi nhiều cơ quan có thẩm quyền.

#### Authoritative Name Server:

Mỗi DNS Zone có ít nhất một Server đóng vai trò là Server có thẩm quyền, Authoritative Name Server, để công bố thông tin của Zone, cung cấp các thông tin trả lời cho các truy vấn DNS.

#### Name Server:

DNS Server (hay còn gọi là Name Server) lưu trữ thông tin về tên miền của một hoặc số Zone. Mỗi DNS Server có thể quản lý một Zone hoặc nhiều Zone.



**Hình 5.13: DNS Server và Zone**

Có 2 loại Name Server là Authoritative và Caching. Trong đó, Authoritative Server lưu trữ và duy trì dữ liệu, được chia làm 2 vai trò là: Master - cho phép chỉnh sửa dữ liệu, và Slave - chỉ làm nhiệm vụ nhân bản dữ liệu; Caching Server lưu trữ dữ liệu thu được từ Authoritative Server.

Cơ chế phân giải tên miền: Root Name Server là máy chủ quản lý các Name Server ở mức Top-Level Domain. Khi có truy vấn về một tên miền nào đó thì Root Name Server phải cung cấp tên và địa chỉ IP của Name Server quản lý Top Level Domain. Đến lượt các Name Server của Top Level Domain cung cấp danh sách các Name Server có quyền trên các Second Level Domain mà tên miền này thuộc vào. Cứ như thế đến khi nào tìm được máy quản lý tên miền cần truy vấn.

### 5.3.3. Truy vấn tên miền

Có hai loại truy vấn được sử dụng trong dịch vụ DNS: truy vấn đệ quy và truy vấn tương tác.

- **Truy vấn đệ quy:** Khi DNS Server nhận được truy vấn loại này, nó sẽ trả lời lại kết quả phân giải mà nó có. Nếu không có câu trả lời thì DNS Server sẽ thực hiện gửi truy vấn đến các DNS Server khác để yêu cầu phân giải. Sau đó, nó sẽ gửi kết quả cho DNS Client.

- **Truy vấn tương tác:** Khi DNS Server nhận được truy vấn loại này, nó sẽ trả lời kết quả tốt nhất mà nó có ở thời điểm đó. DNS Server không thực hiện bất cứ các truy vấn nào thêm.

#### 5.3.4. Cấu hình DNS

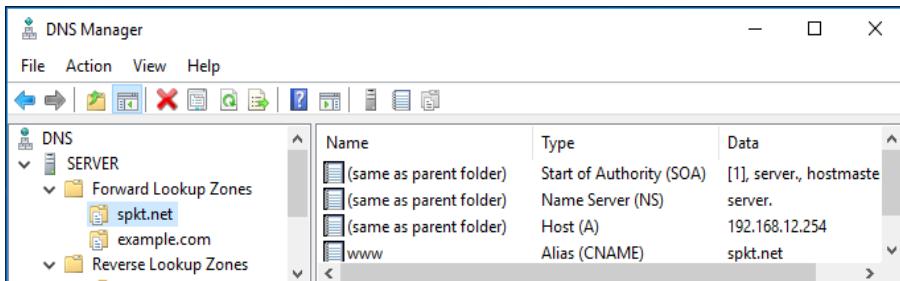
- Phân giải thuận: Là các thiết lập cơ chế phân giải để ánh xạ tên sang địa chỉ IP. Các Record sử dụng trong phân giải tên thuận là: A, CNAME.
- Phân giải nghịch: Là các thiết lập phân giải IP sang tên. Các Record thường dùng trong phân giải tên nghịch là: PTR.

#### Cấu hình DNS trên Windows Server:

Ví dụ: Phân giải các tên miền tương ứng với các địa chỉ như sau:

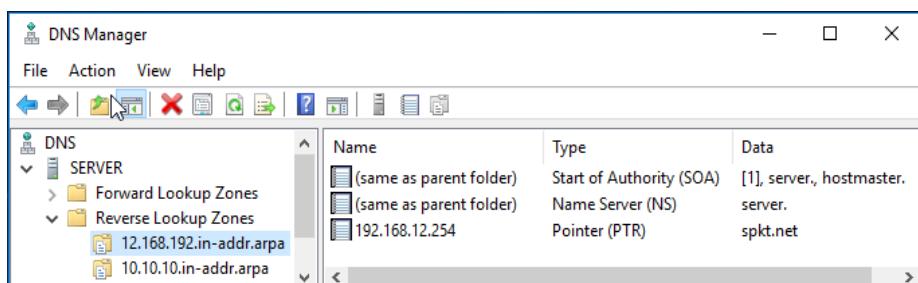
| Tên miền                      | Địa chỉ        |
|-------------------------------|----------------|
| www.spkt.net (spkt.net)       | 192.168.12.254 |
| www.example.com (example.com) | 10.10.10.200   |

Tạo Zone thuận:



**Hình 5.14:** Cấu hình phân giải thuận trên Windows Server

Tạo Zone nghịch:



**Hình 5.15:** Cấu hình phân giải nghịch trên Windows Server

Kiểm tra kết quả phân giải:

```
C:\>Users\Admin>nslookup  
Default Server: spkt.net  
Address: 192.168.12.254  
  
> www.spkt.net  
Server: spkt.net  
Address: 192.168.12.254  
  
Name: spkt.net  
Address: 192.168.12.254  
Aliases: www.spkt.net  
  
> spkt.net  
Server: spkt.net  
Address: 192.168.12.254  
  
Name: spkt.net  
Address: 192.168.12.254  
  
> www.example.com  
Server: spkt.net  
Address: 192.168.12.254  
  
Name: example.com  
Address: 10.10.10.100  
Aliases: www.example.com  
  
> 192.168.12.254  
Server: spkt.net  
Address: 192.168.12.254  
  
Name: spkt.net  
Address: 192.168.12.254  
  
>
```

*Hình 5.16: Kiểm tra kết quả phân giải với NsLookup*

### Cấu hình DNS trên Linux:

Sau khi cài đặt dịch vụ DNS trên Linux, phần cấu hình thực hiện theo các bước sau:

Bước 1. Chính địa chỉ Server DNS lắng nghe trên Port 53 (/etc/named.conf).

```
options {  
    listen-on port 53 { 192.168.1.1 };  
    listen-on-v6 port 53 { ::1 };  
    directory      "/var/named";  
    dump-file     "/var/named/data/cache_dump.db";  
    statistics-file "/var/named/data/named_stats.txt";  
    memstatistics-file "/var/named/data/named_mem_stats.txt";  
    allow-query   { any };  
    recursion yes;  
  
    dnssec-enable yes;  
    dnssec-validation yes;  
    dnssec-lookaside auto;
```

*Hình 5.17: Điều chỉnh địa chỉ của DNS Server và các tham số*

Bước 2. Điều chỉnh #vi /etc/named.rfc1912.zones, khai báo File chứa phân giải thuận và nghịch.

```
zone "spkt.net" IN {
    type master;
    file "spkt.net.zone";
    allow-update { none; };
    allow-query { any; };
};

zone "1.168.192.in-addr.arpa" IN {
    type master;
    file "spkt.net.rr.zone";
    allow-update { none; };
    allow-query { any; };
};
```

Bước 3. Tạo CSDL cho Zone thuận và Zone nghịch vừa khai báo ở bước 2.

```
#vi /var/named/spkt.net.zone
```

```
$TTL 1D
@    IN SOA dns1.spkt.net.    root.spkt.net. (
                                0           ; serial
                                1D          ; refresh
                                1H          ; retry
                                1W          ; expire
                                3H )        ; minimum
                                IN  NS      dns1.spkt.net.
spkt.net.      IN  A       192.168.1.10
www            IN  CNAME   spkt.net
dns1           IN  A       192.168.1.1
```

```
#vi /var/named/spkt.net.rr.zone
```

```
$TTL 1D
@    IN SOA dns1.spkt.net.    root.spkt.net. (
                                0           ; serial
                                1D          ; refresh
                                1H          ; retry
                                1W          ; expire
                                3H )        ; minimum
                                IN  NS      dns1.spkt.net.
1                 IN  PTR     dns1.spkt.net.
10                IN  PTR     spkt.net
```

#### Bước 4. Gán quyền cho 2 File vừa tạo.

```
#chown named:named spkt.net.zone  
#chown named:named spkt.net.rr.zone
```

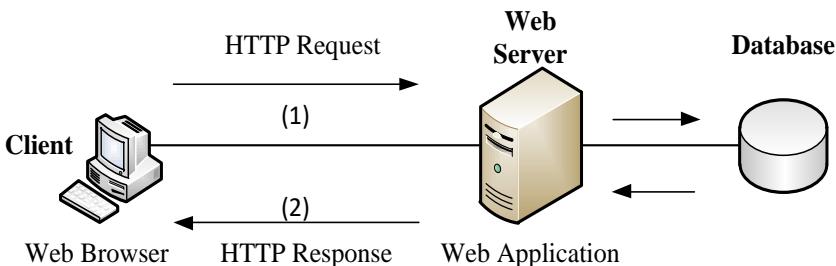
### 5.4. Dịch vụ WEB

#### 5.4.1. Giới thiệu

Dịch vụ World Wide Web (viết tắt là WWW hoặc Web) là một dịch vụ cung cấp thông tin trên hệ thống mạng. Các thông tin này được lưu trữ dưới dạng siêu văn bản và thường được thiết kế bằng ngôn ngữ HTML (Hypertext Markup Language).

Siêu văn bản là các tài liệu có thể là văn bản, hình ảnh tĩnh, hình ảnh động, âm thanh,... được liên kết với nhau qua các mối liên kết và được truyền trên mạng dựa trên giao thức HTTP (Hypertext Transfer Protocol), qua đó người dùng có thể xem các tư liệu có liên quan một cách dễ dàng.

#### 5.4.2. Các thành phần trong dịch vụ Web



**Hình 5.18: Các thành phần trong dịch vụ Web**

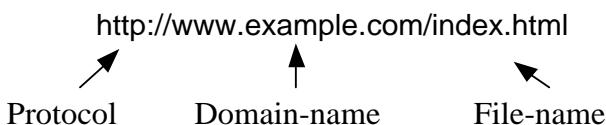
Hệ thống dịch vụ Web thông thường bao gồm 3 thành phần chính: Web Browser, Web Application Server và Database.

- Web Browser là các chương trình phần mềm được cài đặt ở máy tính người dùng, có chức năng gửi các yêu cầu truy cập, nhận kết quả từ Web Server và hiển thị nội dung.
- Web Application Server là Server cài đặt dịch vụ quản trị Website, chứa nội dung trang Web, tiếp nhận và xử lý các yêu cầu từ Web Browser. Database là nơi lưu trữ cơ sở dữ liệu cho trang Web, thông thường nó được đặt trên một Server độc lập với

Web Application Server, tiếp nhận và xử lý các yêu cầu truy vấn thông qua các ngôn ngữ cơ sở dữ liệu.

Để truy cập vào các trang Web, người dùng nhập địa chỉ (URL) vào ô địa chỉ của Web Browser. Mỗi URL là một liên kết xác định một trang trên Web (Web Page), bao gồm 3 thành phần: Protocol, Domain Name:Port và File Directory/File Name.

Ví dụ:



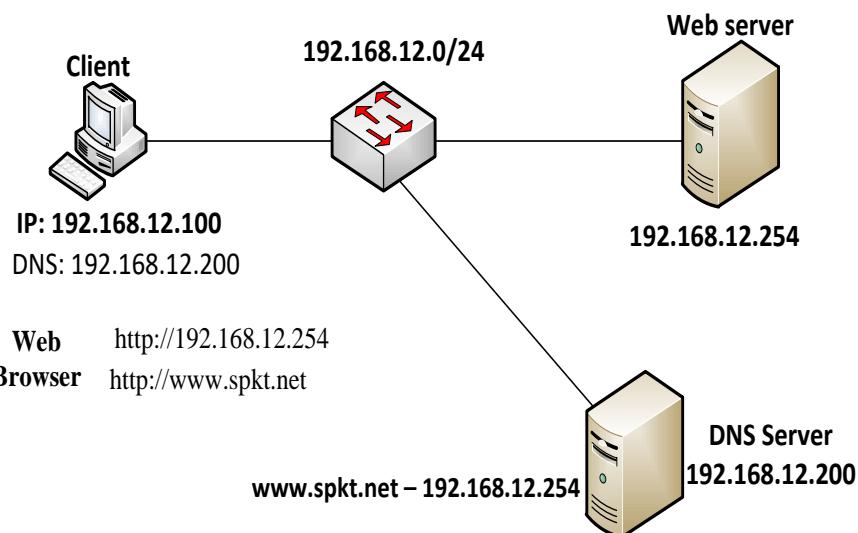
**Hình 5.19:** Tên miền với Port mặc định



**Hình 5.20:** Tên miền với Port đã được điều chỉnh thành 8080

### Triển khai dịch vụ Web:

Để triển khai dịch vụ Web, các bước cần thực hiện như sau:



**Hình 5.21:** Mô hình triển khai dịch vụ Web

Bước 1. Chuẩn bị trang Web. Để có trang Web có thể sử dụng các công cụ lập trình Web như PHP, ASP.NET, JSP,...

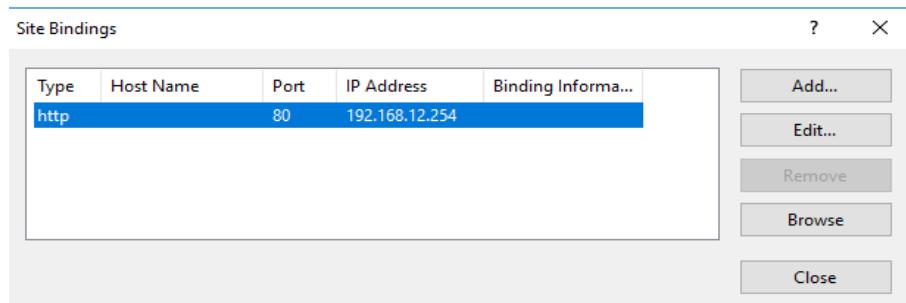
Bước 2. Cài đặt và cấu hình Web Server:

- Lựa chọn hệ điều hành: Windows Server, Linux,...
- Cài đặt dịch vụ Web: Là ứng dụng hỗ trợ cho việc cấu hình. Ví dụ như dịch vụ Web Server (IIS) trên Windows Server,...
- Cấu hình dịch vụ Web: Bao gồm các bước như xác định tên, đường dẫn đến thư mục chứa trang Web (ở bước 1), cổng dịch vụ (mặc định là 80,...).

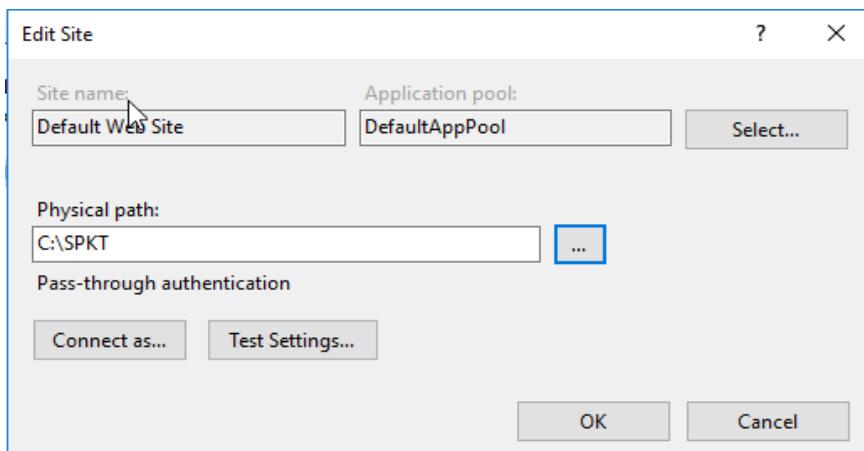
Bước 3. Cấu hình dịch vụ DNS để phân giải tên miền.

Bước 4. Kiểm tra kết quả ở máy tính người dùng.

Ví dụ triển khai trên Windows Server (IIS):



**Hình 5.22: Cấu hình Site Binding**



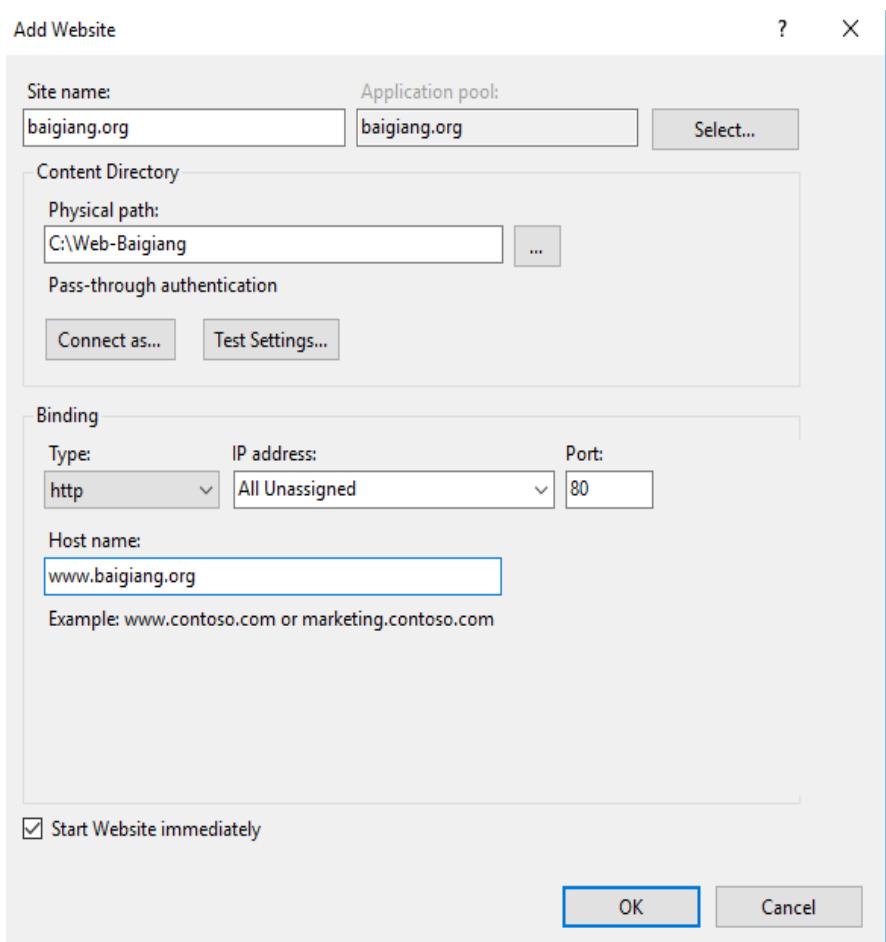
**Hình 5.23: Cấu hình đường dẫn thư mục chứa mã nguồn Web**

### 5.4.3. Triển khai nhiều Website trên 1 Web Server

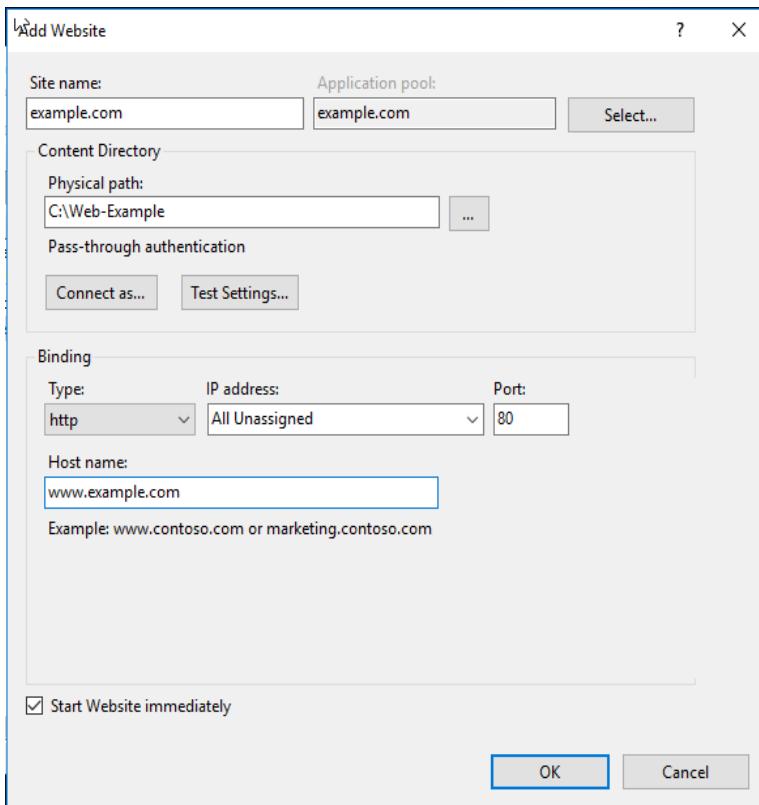
Một Web Server có thể đặt nhiều Website. Ví dụ trên một Server có thể đặt nhiều trang Web như www.example.com, www.baigiang.org,... Trong trường hợp này, trên Web Server sẽ tạo ra các thư mục tương ứng chứa Website và trong bước cấu hình sẽ cấu hình tương ứng phần Binding trên trang Web với Port 80 của ứng dụng Web.

Web Server lắng nghe ở Port 80 (TCP) để tiếp nhận, xử lý và phản hồi các yêu cầu của Web Browser. Trong một số trường hợp khác như tạo ra các trang Web thử nghiệm,... người ta có thể cấu hình cho Web Server lắng nghe ở một Port khác.

- **Triển khai trên Windows Server:**



**Hình 5.24:** Cấu hình cho Website baigiang.org



**Hình 5.25:** Cấu hình cho Website example.org

| Name             | ID | Status         | Binding                         |
|------------------|----|----------------|---------------------------------|
| Default Web Site | 1  | Stopped (http) | 192.168.12.254:80 (http)        |
| baigiang.org     | 2  | Started (http) | www.baigiang.org on *:80 (http) |
| example.com      | 3  | Started (http) | www.example.com on *:80 (http)  |

**Hình 5.26:** Thông tin cấu hình các Website

## - Triển khai trên Linux:

Chỉnh sửa trong File httpd.conf.

```
#vi /etc/httpd/conf/httpd.conf
```

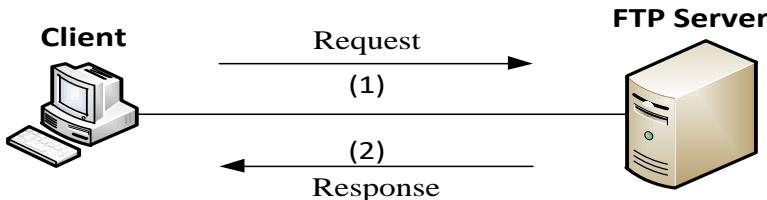
```
<VirtualHost *:80>  
    DocumentRoot /var/www/spkt → thư mục chứa web  
    ServerName ten-domain → thay đổi cho phù hợp  
    ServerAlias www.ten-domain → thay đổi cho phù hợp  
</VirtualHost>
```

## 5.5. Dịch vụ FTP

### 5.5.1. Giới thiệu

FTP (File Transfer Protocol) là giao thức truyền File trên mạng sử dụng giao thức TCP ở tầng Transport.

### 5.5.2. Các thành phần của dịch vụ FTP



**Hình 5.27: Mô hình dịch vụ FTP**

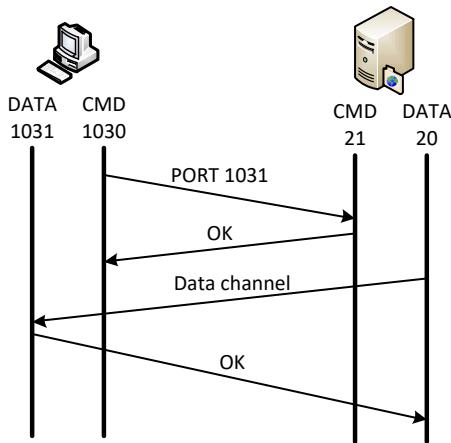
FTP hoạt động ở 2 cổng: Control Port (21) và Data Port (20 hoặc Port khác). FTP Server lắng nghe các yêu cầu dịch vụ từ FTP Client trên cổng 21. Đường kết nối qua cổng 21 tạo nên một kênh điều khiển, cho phép các lệnh được chuyển qua. Để truyền dữ liệu giữa 2 máy thì dùng một kênh khác (Port khác).

### 5.5.3. Phân loại Active FTP và Passive FTP

#### Active FTP:

- Client gửi yêu cầu kết nối với Port ngẫu nhiên ( $N > 1023$ ) đến Port 21 của FTP Server, thông báo về việc mở Port  $N+1$  để nhận dữ liệu từ Server.

