LÝ THUYẾT MẠNG MÁY TÍNH

COMPUTER NETWORKS HANDBOOK

Tặng các bạn sinh viên yêu quý của tôi

Nội dung tài liệu này được tôi biên soạn như là bản tóm tắt rất ngắn gọn các kiến thức cơ bản về mạng máy tính – phần lớn từ khóa học "CCNA: Introduction to Networks" của ® 2025 Cisco tại địa chỉ: https://www.netacad.com/courses/ccna-introduction-networks?courseLang=en-US.

Nếu bạn thấy tài liệu này hữu ích cho việc học tập, hãy động viên tôi bằng cách cài và đánh giá (vote, rate, comment trên Google Play Store) – cứ đánh giá thật (⋆ ⋆ ⋆ ⋆ ⋆ thì tốt mà ⋆ cũng không sao ☺), không cần khen quá mức, ứng dụng này của tôi nhé: https://play.google.com/store/apps/details?id=com.ngohaianh.memoryv2 ← Link tải app ☺ ☺ ☺ ☺ ☺

App này tôi viết hoàn toàn miễn phí, không có quảng cáo – chỉ là một thú vui viết code lúc rảnh rỗi của tôi, nhưng việc được tải về nhiều và có nhiều đánh giá tích cực trên Play Store cũng là niềm vui tinh thần rất lớn góp phần làm tôi có cảm hứng dạy hay hơn → trực tiếp hay gián tiếp đều có lợi cho các em. Do vậy ngoài việc cài trên thiết bị cá nhân thì các em có thể chia sẻ app này cho các bạn cùng trường, người quen... để cài giúp tôi nữa nhé, game này chơi giải trí cũng thú vị đó ☺ ☺ ☺

Mục lục

Chương 1

Mạng máy tính ngày nay

Mục tiêu

Sau khi hoàn thành chương này, bạn sẽ có thể trả lời các câu hỏi sau:

- Mạng ảnh hưởng như thế nào đến cuộc sống hàng ngày của chúng ta?
- Thiết bị đầu cuối và thiết bị mạng được sử dụng ra sao?
- Biểu diễn mạng là gì và chúng được sử dụng như thế nào trong các sơ đồ topo?
- Đặc điểm của các loại mạng phổ biến là gì?
- LAN và WAN kết nối Internet như thế nào?
- Bốn yêu cầu cơ bản của một mạng đáng tin cậy là gì?
- Các xu hướng như BYOD, cộng tác trực tuyến, video, và điện toán đám mây thay đổi cách chúng ta tương tác ra sao?
- Một số mối đe dọa bảo mật cơ bản và giải pháp cho mạng là gì?
- Có những cơ hội việc làm nào trong lĩnh vực mạng?

Thuật ngữ chính

Chương này sử dụng các thuật ngữ quan trọng sau:

- Máy chủ (server)
- Máy khách (client)
- Thiết bị đầu cuối (end device)
- Thiết bị trung gian (intermediary device)
- Topo (topology)
- Mạng văn phòng nhỏ hoặc gia đình (SOHO network)
- Mạng cục bộ (LAN)
- Mạng diện rộng (WAN)
- Internet
- Mạng nội bộ (intranet)
- Mạng ngoại bộ (extranet)
- Nhà cung cấp dịch vụ Internet (ISP)
- Đường thuê bao số (DSL)
- Kết nối di động (cellular connection)
- Kết nối vệ tinh (satellite connection)

- Kết nối quay số (dial-up)
- Mạng dữ liệu hội tụ (converged data network)
- Mạng chịu lỗi (fault-tolerant network)
- Mạng có khả năng mở rộng (scalable network)
- Chất lượng dịch vụ (QoS)
- Tính bảo mật (confidentiality)
- Tính toàn vẹn (integrity)
- Tính sẵn sàng (availability)
- Mang thiết bị cá nhân (BYOD)
- Điện toán đám mây (cloud computing)
- Mạng qua đường điện (powerline networking)
- Nhà cung cấp dịch vụ Internet không dây (WISP)

1.1 Giới thiệu

Xin chúc mừng! Chương này sẽ khởi đầu cho con đường sự nghiệp thành công của bạn trong lĩnh vực công nghệ thông tin bằng cách cung cấp cho bạn nền tảng kiến thức về cách tạo lập, vận hành và duy trì các mạng máy tính.

1.2 Mạng ảnh hưởng đến cuộc sống chúng ta

Mạng máy tính hiện diện ở khắp nơi. Chúng cung cấp cho chúng ta phương tiện để giao tiếp, chia sẻ thông tin và tài nguyên với những người ở cùng vị trí hoặc trên toàn thế giới. Để đáp ứng được điều này, mạng cần đến một tập hợp rộng lớn các công nghệ và quy trình có khả năng thích ứng nhanh chóng với các điều kiện và yêu cầu khác nhau.

1.2.1 Kết nối chúng ta

Trong tất cả những nhu cầu thiết yếu của con người, nhu cầu được tương tác với người khác chỉ đứng ngay sau nhu cầu được duy trì sự sống bằng không khí, nước, thức ăn và nơi ở. Trong thế giới ngày nay, nhờ có mạng, chúng ta được kết nối nhiều hơn bao giờ hết. Những người có ý tưởng có thể tức thời trao đổi với người khác để biến ý tưởng thành hiện thực. Các sự kiện thời sự và khám phá khoa học được lan truyền trên toàn cầu chỉ trong vài giây. Ngay cả những cá nhân ở cách nhau nửa vòng trái đất cũng có thể kết nối và cùng chơi trò chơi trực tuyến.

1.2.2 Không biên giới

Những tiến bộ trong công nghệ mạng có lẽ là một trong những thay đổi quan trọng nhất trong thế giới ngày nay. Chúng đang góp phần kiến tạo một thế giới nơi biên giới quốc gia, khoảng cách địa lý và giới hạn vật lý dần trở nên ít quan trọng, không còn là những rào cản lớn trong kết nối và hợp tác toàn cầu.

1.3 Các thành phần của mạng

Để một mạng có thể cung cấp dịch vụ và tài nguyên, cần có nhiều thành phần khác nhau cùng phối hợp hoạt động. Các thành phần này làm việc với nhau để đảm bảo tài nguyên được phân phối hiệu quả đến người dùng cần chúng.

1.3.1 Vai trò của thiết bị đầu cuối

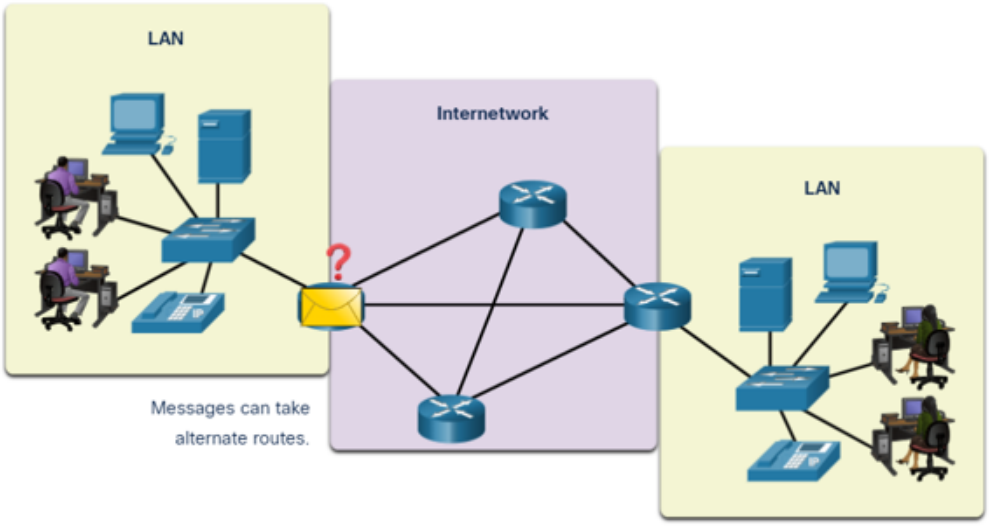
Nếu bạn muốn tham gia vào một cộng đồng trực tuyến toàn cầu, máy tính, máy tính bảng hoặc điện thoại thông minh của bạn trước tiên phải được kết nối vào một mạng, và mạng đó phải kết nối với Internet.

Thiết bị đầu cuối có thể đảm nhận một trong hai vai trò:

- **Máy khách (Client)**: sử dụng phần mềm để yêu cầu và nhận dịch vụ (ví dụ: trình duyệt web, ứng dụng email).

- **Máy chủ (Server)**: chạy phần mềm chuyên dụng để cung cấp dịch vụ cho nhiều máy khách (ví dụ: máy chủ email, máy chủ web, máy chủ file).

Một máy tính cũng có thể đồng thời chạy nhiều loại phần mềm máy khách khác nhau, chẳng hạn như vừa duyệt web, vừa kiểm tra email, vừa trò chuyện trực tuyến.



Hình 1.1: Luồng dữ liệu đi qua mạng.

Một thiết bị đầu cuối có thể là nguồn gửi hoặc đích đến của một thông điệp được truyền qua mạng, như minh họa trong Hình 1.1, trong đó dữ liệu từ một thiết bị đầu cuối sẽ đi qua mạng để đến đích là một thiết bị đầu cuối khác.

1.3.2 Mạng ngang hàng (Peer-to-Peer)

Trong mô hình ngang hàng, một máy tính có thể vừa đóng vai trò máy khách, vừa là máy chủ.

Ưu điểm:

- Dễ thiết lập, ít phức tạp
- Chi phí thấp, không cần thiết bị mạng chuyên dụng
- Phù hợp cho các tác vụ đơn giản như chia sẻ file, in ấn

Nhược điểm:

- Không có quản lý tập trung
- Không an toàn
- Không mở rộng được
- Khi một thiết bị vừa là máy khách vừa là máy chủ, hiệu năng có thể giảm

1.3.3 Thiết bị đầu cuối

Thiết bị đầu cuối là những thiết bị quen thuộc nhất đối với người dùng, chẳng hạn như máy tính, điện thoại thông minh, máy in mạng. Mỗi thiết bị đầu cuối có một địa chỉ duy nhất để phân biệt và giao tiếp. Trong quá trình truyền thông tin, một thiết bị đầu cuối có thể là **nguồn** hoặc **đích** của thông điệp.

1.3.4 Thiết bị trung gian

Thiết bị trung gian kết nối các thiết bị đầu cuối với nhau hoặc kết nối nhiều mạng lại với nhau. Chúng thực hiện các chức năng như:

- Định tuyến dữ liệu đến đúng đích
- Quản lý luồng thông tin
- Bảo mật và lọc dữ liệu
- Khuếch đại hoặc tái tạo tín hiệu truyền thông

Ví dụ: Router, Switch, Firewall.

1.3.5 Phương tiện truyền dẫn

Thông tin trong mạng được truyền qua môi trường truyền dẫn. Có ba loại chính:

- **Dây đồng (cáp xoắn đôi, cáp đồng trục)**: dữ liệu được mã hóa thành tín hiệu điện.
- **Cáp quang**: dữ liệu được mã hóa thành xung ánh sáng truyền qua sợi thủy tinh hoặc nhựa.
- **Truyền dẫn không dây**: dữ liệu được truyền bằng sóng điện từ trên các tần số nhất định.

Mỗi loại môi trường có đặc tính và ưu điểm riêng, phù hợp với những mục đích sử dụng khác nhau.

1.4 Biểu diễn và topo mạng

Cơ sở hạ tầng mạng thường được mô tả bằng các ký hiệu chuẩn để biểu diễn thiết bị và bằng các sơ đồ để thể hiện sự kết nối giữa chúng. Việc hiểu rõ các ký hiệu và sơ đồ này là một phần quan trọng để nắm bắt cách thức truyền thông trong mạng.

1.4.1 Biểu diễn mạng

Các kiến trúc sư và quản trị viên mạng cần có khả năng trình bày mạng của họ một cách trực quan. Họ phải dễ dàng thấy được thiết bị nào kết nối với thiết bị nào, vị trí của chúng, và cách chúng kết nối với nhau.

Trong sơ đồ mạng, các ký hiệu thường được sử dụng để biểu diễn:

- Máy tính cá nhân (PC), máy chủ (Server)
- Thiết bị mạng như Router, Switch, Access Point
- Kết nối mạng (cáp hoặc kết nối không dây)

Các sơ đồ này giúp việc thiết kế, quản lý và xử lý sự cố mạng trở nên dễ dàng hơn.

1.4.2 Sơ đồ Topo

Sơ đồ topo là tài liệu bắt buộc đối với bất kỳ ai làm việc với mạng. Chúng cung cấp bản đồ trực quan về cách mạng được kết nối. Có hai loại chính:

- **Sơ đồ topo vật lý (Physical topology)**: minh họa vị trí vật lý của thiết bị trung gian, vị trí đặt cáp, và bố trí trong phòng.

- **Sơ đồ topo logic (Logical topology)**: minh họa cách dữ liệu di chuyển trong mạng và cách các thiết bị "nhìn thấy" nhau về mặt kết nối logic.

Các sơ đồ này là nền tảng giúp hiểu cấu trúc mạng từ mức cơ bản đến phức tạp. Nếu bạn tìm kiếm trên Internet cụm từ "network topology diagrams" (đặc biệt có thêm từ "Cisco"), bạn sẽ thấy nhiều ví dụ sử dụng các biểu tượng quen thuộc trong ngành.

1.5 Các loại mạng phổ biến

Mạng có thể được phân loại theo nhiều cách, bao gồm kích thước, vị trí địa lý, hoặc chức năng. Dù là loại nào, các nguyên tắc cơ bản về mạng đều được áp dụng chung.

1.5.1 Mạng với nhiều quy mô

Mạng có nhiều kích thước khác nhau, từ đơn giản chỉ có hai máy tính đến phức tạp với hàng triệu thiết bị kết nối.

- **Mạng gia đình nhỏ**: cho phép chia sẻ máy in, tài liệu, hình ảnh, nhạc.
- **Mạng SOHO (Small Office/Home Office)**: cho phép nhân viên làm việc tại nhà hoặc văn phòng từ xa, phục vụ thương mại nhỏ, trao đổi với khách hàng.
- **Mạng vừa và lớn**: cung cấp lưu trữ tập trung, email, nhắn tin nhanh, cộng tác trong doanh nghiệp; kết nối ra Internet để cung cấp sản phẩm/dịch vụ cho khách hàng.
- **Internet**: mạng lớn nhất, đúng nghĩa là "mạng của các mạng" (network of networks), kết nối vô số mạng công cộng và riêng tư.

Trong một số mạng nhỏ, thiết bị có thể vừa làm máy khách vừa làm máy chủ, gọi là *mạng ngang hàng (peer-to-peer)*.

1.5.2 Mạng LAN và WAN

- **LAN (Local Area Network)**: mạng cục bộ, trong một phạm vi nhỏ như văn phòng, trường học, gia đình. LAN thường do một tổ chức hoặc cá nhân sở hữu, quản lý, tốc độ cao.
- **WAN (Wide Area Network)**: kết nối nhiều LAN trên phạm vi rộng (giữa thành phố, quốc gia, châu lục). WAN thường do nhiều nhà cung cấp dịch vụ vận hành, tốc độ thường chậm hơn LAN.

1.5.3 Internet

Internet là tập hợp toàn cầu của các mạng liên kết (LAN và WAN). Nó được vận hành nhờ sự hợp tác của nhiều tổ chức chuẩn hóa và quản lý, bao gồm:

- **IETF (Internet Engineering Task Force)**
- **ICANN (Internet Corporation for Assigned Names and Numbers)**
- **IAB (Internet Architecture Board)**

1.5.4 Mạng nội bộ và ngoại bộ

- **Intranet**: mạng riêng của một tổ chức, kết nối các LAN/WAN nội bộ, chỉ cho phép nhân viên hoặc người được ủy quyền truy cập.
- **Extranet**: mở rộng từ intranet, cung cấp quyền truy cập an toàn cho những người ngoài tổ chức nhưng có nhu cầu, ví dụ như nhà cung cấp hoặc đối tác kinh doanh.

1.6 Kết nối Internet

Thiết bị đầu cuối như máy tính và điện thoại thông minh có thể kết nối vào mạng theo nhiều cách khác nhau, bao gồm cả có dây và không dây. Các kiểu kết nối này cũng được dùng để kết nối các thiết bị trung gian với nhau.

1.6.1 Công nghệ truy cập Internet

Người dùng gia đình, nhân viên làm việc từ xa và các văn phòng nhỏ thường cần kết nối với nhà cung cấp dịch vụ Internet (ISP). Các lựa chọn phổ biến gồm:

- Kết nối băng thông rộng bằng cáp (Cable broadband)
- Kết nối băng thông rộng DSL (Digital Subscriber Line)
- Mạng WAN không dây
- Dịch vụ di động (3G/4G/5G)

Doanh nghiệp thường cần kết nối tốc độ cao và đáng tin cậy, ví dụ: Business DSL, leased line, Metro Ethernet.

1.6.2 Kết nối Internet cho gia đình và văn phòng nhỏ

- **Cable**: sử dụng cùng loại cáp với dịch vụ truyền hình cáp, cung cấp băng thông cao, độ sẵn sàng cao, kết nối luôn mở.
- **DSL**: cung cấp băng thông cao, chạy trên đường dây điện thoại. Thường dùng loại bất đối xứng (ADSL) với tốc độ tải xuống nhanh hơn tải lên.
- **Cellular**: sử dụng mạng di động, chỉ cần có sóng di động là có thể truy cập Internet. Hiệu năng phụ thuộc thiết bị và trạm phát sóng.
- **Satellite**: phù hợp ở vùng xa xôi, cần chảo vệ tinh với đường truyền thẳng đến vệ tinh.
- **Dial-up**: rẻ, dùng đường dây điện thoại để kết nối, tốc độ thấp.

1.6.3 Mạng hội tụ

Trước đây, các mạng dữ liệu, mạng thoại và mạng video tồn tại tách biệt. Mỗi loại mạng sử dụng công nghệ, quy tắc và tiêu chuẩn riêng. Ngày nay, tất cả được hợp nhất thành một **mạng hội tụ**, có khả năng truyền tải nhiều loại dịch vụ trên cùng cơ sở hạ tầng.

1.7 Mạng đáng tin cậy

Mạng là một nền tảng để phân phối nhiều loại dịch vụ cho người dùng theo cách đáng tin cậy, hiệu quả và an toàn. Khi hàng tỷ người trên thế giới dựa vào mạng để làm việc và học tập, độ tin cậy trở thành yêu cầu bắt buộc.

1.7.1 Kiến trúc mạng

Khái niệm **kiến trúc mạng** bao gồm hạ tầng vật lý (thiết bị, cáp), công nghệ hỗ trợ, và các giao thức điều khiển việc truyền dữ liệu. Ngày nay, mạng không chỉ truyền dữ liệu, mà còn kết nối con người, thiết bị và thông tin trong một môi trường hội tụ phong phú.

1.7.2 Mạng chịu lỗi (Fault Tolerance)

Một mạng chịu lỗi là mạng có thể hạn chế số lượng thiết bị bị ảnh hưởng khi xảy ra sự cố và phục hồi nhanh chóng. Đặc điểm chính:

- Có nhiều đường truyền giữa nguồn và đích (**redundancy**).
- Nếu một đường truyền bị lỗi, dữ liệu được tự động định tuyến qua đường khác.
- Sử dụng công nghệ chuyển mạch gói (packet switching), trong đó gói tin có thể đi qua các tuyến đường khác nhau để đến cùng một đích.

1.7.3 Khả năng mở rộng (Scalability)

Mạng có khả năng mở rộng có thể nhanh chóng hỗ trợ thêm người dùng và ứng dụng mà không ảnh hưởng đến hiệu năng hiện tại. Nhờ tuân thủ các tiêu chuẩn và giao thức, các nhà sản xuất phần cứng/phần mềm có thể phát triển sản phẩm mới mà vẫn tương thích.

1.7.4 Chất lượng dịch vụ (QoS)

QoS đảm bảo rằng những loại dữ liệu quan trọng như thoại, video trực tuyến được ưu tiên xử lý, trong khi dữ liệu ít quan trọng hơn được xử lý sau. Điều này giúp trải nghiệm người dùng ổn định và đáng tin cậy.

1.7.5 Bảo mật mạng (Security)

Mạng phải đảm bảo an toàn cho:

- **Hạ tầng mạng**: bảo vệ thiết bị vật lý, ngăn chặn truy cập trái phép vào phần mềm quản lý.
- **Thông tin**: bảo vệ dữ liệu lưu trữ và truyền trên mạng khỏi bị đánh cắp hoặc sửa đổi.

Bảo mật là một trong những yếu tố then chốt của mạng đáng tin cậy, cả trong môi trường cá nhân lẫn doanh nghiệp.

Tóm tắt

- Mạng là một phần thiết yếu trong cuộc sống hiện đại, cho phép mọi người giao tiếp, học tập, làm việc và giải trí.
- Mạng có thể ở quy mô nhỏ (mạng gia đình) hoặc lớn (mạng doanh nghiệp, mạng toàn cầu).
- Internet kết nối hàng triệu mạng nhỏ lại, trở thành hạ tầng thông tin toàn cầu.
- Các thiết bị mạng bao gồm: thiết bị đầu cuối (end devices), thiết bị trung gian (intermediate devices) và phương tiện truyền (media).
- Kiến trúc mạng hiện đại dựa trên các nguyên tắc: khả năng chịu lỗi, khả năng mở rộng, bảo mật, và cung cấp dịch vụ chất lượng.

- Các xu hướng mới như BYOD, điện toán đám mây, mạng xã hội, IoT đang định hình cách mạng được sử dụng.

