

CCNA

HỌC KỲ 1

**Tài liệu hướng dẫn
Version 1.0**

Mục lục

(Học kỳ 1)

<u>Bài 1:</u> Khảo sát chức năng mạng máy tính.....	1-1
<u>Bài 2:</u> Bảo mật mạng.....	2-1
<u>Bài 3:</u> Tìm hiểu về mô hình truyền thông từ máy đến máy.....	3-1
<u>Bài 4:</u> Tìm hiểu lớp Internet của mô hình TCP/IP.....	4-1
<u>Bài 5:</u> Tìm hiểu lớp vận chuyển của mô hình TCP/IP.....	5-1
<u>Bài 6:</u> Khảo sát tiến trình phân phối gói tin.....	6-1
<u>Bài 7:</u> Tìm hiểu mạng Ethernet.....	7-1
<u>Bài 8:</u> Kết nối mạng cục bộ Ethernet.....	8-1
<u>Bài 9:</u> Hiểu về môi trường Mạng cục bộ chia sẻ.....	9-1
<u>Bài 10:</u> Giải quyết các thách thức trong mạng với công nghệ LAN Switched.....	10-1
<u>Bài 11:</u> Khảo sát quy trình phân phối Packet (gói thông tin mạng).....	11-1
<u>Bài 12:</u> Vận hành Hệ Điều Hành Cisco IOS.....	12-1
<u>Bài 13:</u> Khởi động với Switch.....	13-1
<u>Bài 14:</u> Hiểu về bảo mật thiết bị Switch.....	14-1
<u>Bài 15:</u> Tối ưu hóa những tiện ích của Switch.....	15-1
<u>Bài 16:</u> Xử lý các sự cố của Switch.....	16-1
<u>Bài 17:</u> Tìm hiểu mạng WLAN.....	17-1
<u>Bài 18:</u> Tìm hiểu về bảo mật trên WLAN.....	18-1
<u>Bài 19:</u> Thực thi WLAN.....	19-1

Bài 1: Khảo sát chức năng mạng máy tính



Xây dựng một mạng đơn giản

Module 1-1

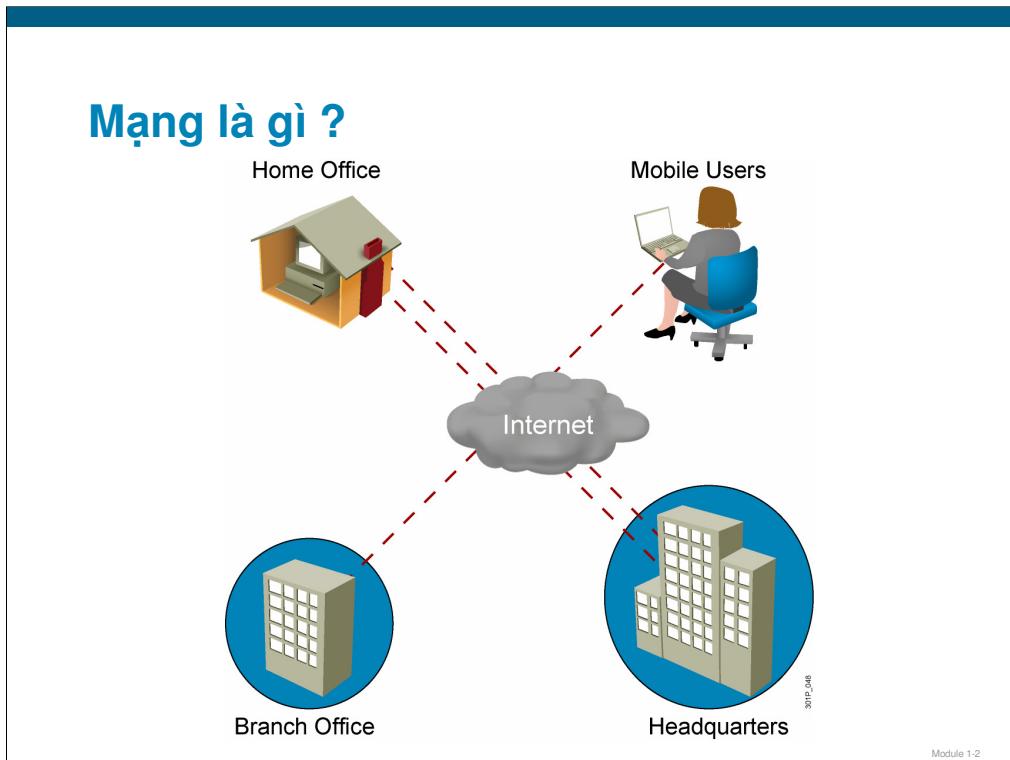
Tổng quan

Hiểu các ưu điểm và cách thức hoạt động của mạng máy tính là quan trọng trong việc tối ưu kênh truyền thông giữa người dùng đầu cuối. Bài học này sẽ mô tả các khái niệm, giới thiệu các thành phần và giải thích các ích lợi của mạng máy tính.

Mục tiêu

Kết thúc bài học này học viên có thể liệt kê các thành phần chính, mục đích và chức năng của một mạng

- Mô tả mạng
- Liệt kê các thành phần chính của mạng
- Diễn dịch mô hình mạng
- Liệt kê các chức chia sẻ tài nguyên chính và các ưu điểm của chúng
- Liệt kê 4 ứng dụng mạng và các ưu điểm của mỗi ứng dụng
- Mô tả ảnh hưởng của ứng dụng trên mạng
- Liệt kê loại đặc trưng dùng để mô tả các loại mạng khác nhau
- So sánh các loại mô hình vật lý và luận lý (physical & logical topologies)
- Liệt kê đặc trưng của mô hình bus
- Liệt kê đặc trưng của mô hình sao & sao mở rộng
- Liệt kê đặc trưng của mô hình vòng đơn & vòng đôn
- Liệt kê đặc trưng của mô hình lưới đầy đủ và không đầy đủ
- Mô tả các phương pháp kết nối với mạng internet



Phần này mô tả đặc trưng và môi trường của các loại mạng khác nhau.

Mạng là một tập hợp được nối kết với nhau giữa thiết bị và end-system (chẳng hạn như PC và servers). Mạng dùng vận chuyển dữ liệu với các phạm vi triển khai khác nhau bao gồm nhà ở, văn phòng nhỏ, và các công ty lớn. Trong các công ty lớn, sẽ có thể bao gồm nhiều vị trí có nhu cầu trao đổi dữ liệu, chúng ta sẽ làm quen với một số thuật ngữ cơ bản như sau :

- Main office:** văn phòng chính là nơi mọi người kết nối đến, đây cũng là nơi lưu trữ khối lượng thông tin quan trọng của công ty. Văn phòng chính có thể phục vụ hàng trăm thậm chí hàng ngàn nhân viên và được triển khai trên nhiều tầng của một cao ốc hoặc một vài tòa nhà trong 1 campus.

- Remote locations:** những trạm kết nối từ xa

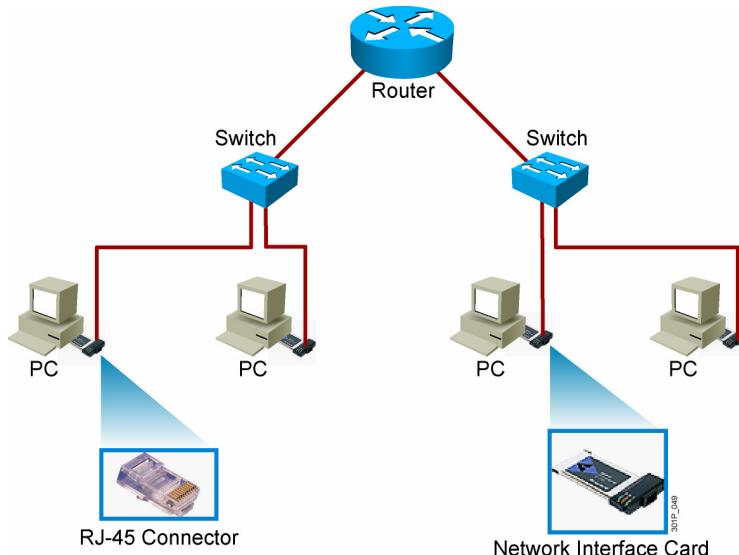
- Branch offices:** văn phòng chi nhánh. Mặc dù một số thông tin có thể được lưu trữ cục bộ tại đây, nhưng phần các dữ liệu sẽ được lấy trực tiếp từ văn phòng chính.

- Home offices:** Khi cá nhân làm việc tại nhà thì các vị trí này được gọi là home office. Các trạm kết nối này thường sử dụng các kết nối dạng on-demand về văn phòng chính để truy cập thông tin.

- Mobile users:** Người dùng dạng này có nhu cầu truy cập thông tin của công ty từ văn phòng chính từ nhiều địa điểm khác nhau.

Bạn có thể dùng mạng tại nhà để truy cập web, đặt mua hàng hóa, gửi thư cho bạn bè. Tại văn phòng làm việc bạn có thể xây dựng một mạng nhỏ để kết nối các PC, máy in Đối với các công ty lớn những kết nối này có thể triển khai kết nối các văn phòng ở cách xa nhau trên toàn cầu.

Các phần tử vật lý thông thường của một mạng

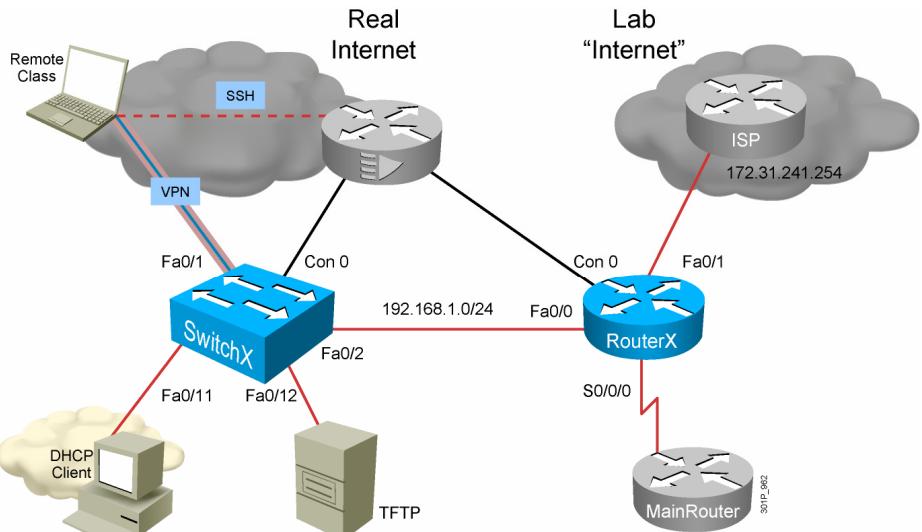


Module 1-3

Có 4 loại thiết bị phần cứng hình thành nên mạng máy tính

- **Personal computers (PCs)**: máy tính cá nhân, dùng gửi và nhận dữ liệu.
- **Interconnections** : bao gồm các thành phần nối kết mạng trên đó dữ liệu được truyền tải :
 - Network interface cards (NICs) : card mạng dùng để chuyển đổi dữ liệu máy tính trên mạng cục
 - Network media : môi trường truyền dẫn ví dụ cáp đồng, cáp quang ... trên đó dữ liệu được truyền đi từ máy này đến máy kia.
 - Connectors : đầu nối cung cấp điểm tiếp xúc vào môi trường truyền
- **Switches**: thiết bị dùng nối kết các máy PC trong mạng cục bộ.
- **Routers**: thiết bị định tuyến dùng chọn đường đi tốt nhất cho dữ liệu.

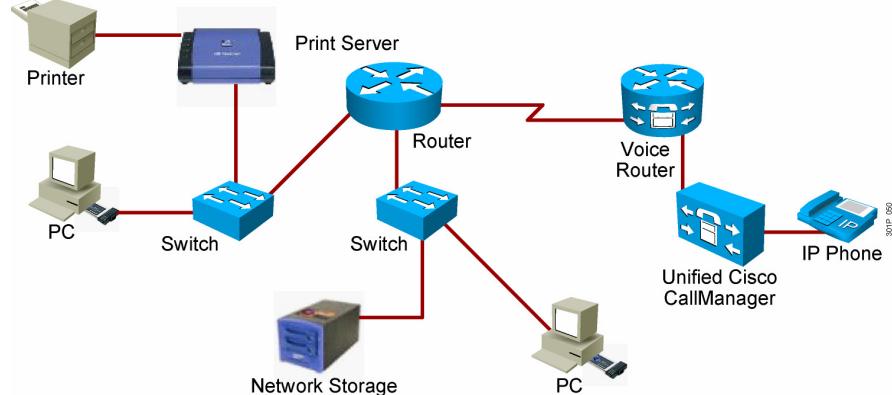
Thông dịch một sơ đồ mạng



Module 1-4

Một số ký hiệu cơ bản trên sơ đồ mạng

Chia sẻ tài nguyên chức năng và các ưu điểm



- Data and applications
- Resources
- Network storage
- Backup devices

Module 1-5

Mạng máy tính cho phép ta chia sẻ thông tin và tài nguyên phần cứng :

- **Data and applications:** người dùng có thể dùng chung dữ liệu, tập tin, phần mềm.
- **Resources:** tài nguyên phần cứng như máy in, máy quét, máy chụp hình ...
- **Network storage:** ngày nay có nhiều cách chia sẻ tài nguyên lưu trữ nhưng hệ thống Direct attached storage (DAS) gắn trực tiếp vào PC. ổ đĩa cứng mạng Network attached storage (NAS). Finally, hệ thống mạng lưu trữ storage area networks (SANs).
- **Backup devices:** mạng máy tính cũng có khả năng sao lưu dữ liệu thông qua băng từ, đĩa cứng ... dùng cho mục đích phục hồi dữ liệu khi có sự cố.

Các ứng dụng mạng

- E-mail (Outlook, POP3, Yahoo, and so on)
- Web browser (IE, Firefox, and so on)
- Instant messaging (Yahoo IM, Microsoft Messenger, and so on)
- Collaboration (Whiteboard, Netmeeting, WebEx, and so on)
- Databases (file servers)

Có rất nhiều ứng dụng trên mạng máy tính. Tuy nhiên có một số ứng dụng ngày nay trở nên rất phổ biến bao gồm

E-mail: thư điện tử cho phép người dùng gửi các bức thư nhanh chóng đến bất kỳ đâu trên mạng internet. Các chương trình mail phổ biến gồm Microsoft Outlook và Eudora.

Web browser: trình duyệt web cho phép hiển thị các trang web. Các trình duyệt phổ biến Microsoft Internet Explorer, Netscape Navigator, Mozilla, và Firefox.

Instant messaging: sử dụng phổ biến trong tán gẫu trên mạng (ví dụ như là AOL, Yahoo, Skype ...)

Collaboration: ứng dụng cộng tác cho phép cá nhân hoặc các nhóm làm việc cùng nhau (ví dụ như Lotus Notes)

Database: ứng dụng cơ sở dữ liệu (ví dụ : file servers).

Ảnh hưởng của chương trình ứng trên mạng máy tính

- Ứng dụng dạng bó
 - FTP, TFTP, cập nhật kiểm kê
 - Không yêu cầu tương tác với người dùng
 - Băng thông là quan trọng, nhưng không yêu cầu cao về độ ưu tiên
- Chương trình dạng tương átc
 - Truy vấn kiểm kê, cập nhật cơ sở dữ liệu.
 - Tương tác người - máy
 - Thời gian dập ứng là quan trọng như không yêu cầu cao độ
- Chương trình thời gian thực
 - Thoại IP, video
 - Tương tác giữa nhiều người dùng
 - Yêu cầu nghiêm ngặt về thời gian trễ



Module 1-7

Ứng dụng và chất lượng của mạng máy tính ảnh hưởng qua lại lẫn nhau. Phần này mô tả mối quan hệ tương tác đó

- Các ứng dụng dạng bó (Batch applications) ví dụ như ứng dụng truyền tập tin từ xa FTP, TFTP được khởi tạo bởi người dùng nhưng sau đó phần mềm sẽ tự điều khiển không cần sự tương tác với người dùng. Các ứng dụng dạng này cần sử dụng nhiều băng thông nhưng không yêu cầu cao về độ ưu tiên
- Các ứng dụng tương tác, thời gian thực (ví dụ như thoại IP, xem film trực tuyến ...) lại có yêu cầu giao tiếp giữa người và máy, do đặc thù của ứng dụng nên các dữ liệu này phải có độ ưu tiên cao nhằm đảm bảo chất lượng dịch vụ. Các hệ thống mạng máy tính thường phải hiện thực cơ chế đảm bảo chất lượng dịch vụ (QoS) đối với các dữ liệu của những ứng dụng này

Đặc trưng của mạng

- Speed
- Cost
- Security
- Availability
- Scalability
- Reliability
- Topology

Các đặc trưng của mạng máy tính bao gồm

Speed: tốc độ

Cost: chi phí cài đặt, bảo hành bảo trì

Security: tính bảo mật

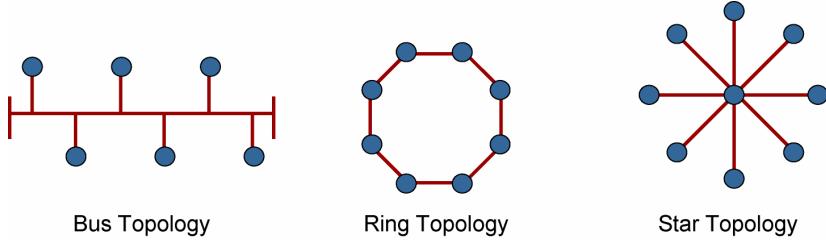
Availability: tính khả dụng, hệ thống mạng máy tính phải hoạt động ổn định suốt 24 giờ một ngày, 7 ngày trong tuần và 256 ngày trong một năm. Tính khả dụng đo bằng thời gian hệ thống bị sự cố. Ví dụ : mạng bị gián đoạn 15 phút trong 1 năm thì tính khả dụng là :

$$([số\ phút\ trong\ năm - số\ phút\ gián\ đoạn] / [số\ phút\ trong\ năm]) * 100 = ([525600 - 15] / [525600]) * 100 = 99.9971\%$$

Scalability: khả năng mở rộng của mạng máy tính về số lượng người dùng lẫn nhu cầu truyền tải dữ liệu đáp ứng các nhu cầu mới. **Reliability:** độ tin cậy phụ thuộc vào các thành tố tạo nên hệ thống mạng như bộ định tuyến, chuyền mạch, máy tính ...

Topology: có 2 loại mô hình : mô hình vật lý - là cách kết nối các thiết bị phần cứng. Mô hình luận lý – con đường dữ liệu truyền đi thông qua mô hình vật lý.

Các loại mô hình vật lý



Module 1-9

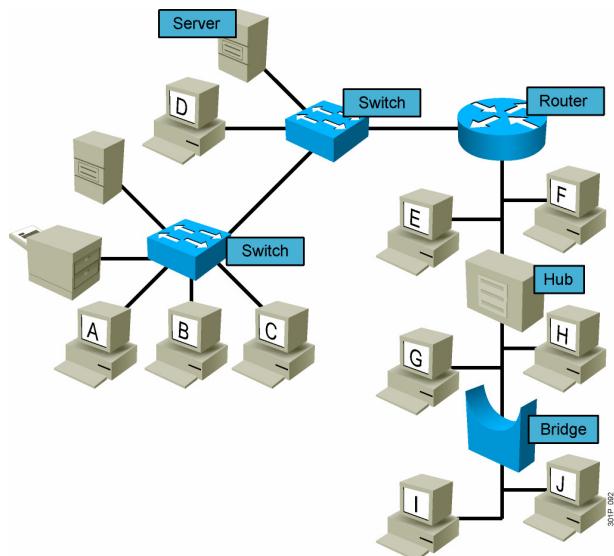
Physical Topologies mô hình vật lý liên quan đến cách bố trí thiết bị và nối dây. Bạn phải chọn mô hình vật lý phù hợp với loại dây cáp (cáp xoắn đôi, cáp đồng trực, cáp quang ...) sẽ cài đặt. Có 3 mô hình chính :

Bus: tất cả thiết bị nối vào đường trực chính sử dụng cáp đồng trực

Ring: máy tính và các thiết bị khác nối thành vòng tròn (đơn hoặc đôi) sử dụng cáp đồng trực hoặc cáp quang

Star: một thiết bị trung tâm dùng kết các thiết bị lại với nhau thường sử dụng cáp xoắn đôi

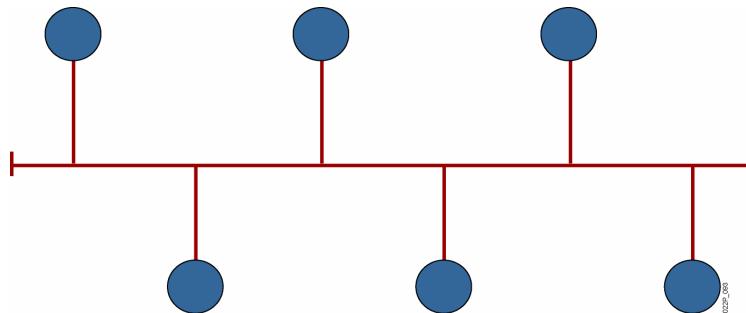
Các loại mô hình luận lý



Module 1-10

Mô hình luận lý của mạng máy tính liên quan đến con đường lô gíc mà tín hiệu lan truyền từ điểm này đến điểm kia trên mạng. Mô hình mạng vật lý và luận lý có thể giống nhau. Ví dụ trong mạng cáp đồng trực cách thức đầu nối và lan truyền dữ liệu thực hiện trên một đường bus chung. Trong một số trường hợp khác 2 mô hình này có thể khác nhau. Ví dụ : mạng lan có sử dụng switch đầu nối theo mô hình sao nhưng mô hình luận lý có thể là dạng vòng tròn. Vì vậy, không thể đoán biết được cách thức lan truyền dữ liệu trên mạng chỉ bằng cách xem xét mô hình vật lý. Ngày nay mô hình đầu nối dạng star được sử dụng phổ biến nhất trong các mạng cục bộ. Mạng Ethernet dùng mô hình vật lý là bus hoặc sao nhưng mô hình luận lý là bus.

Mô hình Bus

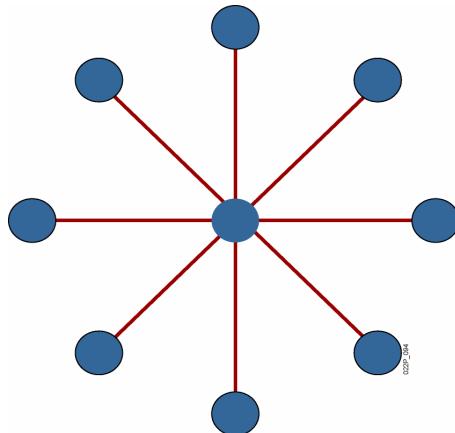


- Tất cả thiết bị đều nhận tín hiệu

Module 1-11

Hình trên minh họa mô hình bus, tất cả các thiết bị đều được nối vào 1 cáp chính. Cáp chính phải được kết thúc sao cho nó hấp thu toàn bộ tín hiệu khi đến điểm cuối cùng. Nếu tín hiệu không được hấp thu tốt dòng điện tử sẽ dội ngược trở lại sinh ra nhiễu trên mạng.

Mô hình sao



- Truyền thông qua 1 điểm tập trung
- Single point of failure.

Module 1-12

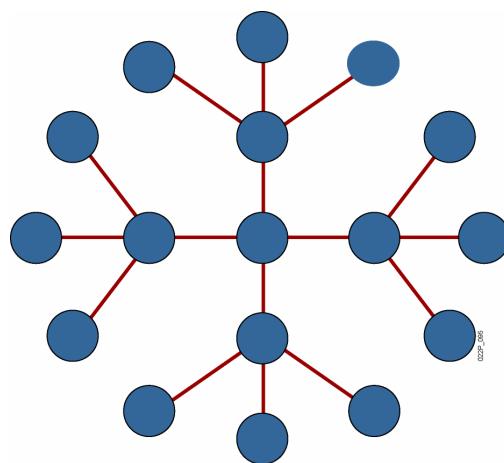
Mô hình sao là mô hình kết nối vật lý dùng trong mạng Ethernet loại mạng cục bộ sử dụng phổ biến nhất ngày nay

Mô hình sao sẽ tồn tại một điểm tập trung tất cả các thiết bị sẽ nối về điểm này hình thành nên hình sao.

Star Topology

Mặc dù chi phí phải bỏ ra khi triển khai mô hình sao so với dạng bus nhưng ưu điểm mà ta có được rất đáng giá. Mỗi thiết bị đều được kết nối vào thiết bị trung tâm vì thế khi một cáp bị hỏng thì chỉ có thiết bị tương ứng bị ảnh hưởng vì thế các mạng cục bộ ngày nay đều dùng mô hình này

Mô hình sao mở rộng



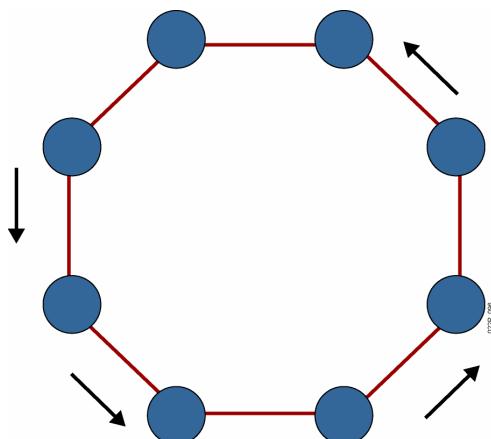
- Mở rộng hơn mô hình sao.

Module 1-13

Extended-Star Topology

Mô hình sao mở rộng bằng cách nối thêm các thiết bị tập trung vào thiết bị chính. Như vậy ta có thể mở rộng mạng tuy nhiên khuyết điểm là nếu điểm chính hỏng hóc thì mạng sẽ bị đình trệ.

Mô hình vòng



- Tín hiệu lan truyền theo vòng tròn.
- Single point of failure.

Module 1-14

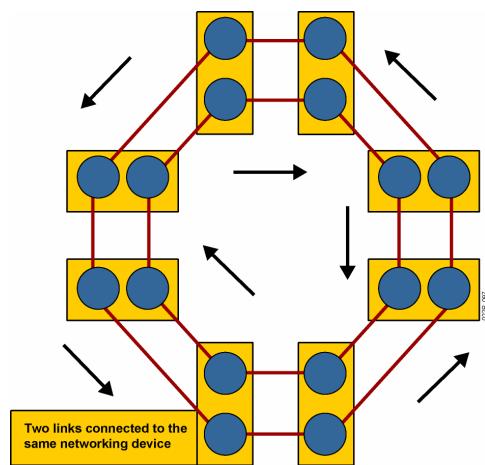
Không giống mô hình bus mô hình vòng không có điểm đầu và cuối vì thế không cần được kết thúc. Dữ liệu được truyền đi theo phương thức rất khác so với mô hình bus. Trong một số hiện thực, người ta dùng một thẻ (token) di chuyển vòng quanh dừng lại ở từng thiết bị. Nếu thiết bị muốn truyền dữ liệu, nó sẽ thêm thông tin và địa chỉ đích vào thẻ. Thẻ tiếp tục di chuyển vòng quanh cho đến khi tìm được thiết bị đích, dữ liệu sẽ được lấy ra khỏi thẻ. Ưu điểm của phương pháp này là không có đụng độ (no collisions) giữa những gói dữ liệu.

Có 2 loại mô hình vòng : vòng đơn và vòng kép

Single-Ring Topology

Mô hình vòng đơn, tất cả thiết bị trên mạng chia sẻ cùng 1 cáp đơn và dữ liệu lan truyền chỉ theo 1 hướng. Từng thiết bị sẽ đến lượt mình để gửi dữ liệu. Tuy nhiên mô hình vòng đơn có khuyết điểm là “single failure” có tính dự phòng kém

Mô hình vòng kép



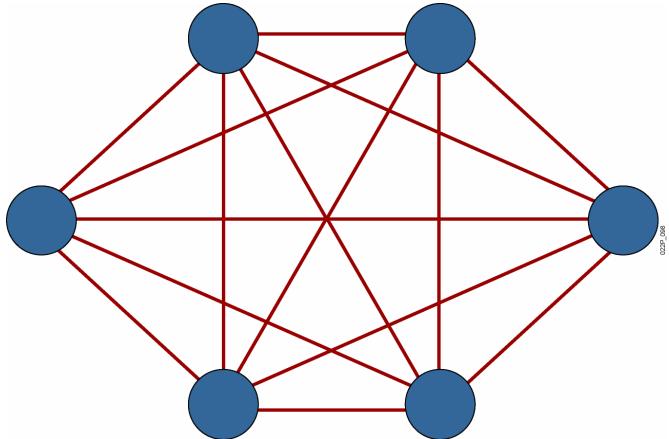
- Tín hiệu lan truyền theo 2 chiều ngược nhau
- mở rộng hơn mô hình vòng

Module 1-15

Dual-Ring Topology

Mô hình vòng kép, hai vòng cho phép dữ liệu được gửi theo cả 2 hướng. Mô hình này tạo ra tính dự phòng (redundancy), nghĩa là nếu 1 vòng hỏng thì dữ liệu vẫn có thể được truyền trên vòng kia

Mô hình lưới đầy đủ



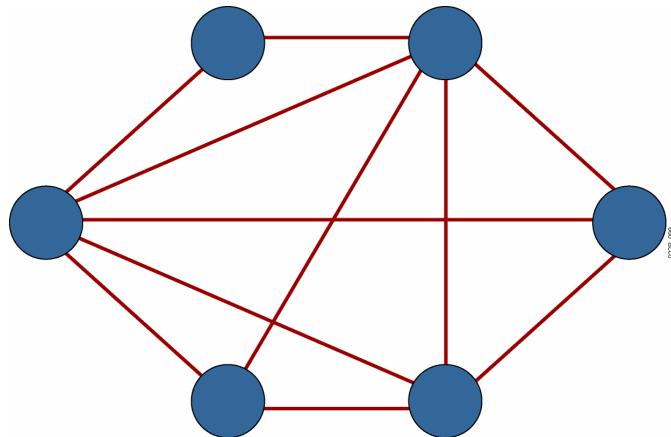
- Tính dự phòng cao
- Triển khai đắt tiền

Module 1-16

Full-Mesh Topology

Mô hình lưới đầy đủ kết nối mỗi điểm đến tất cả các điểm còn lại giúp hệ thống có tính dự phòng cao. Chi phí khi hiện thực mô hình này đắt và khó triển khai.

Mô hình lưới không đầy đủ

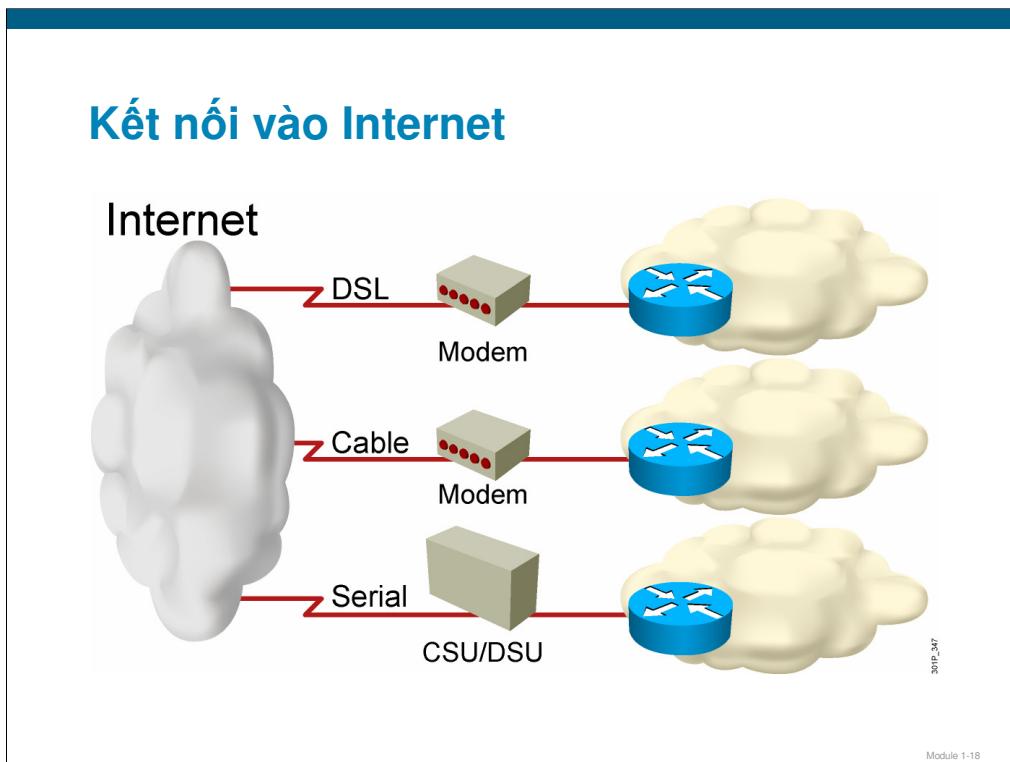


- Cân bằng giữa giá thành và tính dự phòng

Module 1-17

Partial-Mesh Topology

Mô hình lưới không đầy đủ, mỗi thiết bị kết nối đến một số các thiết bị khác nhưng không tồn tại tất cả các liên kết như mô hình lưới đầy đủ. Phương pháp này có chi phí thấp hơn mô hình lưới đầy đủ và cho phép nhà thiết kế mạng chọn lựa những điểm nút quan trọng để triển khai các kết nối phù hợp.



Có ba phương pháp kết nối internet phổ biến dùng cho các văn phòng nhỏ.

Sử dụng DSL trên cáp thoại có sẵn.

Sử dụng truyền hình Cáp (CATV).

Thuê bao đường truyền tuần tự (Serial link)

Nếu sử dụng DSL và truyền hình cáp, tín hiệu đến được kết thúc trên modem và được chuyển thành định dạng Ethernet.

Nếu sử dụng thuê bao đường truyền tuần tự tín hiệu sẽ được kết thúc trên CSU/DSU.

Trong cả 3 phương án đầu ra ethernet sẽ được gửi đến cho thiết bị định tuyến đóng vai trò như một thiết bị CPE (customer premises equipment).

Tóm tắt

- Mạng là một tập hợp được nối kết với nhau giữa thiết bị và máy tính. Mạng dùng vận chuyển dữ liệu với các phạm vi triển khai khác nhau bao gồm nhà ở, văn phòng nhỏ, và các công ty lớn.
- Có 4 loại thiết bị phần cứng hình thành nên mạng máy tính : PC, interconnections, switches, và routers
- Mạng được vẽ bởi 1 tập các biểu tượng chuẩn.
- Những tài nguyên chính được chia sẻ trên mạng bao gồm dữ liệu và ứng dụng, thiết bị ngoại vi, thiết bị lưu trữ & sao lưu.
- Những ứng dụng phổ biến của mạng bao gồm e-mail, web, chat, ứng dụng cộng tác và cơ sở dữ liệu.
- Ứng dụng ảnh hưởng đến mạng thông qua việc tiêu thụ tài nguyên mạng.

Module 1-19

Tóm tắt (tiếp theo).

- Các đặc trưng của mạng bao gồm : tốc độ, giá thành, bảo mật, khả dụng, khả năng mở rộng, tin cậy, và mô hình.
- Mô hình vật lý liên quan đến cách bố trí thiết bị và nối dây, trong khi mô hình luận lý mô tả cách thức tín hiệu lan truyền từ nguồn đến đích.
- Mô hình bus, một dây cáp đơn nối tất cả thiết bị.
- Mô hình sao, mỗi thiết bị được nối vào bộ tập trung bằng dây cáp riêng.
- Khi mô hình sao được mở rộng bằng cách nối vào thêm các bộ tập trung ta có mô hình sao mở rộng.

Module 1-20

Tóm tắt (tiếp theo).

- Mô hình vòng, tất cả các máy được nối thành 1 vòng. Trong mô hình vòng kép, có 2 vòng được tạo ra để dựng phòng mạng.
- Mô hình lưới đầy đủ mỗi thiết bị sẽ nối kết với tất cả phần còn lại; trong mô hình lưới không đầy đủ chỉ một số thiết bị nối với tất cả phần còn lại.
- Có ba phương pháp nối kết văn phòng nhỏ vào mạng internet : DSL sử dụng dây điện thoại, ti vi cáp, và thuê bao đường truyền tuần tự.

Module 1-21



Module 1-22

Bài 2: Bảo mật mạng



Xây dựng một mạng đơn giản

Module 2-1

Tổng quan

Một chiến lược an ninh mạng mạnh mẽ quan trọng như thế nào ? Năm 2005, tổ chức Computer Security Institute (CSI) trong báo cáo *2005 Computer Crime and Security Survey* cho ta thấy tổng quan về ảnh hưởng của tội phạm máy tính ở nước Mỹ. Một trong những tổ chức tham gia khảo sát là San Francisco Federal Bureau of Investigation (FBI) Computer Intrusion Squad. Dựa trên trả lời của hơn 700 chuyên viên an ninh mạng máy tính của các cơ quan chính phủ, tổ chức tài chính, viện y khoa, đại học, cuộc khảo sát khẳng định rằng nguy cơ từ tội phạm máy tính và các vi phạm về an ninh thông tin không hề giảm sút và các thiệt hại tài chính càng ngày càng tăng.

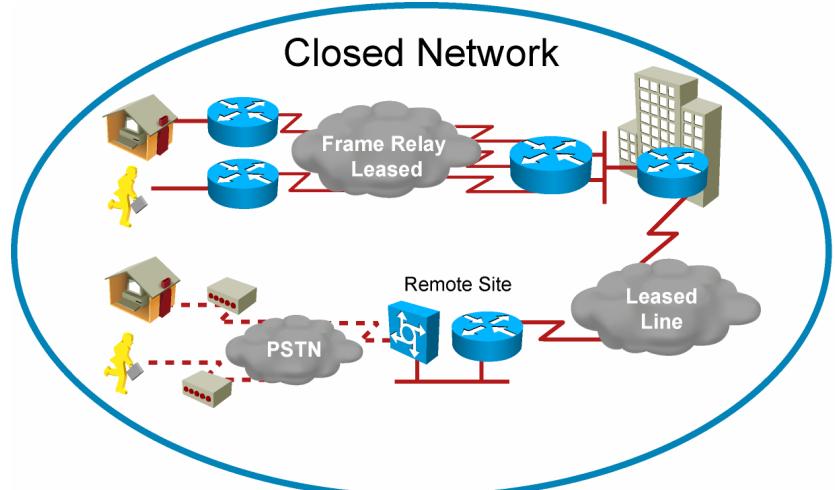
Ứng dụng và chiến lược an ninh hiệu quả là bước rất quan trọng để các tổ chức bảo vệ chính mình. Một chiến lược an ninh mạng hiệu quả là nền tảng cho tất cả các hoạt động nhằm đảm bảo khả năng bảo mật tài nguyên.

Mục tiêu

Kết thúc bài học này, học viên sẽ có thể giải thích được sự cần thiết của chiến lược an ninh mạng :

- Giải thích các công cụ tấn công tinh vi và mạng mở tao ra nhu cầu an ninh mạng cũng như nhu cầu về chiến lược an ninh động.
- Mô tả thách thức về sự cân bằng của an ninh mạng và hoạt động kinh doanh, các vấn đề hợp pháp, các chính sách của chính phủ.
- Mô tả đối thủ của an ninh mạng, động lực của hacker, và các loại tấn công
- Mô tả cách thức giảm bớt các nguy cơ thông thường trên routers và switches của Cisco.

Mạng đóng



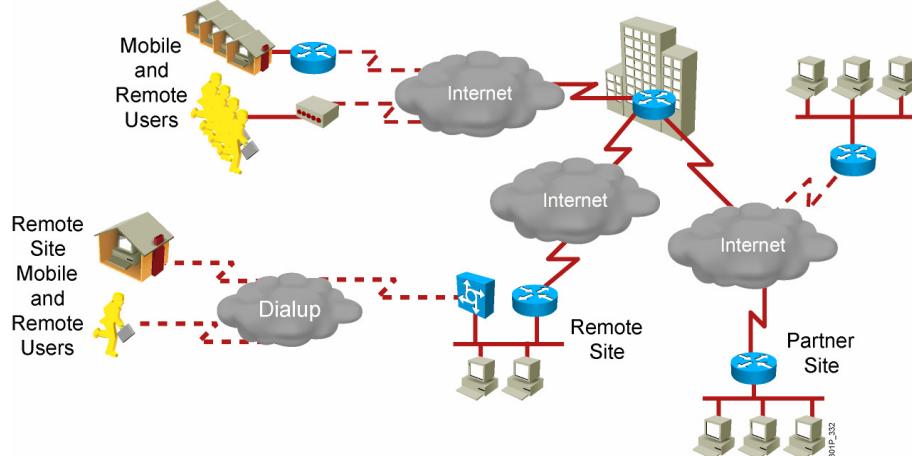
Tấn công từ bên trong vẫn là mối đe doạ

30/10/2011

Module 2-2

Cách thức đơn giản nhất để bảo vệ mạng máy tính khỏi các cuộc tấn công từ bên ngoài là đóng nó hoàn toàn đối với thế giới bên ngoài. Một mạng đóng chỉ cung cấp kết nối chỉ các đối tượng tin cậy không cho phép các kết nối đến mạng công cộng bên ngoài. Bởi vì không có kết nối ra bên ngoài, mạng được thiết kế theo cách thức này được xem là an toàn với các tấn công từ bên ngoài. Tuy nhiên, nó vẫn tồn tại nguy cơ bị tấn công từ phía bên trong. Theo thống kê của tổ chức CSI tại San Francisco, California, thì có từ 60-80% sử dụng sai là xuất phát từ bên trong.

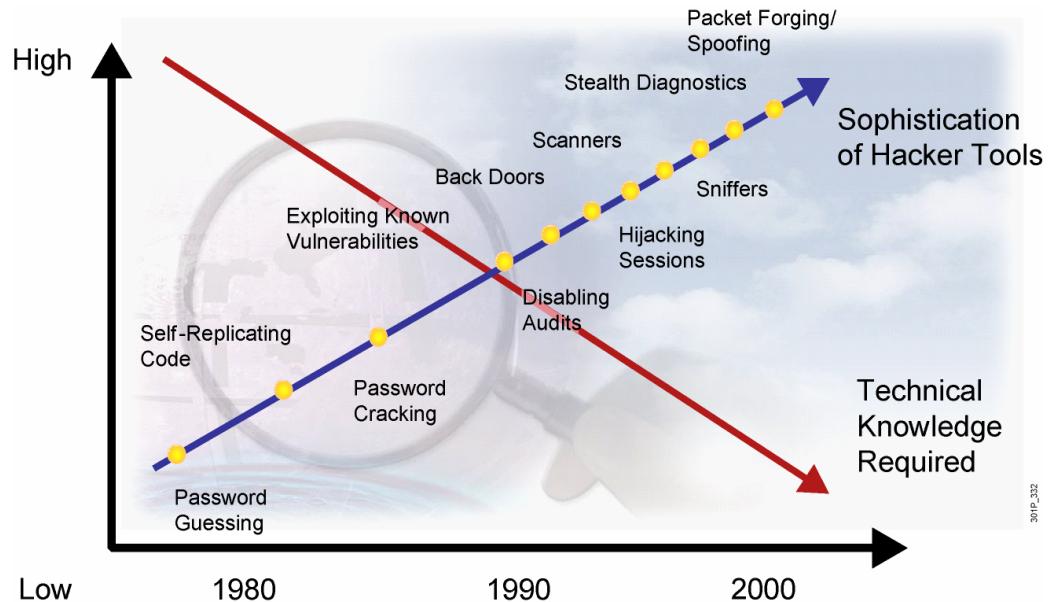
Mạng mở



Module 2-3

Ngày nay, các mạng máy tính đều có nhu cầu kết nối internet hoặc các mạng công cộng khác. Vì thế vấn đề bảo mật mạng mở trở nên cực kỳ quan trọng.

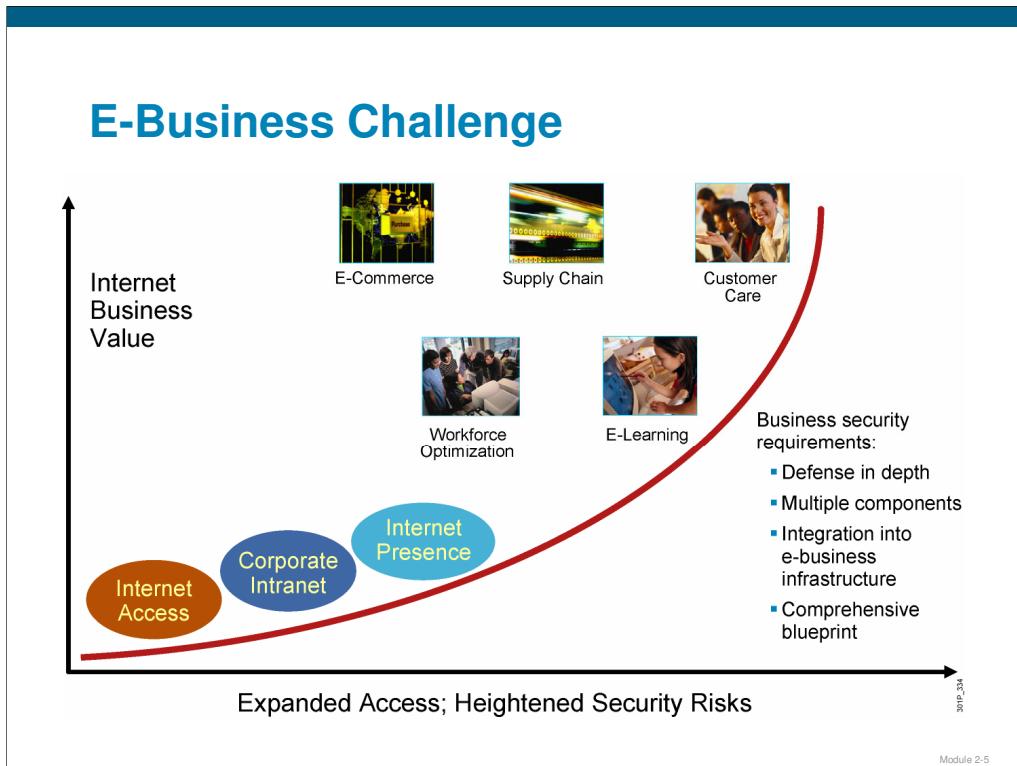
Nguy cơ tiềm tàng



Module 2-4

Các công cụ hack càng ngày càng tinh vi trong khi các kỹ năng cần thiết để sử dụng chúng càng lúc càng đơn giản kéo theo nguy cơ tấn công mạng mở trở nên phổ biến. Cùng với sự phát triển nhanh chóng về phạm vi và kích thước các mạng mở, nguy cơ về an ninh mạng cũng tăng một cách đáng kể.

Trong vòng 20 năm trở lại đây hacker có thể dễ dàng sử dụng các công cụ để tấn công hệ thống mà không cần có quá nhiều kiến thức về IT như trước đây. Chính điều đó làm cho việc bảo mật hệ thống trở nên khó khăn hơn.



Bảo mật tổng thể cần xem xét khả năng cân bằng giữa 2 mặt của vấn đề :

- Tính mở của mạng, hỗ trợ các yêu cầu trong kinh doanh và tự do thông tin
- Tính riêng tư của cá nhân và các thông tin kinh doanh chiến lược.

Bảo mật là mục tiêu hàng đầu trong công tác hiện thực và quản trị mạng. Các hoạt động kinh doanh đòi hỏi cung cấp các truy cập mở vào một số tài nguyên hệ thống (máy chủ web, mail ...) vì thế cần phải có biện pháp bảo mật dữ liệu và tài nguyên hiệu quả. Sự phát triển của thương mại điện tử (ebusiness) sẽ phát sinh nhu cầu truyền dữ liệu quan trọng trên nền mạng máy tính công cộng không an toàn vì thế cần một chính sách về an ninh mạng (network security policy) phù hợp.

Việc xây dựng chính sách an ninh mạng là bước đầu tiên để hướng đến mạng máy tính an toàn.

Mạng Internet ngày nay là một phương tiện hữu hiệu để các tổ chức, công ty xây dựng quan hệ tốt với khách hàng, nhà cung cấp, bạn hàng và nhân viên. Thương mại điện tử làm cho các công ty linh hoạt và cạnh tranh hơn, ưu điểm của thương mại điện tử là tạo ra các ứng dụng mới về thương mại, quản lý chuỗi nhà phân phối, chăm sóc khách hàng, tối ưu hóa lực lượng lao động và dạy học từ xa (e-learning). Những ứng dụng này giúp cải thiện công việc, giảm chi phí trong khi lại giảm thời gian quay vòng vốn và gia tăng sự hài lòng của khách hàng.

Khi người quản trị thực hiện mở cửa mạng máy tính của họ sẽ kéo theo gia tăng nguy cơ bị tấn công từ bên ngoài. Vì thế yêu cầu bảo mật sẽ gia tăng cùng với quá trình mở rộng chiến lược kinh doanh thương mại điện tử.

Đối thủ, động cơ và phân loại tấn công

Adversaries	Motivations	Classes of Attack
<ul style="list-style-type: none"> ▪ Nation-states ▪ Terrorists ▪ Criminals ▪ Hackers ▪ Crackers ▪ Competitors ▪ “Script kiddies” ▪ Disgruntled employees ▪ Government 	<ul style="list-style-type: none"> ▪ Intelligence ▪ Theft ▪ DoS ▪ Embarrassment ▪ Challenge 	<ul style="list-style-type: none"> ▪ Passive ▪ Active ▪ Close-in ▪ Insider ▪ Distributed

Module 2-7

Ba loại nguy cơ cho thông tin (information) và hệ thống thông tin (information systems) bao gồm :

• **Adversaries:** cho đến thập niên 80 đối thủ của bảo mật được biết với tên gọi chung là hacker. Đó là những người am hiểu sâu về mạng máy tính tìm ra những lỗ hổng hệ thống để thâm nhập trái phép. Theo thời gian dần xuất hiện thêm 1 thuật ngữ mới cracker dành cho nhóm người thâm nhập hệ thống với ý đồ xấu, tội phạm hoặc đánh cắp dữ liệu để trực lợi cho cá nhân mình. Hình thành nên 2 nhóm hacker mũ trắng “white hats” và mũ đen “black hats” để chỉ ra các cracker. Nhóm các cracker có ít kinh nghiệm được gọi là “script kiddies.” những đối thủ tiềm năng còn lại bao gồm khùng bô, tội phạm, đối thủ cạnh tranh ...

• **Adversary motivations:** động cơ của hacker có thể thử nghiệm khả năng của mình, đánh cắp dữ liệu, tấn công từ chối dịch vụ (DoS), motivations of adversaries may include intelligence gathering, theft of intellectual property, denial of service (DoS), gây khó khăn cho công ty, hoặc thử nghiệm để tìm ra các lỗ hổng.

• **Classes of attack:** Các loại tấn công bao gồm nghe lén thụ động trên đường truyền, tấn công chủ động vào mạng, tấn công dạng close-in, khai thác nội gián, tấn công phân tán những truy cập từ xa.

Hệ thống thông tin và mạng máy tính là những mục tiêu hấp dẫn cho hacker. Vì vậy, cần xây dựng chiến lược ngăn chặn càng nhiều loại tấn công càng tốt ngoài ra hệ thống cần có khả năng phục hồi lại nhanh chóng khi bị tấn công.

Có 5 loại tấn công

• **Passive:** Tấn công thụ động bao gồm phân tích luồng thông tin, theo dõi các giao tiếp không được bảo vệ, phá mã các dữ liệu có mức độ mật mã hóa kém, chiếm đoạt các thông tin chứng thực như username/password. Tấn công thụ động có thể đánh cắp số thẻ tín dụng, thông tin y tế mà cá nhân không hề hay biết .

- **Active:** Tấn công chủ động bao gồm việc cố gắng lừa đảo hoặc phá vỡ các chức năng bảo vệ như mã độc, đánh cắp hoặc chỉnh sửa lại thông tin. Những cuộc tấn công này nhắm vào mạng đường trực, khai thác thông tin được truyền ngang qua, hoặc tấn công vào một remote user được cấp quyền đang cố gắng truy cập vào hệ thống.
- **Close-in:** Cá nhân cố gắng đến gần các hệ thống, mạng máy tính hoặc các tiện nghi nhằm mục đích chỉnh sửa, thu thập hoặc từ chối truy cập thông tin.
- **Insider:** Các phần tử xấu bên trong tổ chức có thể tiến hành nghe lén, đánh cắp, hoặc phá hủy thông tin, sử dụng thông tin một cách gian dối, hoặc từ chối truy cập của những người dùng được cấp quyền.
- **Distributed:** tập trung vào việc thay đổi ác ý bằng cách thêm các mã độc (như backdoor, trojan horse) vào phần cứng hay phần mềm tại nhà máy hoặc trong quá trình phân phối nhằm mục đích nắm bắt quyền điều khiển thiết bị.

Các nguy cơ phổ biến

- Cài đặt phần cứng
 - Nguy cơ phần cứng
 - Nguy cơ môi trường
 - Nguy cơ điện
 - Nguy cơ bảo trì
- Do thám - tìm hiểu các thông tin về hệ thống mạng mục tiêu bằng các thông tin và chương trình ứng dụng
- Tấn công truy cập - tấn công vào mạng hoặc hệ thống với các lý do sau :
 - Lấy cắp thông tin
 - Dành quyền truy cập
 - Gia tăng quyền hạn
- Tấn công password - dùng công cụ để chiếm password

Module 2-9

Cài đặt thiết bị mạng không phù hợp hoặc không hoàn tất sẽ tạo ra các nguy cơ cho an ninh mạng, nếu không chú ý đến có thể dẫn đến những kết quả rất nghiêm trọng. Các phần mềm an ninh không thể một mình bảo đảm an toàn cho hệ thống với những lỗ hổng phần cứng. Phần này sẽ mô tả cách thức cơ bản để giảm thiểu nguy cơ trên các routers và switches của Cisco.

Cài đặt vật lý

• **Hardware threats:** nguy cơ phần cứng phá hỏng router và switch. Những thiết bị mạng quan trọng nên đặt trong phòng đấu dây thỏa các điều kiện tối thiểu sau :

- Phòng thiết bị trang bị khóa và chỉ người có thẩm quyền truy cập.
- Phòng thiết bị không thể chui vào qua trần nhà, sàn, cửa sổ ...
- Nếu có thể, sử dụng thiết bị khóa điện tử và được theo dõi bởi nhân viên an ninh.
- Nếu có thể nhân viên an ninh sẽ theo dõi truy cập từ xa thông qua camera tự động ghi hình.

• **Environmental threats:** nguy cơ về môi trường như nhiệt độ, độ ẩm (quá cao hay quá thấp). Những hoạt động giới hạn bót tác hại của môi trường

- Trang bị hệ thống điều hòa nhiệt độ và độ ẩm
- Loại bỏ các nguồn nhiễu điện từ và từ trường trong phòng.
- Nếu có thể trang bị các thiết bị cảm biến dùng cảnh báo nguy cơ của môi trường.

•**Electrical threats:** nguy cơ về điện, sụt áp, xung điện, nhiễu cảm ứng, công suất nguồn ... ảnh hưởng đến hoạt động của thiết bị để giảm thiểu ta cần lưu ý các biện pháp sau :

- Sử dụng UPS
- Trang bị máy phát điện dự phòng.
- Thường xuyên kiểm tra hoạt động của hệ thống dự phòng nguồn.
- Trang bị các nguồn dự phòng cho thiết bị quan trọng.
- Theo dõi và cảnh báo tham số nguồn.

•**Maintenance threats:** Nguy cơ do bảo dưỡng như phỏng tĩnh điện làm hư hỏng thiết bị điện tử, cáp hổng, thiêu vật tư dự phòng cho thiết bị quan trọng ...

- Dán nhãn đánh dấu rõ ràng tất cả thiết bị.
- Sử dụng hệ thống giá đỡ cáp.
- Tuân thủ quy định an toàn tiếp đất chống phỏng tĩnh điện.
- Để sẵn các vật tư dự phòng cho các thiết bị quan trọng.
- Luôn logoff ngay khi rời khỏi máy trạm dùng để cấu hình thiết bị.
- Không nên chỉ dựa vào khóa cửa để làm hệ thống an ninh duy nhất.

Reconnaissance Attacks

do thám là quá trình khảo sát ánh xạ các thiết bị, dịch vụ hoặc những điểm yếu kém của hệ thống. Do thám là bước đầu tiên để hacker tấn công hệ thống thông qua việc cố gắng thâm nhập hoặc tấn công DoS. Đầu tiên, hacker sẽ quét qua mạng để tìm các máy tính đang hoạt động. Sau đó hacker xác định các port đang hoạt động trên các PC này. Từ đó hacker xác định hệ điều hành, ứng dụng cũng như phiên bản của máy đích.

Quá trình do thám tương tự như tên ăn trộm làm như tìm ra những kẽ hở của ngôi nhà, cửa nào dễ mở, cửa sổ nào chưa đóng ... từ đó nó sẽ khai thác để đi vào nhà.

Access Attacks

Tấn công truy cập khai thác các điểm yếu trong dịch vụ chứng thực, FTP, web ... để truy cập trái phép vào hệ thống.

Password Attacks

Tấn công password liên quan đến việc liên tục cố gắng các định username hoặc password hoặc cả 2. Phương pháp phổ biến nhất là tấn công theo kiểu “brute-force.” ngoài ra còn có trojan horse, giả địa chỉ IP, và bắt packet.

Thực tế rủi ro an ninh chính là password được lưu trữ ở dạng bản rõ (cleartext), vì thế ta cần mã hóa password để khắc phục khuyết điểm này. Trên hầu hết các hệ thống, passwords được xử lý thông qua một thuật toán mật mã hóa sinh ra 1 số one-way hash (ta không thể chuyên đổi ngược lại giá trị bản rõ từ one-way hash) dựa trên passwords. Hầu hết hệ thống sử dụng giá trị hash này trong tiến trình chứng thực (authentication) bạn cung cấp account và password, hệ thống sẽ tính toán lại giá trị hash và so sánh nếu trùng khớp sẽ cho phép truy cập.

Giảm thiểu nguy cơ tấn công password

Những kỹ thuật cơ bản để giảm thiểu nguy cơ tấn công password bao gồm :

- Không cho phép người dùng sử dụng cùng password cho nhiều hệ thống.
- Vô hiệu hóa tài khoản sau một số lần login không thành công.
- Không dùng password dạng bản rõ.
- Sử dụng password “mạnh”; ví dụ “mY8!Rthd8y” thay cho “mybirthday.”

Module 2-11

Phương pháp giảm thiểu tấn công password bao gồm :

- Không sử dụng cùng password cho nhiều hệ thống.
- Vô hiệu (disable) các account sau một số lần login không thành công.
- Không dùng passwords dạng bản rõ. Sử dụng password dùng 1 lần one-time password (OTP) hoặc password đã mật mã.
- Sử dụng passwords mạnh (passwords bao gồm ít nhất 8 ký tự gồm chữ thường, chữ hoa, số và ký tự đặc biệt).

Tóm tắt

- Các công cụ tấn công tinh vi và mạng mở làm gia tăng sự cần thiết của các kiến trúc và chiến lược bảo mật để bảo vệ công ty trước các cuộc tấn công từ bên trong và ngoài.
- Công ty phải cân bằng giữa bảo mật mạng và tiến trình thương mại điện tử, vấn đề pháp lý, và các luật của chính quyền. Thiết lập chiến lược bảo mật là bước đầu tiên để chuyển mạng thành kiên trúc an ninh.
- Đội thủ của bảo mật mạng ngày càng xuất hiện dưới nhiều hình thức mức độ với những động cơ khác nhau.

Module 2-12

Tóm tắt (tiếp theo)

- Cần lưu ý đến vấn đề bảo mật cài đặt phần cứng đối với các thiết bị mạng của công ty.
- Giảm thiểu nguy cơ tấn công password bằng biện pháp :
 - Giới hạn sử dụng password
 - Vô hiệu hóa tài khoản sau một số lần login không thành công.
 - Không dùng password dạng bẩn rõ, Sử dụng password “mạnh”

Module 2-13



Module 2-14

Bài 3: Tìm hiểu về mô hình truyền thông từ máy đến máy



Xây dựng một mạng đơn giản

Module 3-1

Tổng quan

Mô hình Open Systems Interconnection (OSI) được tạo ra để giúp định nghĩa cách thức hoạt động của mạng một cách tổng quát, bao gồm các thành phần của mạng và phương thức truyền dữ liệu. Hiểu được kiến trúc và mục đích của mô hình OSI là điểm chính yếu để nắm bắt được các thức truyền thông giữa các máy tính trên mạng. Bài học này giới thiệu mô hình OSI và mô tả các lớp của nó.

Mục tiêu

Kết thúc bài này học viên sẽ có khả năng mô tả các lớp của mô hình và mô tả cách thức phân loại thiết bị và chức năng của chúng theo lớp OSI tương ứng :

- Xác định các yêu cầu của mô hình truyền thông từ máy đến máy
- Định nghĩa mục tiêu của mô hình tham khảo OSI
- Định nghĩa đặc trưng, chức năng, và mục đích của mỗi lớp trong mô hình OSI
- Mô tả quá trình đóng gói và giải đóng gói
- Mô tả cách thức hoạt động truyền thông ngang hàng
- Liệt kê mục tiêu và chức năng của mô hình TCP/IP trong truyền thông dữ liệu

Tìm hiểu về truyền thông máy đến máy



- Mô hình cũ
 - độc quyền (Proprietary)
 - Phần mềm ứng dụng & truyền thông do cùng 1 nhà sản xuất
- Mô hình dựa theo chuẩn
 - Phần mềm do nhiều nhà cung cấp
 - Dựa theo phương pháp phân lớp

Module 3-2

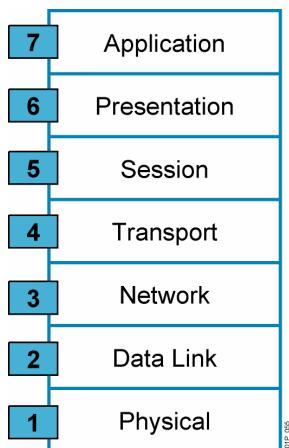
Truyền thông máy đến máy yêu cầu mô hình thống nhất giải quyết các vấn đề từ phần cứng, phần mềm, các thức truyền dữ liệu. Phần này giải thích về loại mô hình này.

Trước kia việc phát triển mạng mang tính độc quyền mỗi nhà phát triển tự xây dựng lấy ứng dụng và các phần mềm truyền thông. Khả năng giao tiếp các hệ thống khác nhau này rất khó thực hiện.

Sự phát triển của công nghệ và sự mở rộng kinh doanh đòi hỏi phải tách biệt phần mềm ứng dụng và phần mềm truyền thông. Việc tách biệt này cho phép nâng cấp các phương tiện truyền thông mới mà không cần phải xây dựng lại phần mềm ứng dụng.

Giải pháp phân các chia lớp có giao tiếp chuẩn cho phép nhiều nhà phát triển cùng tham gia xây dựng hệ thống mạng.

Tại sao mô hình mạng phân lớp



- Giảm độ phức tạp
- Chuẩn hóa giao tiếp
- Thuận tiện trong việc module hoá
- Đảm bảo tính tương tác kỹ thuật
- Tăng tốc phát triển
- Đơn giản hóa việc dạy và học

Module 3-3

Đầu thập niên 80 các công ty nhận thấy lợi ích của mạng máy tính đem lại. Từ đó hình thành rất nhiều mô hình mạng khác nhau. Đến giữa thập niên 80 người ta bắt đầu nhận thấy các khó khăn, bất lợi trong việc truyền thông giữa các mạng có đặc tả khác nhau. Các công ty cảm thấy cần thiết phải tránh xây dựng các hệ thống mạng máy tính độc quyền, từ đó xuất hiện nhu cầu xây dựng hệ thống mạng mở.

Để giải quyết các vấn đề không tương thích của các mạng máy tính hiện hữu, tổ chức ISO đã tiến hành nghiên cứu các mô hình mạng nhằm tạo ra một mô hình thống nhất có khả năng tương thích giữa các sản phẩm của nhiều nhà cung cấp khác nhau.

Vào năm 1984 mô hình OSI ra đời từ kết quả nghiên cứu của tổ chức ISO. Mô hình OSI cung cấp cho các nhà sản xuất một tập các chuẩn đảm bảo tính tương thích và khả năng tương tác giữa những kỹ thuật mạng máy tính do các công ty khác nhau trên khắp thế giới. Mặc dù vẫn tồn tại một số mô hình mạng khác nhưng chúng đều được qui về mô hình OSI làm chuẩn.

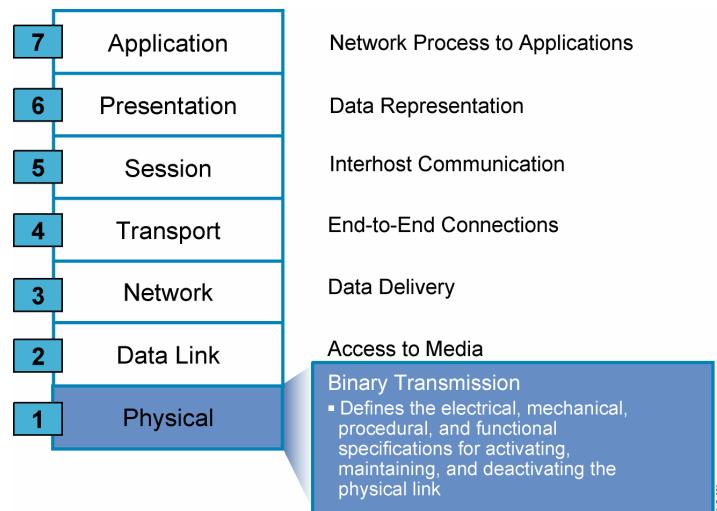
Mô hình OSI được xem là công cụ tốt nhất giảng dạy cách thức dữ liệu được gửi và nhận trên mạng máy tính.

Mô hình OSI được chia thành 7 lớp. Trong đó mỗi lớp đóng 1 vai trò và chức năng cụ thể của mạng máy tính. Quan trọng hơn mô hình OSI chỉ cho chúng ta thấy làm cách nào mà thông tin được lan truyền thông qua hệ thống mạng từ nơi này đến nơi khác. Ví dụ như làm thế nào để dữ liệu trong tập tin excel được truyền từ chương trình ứng dụng trên máy tính này sang máy tính khác ngay cả khi 2 máy này không cùng môi trường truyền dẫn.

Các ưu điểm chính của mô hình OSI :

- Giảm độ phức tạp** : mô hình OSI chia hệ thống thành các phần nhỏ và đơn giản.
- Chuẩn hóa giao tiếp** : mô hình OSI chuẩn hóa các thành phần mạng máy tính cho phép nhiều nhà cung cấp cùng tham gia phát triển và hỗ trợ.
- Thuận tiện trong việc module hóa** : mô hình OSI cho phép các sản phẩm phần cứng, phần mềm của những công ty giao tiếp được với nhau.
- Đảm bảo tính tương tác kỹ thuật** : mô hình OSI ngăn cản sự thay đổi trong 1 lớp ảnh hưởng đến lớp khác, điều đó cho phép khả năng phát triển nhanh hơn.
- Tăng tốc phát triển** : mô hình OSI cung cấp khả năng cải thiện từng phần của hệ thống mà không cần phải xây dựng lại toàn bộ.
- Đơn giản hóa việc dạy và học** : mô hình OSI chia nhỏ hệ thống thành các phần đơn giản hơn để học tập.

Bảy lớp của mô hình OSI



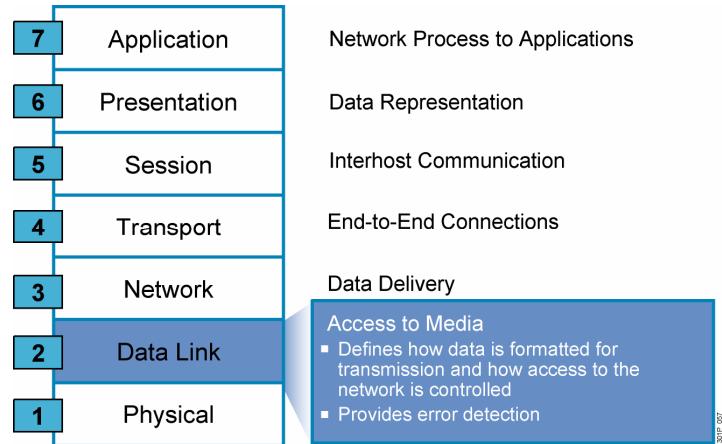
Module 3-5

Lớp 1: lớp vật lý

Đặc tả thành phần cơ khí, điện tử, thủ tục và chức năng để kích hoạt, duy trì và kết thúc các kết nối vật lý giữa các thiết bị đầu cuối.

Bao gồm các đặc tính như điện áp, định thời gian chuyển đổi điện áp, tốc độ truyền dữ liệu vật lý, khoảng cách tối đa, đầu nối ...

Bảy lớp của mô hình OSI (tiếp theo)

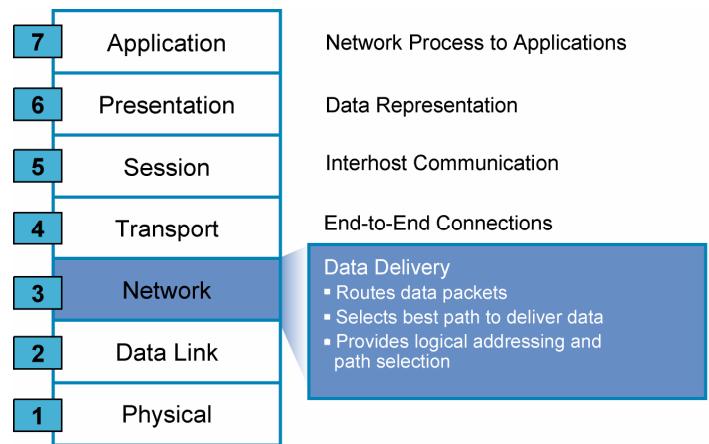


Module 3-6

Lớp 2 : Lớp liên kết dữ liệu

định nghĩa cách thức định dạng dữ liệu cho việc truyền thông và phương pháp truy cập lớp vật lý. Lớp này thường bao gồm cả cơ chế phát hiện lỗi để đảm bảo khả năng tin cậy trong phân phối dữ liệu.