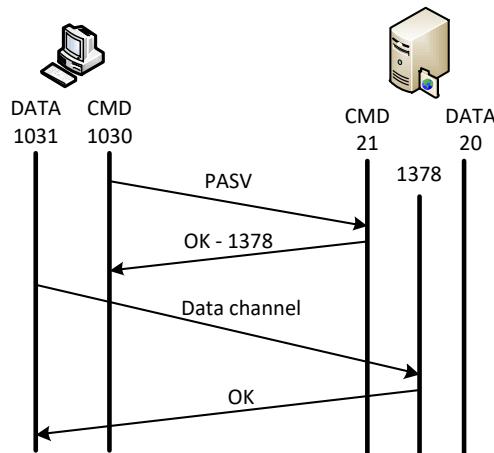
- Server xác nhận.
- Server dùng Port 20 để truyền dữ liệu cho Client.
- Client xác nhận đã nhận dữ liệu.



**Hình 5.28:** Hoạt động của Active FTP

**Passive FTP:** Client khởi tạo 2 phiên kết nối đến Server.

- Client gửi yêu cầu kết nối với Port ngẫu nhiên ( $N > 1023$ ) đến Port 21 của FTP Server.
- Server xác nhận.
- Client mở Port  $N+1$  để nhận dữ liệu từ Server.
- Server dùng Port  $> 1023$  để truyền dữ liệu cho Client.



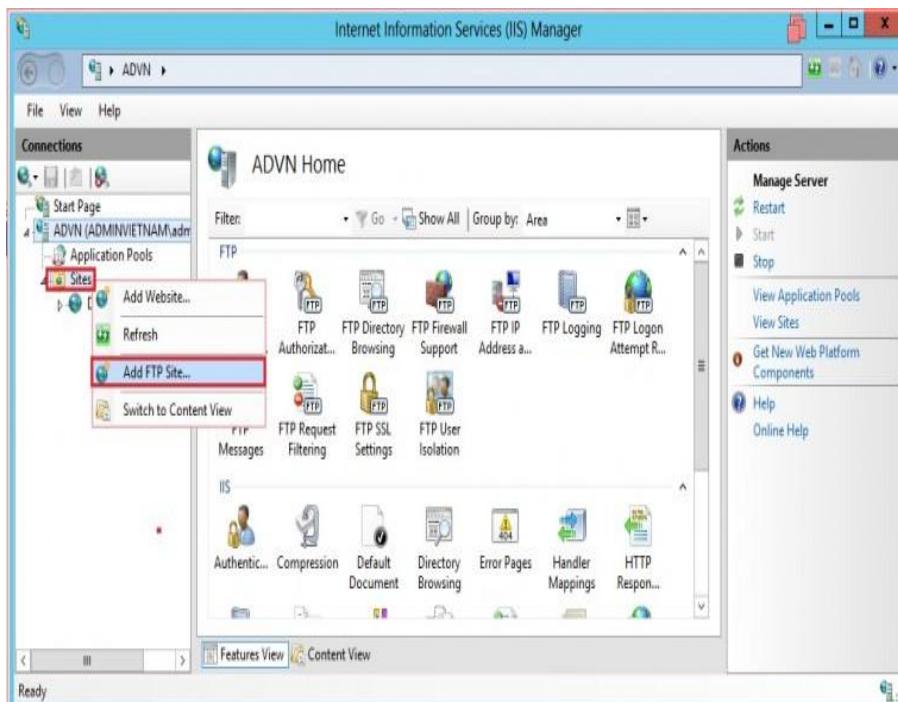
**Hình 5.29:** Hoạt động của Passive FTP

#### 5.5.4. Triển khai dịch vụ FTP

Chúng ta có thể triển khai dịch vụ FTP trên hệ điều hành Windows hoặc Linux với các gói phần mềm cài đặt tương ứng. Với Windows, chúng ta dùng IIS (tương tự như triển khai Web). Với Linux, chúng ta có thể dùng gói cài đặt VSFTPD.

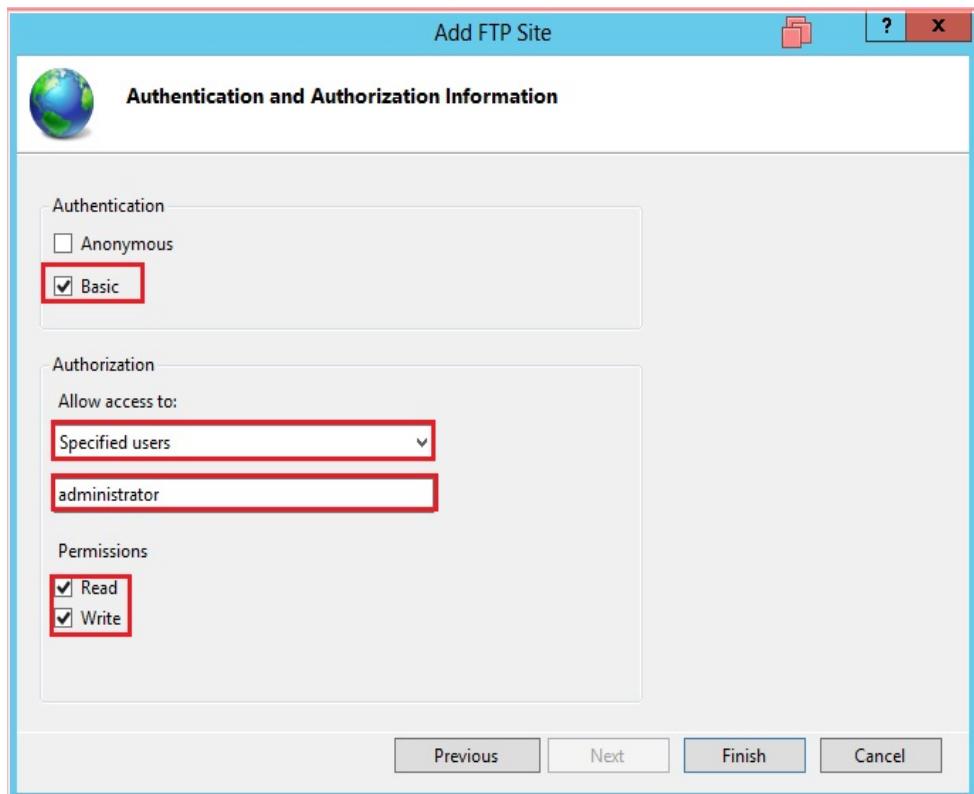
Khi triển khai một FTP Server trên Windows, cần cài sẵn IIS sau đó thực hiện một số tác vụ:

- Tạo 1 thư mục FTP để chứa dữ liệu.
- Tạo User để đăng nhập vào FTP.
- Phân quyền Full Control cho User trên thư mục FTP.
- Tạo mới FTP Site.



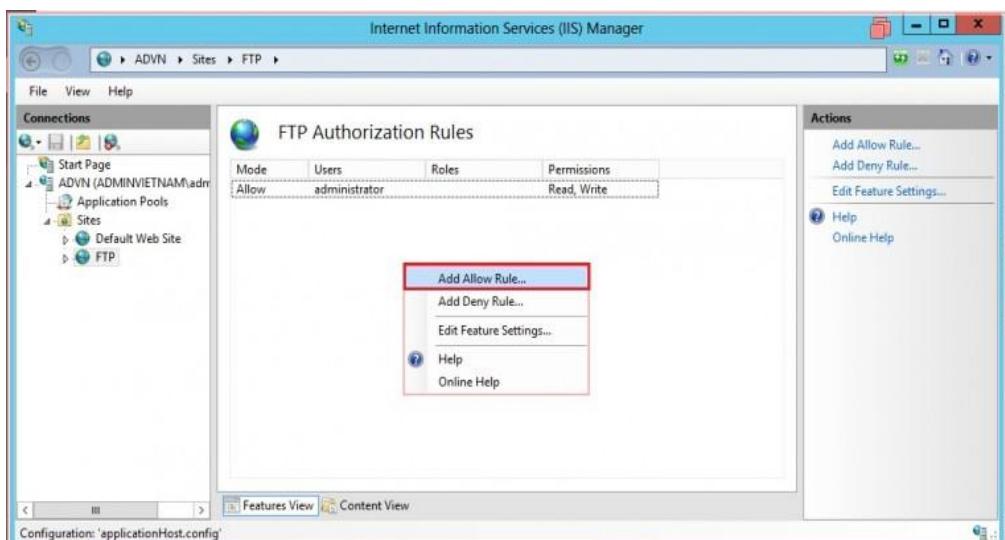
Hình 5.30: Cửa sổ cấu hình FTP Server

- Cấu hình chứng thực FTP - Authentication.



**Hình 5.31:** Cấu hình chung thực

- Cấu hình FTP - Authorization.



**Hình 5.32:** Cấu hình quyền truy cập

Thực hiện test dịch vụ FTP trên một máy tính khác (hoặc test tạm thời trên máy cài FTP Server). Dùng Web Browser để đăng nhập FTP qua địa chỉ IP với tài khoản FTP (ta có thể truy cập FTP bằng tên miền, chỉ cần tạo một Alias trong cấu hình DNS).



**Hình 5.33:** Đăng nhập sử dụng dịch vụ



**Hình 5.34:** Kết quả truy cập FTP Server

Các hệ điều hành Windows đều hỗ trợ FTP Client qua Web hoặc Command Line, ta có thể cài một trình FTP Client khác như: FileZilla, WinSC, Cyberduck.

## 5.6. Dịch vụ E-MAIL

### 5.6.1. Giới thiệu

Dịch vụ E-mail (hay dịch vụ thư điện tử) là một hình thức trao đổi thư từ thông qua mạng Internet. Dịch vụ này được sử dụng rất phổ biến, hữu ích hiện nay.

### 5.6.2. Các thành phần của dịch vụ E-mail

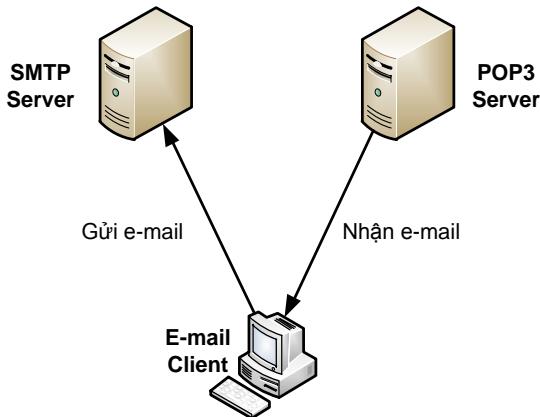
- E-mail Client: Các phần mềm với chức năng soạn thảo nội dung, gửi và nhận thư từ E-mail Server, lưu trữ thư.
- E-mail Server:

Tại mỗi Mail Server thông thường gồm hai dịch vụ: POP3 (Post Office Protocol 3) làm nhiệm vụ giao tiếp Mail giữa Mail Client và Mail Server, SMTP (Simple E-mail Transfer Protocol) làm nhiệm vụ giao tiếp Mail giữa các máy Mail Server.

Khi người dùng gửi một E-mail, máy tính của người dùng sẽ gửi dữ liệu đến SMTP Server. Server sẽ nhìn vào địa chỉ trong E-mail và chuyển tiếp nó đến với Server của người nhận E-mail.

### 5.6.3. Một số giao thức trong dịch vụ E-mail

- POP3 được sử dụng để rút trích E-mail từ một Mail Server. POP3 Server lắng nghe ở Port 110 (TCP), ở phía Client sử dụng Port được sinh ngẫu nhiên (lớn hơn 1024).



**Hình 5.35: Hệ thống E-mail**

Khi người dùng kiểm tra E-mail, E-mail Client kết nối đến POP3 Server (ở Port 110). POP3 Server yêu cầu chứng thực. Sau khi chứng thực thành công, Server cho phép người dùng truy cập đến các dữ liệu của người dùng.

Ưu điểm của POP3 là khả năng “offline”, các E-mail được tải xuống và lưu trữ trong máy người dùng. Khi đó, người dùng có thể truy

cập nội dung E-mail mà không cần thiết phải kết nối Internet. Một số chương trình E-mail Client phổ biến như Microsoft Outlook,...

- Giao thức IMAP: Giao thức này hoạt động cũng tương tự như POP3. Nó có một số ưu điểm như: đầu tiên IMAP chỉ cần Download phần Header của E-mail, khi người dùng chọn đọc E-mail thì phần nội dung mới được tải về.
- SMTP: SMTP hoạt động ở Port 25 (TCP), là giao thức ở tầngỨng dụng, định nghĩa các quy luật về gửi và nhận E-mail giữa các Server.

### **Hoạt động của SMTP:**

Mail Client tạo kết nối TCP đến SMTP Server và tải lên (Upload) nội dung E-mail và địa chỉ đích đến. Thông qua tên miền, Name Server phân giải để xác định việc tự xử lý hay phải chuyển tiếp. Nếu nó biết về người nhận, SMTP Server sẽ chuyển thư đến đó. Nếu nó không biết nó sẽ chuyển đến SMTP Server khác. Trong DNS, Record MX (Mail Exchange) được dùng hỗ trợ cho việc phân phối các E-mail.

- Giao thức S/MIME: Dùng để bảo mật trong dịch vụ E-mail sử dụng các cơ chế mã hóa và chữ ký số.
- Giao thức PGP: Giống như giao thức S/MIME.

#### **5.6.4. Triển khai dịch vụ E-mail**

Chúng ta cần chọn một phần mềm E-mail Server để cài trên một máy, ví dụ như MS Exchange, Mdaemon trên Windows hay Postfix, Sendmail trên Linux. Phía Client sẽ dùng một phần mềm Mail Client để truy xuất E-mail như Outlook Express trên Windows hay Thunderbird trên Linux, hay Webmail trên giao diện Web.

Khi cài đặt mail Server Exchange trên Windows, ta cần chú ý một số tác vụ:

- Cài đặt một bản Windows Server và một số gói phụ thuộc.
- Cài đặt Active Directory Domain Services và các dịch vụ liên quan.
- Cài đặt DNS.
- Tạo các tài khoản người dùng - chính là các tài khoản E-mail.

- Cài đặt Exchange Server và cập nhật.
- Cấu hình Exchange Server để có thể gửi nhận Mail.

Phía Mail Client cần khai báo địa chỉ Mail Server và Username/Password nếu dùng các phần mềm Mail Client trên máy tính. Hoặc chỉ cần mở Web Browser và nhập tên miền của máy Mail Server rồi đăng nhập với Username/Password để vào hộp thư cá nhân.

## 5.7. Tổng kết chương

Nhu cầu sử dụng các dịch vụ mạng ngày càng cao, yêu cầu phía nhà cung cấp dịch vụ mạng càng cần thiết để đáp ứng nhu cầu người dùng, như: Web, Mail, FTP,... Chương này đã trình bày đặc điểm và nguyên tắc hoạt động của một số dịch vụ phổ biến dùng trong hệ thống mạng như DHCP, DNS, Web, FTP, E-mail. Mỗi dịch vụ mạng cung cấp các chức năng giúp người dùng tương tác với các ứng dụng trên mạng. Việc hiểu rõ về nguyên tắc hoạt động, cài đặt và cấu hình các dịch vụ này sẽ giúp người quản trị vận hành tốt hệ thống mạng, đáp ứng nhu cầu sử dụng các dịch vụ mạng.

## 5.8. Câu hỏi và bài tập

1. DNS Record nào ánh xạ từ Hostname ra IP?

- A. A.
- B. CNAME.
- C. PTR.
- D. MX.
- E. SOA.

2. NS Record nào được sử dụng khi phân giải từ IP ra tên miền?

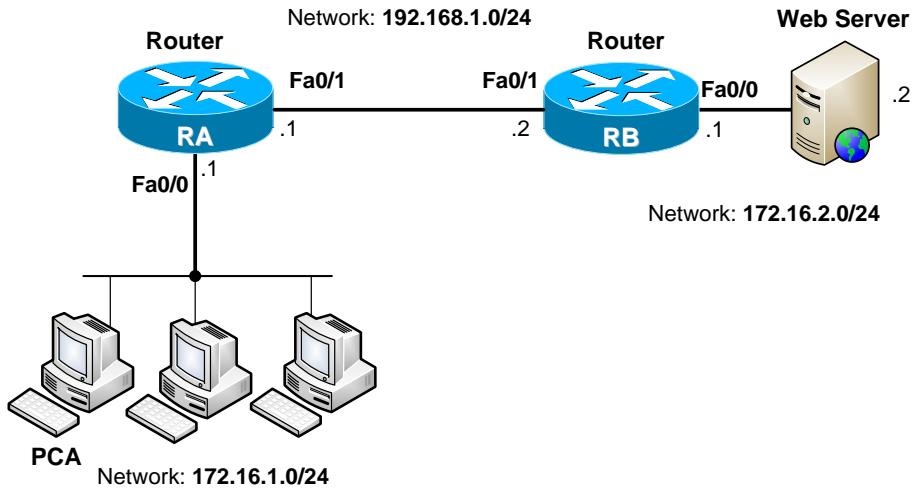
- A. A.
- B. CNAME.
- C. PTR.
- D. MX.
- E. SOA.

3. Chức năng Reservation trong DHCP Server cho phép thực hiện điều gì sau đây?
- Dùng để thiết lập địa chỉ Default Gateway cho các máy tính trong một Scope.
  - Dùng để thiết lập thời gian cho thuê IP trong một Scope.
  - Dùng để cấp phát IP cố định cho một Host dựa vào Hostname của Host đó.
  - Dùng để cấp phát IP cố định cho một Host dựa vào địa chỉ MAC của Host đó.
4. Thứ tự các gói tin trao đổi giữa DHCP Client và DHCP Server để xin cấp phát địa chỉ IP động là?
- DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK.
  - DHCPDISCOVER, DHCPREQUEST, DHCPOFFER, DHCPACK.
  - DHCPREQUEST, DHCPOFFER, DHCPDISCOVER, DHCPACK.
  - DHCPREQUEST, DHCPDISCOVER, DHCPACK, DHCPOFFER.
5. Câu nào sau đây là đúng khi nói về gói tin DHCPDISCOVER?
- Địa chỉ IP đích trong gói tin này là địa chỉ IP của DHCP Server.
  - Địa chỉ IP nguồn trong gói tin này là địa chỉ IP của DHCP Server.
  - Địa chỉ MAC đích trong gói tin này là địa chỉ MAC của DHCP Server.
  - Địa chỉ MAC nguồn trong gói tin này là địa chỉ MAC của DHCP Client.
  - Địa chỉ MAC nguồn trong gói tin này là địa chỉ MAC của DHCP Server.
6. DHCP Server sử dụng giao thức nào ở tầng Transport và cổng bao nhiêu để lắng nghe các yêu cầu cung cấp địa chỉ IP từ DHCP Client?
- TCP/67.

- B. UDP/67.
  - C. TCP/68.
  - D. UDP/68.
  - E. TCP/23.
  - F. UDP/23.
7. Thời điểm nào DHCP Client sẽ liên lạc với DHCP Server để gia hạn thời gian thuê địa chỉ IP?
- A. 25% thời gian thuê.
  - B. 50% thời gian thuê.
  - C. 90% thời gian thuê.
  - D. Khi hết thời gian thuê.
  - E. DHCP Client sẽ không cần liên lạc với DHCP Server, địa chỉ IP được cấp một lần và sử dụng cho đến khi Client chuyển tới một mạng khác.
8. Câu nào sau đây mô tả đúng về phân giải thuận (Forward Lookup) trong DNS?
- A. Phân giải IP từ DNS cục bộ mà không cần sự giúp đỡ của các DNS khác.
  - B. Phân giải tên ra địa chỉ IP.
  - C. Phân giải IP ra tên.
  - D. Chuyển tiếp yêu cầu phân giải tên miền đến một DNS Server khác.
9. Câu nào sau đây là đúng nhất về phân giải ngược (Reverse Lookup) trong DNS?
- A. Yêu cầu phân giải được chuyển đến cho một DNS Server khác để phân giải.
  - B. Phân giải từ IP ra tên miền.
  - C. Yêu cầu phân giải ngược được thực hiện trên DNS Server cục bộ mà không cần trợ giúp từ các DNS Server khác.
  - D. Phân giải từ tên miền ra địa chỉ IP.

10. DNS sử dụng giao thức và cổng nào cho các truy vấn trực tiếp?
- A. UDP/53.
  - B. TCP/53.
  - C. UDP/67.
  - D. TCP/68.
11. DNS sử dụng giao thức và cổng nào cho việc chuyển tiếp các Zone?
- A. UDP/53.
  - B. TCP/53.
  - C. UDP/67.
  - D. TCP/68.
12. Các thông số cấu hình nào trong DHCP Server là tham số tùy chọn khi cấu hình cấp phát địa chỉ IP cho các máy trong mạng?
- A. IP & Subnet Mask.
  - B. IP và Default Gateway.
  - C. Default Gateway và DNS.
  - D. Subnet Mask và DNS.
13. Giao thức nào sau đây dùng để gửi E-mail?
- A. NTP.
  - B. IMAP4.
  - C. POP3.
  - D. SMTP.
14. Giao thức nào sau đây được dùng để nhận E-mail?
- A. POP3.
  - B. SNMP.
  - C. ARP.
  - D. Telnet.
15. Dãy địa chỉ nào sau đây là dãy địa chỉ APIPA?
- A. 169.254.0.1 to 169.254.0.254.

- B. 169.254.0.1 to 169.254.0.255.
  - C. 169.254.0.1 to 169.254.255.254.
  - D. 169.254.0.1 to 169.254.255.255.
16. Cho mô hình mạng:



- PCA** thiết lập một kết nối đến **Web Server**. *Những câu nào sau đây mô tả những thông tin khi dữ liệu bắt đầu xuất phát từ **PCA** đến **Web Server**?*
- A. Port đích (Destination Port) có giá trị 80.
  - B. Địa chỉ IP đích (Destination IP Address) của gói tin là địa chỉ IP của cổng fa0/0 của Router **RA**.
  - C. Địa chỉ IP đích (Destination IP Address) của gói tin là địa chỉ IP của Card mạng của **Web Server**.
  - D. Địa chỉ MAC đích (Destination MAC Address) của Frame là địa chỉ MAC của cổng fa0/0 của **Router RA**.
17. Trong FTP Active, Server FTP dùng cổng nào để truyền dữ liệu đi cho Client:
- A. 21.
  - B. 22.
  - C. 23.

- D. Bất kỳ.
18. Trong các mô hình sau, mô hình nào là mô hình mạng được dùng phổ biến hiện nay:
- Peer To Peer.
  - Remote Access.
  - Terminal Mainframe.
  - Client Server.
19. Dịch vụ Web dùng cặp giao thức và cổng nào?
- HTTP/81.
  - HTTPS/80.
  - HTTP/443.
  - HTTPS/443.
20. Trong FTP Passive, sau khi Server xác nhận yêu cầu truyền dữ liệu được gửi từ Port N của Client thì:
- Client mở Port N+1 để nhận dữ liệu từ Server.
  - Client mở Port 20 để nhận dữ liệu từ Server.
  - Server dùng Port 20 để truyền dữ liệu cho Client.
  - Server dùng Port N+1 để truyền dữ liệu cho Client.

# CHƯƠNG 6

## CÁC MÔ HÌNH QUẢN TRỊ HỆ THỐNG

Chương này sẽ đề cập đến mô hình quản trị mạng Workgroup và Domain, cách thiết lập quyền truy xuất dữ liệu trong Domain, chia sẻ dữ liệu trên mạng và việc quản lý chính sách nhóm. Mô hình dạng Workgroup chỉ phù hợp với mạng nhỏ chỉ vài chục máy trạm - nơi mà các User bình đẳng nhau và từng User sẽ tự quản lý tài nguyên của mình tại mỗi máy cá nhân. Để quản lý một cách tập trung, mô hình Domain được sử dụng nhiều trong các doanh nghiệp. Các thành phần trong Domain, các kiến trúc và các dịch vụ triển khai giúp việc quản lý người dùng và dữ liệu trên mạng đạt hiệu quả cao.

### 6.1. Giới thiệu

Quản lý hệ thống mạng bao gồm các hoạt động: lập kế hoạch, cài đặt và cấu hình, vận hành, xử lý sự cố và duy trì để đảm bảo hệ thống hoạt động liên tục, đáp ứng nhu cầu người sử dụng và đảm bảo hệ thống an toàn, hạn chế các truy cập bất hợp pháp.

Có 2 mô hình quản lý hệ thống mạng:

- Mô hình Workgroup hoặc là Peer To Peer.
- Mô hình sử dụng Domain.