Câu hỏi ôn tập

1. **Ba cách mạng ảnh hưởng đến cuộc sống hàng ngày:**
   - Giúp liên lạc dễ dàng qua email, chat, gọi video.
   - Cho phép học tập và làm việc trực tuyến.
   - Hỗ trợ giải trí qua phim, nhạc, trò chơi trực tuyến.
2. **Khác biệt giữa mạng gia đình và mạng doanh nghiệp:**
   - **Mạng gia đình**: nhỏ, ít thiết bị, chủ yếu để truy cập Internet, chia sẻ file và giải trí.
   - **Mạng doanh nghiệp**: quy mô lớn, hỗ trợ nhiều người dùng, có máy chủ, bảo mật, dịch vụ phức tạp, độ tin cậy cao.
3. **Internet và mạng nội bộ:**
   - **Internet**: mạng toàn cầu, kết nối hàng triệu mạng con, ai cũng có thể truy cập.
   - **Mạng nội bộ (LAN/Intranet)**: chỉ dùng trong một tổ chức hoặc khu vực, thường bảo mật hơn và không công khai.
4. **Đặc điểm giúp mạng hiện đại mạnh mẽ và đáng tin cậy:**
   - Khả năng chịu lỗi.
   - Khả năng mở rộng.
   - Chất lượng dịch vụ (QoS).
   - Bảo mật dữ liệu và quyền truy cập.
5. **Ví dụ IoT thay đổi cách con người tương tác với công nghệ:**
   - Nhà thông minh: điều khiển đèn, điều hòa, khóa cửa bằng điện thoại.
   - Thiết bị đeo thông minh: đồng hồ theo dõi sức khỏe, gửi dữ liệu lên ứng dụng.

1.8 Thuật ngữ cần nhớ

Mạng (Network) Tập hợp các thiết bị kết nối với nhau để chia sẻ dữ liệu, tài nguyên (máy in, lưu trữ), dịch vụ (web, email) và ứng dụng.

Thiết bị đầu cuối (End Device/Host) Điểm tạo ra hoặc tiêu thụ dữ liệu trên mạng, ví dụ: PC, laptop, smartphone, máy in mạng, camera IP. Mỗi host thường có địa chỉ IP riêng.

Thiết bị trung gian (Intermediary Device) Thiết bị chuyển tiếp, điều khiển hoặc lọc lưu lượng giữa các host/mạng: switch, router, firewall, access point, modem, load balancer.

Phương tiện truyền (Network Media) Con đường vật lý/vô tuyến để dữ liệu di chuyển: cáp đồng xoắn đôi (UTP/STP), cáp quang, sóng vô tuyến (Wi-Fi, 4G/5G).

Giao diện/ Cổng (Interface/Port) Điểm kết nối logic hoặc vật lý trên thiết bị mạng (ví dụ `GigabitEthernet0/1`); dùng để gắn cáp, cấu hình địa chỉ và truyền khung/gói.

Địa chỉ IP (IP Address) Định danh logic của thiết bị trong mạng lớp 3 (IPv4 32-bit, IPv6 128-bit); cho phép định tuyến gói tin đến đúng đích.

Cổng mặc định (Default Gateway) Địa chỉ IP của router mà host gửi gói khi đích nằm ngoài mạng con cục bộ.

DNS (Domain Name System) Hệ thống phân giải tên miền (ví dụ `www.example.com`) thành địa chỉ IP tương ứng để ứng dụng có thể kết nối.

DHCP (Dynamic Host Configuration Protocol) Giao thức tự động cấp phát địa chỉ IP, subnet mask, default gateway, DNS cho host, giảm lỗi cấu hình thủ công.

Gói tin (Packet) Đơn vị dữ liệu ở tầng Mạng (L3) gồm header (địa chỉ IP nguồn/đích, TTL, . . .) và payload; có thể bị phân mảnh/định tuyến qua nhiều mạng.

Khung (Frame) Đơn vị dữ liệu ở tầng Liên kết dữ liệu (L2) được truyền trên môi trường; chứa địa chỉ MAC nguồn/đích, FCS/CRC để phát hiện lỗi.

Giao thức (Protocol) Tập quy tắc định nghĩa cách thiết bị giao tiếp (định dạng bản tin, thứ tự trao đổi, xử lý lỗi), ví dụ: HTTP, TCP, IP, 802.11.

Bộ giao thức TCP/IP (TCP/IP Protocol Suite) Tập hợp các giao thức chuẩn công nghiệp vận hành Internet, gồm các lớp: Truy cập mạng, Internet (IP), Vận chuyển (TCP/UDP), Ứng dụng.

Mạng LAN (Local Area Network) Mạng phạm vi nhỏ (nhà, phòng ban, tòa nhà), băng thông cao, độ trễ thấp, thường do một tổ chức quản trị.

Mạng WAN (Wide Area Network) Kết nối các LAN cách xa về địa lý (qua nhà cung cấp dịch vụ), băng thông đa dạng, chi phí theo thuê bao/đường truyền.

Internet "Mạng của các mạng" — hạ tầng toàn cầu kết nối hàng triệu mạng con dựa trên TCP/IP; cung cấp các dịch vụ web, email, DNS, . . .

Intranet Mạng riêng nội bộ của tổ chức (dựa trên công nghệ Internet/TCP-IP) không công khai ra ngoài, dùng cho ứng dụng, dữ liệu nội bộ.

Extranet Phần mở rộng có kiểm soát của intranet cho đối tác/khách hàng/nhà cung cấp truy cập, thông qua cơ chế bảo mật (ví dụ VPN, cổng ident).

ISP (Internet Service Provider) Nhà cung cấp dịch vụ kết nối Internet/đường truyền (cáp quang, DSL, cáp đồng trục, di động) cho cá nhân/tổ chức.

Băng thông (Bandwidth) Khả năng mang dữ liệu tối đa của đường truyền (bit/s). Băng thông lý thuyết ≠ thông lượng thực tế do overhead, tranh chấp, lỗi.

Thông lượng (Throughput) Lượng dữ liệu hữu ích truyền thành công mỗi đơn vị thời gian (bit/s), phản ánh hiệu năng thực tế quan sát được.

Độ trễ (Latency) Thời gian trễ từ khi gửi đến khi nhận; bị ảnh hưởng bởi truyền dẫn, xử lý, hàng đợi, lan truyền đường dài.

QoS (Quality of Service) Cơ chế ưu tiên và đảm bảo hiệu năng cho lưu lượng quan trọng (thoại/video) qua xếp loại (classification), đánh dấu (marking), xếp hàng (queuing), shaping/policing.

Khả năng chịu lỗi (Fault Tolerance) Tính chất mạng tiếp tục hoạt động (dù suy giảm) khi một phần hạ tầng gặp sự cố, nhờ dự phòng (redundancy) và hội tụ nhanh.

Khả năng mở rộng (Scalability) Mạng có thể tăng quy mô người dùng/thiết bị/dịch vụ mà vẫn duy trì hiệu năng và tính quản trị hợp lý.

Bảo mật (Security) Bảo vệ tính **bí mật** (confidentiality), **toàn vẹn** (integrity), **khả dụng** (availability) của dữ liệu/dịch vụ; áp dụng kiểm soát truy cập, mã hóa, tường lửa, IPS/IDS, chính sách.

BYOD (Bring Your Own Device) Xu hướng người dùng dùng thiết bị cá nhân truy cập tài nguyên doanh nghiệp; yêu cầu chính sách truy cập, tách vùng, NAC, MDM/MAM.

Điện toán đám mây (Cloud Computing) Mô hình cung cấp tài nguyên CNTT qua mạng; mô hình dịch vụ: **IaaS** (hạ tầng), **PaaS** (nền tảng), **SaaS** (ứng dụng); mô hình triển khai: public/private/hybrid.

IoT (Internet of Things) Mạng các thiết bị cảm biến/điều khiển kết nối (nhà thông minh, công nghiệp, y tế); yêu cầu kết nối không dây, địa chỉ hóa lớn (IPv6), bảo mật đầu-cuối.

Mạng hội tụ (Converged Network) Kết hợp thoại, video, dữ liệu trên cùng hạ tầng IP thay vì các mạng tách rời; cần QoS và năng lực xử lý phù hợp.

SOHO (Small Office/Home Office) Mạng quy mô nhỏ (văn phòng nhỏ/nhà), thiết bị hợp nhất (router Wi-Fi, switch tích hợp), tập trung vào đơn giản, chi phí thấp.

Sơ đồ/ Tô-pô mạng (Topology) Bố cục kết nối giữa các thiết bị; **vật lý** (cách đi dây) và **logic** (cách dữ liệu/luồng phát tán).

Điện lực hoá mạng (Powerline Networking) Tận dụng dây điện AC hiện hữu để truyền dữ liệu trong gia đình (cần adapter chuyên dụng); tiện triển khai nơi khó đi dây mạng.

Điểm truy cập không dây (Access Point/AP) Thiết bị nối các client Wi-Fi vào mạng có dây; có thể kết hợp router, switch, tường lửa trong thiết bị SOHO.

Firewall (Tường lửa) Thiết bị/phần mềm lọc lưu lượng theo chính sách (stateful, ứng dụng), ngăn truy cập trái phép, tạo ranh giới trust (perimeter/segment).

Chương 2

Cấu hình cơ bản cho switch và thiết bị đầu cuối

Mục tiêu

Sau khi hoàn thành chương này, bạn sẽ có thể:

- Mô tả các **cách truy cập** thiết bị Cisco IOS (Console, AUX, VTY/SSH).
- Phân biệt các **chế độ làm việc** của IOS (user EXEC, privileged EXEC, global configuration, mode con).
- Sử dụng các **lệnh cơ bản** để dẫn hướng, tra cứu trợ giúp, và chỉnh sửa trong CLI.
- **Đặt tên thiết bị**, cấu hình `banner`, `password`, bật `service password-encryption`, và lưu cấu hình.
- Cấu hình **địa chỉ IP** cho thiết bị đầu cuối (PC) và **SVI** trên switch; đặt **default gateway** cho quản trị từ xa.
- Thiết lập **truy cập từ xa an toàn** bằng `SSH` trên switch/router; so sánh SSH với Telnet.
- Xác minh hoạt động mạng với `ping`, `traceroute`, và các lệnh `show`.
- Áp dụng các **thực hành bảo mật cơ bản** để bảo vệ thiết bị và truy cập.

Thuật ngữ chính

- Cisco IOS
- Console
- VTY
- SSH / Telnet
- User EXEC / Privileged EXEC
- Global Configuration
- Subconfiguration Mode
- Hostname
- Banner (MOTD, login)
- Running-config / Startup-config
- NVRAM / RAM / Flash
- Service password-encryption
- Enable secret / enable password
- Line console / line vty
- Username / local database
- Interface VLAN 1 (SVI)

- Default gateway
- DHCP / tĩnh (static)
- ICMP ping / traceroute
- show / debug (giới thiệu)

2.1 Giới thiệu

Chương này hướng dẫn các bước **khởi tạo** và **cấu hình cơ bản** cho switch và thiết bị đầu cuối để một mạng nhỏ có thể hoạt động: đặt tên, bảo mật truy cập, cấu hình địa chỉ IP, bật quản trị từ xa và kiểm tra kết nối. Phần lớn thao tác được thực hiện trên **CLI của Cisco IOS**.

2.2 Tổng quan về truy cập và thao tác trong IOS

2.2.1 Các phương thức truy cập

- **Console**: kết nối trực tiếp cổng `console` của thiết bị bằng cáp console; hoạt động kể cả khi thiết bị chưa có địa chỉ IP. Thường dùng cho cấu hình ban đầu hoặc khôi phục.
- **VTY (Telnet/SSH)**: truy cập từ xa qua mạng IP. **SSH** là lựa chọn khuyến nghị vì mã hoá lưu lượng; **Telnet** gửi thông tin dạng rõ, không an toàn.
- **AUX** (nếu có): cổng dự phòng qua modem/quay số (ít dùng trong mạng hiện đại).

2.2.2 Các chế độ trong IOS

- **User EXEC** (`Switch>`) – thao tác quan sát cơ bản, lệnh `show` giới hạn.
- **Privileged EXEC** (`Switch#`) – quyền cao hơn, có thể dùng `show`, `copy`, `debug`, `reload`. Vào bằng `enable`.
- **Global Configuration** (`Switch(config)#`) – cấu hình toàn cục. Từ đây vào các **chế độ con** như `(config-line)#`, `(config-if)#`, `(config-vty)#`, v.v.

2.2.3 Dẫn hướng và trợ giúp

- **Dấu hỏi** `?`: trợ giúp theo ngữ cảnh. Ví dụ `show ?` liệt kê các từ khoá hợp lệ sau `show`.
- **Hoàn thành lệnh**: gõ một phần rồi nhấn `Tab`.
- **Phím tắt** hữu ích: `Ctrl+A/E` đi về đầu/cuối dòng; `Ctrl+U/W` xoá dòng/từ; `Ctrl+Z` quay lại `EXEC`; `Up/Down` duyệt lịch sử lệnh.
- **Dấu gạch chéo /** và **dấu cách** để nạp đối số. Dấu `?` có thể đặt ở giữa để xem gợi ý tiếp theo.

2.2.4 Tập tin cấu hình và lưu trữ

- **running-config**: cấu hình đang chạy trong **RAM**. Mất khi khởi động lại.
- **startup-config**: cấu hình khởi động trong **NVRAM**. Giữ lại qua lần khởi động.
- **flash**: lưu **image IOS** và có thể chứa tập tin khác.
- Lệnh thường dùng: `copy running-config startup-config`, `show running-config`, `show startup-config`, `erase startup-config` (thận trọng).

2.3 Cấu hình cơ bản cho Switch

2.3.1 Đặt tên thiết bị và thông tin cơ bản

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname SW-Floor-1
SW-Floor-1(config)# no ip domain-lookup
SW-Floor-1(config)# service password-encryption
SW-Floor-1(config)# banner motd #Truy cập được giám sát. Người không phận sự cấm vào.#
```

- `hostname` giúp định danh thiết bị trong sơ đồ và nhật ký.
- `no ip domain-lookup` tránh *DNS lookup* gây trễ khi gõ sai lệnh.
- `service password-encryption` mã hoá mức cơ bản các mật khẩu dạng `password` trong `running-config`.
- `banner` hiển thị *thông điệp pháp lý/cảnh báo* trước khi đăng nhập.

2.3.2 Bảo mật các chế độ truy cập

```
SW-Floor-1(config)# enable secret <MATKHAU_MANH>
SW-Floor-1(config)# line console 0
SW-Floor-1(config-line)# password <MATKHAU_CONSOLE>
SW-Floor-1(config-line)# login
SW-Floor-1(config-line)# logging synchronous
SW-Floor-1(config-line)# exec-timeout 10 0
SW-Floor-1(config-line)# exit
SW-Floor-1(config)# line vty 0 15
SW-Floor-1(config-line)# transport input ssh
SW-Floor-1(config-line)# login local
SW-Floor-1(config-line)# exec-timeout 10 0
```

- `enable secret` (được băm MD5) bảo vệ truy cập `privileged EXEC`.
- `line console 0`: đặt mật khẩu console, đồng bộ nhật ký và **tự đăng xuất** sau thời gian rỗi.
- `line vty 0 15`: chỉ cho phép `ssh`; dùng `login local` để xác thực theo tài khoản cục bộ.

2.3.3 Bật SSH và người dùng cục bộ

```
SW-Floor-1(config)# ip domain-name example.local
SW-Floor-1(config)# username admin secret <MATKHAU_MANH>
SW-Floor-1(config)# crypto key generate rsa modulus 2048
SW-Floor-1(config)# ip ssh version 2
```

- Cần `hostname` và `ip domain-name` trước khi tạo khoá RSA.
- `username ... secret` tạo *user/password* cho `login local`.
- Dùng `ssh -l admin <ip_svi>` từ PC để quản trị.

2.3.4 Cấu hình địa chỉ IP quản trị cho Switch (SVI)

```
SW-Floor-1(config)# interface vlan 1
SW-Floor-1(config-if)# ip address 192.168.10.2 255.255.255.0
SW-Floor-1(config-if)# no shutdown
SW-Floor-1(config)# ip default-gateway 192.168.10.1
```

- **SVI VLAN 1** dùng cho *quản trị* switch qua mạng.
- `ip default-gateway` để lưu lượng quản trị đi ra ngoài subnet.

2.3.5 Lưu cấu hình và kiểm tra

```
SW-Floor-1# copy running-config startup-config
SW-Floor-1# show running-config
SW-Floor-1# show ip interface brief
SW-Floor-1# show version
```

2.4 Cấu hình thiết bị đầu cuối (PC) và kiểm tra kết nối

2.4.1 Đặt địa chỉ IP cho PC

Trên hệ điều hành (hoặc trong công cụ mô phỏng), cấu hình:

- **IP address**: `192.168.10.10`
- **Subnet mask**: `255.255.255.0`
- **Default gateway**: `192.168.10.1`
- **DNS server**: tuỳ môi trường (có thể là `192.168.10.1` hoặc của ISP)

2.4.2 Kiểm tra cơ bản

- `ping 192.168.10.2` (PC → SVI switch) phải **thành công**.
- `ping 192.168.10.1` (PC → gateway) để xác minh đường ra.
- `ssh admin@192.168.10.2` để kiểm tra truy cập từ xa an toàn.
- Nếu `ping` lần đầu *time-out*, thử lại do *ARP* chưa có cache (*ARP warm-up*).

2.5 Định danh và thông điệp hệ thống

2.5.1 Quy ước đặt tên thiết bị

Tên nên:

- Phản ánh vị trí/chức năng (`SW-F1`, `RTR-EDGE`, `ACC-BLDG-A`).
- Không dùng khoảng trắng/ký tự đặc biệt; thống nhất viết hoa/thường.

2.5.2 Banner cảnh báo

- **MOTD/Login banner** dùng cho mục đích cảnh báo pháp lý: "Chỉ người được phép mới được truy cập".
- Tránh lộ thông tin nội bộ (phiên bản, đơn vị) trong banner.

2.6 Bảo mật truy cập cơ bản

2.6.1 Nguyên tắc tối thiểu cần làm

- Dùng `enable secret` thay cho `enable password`.
- Bật `service password-encryption` (bảo vệ mức cơ bản).
- Khoá `console`, `vty` bằng `login` và **mật khẩu mạnh**/`login local`.
- Chỉ cho `transport input ssh`, vô hiệu Telnet.
- Đặt `exec-timeout` để tự đăng xuất phiên rỗi.

2.6.2 Tài khoản cục bộ và chính sách

- Tạo người dùng cá nhân, tránh dùng chung `admin`.
- Gắn `privilege` phù hợp nếu cần, hoặc để mặc định và bảo vệ bằng `enable secret`.

2.7 Sao lưu và khôi phục cấu hình

2.7.1 Lưu và sao chép cấu hình

```
copy running-config startup-config
copy startup-config running-config
copy running-config tftp:
copy startup-config tftp:
```

Lưu ý: kiểm tra kết nối TFTP trước khi sao lưu.

2.7.2 Khôi phục về mặc định