Bảy lớp của mô hình OSI (tiếp theo)

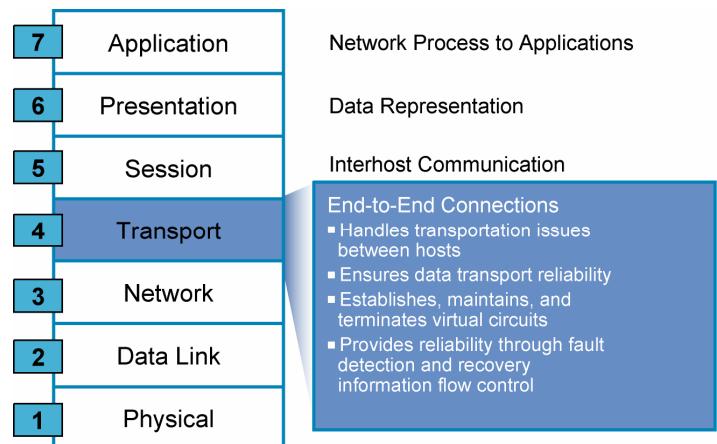


Module 3-7

Lớp 3: Lớp mạng

Cung cấp kết nối và cách chọn đường đi giữa 2 máy bất kỳ trên hệ thống mạng máy tính. Cùng với sự phát triển của Internet số lượng người dùng mạng và nhu cầu truy cập dữ liệu trên khắp thế giới tăng lên mạnh mẽ, lớp mạng giúp đảm bảo việc truyền thông giữa các máy thực hiện nhanh chóng.

Bảy lớp của mô hình OSI (tiếp theo)



Module 3-8

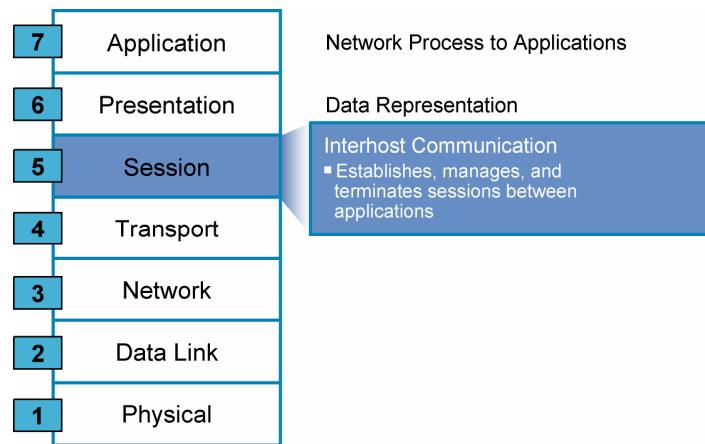
Lớp 4 : Lớp vận chuyển

Phân chia dữ liệu trên máy gửi thành các khối dữ liệu chuẩn cũng như đảm nhận việc lắp ghép các khối này thành dòng dữ liệu ở máy nhận. Ví dụ ta cần gửi 1 tập tin kích thước lớn từ văn phòng chính của công ty đến 1 chi nhánh ở xa, vấn đề đảm bảo dữ liệu được truyền đến đầu cuối chính xác rất quan trọng, để làm điều đó lớp vận chuyển chia nhỏ tập tin thành các đoạn nhỏ và gửi chúng đi, đoạn nào bị hư hỏng sẽ được gửi lại thay vì ta phải gửi lại toàn bộ tập tin lớn ban đầu.

Biên giới giữa lớp phiên và lớp vận chuyển có thể hiểu như là giữa giao thức ứng dụng và giao thức dòng dữ liệu. Trong khi 3 lớp trên cùng của mô hình OSI quan tâm đến các vấn đề về ứng dụng, 4 lớp thấp nhất quan tâm đến các vấn đề vận chuyển dữ liệu.

Lớp vận chuyển bảo vệ các lớp trên của mô hình OSI khỏi việc chi tiết hóa quá trình vận chuyển dữ liệu. Đặc biệt vấn đề làm sao đảm bảo đường truyền tin cậy giữa 2 máy tính. Để thực hiện điều đó lớp vận chuyển tiến hành thiết lập, duy trì và kết thúc các mạch ảo (virtual circuit), phát hiện và khôi phục các lỗi cũng như điều tiết tốc độ truyền tin nhằm cung cấp 1 dịch vụ vận chuyển tin cậy.

Bảy lớp của mô hình OSI (tiếp theo)

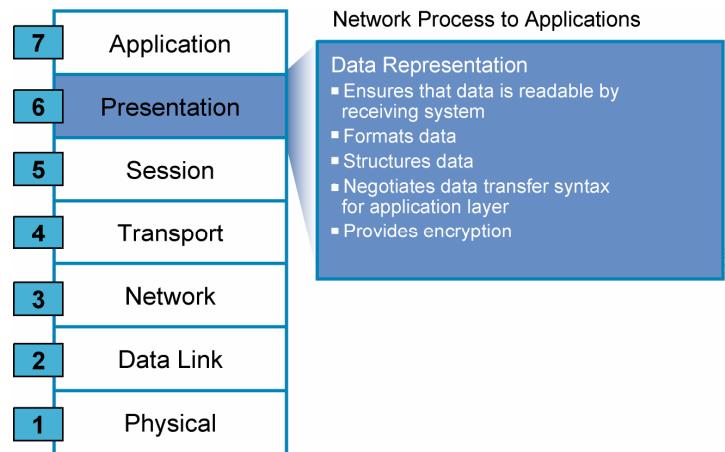


Module 3-9

Lớp 5: Lớp phiên

Thiết lập, quản lý, kết thúc phiên làm việc truyền thông giữa 2 máy. Lớp này cũng đảm nhận vai trò đồng bộ quá trình hội thoại cũng như quá trình trao đổi thông tin giữa lớp trình diễn trên 2 máy. Ví dụ máy chủ web có nhiều người sử dụng vì thế có nhiều tiến trình truyền thông cùng mở ra ở 1 thời điểm. Vấn đề của lớp phiên là làm thế nào để quản lý mỗi người dùng sẽ sử dụng đường dẫn nào. Ngoài ra lớp phiên còn cung cấp cho ta khả năng truyền dữ liệu hiệu quả, phân loại dịch vụ, báo cáo các ngoại lệ xảy ra nếu có.

Bảy lớp của mô hình OSI (tiếp theo)

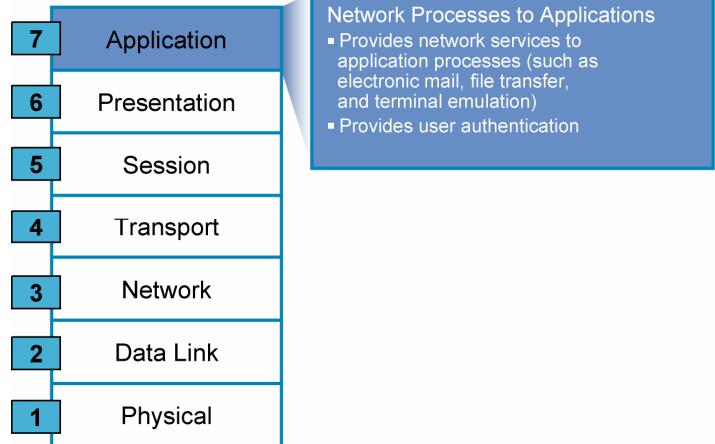


Module 3-10

Lớp 6: Lớp trình diễn

Đảm bảo thông tin gửi từ lớp ứng dụng của máy gửi có thể được hiểu chính xác ở lớp ứng dụng ở máy nhận. Ví dụ máy tính gửi sử dụng bộ mã ký tự EBCDIC trong khi máy nhận sử dụng bộ mã ASCII nhưng vẫn thể hiện chính xác cùng ký tự cần biểu diễn. Nếu cần thiết lớp trình diễn sẽ thực hiện quá trình thông dịch giữa các định dạng dữ liệu nhằm đảm bảo tính chính xác về thông tin biểu diễn.

Bảy lớp của mô hình OSI (tiếp theo)

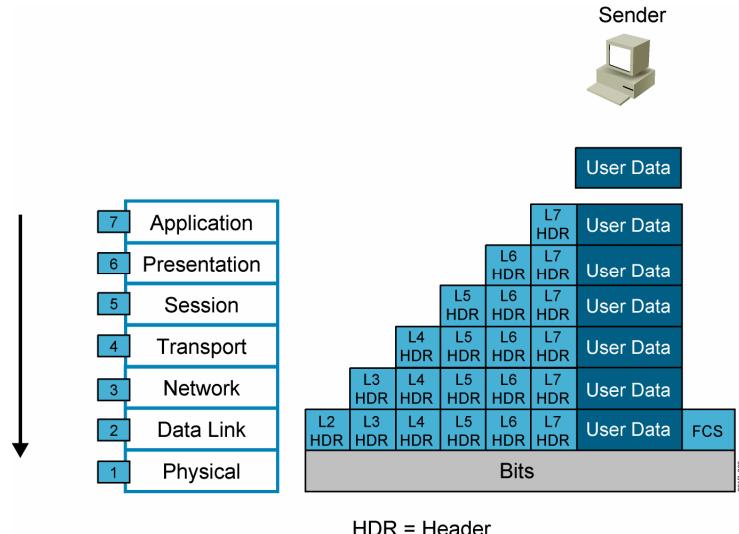


Module 3-11

Lớp 7: Lớp ứng dụng

Là lớp gần với người dùng nhất, lớp ứng dụng cung cấp dịch vụ cho các chương trình ứng dụng (ví dụ thư điện tử, truyền tập tin, web ...). Lớp ứng dụng không cung cấp dịch vụ cho bất kỳ lớp nào khác của mô hình OSI mà cung cấp dịch vụ cho các ứng dụng bên ngoài mô hình. Lớp ứng dụng thiết lập, đồng bộ, khôi phục dữ liệu và điều khiển tính toàn vẹn dữ liệu giữa ứng dụng trên hai máy tính.

Đóng gói dữ liệu



Module 3-12

Thông tin truyền trên mạng phải trải qua quá trình chuyển đổi ở cả 2 đầu truyền thông. Quá trình chuyển đổi này được gọi là đóng gói (encapsulation) và giải đóng gói (de-encapsulation) dữ liệu.

Đóng gói dữ liệu

Thông tin được gửi trên mạng được gọi là gói dữ liệu. Nếu một máy tính muốn gửi dữ liệu cho một máy khác, dữ liệu này phải được đặt vào một khung trong một tiến trình gọi là đóng gói dữ liệu. Quá trình đóng gói thực hiện bao phủ bên ngoài dữ liệu các thông tin giao thức cần thiết trước khi truyền trên mạng. Trong quá trình dữ liệu di chuyển xuống lớp dưới của mô hình OSI, mỗi lớp sẽ thêm vào các thông tin header (có thể có trailer) vào dữ liệu trước khi chuyển nó cho lớp bên dưới. Các header và trailers này chứa đựng thông tin điều khiển dành cho thiết bị mạng và máy nhận nhằm đảm bảo việc phân phối dữ liệu được chính xác.

Hình trên mô tả quá trình đóng gói dữ liệu tiến hành qua các lớp :

Bước 1 dữ liệu người dùng được gửi từ chương trình ứng dụng đến lớp ứng dụng.

Bước 2 lớp ứng dụng thêm vào dữ liệu thông tin header của lớp 7. header lớp 7 và dữ liệu gốc của người dùng được chuyển xuống lớp 6.

Bước 3 lớp trình diễn tiếp tục thêm vào thông tin header của lớp 6 và chuyển xuống lớp 5.

Bước 4 lớp phiên tiếp tục thêm vào thông tin header của lớp 5 và chuyển xuống lớp 4.

Bước 5 lớp vận chuyển tiếp tục thêm vào thông tin header của lớp 4 và chuyển xuống lớp 3.

Bước 6 lớp mạng tiếp tục thêm vào thông tin header của lớp 2 và chuyển xuống lớp 2.

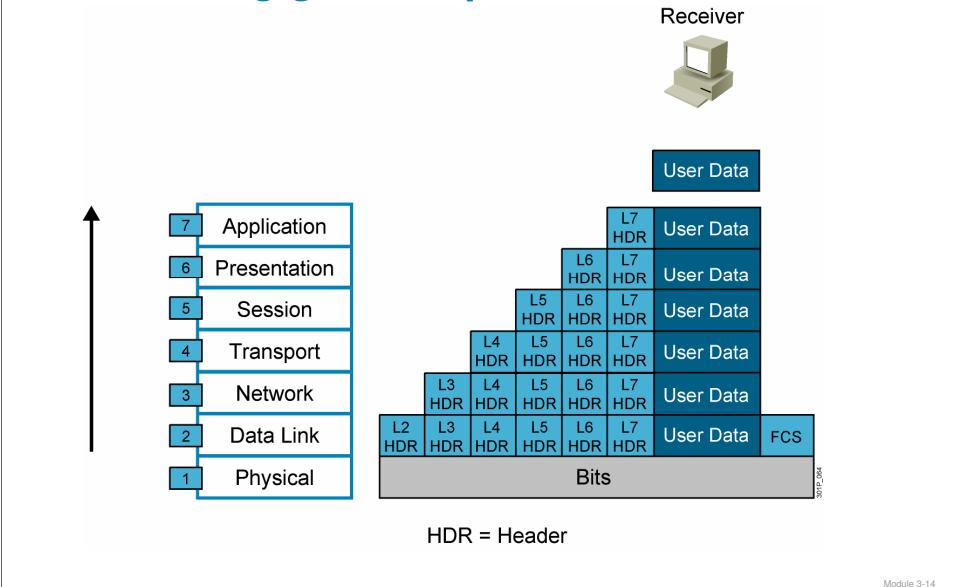
Bước 7 lớp liên kết dữ liệu tiếp tục thêm vào thông tin header và trailer của lớp 2. Trailer của lớp 2 thường là FCS, nó được dùng để phát hiện dữ liệu bị lỗi.

Bước 8 lớp vật lý phát dữ liệu dưới dạng các bit trên môi trường truyền.

Ví dụ gửi bưu phẩm qua dịch vụ phát chuyển hàng

Quá trình đóng gói dữ liệu tương tự như việc gửi bưu kiện đi. Trước tiên bưu phẩm được đóng gói vào một thùng chứa. Kế đến bạn viết địa chỉ cần gửi đến ở bên ngoài kiện hàng. Sau đó bạn chuyển bưu kiện đó đến dịch vụ phát chuyển hàng để gửi đi.

Giải đóng gói dữ liệu



Giải đóng gói dữ liệu

Khi máy đầu cuối nhận được chuỗi các bit, lớp vật lý sẽ chuyển chúng cho lớp liên kết dữ liệu để xử lý :

Bước 1 Lớp liên kết dữ liệu kiểm tra FCS để xem có lỗi dữ liệu hay không.

Bước 2 Nếu có lỗi dữ liệu, nó sẽ bị loại bỏ, và lớp liên kết dữ liệu sẽ yêu cầu gửi lại.

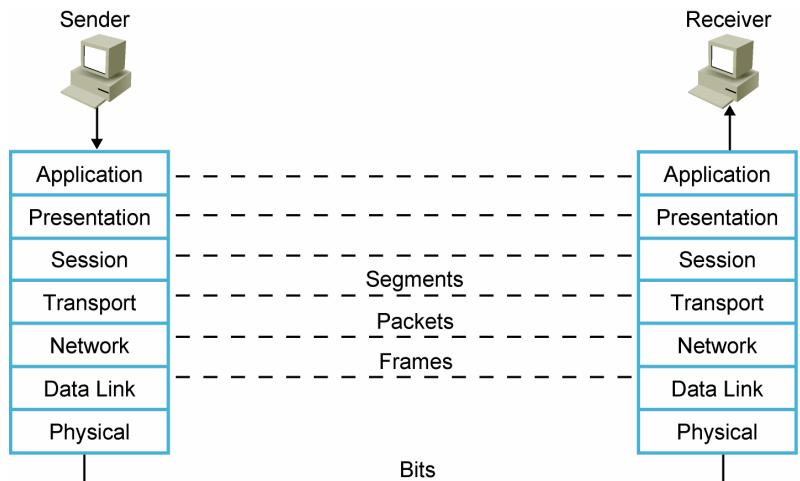
Bước 3 Nếu không có lỗi dữ liệu, lớp liên kết dữ liệu đọc và thông dịch các thông tin điều khiển trong header của dữ liệu nhận được.

Bước 4 Lớp liên kết dữ liệu sẽ tháo bỏ phần header & trailer của dữ liệu lớp 2, sau đó căn cứ theo thông tin điều khiển trong header của dữ liệu lớp 2 để chuyển chúng cho lớp mạng bên trên.

Ví dụ : nhận bưu phẩm qua dịch vụ phát chuyển hàng

Quá trình giải đóng gói tương tự các giai đoạn nhận bưu phẩm. Đầu tiên địa chỉ trên mỗi kiện hàng sẽ được đọc xem có phải gửi cho bạn hay không, nếu trùng với địa chỉ của bạn kiện hàng sẽ được tháo ra để lấy bưu phẩm bên trong.

Truyền thông ngang hàng



Để gói dữ liệu có thể chuyển từ nguồn đến đích mỗi lớp của mô hình OSI ở nguồn phải truyền thông với lớp tương ứng ở đích đến. Trong truyền thông ngang hàng, các giao thức ở mỗi lớp sẽ trao đổi các khối dữ liệu được gọi là đơn vị dữ liệu giao thức (PDUs) giữa các lớp ngang hàng.

Mỗi lớp của mô hình OSI sẽ dựa vào dịch vụ được cung cấp bởi lớp bên dưới. Để phục vụ các dịch vụ này lớp dưới sử dụng quá trình đóng gói dữ liệu để bổ sung các header cần thiết điều khiển chức năng của lớp tương ứng. Khi dữ liệu di chuyển từ lớp 7 xuống đến lớp 2 các header sẽ được thêm vào dần dần.

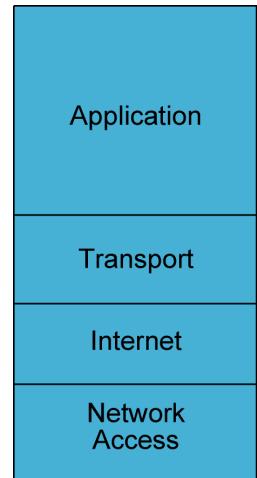
Lớp mạng chuyển dữ liệu thông qua mạng Internet bằng cách đóng gói dữ liệu với các header của gói dữ liệu (packet đơn vị dữ liệu giao thức của lớp 3). Header chứa đựng các thông tin cần thiết để hoàn tất việc truyền dữ liệu ví dụ như địa chỉ luận lý nguồn, đích.

Lớp liên kết dữ liệu cung cấp dịch vụ cho lớp mạng bằng cách đóng gói những gói dữ liệu vào các khung (Frame đơn vị dữ liệu giao thức của lớp 2). Header của khung chứa đựng địa chỉ vật lý cần thiết để xử lý các chức năng của lớp 2, và trailer của khung chứa FCS để phát hiện lỗi của khung nếu có.

Lớp vật lý cung cấp dịch vụ cho lớp liên kết dữ liệu, mã hóa các khung dữ liệu thành các mẫu nhị phân 1 0 và truyền chúng trên môi trường truyền dẫn.

Mô hình TCP/IP

- Bao gồm 4 lớp
- Dùng tên khác từ lớp 1 đến lớp 3
- Ghép lớp 5 đến 7 thành 1 lớp duy nhất



Module 3-16

Mô hình TCP/IP tên được ghép từ 2 giao thức Transmission Control Protocol (TCP) và Internet Protocol (IP) cũng được chia thành lớp, mỗi lớp thực hiện những chức năng đặc biệt trong tiến trình truyền thông.

Mô hình TCP/IP được phát triển gần như cùng thời với mô hình OSI. Tương tự OSI, mô hình TCP/IP cũng được xây dựng theo kiến trúc phân lớp :

• **Lớp truy cập mạng :** lớp này tương ứng với 2 lớp thấp nhất của mô hình OSI

• **Lớp vật lý :** Đặc tả thành phần cơ khí, điện tử, thủ tục và chức năng để kích hoạt, duy trì và kết thúc các kết nối vật lý giữa các thiết bị đầu cuối. Bao gồm các đặc tính như điện áp, định thời gian chuyển đổi điện áp, tốc độ truyền dữ liệu vật lý, khoảng cách tối đa, đầu nối ...

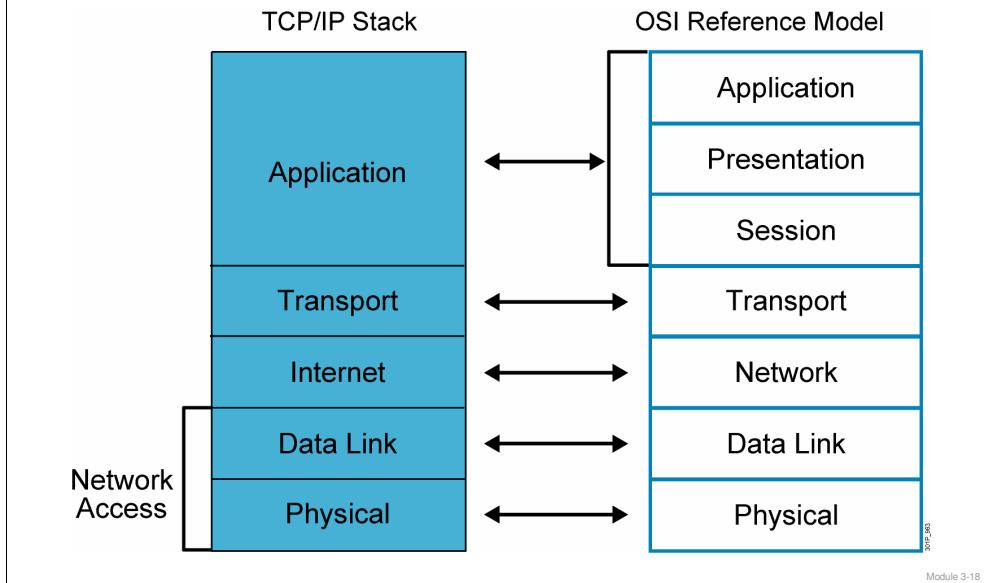
• **Lớp liên kết dữ liệu :** định nghĩa cách thức định dạng dữ liệu cho việc truyền thông và phương pháp truy cập lớp vật lý. Lớp này thường bao gồm cả cơ chế phát hiện lỗi để đảm bảo khả năng tin cậy trong phân phối dữ liệu.

• **Lớp Internet :** lớp này cung cấp khả năng định tuyến dữ liệu từ nguồn đến đích bằng cách định nghĩa gói dữ liệu và hệ thống địa chỉ.

• **Lớp vận chuyển :** lớp này đóng vai trò cốt lõi của mô hình TCP/IP, nó cung cấp dịch vụ truyền thông trực tiếp cho lớp ứng dụng.

- **Lớp ứng dụng :** lớp này cung cấp dịch vụ cho các chương trình ứng dụng như truyền tập tin, tìm và sửa lỗi mạng, các hoạt động liên quan đến mạng internet, hỗ trợ kiến trúc API cho phép lập trình truy cập vào các dịch vụ mạng.

So sánh mô hình TCP/IP và OSI



Cả 2 mô hình OSI và TCP/IP tuy được phát triển bởi những tổ chức khác nhau nhưng chúng được xây dựng gần như cùng một lúc, được sử dụng như công cụ để triển khai hệ thống mạng truyền thông dữ liệu.

- Lớp truy cập mạng của mô hình TCP/IP tương ứng với 2 lớp vật lý và liên kết dữ liệu của mô hình OSI.
- Lớp Internet của mô hình TCP/IP tương ứng với lớp mạng của mô hình OSI liên quan đến địa chỉ và cách định tuyến giữa 2 thiết bị mạng.
- Lớp vận chuyển của mô hình TCP/IP tương tự mô hình OSI, cung cấp phương tiện cho phép nhiều ứng dụng trên máy tính truy cập lớp theo phương thức best-effort hoặc tin cậy.
- Lớp ứng dụng của mô hình TCP/IP bao gồm chức năng của 3 lớp trên cùng của mô hình OSI.

Tóm tắt

- Mô hình tham khảo OSI định nghĩa chức năng mạng ở mỗi lớp.
- Lớp vật lý đặc tả thành phần cơ khí, điện tử, thủ tục và chức năng để kích hoạt, duy trì và kết thúc các kết nối vật lý giữa các thiết bị đầu cuối.
- Lớp liên kết dữ liệu định nghĩa cách thức định dạng dữ liệu cho việc truyền thông và phương pháp truy cập lớp vật lý.
- Lớp mạng cung cấp kết nối và cách chọn đường đi giữa 2 máy bất kỳ trên hệ thống mạng máy tính

Module 3-19

Tóm tắt (tiếp theo)

- Lớp vận chuyển phân chia dữ liệu trên máy gửi thành các khối dữ liệu chuẩn cũng như đảm nhận việc lắp ghép các khối này thành dòng dữ liệu ở máy nhận.
- Lớp phiên thiết lập, quản lý, kết thúc phiên làm việc truyền thông giữa 2 máy.
- Lớp trình diễn Đảm bảo thông tin gửi từ lớp ứng dụng của máy gửi có thể được hiểu chính xác ở lớp ứng dụng ở máy nhận.
- Lớp ứng dụng là lớp gần với người dùng nhất, lớp ứng dụng cung cấp cho các chương trình ứng dụng (ví dụ thư điện tử, truyền tập tin, web ...).

Module 3-20

Tóm tắt (tiếp theo)

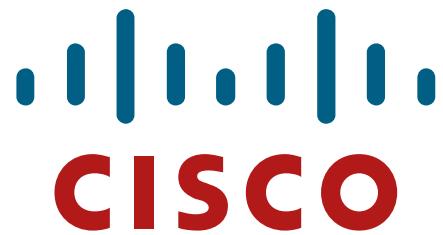
- Thông tin gửi trên mạng được xem là dữ liệu hay gói dữ liệu (data packet). Nếu một máy tính muốn gửi dữ liệu cho một máy khác, dữ liệu trước hết phải được đóng gói lại.
- Khi thiết bị từ xa nhận được chuỗi bit, lớp phần cứng ở thiết bị từ xa đó chuyển các bit lên lớp liên kết dữ liệu để xử lý. Tiến trình này gọi là giải đóng gói.

Module 3-21

Tóm tắt (tiếp theo)

- Ngày nay mô hình TCP/IP được sử dụng phổ biến vì một số nguyên nhân bao gồm cơ chế địa chỉ mềm dẻo, dùng được trên nhiều loại hệ điều hành và máy khác nhau, có nhiều công cụ và tiện ích, và bắt buộc phải dùng để vào mạng Internet.
- Các thành phần của mô hình TCP/IP bao gồm lớp truy cập mạng, lớp Internet, lớp vận chuyển, và lớp ứng dụng
- Mô hình OSI và TCP/IP tương tự nhau về cấu trúc và chức năng, sự tương quan giữa các lớp vật lý, liên kết dữ liệu, mạng, vận chuyển. Mô hình OSI chia lớp ứng dụng thành 3 lớp khác nhau.

Module 3-22



Module 3-23

Bài 4: Tìm hiểu lớp Internet của mô hình TCP/IP



Xây dựng một mạng đơn giản

Module 4-1

Tổng quan

Có nhiều vấn đề liên quan đến địa chỉ IP bao gồm tính toán xây dựng địa chỉ IP, phân lớp địa IP cho các mục đích định tuyến đặc biệt, địa chỉ IP công cộng (public IP addresses) và địa chỉ IP riêng (private IP addresses). Ngoài ra còn có 2 loại địa chỉ IP là IPv4 và IPv6. Địa chỉ IPv4 là số nguyên 32-bit hiện nay được dùng phổ biến nhất, nhưng địa chỉ IPv6 với 128-bit dần sẽ được thay thế trong tương lai. Bài này tập trung vào mô tả địa chỉ IPv4.

Làm thế nào để hệ thống đầu cuối nhận được địa chỉ IP của nó? Chúng ta có thể gán tĩnh địa chỉ IP tuy nhiên cách này bị giới hạn ở tính mở rộng kém, chi phí duy trì cao. Vì thế các giao thức cấp địa chỉ IP động được phát triển. Bài học này mô tả chức năng của địa chỉ IP.

Mục tiêu

Kết thúc bài học này học viên có khả năng liệt kê trình tự mà giao thức IP dùng để quản trị địa chỉ IP và ánh xạ giữa địa chỉ IP và địa chỉ MAC

- Liệt kê các đặc trưng của giao thức IP
- Mô tả các thành phần của địa chỉ IPv4
- Mô tả cấu trúc địa chỉ IPv4
- Mô tả các lớp của địa chỉ IP
- Mô tả các địa chỉ IP dành riêng
- So sánh địa chỉ công cộng và địa chỉ riêng
- Mô tả chức năng của DHCP khi cấp địa chỉ IP.

Đặc trưng của giao thức Internet

- Hoạt động ở lớp mạng của mô hình OSI
- Giao thức không kết nối
- Gói tin được xử lý độc lập
- Địa chỉ phân cấp
- Phân phối theo dạng nỗ lực tối đa
- Không có chức năng khôi phục dữ liệu

Module 4-2

IP là thành phần của mô hình TCP/IP có nhiệm vụ dựa trên địa chỉ đích của định tuyến các gói tin, và IP có các đặc trưng liên quan để thực hiện chức năng này.

Gói dữ liệu được sử dụng để mang thông tin trên mạng. Mỗi gói là một thực thể độc lập có chứa đầy đủ thông tin cho phép các thiết bị mạng chuyển chúng từ máy nguồn đến máy đích mà không cần dựa vào việc trao đổi trước đó..

Các đặc trưng của IP bao gồm :

- IP hoạt động ở lớp mạng (lớp 3) của mô hình OSI.
- IP là giao thức không kết nối trong đó gói dữ liệu một chiều được gửi đến đích mà không cần thông báo trước cho thiết bị đầu cuối. Thiết bị đầu cuối nhận dữ liệu và không gửi lại bất kỳ thông tin gì cho thiết bị gửi.
- IP dùng cấu trúc địa chỉ phân cấp trong đó phần chỉ danh mạng tương tự như tên đường và phần định dạng thiết bị giống như số nhà trên con đường đó.
- IP cung cấp dịch vụ theo dạng nỗ lực tối đa và không đảm bảo việc phân phối dữ liệu. Một gói dữ liệu có thể bị định hướng sai, trùng lặp, hoặc mất trên đường truyền đến đích.
- IP không cung cấp chức năng khôi phục dữ liệu bị hư hỏng. Những dịch vụ như vậy được các hệ thống đầu cuối cung ứng.

Trong các ứng dụng thời gian thực như voice hoặc video, tốc độ là yếu tố quan trọng hơn là khả năng khôi phục dữ liệu bởi vì việc khôi phục lại các gói tin bị mất sẽ làm chậm tính thời gian thực của ứng dụng một vài gói.

Ví dụ : chuyển thư qua bưu điện

Dịch vụ IP tương tự như việc chuyển thư qua bưu điện. Ví dụ, bạn sinh sống ở San Francisco và mẹ bạn sống ở New York. Bạn viết một số thư gửi cho mẹ, bỏ mỗi lá thư vào một bì thư, ghi địa chỉ của mẹ bạn trên mỗi bì thư, và địa chỉ trả lời cho mẹ bạn trên gói trái trên của từng bì thư.

Bạn đem những lá thư đến bưu điện địa phương để gửi cho mẹ bạn. Bưu điện sẽ nỗ lực hết mình để chuyển các lá thư đến cho mẹ bạn ở. Tuy nhiên, bưu điện sẽ không đảm bảo là nhưng lá thư này đến tay mẹ bạn một cách đầy đủ. Cũng như không đảm bảo là các lá thư này đến theo cùng một con đường và theo thứ tự bạn gửi.

Tại sao là địa chỉ IP ?

- Chúng định danh duy nhất mỗi thiết bị trên mạng IP.
- Mỗi thiết bị (máy tính, thiết bị mạng, ngoại vi) phải có một địa chỉ duy nhất.
- chỉ danh thiết bị (Host ID):
 - chỉ danh từng thiết bị
 - Được gán bởi quản trị mạng

Network.Host

Module 4-4

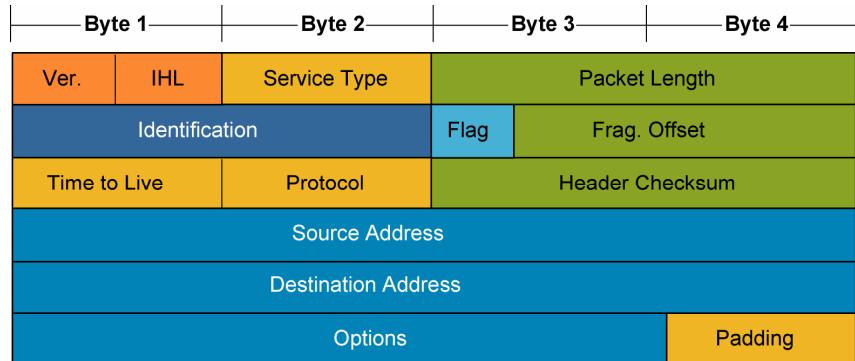
Tương tự như số nhà được dùng xác định vị trí của ngôi nhà để các lá thư có thể được gửi đến trong thế giới thực, địa chỉ luận lý IP cũng được dùng để xác định từng thiết bị trên mạng IP sao cho dữ liệu có thể gửi đến một cách hiệu quả. Mỗi máy tính, thiết bị mạng, ngoại vi kết nối vào Internet phải có một địa chỉ IP dài 32-bit để chỉ danh. Không có kiến trúc phân phối địa chỉ IP, thì sẽ không thể định tuyến hiệu quả các gói tin. Tìm hiểu cách thức tổ chức địa chỉ IP và chức năng của nó trong hoạt động mạng sẽ giúp ta nắm được gói IP gửi đi như thế nào trên mạng TCP/IP.

Địa chỉ IPv4 là loại địa chỉ được dùng phổ biến nhất ngày nay. Địa chỉ này là một số nhị phân 32-bit dùng để mô tả vị trí của thiết bị mạng.

Địa chỉ IP là một kiến trúc phân cấp gồm 2 phần :

- Phần địa chỉ mạng (network ID) mô tả phần mạng của địa chỉ IP. Router duy trì thông tin về những con đường cho mỗi mạng.
- Phần địa chỉ thiết bị (host ID) chỉ danh từng điểm cuối. Điểm cuối bao gồm máy chủ, máy tính, và cá thiết bị khác trên mạng.

Header của gói IP



Module 4-5

Trong bài mô hình truyền thông từ máy đến máy, ta đã biết rằng khi dữ liệu di chuyển xuống các lớp bên dưới chúng sẽ được đóng gói lại. Ở lớp Internet dữ liệu được chuyển thành các gói tin (packet). Header của gói tin có một số trường như hình trên. Trong phần này chúng ta sẽ tập trung vào 2 trường địa chỉ :

Địa chỉ nguồn : đặc tả địa chỉ máy gửi.

Địa chỉ đích : đặc tả địa chỉ máy nhận.

Định dạng địa chỉ IP : ký hiệu chấm thập phân

	Example			
An IP address is a 32-bit binary number	101011000001000010000000000010001			
For readability, the 32-bit binary number can be divided into four 8-bit octets	10101100	00010000	10000000	00010001
Each octet (or byte) can be converted to decimal	172	16	128	17
The address can be written in dotted decimal notation	172.	16.	128.	17

Cách chuyển đổi số nhị phân sang thập phân và ngược lại sẽ được dạy ở phần sau của khóa học

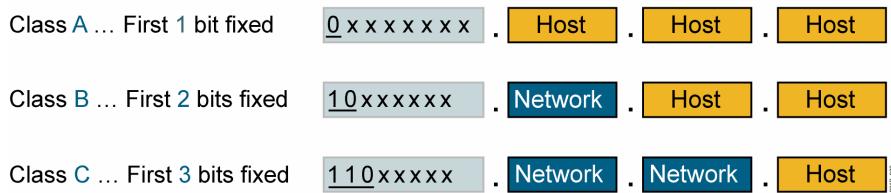
Module 4-6

Trong mỗi địa chỉ IP, một số bit sẽ dùng để biểu diễn phần địa chỉ mạng phần bit nhị phân còn lại biểu diễn phần địa chỉ thiết bị. Trong khi nhiều máy tính chia sẻ cùng địa chỉ mạng, nhưng khi kết hợp địa chỉ mạng với địa chỉ thiết bị sẽ chỉ danh duy nhất một thiết bị trên mạng.

Trong hình trên, địa chỉ IP dạng nhị phân 10101100000100001000000000010001. nhưng để dễ dàng người ta chia chúng thành 4 nhóm số gọi là octet. Mỗi octet được biểu diễn bằng một số nguyên từ 0 đến 255 và được tách biệt bởi dấu chấm. Dạng biểu diễn này được gọi là ký hiệu chấm thập phân. Địa chỉ IP có thể viết thành dạng 172.16.128.17

Các lớp địa chỉ IP : Octet thứ nhất

A B C ... Easy as 1 2 3



Module 4-7

Để phù hợp với các loại kích thước mạng khác nhau và giúp phân loại chúng, địa chỉ IP được chia thành các lớp.

Gán địa chỉ vào các lớp được gọi là địa chỉ phân lớp đầy đủ. Các lớp này được cấp bởi tổ chức Internet Assigned Numbers Authority (IANA). Mỗi địa chỉ IP bao gồm 2 phần chỉ danh mạng và chỉ danh máy. 5 lớp địa chỉ IP bao gồm :

Lớp A

Lớp A dùng octet thứ nhất để chỉ ra phần địa chỉ mạng, ba octet còn lại dùng làm địa chỉ máy. Bit đầu tiên của lớp A luôn là “0.” vì thế lớp A biến thiên từ 0 (00000000) đến 127 (01111111). Tuy nhiên có 2 mạng 0 và 127 được sử dụng với mục đích đặc biệt vì thế có tất cả 126 mạng lớp A có octet thứ nhất từ 1 đến 126.

Lớp B

Lớp B dùng 2 octet đầu để chỉ ra phần địa chỉ mạng, hai octet còn lại dùng làm địa chỉ máy. Hai bit đầu tiên của octet thứ nhất luôn là “10.” như vậy số bé nhất của lớp B ở octet thứ nhất sẽ là 10000000 (128 thập phân), và số lớp nhất là 10111111 (191 thập phân). Vì thế tất cả các mạng lớp B có octet thứ nhất từ 128 đến 191.

Lớp C

Lớp C dùng 3 octet đầu để chỉ ra phần địa chỉ mạng, octet còn lại dùng làm địa chỉ máy. Ba bit đầu tiên của octet thứ nhất luôn là “100.” như vậy số bé nhất của lớp C ở octet thứ nhất sẽ là 11000000 (192 thập phân), và số lớp nhất là 11011111 (223 thập phân). Vì thế tất cả các mạng lớp C có octet thứ nhất từ 192 đến 223.

Vùng địa chỉ IP

IP Address Class	First Octet Binary Value	First Octet Decimal Value	Possible Number of Hosts
Class A	1-126	<u>00000001</u> to <u>01111110</u> *	16,777,214
Class B	128-191	<u>10000000</u> to <u>10111111</u>	65,534
Class C	192-223	<u>11000000</u> to <u>11011111</u>	254

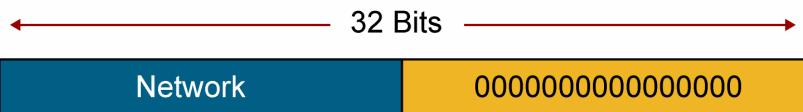
*127 (01111111) là địa chỉ lớp A dành riêng cho việc kiểm tra loopback không được dùng để gán cho mạng.

Module 4-9

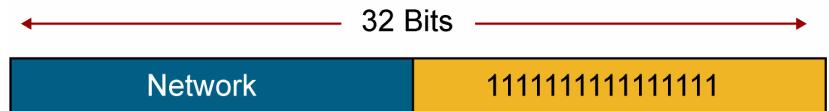
Hình trên cho ta thấy vùng địa chỉ IP của octet thứ nhất cho các lớp A đến C, cũng như số lượng địa chỉ máy khả dụng cho từng lớp.

Địa chỉ dành riêng

▪ Network Addresses



▪ Broadcast Addresses



Module 4-10

Một số địa chỉ IP được dành riêng và không thể gán cho các thiết bị của mạng. Các địa chỉ dành riêng này bao gồm địa chỉ mạng dùng để chỉ danh bản thân mạng, địa chỉ broadcast, dùng để gửi gói tin đến tất cả các máy trong một mạng.

Địa chỉ mạng (Network Address)

Địa chỉ IP có giá trị 0 cho tất cả các bit ở phần địa chỉ máy được dành riêng cho địa chỉ mạng. Ví dụ : địa chỉ lớp A 10.0.0.0 là địa chỉ mạng chứa máy có địa chỉ là 10.1.2.3. Địa chỉ lớp B 172.16.0.0 là địa chỉ mạng và 192.16.1.0 là địa chỉ mạng lớp C. Router dùng địa chỉ mạng để tìm kiếm đường đi trong bảng định tuyến.

Địa chỉ Broadcast trực tiếp (Directed Broadcasts Address)

Để gửi dữ liệu đến tất cả các thiết bị trên một mạng người ta sử dụng địa chỉ broadcast. Địa chỉ broadcast có giá trị 1 cho tất cả các bit ở phần địa chỉ máy. Ví dụ đối với mạng 172.16.0.0, sẽ có địa chỉ broadcast là 172.16.255.255.

Địa chỉ broadcast trực tiếp mặc định không được router định tuyến.

Địa chỉ Broadcast cục bộ (Local Broadcasts Address)

Nếu thiết bị gửi dữ liệu đến tất cả thiết bị trên mạng cục bộ người ta sẽ sử dụng địa chỉ đích là 255.255.255.255. ví dụ khi máy tính không biết địa chỉ IP của nó sẽ gửi yêu cầu đến server trong mạng cục bộ bằng địa chỉ broadcast cục bộ. Mặc định router cũng không định tuyến cho địa chỉ broadcast cục bộ.

Địa chỉ Loopback cục bộ (Local Loopback Address)

Địa chỉ loopback cục bộ được sử dụng để thiết bị gửi thông điệp đến chính nó nhằm mục đích kiểm tra hoạt động địa chỉ loopback tiêu biểu là 127.0.0.1.

Tự cấu hình địa chỉ IP (Autoconfiguration IP Addresses)

Nếu thiết bị không thể lấy được địa chỉ IP bằng cách cấu hình tĩnh hay động khi khởi động thì nó sẽ tự gán cho mình địa chỉ IP link-local (RFC 3927) với thuộc mạng 169.254.0.0/16. Địa chỉ này chỉ được sử dụng cho kết nối cục bộ và không được router định tuyến.

Chỉ danh mạng (Network ID)

Phần địa chỉ mạng của IP được gọi là chỉ danh mạng, nó được sử dụng để router định tuyến dữ liệu đến một mạng khác. Hầu hết tất cả thiết bị trên mạng chỉ có thể truyền thông trực tiếp với những thiết bị trong cùng một mạng, vì thế cần phải có một thiết bị định tuyến dùng chỉ danh mạng để hợp với bảng định tuyến để chuyển dữ liệu đến mạng khác.

Điều này cũng đúng khi các thiết bị trên cùng một đoạn mạng vật lý. chỉ danh mạng cho phép router chuyển gói dữ liệu đến đoạn mạng tương ứng. Phần chỉ danh máy sẽ giúp router phân phối frame dữ liệu lớp 2 đến máy đích phù hợp.

Chỉ danh máy (Host ID)

Mỗi lớp mạng sẽ chứa 1 số cố định máy. Ví dụ lớp mạng A, octet thứ nhất dùng cho mạng, 3 octet còn lại dành cho địa chỉ máy. Địa chỉ đầu tiên là địa chỉ mạng, địa chỉ cuối cùng là địa chỉ broadcasts. Như vậy số lượng địa chỉ máy tối đa mà lớp A cung cấp sẽ là $2^{24} - 2 = 16,777,214$.

Đối với mạng lớp B số lượng địa chỉ máy tối đa là $2^{16} - 2 = 65,534$.

Đối với mạng lớp C số lượng địa chỉ máy tối đa là $2^8 - 2 = 254$.

Địa chỉ IP công cộng

Class	Public IP Ranges
A	1.0.0.0 to 9.255.255.255 11.0.0.0 to 126.255.255.255
B	128.0.0.0 to 172.15.255.255 172.32.0.0 to 191.255.255.255
C	192.0.0.0 to 192.167.255.255 192.168.0.0 to 223.255.255.255

Module 4-12

Một số mạng nối kết với nhau qua Internet, trong khi những mạng khác thì chỉ là mạng riêng (private network). Ví dụ, các địa chỉ dùng trong khóa học này là địa chỉ riêng không thể dùng công cộng được. Cả hai loại địa chỉ công cộng và riêng đều được sử dụng cho các loại mạng tương ứng.

Địa chỉ IP công cộng (Public IP Addresses)

Sự ổn định của mạng Internet phụ thuộc trực tiếp vào tính duy nhất của địa chỉ IP gán cho các thiết bị. Tổ chức chịu trách nhiệm cung cấp địa chỉ IP cho mạng Internet ban đầu là InterNIC (Internet Network Information Center). Sau đó là IANA với nhiệm vụ cấp địa chỉ sao cho không xảy ra sự tranh chấp đảm bảo tính ổn định và khả năng định tuyến của mạng internet.

Để nhận được địa chỉ IP, bạn phải liên hệ với nhà cung cấp dịch vụ internet (ISP). ISP sẽ liên hệ với tổ chức đăng ký cấp cao hơn :

- APNIC (Asia Pacific Network Information Center) cung cấp địa chỉ IP cho Châu Á
- ARIN (American Registry for Internet Numbers) cung cấp địa chỉ IP cho Châu Mỹ
- RIPE NCC (Réseaux IP Européens Network Coordination Centre) cung cấp địa chỉ IP cho Châu Âu

Với sự phát triển nhanh chóng của mạng Internet, địa chỉ IP công cộng bắt đầu cạn kiệt, vì thế một số cơ chế địa chỉ mới được giới thiệu ví dụ cơ chế dịch địa chỉ mạng (NAT), tuyển liên thông vùng không phân lớp (CIDR), và địa chỉ IPv6.

Địa chỉ IP riêng

Class	Private Address Range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255

Module 4-14

Địa chỉ riêng (Private IP Addresses)

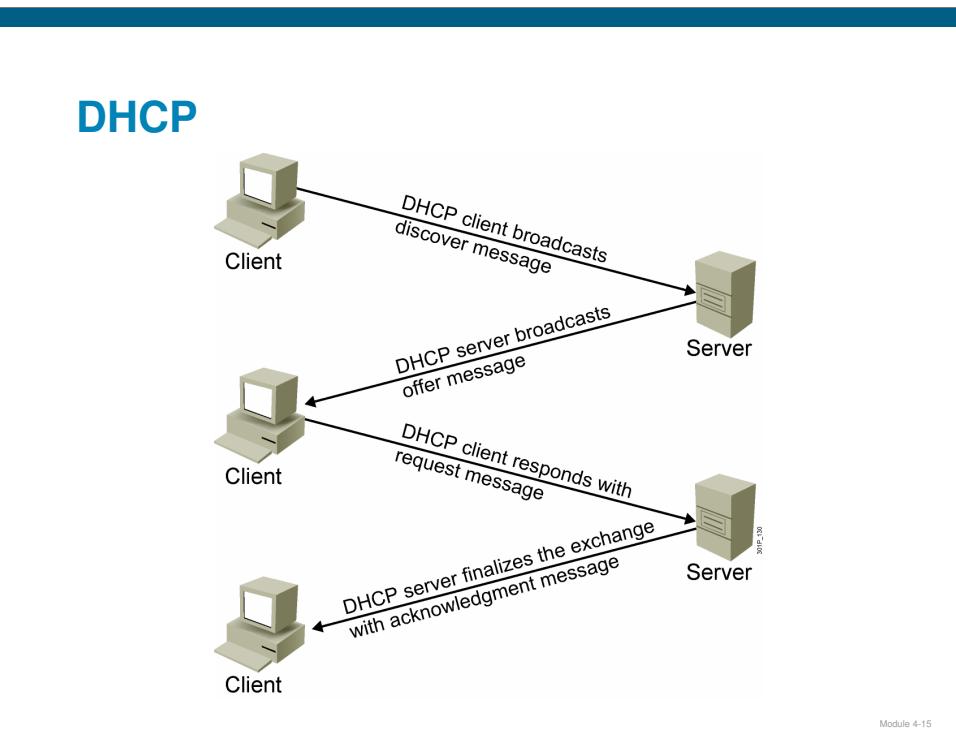
Trong khi các máy kết nối Internet yêu cầu 1 địa chỉ IP toàn cục duy nhất, các máy riêng không kết nối với Internet có thể sử dụng bất kỳ địa chỉ hợp lệ nào có tính duy nhất cục bộ.

Năm 1994, tổ chức IETF đưa ra RFC 1597 sau này được bổ sung thành RFC 1918, đề xuất sử dụng các khối địa chỉ IP riêng cho các mạng riêng không có yêu cầu kết nối Internet.

Có ba khối địa chỉ IP riêng như vậy (1 mạng lớp A, 16 mạng lớp B networks, 256 mạng lớp C) được sử dụng cho các mạng riêng. Các router trên mạng Internet sẽ được cấu hình để bỏ qua các địa chỉ riêng.

Đối với các mạng riêng không kết nối internet, ta có thể dùng địa chỉ riêng thay cho địa chỉ IP công cộng.

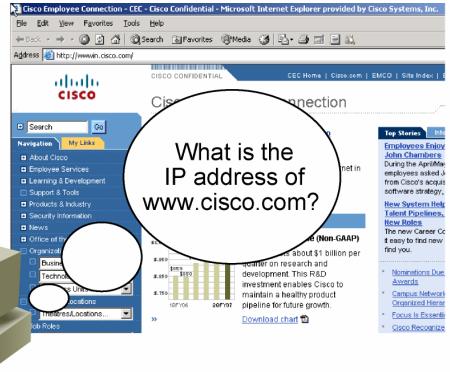
Nếu các mạng dùng địa chỉ IP riêng có nhu cầu kết nối Internet thì ta cần phải dịch (NAT) địa chỉ IP riêng thành IP công cộng.



DHCP dùng để cấp địa chỉ IP động và các tham số TCP/IP như mặt nạ mạng, router mặc định, máy chủ DNS thời gian thuê địa chỉ IP ... DHCP bao gồm 2 phần : giao thức phân phối cấu hình cho máy tính, và cơ chế cung cấp địa chỉ IP cho máy tính.

Sử dụng DHCP, máy tính có thể nhận được IP một cách tự động và nhanh chóng quickly. Cần định nghĩa ra một vùng địa chỉ IP trên máy chủ DHCP. Khi máy tính khởi động, nó sẽ liên hệ với máy chủ DHCP để yêu cầu thông tin địa chỉ. Máy chủ sẽ chọn một địa chỉ và cấp nó cho máy tính. Máy tính sẽ “thuê” địa chỉ này trong một khoảng thời gian. Định kỳ máy tính phải liên hệ lại với máy chủ DHCP để kéo dài thời gian “thuê” địa chỉ. Cơ chế thuê địa chỉ giúp cho các máy tính đã tắt nguồn hay di chuyển không chiếm dụng địa chỉ được cấp.

DNS



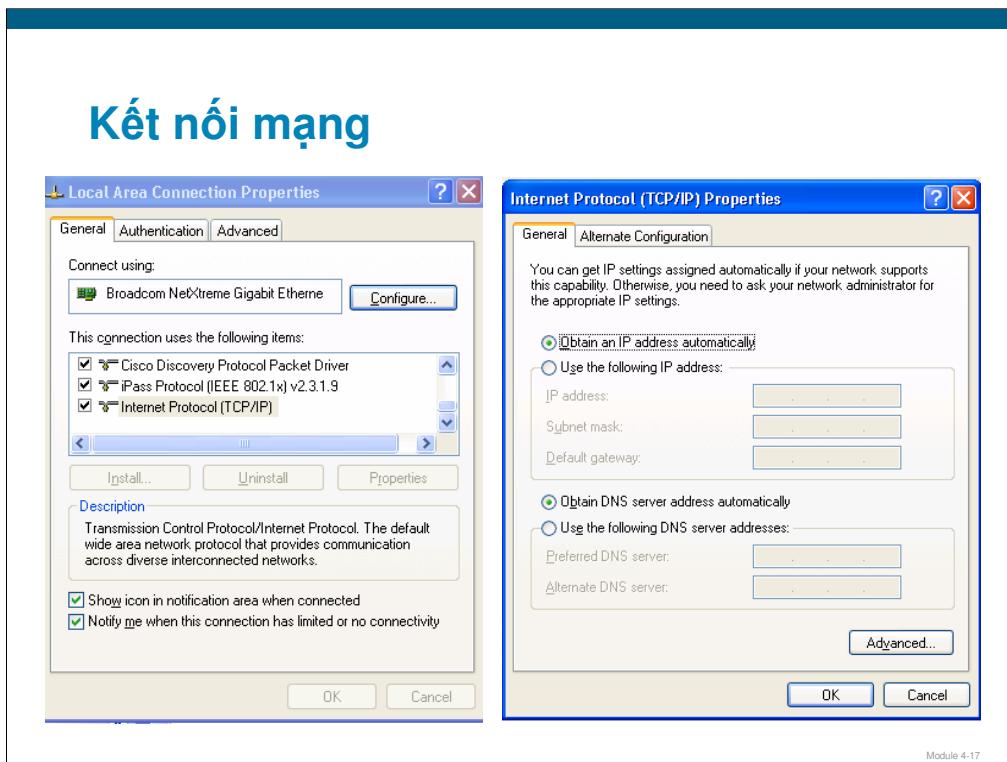
- Ứng dụng DNS phát triển trên mô hình TCP/IP
- Dịch tên miền thành địa chỉ IP

Module 4-16

Ứng dụng Domain Name System (DNS) cung cấp cách thức hiệu quả để chuyển đổi tên miền gọi nhớ thành địa chỉ IP tương ứng.

DNS là cơ chế chuyển tên miền thành địa chỉ IP. Ứng dụng DNS giúp cho người sử dụng tránh phải nhớ địa chỉ IP, chính nhờ vậy mà Internet trở nên rất phổ biến.

Kết nối mạng



Kết nối mạng dùng để thiết lập và xem cấu hình địa chỉ IP của máy tính. Ví dụ trên máy tính lấy địa chỉ IP động từ máy chủ DHCP.

```

C:\> C:\WINDOWS\system32\cmd.exe
C:\>Documents and Settings>ipconfig /all
Windows IP Configuration

Host Name . . . . . : PCUSER
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled . . . . . : No
WINS Proxy Enabled . . . . . : No
DNS Suffix Search List . . . . . :

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . . . . : Intel(R) PRO/1000 MT Desktop Network Connection
Description . . . . . : Intel(R) PRO/1000 MT Desktop Network Connection
Physical Address . . . . . : 00-15-58-2F-21-E6
Dhcp Enabled . . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IP Address . . . . . : 192.168.1.102
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DNS Servers . . . . . : 127.107.241.185
                           127.135.250.69
Lease Obtained . . . . . : Wednesday, April 25, 2007 12:27:51 AM
Lease Expires . . . . . : Thursday, April 26, 2007 12:27:51 AM

```

Module 4-18

IPCONFIG là lệnh dùng để hiển thị cấu hình TCP/IP của máy tính hoặc làm tươi các thiết lập DHCP và DNS. Nếu không dùng tham số lệnh **ipconfig** sẽ hiển thị địa chỉ IP, subnet mask, và default gateway của tất cả card mạng.

Cú pháp

ipconfig [/all] [/renew [Adapter]] [/release [Adapter]] [/flushdns]
[/displaydns] [/registerdns] [/showclassid Adapter] [/setclassid Adapter [ClassID]]

Tham số

/all: hiển thị đầy đủ tham số cấu hình TCP/IP của tất cả các card mạng. Bao gồm card vật lý, lô gíc và kết nối dạng quay số (dialup).

/renew [Adapter]: yêu cầu cấp lại tham số DHCP cho tất cả hoặc 1 card mạng. Tham số này chỉ khả dụng trên máy tính có card mạng đang cấu hình sử dụng DHCP để cấp địa chỉ động.

/release [Adapter]: gửi thông điệp DHCPRELEASE đến máy chủ DHCP để trả lại địa chỉ IP trở lại máy chủ cho tất cả hoặc 1 card mạng. Tham số này sẽ vô hiệu hóa cấu hình do máy chủ DHCP cấp cho card mạng.

/flushdns: xóa nội dung bộ đệm dịch tên miền cục bộ trên máy tính. Thường dùng trong khi tìm các lỗi DNS.

/displaydns: hiển thị nội dung bộ đệm dịch tên miền cục bộ trên máy tính, bao gồm nội dung trong tập tin host và các tên miền nhận được từ máy chủ DNS.

/registerdns: khởi tạo đăng ký tên miền và địa chỉ IP được cấu hình trên máy tính. Dùng để tìm lỗi đăng ký tên miền hoặc giải quyết các cập nhật động giữa máy khách và máy chủ DNS mà không cần khởi động lại máy khách.

/showclassid Adapter: hiển thị chỉ danh lớp của máy chủ DHCP (DHCP class ID) của một card mạng. Để xem tất cả card mạng ta dùng dấu * ở phần adapter. Tham số này chỉ khả dụng trên máy tính có card mạng đang cấu hình sử dụng DHCP để cấp địa chỉ động.

/setclassid Adapter [ClassID]: cấu hình chỉ danh lớp của máy chủ DHCP của 1 card mạng. Để cấu hình tất cả card mạng ta dùng dấu * ở phần adapter. Tham số này chỉ khả dụng trên máy tính có card mạng đang cấu hình sử dụng DHCP để cấp địa chỉ động.

/?: hiển thị trợ giúp của lệnh.

```
c:\> C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings>ipconfig /all
Windows IP Configuration

Host Name . . . . . : PCUSER
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled . . . . . : No
WINS Proxy Enabled . . . . . : No
DNS Suffix Search List . . . . . :

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . . . . : Intel(R) PRO/1000 MT Network Connection
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address . . . . . : 00-15-58-2F-21-E6
Dhcp Enabled . . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IP Address . . . . . : 192.168.1.102
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DNS Servers . . . . . : 127.107.241.185
                                         127.135.250.69
Lease Obtained . . . . . : Wednesday, April 25, 2007 12:27:51 AM
Lease Expires . . . . . : Thursday, April 26, 2007 12:27:51 AM
```

Tóm tắt

- Địa chỉ IP bao gồm 2 phần : chỉ danh mạng (network ID) và chỉ danh máy (host ID).
- Địa chỉ IPv4 là số nhị phân 32 bit và được chia thành các octet. Thường chúng được biểu diễn dưới dạng dấu chấm thập phân (ví dụ : 192.168.54.18).
- Khi viết ở dạng nhị phân, bit đầu tiên của lớp A luôn là 0, lớp B 2 bit đầu tiên là 10 và lớp C 3 bit đầu tiên sẽ là 110.

Module 4-21

Tóm tắt (tiếp theo.)

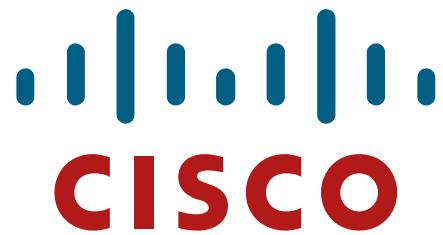
- Một vài địa chỉ IP (địa chỉ mạng và broadcast) được dành sẵn và không thể sử dụng để gán cho thiết bị mạng.
- Máy tính Internet yêu cầu sử dụng địa chỉ IP công cộng duy nhất toàn cục, nhưng máy tính riêng có thể dùng địa chỉ riêng hợp lệ có tính duy nhất trong mạng riêng mà thôi.
- DHCP dùng để cấp địa chỉ IP động, kèm theo đó là tập các tham số TCP/IP ví dụ như mặt nạ mạng, router mặc định, máy chủ DNS.
- DNS là ứng dụng trong TCP/IP, cho phép thông dịch các tên miền gợi nhớ thành các địa chỉ IP.

Module 4-22

Tóm tắt (tiếp theo.)

- Máy tính được trang bị một số công cụ dùng để kiểm tra địa chỉ IP
 - Kết nối mạng
 - IPCONFIG

Module 4-23



Module 4-24

Bài 5: Tìm hiểu lớp vận chuyển của mô hình TCP/IP



Xây dựng một mạng đơn giản

Module 5-1

Tổng quan

Để thực hiện truyền dữ liệu cho máy khác trên mạng máy tính cần sử dụng một số luật hoặc giao thức để cho phép nó truyền và nhận dữ liệu một cách có trật tự. Giao thức được sử dụng phổ biến nhất ngày nay là TCP/IP. Hiểu biết về cách thức hoạt động của TCP/IP là điểm mấu chốt để nắm bắt được cách thực hiện truyền dữ liệu trên môi trường mạng.

Cách thức IP phân phối gói tin thông qua mạng là khái niệm cơ bản trong kiến trúc TCP/IP. Hiểu được cách truyền dữ liệu thông qua IP là điểm chính yếu để hiểu được tổng quát chức năng của giao thức TCP/IP. Từ đó ta có thể tối ưu, sắp độ ưu tiên, bảo mật, giới hạn hoạt động truyền thông dữ liệu trên mạng. Bài này mô tả chuỗi các bước thực hiện quá trình gửi gói tin IP, các khái niệm và kiến trúc đi kèm như gói tin (packets), datagrams, trường giao thức (protocol field), cung cấp cho ta cái nhìn tổng quan về truyền thông dữ liệu trên mạng lớn.

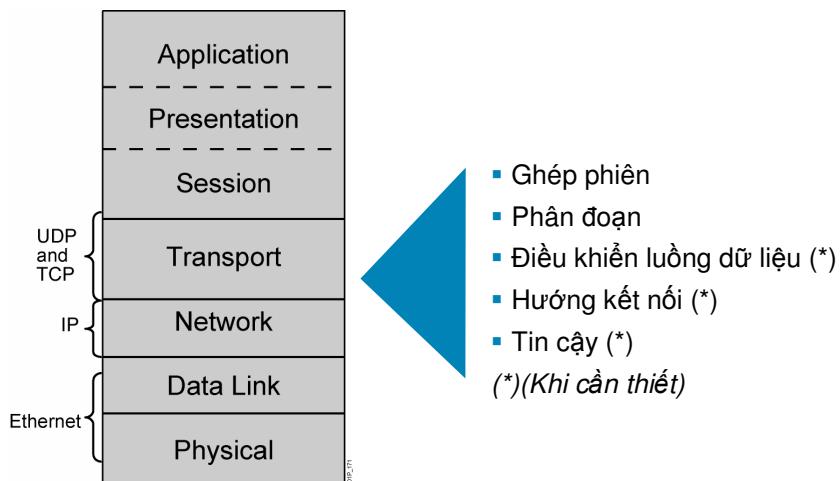
Để mạng Internet hoạt động chính xác, dữ liệu phải được phân phối một cách tin cậy. Bạn có thể bảo đảm việc phân phối dữ liệu tin cậy thông qua việc phát triển các ứng dụng và bởi các dịch vụ cung cấp bởi giao thức mạng. Trong mô hình OSI và TCP/TP, lớp vận chuyển (transport layer) đảm nhận chức năng này. Lớp vận chuyển che dấu chi tiết các thông tin của lớp mạng bên dưới khỏi lớp bên trên. Chẳng hạn như giao thức TCP và UDP hoạt động ở lớp vận chuyển chúng che dấu các thông tin chi tiết của lớp mạng bên dưới khỏi lớp ứng dụng. Bài này mô tả chức năng của lớp vận chuyển và cách thức UDP & TCP hoạt động.

Mục tiêu

Kết thúc bài học này, học viên sẽ có thể so sánh sự tương phản của 2 mô hình TCP/IP và OSI :

- Giải thích mục đích và chức năng của lớp vận chuyển
- sự tương phản của dịch vụ vận chuyển hướng kết nối (connection-oriented) và phi kết nối (connectionless)
- Liệt kê các đặc trưng của UDP
- Liệt kê các đặc trưng của TCP
- Liệt kê các ứng dụng phổ biến dùng TCP/IP
- Mô tả cách thức ánh xạ giao thức lớp 3 - lớp 4
- Mô tả cách thức ánh xạ giao thức lớp 4 - ứng dụng
- Thứ tự các bước khởi tạo kết nối TCP
- Mô tả các nguyên nhân và cơ chế điều khiển luồng dữ liệu (flow control)
- Thứ tự các bước trong trình tự tin báo nhận (acknowledgment)
- Mô tả chức năng của windowing
- Định nghĩa số tuần tự (sequence number) và số tin báo nhận (acknowledgment number)

Lớp vận chuyển



Module 5-3

Bên cạnh lớp ứng dụng, lớp mạng, lớp vận chuyển là hoạt động cơ bản của kiến trúc phân lớp TCP/IP.

Lớp mạng định tuyến dữ liệu đến máy đích nhưng nó không đảm bảo dữ liệu gửi đến đích đúng trật tự, không có lỗi hoặc thậm chí có thể không đến được đích. Lớp vận chuyển cung cấp 2 giao thức UDP and TCP, chúng cung cấp dịch vụ truyền thông cho ứng dụng trên máy. Các dịch vụ cơ bản của lớp vận chuyển gồm phân đoạn (segmentation) và ghép phiên (session multiplexing) xuất hiện trong cả UDP và TCP. Dịch vụ trả phí (“premium service”) cung cấp bởi lớp vận chuyển đảm bảo rằng dữ liệu được phân phối một cách tin cậy chỉ xuất hiện trong TCP.

Nhiệm vụ cơ bản của lớp vận chuyển là làm cầu nối giữa ứng dụng và lớp mạng, chúng được cung cấp thông qua UDP và TCP. Nếu sử dụng TCP lớp vận chuyển sẽ thực hiện thêm các nhiệm vụ sau thiết lập kết nối (connection oriented, phân đoạn (segmentation), điều khiển luồng dữ liệu (flow control), và áp dụng các cơ chế đảm bảo độ tin cậy (reliability).

Ví dụ : UDP - Gửi thư thông thường

Dịch vụ gửi thư thông thường là một ví dụ minh họa tương tự hoạt động của UDP. Khi gửi thư bạn ghi địa chỉ người nhận và địa chỉ người nhận, dán tem và gửi cho bưu điện. Bưu điện sẽ cố gắng hết mình để gửi đến địa chỉ đích của bức thư. Tuy nhiên không có gì bảo đảm rằng lá thư được gửi đến đích thành công hay không.

Ví dụ : TCP - gửi thư bảo đảm

Dịch vụ gửi thư bảo đảm là một ví dụ minh họa tương tự hoạt động của TCP. Tưởng tượng rằng bạn đang sống ở San Francisco và muốn gửi một quyển sách cho mẹ bạn đang sống ở New York. Giả sử rằng bạn chỉ cho phép gửi thư mà không cho gửi bưu phẩm. Bạn thực hiện tháo rời sách và đóng gói các trang sách vào các bì thư riêng. Để đảm bảo mẹ bạn có thể sắp xếp thành quyển sách chính xác như ban đầu, bạn đánh số các bì thư. Bạn ghi địa chỉ các bì thư và gửi chúng đi với dịch vụ gửi thư bảo đảm. Bưu điện sẽ gửi đi bằng nhiều cách máy bay, tàu hỏa, xe thư ... nhưng bởi vì đây là thư bảo đảm bưu điện sẽ phải lấy chữ ký xác nhận đã nhận thư từ mẹ bạn và gửi nó cho bạn.

Gửi từng lá thư một sẽ nhàn chán vì thế bạn sẽ gửi cùng lúc một vài lá thư thay vì chỉ gửi 1. Bưu điện một lần nữa sẽ gửi từng lá thư đi bằng nhiều cách máy bay, tàu hỏa, xe thư ... nhưng bởi vì đây là thư bảo đảm bưu điện sẽ phải lấy chữ ký xác nhận đã nhận thư từ mẹ bạn cho từng lá thư và gửi nó cho bạn. Nếu một lá thư bị mất bạn sẽ không nhận được chữ ký xác nhận và bạn có thể gửi lại những trang sách đó cho mẹ bạn. Sau khi nhận được tất cả các lá thư, mẹ bạn sẽ sắp xếp chúng lại theo thứ tự và ghép chúng lại thành quyển sách ban đầu.

Ghép phiên (Session Multiplexing)

Ghép phiên là hoạt động xảy ra trong mỗi máy tính, với một địa chỉ IP, máy sẽ có khả năng thực hiện nhiều phiên làm việc cùng một lúc. Một phiên được tạo ra khi máy nguồn cần gửi dữ liệu cho máy đích. Trình ứng dụng mạng tạo ra các phiên và điều khiển nó trong đó bao gồm chức năng của các lớp 5-7 của mô hình OSI.

Phiên best-effort rất đơn giản các tham số phiên được gửi bằng dịch vụ UDP. Phiên best-effort sử dụng cổng (port number) để gửi dữ liệu tới địa chỉ đích. Mỗi yêu cầu truyền dữ liệu là một sự kiện độc lập, và không có bộ nhớ hay liên hệ gì được duy trì.