### 6.2. Mô hình quản trị không sử dụng Domain

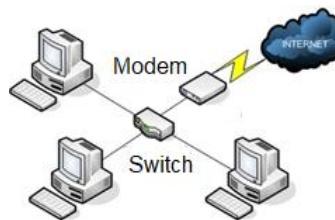
Mô hình mạng Workgroup còn gọi là mô hình mạng Peer To Peer là mô hình mà trong đó các máy tính có vai trò như nhau được nối kết với nhau. Các máy tính tự bảo mật và quản lý các tài nguyên của riêng mình, và tự chứng thực cho người dùng cục bộ.

**Một số đặc trưng:**

- Các dữ liệu và tài nguyên được lưu trữ phân tán tại các máy cục bộ, các máy tự quản lý tài nguyên cục bộ của mình.
- Các Server trong hệ thống mạng có tính chất độc lập, mỗi ứng dụng/dịch vụ có thể phát sinh tài khoản cho người sử dụng.
- Kiến thức quản trị không quá phức tạp, tiết kiệm chi phí đầu tư Server cho việc triển khai Domain.

- Khó đảm bảo tính nhất quán, triển khai áp đặt chính sách/ứng dụng khó khăn, mất nhiều thời gian.
- Phù hợp cho các mạng nhỏ và vừa, dưới mười máy tính và yêu cầu bảo mật không cao.

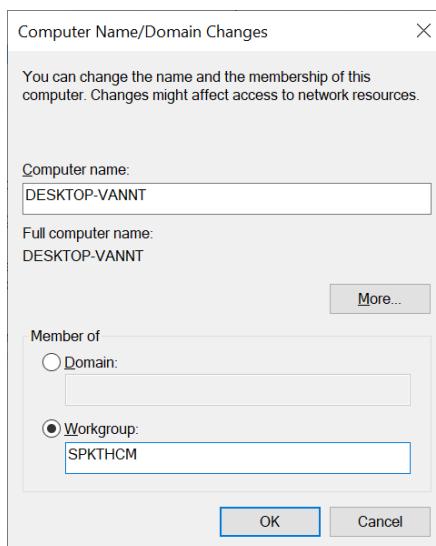
Thông tin người dùng trong một tập tin SAM (Security Accounts Manager) đã được mã hóa và lưu ở trên máy tính cục bộ: \Windows\system32\config\SAM.



**Hình 6.1:** Mô hình quản trị Workgroup

Cấu hình 1 máy tính gia nhập vào 1 Workgroup trên Windows:

- Click **Start**, click **Control Panel** và double-click **System**.
- Click Advanced System Settings, click Computer Name.
- Click Change, trong Workgroup Box nhập tên nhóm làm việc mà ta muốn gia nhập vào:



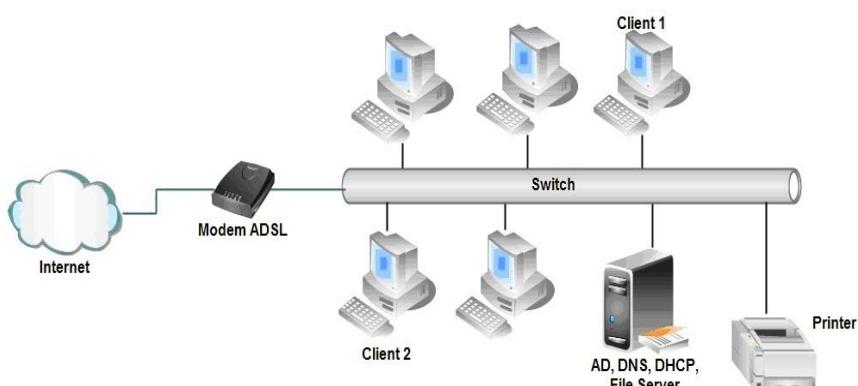
**Hình 6.2:** Thiết lập tên cho Workgroup

### 6.3. Mô hình quản trị sử dụng Domain

Khác với mô hình Workgroup, mô hình Domain hoạt động theo cơ chế Client Server, trong hệ thống mạng phải có ít nhất một máy tính làm chức năng điều khiển vùng (Domain Controller), máy tính này sẽ điều khiển toàn bộ hoạt động của hệ thống mạng.

#### Một số đặc trưng:

- Việc chứng thực người dùng và quản lý tài nguyên mạng được tập trung lại tại các Server trong miền.
- Có ưu điểm về quản trị nhất quán, phân quyền, áp đặt chính sách tốt hơn, kiểm soát hoạt động của hệ thống chặt chẽ, người dùng có thể truy xuất các tài nguyên mạng mà họ được phép truy cập.
- Các Server cung cấp dịch vụ được ủy quyền mới hoạt động được, giúp giảm thiểu các rủi ro xảy ra trong hệ thống.
- Triển khai phần mềm, các chính sách bảo mật nhanh chóng và tự động hóa.
- Phù hợp cho các công ty vừa và lớn, đa chi nhánh.



Hình 6.3: Máy chủ quản lý tập trung bên trong mạng

#### 6.3.1. Các thành phần trong Domain

##### 6.3.1.1. Directory Services

Là một mô hình tổ chức dữ liệu, thông tin và mối quan hệ giữa chúng với nhau, cho phép quản lý tập trung các đối tượng, giúp đơn giản hóa việc quản lý tài nguyên. Là một dịch vụ hoạt động như một tổng đài

(Switchboard) chính trong các OS máy chủ, nó hỗ trợ các nguồn Resources độc lập và phân tán có thể làm việc với nhau, có thể kết nối với nhau. Là một dịch vụ cơ sở làm nền tảng để hình thành một hệ thống Active Directory. Nó được chứa trong NTDS.DIT và các chương trình quản lý, khai thác tập tin này.

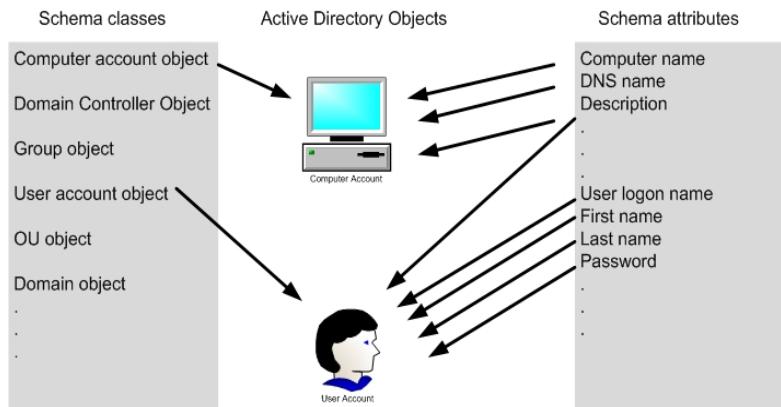
Các thành phần trong Directory Services:

- Object (đối tượng): Bao gồm các máy in, người dùng mạng, các Server, các máy trạm, các thư mục dùng chung, dịch vụ mạng,... là thành tố căn bản nhất của dịch vụ danh bạ.
- Attribute (thuộc tính): Một thuộc tính mô tả một đối tượng. Các đối tượng khác nhau có danh sách thuộc tính khác nhau, tuy nhiên, các đối tượng khác nhau cũng có thể có một số thuộc tính giống nhau. Ví dụ như một máy in và một máy trạm cả hai đều có một thuộc tính là địa chỉ IP.
- Schema (cấu trúc tổ chức): Một Schema định nghĩa danh sách các thuộc tính dùng để mô tả một loại đối tượng nào đó.

**Schema Classes:** Định nghĩa các kiểu đối tượng \_được lưu trữ trong AD.

**Schema Attributes:** Định nghĩa các thông tin về kiểu của từng đối tượng trong AD.

Schema có đặc tính là tùy biến được - các thuộc tính dùng để định nghĩa một lớp đối tượng có thể sửa đổi được.



**Hình 6.4: Các thành phần trong AD**

- Container (vật chứa): Một vật chứa có thể chứa các đối tượng và các vật chứa khác. Vật chứa cũng có các thuộc tính như đối tượng mặc dù vật chứa không thể hiện một thực thể thật sự nào đó như đối tượng. Có ba loại vật chứa là:
  - + Domain: Khái niệm này được trình bày chi tiết ở phần sau.
  - + Site: Một Site là một vị trí. Site được dùng để phân biệt giữa các vị trí cục bộ và các vị trí xa xôi. Ví dụ: các chi nhánh của 1 công ty.
  - + OU (Organizational Unit): Gồm người dùng, nhóm, máy tính và những OU khác. Một OU không thể chứa các đối tượng nằm trong Domain khác.

Ta có thể xây dựng một mô hình thứ bậc của các vật chứa để mô hình hóa cấu trúc của một tổ chức bên trong một Domain. Ta nên sử dụng OU để giảm thiểu số lượng Domain cần phải thiết lập trên hệ thống.

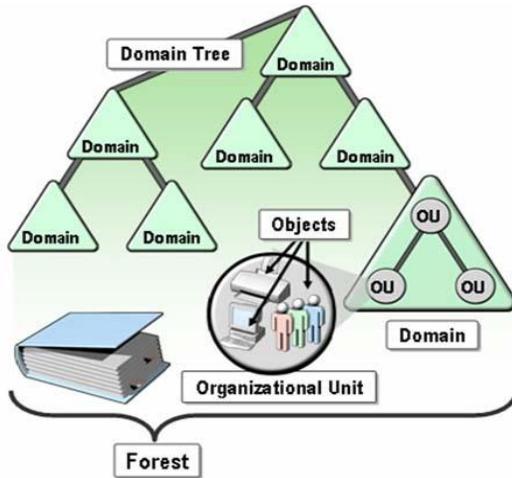
### 6.3.1.2. Active Directory

Là một dịch vụ được Microsoft phát triển và là trái tim của hệ thống Domain Controller. Ra đời từ phiên bản Windows NT 4.0 Server và tồn tại trong các phiên bản Windows Server đến ngày nay. Nó cung cấp một số tính năng quan trọng giúp thiết kế, triển khai, quản trị hệ thống một cách dễ dàng và hiệu quả. Như khả năng lưu trữ tập trung, toàn bộ dữ liệu và thông tin hệ thống được lưu trữ tập trung, cho phép người dùng có thể truy cập dữ liệu từ bất kỳ đâu. Active Directory sử dụng dịch vụ thư mục giúp việc quản lý và truy xuất tài nguyên dễ dàng. Ngoài ra, với tính năng đồng bộ dữ liệu cho phép triển khai tính năng dự phòng, giảm thiểu rủi ro và nâng cao hiệu suất hoạt động của mạng.

Dữ liệu của Active Directory được tổ chức như Service Directory theo kiến trúc logic và vật lý nhất định nhằm quản lý được hệ thống mạng lớn, cung cấp một mức độ ứng dụng mới cho môi trường xí nghiệp.

## 6.3.2. Kiến trúc Active Directory

### 6.3.2.1. Kiến trúc logic của Active Directory

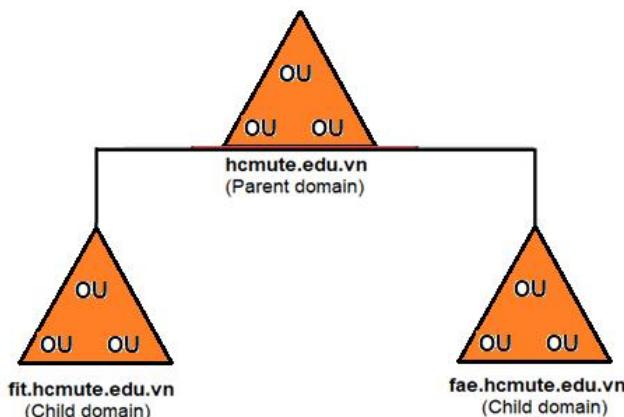


**Hình 6.5: Kiến trúc logic của Active Directory**

Kiến trúc logic giúp ta có thể định hình giao diện của dịch vụ thư mục của tổ chức theo một cấu trúc logic của cơ quan hay đơn vị đó. Active Directory được tạo thành từ 5 thành phần: Objects, Organizational Units, Domain, Domain Tree, Forest.

- **Object** (đối tượng): Bao gồm các máy in, người dùng mạng, các Server, các máy trạm, các thư mục dùng chung, dịch vụ mạng.
- **Organizational Units (OU)**: Là một đối tượng chứa được sử dụng để tổ chức các đối tượng trong Domain thành các nhóm luận lý giúp dễ dàng quản trị. Một OU có thể chứa các đối tượng như tài khoản User, nhóm User, máy tính, máy in, chương trình, thư mục chia sẻ hoặc các OU khác trong cùng Domain. Cấu trúc OU trong một Domain độc lập với cấu trúc OU của domain khác. OU là một cách để phân quyền quản trị trên một Domain giúp giảm nhẹ công tác quản trị trên Domain.
- **Domain**: Là đơn vị chức năng nòng cốt của cấu trúc logic AD. Nó là phương tiện để quy định một tập hợp những người dùng, máy tính, tài nguyên chia sẻ có những quy tắc bảo mật giống nhau, từ đó giúp cho việc quản lý các truy cập vào các Server dễ dàng hơn. Domain có các chức năng chính:

- + Một khu vực quản trị (Administrative Boundary): Các chính sách bảo mật, các quan hệ ủy quyền với các Domain khác.
- + Quản lý bảo mật các tài nguyên chia sẻ.
- + Cung cấp các Server dự phòng làm chức năng điều khiển vùng (Domain Controller), đồng thời đảm bảo các thông tin trên các Server này được đồng bộ với nhau.
- **Domain Tree:** Là một nhóm các Domain được tạo bằng cách thêm một hoặc nhiều Domain con (Child Domain) vào một Domain (Parent Domain) nào đó. Cây có các đặc điểm sau:
  - + Tuân theo cấu trúc không gian tên miền DNS. Tên miền của một Domain cấp dưới là tên tương đối của Domain đó ghép thêm tên của miền cấp trên.
  - + Mọi Domain trên cây sử dụng chung một danh mục gọi là **Global Catalog** chứa thông tin về các đối tượng trên cây.



**Hình 6.6: Domain Tree**

- **Forest:** Là tập hợp các Domain Tree có thiết lập quan hệ và ủy quyền cho nhau.

### 6.3.2.2. Kiến trúc vật lý của Active Directory

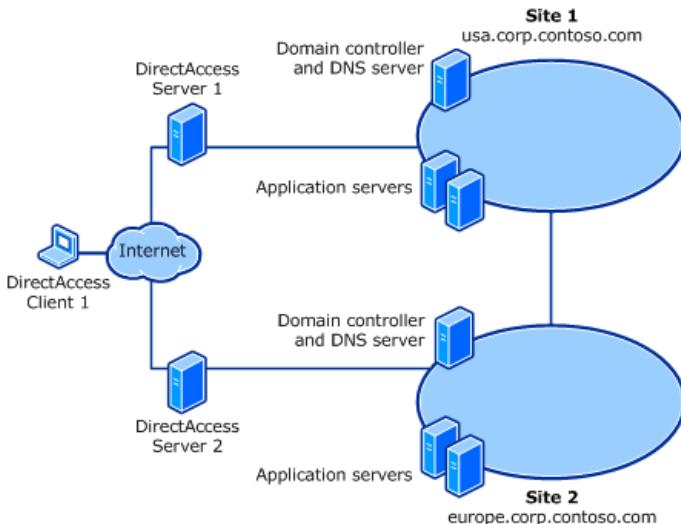
Gồm các thành phần: Site, Domain Controller.

- **Site:** Là tập hợp của một nhóm máy tính trên cùng một Subnet, nhóm các Subnet và Domain Controller có kết nối tốc độ cao. Một Site có thể thuộc về nhiều Domain; một cách tương tự, một

Domain có thể chứa nhiều Site. Site còn được sử dụng để tối ưu hóa hoạt động sao chép (Replication) trên thư mục. Người quản trị có thể lập lịch để việc sao chép giữa các Site (Intersite) được thực hiện vào các giờ rảnh còn việc sao chép trong cùng Site (Intrasite) có thể thực hiện thường xuyên hơn.

Các thành phần của Site:

- + **Subnets:** Là mạng con trong Site, gồm máy tính và các thiết bị nối mạng.
- + **Site Links:** Dùng để kết nối 2 hoặc nhiều Site. Xác định thời gian và tần số đồng bộ giữa 2 Site.
- + **Bridgehead Servers:** Việc đồng bộ giữa các Site xảy ra giữa các Server đầu cầu ở mỗi Site.



*Hình 6.7: Kết nối giữa các Site*

- **Domain Controller (DC):** Là một máy điều khiển miền, quản lý tất cả các tương tác của User trên Domain như xác nhận đăng nhập mạng hoặc tìm kiếm đối tượng trên Active Directory. Các đặc điểm của DC:
  - + Mỗi DC chứa thông tin về Active Directory của Domain và sao chép thông tin đó cho các DC khác thuộc Domain.
  - + Các DC trong một Domain tự động sao chép thông tin về các đối tượng thuộc Domain cho nhau. Khi có một thay đổi trên

Active Directory, thay đổi đó được tự động cập nhật cho các DC trong Domain.

- + Sử dụng nhiều DC trong một Domain cho phép tăng cường khả năng chịu lỗi.

### 6.3.3. Các thành phần trong AD

- **Schema:** Là danh sách các quy tắc định nghĩa các loại đối tượng và các loại thông tin về đối tượng có thể chứa trong Active Directory. Nói một cách khác Schema bao gồm một tập các quy tắc định nghĩa nội dung và cấu trúc của Active Directory.
- **Global Catalog:** Là cơ sở dữ liệu quản lý thông tin về các đối tượng trên một Tree hoặc Forest. Mặc định Global Catalog được tạo ra một cách tự động trên Domain Controller trong một Forest. Server chứa Global Catalog được gọi là Global Catalog Server. Global Catalog thực hiện hai chức năng chính trên Active Directory, đó là:
  - + Cho phép User thực hiện các thao tác đăng nhập (Log-on) bằng cách cung cấp thông tin về thành viên nhóm cho Active Directory.
  - + Cho phép tìm kiếm thông tin trên Active Directory bất kể Domain nào trong Forest chứa dữ liệu thực sự.

### 6.3.4. Quy tắc viết tên đối tượng trên Active Directory

Mỗi đối tượng trên Active Directory được xác định thông qua tên. Active Directory sử dụng các quy tắc viết tên đó là: tên đầy đủ (Distinguished Name), tên tương đối (Relative Distinguished Name), tên định danh duy nhất toàn cục (Globally Unique Identifier).

#### 6.3.4.1. Tên đầy đủ (Distinguished Name DN)

Là cách viết tên đầy đủ nhất, tên đầy đủ bao gồm tên Domain chứa đối tượng và toàn bộ đường dẫn trên cấu trúc cây Domain đến đối tượng.

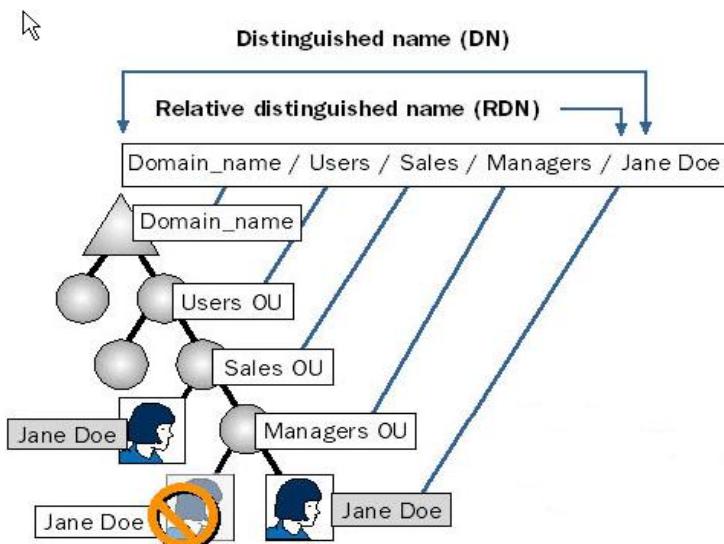
Ví dụ: DC=com,DC=microsoft,OU=dev,CN=Users,CN=Firstname.

Trong đó DC, OU và CN là các thuộc tính của tên đầy đủ, nghĩa của các ký hiệu như sau:

| Thuộc tính | Ý nghĩa                  |
|------------|--------------------------|
| DC         | Domain Component Name    |
| OU         | Organizational Unit Name |
| CN         | Common Name              |

#### 6.3.4.2. Tên tương đối (Relative Distinguished Name RDN)

- Tên tương đối của một đối tượng là phần của tên đầy đủ mà cũng chính là một thuộc tính của đối tượng đó. Ví dụ tên tương đối của Firstname của một đối tượng User là Firstname, tên tương đối của đối tượng cha là Users.
- Tên tương đối các đối tượng có thể trùng trên Active Directory nhưng không thể có hai đối tượng cùng tên tương đối trong cùng OU.



**Hình 6.8: Sơ đồ tên tương đối DN**

#### 6.3.4.3. Tên định danh duy nhất toàn cục (GUID)

Là một giá trị 128 bit được gán cho mỗi đối tượng mỗi khi đối tượng được tạo ra trên Active Directory. Đối tượng trên Active Directory có thể bị di chuyển hoặc đổi tên nhưng giá trị này không bao giờ thay đổi.

## 6.3.5. Cài đặt Domain Controller trên Windows Server

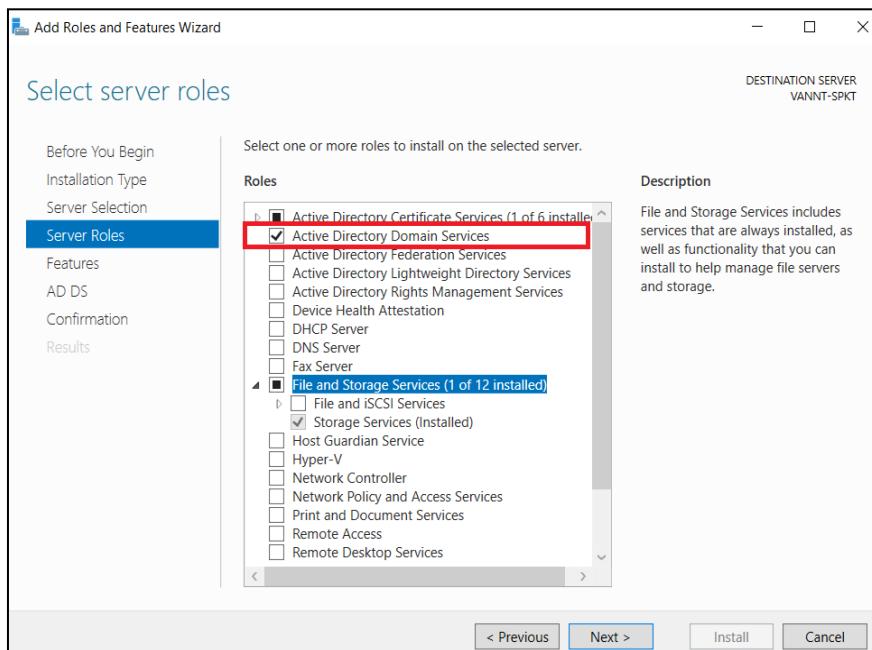
### 6.3.5.1. Yêu cầu cài đặt

Khai báo đầy đủ các thông số TCP/IP, DNS Server có địa chỉ chính là địa chỉ IP của Server cần nâng cấp. Nên cấu hình dịch vụ trước khi nâng cấp Server, hoặc cài đặt DNS tự động trong quá trình nâng cấp. Muốn tạo máy DC thì phải cần đến dịch vụ miền AD (ADDS - Active Directory Domain Services). Các minh họa cài đặt dưới đây được thực hiện trên Windows Server 2016. Các Version Windows Server, giao diện có thể khác một chút khi tiến hành cài đặt và cấu hình.