```
erase startup-config
reload
```

Thao tác này xoá cấu hình khởi động và tái khởi động thiết bị; chỉ thực hiện khi đã sao lưu.

2.8 Khắc phục sự cố ban đầu

- **Cáp/kết nối**: kiểm tra `link`, đèn LED, cổng đúng chuẩn (cáp thẳng/chéo trên thiết bị cũ).
- **Trạng thái interface**: `show ip interface brief`, `show interface status`.
- **Địa chỉ IP/mask/gateway**: đảm bảo cùng mạng; xem `show running-config`.
- **VLAN và cổng truy cập**: PC ở VLAN đúng; `show vlan brief`.

- **SSH**: khoá `RSA`, `ip domain-name`, `username`, `line vty`, `transport input ssh`.
- **Lưu lượng bị chặn**: kiểm tra ACL (nếu có), tính năng bảo mật cổng.

Tóm tắt

- Thiết bị Cisco IOS được truy cập qua **console** và **SSH**; Telnet không an toàn.
- Nắm vững **chế độ IOS**, các lệnh `show`, `copy`, và trợ giúp `?`.
- Cấu hình cơ bản gồm: `hostname`, `banner`, `enable secret`, `line console/vty`, `service password-encryption`.
- Đặt **IP quản trị** trên **SVI**, `ip default-gateway`; cấu hình IP cho PC.
- Bật **SSH**, tạo người dùng cục bộ, giới hạn `transport input` chỉ `ssh`.
- Xác minh bằng `ping`, `ssh`, và các lệnh `show`.

Câu hỏi ôn tập

1. **Mục đích của lệnh `no shutdown`:**
   - Kích hoạt cổng mạng trên switch hoặc router.
   - Nếu không dùng lệnh này, cổng vẫn ở trạng thái *administratively down* và không truyền dữ liệu.
2. **Lý do cần đặt mật khẩu cho console, vty và enable secret:**
   - Ngăn truy cập trái phép và bảo vệ thiết bị mạng.
   - Console: bảo vệ quyền truy cập trực tiếp bằng cáp console.
   - VTY: bảo vệ quyền truy cập từ xa (Telnet/SSH).
   - Enable secret: bảo vệ chế độ đặc quyền (privileged EXEC).
3. **Ý nghĩa của lệnh `copy running-config startup-config`:**
   - Lưu cấu hình hiện tại (RAM) vào NVRAM.
   - Giúp giữ cấu hình khi thiết bị khởi động lại.
4. **Ý nghĩa các thông số khi cấu hình địa chỉ IPv4 cho PC:**
   - **Địa chỉ IP**: định danh logic của thiết bị trong mạng.
   - **Subnet mask**: xác định phần mạng và phần host của địa chỉ.
   - **Default gateway**: địa chỉ router để kết nối ra ngoài mạng cục bộ.
   - **DNS server**: phân giải tên miền thành địa chỉ IP.
5. **Lợi ích của SSH so với Telnet:**
   - SSH mã hóa toàn bộ dữ liệu truyền, bao gồm mật khẩu và lệnh.
   - Telnet gửi dữ liệu dạng văn bản thuần, dễ bị nghe lén.
   - Do đó SSH an toàn hơn và được khuyến khích sử dụng trong quản trị mạng.

2.9 Thuật ngữ cần nhớ

Switch Thiết bị mạng tầng Liên kết dữ liệu (Layer 2) dùng để kết nối nhiều thiết bị đầu cuối trong cùng một mạng LAN, chuyển tiếp khung dựa trên địa chỉ MAC.

Router Thiết bị mạng tầng Mạng (Layer 3) có chức năng định tuyến, kết nối nhiều mạng khác nhau và quyết định đường đi tốt nhất cho gói tin.

CLI (Command Line Interface) Giao diện dòng lệnh để quản trị và cấu hình thiết bị mạng Cisco; người dùng nhập lệnh trực tiếp thay vì dùng giao diện đồ họa.

User EXEC Mode Chế độ EXEC người dùng trên thiết bị Cisco, cho phép thực hiện một số lệnh cơ bản để kiểm tra trạng thái nhưng không thay đổi cấu hình (`Router>`).

Privileged EXEC Mode Chế độ EXEC đặc quyền, cho phép thực hiện các lệnh nâng cao như kiểm tra chi tiết hoặc truy cập cấu hình (`Router#`).

Global Configuration Mode Chế độ cấu hình toàn cục, nơi người quản trị thay đổi cấu hình chung cho toàn bộ thiết bị (`Router(config)#`).

Interface Configuration Mode Chế độ cấu hình giao diện, cho phép thiết lập thông số (IP, trạng thái) cho từng cổng mạng cụ thể (`Router(config-if)#`).

Line Configuration Mode Chế độ cấu hình cho các đường truy cập (console, VTY), dùng để kiểm soát việc đăng nhập và các thiết lập bảo mật liên quan.

Hostname Tên gán cho thiết bị mạng, dùng để dễ nhận diện trong quá trình quản trị (ví dụ: `Switch1`, `RouterA`).

Banner Message Thông điệp hiển thị khi người dùng truy cập thiết bị, thường là thông báo cảnh báo an ninh hoặc nội quy sử dụng.

Password (Enable/Console/VTY) Chuỗi ký tự bảo mật được cấu hình để kiểm soát quyền truy cập:

- **Console password**: bảo vệ truy cập qua cổng console.
- **VTY password**: bảo vệ truy cập từ xa qua Telnet/SSH.
- **Enable secret**: mật khẩu mã hóa dùng để vào chế độ EXEC đặc quyền.

Saves Configuration Lưu cấu hình hiện tại từ RAM vào NVRAM bằng lệnh `copy running-config startup-config`, đảm bảo thiết bị khởi động lại vẫn giữ cấu hình.

Running-config Cấu hình hiện đang hoạt động trong RAM của thiết bị; mọi thay đổi khi gõ lệnh sẽ tác động ngay đến running-config.

Startup-config Cấu hình được lưu trong NVRAM, sẽ được thiết bị tải lên khi khởi động.

IP Address Địa chỉ logic được gán cho giao diện của thiết bị, dùng để định danh và giao tiếp trong mạng IP.

Subnet Mask Mặt nạ mạng xác định phần nào của địa chỉ IP thuộc mạng, phần nào thuộc host; cần thiết để phân biệt mạng con.

Default Gateway Địa chỉ IP của router trong mạng LAN, nơi host gửi gói tin khi đích nằm ngoài mạng con cục bộ.

ICMP Echo Request/Reply Thông điệp ICMP dùng trong lệnh `ping`, để kiểm tra khả năng kết nối giữa hai thiết bị.

Show Commands Các lệnh hiển thị trạng thái cấu hình và hoạt động, ví dụ: `show running-config`, `show ip interface brief`, `show version`.

Ping Lệnh kiểm tra kết nối IP bằng cách gửi gói ICMP Echo Request và nhận Echo Reply từ đích.

Traceroute Lệnh xác định đường đi của gói tin đến đích, hiển thị các router trung gian mà gói đi qua.

Chương 3

Các Giao thức và Mô hình

Mục tiêu

Sau khi hoàn thành chương này, bạn sẽ có thể:

- Giải thích lý do vì sao mạng cần các **giao thức** và mô hình tham chiếu.
- Mô tả các lớp trong mô hình **OSI** và mô hình **TCP/IP**.
- So sánh mô hình OSI và TCP/IP, nêu các điểm tương đồng và khác biệt.
- Trình bày các chức năng cơ bản của từng lớp trong giao tiếp mạng.
- Hiểu khái niệm **encapsulation**, **PDU** và cách dữ liệu di chuyển qua các lớp.
- Xác định vai trò của **chuẩn hóa** (IETF, IEEE, ITU, ISO).
- Liên hệ các giao thức phổ biến (HTTP, TCP, IP, Ethernet, v.v.) với các lớp trong mô hình.

Thuật ngữ chính

- Protocol
- Encapsulation
- PDU (Protocol Data Unit)
- OSI model
- TCP/IP model
- Standardization
- Segmentation
- Reliability
- Flow control
- Unicast / Multicast / Broadcast
- Application, Transport, Internet, Network Access
- IETF, IEEE, ISO, ITU
- Port number
- Addressing
- Data link frame

3.1 Giới thiệu

Các thiết bị mạng cần có ngôn ngữ chung để giao tiếp. Ngôn ngữ này được tạo thành từ **giao thức**, quy định cách thức dữ liệu được đóng gói, truyền tải, định địa chỉ và giải mã. Các **mô hình tham chiếu** như OSI và TCP/IP giúp hình dung quá trình truyền dữ liệu phức tạp thành các lớp dễ hiểu và quản lý.

3.2 Các Giao thức và Chuẩn

3.2.1 Giao thức là gì?

Một **giao thức** (protocol) là tập hợp các quy tắc xác định cách thức hai hay nhiều thiết bị trao đổi thông tin. Giao thức định nghĩa:

- Định dạng dữ liệu
- Thời gian gửi và nhận
- Phương thức báo hiệu kết thúc, lỗi, xác nhận

3.2.2 Tính năng của giao thức

Giao thức có thể cung cấp các tính năng như:

- Địa chỉ hóa nguồn và đích
- Phân mảnh dữ liệu thành gói nhỏ hơn (segmentation)
- Phát hiện và sửa lỗi
- Kiểm soát luồng (flow control)
- Cơ chế bắt tay (handshake) để đảm bảo kết nối

3.2.3 Chuẩn hóa và tổ chức quốc tế

Sự hợp tác toàn cầu yêu cầu các chuẩn chung. Một số tổ chức chính:

- **IETF** (Internet Engineering Task Force): phát triển chuẩn Internet (TCP/IP).
- **IEEE**: định nghĩa Ethernet, Wifi (802.x).
- **ISO**: phát triển mô hình OSI.
- **ITU-T**: chuẩn viễn thông toàn cầu.

3.3 Mô hình OSI

3.3.1 Giới thiệu mô hình OSI

Mô hình OSI (Open Systems Interconnection) có 7 lớp:

1. **Application** – cung cấp dịch vụ mạng cho ứng dụng (HTTP, SMTP)
2. **Presentation** – định dạng, mã hóa, nén dữ liệu
3. **Session** – quản lý phiên làm việc (duy trì, đồng bộ, kết thúc)
4. **Transport** – vận chuyển dữ liệu, cung cấp độ tin cậy (TCP, UDP)
5. **Network** – định địa chỉ và định tuyến (IP)
6. **Data Link** – đóng gói khung (frame), địa chỉ MAC, kiểm soát truy cập
7. **Physical** – truyền bit qua môi trường vật lý (cáp, sóng)

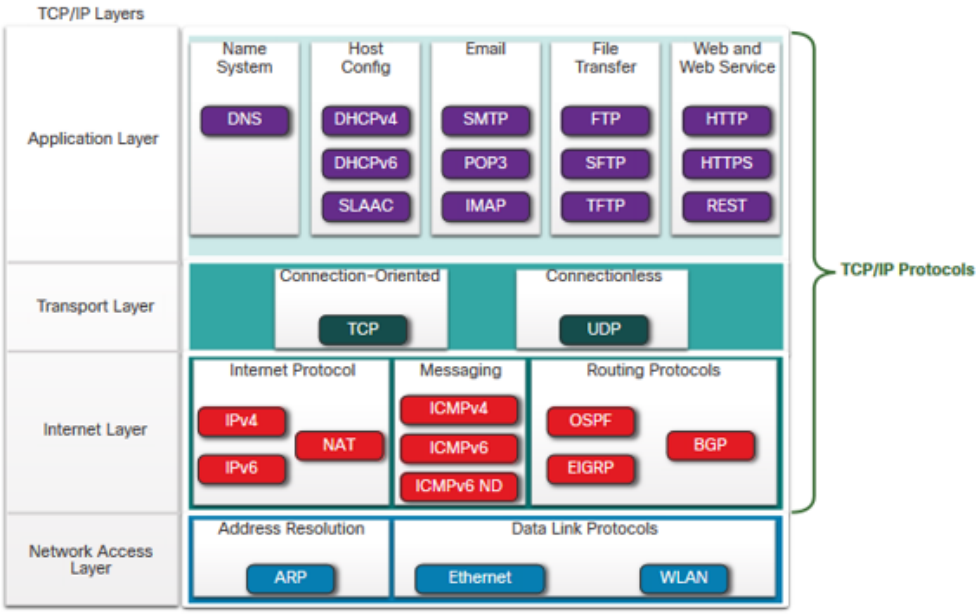
3.3.2 Chức năng từng lớp

- Mỗi lớp phục vụ cho lớp phía trên và nhận dịch vụ từ lớp phía dưới.
- Mỗi lớp thực hiện chức năng riêng biệt, độc lập.

3.4 Mô hình TCP/IP

3.4.1 Giới thiệu mô hình TCP/IP

Mô hình TCP/IP thực tế được dùng trong Internet, gồm 4 lớp như trong Hình 3.1



Hình 3.1: Các giao thức chính trong mô hình TCP/IP.

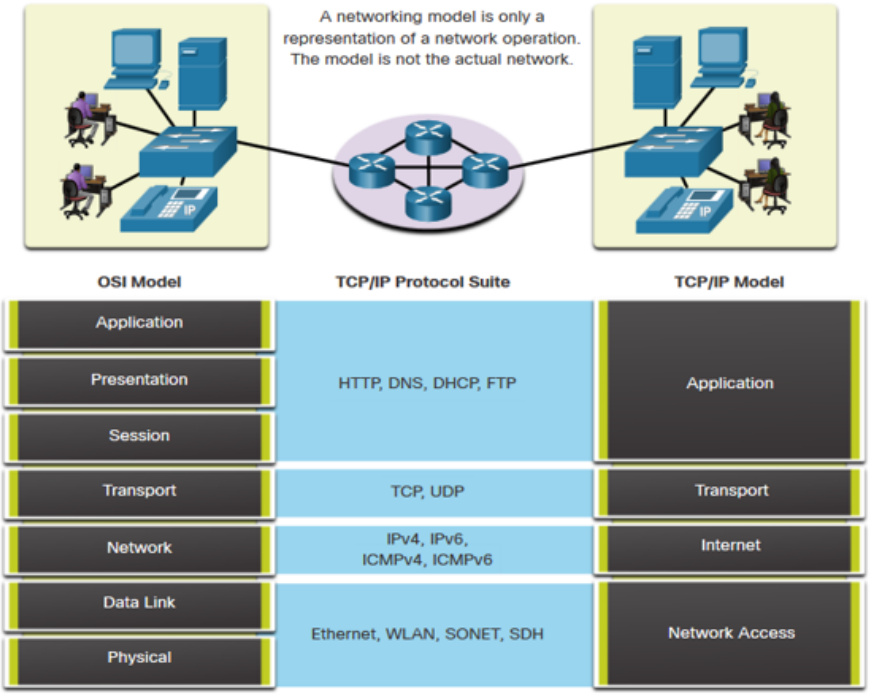
Các giao thức phổ biến ở từng lớp gồm:

1. **Application**: kết hợp Application, Presentation, Session của OSI (HTTP, DNS, FTP, SMTP).
2. **Transport**: TCP, UDP.
3. **Internet**: IP, ICMP.
4. **Network Access**: Ethernet, PPP, Frame Relay, Wifi.

3.4.2 So sánh OSI và TCP/IP

Hai mô hình OSI và TCP/IP được mô tả ngắn gọn trong Hình 3.2, một số điểm chú ý:

- OSI có 7 lớp, TCP/IP có 4 lớp.
- TCP/IP thực tế hơn, OSI mang tính lý thuyết, nhưng giúp học dễ hơn.
- Nhiều giao thức được ánh xạ từ TCP/IP sang OSI để giải thích.



Hình 3.2: Hai mô hình OSI và TCP/IP.

3.5 Quá trình truyền dữ liệu và bọc/dỡ (en/de-capsulation)

3.5.1 Encapsulation

Dữ liệu đi xuống các lớp, mỗi lớp thêm **header** riêng:

- Transport: thêm TCP/UDP header → **segment**
- Network: thêm IP header → **packet**
- Data Link: thêm MAC header/trailer → **frame**
- Physical: chuyển thành bit truyền qua cáp hoặc sóng

3.5.2 De-encapsulation

Khi tới đích, các header bị loại bỏ dần theo chiều ngược lại, cho đến khi dữ liệu gốc được chuyển cho ứng dụng.

3.6 Các loại truyền thông

- **Unicast**: một gửi đến một.
- **Multicast**: một gửi đến nhiều, chỉ những ai quan tâm.
- **Broadcast**: một gửi đến tất cả trong cùng mạng LAN.

Tóm tắt

- Giao thức quy định cách thức trao đổi dữ liệu, gồm định dạng, thời gian, kiểm soát lỗi, xác nhận.

- Mạng toàn cầu yêu cầu chuẩn hóa (IETF, IEEE, ISO, ITU).
- Mô hình OSI có 7 lớp, mô hình TCP/IP có 4 lớp; cả hai đều được dùng để giảng dạy và triển khai.
- Dữ liệu được đóng gói thành PDU ở mỗi lớp: segment, packet, frame, bit.
- Có 3 loại truyền thông chính: unicast, multicast, broadcast.

Câu hỏi ôn tập

1. **Tại sao cần mô hình phân lớp trong truyền thông mạng?**
   - Giúp chia nhỏ quá trình truyền thông phức tạp thành nhiều phần dễ quản lý.
   - Chuẩn hóa cách các thiết bị và phần mềm của nhiều nhà sản xuất khác nhau hoạt động cùng nhau.
   - Cho phép thay đổi, nâng cấp ở một lớp mà không ảnh hưởng đến các lớp khác.
2. **Khác biệt giữa mô hình OSI và TCP/IP là gì?**
   - OSI có 7 tầng: Vật lý, Liên kết dữ liệu, Mạng, Vận chuyển, Phiên, Trình bày, Ứng dụng.
   - TCP/IP có 4 tầng: Truy cập mạng, Internet, Vận chuyển, Ứng dụng.
   - TCP/IP được triển khai thực tế, còn OSI chủ yếu mang tính tham chiếu, giảng dạy.
3. **Chức năng chính của tầng vận chuyển là gì?**
   - Đảm bảo dữ liệu từ tiến trình nguồn đến tiến trình đích chính xác.
   - Cung cấp cơ chế phân chia (segmentation), kiểm soát luồng, kiểm tra lỗi và tái sắp xếp dữ liệu.
4. **Tại sao lại cần các chuẩn giao thức?**
   - Đảm bảo thiết bị của các hãng khác nhau có thể giao tiếp được với nhau.
   - Giúp Internet mở rộng và phát triển đồng nhất.
   - Giảm chi phí, tránh phụ thuộc vào nhà cung cấp duy nhất.
5. **Cho ví dụ về giao thức và lớp mà nó thuộc về.**
   - HTTP – Tầng Ứng dụng.
   - TCP – Tầng Vận chuyển.
   - IP – Tầng Mạng (Internet trong TCP/IP).
   - Ethernet – Tầng Liên kết dữ liệu.

3.7 Bài tập Chương 3

1. Một gói dữ liệu ở tầng Ứng dụng có kích thước 1.000 byte. Header của TCP là 20 byte, header của IP là 20 byte, header của Ethernet là 18 byte. Hãy tính kích thước toàn bộ frame khi truyền trên mạng LAN.

   Kích thước frame khi truyền trên LAN

   Dữ liệu ứng dụng: 1000 B; TCP header: 20 B; IP header: 20 B; Ethernet header: 18 B.

   $$\text{Kích thước frame} = 1000 + 20 + 20 + 18 = \boxed{1058 \text{ byte}}$$

2. Một máy chủ cần gửi 10 MB dữ liệu cho client. Nếu mỗi segment TCP chứa tối đa 1.460 byte dữ liệu (MTU = 1.500 byte, trừ IP 20 byte và TCP 20 byte), hãy tính số segment TCP được tạo ra.

   Số segment TCP cho 10 MB dữ liệu (MTU 1500, payload TCP tối đa 1460 B)

   Giả định: 1 MB = 2^{20} B = 1,048,576 B.
   Tổng dữ liệu: $10 \times 1{,}048{,}576 = 10{,}485{,}760$ B.
   Mỗi segment chở tối đa 1460 B ⇒ số segment

   $$N = \left\lceil \frac{10{,}485{,}760}{1460} \right\rceil = \boxed{7183 \text{ segment}}$$

   (7182 full + 1 segment cuối ≈ 40 B).

3. Giả sử một mạng LAN có 5 máy tính cần giao tiếp trực tiếp theo mô hình peer-to-peer. Hãy tính số phiên kết nối tối đa có thể hình thành đồng thời (theo công thức $nn-1 \atop \Uparrow 2$).

   Số phiên P2P tối đa với 5 máy

   $$N = \frac{nn-1}{2} = \frac{5 \times 4}{2} = \boxed{10 \text{ kết nối}}$$

4. Một frame Ethernet có payload 1.500 byte và overhead của các header/tailer là 38 byte. Tính tỷ lệ overhead so với toàn bộ frame.

   Tỷ lệ overhead của frame Ethernet

   Payload: 1500 B; Overhead: 38 B ⇒ tổng 1538 B. Tỷ lệ overhead:

   $$\frac{38}{1538} \approx 0.0247 = \boxed{2.47\%}$$

5. Một hệ thống gửi 1.000 gói tin, mỗi gói có header tổng cộng 58 byte (TCP + IP + Ethernet). Nếu payload mỗi gói là 1.000 byte, hãy tính tổng dung lượng overhead được truyền trên mạng.

   Tổng overhead khi gửi 1000 gói, mỗi gói header 58 B, payload 1000 B

   $$\text{Tổng overhead} = 1000 \times 58 = \boxed{58{,}000 \text{ byte}} \approx 56.64 \text{ KiB}$$

   (Tổng dữ liệu người dùng: $1000 \times 1000 = 1{,}000{,}000$ B).

6. Khi encapsulation, dữ liệu 2.000 byte từ tầng Ứng dụng được phân mảnh thành 3 segment TCP (mỗi segment chứa tối đa 800 byte dữ liệu). Với header TCP = 20 byte, IP = 20 byte, Ethernet = 18 byte, hãy tính tổng số byte được truyền đi.

   Encapsulation cho 2000 B ứng dụng, chia thành các segment 800 B

   Số segment: $\left\lceil 2000 \atop \Uparrow 800 \right\rceil = 3$ (lần lượt 800, 800, 400 B).

   Mỗi gói có overhead: TCP 20 + IP 20 + Eth 18 = 58 B.
   Tổng byte truyền:

   $$2000 + 3 \times 58 = \boxed{2174 \text{ byte}}$$

7. Giả sử một host cần mở 200 kết nối TCP đồng thời tới nhiều server khác nhau. Nếu mỗi kết nối chiếm trung bình 80 byte thông tin điều khiển (control info) trong bộ nhớ, hãy tính tổng dung lượng bộ nhớ cần thiết.

   Bộ nhớ điều khiển cho 200 kết nối TCP, mỗi kết nối 80 B

   $$200 \times 80 = \boxed{16{,}000 \text{ byte}} \approx 15.625 \text{ KiB}$$

8. Một frame Ethernet gửi qua đường truyền 100 Mbps. Kích thước frame = 1.538 byte. Tính thời gian truyền (transmission time) của frame này (theo micro giây).

   Thời gian truyền một frame 1538 B trên đường 100 Mbps

   Kích thước: $1538 \times 8 = 12{,}304$ bit. Tốc độ: 100 Mbps = 100×10^6 bit/s.

   $$t = \frac{12{,}304}{100 \times 10^6}\ \text{s} = 1.2304 \times 10^{-4}\ \text{s} = \boxed{123.04\ \mu s}$$

9. Một mạng có 50 host, mỗi host cần giao tiếp với tất cả host khác. Hãy tính tổng số kết nối cần thiết nếu dùng: (a) Mạng peer-to-peer, (b) Mô hình client-server (1 server trung tâm + 49 client).

   Số kết nối với 50 host

   - (a) **Peer-to-peer full-mesh**: $\frac{50 \times 49}{2} = \boxed{1225}$.
   - (b) **Client-server** (1 server + 49 client): mỗi client 1 kết nối tới server $\Rightarrow \boxed{49}$.

10. Một ứng dụng gửi file 8 MB qua TCP. Nếu mỗi segment chứa 1.460 byte dữ liệu và 40 byte header (IP + TCP), hãy tính: (a) Số segment cần gửi. (b) Tổng số byte header được truyền.

    Gửi file 8 MB qua TCP (payload 1460 B/segment, header (IP+TCP) = 40 B)

    Giả định: 1 MB = 2^{20} B $\Rightarrow$ 8 MB = 8,388,608 B.
    (a) Số segment:

    $$N = \left\lceil \frac{8{,}388{,}608}{1460} \right\rceil = \boxed{5746\ \text{segment}}$$

    (b) Tổng byte header:

    $$5746 \times 40 = \boxed{229{,}840\ \text{byte}} \approx 224.06\ \text{KiB}$$

3.8 Thuật ngữ cần nhớ

Protocol Bộ quy tắc xác định cách thức dữ liệu được định dạng, truyền tải và xử lý trong mạng. Gồm các thành phần: cú pháp (format), ngữ nghĩa (ý nghĩa trường thông tin), và thời gian (thứ tự, đồng bộ).