Khi sử dụng dịch vụ truyền tin cậy TCP, một kết nối phải được thiết lập giữa nguồn và đích trước khi dữ liệu thực sự được truyền giữa 2 máy. TCP mở kết nối và thỏa thuận các tham số với đích đến. Trong lúc truyền dữ liệu, TCP sẽ duy trì kết nối này để đảm bảo việc truyền dữ liệu là tin cậy, khi không có nhu cầu truyền dữ liệu tiếp tục, kết nối sẽ được đóng lại.

Ví dụ bạn nhận địa chỉ URL của Yahoo vào cửa sổ IE, và Yahoo sẽ trả về nội dung trang web tương ứng. Khi nội dung website Yahoo đã hiện thị, bạn có thể mở một cửa sổ khác để duyệt một trang web khác ví dụ Google. Cả 2 website này đều tạo kết nối với máy bạn với duy nhất 1 địa chỉ IP, vì thế để phân biệt các kết nối người ta dùng cổng (port number).

Phân đoạn (Segmentation)

TCP nhận khối dữ liệu từ lớp ứng dụng và chuẩn bị để truyền chúng trên mạng. Mỗi khối dữ liệu sẽ được chia nhỏ thành các đoạn (segment) nhỏ hơn phù hợp với đơn vị truyền tối đa (Maximum Transmission Unit - MTU) của lớp mạng bên dưới. Dịch vụ UDP đơn giản hơn sẽ không thực hiện kiểm tra hoặc thỏa thuận và mong đợi trình ứng dụng sẽ làm điều đó thay cho UDP.

Điều khiển luồng dữ liệu (Flow Control)

Nếu thiết bị nguồn truyền dữ liệu nhanh hơn khả năng nhận của thiết bị đích dữ liệu, nó sẽ bị bỏ đi, vì thế dữ liệu sẽ phải gửi lại. Việc gửi lại dữ liệu sẽ làm lãng phí thời gian và tài nguyên mạng, do vậy chức năng điều khiển luồng dữ liệu được sử dụng để tối đa tốc độ truyền dữ liệu trong điều kiện tối thiểu nhu cầu gửi lại dữ liệu.

Trong TCP cơ chế điều khiển luồng dữ liệu cơ bản được hiện thực bằng tin báo nhận (acknowledgment) mà thiết bị nhận trả về; thiết bị gửi phải đợi tin báo nhận trước khi gửi dữ liệu kế tiếp. Tuy nhiên, nếu thời gian quay vòng tín hiệu (round-trip time - RTT) là đáng kể, thì tốc độ truyền thông quan sẽ không thể chấp nhận được. Một cơ chế khác gọi là cơ chế cửa sổ (windowing) được sử dụng để gia tăng hiệu quả khi kết hợp với cơ chế điều khiển luồng dữ liệu cơ bản ở trên. Cơ chế cửa sổ cho phép máy nhận khuyến cáo khôi lượng dữ liệu sẽ nhận trước khi gửi tin báo nhận để xác nhận cho máy gửi.

Giao thức hướng kết nối (Connection-Oriented Transport Protocol)

Trong lớp vận chuyển TCP là giao thức hướng kết nối, nó thiết lập, duy trì kết nối phiên trong suốt qua trình truyền dữ liệu. Khi việc truyền nhận kết thúc, phiên cũng bị xóa đi.

Tin cậy (Reliability)

Chức năng tin cậy của TCP có 3 mục tiêu :

- Nhận biết và sửa lỗi mất dữ liệu
- Nhận biết và sửa lỗi trùng lắp và sai thứ tự dữ liệu
- Tránh nghẽn trên mạng

Tính tin cậy không phải lúc nào cũng cần. Ví dụ, trong luồng video (video stream), nếu gói tin bị bỏ và được gửi lại, nó sẽ xuất hiện không đúng thứ tự. Điều đó sẽ làm khán giả khó chịu và khó theo dõi nội dung. Trong ứng dụng thời gian thực (real-time application), ví dụ voice và video streaming, gói tin bị bỏ là chấp nhận được nếu tỉ lệ rớt gói chung là đủ nhỏ.

So sánh tin cậy và cố gắng hết khả năng

	Reliable	Best-Effort
Connection Type	Connection-oriented	Connectionless
Protocol	TCP	UDP
Sequencing	Yes	No
Uses	<ul style="list-style-type: none">▪ E-mail▪ File sharing▪ Downloading	<ul style="list-style-type: none">▪ Voice streaming▪ Video streaming

Module 5-6

“Tin cậy” and “cố gắng hết mình” là thuật ngữ mô tả 2 loại kết nối giữa máy tính trên mạng. Mỗi loại đều có ưu khuyết điểm riêng.

Tin cậy - Hướng kết nối (Reliable - Connection-Oriented)

TCP là giao thức tin cậy ở lớp vận chuyển. Để đảm bảo tính tin cậy TCP thiết lập kết nối. Trong quá trình khởi tạo, các tham số về khả năng của thiết bị nhận được thỏa thuận, các tham số này được sử dụng để theo dõi quá trình truyền dữ liệu trên kết nối tương ứng.

Khi máy gửi truyền dữ liệu, nó đánh số tuần tự (sequence number) các khối dữ liệu. Máy nhận đáp ứng lại với các tin báo nhận có số hiệu tương ứng các số tuần tự được mong đợi. Việc trao đổi số tuần tự và số hiệu tin báo nhận giúp cho giao thức phát hiện các khối dữ liệu bị mất, trùng lắp, hoặc đến sai thứ tự. TCP là một giao thức vận chuyển phức tạp.

Cố gắng hết khả năng – Phi kết nối (Best-Effort - Connectionless)

UDP là giao thức cố gắng hết khả năng, nó không cần hoặc không muốn duy trì thông tin dữ liệu đã gửi trước đó. Vì thế UDP không cần thiết phải thiết lập bất kỳ kết nối nào với thiết bị nhận. Vì thế người ta gọi dịch vụ này là phi kết nối (“connectionless.”). Có rất nhiều tình huống dịch vụ phi kết nối loại này được ưa chuộng hơn là dịch vụ tin cậy. Các ứng dụng dùng dịch vụ này khi đòi hỏi việc truyền thông nhanh hơn và không cần kiểm tra tin báo nhận.

Đặc trưng của UDP

- Hoạt động ở lớp vận chuyển của mô hình OSI và TCP/IP
- Cung cấp cho ứng dụng khả năng truy cập lớp mạng không có chi phí cho các cơ chế tin cậy.
- Là giao thức phi kết nối
- Cung cấp khả năng kiểm tra lỗi hạn chế
- Cung cấp khả năng phân phối cố gắng hết khả năng
- Không có chức năng khôi phục dữ liệu

Module 5-7

Các đặc trưng của UDP bao gồm :

- Hoạt động ở lớp vận chuyển của mô hình OSI và TCP/IP
- Cung cấp cho ứng dụng khả năng truy cập lớp mạng không có chi phí cho các cơ chế tin cậy.
- Tương tự IP, UDP Là giao thức phi kết nối, trong đó khôi dữ liệu gửi đến đích mà không cần thông báo cho đích đến biết trước
- UDP có rất ít khả năng kiểm tra lỗi hạn chế. Khối dữ liệu UDP có tùy chọn checksum dùng cho kiểm tra lỗi. Máy đích có thể sử dụng tham số này để kiểm tra tính toàn vẹn (integrity) của dữ liệu. Hơn nữa, trong header của UDP có thông tin về cổng, nếu máy đích kiểm tra thấy rằng dữ liệu chuyển đến một cổng không hoạt động, nó sẽ loại bỏ dữ liệu và gửi lại thông điệp port is unreachable.
- UDP cung cấp dịch vụ phân phối cố gắng hết khả năng, nó không đảm bảo dữ liệu được phân phối thành công mà không bị mất, trùng lặp hoặc sai thứ tự tại đích đến.
- UDP không có chức năng khôi phục dữ liệu bị mất hay có lỗi. Các ứng dụng bên trên phải thực hiện chức năng này nếu cần.

Ví dụ : gửi tờ bướm quảng cáo (Advertising Flyers)

ví dụ minh họa cho dịch vụ UDP chính là dịch vụ phát tờ bướm quảng cáo qua bưu điện. Bạn có nhu cầu thông báo cho những người xung quanh về món hàng định bán. Bạn sẽ viết một tờ bướm quảng cáo ghi ngày giờ, địa chỉ và thông tin món hàng sau đó bạn ghi rõ địa chỉ người nhận trong bán kính 2 km xung quanh nhà bạn và gửi cho bưu điện để chuyển đến hàng xóm. Ở đây ta không cần quan tâm đến tin báo nhận từ hàng xóm cũng như khả năng tờ bướm bị thất lạc.

Header của UDP



Module 5-9

Header của UDP có chiều dài 64 bit. Bao gồm các trường sau :

- Cổng nguồn (Source port)** : số nguyên 16 bit của cổng đang gọi.
- Cổng đích (Destination port)** : số nguyên 16 bit của cổng được gọi.
- Chiều dài (Length)** : chiều dài của header khói dữ liệu UDP (16 bit)
- Checksum** : Checksum được tính toán dựa trên header và nội dung khói dữ liệu UDP (16 bit)
- Dữ liệu (Data)** : Khối dữ liệu của lớp ứng dụng bên trên (kích thước thay đổi)

Các ứng dụng sử dụng dịch vụ UDP bao gồm TFTP, Simple Network Management Protocol (SNMP), Network File System (NFS), và Domain Name System (DNS).

Đặc trưng của TCP

- Lớp vận chuyển của mô hình TCP/IP
- Cung cấp lớp ứng dụng khả năng truy cập lớp mạng
- Giao thức hướng kết nối
- Hoạt động ở chế độ song công (Full-duplex)
- Kiểm tra lỗi
- Đánh số thứ tự các gói dữ liệu
- Tin báo nhận (Acknowledgement)
- Chức năng khôi phục dữ liệu

Module 5-10

TCP viết tắt của cụm từ Transmission Control Protocol. Đây là giao thức hướng kết nối cung cấp dịch vụ truyền dữ liệu tin cậy giữa các máy. TCP có một số đặc trưng liên quan đến cách thức hoàn tất chức năng truyền thông tin cậy.

TCP là một giao thức khác của mô hình TCP/IP nó giải quyết vấn đề truyền thông dữ liệu trên mạng

- Tương tự UDP, TCP hoạt động ở lớp vận chuyển của mô hình OSI & TCP/IP.
- Tương tự UDP, TCP Cung cấp lớp ứng dụng khả năng truy cập lớp mạng.
- TCP là giao thức hướng kết nối trong đó 2 thiết bị mạng thiết lập một kết nối để trao đổi dữ liệu. Hệ thống đầu cuối đồng bộ với thiết bị khác để quản trị dòng thông tin nhằm tránh nghẽn trên mạng.
- Kết nối TCP là một cặp mạch ảo (virtual circuit), mỗi mạch ảo trên 1 hướng, vì thế nó hoạt động ở chế độ song công.
- TCP cung cấp cơ chế kiểm tra lỗi thông qua checksum và các thông tin header TCP.
- Các đoạn (segment) dữ liệu của TCP được đánh số thứ tự để cho phép đích đến có thể sắp xếp chúng theo trình tự ban đầu cũng như phát hiện các đoạn dữ liệu bị mất.
- Khi nhận được một hay các đoạn dữ liệu TCP, máy nhận sẽ phản hồi lại máy gửi các tin báo nhận để xác nhận các đoạn dữ liệu đã nhận thành công. Đoạn dữ liệu nào chưa có tin báo nhận, máy gửi sẽ phải truyền lại thông tin này, hoặc nó sẽ kết thúc kết nối nếu nhận thấy rằng máy nhận không còn trên kết nối.

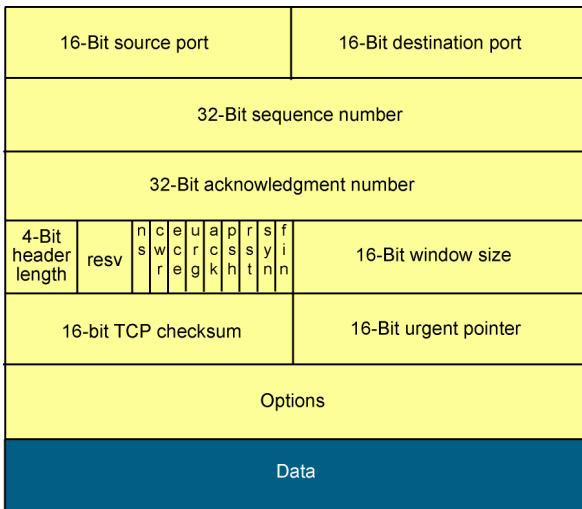
- TCP cung cấp dịch vụ khôi phục dữ liệu trong đó máy nhận có thể yêu cầu gửi lại một đoạn dữ liệu. Máy gửi sẽ truyền lại các đoạn dữ liệu không có tin báo nhận. Dịch vụ phân phối dữ liệu tin cậy rất cần thiết đối với các ứng dụng như truyền tập tin, cơ sở dữ liệu, xử lý giao dịch, và các ứng dụng có yêu cầu dữ liệu phải được đảm bảo phân phối thành công.

Ví dụ : TCP - gửi thư bảo đảm

Dịch vụ gửi thư bảo đảm là một ví dụ minh họa tương tự hoạt động của TCP. Tưởng tượng rằng bạn đang sống ở San Francisco và muốn gửi một quyển sách cho mẹ bạn đang sống ở New York. Giả sử rằng bưu điện chỉ cho phép gửi thư mà không cho gửi bưu phẩm. Bạn thực hiện tháo rời sách và đóng gói các trang sách vào các bì thư riêng. Để đảm bảo mẹ bạn có thể sắp xếp thành quyển sách chính xác như ban đầu, bạn đánh số các bì thư. Bạn ghi địa chỉ các bì thư và gửi chúng đi với dịch vụ gửi thư bảo đảm. Bưu điện sẽ gửi đi bằng nhiều cách máy bay, tàu hỏa, xe thư ... nhưng bởi vì đây là thư bảo đảm bưu điện sẽ phải lấy chữ ký xác nhận đã nhận thư từ mẹ bạn và gửi nó cho bạn.

Gửi từng lá thư một sẽ nhàn chán vì thế bạn sẽ gửi cùng lúc một vài lá thư thay vì chỉ gửi 1. Bưu điện một lần nữa sẽ gửi từng lá thư đi bằng nhiều cách máy bay, tàu hỏa, xe thư ... nhưng bởi vì đây là thư bảo đảm bưu điện sẽ phải lấy chữ ký xác nhận đã nhận thư từ mẹ bạn cho từng lá thư và gửi nó cho bạn. Nếu một lá thư bị mất bạn sẽ không nhận được chữ ký xác nhận và bạn có thể gửi lại những trang sách đó cho mẹ bạn. Sau khi nhận được tất cả các lá thư, mẹ bạn sẽ sắp xếp chúng lại theo thứ tự và ghép chúng lại thành quyển sách ban đầu.

Header TCP



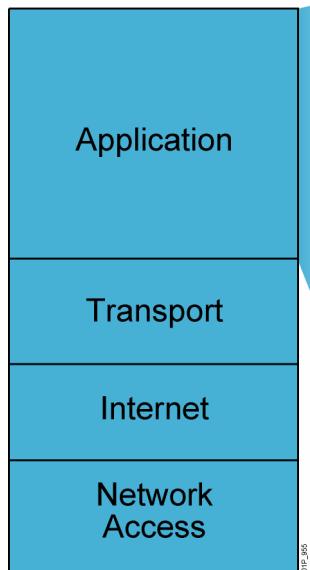
Module 5-12

Các đoạn dữ liệu TCP được đóng gói vào gói tin IP. Header của TCP cung cấp các thông tin cho hoạt động của giao thức TCP.

- **Cổng nguồn (Source port)** : số nguyên 16 bit của cổng đang gọi.
- **Cổng đích (Destination port)** : số nguyên 16 bit của cổng được gọi.
- **Số tuần tự (Sequence number)** : số tuần tự của octet dữ liệu đầu tin trong đoạn (segment) này, được sử dụng để đảm bảo dữ liệu nhận được sắp xếp đúng trình tự (32 bit)
- **Số tin báo nhận (Acknowledgment number)** : octet TCP được mong đợi kết tiếp (32 bit)
- **Chiều dài header (Header length)** : chiều dài của header TCP tính bằng đơn vị 32-bit (4 bit)
- **Dành riêng (Reserved)** : đặt về 0 (3 bit)
- **Bit điều khiển (Control bits)**: dùng cho các chức năng điều khiển như thiết lập, tránh nghẽn, kết thúc phiên (9 bit) (mỗi bit có ý nghĩa riêng và được xem là 1 cờ hiệu (flag))
- **Window**: số octets mà thiết bị sẽ chấp nhận trước khi gửi tin báo nhận (16 bit)
- **Checksum** : Checksum được tính toán dựa trên header và nội dung khôi dữ liệu TCP (16 bit)
- **Urgent**: chỉ đến cuối của thông tin urgent (16 bit)

- **Options:** tùy chọn được thêm vào header nhằm đảm bảo đủ chiều dài của header TCP (0 hoặc 32 bit, nếu có)
- **Dữ liệu (Data) :** Khối dữ liệu của lớp ứng dụng bên trên (kích thước thay đổi)

Tổng quan lớp ứng dụng mô hình TCP/IP



- Truyền file
 - FTP
 - TFTP
 - Network File System
- E-mail
 - Simple Mail Transfer Protocol
- Login từ xa
 - Telnet
 - rlogin
- Quản trị mạng
 - Simple Network Management Protocol
- Quản trị tên miền
 - Domain Name System

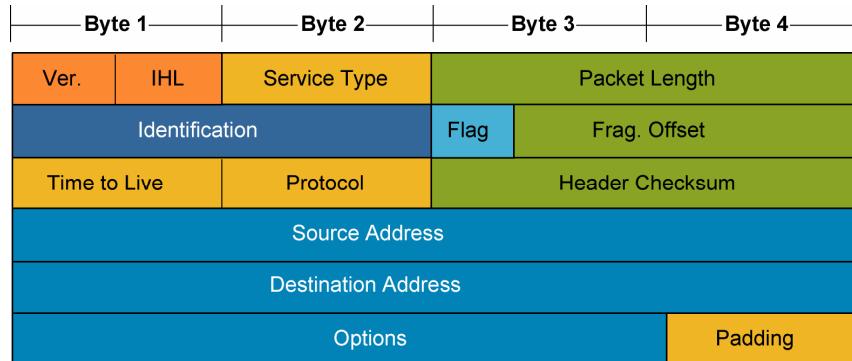
Module 5-14

Lớp ứng dụng mô hình TCP/IP

Một số ứng dụng tiêu biểu của TCP/IP:

- **File Transfer Protocol (FTP):** dịch vụ truyền file tin cậy, là dịch vụ hướng kết nối sử dụng TCP để truyền tập tin giữa 2 máy. FTP hỗ trợ tập tin nhị phân và văn bản theo cả 2 chiều.
- **Trivial File Transfer Protocol (TFTP):** TFTP là dịch vụ truyền file phi kết nối sử dụng UDP. Routers dùng TFTP để truyền tập tin cấu hình cũng như Cisco IOS.
- **Telnet:** Telnet cung cấp khả năng truy cập hệ thống từ xa. Telnet cho phép người dùng login vào máy từ xa và thực thi cách lệnh.

Ánh xạ lớp 3 - lớp 4



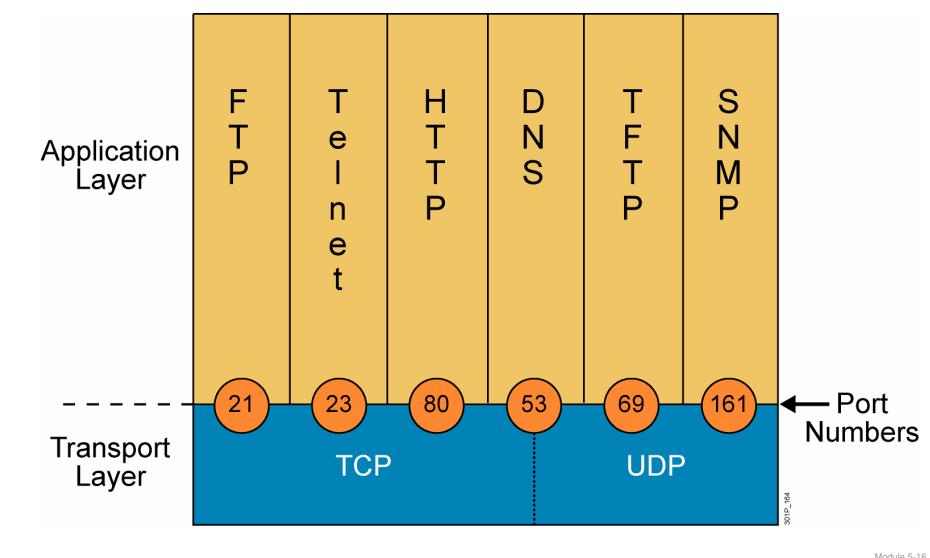
Module 5-15

Phần này chúng ta tập trung vào trường protocol trong header của gói tin IP. Giao thức IP sử dụng số hiệu của trường protocol trong gói tin để chỉ ra giao thức lớp trên tương ứng sẽ xử lý gói tin đó, mỗi số hiệu này tương ứng với 1 giao thức khác nhau.

Máy tính hoặc thiết bị mạng sẽ đọc số hiệu protocol trong header của gói tin so sánh nó với danh sách trong bảng giao thức và chuyển gói tin đến giao thức tương ứng. Ví dụ nếu số hiệu protocol là 6, IP sẽ chuyển dữ liệu đó cho TCP. Ví dụ nếu số hiệu protocol là 17, IP sẽ chuyển dữ liệu đó cho UDP.

Hầu hết các thông tin sử dụng TCP hoặc UDP, chúng sử dụng IP là lớp mạng để vận chuyển dữ liệu. Có khoảng 100 giao thức lớp vận chuyển đăng ký số hiệu protocol để sử dụng IP như dịch vụ vận chuyển dữ liệu.

Ánh xạ lớp 4 - ứng dụng



UDP và TCP sử dụng cổng phần mềm nội tại để hỗ trợ các truyền thông giữa những thiết bị mạng khác nhau.

Mỗi máy có thể mở nhiều phiên đồng thời kết nối với một hay nhiều máy tính khác. Mỗi phiên phải được phân biệt với phiên khác, điều đó được thực hiện nhờ vào số hiệu cổng (port number). Các phiên này sẽ được ghép thông qua cùng card mạng. Các đoạn dữ liệu từ các phiên khác nhau có thể được truyền xen kẽ thông qua card mạng. Cổng có thể được xem là một hàng đợi mà ở đó các đoạn dữ liệu sẽ đi qua.

tổ chức (Internet Assigned Numbers Authority - IANA) điều phối số hiệu cổng. Một số ứng dụng phổ biến sẽ được gán các cổng cố định được nhiều người biết (well-known port). Ví dụ, Telnet luôn luôn dùng cổng 23. Những ứng dụng khác sử dụng cổng được gán động, mặc dù chúng cũng được giới hạn trong một khoảng cụ thể. Các thiết bị đầu cuối dùng cổng được nhiều người biết hoặc cổng được đăng ký để chỉ định các ứng dụng đích. Cổng chính định các phiên lớp trên được gán động trong khoảng 49152 đến 65535.

Ứng dụng dùng UDP

- **Trivial File Transfer Protocol (TFTP):** TFTP giao thức truyền file đơn giản. Thường được sử dụng để sao chép và cài đặt hệ điều hành thiết bị từ các file nằm trên máy chủ TFTP. Ứng dụng TFTP nhỏ hơn FTP, và sử dụng phổ biến trong mạng để truyền file đơn giản. TFTP không có cơ chế kiểm tra lỗi và sót tuần tự.

- **Simple Network Management Protocol (SNMP):** SNMP dùng để theo dõi quản trị mạng, các thiết bị, và thông tin về hiệu suất của mạng. SNMP gửi các thông điệp cho phép các phần mềm quản trị mạng điều khiển thiết bị.

Ứng dụng dùng TCP

- **FTP:** FTP là ứng dụng truyền file đầy đủ tính năng bằng cách sử dụng các trình ứng dụng client trên máy tính nối kết vào máy chủ FTP để truyền file.

- **Telnet:** Telnet cho phép giải lập phiên thiết bị cuối (terminal) tới một máy từ xa, thường là máy UNIX, Router, hoặc Switch. Với trình mô phỏng thiết bị cuối, bạn có thể quản trị thiết bị mạng như thể bạn đấu nối trực tiếp bằng thiết bị cuối. Telnet chỉ hữu ích với các hệ thống dùng giao diện dòng lệnh nó không hỗ trợ môi trường giao diện đồ họa. Bởi vì Telnet gửi thông điệp ở dạng không mật mã hóa nên kém an toàn, bạn có thể dùng Secure Shell (SSH) thay thế cho telnet để mật mã hóa dữ liệu.

The figure shows the range of port numbers available for each protocol and some of the corresponding applications.

Các cổng được nhiều người biết (Well-Known port)

Các cổng này do IANA gán và có giá trị nhỏ hơn 1023. Những cổng này được gán cho các ứng dụng cẩn bản trên Internet.

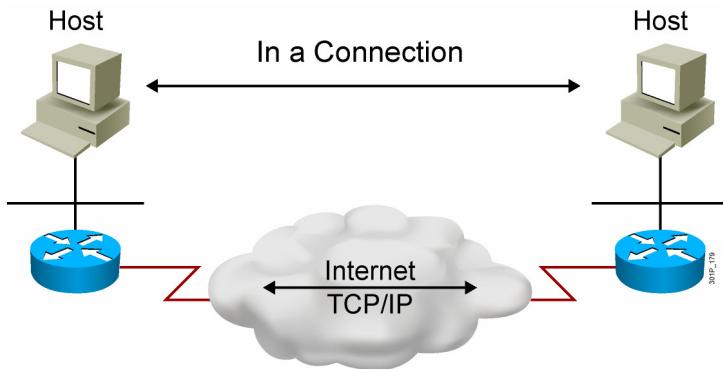
Các cổng được đăng ký (Registered Port)

Các cổng được đăng ký được IANA liệt kê trong khoảng từ 1024 đến 49151. Những cổng này được dùng cho các ứng dụng độc quyền chẳng hạn như Lotus Mail.

Các cổng gán động (Dynamically Assigned Port)

Các cổng động được gán trong khoảng từ 49152 đến 65535. Các cổng này được gán động trong suốt quá trình hoạt động của các phiên.

Thiết lập kết nối



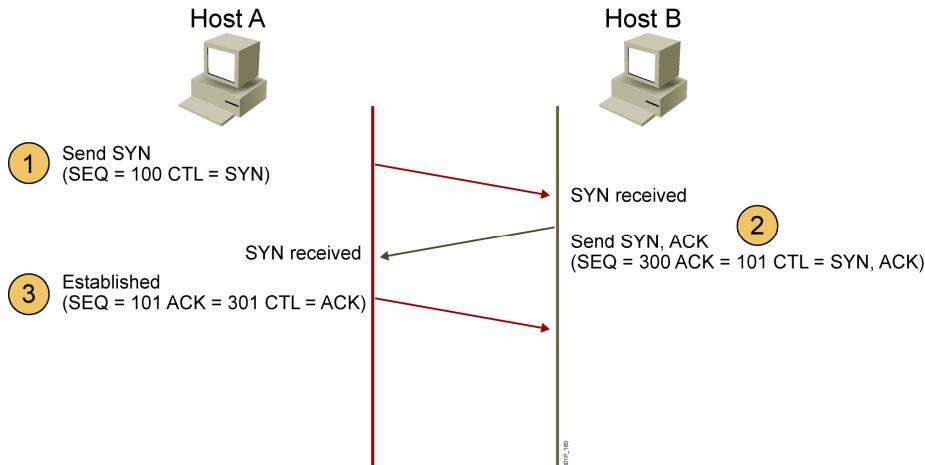
Module 5-18

Người sử dụng dịch vụ vận chuyển tin cậy phải thiết lập một phiên hướng kết nối giữa 2 máy.

Để bắt đầu truyền dữ liệu, cả hai ứng dụng gửi và nhận phải thông báo cho hệ điều hành tương ứng của chúng yêu cầu thiết lập một kết nối. Một máy khởi tạo kết nối phải được chấp nhận bởi máy còn lại. Các khôi chúc năng của 2 hệ điều hành truyền thông với nhau bởi việc gửi các thông điệp thông qua mạng để kiểm tra quyền hạn và tính sẵn sàng của cả hai phía.

Sau khi đồng bộ thành công, hai hệ thống đầu cuối thiết lập một kết nối và dữ liệu có thể bắt đầu được truyền nhận. Trong suốt quá trình truyền thông, 2 máy tiếp tục kiểm tra rằng kết nối vẫn còn hợp lệ và được duy trì.

Bắt tay ba bước



Module 5-19

TCP sử dụng tiến trình bắt tay 3 bước (three-way handshake) để thiết lập kết nối. Tiến trình này bao gồm việc đặt bit đồng bộ (synchronization - SYN) bit và bit tin báo nhận (acknowledgment - ACK) trong các đoạn dữ liệu giữa 2 thiết bị. Một chức năng quan trọng khác được thực hiện trong giai đoạn thiết lập đó là thiết bị thứ nhất thông báo cho thiết bị thứ hai giá trị số tuần tự khởi tạo (initial sequence number - ISN), tham số này dùng để theo dõi số lượng dữ liệu trong kết nối

Thủ tục thiết lập kết nối (TCP Connection Setup Procedure)

Bước 1 : thiết bị gửi khởi tạo gửi segment đồng bộ cho thiết bị nhận (trong đó bit SYN được đặt), bắt đầu quá trình bắt tay.

Lưu ý : segment đồng bộ chỉ ra cổng mà người gửi muốn kết nối. segment này cũng chứa số ISN được dùng trong quá trình gửi tin báo nhận (acknowledgment).

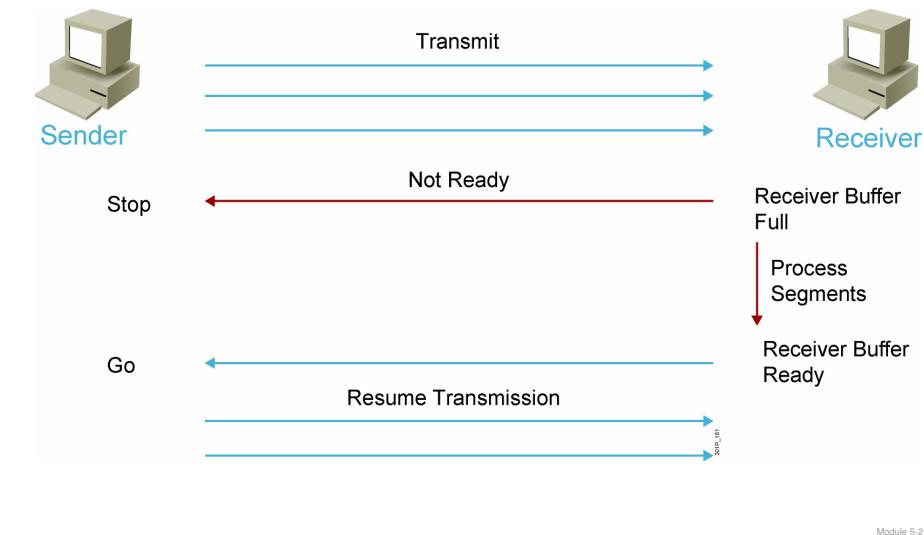
Bước 2. thiết bị nhận đáp ứng lại với segment có bit SYN và ACK được đặt để tiến hành thỏa thuận kết nối và tin báo nhận cho quá trình đồng bộ từ thiết bị gửi.

Lưu ý : thiết bị nhận đáp ứng bằng cách chỉ định giá trị số tuần tự của byte dữ liệu kế tiếp mà nó nhận được trước đó từ thiết bị gửi. Giá trị số tuần tự là ISN của thiết bị gửi cộng thêm 1.

Bước 3. thiết bị gửi gửi tin báo nhận cho segment đồng bộ của thiết bị nhận.

Lưu ý: bit SYN không được đặt trong header TCP, xác nhận rằng quá trình bắt tay ba bước đã hoàn tất.

Điều khiển luồng dữ liệu



Điều khiển luồng dữ liệu ngăn chặn vấn đề của máy gửi làm tràn bộ đệm của máy nhận.

Trong quá trình truyền dữ liệu có thể xảy ra nghẽn đường truyền. Máy gửi có thể là thiết bị tốc độ cao phát sinh dữ liệu nhanh hơn khả năng mà mạng có thể truyền tải. Tương tự vậy, nếu đồng thời nhiều máy tính cùng gửi dữ liệu đến một máy đích, thiết bị đích sẽ nghẽn khi cố gắng nhận tất cả các dữ liệu này. Khi dữ liệu đến quá nhanh so với khả năng xử lý thiết bị nhận sẽ tạm thời lưu chúng vào bộ nhớ. Vùng nhớ này gọi là bộ đệm (buffer), tuy nhiên bộ đệm có kích thước hữu hạn, vì thế có khả năng bộ đệm bị tràn và dữ liệu mới đến sẽ bị bỏ đi.

Bởi vì dữ liệu bị mất là không chấp nhận được, nên chức năng điều khiển luồng dữ liệu là cần thiết. Chức năng vận chuyển có thể thông báo tín hiệu không sẵn sàng cho máy gửi. Tín hiệu này sẽ thông báo máy gửi ngừng truyền dữ liệu và đợi tín hiệu sẵn sàng. Khi máy nhận xử lý các gói tin và tạo đủ chỗ trống trong bộ đệm, chức năng vận chuyển sẽ gửi tín hiệu sẵn sàng cho máy gửi. Khi đó máy gửi sẽ thực hiện tiếp tục quá trình truyền dữ liệu.

Tin báo nhận (Acknowledgment)

TCP là kết nối tin cậy, vì thế máy gửi và máy nhận sử dụng tin báo nhận để phải đảm bảo rằng dữ liệu được gửi thành công không có lỗi và đúng thứ tự.

Cơ chế cửa sổ (Windowing)

Cơ chế cửa sổ cho phép máy gửi truyền một số gói tin trước khi yêu cầu tin báo nhận. Điều đó giúp đảm bảo cân bằng tốc độ và tính tin cậy của đường truyền.

Tin báo nhận TCP



Module 5-23

TCP thực hiện đánh số tuần tự các segment với một tin báo nhận tham khảo. Tin báo nhận tham khảo được gửi trả lại từ máy nhận để báo cho máy gửi biết segment mà máy gửi mong muốn nhận được kế tiếp.

Trong bài này để giảm bớt tính phức tạp trong hoạt động của TCP. Người ta sử dụng phép tăng đơn giản các số nguyên để minh họa số tuần tự và tin báo nhận, trong thực tế số tuần tự dùng theo dõi số byte đã nhận thành công. Trong quá trình sử dụng tin báo báo nhận đơn giản này của TCP, máy gửi sẽ truyền 1 segment, khởi động một bộ định thời (timer), và chờ đợi tin báo nhận trước khi phát segment kế tiếp. Nếu hết thời gian chờ trong bộ định thời mà vẫn không nhận được tin báo nhận, máy gửi sẽ truyền lại segment và khởi động một bộ định thời lần nữa.

Tưởng tượng rằng mỗi segment được đánh số trước khi phát (nhớ rằng thực tế người ta đếm số byte được gửi đi). Ở máy nhận, TCP sẽ sắp xếp lại các segment thành dữ liệu hoàn chỉnh. Nếu một số tuần tự bị thất lạc, segment đó và những segments sau đó có thể phải gửi lại.

Tiến trình tin báo nhận (Acknowledgment Process)

Bước 1. Máy gửi và nhận thỏa thuận mỗi segment phải có tin báo nhận trước khi segment khác được gửi.

Lưu ý : Điều này xảy ra trong quá trình thiết lập kết nối bằng cách đặt kích thước cửa sổ (window size) là 1.

Bước 2. Máy gửi truyền segment số 1 cho máy nhận.

Lưu ý : Máy gửi khởi động một bộ định thời, và chờ đợi tin báo nhận từ máy nhận.

Bước 3. Máy nhận nhận segment 1 và gửi lại tin báo nhận với ACK = 2.

Lưu ý : Máy nhận thông báo segment trước đã nhận thành công và mong đợi segment kế tiếp (segment 2).

Bước 4. Máy gửi nhận được tin báo nhận có ACK = 2 và tiến hành phát segment 2 tiếp cho máy nhận.

Lưu ý : Máy gửi khởi động một bộ định thời, và chờ đợi tin báo nhận từ máy nhận.

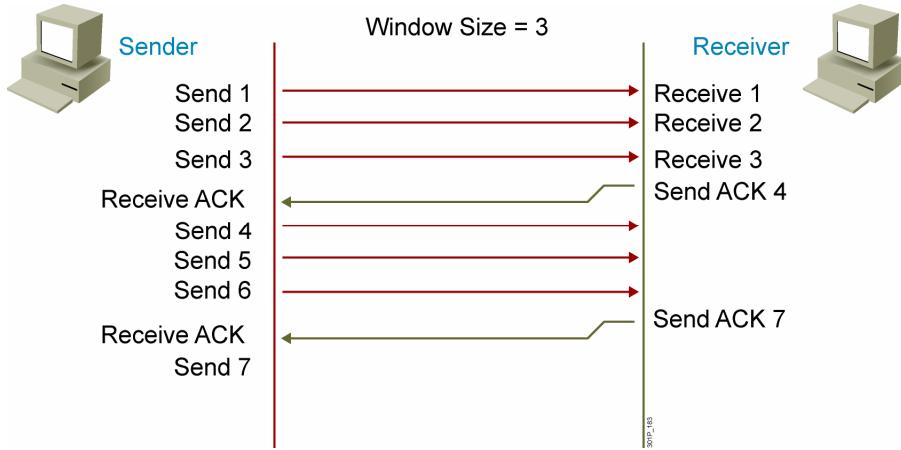
Bước 5. Máy nhận nhận segment 2 và gửi lại tin báo nhận với ACK = 3.

Lưu ý : Máy nhận thông báo segment trước đã nhận thành công..

Bước 6. Máy gửi nhận được tin báo nhận có ACK = 3 và tiến hành phát segment 3 tiếp cho máy nhận.

Lưu ý : Quá trình tiếp tục như vậy cho đến khi tất cả dữ liệu được gửi đi.

Cơ chế cửa sổ cố định



Module 5-25

Trong TCP cửa sổ (window) dùng điều khiển tốc độ truyền dữ liệu đến mức sao cho máy nhận không bị nghẽn và bỏ mất dữ liệu.

Cơ chế cửa sổ cố định (Fixed Windowing)

Trong hầu hết các hiện thực cơ bản dịch vụ truyền dữ liệu hướng kết nối nếu ta bỏ qua vấn đề nghẽn thì cơ chế tín báo nhận cho các segment đủ để đảm bảo tính toàn vẹn, tin cậy của thông tin truyền nhận. Tuy nhiên, nếu máy gửi phải đợi tín báo nhận sau mỗi segment được gửi đi sẽ làm cho thông lượng (throughput) truyền tin rất thấp, nó phụ thuộc vào thời gian quay vòng tín hiệu (round-trip time - RTT) từ lúc gửi dữ liệu đến khi nhận được tín báo nhận.

Thực tế đa số các giao thức truyền tin cậy hướng kết nối đều cho phép gửi nhiều cùng lúc trước khi chờ tín báo nhận. Điều này là hợp lý vì có một khoảng thời gian khả dụng sau khi máy gửi hoàn tất việc phát segment cho đến khi tín báo nhận được gửi trả lại và máy gửi xử lý nó. Trong thời gian này, máy gửi có thể truyền tiếp các segment, đòi hỏi cửa sổ ở máy nhận phải đủ lớn để xử lý nhiều hơn 1 segment ở mỗi thời điểm. Cửa sổ là số segment dữ liệu mà máy gửi được phép truyền mà không cần chờ tín báo nhận.

Cơ chế cửa sổ cho phép chỉ định số lượng segment được gửi đến máy nhận trước khi chờ tín báo nhận, nhờ đó sẽ giảm được độ chậm trễ. Thời gian trễ (latency) trong trường hợp này là tổng số thời lượng tính từ lúc dữ liệu được gửi cho đến khi tin báo nhận được hồi đáp.

Ví dụ : ném quả bóng

Giả sử có 2 người đứng cách xa nhau 50 bộ (15.24 mét). Một người ném quả bóng về phía người kia, và thời gian di chuyển của bóng là 3 giây. Người thứ hai nhận được bóng và ném trả lại (tin báo nhận - acknowledgment), và cũng mất 3 giây. Thời gian quay vòng (round trip time) là 6 giây. Thực hiện 3 lần như vậy sẽ mất $3 \times 6 = 18$ giây. Nay giờ hãy tưởng tượng người thứ nhất lần lượt ném 3 quả bóng cho người thứ 2. Thời gian để ném 3 quả bóng mất là 3 giây. Người thứ hai ném trả lại một quả bóng để thông báo đã nhận được 3 quả bóng và thời gian này cũng mất 3 giây. Như vậy tổng thời lượng trong trường hợp này chỉ là 6 giây (dĩ nhiên ta bỏ qua thời gian xử lý của 2 người).

Tiến trình xử lý của cơ chế cửa sổ cố định với kích thước cửa sổ là 3

Basic Operation, Window Size = 3

Bước 1. Máy gửi và nhận trao đổi kích thước cửa sổ khởi tạo là 3 segment trước khi gửi lại tin báo nhận.

Lưu ý : Xảy ra trong giai đoạn thiết lập kết nối.

Bước 2. Máy gửi truyền segment 1,2 và 3 cho máy nhận.

Lưu ý : Máy gửi truyền các segment, khởi động bộ định thời và chờ tin báo nhận từ máy nhận.

Bước 3. Máy nhận nhận các segment 1, 2 và 3 sau đó gửi trả về tin báo nhận có ACK = 4.

Lưu ý : Máy nhận thông báo segment trước đã nhận thành công.

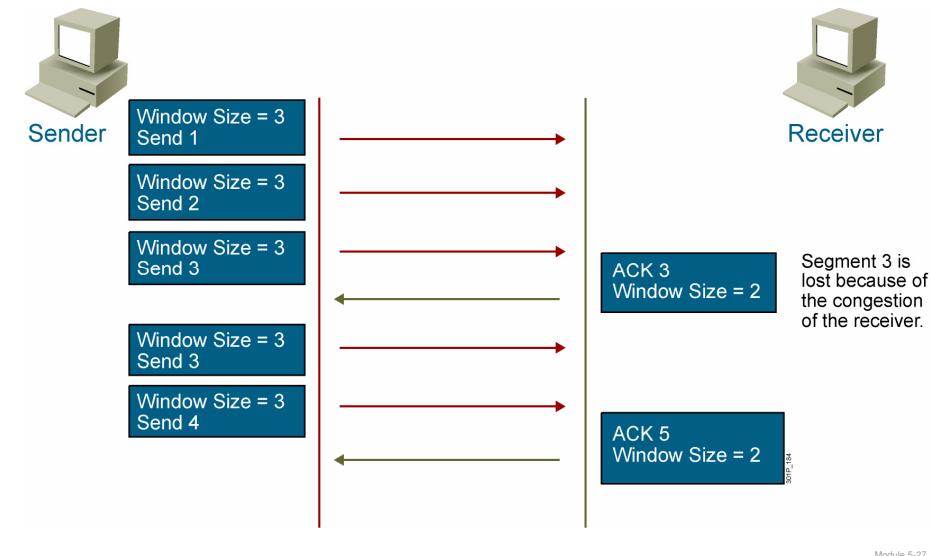
Bước 4. Máy gửi nhận được ACK = 4 sẽ truyền tiếp segment 4,5 và 6 cho máy nhận.

Lưu ý : Máy gửi truyền các segment, khởi động bộ định thời và chờ tin báo nhận từ máy nhận.

Bước 5. Máy nhận nhận các segment 4, 5 và 6 sau đó gửi trả về tin báo nhận có ACK = 7.

Lưu ý : Máy nhận thông báo segment trước đã nhận thành công.

Cơ chế cửa sổ trượt



Cơ chế cửa sổ trượt (Sliding Windowing)

TCP dùng cơ chế cửa sổ trượt để chỉ định số lượng segment, bắt đầu với tin báo nhận mà máy gửi có thể chấp nhận.

Trong cơ chế cửa sổ cố định, kích thước cửa sổ được thiết lập và không thay đổi. Trong cơ chế cửa sổ trượt, kích thước cửa sổ được thỏa thuận khi bắt đầu kết nối và có thể thay đổi động trong suốt phiên TCP. Kỹ thuật cửa sổ trượt tăng tính hiệu quả sử dụng băng thông bởi vì kích thước cửa sổ lớn cho phép nhiều dữ liệu hơn được truyền trước khi phải chờ tin báo nhận. Nếu máy nhận giảm kích thước cửa sổ xuống 0 sẽ làm ngừng quá trình truyền dữ liệu và đợi cho đến khi một kích thước cửa sổ khác > 0 được gửi đi.

Trong hình trên, kích thước cửa sổ là 3. Máy gửi có thể truyền 3 segment cho máy nhận. Ở điểm này, máy gửi phải đợi tin báo nhận từ máy nhận. Sau khi máy nhận xác nhận rằng đã nhận thành công 3 segment, máy gửi có thể truyền tiếp 3 segment. Tuy nhiên, nếu tài nguyên ở máy nhận trở nên khan hiếm, máy nhận có thể giảm kích thước cửa sổ xuống để sao cho nó không trở nên quá tải hoặc phải bỏ mất các segment.

Mỗi tin báo nhận được truyền bởi máy nhận có chỉ định số byte mà máy nhận có thể chấp nhận (kích thước cửa sổ - window size). Điều đó cho phép cửa sổ có thể mở rộng hoặc thu hẹp khi cần thiết để quản trị không gian bộ đệm và tiến trình. TCP duy trì tham số kích thước cửa sổ nghẽn (congestion window size - CWS), nó thường có cùng giá trị với kích thước cửa sổ, nhưng CWS sẽ giảm xuống $\frac{1}{2}$ khi các segment bị bỏ mất. Segment bị bỏ mất khi mạng nghẽn. TCP sử dụng thuật toán back off và restart tinh vi cho phép giảm bớt khả năng nghẽn trên mạng.

Hoạt động của cơ chế cửa sổ trượt

Bước 1. Máy gửi và máy nhận trao đổi nhau giá trị khởi tạo kích thước cửa sổ. Trong ví dụ này, kích thước cửa sổ là 3 segment trước khi một tin báo nhận phải được gửi.

Lưu ý : Xảy ra trong quá trình thiết lập kết nối.

Bước 2. Máy gửi truyền segment 1, 2, và 3 cho máy nhận.

Lưu ý : Máy gửi sẽ chờ tin báo nhận từ máy nhận sau khi đã gửi segment thứ 3.

Bước 3. Máy nhận tiếp nhận segment 1 và 2, nhưng bây giờ chỉ có khả năng xử lý kích thước cửa sổ là 2. ACK = 3 WS = 2

Lưu ý : Khả năng xử lý của máy nhận có thể bị giảm xuống do nhiều nguyên nhân, chẳng hạn như khi CPU đang tìm kiếm cơ sở dữ liệu hoặc đang tải về một tập tin ảnh kích thước lớn.

Bước 4. Máy gửi truyền segment 3 và 4.

Lưu ý : Máy gửi sẽ đợi tin báo nhận từ máy nhận sau khi đã gửi 5 segment, when it has two outstanding segments.

Bước 5. Máy nhận thông báo segment 3 và 4 đã nhận thành công, nhưng kích thước cửa sổ vẫn là 2. ACK = 5 WS = 2

Lưu ý : Máy nhận thông báo segment 3 và 4 đã nhận thành công và yêu cầu gửi cho nó segment 5.

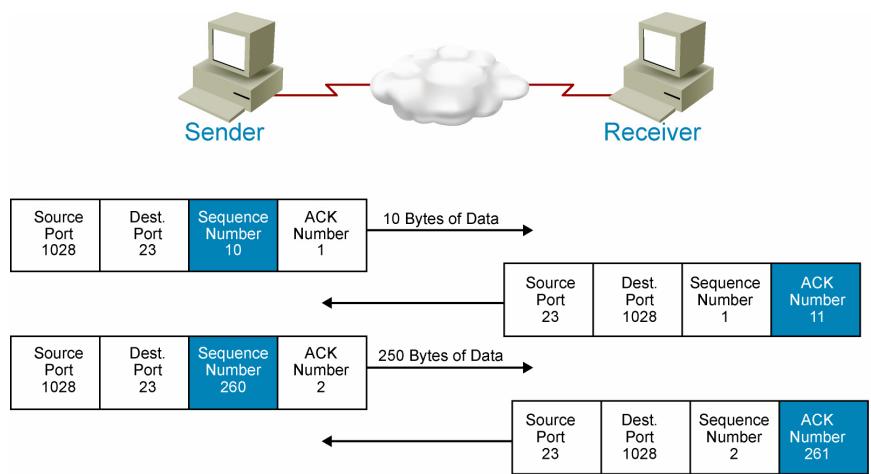
Tối đa thông lượng (Maximize Throughput)

Thuật toán giảm nghẽn dùng cơ chế cửa sổ quản trị tốc độ gửi dữ liệu, giảm thiểu tối đa 2 vấn đề bỏ sót gói và chi phí cho thời gian phục hồi dữ liệu bị bỏ sót vì thế cải thiện hiệu quả.

Đồng bộ toàn cục (Global Synchronization)

Trong khi thuật toán giảm nghẽn dùng cơ chế cửa sổ giúp cải thiện hiệu quả mang một cách tổng quát, thì nó cũng có thể làm ảnh hưởng đến hoạt động mang do hiện tượng đồng bộ toàn cục của tiến trình TCP. Đồng bộ toàn cục xảy ra khi tất cả máy gửi sử dụng cùng một thuật toán và hoạt động đồng bộ. Tất cả máy gửi đều chịu ảnh hưởng của nghẽn và cùng lúc thực hiện back off. Sau đó lại cùng restart tạo nên những làn sóng nghẽn kề nhau.

Số tuần tự và số tin báo nhận TCP



Module 5-29

TCP thực hiện trật tự của các segment bằng số tuần tự và số tin báo nhận trong headers TCP.

Mỗi segment chứa cổng của máy gửi (source port), cổng của máy nhận (destination port), số tuần tự (sequence number), và số tin báo nhận (acknowledgment number). Các cổng được thiết lập trong quá trình khởi tạo kết nối TCP, và chúng duy trì tính trong suốt kết nối. Máy gửi tạo ra số tuần tự trước khi gửi các segment đi. Mỗi segment đến với một số ACK tham khảo. TCP tiến hành sắp xếp lại các segment theo thứ tự ở máy nhận. Chú ý rằng trên hình số tuần tự tính theo số byte dữ liệu được gửi trong mỗi segment.

Tóm tắt

- Mục đích của lớp vận chuyển là che dấu các yêu cầu của lớp mạng khỏi lớp ứng dụng.
- Vận chuyển hướng kết nối cung cấp dịch vụ tin cậy; vận chuyển phi kết nối cung cấp dịch vụ cố gắng hết khả năng.
- UDP là giao thức hoạt động lớp vận chuyển và cung cấp cho ứng dụng khả năng truy cập lớp mạng không có chi phí cho các cơ chế tin cậy như TCP. UDP là phi kết nối, giao thức phân phối cố gắng hết khả năng của mình.
- TCP là giao thức hoạt động lớp vận chuyển và cung cấp cho ứng dụng khả năng truy cập lớp mạng. TCP là giao thức hướng kết nối, cung cấp kiểm tra lỗi, phân phối tin cậy, hoạt động song công, và cung cấp cơ chế khôi phục dữ liệu.

Module 5-30

Tóm tắt (tiếp tục)

- TCP/IP hỗ trợ một số ứng dụng bao gồm FTP (cho phép truyền file nhị phân và văn bản), TFTP (truyền file cấu hình và Cisco IOS), và Telnet (cung cấp khả năng truy cập máy tính khác từ xa).
- IP dùng số protocol trong header gói tin để xác định giao thức nào sẽ xử lý gói tin tương ứng.
- Cổng được dùng để ánh xạ giữa lớp 4 và ứng dụng.

Module 5-31

Tóm tắt (tiếp tục)

- Điều khiển luồng dữ liệu nhằm tránh vấn đề truyền dữ liệu làm tràn bộ nhớ của máy nhận và giảm hiệu suất mạng.
- TCP cung cấp số tuần tự của các segment với một tin báo nhận tham khảo. Khi một segment được gửi đi và máy nhận được tin báo nhận của nó thì segment sẽ được gửi tiếp.

Module 5-32

Tóm tắt (tiếp tục)

- Kích thước cửa sổ (window) của TCP giảm tốc độ truyền dữ liệu tới một mức ở đó nghẽn và mất dữ liệu không xảy ra. Kích thước cửa sổ cho phép TCP đặc tả số lượng các segment không tin báo nhận được gửi.
- Cửa sổ cố định có giá trị không thay đổi được chọn phù hợp với dòng dữ liệu các segment.
- Cửa sổ trượt là cửa sổ mà có thể thay đổi kích thước động để phù hợp với dòng dữ liệu các segment.
- TCP cung cấp trật tự của các segment bằng số tuần tự và số tin báo nhận trong headers TCP.

Module 5-33



Module 5-34

Bài 6: Khảo sát tiến trình phân phối gói tin



Xây dựng một mạng đơn giản

Module 6-1

Tổng quan

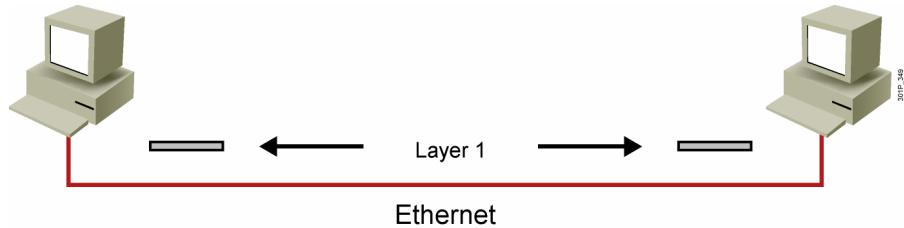
Các bài học trước đã bàn về các thành phần trong truyền thông từ máy đến máy. Điều quan trọng nhất là phải hiểu được cách thức các thành phần này tương tác với nhau. Bài học này sẽ trình bày về vấn đề này.

Mục tiêu

Kết thúc bài học này, học viên sẽ có khả năng mô tả cách thức kết nối từ máy đến máy được thiết lập và duy trì :

- Mô tả chức năng các thiết bị lớp 1
- Mô tả chức năng các thiết bị lớp 2
- Mô tả địa chỉ lớp 2
- Mô tả chức năng các thiết bị lớp 3
- Mô tả địa chỉ lớp 3
- Mô tả ánh xạ địa chỉ giữa lớp 2 và lớp 3
- Mô tả bảng ARP
- Mô tả quá trình phân phối gói tin (từ máy đến máy)
- Mô tả chức năng của default gateway
- sử dụng các công cụ để xác định đường đi giữa 2 máy trên mạng

Thiết bị lớp 1



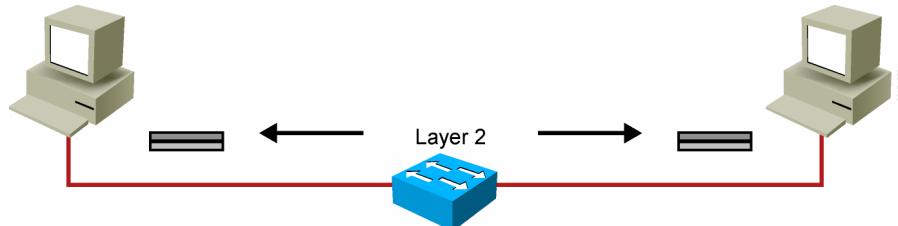
- Thiết bị lớp 1 cung cấp môi trường truyền vật lý và cách mã hóa dữ liệu.
- Ví dụ :
 - Ethernet
 - Serial
 - Bộ lặp lại (Repeater)
 - Giao tiếp vật lý của card mạng

Module 6-2

Lớp 1 định nghĩa phần điện tử, cơ khí, thủ tục và chức năng kích hoạt, duy trì và kết thúc đường truyền vật lý giữa các hệ thống đầu cuối. Ví dụ như đoạn mạng Ethernet, kết nối tuần tự như like Frame Relay và luồng T1. bộ lặp lại (repeater) cung cấp khả năng khuếch đại tín hiệu cũng được xem là thiết bị lớp 1.

Giao tiếp vật lý của NIC cũng được xem là thuộc lớp 1.

Thiết bị lớp 2

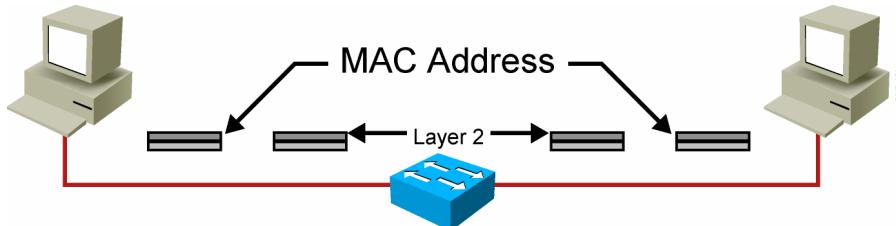


- Thiết bị lớp 2 cung cấp giao tiếp với môi trường truyền vật lý.
- Ví dụ :
 - Card mạng (NIC)
 - Bridge
 - Switch

Module 6-3

Lớp 2 định nghĩa cách thức định dạng dữ liệu phục vụ truyền tin, cách thức truy xuất môi trường truyền vật lý. Những thiết bị này cũng cung cấp một giao tiếp với môi trường truyền vật lý. Ví dụ card mạng, bridge, hoặc switch.

Địa chỉ lớp 2



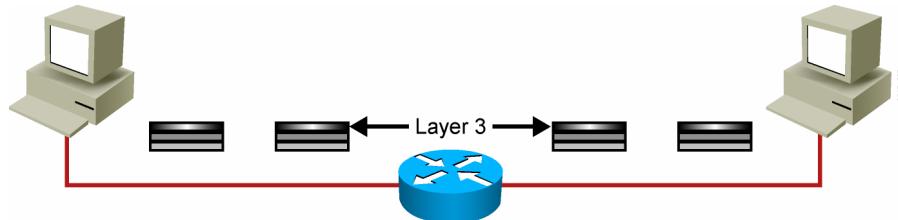
Module 6-4

Để giao tiếp máy tính cần địa chỉ lớp 2.

Giai đoạn đầu tiên khi truyền thông từ máy đến máy được phát triển nhiều giao thức mạng hay còn gọi là hệ điều hành mạng (network operating systems - NOS) ví dụ như Netware, IP, Open Systems Interconnection (OSI), Banyan-Vines đã được sử dụng. Để đạt được tính độc lập NOS thiết bị cần địa chỉ lớp 2 từ đó địa chỉ vật lý MAC được tạo ra.

Địa chỉ MAC được gán cho thiết bị đầu cuối như máy tính, server, máy in ... Trong đa số trường hợp, thiết bị mạng lớp 2 chẳng hạn như bridges và switches không được gán địa chỉ MAC. Tuy nhiên, trong một trường hợp đặc biệt switch có thể được gán địa chỉ MAC.

Thiết bị lớp 3 và chức năng của chúng

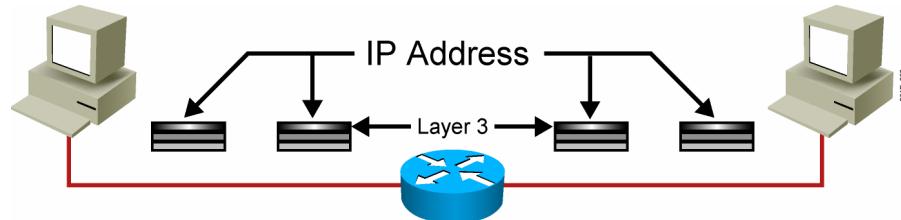


- Lớp mạng cung cấp khả năng nối kết và chọn đường giữa 2 hệ thống đầu cuối.
- Trong máy tính, đó là con đường giữa lớp liên kết dữ liệu và lớp trên của hệ điều hành mạng (NOS).
- Trong router, đó là con đường thực tế gửi dữ liệu trên mạng.

Module 6-5

Lớp mạng cung cấp khả năng nối kết và chọn đường giữa 2 hệ thống đầu cuối thuộc 2 mạng tách biệt. Trong máy tính, đó là con đường giữa lớp liên kết dữ liệu và lớp trên của hệ điều hành mạng (NOS). Trong router, đó là con đường thực tế gửi dữ liệu trên mạng.

Địa chỉ lớp 3

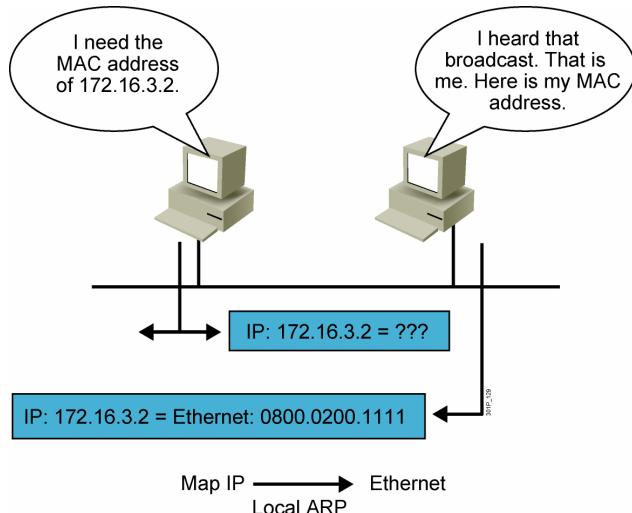


- Mỗi NOS có định dạng địa chỉ lớp 3 riêng.
- OSI dùng địa chỉ NSAP.
- TCP/IP dùng địa chỉ IP.

Module 6-6

Mỗi NOS có định dạng địa chỉ lớp 3 riêng. Ví dụ mô hình OSI dùng địa chỉ NSAP trong khi mô hình TCP/IP dùng địa chỉ IP.

ARP



Module 6-7

Ánh xạ địa chỉ lớp 2 - lớp 3

Để giao tiếp IP trên nền mạng Ethernet cần phải có sự ánh xạ địa chỉ luân lý lớp 3 (địa chỉ IP) và địa chỉ vật lý (địa chỉ MAC) tung ứng cho thiết bị đích. Quá trình này được thực hiện nhờ giao thức phân giải địa chỉ (Address Resolution Protocol - ARP).

Để thực hiện gửi dữ liệu đến máy đích trên mạng Ethernet, máy gửi phải biết địa chỉ vật lý của máy đích. ARP cung cấp dịch vụ cẩn bản ánh xạ địa chỉ IP thành địa chỉ MAC trên mạng Ethernet.

Thuật ngữ phân giải địa chỉ (address resolution) liên quan đến tiến trình gắn kết địa chỉ lớp 3 với địa chỉ lớp 2 của máy đích cục bộ khả chuyển tung ứng. Địa chỉ được phân giải khi thiết bị gửi thông điệp ARP broadcast chứa các thông tin đã biết (địa chỉ IP đích và địa chỉ IP của máy yêu cầu ARP). Thông điệp broadcast được nhận bởi tất cả các thiết bị trên mạng Ethernet. Khi máy đích nhận thấy địa chỉ của mình trùng với IP đích trong gói ARP request, nó sẽ tiến hành trả lời với địa chỉ MAC của nó trong gói ARP reply. Thủ tục phân giải địa chỉ kết thúc khi thiết bị ban đầu nhận được gói ARP reply (chứa địa chỉ MAC) từ máy đích và cập nhật áp xạ IP – MAC vào bảng ARP (hay còn gọi là ARP cache) bảng ARP được dùng để duy trì quan hệ giữa địa chỉ IP và địa chỉ MAC tương ứng.

Mỗi thông tin ánh xạ sẽ được làm tươi mỗi khi máy nguồn gửi dữ liệu máy đích. Nếu không có nhu cầu gửi dữ liệu thì thông tin này sẽ được duy trì trong khoảng thời gian aging-out mặc định là 5 phút (300 giây).

Bảng ARP

Interface:	Internet Address	Physical Address	Type
192.168.1.101	00-04-5a-22-ec-c7	dynamic	
192.168.1.40	00-02-4b-cc-d6-d9	dynamic	
192.168.1.42	00-02-fd-65-9f-82	dynamic	
192.168.1.43	00-03-6b-09-59-29	dynamic	
192.168.1.100	00-02-4b-cc-d6-d0	dynamic	
192.168.1.135	00-03-6d-1e-6a-a5	dynamic	
192.168.1.149	00-50-8b-f7-cf-59	dynamic	

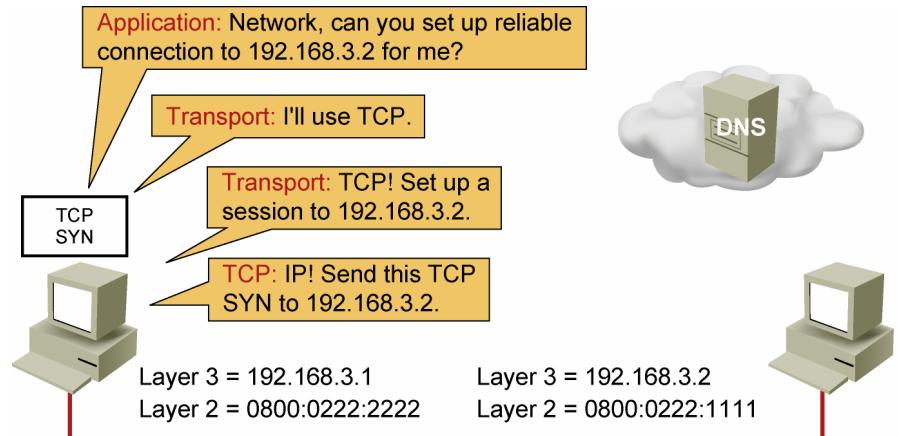
Module 6-8

Bảng ARP hay ARP cache chứa các mảng tin ánh xạ giữa địa chỉ IP và địa chỉ MAC.

Mỗi thiết bị IP trên mạng đều duy trì bảng ARP trong bộ nhớ. Bảng này chứa thông tin ánh xạ IP - MAC. Khi máy tính muốn gửi dữ liệu đến cho máy khác trong cùng một mạng, nó sẽ tìm kiếm thông tin trong bảng ARP. Nếu tìm thấy, máy tính sẽ dùng địa chỉ MAC tương ứng để đóng gói dữ liệu truyền đi trên mạng, nhưng nếu không tìm thấy, ARP sẽ được thực hiện để lấy địa chỉ MAC tương ứng của máy đích.

Bảng ARP được tạo ra và duy trì động, việc thêm và thay đổi ánh xạ địa chỉ thực hiện trên cục bộ từng máy. Các dòng trong bảng ARP thường hết hiệu lực sau một khoảng thời gian mặc định là 5 phút; tuy nhiên, nếu máy tính có nhu cầu truyền dữ liệu tiếp tục đến máy đích thì dòng thông tin tương ứng trong bảng ARP sẽ được làm tươi.

Phân phối gói tin từ máy đến máy (1/22)

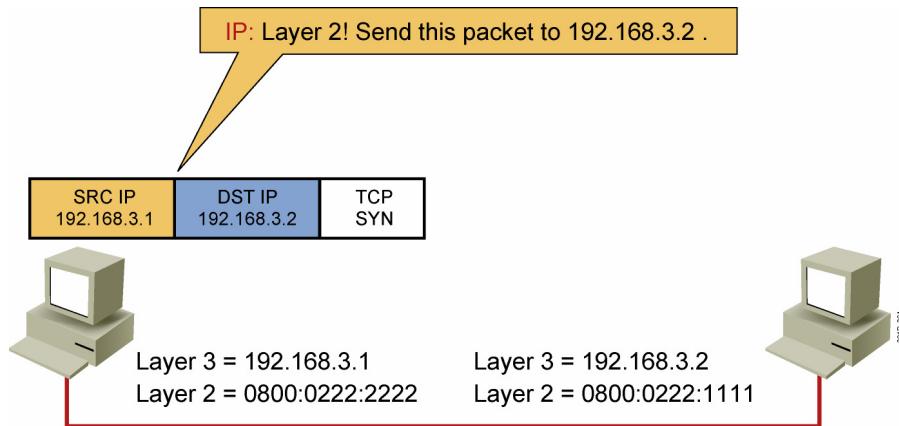


Module 6-9

Trong ví dụ này, một ứng dụng trên máy tính có địa chỉ IP 192.168.3.1 muốn gửi dữ liệu đến máy tính có địa chỉ IP là 192.168.3.2. Ứng dụng muốn sử dụng kết nối tin cậy vì thế nó yêu cầu dịch vụ này từ lớp vận chuyển (transport layer).

Lớp vận chuyển chọn dịch vụ TCP để thiết lập phiên truyền thông (session). TCP khởi tạo phiên truyền thông bằng cách chuyển thông tin header TCP với bit SYN và địa chỉ IP đích là 192.168.3.2.

Phân phối gói tin từ máy đến máy (2/22)



Module 6-10

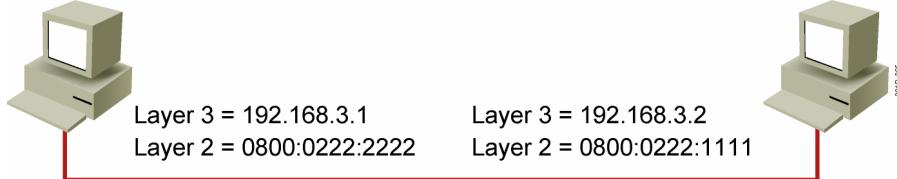
Lớp IP đóng gói dữ liệu SYN của TCP vào gói tin bằng cách gắn thêm vào phía trước dữ liệu TCP địa chỉ lớp 3 của máy gửi và máy nhận. Sau đó chuyển chúng cho lớp 2 để xử lý tiếp tục.