### 6.3.5.2. Cài đặt ADDS

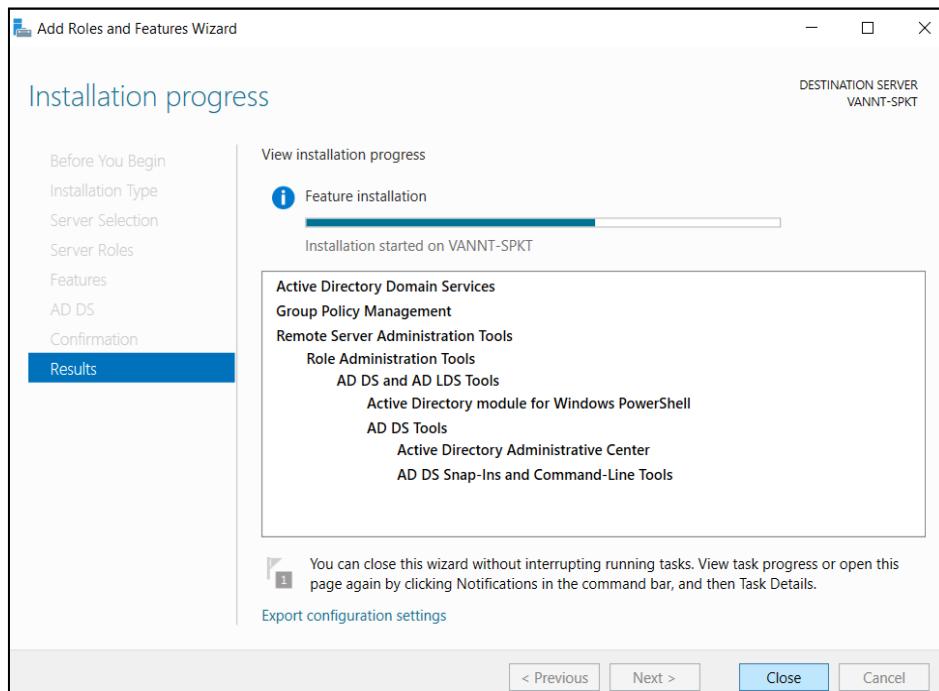
Dịch vụ miền AD (ADDS) sẽ lưu trữ thông tin về các đối tượng trong mạng và tổ chức các thông tin này sao cho những người dùng có thể tiếp cận một cách dễ dàng. ADDS dùng DC để giúp những người dùng mạng truy nhập vào các tài nguyên mạng chỉ cần thông qua việc Log-in của User vào hệ thống.

Thực hiện: Từ Server Manager, chọn Add Roles and Features\Server Roles.



**Hình 6.9:** Cài đặt dịch vụ AD

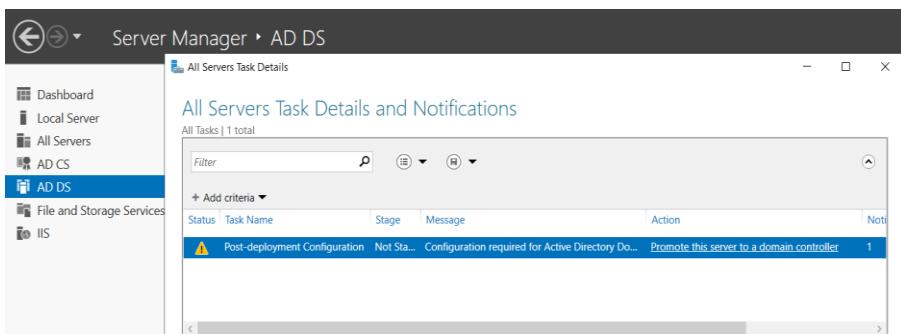
Trong quá trình cài đặt, một số gói phụ thuộc sẽ được yêu cầu cài đặt. Kết quả cài đặt:



**Hình 6.10:** Quá trình cài đặt AD

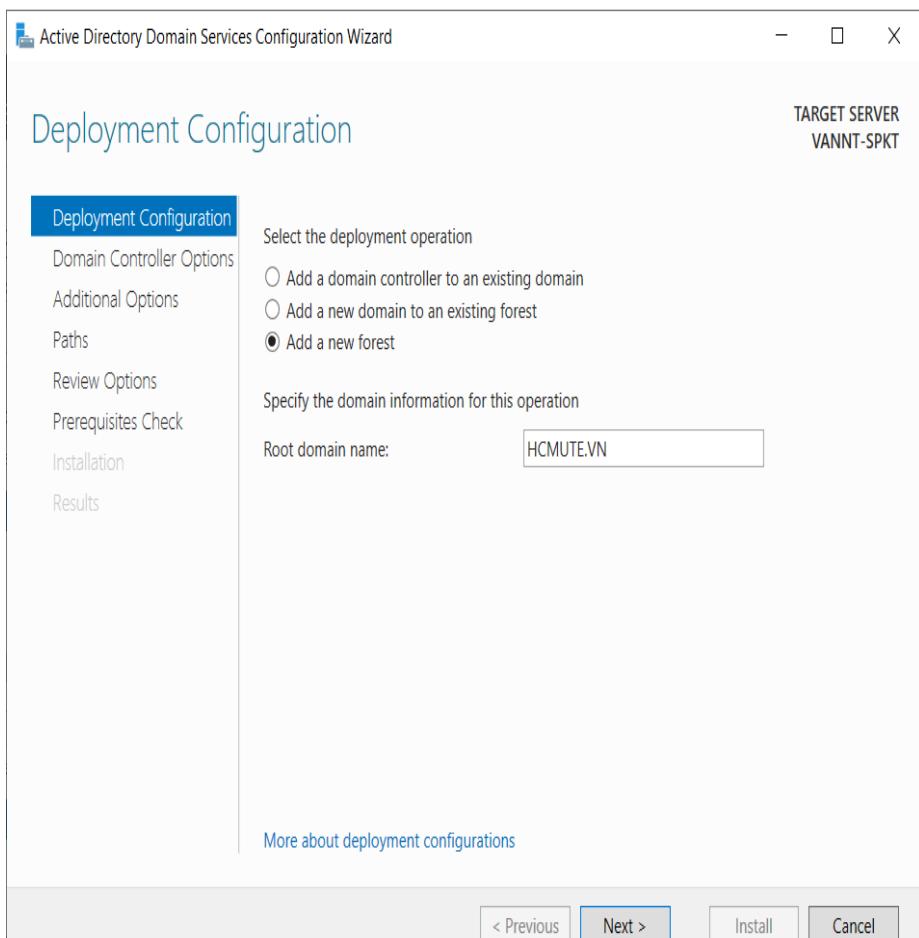
### 6.3.5.3. Cài đặt Domain Controller

Để bắt đầu tạo Domain Controller, vào link “Promote this server to a domain controller” tại màn hình giao diện Server Manager/ADDS:



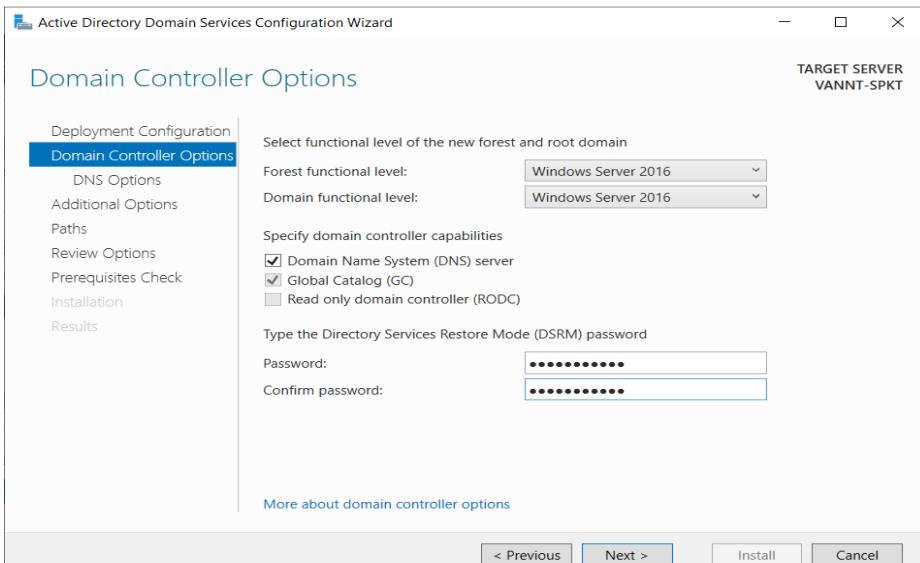
**Hình 6.11:** Giao diện cấu hình AD

Chúng ta cần khai báo DC được tạo là đầu tiên hay thêm vào một Forest đã có, dưới đây là 1 Domain trong 1 Forest mới:



**Hình 6.12:** Đặt tên cho Domain

Trong quá trình tạo, một số khai báo khác như đường dẫn, DNS,... Quá trình tạo DC sẽ yêu cầu nhập mật khẩu DSRM - Directory Services Restore Mode, là một thành phần trong chế độ khởi động Safe Mode của Windows Server khi đã thực hiện nâng cấp lên Domain Controllers. DSRM cho phép người quản trị (Administrator) có thể Repair, Recover, Restore cơ sở dữ liệu của Active Directory. DSRM không được dùng để đăng nhập ở chế độ khởi động bình thường của Windows Server khi đã nâng cấp thành Active Directory.

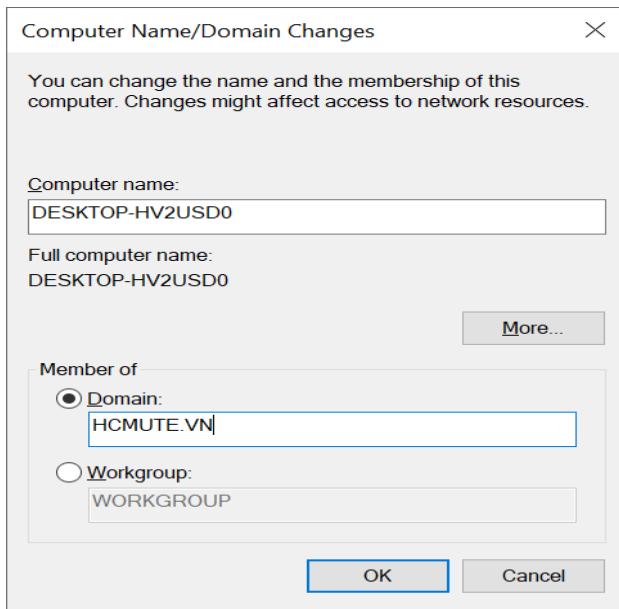


**Hình 6.13:** Cấu hình Password cho Mode Restore

Cần khởi động lại máy khi quá trình tạo DC kết thúc.

#### 6.3.5.4. Gia nhập máy trạm vào Domain

Dùng một máy trạm trong mạng, gia nhập vào Domain vừa tạo. Chọn Control Panel\All Control Panel Items\System\Advanced System Setting, chọn Computer Name, nhập Domain:



**Hình 6.14:** Máy Client gia nhập vào Domain

### 6.3.5.5. Xây dựng các Domain Controller đồng hành

Trong các hệ thống Active Directory lớn, nếu chỉ có một Domain Controller thì Server này có thể bị quá tải khi nhiều User cùng yêu cầu chứng thực. Bên cạnh đó khi Domain Controller này bị lỗi thì toàn bộ hệ thống sẽ bị ngưng hoạt động, các User sẽ không được chứng thực. Trong phần này sẽ hướng dẫn các bạn triển khai Additional Domain Controller (ADC) - DC đồng hành sẽ chạy song song với Domain Controller chính để đảm bảo hệ thống luôn sẵn sàng.

Các bước thực hiện:

- Chọn 1 Server muốn cài DC đồng hành.
- Cài ADDS (như bước cài đặt máy DC đầu tiên ở trên).
- Cài DC đồng hành.
  - + Ở màn hình Deployment Configuration, chúng ta cần chọn kiểu DC, do cần xây dựng Additional DC nên ta chọn “Add a domain controller to an existing domain”. Nhập tên Domain. Cần xác thực là người quản trị cấp miền thì mới có quyền tạo Additional DC.
  - + Tại Domain Controller Options, đặt mật khẩu khôi phục hệ thống Domain khi có sự cố.
  - + Tại Additional Options, chọn Server để đồng bộ dữ liệu - chính là Server đã xây dựng DC đầu tiên.
  - + Paths, chỉ định đường dẫn lưu trữ CSDL của hệ thống miền.
  - + Cuối cùng chọn Install để cài đặt.
- Sau khi cài đặt xong, chúng ta có thể kiểm tra DC đồng hành đã được cài đặt thành công hay chưa bằng cách dùng công cụ Active Directory Users and Computers. Ví dụ:

| Name      | Type     | DC Type | Site                    | Description |
|-----------|----------|---------|-------------------------|-------------|
| K16-SRV01 | Computer | GC      | Default-First-Site-Name |             |
| K16-SRV02 | Computer | GC      | Default-First-Site-Name |             |

Hình 6.15: Công cụ quản trị trên Domain

### 6.3.5.6. Xây dựng Child Domain

Khi công ty có nhu cầu mở rộng, cần xây dựng thêm Domain để quản lý người dùng và tài nguyên thì Domain con là lựa chọn để mở rộng từ Domain cha đang tồn tại. Ví dụ Child Domain “fit.hcmute.vn” được tạo từ Domain cha “hcmute.vn”.

Các bước thực hiện:

- Chọn 1 Server muốn cài Child Domain.
- Cài ADDS (như bước cài đặt máy DC đầu tiên ở trên).
- Cài Child Domain.
  - + Ở màn hình Deployment Configuration, chúng ta cần chọn kiểu DC, do cần xây dựng Child Domain nên ta chọn “Add a new domain to an existing forest”. Nhập thông tin Domain gồm: Domain cha, tên Child Domain. Cần xác thực là người quản trị cấp miền thì mới có quyền tạo Child Domain.
  - + Tại Domain Controller Options, đặt mật khẩu khôi phục hệ thống Domain khi có sự cố.
  - + Đặt lại tên NetBIOS hoặc sử dụng tên NetBIOS mặc định.
  - + Paths, chỉ định đường dẫn lưu trữ CSDL của hệ thống miền.
  - + Cuối cùng chọn Install để cài đặt.

### 6.3.6. Quản trị User, Group trên Windows Server

User và Group là những thành phần cơ bản để quản lý và sử dụng tài nguyên trên máy tính hay trên hệ thống mạng. Tùy vào mức độ được cấp quyền mà người dùng có quyền truy xuất vào những tài nguyên nào trong hệ thống mạng (Domain), hoặc trên máy tính (Local) trong trường hợp Windows Server chưa lên Domain.

User là một đối tượng để xác định cá nhân nào sử dụng trong hệ thống. Thông tin về User Account có nhiều tham số nhưng một Account phải có tối thiểu 2 tham số là **Username** và **Password**.

Group là một nhóm các User có cùng tính chất. Group được tạo ra nhằm đơn giản hóa quá trình quản lý và phân quyền.

### 6.3.6.1. Quản lý User và Group trên máy cục bộ (Local Host)

Việc quản lý cục bộ có thể thực hiện ở: Windows XP Pro, Windows Vista và Windows 7 Professional, Ultimate, Windows Server (chưa dựng Domain). User và Group cục bộ chỉ có giá trị trên máy và tài nguyên trên chính máy chứa nó. Trong máy có một số User và Group được tạo sẵn, chúng không thể xóa, nhưng có thể Disable.

Có hai User được tạo sẵn (Built-in Account):

|                |                                                                                                                                                                                                    |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administrators | Tài khoản có quyền cao nhất trong hệ thống. Administrator bị Disabale thì vẫn có thể Log-in vào chế độ Safe Mode, vì vậy việc tạo Password của User này là rất quan trọng để bảo mật cho hệ thống. |
| Guest          | Tài khoản khách, thường bị Disabale.                                                                                                                                                               |

Có một số Groups được tạo sẵn:

|                    |                                                                                                                                                                                                                           |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administrators     | Các thành viên thuộc nhóm có thể thực hiện tất cả các chức năng quản trị trên máy tính. Mặc định, tài khoản User Administrator thuộc về nhóm này.                                                                         |
| Backup Operators   | Các thành viên thuộc nhóm có thể chạy chương trình Windows Backup để sao lưu và khôi phục dữ liệu.                                                                                                                        |
| Guests             | Các thành viên thuộc nhóm chỉ có thể truy xuất một cách hạn chế trên các tài nguyên đã được gán quyền sở hữu. Thành viên thuộc nhóm này không thể làm thay đổi Desktop. Mặc định, tài khoản User Guest thuộc về nhóm này. |
| Power Users        | Các thành viên thuộc nhóm có thể tạo mới, điều chỉnh tài khoản User cục bộ và chia sẻ tài nguyên.                                                                                                                         |
| Users              | Các thành viên thuộc nhóm chỉ có thể thực hiện một số tác vụ nhất định tùy thuộc vào quyền sở hữu được gán. Khi một tài khoản User cục bộ được định nghĩa, tài khoản đó sẽ thuộc về nhóm Users.                           |
| Một số Groups khác | Xem trong Computer Management\Local Users and Groups\Groups.                                                                                                                                                              |

Tạo User và Group cục bộ được thực hiện trong Computer Management\Local Users and Groups, và được lưu trong File SAM, nó chỉ có giá trị trên máy chứa thông tin tài khoản đó.

| Name                      | Description                                 | Actions |
|---------------------------|---------------------------------------------|---------|
| Access Control Assistance | Members of this group can remotely qu...    | Groups  |
| Administrators            | Administrators have complete and unres...   |         |
| Backup Operators          | Backup Operators can override security r... |         |
| Cryptographic Operators   | Members are authorized to perform cryp...   |         |
| Device Owners             | Members of this group can change syste...   |         |
| Distributed COM Users     | Members are allowed to launch, activate ... |         |
| Event Log Readers         | Members of this group can read event lo...  |         |
| Guests                    | Guests have the same access as member...    |         |
| Hyper-V Administrators    | Members of this group have complete a...    |         |
| IIS_IUSRS                 | Built-in group used by Internet Informat... |         |
| Network Configuration     | Members in this group can have some a...    |         |
| Performance Log Users     | Members of this group may schedule lo...    |         |
| Performance Monitor       | Members of this group can access perfor...  |         |
| Power Users               | Power Users are included for backwards c... |         |
| Remote Desktop Users      | Members in this group are granted the ri... |         |
| Remote Management         | Members of this group can access WMI r...   |         |
| Replicator                | Supports file replication in a domain       |         |
| System Managed Accounts   | Members of this group are managed by ...    |         |
| Users                     | Users are prevented from making accide...   |         |
| _vmware_                  | VMware User Group                           |         |

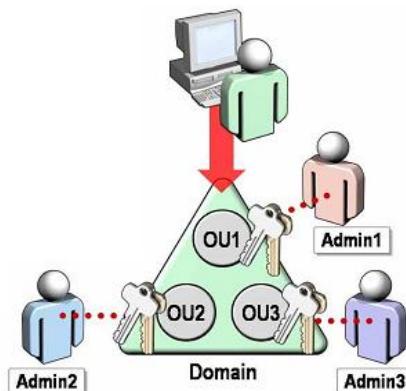
**Hình 6.16:** Các Group mặc định trên Domain

### 6.3.6.2. Quản lý User, Group và OU trên hệ thống mạng (Domain)

Sau khi xây dựng thành công máy chủ Domain Controller trên Windows Server bằng cách cài đặt dịch vụ ADDS, chúng ta sẽ tạo và quản lý các User, Group và OU trong hệ thống mạng Domain bằng công cụ Active Directory Users and Computers. Khác với các User và Groups cục bộ chỉ được dùng tài nguyên trong máy tính cục bộ, các User và Groups trong hệ thống mạng Domain có thể sử dụng các tài nguyên trên mạng tùy theo quyền được cấp. Các thông tin User, Group và OU sẽ được lưu trữ tại Server Domain.

- Organizational Unit (OU): Là một đối tượng trong Active Directory, nó chứa các đối tượng bên trong như User, Computer, Group và OU. Chức năng của OU:

- + Dùng ủy quyền quản trị (Delegation of Administration). Cho phép OU có quyền quản lý các đối tượng User, Group như chỉnh sửa thông tin, thêm, xóa các đối tượng trong OU này. Việc ủy quyền này sẽ giảm tải trách nhiệm của người quản trị chính Administrator.
- + Dùng áp dụng các chính sách (Group Policy). Group Policy sẽ được tự động áp dụng cho các đối tượng là User và Computer bên trong 1 OU. Một OU có thể được áp dụng nhiều Group Policy.



**Hình 6.17: Các Object trên Domain**

- Group: Là đối tượng của Active Directory. Các User thành viên của Group sẽ có quyền truy cập tài nguyên mà Group đó có được phân quyền truy cập. Thành viên của Group là User và Group. Group được chứa trong các OU.

Có hai kiểu Group là Security Groups và Distribution Groups.

- Security Groups: Được sử dụng để cấp quyền cho phép hoặc không cho phép truy cập.
- Distribution Groups: Dùng để phân phối E-mail (chủ yếu dùng cho Microsoft Exchange), đối với các User không cần truy cập tài nguyên hoặc Log-in máy tính sẽ được đưa vào kiểu Group này.
- + Phạm vi Group (Group Scopes) gồm có:
  - Domain Local: Có thể có thành viên là bất kỳ Domain nào trong Forest, có thể cấp quyền trong cùng Domain.
  - Global: Có thể có thành viên cùng Domain, có thể cầm quyền trong bất kỳ Domain nào trong Forest.

- Universal: Có thể có thành viên trong bất kỳ Domain nào trong Forest, có thể cấp quyền bất kỳ Domain hoặc Forest.
- User và Computer:

User là lớp cuối cùng trong kiến trúc của Active Directory. User có thể là thành viên của một hoặc nhiều Group và được thừa hưởng chính sách từ Group. User cũng được chứa trong các OU. User cũng là đối tượng chủ yếu được áp dụng các Group Policy. Computer cũng tương tự như User, chỉ khác đó là một máy tính cụ thể nào đó.

**Administrators:** Tài khoản có quyền cao nhất trong hệ thống Domain. Administrator có thể bị Disable nhưng vẫn có thể Log-in vào chế độ Safe Mode, vì vậy việc tạo Password của User này là rất quan trọng để bảo mật cho hệ thống.

Người dùng Administrator sẽ có quyền tạo User, Group, hoặc OU. Dùng: Start\Programs\Administrative Tools\Active Directory Users and Computers. Nhấp phải chuột trên mục Users\New: chọn User, Group, hoặc OU.

Khi tạo các đối tượng User, Group, hoặc OU cần khai báo các thông tin thuộc tính đầy đủ để thuận tiện trong quản lý. Các tác vụ khi quản lý các đối tượng như: chỉnh sửa, thêm, vô hiệu hóa (Disable), xóa.

### 6.3.6.3. Quản lý User Profile

User Profile là 1 tập hợp các File và các thiết lập về môi trường làm việc của người dùng. Hệ thống tạo hồ sơ người dùng vào lần đầu tiên người dùng đăng nhập vào máy tính. Tại các lần đăng nhập tiếp theo, hệ thống tải hồ sơ của người dùng, sau đó các thành phần hệ thống khác cấu hình môi trường của người dùng theo thông tin trong hồ sơ.

Các dạng Profile:

- **Local Profile:**

Hồ sơ người dùng cục bộ được tạo lần đầu tiên khi người dùng đăng nhập vào máy tính. Hồ sơ được lưu trữ trên đĩa cứng cục bộ của máy tính. Các thay đổi được thực hiện đối với hồ sơ người dùng cục bộ dành riêng cho người dùng và máy tính thực hiện các thay đổi.

- **Roaming Profile:**

Bản sao của hồ sơ cục bộ được sao chép vào và lưu trữ trên một chia sẻ máy chủ. Hồ sơ này được tải xuống bất kỳ máy tính nào mà người

dùng đăng nhập trên mạng. Các thay đổi được thực hiện đối với hồ sơ người dùng chuyển vùng được đồng bộ hóa với bản sao máy chủ của hồ sơ khi người dùng đăng xuất. Ưu điểm của việc chuyển vùng hồ sơ người dùng là người dùng không cần phải tạo hồ sơ trên mỗi máy tính mà họ sử dụng trong mạng.

- **Mandatory Profile:**

Hồ sơ người dùng bắt buộc là loại hồ sơ mà quản trị viên có thể sử dụng để chỉ định cài đặt cho người dùng. Chỉ quản trị viên hệ thống mới có thể thực hiện các thay đổi đối với hồ sơ người dùng bắt buộc. Các thay đổi do người dùng thực hiện đối với cài đặt trên màn hình sẽ bị mất khi người dùng đăng xuất.

- **Temporary Profile:**

Hồ sơ tạm thời được phát hành mỗi khi tình trạng lỗi ngăn hồ sơ của người dùng tái. Cấu hình tạm thời bị xóa vào cuối mỗi phiên và các thay đổi do người dùng thực hiện đối với cài đặt và tệp trên máy tính để bàn sẽ bị mất khi người dùng đăng xuất. Cấu hình tạm thời chỉ có sẵn trên máy tính chạy Windows 2000 trở lên.