Protocol Suite Tập hợp nhiều giao thức hoạt động cùng nhau để thực hiện đầy đủ chức năng truyền thông. Ví dụ: bộ giao thức TCP/IP bao gồm IP, TCP, UDP, HTTP, FTP, DNS, v.v.

Encapsulation Quá trình đóng gói dữ liệu khi truyền qua các tầng: tầng trên thêm thông tin điều khiển (header/trailer) và giao xuống tầng dưới. Dữ liệu tầng trên trở thành payload của tầng dưới.

De-encapsulation Quá trình ở phía nhận: mỗi tầng bỏ phần header/trailer tương ứng để chuyển payload lên tầng trên cho đến ứng dụng.

PDU (Protocol Data Unit) Đơn vị dữ liệu ở mỗi tầng:

- Tầng Ứng dụng: Data
- Tầng Vận chuyển: Segment (TCP) hoặc Datagram (UDP)
- Tầng Mạng: Packet
- Tầng Liên kết dữ liệu: Frame
- Tầng Vật lý: Bits

OSI Reference Model Mô hình tham chiếu chuẩn gồm 7 tầng: Vật lý, Liên kết dữ liệu, Mạng, Vận chuyển, Phiên, Trình bày, Ứng dụng. Mục đích: chuẩn hóa, phân lớp, thuận tiện cho học tập và phân tích.

TCP/IP Model Mô hình giao thức Internet gồm 4 tầng: Truy cập mạng (Network Access), Internet, Vận chuyển (Transport), Ứng dụng (Application). Đây là mô hình thực tế triển khai trên Internet.

Application Layer (TCP/IP) Lớp cao nhất trong TCP/IP, gồm các giao thức dịch vụ ứng dụng như HTTP, DNS, FTP, SMTP. Nó định nghĩa cách ứng dụng giao tiếp với mạng.

Transport Layer Đảm bảo truyền thông đầu cuối – đầu cuối (end-to-end). TCP cung cấp kết nối tin cậy, UDP cung cấp dịch vụ không tin cậy nhưng nhanh. Cung cấp cơ chế phân mảnh dữ liệu và kiểm soát lỗi.

Internet Layer Chịu trách nhiệm định tuyến gói tin từ nguồn đến đích qua nhiều mạng. Giao thức chính: IPv4, IPv6, ICMP.

Network Access Layer (còn gọi là Link Layer) Kết hợp chức năng của tầng Vật lý và Liên kết dữ liệu trong OSI. Định nghĩa cách dữ liệu truyền qua phương tiện vật lý, địa chỉ MAC, kiểm soát truy cập môi trường.

Standards Organization Các tổ chức xây dựng tiêu chuẩn mở cho mạng máy tính: IEEE (chuẩn Ethernet 802.3, Wi-Fi 802.11), IETF (chuẩn TCP/IP, RFC), ISO (mô hình OSI).

IETF (Internet Engineering Task Force) Tổ chức phát triển các chuẩn mở của Internet, công bố dưới dạng RFC (Request for Comments). Ví dụ: chuẩn hóa TCP/IP, HTTP, IPv6.

IEEE (Institute of Electrical and Electronics Engineers) Tổ chức ban hành các chuẩn mạng tầng thấp, ví dụ: Ethernet (802.3), Wi-Fi (802.11), Bluetooth (802.15).

ISO (International Organization for Standardization) Tổ chức quốc tế xây dựng chuẩn OSI, đặt nền tảng lý thuyết về phân lớp giao thức.

Interoperability Khả năng các thiết bị và phần mềm từ nhiều nhà sản xuất khác nhau hoạt động cùng nhau nhờ tuân thủ các chuẩn chung.

Segmentation Quá trình tầng Vận chuyển chia dữ liệu lớn thành các phần nhỏ (segment) để dễ dàng truyền tải, sau đó tái lắp ghép ở đầu nhận.

Multiplexing Kỹ thuật tầng Vận chuyển cho phép nhiều ứng dụng chia sẻ cùng một kết nối mạng vật lý. Thực hiện nhờ các số cổng (port number).

Well-known Ports Các cổng từ 0–1023 dành cho các dịch vụ mạng chuẩn: HTTP (80), HTTPS (443), FTP (21), SSH (22), SMTP (25), DNS (53).

Port Number Số hiệu định danh ứng dụng hoặc tiến trình giao tiếp. Ví dụ: port 80 cho web, port 25 cho email.

Flow Control Cơ chế tầng Vận chuyển điều chỉnh tốc độ gửi dữ liệu để tránh tràn bộ đệm phía nhận.

Reliability Đặc tính truyền thông tin cậy (như TCP) nhờ các cơ chế: đánh số thứ tự, ACK (acknowledgment), retransmission (truyền lại).

IP Address Địa chỉ logic ở tầng Mạng để định danh host. IPv4 dài 32 bit, IPv6 dài 128 bit.

MAC Address Địa chỉ vật lý gắn cho card mạng, dài 48 bit (theo chuẩn IEEE). Được dùng ở tầng Liên kết dữ liệu.

Default Gateway Router trong cùng mạng LAN mà host gửi gói tin để ra ngoài mạng con cục bộ.

Chương 4

Tầng Vật lý

Mục tiêu

Sau khi hoàn thành chương này, bạn sẽ có thể:

- Mô tả vai trò của tầng vật lý trong mô hình OSI.
- Liệt kê các chức năng chính của tầng vật lý: mã hóa tín hiệu, tốc độ bit, topo vật lý.
- Phân biệt các loại phương tiện truyền dẫn: cáp đồng, cáp quang, không dây.
- Trình bày ưu và nhược điểm của từng loại môi trường truyền.
- Hiểu cách tiêu chuẩn hóa (IEEE, ISO, TIA/EIA) đảm bảo tính tương thích.

Thuật ngữ chính

- Physical layer
- Encoding
- Signaling
- Bandwidth
- Throughput
- Goodput
- Latency
- Copper cabling
- UTP, STP, Coaxial
- Fiber-optic
- Wireless LAN, Bluetooth, Cellular
- Topology

4.1 Giới thiệu

Tầng vật lý là tầng thấp nhất trong mô hình OSI. Nó định nghĩa cách dữ liệu được truyền dưới dạng **tín hiệu điện, ánh sáng hoặc sóng vô tuyến**. Tầng vật lý không quan tâm nội dung dữ liệu, chỉ quan tâm đến cách **biểu diễn bit** và truyền chúng qua môi trường.

4.2 Mục đích của tầng vật lý

4.2.1 Các chức năng chính

- **Mã hóa tín hiệu**: biến dữ liệu nhị phân thành tín hiệu điện/tín hiệu quang/sóng vô tuyến.

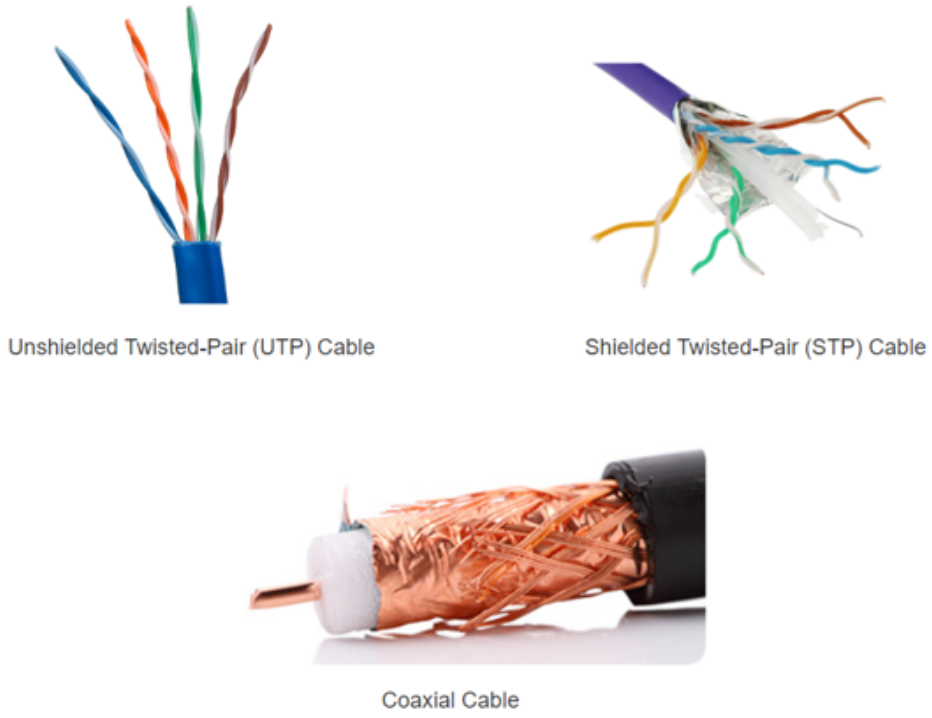
- **Tốc độ bit**: xác định số lượng bit truyền trong một giây (bps).
- **Định nghĩa topo vật lý**: bố trí cáp và thiết bị.
- **Tiêu chuẩn hóa**: quy định đầu nối, điện áp, bước sóng, tần số.

4.2.2 Băng thông, thông lượng và độ trễ

- **Bandwidth**: dung lượng tối đa lý thuyết của đường truyền (bps).
- **Throughput**: tốc độ thực tế đạt được.
- **Goodput**: tốc độ dữ liệu hữu ích, loại bỏ overhead và gói lỗi.
- **Latency**: độ trễ từ khi gửi đến khi nhận.

4.3 Phương tiện truyền dẫn

4.3.1 Cáp đồng



Hình 4.1: Các loại cáp đồng.

Có ba loại chính như Hình 4.1

- **UTP (Unshielded Twisted Pair)**: phổ biến nhất, giá rẻ, dễ lắp đặt, dễ bị nhiễu điện từ (EMI).
- **STP (Shielded Twisted Pair)**: có lớp chắn chống nhiễu, đắt hơn, khó thi công.
- **Coaxial**: lõi đồng, dùng trong truyền hình cáp, ít dùng cho LAN hiện đại.

Chuẩn cáp UTP: TIA/EIA 568A và 568B quy định thứ tự màu dây.

4.3.2 Cáp quang

Truyền dữ liệu bằng **xung ánh sáng**, có băng thông và khoảng cách rất lớn.

- **Single-mode fiber (SMF)**: lõi nhỏ, truyền xa (hàng chục km), dùng trong ISP và mạng đường trục.
- **Multimode fiber (MMF)**: lõi to hơn, truyền ngắn (dưới 2 km), dùng trong LAN, data center.

Ưu điểm: miễn nhiễm EMI, bảo mật tốt. Nhược điểm: chi phí cao, lắp đặt khó.

4.3.3 Truyền dẫn không dây

Sử dụng sóng điện từ để truyền dữ liệu:

- **Wi-Fi (IEEE 802.11)**: LAN không dây.
- **Bluetooth**: kết nối tầm ngắn giữa thiết bị cá nhân.
- **Mạng di động (3G/4G/5G)**: vùng phủ rộng.

Ưu điểm: tiện lợi, di động. Nhược điểm: dễ bị nhiễu, suy hao tín hiệu, cần mã hóa bảo mật.

4.4 Tiêu chuẩn hóa tầng vật lý

Một số tổ chức chính:

- **IEEE**: chuẩn Ethernet (802.3), Wi-Fi (802.11).
- **TIA/EIA**: chuẩn cáp xoắn đôi (UTP).
- **ISO/IEC**: tiêu chuẩn hóa toàn cầu.

Tiêu chuẩn giúp các thiết bị từ nhiều hãng có thể tương tác.

Tóm tắt

- Tầng vật lý định nghĩa cách truyền bit qua môi trường truyền.
- Chức năng chính: mã hóa tín hiệu, tốc độ bit, định nghĩa topo, chuẩn giao tiếp.
- Các khái niệm quan trọng: bandwidth, throughput, goodput, latency.
- Có ba loại phương tiện truyền: cáp đồng, cáp quang, không dây.
- Tiêu chuẩn hóa đảm bảo tính tương thích và tương tác thiết bị.

Câu hỏi ôn tập

1. **Chức năng chính của tầng Vật lý là gì?**
    - Chuyển đổi dữ liệu thành tín hiệu điện, quang hoặc sóng vô tuyến để truyền qua môi trường vật lý.
    - Xác định các đặc tính về điện áp, tần số, tốc độ truyền, loại đầu nối, chuẩn cáp.
2. **Ba loại phương tiện truyền dẫn phổ biến trong mạng là gì?**

- Cáp xoắn đôi (UTP/STP).
- Cáp quang (fiber optic).
- Sóng vô tuyến (wireless).

3. **Ưu điểm và nhược điểm của cáp xoắn đôi (UTP) so với cáp quang?**
   - **UTP**: giá rẻ, dễ lắp đặt, phổ biến nhưng khoảng cách hạn chế, dễ bị nhiễu.
   - **Cáp quang**: tốc độ cao, khoảng cách xa, chống nhiễu tốt nhưng chi phí cao, lắp đặt phức tạp.
4. **Mục đích của chuẩn hóa (standards) ở tầng Vật lý là gì?**
   - Đảm bảo thiết bị của các hãng khác nhau có thể hoạt động cùng nhau.
   - Giúp triển khai mạng đồng nhất, giảm chi phí và tăng tính tương thích.
5. **Tín hiệu số khác gì tín hiệu tương tự trong truyền dữ liệu?**
   - **Tín hiệu số**: biểu diễn dữ liệu bằng các mức rời rạc (0 và 1), dễ phát hiện lỗi, ít nhiễu.
   - **Tín hiệu tương tự**: biểu diễn dữ liệu bằng sóng liên tục, dễ bị suy hao và nhiễu.

4.5 Bài tập Chương 4

1. Một frame Ethernet có kích thước 1,538 byte được truyền trên đường truyền 100 Mbps. Hãy tính thời gian truyền (transmission time) của frame này.

   Đáp án: $1538 \times 8 = 12,304$ bit. Thời gian $t = \dfrac{12,304}{100 \times 10^6} = 1.2304 \times 10^{-4}$ s = 123.04 μs.

2. Một đường truyền 1 Gbps có độ trễ lan truyền 5 µs/km. Tính độ trễ lan truyền trên đường cáp quang dài 200 km.

   Đáp án: Độ trễ = $200 \times 5 = 1000$ $\mu s = 1$ ms.

3. Một tín hiệu có băng thông 5 MHz. Theo định lý Nyquist, tốc độ dữ liệu tối đa là bao nhiêu khi dùng 4 mức tín hiệu (M = 4)?

   Đáp án: Công thức: $C = 2 \times B \times \log_2 M$. $C = 2 \times 5 \times 10^6 \times \log_2 4 = 10^7 \times 2 = 20$ Mbps.

4. Một đường truyền có băng thông 1 MHz và tỉ số tín hiệu/nhiễu (SNR) = 20 dB. Tính dung lượng kênh theo định lý Shannon.

   Đáp án: $SNR_{linear} = 10^{20 \Uparrow 10} = 100$. $C = B \times \log_2 1 + SNR = 10^6 \times \log_2 101 \approx 10^6 \times 6.658 = 6.658$ Mbps.

5. Một đường truyền tốc độ 100 Mbps, độ trễ lan truyền 200 µs. Hãy tính *delay-bandwidth product* (kích thước đường ống bit).

   Đáp án: $100 \times 10^6 \times 200 \times 10^{-6} = 20,000$ bit = 2.5 KB.

6. Một cáp UTP loại Cat5e hỗ trợ tốc độ 1000 Mbps. Nếu chiều dài cáp là 80 m, với tốc độ truyền ánh sáng trong cáp là 2×10^8 m/s, tính độ trễ lan truyền.

   Đáp án: $t = \dfrac{80}{2 \times 10^8} = 4 \times 10^{-7}$ s = 0.4 μs.

7. Một frame 1500 byte được truyền qua đường 10 Mbps. Hãy tính thời gian truyền frame.

   Đáp án: $1500 \times 8 = 12,000$ bit. $t = \dfrac{12,000}{10 \times 10^6} = 1.2 \times 10^{-3}$ s = 1.2 ms.

8. Một tín hiệu số có tốc độ baud là 2,400 baud. Nếu mỗi symbol mang 8 bit thông tin, hãy tính tốc độ dữ liệu.

   Đáp án: $R = 2400 \times 8 = 19,200$ bps.

9. Một đường truyền có băng thông 2 MHz, SNR = 30 dB. Hãy tính dung lượng kênh tối đa theo định lý Shannon.

   Đáp án: $SNR_{linear} = 10^{30 \Uparrow 10} = 1000$. $C = 2 \times 10^6 \times \log_2 1001 \approx 2 \times 10^6 \times 9.967 = 19.934$ Mbps.

10. Một frame có kích thước 1200 byte. Trên đường truyền 1.5 Mbps, hãy tính thời gian truyền frame.

    Đáp án: $1200 \times 8 = 9600$ bit. $t = \dfrac{9600}{1.5 \times 10^6} = 6.4 \times 10^{-3}$ s = 6.4 *ms*.

4.6 Thuật ngữ cần nhớ

Physical Layer (Tầng Vật lý) Tầng thấp nhất trong mô hình OSI, chịu trách nhiệm truyền các bit 0/1 dưới dạng tín hiệu điện, quang hoặc vô tuyến qua phương tiện vật lý.

Encoding Quá trình chuyển đổi dãy bit thành tín hiệu cụ thể (điện áp, ánh sáng, sóng) để có thể truyền đi trên đường truyền vật lý.

Signaling Phương pháp biểu diễn và truyền các bit trên phương tiện truyền: tín hiệu số (digital) hoặc tín hiệu tương tự (analog).

Bandwidth Dải tần số hoặc dung lượng tối đa mà đường truyền có thể hỗ trợ, ảnh hưởng đến tốc độ dữ liệu.

Throughput Tốc độ dữ liệu thực tế đạt được trên đường truyền sau khi tính đến nhiễu, tranh chấp và các yếu tố hạn chế khác.

Goodput Tốc độ dữ liệu hữu ích đến được ứng dụng cuối, không tính phần overhead (header, trailer) hoặc gói bị lỗi.

UTP Cable (Unshielded Twisted Pair) Loại cáp đồng xoắn đôi không bọc chống nhiễu, phổ biến trong Ethernet LAN. Gồm 4 cặp dây xoắn để giảm nhiễu chéo.

STP Cable (Shielded Twisted Pair) Cáp xoắn đôi có bọc kim loại chống nhiễu, dùng trong môi trường nhiều nhiễu điện từ.

Fiber-optic Cable Cáp sợi quang dùng ánh sáng để truyền tín hiệu. Ưu điểm: tốc độ cao, khoảng cách xa, miễn nhiễm nhiễu điện từ.

Wireless Media Phương tiện truyền vô tuyến dùng sóng radio, hồng ngoại hoặc vi ba. Ví dụ: Wi-Fi, Bluetooth, 4G/5G.

EMI (Electromagnetic Interference) Nhiễu điện từ gây ảnh hưởng đến tín hiệu truyền trên dây cáp đồng.

RFI (Radio Frequency Interference) Nhiễu tần số vô tuyến do các nguồn phát sóng radio gây ra, làm suy giảm chất lượng tín hiệu.

Crosstalk Hiện tượng nhiễu chéo giữa các cặp dây trong cùng một bó cáp, làm sai lệch tín hiệu.

Straight-through Cable Loại cáp UTP có đầu nối theo chuẩn giống nhau ở hai đầu, dùng để kết nối các thiết bị khác loại (PC ↔ switch, switch ↔ router).

Crossover Cable Loại cáp UTP có đầu nối đảo ngược một số cặp dây, dùng để kết nối các thiết bị cùng loại (PC ↔ PC, switch ↔ switch).

Rollover Cable Cáp dùng để kết nối PC với cổng console của thiết bị mạng để cấu hình, còn gọi là console cable.

Pinout Sơ đồ xác định chức năng của từng chân (pin) trong đầu nối cáp, ví dụ: chuẩn T568A, T568B cho RJ-45.

T568A/T568B Hai chuẩn bấm dây phổ biến cho cáp Ethernet. Straight-through dùng cùng một chuẩn ở hai đầu; crossover dùng một đầu T568A, một đầu T568B.

Data Rate Tốc độ dữ liệu (bit/s) mà đường truyền có thể đạt được, phụ thuộc vào phương tiện truyền và công nghệ mã hóa.

Latency Độ trễ khi dữ liệu đi từ nguồn tới đích, bao gồm thời gian xử lý, truyền dẫn và lan truyền.

Physical Topology Cách bố trí kết nối vật lý (hình sao, bus, vòng, lưới) giữa các thiết bị mạng.

Hub Thiết bị tầng vật lý, nhận tín hiệu từ một cổng rồi phát lại ra tất cả các cổng khác, không phân biệt địa chỉ.

Bit Đơn vị dữ liệu nhỏ nhất trong máy tính, chỉ có giá trị 0 hoặc 1; là thông tin cơ bản mà tầng Vật lý truyền tải.

Chương 5

Hệ thống số

Mục tiêu

Sau khi hoàn thành chương này, bạn sẽ có thể:

- Giải thích lý do tại sao cần nhiều hệ thống số trong mạng máy tính.
- Chuyển đổi giữa hệ thập phân, nhị phân và thập lục phân.
- Biểu diễn địa chỉ IPv4, IPv6 và địa chỉ MAC bằng nhiều hệ thống số.
- Hiểu cách máy tính xử lý dữ liệu dạng bit và byte.

Thuật ngữ chính

- Decimal (thập phân)
- Binary (nhị phân)
- Hexadecimal (thập lục phân)
- Bit, Byte, Nibble
- IPv4, IPv6
- MAC address
- Conversion (chuyển đổi)

5.1 Giới thiệu

Máy tính và thiết bị mạng lưu trữ và xử lý dữ liệu bằng **hệ nhị phân**. Con người lại quen làm việc với **hệ thập phân**. Để kết nối hai thế giới này, ta phải biết cách chuyển đổi giữa các hệ thống số: nhị phân, thập phân và thập lục phân.

5.2 Hệ Thập phân

- Cơ số: 10
- Các chữ số: 0–9
- Ví dụ: 247 trong thập phân = $2 \times 10^2 + 4 \times 10^1 + 7 \times 10^0$

5.3 Hệ Nhị phân

- Cơ số: 2
- Các chữ số: 0 và 1
- Mỗi chữ số gọi là một **bit** (binary digit).
- 1 byte = 8 bit, 1 nibble = 4 bit.
- Ví dụ: 1101 trong nhị phân = $1 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$ = 13 thập phân.

5.4 Hệ Thập lục phân

- Cơ số: 16
- Các chữ số: 0–9 và A–F (A=10, B=11, . . . , F=15)
- Ví dụ: 0x2F (hex) = $2 \times 16^1 + 15 \times 16^0$ = 47 thập phân.

5.5 Chuyển đổi giữa các hệ thống số

5.5.1 Thập phân – Nhị phân

- **Ví dụ**: 10 thập phân = 1010 nhị phân.
- Cách làm: chia liên tiếp cho 2, lấy phần dư, đọc ngược.

5.5.2 Thập phân – Thập lục phân

- **Ví dụ**: 255 thập phân = FF hex.
- Cách làm: chia liên tiếp cho 16, lấy phần dư, đọc ngược.

5.5.3 Nhị phân – Thập lục phân

- Nhóm 4 bit = 1 ký tự hex.
- **Ví dụ**: 1111 1111 (binary) = FF (hex).

5.6 Ứng dụng trong địa chỉ mạng

5.6.1 IPv4

- Được viết theo dạng thập phân chấm (dot-decimal).
- Ví dụ: 192.168.1.1 trong nhị phân là 11000000.10101000.00000001.00000001

5.6.2 IPv6

- Được viết ở dạng thập lục phân, gồm 8 nhóm 16 bit (4 ký tự hex).
- Ví dụ: 2001:0db8:0000:0000:0000:ff00:0042:8329
- Có thể rút gọn bằng cách bỏ số 0 ở đầu hoặc thay chuỗi các nhóm 0 bằng “::”.

5.6.3 Địa chỉ MAC

- Viết bằng hex, 6 byte (48 bit).
- Ví dụ: 00-1A-2B-3C-4D-5E

Tóm tắt

- Máy tính sử dụng hệ nhị phân để lưu trữ dữ liệu.
- Người dùng thường sử dụng thập phân; hex được dùng để rút gọn nhị phân.
- Cần thành thạo chuyển đổi giữa ba hệ số này để đọc và phân tích địa chỉ mạng.
- IPv4 dùng thập phân chấm, IPv6 và MAC dùng hex.

Câu hỏi ôn tập

1. **Tại sao kỹ sư mạng cần hiểu các hệ thống số?**