Phân phối gói tin từ máy đến máy (3/22)

Layer 2: ARP, do you have a mapping for 192.168.3.2?

ARP: Is 192.168.3.2 in my ARP table? No, I guess Layer 2 will have to put the packet in the parking lot until I do an ARP.

SRC IP 192.168.3.1	DST IP 192.168.3.2	TCP SYN
-----------------------	-----------------------	------------

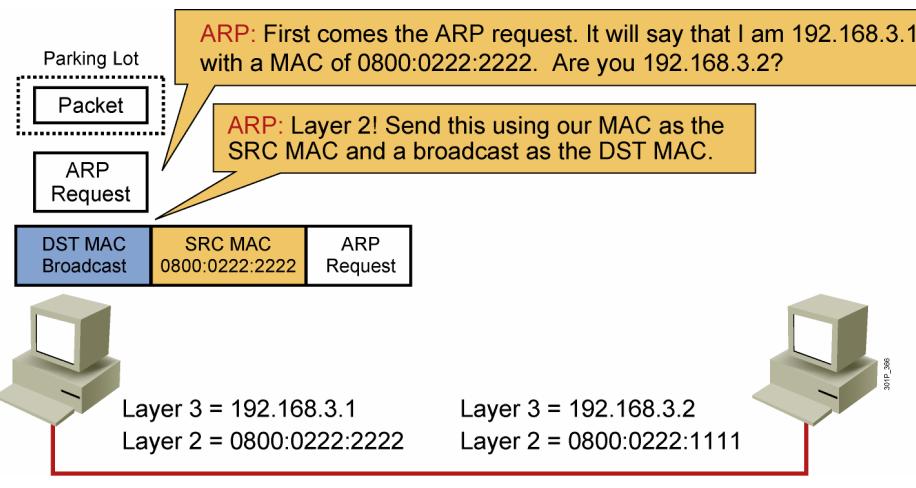


Module 6-11

Lớp 2 thực hiện đóng gói dữ liệu lớp 3 (IP packet) vào trong Frame lớp 2. Để làm điều đó, lớp 2 cần ánh xạ địa chỉ IP - MAC của máy đích bằng cách gửi yêu cầu đến chương trình ARP.

ARP kiểm tra bảng cache của mình. Trong ví dụ này, giả sử rằng máy này chưa bao giờ giao tiếp với các máy khác do đó bảng ARP rỗng. Kết quả là lớp 2 sẽ giữ lại gói tin cho đến khi ánh xạ ARP được tạo ra.

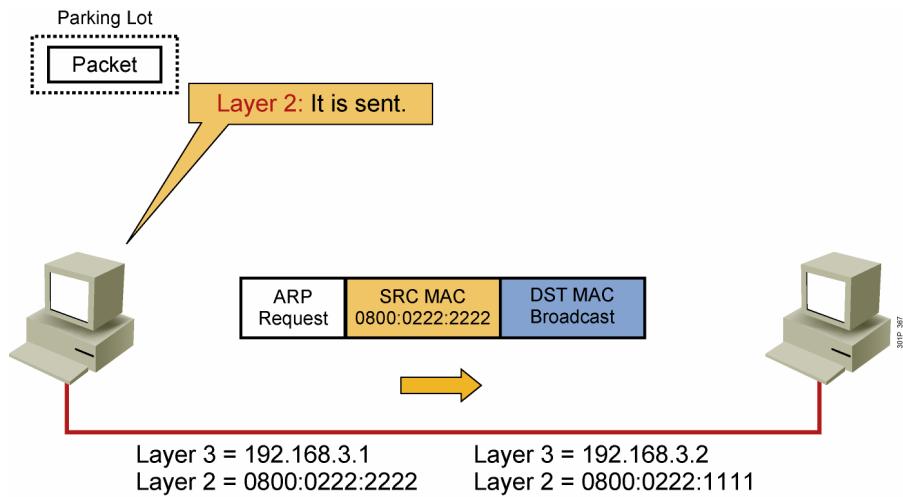
Phân phối gói tin từ máy đến máy (4/22)



Module 6-12

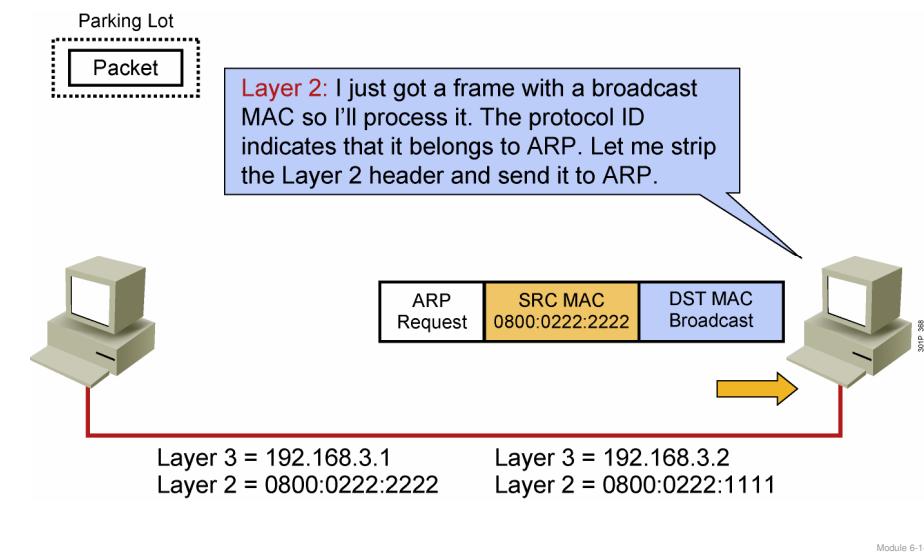
Chương trình ARP xây dựng gói tin ARP Request và chuyển nó cho lớp 2, yêu cầu lớp 2 gửi thông tin với địa chỉ đích là broadcast (tất cả các bit đều là 1). Lớp 2 đóng gói ARP Request trong frame lớp 2 dùng địa chỉ MAC đích là broadcast, và địa chỉ MAC nguồn là của máy yêu cầu phân giải địa chỉ.

Phân phối gói tin từ máy đến máy (5/22)



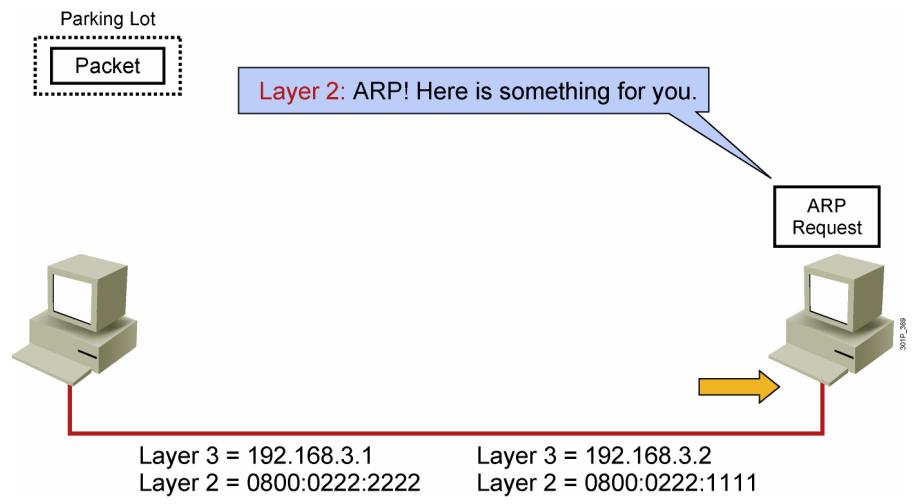
Module 6-13

Phân phối gói tin từ máy đến máy (6/22)



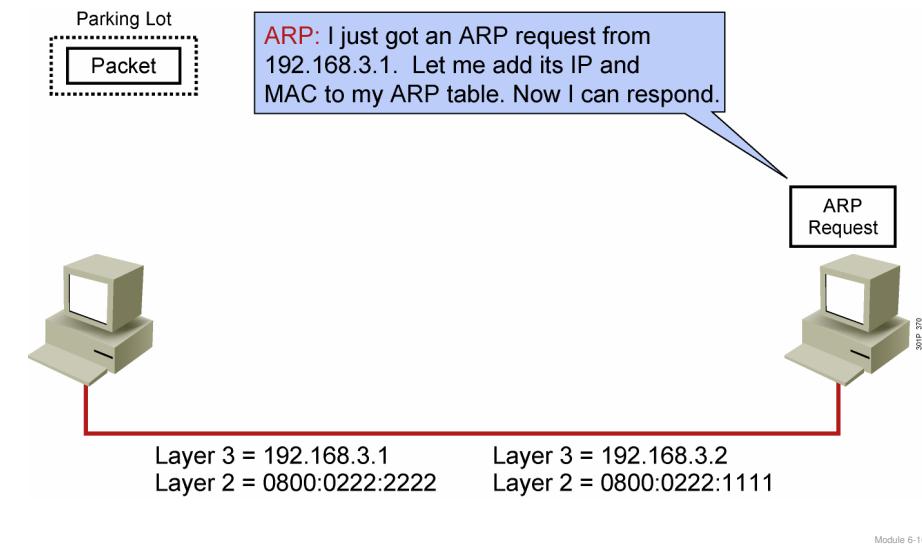
Khi máy 192.168.3.2 nhận được frame, nó sẽ lưu ý địa chỉ broadcast và thực hiện giải đóng gói frame lớp 2.

Phân phối gói tin từ máy đến máy (7/22)



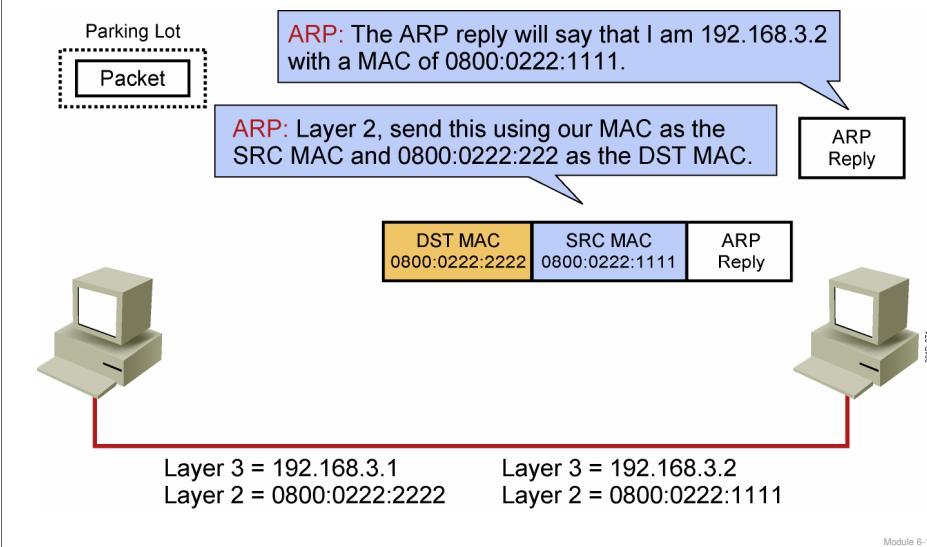
Thông tin ARP Request được chuyển đến cho chương trình ARP.

Phân phối gói tin từ máy đến máy (8/22)



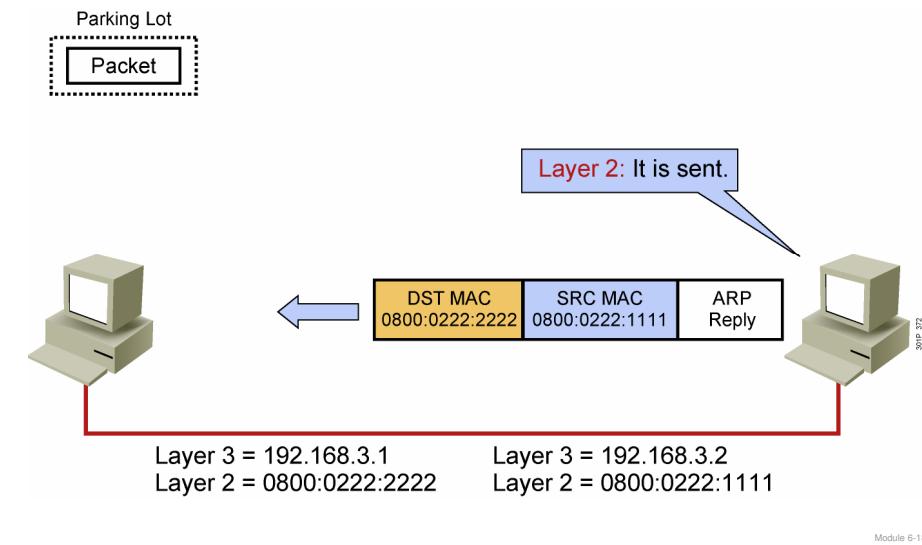
Sử dụng thông tin ARP Request, chương trình ARP cập nhật bảng cache của nó.

Phân phối gói tin từ máy đến máy (9/22)



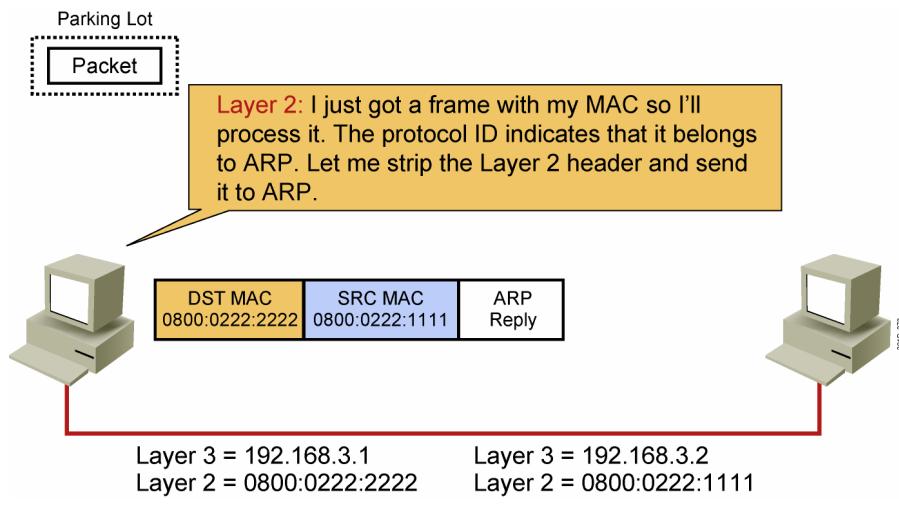
Chương trình ARP xây dựng gói tin ARP Reply và chuyển nó cho lớp 2, yêu cầu lớp 2 gửi đến địa chỉ MAC 0800:0222:2222 (của máy có địa chỉ IP là 192.168.3.1).

Phân phối gói tin từ máy đến máy (10/22)



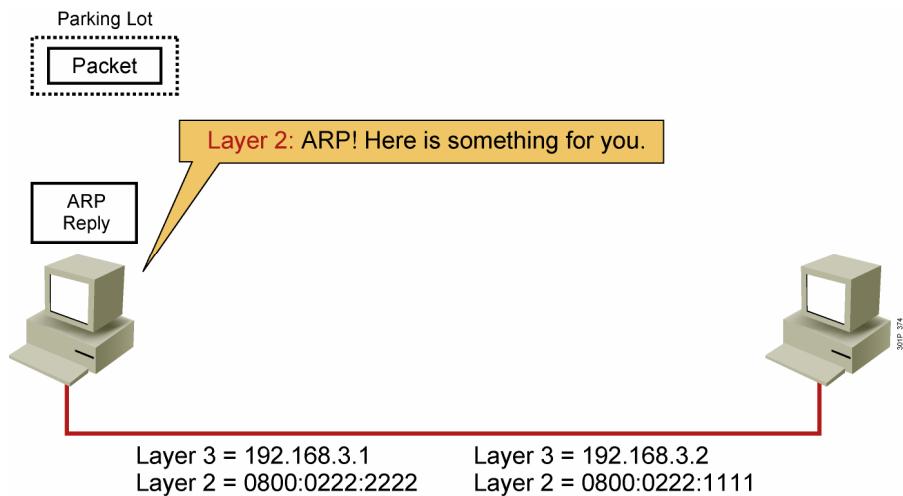
Lớp 2 đóng gói ARP Reply vào frame lớp 2 với địa chỉ MAC đích cung cấp bởi bảng ARP và địa chỉ nguồn của máy gửi.

Phân phối gói tin từ máy đến máy (11/22)



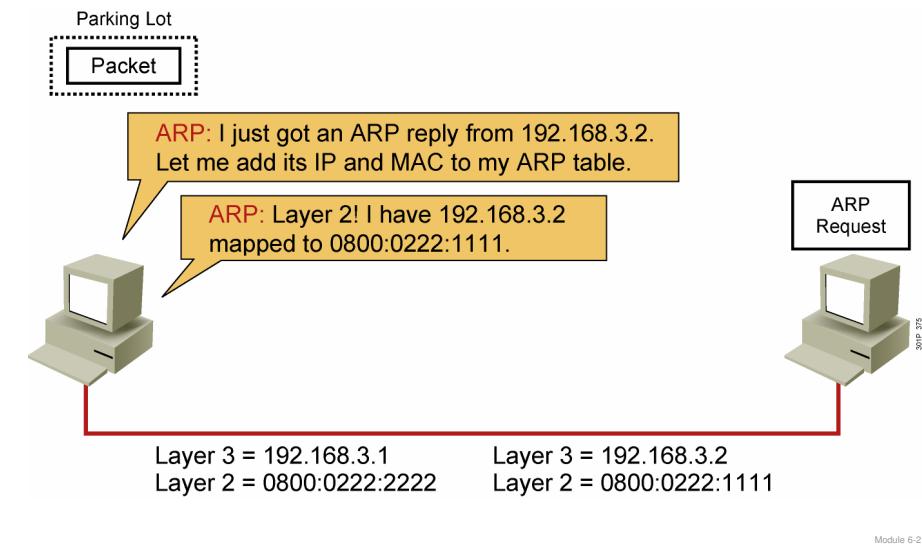
Khi máy 192.168.3.1 nhận được frame, nó lưu ý đến địa chỉ MAC đích là của nó. Máy đích sẽ thực hiện giải đóng gói frame lớp 2

Phân phối gói tin từ máy đến máy (12/22)



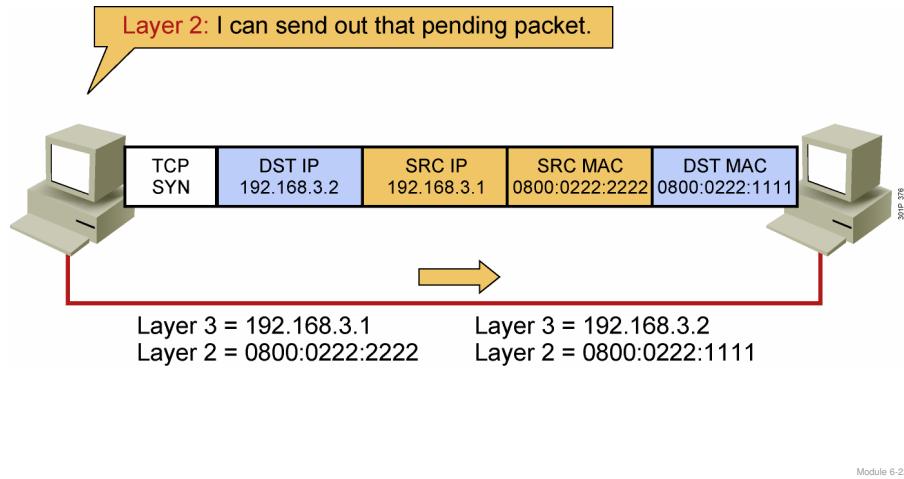
Phần thông tin ARP reply sẽ được chuyển đến cho chương trình ARP.

Phân phối gói tin từ máy đến máy (13/22)



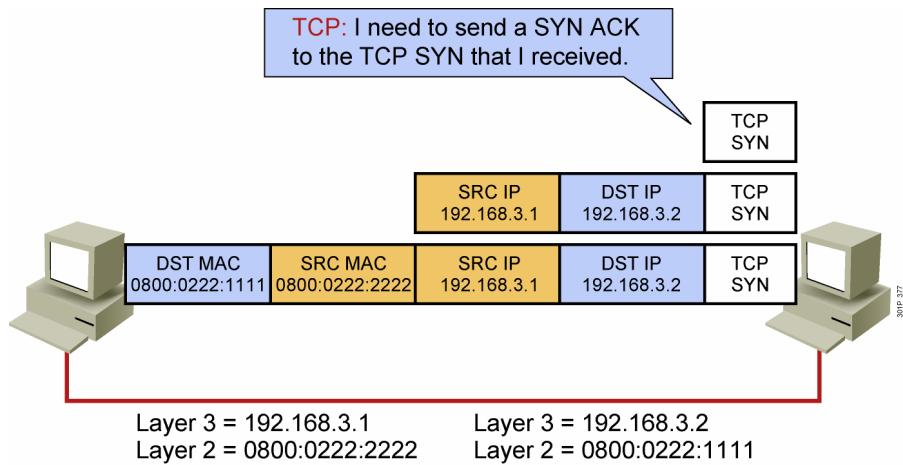
ARP thực hiện cập nhật bảng cache ánh xạ IP – MAC tương ứng.

Phân phối gói tin từ máy đến máy (14/22)



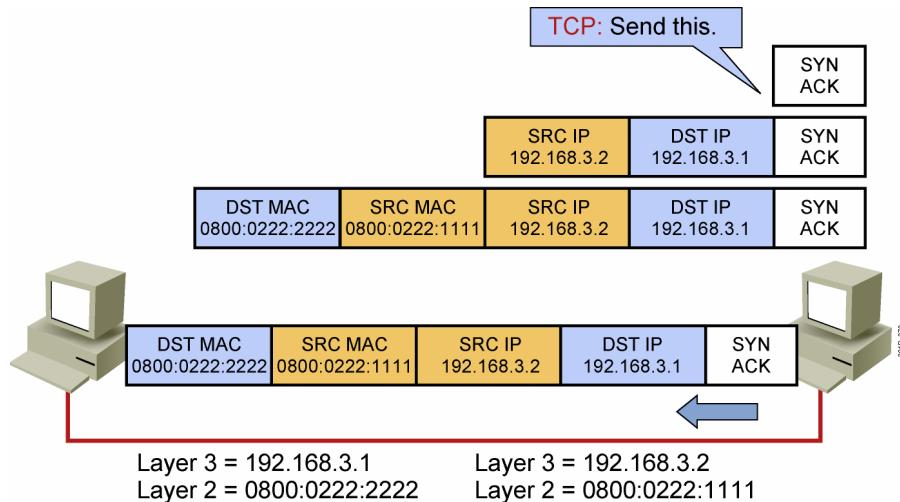
Lớp 2 bây giờ đã có thể gửi gói tin bị treo lúc nãy.

Phân phối gói tin từ máy đến máy (15/22)



Ở máy 192.168.3.2, frame được chuyển lên cho các lớp phía trên (giải đóng gói dữ liệu). Phần PDU tương ứng còn lại được chuyển cho TCP.

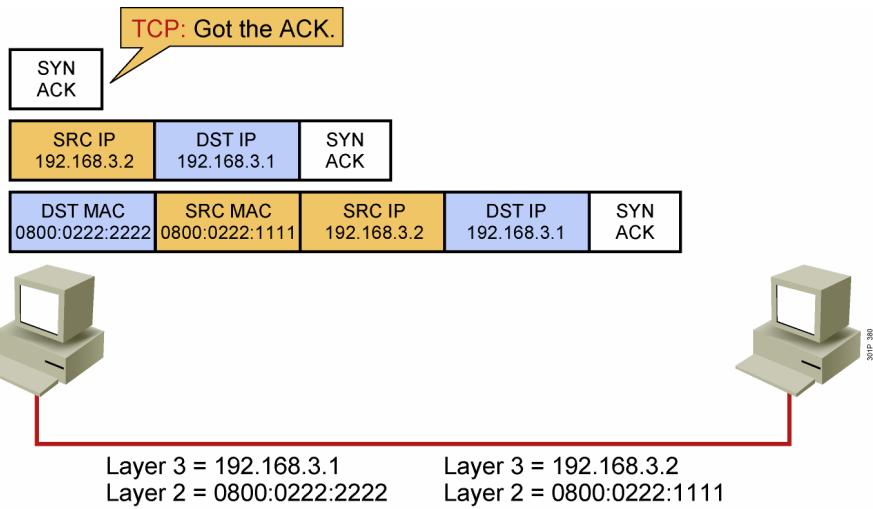
Phân phối gói tin từ máy đến máy (16/22)



Module 6-24

Để trả lời cho SYN, TCP chuyển dữ liệu SYN ACK xuống cho các lớp bên dưới thực hiện đóng gói.

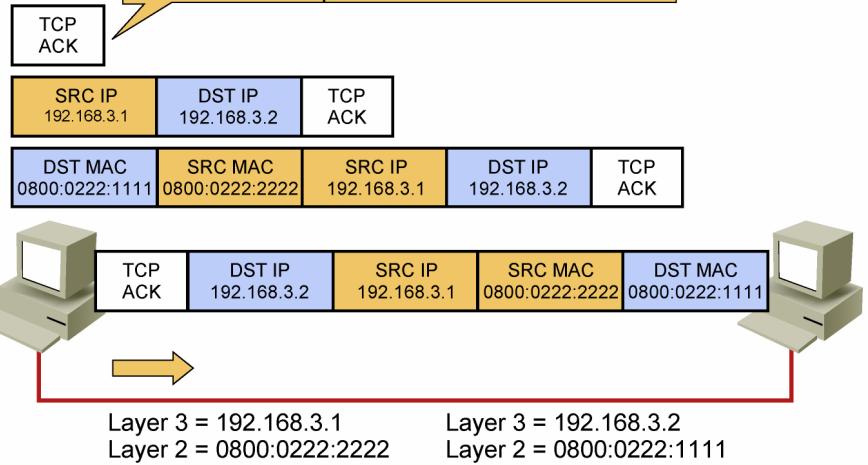
Phân phối gói tin từ máy đến máy (17/22)



Module 6-25

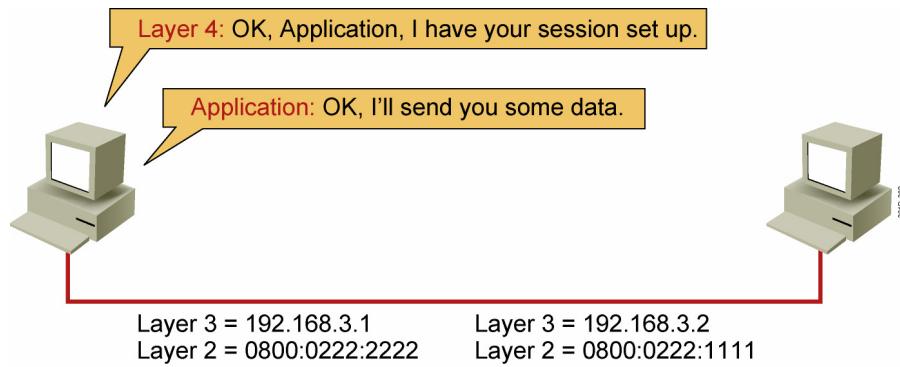
Phân phối gói tin từ máy đến máy (18/22)

TCP: I need to let the other end know I got the SYN ACK to complete the session establishment.



Module 6-26

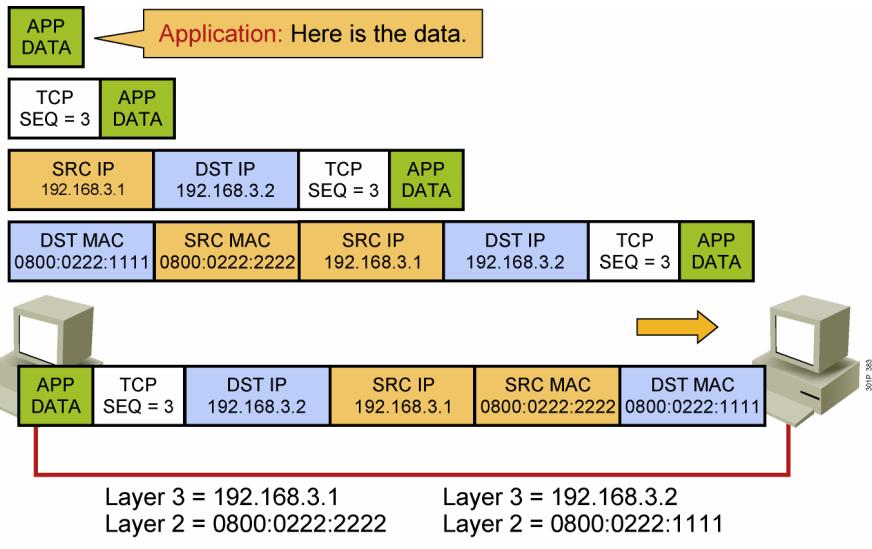
Phân phối gói tin từ máy đến máy (19/22)



Module 6-27

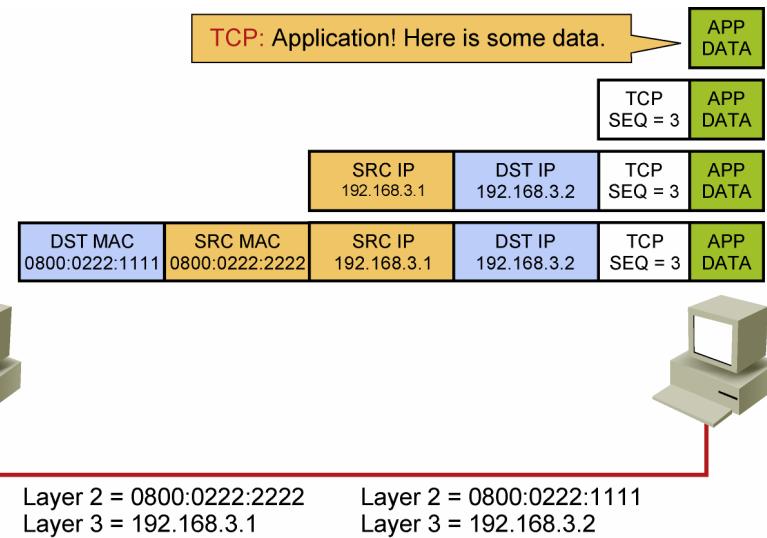
Khi quá trình bắt tay 3 bước (three-way handshake) kết thúc, TCP có thể báo cho ứng dụng biết rằng phiên truyền thông (session) đã được thiết lập.

Phân phối gói tin từ máy đến máy (20/22)



Bây giờ ứng dụng có thể gửi dữ liệu thông qua phiên truyền thông dựa trên TCP để sửa các lỗi nếu có.

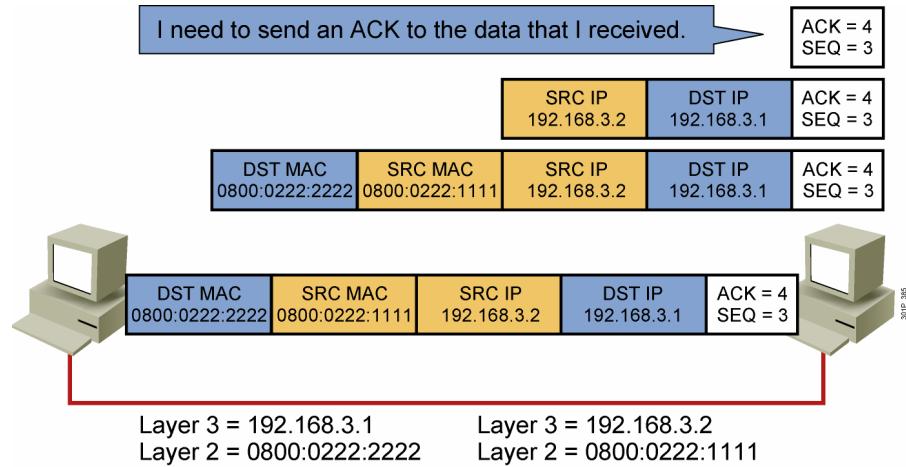
Phân phối gói tin từ máy đến máy (21/22)



Module 6-29

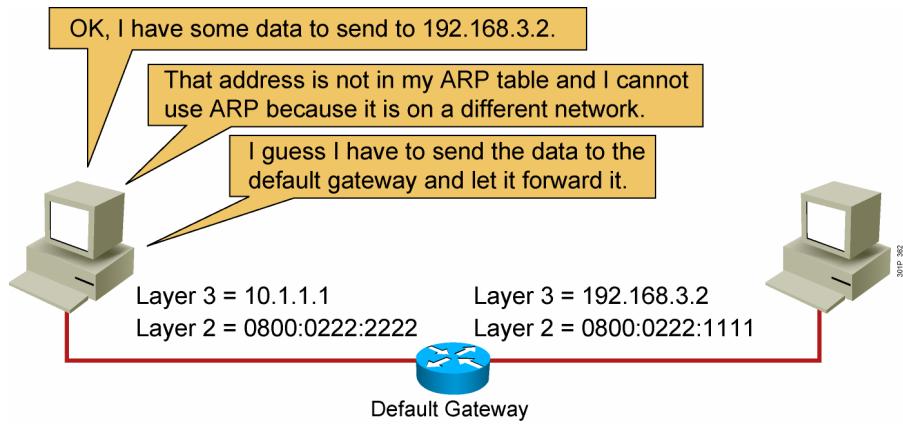
Dữ liệu tiếp tục được trao đổi cho đến khi ứng dụng dừng việc gửi dữ liệu.

Phân phối gói tin từ máy đến máy (22/22)



Module 6-30

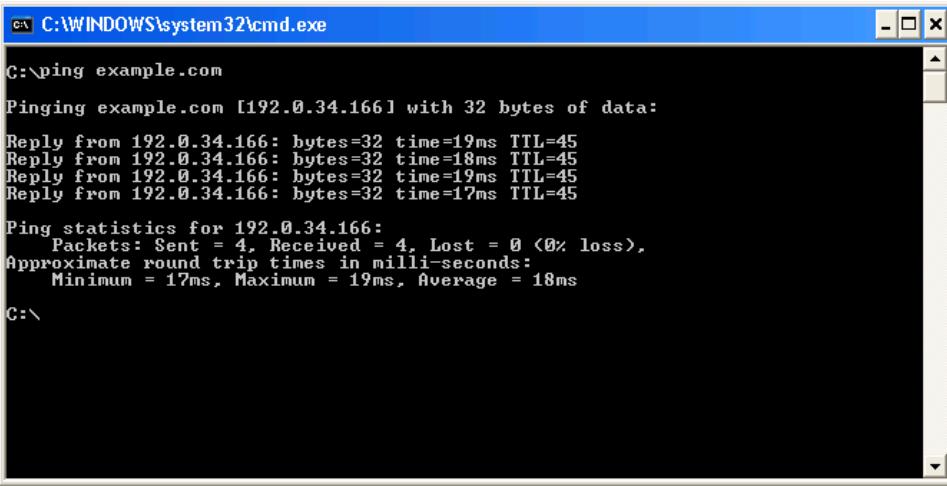
Default Gateway



Module 6-31

Trong ví dụ trước, máy gửi dùng ARP để ánh xạ địa chỉ IP – MAC của máy đích trên cùng một mạng. Nếu 2 máy trên 2 mạng khác nhau, máy gửi phải gửi dữ liệu đến cho default gateway, có nhiệm vụ chuyển tiếp dữ liệu đến máy tích ở một mạng từ xa khác.

Công cụ máy tính : ping



```
C:\>ping example.com

Pinging example.com [192.0.34.166] with 32 bytes of data:
Reply from 192.0.34.166: bytes=32 time=19ms TTL=45
Reply from 192.0.34.166: bytes=32 time=18ms TTL=45
Reply from 192.0.34.166: bytes=32 time=19ms TTL=45
Reply from 192.0.34.166: bytes=32 time=17ms TTL=45

Ping statistics for 192.0.34.166:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 17ms, Maximum = 19ms, Average = 18ms

C:\>
```

Module 6-32

Ping là chương trình máy tính dùng kiểm tra khả năng gửi/nhận thông tin qua mạng IP. Ping hoạt động bằng cách gửi gói ICMP “echo request” cho máy đích và lắng nghe gói tin trả lời ICMP “echo response”. sử dụng thời gian và tốc độ đáp ứng, ping có thể đánh giá thời gian quay về và tốc độ rót gói giữa 2 máy tính.

Cú pháp

```
ping [-t] [-a] [-n Count] [-l Size] [-f] [-i TTL] [-v TOS] [-r Count] [-s Count] [{-j HostList | -k HostList}] [-w Timeout] [TargetName]
```

Tham số

- t:** chỉ định ping tiếp tục cho đến khi bị ngắt. Ngắt và thông kê ấn **Ctrl-Break**. Ngắt và thoát lệnh ping, ấn **Ctrl-C**.
- a:** chỉ định đích IP Address thành tên miền. Nếu thành công, ping sẽ hiện tên miền máy đích.
- n Count:** chỉ định số lần gửi thông điệp echo-request. Mặc định là 4.
- l Size:** chỉ định kích thước bằng byte của trường dữ liệu trong gói tin echo-request. Mặc định là 32. giá trị tối đa là 65,527.
- f:** chỉ định gói tin Echo Request được gửi với cờ hiệu Don't Fragment đặt về 1. Thông điệp echo-request không thể bị fragment bởi các router trung gian trên đường truyền đến máy đích. Tham số này rất có ích trong việc gỡ rối vấn đề MTU của đường truyền.

-i TTL: chỉ định giá trị trường Time-To-Live (TTL) của gói Echo Request. Mặc định giá trị TTL phụ thuộc vào hệ điều hành. Ví dụ Windows XP là 128. Giá trị tối đa của TTL là 255.

-v TOS: chỉ định giá trị Type of Service (TOS) của gói Echo Request. Mặc định là 0, TOS nhận giá trị từ 0 đến 255.

-r Count: chỉ định tùy chọn Record Route trong IP header IP được dùng để ghi nhận lại danh sách các thiết bị trung gian (hop) trên đường truyền từ nguồn đến đích. Mỗi thiết bị trung gian (hop) sẽ tạo ra 1 dòng thông tin, nếu sử dụng tham số Count sẽ chỉ định số lượng tối đa các dòng thông tin được ghi nhận lại giá trị hợp lệ của count là từ 1 đến 9.

-s Count: chỉ định tham số Internet Timestamp trong IP header được sử dụng để ghi nhận lại thời gian đến của thông điệp Echo Request tương ứng với Echo Reply của mỗi thiết bị trung gian (hop), count có giá trị từ 1 đến 4.

-j HostList: chỉ định gói tin Echo Request sử dụng Loose Source Route option trong IP header với tập danh sách các thiết bị trung gian chỉ định trong HostList. Host list là 1 chuỗi tối đa là 9 địa chỉ IP cách nhau bởi khoảng trắng.

-k HostList: chỉ định gói tin Echo Request sử dụng Strict Source Route option trong IP header với tập danh sách các thiết bị trung gian chỉ định trong HostList. Tham số strict source routing, các thiết bị trung gian kế tiếp phải nối trực tiếp với nhau. Host list là 1 chuỗi tối đa là 9 địa chỉ IP cách nhau bởi khoảng trắng.

-w Timeout: chỉ định thời gian chờ tính mili giây bằng gói tin Echo Reply. Nếu gói tin Echo Reply nhận được sau thời gian time-out thì thông báo lỗi "Request timed out" sẽ hiển thị, giá trị mặc định của time-out là 4000 (4 giây).

-TargetName: chỉ định đích đến bằng tên miền hoặc địa chỉ IP.

-?: hiển thị trợ giúp

```
C:\> ping example.com

Pinging example.com [192.0.34.166] with 32 bytes of data:
Reply from 192.0.34.166: bytes=32 time=19ms TTL=45
Reply from 192.0.34.166: bytes=32 time=18ms TTL=45
Reply from 192.0.34.166: bytes=32 time=19ms TTL=45
Reply from 192.0.34.166: bytes=32 time=17ms TTL=45

Ping statistics for 192.0.34.166:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
        Minimum = 17ms, Maximum = 19ms, Average = 18ms

C:\>
```

Công cụ máy tính : ARP Table

Interface:	Internet Address	Physical Address	Type
192.168.1.101	00-04-5a-22-ec-c7	dynamic	
192.168.1.40	00-02-4b-cc-d6-d9	dynamic	
192.168.1.42	00-02-fd-65-9f-82	dynamic	
192.168.1.43	00-03-6b-09-59-29	dynamic	
192.168.1.100	00-02-4b-cc-d6-d0	dynamic	
192.168.1.135	00-03-6d-1e-6a-a5	dynamic	
192.168.1.149	00-50-8b-f7-cf-59	dynamic	

Module 6-35

Lệnh **arp** dùng hiển thị và thay đổi nội dung thông tin trong bảng ARP. Mỗi card mạng trên máy tính sẽ có 1 bảng ARP khác nhau.

Sử dụng lệnh **arp** không có tham số sẽ hiển thị hướng dẫn sử dụng lệnh arp.

Cú pháp

```
arp [-a [InetAddr] [-N IfaceAddr]] [-g [InetAddr] [-N  
IfaceAddr]] [-d InetAddr [IfaceAddr]] [-s InetAddr EtherAddr  
[IfaceAddr]]
```

Tham số

-a [InetAddr] [-N IfaceAddr]: hiển thị nội dung bảng ARP của 1 hay tất cả các card mạng. Để hiển thị ánh xạ IP – MAP cho 1 địa chỉ IP cụ thể dùng tham số -a <InetAddr> (InetAddr là địa chỉ IP cần xem ánh xạ) . Để hiển thị nội dung bảng arp của 1 card mạng dùng tham số -N <IfaceAddr> (lưu ý -N là ký tự hoa, <IfaceAddr> là địa chỉ IP gán cho card mạng cần xem ánh xạ).

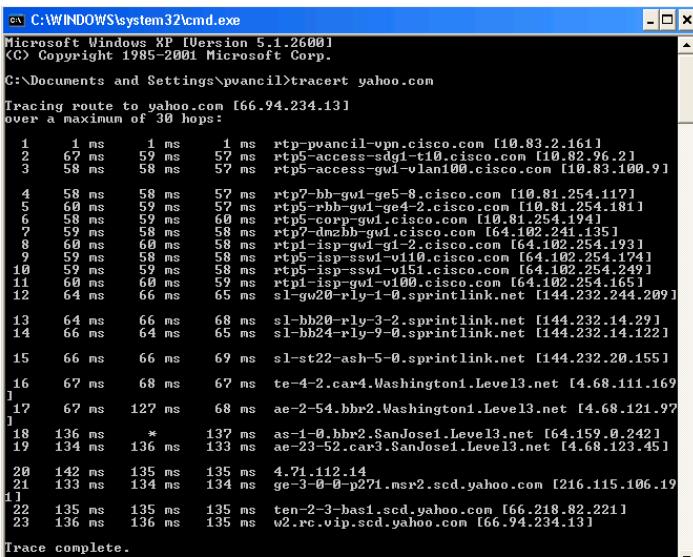
-g [InetAddr] [-N IfaceAddr]: tương tự tham số -a .

-d InetAddr [IfaceAddr] : xoá nội dung arp cache. để xoá tất cả nội dung ta dùng tham số (*) thay cho InetAddr.

- **-s InetAddr EtherAddr [IfaceAddr]:** bổ sung một ánh xạ tĩnh vào ARP cache cặp tham số IP – MAC là InetAddr – EtherAddr, IfaceAddr là địa chỉ IP gán cho card mạng tương ứng.

- **?/?:** hiển thị hướng dẫn sử dụng.

Công cụ máy tính : tracert



The screenshot shows a command prompt window titled "cmd C:\WINDOWS\system32\cmd.exe". The window displays the output of the "tracert yahoo.com" command. The output shows the tracing route to yahoo.com (66.94.234.13) over a maximum of 30 hops. The route passes through various Cisco routers and switches, including rtp-puancil-upn.cisco.com, rtp5-access-sdgl-t10.cisco.com, rtp5-access-gwl-vlan100.cisco.com, rtp7-hb-gwl-ge5-8.cisco.com, rtp5-rbb-gwl-ge4-2.cisco.com, rtp5-corp-gwl.cisco.com, rtp1-dmzbb-ge1.cisco.com, rtp5-isp-ssvl-w16.cisco.com, rtp5-isp-ssvl-w151.cisco.com, rtp1-isp-gwl-v100.cisco.com, sl-gw20-rly-1-0.sprintlink.net, sl-bh20-rly-3-2.sprintlink.net, sl-bh24-rly-9-0.sprintlink.net, sl-st22-ash-5-0.sprintlink.net, te-4-2.car4.Washington1.Level3.net, ae-2-54.bbr2.Washington1.Level3.net, as-1-0.bbr2.SanJose1.Level3.net, ae-23-52.car3.SanJose1.Level3.net, ge-3-0-p271.msr2.scd.yahoo.com, ten-2-3-has1.scd.yahoo.com, and w2.rc.vip.scd.yahoo.com. The trace completes at hop 23.

```
C:\Documents and Settings\pvancil>tracert yahoo.com
Tracing route to yahoo.com [66.94.234.13]
over a maximum of 30 hops:
  1  1 ms   1 ms   1 ms  rtp-puancil-upn.cisco.com [10.83.2.161]
  2  67 ms   59 ms   57 ms  rtp5-access-sdgl-t10.cisco.com [10.82.96.2]
  3  58 ms   58 ms   57 ms  rtp5-access-gwl-vlan100.cisco.com [10.83.100.9]
  4  58 ms   58 ms   57 ms  rtp7-hb-gwl-ge5-8.cisco.com [10.81.254.117]
  5  60 ms   59 ms   57 ms  rtp5-rbb-gwl-ge4-2.cisco.com [10.81.254.181]
  6  58 ms   59 ms   60 ms  rtp5-corp-gwl.cisco.com [10.81.254.194]
  7  59 ms   58 ms   58 ms  rtp1-dmzbb-ge1.cisco.com [64.102.254.135]
  8  60 ms   59 ms   58 ms  rtp5-isp-ssvl-w16.cisco.com [64.102.254.193]
  9  59 ms   58 ms   58 ms  rtp5-isp-ssvl-w151.cisco.com [64.102.254.174]
 10  59 ms   59 ms   58 ms  rtp1-isp-gwl-v100.cisco.com [64.102.254.249]
 11  60 ms   60 ms   59 ms  rtp1-isp-gwl-v100.cisco.com [64.102.254.165]
 12  64 ms   66 ms   65 ms  sl-gw20-rly-1-0.sprintlink.net [144.232.244.209]
 13  64 ms   66 ms   68 ms  sl-bh20-rly-3-2.sprintlink.net [144.232.14.29]
 14  66 ms   64 ms   65 ms  sl-bh24-rly-9-0.sprintlink.net [144.232.14.122]
 15  66 ms   66 ms   69 ms  sl-st22-ash-5-0.sprintlink.net [144.232.20.155]
 16  67 ms   68 ms   67 ms  te-4-2.car4.Washington1.Level3.net [4.68.111.169]
 17  67 ms   127 ms   68 ms  ae-2-54.bbr2.Washington1.Level3.net [4.68.121.97]
 18  136 ms   *       137 ms  as-1-0.bbr2.SanJose1.Level3.net [64.159.0.242]
 19  134 ms   136 ms   133 ms  ae-23-52.car3.SanJose1.Level3.net [4.68.123.45]
 20  142 ms   135 ms   135 ms  4.71.112.14
 21  133 ms   134 ms   134 ms  ge-3-0-p271.msr2.scd.yahoo.com [216.115.106.19]
 22  135 ms   135 ms   135 ms  ten-2-3-has1.scd.yahoo.com [66.218.82.221]
 23  136 ms   136 ms   135 ms  w2.rc.vip.scd.yahoo.com [66.94.234.13]

Trace complete.
```

Công cụ TRACERT dùng để xác định đường đi đến đích bằng cách sử dụng gói tin ICMP gửi đến máy đích, TRACERT dùng gói IP có giá trị TTL khác nhau. Bởi vì mỗi router trên đường đi phải trừ giá trị TTL của gói tin 1 đơn vị trước khi gửi chúng đi, giá trị TTL đóng vai trò như 1 bộ đếm hop. Khi TTL của gói tin bằng 0, router sẽ gửi thông điệp ICMP "Time Exceeded" trả về cho máy nguồn.

TRACERT gửi gói tin echo đầu tiên với ttl = 1 và tăng dần giá trị ttl cho các gói sau đó mỗi lần 1 đơn vị, cho đến khi gói tin đi đến đích hoặc đạt được giá trị tối đa của TTL. Thông điệp ICMP "Time Exceeded" mà các router trung gian gửi trả lại máy nguồn sẽ cho phép hiển thị lại danh sách các router trung gian. Tuy nhiên có 1 số router bỏ các gói tin có ttl=0 nhưng không gửi lại ICMP "Time Exceeded" và như vậy các router này là không nhìn thấy bởi TRACERT.

TRACERT in ra thứ tự các router trung gian căn cứ theo thông điệp ICMP "Time Exceeded" trả về. sử dụng tham số **-d** sẽ cho phép **tracert** không thực hiện truy vấn DNS cho mỗi địa chỉ IP nhận được.

Cú pháp

```
tracert -d -h maximum_hops -j host-list -w timeout target_host
```

Parameters

-d: không thực hiện phân giải tên miền

- **-h maximum_hops:** chỉ định số lượng hop tối đa trong quá trình thực hiện
- **-j host-list:** chỉ định loose source route bằng danh sách host-list
- **-w timeout:** đợi trong khoảng thời gian tính bằng milli giây để nhận các trả lời
- **target_host:** chỉ định máy đích theo tên hoặc địa chỉ IP

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\pvancil>tracert yahoo.com
Tracing route to yahoo.com [66.94.234.13]
over a maximum of 30 hops:
 1   1 ms    1 ms    1 ms  rtp-pvancil-vpn.cisco.com [10.83.2.161]
 2   67 ms    59 ms    57 ms  rtp5-access-sdg1-t10.cisco.com [10.82.96.2]
 3   58 ms    58 ms    57 ms  rtp5-access-gw1-vlan100.cisco.com [10.83.100.9]
 4   58 ms    58 ms    57 ms  rtp7-bb-gw1-ge5-8.cisco.com [10.81.254.117]
 5   60 ms    59 ms    57 ms  rtp5-rbb-gw1-ge4-2.cisco.com [10.81.254.181]
 6   58 ms    59 ms    60 ms  rtp5-corp-gw1.cisco.com [10.81.254.194]
 7   59 ms    58 ms    58 ms  rtp7-dmzbb-gw1.cisco.com [64.102.241.135]
 8   60 ms    60 ms    58 ms  rtp1-isp-gw1-g1-2.cisco.com [64.102.254.193]
 9   59 ms    58 ms    58 ms  rtp5-isp-sswl-v110.cisco.com [64.102.254.174]
10   59 ms    59 ms    58 ms  rtp5-isp-sswl-v151.cisco.com [64.102.254.249]
11   60 ms    60 ms    59 ms  rtp1-isp-gw1-v100.cisco.com [64.102.254.165]
12   64 ms    66 ms    65 ms  sl-gw20-rly-1-0.sprintlink.net [144.232.244.209]
13   64 ms    66 ms    68 ms  sl-bb20-rly-3-2.sprintlink.net [144.232.14.29]
14   66 ms    64 ms    65 ms  sl-bb24-rly-9-0.sprintlink.net [144.232.14.122]
15   66 ms    66 ms    69 ms  sl-st22-ash-5-0.sprintlink.net [144.232.20.155]
16   67 ms    68 ms    67 ms  te-4-2.car4.Washington1.Level3.net [4.68.111.169]
17   67 ms   127 ms    68 ms  ae-2-54.bbr2.Washington1.Level3.net [4.68.121.97]
18   136 ms    *    137 ms  as-1-0.bbr2.SanJose1.Level3.net [64.159.0.242]
19   134 ms   136 ms   133 ms  ae-23-52.car3.SanJose1.Level3.net [4.68.123.45]
20   142 ms   135 ms   135 ms  4.71.112.14
21   133 ms   134 ms   134 ms  ge-3-0-0-p271.msr2.scd.yahoo.com [216.115.106.19]
22   135 ms   135 ms   135 ms  ten-2-3-basi.scd.yahoo.com [66.218.82.221]
23   136 ms   136 ms   135 ms  w2.rc.vip.scd.yahoo.com [66.94.234.13]