## **6.4. Quản trị truy xuất dùng NTFS**

### **6.4.1. Giới thiệu**

NTFS - New Technology File System là hệ thống tập tin tiêu chuẩn của Windows NT, kể cả các phiên bản Windows 2000 trở về sau này. NTFS thay thế hệ thống tập tin FAT (File Allocation Table) vốn là hệ thống tập tin phổ biến cho các hệ điều hành Windows của Microsoft. NTFS có nhiều cải tiến hơn FAT như:

- **NTFS đáng tin cậy, thể hiện:**

- + NTFS dùng nhật ký File và thông tin kiểm tra để khôi phục tính toàn vẹn của hệ thống tệp khi máy tính được khởi động lại.
- + Nếu có lỗi vùng dữ liệu trên đĩa (Sector), NTFS sẽ tự động gán lại vùng Sector bị lỗi và phân bổ một vùng mới cho dữ liệu. Đồng thời, NTFS cũng đánh dấu vùng Sector nào không sử dụng được.

- **Bảo mật:**

- + Các tệp NTFS sử dụng hệ thống tệp mã hóa (EFS) để bảo mật các tệp và thư mục, nó có thể được mã hóa để sử dụng cho một hoặc nhiều người dùng.

- + NTFS cũng lưu trữ danh sách kiểm soát truy cập (ACL - Access Control List) với mọi tệp và thư mục trên phân vùng NTFS.
- **Cải tiến tăng trưởng bộ nhớ:**
  - + Sử dụng các cấu trúc dữ liệu tiên tiến để cải thiện hiệu suất
  - + NTFS hỗ trợ các tệp lớn hơn và số lượng tệp trên mỗi ổ đĩa lớn hơn FAT hoặc FAT32. Cụ thể, số lượng tập tin tối đa trong 1 phân vùng là  $4.294.967.295$  ( $2^{32} - 1$ ), dung lượng ổ đĩa tối đa là 16 EiB (Exbibyte, 1 EiB = 1.073.741.824 Gigabytes) trên thực tế là 256 TiB (Tebibyte, 1 TiB = 1.024 Gibabytes).
  - + Hỗ trợ nhiều quyền người dùng.

#### **6.4.2. Các quyền truy xuất NTFS**

Quyền truy xuất NTFS là hệ thống tập hợp các quyền cho phép hoặc không cho phép Group hay User truy cập vào các đối tượng chứa trên một phân vùng NTFS bao gồm các Folder và File.

Quyền NTFS có thể được định cấu hình trên các thư mục và tệp.

- 6 quyền cơ bản và 14 quyền đặc biệt cho các thư mục.
- 5 quyền cơ bản và 13 quyền đặc biệt cho tệp.

##### **6.4.2.1. Các quyền cơ bản trên hệ thống NTFS**

| Quyền truy cập       | Điễn giải                                                                                                                                                   |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Read                 | <ul style="list-style-type: none"> <li>- Xem nội dung thư mục và đọc tập tin</li> <li>- Xem thuộc tính thư mục và tập tin</li> </ul>                        |
| Read & Execute       | <ul style="list-style-type: none"> <li>- Read</li> <li>- Duyệt thư mục và chạy chương trình trong thư mục</li> </ul>                                        |
| List Folder Contents | <ul style="list-style-type: none"> <li>- Read</li> <li>- Duyệt thư mục và chạy chương trình trong thư mục</li> </ul>                                        |
| Write                | <ul style="list-style-type: none"> <li>- Thay đổi thuộc tính thư mục và tập tin</li> <li>- Tạo mới thư mục và tập tin</li> <li>- Ghi lên tập tin</li> </ul> |

|              |                                                                                                                                                          |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Modify       | <ul style="list-style-type: none"> <li>- Read &amp; Execute</li> <li>- Write</li> <li>- Xóa thư mục con và tập tin</li> </ul>                            |
| Full Control | <ul style="list-style-type: none"> <li>- Modify</li> <li>- Thay đổi quyền sở hữu trên thư mục và tập tin</li> <li>- Sở hữu thư mục và tập tin</li> </ul> |

#### 6.4.2.2. Các quyền đặc biệt trên hệ thống NTFS

Quyền đặc biệt chỉ được check khi tiến hành cấu hình thêm các quyền nhỏ trong Advanced Permissions để giúp người quản trị có thể phân quyền chi tiết hơn. Sau đây là mối quan hệ giữa quyền cơ bản và quyền đặc biệt:

| Permissions                 | Basic<br>Full<br>Control | Basic<br>Modify | Basic<br>Read &<br>Execute | Basic List<br>Folder<br>Contents | Basic<br>Read | Basic<br>Write |
|-----------------------------|--------------------------|-----------------|----------------------------|----------------------------------|---------------|----------------|
| Travers Folder/Execute File | x                        | x               | x                          | x                                |               |                |
| List Folder/Read Data       | x                        | x               | x                          | x                                | x             |                |
| Read Attributes             | x                        | x               | x                          | x                                | x             |                |
| Read Extended Attributes    | x                        | x               | x                          | x                                | x             |                |
| Create Files/Write Data     | x                        | x               |                            |                                  |               | x              |
| Create Folders/Append Data  | x                        | x               |                            |                                  |               | x              |
| Write Attributes            | x                        | x               |                            |                                  |               | x              |
| Write Extended Attributes   | x                        | x               |                            |                                  |               | x              |
| Delete Subfolders and Files | x                        |                 |                            |                                  |               |                |
| Delete                      | x                        | x               |                            |                                  |               |                |
| Read Permissions            | x                        | x               | x                          | x                                | x             | x              |
| Change Permissions          | x                        |                 |                            |                                  |               |                |
| Take Ownership              | x                        |                 |                            |                                  |               |                |
| Synchronize                 | x                        | x               | x                          | x                                | x             | x              |

### 6.4.3. Các quy tắc phân quyền NTFS

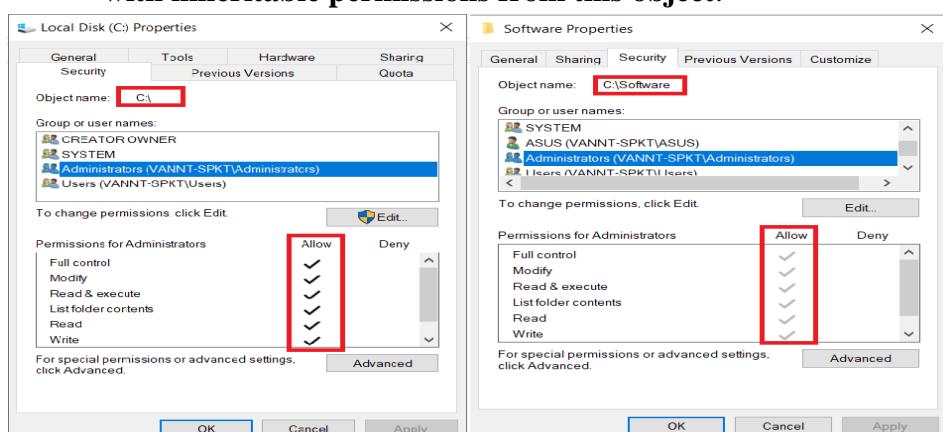
Khi thiết lập quyền truy xuất NTFS trên thư mục và File cần tuân thủ các quy tắc:

#### - Sự tích lũy quyền thừa kế:

- + Quyền thực sự của một User trên một thư mục hoặc tập tin là tổng quyền sở hữu mà User được gán với quyền sở hữu gán cho nhóm mà User thuộc về.
- + Ví dụ: Một User được gán quyền **Read** trên một thư mục, User cũng thuộc về một **nhóm** có quyền **Write** trên thư mục đó. Như vậy quyền của User trên thư mục sẽ là **Read và Write**.

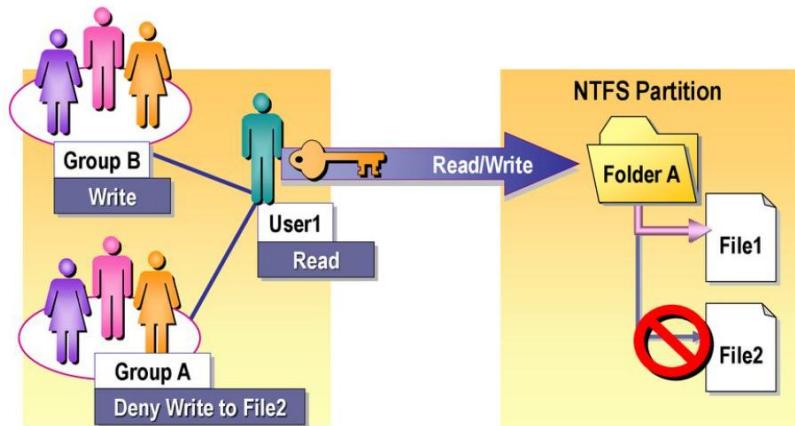
#### - Ké thừa:

- + Quyền sở hữu gán cho một thư mục được mang xuống (thừa kế) cho các thư mục con và tập tin chứa trong thư mục đó.
- + Tuy nhiên sự thừa kế này có thể điều chỉnh được. Các quyền NTFS kế thừa sẽ có dấu check bị mờ đi.
- + Ví dụ: Thư mục **Software** là thư mục nằm trong phân vùng ổ đĩa C, nó được kế thừa các quyền của ổ đĩa C; khi xem thuộc của thư mục **Software** có dấu check bị mờ - xem trong Properties của thư mục – hình,... Để có thể phân quyền lại, ta phải loại bỏ tính kế thừa (**Inheritance**) của thư mục cần phân quyền: click vào thư mục **Software**, chọn **Properties**, trong **Security Setting**, chọn **Advanced**, chọn lên dòng **Replace all child object permission with inheritable permissions from this object**.



Hình 6.18: Phân quyền truy cập

- **Ưu tiên:**
  - + Quyền sở hữu tập tin có độ ưu tiên cao hơn quyền sở hữu trên thư mục.
  - + Một User không có quyền truy xuất một thư mục vẫn có thể truy xuất tập tin chứa trong thư mục đó bằng cách sử dụng quy tắc viết tên UNC (Unique Name Convention) hoặc tên đường dẫn cục bộ để mở tập tin.
- **Phủ nhận quyền sở hữu:**
  - + Một quyền sở hữu của một User có thể bị ngăn chặn bằng cách phủ nhận (Deny) quyền đó.
  - + Ví dụ: User1 có quyền Read trên FolderA và là một thành viên của nhóm A và nhóm B. Nhóm A bị phủ nhận quyền Write trên File2, nhóm B có quyền Write trên thư mục FolderA. User có thể Read và Write trên File1, User cũng có thể Read File2 nhưng không thể Write trên File2 vì User thuộc về nhóm A, nhóm này bị phủ nhận quyền Write trên File2.



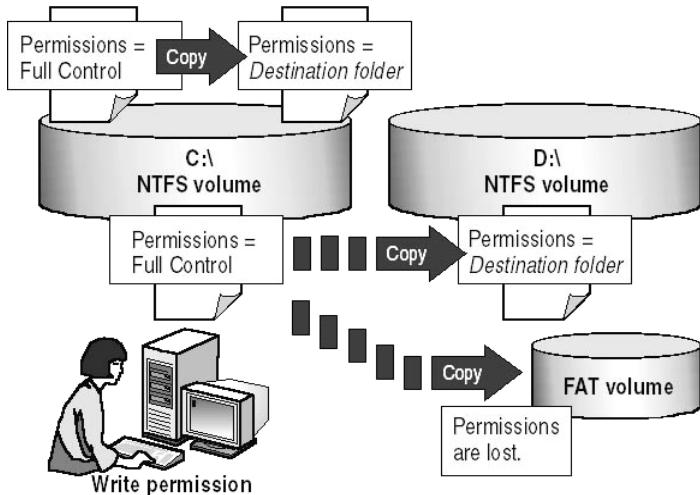
**Hình 6.19: Phủ nhận quyền truy cập dữ liệu**

- **Di chuyển/sao chép thư mục/tập tin**

Khi sao chép thư mục hoặc tập tin từ thư mục này sang thư mục khác hoặc từ Volume này sang Volume khác (sử dụng hệ thống tập tin NTFS), cần lưu ý một số đặc điểm sau:

- + Thư mục/tập tin sẽ mang quyền sở hữu của thư mục đích.
- + Người sao chép phải có quyền Write.

- + Người sao chép sẽ trở thành CREATOR.
- + Khi sao chép thư mục hoặc tập tin sang Volume sử dụng FAT, các quyền sở hữu sẽ không còn hiệu lực vì hệ thống tập tin FAT không có tính bảo mật.



**Hình 6.20: Quyền truy cập khi Copy dữ liệu**

Khi di chuyển thư mục/tập tin, quyền sở hữu có thể thay đổi hoặc không thay đổi tùy thuộc vào thư mục đích nằm ở đâu.

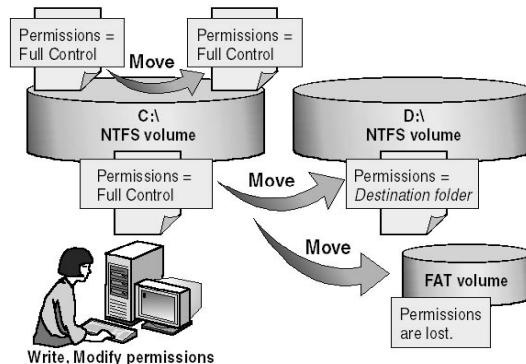
Trường hợp di chuyển trên cùng Volume NTFS:

- Người thực hiện lệnh di chuyển phải có quyền Write trên thư mục đích.
- Người thực hiện lệnh di chuyển phải có quyền Modify trên thư mục nguồn vì nguồn sẽ được xóa sau khi di chuyển.
- Người sở hữu trên thư mục/tập tin không thay đổi.

Trường hợp di chuyển sang Volume NTFS khác:

- Tập tin/thư mục sẽ thừa kế quyền sở hữu trên thư mục đích.
- Người thực hiện lệnh di chuyển phải có quyền Write trên thư mục đích.
- Người thực hiện lệnh di chuyển phải có quyền Modify trên thư mục nguồn vì nguồn sẽ được xóa sau khi di chuyển.
- Người thực hiện lệnh di chuyển sẽ trở thành CREATOR OWNER của thư mục/tập tin.

Trường hợp di chuyển thư mục hoặc tập tin sang Volume sử dụng FAT, các quyền sở hữu sẽ không còn hiệu lực vì hệ thống tập tin FAT không có tính bảo mật.

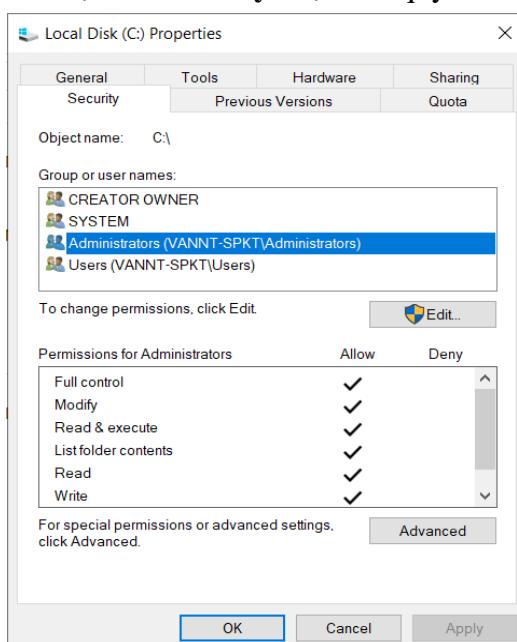


**Hình 6.21:** Quyền truy cập khi di chuyển dữ liệu

- Gán/thay đổi quyền:

Để gán hoặc điều chỉnh quyền sở hữu trên thư mục hoặc tập tin, thực hiện như sau:

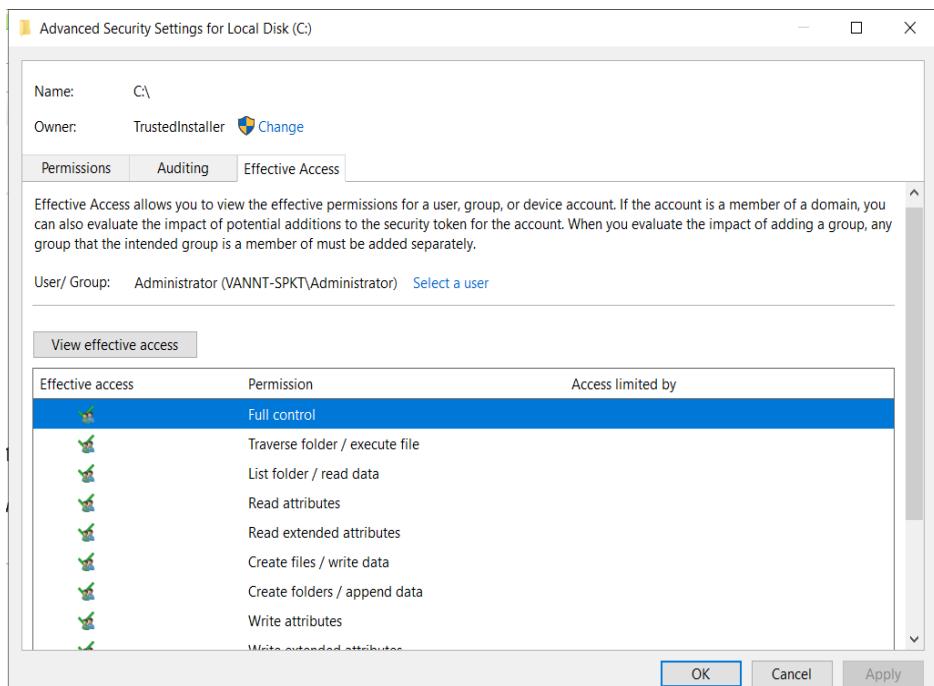
Tại thư mục/tập tin muốn gán hoặc điều chỉnh quyền sở hữu, chọn Properties, click tại thẻ **Security** chọn các quyền muốn thiết lập.



**Hình 6.22:** Cấu hình thay đổi quyền truy cập

- Quyền có hiệu lực:

Đây là kết quả của các quyền được chỉ định trực tiếp cho tệp hoặc thư mục và quyền được thừa kế từ các thư mục mẹ. Để xem các quyền hiệu lực, trong hộp **Advanced Security Settings**, click **Effective Permissions**, chọn người dùng hoặc nhóm, sau đó click **View Effective Access**:



**Hình 6.23:** Một số chức năng cấu hình phân quyền nâng cao

## 6.5. Chia sẻ dữ liệu trên mạng

### 6.5.1. Đặc điểm của chia sẻ dữ liệu

Chia sẻ dữ liệu (Share) là một trong những công việc chủ yếu khi quản trị một hệ thống mạng. Khi dữ liệu được chia sẻ sẽ cho phép nhiều người dùng cùng một lúc qua mạng. Người dùng có thể truy cập vào một tập tin và thư mục con trong thư mục chia sẻ nếu họ được cấp giấy phép.

Chia sẻ dữ liệu có các đặc điểm sau:

- Chỉ áp dụng cho thư mục, không áp dụng cho tập tin.
- Chỉ áp dụng cho những User từ máy khác truy xuất vào thư mục, không áp dụng cho User cục bộ trên máy chứa thư mục chia sẻ.

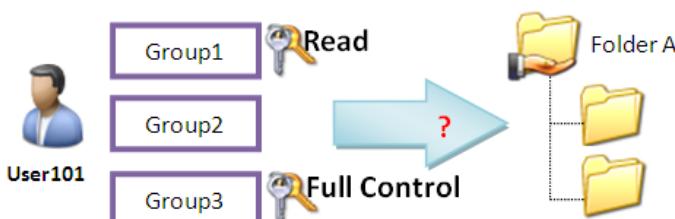
- Là cách duy nhất để bảo vệ dữ liệu chia sẻ trên Volume FAT vì các quyền bảo mật NTFS không có tác dụng trên Volume FAT.
- Khi một thư mục được chia sẻ, quyền mặc định trên thư mục là Read gán cho nhóm Everyone.
- Chia sẻ thư mục có thể thực hiện trong một nhóm mạng Workgroup hoặc trong một Domain.

Các quyền trên thư mục chia sẻ:

|                     |                                                                                                                                                                                                                  |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Read</b>         | <ul style="list-style-type: none"> <li>- Xem thư mục.</li> <li>- Đọc nội dung tập tin.</li> <li>- Xem thuộc tính thư mục tập tin.</li> <li>- Thực thi chương trình.</li> </ul>                                   |
| <b>Change</b>       | <ul style="list-style-type: none"> <li>- Có quyền <b>Read</b>.</li> <li>- Tạo thư mục, tập tin.</li> <li>- Sửa đổi nội dung tập tin.</li> <li>- Thay đổi thuộc tính.</li> <li>- Xóa thư mục, tập tin.</li> </ul> |
| <b>Full Control</b> | <ul style="list-style-type: none"> <li>- Có quyền <b>Read</b> và <b>Change</b>.</li> <li>- Gán, rút quyền sở hữu.</li> <li>- Sở hữu tập tin.</li> </ul>                                                          |

#### 6.5.2. Các quy tắc khi chia sẻ thư mục

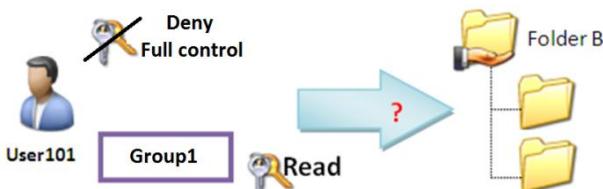
- **Quyền thực sự trên thư mục chia sẻ:**
  - + Là kết hợp của quyền được gán và quyền sở hữu gán cho nhóm.
  - + Ví dụ User có quyền **Read** thuộc về nhóm Group3 có quyền **Full Control** thì quyền thực sự của User sẽ là **Full Control** - quyền này bao hàm quyền **Read** của Group2.



Hình 6.24: Quyền trên thư mục chia sẻ

## - Phủ nhận quyền:

- + Việc phủ nhận một quyền làm mất tác dụng của quyền đã gán cho User hoặc nhóm User. Nếu một User bị phủ nhận quyền sở hữu trên một thư mục chia sẻ, User sẽ không có khả năng truy xuất thư mục mặc dù User thuộc về nhóm đã được gán quyền trên thư mục chia sẻ.
- + Ví dụ: User101 thuộc về nhóm Group1, nhóm này được gán quyền Read trên thư mục FolderB. Tuy nhiên User101 bị phủ nhận quyền Full Control trên FolderB, vậy User101 không có quyền gì trên FolderB.



**Hình 6.25: Phủ nhận quyền trên thư mục chia sẻ**

## - Chia sẻ thư mục có quyền NTFS:

- + Khi sao chép một thư mục sử dụng thêm quyền NTFS để việc kiểm soát dữ liệu thư mục chia sẻ, thư mục nguồn vẫn còn chia sẻ nhưng thư mục đích thì không.
- + Đối với các thư mục chia sẻ nằm trên Volume FAT, quyền trên thư mục chia sẻ là cách duy nhất để bảo vệ dữ liệu. Tuy nhiên, đối với các thư mục chia sẻ nằm trên Volume NTFS thì được gán quyền đầy đủ hơn.

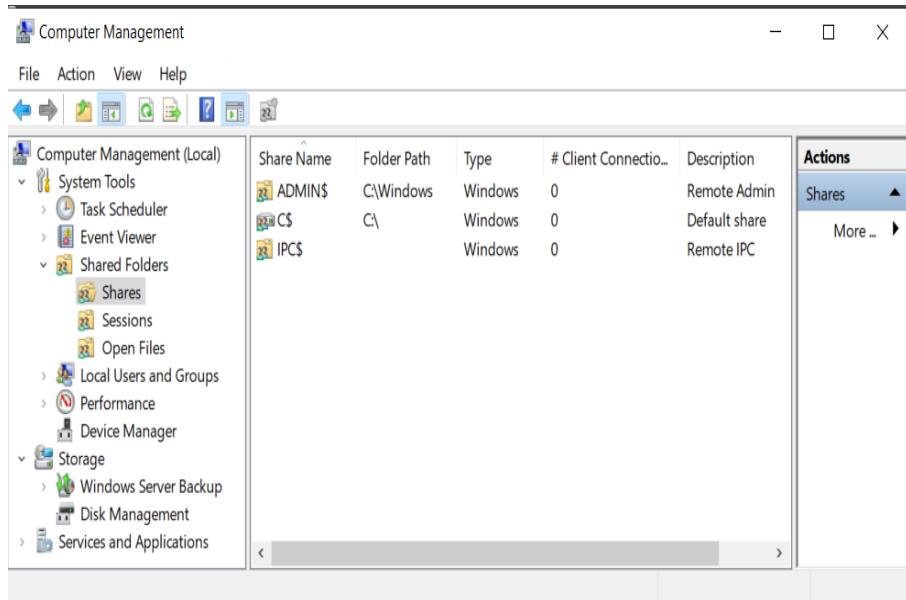
## - Gán/thay đổi quyền:

- + Gán quyền chia sẻ cho nhóm thay vì gán cho từng User.
- + Gán quyền chia sẻ một cách chặt chẽ nhất nhưng vẫn đảm bảo cho User có thể thực hiện được các tác vụ cần thiết của mình. Ví dụ nếu User chỉ cần đọc, không bao giờ xóa hoặc tạo tập tin trên một thư mục thì chỉ cần gán quyền Read trên thư mục đó.
- + Nên tổ chức dữ liệu sao cho các thư mục sẽ có cùng quyền sở hữu chung trong cùng một thư mục. Ví dụ nếu User cần chạy một số ứng dụng nào đó thì nên chứa thư mục của các ứng dụng đó trong cùng một thư mục.