   - Địa chỉ IP, địa chỉ MAC, mặt nạ mạng và nhiều giá trị cấu hình được biểu diễn bằng hệ nhị phân hoặc thập lục phân.
   - Hiểu hệ số giúp phân tích, chuyển đổi và xử lý dữ liệu mạng chính xác.
2. **Sự khác nhau cơ bản giữa hệ thập phân, nhị phân và thập lục phân là gì?**
   - **Thập phân (Decimal)**: cơ số 10, ký số 0–9.
   - **Nhị phân (Binary)**: cơ số 2, ký số 0 và 1.
   - **Thập lục phân (Hexadecimal)**: cơ số 16, ký số 0–9 và A–F.
3. **Chuyển đổi số nhị phân 110101 thành số thập phân.**
   - $110101_2 = 1 \times 2^5 + 1 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$
   - $= 32 + 16 + 0 + 4 + 0 + 1 = 53$
   - Vậy $110101_2 = 53_{10}$
4. **Chuyển số thập phân 255 sang hệ nhị phân và thập lục phân.**
   - Nhị phân: $255_{10} = 11111111_2$
   - Thập lục phân: $255_{10} = FF_{16}$
5. **Tại sao địa chỉ IPv6 thường viết bằng thập lục phân thay vì nhị phân?**
   - Địa chỉ IPv6 dài 128 bit → nếu viết nhị phân sẽ rất dài và khó đọc.
   - Thập lục phân rút gọn, dễ biểu diễn và dễ quản lý hơn.

5.7 Bài tập Chương 5

1. Chuyển số nhị phân 11010101_2 sang thập phân và thập lục phân.

   Đáp án:
   Thập phân: $1\cdot 2^7 + 1\cdot 2^6 + 0\cdot 2^5 + 1\cdot 2^4 + 0\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0 = 213_{10}$.
   Thập lục phân: nhóm nibble $1101\,0101_2 = D5_{16}$.

2. Chuyển 345_{10} sang nhị phân và thập lục phân.

   Đáp án:
   Nhị phân: $345 = 256 + 64 + 16 + 8 + 1 \Rightarrow 1\,0101\,1001_2 = 101011001_2$.
   Thập lục phân: chia $1010\,1100\,1 \Rightarrow 0010\,1011\,0001_2 = 0x161$ (hoặc tính trực tiếp: $345 \uparrow 16 = 21$ dư 9, $21 \uparrow 16 = 1$ dư 5, $1 \uparrow 16 = 0$ dư $1 \Rightarrow 0x159$).
   Lưu ý: Cách chia nhị phân ở trên bị lệch; làm lại theo phép chia 16 đúng: $345 = 16\cdot 21 + 9$, $21 = 16\cdot 1 + 5$ $\Rightarrow \boxed{345_{10} = 0x159}$. Kiểm tra: $1\cdot 256 + 5\cdot 16 + 9 = 256 + 80 + 9 = 345$.

3. Viết địa chỉ IPv4 192.168.14.200 ở dạng nhị phân (theo từng octet).

   Đáp án:
   192 = 11000000, 168 = 10101000, 14 = 00001110, 200 = 11001000.
   $\Rightarrow \boxed{11000000.10101000.00001110.11001000}$.

4. Cho nhị phân $1011\,0110_2$. Hãy đổi sang thập lục phân và giải thích cách nhóm nibble.

   Đáp án:
   Nhóm nibble từ trái: $1011\,0110 = B6_{16}$ vì $1011_2 = B$, $0110_2 = 6$.
   $\Rightarrow \boxed{0xB6}$.

5. Biểu diễn số thập phân -37 bằng bù hai (two's complement) trên 8 bit.

   Đáp án:
   $37_{10} = 0010\,0101_2$ (8 bit). Đảo bit: 1101 1010. Cộng 1: 1101 1011.
   $\Rightarrow \boxed{11011011_2}$.

6. Cho số thập lục phân $0xCAF3$. Hãy chuyển sang nhị phân và thập phân.

   Đáp án:
   Nhị phân: $C = 1100$, $A = 1010$, $F = 1111$, $3 = 0011 \Rightarrow \boxed{1100\,1010\,1111\,0011_2}$.
   Thập phân: $C\cdot 16^3 + A\cdot 16^2 + F\cdot 16 + 3 = 12\cdot 4096 + 10\cdot 256 + 15\cdot 16 + 3$
   $= 49{,}152 + 2{,}560 + 240 + 3 = \boxed{51{,}955_{10}}$.

7. Một subnet /27 có bao nhiêu địa chỉ host khả dụng? Viết subnet mask dạng thập phân chấm.

   Đáp án:
   Số bit host = $32 - 27 = 5 \Rightarrow$ tổng địa chỉ $2^5 = 32$, host khả dụng = $32 - 2 = \boxed{30}$.
   Subnet mask: /27 = $255.255.255.11100000_2 = \boxed{255.255.255.224}$.

8. Đổi $1001\,1101\,0110_2$ sang thập lục phân và thập phân.

   Đáp án:
   Bổ sung 0 cho đủ bội số 4: 0010 0111 0101 10 → đúng là 1001 1101 0110 đã là 12 bit, nhóm: 1001 1101 0110 = $9D6 \Rightarrow \boxed{0x9D6}$.
   Thập phân: $9\cdot 16^2 + 13\cdot 16 + 6 = 9\cdot 256 + 208 + 6 = 2304 + 214 = \boxed{2{,}518}$.

9. Viết địa chỉ MAC `00:1A:2B:3C:4D:5E` thành nhị phân (theo từng octet 8 bit).

Đáp án:
00 = 00000000, 1A = 00011010, 2B = 00101011, 3C = 00111100, 4D = 01001101, 5E = 01011110.
$\Rightarrow$ $\boxed{0000000000011010010101100111100010011010101110}$.

10. Một dải mạng có prefix `/20`. Hãy cho biết:

    (a) Số bit dành cho host.

    (b) Số địa chỉ tổng và số host khả dụng.

    (c) Subnet mask dạng thập phân chấm.

Đáp án:
(a) 32 – 20 = 12 bit host.
(b) Tổng địa chỉ = 2^{12} = 4096, host khả dụng = 4096 – 2 = $\boxed{4094}$.
(c) /20 = 255.255.11110000_2.0 = 255.255.240.0 $\Rightarrow$ $\boxed{255.255.240.0}$.

5.8 Thuật ngữ cần nhớ

Number System (Hệ thống số) Tập hợp các ký hiệu và quy tắc dùng để biểu diễn số. Trong mạng máy tính, thường dùng hệ thập phân, nhị phân, thập lục phân.

Decimal (Thập phân) Hệ số có cơ số 10, sử dụng các chữ số từ 0 đến 9. Đây là hệ số phổ biến nhất trong đời sống hàng ngày của con người.

Binary (Nhị phân) Hệ số có cơ số 2, chỉ gồm hai chữ số 0 và 1. Mọi dữ liệu trong máy tính và mạng đều được biểu diễn dưới dạng nhị phân.

Hexadecimal (Thập lục phân) Hệ số có cơ số 16, sử dụng các chữ số 0–9 và ký tự A–F (A=10, B=11, . . . , F=15). Được dùng nhiều trong biểu diễn địa chỉ MAC và IPv6.

Bit Đơn vị dữ liệu nhỏ nhất, có thể là 0 hoặc 1. Tất cả thông tin đều được lưu trữ và truyền tải dưới dạng bit.

Nibble Nhóm gồm 4 bit, có thể biểu diễn giá trị từ 0 đến 15 (tương đương một chữ số thập lục phân).

Byte Nhóm gồm 8 bit, biểu diễn giá trị từ 0 đến 255 trong hệ thập phân. Byte là đơn vị cơ bản để đo kích thước dữ liệu.

Word Tập hợp nhiều byte (thường 2 hoặc 4 byte) mà CPU xử lý trong một chu kỳ. Kích thước word phụ thuộc vào kiến trúc bộ xử lý (16-bit, 32-bit, 64-bit).

Base (Cơ số) Số lượng ký hiệu trong một hệ thống số. Ví dụ: cơ số của hệ nhị phân là 2, của hệ thập phân là 10, của hệ thập lục phân là 16.

Positional Notation (Ký hiệu vị trí) Giá trị của mỗi chữ số phụ thuộc vào vị trí của nó trong số, tính bằng: chữ số $\times$ (cơ số)$^{\text{vị trí}}$. Ví dụ: $1011_2 = 1\times2^3 + 0\times2^2 + 1\times2^1 + 1\times2^0$.

Conversion (Chuyển đổi hệ số) Quá trình đổi số từ hệ này sang hệ khác, ví dụ: từ nhị phân sang thập phân, từ thập phân sang thập lục phân.

Octal (Bát phân) Hệ số có cơ số 8, dùng các chữ số 0–7. Trước đây được dùng trong máy tính vì dễ chuyển đổi từ nhị phân (3 bit = 1 chữ số bát phân).

Most Significant Bit (MSB) Bit quan trọng nhất, nằm bên trái cùng trong một số nhị phân. Nó có trọng số lớn nhất.

Least Significant Bit (LSB) Bit ít quan trọng nhất, nằm bên phải cùng trong một số nhị phân. Nó có trọng số nhỏ nhất.

Two's Complement Phương pháp biểu diễn số nguyên âm trong nhị phân bằng cách đảo bit và cộng thêm 1. Đây là cách phổ biến trong máy tính.

IPv4 Address Representation Địa chỉ IPv4 32 bit thường viết dưới dạng thập phân chấm, ví dụ: 192.168.1.1.

IPv6 Address Representation Địa chỉ IPv6 128 bit thường viết dưới dạng thập lục phân, chia thành 8 nhóm cách nhau bởi dấu hai chấm, ví dụ: 2001:0db8::1.

Address Notation Cách viết biểu diễn địa chỉ. IPv4 dùng dạng dotted decimal, IPv6 dùng dạng colon-hexadecimal.

Subnet Mask Một giá trị nhị phân dùng để phân biệt phần mạng và phần host trong địa chỉ IP. Thường viết dưới dạng thập phân chấm (ví dụ: 255.255.255.0).

CIDR Notation Cách viết rút gọn mặt nạ mạng bằng ký hiệu "/n" trong đó n là số bit của phần mạng. Ví dụ: 192.168.1.0/24.

Chương 6

Tầng Liên kết dữ liệu

Mục tiêu

Sau khi hoàn thành chương này, bạn sẽ có thể:

- Mô tả vai trò của tầng liên kết dữ liệu trong truyền thông mạng.
- Phân biệt các chức năng chính: đóng gói khung, địa chỉ hóa, phát hiện lỗi, truy cập môi trường.
- Giải thích cách tầng liên kết dữ liệu hỗ trợ các công nghệ LAN và WAN.
- Mô tả các loại topo logic và vật lý liên quan.
- Liên hệ chuẩn IEEE 802 với hoạt động của tầng liên kết.

Thuật ngữ chính

- Data Link Layer
- Frame
- MAC address
- LLC (Logical Link Control)
- Access Method
- Error detection
- CSMA/CD, CSMA/CA
- Point-to-Point, Multiaccess
- Half-duplex, Full-duplex
- ARP
- Encapsulation
- WAN protocols (PPP, HDLC)

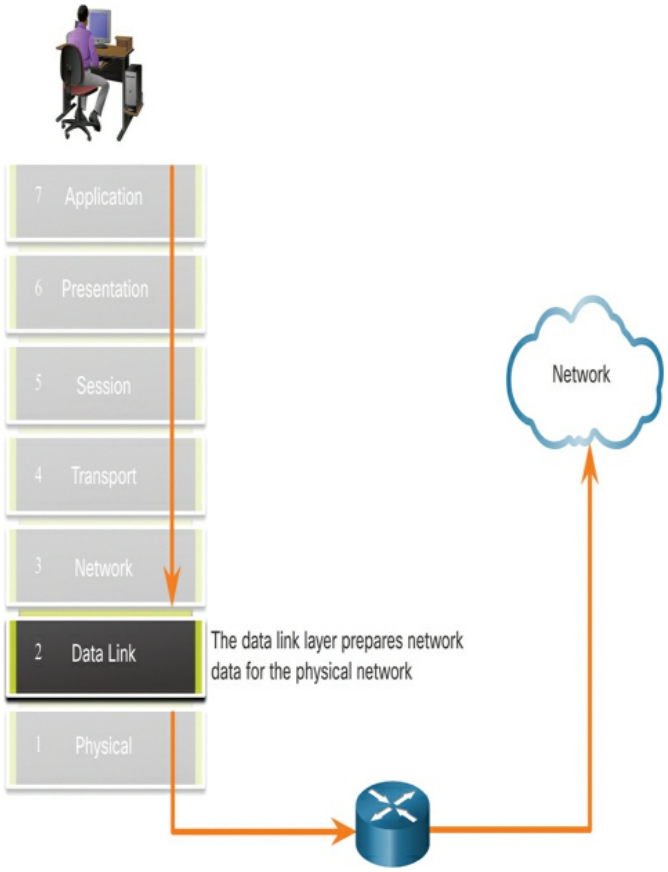
6.1 Giới thiệu

Tầng liên kết dữ liệu của mô hình OSI chuẩn bị gói dữ liệu từ tầng mạng để truyền qua phương tiện vật lý, như minh họa trong Hình 6.1. Nó chịu trách nhiệm **đóng gói khung (frame)**, địa chỉ hóa ở mức liên kết, phát hiện lỗi cơ bản và kiểm soát truy cập môi trường.

6.2 Chức năng của tầng liên kết dữ liệu

6.2.1 Đóng gói dữ liệu

- Nhận **gói tin** từ tầng mạng, thêm tiêu đề (header) và phần kiểm tra (trailer) để tạo **khung (frame)**.



Hình 6.1: Mục đích của tầng Liên kết dữ liệu.

- Header chứa địa chỉ MAC nguồn và đích.
- Trailer thường chứa **FCS (Frame Check Sequence)** để phát hiện lỗi.

6.2.2 Điều khiển truy cập

- Quy định thiết bị nào có quyền sử dụng đường truyền tại một thời điểm.
- Ví dụ: Ethernet dùng **CSMA/CD**, Wifi dùng **CSMA/CA**.

6.2.3 Địa chỉ hóa ở tầng liên kết

- Sử dụng địa chỉ vật lý (MAC, 48 bit) để định danh thiết bị trong mạng LAN.
- Địa chỉ MAC thường được ghi sẵn trong card mạng, biểu diễn bằng hex.

6.3 Cấu trúc khung dữ liệu

Một khung điển hình gồm:

- **Preamble**: đồng bộ tín hiệu.
- **Header**: chứa địa chỉ MAC nguồn và đích, loại EtherType hoặc độ dài.
- **Payload**: dữ liệu thực tế từ tầng mạng.

- **Trailer**: FCS dùng để phát hiện lỗi.

6.4 Các phương thức truyền

6.4.1 Kết nối điểm-điểm (Point-to-Point)

Liên kết trực tiếp hai thiết bị. Đơn giản, hiệu quả cho WAN.

6.4.2 Kết nối đa truy nhập (Multiaccess)

Nhiều thiết bị cùng chia sẻ một đường truyền, cần cơ chế kiểm soát truy cập (CSMA/CD, CSMA/CA).

6.4.3 Truyền song công (Duplex)

- **Half-duplex**: dữ liệu chỉ truyền theo một hướng tại một thời điểm (giống bộ đàm).
- **Full-duplex**: dữ liệu có thể truyền hai hướng đồng thời.

6.5 Tầng LLC và MAC

- **LLC (Logical Link Control)**: xác định giao thức lớp mạng nào được đóng gói (IPv4, IPv6).
- **MAC (Media Access Control)**: xác định địa chỉ vật lý, điều khiển truy cập môi trường.

6.6 Tầng liên kết trong LAN và WAN

6.6.1 LAN

- LAN dựa trên chuẩn IEEE 802 (Ethernet 802.3, Wifi 802.11).
- Sử dụng địa chỉ MAC để định danh thiết bị.

6.6.2 WAN

- WAN có nhiều công nghệ khác nhau: PPP, HDLC, Frame Relay, MPLS.
- Các giao thức này cũng hoạt động ở tầng liên kết để đóng gói dữ liệu qua đường truyền diện rộng.

6.7 Topo logic và vật lý

- **Topo vật lý**: cách thiết bị và cáp bố trí thực tế (sao, bus, vòng, lưới).
- **Topo logic**: cách dữ liệu thực sự di chuyển (broadcast, point-to-point, switched).

Tóm tắt

- Tầng liên kết dữ liệu chuẩn bị dữ liệu từ tầng mạng để truyền qua môi trường vật lý.
- Các chức năng: đóng gói khung, địa chỉ hóa, phát hiện lỗi, kiểm soát truy cập.
- Khung dữ liệu gồm header (địa chỉ MAC), payload, trailer (FCS).

- LAN dùng địa chỉ MAC và chuẩn IEEE 802; WAN có các giao thức riêng như PPP, HDLC.
- Topo vật lý và topo logic là hai cách nhìn khác nhau về mạng.

Câu hỏi ôn tập

1. **Chức năng chính của tầng Liên kết dữ liệu (Data Link Layer) là gì?**
   - Đóng gói dữ liệu từ tầng Mạng thành khung (frame) để truyền qua phương tiện vật lý.
   - Phát hiện lỗi cơ bản trong quá trình truyền.
   - Điều khiển truy cập vào môi trường truyền (MAC).
2. **Sự khác biệt giữa điều khiển truy cập theo điểm-điểm (point-to-point) và đa điểm (multipoint)?**
   - **Point-to-point**: kết nối trực tiếp giữa hai nút, không cần cơ chế chia sẻ môi trường.
   - **Multipoint**: nhiều nút dùng chung môi trường → cần cơ chế điều khiển truy cập để tránh xung đột.
3. **Địa chỉ MAC khác địa chỉ IP ở điểm nào?**
   - MAC: địa chỉ vật lý, gắn cố định trong card mạng, duy nhất toàn cầu.
   - IP: địa chỉ logic, có thể thay đổi, dùng để định tuyến qua nhiều mạng.
4. **Mục đích của CRC (Cyclic Redundancy Check) trong khung dữ liệu là gì?**
   - Phát hiện lỗi trong quá trình truyền dữ liệu.
   - Bên nhận kiểm tra CRC, nếu sai thì loại bỏ khung.
5. **Ví dụ về giao thức hoạt động ở tầng Liên kết dữ liệu.**
   - Ethernet (IEEE 802.3).
   - Wi-Fi (IEEE 802.11).
   - PPP (Point-to-Point Protocol).

6.8 Bài tập Chương 6

1. Một frame Ethernet có tổng chiều dài 1518 byte, trong đó header + trailer chiếm 18 byte. Hãy tính kích thước phần dữ liệu (payload) và phần overhead.

   Đáp án:
   Payload = 1518 – 18 = 1500 byte. Overhead = 18 byte.

2. Một mạng LAN có 12 thiết bị kết nối qua một switch. Hãy tính số miền va chạm (collision domain) và số miền quảng bá (broadcast domain).

   Đáp án:
   Switch tạo ra một collision domain cho mỗi cổng ⇒ 12 collision domain. Broadcast domain chỉ có 1 (toàn bộ switch).

3. Một mạng dùng hub kết nối 10 thiết bị. Hãy cho biết số miền va chạm và miền quảng bá.

   Đáp án:
   Hub không tách miền va chạm ⇒ toàn bộ là 1 collision domain. Broadcast domain = 1.

4. Một khung Ethernet có payload 1000 byte. Header 18 byte. Hãy tính tỷ lệ overhead so với toàn bộ frame.

   Đáp án:
   Tổng = 1000 + 18 = 1018 byte. Overhead ratio = $\frac{18}{1018} \approx 1.77\%$.

5. Một switch có 24 cổng, mỗi cổng 100 Mbps full-duplex. Hãy tính tổng băng thông lý thuyết toàn bộ switch có thể hỗ trợ.

   Đáp án:
   Mỗi cổng full-duplex: $100 \times 2 = 200$ Mbps. 24 cổng $\Rightarrow 24 \times 200 = 4800$ Mbps = 4.8 Gbps.

6. Một frame Ethernet gồm: địa chỉ MAC nguồn 6 byte, MAC đích 6 byte, Ethertype 2 byte, dữ liệu 46–1500 byte, FCS 4 byte. Hãy tính kích thước frame tối thiểu và tối đa.

   Đáp án:
   Tối thiểu = 6 + 6 + 2 + 46 + 4 = 64 byte. Tối đa = 6 + 6 + 2 + 1500 + 4 = 1518 byte.

7. Một frame 1200 byte được truyền trên đường truyền 100 Mbps. Hãy tính thời gian truyền frame này.

   Đáp án:
   $1200 \times 8 = 9600$ bit. $t = \frac{9600}{100 \times 10^6} = 9.6 \times 10^{-5}$ s = 96 μs.

8. Một VLAN có 200 host. Hãy tính số bit host tối thiểu cần thiết trong subnet và subnet mask tương ứng.

   Đáp án:
   Cần ≥ 200 host khả dụng $\Rightarrow 2^n - 2 \geq 200 \Rightarrow n = 8$. Subnet mask = 32 − 8 = 24 $\Rightarrow$ 255.255.255.0.

9. Một switch học được 4 địa chỉ MAC: A trên cổng 1, B trên cổng 2, C trên cổng 3, D trên cổng 4. Nếu A gửi unicast đến C, hãy mô tả cách switch xử lý.

   Đáp án:
   Switch nhìn bảng MAC, thấy C ở cổng 3. Switch chuyển tiếp frame chỉ ra cổng 3 (unicast forwarding).

10. Một switch có 8 cổng, mỗi cổng kết nối một PC. Nếu PC1 gửi broadcast, hãy tính số frame được gửi ra và đến bao nhiêu thiết bị.

    Đáp án:
    Switch sẽ sao chép frame broadcast ra tất cả 7 cổng còn lại. Tổng số frame gửi ra = 7. Tổng số thiết bị nhận được = 7.

6.9 Thuật ngữ cần nhớ

Data Link Layer (Tầng Liên kết dữ liệu) Tầng 2 trong mô hình OSI, chịu trách nhiệm đóng gói dữ liệu từ tầng Mạng thành khung (frame), kiểm soát truy cập môi trường, phát hiện lỗi và quản lý địa chỉ MAC.

Frame (Khung dữ liệu) Đơn vị dữ liệu tại tầng Liên kết dữ liệu, bao gồm: header (địa chỉ MAC nguồn/đích, thông tin kiểm soát), payload (dữ liệu từ tầng Mạng), trailer (FCS).

MAC Address (Địa chỉ MAC) Địa chỉ vật lý duy nhất gán cho mỗi card mạng, dài 48 bit (6 byte), thường viết ở dạng thập lục phân: `00:1A:2B:3C:4D:5E`.

Logical Link Control (LLC) Tiểu tầng trên của tầng Liên kết dữ liệu, cung cấp giao diện giữa tầng Mạng và tầng Liên kết dữ liệu, xác định giao thức lớp trên (IP, IPv6).

Media Access Control (MAC sublayer) Tiểu tầng dưới của tầng Liên kết dữ liệu, kiểm soát việc truy cập phương tiện truyền, xác định địa chỉ MAC nguồn/đích trong khung.

FCS (Frame Check Sequence) Chuỗi bit trong trailer của frame, dùng thuật toán CRC để phát hiện lỗi truyền.

CRC (Cyclic Redundancy Check) Cơ chế toán học tạo giá trị kiểm tra trong FCS, giúp phát hiện lỗi trong quá trình truyền khung.

Half-duplex Kiểu truyền trong đó thiết bị chỉ có thể gửi hoặc nhận tại một thời điểm (không đồng thời). Ví dụ: mạng Ethernet dùng hub.

Full-duplex Kiểu truyền trong đó thiết bị có thể đồng thời gửi và nhận dữ liệu. Ví dụ: mạng Ethernet dùng switch.

Point-to-Point Topology Tô-pô kết nối trực tiếp giữa hai thiết bị mạng, đơn giản và hiệu quả.

Multiaccess Topology Tô-pô trong đó nhiều thiết bị chia sẻ cùng một phương tiện truyền, ví dụ: nhiều PC cùng kết nối Wi-Fi.

Ring Topology Tô-pô vòng, trong đó các thiết bị được kết nối tuần tự và khép kín thành một vòng.