Trace complete.
```

Tóm tắt

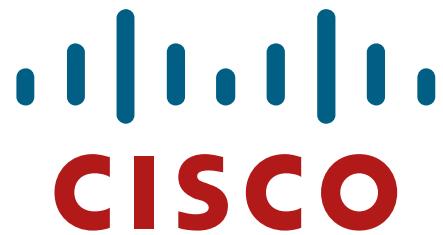
- Lớp 1 cung cấp môi trường vật lý và cách mã hóa.
- Thiết bị lớp 2 cung cấp cổng giao tiếp với môi trường truyền vật lý.
- Địa chỉ lớp 2 - địa chỉ MAC.
- Lớp mạng cung cấp kết nối và chọn đường giữa 2 máy.
- Địa chỉ lớp 3 - địa chỉ IP.

Module 6-40

Tóm tắt (tiếp theo)

- Trước khi một máy có thể gửi dữ liệu đến một máy khác, nó phải biết địa chỉ MAC của máy đích.
- Nếu địa chỉ MAC không tìm thấy, ARP được sử dụng để ánh xạ giữa địa chỉ lớp 2 - lớp 3.
- Truyền thông tin cần sử dụng phiên TCP.
- Dữ liệu gửi phải được xác nhận bằng acknowledged.
- Nếu máy đích thuộc mạng khác thì cần phải có một default gateway.
- Một số công cụ khả dụng để kiểm tra kết nối giữa 2 máy :
 - ping
 - tracert
 - arp

Module 6-41



Module 6-42

Bài 7: Tìm hiểu mạng Ethernet



Xây dựng một mạng đơn giản

Module 7-1

Tổng quan

Mạng cục bộ rất phổ biến ở nhà, trong văn phòng nhỏ và cả ở các công ty lớn. Hiểu được cách thức hoạt động của mạng cục bộ , bao gồm các thành phần mạng, frame, địa chỉ Ethernet, và đặc trưng hoạt động sẽ giúp ta nắm bắt được tri thức mạng máy tính tốt hơn.

Bài này mô tả mạng cục bộ và cung cấp kiến thức cơ bản về đặc trưng, thành phần, chức năng mạng LAN cũng như hoạt động cơ bản của mạng Ethernet và cách thức frames được truyền.

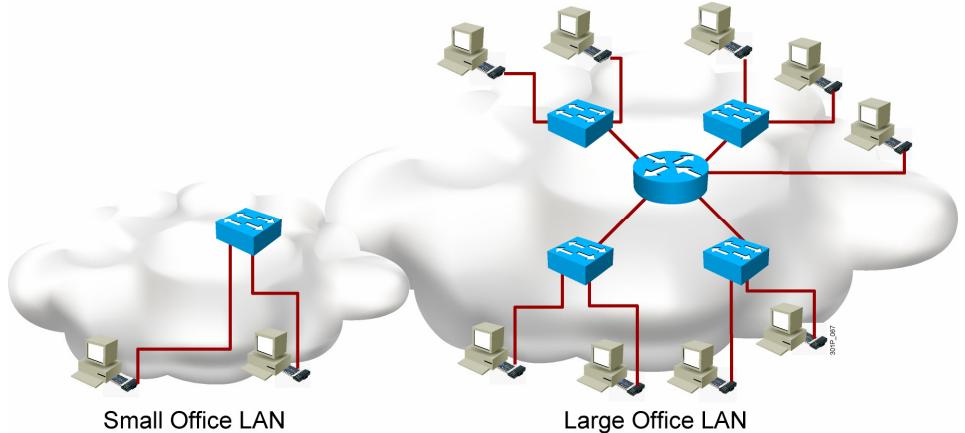
Mục tiêu

Kết thúc bài này học viên có thể liệt kê các đặc trưng và ưu điểm của mạng cục bộ, bao gồm các thành phần và chức năng của chúng :

- Định nghĩa mạng cục bộ (LAN)
- Nhận diện các thành phần của mạng cục bộ
- Liệt kê chức năng của mạng LAN
- Định nghĩa kích thước mạng LAN
- Mô tả quá trình phát triển của mạng Ethernet (IEEE 802.3)
- Mô tả các chuẩn dùng trong Ethernet
- Định nghĩa cách thức hoạt động của CSMA/CD

- Định danh các trường của frame Ethernet và giải thích chức năng của chúng
- Liệt kê đặc trưng của địa chỉ Ethernet
- Định nghĩa mục đích và các thành phần của địa chỉ Ethernet
- Định cấu trúc số thập lục phân và chức năng của địa chỉ MAC trong mạng Ethernet

Mạng cục bộ (Local Area Network)



Module 7-3

Định nghĩa mạng cục bộ

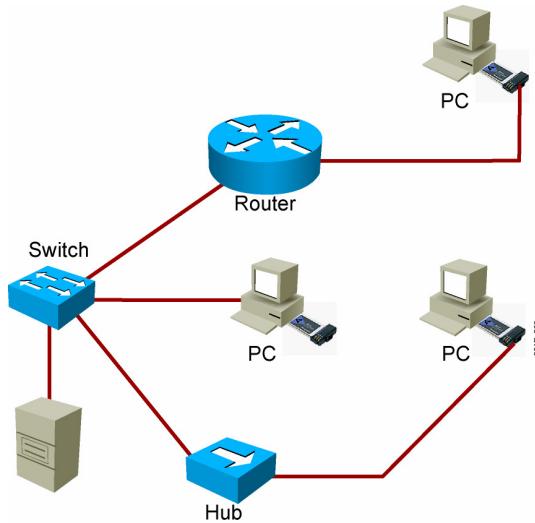
LAN là mạng máy tính mà các thiết bị nối kết trong 1 phạm vi địa lý gần nhau. Mạng cục bộ có thể chỉ gồm 2 máy tính ở nhà, văn phòng nhỏ hoặc hàng trăm máy trong những toà nhà gần nhau đối với các công ty lớn.

Ví dụ : mạng cục bộ văn phòng nhỏ và công ty lớn

Đối với những mạng cục bộ văn phòng nhỏ chỉ bao gồm 1 vài máy tính kết nối với vài thiết bị ngoại vi như máy in. Với mạng LAN công ty lớn số lượng máy tính kết nối có thể lên đến hàng trăm trải dài trên nhiều tầng lầu hoặc toà nhà lân cận.

Thành phần mạng LAN

- Máy tính
 - PCs
 - Máy chủ
- Phần Nối kết
 - Card mạng
 - Môi trường truyền
- Thiết bị mạng
 - Hubs
 - Switches
 - Routers
- Giao thức
 - Ethernet
 - IP
 - ARP ...



Module 7-4

Mạng LAN có những thành phần như phần cứng, thiết bị nối kết, phần mềm.

Bỏ qua kích thước mạng cục bộ những thành phần cơ bản của LAN bao gồm

• **Máy tính** : máy tính là điểm cuối của mạng, nơi gửi và nhận dữ liệu.

• **Phần nối kết (Interconnections)**: cho phép dữ liệu truyền từ điểm này đến điểm kia trên mạng

— **Card mạng (NICs)**: card mạng dịch dữ liệu thành các định dạng có thể truyền trên mạng cục bộ.

— **Môi trường truyền dẫn (Network media)**: ví dụ như dây cáp hay không gian (truyền không dây), truyền tín hiệu từ thiết bị này đến thiết bị kia trên mạng LAN.

• **Thiết bị mạng (Network devices)**:

— **Hubs**: điểm tập trung đầu nối hoạt động ở lớp 1 của mô hình OSI. Ngày nay người ta dùng switch thay thế cho hub.

— **Switches**: Switches Ethernet là điểm tập trung của mạng LAN hoạt động ở lớp 2 mô hình OSI cung cấp khả năng phân phối các frame dữ liệu thông minh trên mạng LAN để tăng hiệu quả sử dụng.

— **Routers**: còn được gọi là gateways, cung cấp khả năng nối kết các mạng LAN lại với nhau. Routers hoạt động ở lớp 3 của mô hình OSI.

• **Giao thức (Protocols):** là tập các quy tắc điều hành việc truyền dữ liệu trên mạng LAN:

- Giao thức Ethernet
- Giao thức IP (Internet Protocol - IP)
- Giao thức phân giải địa chỉ (Address Resolution Protocol - ARP và Reverse ARP - RARP)
- Giao thức cấp địa chỉ động (Dynamic Host Configuration Protocol - DHCP)

Chức năng của mạng cục bộ

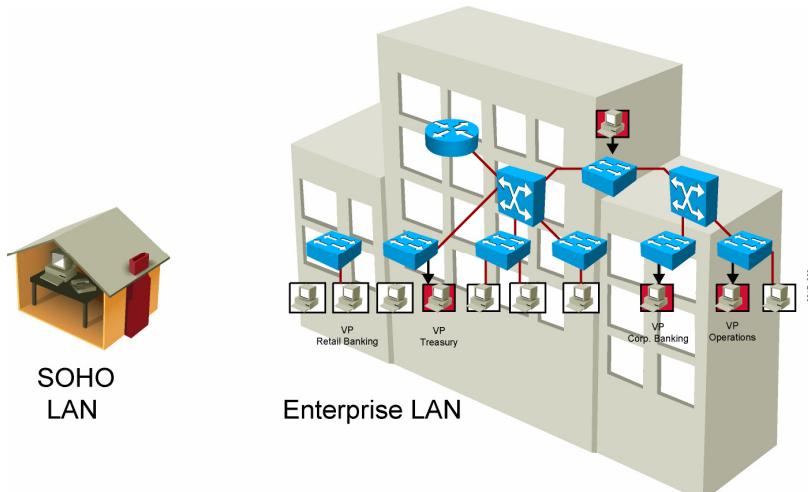
- Dữ liệu và ứng dụng
- Chia sẻ tài nguyên
- Cung cấp con đường kết nối đến các mạng khác

Module 7-6

LANs cung cấp cho người dùng khả năng truyền thông và chia sẻ tài nguyên :

- **Dữ liệu và ứng dụng :** khi người dùng được kết nối vào LAN, họ có thể chia sẻ tập tin và ngay cả các chương trình ứng dụng. Điều đó cho phép xây dựng các ứng dụng cộng tác một cách hiệu quả.
- **Tài nguyên (Resources):** tài nguyên là những thứ được chia sẻ bao gồm thiết bị xuất/nhập như camera, máy in, máy quét
- **Con đường nối kết đến các mạng khác :** đối với các tài nguyên ở xa mạng cục bộ thông qua gateway có thể cung cấp con đường nối kết đến các tài nguyên từ xa này ví dụ như truy cập trang web từ xa chẳng hạn.

Kích thước mạng cục bộ



Module 7-7

Mạng cục bộ có kích thước thay đổi phụ thuộc vào yêu cầu và môi trường chúng hoạt động :

- **Văn phòng nhỏ (Small office, home office - SOHO):** SOHO là môi trường tiêu biểu chỉ có một số PC và thiết bị ngoại vi như máy in.
- **Mạng xí nghiệp (Enterprise):** môi trường mạng công ty bao gồm nhiều mạng LAN tách biệt trong một hoặc một vài văn phòng trong cùng 1 khu vực, số lượng PC và thiết bị trong mạng này lên đến hàng trăm.

Quá trình phát triển mạng Ethernet

Year	Ethernet Activity
1970	First packet radio network
1973	Ethernet invented at Xerox
1977	U.S. patent no. 4063220 issued
1982	DIX releases 10-Mb/_s Ethernet
1992	First stackable Ethernet hub
2002	IEEE approves 802.3ae; 10 billion bps

BRG/DO

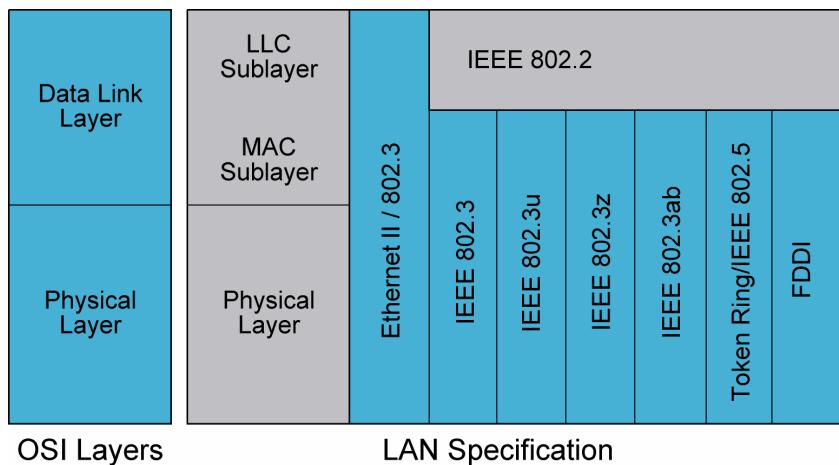
Module 7-8

Ethernet là mạng cục bộ sử dụng phổ biến ngày nay.

Ethernet được phát triển đầu tiên vào thập niên 70 bởi DEC, Intel, and Xerox, và được đặt tên là DIX Ethernet. Sau đó nó được biết đến với tên là Thick Ethernet (bởi vì mạng này sử dụng cáp đồng trực kích thước lớp) tốc độ truyền dữ liệu đạt được 10 Mb/s. Chuẩn Ethernet ra đời vào thập niên 80 được bổ sung thêm khả năng được đặt tên là Ethernet phiên bản 2 (hay Ethernet II).

Tổ chức The Institute of Electrical and Electronic Engineers vào giữa thập niên 80 dựa trên nền tảng Ethernet đã định nghĩa ra 1 chuẩn mới tương tự Ethernet 802.3 hoạt động gửi dữ liệu trên mạng Ethernet dựa trên phương thức Carrier Sense Multiple Access with Collision Detection (CSMA/CD). Ethernet 802.3 đặc tả lớp vật lý (lớp 1 mô hình OSI), và phần Media Access Control (MAC) của lớp liên kết dữ liệu (lớp 2 mô hình OSI). Ngày nay, tập các chuẩn này được gọi với tên đơn giản là “Ethernet.”

LAN Standards



Module 7.9

Chuẩn Ethernet đặc tả cáp và tín hiệu ở 2 lớp vật lý và lớp liên kết dữ liệu của mô hình OSI.

Hình trên minh họa ánh xạ giữa giao thức mạng LAN và các lớp 1 & 2 của OSI.

IEEE chia lớp liên kết dữ liệu thành 2 lớp thứ cấp :

- Lớp kiểm soát kết nối luận lý (Logical Link Control - LLC):** chuyển tiếp lên lớp mạng
- Lớp kiểm soát truy cập môi trường truyền (Media Access Control - MAC):** chuyển tiếp xuống lớp vật lý

Lớp thứ cấp LLC

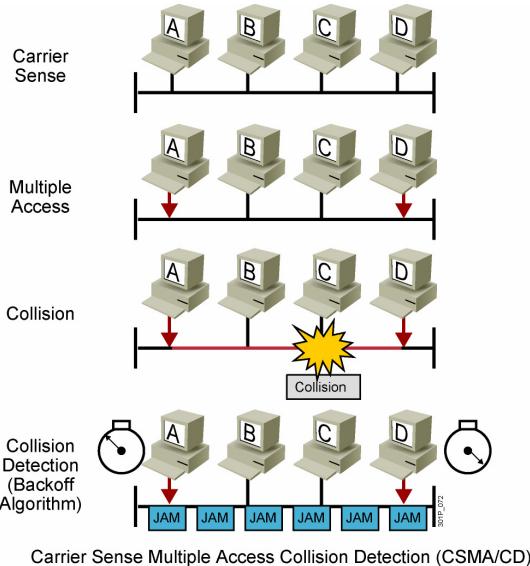
IEEE tạo lớp thứ cấp LLC cho phép chức năng của lớp liên kết dữ liệu độc lập với các kỹ thuật vật lý được sử dụng. Lớp này cung cấp tính mềm dẻo cho các dịch vụ của lớp mạng không phụ thuộc những kỹ thuật truyền thông ở lớp MAC và lớp 1 bên dưới. Lớp tham gia vào tiến trình đóng gói dữ liệu participates in the encapsulation process.

Header của LLC thông tin cho lớp liên kết dữ liệu cách xử lý gói tin được đóng gói bên trong frame dữ liệu lớp 2.

Lớp thứ cấp MAC

Lớp MAC liên quan đến môi trường truyền vật lý. IEEE 802.3 đặc tả địa chỉ MAC dùng định danh duy nhất từng thiết bị ở lớp 2 mô hình OSI. Để kết nối vào mạng mỗi thiết bị đều phải có 1 địa chỉ vật lý (địa chỉ MAC) duy nhất.

CSMA/CD



Module 7-10

Tín hiệu Ethernet được phát từ mỗi máy nối vào mạng, dùng một tập các qui tắc đặc biệt để xác định trạm nào đang phát.

Ethernet quản trị tín hiệu trên mạng bằng phương thức Carrier Sense Multiple Access with Collision Detection (CSMA/CD), hình trên minh họa tiến trình CSMA/CD thực hiện.

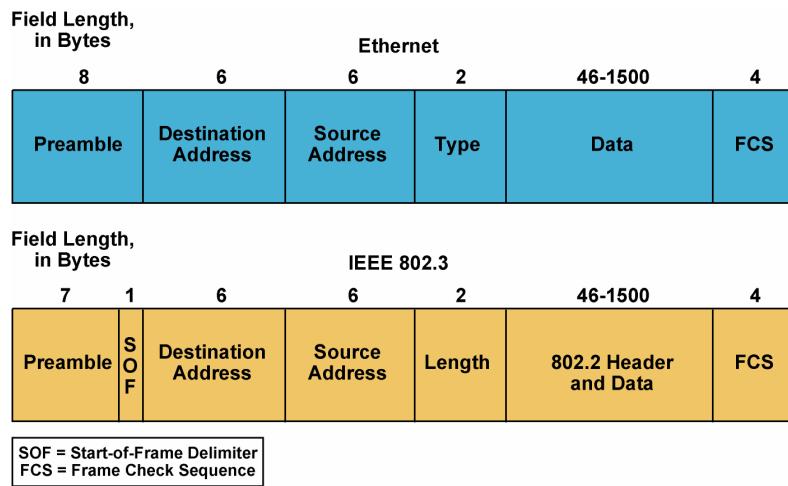
Trong mạng Ethernet, trước khi phát tín hiệu, máy tính phải lắng nghe trên môi trường truyền. Nếu môi trường truyền đang ở trạng thái nghỉ, máy tính sẽ gửi dữ liệu. Sau khi tín hiệu được phát đi, tất cả các máy tính khác trên mạng sẽ cạnh tranh nhau tìm thời gian nghỉ kế tiếp để gửi frame khác. Quá trình cạnh tranh tìm thời gian nghỉ có nghĩa là không có trạm nào có ưu thế hơn các trạm còn lại.

Các trạm trên mạng cục bộ CSMA/CD có thể truy cập mạng bất kỳ lúc nào. Trước khi gửi dữ liệu, các trạm CSMA/CD lắng nghe mạng để xác định xem mạng đã được sử dụng hay không. Nếu mạng đang được sử dụng các trạm sẽ phải đợi. Nếu mạng đang rảnh rồi, các trạm sẽ phát dữ liệu. Đụng độ (collision) xảy ra khi 2 trạm cùng phát dữ liệu một lúc (xem hình). Trong trường hợp đó, cả hai tín hiệu đều bị hỏng, và các trạm phải gửi lại tín hiệu sau đó. Trạm CSMA/CD phải có khả năng phát hiện đụng độ để gửi lại tín hiệu khi cần thiết.

Khi một trạm phát, tín hiệu được xem như là carrier. Card mạng sẽ nhận biết được carrier và tự kiềm chế việc phát tín hiệu lên mạng. Nếu không có carrier, một trạm đang đợi sẽ biết rằng đã sẵn sàng để phát tín hiệu. Chức năng này được gọi là nhận diện carrier (“carrier sense”). Toàn bộ phần mạng trên đó xảy ra đụng độ được gọi là miền đụng độ (collision domain). Kích thước miền đụng độ ảnh hưởng đến hiệu năng và thông lượng của mạng Ethernet.

Trong tiến trình CSMA/CD, không có độ ưu tiên cho các trạm, vì thế tất cả các trạm trên mạng đều có quyền truy xuất như nhau, vì thế xuất hiện khả năng cùng truy cập (“multiple access”). Nếu có từ 2 trạm trở lên cố gắng phát dữ liệu cùng lúc đụng độ sẽ xảy ra. Khi xảy ra đụng độ các trạm sẽ thực hiện thuật toán backoff sinh ra thời gian chờ ngẫu nhiên trước khi phát lại tín hiệu. Cách làm này sẽ giúp ngăn chặn các máy tiếp tục cố gắng tín hiệu đồng thời đó là kỹ thuật giải quyết đụng độ “collision detection”

Cấu trúc Frame Ethernet



Module 7-12

Các bit nhị phân truyền trên mạng Ethernet được tổ chức thành từng frame.

Frame là đơn vị dữ liệu trong ethernet bao gồm thông tin header, thông tin trailer, và nội dung thông tin cần truyền tải.

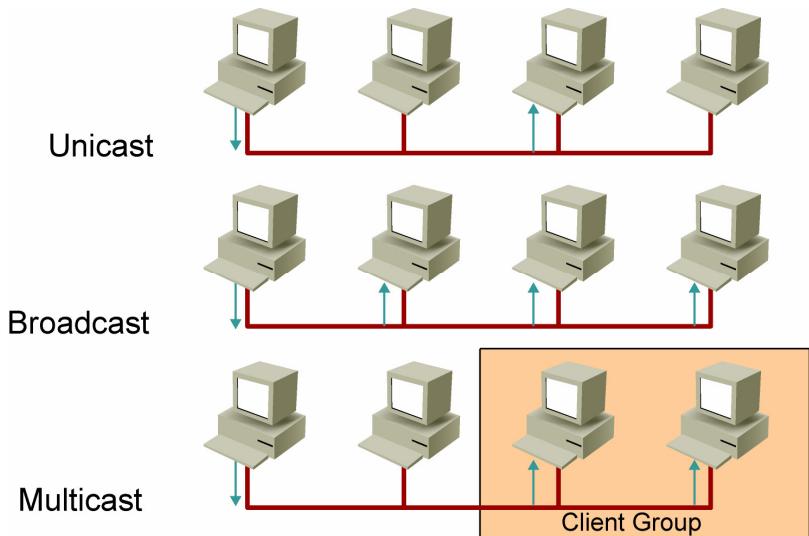
Hình trên minh họa các trường thông tin của Frame Ethernet :

- **Preamble:** trường thông tin gồm 7 bytes chứa các bit 1, 0 liên tiếp, nó có tác dụng đồng bộ tín hiệu.
- **Bắt đầu frame (Start-of-frame - SOF chỉ có trong 802.3):** Trường thông tin gồm 1 byte có giá trị 10101011, dùng thông báo cho máy nhận biết điểm bắt đầu của Frame.
- **Địa chỉ đích (Destination address):** Trường địa chỉ đích chứa địa chỉ vật lý của card mạng máy nhận.
- **Địa chỉ nguồn (Source address):** Trường địa chỉ nguồn chứa địa chỉ vật lý của card mạng máy gửi.
- **Loại/chiều dài (Type/length):** Trong chuẩn Ethernet II, trường này chứa mã số xác định giao thức lớp mạng. Trong chuẩn 802.3, trường này chứa chiều dài của trường dữ liệu (data). Thông tin về giao thức lớp network chứa trong trường 802.2, lớp LLC chứa 802.2 header và trường dữ liệu.

- **Dữ liệu (Data):** Trường này chứa dữ liệu nhận được từ lớp mạng của máy gửi. Nếu dữ liệu quá ngắn một chuỗi bit vô nghĩa sẽ được thêm vào (được gọi là pad) để đảm bảo chiều dài tối thiểu của dữ liệu là 46 bytes.

- **Frame check sequence (FCS):** Trường này dùng để kiểm tra xem nội dung của frame nhận có bị lỗi hay không.

Truyền thông trong mạng LAN



Module 7-14

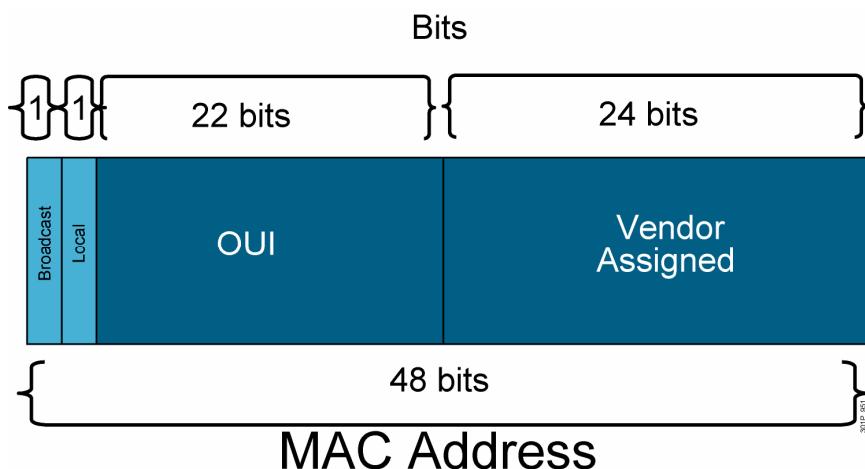
Truyền thông trong mạng xảy ra theo 1 trong 3 dạng : unicast, broadcast, and multicast.

• **Unicast:** truyền thông trong đó fram được gửi từ một máy đến một máy duy nhất khác. Unicast là cách thức truyền thông phổ biến trong mạng LAN và Internet.

• **Broadcast:** truyền thông trong đó 1 môt fram được gửi đến tất cả các máy còn lại. Broadcast là cách thức truyền thông cơ bản khi cần gửi cùng thông điệp đến tất cả các thiết bị trong mạng LAN.

• **Multicast:** truyền thông trong đó thông tin được gửi đến một nhóm máy hoặc thiết bị. Không giống như broadcast, chỉ các máy là thành viên của nhóm multicast mới nhận được thông tin.

Thành phần địa chỉ MAC



Module 7-15

Địa chỉ vật lý MAC được ghi trong ROM (burned-in address - BIA) của card mạng và một số nhà cung cấp cho phép sửa đổi lại giá trị này để phù hợp với nhu cầu cục bộ. Địa chỉ MAC 48-bit gồm 2 thành phần như sau :

•**24-bit Organizational Unique Identifier (OUI):** OUI chỉ danh nhà sản xuất card mạng. Tổ chức IEEE gán các giá trị OUI cho nhà sản xuất . Trong OUI, có 2 bit chỉ có ý nghĩa trong địa chỉ đích đó là :

— **Broadcast hay multicast bit:** bit này báo cho giao tiếp đích biết rằng frame này được gửi cho tất cả hoặc một nhóm các máy trong đoạn mạng LAN.

— **Locally administered address bit:** thông thường OUI + 24-bit địa chỉ trạm (station address) tạo nên 1 địa chỉ MAC duy nhất toàn cục, nếu địa chỉ MAC bị sửa đổi lại thì bit này sẽ được đặt là 1.

•**24-bit vendor-assigned end station address:** thông tin chỉ danh duy nhất card mạng.

Địa chỉ MAC

00:00:0c:43:2e:08



30/10/2016

Module 7-16

Lớp thứ cấp MAC xử lý vấn đề địa chỉ vật lý, địa chỉ này có định dạng số thập lục phân và được ghi trong ROM của card mạng. Biểu diễn địa chỉ MAC có dạng : 00:00:0c:43:2e:08 hoặc 0000:0c43:2e08

Mỗi thiết bị trên mạng LAN phải có một địa chỉ MAC duy nhất khi tham gia vào mạng cục bộ. Địa chỉ MAC xác định ra vị trí của một máy tính cụ thể trên mạng LAN. Không giống như các loại địa chỉ khác dùng trên mạng, địa chỉ MAC không nên thay đổi trừ khi dùng cho mục đích đặc biệt nào đó.

Tóm tắt

- LAN là mạng máy tính mà các thiết bị nối kết trong 1 phạm vi địa lý gần nhau.
- Bỏ qua kích thước mạng cục bộ những thành phần cơ bản của LAN bao gồm máy tính, phần nối kết, thiết bị mạng, giao thức.
- LAN cung cấp chức năng truyền thông và chia sẻ tài nguyên cho người dùng.
- LAN có thể được cấu hình với những kích thước khác nhau để phù hợp với môi trường từ SOHO đến mạng xí nghiệp.

Module 7-17

Tóm tắt (tiếp tục)

- Mạng Ethernet phát triển đầu tiên vào thập niên 70 bởi DEC, Intel, và Xerox được đặt tên là DIX Ethernet. Tổ chức IEEE dựa trên đó phát triển một chuẩn mở mới đặt tên là 802.3 vào giữa thập niên 80, các chuẩn liên quan gồm 802.3 và 802.2.
- Chuẩn Ethernet đặc tả cáp và tín hiệu ở cả 2 lớp vật lý và lớp liên kết dữ liệu của mô hình OSI.
- Các trạm trên CSMA/CD LAN có thể truy cập mạng bất kỳ lúc nào. Trước khi gửi dữ liệu, các trạm CSMA/CD sẽ lắng nghe xem mạng đã được sử dụng hay chưa. Nếu mạng đang được sử dụng, chúng sẽ phải đợi. Nếu mạng đang rảnh rỗi, trạm sẽ tiến hành phát dữ liệu. Đụng độ (collision) xảy ra khi 2 trạm cùng cố gắng phát dữ liệu đồng thời.

Module 7-18

Tóm tắt (tiếp tục)

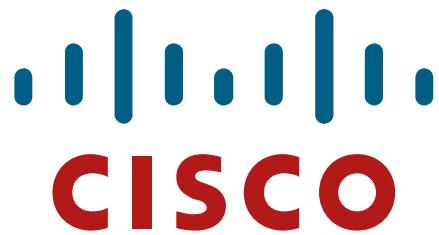
- Frame Ethernet bao gồm nhiều trường : preamble, start-of-frame delimiter, địa chỉ đích, địa chỉ nguồn, loại/chiều dài, dữ liệu, và FCS.
- Có 3 cách thức truyền thông trên mạng : unicast, trong đó frame được gửi từ một máy đến duy nhất một máy đích khác. broadcast, trong đó trong một frame được gửi từ một máy đến tất cả những máy còn lại; multicast, trong đó địa chỉ đích là một nhóm các thiết bị.
- Địa chỉ dùng trong Ethernet là phương tiện để dữ liệu được gửi đến thiết bị nhận tương ứng.

Module 7-19

Tóm tắt (tiếp tục)

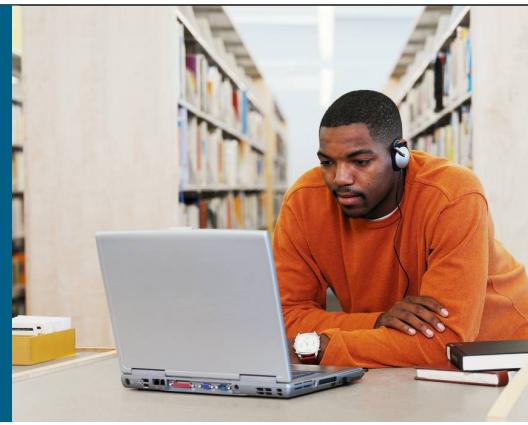
- Lớp thứ cấp MAC xử lý các vấn đề của địa chỉ vật lý, địa chỉ MAC là số nguyên 48 bit và có định dạng số thập lục phân.

Module 7-20



Module 7-21

Bài 8: Kết nối mạng cục bộ Ethernet



Xây dựng một mạng đơn giản

Module 8-1

Tổng quan

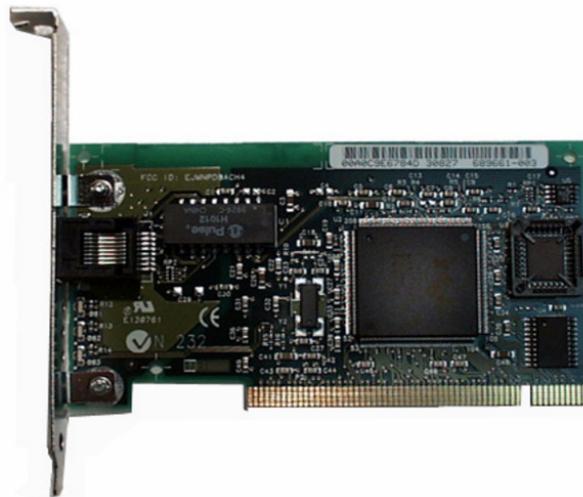
Bên cạnh việc hiểu các thành phần và chuẩn của mạng cục bộ Ethernet, chúng ta cũng cần nắm bắt cách kết nối các thành phần của mạng Ethernet. Bài học này sẽ cung cấp cho bạn cách thức kết nối các thành phần của mạng Ethernet LAN.

Mục tiêu

Kết thúc bài học này học viên có thể liệt kê loại và chức năng của các thành phần kết nối trong mạng Ethernet

- Liệt kê chức năng của card mạng (NIC) trong Ethernet.
- Liệt kê các yêu cầu kết nối của Ethernet.
- Định nghĩa các loại môi trường nối kết Ethernet.
- Liệt kê đặc trưng của cáp xoắn đôi không bọc giáp (UTP).
- Nhận diện điểm khác biệt giữa cáp thẳng và cáp chéo, giải thích cách sử dụng phù hợp cho từng loại.

Card mạng (Network Interface Card)



Module 8-2

Card mạng là một mạch điện tử cung cấp khả năng truyền thông giữa máy tính mà mạng. Còn được gọi với một tên khác là bộ điều hợp mạng (LAN adapter), card mạng được cắm vào bo mạch chủ và cung cấp cổng giao tiếp giữa PC và mạng cục bộ.

Card mạng truyền thông với mạng thông qua kết nối tuần tự, và với PC qua kết nối song song. Khi card mạng cài đặt vào máy tính nó sẽ đòi hỏi 1 ngắt (IRQ), một địa chỉ xuất/nhập (I/O address), một vùng nhớ trong hệ điều hành (DOS hay Windows), và một driver điều khiển hoạt động của nó. Ngắt là tín hiệu thông báo cho bộ xử lý rằng có một sự kiện cần phải xử lý. Ví dụ khi bạn ấn một phím, CPU chuyển ký tự được ấn từ bàn phím vào bộ nhớ. Địa chỉ xuất/nhập là vùng nhớ các thiết bị ngoại vi có thể nhập hoặc truy xuất dữ liệu từ máy tính.

Địa chỉ vật lý duy nhất MAC được nhà sản xuất ghi vào ROM của card mạng.

So sánh các yêu cầu môi trường truyền Ethernet

Requirement	10 BASE-T	100 BASE-TX	100 BASE-FX	1000 BASE-CX	1000 BASE-T	1000 BASE-SX	1000 BASE-LX
Media	EIA/TIA Category 3, 4, 5 UTP 2 pair	EIA/TIA Category 5 UTP 2 pair	62.5/125 micron multimode fiber	STP	EIA/TIA Category 5 UTP 4 pair	62.5/50 micron multimode fiber	9 micron single-mode fiber
Maximum Segment Length	100 m (328 ft)	100 m (328 ft)	400 m (1312.3 ft)	25 m (82 ft)	100 m (328 ft)	275 m (62.5 micron) 550 m (50 micron)	3-10 km (1.86-6.2 miles)
Connector	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)	Duplex media interface connector (MIC) ST	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)	—	—

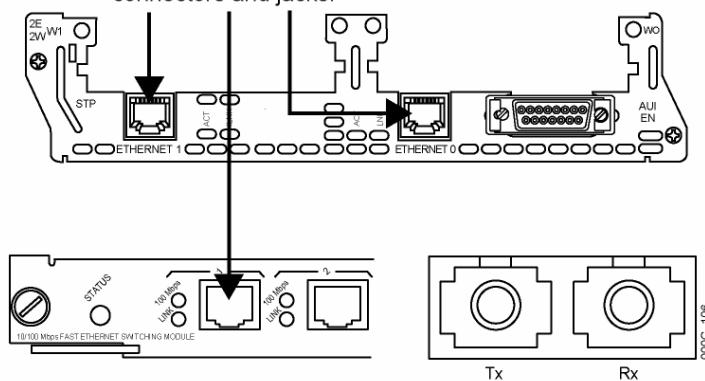
Module 8-3

Đặc tả cáp và kết nối dùng trong mạng Ethernet được lấy theo chuẩn EIA/TIA. Loại cáp dùng trong Ethernet tuân theo chuẩn EIA/TIA-568 (SP-2840). EIA/TIA qui định đầu nối RJ-45 dành cho cáp xoắn đôi không bọc giáp (UTP).

Hình trên cho ta thấy bảng so sánh các loại cáp và đầu nối phổ biến trong mạng Ethernet. Điểm khác nhau quan trọng cần lưu ý là tốc độ truyền 10-Mb/s và 100-Mb/s. Ngày nay mạng Ethernet, có khả năng bao gồm cả 2 loại 10- và 100-Mb/s, bạn phải dùng cáp UTP loại 5 trở lên đối với mạng Fast Ethernet.

Các dạng nối kết khác nhau

ISO 8877 (RJ-45)
connectors and jacks
are slightly larger than
RJ-11 phone
connectors and jacks.



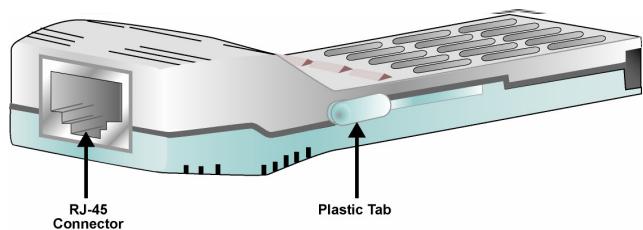
ISO = International Organization for Standardization

Module 8-4

Có nhiều dạng nối kết khác nhau trong mạng Ethernet

Dạng phổ biến nhất là kết nối RJ-45 gôò m đầu nối và giắc cắm (xem hình). Ký hiệu “RJ” viết tắt của “registered jack” và 45 liên quan đến đặc tả vật lý đầu nối có 8 dây dẫn.

1000BASE-T GBIC



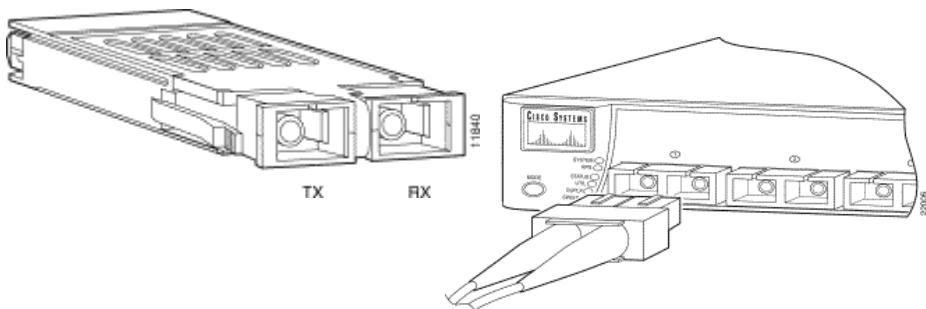
Module 8-5

Bộ chuyển đổi giao tiếp gigabit (GBIC) là thiết bị hỗ trợ cảm nóng đưa vào cổng Gigabit Ethernet. Ưu điểm chính khi sử dụng GBIC là tính khả chuyển cho phép chúng ta triển khai mạng gigabit trên cả cáp đồng và cáp quang mà không phải thay đổi công vật lý hay loại router hay switch.

Thông thường GBIC được sử dụng cho các đường uplink và các kết nối đường trực (backbone).

Cisco GBIC quang học

- Short wavelength (1000BASE-SX)
- Long wavelength/long haul (1000BASE-LX/LH)
- Extended distance (1000BASE-ZX)



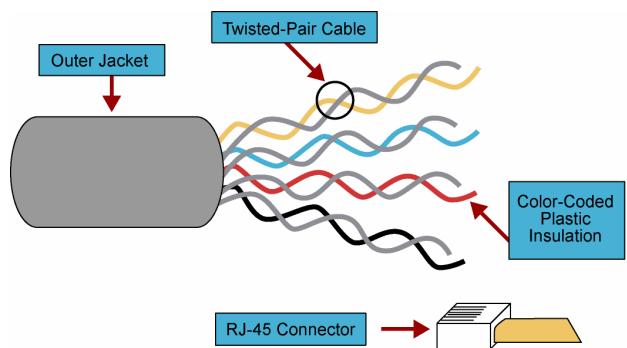
Module 8-6

GBIC quang học là một bộ thu phát (transceiver) có chức năng chuyển đổi tín hiệu điện tuần tự thành các tín hiệu ánh sáng và ngược lại, GBIC bao gồm các loại sau:

- Sóng ngắn (1000BASE-SX)
- Sóng dài (1000BASE-LX/LH)
- Khoảng cách mở rộng (1000BASE-ZX)
- Cáp xoắn đôi không bọc giáp

Xoắn đôi là cáp đồng có 2 dạng chính là bọc giáp và không bọc giáp. Loại cáp UTP ngày nay được sử dụng phổ biến nhất trong mạng cục bộ.

Cáp xoắn đôi không bọc giáp



- Tốc độ và thông lượng : từ 10 đến 1000 Mb/s
- Giá thành trên từng node: không đắt
- Môi trường truyền và đầu nối : nhỏ
- Khoảng cách tối đa của cáp : thay đổi

Module 8-7

Cáp xoắn đôi không bọc giáp (UTP cable) gồm 4 đôi dây. Mỗi dây đồng được bọc bằng vật liệu cách điện, sau đó từng đôi một chúng được xoắn lại với nhau. Ưu điểm của cáp UTP là khả năng làm giảm nhiễu, bởi vì dây xoắn đôi giới hạn ảnh hưởng của nhiễu điện từ trường (EMI) và nhiễu sóng radio (RFI). Để giảm thiểu nhiễu xuyên âm (crosstalk) giữa các cặp dây cáp người ta thay đổi bước xoắn của các cặp dây. Cả hai loại cáp xoắn đôi bọc giáp (STP) và không bọc giáp (UTP) phải tuân thủ qui định EIA/TIA về bước xoắn trên mỗi mét của các cặp dây.

Cáp UTP được dùng trong nhiều loại mạng. Khi dùng làm cáp mạng máy tính, cáp UTP gồm 4 đôi có đường kính lõi đồng từ 22-24 gauge, trở kháng của dây là 100 ohms. Trong mạng điện thoại dây xoắn đôi UTP có đường kính ngoài khoảng 0.43 cm dây nhỏ hơn nên thuận tiện khi đi dây.

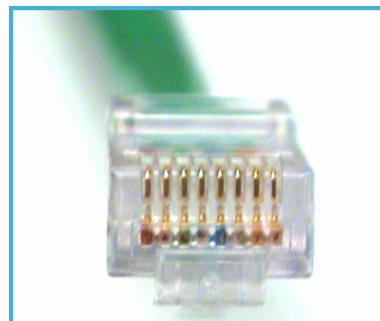
Các loại cáp UTP:

- **Category 1:** Dùng trong điện thoại; không phù hợp để truyền dữ liệu
- **Category 2:** Có khả năng truyền dữ liệu tốc độ tối đa 4 Mb/s
- **Category 3:** Dùng trong mạng 10BASE-T; có thể truyền dữ liệu tốc độ tối đa 10 Mb/s
- **Category 4:** Dùng trong mạng Token Ring; có thể truyền dữ liệu tốc độ tối đa 16 Mb/s

- Category 5:** Có thể truyền dữ liệu tốc độ tối đa 100 Mb/s
- Category 5e:** Có thể truyền dữ liệu tốc độ tối đa 1000 Mb/s (1 Gb/s)
- Category 6:** Bao gồm 4 đôi dây đồng 24-gauge, có thể truyền dữ liệu tốc độ tối đa 1000 Mb/s

Ngày nay cáp UTP dùng phổ biến là Categories 1 (dùng trong mạng điện thoại), 5, 5e, và 6.

Đầu nối RJ-45



Module 8-9

Để hiện thực UTP trong mạng cục bộ, bạn phải xác định chuẩn EIA/TIA cáp cần sử dụng, loại dây thẳng hoặc chéo và đầu nối tương ứng.

Nếu nhìn đầu nối RJ-45 như hình trên, bạn sẽ thấy 8 dây cáp màu được xoắn lại thành 4 cặp. Bốn dây (2 cặp) mang điện áp dương được gọi là “tip” (T1 tới T4); 4 dây còn lại mang điện áp âm (so với điện áp đất) được gọi là “ring” (R1 tới R4). Tip và ring là thuật ngữ xuất hiện từ ngày đầu trong điện thoại. Ngày nay, thuật ngữ này liên quan đến dây dương và âm trong mỗi cặp. Cặp dây thứ nhất gọi là T1 và R1, cặp thứ 2 là T2 và R2 ...

Đầu cắm RJ-45 được bấm ở đầu sợi cáp như hình trên các chân được đánh số 8 đến 1 tính từ trái sang phải.

Giắc cắm RJ-45



Module 8-10

Giắc cắm RJ-45 được gắn ở các hộp đấu nối hoặc patch panel như hình trên các chân được đánh số từ 1-8 tính từ trái sang phải.

Cáp thẳng UTP

Cable 10BASE-T/
100BASE-TX Straight-Through

Straight-Through Cable



Pin Label

1 TX+	1
2 TX-	2
3 RX+	3
4 NC	4
5 NC	5
6 RX-	6
7 NC	7
8 NC	8

Pin Label

TX+
TX-
RX+
NC
NC
RX-
NC
NC



Dây ở 2 đầu cáp có cùng thứ tự

Module 8-11

Cáp mạng UTP dùng kết nối các thiết bị có 2 loại là :

- Cáp thẳng (straight-through)
- Cáp chép (crossover)

Đối với cáp thẳng đầu nối RJ-45 ở hai phía của dây cáp có cùng thứ tự các chân. Trên hình vẽ ta thấy cách bố trí các cặp cáp đồng ở hai đầu dây cáp thẳng.

Hub hoặc máy chủ

Máy chủ hay máy tính

Chân số	Màu Màu	Máy chủ hay máy tính	Chức năng Chức năng	Chân số
1		Trắng/Xanh lá 1	TX+	
2		Xanh lá 2	TX-	Xanh lá
3		Trắng/Cam 3	RX+	Trắng/Cam
6		Cam 6	RX-	Cam
		RX+		

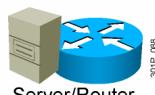
Cáp chép UTP

Cable 10BASE-T or
100BASE-TX Straight-Through

Crossover Cable



Hub/Switch



Server/Router

Pin Label

1 TX+	1
2 TX-	2
3 RX+	3
4 NC	4
5 NC	5
6 RX-	6
7 NC	7
8 NC	8

Pin Label

TX+
TX-
RX+
NC
NC
RX-
NC
NC

EIA/TIA T568A

1	white green
2	green
3	white orange
4	blue
5	white blue
6	orange
7	white brown
8	brown

EIA/TIA T568B

8	brown
7	white brown
6	green
5	white blue
4	blue
3	white green
2	orange
1	white orange

Một số dây ở 2 đầu cáp được bắt chéo

Module 8-12

Dây cáp chéo 2 đôi cáp 1-2, 3-6 được hoán chuyển vị trí ở 2 đầu cáp (xem hình vẽ)

Hub hoặc máy chủ

Máy chủ hay máy tính

Chân số

Màu

Màu

1

Trắng/Xanh lá
3

RX+

2

Xanh lá
6
RX

3

Trắng/Cam
1

TX+

6

Cam
2

TX-

Chức năng
Chức năng

TX+

Trắng/Cam

TX-

Cam

RX+

Trắng/Xanh

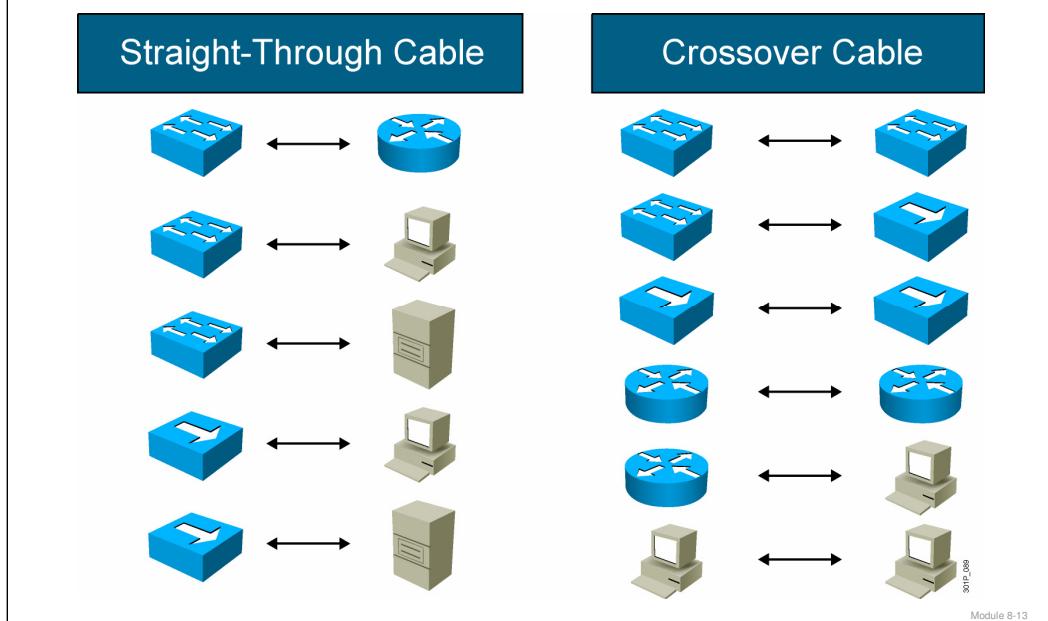
Chân

số

lá

RX-
Xanh lá

UTP Implementation: Straight-Through vs. Crossover



Module 8-13

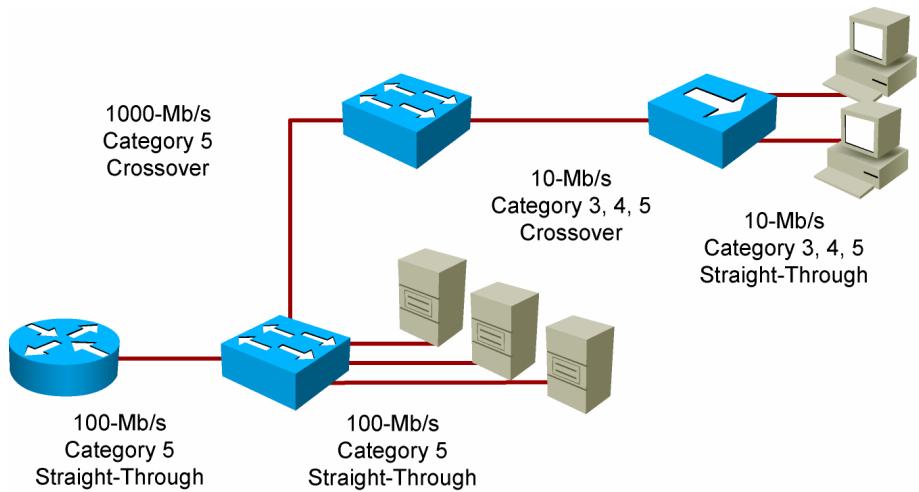
Hình trên minh họa cách sử dụng cáp trong đầu nối thiết bị của mạng Ethernet
Cáp thẳng dùng trong trường hợp sau :

- Switch nối router
- Switch nối PC hoặc server
- Hub nối PC hoặc server

Cáp chéo dùng trong các trường hợp sau :

- Switch nối switch
- Switch nối hub
- Hub nối hub
- Router nối router
- Nối cổng Ethernet của router và PC
- PC nối PC

Sử dụng các loại cáp UTP



Module 8-14

Hình trên minh họa cách sử dụng các loại cáp khác nhau trong một mô hình mạng

Tóm tắt

- Còn được gọi là bộ điều hợp mạng, các mạng được gắn vào bo mạch chủ và cung cấp cổng để nối vào mạng.
- Địa chỉ MAC được ghi vào các mạng bởi nhà cung cấp, địa chỉ vật lý duy nhất cho phép thiết bị tham gia vào mạng.
- Cáp và đầu nối dùng cho mạng Ethernet tuân thủ theo chuẩn EIA/TIA.
- Loại cáp sử dụng trong mạng Ethernet được đặc tả theo chuẩn EIA/TIA-568 (SP-2840).

Module 8-15

Tóm tắt (tiếp tục.)

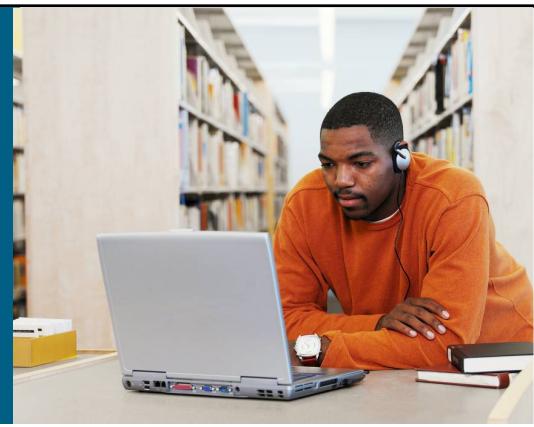
- Cáp UTP gồm 4 đôi dây. Mỗi dây đồng được phủ một lớp cách điện và từng đôi được xoắn lại với nhau.
- Dây cáp chéo được dùng nối kết các thiết bị cùng loại (ví dụ switch nối switch, router nối router, PC nối PC, và hub nối hub).
- Dây thẳng dùng nối kết các thiết bị không cùng loại (ví dụ switch nối router, switch nối PC, hub nối router, và hub nối PC).

Module 8-16



Module 8-17

Bài 9: Hiểu về môi trường Mạng cục bộ chia sẻ



Mạng cục bộ Ethernet

© 2007 Cisco Systems, Inc. All rights reserved.

Module 9-1

- **Tổng quan:**

Môđun này mô tả các kiểu topo mạng nội bộ (LAN), chi tiết của những thông tin được chia sẻ trong LAN và những thông tin ấy được trao đổi trong công nghệ LAN chuyển mạch (switched LAN) như thế nào, đồng thời chỉ ra các phương pháp tối ưu hóa việc trao đổi dữ liệu trong LAN.

- **Mục tiêu:** Sau khi hoàn tất, HV có thể hiểu cách mở rộng LAN bằng cách thêm HUB (thiết bị mạng ở lớp 1)

- Mô tả các vấn đề liên quan đến việc thông tin trao đổi trong mạng LAN Ethernet.
- Định dạng các giải pháp cho mạng Ethernet trong môi trường LAN chuyển mạch.
- Mô tả việc di chuyển dữ liệu từ máy này sang máy khác (host-to-host. Host có thể xem là 1 PC hay 1 thiết bị mạng) thông qua các thiết bị chuyển mạch (switch).
- Mô tả các điểm đặc trưng và nhiệm vụ của Cisco IOS (hệ điều hành Cisco).
- Cấu hình các bộ chuyển mạch bắt đầu từ các bộ chuyển mạch ở tầng truy cập (access layer).
- Kích hoạt bảo mật trên bộ chuyển mạch (Switch) ở các mức độ: vật lý (physical), truy cập (access) và cổng liên kết (port).
- Liệt kê các biện pháp tối ưu hệ thống LAN switch
- Mô tả phương pháp giải quyết sự cố trong môi trường LAN Switch.

- Tổng quan về Bài 9:

- LAN nghĩa là chia sẻ tài nguyên mạng đất tiền. LAN cho phép nhiều người dùng trong một khu vực địa lý giới hạn trao đổi các tập tin, các thông điệp và truy cập vào các máy chủ dùng chung. LAN có mức tiến hóa nhanh chóng trong việc hỗ trợ các giao dịch cấp thiết trong môi trường công ty, doanh nghiệp. Bài học mô tả việc trao đổi thông tin trong LAN phải đôi mặt với việc nhu cầu về băng thông (bandwidth) tăng nhanh và yêu cầu tốc độ cao đáp ứng đồng thời cho các nhu cầu của nhiều người dùng.
- Mục tiêu của bài 9: Sau khi hoàn tất, HV có thể hiểu cách các vấn đề liên quan đến nhu cầu mở rộng
 - Định nghĩa và tìm giới hạn của việc phân đoạn mạng LAN (LAN segments).
 - Liệt kê các tính chất và nhiệm vụ của HUB trong Ethernet LAN
 - Định nghĩa việc Đụng Độ (collisions) trên LAN và liệt kê các điều kiện gây ra.
 - Định nghĩa việc miền xảy ra Đụng Độ trong Ethernet LAN

Các giới hạn về phân vùng mạng nội bộ



- Tín hiệu bị suy giảm khi thông tin di chuyển xa.
- Mỗi kiểu mạng Ethernet bị giới hạn về độ dài phân đoạn mạng.

© 2007 Cisco Systems, Inc. All rights reserved.

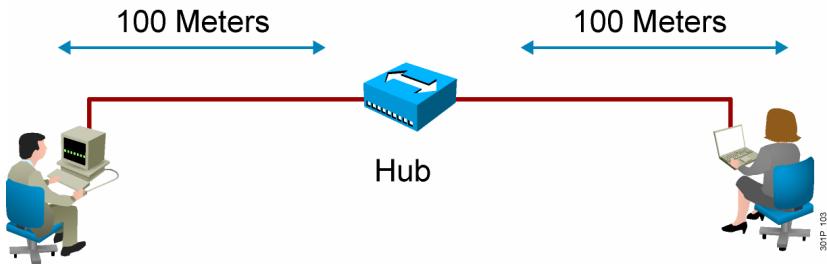
Module 9-3

- Chiều dài đoạn mạng là một vấn đề quan trọng khi dùng công nghệ Ethernet trong LAN. Chủ đề này mô tả công việc phân đoạn mạng và giới hạn của nó.
- Một đoạn (segment) mạng là một mạng kết nối vào một hệ cáp đơn liên tục. Cáp Ethernet và phân đoạn tương ứng có thể mở rộng theo sự giới hạn về khu vực, nếu càng xa thì việc di chuyển dữ liệu càng bị giảm thiểu do bị nhiễu, suy hao hay bị triệt tiêu... Theo chuẩn “Carrier Sense Multiple Access with Collision Detection (CSMA/CD)” trong cơ chế phát hiện đụng độ. Kiểu cáp, tỉ lệ dữ liệu truyền, kỹ thuật modun hóa ảnh hưởng chiều dài giới hạn của phân đoạn mạng.
- Các thiết bị hoạt động ở tầng 1 (vật lý) trong mô hình OSI sẽ không thể dùng để kết thúc phân đoạn mạng Ethernet trong LAN, bởi vì thiết bị tầng 1 chỉ lặp lại tín hiệu điện.
- Mỗi kiểu Ethernet quy chuẩn loại Cáp, tỉ lệ truyền thông tin, kỹ thuật modun hóa sẽ xác định chiều dài cực đại của đoạn mạng tương ứng. Xem bảng để biết chi tiết: Đây là vài hướng dẫn, dùng chuẩn 10BASE-T (Ethernet chạy trên cáp xoắn đôi - twisted pair):
 - 10 : Tốc độ, tương đương 10 triệu bit trên giây (Mb/s).
 - Base : nghĩa là baseband Ethernet.
 - T : Nghĩa là twisted-pair, Category 5 hay cao hơn.
 - FL: Nghĩa là cáp quang (fiber-optic).

- Ethernet Segment Distance Limitations

Chuẩn Ethernet	Mô tả	Chiều dài cực đại
10BASE-T 10-Mb/s	Ethernet over twisted pair	100 m
10BASE-FL 10-Mb/s	Ethernet over fiber-optic cable	2000 m
100BASE-TX 100-Mb/s	Ethernet over twisted pair	100 m
100BASE-FX	FEthernet over fiber-optic cable	400 m
•		

Mở rộng mạng cục bộ.



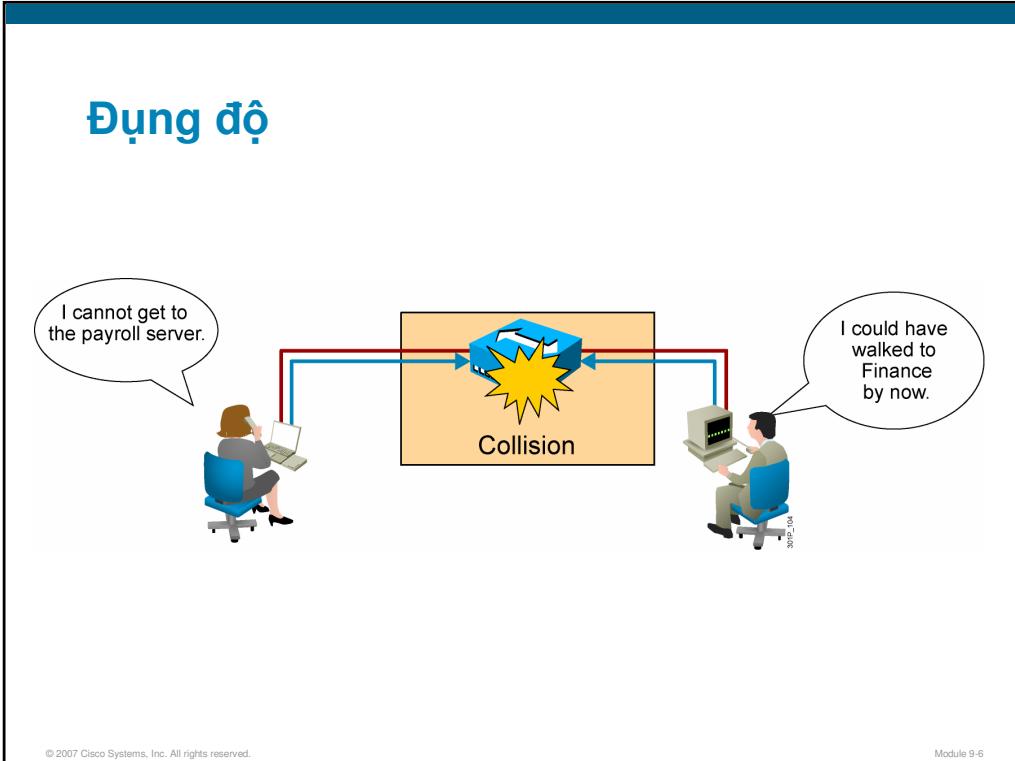
- Bandwidth dùng chung
- Mở rộng bằng Cable
- Lắp lại hay khuyếch đại tín hiệu.

© 2007 Cisco Systems, Inc. All rights reserved.

Module 9-5

- Bạn có thể thêm thiết bị để mở rộng đoạn mạng LAN. Chủ đề này mô tả cách thêm bộ lặp lại (repeater) hay hub có thể giúp cho việc mở rộng sự giới hạn về khoảng cách của Ethernet LAN.
- Repeater là thiết bị ở tầng vật lý (physical-layer) thực hiện nhận tín hiệu từ một thiết bị trên mạng và thực hiện việc khuyếch đại tín hiệu ấy trở lại như nguyên bản. Thêm repeater vào mạng có thể mở rộng phân đoạn mạng, nhờ đó dữ liệu có thể được chuyển thành công trong khoảng cách xa hơn. Tuy thế, số repeater thêm vào một phân đoạn mạng là giới hạn (theo quy luật 5-4-3-2-1).
- Hub, cũng là thiết bị ở tầng vật lý, hoạt động như một repeater. Khi Hub nhận một tín hiệu, nó khuyếch đại và gửi lại tín hiệu trên dây. HUB khác với repeater ở chỗ nó có nhiều cổng, cùng lúc kết nối vào nhiều thiết bị. Do đó, tín hiệu sẽ được nhắc lại trên tất cả các cổng có thiết bị kết nối. Hub không đọc dữ liệu đi ngang qua nó đồng thời không quan tâm đến nguồn gốc cũng như đích đến của dữ liệu (frame). Nói một cách đơn giản, HUB nhận các bit dữ liệu, khuyếch đại tín hiệu điện và gởi tiếp tín hiệu này đến tất cả các cổng (port hub) có thiết bị gắn vào.
- hub mở rộng mạng Ethernet LAN. Sự giới hạn của băng thông trong môi trường dùng chung (shared technology) vẫn còn tồn tại. Mặc dù mỗi thiết bị có cáp nối riêng, nhưng tất cả chúng (các thiết bị nối vào HUB – hay các người dùng cuối) chia sẻ nhau cùng một băng thông.

Đụng độ

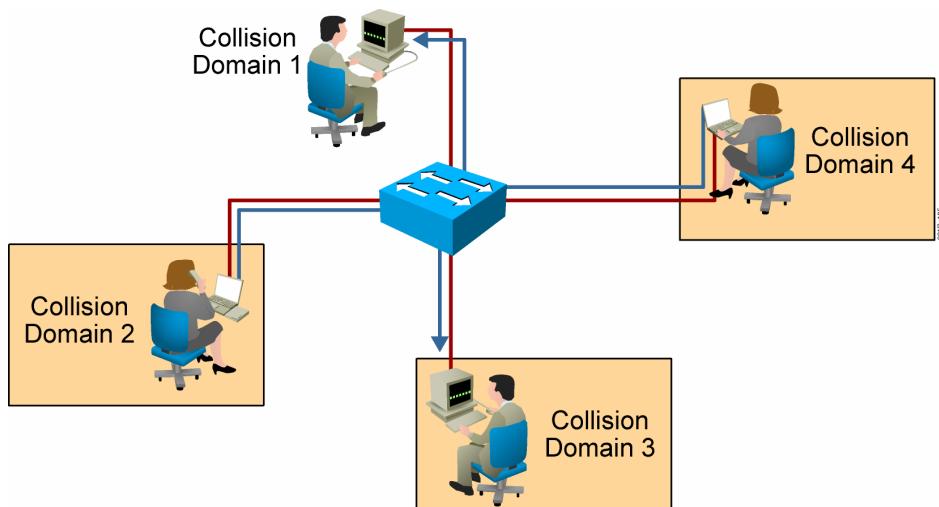


© 2007 Cisco Systems, Inc. All rights reserved.

Module 9-6

- Đụng độ (Collision) là phần hoạt động không thể thiếu trong Ethernet, nó xảy ra khi hai trạm cùng muốn chuyển dữ liệu trong cùng một lúc. Chủ đề này mô tả đụng độ xảy ra như thế nào trên LAN.
- Collisions là hệ quả của phương pháp truyền dẫn CSMA/CD trong Ethernet. Một mạng Ethernet, nhiều thiết bị chia sẻ chung một phân đoạn mạng. Mặc dù phải lắng nghe xem môi trường truyền có rảnh hay kô, các máy trạm cũng đồng thời muốn gửi dữ liệu của mình ra dây. Nếu 2 hay nhiều trạm chuyển dữ liệu cùng lúc đụng độ xảy ra và khung dữ liệu truyền từ các trạm sẽ bị hủy bỏ. Khi máy gửi phát hiện ra đụng độ, nó tự động gửi tín hiệu đặc biệt gọi là "tín hiệu jam" theo một quy định trước về thời gian do đó các thiết bị khác trên phân đoạn mạng biết về tình trạng đụng độ, các khung dữ liệu đang truyền sẽ bị hỏng và chấm dứt việc liên lạc. Các trạm sẽ bắt đầu chờ một khoảng thời gian ngẫu nhiên theo quy định cho đến lúc có thể bắt đầu chuyển dữ liệu trở lại.
- Khi mạng trở nên lớn hơn và dùng nhiều băng thông hơn, việc xảy ra đụng độ và tái chuyển dữ liệu xảy ra nhiều hơn. Điều này có thể dẫn đến mạng bị nghẽn hay thậm chí không tồn tại.
- Thêm HUB vô mạng Ethernet LAN có thể giải bài toán về khoảng cách nhưng không xử lý được yêu cầu về đụng độ.

Vùng xảy ra nhiều đụng độ



© 2007 Cisco Systems, Inc. All rights reserved.

Module 9-7

- Khi mở rộng mạng LAN cho phù hợp nhu cầu tăng thêm người dùng, băng thông hữu dụng ... Chúng ta có thể tạo ra các phân đoạn mạng vật lý độc lập gọi là Vùng đụng độ (collision domain), do đó hiện tượng đụng độ chỉ xảy ra trong khu vực giới hạn thay vì trên một mạng lớn. Slide này mô tả collision domain.
- Theo phân đoạn mạng Ethernet truyền thống, Các thiết bị mạng chia sẻ cùng băng thông nhưng chỉ có 1 thiết bị chuyển dữ liệu ra dây tại 1 thời điểm. Phân đoạn mạng như thế gọi là collision domain, bởi vì khi 2 hay nhiều thiết bị gửi dữ liệu cùng lúc đụng độ sẽ xảy ra.
- Do đó, dùng thiết bị mạng ở lớp 2 (Data link) của mô hình OSI sẽ phân hoạch mạng thành nhiều colission domain nhỏ hơn trong đó số thiết bị sẽ ít lại giúp cho việc băng thông hữu dụng sẽ nhiều hơn và đụng độ xảy ra tại một phân đoạn sẽ không ảnh hưởng đến các phân đoạn còn lại.
- Vùng quảng bá (broadcast domain) là một vùng trong đó thông tin được gửi tới tất cả các thiết bị được kết nối. Bộ lọc các khung (frame) dữ liệu dựa trên địa chỉ Media Access Control (MAC) tại Switch không thể lọc các dữ liệu loại quảng bá (broadcast frames). Theo cách bình thường, broadcast frames buộc phải chuyển tiếp do đó môi trường mạng do các switch kết nối tạo ra một broadcast domain. Cần phải có thiết bị ở tầng 3 giới hạn miền quảng bá ví dụ bộ định tuyến (router). Như vậy mỗi một giao diện (interface) của Router là một Broadcast domain. Một Broadcast domain có thể gồm nhiều Collision domain.

Tóm tắt

- Một đoạn mạng hình thành từ việc liên kết liên tục cable mạng. Cable mạng Ethernet và phân đoạn mạng bị giới hạn về độ dài vật lý, khi trao đổi thông tin trên khoảng cách xa, thông tin bị suy hao.
- HUB mở rộng mạng. HUB nhận thông tin đến khuyếch đại và chuyển đến tất cả các cổng ra khác đến tất cả các thiết bị mạng kết nối vào HUB.
- Nếu có nhiều hơn 1 thiết bị chuyển thông tin ra dây trên một phân đoạn mạng, quá trình đụng độ xảy ra.

Tóm tắt (tiếp theo.)

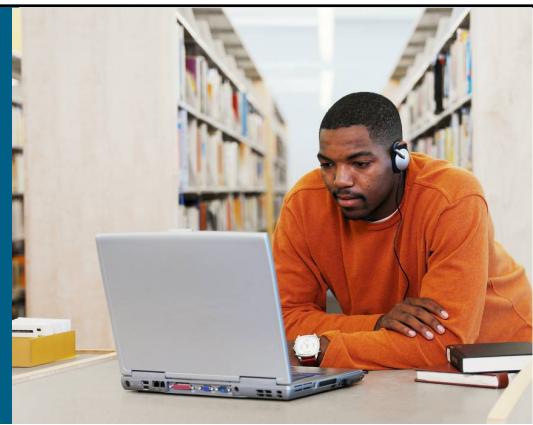
- Phân đoạn mạng cùng chia sẻ bandwidth được gọi là vùng dụng độ.
- Nếu dùng thiết bị vận hành ở layer 2 trở lên trong mô hình OSI thì có thể giảm bớt số thiết bị đồng thời tăng thêm bandwidth cho các thiết bị mạng trong phân đoạn.



© 2007 Cisco Systems, Inc. All rights reserved.

Module 9-10

Bài 10: Giải quyết các thách thức trong mạng với Công nghệ LAN Switched



Ethernet LANs

Module 10-1

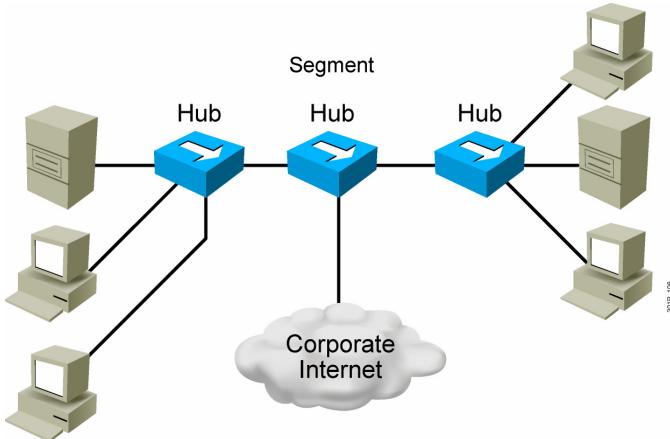
- **Tổng quan:**

Khi LAN trở nên quá tải và bị nghẽn nặng hơn, một vài nhân tố cùng ảnh hưởng đến năng lực của LAN. Các CPU của PC hiện đại có thể tính toán hơn 50,000 MIPS (Million Instructions Per Second). Các CPU nhanh hơn đòi hỏi tài nguyên mạng nhiều hơn, kết nối nhanh hơn, trao đổi dữ liệu nhiều hơn. Công nghệ mạng dùng Switch (Switching technology) cung ứng giải pháp cho các yêu cầu này. Ngoài ra, Bridge và Switch có thể giúp hệ thống mạng tăng tốc độ truyền tối đa và làm giảm thiểu sự cố nghẽn và dùng băng thông nhiều lên. Bài học mô tả switching technology giúp tăng cường hiệu quả của LAN.

- **Mục tiêu:** Sau khi kết thúc bài này, bạn có thể nhận thức được giải pháp dùng công nghệ **Switched LAN** trong môi trường LAN.:

- Xác định các lý do căn bản làm cho Ethernet LAN bị nghẽn.
- Liệt kê danh sách các thuộc tính và nhiệm vụ của bridge trong việc làm giảm sự cố nghẽn mạng.
- Liệt kê danh sách các thuộc tính và nhiệm vụ của switch
- So sánh hiệu quả hoạt động của một mạng khi dùng Switch và Bridge
- Liệt kê 3 nhiệm vụ của switch
- Mô tả cách thức làm việc của Switch
- Mô tả Hệ thống mạng LAN ngày nay khi dùng công nghệ Switching

Nghẽn mạng

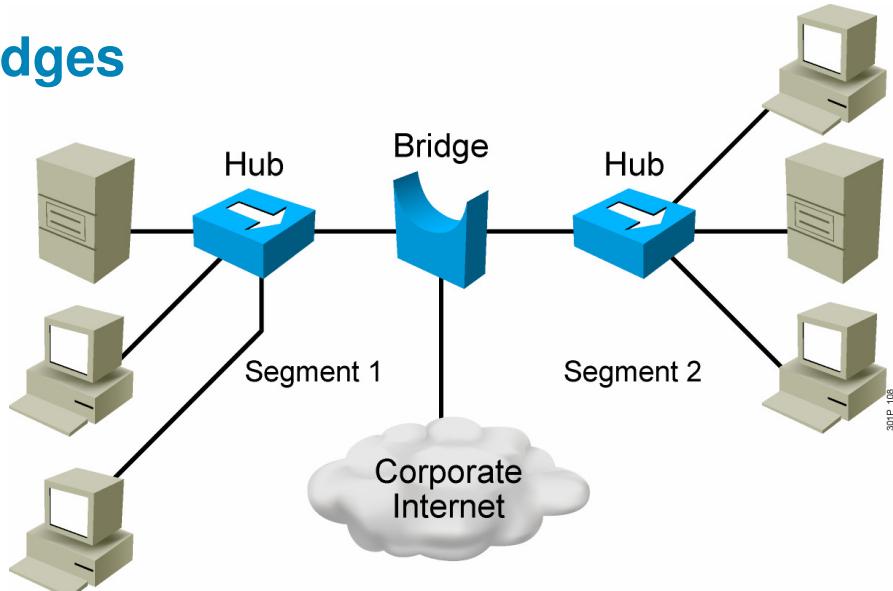


- Các PC có hiệu suất cao.
- Dữ liệu truyền trên mạng nhiều hơn
- Các ứng dụng đòi hỏi bandwidth nhiều hơn.

Module 10-2

- Mạng sẽ gặp sự cố nghẽn khi phát triển. Slide này mô tả các lý do thông thường nhất dẫn đến nghẽn mạng:
 - Nâng cấp PC và công nghệ mạng: Hiện nay, CPUs, Tuyến tải dữ liệu, các thiết bị ngoại vi hoạt động rất nhanh và mạnh so với hệ thống mạng trước đây do đó nhu cầu truyền data (dữ liệu) tốc độ cao trong mạng tăng nhanh.
 - Lượng data trao đổi tăng nhanh: dữ liệu trao đổi trên mạng hiện tại rất thông dụng, tài nguyên mạng dùng chung để ở xa, ngoài ra các dữ liệu loại quảng bá làm ảnh hưởng lớn đến hiệu suất mạng mặc dù TCP/IP không tạo ra nhiều thông tin loại quảng bá trong mạng.
 - Các ứng dụng đòi hỏi nhiều băng thông: Các ứng dụng đang ngày càng trở nên đa dạng, nhiều chức năng và đòi hỏi nhiều băng thông hơn. Thiết kế cho các nhà xuất bản nhỏ (Desktop publishing), Thiết kế kỹ thuật, video theo yêu cầu (VoD), Học từ xa qua mạng (e-learning), và Xem phim qua mạng ... — Tất cả các loại ứng dụng như thế đòi hỏi CPU mạnh và tốc độ truyền cao. Điều này làm cho hệ thống mạng dễ dàng quá tải

Bridges



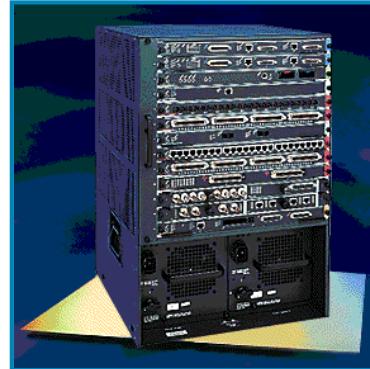
- Làm việc ở tầng 2 – mô hình OSI có thể chuyển, lọc hay làm tràn các cổng.
- Có ít cổng
- Chậm

Module 10-3

- Phân đoạn mạng ở lớp 2 trong mô hình OSICó thể giảm thiểu nghẽn, Bridge thực hiện việc này. Slide này mô tả cách bridge giả quyết nghẽn mạng như thế nào.
- Ethernet bridge dùng để chia nhỏ Ehternet LAN thành nhiều đoạn mạng nhỏ hơn. Điều này giúp tăng thêm nhiều collision domains và giảm tình trạng nghẽn mạng.
- Vài thuộc tính quan trọng của bridge:
 - Bridges làm việc ở lớp 2 trong mô hình OSI.
 - Bridges thông minh hơn HUB; bridge có thể phân tích frame (khung dữ liệu lớp 2) nhận vào và chuyển tiếp frame dựa vào thông tin địa chỉ đích đến.
 - Bridges có thể chứa frames giữa 2 hay nhiều đoạn mạng.
 - Bridges tạo nhiều collision domains và cho phép hơn 1 thiết bị chuyển data cùng lúc mà không gây ra đụng độ.
 - Bridges duy trì bảng địa chỉ MAC .
- Những lợi ích khi thêm bridges vào mạng:
 - Cố lập đoạn mạng có vấn đề trong một phân đoạn cụ thể.
 - Giảm tối thiểu data không cần thiết trên mạng nhờ lọc các frame trao đổi trong hay giữa các phân đoạn mạng.
 - Mở rộng LAN bằng cách kết nối nhiều phân đoạn mạng.

LAN Switch

- Cổng có dung lượng cao
- Bộ nhớ đệm (buffers) cho khung data (frame) lớn
- Tốc độ cổng đa trị.
- Chuyển mạch nội bộ nhanh
- Các mô hình chuyển mạch:
 - Cut-through
 - Store-and-forward
 - Fragment-free

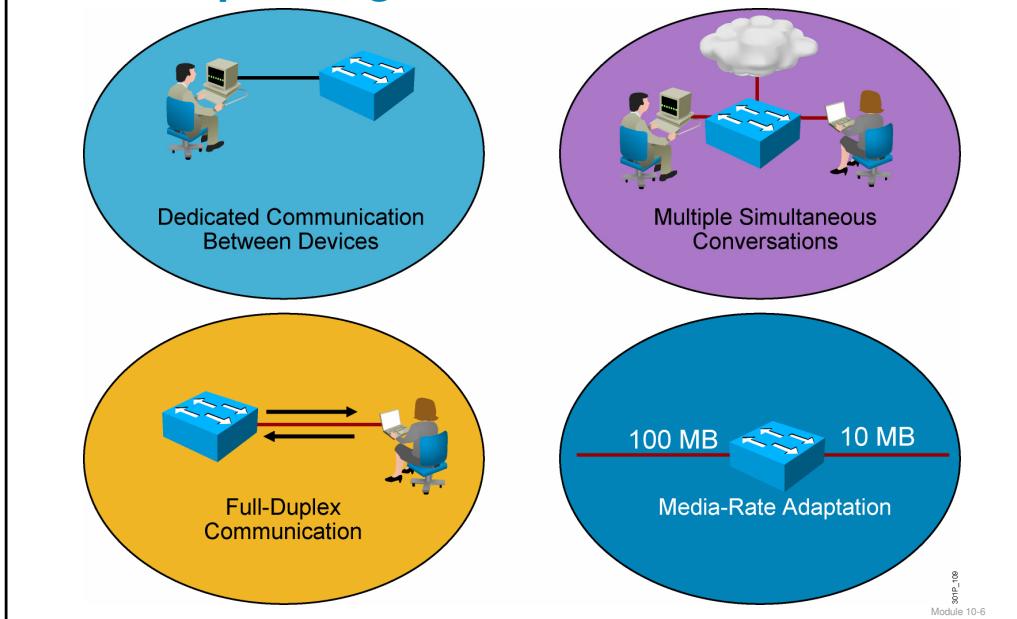


Module 10-4

- Hầu như giống Bridge nhưng LAN switches có thêm những thuộc tính đặc biệt giúp cho hệ thống mạng hoạt động tốt hơn.
- Switches kết nối các đoạn mạng LAN, dùng bảng địa chỉ MAC để xác định data được gửi đến đâu qua switch hay không được gửi qua switch để đến đoạn mạng khác, nhờ đó giảm được nghẽn mạng. Tuy nhiên, Switches hoạt động nhanh hơn và có nhiều ưu điểm hơn Bridge:
 - Cổng kết nối có tốc độ cao hơn: Switch có 24-port và 48-port rất thông dụng với tốc độ port 10 Mb/s và 100 Mb/s. Các doanh nghiệp lớn hơn có thể dùng những Switch đến hàng trăm port.
 - Bộ nhớ đệm lớn hơn: Năng lực chứa các khung dữ liệu nhận được trước khi bỏ chúng là một vấn đề, không thỏa mãn điều này có thể dẫn đến bị nghẽn ở các port nối với máy chủ.
 - Tốc độ Port: Tùy theo giá thành của Switch và có thể thay đổi từ 10 Mb/s, 100 Mb/s đến 1-Gb/s hay 10-Gb/s ports.
 - Chuyển mạch bên trong nhanh: Chuyển mạch bên trong Switch cho phép hỗ trợ nhiều loại tốc độ từ 10 Mb/s, 100 Mb/s, đến 1000 Mb/s. Phương pháp dùng chính thường là dùng bộ nhớ đệm trong hay dùng chung bộ nhớ ngoài, điều này ảnh hưởng khá lớn đến hiệu suất của Switch.

- Switches dùng 1 trong 2 phương pháp để chuyển data giữa các port :
 - Cut-through switching: Theo phương pháp này, Switch thực hiện việc chuyển data sang port đích ngay khi đọc đến địa chỉ đích trong khung (frame) data mà không cần dùng đến bộ nhớ đệm và chưa nhận frame hoàn tất . Phương pháp này nhanh nhất trong hai phương pháp nhưng không thể kiểm lỗi. Một phương pháp kế thừa có tên fragment-free switching, phương pháp này ngoài cách hoạt động giống như “Cut-through” còn giúp nhận biết đúng độ có xảy ra lỗi khi chuyển data.
 - Store-and-forward switching: Theo phương pháp này, khi Switch nhận data, nó chứa toàn bộ frame vào bộ nhớ đệm. Trong khi lưu trữ switch phân tích frame, kiểm tra lỗi và đích của nó trước khi thực hiện việc chuyển tiếp.
 - Fragment-free switching: Phương pháp Cut-through làm cho hệ thống chậm lại, và có thể chuyển tiếp data bị hỏng (kô kiểm lỗi), Switch phải bắt đầu chuyển tiếp Frame khi đã đọc hết phần đầu frame (header – hơn 64B) để bảo đảm kô bị đụng độ.

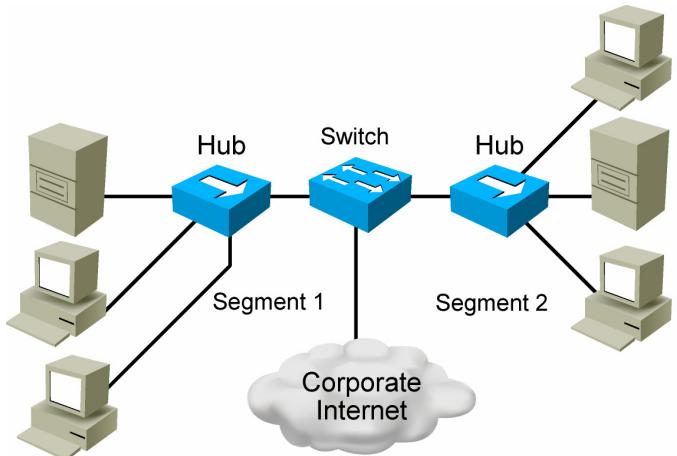
Các đặc trưng của LAN Switch



- Những điểm chung giữa bridges và switches:
 - Dùng để kết nối các phân đoạn mạng.
 - Dùng bảng địa chỉ MAC để nhận diện phân đoạn mạng nào data frame buộc phải gửi đến.
 - Giảm data không hợp lệ gửi trên hệ thống mạng.
- Để giới hạn nghẽn mạng, Switches cung ứng những vai trò quan trọng sau:
 - Dành riêng việc trao đổi giữa 2 thiết bị: Điều này tăng băng thông. Switches với việc chia 1 người dùng/Cổng có thể chia nhỏ phân đoạn mạng. Theo kiểu này, mỗi người dùng có thể dùng trọn vẹn bandwidth và tránh được việc bị đụng độ xảy ra trên hệ thống mạng.
 - Nhiều kiểu trao đổi dữ liệu đồng thời: có thể thấy thông qua việc chuyển tiếp hay chuyển mạch nhiều gói data cùng 1 thời điểm. Điều này giúp tăng cường năng lực hữu dụng của mạng. Một switch có thể hỗ trợ việc chuyển data giữa các cổng trên switch đồng thời ở tốc độ vật lý (wire-speed) và không bị khóa hiệu suất.
 - Kết nối 2 chiều: (Full-duplex communication) sau khi tạo kết nối, switch có thể cấu hình trên cổng (port) có thể đồng thời vừa gửi, vừa nhận tại một thời điểm (Full-duplex communication). Cấu hình half-duplex và full-duplex theo kiểu tự động có thể tự đàm phán khi liên kết được thiết lập. (Half-duplex nghĩa là chỉ trao đổi 1 chiều tại một thời điểm).

- Tỉ lệ tốc độ thích nghi: (Media-rate adaptation): Các cổng của switch có thể chạy với tốc độ từ 10Mbps đến 1000Mbps. Có thể cấu hình “cứng” không cho thay đổi tốc độ cổng nếu cần.

Switches thay thế Bridges

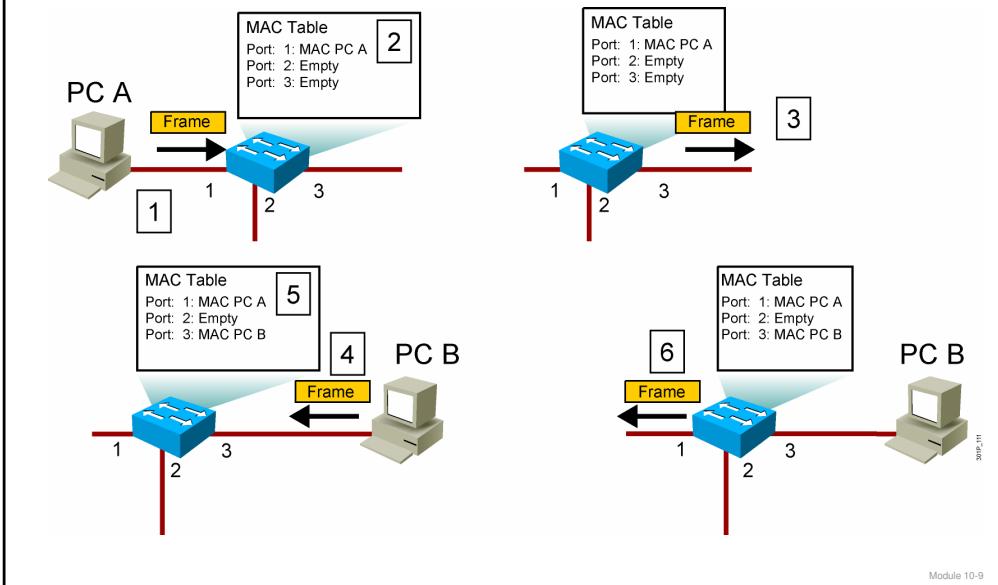


- Làm việc ở tầng 2 – mô hình OSI
- Có thẻ chuyển, lọc hay làm tràn các cổng.
- Có nhiều cổng
- Nhanh

Module 10-8

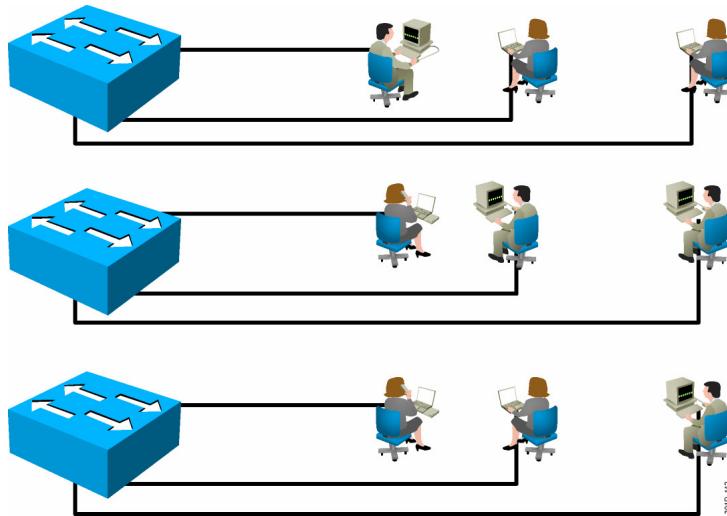
- Switches thay thế cho bridges.
- Switches xây dựng bảng địa chỉ MAC phù hợp với cổng kết nối tương ứng. Switches dùng bảng này để quyết định lọc, chuyển hay làm tràn các frame data.
- Bảng sau liệt kê hoạt động chuyển các unicast frames (khung dữ liệu đơn trị) trên Ethernet LAN; Các bước như sau:
 - 1. Khi unicast frame được nhận trên 1 port, switch so sánh giá trị địa chỉ MAC của nơi nhận chứa trong bảng MAC.
 - 2. Nếu switch nhận diện địa chỉ đích nằm trong cùng phân đoạn mạng với địa chỉ nguồn, nó không chuyển tiếp frame. Quá trình này gọi là lọc “filtering”, và thông qua cách này switches có thể giảm bớt các data không cần thiết chuyển qua phân đoạn mạng khác.
 - 3. Nếu switch nhận diện địa chỉ đích không nằm trong cùng phân đoạn mạng với địa chỉ nguồn, nó sẽ chuyển tiếp data (frame) đến phân đoạn mạng phù hợp.
 - 4. Nếu switch không nhận diện được địa chỉ đích (địa chỉ đích không nằm trong bảng MAC), nó sẽ chuyển đến tất cả các ports trừ port nhận thông tin. Quy trình này gọi là làm tràn (flooding).

Chuyển Frames trong Switch



- Khi một địa chỉ chưa được nhận biết, switch sẽ học bằng cách nhận diện địa chỉ nguồn từ frame nhận. Các bước thực hiện như sau:
 1. Switch nhận một broadcast frame từ PC A trên port 1.
 2. Switch nhập địa chỉ source MAC (địa chỉ MAC của PC A) vào bảng MAC.
 3. Bởi vì địa chỉ đích là địa chỉ broadcast, switch làm tràn tất cả các ports, ngoại trừ ports nhận frame.
 4. Thiết bị nhận trả lời bằng một unicast frame cho PC A.
 5. Switch nhập địa chỉ MAC của PC B và port nhận frame từ B vào bảng MAC. Địa chỉ đích của frame và port tương ứng được tìm thấy trong bảng MAC.
 6. Lúc này Switch có thể chuyển tiếp frames giữa 2 thiết bị (PC A và B) mà không cần dùng kỹ thuật làm tràn (flooding).

Mạng cục bộ hiện nay

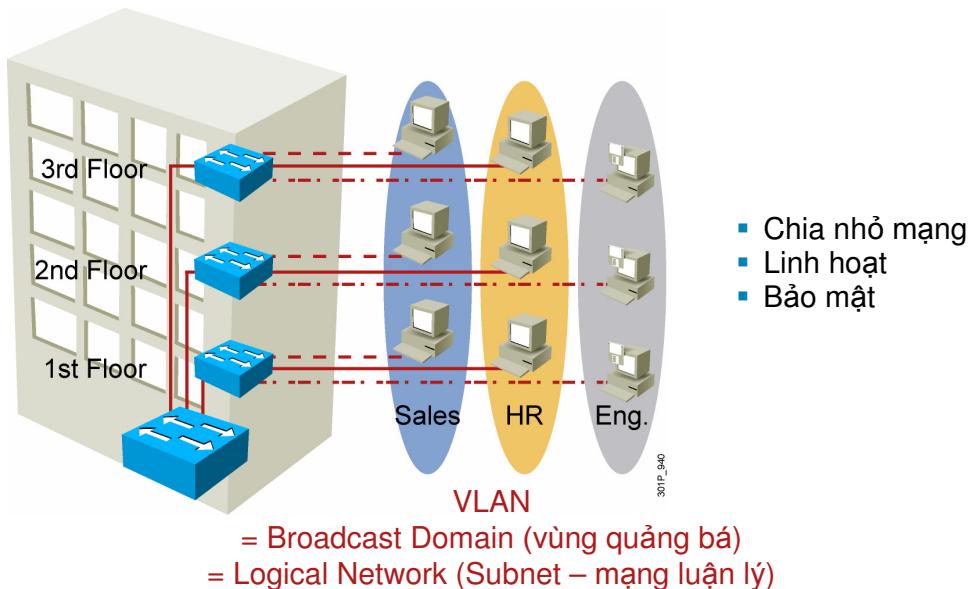


- Người dùng được nhóm theo khu vực vật lý.
- Nhiều switches được thêm vào mạng dễ dàng
- Kết nối các switch bằng đường truyền tốc độ cao.

Module 10-10

- Mạng các Switched rất thông dụng hiện nay. Giá thành theo port sẽ tăng lên rất nhiều do đó bridge và hub càng ít được chọn khi thiết kế mạng.
- Trong mạng switched, người dùng được nhóm theo các khu vực địa lý. Kiểu sắp xếp này cho phép các nhóm người dùng truy cập nhiều thiết bị khác trên mạng như máy chủ, đồng thời giảm đi khả năng bị xảy ra đụng độ cũng như tăng cường hiệu suất làm việc của hệ thống mạng.
- Để điều tiết nhiều người dùng phù hợp với các yêu cầu tăng cao về bandwidth, ngày càng nhiều switches được thêm vào hệ thống mạng. Qua đó giao thông tin giữa các switch sẽ tăng lên do đó việc xác định rõ ràng các phương cách liên kết hệ thống switch cần được tăng cường.

Tổng quan về VLAN



Module 10-11

- Một VLAN là một vùng quảng bá luận lý có thể mở rộng trong nhiều khu vực phân đoạn mạng vật lý. Trong khu vực liên kết các switch, VLANs có thể cung ứng cách phân chia và tổ chức hệ thống mạng một cách mềm dẻo. Bạn có thể thiết kế các cấu trúc các VLAN nhóm các người dùng cùng một tác vụ lại với nhau mà không cần quan ngại đến khu vực vật lý mà họ đang kết nối vào hệ thống mạng. Bạn có thể gán một port switch thuộc 1 VLAN, do đó tăng cường bảo mật cho hệ thống. Các Ports cùng VLAN sẽ cùng chia sẻ các quảng bá (broadcast); khác VLAN, ports không chia sẻ data loại quảng bá.
- Một VLAN có thể tồn tại trên một switch hay đồng thời nhiều switch. VLAN cũng có thể liên kết các trạm làm việc trong cùng tòa nhà hay giữa các tòa nhà. VLAN cũng có thể liên kết thông qua môi trường WAN.

Summary

- Nguyên nhân chính làm nghẽn mạng là máy tính mạnh hơn, công nghệ mạng đòi hỏi truyền dữ liệu nhiều hơn, các ứng dụng đòi hỏi băng thông lớn hơn ví dụ như: phần mềm xuất bản sách trên máy PC, học từ xa hay xem phim trực tuyến...
- Các bridges dùng để chia nhỏ mạng. Điều này làm giảm tình trạng úng độ trên phân đoạn mạng và giảm nghẽn mạng.
- Các Switches hoạt động ở tốc độ cao hơn bridges, cung ứng các cổng giao tiếp, chuyển mạch nội tốc độ cao. Ngoài ra switch cung cấp 2 phương pháp chính để chuyển mạch nhằm chuyển thông tin từ cổng này sang cổng khác: cut-through switching hay store-and-forward.

Module 10-12

Summary (Cont.)

- Switch cung cấp nhiều tính năng tốt hơn bridge như giúp cho giới hạn việc nghẽn mạng, cung ứng một bandwidth xác định và riêng cho từng port, giúp các thiết bị có thể gửi nhận cùng lúc và bandwidth có thể tự động thích nghi tốc độ giữa thiết bị.
- Switch hoạt động ở Layer 2 của mô hình OSI, sẽ phân tích các frame nhận và chuyển tiếp, lọc hay làm tràn tùy theo địa chỉ đích có trong bảng MAC hay chưa. Switch có thể tập hợp và chuyển các frame giữa hai phân đoạn mạng. Qua đó, switch làm tăng số vùng đụng độ (collision domain).
- Switch xây dựng bảng địa chỉ MAC về các thiết bị và áp vào port tương ứng. Switch dùng bảng MAC này để phân tích các frame.

Module 10-13

Summary (Cont.)

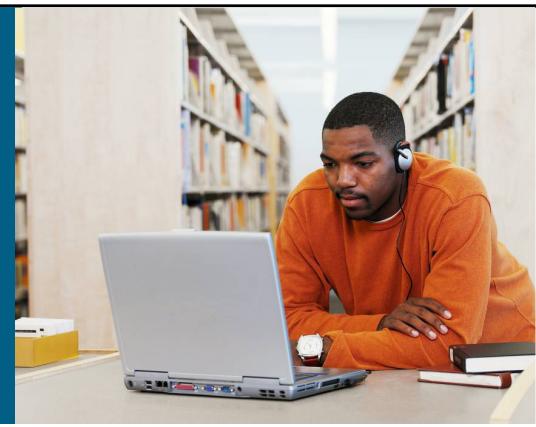
- Trong môi trường mạng switch, người dùng có thể được nhóm theo nhiệm vụ nhằm dùng chung tài nguyên mạng mà không cần quan tâm đến khu vực vật lý họ đang thuộc vào thông qua các VLAN. Switch cần được liên kết với nhau bằng các port tốc độ cao nhằm tăng cường hiệu suất làm việc trên mạng.

Module 10-14



Module 10-15

Bài 11: Khảo sát quy trình phân phối Packet (gói thông tin mạng)



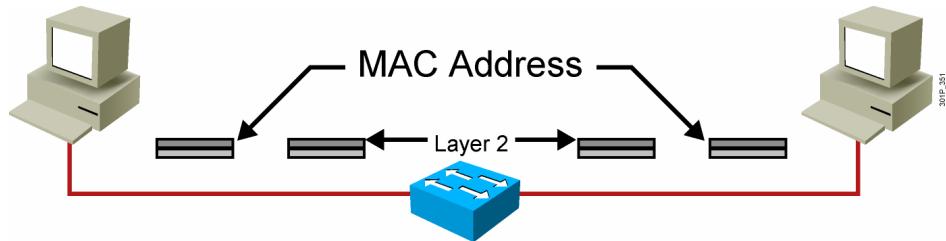
Ethernet LANs

Module 11-1

- **Mục tiêu:**

- Bài học cung cấp hình ảnh các data được chuyển từ máy này sang máy khác thông qua switch.
- Bạn được mô tả:
 - Địa chỉ Layer 2, 3
 - Gói thông tin được phân phối ra sao từ máy đến máy.

Địa chỉ Layer 2

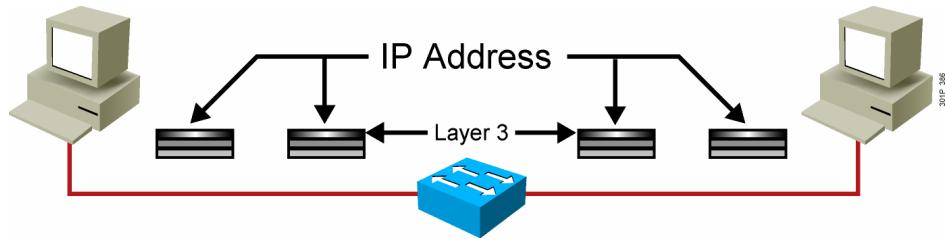


- Dùng địa chỉ MAC
- Được gán vào thiết bị đầu cuối.

Module 11-2

- Nhắc lại trong modun “Building a Simple Network”, Địa chỉ MAC được gán cho các thiết bị đầu cuối. Trong hầu hết các trường hợp, thiết bị ở Layer 2 như bridge và switch không được gán địa chỉ MAC. Tuy nhiên, trong vài tình huống đặc biệt, switch sẽ được gán địa chỉ MAC.

Địa chỉ Layer 3

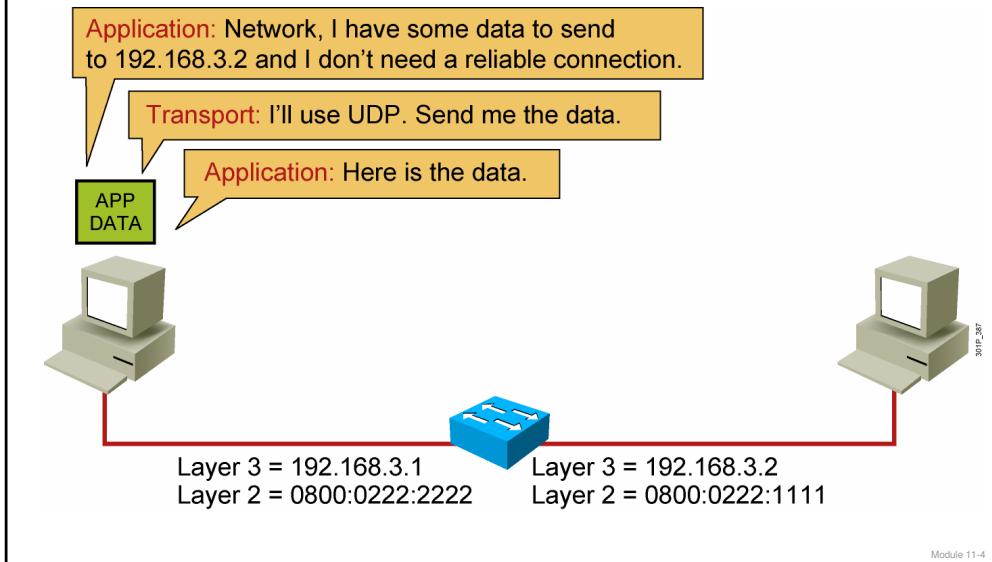


- Mỗi một NOS có một địa chỉ Layer 3.
- OSI dùng NSAP.
- TCP/IP dùng IP.

Module 11-3

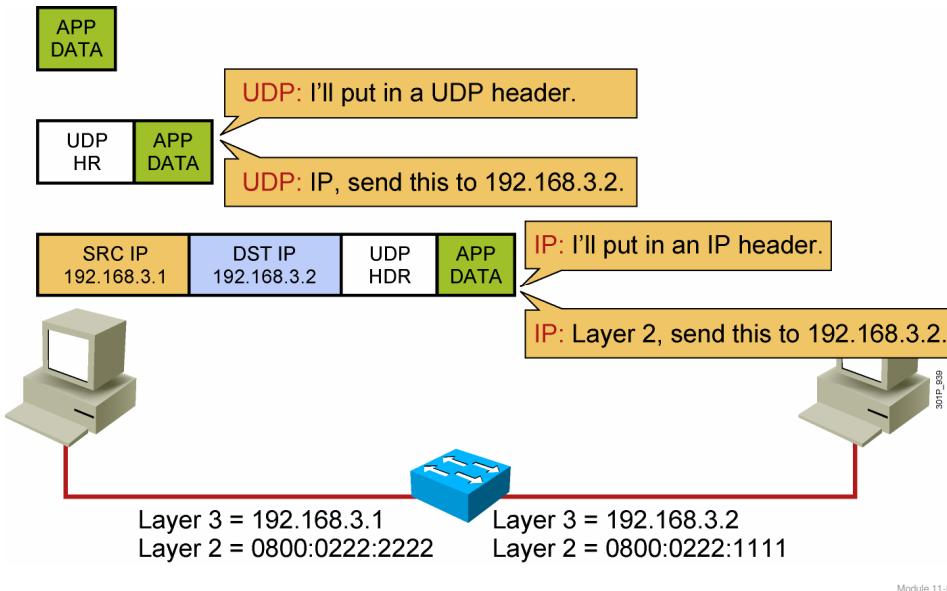
- Mỗi một NOS (network operating system) có một địa chỉ theo layer 3.

Sự phân phối dữ liệu từ Host - đến - Host (1 of 10)



- Ví dụ host 192.168.3.1 có data muỐc chuyẾn cho host 192.168.3.2. Ứng dụng không cần một liên kết đáng tin cậy. Giao thức UDP - User Datagram Protocol được dùng.

Sự phân phối dữ liệu từ Host- đến – Host (2 of 10)



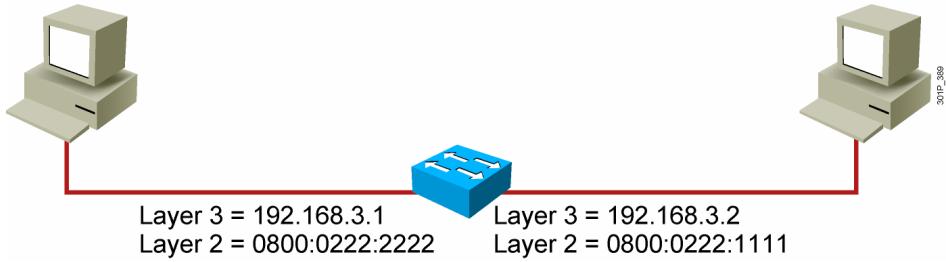
- Bởi không cần thiết lập phiên làm việc, ứng dụng có thể bắt đầu gửi data. UDP sẽ thêm phần đầu (UDP header) và chuyển protocol data unit (PDU) đến IP (Layer 3) với các chỉ thị để gửi thông tin này (PDU) đến 192.168.3.2. IP đóng gói PDU trong Layer 3 và chuyên nó đến Layer 2.

Sự phân phối dữ liệu từ Host- đến – Host (3 of 10)

Layer 2: ARP, do you have a mapping for 192.168.3.2 ?

ARP: Is 192.168.3.2 in my ARP table? No, I guess Layer 2 will have to hold the packet while I resolve the addressing.

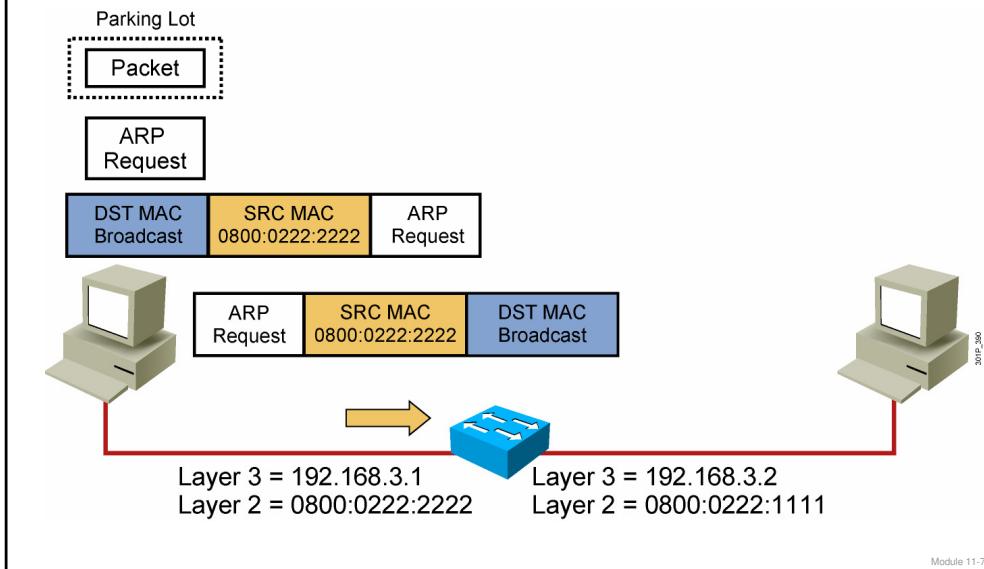
SRC IP 192.168.3.1	DST IP 192.168.3.2	UDP HDR	APP DATA
-----------------------	-----------------------	------------	-------------



Module 11-6

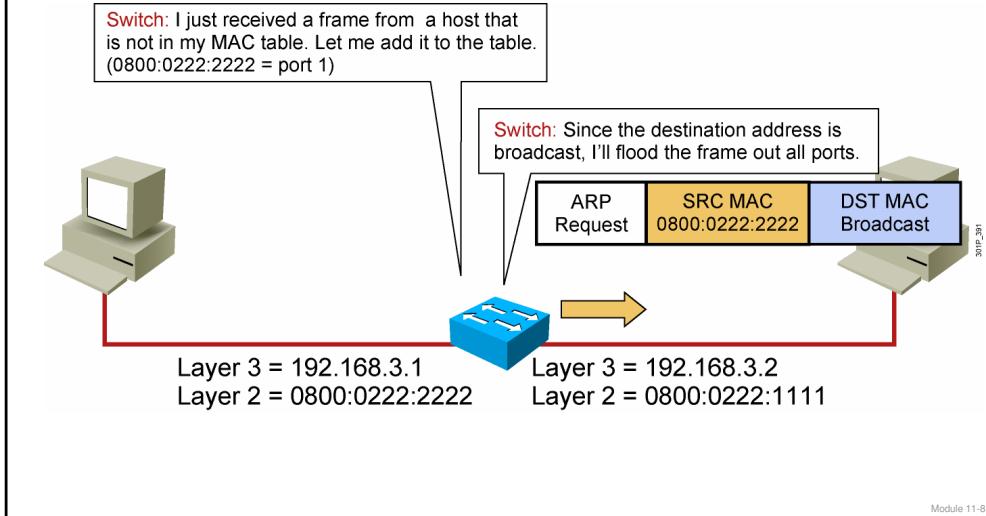
- Giao thức Address Resolution Protocol (ARP) không tham gia thành một mục trong bảng.

Sự phân phối dữ liệu từ Host- đến – Host (4 of 10)



- Host 192.168.3.1 gửi ARP request. Tuy thế trong ví dụ nó sẽ nhận thông tin từ switch trước khi liên lạc được máy ở xa.

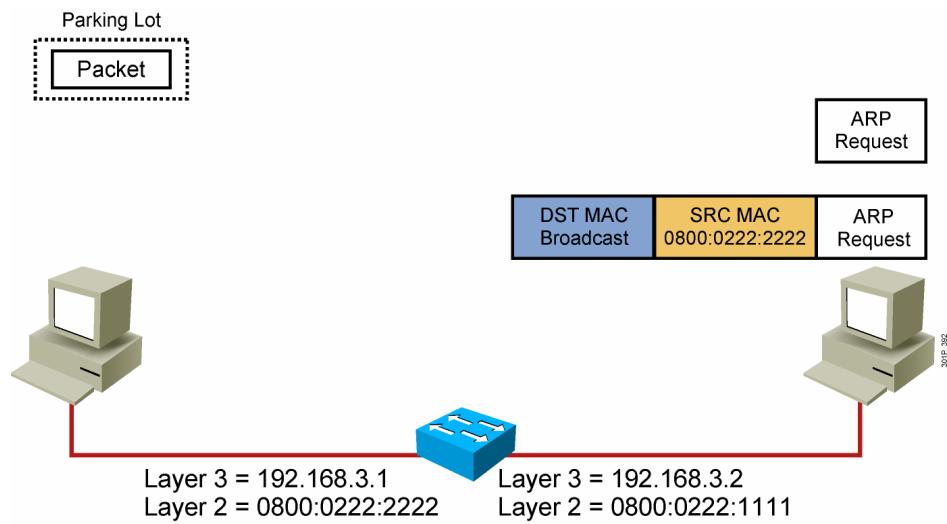
Sự phân phối dữ liệu từ Host- đến – Host (5 of 10)



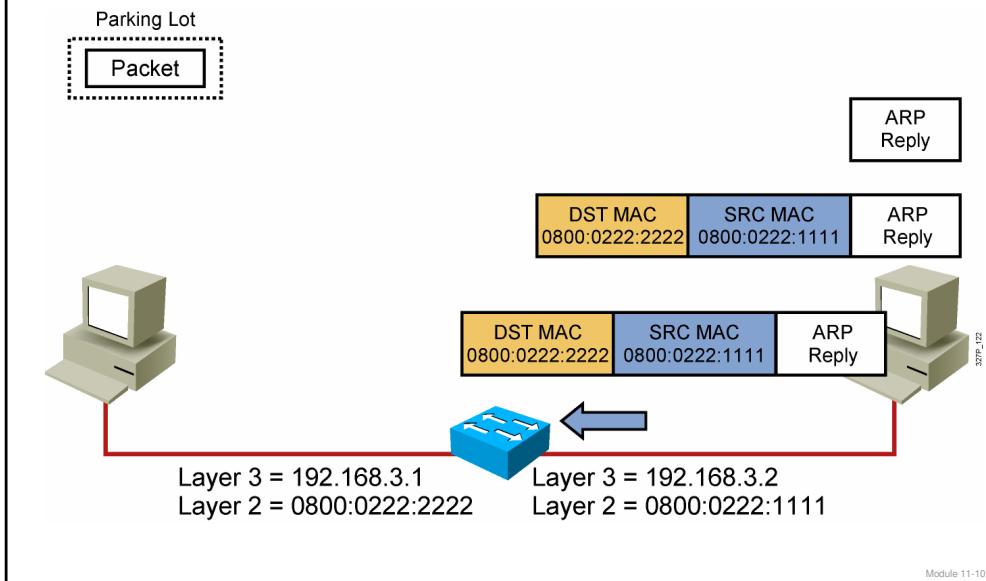
Module 11-8

- Khi switch nhận frame, nó phải chuyển đến port thích hợp. Tuy nhiên, trong ví dụ này, hoặc địa chỉ nguồn hay địa chỉ đích đang được lưu trong bảng MAC của switch. Switch có thể học việc đồng bộ địa chỉ MAC và port trong frame do đó switch có thể thêm như sau : 0800:0222:2222 = port 1). Bởi vì đích chỉ đích là địa chỉ quảng bá (broadcast) nên switch sẽ làm trá gói tông tin nhận ra tất cả các port còn lại. Ghi chú, switch không thay đổi nội dung của frame.

Sự phân phối dữ liệu từ Host- đến – Host (6 of 10)

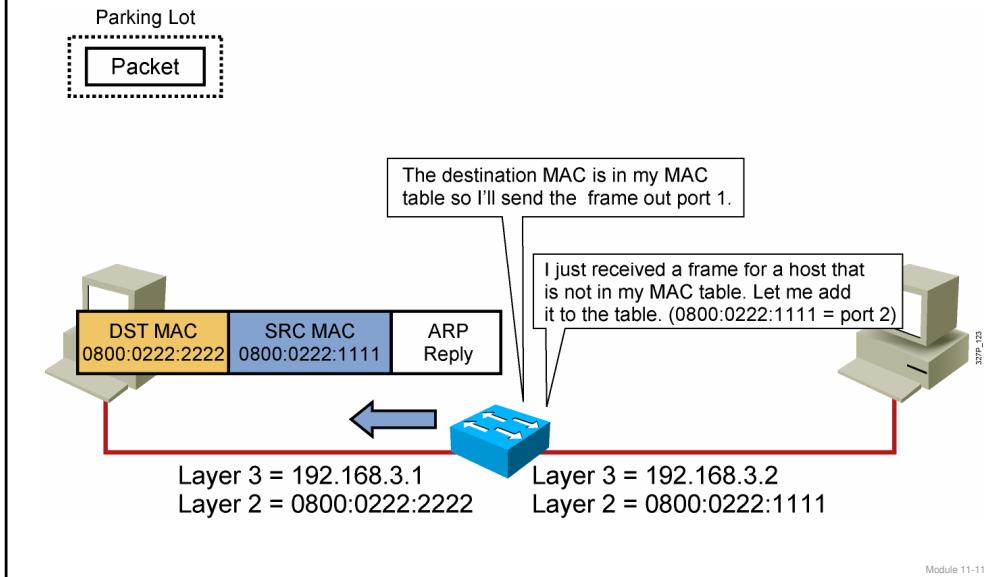


Sự phân phối dữ liệu từ Host- đến – Host (7 of 10)



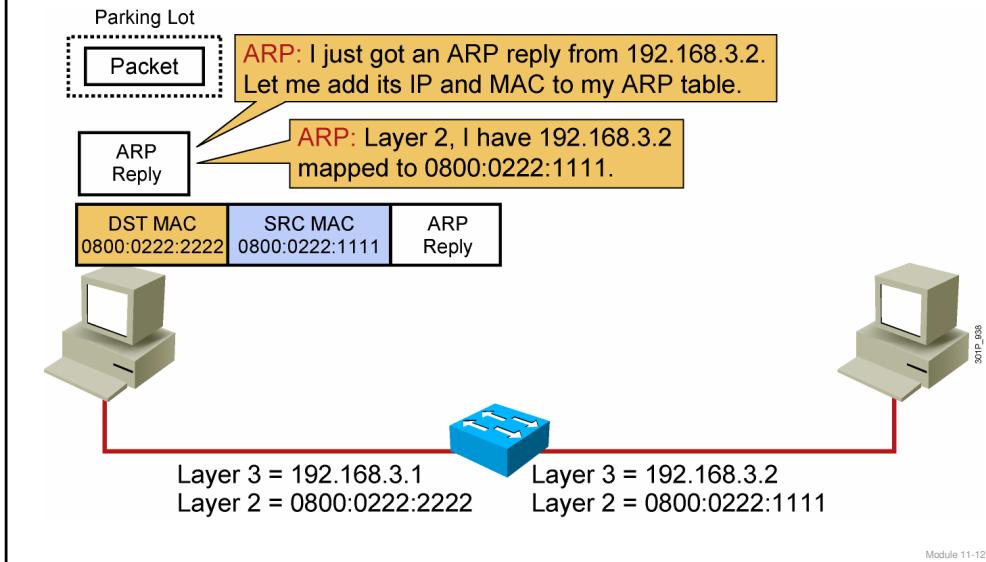
- Máy đích nhận yêu cầu ARP (ARP request) rồi trả lời.

Sự phân phối dữ liệu từ Host- đến – Host (8 of 10)

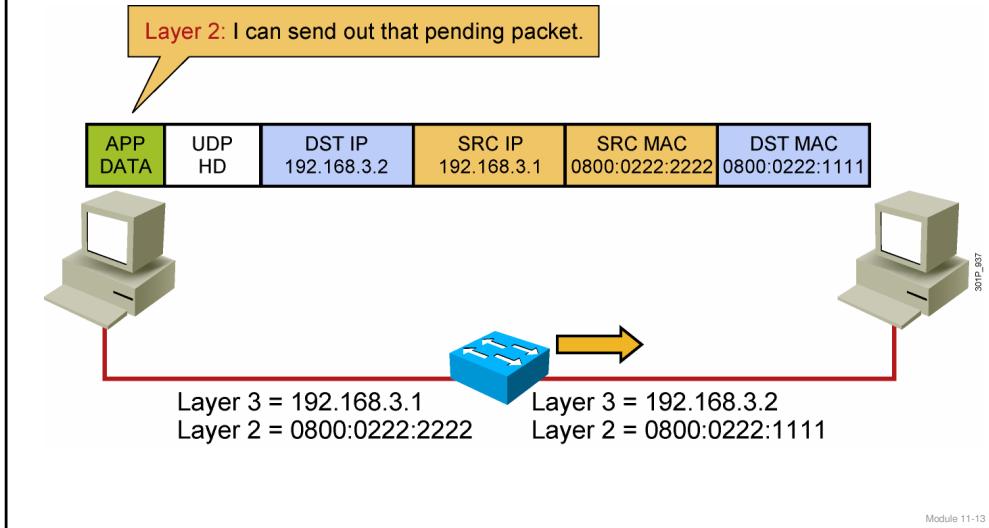


- Switch học được địa chỉ MAC của máy nguồn tương ứng với port trên switch. Vì thế, switch thêm một bản ghi vào bảng MAC 0800:0222:1111 = port 2. Bởi vì máy đích đã được thêm địa chỉ MAC vào bảng MA của switch do đó switch sẽ chuyển tiếp ra port 1.
- Ghi chú, switch không thay đổi nội dung của frame.

Sự phân phối dữ liệu từ Host- đến – Host (9 of 10)



Sự phân phối dữ liệu từ Host- đến – Host (10 of 10)



- Data được gửi và nhận. Mọi frames chuyển qua switch không thay đổi nội dung bên trong.

Tóm tắt

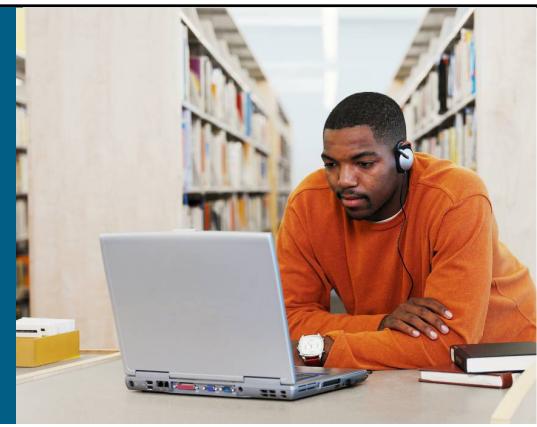
- Địa chỉ Layer 2 là Địa chỉ MAC.
- Địa chỉ Layer 3 là Địa chỉ IP.
- Nếu máy chưa biết địa chỉ MAC máy đích, giao thức dùng để đồng bộ địa chỉ Layer 2 vào Layer 3.
- Switches học Địa chỉ MAC và đăng ký vào port tương ứng bằng cách theo dõi đích chỉ nguồn của frame.
- Khi switch chuyển frame, nó không thay đổi địa chỉ layer 2 nguồn hay đích.

Module 11-14



Module 11-15

Bài 12: Vận hành Hệ Điều Hành Cisco IOS



Ethernet LANs

Module 12-1

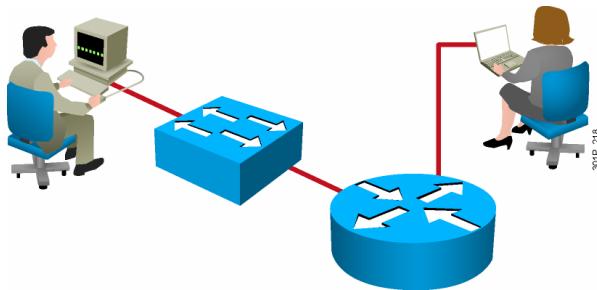
- **Tổng quan:**

- Những hiểu biết về môi trường mạng của doanh nghiệp sẽ tạo ra một viễn cảnh về những nhu cầu vận hành và điều khiển trên những thành phần mạng, điều đó được thực hiện bởi những thiết bị mạng phù hợp, ví dụ như các thiết bị Phần mềm Cisco IOS là một phần mềm mạng với nhiều đặc tính mạnh, cung cấp những giải pháp mạng thông minh cho những môi trường kinh doanh quan. Bài học này so sánh các chức năng của switches và các thiết bị trong những môi trường mạng nhỏ, mạng gia đình (SOHO) với các thành phần mạng trong môi trường mạng lớn, đồng thời mô tả các chức năng và cách vận hành của phần mềm Cisco IOS.

- **Mục tiêu:**

- Sau khi học, bạn có thể cài đặt kết nối vào các thiết bị Cisco. Bài học liệt kê các thuộc tính và nhiệm vụ của Cisco IOS trong các quan hệ môi trường mạng doanh nghiệp.
- Mô tả việc khởi tạo hoạt động của thiết bị Cisco
- Mô tả việc cấu hình từ ngoài các thiết bị Cisco
- Định nghĩa các thuộc tính của Cisco IOS CLI (các tương tác dạng câu lệnh - command line interactive)
- Mô tả làm thế nào để khởi động một phiên EXEC và thay đổi mode EXEC
- Định các tác vụ hỗ trợ online phù hợp với các CLI
- Mô tả các tác vụ mở rộng cho phần soạn thảo câu lệnh trong Cisco IOS CLI
- Dùng các thuộc tính lưu trữ lịch sử các câu lệnh trong CLI .

Hệ điều hành Cisco IOS



- Thuộc tính có thể giúp chọn giao thức mạng và nhiệm vụ.
- Kết nối tốc độ cao giữa các thiết bị.
- Quản trị việc truy cập vào thiết bị một cách bảo mật và ngăn chặn các truy cập trái phép.
- Khả năng thêm các cổng giao tiếp (interface) để mở rộng năng lực mạng.
- Tính đáng tin cậy để chắc chắn khả năng truy cập vào tài nguyên mạng.

Module 12-2

- Hạ tầng hệ thống Cisco IOS Software được hoàn thiện trong hầu hết các phần cứng của Cisco. Đó là phần mềm kiến trúc được nhúng vào bên trong tất cả các thiết bị Cisco và điều hành hoạt động của chúng (kể cả Cisco Catalyst switch).
- Hệ điều hành Cisco IOS cho phép thực hiện các dịch vụ sau trong các sản phẩm Cisco :
 - Thuộc tính có thể giúp chọn giao thức mạng và nhiệm vụ.
 - Kết nối tốc độ cao giữa các thiết bị
 - Quản trị việc truy cập vào thiết bị một cách bảo mật và ngăn chặn các truy cập trái phép.
 - Khả năng thêm các cổng giao tiếp (interface) để mở rộng năng lực mạng.
 - Tính đáng tin cậy để chắc chắn khả năng truy cập vào tài nguyên mạng
- Giao tiếp dạng câu lệnh trong Hệ điều hành Cisco IOS (CLI) là các truy cập thông qua kết nối vào màn hình cấu hình thiết bị (console), qua modem, hay Telnet. Tùy theo dạng kết nối được dùng, các truy cập vào thiết bị Cisco và dùng câu lệnh theo một cách tổng quát được xem như một phiên EXEC (EXEC session). (EXEC : Thi hành)

Cấu hình thiết bị mạng

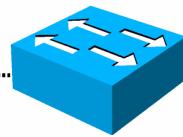
- Khởi động giá trị mặc định đủ cho switch hoạt động ở Layer 2.
- Một thiết bị Cisco sẽ thông tin qua dấu nhắc các giá trị khởi động mặc định nếu không có cấu hình nào trong bộ nhớ.
- Các cấu hình thêm bao gồm:
 - Địa chỉ cho giao thức mạng và các tham số.
 - Các tùy chọn cho quản trị và quản lý.

Module 12-3

- Khi các Cisco switch được khởi động lần đầu tiên, các giá trị khởi động mặc định trên thiết bị đủ cho switch hoạt động ở layer 2. Khi Cisco router được khởi động lần đầu tiên, cần có thông tin cấu hình để hoạt động ở layer 3 ví dụ địa chỉ IP trên switch dùng quản trị, do đó IOS trên switch có thể xuất hiện các đàm thoại gọi là trình: setup.
- Cấu hình “sets up” trên thiết bị bao gồm:
 - Địa chỉ cho giao thức mạng và các tham số. (ví dụ địa chỉ IP và subnetmask trên cổng giao tiếp)
 - Các tùy chọn cho quản trị và quản lý. (ví dụ mật khẩu truy cập...)
- Trong bài học, các cấu hình tối thiểu trên thiết bị sẽ được đề cập. Đây cũng là nhiệm vụ của quản trị mạng.

Tổng quan về khởi động đầu tiên trên các thiết bị CISCO

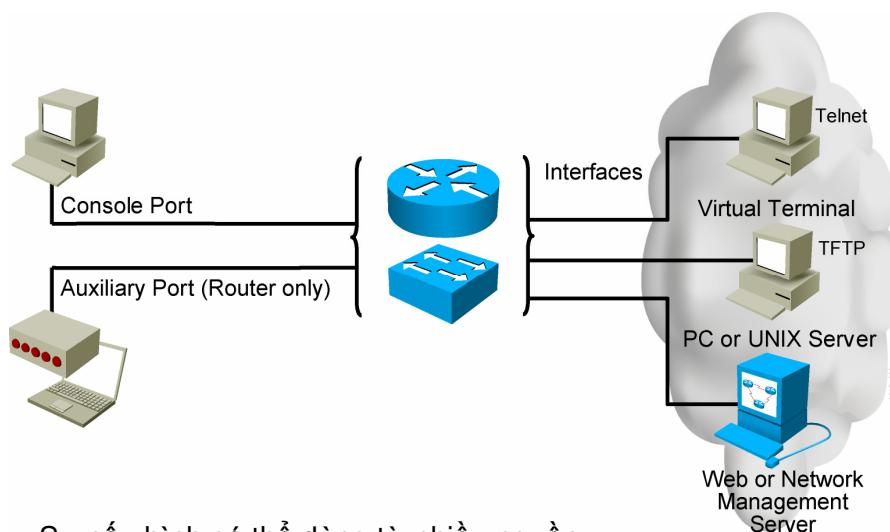
1. Find and check device hardware.
2. Find and load Cisco IOS software image.
3. Find and apply device configurations.



Module 12-4

- Khi khởi động lần đầu tiên, có 3 tác vụ chính được thực hiện trên thiết bị mạng Cisco:
 - 1. Thiết bị tự kiểm tra hardware. Trình power-on self-test (POST) thực hiện.
 - 2. Sau khi phần cứng đã được kiểm tra và tình trạng tốt, sẵn sàng để hoạt động, thiết bị sẽ thực hiện thủ tục khởi động. Thủ tục này sẽ “LOAD” (sao chép) hệ điều hành (software image) vào bộ nhớ.
 - 3. Sau khi HĐH đã LOAD, thiết bị sẽ tìm và chép tập tin cấu hình của thiết bị. (tập tin cấu hình dùng thiết lập hoạt động của thiết bị trong môi trường mạng).
- Một cách tự nhiên, sẽ có thủ tục trở ngược để thực hiện việc khởi động nếu cần thiết.

Cấu hình từ ngoài



- Sự cấu hình có thể dùng từ nhiều nguồn.
- Sự cấu hình thực hiện trên bộ nhớ của thiết bị.

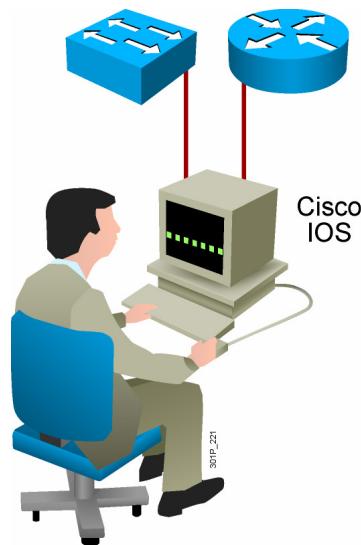
Module 12-5

- Bạn có thể truy cập các thiết bị từ xa bằng cách quay số qua modem đến cổng AUX hay CONSOLE trên thiết bị. Thông thường cổng console được dùng nhiều nhất bởi vì các thông báo khi thiết bị khởi động chỉ hiển thị khi nối kết qua cổng console. Khi kết nối bằng cổng CONSOLE, các yêu cầu cấu hình sau phải tuân theo:
 - 1. Dùng cáp RJ-45-to-RJ-45 rollover
 - 2. Trên PC chương trình dùng để kết nối (Hyper Terminal trong Windows) có các thiết lập như sau:
 - Speed: 9600 b/s
 - Data bits: 8
 - Parity: None
 - Stop bit: 1
 - Flow control: None
- Thực hiện thao tác từ xa: Có một modem nối vào cổng auxiliary trên thiết bị từ phần mềm terminal từ xa. Khi ấy cổng auxiliary của thiết bị phải được cấu hình có thể “hiểu” (communication) với modem ngoài (external modem). Các cấu hình cần thiết:
 - — Cáp Straight-through serial
 - — 14.4-kb/s modem
 - — chương trình dùng trên PC để kết nối.

- Sau khi khởi động lần đầu, bạn có thể kết nối vào thiết bị bằng các cách:
 - Thiết lập phiên terminal dùng trình Telnet.
 - Cấu hình thiết bị qua kết nối ở lớp 7 bằng Trivial File Transfer Protocol (TFTP) server trên mạng để nhận tập tin cấu hình.
 - Chép tập tin cấu hình dùng các trình/ hệ thống quản trị mạng ví dụ :CiscoWorks.
- Ghi chú: Không phải tất cả các thiết bị đều có đủ các cổng như trên hình.

Nhiệm vụ giao tiếp với người dùng của Cisco IOS

- CLI được dùng để gõ các câu lệnh.
- Tương Tác vào các thiết bị có nhiều cách.
- Người dùng sẽ gõ hay “dán” các dòng lệnh vào màn hình console.
- Mode Command có nhiều kiểu dấu nhắc.
- Phím “**Enter**” xác định cho thiết bị chấp nhận lệnh và thi hành.
- Có hai mode EXEC quan trọng :
 - User mode
 - Privileged mode.

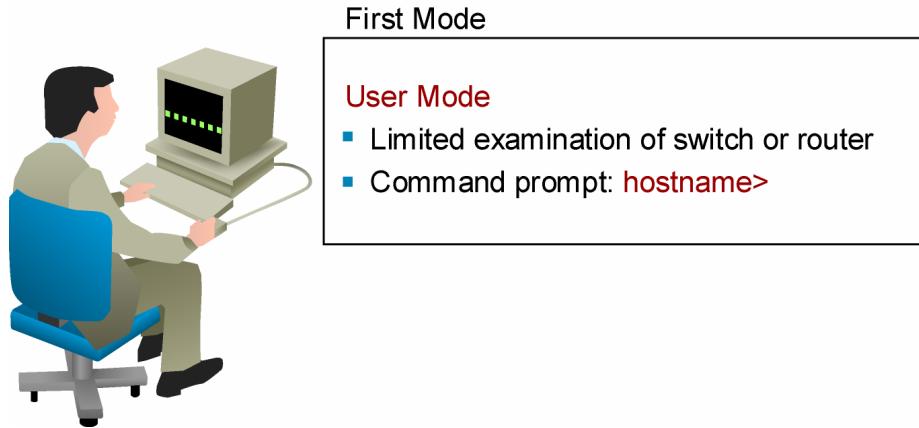


Module 12-7

- Để gõ câu lệnh vào CLI, người dùng sẽ gõ hay “dán” các dòng lệnh vào màn hình console. Mode Command có nhiều kiểu dấu nhắc. Phím “**Enter**” xác định cho thiết bị chấp nhận lệnh và thi hành.
- Phần mềm Cisco IOS dùng mô hình câu lệnh có cấu trúc. Mỗi mode hỗ trợ các cấu hình đặc biệt tương ứng cho việc vận hành của thiết bị.
- Như một dạng bảo mật, phần mềm Cisco IOS chia hai loại phiên làm việc (EXEC sessions) theo hai mức độ truy cập:
 - User EXEC: Cho phép người dùng truy cập một số giới hạn câu lệnh dạng theo dõi (monitoring command)
 - Privileged EXEC: Cho phép người dùng truy cập tất cả các câu lệnh dùng cấu hình và quản trị thiết bị. Việc truy cập có thể được bảo vệ cho người dùng hợp lệ qua hệ thống mật khẩu.

Phần mềm Cisco IOS : EXEC Mode (User)

Có hai mode EXEC quan trọng dùng để nhập câu lệnh:



Module 12-8

- Thủ tục dưới mô tả làm thế nào để kích hoạt mode EXEC trên thiết bị Cisco.
- Các bước:
 - 1. Đăng nhập vào thiết bị bằng username và password (nếu login có cấu hình).
 - Kết quả:
 - Một dấu nhắc xuất hiện cho biết đang ở user mode: dấu (>) ví dụ: hostname>
 - Gõ “exit” để đóng phiên làm việc ở user EXEC mode.
 - 2. Gõ lệnh “?” ở mức dấu nhắc user EXEC mode sẽ hiển thị tất cả các tham số trong mode này.
 - Kết quả:
 - Lệnh “?” trong privileged EXEC mode sẽ có nhiều tham số hơn so với user EXEC. Các tham số này được tham chiếu theo cách giúp đỡ theo ngữ cảnh (context-sensitive help).
- Mức user EXEC không chứa các lệnh điều khiển hoạt động của thiết bị. Ví dụ, mode user EXEC không cho phép chép hay đặt cấu hình cho thiết bị hay switch.

Phần mềm Cisco IOS : EXEC Mode (Privileged)

Second Mode (and Most Commonly Used)

Privileged (aka Enabled) Mode

- Detailed examination of switch or router
- Enables configuration and debugging
- Prerequisite for other configuration modes
- Command prompt: **hostname#**



327/124

Module 12-9

- Các câu lệnh nguy hiểm có liên quan đến cấu hình và quản trị yêu cầu bạn phải đang nằm ở mode privileged EXEC.
- Để thay đổi (chuyển) đến mode privileged EXEC từ mode user EXEC, gõ lệnh “enable” ở dấu nháy hostname>. Nếu có một “enable password” hay “enable secret password” được cấu hình trước thiết bị hay switch sẽ hỏi bạn mật khẩu.
- Khi mật khẩu hợp lệ cung cấp thiết bị chuyển dấu nháy thành hostname#, “#” thông báo cho người dùng đang ở trạng thái mức privileged EXEC.
- Để trở về mức user EXEC, gõ lệnh “disable” ở dấu nháy hostname#.
- Ghi chú:
 - Vì lý do bảo mật, Thiết bị Cisco sẽ không hiển thị mật khẩu được gõ vào. Tuy nhiên khi cấu hình thiết bị từ xa qua modem hay Telnet mật khẩu là “cleartext” (nghĩa là mật khẩu không mã hoá và được gửi qua mạng).
 - Secure Shell Protocol (SSH), chạy trên hầu hết các thiết bị Cisco, cho phép liên lạc một cách bảo mật trong môi trường không an toàn và cung cấp một cơ chế xác thực mạnh.

Tương tác với trình HELP trên câu lệnh Switch

Context-Sensitive Help	Console Error Messages
Provides a list of commands and the arguments associated with a specific command.	Identifies problems with any switch commands that are incorrectly entered so that they can be altered or corrected.
Command History Buffer	
Allows recall of long or complex commands or entries for re-entry, review, or correction.	

Module 12-10

- Hệ Điều hành Cisco IOS CLI trên thiết bị Cisco devices cung cấp các cách giúp đỡ sau:
 - Từ help: Gõ theo tuần tự “ký tự bạn muốn” và dấu “?” (không có khoảng trắng giữa ký tự và ?), thiết bị sẽ liệt kê danh sách câu lệnh bắt đầu bằng ký tự bạn cung cấp cho thiết bị. Ví dụ, gõ vào lệnh “sh?” rồi Enter, thiết bị sẽ liệt kê tất cả các câu lệnh bắt đầu bằng sh.
 - Gõ “?” trong mỗi lệnh hay từ khoá với khoảng trắng ở giữa, thiết bị sẽ liệt kê danh sách các tham số cho lệnh tương ứng. Ví dụ: gõ “show ?” bạn sẽ thấy danh sách các tham số có trong lệnh “show”.
- Ghi chú:
 - Thiết bị và switch Cisco có các lệnh tương tự nhau. Các mô hình giúp đỡ trên cũng giống nhau trừ khi có mô hình đặc biệt khác.
 - Hệ Điều hành Cisco cung cấp vài lệnh giúp cho việc gọi lại các lệnh cũ nằm trong bộ nhớ đệm (history buffer) nhanh chóng mà không phải gõ lại nguyên câu lệnh.
 - Các thông báo lỗi trên màn hình Console giúp nhận diện các lệnh không đúng hay chưa đầy đủ. Xem bảng.

Giúp đỡ theo ngữ cảnh