- + Nên sử dụng tên chia sẻ gợi nhớ giúp User dễ dàng định vị và nhận dạng dữ liệu chia sẻ.

### 6.5.3. Thư mục chia sẻ mặc định

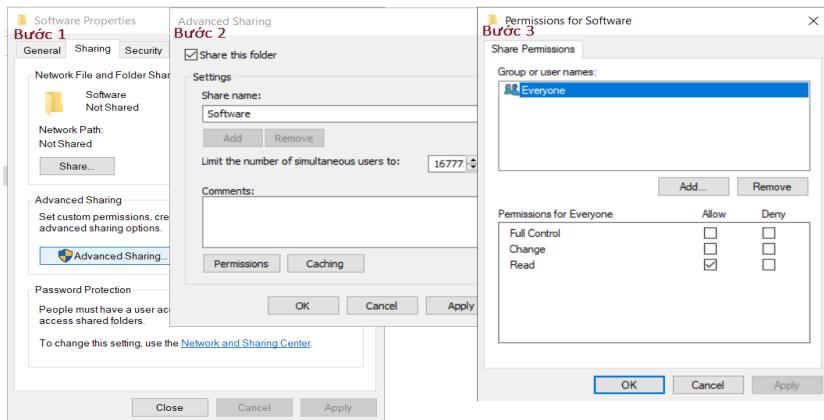
Các thư mục được chia sẻ mặc định gồm thư mục gốc của mỗi Volume, thư mục gốc hệ thống và thư mục chứa chương trình điều khiển máy in. Để xem các thư mục chia sẻ này, vào Computer Management, click Shared Folders, click Shares.



**Hình 6.26:** Các thư mục chia sẻ mặc định

### 6.5.4. Thực hiện chia sẻ thư mục

- Các thông tin cần khai báo khi chia sẻ:
  - + Tên chia sẻ: Share Name.
  - + Số User truy xuất vào thư mục chia sẻ: Limit the number of simultaneous users to.
  - + Quyền: Permissions.
- Các bước thực hiện chia sẻ:
  - + Chọn thư mục, click Properties, click Network and Sharing Center.
  - + Nhập tên chia sẻ và số User.
  - + Click Permissions để gán quyền.



**Hình 6.27:** Chia sẻ thư mục và gán quyền truy cập

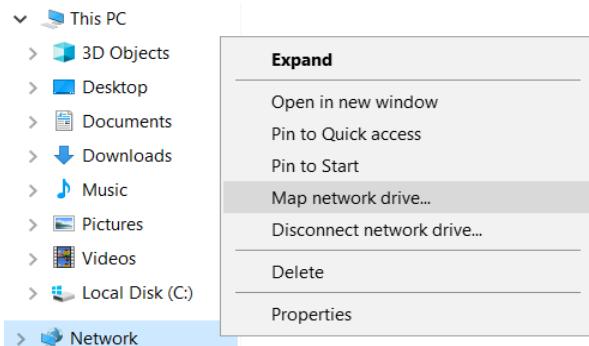
- Share ẩn và Share công khai:

- + Để Share ẩn người ta thêm dấu \$ phía sau cùng của Share Name. Với Share ẩn, User cần biết chính xác tên của thư mục Share là gì và điền chính xác tên đó cùng với dấu \$ phía sau cùng thì mới có thể truy cập được.
- + Đối với Share công khai, người dùng không cần phải gõ chính xác địa chỉ và tên thư mục Share, người dùng chỉ cần truy cập vào địa chỉ IP hoặc tên máy thực hiện Share dữ liệu là được.

#### 6.5.5. Truy xuất dữ liệu chia sẻ

Có 3 phương pháp thường sử dụng để sử dụng dữ liệu chia sẻ:

- Thông qua biểu tượng My Network Places.
- Định nghĩa ánh xạ ổ đĩa:



**Hình 6.28:** Ánh xạ ổ đĩa mạng

- Sử dụng tiện ích dòng lệnh Net use: net use <đĩa> <Tên UNC> rồi bấm Enter (UNC: Universal Naming Convention).

Ví dụ: Để chia sẻ thư mục My Document với Share Name là My\_Docs, nhập lệnh như sau tại dòng lệnh rồi bấm Enter:

```
C:\> net use k: \\servername\My_Docs
```

#### 6.5.6. Kiểm soát dữ liệu chia sẻ

Quản lý các thư mục chia sẻ cho phép người quản trị mạng có cái nhìn đầy đủ về các thư mục đã chia sẻ trên mạng, tránh tình trạng chia sẻ những thư mục không cần thiết.

Để xem danh sách các thư mục chia sẻ có thể thực hiện bằng các cách sau:

- Sử dụng tiện ích dòng lệnh Net Share:

```
Command Prompt
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\ASUS>net share

Share name   Resource           Remark
-----       -----             -----
C$           C:\                Default share
IPC$          Remote IPC
ADMIN$        C:\Windows        Remote Admin
The command completed successfully.
```

**Hình 6.29: Kiểm tra các thư mục chia sẻ trên máy tính**

- Sử dụng cửa sổ Computer Management: vào Computer Management, click Shared Folders, click Shares.

#### 6.6. Kết hợp quyền thư mục được chia sẻ và quyền NTFS

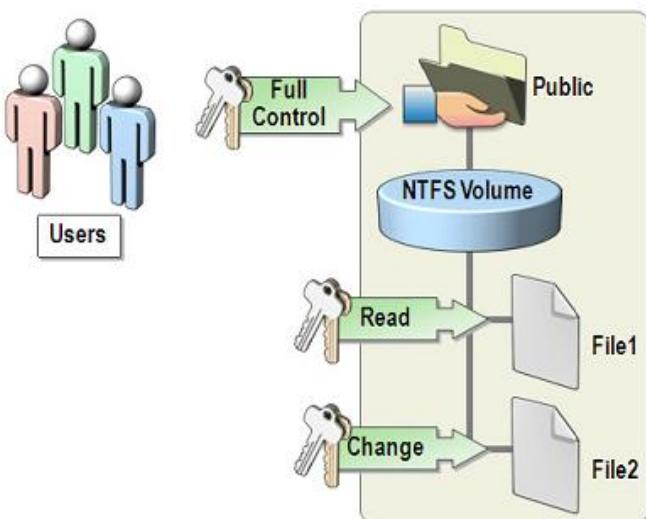
Khi bạn sử dụng quyền đối với thư mục chia sẻ trên ổ đĩa NTFS, các quy tắc sau sẽ được áp dụng:

- Có thể áp dụng quyền NTFS cho các tệp và thư mục con trong thư mục chia sẻ.
- Có thể áp dụng các quyền NTFS khác nhau cho từng tệp và thư mục con chứa bên trong một thư mục chia sẻ.
- Ngoài quyền trên thư mục chia sẻ, User cần được kiểm soát quyền truy xuất bằng quyền NTFS trên tập tin và thư mục con

trong thư mục chia sẻ. Điều này khác với việc chia sẻ một thư mục trên Volume FAT, quyền chia sẻ là quyền cơ chế bảo mật duy nhất.

- Khi kết hợp quyền trên thư mục chia sẻ với quyền NTFS, quyền thực sự sẽ là quyền chặt chẽ (hạn chế) hơn trong hai loại quyền.

Ví dụ: Nhóm Everyone có quyền **Full Control** trên thư mục chia sẻ Public và quyền NTFS là Read trên tập tin FileA. Như vậy quyền thực sự của nhóm Everyone trên tập tin FileA là **Read**, còn quyền thực sự của nhóm Everyone trên tập tin FileB là **Change**.



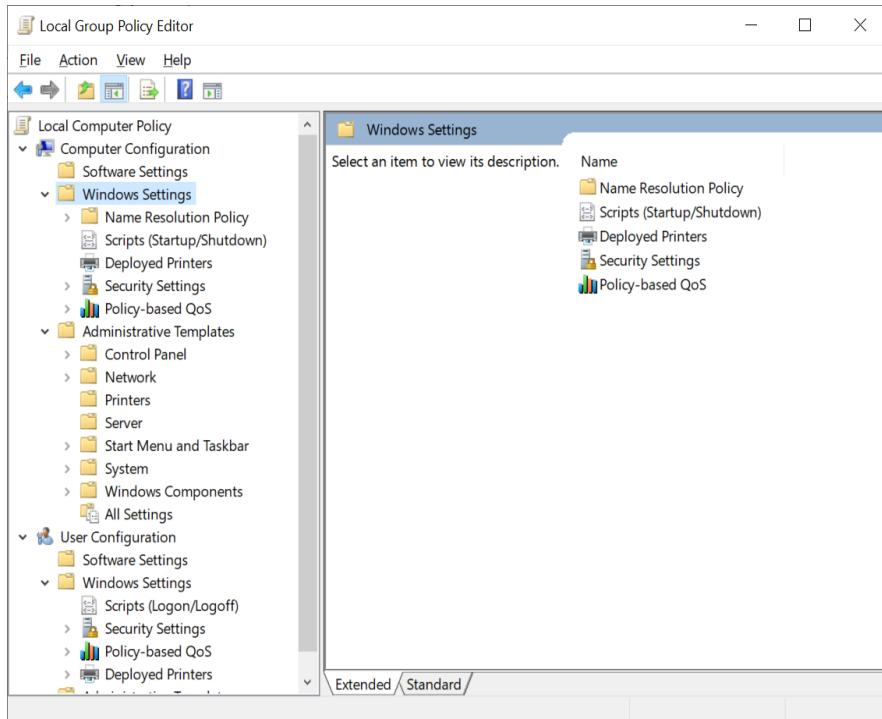
**Hình 6.30:** Kết hợp quyền NTFS và quyền chia sẻ

## 6.7. Thiết lập các chính sách quản trị (GPO)

Group Policy là tập hợp các thiết lập cấu hình cho Computer và Users, xác định cách thức để các chương trình, tài nguyên mạng và hệ điều hành làm việc với người dùng và máy tính trong 1 tổ chức. Group Policy sẽ giúp việc quản lý người dùng chặt chẽ và hiệu quả hơn.

Group Policy có thể triển khai ở 2 dạng:

- Tại máy tính cục bộ - dùng Local Group Policy Editor trong Control Panel\All Control Panel Items\Administrative Tools để thiết lập các chính sách về Computer và Users gồm các mục: phần mềm, Windows, quản trị.



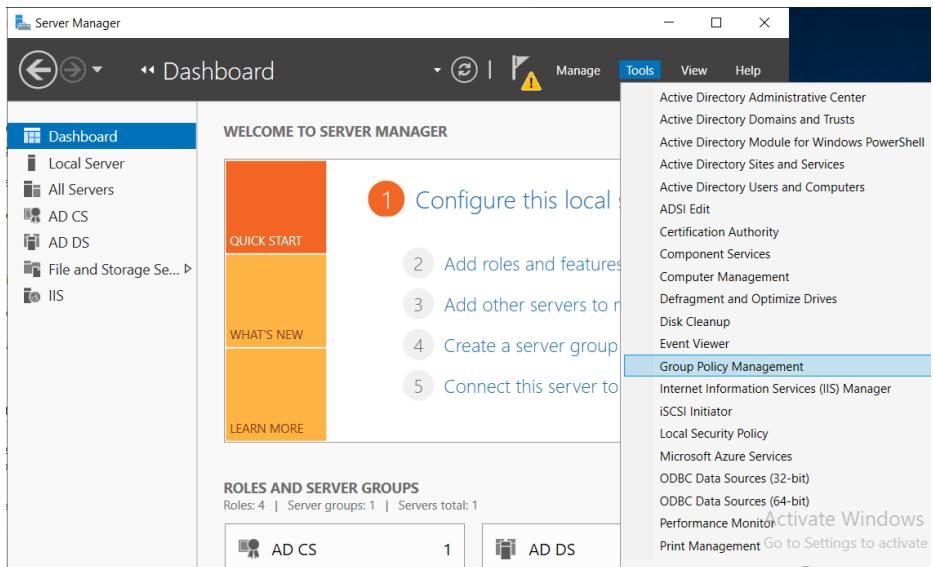
**Hình 6.31: Giao diện cấu hình các chính sách quản trị (GPO)**

- Trong Domain: Các Group Policy được áp dụng cho các Site, Domain và OU (Organizational Unit). Các Group Policy áp dụng cho các đối tượng gọi là Group Policy Object (GPO).

Các đặc điểm của GPO:

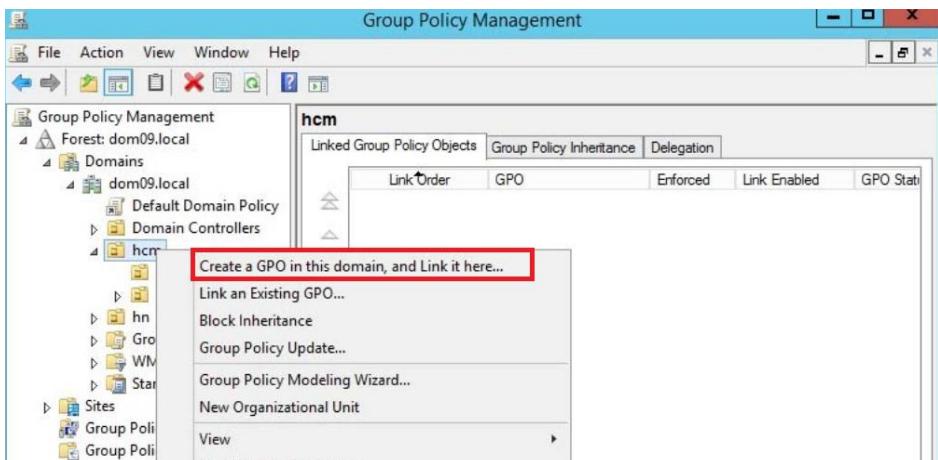
- + Các GPO được lưu trữ một phần trong cơ sở dữ liệu của AD và một phần trong Share SYSVOL. Mục đích sử dụng GPO trong Domain là nhằm triển khai các chính sách từ miền máy chủ Domain Controller xuống Users.
- + GPO có tính kế thừa: Các OU con tự động liên kết và áp dụng các GPO đã được tạo ra trong các OU cha, đây là thuộc tính mặc định của OU. Có thể ngăn chặn tính kế thừa trong Group Policy: “Block Policy Inheritance”.
- + Chương trình để tạo ra và chỉnh sửa GPO có tên là Group Policy Object Editor (đây là 1 dạng Console tên là gpedit.msc, Console của Active Directory Users and Computers là dsa.msc).

Cáu hình GPO: Chọn Server Manager\Tool, chọn Group Policy Management:



**Hình 6.32:** Giao diện chọn chức năng cấu hình GPO

Sau đó, chúng ta sẽ tạo GPO cho các OU trong Domain. Ví dụ:



**Hình 6.33:** Tạo mới một GPO

Các Group Policy thông dụng:

- Triển khai phần mềm cho một hoặc nhiều máy trạm nào đó một cách tự động.
- Án định quyền hạn cho một số người dùng mạng.

- Giới hạn những ứng dụng mà người dùng được phép chạy.
- Kiểm soát hạn ngạch sử dụng đĩa trên các máy trạm.
- Thiết lập các kịch bản (Script) đăng nhập (Log-on), đăng xuất (Log-out), khởi động (Start-up), và tắt máy (Shut-down).
- Chuyển hướng (Redirector) một số Folder trên máy khách (như Computer, My Document) lên DC,...

## 6.8. Tổng kết chương

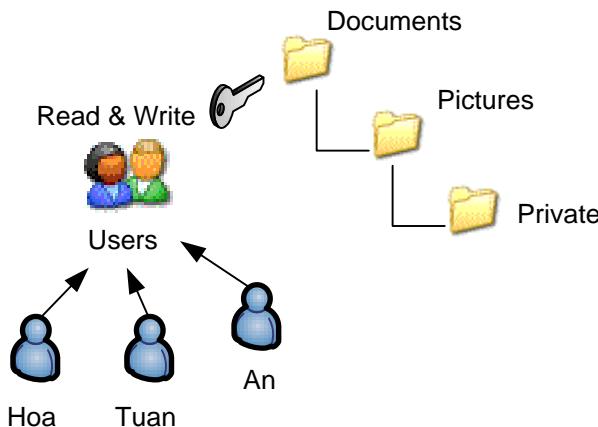
Các kiến thức về mô hình mạng Workgroup và Domain được mô tả đầy đủ với các thành phần, kiến trúc và các dịch vụ triển khai. Mô hình Domain được sử dụng quản lý người dùng và tài nguyên hiệu quả với các hỗ trợ về chia sẻ thư mục, gán quyền truy xuất NTFS và thiết lập các chính sách nhóm.

## 6.9. Câu hỏi và bài tập

1. Máy hoạt động trong mô hình Workgroup được gọi là?
  - A. Server.
  - B. Client.
  - C. Peer To Peer.
  - D. Workstation.
2. Mô hình Workgroup sử dụng User đăng nhập là?
  - A. Domain User.
  - B. Local User.
  - C. Anonymous.
  - D. Bất kỳ loại User nào.
3. Thành phần nào **không** thuộc kiến trúc logic của Active Directory?
  - A. Domain.
  - B. Domain Controller.
  - C. Object.
  - D. Organizational Units (OU).
4. Thành phần nào thuộc kiến trúc vật lý của Active Directory?
  - A. Domain.
  - B. Domain Controller.
  - C. Object.
  - D. Organizational Units (OU).

5. Organizational Units (OU) có thể chứa gì?
- A. Domain.
  - B. Domain Controller.
  - C. Object.
  - D. Forest.
6. Dịch vụ nào sẽ lưu trữ thông tin về các đối tượng trong Domain?
- A. Active Directory Domain Services (ADDS).
  - B. Active Directory Lightweight Directory Services (ADLDS).
  - C. Active Directory Federation Services (ADFS).
  - D. Active Directory Rights Management Services (ADRMS).
7. Khi Roaming Profile cho User đến máy DC1, lưu trong thư mục đã chia sẻ Homedir. Câu lệnh là?
- A. \\DC1\Homedir\Username.
  - B. \\DC1\Homedir%\Username%.
  - C. \\DC1\Homedir%\User%.
  - D. \\DC1\Homedir\User.
8. Máy chủ DC là?
- A. Máy chủ quản lý miền.
  - B. Máy chủ quản lý User và Computer.
  - C. Máy chủ các tài nguyên trong mạng công ty.
  - D. Máy chủ cung cấp các dịch vụ và quản lý toàn bộ mạng.
9. Để truy cập thư mục Data được Share ẩn trên PC01, sử dụng lệnh?
- A. \\PC01\Data\$.
  - B. \\Data\$.
  - C. \\PC01/Data.
  - D. \\Data.
10. User U1 phân quyền NTFS bị cấm truy xuất tới thư mục Data, biết thư mục Data được chia sẻ cho nhóm Everyone với quyền Read, lúc này U1 có quyền?
- A. U1 không thể truy xuất thư mục chia sẻ Data.
  - B. U1 có thể đọc dữ liệu trong thư mục Data.
  - C. U1 có thể truy xuất thư mục chia sẻ Data, nhưng chỉ có quyền đọc.

- D. U1 có toàn quyền truy xuất thư mục chia sẻ Data.
11. User U1 thuộc 2 Group G1 và G2, G1 có quyền List, Read, Read & Execute trên thư mục Data, G2 bị cấm quyền truy xuất thư mục Data. Quyền của U1 là?
- A. U1 chỉ có thể xem nội dung thư mục Data, nhưng không mở được các File trên thư mục này.
  - B. U1 không có quyền truy xuất thư mục Data.
  - C. U1 có thể đọc và thực thi các tập tin chương trình đặt trong thư mục Data.
  - D. U1 có quyền truy xuất thư mục Data.
12. Nhóm Users gồm các User Hoa, Tuan, An có quyền Read & Write trên thư mục Documents.
- + Các User Hoa, Tuan, An có quyền gì trên thư mục Pictures?
  - + Muốn cho An có quyền Read trên thư mục Private còn các User Hoa và Tuan không có quyền gì cả thì phải làm gì?



13. Trong môi trường Microsoft, mô hình nào có các thông tin người dùng được lưu trữ trung và người dùng phải chứng thực khi đăng nhập vào mạng:
- A. Server.
  - B. Client.
  - C. Domain.
  - D. Workgroup.

14. Jery vừa thuộc nhóm Marketing và nhóm Accounting, User Jery có quyền Read thư mục D:\Data. Trong khi đó, nhóm Marketing có quyền Write thư mục D:\Data, nhưng nhóm Accounting bị cấm quyền Write File D:\Data\vb2.txt. Vậy Jery có quyền gì trên File vb2.txt?
- A. Read.
  - B. Read & Write.
  - C. Write.
  - D. Không có quyền gì.
15. Quyền nào là quyền đặc biệt trên NTFS?
- A. Take Ownership.
  - B. Execute.
  - C. Write.
  - D. Modify.
16. Quyền nào là quyền cơ bản trên NTFS?
- A. Take Ownership.
  - B. Delete.
  - C. Synchronize.
  - D. Modify.
17. Trong Windows, User Profile là nơi?
- A. Lưu tất cả các thông tin liên quan đến User (Desktop, Start Menu,...).
  - B. Là thư mục gốc của User khi đăng nhập.
  - C. Là nơi lưu tất cả các thuộc tính của User.
  - D. Các User khác có thể đọc thư mục này.
18. Máy PC01 chia sẻ thư mục Shared với tên là Shared\_PC01, máy trong LAN có thể truy cập trực tiếp thư mục này bằng lệnh?
- A. \\PC01\Shared.
  - B. \\PC01.
  - C. \\PC01\shared\_pc01.
  - D. \\PC01\SharedShared\_PC01.

19. Để Share ảnh một thư mục, ta thêm?
- A. Chữ & vào sau tên chia sẻ.
  - B. Chữ & vào trước tên chia sẻ.
  - C. Chữ \$ vào sau tên chia sẻ.
20. Chữ \$ vào trước tên chia sẻ. Quyền Change trên thư mục chia sẻ không được làm gì?
- A. Gán, rút quyền sở hữu.
  - B. Tạo thư mục, tập tin.
  - C. Thay đổi thuộc tính.

## CHƯƠNG 7

# XÓA THƯ MỤC, TẬP TIN. AN NINH MẠNG

Chương này sẽ đề cập đến một số khái niệm về an ninh mạng, phân loại các lỗ hổng bảo mật. Học xong chương này, người học có khả năng:

- Trình bày được một số khái niệm cơ bản về lĩnh vực an ninh mạng.
- Trình bày được một số đặc điểm cơ bản của các loại lỗ hổng bảo mật.
- Trình bày được các bước cơ bản của quá trình tấn công xâm nhập, khai thác lỗ hổng.
- Trình bày được các cách phòng chống, hạn chế hậu quả trong an toàn thông tin.
- Trình bày được vai trò của hệ thống giám sát mạng.
- Trình bày được những đặc điểm quan trọng của hệ thống giám sát.
- Cài đặt được một tấn công đơn giản.

### 7.1. Giới thiệu

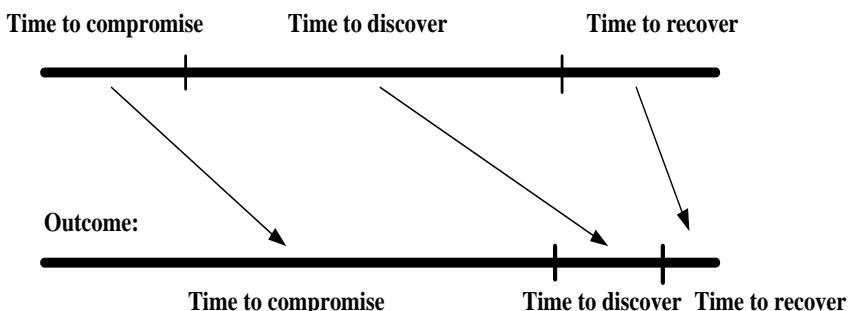
Trong thời đại công nghệ thông tin ngày nay, đặc biệt là công nghệ mạng phát triển cực kỳ mau lẹ, từ đó phát sinh vấn đề an toàn thông tin là một thách thức rất lớn bao trùm hầu hết từ phần cứng đến phần mềm và cả vai trò của người sử dụng. Ba mục tiêu chính trong an toàn thông tin, được biết đến với tên gọi là mô hình CIA (Confidentiality, Integrity, Availability), cần được đảm bảo là: tính bí mật, tính toàn vẹn và tính sẵn sàng. Bất kỳ sự vi phạm nào trong ba tính chất trên đều dẫn đến nguy cơ mất an toàn thông tin.