Ethernet Công nghệ mạng LAN phổ biến dựa trên chuẩn IEEE 802.3, sử dụng CSMA/CD để kiểm soát truy cập môi trường trong các hệ thống cũ (dùng hub), còn switch hiện đại loại bỏ va chạm.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) Cơ chế truy cập môi trường của Ethernet truyền thống: thiết bị "nghe sóng mang" trước khi truyền, và khi va chạm xảy ra, sẽ phát hiện và truyền lại sau thời gian ngẫu nhiên.

Switch Thiết bị mạng tầng 2 có khả năng học địa chỉ MAC và chuyển tiếp khung đến đúng cổng đích, giảm thiểu va chạm so với hub.

Hub Thiết bị tầng vật lý hoạt động theo cơ chế quảng bá: nhận tín hiệu ở một cổng và phát lại ra tất cả các cổng khác, gây ra nhiều va chạm.

Collision Domain Miền va chạm, tập hợp các thiết bị chia sẻ cùng một phương tiện truyền, trong đó chỉ một thiết bị có thể truyền tại một thời điểm. Switch giảm kích thước collision domain xuống từng cổng.

Broadcast Domain Miền quảng bá, tập hợp thiết bị có thể nhận gói broadcast (địa chỉ MAC FF:FF:FF:FF:FF:FF). Router chia tách broadcast domain.

VLAN (Virtual LAN) Mạng LAN ảo, cho phép tách lưu lượng trong cùng một switch thành các miền logic khác nhau nhằm tăng bảo mật và hiệu quả.

MTU (Maximum Transmission Unit) Kích thước payload lớn nhất của frame có thể truyền qua một giao diện mạng, ví dụ: Ethernet MTU = 1500 byte.

Chương 7

Chuyển mạch Ethernet

Mục tiêu

Sau khi hoàn thành chương này, bạn sẽ có thể:

- Mô tả cấu trúc và chức năng của Ethernet trong LAN.
- Giải thích cách switch xây dựng và sử dụng bảng địa chỉ MAC.
- Mô tả quá trình chuyển tiếp và lọc khung trong mạng Ethernet.
- Phân biệt collision domain và broadcast domain.
- Giải thích nguyên lý hoạt động full-duplex và half-duplex.
- Liên hệ chuẩn IEEE 802.3 với hoạt động Ethernet hiện đại.

Thuật ngữ chính

- Ethernet
- MAC address
- Switch
- Frame forwarding
- Collision domain
- Broadcast domain
- Learning process
- Aging process
- Duplex
- Auto-MDIX

7.1 Giới thiệu

Ethernet là công nghệ LAN phổ biến nhất hiện nay. Nó dựa trên chuẩn IEEE 802.3 và sử dụng địa chỉ MAC để định danh thiết bị. Các switch Ethernet hiện đại cho phép truyền thông hiệu quả, giảm xung đột và mở rộng mạng dễ dàng.

7.2 Nguyên lý hoạt động của Ethernet

7.2.1 Cấu trúc khung Ethernet

Một khung Ethernet gồm:

- Preamble và SFD (Start Frame Delimiter)
- Địa chỉ MAC đích và nguồn (48 bit)
- EtherType/Length
- Payload (dữ liệu)
- FCS (Frame Check Sequence)

7.2.2 Địa chỉ MAC

- Địa chỉ MAC là địa chỉ vật lý 48 bit, được ghi trong NIC.
- Viết ở dạng hex, ví dụ: 00:1A:2B:3C:4D:5E
- Bao gồm phần OUI (Organizationally Unique Identifier) và phần định danh NIC.

7.3 Chuyển mạch Ethernet

7.3.1 Switch và bảng MAC

Switch học địa chỉ MAC bằng cách:

- Quan sát địa chỉ MAC nguồn trong các khung đến.
- Ghi địa chỉ đó vào bảng MAC, gắn với cổng nhận.
- Khi có khung gửi đến địa chỉ đích, switch tra bảng để chuyển tiếp đến đúng cổng.
- Nếu chưa biết địa chỉ, switch phát khung ra tất cả các cổng (flooding).

7.3.2 Quá trình aging

Các bản ghi trong bảng MAC có thời gian sống. Nếu không thấy địa chỉ được dùng lại sau một khoảng thời gian, switch sẽ xóa bản ghi để tiết kiệm bộ nhớ.

7.3.3 Chuyển tiếp khung

Switch hoạt động ở tầng liên kết dữ liệu, chuyển tiếp khung dựa trên địa chỉ MAC. Điều này khác router, hoạt động ở tầng mạng và dựa vào địa chỉ IP.

7.4 Miền xung đột và miền quảng bá

- **Collision domain**: tập hợp các thiết bị mà khi hai thiết bị truyền cùng lúc sẽ xảy ra xung đột. Switch tạo collision domain riêng cho mỗi cổng.
- **Broadcast domain**: tập hợp các thiết bị nhận cùng một gói broadcast. Switch không tách broadcast domain; để tách cần dùng router hoặc VLAN.

7.5 Chế độ song công và tốc độ

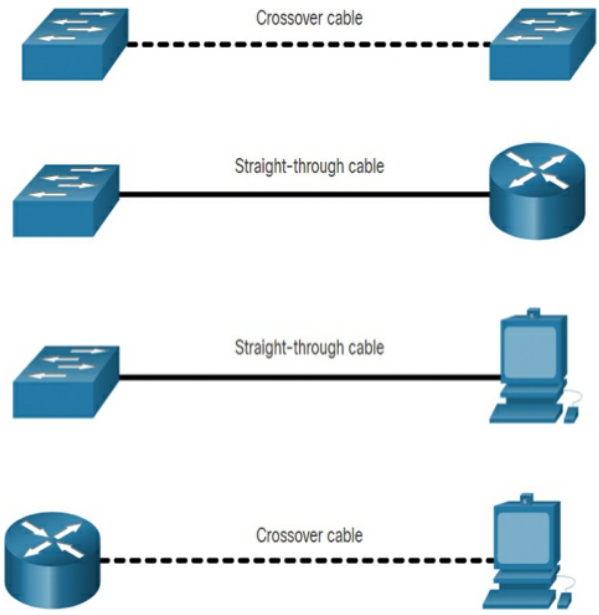
7.5.1 Half-duplex

Thiết bị chỉ truyền hoặc nhận tại một thời điểm. Thường dùng trong hub cũ.

7.5.2 Full-duplex

Thiết bị có thể truyền và nhận đồng thời, loại bỏ xung đột, tăng hiệu quả. Hầu hết thiết bị hiện đại đều hỗ trợ full-duplex.

7.5.3 Auto-negotiation và Auto-MDIX



Hình 7.1: Các loại cáp và mục đích kết nối.

- **Auto-negotiation**: thiết bị tự thương lượng tốc độ và chế độ duplex.
- **Auto-MDIX**: cổng switch tự động điều chỉnh loại cáp (thẳng hoặc chéo).

Tóm tắt

- Ethernet là công nghệ LAN chính, dựa trên địa chỉ MAC để chuyển tiếp khung.
- Switch học địa chỉ MAC và lưu trong bảng MAC để chuyển tiếp hiệu quả.
- Collision domain bị chia nhỏ bởi switch, nhưng broadcast domain thì không.
- Ethernet hỗ trợ half-duplex và full-duplex, với full-duplex mang lại hiệu quả cao hơn.
- Các tính năng auto-negotiation và auto-MDIX giúp đơn giản hóa cấu hình và triển khai.

Câu hỏi ôn tập

1. **Chức năng chính của switch trong mạng Ethernet là gì?**
   - Kết nối nhiều thiết bị trong cùng một mạng LAN.
   - Chuyển tiếp khung dữ liệu dựa trên địa chỉ MAC.
   - Giảm va chạm (collision) bằng cách tạo các miền xung đột riêng cho mỗi cổng.
2. **Bảng địa chỉ MAC (MAC address table) được switch xây dựng như thế nào?**
   - Switch học địa chỉ MAC nguồn từ khung đi vào cổng.
   - Ghi ánh xạ giữa địa chỉ MAC và cổng tương ứng vào bảng.
   - Dùng bảng để quyết định chuyển khung ra cổng nào.
3. **Sự khác biệt giữa unicast, broadcast và multicast trong Ethernet?**
   - **Unicast**: khung gửi từ một nguồn đến một đích cụ thể.
   - **Broadcast**: khung gửi đến tất cả thiết bị trong mạng LAN.
   - **Multicast**: khung gửi đến một nhóm thiết bị quan tâm.
4. **Tại sao cần VLAN trong mạng Ethernet?**
   - Tách biệt logic các thiết bị trong cùng switch thành nhiều mạng LAN ảo.
   - Tăng tính bảo mật và hiệu quả sử dụng băng thông.
   - Giúp quản lý dễ dàng hơn.
5. **Lệnh nào thường dùng để kiểm tra trạng thái cổng và bảng MAC trên switch Cisco?**
   - `show mac address-table` – xem bảng địa chỉ MAC.
   - `show interfaces status` – xem trạng thái các cổng.

7.6 Bài tập Chương 7

1. Một switch có 48 cổng, mỗi cổng hỗ trợ 1 Gbps full-duplex. Hãy tính tổng băng thông lý thuyết tối đa mà switch có thể xử lý.

   Đáp án:
   Mỗi cổng full-duplex: $1 \times 2 = 2$ Gbps. $48 \times 2 = 96$ Gbps.

2. Một switch có bảng MAC như sau: {MAC A–cổng1, MAC B–cổng2, MAC C–cổng3}. Nếu một frame từ A gửi đến D (chưa có trong bảng), switch xử lý thế nào?

   Đáp án:
   Switch chưa biết MAC D, sẽ flood frame ra tất cả các cổng ngoại trừ cổng 1 (nguồn).

3. Một frame 1500 byte được truyền qua switch tốc độ 100 Mbps. Hãy tính thời gian truyền frame qua một cổng.

   Đáp án:
   $1500 \times 8 = 12{,}000$ bit. $t = \dfrac{12{,}000}{100 \times 10^6} = 1.2 \times 10^{-4}$ s $= 120\ \mu s$.

4. Một switch nhận 1000 frame/giây, mỗi frame dài trung bình 800 byte. Hãy tính tổng lưu lượng dữ liệu (throughput) mà switch đang xử lý.

   Đáp án:
   $1000 \times 800 \times 8 = 6.4 \times 10^6$ bit/s = 6.4 Mbps.

5. Một switch hoạt động ở chế độ cut-through. Nếu độ dài khung là 1200 byte và switch chỉ cần đọc 14 byte đầu để xác định cổng đích, hãy tính độ trễ xử lý (switching latency) khi tốc độ đường truyền là 100 Mbps.

   Đáp án:
   $14 \times 8 = 112$ bit. Thời gian đọc = $112 \Uparrow 100 \times 10^6 = 1.12\ \mu s$.

6. Một switch store-and-forward nhận 1518 byte/frame. Nếu tốc độ đường truyền 1 Gbps, hãy tính độ trễ xử lý tối thiểu do cơ chế store-and-forward.

   Đáp án:
   $1518 \times 8 = 12,144$ bit. Thời gian đọc toàn bộ frame = $12,144 \Uparrow 10^9 = 12.144\ \mu s$.

7. Một switch có 24 cổng, mỗi cổng 100 Mbps. Nếu tất cả các cổng hoạt động đồng thời và đều gửi lưu lượng đến cùng một cổng uplink 1 Gbps, hãy xác định mức độ tắc nghẽn (congestion).

   Đáp án:
   Tổng lưu lượng vào = $24 \times 100 = 2400$ Mbps. Cổng uplink chỉ 1000 Mbps. Tắc nghẽn = $2400 - 1000 = 1400$ Mbps (tương đương thừa 140% so với khả năng uplink).

8. Một switch có bảng MAC lưu được tối đa 4096 địa chỉ. Nếu trong mạng có 5000 thiết bị hoạt động, hãy cho biết điều gì xảy ra.

   Đáp án:
   Khi số địa chỉ MAC vượt quá khả năng lưu trữ, switch sẽ loại bỏ (aging) hoặc quên một số bản ghi. Các frame đến đích bị quên sẽ phải flood ra tất cả các cổng, gây tăng broadcast traffic.

9. Một switch học được địa chỉ MAC với thời gian aging 300 giây. Nếu một host không truyền dữ liệu trong 10 phút, điều gì xảy ra?

   Đáp án:
   10 phút = 600 giây > 300 giây. Địa chỉ MAC của host sẽ bị xóa khỏi bảng. Khi host gửi lại, switch sẽ học lại địa chỉ đó.

10. Một VLAN trên switch chứa 120 host. Hãy tính số bit host cần thiết và subnet mask phù hợp.

    Đáp án:
    Cần ≥ 120 host khả dụng. $2^7 - 2 = 126$ host ≥ 120. Vậy cần 7 bit cho phần host. Subnet mask = $32 - 7 = 25 \Rightarrow$ 255.255.255.128.

7.7 Thuật ngữ cần nhớ

Ethernet Switching Công nghệ chuyển mạch trong Ethernet dùng switch để chuyển tiếp khung dữ liệu dựa trên địa chỉ MAC, thay thế hub nhằm tăng hiệu năng và giảm va chạm.

MAC Address Table (Bảng địa chỉ MAC) Bảng trong switch lưu trữ ánh xạ giữa địa chỉ MAC của thiết bị và cổng switch tương ứng. Switch học địa chỉ MAC bằng cách quan sát địa chỉ nguồn của khung đi vào.

Frame Forwarding Cơ chế switch quyết định chuyển tiếp khung đến cổng nào dựa trên địa chỉ MAC đích trong bảng MAC.

Flooding Khi switch không biết địa chỉ MAC đích, nó sẽ phát (flood) khung ra tất cả các cổng ngoại trừ cổng nhận, cho đến khi học được vị trí của MAC đích.

Unicast Gói tin gửi đến một địa chỉ MAC duy nhất, chỉ được chuyển đến đúng thiết bị đích.

Broadcast Gói tin có địa chỉ MAC FF:FF:FF:FF:FF:FF, được chuyển đến tất cả thiết bị trong cùng một broadcast domain.

Multicast Gói tin gửi đến một nhóm thiết bị quan tâm, sử dụng địa chỉ MAC multicast đặc biệt.

Switching Table Lookup Quá trình switch tra cứu bảng MAC để xác định cổng chuyển tiếp khung.

Collision Domain Miền va chạm, trong đó các thiết bị chia sẻ cùng phương tiện truyền và có thể gây va chạm khi truyền đồng thời. Switch tách collision domain theo từng cổng.

Broadcast Domain Tập hợp tất cả thiết bị nhận được bản tin broadcast. Router hoặc Layer 3 switch giới hạn phạm vi broadcast domain.

Store-and-Forward Switching Chế độ hoạt động của switch: nhận toàn bộ frame, kiểm tra lỗi (FCS) trước khi chuyển tiếp. Độ trễ cao hơn nhưng an toàn.

Cut-Through Switching Chế độ switch chuyển tiếp frame ngay khi đọc được địa chỉ MAC đích (trước khi nhận toàn bộ frame). Độ trễ thấp nhưng dễ chuyển tiếp khung lỗi.

Fragment-Free Switching Phiên bản trung gian: switch đọc 64 byte đầu tiên (vì va chạm thường xảy ra trong 64 byte đầu), rồi mới chuyển tiếp.

Port-based Microsegmentation Mỗi cổng của switch tạo thành một miền va chạm riêng, cung cấp băng thông đầy đủ cho từng kết nối.

Duplex Setting Cấu hình chế độ truyền cho cổng: half-duplex hoặc full-duplex. Full-duplex loại bỏ va chạm và tăng băng thông hiệu quả.

Auto-MDIX (Automatic Medium-Dependent Interface Crossover) Chức năng tự động trên switch hiện đại, cho phép cổng Ethernet tự động điều chỉnh để dùng được cả cáp thẳng và cáp chéo.

Switch Boot Sequence Trình tự khởi động của switch: POST (Power-On Self-Test), tải hệ điều hành IOS, tải cấu hình khởi động từ NVRAM.

Forwarding Rate Tốc độ switch có thể xử lý và chuyển tiếp khung, đo bằng số khung/giây (fps) hoặc bit/giây.

Switch Security Features Các cơ chế bảo mật cơ bản trên switch, ví dụ: Port Security (giới hạn số lượng MAC), bảo vệ DHCP Snooping, BPDU Guard.

Chương 8

Tầng Mạng

Mục tiêu

Sau khi hoàn thành chương này, bạn sẽ có thể:

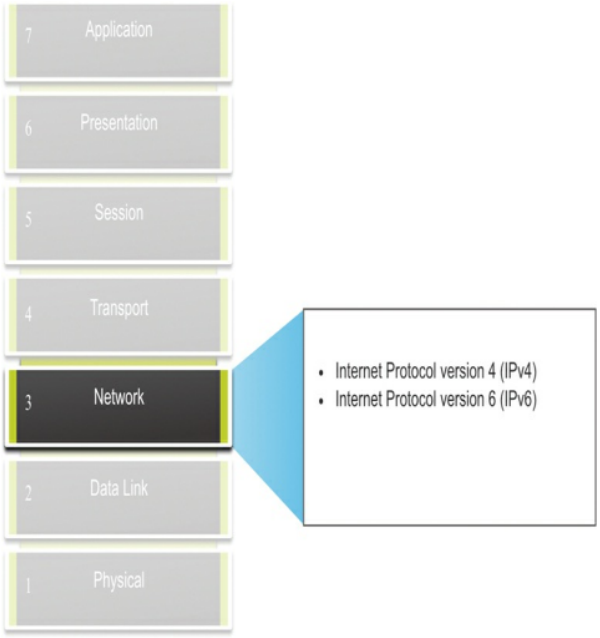
- Mô tả vai trò của tầng mạng trong mô hình OSI.
- Giải thích chức năng định địa chỉ logic và định tuyến.
- Mô tả sự khác biệt giữa IPv4 và IPv6.
- Trình bày quá trình đóng gói và chuyển tiếp gói dữ liệu (packet).
- Phân tích bảng định tuyến và quyết định chuyển tiếp.
- Hiểu nguyên lý hoạt động của router trong mạng.

Thuật ngữ chính

- Network layer
- Packet
- IPv4, IPv6
- Routing
- Router
- Hop
- Encapsulation
- Connectionless
- Best-effort delivery
- MTU (Maximum Transmission Unit)
- Routing table
- Static route / Dynamic routing

8.1 Giới thiệu

Tầng mạng nằm trên tầng Liên kết dữ liệu (Data Link) và dưới tầng Vận chuyển (Transport) như minh họa trong Hình 8.1, chịu trách nhiệm cung cấp dịch vụ truyền dữ liệu từ thiết bị nguồn đến thiết bị đích qua nhiều mạng trung gian. Nó sử dụng **địa chỉ logic** (IP) để định danh thiết bị và **router** để chọn đường đi tối ưu.



Hình 8.1: Vị trí tầng Mạng trong mô hình OSI.

8.2 Chức năng của tầng mạng

8.2.1 Định địa chỉ logic

- Địa chỉ IP xác định vị trí của thiết bị trong mạng.
- Địa chỉ IP khác với địa chỉ MAC: MAC là cố định phần cứng, IP có thể thay đổi.

8.2.2 Kết nối không hướng kết nối

- Tầng mạng hoạt động theo cơ chế **connectionless** (không thiết lập phiên trước).
- Các gói có thể đi theo các tuyến khác nhau và đến không theo thứ tự.

8.2.3 Dịch vụ best-effort

- Không đảm bảo gói tin luôn đến đích, cũng không đảm bảo thứ tự.
- Tầng vận chuyển (TCP) sẽ chịu trách nhiệm độ tin cậy nếu cần.

8.2.4 Tính độc lập của phương tiện

Tầng mạng hoạt động độc lập với loại phương tiện truyền dẫn. Gói IP có thể đi qua Ethernet, Wifi, PPP, Frame Relay, MPLS.

8.3 Cấu trúc gói IP

8.3.1 IPv4 Packet

Gồm các trường chính:

- Địa chỉ nguồn và đích (32 bit)
- TTL (Time to Live)
- Protocol (xác định tầng trên, ví dụ TCP, UDP, ICMP)
- Header checksum

8.3.2 IPv6 Packet

- Địa chỉ nguồn và đích (128 bit)
- Fixed header đơn giản hơn IPv4
- Không có checksum trong header
- Hỗ trợ extension header cho tính năng bổ sung

8.4 Router và chuyển tiếp gói

8.4.1 Chức năng của router

- Nhận gói từ một giao diện, tra cứu bảng định tuyến, chuyển tiếp qua giao diện khác.
- Tách biệt broadcast domain.

8.4.2 Quá trình định tuyến

1. Nhận gói và kiểm tra địa chỉ đích.
2. Tìm tuyến phù hợp nhất trong bảng định tuyến.
3. Nếu tìm thấy, chuyển tiếp gói qua giao diện tương ứng.
4. Nếu không, bỏ gói hoặc gửi ICMP unreachable.

8.5 Bảng định tuyến

- Chứa danh sách các mạng đích và cổng/giao diện tương ứng.
- Có thể cấu hình tĩnh (static route) hoặc học động (dynamic routing protocols: RIP, OSPF, EIGRP, BGP).

8.6 Định tuyến tĩnh và động

8.6.1 Định tuyến tĩnh

- Do quản trị viên cấu hình thủ công.
- Ưu điểm: đơn giản, kiểm soát tốt.
- Nhược điểm: không tự thích ứng khi có thay đổi.

8.6.2 Định tuyến động

- Router trao đổi thông tin để tự động cập nhật bảng định tuyến.
- Có nhiều giao thức: RIP (simple), OSPF (link-state), EIGRP (hybrid), BGP (inter-domain).

Tóm tắt

- Tầng mạng cung cấp dịch vụ truyền gói giữa các thiết bị qua nhiều mạng.
- Địa chỉ IP là định danh logic, khác với địa chỉ MAC.
- IP hoạt động connectionless, best-effort, độc lập phương tiện.
- IPv4 có địa chỉ 32 bit, IPv6 có 128 bit với header đơn giản hơn.
- Router định tuyến và chuyển tiếp gói dựa trên bảng định tuyến.
- Có hai loại định tuyến: tĩnh và động.

Câu hỏi ôn tập

1. **Chức năng chính của tầng Mạng là gì?**
    - Định tuyến gói tin từ nguồn đến đích qua nhiều mạng trung gian.
    - Gán địa chỉ logic (IP) cho thiết bị để định danh toàn cầu.
2. **Sự khác biệt giữa địa chỉ IP và địa chỉ MAC?**
    - Địa chỉ IP: logic, có thể thay đổi, dùng để định tuyến qua nhiều mạng.
    - Địa chỉ MAC: vật lý, gắn cố định trong phần cứng, dùng trong phạm vi LAN.
3. **Tại sao cần chia gói dữ liệu thành các packet thay vì gửi nguyên khối lớn?**
    - Giúp truyền tải hiệu quả và quản lý băng thông.
    - Cho phép định tuyến linh hoạt, các packet có thể đi theo đường khác nhau.
    - Giảm rủi ro mất mát: nếu một packet bị mất thì chỉ cần gửi lại phần đó.
4. **Vai trò của router trong tầng Mạng là gì?**
    - Kết nối các mạng khác nhau.
    - Quyết định đường đi tốt nhất cho packet dựa trên bảng định tuyến.
5. **Một số giao thức hoạt động ở tầng Mạng?**
    - IPv4, IPv6.
    - ICMP (hỗ trợ báo lỗi và chẩn đoán).
    - Các giao thức định tuyến: OSPF, EIGRP, RIP, BGP.

8.7 Bài tập Chương 8

1. Một gói IPv4 có TTL ban đầu là 64. Nó đi qua 12 router trước khi đến đích. TTL còn lại tại đích là bao nhiêu?