```
SwitchX# clok
Translating "CLOK"
% Unknown command or computer name, or unable to find computer address

SwitchX# cl?
clear    clock

SwitchX# clock
% Incomplete command.

SwitchX# clock ?
set      Set the time and date

SwitchX# clock set
% Incomplete command.

SwitchX# <Ctrl-P> clock set
hh:mm:ss Current Time
```

Diagram illustrating the three components of context-sensitive help:

- Symbolic Translation
- Command Prompting
- Last Command Recall

SOP-862

Module 12-11

- Giúp đỡ theo ngữ cảnh (context-sensitive help) giúp định dạng cú pháp cho một câu lệnh cụ thể được chính xác.
- Giúp đỡ theo ngữ cảnh cung cấp công cụ cho người dùng chỉ cần gõ vào một phần từ khóa của lệnh kết hợp với “?”; ví dụ “cl?” hệ điều hành sẽ giúp hoàn tất câu lệnh tương ứng bằng cách cung cấp thêm các tham số (nếu có khoảng trắng giữa từ khóa và “?”) hay liệt kê danh sách các lệnh liên quan (nếu kô có khoảng trắng giữa từ khóa và “?”)
- Ví dụ bạn gõ vào lệnh “clock” như trên màn hình slide.

Giúp đỡ theo ngữ cảnh (Cont.)

```
SwitchX# clock  
Translating "CLOCK"  
% Unknown command.  
SwitchX# clock set 19:56:00  
% Incomplete command.  
SwitchX# clear ?  
<1-31> Day of the month  
SwitchX# MONTH Month of the year  
% Incomplete command.  
SwitchX# clock set 19:56:00 04 8  
^  
% Invalid input detected at the '^' marker  
SwitchX# clock set 19:56:00 04 August  
% Incomplete command.  
SwitchX# clock set 19:56:00 04 August ?  
<1993-2035> Year
```

- Command Prompting
- Syntax Checking
- Command Prompting

Module 12-12

- Slide mô tả cách gõ lệnh “clock” để thiết lập ngày giờ hệ thống cho thiết bị

Mode soạn thảo Lệnh mở rộng

SwitchX>Shape the future of internetworking by creating unpreced

Shape the future of internetworking by creating
unprecedented value for customers, employees, and
partners.

Module 12-13

- Mặc dù mode soạn thảo mở rộng tự động kích hoạt bạn có thể ngừng (disable) nó. Có thể ngừng kích hoạt mode soạn thảo mở rộng khi bạn có một kích bản không cần tương tác.
- Dùng lệnh terminal editing EXEC để bật và terminal no editing EXEC để tắt mode soạn thảo lệnh mở rộng.
- Một trong những thuận lợi của mode soạn thảo Lệnh mở rộng là cung cấp cho bạn cơ chế trượt ngang (horizontal scrolling) cho các câu lệnh có chiều dài vượt quá khung màn hình (80 cột). Khi con trỏ lệnh đang lè phải dòng lệnh sẽ trược sang trái 10 khoảng trắng. Khi đó, 10 ký tự đầu tiên của dòng lệnh sẽ bị che khuất, bạn có thể trượt ngược lại các ký tự bị khuất này dễ dàng.

Mode soạn thảo Lệnh mở rộng (Cont.)

```
SwitchX>$ value for customers, employees, and partners.
```

	(Automatic scrolling of long lines)
Ctrl-A	Move to the beginning of the command line.
Ctrl-E	Move to the end of the command line.
Esc-B	Move back one word.
Esc-F	Move forward one word.
Ctrl-B	Move back one character.
Ctrl-F	Move forward one character.
Ctrl-D	Delete a single character.

Module 12-14

- Trong ví dụ trên, câu lệnh vượt quá khung màn hình. Dấu (\$) ở đầu dòng lệnh thể hiện điều này và đồng thời thông báo cho bạn rằng, bạn có thể trượt ngược lại nếu cần bằng cách dùng Ctrl-B hay phím mũi tên trái. Bấm Ctrl-A để chuyển đến đầu dòng lệnh.
- Xem bảng để biết các tổ hợp phím tương ứng.

Lệnh lấy lại câu lệnh cũ trong router

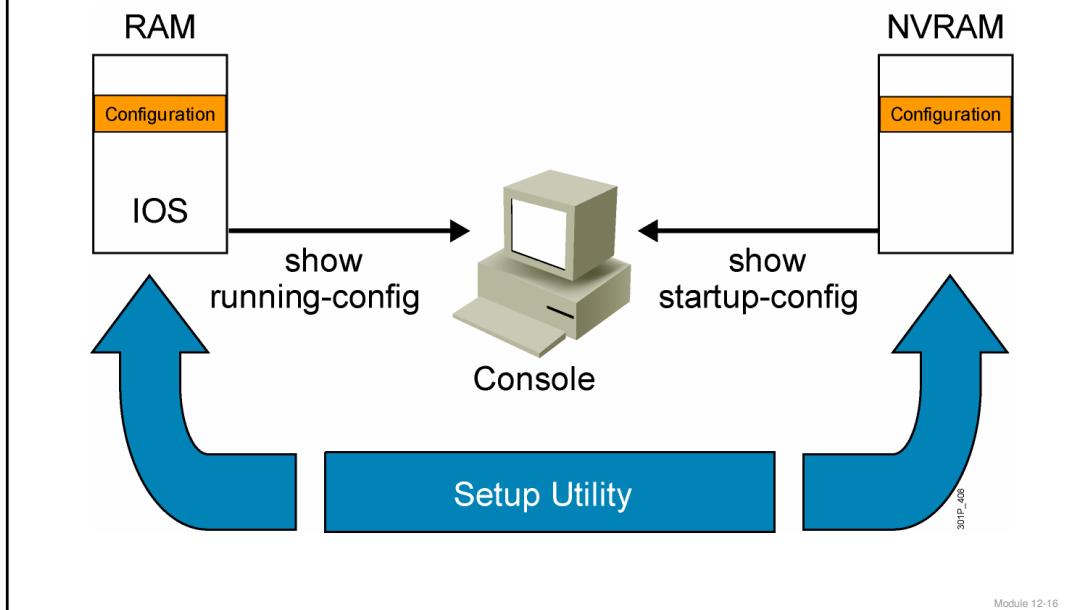
Ctrl-P or Up Arrow	Recalls last (previous) commands.
Ctrl-N or Down Arrow	Recalls more recent commands.
show history	Shows command buffer contents.
terminal history size lines	Sets session command buffer size.

Module 12-15

CCNP 2/49

- Với cơ chế này, bạn có thể:
 - Xem nội dung trong bộ nhớ đệm lưu các câu lệnh cũ
 - Thiết lập kích thước bộ nhớ đệm.
 - Gọi lại các câu lệnh cũ đã lưu trong bộ nhớ đệm. Có một vùng nhớ đệm cho mode EXEC và một phần nhớ khác cho mode cấu hình.
- Mặc định, vùng nhớ này được kích hoạt tự động và có thể chứa 10 câu lệnh cuối. Thay đổi số này hệ thống có thể lưu thêm các câu lệnh trong quá trình cấu hình.
- Để gọi lại các lệnh cũ dùng Ctrl-P hay phím mũi tên lên (Up Arrow key). Thực hiện nhiều lần, bạn sẽ lấy lại được các câu lệnh thi hành thành công trước đây.
- Gõ Ctrl-N hay mũi tên xuống để lấy lại các câu lệnh thành công đã thực hiện gần hơn.
- Trong hầu hết các PC luôn có cơ chế “Copy” và “Paste” các thông tin mà bạn cần.

Xem Cấu hình hiện hành



Module 12-16

- Một router Cisco có 3 kiểu vùng nhớ:
 - RAM: Chứa bảng định tuyến, bộ nhớ chuyển mạch nhanh (fast switching cache), cấu hình đang hoạt động ...
 - NVRAM: Dùng lưu vĩnh viễn (không bị mất khi tắt nguồn) cấu hình khởi động (startup configuration)
 - Flash: Cung cấp bộ nhớ vĩnh viễn lưu trữ hệ điều hành Cisco IOS, Cấu hình lưu (backup configuration), và những tập tin khác
- Câu lệnh “show startup-config” xem cấu hình trong NVRAM.
- Câu lệnh “ show running-config” xem cấu hình trong RAM.

Lệnh show running-config và show startup-config

In RAM

```
SwitchX#show running-config
Building configuration...??
Current configuration:?
!?
version 12.0
!
-- More --
```

In NVRAM

```
SwitchX#show startup-config
Using 1359 out of 32762 bytes
!
version 12.0
!
-- More --
```

Hiển thị cấu hình hiện thời và đã lưu trữ

Module 12-17

Tóm tắt

- HĐH Cisco IOS là một phần mềm nhúng cung cấp việc quản lý và điều khiển thiết bị Cisco. Nhiệm vụ của nó bao gồm chọn giao thức mạng, thiết lập kết nối, bảo mật, khả năng mở rộng và tính đáng tin cậy.
- Một switch hay thiết bị chứa IOS có thể được cấu hình tại chỗ qua cổng Console hay từ xa qua modem + cổng AUX.
- CLI được dùng để giúp quản trị mạng theo dõi, cấu hình các thiết bị Cisco khác nhau. CLI cũng cung cấp các trình giúp đỡ đa dạng nhằm giúp quản trị mạng kiểm tra tính đúng đắn của câu lệnh và thực hiện nó.

Module 12-18

Tóm tắt (tiếp theo.)

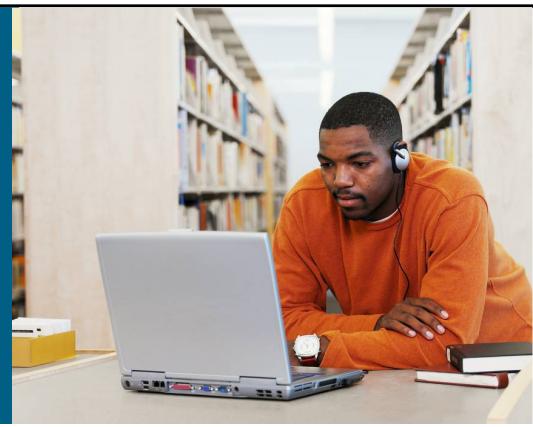
- CLI hỗ trợ hai mode thi hành (EXEC mode): user và privileged. Mode privileged EXEC cung cấp nhiều chức năng hơn mode user EXEC.
- Cisco IOS dùng các phần hỗ trợ, giúp đỡ theo ngữ cảnh và mở rộng.
- Cisco IOS cung cấp công cụ “history” (bộ nhớ lưu các lệnh thành công cũ). Nó cho phép quản trị mạng gọi lại các câu lệnh cũ nhanh chóng.

Module 12-19



Module 12-20

Bài 13: Khởi động với Switch



Ethernet LANs

Module 13-1

- **Tổng quan:**

- Khi bật nguồn, một Cisco Catalyst switch sẽ khởi động, khi khởi động hoàn tất bạn có thể thiết lập cấu hình cho switch. Nhận thức được quá trình khởi động (bình thường, kô có lỗi) của switch là bước đầu để triển khai hệ thống switch trong mạng.

- **Mục tiêu:** Học xong bài này các bạn có thể:

- Khởi động với một Cisco IOS switch
- Nhận dạng các đèn trên switch phản ánh điều kiện làm việc của switch
- Mô tả các kết quả hiển thị của quá trình khởi động trên switch
- Đăng nhập vào Cisco IOS switch
- Cấu hình switch từ dòng lệnh
- Kiểm định hoạt động ban đầu của switch
- Dùng các lệnh show tương ứng để quản lý bảng MAC

Khởi động Catalyst Switch

- Thủ tục khởi động hệ thống HĐH của switch.
- hệ thống khởi động dùng các tham số cấu hình mặc định.

1. Before you start the switch, verify the cabling and console connection.
2. Attach the power cable plug to the switch power supply socket.
3. Observe the boot sequence:
 - LEDs on the switch chassis
 - Cisco IOS software output text



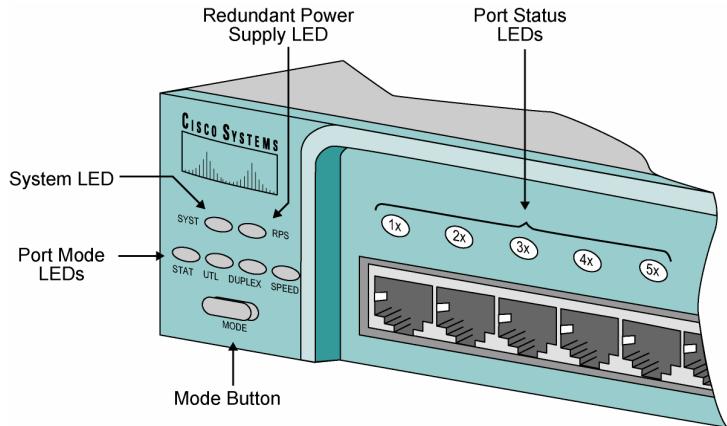
Module 13-2

• Thủ tục khởi động hệ thống HĐH của switch như sau:

- Bước 1: Trước khi khởi động kiểm tra: Tất cả các cáp kết nối là an toàn. Thiết bị cấu hình (Your terminal) đã kết nối vào cổng console. Ứng dụng console terminal như HyperTerminal đã được chọn.
- Bước 2: Nối dây nguồn. Switch sẽ khởi động. Thường không có công tắc nguồn trên switch, Kê cá dòng Cisco Catalyst 2960.
- Bước 3: Theo dõi thứ tự khởi động như sau: Nhìn đèn LED trên switch. Theo dõi kết quả hiển thị trên màn hình console.

• Ghi chú: Khóa học mô tả chủ yếu các hoạt động trên dòng Switch Catalyst 2960. Các dòng switch khác có thể thay đổi.

Đo lường bằng đèn LED trên Switch Catalyst 2960



Module 13-3

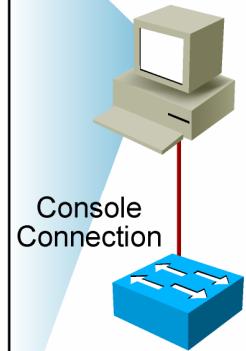
- Trên switch Catalyst 2960-12 và 2960-24 được mô tả như dưới:
 - Đèn System :
 - Tắt : Switch không được cấp nguồn.
 - Xanh: Switch được cấp nguồn và hoạt động.
 - Vàng cam (Amber): Hệ thống bị lỗi. Một hay nhiều lỗi xuất hiện trong trình power-on self-test (POST).
 - Đèn RPS (Redundant power supply)
 - Tắt : Module RPS không cài đặt
 - Xanh : Module RPS đang hoạt động.
 - Chớp Xanh (Flashing green): RPS đã kết nối nhưng không hoạt động vì đang cấp nguồn cho thiết bị khác.
 - Vàng cam (Amber): RPS đã cài đặt nhưng không hoạt động.
 - Chớp Vàng cam (Flashing Amber): Nguồn nội bộ hỏng và RPS đang cung cấp nguồn cho switch.
 - Đèn “port Mode” hiển thị:
 - Đèn STAT trên mỗi cổng:(STAT LED on)
 - Tắt: Không có link.
 - Xanh: Link có, không kích hoạt.

- Chớp Xanh: ó link + có dữ liệu truyền..
- Xen kẽ Xanh và Vàng cam (Alternating green and amber): Link có lỗi. Một số frames có thể ảnh hưởng đến kết nối. Số lần đụng độ tăng cao, lỗi trong frame (cyclic redundancy check, alignment, và jabber) được theo dõi xem như thước đo lỗi link.
- Vàng cam (Amber): Cổng kẽ chuyển tiếp bởi vì cổng kẽ được kích hoạt vì lý do quản trị (ví dụ: vi phạm địa chỉ, bị khoá do Spanning Tree Protocol (STP)).
- Đèn theo dõi tải (Bandwidth utilization (UTL LED on)):
 - Xanh : Hiện trạng đang dùng tải so với màu vàng cam nền theo thang đo logarithm.
 - Vàng cam: số tải cực đại đang dùng bên (backplane) vì switch đang được dùng.
 - Xanh và Vàng cam (Green and amber): tùy theo model ví dụ:
 - Catalyst 2960-12, 2960-24, 2960C-24, và 2960T-24 switch: Nếu tắt cả màu xanh, switch đang dùng từ 50% bandwidth trở lên. Nếu các đèn LED cuối bên phải tắt, Switch dùng từ 25 đến 50% bandwidth.... Nếu chỉ có 1 đèn LED bên trái đầu tiên xanh thì switch chỉ dùng ít hơn 0.0488 % bandwidth.
 -
- Đèn Full-duplex (FDUP LED on)
 - Xanh: Cổng được cấu hình full-duplex.
 - Tắt: Cổng được cấu hình half-duplex.

Kết quả khởi động hiển thị trên Catalyst 2960 Switch

```
Base ethernet MAC Address: 00:19:30:38:bd:00
Xmodem file system is available.
The password-recovery mechanism is enabled.
Initializing Flash...
flashfs[0]: 598 files, 19 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 32514048
flashfs[0]: Bytes used: 8210432
flashfs[0]: Bytes available: 24303616
flashfs[0]: flashfs fsck took 9 seconds.
...done Initializing Flash.
Boot Sector Filesystem (bs) installed, fsid: 3
done.
Loading "flash:c2960-lanbasek9-mz.122-25.SEE2/c2960-lanbasek9
-mz.122-25.SEE2.bin"...0000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
File "flash:c2960-lanbasek9-mz.122-25.SEE2/c2960-lanbasek9-mz.
122-25.SEE2.bin" uncompressed and installed, entry point: 0x3000
executing...