- Tính bí mật: Đảm bảo rằng chỉ những người dùng hợp pháp mới có thể truy cập được hệ thống, dữ liệu.
- Tính toàn vẹn: Đảm bảo rằng dữ liệu không bị thay đổi bởi những người không được phép.

- Tính sẵn sàng: Đảm bảo rằng dữ liệu, hệ thống có thể phục vụ được việc truy cập của người dùng hợp pháp.

Để đảm bảo an toàn tuyệt đối cho một hệ thống CNTT là một việc khó bởi các điểm yếu, mối đe dọa, rủi ro tồn tại ở rất nhiều thành phần trong một hệ thống CNTT. Có thể chia vấn đề bảo mật ra làm 3 giai đoạn:

- Time to compromise: Thời gian để xâm nhập vào một hệ thống.
- Time to discover: Thời gian phát hiện xâm nhập.
- Time to recover: Thời gian khôi phục hệ thống.



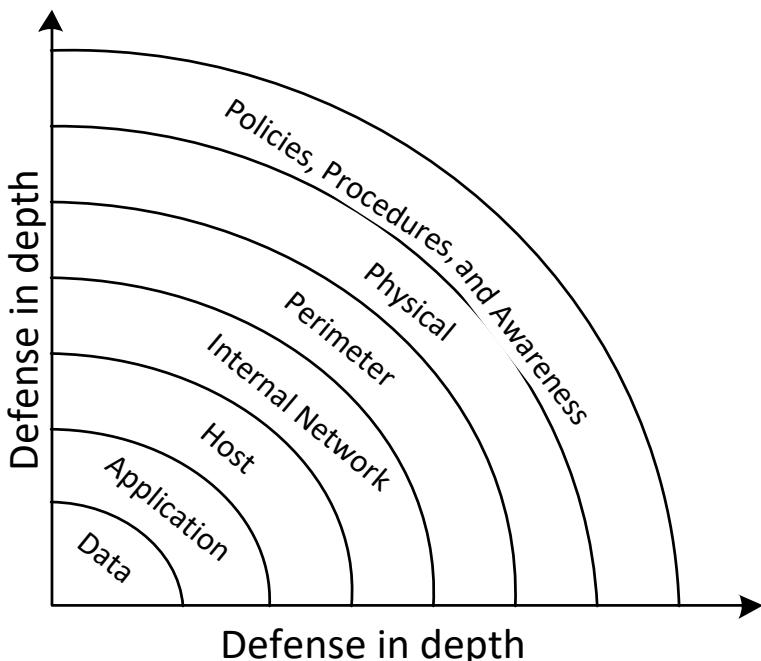
**Hình 7.1: Ba giai đoạn trong bảo vệ hệ thống**

Như vậy, đứng về phương diện người làm an ninh mạng thì mục tiêu quan trọng để bảo mật cho một hệ thống CNTT là làm sao để:

- + Tăng thời gian Time To Compromise, nghĩa là sử dụng các giải pháp để làm khó kẻ tấn công, làm cho chúng mất rất nhiều thời gian mới có thể tìm ra các điểm yếu bảo mật và xâm nhập vào hệ thống.
- + Giảm thời gian Time To Discover, nghĩa là sử dụng các giải pháp để nhận diện sớm các bất thường, nhận diện sớm hệ thống đang bị tấn công.
- + Giảm thời gian Time To Recovery, nghĩa là sử dụng các giải pháp để phòng khi hệ thống bị tấn công thì vẫn có khả năng khôi phục lại hiện trạng như trước khi bị tấn công.

Xây dựng hệ thống bảo mật nhiều lớp (hay bảo mật theo chiều sâu - Defense In Depth):

Như đã đề cập ở trên, các điểm yếu bảo mật tồn tại trong từng phần cấu thành nên hệ thống CNTT. Do đó, để có thể thực hiện các biện pháp phòng chống có hiệu quả, giải pháp bảo mật nhiều lớp nên được xem xét áp dụng để việc bảo mật toàn diện có hiệu quả. Hệ thống bảo mật nhiều lớp còn có tên gọi khác là bảo vệ theo chiều sâu (Defense In Depth).



**Hình 7.2: Bảo mật theo chiều sâu**

Vấn đề bảo mật ngày càng quan trọng cho các tổ chức, doanh nghiệp. Để không ngừng nâng cao năng lực bảo mật cho hệ thống CNTT, các tổ chức nên chú ý phát triển 3 yếu tố quan trọng, viết tắt là P-P-T, đó là: Con người - Quy trình - Công nghệ. Nâng cao khả năng quản trị bảo mật cho hệ thống với: chính sách an toàn thông tin, hệ thống ghi nhận sự kiện ATTT và đào tạo nâng cao nhận thức.

Một nguyên tắc quan trọng khác khi làm về an ninh mạng là “nguyên tắc quyền tối thiểu”, nghĩa là chỉ cung cấp các quyền cần thiết nhất đủ cho người dùng các chương trình hay tiến trình thực hiện các tác vụ của mình. Đi kèm với nguyên tắc này, một thuật ngữ được sử dụng nhiều trong vấn đề an ninh mạng là “Hardening”. Ý nghĩa của nó là các cổng trên thiết bị phần cứng, các ứng dụng, các dịch vụ,... nào không cần

sử dụng thì phải tắt đi hay xóa đi. Điều này giúp làm giảm các nguy cơ phát sinh tấn công hệ thống.

Trong lĩnh vực rộng lớn của an toàn thông tin, trong chương này chúng ta chỉ tập trung vào một số vấn đề cơ bản của an ninh mạng. Trong đó đề cập đến các loại lỗ hổng trong mạng, cách khai thác và phòng chống ở các mức độ khác nhau.

## 7.2. Phân loại lỗ hổng mạng

Hiểu được những điểm yếu trong bảo mật là một vấn đề hết sức quan trọng để tiến hành những chính sách bảo mật có hiệu quả. Những điểm yếu trong bảo mật mạng có thể được phân thành 3 loại như sau:

- Điểm yếu về mặt kỹ thuật:

Điểm yếu trong kỹ thuật gồm có điểm yếu trong giao thức, trong các hệ điều hành và các thiết bị phần cứng.

- Điểm yếu trong cấu hình hệ thống:

Đây là lỗi do người quản trị tạo ra. Lỗi này do các thiếu sót trong việc cấu hình hệ thống như: sử dụng các cấu hình mặc định, Password đơn giản,...

- Điểm yếu trong chính sách bảo mật:

Chính sách bảo mật diễn tả cách thức, quy định và vị trí thực hiện. Đây là điều kiện quan trọng giúp việc bảo mật có hiệu quả tốt nhất. Mỗi công ty, tổ chức nên xây dựng chính sách bảo mật đặc thù cho đơn vị mình.

## 7.3. Các dạng tấn công mạng

Có nhiều dạng tấn công mạng đã được biết đến, có thể phân loại dựa vào những tiêu chí khác nhau. Nếu dựa vào hành động của cuộc tấn công thì có thể chia tấn công làm 2 loại: tấn công chủ động và tấn công bị động.

- Tấn công chủ động: Kẻ tấn công làm thay đổi hoạt động của hệ thống và hoạt động của mạng khi tấn công làm ảnh hưởng đến tính toàn vẹn, sẵn sàng và xác thực của dữ liệu.
- Tấn công bị động: Kẻ tấn công cố gắng thu thập thông tin từ hoạt động của hệ thống và hoạt động của mạng làm phá vỡ tính bí mật của dữ liệu.

Nếu dựa vào nguồn gốc của cuộc tấn công thì có thể phân loại tấn công làm 2 loại: tấn công từ bên trong và tấn công từ bên ngoài.

- Tấn công từ bên trong: Là những tấn công xuất phát từ bên trong hệ thống mạng. Người sử dụng muốn truy cập, lấy thông tin nhiều hơn quyền cho phép.
- Tấn công từ bên ngoài: Là những tấn công xuất phát từ bên ngoài Internet hay các kết nối truy cập từ xa.

## 7.4. Một số tấn công mạng phổ biến

### 7.4.1. Tấn công vào các trang Web

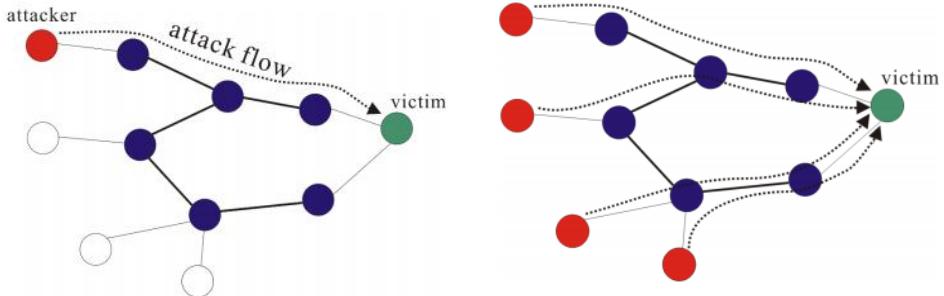
Web là dịch vụ được sử dụng rất phổ biến trên mạng, do đó nó là mục tiêu của nhiều cuộc tấn công. Website bị hacker tấn công chủ yếu do các vấn đề:

Lỗi kiểm soát truy cập: Việc truy cập vào các ứng dụng Web không được bảo vệ an toàn sẽ bị các hacker đoán mật khẩu để truy cập một cách trái phép. Ví dụ, tấn công Cross Site Scripting (XSS) hoặc Cross Site Request Forgery (CSRF), trong đó kẻ tấn công cố gắng đánh chặn các thông tin đăng nhập của người dùng thông qua trình duyệt của chính họ.

Lỗ hổng phần mềm: Những phần mềm dùng viết và quản lý Website cũng có những lỗ hổng như: máy chủ Web, cơ sở hạ tầng, công cụ viết Web,... Ví dụ các lỗ hổng phần mềm như Remote Code Execution (RCE), Remote/Local File Inclusion (R/LFI) - đây là hai lỗ hổng liên quan đến máy chủ Web; SQL Injection (SQLi) - lỗ hổng của SQL;... Các kẻ tấn công có thể khai thác các lỗ hổng này để tấn công vào các Website.

### 7.4.2. Tấn công từ chối dịch vụ

Tấn công từ chối dịch vụ (DoS hay DDoS) là sự nỗ lực làm cho những người dùng bình thường không thể sử dụng tài nguyên của một hay nhiều máy tính hoặc làm cho hệ thống đó chậm đi một cách đáng kể, bằng cách làm quá tải tài nguyên của hệ thống.



**Hình 7.3: Tấn công DoS và DDoS**

Điểm khác biệt cơ bản giữa tấn công DoS và DDoS là: tấn công DoS xuất phát từ một nguồn còn tấn công DDoS xuất phát từ rất nhiều nguồn tấn công, tạo thành một hệ thống mạng lưới gọi là mạng Botnet. Hệ thống Botnet ngày càng lớn về quy mô và trở nên rất nguy hiểm cho bất cứ một hệ thống mạng nào. So với tấn công DoS, tấn công DDoS có sức mạnh lớn hơn rất nhiều lần với số lượng gói tin rất lớn ào ạt gửi tới nạn nhân nhằm chiếm dụng tài nguyên và làm tràn ngập đường truyền của mục tiêu xác định.

Dấu hiệu của một vụ tấn công từ chối dịch vụ gồm có:

- Mạng thực thi chậm khác thường khi mở tập tin hay truy cập Website.
- Không thể dùng một Website cụ thể.
- Không thể truy cập bất kỳ Website nào.
- Tăng lượng thư rác nhận được.

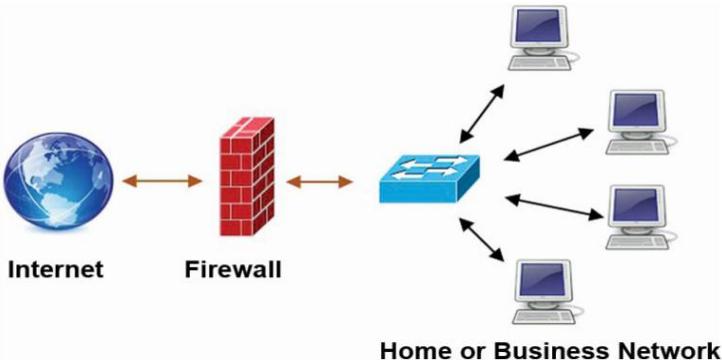
#### 7.4.3. Tấn công bằng mã độc

Mã độc là một loại phần mềm được tạo ra và chèn vào hệ thống một cách bí mật với mục đích thâm nhập, phá hoại hệ thống hoặc lấy cắp thông tin, làm gián đoạn, tổn hại tới tính bí mật, tính toàn vẹn và tính sẵn sàng của máy tính nạn nhân. Một số mã độc phổ biến như: Virus, Worm, Trojan,...

### 7.5. Các hệ thống an ninh mạng

Không có một giải pháp nào là hoàn hảo, có khả năng phát hiện, ngăn chặn tất cả các loại tấn công mạng. Để đảm bảo an toàn thông tin

nói chung và an ninh mạng nói riêng, các giải pháp kết hợp nên được thực hiện nhằm phát hiện nhanh, ngăn chặn các tấn công mạng, kịp thời khôi phục hệ thống, chủ động và tự động vận hành. Thực hiện các giải pháp bảo vệ theo chiều sâu, chia thành nhiều lớp phòng vệ. Một số giải pháp an ninh mạng phổ biến hiện nay được trình bày sau đây.



**Hình 7.4: Bảo vệ mạng LAN với Firewall**

### 7.5.1. Firewall

Firewall là phần cứng hoặc phần mềm máy tính giúp bảo vệ các hệ thống khỏi sự truy cập trái phép. Chức năng cơ bản nhất của tường lửa là kiểm soát các truy cập vào/ra hệ thống thông qua các luật (Rules). Các luật của Firewall được thiết kế theo chính sách bảo mật của tổ chức. Firewall giám sát tất cả các kết nối đi vào/ra hệ thống mạng và cho phép hoặc từ chối truy cập theo các luật được xác định trước.

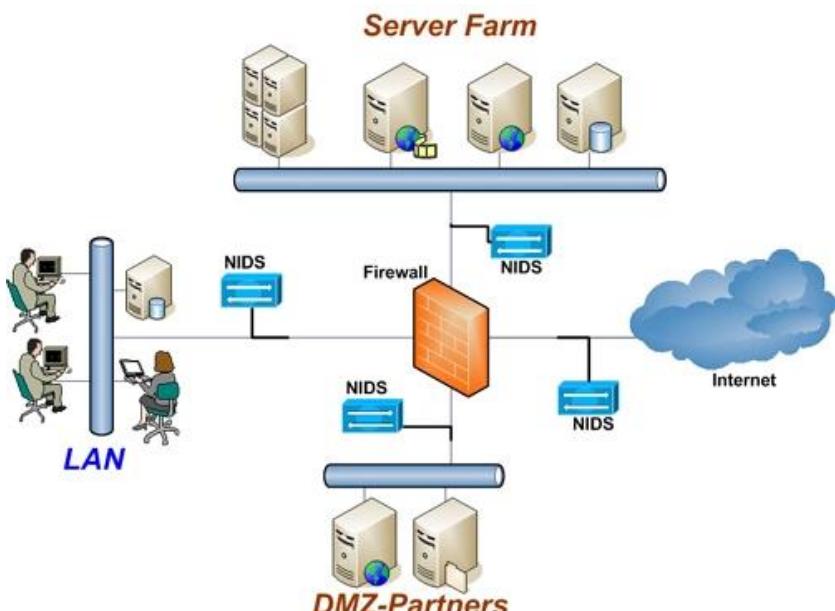
Có các dạng Firewall:

- Packet Filter: Tường lửa lọc gói hoạt động ở lớp Mạng của mô hình OSI và kiểm tra mọi gói đi qua để khớp với danh sách kiểm soát truy cập được xác định trước. Một số yếu tố mà tường lửa lọc gói sử dụng để đưa ra quyết định như địa chỉ IP nguồn, địa chỉ IP đích,...
- Circuit Level Gateways: Firewall này hoạt động ở lớp Phiên của mô hình OSI. Nó không lọc các gói riêng lẻ. Thay vào đó, nó giám sát tất cả các yêu cầu thiết lập phiên mới và kiểm tra xem việc bắt tay ba bước TCP đã được hoàn thành hay chưa để xác minh tính hợp lệ của phiên.

- Application Level Gateways: Firewall này hoạt động ở lớp Ứng dụng của mô hình OSI. Loại tường lửa này lọc lưu lượng dựa trên các lệnh dành riêng cho ứng dụng, như HTTP GET hoặc POST.

### 7.5.2. IDS/IPS

Hệ thống phát hiện xâm nhập (IDS) là một hệ thống lắng nghe, giám sát lưu lượng mạng và phát cảnh báo khi phát hiện bất kỳ loại xâm nhập nào vào hệ thống mạng. Ngay khi IDS phát hiện ra một vụ xâm nhập và đưa ra cảnh báo, quản trị viên có thể thực hiện hành động thích hợp để ngăn chặn hoặc giảm tác động của xâm nhập. IDS chủ yếu làm việc bằng cách sử dụng chữ ký, do đó nó có một cơ sở dữ liệu chữ ký được xác định trước cho các loại tấn công khác nhau. Ngoài ra, IDS còn hoạt động dựa vào các dấu hiệu bất thường - tức hệ thống sẽ tìm ra những điểm khác so với các dữ liệu bình thường và cảnh báo chúng là xâm nhập. Tập luật là thành phần quan trọng nhất của một hệ thống phát hiện xâm nhập. Đây là tập sẽ định ra dấu hiệu (mẫu) để so sánh, đối chiếu với dữ liệu ở đầu vào. Tùy vào mục tiêu bảo vệ, IDS có 2 dạng: Host Based IDS và Network Based IDS.



**Hình 7.5:** Một số thiết bị an ninh trong hệ thống mạng

Hệ thống ngăn chặn/phòng chống xâm nhập (IPS) là hệ thống theo dõi, ngăn ngừa kịp thời các hoạt động xâm nhập không mong muốn. Chức năng chính của IPS là xác định các hoạt động nguy hại, lưu giữ các thông tin này, sau đó kết hợp với Firewall để dừng ngay các hoạt động này, và cuối cùng đưa ra các báo cáo chi tiết về các hoạt động xâm nhập trái phép trên. Hệ thống IPS được xem là trường hợp mở rộng của hệ thống IDS, cách thức hoạt động cũng như đặc điểm của 2 hệ thống này tương tự nhau. Điểm khác nhau duy nhất là hệ thống IPS ngoài khả năng theo dõi, giám sát thì còn có chức năng ngăn chặn kịp thời các hoạt động nguy hại đối với hệ thống. Hệ thống IPS sử dụng tập luật tương tự như hệ thống IDS.

### 7.5.3. SIEM

SIEM (Security Information and Event Management) được thiết kế để thu thập các sự kiện an ninh từ các thiết bị đầu cuối và lưu trữ dữ liệu một cách tập trung, cho phép phân tích tập trung và báo cáo sự kiện an toàn của một hệ thống mạng, có thể phát hiện các cuộc tấn công mà không thể phát hiện được theo các phương pháp thông thường.

Kiến trúc của SIEM:

- Phần mềm được cài đặt trên máy chủ cục bộ.
- Phần cứng hoặc máy ảo dành riêng cho SIEM.
- Dịch vụ đám mây SIEM.

Lợi ích của SIEM:

Quản lý tập trung: Tập hợp dữ liệu thông qua giải pháp nhật ký (Log) tập trung. Mỗi hệ thống đầu cuối cần có hệ thống ghi lại sự kiện an ninh và thường xuyên truyền Log về máy chủ SIEM. Máy chủ SIEM nhận dữ liệu nhật ký từ rất nhiều thiết bị khác nhau và sau đó thực hiện thống kê, phân tích, báo cáo. Tạo ra báo cáo duy nhất cho thấy sự tương quan giữa các sự kiện an ninh của các thiết bị.

Giám sát an toàn mạng: Nhiều thiết bị có khả năng ghi Log sự kiện an ninh nhưng thiếu khả năng phân tích để xác định các hành vi độc hại. SIEM có khả năng cho thấy sự tương quan sự kiện giữa các thiết bị, sau đó cấu trúc lại chuỗi sự kiện và xác định cuộc tấn công

Cải thiện hoạt động xử lý sự cố hiệu quả: Cung cấp giao diện quản lý đơn giản để xem xét tất cả các dữ liệu nhật ký an ninh từ nhiều thiết bị, xác định nhanh chóng tất cả các thiết bị đầu cuối bị ảnh hưởng bởi cuộc tấn công, cung cấp cơ chế cách ly các thiết bị đầu cuối đã bị tấn công.

#### **7.5.4. Một số giải pháp nâng cao hiệu quả bảo mật**

- Nâng cao nhận thức về an toàn thông tin cho toàn thể tổ chức, doanh nghiệp, bao gồm các hoạt động thay đổi quan điểm của cấp lãnh đạo; tập huấn, đào tạo nâng cao nhận thức an toàn bảo mật thông tin cho toàn bộ nhân viên và cấp quản trị trong doanh nghiệp, trong tổ chức; thử nghiệm, diễn tập các kiểu tấn công giả mạo vào doanh nghiệp.
- Ưu tiên ngân sách cho các hoạt động về an toàn thông tin, bao gồm các hoạt động đầu tư trang thiết bị, công cụ, dụng cụ, giải pháp; chi phí cho các hoạt động thường xuyên về an toàn thông tin, lương cho chuyên gia và đội ngũ làm an toàn thông tin, các hoạt động đào tạo - vận hành; các hoạt động đánh giá, diễn tập về an toàn thông tin.
- Nhân sự về an toàn thông tin: xây dựng đội ngũ chuyên về an toàn thông tin; tạo điều kiện cho những người làm an toàn thông tin tham gia các khóa đào tạo chuyên môn và chuyên sâu, các hội thảo diễn đàn chuyên môn.
- Xây dựng các quy trình, quy định hoặc chuẩn quốc tế về an toàn thông tin. Xây dựng hệ thống ISMS (Information Security Management System) - hệ thống quản lý bảo mật thông tin mô tả các kiểm soát mà một tổ chức cần thực hiện để đảm bảo rằng nó bảo vệ một cách hợp lý tính bảo mật, tính sẵn có và tính toàn vẹn của tài sản khỏi các mối đe dọa và lỗ hổng.

### **7.6. Hệ thống giám sát mạng**

#### **7.6.1. Giới thiệu**

Trong những hệ thống mạng lớn, người quản trị mạng cần có công cụ để có thể theo dõi hoạt động của hệ thống. Việc theo dõi hoạt động của hệ thống bao gồm theo dõi tình trạng hoạt động của các thiết bị và

dịch vụ nhằm hạn chế các rủi ro gây ra. Từ đó giúp người quản trị kịp thời khắc phục, đảm bảo hệ thống hoạt động ổn định.

Bên cạnh việc theo dõi các gói tin để phát hiện những dấu hiệu tấn công mạng đã tìm hiểu ở các phần trên thì việc giám sát những hoạt động khác của hệ thống mạng như giám sát các luồng lưu lượng mạng, hoạt động của CPU, bộ nhớ, trạng thái hoạt động các máy chủ, theo dõi trạng thái hoạt động của các dịch vụ mạng trên nó và trạng thái của các thiết bị mạng (Router, Switch,...) là một trong những yêu cầu đặt ra để giám sát hệ thống một cách hiệu quả hơn. Điều này giúp cho người quản trị mạng có thể nắm bắt được tình trạng hoạt động của toàn bộ hệ thống mạng một cách nhanh chóng và tiện lợi.

Một hệ thống IDS/IPS có thể phát hiện và phòng chống các cuộc tấn công xâm nhập mạng dựa vào các dấu hiệu tấn công được lưu trữ và cập nhập thường xuyên. Tuy nhiên cũng không tránh khỏi những trường hợp có những dạng tấn công mới mà những dấu hiệu chưa được biết tới, tập luật của hệ thống phát hiện chưa được cập nhật.