   Đáp án:
   TTL giảm 1 mỗi lần qua router. 64 – 12 = 52.

2. Một mạng có prefix `192.168.16.0/20`. Hãy tính số địa chỉ IP tổng cộng và số host khả dụng trong mạng này.

   Đáp án:
   Số bit host = 32 – 20 = 12. Tổng địa chỉ = 2^{12} = 4096. Host khả dụng = 4096 – 2 = 4094.

3. Một router có 3 tuyến: `192.168.0.0/16 via S0/0`, `192.168.64.0/18 via S0/1`, `192.168.64.0/24 via S0/2`. Nếu gói tin có đích `192.168.64.55`, nó sẽ đi theo tuyến nào?

   Đáp án:
   Cả 3 tuyến đều khớp. Router chọn tuyến có prefix dài nhất (/24). ⇒ gói đi ra `S0/2`.

4. Một router kết nối 4 mạng LAN, mỗi mạng cần 500 host. Hãy chọn mặt nạ mạng tối thiểu phù hợp cho từng mạng con.

   Đáp án:
   Cần ≥ 500 host ⇒ $2^9 - 2 = 510$. Cần 9 bit host, subnet mask = 32 – 9 = 23. ⇒ mỗi mạng con /23.

5. Một gói IPv4 dài 3000 byte đi qua đường truyền có MTU = 1500 byte. Hãy tính số mảnh IP được tạo và kích thước mỗi mảnh.

   Đáp án:
   MTU = 1500 byte (bao gồm header 20 byte). Payload tối đa mỗi mảnh = 1480 byte. 3000 payload / 1480 = 2 mảnh (1 mảnh 1480, 1 mảnh 1520). Thực tế: 1 mảnh = 1480 + 20 = 1500 byte, 1 mảnh = 1520 + 20 = 1540 byte. Tổng số mảnh = 2.

6. Một mạng có prefix `10.0.0.0/8`. Nếu chia thành các subnet /20, hãy tính số subnet tạo được.

   Đáp án:
   Số bit mượn = 20 – 8 = 12. Số subnet = 2^{12} = 4096.

7. Một router có default route `0.0.0.0/0` trỏ về `Serial0/0`. Nếu một gói tin có đích `8.8.8.8` không khớp tuyến cụ thể nào, nó sẽ đi theo đâu?

   Đáp án:
   Router dùng default route. Gói đi ra cổng `Serial0/0`.

8. Một mạng `172.16.0.0/16` được chia thành 64 subnet bằng VLSM. Hãy tính prefix length của mỗi subnet.

   Đáp án:
   Cần 64 subnet ⇒ $\log_2 64 = 6$ bit mượn. Prefix = 16 + 6 = 22. ⇒ mỗi subnet là /22.

9. Một router xử lý trung bình 100,000 gói/giây. Mỗi gói có chiều dài 1000 byte. Hãy tính throughput (tốc độ xử lý dữ liệu) của router này.

   Đáp án:
   $100{,}000 \times 1000 \times 8 = 8 \times 10^8$ bps = 800 Mbps.

10. Một gói IPv4 có header 20 byte và payload 1480 byte. Hãy tính: (a) Kích thước gói IP. (b) Tỷ lệ overhead so với toàn bộ gói.

    Đáp án:
    (a) 20 + 1480 = 1500 byte. (b) Overhead ratio = $\frac{20}{1500} \approx 1.33\%$.

8.8 Thuật ngữ cần nhớ

Network Layer (Tầng Mạng) Tầng 3 trong mô hình OSI, chịu trách nhiệm định tuyến và chuyển tiếp gói tin từ nguồn đến đích qua một hoặc nhiều mạng trung gian.

Packet (Gói tin) Đơn vị dữ liệu của tầng Mạng, bao gồm header (địa chỉ IP nguồn/đích, TTL, v.v.) và payload (dữ liệu từ tầng Vận chuyển).

IPv4 Phiên bản địa chỉ IP dài 32 bit, cung cấp khoảng 2^{32} địa chỉ. Viết dưới dạng thập phân chấm (ví dụ: 192.168.1.1).

IPv6 Phiên bản địa chỉ IP dài 128 bit, cung cấp không gian địa chỉ rất lớn (2^{128}). Viết dưới dạng thập lục phân, phân cách bởi dấu hai chấm (ví dụ: 2001:db8::1).

Routing Quá trình lựa chọn đường đi tối ưu để gói tin đi từ nguồn đến đích qua các mạng trung gian.

Router Thiết bị mạng tầng 3, dùng bảng định tuyến để quyết định hướng đi của gói tin.

Routing Table (Bảng định tuyến) Cơ sở dữ liệu trong router chứa các mạng đích, địa chỉ kế tiếp (next-hop) và giao diện ra tương ứng.

Default Gateway Router trong mạng LAN mà host gửi gói tin khi đích nằm ngoài subnet cục bộ.

Hop Một lần gói tin được chuyển tiếp qua một router trung gian.

Time-to-Live (TTL) Trường trong header IP, giảm đi 1 khi gói tin đi qua một router; khi TTL = 0 thì gói bị loại bỏ. Dùng để ngăn vòng lặp định tuyến.

Connectionless Đặc điểm của giao thức IP: không thiết lập kết nối trước khi gửi gói tin, mỗi gói được xử lý độc lập.

Best-effort Delivery IP chỉ cố gắng chuyển gói đến đích mà không đảm bảo độ tin cậy (không xác nhận, không sửa lỗi).

Media Independent Tầng Mạng hoạt động độc lập với phương tiện truyền vật lý; IP có thể chạy trên Ethernet, Wi-Fi, cáp quang, v.v.

Network Address Phần địa chỉ IP dùng để xác định một mạng hoặc subnet, thường có các bit host bằng 0.

Host Address Phần địa chỉ IP dùng để định danh một thiết bị cụ thể trong subnet.

Subnet Mask Giá trị 32 bit đi kèm địa chỉ IPv4, chỉ rõ bao nhiêu bit thuộc phần mạng và bao nhiêu bit thuộc phần host.

Prefix Length Cách viết rút gọn subnet mask bằng CIDR, ví dụ: /24 thay cho 255.255.255.0.

Default Route Tuyến mặc định trong bảng định tuyến, được dùng khi không tìm thấy mạng đích cụ thể nào khác (`0.0.0.0/0` hoặc `::/0`).

Static Route Tuyến được cấu hình thủ công trên router, không thay đổi tự động.

Dynamic Routing Protocol Giao thức giúp router học và cập nhật bảng định tuyến tự động, ví dụ: RIP, OSPF, EIGRP, BGP.

ICMP (Internet Control Message Protocol) Giao thức hỗ trợ báo lỗi và chẩn đoán, ví dụ: thông điệp Destination Unreachable, Echo Request/Reply (ping).

ARP (Address Resolution Protocol) Giao thức phân giải địa chỉ IPv4 sang địa chỉ MAC trong mạng LAN.

NDP (Neighbor Discovery Protocol) Giao thức trong IPv6 thay thế ARP, ICMPv4, và cung cấp thêm khả năng tự động cấu hình (SLAAC).

Fragmentation Quá trình chia gói IP thành nhiều mảnh nhỏ khi vượt quá MTU của đường truyền; mỗi mảnh có header riêng.

Chương 9

Phân giải địa chỉ

Mục tiêu

Sau khi hoàn thành chương này, bạn sẽ có thể:

- Giải thích sự cần thiết của phân giải địa chỉ trong mạng TCP/IP.
- Mô tả hoạt động của ARP trong IPv4.
- Mô tả hoạt động của Neighbor Discovery trong IPv6.
- Hiểu cách phân giải tên thành địa chỉ bằng DNS.
- Mô tả vai trò của giao thức DHCP trong cấp phát địa chỉ IP động.

Thuật ngữ chính

- ARP (Address Resolution Protocol)
- ARP request / ARP reply
- ARP table / cache
- Gratuitous ARP
- DNS (Domain Name System)
- DHCP (Dynamic Host Configuration Protocol)
- IPv6 Neighbor Discovery (ND)
- ICMPv6
- SLAAC (Stateless Address Autoconfiguration)

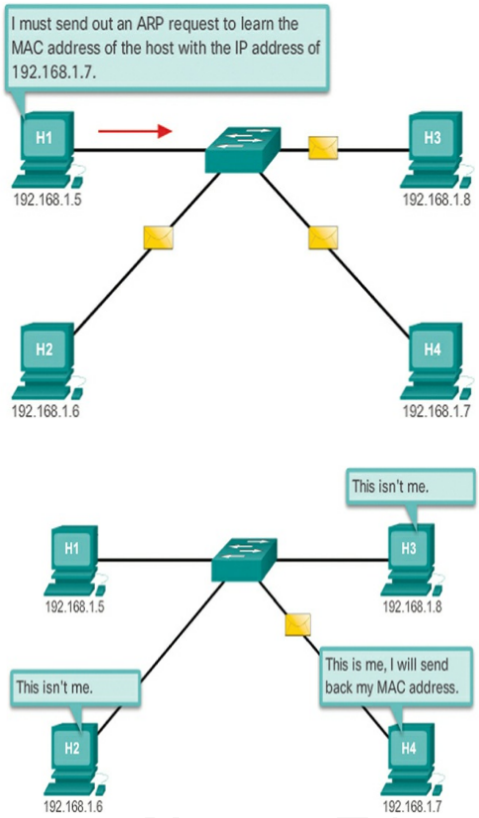
9.1 Giới thiệu

Các thiết bị trong mạng giao tiếp bằng địa chỉ IP (logic) và địa chỉ MAC (vật lý). Để truyền một gói tin, thiết bị cần ánh xạ từ địa chỉ IP sang địa chỉ MAC của đích trong cùng mạng. Đây chính là chức năng của **Address Resolution**.

9.2 Phân giải địa chỉ trong IPv4

9.2.1 ARP

- **ARP** dùng để tìm địa chỉ MAC tương ứng với địa chỉ IPv4 trong cùng subnet.
- Khi thiết bị cần gửi gói IP ($H1$) mà chưa biết MAC đích, nó gửi **ARP Request** (broadcast).
- Thiết bị có địa chỉ IP khớp ($H4$) sẽ trả lời bằng **ARP Reply** (unicast).



9.2.2 Bảng ARP

- Thiết bị lưu kết quả phân giải trong **ARP cache**.
- Mỗi bản ghi có thời hạn, sau đó sẽ bị xóa nếu không dùng lại.

9.2.3 Vấn đề bảo mật

- ARP không có cơ chế xác thực, dễ bị tấn công **ARP spoofing/poisoning**.
- Giải pháp: dùng bảo mật switch (DHCP snooping, Dynamic ARP Inspection).

9.3 Phân giải địa chỉ trong IPv6

9.3.1 Neighbor Discovery (ND)

- IPv6 không dùng ARP, thay vào đó dùng **ICMPv6 Neighbor Discovery**.
- Các thông điệp chính: **Neighbor Solicitation**, **Neighbor Advertisement**.
- Cơ chế này vừa phân giải địa chỉ MAC, vừa kiểm tra tính sẵn sàng của nút đích.

9.3.2 SLAAC và DHCPv6

- **SLAAC** cho phép host tự cấu hình địa chỉ IPv6 dựa trên prefix từ router.
- **DHCPv6** có thể cấp phát thông tin bổ sung (DNS, gateway).

9.4 Phân giải tên miền

9.4.1 DNS

- Con người dùng tên miền (www.example.com), trong khi máy dùng địa chỉ IP.
- DNS phân giải tên miền sang địa chỉ IP.
- DNS dùng hệ thống phân cấp máy chủ: Root, TLD, Authoritative.

9.4.2 Quy trình truy vấn DNS

1. Ứng dụng gửi truy vấn DNS (thường UDP port 53).
2. Resolver cục bộ hỏi máy chủ gốc, rồi TLD, rồi máy chủ có thẩm quyền.
3. Đáp án được trả về và có thể lưu cache.

9.5 Cấp phát địa chỉ IP động

9.5.1 DHCP cho IPv4

- Thiết bị gửi **DHCP Discover** (broadcast).
- Máy chủ DHCP trả lời bằng **DHCP Offer**.
- Thiết bị phản hồi **DHCP Request**.
- Máy chủ xác nhận bằng **DHCP Acknowledgment**.

9.5.2 DHCPv6

- Tương tự quy trình trên, dùng các thông điệp DHCPv6.
- Có thể hoạt động song song với SLAAC.

Tóm tắt

- Trong IPv4, phân giải địa chỉ dùng ARP để tìm MAC từ IP.
- Trong IPv6, dùng Neighbor Discovery thay cho ARP.
- DNS phân giải tên miền thành địa chỉ IP.
- DHCP cấp phát địa chỉ IP động và thông số cấu hình mạng.

Câu hỏi ôn tập

1. **Chức năng của ARP trong IPv4 là gì?**
    - Ánh xạ địa chỉ IPv4 (logic) sang địa chỉ MAC (vật lý) trong cùng mạng LAN.
    - Cho phép thiết bị gửi gói dữ liệu đến đúng máy đích trong subnet.
2. **Tại sao IPv6 không sử dụng ARP?**

- IPv6 dùng Neighbor Discovery Protocol (NDP) dựa trên ICMPv6 để thay thế ARP.
- NDP vừa phân giải địa chỉ, vừa phát hiện trùng lặp địa chỉ, và hỗ trợ tự cấu hình SLAAC.

3. **Các bước cơ bản của quy trình phân giải DNS là gì?**
   - Client gửi truy vấn DNS (thường UDP port 53).
   - Resolver hỏi lần lượt máy chủ gốc, TLD, rồi máy chủ có thẩm quyền.
   - Địa chỉ IP được trả về cho client và có thể lưu trong cache.
4. **Sự khác biệt giữa DHCPv4 và DHCPv6 là gì?**
   - DHCPv4 cấp phát địa chỉ IPv4 động cùng subnet mask, gateway, DNS.
   - DHCPv6 cấp phát địa chỉ IPv6 và thông tin bổ sung, có thể phối hợp với SLAAC.
5. **Rủi ro bảo mật nào liên quan đến ARP?**
   - ARP không có cơ chế xác thực → dễ bị tấn công giả mạo (ARP spoofing/poisoning).
   - Kẻ tấn công có thể chuyển hướng lưu lượng để nghe lén hoặc tấn công từ chối dịch vụ.

9.6 Bài tập Chương 9

1. Một host gửi gói đến đích `192.168.1.50`, nhưng bảng ARP cache trống. Hãy mô tả và tính số bản tin ARP cần trao đổi trước khi host có thể gửi gói tin đến đích.

   Đáp án:
   Host gửi 1 bản tin ARP Request (broadcast). Đích trả lời 1 bản tin ARP Reply (unicast). Tổng số bản tin ARP cần trao đổi = 2.

2. Một bảng ARP chứa 80 bản ghi, mỗi bản ghi chiếm 32 byte bộ nhớ. Hãy tính dung lượng bộ nhớ bảng ARP cần.

   Đáp án:
   $80 \times 32 = 2560$ byte = 2.5 KB.

3. Một host có thời gian sống (timeout) cho bản ghi ARP là 300 giây. Nếu host cần liên lạc 100 lần với cùng một đích trong vòng 10 phút, hãy tính số lần phải phát sinh lại ARP.

   Đáp án:
   10 phút = 600 giây. Thời gian sống bản ghi = 300 giây. Sau khi hết hạn, host phải gửi ARP lại. Trong 600 giây, ARP cần phát sinh lại $600 \uparrow 300 = 2$ lần. Tổng số lần ARP = 1 lần ban đầu + 1 lần gia hạn = 2 lần.

4. Trong một LAN có 200 thiết bị, một host gửi ARP Request broadcast. Hãy tính số thiết bị nhận được gói ARP Request.

   Đáp án:
   Tất cả thiết bị trong LAN đều nhận. Tổng số thiết bị nhận = 199 (trừ thiết bị gửi).

5. Một attacker gửi 500 gói ARP Spoofing/giây vào mạng. Nếu bảng ARP của switch chứa tối đa 4096 bản ghi, hãy ước tính thời gian để bảng bị tràn.

   Đáp án:
   $4096 \uparrow 500 \approx 8.19$ giây. Vậy khoảng 8 giây bảng ARP sẽ bị tràn.

6. Một địa chỉ IPv6 link-local bắt đầu bằng `FE80::/10`. Hãy cho biết prefix length của dải này và tính số địa chỉ IPv6 khả dụng trong dải.

   Đáp án:
   Prefix length = 10 bit. Số bit host = 128-10 = 118. Tổng số địa chỉ = 2^{118} (rất lớn, thực tế giới hạn bởi phạm vi liên kết).

7. Một host gửi Neighbor Solicitation trong IPv6 để phân giải địa chỉ. Nếu mạng có 50 host, hãy tính số bản tin nhận được trong trường hợp broadcast (ARP của IPv4) và trong multicast (IPv6 NDP).

   Đáp án:
   IPv4 ARP: tất cả 49 host khác nhận. IPv6 NDP: chỉ nhóm multicast liên quan nhận (thường 1 host mục tiêu). So sánh: 49 gói vs 1 gói.

8. Nếu một host IPv4 dùng ARP để phân giải địa chỉ MAC và mất trung bình 2 ms cho một lần ARP, hãy tính tổng độ trễ khi 20 địa chỉ mới cần phân giải.

   Đáp án:
   $20 \times 2 = 40$ ms.

9. Một switch lưu trữ 1024 bản ghi ARP. Nếu mỗi bản ghi có thời gian sống 240 giây và trong 1 giờ có 3000 host tham gia, hãy ước tính bao nhiêu bản ghi có nguy cơ bị xóa do timeout.

   Đáp án:
   1 giờ = 3600 giây. Số chu kỳ timeout = $3600 \Uparrow 240 = 15$. Nếu host không gửi dữ liệu lại, bản ghi sẽ bị xóa sau 240 giây. Do có 3000 host và chỉ 1024 slot, tối thiểu $3000 - 1024 = 1976$ host có thể bị mất bản ghi.

10. Một attacker thực hiện ARP Spoofing, gửi sai MAC cho địa chỉ IP gateway. Nếu gateway MAC gốc là `AA:BB:CC:DD:EE:FF`, attacker giả mạo thành `11:22:33:44:55:66`, hãy giải thích điều gì xảy ra khi host gửi dữ liệu ra ngoài mạng.

    Đáp án:
    Host cập nhật ARP Cache bằng MAC giả. Tất cả gói tin gửi ra ngoài đi đến attacker thay vì router. Attacker có thể chặn, nghe lén, hoặc chỉnh sửa dữ liệu (Man-in-the-Middle).

9.7 Thuật ngữ cần nhớ

Address Resolution Quá trình ánh xạ địa chỉ logic (IP) sang địa chỉ vật lý (MAC) để gói tin có thể được truyền trong mạng LAN.

ARP (Address Resolution Protocol) Giao thức ánh xạ địa chỉ IPv4 sang địa chỉ MAC. Host gửi bản tin ARP Request để hỏi MAC tương ứng với một IP, và nhận về ARP Reply.

ARP Table (Bảng ARP Cache) Bảng lưu trữ tạm thời ánh xạ giữa địa chỉ IPv4 và địa chỉ MAC trên host hoặc router. Các bản ghi có thời gian sống (timeout).

ARP Request Bản tin broadcast trong đó một host hỏi "Ai có địa chỉ IP X.X.X.X? Hãy trả lời bằng địa chỉ MAC của bạn".

ARP Reply Bản tin unicast trả lời yêu cầu ARP, chứa địa chỉ MAC của host sở hữu IP được hỏi.

Gratuitous ARP Một gói ARP Reply không được yêu cầu, được host gửi đi để thông báo sự thay đổi địa chỉ MAC–IP, hoặc để phát hiện trùng lặp IP.

Inverse ARP (InARP) Phiên bản ARP mở rộng dùng trong các mạng WAN như Frame Relay, để ánh xạ địa chỉ tầng 2 sang địa chỉ IP.

ARP Spoofing / ARP Poisoning Hình thức tấn công trong đó kẻ xấu gửi các bản tin ARP giả mạo để đánh lừa host cập nhật sai bảng ARP, từ đó chặn hoặc nghe lén lưu lượng.

IPv6 Address Resolution Trong IPv6, quá trình phân giải địa chỉ được thực hiện bởi Neighbor Discovery Protocol (NDP), thay thế ARP.

Neighbor Discovery Protocol (NDP) Giao thức trong IPv6, dùng bản tin ICMPv6 để thực hiện các chức năng: Neighbor Solicitation/Advertisement (phân giải địa chỉ), Router Solicitation/Advertisement (tự động cấu hình), phát hiện trùng lặp địa chỉ (DAD).

Neighbor Cache Bảng tương tự ARP Cache nhưng trong IPv6, lưu ánh xạ giữa địa chỉ IPv6 và địa chỉ MAC.

NS (Neighbor Solicitation) Bản tin ICMPv6 gửi đi để hỏi địa chỉ MAC của một địa chỉ IPv6 đích trong cùng mạng.

NA (Neighbor Advertisement) Bản tin ICMPv6 trả lời, cung cấp địa chỉ MAC tương ứng với địa chỉ IPv6 được yêu cầu.

RS (Router Solicitation) Bản tin ICMPv6 mà host gửi để yêu cầu router gửi thông tin cấu hình.

RA (Router Advertisement) Bản tin ICMPv6 mà router gửi định kỳ hoặc để trả lời RS, cung cấp thông tin prefix, default gateway, cơ chế SLAAC hoặc DHCPv6.

SLAAC (Stateless Address Autoconfiguration) Cơ chế trong IPv6 cho phép host tự động cấu hình địa chỉ mà không cần DHCPv6, dựa vào thông tin prefix nhận từ RA.

DAD (Duplicate Address Detection) Quá trình host IPv6 kiểm tra xem địa chỉ của mình có bị trùng trong mạng LAN hay không, bằng cách gửi Neighbor Solicitation cho chính địa chỉ đó.

Chương 10

Cấu hình cơ bản cho Router

Mục tiêu

Sau khi hoàn thành chương này, bạn sẽ có thể:

- Mô tả chức năng cơ bản của router trong mạng.
- Truy cập vào CLI của router và phân biệt các chế độ.
- Cấu hình tên, mật khẩu, banner và bảo mật cơ bản cho router.
- Cấu hình địa chỉ IPv4 và IPv6 trên các giao diện.
- Cấu hình default gateway để kết nối liên mạng.
- Kiểm tra hoạt động của router bằng các lệnh show và ping.

Thuật ngữ chính

- Router
- Interface
- CLI modes
- Running-config / Startup-config
- Enable secret
- Line console / vty
- Banner MOTD
- IPv4 address / IPv6 address
- Default gateway
- show ip interface brief
- ping / traceroute

10.1 Giới thiệu

Router là thiết bị lớp mạng, kết nối các mạng khác nhau với nhau. Nó định tuyến gói tin dựa trên địa chỉ IP đích. Để một router hoạt động, cần cấu hình cơ bản: tên, mật khẩu, địa chỉ IP trên giao diện, và kiểm tra kết nối.

10.2 Truy cập CLI của router

- Truy cập qua console hoặc SSH (sau khi cấu hình).
- Các chế độ CLI giống switch: user EXEC, privileged EXEC, global configuration, subconfiguration.

10.3 Cấu hình cơ bản cho router

10.3.1 Đặt tên, banner và mật khẩu