!Rest of startup text omitted
```



Module 13-5

- Sau khi trình POST hoàn tất thành công, Catalyst 2960 switch xuất hiện nhắc nhở đang tiến vào trình khởi động cấu hình cho switch. Một trình khởi tạo khởi động tự động (automatic setup program) được dùng để gán switch IP, tên host và cluster, mật khẩu, và tạo cấu hình mặc định (default configuration) để switch tiếp tục hoạt động. Sau đó, CLI có thể dùng để thay đổi cấu hình. Thực hiện trình setup (setup program), truy cập vào switch từ máy tính dùng terminal (đá kết nối vào cổng console của switch).

Kết quả khởi động trên Catalyst 2960 Switch bằng trình Setup

```
--- System Configuration Dialog ---  
Would you like to enter the initial configuration dialog? [yes/no]:  
y  
At any point you may enter a question mark '?' for help.  
Use ctrl-c to abort configuration dialog at any prompt.  
Default settings are in square brackets '['].  
  
Basic management setup configures only enough connectivity  
for management of the system, extended setup will ask you  
to configure each interface on the system  
Would you like to enter basic management setup? [yes/no]: no  
First, would you like to see the current interface summary? [yes]:  
no  
Configuring global parameters:  
..  
..text omitted ..  
..  
[0] Go to the IOS command prompt without saving this config.  
[1] Return back to the setup without saving this config.  
[2] Save this configuration to nvram and exit.  
  
Enter your selection [2]:  
Building configuration...  
[OK]  
Use the enabled mode 'configure' command to modify this  
configuration.
```

Module 13-6

- Sau khi các yêu cầu được nhập vào, trình “setup” sẽ hiển thị :

```
hostname SwitchX  
enable secret 5 $1$oV63$8z7cBuVeTibpCn1Rf5uI01  
enable password enable_password  
line vty 0 15  
password vty_password  
no snmp-server  
!  
!  
interface Vlan1  
ip address 10.1.1.140 255.255.255.0  
!  
interface FastEthernet0/1  
..text omitted..  
interface FastEthernet0/24  
!  
end  
....
```

[0] Go to the IOS command prompt without saving this config.

[1] Return back to the setup without saving this config.

[2] Save this configuration to nvram and exit.

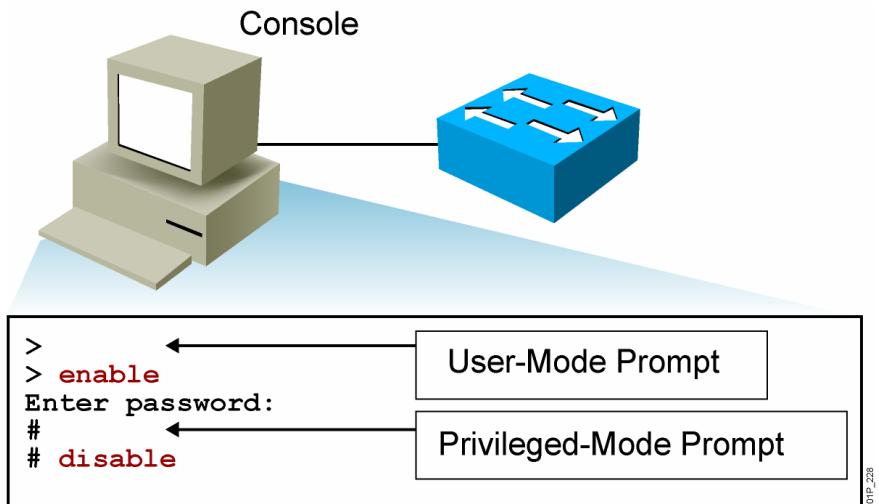
Enter your selection [2]:2

Building configuration...

[OK]

- Dùng “enabled mode” bằng lệnh 'configure' để thay đổi nội dung cấu hình.
- Nhập “2” để hoàn tất phần cấu hình khởi động.

Đăng nhập vào switch và vào mode Privileged EXEC



Module 13-8

- Vì lý do bảo mật. Phần EXEC có 2 mức:
 - User mode và Privileged mode
- Mode này cũng gọi là “enable mode”.

Cấu hình Switch



Configuration modes:

- Global configuration mode
 - `SwitchX#configure terminal`
 - `SwitchX(config)#`
- Interface configuration mode
 - `SwitchX(config)#interface fa0/1`
 - `SwitchX(config-if)#`

Module 13-9

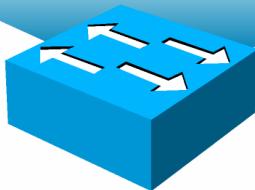
- Cấu hình các tham số ở mode toàn cục (global mode): host name và Địa chỉ IP của switch Cấu hình chi tiết theo cổng (port hay interface), dùng mode “interface configuration”.
- Ghi chú: Hầu hết các mode chi tiết sẽ làn lượt cung cấp trong khóa học.

Configuring Switch Identification

Switch Name

```
(config) #hostname SwitchX  
SwitchX(config) #
```

301P_231



Thiết lập xác nhận nội bộ (local identity) cho switch

Module 13-10

- 1 trong những công việc đầu tiên là cấu hình tên cho switch. Tên phải là duy nhất.

Cấu hình địa chỉ IP cho Switch

```
SwitchX(config)#interface vlan 1  
SwitchX(config-if)#ip address {ip address} {mask}
```

Example:

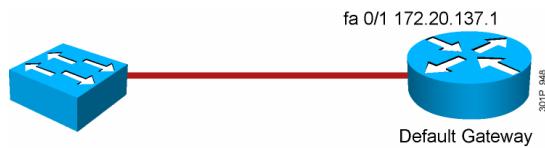
```
SwitchX(config)#interface vlan 1  
SwitchX(config-if)#ip address 10.5.5.11 255.255.255.0  
SwitchX(config-if)#no shutdown
```

Ghi chú: Nếu cần, phải thêm lệnh **no shutdown** để cho interface được hoạt động.

Module 13-11

- IP của switch là địa chỉ dùng quản trị ở Layer 3 cho một switch ở Layer 2. Địa chỉ này thường dùng quản trị từ xa. Interface quản trị nằm trong VLAN 1 do đó IP được gán vào VLAN 1.
- Để cấu hình IP, phải vào mode interface và đứng ở interface VLAN 1. phải thêm lệnh **no shutdown** để cho interface được hoạt động

Cấu hình Default Gateway cho Switch



```
SwitchX (config) #ip default-gateway {ip address}
```

Example:

```
SwitchX (config) #ip default-gateway 172.20.137.1
```

Module 13-12

- Dùng lệnh “**ip default-gateway**” để nhập địa chỉ IP của cổng router kết nối trực tiếp vào switch. Default gateway nhận các gói IP với địa chỉ đích chưa xác định từ hoạt động của switch (switch EXEC process).
- Khi “default gateway” được cấu hình, switch có thể liên kết với network bên ngoài.

Lưu cấu hình

```
SwitchX
SwitchX copy running-config startup-config
Destination filename [startup-config]?
Building configuration...

SwitchX
```

Chép cấu hình hiện hành vào NVRAM

Module 13-13

- Sau khi cấu hình xong phải lưu cấu hình hiện hành vào NVRAM : “**copy running-config startup-config**”
- Nếu cấu hình không được lưu, trường hợp khởi động lại tất cả các cấu hình đang có sẽ mất.

Xem tình trạng khởi tạo khởi động trên switch

SwitchX#show version

- Xem cấu hình phần cứng hệ thống, phiên bản HĐH, tên và nguồn tập tin cấu hình và tập tin khởi động (IOS - boot image)

SwitchX#show running-config

- Xem cấu hình hiện hành đang hoạt động

SwitchX#show interfaces

- Xem thống kê tình trạng trên tất cả các cổng.

Module 13-14

- Tình trạng Switch:

- **show version:** Xem cấu hình phần cứng hệ thống, phiên bản HĐH, tên và nguồn tập tin cấu hình và tập tin khởi động (IOS - boot image) .
- **show running-config:** Xem cấu hình hiện hành đang hoạt động.Lệnh này dùng ở privileged EXEC mode. Địa chỉ IP, subnet mask, và default-gateway đang chọn sẽ được hiển thị.
- **show interfaces:** Xem thống kê tình trạng trên tất cả các cổng switch.
- Cả hai loại cổng switch trunks và switch line được xem như interface. Kết quả hiển thị có thể thay đổi theo tình huống. Thường phải chỉ định thêm chính xác cổng cần quan tâm để giới hạn thông tin hiển thị ra theo nhu cầu ví dụ chỉ xem cổng e0/1.
- Tùy theo loại thiết bị, lệnh đầy đủ thường là: **SwitchX#show interfaces module/slot/number**

Lệnh show version

```
Switch#show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(25)SEE2, RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 28-Jul-06 11:57 by yenanh
Image text-base: 0x00003000, data-base: 0x00BB7944

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)SEE1, RELEASE SOFTWARE (fc1)

Switch uptime is 24 minutes

System returned to ROM by power-on
System image file is "flash:c2960-lanbasek9-mz.122-25.SEE2/c2960-lanbasek9-mz.122-
25.SEE2.bin"

cisco WS-C2960-24TT-L (PowerPC405) processor (revision B0) with 61440K/4088K bytes of
memory.

Processor board ID FOC1052W3XC
Last reset from power-on
1 Virtual Ethernet interface
24 FastEthernet interfaces
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

! Text omitted

Switch#
```

Module 13-15

Lệnh show interfaces

```
SwitchX#show interfaces FastEthernet0/2
FastEthernet0/2 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0008.a445.ce82 (bia 0008.a445.ce82)
    MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
      reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA, loopback not set
    Keepalive set (10 sec)
    Half-duplex, 10Mb/s
      input flow-control is unsupported output flow-control is unsupported
    ARP type: ARPA, ARP Timeout 04:00:00
    Last input 4w6d, output 00:00:01, output hang never
    Last clearing of "show interface" counters never
    Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
    Queueing strategy: fifo
    Output queue: 0/40 (size/max)
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
      182979 packets input, 16802150 bytes, 0 no buffer
      Received 49954 broadcasts (0 multicast)
      0 runts, 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 8 ignored
      0 watchdog, 20115 multicast, 0 pause input
      0 input packets with dribble condition detected
      3747473 packets output, 353656347 bytes, 0 underruns
--More--
```

Module 13-16

Quản lý bảng địa chỉ MAC

Catalyst 2960 Series

```
SwitchX#show mac-address-table
      Mac Address Table
-----
Vlan   Mac Address        Type      Ports
----  -----
All    0008.a445.9b40    STATIC    CPU
All    0100.0ccc.cccc    STATIC    CPU
All    0100.0ccc.ccccd   STATIC    CPU
All    0100.0cdd.dddd    STATIC    CPU
1      0008.e3e8.0440    DYNAMIC   Fa0/2
Total Mac Addresses for this criterion: 5
SwitchX#
```

Module 13-17

- Switches dùng bảng MAC để chuyển tiếp dữ liệu giữa các cổng. Bảng MAC chứa địa chỉ động, vĩnh viễn, và tĩnh (dynamic, permanent, and static).
- Địa chỉ động là địa chỉ nguồn switch tự học từ các frame nhận vào ở mỗi cổng, switch lưu trữ địa chỉ này tương ứng với cổng nhận. Bản tin sẽ bị hủy khi không được làm tươi hay hết hạn. Khi một trạm thêm hay bỏ ra khỏi mạng, switch tự động thêm vào một bản tin (new entry) và hủy bỏ các entry hết hạn.
- Quản trị mạng có thể gán vĩnh viễn địa chỉ MAC (permanent address) vào một cổng switch, địa chỉ này không bị hủy.
- Kích thước bảng MAC tùy thuộc vào loại switch. Catalyst 2960 có thể lưu 8192 MAC. Khi bảng MAC bị tràn, switch sẽ không biết địa chỉ nhận ở đâu (thuộc cổng nào) dữ liệu sẽ bị làm tràn ra tất cả các cổng (trừ cổng nhận).

Tóm tắt

- Khởi động một Cisco IOS switch cần kiểm tra các cài đặt vật lý, nguồn, và xem các kết quả hiển thị trên màn hình console.
- Cisco IOS switch có vài đèn LED thể hiện tình trạng . Thường có màu xanh. Nếu có bất thường sẽ chuyển sang vàng cam.
- Trình Cisco Catalyst POST được thực hiện khi gắn nguồn vào switch.
- Trong trình khởi động quá trình khởi tạo (initial startup),nếu trình POST được phát hiện là có lỗi (failure), nó sẽ thông báo trên màn hình console. Nếu POST hoàn tất thành công switch có thể được cấu hình.

Module 13-18

Tóm tắt (tiếp theo.)

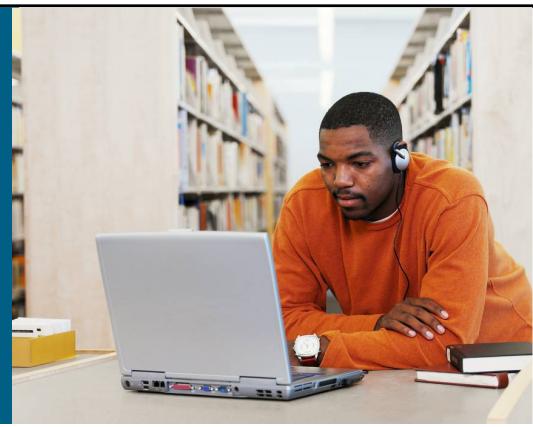
- Khi khởi động, Switch bắt đầu bằng mode user EXEC. Để vào các mode khác, có thể phải nhập mật khẩu.
- Catalyst IOS switch có thể được cấu hình ở mode global và các mode khác tương tự như Router.
- Cấu hình Cisco IOS switch từ dòng lệnh ở mode toàn cục (global): tên và địa chỉ IP.
- Sau khi đăng nhập vào Catalyst switch, tình trạng HĐH và phần cứng của switch có thể kiểm tra bằng các lệnh: **show version**, **show running-config**, và **show interfaces**.

Module 13-19



Module 13-20

Bài 14: Hiểu về bảo mật thiết bị Switch



Ethernet LANs

Module 14-1

Common Threats to Physical Installations

- Hardware threats
- Environmental threats
- Electrical threats
- Maintenance threats



Module 14-2

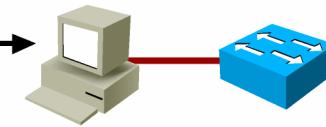
Bốn loại cài đặt không an toàn hoặc những mối đe dọa ở mức truy cập vật lý:

- Đe dọa về phần cứng: nguy hiểm đến switch hay phần cứng switch
- Đe dọa về môi trường: nhiệt độ quá nóng hoặc quá lạnh, hay quá ẩm ướt hoặc quá khô
- Đe dọa về điện: cung cấp hiệu điện thế không hiệu quả, nhiễu, mất nguồn
- Đe dọa về sự bảo quản: dùng tay cầm những thành phần điện quan trọng (phóng điện), cáp không tốt, đánh nhau không tốt, ..

Configuring a Switch Password

Console Password

```
SwitchX(config)#line console 0  
SwitchX(config-line)#login  
SwitchX(config-line)#password cisco
```



Virtual Terminal Password

```
SwitchX(config)#line vty 0 4  
SwitchX(config-line)#login  
SwitchX(config-line)#password sanjose
```



Enable Password

```
SwitchX(config)#enable password cisco
```



Secret Password

```
SwitchX(config)#enable secret sanfran
```



Service Password-Encryption Commands

```
SwitchX(config)#service password-encryption  
SwitchX(config)#no service password-encryption
```

301P-208

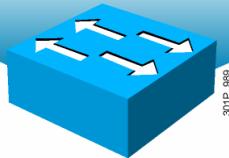
Module 14-3

- Bạn có thể bảo vệ switch bằng cách đặt password để giới hạn truy cập. Sử dụng password và gán quyền là cách điều khiển truy cập trong mạng đơn giản nhất. Password có thể được cấu hình trên từng line, như console, và privileged EXEC mode. Password phân biệt chữ hoa và thường.
- Mỗi cổng telnet trên switch được xem như là một virtual type terminal (vty). Trên switch có tối đa 5 port telnet, cho phép 5 giao dịch telnet đồng thời. Trên switch cổng vty được đánh số từ 0 đến 4
- Sử dụng lệnh **line console 0**, sau đó dùng lệnh **con password** và **login** để cho phép đăng nhập và thiết lập password khi đăng nhập vào cổng console hoặc cổng vty. Mặc định, cổng console và vty không cho phép đăng nhập.
- Sử dụng lệnh **line vty 0 4**, sau đó dùng lệnh **con password** và **login** để cho phép đăng nhập và thiết lập password khi đăng nhập khi thực hiện các giao dịch telnet đến switch.
- Lệnh **login local** có thể được sử dụng để kiểm tra password của user được tạo từ lệnh **username** trong global configuration. Lệnh **username** thiết lập chứng thực user với password được mã hóa
- Lệnh **enable password** trong global configuration mode giới hạn truy cập đến privileged EXEC mode. Bạn có thể cấu hình mã hóa enable password, được gọi là enable secret password, bằng cách dùng lệnh **enable secret** tại dấu nhắc global configuration. Nếu enable secret password được cấu hình, nó sẽ thay thế enable password.
- Những password được hiển thị hay cấu hình sau khi bạn cấu hình lệnh **service password-encryption** sẽ được mã hóa
- Để xóa một lệnh, thêm **no** trước mỗi lệnh. Ví dụ, **no service password-encryption** sẽ bỏ lệnh mã hóa password

Configuring the Login Banner

- Defines and enables a customized banner to be displayed before the username and password login prompts.

```
SwitchX# banner login " Access for authorized users only. Please enter your  
username and password. "
```



301P_989

Module 14-4

- Bạn có hiển thị một thông điệp trước khi user được nhắc nhập vào username và password, bằng cách dùng lệnh **banner login** tại global configuration mode. Để bỏ thông điệp thêm **no** trước lệnh này.
- Khi lệnh **banner login** được cấu hình, sau lệnh với một hay nhiều khoảng trắng và một ký tự định ranh giới bất kỳ. Trong ví dụ, ký tự định ranh giới là dấu (""). Sau khi thông điệp được gõ vào, ngắt thông điệp với cùng ký tự định ranh giới

Telnet vs. SSH Access

- Telnet
 - Most common access method
 - Insecure
- SSH-encrypted

```
!- The username command create the username and password for the SSH session
Username cisco password cisco

ip domain-name mydomain.com

crypto key generate rsa

ip ssh version 2

line vty 0 4
  login local
  transport input ssh
```



Module 14-5

- Telnet là một cách truy cập thiết bị mạng thường dùng nhất. Tuy nhiên, telnet không an toàn và vì thế không phải là một chọn lựa. Secure Shell Protocol (SSH) là một tiện ích an toàn thay thế telnet. Giao tiếp giữa client và server được mã hóa trong cả SSH1 và SSH2. nên sử dụng SSH2 vì nó sử dụng thuật toán mã hóa an toàn hơn.
- Đầu tiên kiểm tra chứng thực không dùng SSH để chắc chắn sự chứng thực trên switch đã được. Sự chứng thực có thể với một username và password hoặc với một chứng thực, sự cho phép, và AAA Server chạy TACACS+ hoặc RADIUS. Ví dụ sau chỉ ra chứng thực cục bộ, cho phép telnet với username và password cisco
- Để kiểm tra chứng thực với SSH, bạn phải cấu hình thêm enable SSH. Sau đó test SSH từ PC hoặc máy UNIX
- Nếu bạn muốn ngăn chặn những kết nối không phải SSH, cấu hình lệnh **transport input ssh** trong các line. Ví dụ

```
line vty 0 4
  transport input ssh
```

- Kiểm tra bằng telnet. Nếu không telnet được đến switch thì đã hoàn thành.

Configuring Port Security

Cisco Catalyst 2960 Series

```
SwitchX(config-if)#switchport port-security [ mac-address  
mac-address | mac-address sticky [mac-address] | maximum  
value | violation {restrict | shutdown}]
```

```
SwitchX(config)#interface fa0/5  
SwitchX(config-if)#switchport mode access  
SwitchX(config-if)#switchport port-security  
SwitchX(config-if)#switchport port-security maximum 1  
SwitchX(config-if)#switchport port-security mac-address sticky  
SwitchX(config-if)#switchport port-security violation shutdown
```

Module 14-6

- Bạn có thể dùng tính năng port security để giới hạn truy cập đến một interface bằng cách giới hạn hay nhận diện địa chỉ MAC của các máy được phép truy cập đến port. Khi bạn gán một địa chỉ MAC đến một port, port này sẽ không chuyển packet nếu địa chỉ MAC khác địa chỉ đã gán.
- Với Cisco Catalyst 2960 Series, sử dụng lệnh **switchport port-security** trong interface mode không có các tham số phía sau để cho phép port security trên một interface. Sử dụng lệnh **switchport port-security** với các tham số để cấu hình địa chỉ MAC, số địa chỉ MAC tối đa, hoặc violation mode. Thêm **no** trước lệnh này để bỏ port security
- Bạn có thể gán những địa chỉ cho phép vào bảng địa chỉ sau khi bạn chỉ ra số địa chỉ cho phép tối đa trên một port theo những cách sau:
 - Cấu hình bằng tay tất cả các địa chỉ (**switchport port-security mac-address 0080.eeee.eeee**)
 - Cho phép port tự động học các địa chỉ (**switchport port-security mac-address sticky**)
 - Cấu hình một số địa chỉ MAC và cho phép học động một số địa chỉ
- Bạn có thể cấu hình một interface sẽ chuyển tất cả địa chỉ MAC đã được học tự động thành địa chỉ sticky secure MAC và gán chúng vào running-config bằng cách cho phép sticky. Để đạt được yêu cầu này bạn dùng lệnh **switchport port-security mac-address sticky** trong interface mode. Khi bạn cấu hình lệnh này, interface sẽ chuyển tất cả địa chỉ MAC đã học tự động, bao gồm cả những địa chỉ đã học trước khi cấu hình lệnh này, thành địa chỉ sticky secure MAC.

- Nếu bạn lưu những địa chỉ sticky secure MAC vào startup-config, khi switch khởi động lại interface không cần phải học lại những địa chỉ này. Ngược lại, những địa chỉ MAC này sẽ bị mất khi switch khởi động lại. Nếu sticky bị hủy thì những địa chỉ sticky secure MAC sẽ được chuyển thành địa chỉ động và bị xóa khỏi running-config. Một port có thể gán từ 1 đến 132 địa chỉ MAC. Tổng số địa chỉ trên switch là 1024
- Trường hợp violation như sau:
 - Số địa chỉ MAC tối đa được gán vào bảng địa chỉ, và một máy có địa chỉ MAC không tồn tại trong bảng địa chỉ có gắng truy cập đến interface
 - Một địa chỉ được học hay cấu hình trên một interface sẽ được thấy trên interface khác nếu các interface cùng VLAN

Verifying Port Security on the Catalyst 2960 Series

```
SwitchX#show port-security [interface interface-id] [address] [ |  
{begin | exclude | include} expression]
```

```
SwitchX#show port-security interface fastethernet 0/5  
Port Security : Enabled  
Port Status : Secure-up  
Violation Mode : Shutdown  
Aging Time : 20 mins  
Aging Type : Absolute  
SecureStatic Address Aging : Disabled  
Maximum MAC Addresses : 1  
Total MAC Addresses : 1  
Configured MAC Addresses : 0  
Sticky MAC Addresses : 0  
Last Source Address : 0000.0000.0000  
Security Violation Count : 0
```

Module 14-8

- Trên Catalyst 2960, dùng lệnh **show port-security interface** trong privileged EXEC mode để xem những cấu hình port security của interface.
- Một địa chỉ vi phạm xảy ra khi một port đã cấu hình secure nhận một địa chỉ MAC nguồn mà nó không được gán đến port hay vượt quá địa chỉ tối đa của port (**switchport port-security maximum**)
- Bảng sau đây liệt kê những biến trong lệnh **show port-security**
- Interface *interface-id*: (tùy chọn) hiển thị những cấu hình port-security của interface chỉ định
- Address: (tùy chọn) hiển thị tất cả địa chỉ trên tất cả các port
- Begin: (tùy chọn) hiển thị bắt đầu từ dòng đầu tiên phù hợp với biểu thức chỉ định
- Exclude: (tùy chọn) chỉ hiển thị những dòng mà loại trừ những dòng phù hợp với biểu thức chỉ định
- Include: (tùy chọn) chỉ hiển thị những dòng phù hợp với biểu thức chỉ định
- Expression: biểu thức sẽ được tham chiếu khi xuất kết quả theo yêu cầu.

Verifying Port Security on the Catalyst 2960 Series (Cont.)

```
SwitchX#sh port-security address
Secure Mac Address Table
-----
Vlan   Mac Address      Type        Ports    Remaining Age
                                         (mins)
-----
1      0008.dddd.eeee  SecureConfigured  Fa0/5    -
-----
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

```
SwitchX#sh port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                                         (Count)       (Count)       (Count)
-----
Fa0/5      1              1             0            Shutdown
-----
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

Module 14-9

- Sử dụng lệnh **show port-security address** để hiển thị địa chỉ MAC trên tất cả các port. Sử dụng lệnh **show port-security** sẽ hiển thị những cấu hình port-security của switch.

Securing Unused Ports

- Unsecured ports can create a security hole.
- A switch plugged into an unused port will be added to the network.
- Secure unused ports by disabling interfaces (ports).

Module 14-10

- Ở nhà, một cánh cửa không có khóa sẽ là mối nguy hiểm. Điều này cũng đúng cho port trên switch không được sử dụng. Một hacker có thể gắn một switch vào một port không được sử dụng và trở thành một phần của mạng. Vì thế, một port không được sử dụng có thể tạo ra một lỗ hổng bảo mật. Để ngăn chặn điều này, bạn nên bảo vệ port không được sử dụng bằng cách khóa những port này

Disabling an Interface (Port)

```
SwitchX(config-int) #
```

```
shutdown
```

- To disable an interface, use the **shutdown** command in interface configuration mode.
- To restart a disabled interface, use the **no** form of this command.

Module 14-11

- Để khóa một interface(port), sử dụng lệnh **shutdown** trong interface mode. Để interface hoạt động trở lại dùng lệnh **no shutdown**

Tóm tắt

- Mức độ bảo mật đầu tiên là tầng vật lý.
- Mật khẩu có thể được dùng để giới hạn sự truy cập của người dùng.
- Logging banner có thể được dùng để hiển thị một thông báo đến người dùng khi họ truy cập thiết bị
- Nghi thức telnet gửi dữ liệu dưới dạng thông điệp rõ ràng, SSH mã hóa dữ liệu khi được gửi đi.
- Tính năng Port security có thể dùng để giới hạn số lượng địa chỉ MAC trên mỗi cổng.
- Những cổng không sử dụng nên vô hiệu hóa.

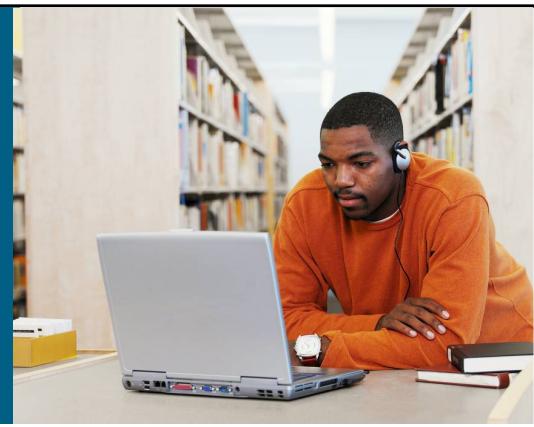
Module 14-12

- Tầng bảo mật đầu tiên là tầng vật lý
- Cấu hình password để giới hạn truy cập của người dùng
- Login banner được sử dụng để hiển thị một thông điệp trước khi người dùng được nhắc nhập vào username.
- Những thông tin trong giao dịch telnet không được mã hóa; SSH thì mã hóa
- Port security có thể được sử dụng để giới hạn địa chỉ MAC của 1 port
- Những port không được sử dụng nên khóa.



Module 14-13

Bài 15: Tối ưu hóa những tiện ích của Switch

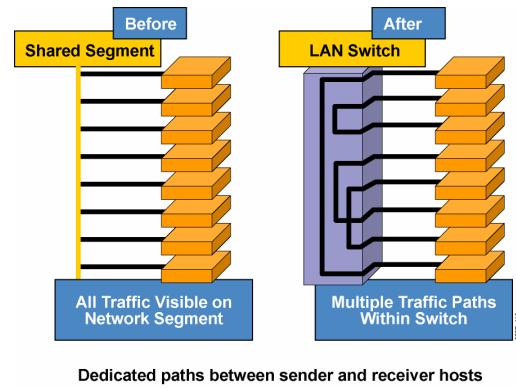


Ethernet LANs

15-1

Microsegmentation

Microsegmentation of the Network



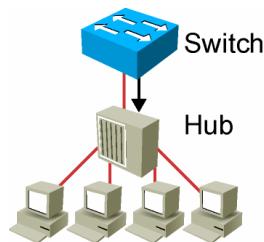
15-2

- Khi triển khai switch trên LAN sẽ cung cấp tính năng phân đoạn. Mỗi port của switch là một đoạn mạng. Mỗi thiết bị trên đoạn mạng này sẽ không tranh chấp với bất kỳ thiết bị nào trên đoạn mạng khác về băng thông. Tính năng quan trọng này hạn chế collision và tăng tốc độ truyền với kỹ thuật full-duplex.

Duplex Overview

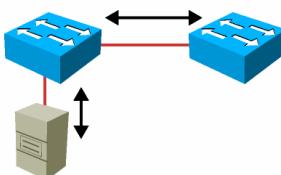
Half Duplex (CSMA/CD)

- Unidirectional data flow
- Higher potential for collision
- Hub connectivity



Full Duplex

- Point-to-point only
- Attached to dedicated switched port
- Requires full-duplex support on both ends
- Collision-free
- Collision detect circuit disabled



3015_126

15-3

- Cơ chế truyền half-duplex thực hiện CSMA/CD. Shared LAN truyền thông hoạt động theo half-duplex và dễ xảy ra collision.
- Full-duplex Ethernet cải tiến hiệu quả mạng ngoài việc mở rộng mạng. Để truyền full-duplex giữa các trạm sử dụng những kết nối point-to-point Ethernet, Fast Ethernet, và Gigabit Ethernet. Sự sắp xếp này sẽ không có collision. Việc gởi dữ liệu giữa hai máy đầu cuối có kết nối với nhau không có dung độ bởi mỗi máy đầu cuối sử dụng hai mạch riêng biệt trong cáp Cat5 hay Cat3. Mỗi kết nối full-duplex chỉ sử dụng 1 port
- Những kết nối full-duplex là những kết nối point-to-point giữa switch và máy đầu cuối, nhưng không phải giữa các shared hub. Những máy nào có NICs hỗ trợ full-duplex nên gắn vào port của switch có cấu hình full-duplex. Hầu hết những NICs Ethernet, Fast Ethernet, Gigabit Ethernet ngày nay đều hỗ trợ full-duplex. Trong cơ chế full-duplex không có collision.
- Những máy gắn vào các hub mà chia sẻ kết nối của chúng đến một port trên switch phải hoạt động trong cơ chế half-duplex vì thế những máy đầu cuối phải có khả năng phát hiện collision.
- Shared Ethernet đạt khoảng 50 đến 60% của 10Mbps. Full-duplex Ethernet đạt được 100% trong cả 2 hướng (10Mbps truyền và 10Mbps nhận)

- **Giao tiếp full-duplex**

- Trong mạng LAN dùng switch, mỗi thiết bị gắn vào một port của switch là một kết nối point-to-point. Trong mạng với hub, các thiết bị chỉ có thể giao tiếp một hướng tại một thời điểm vì thế chúng phải tranh chấp băng thông. Loại giao tiếp này được gọi là half-duplex. Switch có thể cung cấp cho các thiết bị kết nối đến nó giao tiếp full-duplex; mỗi người có thể nói và nghe đồng thời với những người khác.

- **Ví dụ: trao đổi dữ liệu**

- Nếu bạn sử dụng một thiết bị giao tiếp voice như walkie-talkie, bạn sẽ giao tiếp trong half-duplex. Bạn có thể nói, nhưng sau đó bạn dừng nói để nghe người bên kia nói lại. Tuy nhiên, với telephone bạn có thể giao tiếp với nhiều người khác trong full-duplex; mỗi người có thể nói và nghe đồng thời.

Setting Duplex and Speed Options

Cisco Catalyst 2960 Series

```
SwitchX(config)#interface fa0/1  
SwitchX(config-if)#duplex {auto | full | half}
```

Cisco Catalyst 2960 Series

```
SwitchX(config)#interface fa0/1  
SwitchX(config-if)#speed {10 | 100 | 1000 | auto}
```

15-5

- Sử dụng lệnh **duplex** trong interface mode để cấu hình duplex của interface. Những biến của lệnh duplex trên Catalyst 2960 như sau:
 - **Auto:** đàm phán tự động duplex. Hai port sẽ tự quyết định cơ chế nào tốt nhất.
 - **Full:** cấu hình full-duplex
 - **Half:** cấu hình half-duplex
- Fast Ethernet và những port 10/100/1000, mặc định là auto. 100Base-fx mặc định là full. Những port 10/100/1000 sẽ hoạt động half hoặc full khi cấu hình 10 hoặc 100, nhưng khi cấu hình 1000 chỉ có 1 cơ chế là full-duplex
- Những port 100base-fx chỉ hoạt động 100mbps trong cơ chế full-duplex

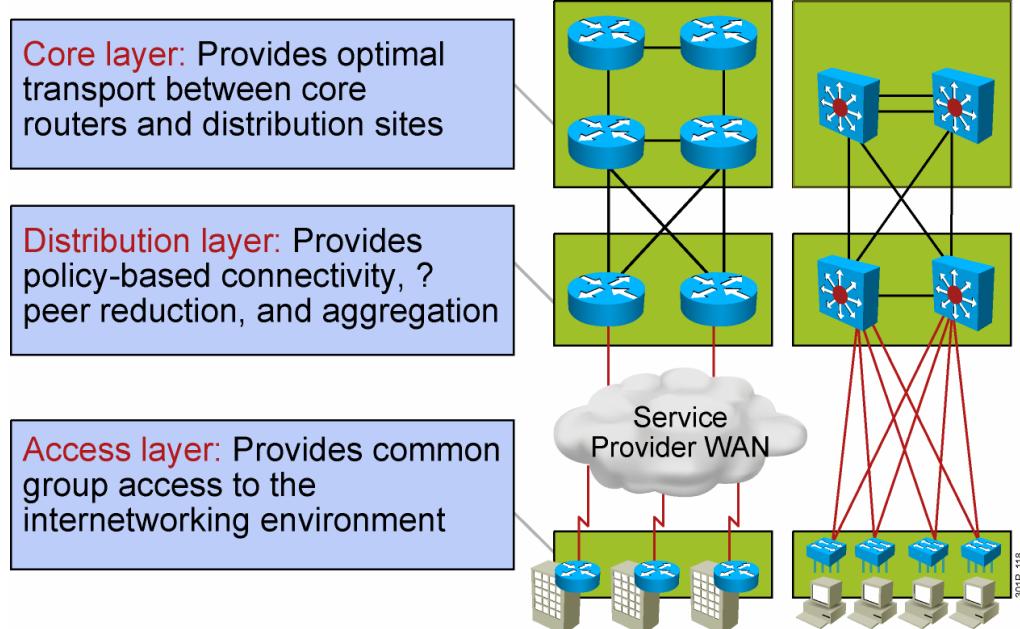
Showing Duplex Options

```
SwitchX#show interfaces fastethernet0/2
FastEthernet0/2 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0008.a445.9b42 (bia 0008.a445.9b42)
    MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
      reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA, loopback not set
    Keepalive set (10 sec)
    Half-duplex, 10Mb/s
      input flow-control is unsupported output flow-control is unsupported
      ARP type: ARPA, ARP Timeout 04:00:00
      Last input 00:00:57, output 00:00:01, output hang never
      Last clearing of "show interface" counters never
      Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
      Queueing strategy: fifo
      Output queue: 0/40 (size/max)
      5 minute input rate 0 bits/sec, 0 packets/sec
      5 minute output rate 0 bits/sec, 0 packets/sec
        323479 packets input, 44931071 bytes, 0 no buffer
        Received 98960 broadcasts (0 multicast)
        1 runts, 0 giants, 0 throttles
        1 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
        0 watchdog, 36374 multicast, 0 pause input
        0 input packets with dribble condition detected
        1284934 packets output, 103121707 bytes, 0 underruns
        0 output errors, 2 collisions, 6 interface resets
        0 babbles, 0 late collision, 29 deferred
        0 lost carrier, 0 no carrier, 0 PAUSE output
        0 output buffer failures, 0 output buffers swapped out
```

15-6

- Sử dụng lệnh **show interface** trên catalyst 2960 để kiểm tra cấu hình duplex. Lệnh này hiển thị những thông kê và trạng thái của tất cả interface hoặc những interface chỉ định. Hình vẽ chỉ ra cấu hình duplex của một interface.
- Autonegotiation có thể đạt kết quả không mong muốn. Mặc định, khi autonegotiation bị lỗi, switch sẽ cấu hình port đó là half-duplex. Lỗi này xảy ra khi thiết bị gắn vào port không hỗ trợ autonegotiation. Nếu thiết bị được cấu hình half-duplex bằng tay, nó sẽ phù hợp với cơ chế mặc định của switch. Tuy nhiên, lỗi autonegotiation có thể xảy ra khi thiết bị được cấu hình full-duplex bằng tay. Nếu một đầu cấu hình half-duplex, và đầu bên kia cấu hình full-duplex sẽ gây ra lỗi late collision tại đầu half-duplex. Để tránh trường hợp này, cấu hình duplex cho port của switch phù hợp với thiết bị gắn vào port
- Nếu port của switch là full-duplex và thiết bị gắn vào là half-duplex, kiểm tra lỗi FCS trên port full-duplex
- Bạn có thể dùng lệnh **show interface** để kiểm tra lỗi FCS late collision.

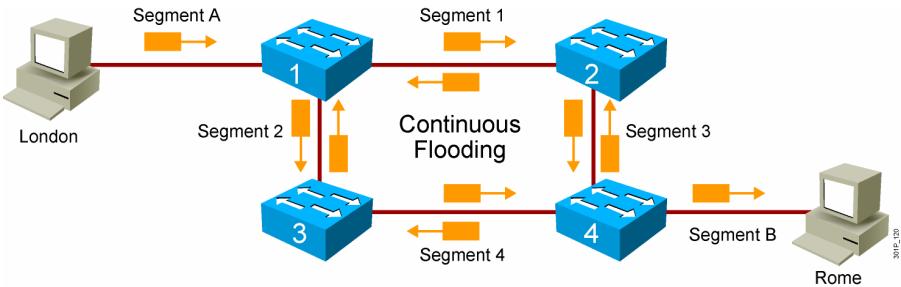
The Hierarchy of Connectivity



15-7

- Có một số giao thức Ethernet tốc độ cao (như Fast Ethernet và Gigabit Ethernet). Yêu cầu về performance là quan trọng trong những mạng lớn, vì thế những giao thức này đáp ứng được yêu cầu này. Tuy nhiên, chi phí cho việc triển khai kết nối tốc độ cao này trong tất cả mạng sẽ rất đắt và các user và thiết bị sẽ sử dụng không đạt hiệu quả. Triển khai mô hình kết nối phân cấp là cách hiệu quả nhất để cung cấp tốc độ truyền.
- Trong mô hình kết nối phân cấp, những thiết bị đầu cuối được xem như là access-level system, bởi vì chúng là những điểm chính truy cập mạng để truyền dữ liệu. Những thiết bị đầu cuối sẽ hội tụ tại server level hay workgroup (distribution) level, và nếu cần thiết, những thiết bị đầu cuối sẽ sử dụng backbone (core) để đến những thiết bị distribution khác. Tốc độ cao thường được cấu hình ở những thiết bị truyền tải lượng dữ liệu lớn từ nhiều user, đặc biệt tại distribution và core level

Loops



15-8

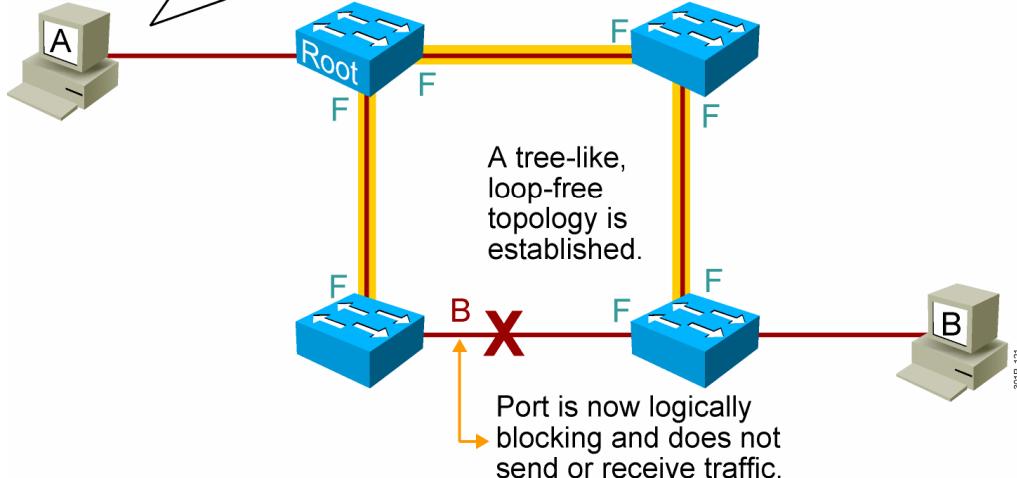
- Triển khai LAN với switch có thể đạt được lợi ích của việc dự phòng (redundancy); chẳng hạn, kết nối 2 switch đến cùng một segment để chắc chắn rằng hoạt động liên tục nếu có những vấn đề xảy ra với một trong những segment. Redundancy chắc chắn rằng mạng hoạt động liên tục tất cả thời gian. Tuy nhiên, khi triển khai redundancy có thể xảy ra loop. Khi một máy trên một segment gửi dữ liệu đến một máy trên segment khác, có 2 kết nối giữa 2 segment bởi 2 hay nhiều switch, mỗi switch nhận frame, tìm vị trí của thiết bị nhận, và chuyển frame. Cuối cùng host nhận được 2 frame giống nhau. Bảng MAC cũng có thể được cập nhật với thông tin địa chỉ không đúng, kết quả là chuyển frame không chính xác.
- Khi nhận được những frame có địa chỉ multicast, broadcast, hoặc những địa chỉ chưa biết, switch sẽ chuyển đến tất cả các port trừ port nhận. Kết quả của việc chuyển này sẽ gây nên “storm traffic”

Ví dụ:

- Gọi ý host London gửi một frame đến host Rome. London thuộc segment A, và Rome thuộc segment B. kết nối Redundancy giữa các host sẽ đảm bảo hoạt động liên tục trong trường hợp lỗi segment xảy ra. Ví dụ, không có switch nào học được địa chỉ của host Rome.
- Switch 1 nhận frame có địa chỉ đích là Rome và sẽ flood frame đến switch 2 và 3. Cả 2 switch 2 và 3 đều nhận được frame từ London (switch 1) và học địa chỉ London là trên segment 1 và 2. Mỗi switch sẽ chuyển frame đến switch 4.
- Switch 4 nhận 2 bản copy của frame từ London, một cái từ switch 2 và một cái từ switch 3. Giả sử frame trên switch 2 đến trước. Switch 4 biết rằng London trên segment 3. Vì switch 4 không biết địa chỉ của Rome, nó sẽ chuyển frame đến Rome và switch 3. Khi frame từ switch 3 đến switch 4, switch 4 cập nhật bảng địa chỉ với London trên segment 4. Sau đó nó chuyển frame đến Rome và switch 2.
- Switch 2 và 3 bây giờ thay đổi bảng địa chỉ của mình liên tục để chỉ rằng London là trên segment 3 hoặc 4. Nếu frame gửi từ London là một broadcast frame, cả 2 switch sẽ chuyển các frame một cách liên tục, sử dụng tất cả băng thông và khóa việc truyền những packet khác trên cả 2 segment. Trường hợp này gọi là broadcast storm.

Spanning Tree Protocol

One switch is elected the root based on lowest bridge ID (priority and MAC address concatenated).



15-10

- Giải pháp chống lặp là sử dụng nghi thức STP (Spanning-Tree Protocol). STP sẽ quản lý các đường chuyển vật lý cho những đoạn mạng. STP duy trì mô hình đường chuyển dự phòng vật lý (physical loop), và tạo ra một môi trường chuyển dẫn không bi lặp trong mạng (free logical loop). STP được kích hoạt chạy mặc định trên các dòng Catalyst switches.
- STP hoạt động như sau:
 - STP sẽ định ra một số cổng (ports) ở trạng thái nghỉ (standby), vì vậy những cổng này không thể truyền, xử lý dữ liệu frames. Điều này sẽ tạo ra được chỉ một đường mạng đến mỗi đoạn mạng trong 1 thời điểm.
 - Nếu có sự cố xảy ra với những kết nối đến những đoạn mạng, STP sẽ tái thiết lập kết nối bằng cách tự động kích hoạt những đường mạng đang ở trạng thái nghỉ.
- Lưu ý: Spanning Tree Protocol sẽ được nói đến chi tiết hơn trong phần ICND2.

Tóm tắt

- Mạng Switched LANs cung cấp cơ chế microsegmentation cho phép mỗi thiết bị trên một đoạn mạng được kết nối trực tiếp đến cổng của switch và được truyền dữ liệu với băng thông tối đa của cổng switch. Mỗi thiết bị sẽ không cần phải chia sẻ băng thông với các thiết bị khác trên mạng.
- Giao tiếp ở chế độ half-duplex trong một mạng Ethernet LAN cho phép việc trao đổi dữ liệu theo 1 hướng trong 1 thời điểm(chuyền hoặc nhận). Giao tiếp ở chế độ full-duplex cho phép chuyển và nhận dữ liệu cùng lúc. Switches có giao tiếp ở chế độ full-duplex.
- Sử dụng kết nối Ethernet theo mô hình phân cấp là cách hiệu quả nhất về tốc độ chuyển trong một mạng campus, thiết lập FastEthernet và GigabitEthernet cho môi trường mạng workgroup và kết nối backbone.

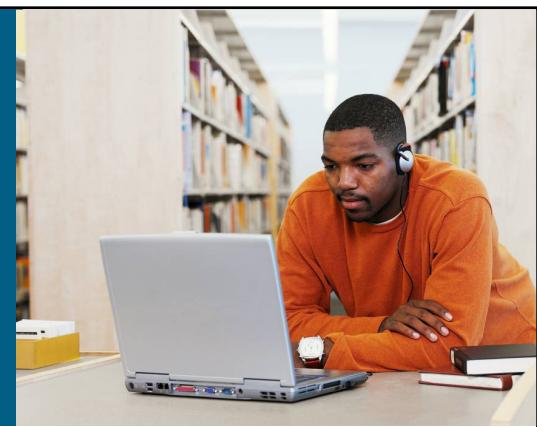
Tóm tắt (tiếp theo.)

- Nguyên nhân của lặp (loop) dữ liệu là khi các switches kết nối đến cùng một đoạn mạng chuyền nhận giữ liệu như nhau. Khung dữ liệu di chuyển tuần hoàn giữa 2 đường mạng mà không thể dừng việc di chuyển này và có thể dẫn đến làm sai lệch nội dung bảng MAC.
- Giải pháp để chống lặp là sử dụng nghi thức STP (Spanning-Tree Protocol). STP sẽ quản lý cách dữ liệu được chuyền nhận trong những đoạn mạng. STP đưa ra một đường dự phòng trong mạng Ethernet LAN (physical loop), nhưng vẫn đảm bảo dữ liệu không bị lặp.



15-13

Bài 16: Xử lý các sự cố của Switch.



Ethernet LANs

Module 16-1

- **Tổng quan:**

Hầu hết những vấn đề gặp phải trong một mạng chuyển mạch đều bắt nguồn trong quá trình thiết lập cấu hình ban đầu. Theo lý thuyết, một khi được cài đặt, hệ thống mạng vẫn tiếp tục vận hành mà không có vấn đề. Tuy nhiên đó chỉ là lý thuyết. Mọi thứ đều thay đổi: cáp hụt, cấu hình thay đổi, có thiết bị mới kết nối vào switch, những điều này yêu cầu thay đổi cấu hình của switch. Vì vậy chúng ta luôn cần phải thường xuyên làm công việc bảo trì.

- **Mục tiêu:** Sau khi hoàn thành bài học, bạn có khả năng xác định và giải quyết những vấn đề chung nhất trong mạng switch. Khả năng này bao gồm một số mục tiêu:

- Miêu tả cách giải quyết sự cố trong môi trường switch theo mô hình lớp.
- Xác định và giải quyết những vấn đề chung nhất của phương tiện truyền dẫn trong môi trường mạng chuyển mạch.
- Xác định và giải quyết những vấn đề chung nhất của access port
- Xác định và giải quyết những vấn đề chung nhất trong cấu hình.

The Layered Approach

- Switches hoạt động ở lớp 2 của mô hình tham chiếu OSI
- Switches cung cấp một giao tiếp với phương tiện chuyền dẫn lớp vật lý.
- Có nhiều sự cố thường được thấy tại lớp 1 và lớp 2.
- Một số vấn đề lớp 3 có thể nảy sinh liên quan đến việc truy cập vào các chức năng quản lý của switch.

Module 16-2

- Tại lớp 1 của mô hình tham chiếu OSI, switches cung cấp một giao tiếp đến phương tiện chuyền dẫn vật lý. Tại lớp 2 của mô hình tham chiếu OSI switches thực hiện việc chuyển frame dựa trên địa chỉ MAC. Ví thế những vấn đề thường được thấy tại lớp 1 và lớp 2. Cũng có một số vấn đề lớp 3, như là việc kết nối IP đến switch dùng cho mục đích quản trị.
- Lưu ý: Xử lý sự cố lớp 3 sẽ được đề cập trong bài “LAN Connections”.

Switched Media Issues

Những vấn đề của phương tiện truyền dẫn có nhiều nguyên nhân, có thể có bắt nguồn từ:

- Dây cáp bị hư hỏng.
- Nhiều điện tử.
- Các định dạng của dữ liệu bị thay đổi.
- Khi cài đặt thiết bị mới.

Module 16-3

- Những vấn đề về phương tiện truyền dẫn là thường xảy ra. Trong thực tế đó là hư cáp. Một vài ví dụ cho những cho những vấn đề liên quan đến phương tiện truyền dẫn:
 - Trong môi trường sử dụng loại cáp 3, việc lắp đặt hệ thống máy điều hòa không khí là nguyên nhân gây ra nhiều điện tử cho môi trường.
 - Trong môi trường sử dụng loại cáp 5, nếu vị trí cáp quá gần động cơ thang máy cũng bị ảnh hưởng.
 - Quản lý cáp không tốt: dây bị đứt trọng đầu nối RJ-45 do quá căng,...
 - Những ứng dụng mới có thể làm thay đổi định dạng của dữ liệu.
- Đôi khi một điều đơn giản như việc một người sử dụng nào đó kết nối 1 HUB đến 1 port của switch, rồi sau đó người đó kết nối đến HUB bằng nhiều máy tính, điều này có thể gây ra sự đụng độ trên mạng.

show interface

```
SwitchX#show interface fastethernet 0/0
Fastethernet 0/0 is up, line protocol is up [1]
Hardware is MCI Ethernet, address is aa00.0400.0134 (via 0000.0c00.4369
Internet address is 131.108.1.1, subnet mask is 255.255.255.0

.
.
.
Output Omitted

.
.
.