Với sự kết hợp hệ thống giám sát trực quan, những hoạt động của những thiết bị trong hệ thống được theo dõi và hiển thị thời gian thực các hoạt động của hệ thống một cách trực quan thông qua những đồ thị về lưu lượng mạng, trạng thái hoạt động của CPU, RAM, dịch vụ mạng,... cho phép người quản trị có những phân tích để đưa ra các giải pháp phù hợp tránh những nguy hại cho hệ thống mạng.

Ngoài ra, người quản trị có thể thiết lập những ngưỡng cảnh báo kết hợp với hệ thống báo động để người quản trị nhanh chóng có được những thông tin về những cuộc tấn công hay phát hiện những bất thường trong hệ thống. Những bất thường ở đây như là một dịch vụ mạng ngừng hoạt động, máy chủ ngừng hoạt động, hay CPU hoạt động quá tải (đặt ngưỡng cảnh báo),...

### **7.6.2. Các giao thức của hệ thống giám sát**

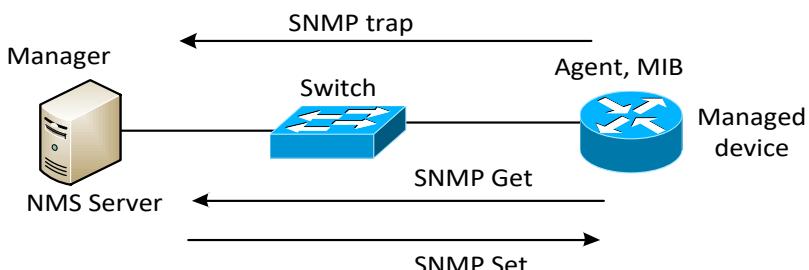
Để có thông tin cho việc giám sát trạng thái hoạt động của các thiết bị và dịch vụ mạng, trong hệ thống giám sát sử dụng giao thức SNMP (Simple Network Management Protocol).

SNMP là một giao thức chính được sử dụng cho mục đích theo dõi tình trạng hoạt động của các thiết bị và dịch vụ trong hệ thống mạng. SNMP làm nhiệm vụ thu thập thông tin từ các thiết bị mạng (Router, Switch, Server,...) cần giám sát và gửi về cho chương trình giám sát để phân tích và sử dụng để hiển thị ra giao diện quản trị các thông tin cần thiết theo mục đích của chương trình giám sát.

Trong SNMP có 3 vấn đề cần quan tâm: Manager, Agent và MIB.

- + **MIB**: Là cơ sở dữ liệu dùng phục vụ cho Manager và Agent.
- + **Manager**: Nằm trên máy chủ giám sát hệ thống mạng.
- + **Agent**: Là một chương trình nằm trên các thiết bị cần giám sát, quản lý. Agent có thể là một chương trình riêng biệt (ví dụ như Daemon trên Unix) hay được tích hợp vào hệ điều hành. Ví dụ như trong IOS của các thiết bị Cisco. Nhiệm vụ của các Agent là thông báo các thông tin đến cho thành phần điều khiển được cấu hình nằm trên máy chủ giám sát.

SNMP sử dụng UDP làm giao thức truyền tải thông tin giữa các Manager và Agent. Việc sử dụng UDP, thay vì TCP, bởi vì UDP là phương thức truyền mà trong đó hai đầu thông tin không cần thiết lập kết nối trước khi dữ liệu được trao đổi, thuộc tính này phù hợp trong điều kiện mạng gấp trực tiếp, hư hỏng,...



**Hình 7.6:** Các gói tin cơ bản trong SNMP

### 7.6.3. Các hoạt động giám sát

- Giám sát lưu lượng:

Giám sát lưu lượng được áp dụng ở các thiết bị mạng dùng là vai trò quan trọng trong việc chuyển tải các lưu lượng trên đường truyền như ở các Router, Core Switch,...

- Giám sát tình trạng hoạt động:

Giám sát tình trạng hoạt động của các thiết bị là theo dõi trạng thái còn hoạt động hay đã ngưng hoạt động. Trong những hệ thống có triển khai các thiết bị dự phòng thì khó nhận ra một thiết bị đang trong tình trạng ngưng hoạt động vì trong khi đó hệ luồng lưu lượng sẽ đi qua thiết bị dự phòng.

- Giám sát dịch vụ:

Giám sát dịch vụ thường được triển khai áp dụng ở các máy chủ để theo dõi tình trạng hoạt động của các dịch vụ cần giám sát. Có thể xảy ra trường hợp máy chủ vẫn đang hoạt động như dịch vụ bị tắt đi.

- Giám sát tài nguyên của thiết bị:

Giám sát các tài nguyên như hoạt động của CPU, RAM, dung lượng đĩa cứng,... giúp theo dõi tình trạng hoạt động, khả năng đáp ứng, từ đó tiến hành các biện pháp nâng cấp, thay thế.

## 7.7. SDN, KDN và xu hướng quản trị

### 7.7.1. Một số khái niệm

Trước hết hãy xem xét lại các thiết bị mạng hoạt động chuyển tiếp dữ liệu như thế nào. Các kết nối vật lý kết nối các thiết bị với nhau bằng cáp mạng hoặc dùng mạng không dây. Switch chuyển tiếp dữ liệu là các Ethernet Frame, Router chuyển tiếp các gói tin. Chúng sử dụng các giao thức khác nhau để học các thông tin hữu dụng, như các giao thức định tuyến học các đường đi ở tầng Mạng.

Mọi thứ mà các thiết bị mạng có thể làm được phân loại trong các mặt phẳng cụ thể. Trong phần này trình bày 3 loại mặt phẳng thường dùng nhất là: Data Plane, Control Plane và Management Plane.

- Data Plane:

Mặt phẳng dữ liệu (Data Plane) liên quan đến các tác vụ chuyển tiếp dữ liệu của các thiết bị mạng, liên quan đến các vấn đề nhận dữ liệu, xử lý và chuyển tiếp nó. Một số hành động được thực hiện trên các thiết bị mạng trong Data Plane:

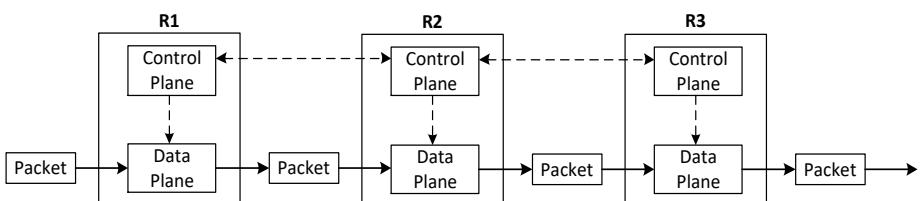
- + Mở gói và đóng gói (Router, Switch Layer 3).

- + Gán thêm và bỏ Header trong 802.1Q (Router, Switch).
- + So khớp địa chỉ MAC đích với bảng địa chỉ MAC (Layer 2 Switch).
- + So khớp địa chỉ IP đích với thông tin trong bảng định tuyến (Router, Layer 3 Switch).
- + Mã hóa dữ liệu và thêm IP Header mới (trong VPN).
- + Chuyển đổi địa chỉ IP (trong NAT).
- + Lọc gói tin (trong ACL, Port Security).

- Control Plane:

Router cần biết các đường đi trong bảng định tuyến trước khi Data Plane có thể chuyển tiếp các gói tin. Layer 2 Switch cần thiết lập bảng địa chỉ MAC trước khi nó có thể chuyển tiếp các Ethernet Frame ra cổng nào để đến đích. Switch phải sử dụng STP khóa một số cổng để đảm bảo Data Plane hoạt động tốt và chống Switching Loop.

Khái niệm mặt phẳng điều khiển (Control Plane) liên quan tới các hành động điều khiển của Data Plane. Hầu hết các hành động này phải thực hiện với việc tạo ra các bảng cho Data Plane sử dụng, các bảng này như là bảng định tuyến, bảng ARP, bảng địa chỉ MAC trên Switch,... Bằng cách vụ thêm, xóa, sửa các dòng trong các bảng này, Control Plane xử lý việc điều khiển những gì mà Data Plane thực hiện. Một số giao thức trong Control Plane như các giao thức định tuyến, các giao thức và thiết bị mạng truyền thống tích hợp Data Plane và Control Plane vào mỗi thiết bị.



**Hình 7.7: Mặt phẳng điều khiển và mặt phẳng dữ liệu**

- Một số giao thức Control Plane phổ biến như:
  - + Các giao thức định tuyến.
  - + IPv4 ARP.

- + IPv6 NDP.
- + Học địa chỉ MAC trên Switch.
- + STP.

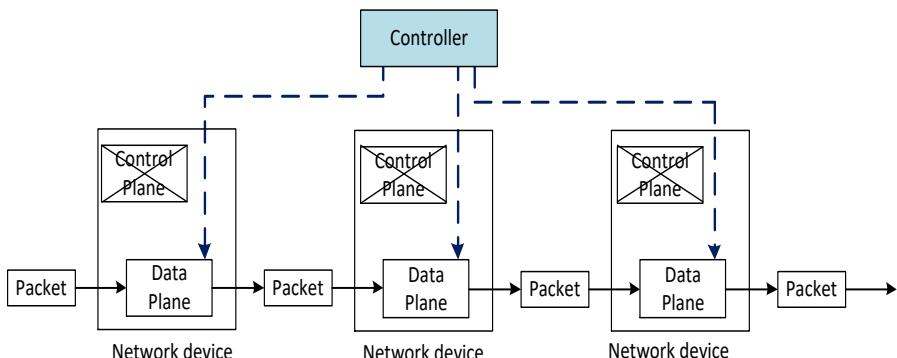
Nếu không có các giao thức và các hoạt động của Control Plane, Data Plane trên các thiết bị mạng truyền thông không thể hoạt động được. Router có thể không được dùng nếu các đường đi không thể học được từ các giao thức định tuyến. Nếu không có các dòng địa chỉ MAC học được trong bảng MAC, Switch chỉ có thể chuyển tiếp các gói tin Unicast bằng cách gửi chúng ra tất cả các cổng của nó. Do đó, Data Plane dựa vào Control Plane để đưa ra các thông tin hữu dụng.

- Management Plane:

Mặt phẳng quản trị (Management Plane) bao gồm các giao thức cho phép người quản trị điều khiển các thiết bị. Telnet và SSH là 2 giao thức phổ biến của Management Plane.

### 7.7.2. Controller

Từ những năm 2010, một số hướng tiếp cận mới được hình thành. Trong đó có phương pháp chuyên Control Plane làm việc trong phần mềm chạy như một ứng dụng tập trung gọi là Controller. Hầu hết Control Plane truyền thống sử dụng kiến trúc phân tán, chạy trên nhiều thiết bị. Ví dụ như mỗi Router chạy một tiến trình OSPF riêng. Để phối hợp hoạt động, Control Plane sử dụng các thông điệp để giao tiếp với nhau. SDN sử dụng kiến trúc tập trung với Control Plane tập trung, gọi là SDN Controller, để tập trung điều khiển các thiết bị mạng.



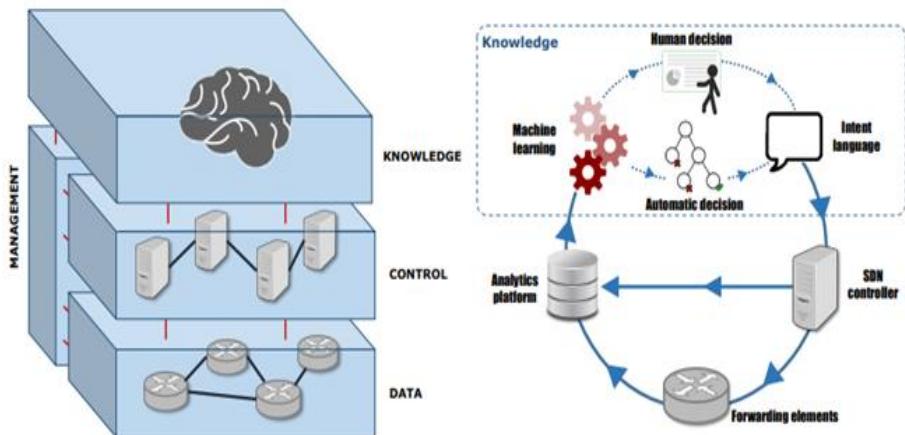
**Hình 7.8: Quản lý tập trung với Controller**

### 7.7.3. SDN

SDN (Software Defined Network) là một cách thức để xây dựng mạng. Các thiết bị mạng vẫn được triển khai và chuyển tiếp dữ liệu nhưng các chức năng của Control Plane và vị trí của nó có sự thay đổi. Các Control Plane chuyển từ mô hình phân tán sang mô hình tập trung.

### 7.7.4. KDN

KDN (Knowledge Defined Network) dựa vào các kỹ thuật Machine Learning và các kỹ thuật nhận thức để vận hành hệ thống mạng. Trong đó, Knowledge Plane được sử dụng mang lại nhiều điểm nổi bật như sự tự động hóa (Recognize Act) và sự đề xuất dựa trên các quy luật nhận diện (Recognize Explain Suggest) hỗ trợ cho sự vận hành, tối ưu và khắc phục sự cố đạt hiệu quả.



*Hình 7.9: Mặt phẳng và quy trình hoạt động của KDN*

## 7.8. Tổng kết chương

Mỗi ngày thế giới phải đối mặt với hàng nghìn cuộc tấn công an ninh mạng. Thiệt hại từ mất an toàn thông tin lên tới hàng nghìn tỷ USD do các vụ đánh cắp dữ liệu hoặc các vụ tấn công nhắm vào các hệ thống thông tin trọng yếu. Trong thế giới kết nối, an ninh mạng có thể coi là một trong những trụ cột của nền kinh tế số. Hiểu biết được các vấn đề về an ninh mạng, chúng ta sẽ nâng cao ý thức trong việc bảo vệ thông tin cá nhân và tổ chức, đồng thời cũng nắm được các kỹ thuật để bảo vệ hệ thống mạng máy tính khỏi các tấn công như: Firewall, IDS/IPS, SIEM,...

## 7.9. Câu hỏi và bài tập

1. Phát biểu nào sau đây không đúng về vùng DMZ?
  - A. Thường chứa E-mail Server, hoặc Web Server.
  - B. Có thể bao gồm Front End Firewall và Backend Firewall.
  - C. Chứa các Server chỉ phục vụ cho người dùng bên trong.
  - D. Để nâng cao sự bảo mật cho hệ thống.
2. Điều nào sau đây không đúng khi nói về lỗ hổng 0-day?
  - A. Là lỗ hổng nhà sản xuất chưa kịp vá.
  - B. Là lỗ hổng phá hoại hệ thống trong vòng một ngày.
  - C. Là lỗ hổng hacker chưa công bố rộng rãi.
  - D. Là lỗ hổng nguy hiểm khi tấn công vào hệ thống chưa có giải pháp bảo vệ.
3. Việc gỡ bỏ những dịch vụ và giao thức không cần thiết gọi là:
  - A. Nonrepudiation.
  - B. Hardening.
  - C. Auditing.
  - D. Hashing.
4. Giao thức nào được dùng để mã hóa dữ liệu trao đổi giữa Web Browser và Web Server?
  - A. IPSec.
  - B. HTTP.
  - C. SSL.
  - D. VPN.
5. Tấn công một máy tính bằng cách gửi các gói TCP Handshake không đúng thứ tự đến đích (Wrong Order) xảy ra ở tầng nào?
  - A. Network Interface Layer.
  - B. Internet Layer.
  - C. Transport Layer.
  - D. Application Layer.

6. Kỹ thuật tấn công nào sau đây có thể vượt qua các cơ chế bảo mật vật lý và logic để có thể truy cập vào hệ thống?
- A. Brute Force.
  - B. Denial of Service.
  - C. Social Engineering.
  - D. Port Scanning.
  - E. Man-In-The-Middle.
7. Các dịch vụ chạy trên hệ thống thường được hacker xác định dựa vào đâu?
- A. Địa chỉ IP của hệ thống.
  - B. Active Directory.
  - C. Tên của hệ thống.
  - D. Chỉ số Port.
8. Chức năng của giao thức IPSec hoạt động ở tầng nào trong mô hình OSI?
- A. Data Link.
  - B. Transport.
  - C. Session.
  - D. Network.
  - E. Application.
9. Cách tốt nhất để nhận ra hành vi bất thường và đáng ngờ trên hệ thống mạng của bạn là gì?
- A. Nhận biết được các cuộc tấn công mới nhất.
  - B. Cấu hình IDS để phát hiện và cảnh báo các lưu lượng bất thường.
  - C. Nhận biết được các hoạt động bình thường hệ thống.
  - D. Nghiên cứu dấu hiệu hoạt động của các loại tấn công quan trọng trên hệ thống.
10. Trong IDS, khái niệm False Positive nghĩa là gì?

- A. Không có tấn công nhưng hệ thống vẫn phát cảnh báo.
  - B. Có tấn công và hệ thống phát cảnh báo.
  - C. Có tấn công nhưng hệ thống không phát cảnh báo.
  - D. Không có tấn công và hệ thống không phát cảnh báo.
11. Bạn là người tư vấn giải pháp an toàn thông tin, một khách hàng của bạn quan tâm đến việc chống lại giả mạo và nhiễm độc ARP trong mạng của họ. Giải pháp nào dưới đây KHÔNG áp dụng cho mục đích này?
- A. Sử dụng Port Security trên các Switch.
  - B. Sử dụng công cụ giám sát ARP trong mạng (kiểu như ARPwatch).
  - C. Sử dụng Firewall giữa các phân vùng trong LAN.
  - D. Nếu trong một mạng nhỏ thì sử dụng ARP tĩnh.
12. Phát biểu nào sau đây không đúng về vùng DMZ?
- A. Thường chứa E-mail Server, hoặc Web Server.
  - B. Có thể bao gồm Front End Firewall và Backend Firewall.
  - C. Chứa các Server chỉ phục vụ cho người dùng bên trong.
  - D. Để nâng cao sự bảo mật cho hệ thống.
13. Kiểu tấn công nào sau đây không phải khai thác các lỗ hổng của ứng dụng Web?
- A. Cross Site Scripting.
  - B. SQL Injection.
  - C. Social Engineering.
  - D. Cross Site Request Forgery.
14. Các cổng hoạt động của các dịch vụ Web, DNS, Telnet theo thứ tự là?
- A. 80, 53, 23.
  - B. 80, 20, 23.
  - C. 53, 23, 80.
  - D. 20, 23, 80.

15. Mục tiêu của đảm bảo an toàn cho một hệ thống CNTT được biết đến với mô hình có tên gọi là CIA gồm các tính chất?
- A. Tính bí mật, tính xác thực, tính toàn vẹn.
  - B. Tính bí mật, tính toàn vẹn, tính sẵn sàng.
  - C. Tính toàn vẹn, tính sẵn sàng, tính xác thực.
  - D. Tính bí mật, tính toàn vẹn, tính chống chối bỏ.
16. Giải pháp nào sau đây được xem là tốt nhất để chống lại tấn công dựa vào việc bắt gói tin trên mạng (Sniffing)?
- A. Sử dụng Switch thay cho Hub.
  - B. Sử dụng mạng có dây, không nên sử dụng mạng không dây.
  - C. Sử dụng Gateway.
  - D. Sử dụng các kỹ thuật mã hóa dữ liệu khi truyền.
17. Mục tiêu chính của các kỹ thuật điều khiển truy cập trong hệ thống CNTT là?
- A. Để cấp toàn bộ quyền truy cập cho người dùng đã được chứng thực.
  - B. Để giới hạn các quyền và hoạt động của người dùng đã được chứng thực.
  - C. Để ngăn chặn các người dùng trái phép vào các tài nguyên hệ thống.
  - D. Để bảo vệ máy tính khỏi nhiễm virus.
18. Giao thức nào sau đây được sử dụng để truyền thông tin giám sát giữa Manager và Agent trong hệ thống giám sát mạng?
- A. UDP.
  - B. SNMP.
  - C. TCP.
  - D. IP.
19. Switch Layer 2 xem xét địa chỉ MAC đích trong Frame và lựa chọn để chuyển tiếp Frame này chỉ ra cổng Gi0/1. Hành động này diễn ra là một phần của mặt phẳng nào của Switch?

- A. Mặt phẳng dữ liệu.
  - B. Mặt phẳng quản lý.
  - C. Mặt phẳng điều khiển.
  - D. Mặt phẳng bảng.
20. Một Router sử dụng OSPF để học các mạng và thêm chúng vào bảng định tuyến. Hành động này xảy ra ở mặt phẳng nào của Router?
- A. Mặt phẳng dữ liệu.
  - B. Mặt phẳng quản lý.
  - C. Mặt phẳng điều khiển.
  - D. Mặt phẳng bảng.

## TÀI LIỆU THAM KHẢO

- [1] Wendell Odom, *CCNA 200-301 Official Cert Guide*, Volume 1, Cisco Press, 2020.
- [2] Wendell Odom, *CCNA 200-301 Official Cert Guide*, Volume 2, Cisco Press, 2020.
- [3] Jordan Krause, *Mastering Windows Server 2019*, 2nd Edition, PACK, 2019.
- [4] Christine Bresnahan & Richard Blum, *LPIC-1 Linux Professional Institute Certification Study Guide*, Sybex, 2019.
- [5] Christine Bresnahan & Richard Blum, *LPIC2 - Linux Professional Institute Certification Study Guide - Second Edition*, Sybex, 2016.
- [6] Mestres A., Rodriguez-Natal A., Carner J., Barlet-Ros P., Alarcón E., Solé M.,... & Estrada G. (2017), *Knowledge-defined networking*, ACM SIGCOMM Computer Communication Review, 47(3), 2-10.

**Giáo trình mạng máy tính căn bản**  
(Giáo trình dành cho sinh viên ngành Công nghệ thông tin)

**Huỳnh Nguyên Chính (chủ biên), Nguyễn Thị Thanh Vân  
Trường Đại học Sư phạm Kỹ thuật Thành phố Hồ Chí Minh**

**NHÀ XUẤT BẢN ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH**

**Trụ sở:**

Phòng 501, Nhà Điều hành ĐHQG-HCM,  
phường Linh Trung, thành phố Thủ Đức,  
Thành phố Hồ Chí Minh.

ĐT: 028 62726361

E-mail: vnuhp@vnuhcm.edu.vn

**Văn phòng đại diện:**

Tòa nhà K-Trường Đại học Khoa học Xã hội & Nhân  
văn, số 10-12 Đinh Tiên Hoàng, phường Bến Nghé,  
Quận 1, Thành phố Hồ Chí Minh

ĐT: 028 62726390

Website: www.vnuhcmpress.edu.vn

**Chịu trách nhiệm xuất bản và nội dung**

**TS ĐỖ VĂN BIÊN**

**Biên tập**

**NGUYỄN THỊ NGỌC ANH**

**Sửa bản in**

**PHƯỚC HUỆ**

**Trình bày bìa**

**TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT THÀNH PHỐ HỒ CHÍ MINH**

**Đối tác liên kết**

**TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT THÀNH PHỐ HỒ CHÍ MINH**

Xuất bản lần thứ 1. Số lượng in: 250 cuốn, khổ 16 x 24cm. Số  
XNĐKXB: 1946-2022/CXBIPH/4-25/ĐHQGTPHCM. QĐXB số: 198/QĐ-  
NXB cấp ngày 12/7/2022. In tại: Công ty TNHH In và Bao bì Hưng Phú; Địa  
chi: 162A/1, KP1A, phường An Phú, TP Thuận An, Bình Dương. Nộp lưu  
chiểu: Năm 2022. ISBN: **978-604-73-9135-6**.

Bản quyền tác phẩm đã được bảo hộ bởi Luật Xuất bản và Luật Sở hữu  
trí tuệ Việt Nam. Nghiêm cấm mọi hình thức xuất bản, sao chụp, phát tán nội  
dung khi chưa có sự đồng ý của tác giả và Nhà xuất bản.

**ĐỀ CÓ SÁCH HAY, CẦN CHUNG TAY BẢO VỆ TÁC QUYỀN!**





## CHÍNH SÁCH CHẤT LƯỢNG

*Không ngừng nâng cao chất lượng dạy, học, nghiên cứu khoa học  
và phục vụ cộng đồng nhằm mang đến cho người học những điều kiện tốt nhất  
để phát triển toàn diện các năng lực đáp ứng nhu cầu phát triển và hội nhập quốc tế.*

ISBN: 978-604-73-9135-6



9 786047 391356