2295197 packets input, 305539992 bytes, 0 no buffer
Received 1925500 broadcasts, 0 runts, 0 giants
3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort [2]
0 input packets with dribble condition detected
3594664 packets output, 436549843 bytes, 0 underruns
8 output errors, [3]
1790 collisions, [4]
10 interface resets,
0 restarts [5]
```

Module 16-4

- Sử dụng lệnh **show interface** việc hư hỏng cáp và cáp bị nhiễu điện từ thường thể hiện qua những giá trị excessive và noise. Việc thay đổi định dạng dữ liệu và việc cài đặt thêm HUB gây ra những lỗi sẽ được thể hiện qua những giá trị collisions và runts frames.

Excessive Noise

Những bước đề nghị cần làm:

- Sử dụng lệnh **show interface ethernet** để xem tình trạng của các giao tiếp Ethernet. Nếu kết quả thấy có nhiều lỗi CRC và ít lỗi đụng độ (collisions) thì đó là dấu hiệu chỉ ra có quá nhiều nhiễu.
- Kiểm tra cáp truyền dẫn xem có bị hư hỏng hay không.
- Nếu chúng ta dùng loại cáp 100Base-TX, thi phải bảo đảm rằng chúng ta đang dùng chủng loại cáp 5.

Module 16-5

- Khi bạn xử lý các sự cố có liên quan đến excessive noise, thi có 3 bước được đề nghị để giúp bạn cách ly và giải quyết các sự cố:
 - Sử dụng lệnh **show interface ethernet** để xem tình trạng của các giao tiếp Ethernet. Nếu kết quả thấy có nhiều lỗi CRC và ít lỗi đụng độ (collisions) thì đó là dấu hiệu chỉ ra có quá nhiều nhiễu.
 - Kiểm tra cáp truyền dẫn xem có bị hư hỏng hay không.
 - Nếu chúng ta dùng loại cáp 100Base-TX, thi phải bảo đảm rằng chúng ta đang dùng chủng loại cáp 5.

Excessive Collisions

Suggested steps:

Những bước đề nghị cần làm:

- Dùng lệnh **show interface ethernet** để kiểm tra tỉ lệ đụng độ. Tổng số lần đụng độ so với tổng số gói gửi ra nên ở mức 0.1% hoặc ít hơn.
- Dùng thiết bị TDR để tìm ra những chỗ đứt đoạn của cáp Ethernet. Thiết bị TDR kiểm tra tính liên tục và những thuộc tính khác của cáp bằng cách gửi ra những tín hiệu trên phương tiện truyền dẫn.
- Tìm kiếm jabbering trên những đầu thu phát được gắn vào thiết bị. Điều này có lẽ yêu cầu cần theo dõi kết nối giữa 2 thiết bị bằng cách dùng những chương trình phân tích nghi thức (protocol analyzer). Jabber xảy ra khi một thiết bị liên tục gửi dữ liệu một cách bất định.

Module 16-6

- Khi bạn xử lý các sự cố liên quan đến excessive collisions, thi có 3 bước được đề nghị để giúp bạn cách ly và giải quyết các sự cố:
 - Dùng lệnh **show interface ethernet** để kiểm tra tỉ lệ đụng độ. Tổng số lần đụng độ so với tổng số gói gửi ra nên ở mức 0.1% hoặc ít hơn.
 - Dùng thiết bị TDR để tìm ra những chỗ đứt đoạn của cáp Ethernet. Thiết bị TDR kiểm tra tính liên tục và những thuộc tính khác của cáp bằng cách gửi ra những tín hiệu trên phương tiện truyền dẫn.
 - Tìm kiếm jabbering trên những đầu thu phát được gắn vào thiết bị. Điều này có lẽ yêu cầu cần theo dõi kết nối giữa 2 thiết bị bằng cách dùng những chương trình phân tích nghi thức (protocol analyzer). Jabber xảy ra khi một thiết bị liên tục gửi dữ liệu một cách bất định.

Late Collisions

Suggested steps:

Những bước đề nghị cần làm:

- Sử dụng chương trình phân tích nghi thức (protocol analyzer) để kiểm tra late collisions. Late collisions không nên xảy ra trong một hệ thống mạng Ethernet khi được thiết kế hoàn chỉnh. Chúng chỉ thường xảy ra khi cáp Ethernet quá dài hoặc khi có quá nhiều bộ lặp dữ liệu (repeaters) trong mạng.
- Xác định khoảng cách giữa thiết bị đầu và thiết bị cuối trên một đoạn mạng phải theo đúng tiêu chuẩn về khoảng cách.

Module 16-7

- Khi bạn xử lý các sự cố liên quan đến excessive late collisions, thi có 2 bước được đề nghị để giúp bạn cách ly và giải quyết các sự cố:
 - Sử dụng chương trình phân tích nghi thức (protocol analyzer) để kiểm tra late collisions. Late collisions không nên xảy ra trong một hệ thống mạng Ethernet khi được thiết kế hoàn chỉnh. Chúng chỉ thường xảy ra khi cáp Ethernet quá dài hoặc khi có quá nhiều bộ lặp dữ liệu (repeaters) trong mạng.
 - Xác định khoảng cách giữa thiết bị đầu và thiết bị cuối trên một đoạn mạng phải theo đúng tiêu chuẩn về khoảng cách.

Port Access Issues

- Media-related issues
- Duplex-related issues
- Speed-related issues

Module 16-8

- Những sự cố liên quan đến phương tiện truyền dẫn thường được xem như là sự cố truy nhập, (ví dụ: người sử dụng báo với chúng ta rằng “Tôi không thể truy cập vào mạng được”). Các sự cố của phương tiện truyền dẫn nên được cách ly và giải quyết theo những chủ đề chung ta nếu ở các phần trước. Những sự cố liên quan đến Duplex thường bị gây ra bởi việc không cùng cấu hình Duplex giữa 2 đầu kết nối. Những sự cố liên quan đến tốc độ truyền thường bị gây ra bởi không cùng cấu hình tốc độ giữa 2 đầu kết nối.

Duplex-Related Issues

Duplex modes:

- One end set to full and the other set to half results in a mismatch.
- One end set to full and autonegotiation set on the other end:
 - Autonegotiation fails, and that end reverts to half.
 - Results in a mismatch.
- One end set to half and autonegotiation set on the other:
 - Autonegotiation fails, and that end reverts to half.
 - Both ends at half; no mismatch.
- Autonegotiation on both ends:
 - One end fails to full, and the other end fails to half.
 - Example: A Gigabit Ethernet interface defaults to full, while a 10/100 defaults to half.
- Autonegotiation on both ends:
 - Autonegotiation fails on both ends, and they revert to half.
 - Both end at half; no mismatch.

Module 16-9

- Sử dụng lệnh **show interface** để xác định cấu hình Duplex.

Speed-Related Issues

Duplex modes:

- One end set to one speed and the other set to another, resulting in a mismatch.
- One end set to a higher speed and autonegotiation enabled on the other end.
 - If autonegotiation fails, the autonegotiation end reverts to its lowest speed.
 - Results in a mismatch.
- Autonegotiation on both ends:
 - Autonegotiation fails on both ends, and they revert to their lowest speed.
 - Both end at half; no mismatch.

Module 16-10

Configuration Issues

- Know what you have before you start.
 - Hard copy
 - Text file
 - TFTP server
- Verify changes before you save.
 - Confirm that the issue was corrected and no new issues were created.
- Save the current configuration.
 - **copy running-config start-config**
- Secure the configuration.
 - Password-protect the console.
 - Password-protect the vty.
 - Password-protect EXEC mode.

Module 16-11

- Khi bạn muốn cấu hình một thiết bị, bạn nên luôn luôn cần biết một số thông tin trước khi bắt đầu cấu hình như là: cấu hình thiết bị, phần cứng thiết bị, và mô hình mạng. Khi bạn cấu hình thiết bị, luôn luôn phải lưu trữ lại 1 bản sao cấu hình. Ví dụ: bạn lưu trữ lại cả 2 bản cấu hình cứng, lẫn bản cấu hình băng điện tử - bạn có thể lưu trữ trên một máy tính hoặc trên một TFTP server.
- Khi bạn thay đổi cấu hình, trước khi bạn lưu trữ lại cấu hình mới, bạn cần kiểm tra lại những thay đổi cấu hình mới đó có đáp ứng được những yêu cầu của bạn chưa, điều này cần làm để tránh gặp những sự cố đáng tiếc có thể xảy ra.
- Những thay đổi về cấu hình được thực hiện bởi những người không có thẩm quyền có thể gây ra những điều đáng tiếc. Để chắc rằng không có những sự đáng tiếc đó, bạn nên bảo mật cấu hình của thiết bị, đặt mật khẩu cho các cổng **console** và **vty** bằng mật khẩu mạnh (mật khẩu khó đoán được). Và điều đó cũng được thực hiện cho chế độ EXEC.

Tóm tắt

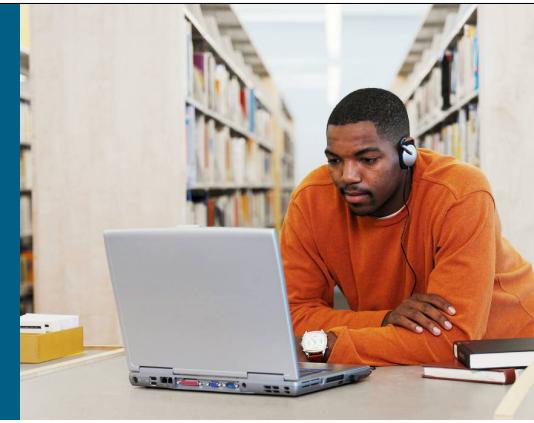
- Xử lý sự cố theo mô hình lớp.
- Sử dụng lệnh **show interface** để xử lý các sự cố:
 - Media issues
 - Duplex issues
 - Speed issues
- Lưu trữ bản sao các tập tin cấu hình và bảo vệ cấu hình đang vận hành.

Module 16-12



Module 16-13

Bài 17: Tìm hiểu mạng WLAN



Mạng không dây cục bộ (Wireless LANs)

Module 17-1

TÌM HIỂU HỆ THỐNG MẠNG KHÔNG DÂY

Tổng quan

Truy cập không dây vào hệ thống mạng được phát triển giống như hầu hết các công nghệ mới khác: nhu cầu thực tế thúc đẩy sự phát triển của công nghệ, công nghệ mới ra đời lại thúc đẩy các nhu cầu thực tế mới khác, và cứ như vậy nhu cầu thực tế mới lại thúc đẩy công nghệ mới khác ra đời. Để giữ vòng xoay này không rời ngoài tầm kiểm soát, một vài tổ chức đã phát triển để xây dựng cho chúng ta những tiêu chuẩn kỹ thuật và hệ thống chứng nhận cho các công nghệ. Bài học này sẽ mô tả những xu hướng và chuẩn kỹ thuật gấp phải trong việc phát triển mạng LAN không dây (WLAN)

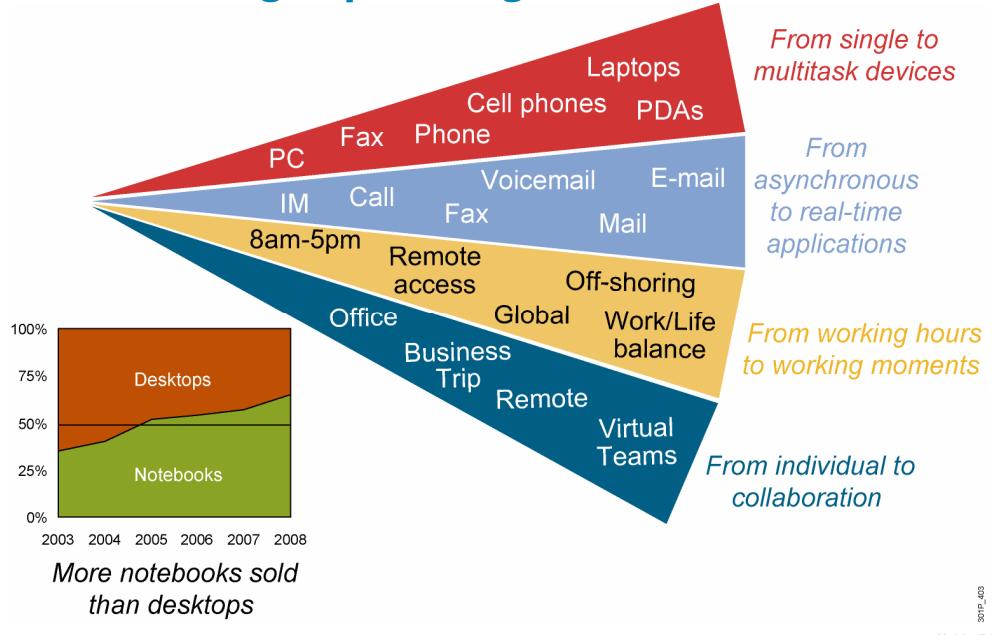
Mục tiêu

Sau khi hoàn tất bài học, bạn có khả năng mô tả những yếu tố ảnh hưởng và những tiêu chuẩn áp đặt trên hệ thống mạng LAN không dây qua các nhiệm vụ sau:

- Mô tả những nhu cầu thực tế cần đến dịch vụ WLAN
- Mô tả sự khác biệt giữa việc thực thi mạng WLAN và LAN
- Xác định các đặc tính của việc truyền dẫn sử dụng sóng radio trong mạng WLAN

- Xác định các tổ chức định ra các chuẩn cho mạng WLAN
- Mô tả hệ thống 3 băng tầng không đăng ký được sử dụng trong mạng không dây FCC bởi tổ chức ITU-R
- So sánh những sự khác biệt giữa những chuẩn trong IEEE 802.11
- Mô tả về hệ thống chứng nhận Wi-Fi

Xu hướng thị trường



Module 17-3
201P_403

Ngày nay, hiệu suất lao động không còn bị giới hạn trong việc bạn phải làm việc trong một vị trí cố định hay trong một khoảng thời gian ràng buộc được định sẵn. Chúng ta được mong đợi trong việc có thể thực hiện kết nối tại bất cứ nơi đâu vào bất cứ thời gian nào, từ văn phòng đến sân bay hay thậm chí là tại nhà. Thông thường, một số nhân viên đi công tác hay bị hạn chế trong việc phải trả cước phí điện thoại để kiểm tra một vài tin nhắn và phải trả lời một số cuộc gọi giữa các chuyến bay. Giờ đây, họ có thể kiểm tra thư điện tử, duyệt web, trong khi lên máy bay qua các thiết bị hỗ trợ cá nhân (PDA) của mình.

Ngay tại nhà, giờ đây con người cũng đã thay đổi cách học tập và cách sống. Mạng Internet đã trở thành một chuẩn mực có trong nhà ngoài các dịch vụ TV hay điện thoại. Các phương pháp truy cập Internet cũng thay đổi một cách nhanh chóng từ những kết nối tạm thời qua dịch vụ quay số cho đến những đường truyền băng thông rộng được dành riêng trên công nghệ DSL hay Calbe. Trong năm 2005, người sử dụng đã mua những máy tính xách tay có khả năng hỗ trợ Wi-Fi nhiều hơn là những máy tính để bàn cố định.

Một trong những lợi ích rõ ràng nhất mà mạng không dây mang lại chính là việc giảm giá thành. Hai ngũ cảnh sau sẽ thể hiện lợi ích này. Với ngũ cảnh thứ nhất, trên một cơ sở hạ tầng mạng không dây sẵn có, việc tiết kiệm chi phí sẽ được nhận ra khi chuyển một người dùng từ một vị trí này sang vị trí khác, việc sắp xếp lại một phòng LAB, hay việc di chuyển đi từ một nơi tạm thời,... Trung bình, chi phí IT cho việc chuyển một nhân viên từ vị trí làm việc này sang vị trí làm việc khác là 375\$. Và trong thực tế thông thường sẽ có khoản 15% số nhân viên ra vào trong một năm. Ngũ cảnh thứ hai được nhận ra khi một công ty chuyển sang một tòa nhà mới mà không có sẵn bất kỳ một cơ sở hạ tầng truyền dẫn bằng dây nào. Trong ngũ cảnh này, việc tiết kiệm chi phí của mạng không dây lại càng đáng kể hơn bởi việc đi dây trong tường, trên trần hay dưới sàn nhà là việc rất nặng nhọc và tốn kém.

Một lợi ích kế tiếp khác của việc sử dụng mạng WLAN là tăng sự thỏa mãn của nhân viên, lợi ích này sẽ giúp ít thay đổi xảy ra trong nguồn nhân sự và giúp tiết kiệm chi phí trong việc tuyển thêm nhân viên mới, đồng thời thúc đẩy các nhân viên phục vụ khách hàng tốt hơn. Lợi ích này không thể lượng hóa được nhưng lại là một lợi ích quan trọng.

Khác nhau giữa WLAN và LAN

- WLAN sử dụng sóng radio như một phương tiện truyền dẫn lớp vật lý.
 - WLANs sử dụng CSMA/CA thay vì CSMA/CD cho việc truy xuất vào phương tiện truyền
 - Giao tiếp ở cơ chế bán song công.
- Một số vấn đề của sóng radio.
 - Vấn đề kết nối:
 - Tầm phủ sóng
 - Can nhiễu, nhiễu
 - Vấn đề riêng tư
- Access point là thiết bị chia sẻ băng thông có vai trò như HUB trong môi trường Ethernet.
- WLANs phải phù hợp với quy định tần số tại nước sở tại.

Module 17-5

• Trong môi trường WLAN, sóng radio được sử dụng tại lớp vật lý (trong mô hình OSI) như một phương tiện truyền dẫn

- WLAN sử dụng phương thức truy nhập CSMA/CA thay vì CSMA/CD trong mạng LAN Ethernet. Khả năng phát hiện xung đột không được trang bị trong hệ thống WLAN bởi vì một máy khi gửi sẽ không đồng thời nhận tín hiệu vào tại thời điểm đó. Thay vào đó, hệ thống WLAN sử dụng tín hiệu RTS (Ready to send – sẵn sàng gửi) và CTS (Clear to send – sẵn sàng nhận) để tránh xung đột trong quá trình truyền dẫn.

- Định dạng khung dữ liệu mà hệ thống WLAN sử dụng khác định dạng khung dữ liệu trong hệ thống Ethernet LAN. WLANs có thêm một số yêu cầu trên phần định dạng khung lớp 2.

Sóng radio sẽ tạo ra một số vấn đề không gặp như trong môi trường LAN

- Vấn đề kết nối trong mạng WLAN xảy ra thường là liên quan đến vấn đề tầm phủ sóng, quá trình truyền sóng radio, méo dạng sóng và can nhiễu từ những dịch vụ không dây hay những hệ thống WLANs khác.

- Vấn đề đám bảo sự riêng tư cũng là một thử thách bởi sóng radio có thể lọt ra ngoài tầm kiểm soát vật lý.

Trong môi trường WLAN, những người dùng di động kết nối với hệ thống mạng thông qua điểm truy cập (Access Point), được xem như tương tự với HUB trong môi trường Ethernet LAN

- Người dùng di động không có kết nối vật lý vào môi trường mạng.
- Những thiết bị di động thường sử dụng pin làm nguồn năng lượng chính, khác với các thiết bị gắn vào môi trường LAN.
- WLAN phải tuân theo một số quy định về tần số ở nước sở tại
- Mục tiêu của việc chuẩn hóa để đưa ra các tiêu chuẩn nhằm giúp mạng WLAN có mặt rộng khắp trên toàn thế giới. Bởi vì mạng WLAN sử dụng tần số radio, do vậy phải tuân theo quy định về tần số và công suất phát ở nước sở tại. Yêu cầu này không xảy ra trong hệ thống mạng LAN có dây.

Tuyên sóng Radio

- Tần số radio được bức xạ vào không khí qua các anten tạo thành sóng radio.
- Các vật thể có thể làm sóng radio bị:
 - Phản xạ
 - Tán xạ
 - Hấp thu
- Tần số cao cho phép truyền tốc độ nhanh nhưng khoản cách truyền lại ngắn.

Module 17-7

•Tần số radio trải từ dải băng tần AM đến dải tần số sử dụng cho điện thoại di động (cell phone). Chủ đề này nhằm xác định đặc tính của tần số radio được sử dụng truyền dẫn trong mạng WLAN

•Tần số radio được bức xạ ra không gian nhờ các anten, và anten là nơi tạo ra các sóng radio. Khi sóng radio truyền, nó có thể bị hấp thu (bởi vật ngăn trở như bức tường,...) hay bị phản xạ (bởi bề mặt kim loại,...). Những nguyên nhân này sẽ khiến vùng phủ sóng bị thiếu sóng hay chất lượng tín hiệu thấp.

•Việc truyền dẫn của sóng radio bị ảnh hưởng bởi những yếu tố sau:

- Phản xạ: xảy ra khi tần số sóng radio bị dội ra trên bề mặt của các vật thể như bề mặt của kim loại hoặc gương.

- Tán xạ: xảy ra khi tần số sóng radio va phải những bề mặt gồ ghề và bị phản xạ ra nhiều hướng khác nhau.

- Hấp thu: xảy ra khi tần số sóng radio bị hút vào các vật thể như bức tường.

•Một số quy luật sau được áp dụng cho việc truyền dẫn dữ liệu trên sóng radio:

- Tốc độ dữ liệu càng cao thì khoảng cách truyền càng ngắn bởi thiết bị nhận yêu cầu một tín hiệu mạnh phải có thông số SNR (Signal-to-Noise—tỷ số tín hiệu trên nhiễu) tốt để có thể nhận được thông tin.

-

- Công suất truyền càng cao, tầm phủ sóng càng xa. Để tăng gấp đôi tầm phủ sóng, công suất phát sẽ phải tăng lên 4 lần.
- Tốc độ truyền cao yêu cầu nhiều băng thông. Việc tăng băng thông có thể được thực hiện qua việc tăng tần số hoặc sử dụng một số phương pháp điều chế phức tạp.
- Tần số truyền càng cao khoảng cách truyền càng ngắn bởi nó dễ dàng bị hấp thu và suy hao. Vấn đề này có thể được giải quyết bởi một số anten thích hợp.

Các tổ chức định ra chuẩn cho mạng WLAN

ITU-R:

- International Telecommunication Union-Radiocommunication Sector
- Chỉ ra các tần số sóng được sử dụng trong WLAN

IEEE:

- Institute of Electrical and Electronic Engineers
- 802.11 là tài liệu về các chuẩn kỹ thuật



Wi-Fi Alliance:

- Tổ chức phi lợi nhuận
- Thúc đẩy sự phát triển của WLAN qua các chứng nhận liên vận hành giữa các hãng trên dòng sản phẩm cho WLAN

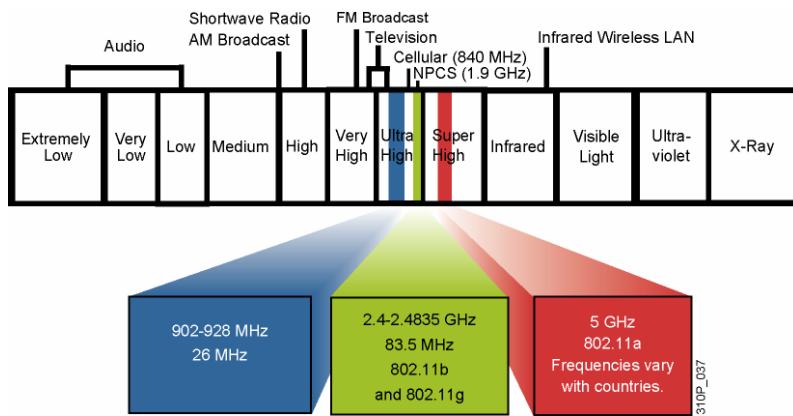


Module 17-9

- Một số tổ chức đã phát triển để thiết lập các tiêu chuẩn và hệ thống chứng nhận cho mạng WLAN. Chủ đề này sẽ đi kèm qua các tổ chức đó.
- Một tổ chức quản lý có nhiệm vụ điều khiển quá trình sử dụng của băng tần radio. Với sự khởi đầu của dải băng tần 900-MHz dành cho Công nghiệp, Khoa học và Y tế năm 1985, sự phát triển của WLAN đã được bắt đầu. Những cách truyền dẫn mới, điều chế mới, tần số mới phải được thông qua bởi tổ chức quản lý. Một sự thống nhất chung trên toàn thế giới cần được đưa ra. Các tổ chức quản lý bao gồm FCC (Federal Communication Commission) tại Mỹ (<http://www.fcc.gov>) và ETSI (Europe Telecommunication Standards Institute) tại châu Âu (<http://www.etsi.org>).
- IEEE (Institute of Electrical and Electronic Engineers) định ra các tiêu chuẩn. IEEE 802.11 là một phần của tiến trình chuẩn 802 dành cho hệ thống mạng. Bạn có thể tải về bản phê chuẩn các tiêu chuẩn từ IEEE trên website (<http://standards.ieee.org/getieee802>).

•Wi-Fi alliance đưa lại các chứng nhận cho khả năng liên vận hành giữa các hãng trên các sản phẩm 802.11 của họ. Các chứng nhận này là một cách để mang lại sự yên tâm cho người dùng khi chọn mua những sản phẩm này. Nó cũng giúp cho thị phần của công nghệ WLAN bằng cách xúc tiến khả năng liên vận hành giữa các hãng khác nhau. Những chứng nhận này bao gồm trên cả 3 băng tần sóng radio của chuẩn 802.11 và cả cho WPA (Wi-Fi Protected Access), một mô hình bảo mật được đưa ra năm 2003, được phê chuẩn vào năm 2004 dựa trên chuẩn bảo mật mới 802.11i. Wi-Fi Alliance xúc tiến và ảnh hưởng đến các tiêu chuẩn của mạng WLAN. Danh sách các sản phẩm được phê chuẩn có thể được tìm thấy tại trang web của Wi-Fi (<http://www.wi-fi.org>)

ITU-R với FCC Wireless



- ISM: industry, scientific, and medical frequency band
- Không cần đăng ký sử dụng
- Không được dành riêng
- Có khả năng bị can nhiễu

Module 17-11

- Có một vài băng tần radio không cần đăng ký tần số khi hoạt động. Chủ đề này mô tả 3 dãy băng tần không cần đăng ký được sử dụng cục bộ trong mạng không dây FCC của tổ chức ITU-R
- Có 3 băng tần không cần đăng ký tần số khi sử dụng: 900 MHz, 2.4 GHz và 5 GHz. Dãy băng tần 900 MHz và 2.4 GHz được biết đến như dãy băng tần dùng cho Công nghiệp, Khoa học và Y tế, trong khi đó dãy băng tần 5 GHz thì thường được biết đến như dãy băng tần UNII (Unlicensed National Information Infrastructure).
- Những tần số nằm trong những dải băng tần trên bao gồm:
 - Băng tần 900-MHz: 902 MHz đến 928 MHz
 - Băng tần 2.4 GHz: 2.400 MHz đến 2.483 MHz (tại Nhật, dải băng tần này được mở rộng đến 2.495 MHz)
 - Băng tần 5GHz: 5.150 MHz đến 5.350 MHz, 5.725 MHz đến 5.825 MHz, một số nước hỗ trợ việc sử dụng các dãy băng tần giữa 5.350 MHz và 5.725 MHz. Không phải tất cả các quốc gia đều cho phép sử dụng chuẩn 802.11a với dãy băng tần 5GHz. Danh sách các quốc gia cho phép chuẩn 802.11a hiện còn đang thay đổi.

- Hình trên biểu diễn dãy tần số của hệ thống WLAN. Kế tiếp dãy tần số của WLAN trong dãy phô trên là tần số của những dịch vụ không dây khác như điện thoại di động và dãy băng tần hẹp cho các dịch vụ giao tiếp cá nhân (PCS – Personal Communication Services). Những tần số sử dụng cho mạng WLAN là những dãy tần của ISM.
- Vận hành các thiết bị không dây trên những tần số không cần đăng ký thì không cần sự cấp phép. Tuy nhiên không một người dùng nào được độc chiếm bất kỳ một tần số nào. Ví dụ, băng tần 2.4 GHz được sử dụng cho mạng WLAN, truyền hình, Bluetooth, vi ba và các hệ thống điện thoại không dây (cordless).
- Mặc dù 3 dãy băng tần không cần đăng ký thì không cần phải được cấp phép để vận hành cá thiết bị, tuy nhiên chúng cũng phải được tuân theo qui định của một số quốc gia sở tại trong một số lĩnh vực như công suất truyền, độ lợi anten, tổng suy hao trên: thiết bị truyền dẫn, cáp, và độ lợi của anten.
- Công suất bức xạ vô hướng hiệu dụng (EIRP) là đơn vị cuối cùng của việc đo lường được giám sát bởi các tổ chức quản lý nội tại. Do đó, cần cẩn trọng trong việc thay đổi các thành phần của thiết bị không dây như việc thêm vào hoặc nâng cấp anten để mở rộng tầm phủ sóng. Kết quả có thể làm cho hệ thống WLAN không còn hợp pháp theo những quy định của cơ quan quản lý nội tại nữa.

EIRP = công suất phát + độ lợi anten – suy hao trên cáp dẫn.

Chú ý: Chỉ sử dụng anten và cáp dẫn được cung cấp theo danh sách dành cho những Access Point riêng biệt của nhà sản xuất. Chỉ dùng những người kỹ thuật am hiểu về các quy định về tần số của nhà quản lý nội tại.

So sánh các chuẩn IEEE 802.11

	802.11b	802.11a	802.11g	
Băng tần	2.4 GHz	5 GHz	2.4 GHz	
Số lượng kênh	3	Up to 23	3	
Truyền phát	Direct Sequence Spread Spectrum (DSSS)	Orthogonal Frequency Division Multiplexing (OFDM)	Direct Sequence Spread Spectrum (DSSS)	Orthogonal Frequency Division Multiplexing (OFDM)
Tốc độ [Mb/s]	1, 2, 5.5, 11	<u>6, 9, 12, 18, 24,</u> 36, 48, 54	1, 2, 5.5, 11	<u>6, 9, 12, 18,</u> <u>24, 36, 48, 54</u>

Module 17-13

- Các tiêu chuẩn của IEEE định nghĩa trên lớp vật lý và phân lớp MAC của lớp liên kết dữ liệu theo tham chiếu trong mô hình OSI. Những chuẩn không dây 802.11 nguyên gốc đã được hoàn tất vào năm 1997. Vào năm 1999 các chuẩn này đã được điều chỉnh lại để tạo ra chuẩn 802.11a/b và sau đó một lần nữa được xác nhận lại ở chuẩn 802.11g vào năm 2003.
- 1 kênh truyền và trái dữ liệu qua tất cả các tần số được định nghĩa trên kênh truyền đó.
- Chuẩn IEEE 802.11 chia băng tần ISM 2.4 GHz thành 14 kênh truyền, tuy nhiên một số cơ quan quản lý như FCC sẽ chỉ định kênh truyền nào được sử dụng, ví dụ như việc sử dụng kênh truyền từ số 1 đến 11 tại Mỹ. Mỗi kênh truyền trong dãy băng tần 2.4 GHz có băng thông là 22 MHz và chỉ cách nhau 5 MHz trên phổ tần số, do đó phổ của một kênh truyền sẽ bị chia làm hai phần với phổ của các kênh truyền liền trước và sau nó. Vì vậy, các kênh truyền cần được cách nhau qua 5 kênh truyền khác để không xảy ra hiện tượng chồng phổ này. Ví dụ, khi ta sử dụng 11 kênh truyền FCC, có 3 kênh truyền không trùng nhau là: 1, 6 và 11.
- Mạng không dây sử dụng cơ chế truyền bán song công (half-duplex), do vậy thông lượng truyền dẫn cơ bản chỉ vào khoảng một nửa tốc độ dữ liệu. Do đó, mục tiêu chính của chuẩn 802.11b là nhằm đạt được tốc độ truyền cao hơn ở băng tần ISM 2.4 GHz để tăng thị phần khách hàng và khuyến khích sự chấp nhận của khách hàng của hệ thống chứng nhận Wi-Fi.

• Chuẩn 802.11b định nghĩa việc sử dụng DSSS với thuật toán điều chế mới CCK (Complementary Code Keying) cho một tốc độ truyền cao hơn là 5.5 và 11 Mbps trong khi đó vẫn giữ kiểu điều chế cũ Barker ở tốc độ 1 và 2 Mbps. Chuẩn 802.11b vẫn dùng băng tầnISM 2.4 GHz như chuẩn 802.11 trước đó, mục tiêu nhằm đưa vào chuẩn 802.11b khả năng tương thích lùi với chuẩn cũ 802.11 ở tốc độ truyền liên quan là 1 và 2 Mbps.

• Vào năm mà chuẩn 802.11 được chấp nhận và thực hiện, IEEE đã phát triển một chuẩn khác là 802.11a. Động cơ thúc đẩy 802.11a là sử dụng một kiểu trai phổ (OFDM – Orthogonal Frequency Division Multiplexing) và công nghệ điều chế tín hiệu khác. 802.11a sử dụng dãy tần số rộng hơn trên dãy tần 5 GHz UNII. Trong thời điểm này, băng tầnISM 2.4 GHz đã được sử dụng rộng rãi cho hầu hết các thiết bị không dây như Bluetooth, điện thoại không dây, hệ thống giám sát, truyền video, games và thậm chí là tần số này còn được sử dụng trong lò vi sóng.Thêm vào đó, chuẩn 802.11a không được chấp nhận rộng rãi bởi vì các tài liệu để sản xuất các chip hỗ trợ chuẩn 802.11a ít phổ biến và điều này cũng tạo ra tiền đề dẫn đến giá thành cao trong việc phát triển hệ thống mạng sử dụng chuẩn 802.11a.

• Những chuẩn mới đây được phát triển bởi IEEE đều duy trì việc sử dụng chuẩn 802.11 MAC với tốc độ cao hơn trên băng tầnISM 2.4 GHz. IEEE 802.11g ra đời với sự cải thiện việc sử dụng kiểu trai phổ OFDM từ chuẩn 802.11a để đạt được tốc độ cao hơn và tương thích với chuẩn 802.11b sử dụng kiểu trai phổ DSSS. 802.11g hoạt động trên băng tầnISM 2.4 GHz. Tốc độ dữ liệu DSSS là 1, 2, 5.5 và 11Mbps và tốc độ dữ liệu OFDM là 6, 9, 12, 18, 24, 48 và 54Mbps đều được hỗ trợ bởi chuẩn 802.11g. IEEE chỉ yêu cầu trên 3 tốc độ dữ liệu bắt buộc là 6, 12 và 24Mbps mà sẽ không quan tâm đến các thiết bị hỗ trợ chuẩn 802.11a hay 802.11g OFDM.

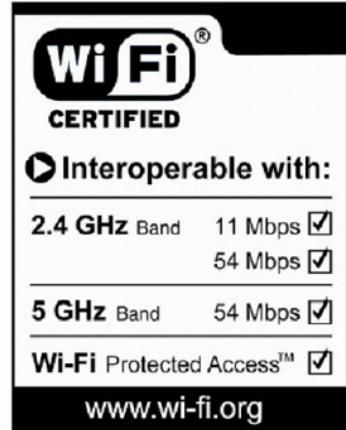
Chứng nhận Wi-Fi

Wi-Fi Alliance chứng nhận khả năng liên vận hành giữa các sản phẩm.

- Các sản phẩm bao gồm 802.11a, 802.11b, 802.11g, dual-band và kiểm tra về bảo mật.

Cisco là một thành viên sáng lập của Wi-Fi Alliance.

Những sản phẩm được chứng nhận có thể tham khảo tại <http://www.wi-fi.com>.



Module 17-15

• Mặc dù chuẩn 802.11 đã được thiết lập, nhu cầu để đảm bảo rằng tất cả các sản phẩm 802.11 đều có khả năng liên vận hành với nhau vẫn tồn tại. Chủ đề này sẽ mô tả làm cách nào chứng nhận Wi-Fi có thể đảm bảo khả năng liên vận hành này.

• Wi-Fi Alliance là tổ chức toàn cầu và phi lợi nhuận ra đời nhằm cải thiện sự phát triển và khả năng được chấp nhận của WLAN. Một trong những lợi điểm lớn nhất của Wi-Fi Alliance là nhằm đảm bảo khả năng liên vận hành giữa các sản phẩm 802.11 từ các hãng khác nhau bằng cách cung cấp các chứng nhận. Những hãng được chứng nhận khả năng liên vận hành này mang lại khả năng chắc chắn cho người sử dụng các sản phẩm của họ. Chứng nhận Wi-Fi bao gồm trên cả 3 công nghệ của IEEE cũng như những chuẩn mới đang phát triển như chuẩn về bảo mật. Wi-Fi Alliance cũng đã chứng nhận chuẩn bảo mật IEEE 802.11i là WPA (Wi-Fi Protected Access), và sau này được chỉnh sửa lại thành chứng nhận WPA2 sau bản ra đời cuối của chuẩn IEEE 802.11i.

Tóm tắt

- Con người luôn mong đợi một kết nối tại mọi lúc mọi nơi, tuy nhiên lợi điểm lớn nhất của WLAN là giảm thiểu chi phí.
- Cả WLAN và LAN đều dùng phương thức CSMA nhưng WLAN thì tránh còn LAN thì dùng phương pháp phát hiện va đụng.
- Tần số radio được bức xạ ra khỏi không trung nhờ anten, nơi nó có thể bị phản xạ, tán xạ, hay hấp thu
- IEEE định nghĩa các chuẩn cho WLAN

Module 17-16

Tóm tắt (tiếp theo.)

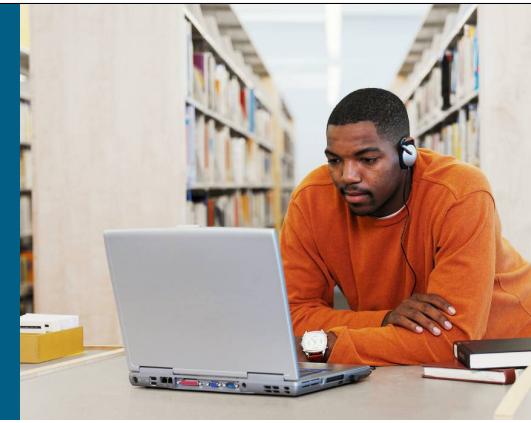
- Các tần số quy định cho WLAN bởi ITU là không cần đăng ký.
- Chuẩn 802.11 là một bộ chuẩn định nghĩa về tần số và băng tần cho WLAN.
- Một trong những lợi điểm của Wi-Fi là mang lại chứng nhận sự tương thích giữa các sản phẩm 802.11

Module 17-17



Module 17-18

Bài 18: Tìm hiểu về bảo mật trên WLAN



Mạng không dây cục bộ (Wireless LANs)

Module 18-1

Tổng quan

Một lợi ích rõ ràng nhất mà hệ thống không dây mang lại đó là khả năng giảm chi phí. Bên cạnh việc tăng hiệu suất, hệ thống WLAN cũng làm tăng chất lượng làm việc. Tuy nhiên chỉ cần một lỗ hổng xảy ra trên bất kỳ một Access Point nào cũng gây ảnh hưởng nghiêm trọng hay thậm chí có thể phá hủy cả một tổ chức. Hiểu được khái niệm bảo mật trong hệ thống mạng WLAN và làm thế nào để giảm thiểu các rủi ro này là một vấn đề khá quan trọng.

Mục tiêu

Sau khi hoàn tất bài học, bạn có khả năng mô tả các vấn đề liên quan đến việc bảo mật trên môi trường WLAN và những tính năng sẵn sàng nhằm tăng khả năng bảo mật trên hệ thống mạng. Khả năng này được thể hiện qua các nhiệm vụ sau:

- Mô tả những nguy cơ trong các dịch vụ WLAN
- Mô tả những phương pháp làm giảm nhẹ các mối nguy hiểm trong dịch vụ WLAN
- Mô tả sự tiến triển của các công nghệ bảo mật trong WLAN
- Mô tả quá trình liên kết của các WLAN Client
- Mô tả quá trình tăng cường khả năng bảo mật của IEEE 802.1X
- Mô tả các kiểu WPA

Các mối đe dọa trên môi trường WLAN

“WAR DRIVERS”	HACKERS	EMPLOYEES
Find “Open” Networks; Use Them to Gain Free Internet Access	Exploit Weak Privacy Measures to View Sensitive WLAN Info and Even Break into WLANs	Plug Consumer-Grade APs/Gateways into Company Ethernet Ports to Create Own WLANs
		

Module 18-2

- Với những hệ thống IEEE 802.11b/g giá thành thấp, chúng ta không thể tránh được khả năng hacker sẽ có thêm những hệ thống WLAN không bảo mật để lựa chọn. Ta có thể dùng khá nhiều những phần mềm mã nguồn mở để thu thập vào khai thác những điểm yếu trong phương thức bảo mật WEP (Wired Equivalent Privacy) của chuẩn 802.11. Một số phần mềm sniffer cho phép những kỹ sư mạng có thể thu thập dữ liệu để phân tích, kiểm tra và chỉnh sửa những vấn đề tồn tại trong hệ thống mạng của họ. Tuy nhiên cũng chính những phần mềm này có thể sẽ được sử dụng bởi những hacker để dò tìm và khai thác các lỗ hổng bảo mật trên mạng.
- Thuật ngữ “war driving” ban đầu được dùng với nghĩa là dùng một thiết bị quét số điện thoại di động (cell phone) nhằm tìm ra một số điện thoại nào đó để khai thác. Giờ đây, thuật ngữ này lại lại được hiểu như việc dùng một laptop như một Client để dò tìm một hệ thống WLAN 802.11b/g nào đó.
- Hầu hết các thiết bị được bán ra hiện nay đều được tính hợp sẵn khả năng WLAN. Người dùng đầu cuối thường thì cũng không chỉnh những thông số mặc định của nhà sản xuất hoặc chỉ sử dụng chuẩn bảo mật WEP, điều này không tối ưu hóa được quá trình bảo mật trong mạng WLAN. Với việc kích hoạt chuẩn mã hóa WEP cơ bản hay thậm chí là không bảo mật, việc bị thu thập và lấy đi một số thông tin nhạy cảm như thông tin đăng nhập, số tài khoản và một số thông tin riêng tư khác là hoàn toàn có thể.

•Một rogue Access point là một Access point đặt trong môi trường mạng WLAN, Access point này được sử dụng để can thiệp vào sự vận hành bình thường của hệ thống mạng. Nếu một rogue Access point được thiết lập với từ khóa WEP đúng đang dùng trong mạng, dữ liệu phía người dùng có thể bị nghe lén. Một rogue Access point cũng có thể được cấu hình để cung cấp cho những người dùng không có quyền trên hệ thống những thông tin như địa chỉ MAC của các người dùng khác trong mạng cả mạng không dây và có dây, hay có thể thu thập và tạo ra những gói dữ liệu giả, hay thậm chí là chiếm quyền vào truy xuất vào các máy chủ. Kiểu thông dụng và đơn giản nhất để thiết lập một rogue Access point là được cài đặt bởi người dùng hợp lệ trong hệ thống. Những người dùng thiết lập các Access point để sử dụng cho mục tiêu gia đình trên hệ thống mạng doanh nghiệp mà không quan tâm đến vấn đề bảo mật sẽ tạo ra những nguy cơ bảo mật khá lớn.

Giảm nhẹ các mối đe dọa

Control and Integrity	Privacy and Confidentiality	Protection and Availability
Xác thực	Mã hóa	Ngăn ngừa xâm nhập (IPS)
Đảm bảo những client hợp lệ liên kết với những access point tin cậy.	Bảo vệ dữ liệu khi truyền và nhận.	Theo dõi và giảm nhẹ những truy xuất không được phép hay những truy xuất không hợp lệ.

Module 1B-4

- Chủ đề này mô tả quá trình làm giảm nhẹ các mối nguy hiểm về vấn đề bảo mật trên hệ thống WLAN
- Để bảo vệ hệ thống WLAN, yêu cầu phải thực hiện thông qua các bước sau:
 - Xác thực người dùng, mục tiêu nhằm đảm bảo những người dùng hợp pháp có thể truy xuất vào hệ thống mạng thông qua những Access point tin cậy.
 - Mã hóa, mục tiêu nhằm tạo sự riêng tư và bí mật
 - Triển khai hệ thống phát hiện xâm nhập (IDS – Intrusion Detection System) và hệ thống ngăn chặn xâm nhập (IPS – Intrusion Prevention System) để bảo vệ hệ thống mạng trước những nguy cơ bảo mật
- Một giải pháp cơ bản cho vấn đề bảo mật mạng không dây là triển khai tính năng xác thực và mã hóa để bảo vệ dữ liệu. Hai giải pháp này có thể được triển khai theo từng cấp độ tùy thuộc vào quy mô hệ thống mạng. Những hệ thống mạng doanh nghiệp lớn hơn cần có thêm những cấp độ bảo mật được mang lại bởi những thiết bị như IPS. Hiện tại IPS không những có khả năng phát hiện các cuộc tấn công vào mạng không dây mà còn có thể bảo vệ hệ thống mạng trước những người dùng không hợp pháp.

Quá trình phát triển các chuẩn bảo mật trên mạng LAN không dây

1997	2001	2003	2004 hiện tại
WEP <ul style="list-style-type: none"> ▪ Mã hóa cơ bản ▪ Xác thực không mạnh ▪ Khó tính, dễ bị bẽ gãy ▪ Không mở rộng ▪ Lọc MAC và SSID-cloaking được sử dụng để tăng cường bảo mật 	802.1x EAP <ul style="list-style-type: none"> ▪ Khóa động ▪ Cải tiến mã hóa ▪ Xác thực người dùng ▪ 802.1X EAP (LEAP, PEAP) ▪ RADIUS 	WPA <ul style="list-style-type: none"> ▪ Chuẩn hóa ▪ Cải tiến mã hóa ▪ Xác thực người dùng mạnh (ví dụ, LEAP, PEAP, EAP-FAST) 	802.11i / WPA2 <ul style="list-style-type: none"> ▪ Mã hóa AES mạnh ▪ Xác thực ▪ Quản lý khóa động

Module 18-5

• Hầu hết ngay khi các chuẩn bảo mật mới ra đời, các hacker sẽ cố gắng khai thác những điểm yếu trên những chuẩn này. Để chống lại quá trình đó, các chuẩn bảo mật lại liên tục được nâng cấp để tăng cường khả năng bảo mật. Chủ đề này sẽ mô tả quá trình phát triển của vấn đề bảo mật trong mạng WLAN.

• Ban đầu, bảo mật trong môi trường WLAN được định nghĩa dựa trên từ khóa WEP 64 bit cho cả 2 tiến trình mã hóa và xác thực. Từ khóa WEP 64 bit bao gồm 40 bit cho từ khóa thực sự và 24 bit cho Vector khởi tạo. Phương pháp xác thực này thực sự không mạnh và thậm chí có thể bị dàn xếp từ khóa giữa các người dùng. Bởi vì các từ khóa được quản lý một cách thủ công do vậy phương pháp này không thể mở rộng một cách linh động trên các hệ thống mạng lớn được. Các công ty cố gắng khắc phục yếu điểm này với một số kỹ thuật SSID và lọc địa chỉ MAC.

• SSID là tên dùng để xác định hệ thống mạng WLAN và là thông số có thể cấu hình được. Cả Client và Access point phải cùng sử dụng giống nhau giá trị SSID này để giao tiếp. Nếu Access point được cấu hình để broadcast giá trị SSID trên toàn hệ thống mạng, Client sẽ liên kết với Access point đó bằng giá trị SSID nhận được. Access point có thể được cấu hình để không broadcast giá trị SSID ra ngoài (SSID cloaking), điều này mang lại cấp độ bảo mật đầu tiên trên hệ thống mạng WLAN bởi các hacker sẽ gặp khó khăn hơn để xác định sự tồn tại của Access point này.

Để các client biết giá trị SSID của Access point, chuẩn 802.11 cho phép các client sử dụng một chuỗi rỗng trong phần SSID để yêu cầu các Access point broadcast giá trị SSID. Kỹ thuật này cũng đã làm cho việc bảo mật dùng phương pháp SSID không còn hiệu quả bởi các hacker có thể gởi ra các chuỗi rỗng này cho đến khi tìm được các Access point. Bên cạnh phương pháp dùng SSID, Access point cũng hỗ trợ việc bảo mật dựa trên kỹ thuật lọc địa chỉ MAC. Thông tin lọc địa chỉ sẽ được cấu hình bằng tay trên Access point để cho phép hoặc không cho phép dựa trên địa chỉ vật lý của các client. Tuy nhiên địa chỉ MAC có thể dễ dàng bị giả, do đó phương pháp lọc địa chỉ MAC không còn được xem là một đặc tính bảo mật nữa.

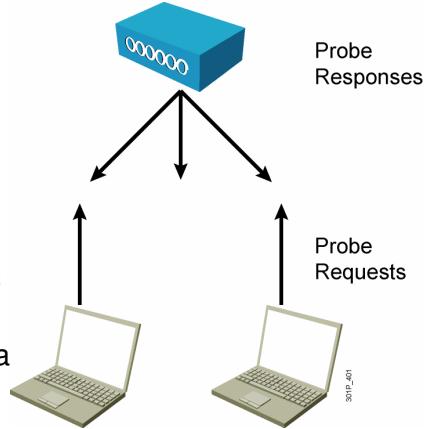
•Trong thời gian mà ủy ban 802.11 bắt đầu tiến trình nâng cấp khả năng bảo mật trên hệ thống WLAN, các hãng độc lập đã sớm triển khai các chuẩn bảo mật trên hệ thống mạng WLAN của họ. Cisco đã sớm phát triển chuẩn mã hóa WEP trên việc cải thiện thuật toán RC4. Cisco thực thi chuẩn TKIP (Temporal Key Integrity Protocol) để mã hóa trên từng gói dữ liệu và Cisco MIC (Message Integrity Check) để bảo vệ từ khóa WEP. Cisco cũng đã dùng chuẩn xác thực 802.11x từ môi trường dây dẫn sang môi trường không dây và tự động hóa các từ khóa sử dụng bằng Cisco LEAP (Lightweight Extensible Authentication Protocol) nhằm tập trung hóa cơ sở dữ liệu.

•Ngay sau khi Cisco triển khai các chuẩn bảo mật trên mạng WLAN, Wi-Fi Alliance đã đưa ra chuẩn WPA (Wi-Fi Protected Access) như một chuẩn tạm thời cho một phần của chuẩn bảo mật 802.11i đang được mong đợi dùng chuẩn xác thực 802.11x và cải thiện quá trình mã hóa WEP. Chuẩn TKIP mới ra đời tương tự như Cisco TKIP và Cisco MIC nhưng các chuẩn này không tương thích với nhau.

•Ngày nay, 802.11i đã được phê chuẩn và chuẩn bảo mật AES (Advanced Encryption Standard) đã thay thế WEP và được xem như một chuẩn bảo mật nhất để mã hóa dữ liệu. Những hệ thống IDS trên WLAN cũng được triển khai để xác định những cuộc tấn công và bảo vệ hệ thống mạng. Wi-Fi Alliance chứng nhận các thiết bị 802.11i dưới chuẩn WPA2.

Quá trình liên kết Client không dây

- Access point gửi ra các beacon thông báo SSID, tốc độ và các thông tin khác.
- Client dò tất cả các kênh.
- Client lắng nghe beacon và phản hồi với access point.
- Client sẽ liên kết với access point nào có sóng mạnh nhất.
- Client vẫn lắng nghe các beacon khác để có thể thực hiện tiến trình roaming
- Trong suốt quá trình liên kết, SSID, địa chỉ MAC và các thông số bảo mật sẽ được gửi đến access point.



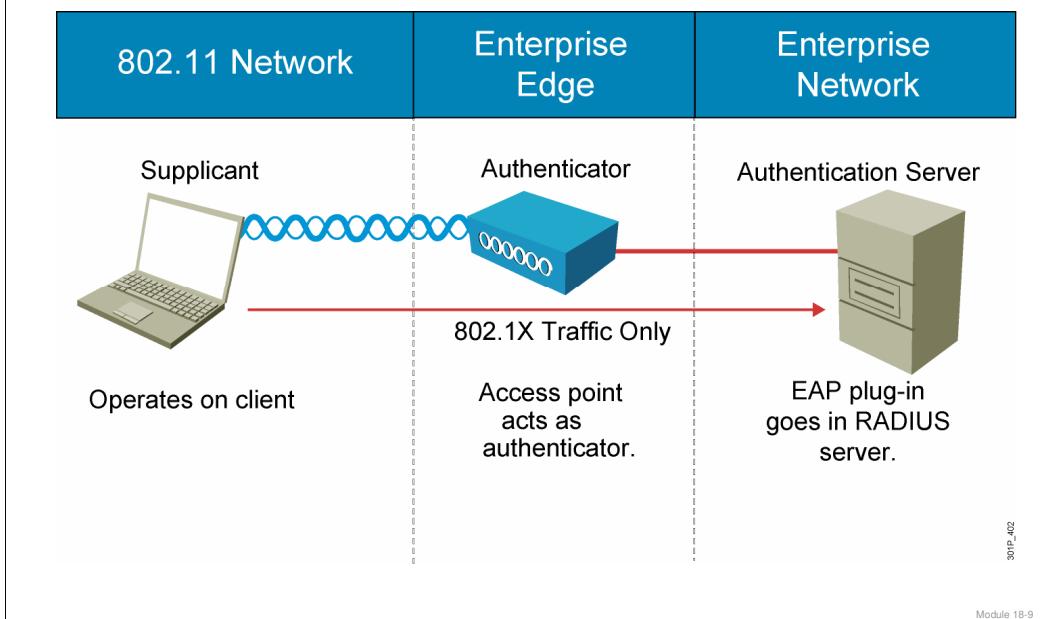
Module 18-7

Trong quá trình liên kết với Access point, các Access point sẽ gửi ra tín hiệu beacon để thông báo một số thông tin bao gồm SSID, tốc độ dữ liệu, và các thông tin khác. Các Client quét tất cả kênh truyền, lắng nghe các beacon và phản hồi lại cho các Access point. Client sẽ liên kết với Access point nào có tín hiệu sóng mạnh nhất. Nếu tín hiệu sóng yếu đi, client sẽ lập lại quá trình quét để liên kết với Access point khác (tiến trình này được gọi là roaming). Trong suốt quá trình liên kết, các thông số SSID, địa chỉ MAC và các thông số bảo mật sẽ được gửi lên Access point từ client và các Access point sẽ kiểm tra các thông số này.

Quá trình liên kết từ client đến Access point thực sự chỉ là quá trình thứ 2 trong tiến trình 2 bước. Tiến trình đầu tiên là xác thực, kế đến là liên kết, các client phải trải qua cả 2 tiến trình này để có thể trao đổi dữ liệu với các client khác thông qua Access point. Quá trình xác thực client xảy ra tại tiến trình đầu tiên không giống như quá trình xác thực trên mạng (nhập vào tên người dùng và mật khẩu để truy cập vào mạng). Quá trình xác thực client ở đây chỉ đơn giản là bước đầu tiên (kế theo là quá trình liên kết) giữa client và Access point để có thể thiết lập kết nối. Chuẩn 802.11 chỉ đưa ra 2 phương pháp để xác thực, xác thực mở (open authentication) và xác thực dùng khóa chia sẻ (shared key authentication). Chứng thực mở đơn thuần chỉ là quá trình trao đổi 4 gói dữ liệu hello ban đầu mà không cần phải kiểm tra bởi client hay Access point nhằm cho phép kết nối được dễ dàng thực hiện.

Chứng thực kiểu dùng khóa chia sẻ sử dụng một từ khóa được định nghĩa và sẵn giống nhau giữa client và Access point để kiểm tra. Từ khóa giống nhau này có thể có hoặc không sử dụng tiếp để mã hóa dữ liệu giữa client và Access point tùy thuộc vào cấu hình.

Cách vận hành của 802.1X trên mạng LAN không dây



- Access point đóng vai trò như người yêu cầu xác thực cho phép client thực hiện liên kết qua chuẩn xác thực mở. Access point sẽ đóng gói tất cả dữ liệu 802.11x yêu cầu xác thực và gửi đến server xác thực. Tất cả các dữ liệu khác truy xuất vào tài nguyên mạng sẽ bị khóa lại.
- Sau khi nhận được dữ liệu trả về từ RADIUS server, Access point sẽ đóng gói lại và chuyển về client. Mặc dù tiến trình xác thực này nhằm để xác định người dùng hợp lệ trên hệ thống mạng nhưng nó cũng có nghĩa là các client cũng đang xác thực server để đảm bảo client không truy xuất vào một server giả mạo.
- Trong khi một hệ thống mạng lớn sử dụng một server xác thực tập trung, các mạng doanh nghiệp nhỏ sẽ đơn thuần chỉ dùng Access point với từ khóa chia sẻ như một server để xác thực cho các client.

Mode WPA và WPA2

	WPA	WPA2
Enterprise mode (Kinh doanh, giáo dục, chính phủ)	Xác thực: IEEE 802.1X/EAP Mã hóa: TKIP/MIC	Xác thực : IEEE 802.1X/EAP Mã hóa: AES-CCMP
Personal mode (SOHO, sử dụng tại nhà hay cá nhân)	Xác thực: PSK Mã hóa: TKIP/MIC	Xác thực: PSK Mã hóa: AES-CCMP

Module 18-10

• Chuẩn WPA cung cấp khả năng xác thực được hỗ trợ thông qua chuẩn 802.1x và khóa chia sẻ (Pre-shared Key). WPA cung cấp khả năng mã hóa được hỗ trợ thông qua chuẩn TKIP. Chuẩn TKIP bao gồm MIC và PPK (Per-packet Keying) sử dụng thông qua “initialization vector hashing” và broadcast key rotation”.

• Khi so sánh với WPA, quá trình xác thực của WPA2 thì vẫn không thay đổi nhưng quá trình mã hóa được thực hiện bởi AES với giao thức AES-CCMP (AES Counter with CBC MAC Protocol).

• Enterprise mode

“Enterprise mode” là thuật ngữ dành cho những sản phẩm đã được kiểm tra về khả năng liên vận hành ở cả 2 kiểu PSK và 802.1X/ EAP cho chức năng xác thực. Chuẩn 802.1X yêu cầu phải có một AAA server khi được sử dụng. “Enterprise mode” được đưa ra nhằm đáp ứng nhu cầu trong môi trường mạng doanh nghiệp.

• Personal mode

“Personal mode” là thuật ngữ được sử dụng cho những sản phẩm đã được kiểm tra về khả năng liên vận hành duy nhất kiểu PSK cho chức năng xác thực. Quá trình này yêu cầu cấu hình PSK bằng tay trên cả Access point và client. PSK xác thực người dùng thông qua mật mã hoặc mã định danh trên cả client và Access point. Trong trường hợp này không cần phải sử dụng đến server xác thực. “Personal mode” được đưa ra nhằm đáp ứng nhu cầu trong môi trường SOHO.

Tóm tắt

- Một điều chắc chắn là các hacker sẽ xâm nhập vào mạng WLAN không bảo mật.
- Giải pháp cơ bản nhất để bảo mật WLAN là xác thực người dùng và mã hóa dữ liệu.
- Những chuẩn WLAN bao gồm các chuẩn bảo mật.
 - WEP
 - 802.1x EAP
 - WPA
 - 802.11i/WPA2
- Access point gửi ra các beacon thông báo SSID, tốc độ và các thông tin khác.

Module 18-11

Tóm tắt (tiếp theo.)

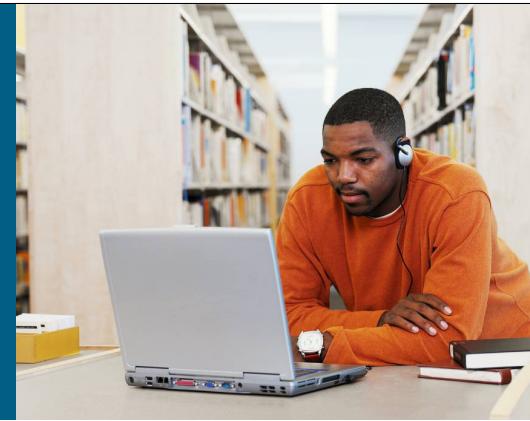
- Với chuẩn 802.1X access point đóng vai trò như một người đòi xác thực.
- WPA cung cấp xác thực qua IEEE 802.1X và PSK và bao gồm hai mode
 - Enterprise mode
 - Personal mode

Module 18-12



Module 18-13

Bài 19: Thực thi WLAN



Mạng không dây cục bộ (Wireless LANs)

© 2007 Cisco Systems, Inc. All rights reserved.

Module 19-1

Tổng quan

Có nhiều việc phải thiết lập hơn là chỉ lựa chọn các thông số mặc định theo tiêu chuẩn trong việc thực thi mạng WLAN. Việc sắp đặt vị trí của Access point ảnh hưởng đến hiệu quả của thông lượng truyền nhiều hơn là các chuẩn. Việc hiểu được các hiệu suất của mạng WLAN bị tác động như thế nào bởi các thông số như cách thiết lập mô hình, khoảng cách truyền sóng và cách thiết lập vị trí của Access point là một vấn đề hết sức quan trọng trong việc thực thi triển khai mạng WLAN.

Mục tiêu

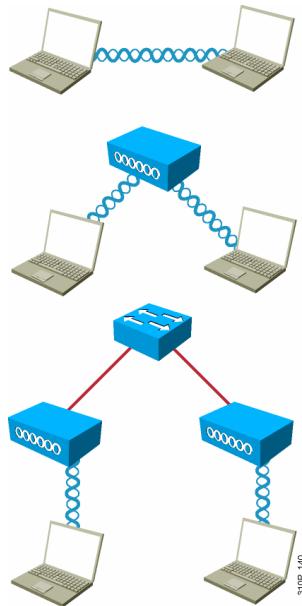
Sau khi hoàn tất bài học, bạn có khả năng mô tả những nhân tố ảnh hưởng đến việc thực thi mạng WLAN thông qua các nhiệm vụ sau:

- Mô tả mô hình IEEE 802.11
- Mô tả dịch vụ WLAN BSA
- Mô tả ảnh hưởng của khoảng cách và tốc độ trên dịch vụ WLAN
- Mô tả các nhân tố cần quan tâm trong việc thực thi triển khai các Access point
- Mô tả cách triển khai mạng WLAN cơ bản
- Mô tả các phương pháp để đưa mạng không dây vào laptop
- Mô tả các vấn đề phổ biến gặp phải và phương pháp khắc phục trên mạng WLAN

Xây dựng khối mô hình 802.11

Ad hoc mode:

- Independent Basic Service Set (IBSS)
 - Các client di động kết nối mà không cần access point ở giữa.



Infrastructure mode:

- Basic Service Set (BSS)
 - Các client di động dùng một access point để giao tiếp với nhau và với mạng có dây.
- Extended Service Set (ESS):
 - Hai hay nhiều kiểu BSS được kết nối với nhau.



© 2007 Cisco Systems, Inc. All rights reserved.

Module 19-2

• Chuẩn 802.11 cung cấp một số mô hình (mode) có thể sử dụng để xây dựng các khối mạng WLAN

• Ad hoc mode: IBSS (Independent Basic Service Set) là mô hình ad hoc mode. Các client di động kết gắng trực tiếp với nhau mà không thông qua thiết bị Access point trung gian ở giữa. Một số hệ điều hành như Windows cũng đã giúp cho mô hình peer-to-peer như thế này được dễ dàng thiết lập hơn. Kiểu thiết lập này cho thường được sử dụng cho các văn phòng nhỏ, nơi mà các laptop có thể nối không dây với các PC hay các laptop khác để đơn thuận là chia sẻ dữ liệu. Môi trường này có tầm phủ giới hạn, tất cả mọi người đều phải thấy nhau. Một yếu điểm trong môi trường này là khó khăn trong vấn đề bảo mật.

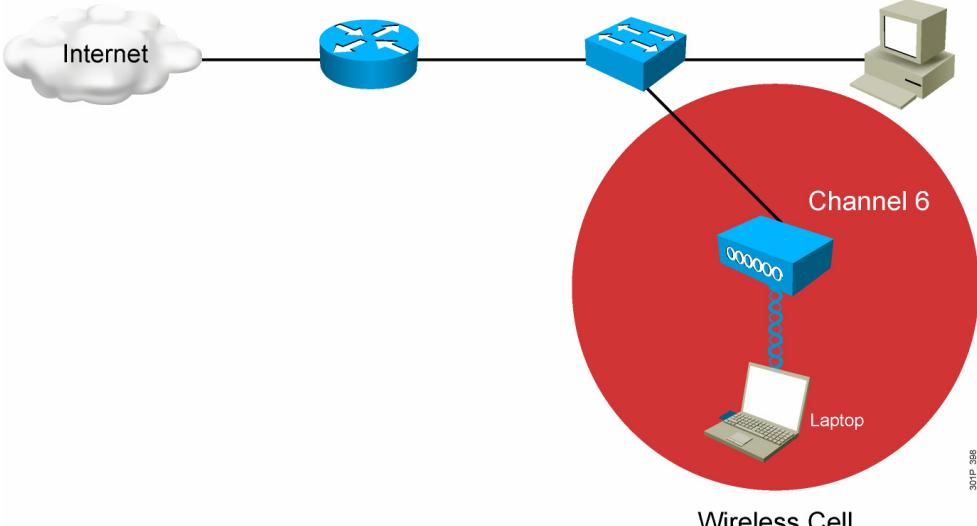
• Infrastructure mode: trong mode này, các client sẽ nối thông qua Access point. Infrastructure mode tồn tại dưới 2 hình thức:

- BSS (Basic Service Set): Trong mode này, tất cả các client chỉ sử dụng một Access point để nối với nhau hoặc để nối về mạng có dây. BSSID (Basic Service Set Identifier) là địa chỉ MAC của card radio trên Access point trong mode này. Trong khi BSS là mode cơ bản để xây dựng mô hình WLAN và BSS Access point được duy nhất xác định thông qua BSSID thì bản thân nguyên cả hệ thống WLAN sẽ dùng SSID để quảng bá sự tồn tại của nó với các client. SSID được xem như tên của hệ thống WLAN, có thể được cấu bởi người dùng và được tạo từ 32 ký tự có phân biệt chữ hoa và chữ thường.

- ESS (Extended Service Set): Là hệ thống mạng WLAN được mở rộng với hai hay nhiều hơn các BSS gắn kết với nhau thông qua hệ thống kết nối trung gian hoặc môi trường dây dẫn. ESS thông thường cũng sử dụng chung giá trị SSID để cung cấp khả năng roaming giữa Access point này và Access point khác mà người dùng không cần phải thiết lập lại cấu hình.

• Trên là những mô hình chuẩn được đưa ra bởi 802.11, tuy nhiên các mô hình khác như repeater, bridges và workgroup bridge là những mô hình mở rộng được đưa ra từ các hãng.

Mô hình BSA – Tầm phủ cơ bản



© 2007 Cisco Systems, Inc. All rights reserved.

Module 19-4

301P_388

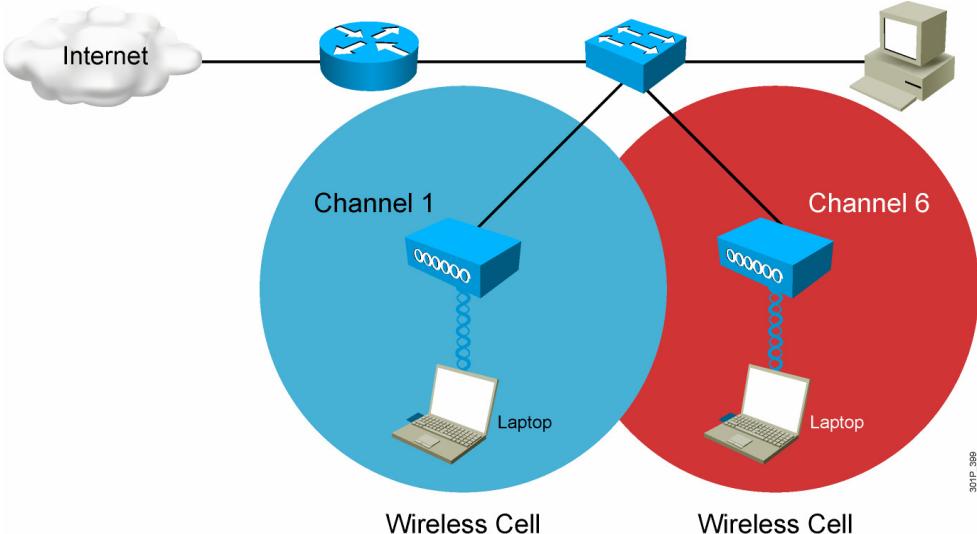
BSA (Basic Service Area) là một khu vực vật lý của tầm phủ sóng sóng radio được cung cấp bởi Access point trong mode BSS. Diện tích khu vực này tùy thuộc vào năng lượng sóng radio mà Access point phát ra. Những năng lượng này lại phục thuộc vào các yếu tố như công suất phát, loại anten, và các vật thể xung quanh ảnh hưởng đến sóng radio. Khu vực phủ sóng như vậy được biết đến như một cell. Vậy khi BSS là kiểu mô hình thì BSA lại được biết đến như một dạng vùng phủ sóng và hai thuật ngữ này có thể được dùng qua lại trong một khái niệm không dây cơ bản.

Access point sẽ được gắn vào backbone mạng Ethernet và giao tiếp với tất cả các thiết bị không dây khác trong khu vực cell. Access point được xem là master trong cell và điều khiển tất cả các lưu lượng luồng dữ liệu đến và từ hệ thống mạng. Các thiết bị từ xa sẽ không giao tiếp trực tiếp với nhau mà chỉ giao tiếp trực tiếp với Access point. Access point có thể được điều chỉnh về thông số kênh truyền và tên SSID duy nhất trên hệ thống mạng.

Access point broadcast tên của hệ thống mạng trong cell thông qua giá trị SSID qua các beacon. Các beacon được Access point broadcast nhằm thông báo sự tồn tại của dịch vụ không dây. Các giá trị SSID được sử dụng để cách ly về mặt luận lý các hệ thống WLAN. Giá trị này phải hoàn toàn giống nhau giữa Access point và các client. Tuy nhiên, các client có thể cấu hình không cần giá trị SSID (SSID rỗng) để có thể phát hiện tất cả các Access point và nhận giá trị SSID của một Access point cụ thể nào đó.

Một ví dụ phổ biến của tiến trình dò tìm là quá trình dò tìm được sử dụng bởi ứng dụng tích hợp sẵn WZC (Wireless Zero Configuration) khi mà một laptop được sử dụng tại một vị trí mới. Người dùng sẽ được hiển thị thông tin của dịch vụ không dây mới và được yêu cầu để kết nối hoặc được cung cấp các thông số về từ khóa để truy cập. Quá trình broadcast SSID có thể được ngưng kích hoạt trên Access point, nhưng sẽ làm người dùng không còn thấy được SSID trong beacon nữa.

Mô hình ESA – Tầm phủ mở rộng



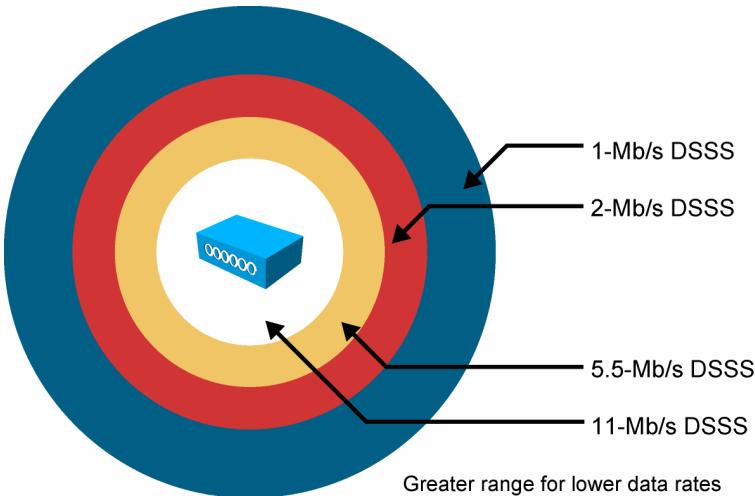
© 2007 Cisco Systems, Inc. All rights reserved.

Module 19-6

301P_389

- Nếu một cell không cung cấp đủ vùng phủ sóng, có thể đưa thêm bất kỳ các cell nào vào hệ thống mạng để mở rộng tầm phủ sóng. Tầm phủ sóng được tạo từ nhiều cell được gọi là ESA (Extended Service Area).
- Các chuẩn khuyến nghị rằng giữa các cell trong ESA nên phủ lên nhau khoảng từ 10% đến 15% để giúp người dùng có khả năng roaming mà không mất sóng. Trong hệ thống mạng không dây sử dụng cho voice, độ phủ lấp giữa các cell từ 15% đến 20% được khuyến nghị. Các cell nằm tại biên nên được thiết lập hoạt động tại những tần số không chồng lấp nhau để đạt được khả năng vận hành tốt nhất.

Tốc độ dữ liệu 802.11b



© 2007 Cisco Systems, Inc. All rights reserved.

301P_400
Module 19-7

- Các client WLAN có khả năng dịch chuyển tốc độ khi di chuyển. Kỹ thuật này cho phép cùng một client hoạt động ở tốc độ 11 Mbps chuyển sang tốc độ 5Mbps sau đó đến 2Mbps và cuối cùng vẫn có thể giao tiếp ở vùng ngoài cùng với tốc độ 1Mbps. Quá trình dịch chuyển tốc độ này xảy ra mà không làm mất đi kết nối mà người dùng đang có và người dùng không phải can thiệp gì vào quá trình này. Sự dịch chuyển tốc độ xảy ra trên từng quá trình truyền dẫn một, do đó Access point có khả năng hỗ trợ nhiều client hoạt động tại nhiều tốc độ khác nhau tùy vào vị trí đang có của từng client.
- Tốc độ truyền cao yêu cầu tín hiệu mạnh tại ngay đầu nhận, do vậy tốc độ càng thấp thì tầm truyền càng xa.
- Các client không dây luôn cố gắng giao tiếp với tốc độ truyền cao nhất.
- Các client sẽ chỉ giảm tốc độ nếu xảy ra lỗi trong quá trình truyền.
- Quá trình này cung cấp thông lượng truyền dẫn tối đa trong một cell mạng không dây. Hình trên biểu diễn cho chuẩn 802.11b, khái niệm này cũng tương tự cho chuẩn 802.11a và 802.11g.

Cấu hình Access Point

Thông số cơ bản:

- Địa chỉ IP, Subnet mask, và default gateway
- Giao thức không dây (chỉ 802.11g, 802.11a/b/g, 802.11a)
- Điều chỉnh kênh truyền – kênh 1, 6, hay 11
- Điều chỉnh công suất, hay thay thế anten

Thông số bảo mật:

- Xác định mạng qua SSID
- Phương thức xác thực, thường là WPA hay WPA2 PSK
- Phương pháp mã hóa, thường là TKIP, hay AES nếu phần cứng hỗ trợ

•Access point có thể được cấu hình dùng giao diện dòng lệnh (CLI) hay bằng phương pháp phổ biến hơn là giao diện đồ họa (GUI). Tuy nhiên cách cấu hình Access point ở những thông số cơ bản là giống nhau cho cả hai phương pháp. Các thông số cơ bản để cấu hình Access point bao gồm cấu hình SSID, kênh truyền RF đi kèm với các thông số tùy chọn như công suất, xác thực,... Các client cần ít thông số cấu hình hơn vì các card không dây có thể quét tất cả các tần số có thể (những card thuộc chuẩn 802.11b/g không thể quét được sóng ở tần số 5GHz) để định ra nơi cung cấp dịch vụ. Thường thì các client sẽ khởi tạo kết nối với giá trị SSID rỗng. Do vậy với thiết kế của chuẩn 802.11b, nếu sử dụng chuẩn xác thực mở, quá trình sẽ là “plug-and-play”. Khi chuẩn bảo mật được cấu hình dùng kiểu từ khóa chia sẻ (PSK) hay cũ hơn là chuẩn WEP hoặc như hiện tại ở chuẩn WPA, các từ mã buộc phải khớp giữa hai bên (Access point và client) để có thể giao tiếp.

•Tùy vào phần cứng của Access point được lựa chọn mà Access point có thể hoạt động trên cả hai băng tần ISM 2.4 GHz và UNII 5 GHz với sự hỗ trợ của cả ba chuẩn 802.11a/b/g. Khi các client chuẩn 802.11b sử dụng chung với các client chuẩn 802.11g, thông lượng truyền dữ liệu sẽ giảm bởi vì Access point phải duy trì thực thi giao thức RTS/CTS. Do vậy một môi trường chỉ có một loại client sẽ thông lượng truyền dữ liệu sẽ nhanh hơn.

•Sau khi cấu hình cơ bản các thông số không dây cho Access point, một số thông số cơ bản khác liên quan đến môi trường dây dẫn cũng phải được thiết lập như default router hay DHCP server. Với một hệ thống mạng LAN tồn tại sẵn, ta phải có một giá trị default router để ra hệ thống mạng bên ngoài và DHCP server để cung cấp địa chỉ IP cho các PCs trong mạng LAN.

Access point đơn giản sẽ đóng vai trò trung gian chuyển các giá trị này cho các client không dây khi kết nối vào. Và vì hệ thống được mở rộng thêm như, do vậy phải đảm bảo tầm địa chỉ DHCP đủ rộng để cấp cho tất cả các client.

Cá bước cấu hình hệ thống mạng không dây

Bước 1: Kiểm tra sự vận hành mạng có dây, DHCP, ISP.

Bước 2: Cài đặt access point.

Bước 3: Cấu hình access point – SSID, không bảo mật.

Bước 4: Cài đặt một client không dây – không bảo mật.

Bước 5: Kiểm tra sự vận hành mạng.

Bước 6: Cấu hình bảo mật – WPA với PSK.

Bước 7: Kiểm tra sự vận hành mạng.

- Quá trình cơ bản để thực thi một hệ thống mạng không dây (cũng như với tất cả các hệ thống mạng cơ bản khác) là từng bước cấu hình và kiểm tra.

- Trước khi thực hiện bất kỳ cấu hình nào về yếu tố không dây, kiểm tra hệ thống mạng có sẵn và các thức truy cập vào Internet cho các client trong mạng dùng dây.Thực thi mạng không dây với chỉ một Access point, một client và không có bất kỳ chuẩn bảo mật nào. Kiểm tra rằng client có thể nhận IP từ DHCP server, ping được default gateway và có thể truy cập Internet. Cuối cùng, cấu hình Access point với các chuẩn bảo mật WPA. Chỉ sử dụng WEP trong trường hợp phần cứng không hỗ trợ WPA.

Các client không dây

Wireless Zero Configuration (WZC):

- Mặc định trên hệ điều hành Windows
- Những tính năng hạn chế cho PSK
- Kiểm tra client dùng đúng kiểu mã hóa và password

Cisco Compatible Extensions Program

- Tăng tốc những đặc tính triển khai cho các client bên thứ 3
- Được triển khai bởi nhiều hãng khác nhau

Cisco Secure Services Client

- Chức năng client đầy đủ cho doanh nghiệp
- Cho mạng có dây và không dây

• Hiện tại, có khá nhiều phương pháp khác nhau để đưa các nhân tố không dây vào laptop. Phương pháp phổ biến nhất là sử dụng các thiết bị USB có hỗ trợ anten cố định và phần mềm kèm theo, cả hai sẽ cho phép tham gia mạng không dây đi kèm với một số tính năng về xác thực và mã hóa dữ liệu. Những laptop mới hiện giờ có nhiều hình thức khác nhau giúp truy cập vào mạng không dây. Những hệ điều hành mới của Windows được trang bị dịch vụ WZC cho phép khả năng “plug-and-play” bằng cách tìm ra các SSID và người dùng chỉ đơn giản nhập vào các từ khóa trong trường hợp sử dụng PSK, WEP hay WPA. Các tính năng cơ bản của WZC thích hợp cho các giải pháp văn phòng nhỏ.

• Một số hệ thống mạng lớn yêu cầu các client đầu cuối có nhiều tính năng hơn là những tính năng được cung cấp sẵn trong hệ điều hành. Bảng sau đây đã tóm tắt một số phiên bản và tính năng mà Cisco đưa thêm vào trong chương trình chứng nhận của mình từ năm 2000:

Version 1 (Security): Wi-Fi compliant, 802.1x, LEAP, Cisco Key Integrity Protocol.

Version 2 (Scaling): WPA, access point assisted roaming.

Version 3 (Performance and Security): WPA2, Wi-Fi Multimedia (WMM).

Version 4 (Voice over WLAN): Call Admission Control (CAC), voice metric.

Version 5 (Management and Intrusion Prevention System - IPS): Management Frame Protection, client reporting.

- Cho đến khi Cisco mang lại các tính năng đầy đủ gọi là Cisco Secure Service Client cho cả các client trong mạng không dây và có dây thì trước đó quản lý các client không dây và có dây theo những bộ chuẩn khác nhau. Lợi ích cho người dùng là chỉ sử dụng một chương trình client duy nhất cho vấn đề kết nối và bảo mật trên mạng không dây và có dây.

Một số vấn đề phổ biến trên mạng không dây

Vấn đề phổ biến nhất thường liên quan đến việc cấu hình không đúng:

- Kiểm tra access point chạy firmware mới nhất.
- Kiểm tra cấu hình kênh truyền. Thử các kênh 1, 6, 11.
- Kiểm tra client dùng đúng kiểu mã hóa và password.

Một số vấn đề phổ biến khác:

- Nhiều sóng
- Không kết nối
- Không kích hoạt sóng
- Đặt anten sai vị trí

• Trong quá trình cấu hình, có những nguyên nhân chủ yếu như sau dẫn đến các vấn đề trong môi trường WLAN:

– Cấu hình SSID trên client không khớp với trên Access point do khác nhau về phương pháp quét SSID hay do lỗi phân biệt chữ thường và chữ hoa.

– Cấu hình các chuẩn bảo mật không tương thích với nhau.

• Access point và các client phải khớp nhau trong phương pháp xác thực (EAP hay PSK) và phương pháp mã hóa (TKIP hay AES)

• Một số vấn đề khác có thể xuất phát từ việc liên quan đến vấn đề cấu hình tần số sóng, ví dụ:

– Tần số được cấu hình trên client và Access point có khớp nhau hay không (ISM 2.4 GHz hay UNII 5 GHz)?

– Anten ngoài đã được kết nối và phát đúng hướng hay chưa?

– Vị trí của Anten có quá cao hay quá thấp so với các client (quy chiếu khoảng 20 feet đối với client)?

– Các vật thể kim loại trong phòng có phản xạ sóng dẫn đến chất lượng truyền bị giảm đi hay không?

– Bạn có đang triển khai một hệ thống không dây vượt quá tầm với hay không?

Sửa lỗi mạng không dây

- Đặt access point ngay tại vị trí trung tâm.
- Tránh đặt gần các vật thể kim loại.
- Kiểm tra kết nối khi chưa kích hoạt tính năng bảo mật.
- Tránh nhiễu sóng với các thiết bị khác (bluetooth, viba,...)
- Nếu cầm phát sóng trong phạm vi rộng, cần dùng nhiều hơn một access point.
- Đảm bảo rằng access point sử dụng kênh truyền duy nhất, không trùng kênh với các thiết bị gần đó.

© 2007 Cisco Systems, Inc. All rights reserved.

Module 19-14

•Bước đầu tiên trong quá trình khắc phục sự cố trong mạng không dây là tách biệt hệ thống mạng không dây và môi trường dây dẫn. Tiếp đó là tách rời phần cấu hình mạng không dây với các vấn đề về sóng radio. Bắt đầu bằng quá trình kiểm tra cơ sở hạ tầng và các dịch vụ trên môi trường dây dẫn. Đảm bảo rằng các máy trong môi trường Ethernet có khả năng nhận đại chỉ từ DHCP server và có thể truy cập Internet.

•Kế tiếp, thực hiện kết nối giữa Access point và client tại cùng một địa điểm nhằm kiểm tra cấu hình và loại trừ các vấn đề về sóng radio. Luôn luôn bắt đầu từ chuẩn xác thực mở để thiết lập kết nối. Sau đó thực thi các chuẩn bảo mật mong muốn.

•Nếu các client có thể kết nối tại điểm này, vấn đề còn lại chỉ liên quan đến các vấn đề về sóng radio. Trước tiên phải xem xét thử có bất kỳ vật thể kim loại nào đặt trong khu vực phát sóng hay. Nếu có, ta có thể chuyển vật thể đi hoặc thay đổi vị trí của Access point. Nếu khoảng cách truyền là quá lớn, lưu ý là phải dùng thêm các Access point khác với cùng giá trị SSID nhưng truyền với tần số khác nhau . Cuối cùng là xem xét môi trường truyền sóng. Tương tự môi trường dây dẫn, mạng không dây cũng có thể bị nghẽn khi có quá nhiều lưu lượng dữ liệu.

• Nếu khả năng vận hành của hệ thống mạng có vẻ như liên quan đến một số khoảng thời gian trong ngày thì nguyên nhân là do hệ thống mạng bị can nhiễu từ các thiết bị khác. Ví dụ như khả năng vận hành của mạng chậm lại vào giờ trưa vì bị ảnh hưởng bởi tần số của lò vi sóng do các nhân viên sử dụng. Mặc dù hầu hết lò vi sóng chỉ ảnh hưởng đến kênh truyền số 11 thì một số lò vi sóng khác lại ảnh hưởng đến toàn bộ các kênh truyền. Một vấn đề khác ảnh hưởng đến sóng truyền là khi gặp các thiết bị sử dụng công nghệ điều chế kiểu nhảy tần (FHSS) như cordless phone. Do đó, có khá nhiều nguồn nhiễu khác nhau ảnh hưởng đến hệ thống WLAN, bởi vậy ban đầu, luôn luôn đặt Access point và client tại cùng một vị trí, sau đó di chuyển client xa dần cho đến khi có thể phát hiện được nguyên nhân. Hầu hết các phần mềm phía client đều cung cấp khả năng khắc phục sự cố bằng cách thể hiện độ mạnh yếu và chất lượng của sóng đối với các tần số liên quan.

Tóm tắt

- Mô hình 802.11 hoạt động trên nhiều mode khác nhau:
 - In ad hoc mode.
 - In infrastructure mode.

Tóm tắt (tt.)

- Access point có thể được cấu hình qua giao diện CLI hay GUI.
- Để triển khai hệ thống WLAN, nên thực hiện từng bước một.
- Có một vài dạng client không dây:
 - Wireless Zero Configuration
 - Cisco Compatible Extensions
 - Cisco Secure Services Client
- Ta có thể sửa lỗi mạng không dây bằng cách tách biệt mạng không dây và có dây.
- Tốc độ WLAN có thể bị ảnh hưởng bởi chuẩn, khoảng cách và vị trí đặt access point.



© 2007 Cisco Systems, Inc. All rights reserved.

Module 19-18