```
Router> enable
Router# configure terminal
Router(config)# hostname R1
R1(config)# no ip domain-lookup
R1(config)# enable secret <MATKHAU_MANH>
R1(config)# service password-encryption
R1(config)# banner motd #Truy cập được giám sát. Người không phận sự cấm vào.#
```

10.3.2 Mật khẩu console và vty

```
R1(config)# line console 0
R1(config-line)# password <MATKHAU_CONSOLE>
R1(config-line)# login
R1(config)# line vty 0 4
R1(config-line)# password <MATKHAU_VTY>
R1(config-line)# login
```

10.4 Cấu hình địa chỉ IPv4

```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
```

- Mỗi giao diện router cần có địa chỉ IP và subnet mask.
- Lệnh `no shutdown` kích hoạt giao diện.

10.5 Cấu hình địa chỉ IPv6

```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config)# ipv6 unicast-routing
```

- `ipv6 unicast-routing` cần bật để router chuyển tiếp gói IPv6.

10.6 Cấu hình default gateway

- Nếu router kết nối nhiều mạng, nó sẽ học đường đi.
- Nếu router chỉ có một đường ra, ta cấu hình **default route**.

```
R1(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.254
R1(config)# ipv6 route ::/0 2001:db8:acad:2::1
```

10.7 Kiểm tra và xác minh

```
R1# show ip interface brief
R1# show running-config
R1# ping 192.168.1.2
R1# traceroute 8.8.8.8
```

- `show ip interface brief` để xem trạng thái giao diện.
- `ping` và `traceroute` để kiểm tra kết nối.

Tóm tắt

- Router là thiết bị tầng mạng, định tuyến gói giữa các mạng.
- Cấu hình cơ bản gồm: hostname, mật khẩu, banner, địa chỉ IP cho các giao diện.
- Router cần default route để ra Internet.
- Kiểm tra hoạt động bằng các lệnh show, ping, traceroute.

Câu hỏi ôn tập

1. **Chức năng cơ bản của router là gì?**
   - Kết nối nhiều mạng khác nhau.
   - Định tuyến gói tin dựa trên địa chỉ IP đích.
2. **Lệnh nào dùng để cấu hình mật khẩu enable secret?**
   - `Router(config)# enable secret <mật_khẩu>`
3. **Tại sao cần lệnh `no shutdown` trên giao diện router?**
   - Giao diện mặc định ở trạng thái tắt (administratively down).
   - `no shutdown` kích hoạt giao diện để nó có thể truyền dữ liệu.
4. **Cấu hình default route trong IPv4 và IPv6 như thế nào?**
   - IPv4: `ip route 0.0.0.0 0.0.0.0 <next-hop>`
   - IPv6: `ipv6 route ::/0 <next-hop>`
5. **Lệnh nào hiển thị nhanh trạng thái các giao diện?**
   - `show ip interface brief`

10.8 Thuật ngữ cần nhớ

Router Thiết bị mạng tầng 3 (mạng) có chức năng chính là định tuyến gói tin giữa các mạng khác nhau và chọn đường đi tối ưu dựa vào bảng định tuyến.

Routing Quá trình xác định đường đi tốt nhất cho gói tin từ nguồn đến đích qua nhiều mạng trung gian.

Routing Table (Bảng định tuyến) Cơ sở dữ liệu trong router chứa thông tin về mạng đích, địa chỉ next-hop, giao diện ra và chi phí đường đi.

Default Gateway Địa chỉ router mà các host trong mạng LAN gửi gói tin đến khi đích nằm ngoài subnet cục bộ.

Default Route Tuyến mặc định trong bảng định tuyến, dùng khi không có tuyến nào cụ thể đến mạng đích (`0.0.0.0/0` hoặc `::/0`).

Static Route Tuyến được cấu hình thủ công bởi quản trị viên, không thay đổi trừ khi người quản trị sửa cấu hình.

Dynamic Routing Phương pháp dùng các giao thức định tuyến (RIP, OSPF, EIGRP, BGP) để router tự động học và cập nhật tuyến.

Cisco IOS (Internetwork Operating System) Hệ điều hành mạng của Cisco dùng để cấu hình, vận hành và quản lý router và switch.

CLI (Command Line Interface) Giao diện dòng lệnh cho phép nhập lệnh để cấu hình và kiểm soát router Cisco.

User EXEC Mode Chế độ EXEC cơ bản (`Router>`), cho phép thực hiện một số lệnh giám sát đơn giản nhưng không thay đổi cấu hình.

Privileged EXEC Mode Chế độ EXEC đặc quyền (`Router#`), cho phép chạy các lệnh kiểm tra chi tiết và truy cập vào chế độ cấu hình.

Global Configuration Mode Chế độ cấu hình toàn cục (`Router(config)#`), nơi quản trị viên thiết lập các tham số cấu hình cho toàn bộ router.

Interface Configuration Mode Chế độ cấu hình dành riêng cho một giao diện mạng trên router (`Router(config-if)#`), dùng để gán địa chỉ IP, bật/tắt giao diện.

Hostname Tên định danh của router, giúp phân biệt thiết bị trong quá trình quản trị.

Banner Message Thông báo hiển thị khi người dùng đăng nhập vào thiết bị, thường dùng cho cảnh báo bảo mật hoặc thông tin quản trị.

Enable Secret Mật khẩu mã hóa được cấu hình để bảo vệ truy cập vào chế độ EXEC đặc quyền.

Console Password Mật khẩu bảo vệ truy cập qua cổng console.

VTY Password Mật khẩu bảo vệ truy cập từ xa qua Telnet/SSH vào router.

Show Commands Nhóm lệnh hiển thị trạng thái và cấu hình của router, ví dụ: `show running-config`, `show ip route`, `show interfaces`.

Ping Lệnh kiểm tra khả năng kết nối IP giữa router và thiết bị đích bằng cách gửi ICMP Echo Request và nhận Echo Reply.

Traceroute Lệnh hiển thị đường đi của gói tin qua các router trung gian đến đích, giúp chẩn đoán sự cố mạng.

Running-config Cấu hình đang hoạt động trong RAM của router, có thể thay đổi trực tiếp bằng các lệnh cấu hình.

Startup-config Cấu hình được lưu trong NVRAM, sẽ được nạp khi router khởi động lại.

Save Configuration Hành động sao chép cấu hình hiện tại (running-config) sang startup-config để đảm bảo cấu hình được giữ lại sau khi khởi động lại (`copy running-config startup-config`).

Chương 11

Địa chỉ IPv4

Mục tiêu

Sau khi hoàn thành chương này, bạn sẽ có thể:

- Giải thích cấu trúc của địa chỉ IPv4 và subnet mask.
- Phân biệt các loại địa chỉ IPv4: unicast, broadcast, multicast.
- Mô tả khái niệm subnetting và vai trò của nó.
- Tính toán số mạng con và số host khả dụng.
- Cấu hình địa chỉ IPv4 trên thiết bị mạng và PC.
- Hiểu các khái niệm đặc biệt: địa chỉ riêng, địa chỉ công cộng, APIPA.

Thuật ngữ chính

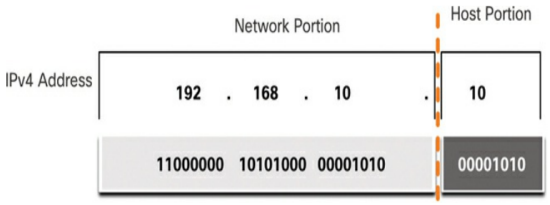
- IPv4 address
- Subnet mask
- Network address
- Host address
- Default gateway
- Broadcast address
- Private / Public address
- APIPA (Automatic Private IP Addressing)
- CIDR (Classless Inter-Domain Routing)
- Subnetting
- VLSM (Variable Length Subnet Mask)

11.1 Giới thiệu

Địa chỉ IPv4 là nền tảng của giao tiếp mạng trong nhiều thập kỷ. Nó cung cấp cách định danh logic cho thiết bị và xác định cách định tuyến gói tin. Chương này giải thích chi tiết cấu trúc và phân loại địa chỉ IPv4, cách subnetting và cách cấu hình trong môi trường mạng.

11.2 Cấu trúc địa chỉ IPv4 (IPv4 Addressing)

- Độ dài: 32 bit, viết dưới dạng thập phân chấm (ví dụ: 192.168.1.1).
- Gồm hai phần: **Network ID** và **Host ID**.
- **Subnet mask** xác định bao nhiêu bit là phần mạng, bao nhiêu bit là phần host.



Hình 11.1: Cấu trúc địa chỉ IPv4.

11.3 Phân loại địa chỉ IPv4

11.3.1 Địa chỉ unicast

Gửi từ một nguồn đến một đích cụ thể.

11.3.2 Địa chỉ broadcast

- Gửi đến tất cả host trong cùng mạng con.
- Ví dụ: địa chỉ cuối trong subnet (192.168.1.255/24).

11.3.3 Địa chỉ multicast

- Gửi đến một nhóm host quan tâm (224.0.0.0 đến 239.255.255.255).

11.3.4 Địa chỉ đặc biệt

- 127.0.0.1: loopback (localhost).
- 169.254.0.0/16: APIPA khi DHCP không phản hồi.

11.4 Địa chỉ công cộng và địa chỉ riêng

- **Công cộng**: dùng trên Internet, phải duy nhất toàn cầu.
- **Riêng**: dùng trong mạng nội bộ, các dải chính:
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16

11.5 Subnetting

11.5.1 Khái niệm

Chia một mạng lớn thành nhiều mạng con nhỏ hơn để sử dụng hiệu quả địa chỉ và tăng tính bảo mật.

11.5.2 Tính toán cơ bản

- Số mạng con = 2^n (với n là số bit mượn).
- Số host khả dụng mỗi subnet = $2^h - 2$ (với h là số bit host còn lại).

11.5.3 Ví dụ

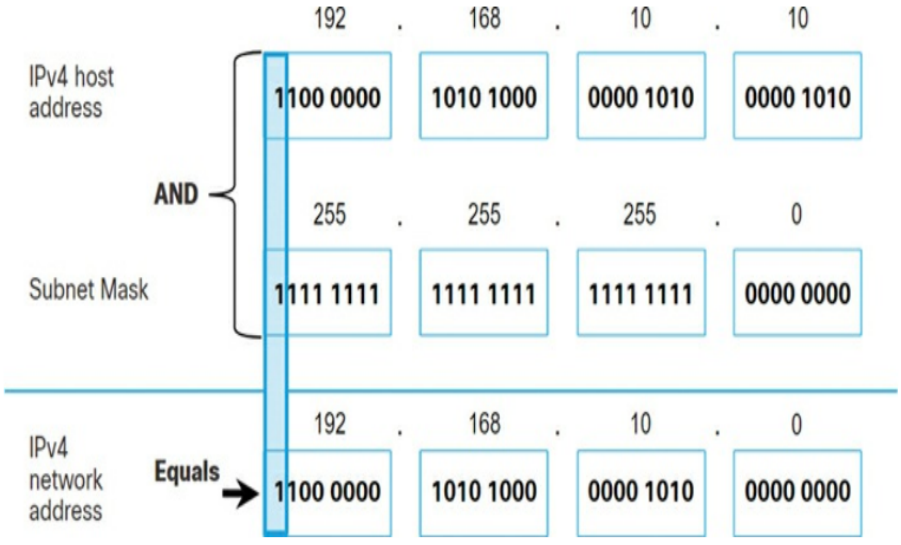
- Mạng gốc: 192.168.1.0/24.
- Mượn 2 bit host → /26.
- Số subnet: $2^2 = 4$, mỗi subnet có $2^6 - 2 = 62$ host khả dụng.

11.6 CIDR và VLSM

- **CIDR**: viết subnet mask theo dạng /n (prefix length).
- **VLSM**: cho phép chia mạng với độ dài subnet mask khác nhau tùy nhu cầu.

Xác định mạng nhờ phép AND logic

Để xác định địa chỉ mạng của một máy chủ IPv4, địa chỉ IPv4 được thực hiện phép AND logic từng bit với mặt nạ mạng con. Phép AND giữa địa chỉ và mặt nạ mạng con sẽ cho ra địa chỉ mạng. Để minh họa cách sử dụng phép AND để tìm địa chỉ mạng, hãy xem xét một máy chủ có địa chỉ IPv4 là 192.168.10.10 và mặt nạ mạng con là 255.255.255.0, như thể hiện trong Hình 11.2.



Hình 11.2: Xác định mạng nhờ phép AND logic.

11.7 Cấu hình địa chỉ IPv4 trên thiết bị

11.7.1 Trên router hoặc switch layer 3

```
R1(config)# interface g0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
```

11.7.2 Trên PC (Windows)

- IP address: 192.168.10.10
- Subnet mask: 255.255.255.0
- Default gateway: 192.168.10.1
- DNS server: 8.8.8.8

Tóm tắt

- IPv4 dài 32 bit, viết theo thập phân chấm.
- Có ba loại địa chỉ: unicast, broadcast, multicast.
- Địa chỉ riêng dùng trong mạng nội bộ; địa chỉ công cộng dùng trên Internet.
- Subnetting giúp chia nhỏ mạng, tiết kiệm địa chỉ, tăng bảo mật.
- CIDR và VLSM cung cấp cách chia mạng linh hoạt.

Câu hỏi ôn tập

1. **Địa chỉ IPv4 có độ dài bao nhiêu bit?**
    - Địa chỉ IPv4 có độ dài 32 bit, thường viết dưới dạng thập phân chấm (ví dụ: 192.168.1.1).
2. **Địa chỉ broadcast được xác định như thế nào?**
    - Địa chỉ broadcast là địa chỉ cuối cùng trong một subnet.
    - Ví dụ: mạng 192.168.1.0/24 có địa chỉ broadcast là 192.168.1.255.
3. **Sự khác biệt giữa địa chỉ công cộng và địa chỉ riêng?**
    - **Địa chỉ công cộng**: có thể định tuyến trên Internet, phải duy nhất toàn cầu.
    - **Địa chỉ riêng**: chỉ sử dụng trong mạng nội bộ, không định tuyến trực tiếp trên Internet.
4. **Công thức tính số mạng con và số host khả dụng?**
    - Số mạng con = 2^n (với n là số bit mượn cho phần mạng).
    - Số host khả dụng = $2^h - 2$ (với h là số bit còn lại cho phần host).
5. **CIDR và VLSM mang lại lợi ích gì?**
    - CIDR cho phép viết subnet mask dưới dạng prefix length (/n), linh hoạt hơn so với phân lớp truyền thống.
    - VLSM cho phép chia mạng với subnet mask có độ dài khác nhau, giúp sử dụng địa chỉ hiệu quả.

11.8 Bài tập Chương 11

1. Một mạng có địa chỉ `192.168.10.0/26`. Hãy tính số host khả dụng, địa chỉ mạng, và địa chỉ broadcast.

   Đáp án:
   /26 $\Rightarrow 2^6 - 2 = 62$ host khả dụng. Địa chỉ mạng: 192.168.10.0. Địa chỉ broadcast: 192.168.10.63.

2. Một công ty được cấp dải `172.16.0.0/16`. Họ cần chia thành ít nhất 400 subnet. Hãy xác định prefix mới.

   Đáp án:
   $2^n \geq 400 \Rightarrow n = 9$ bit mượn. Prefix = $16 + 9 = 25 \Rightarrow$ /25. Mỗi subnet có 126 host khả dụng.

3. Một mạng có prefix `/20`. Hãy tính số host khả dụng.

   Đáp án:
   Host bit = $32 - 20 = 12$. Host khả dụng = $2^{12} - 2 = 4094$.

4. Một mạng `10.0.0.0/18`. Hãy tính số subnet tạo được từ dải `10.0.0.0/16` khi chia thành /18.

   Đáp án:
   Bit mượn = $18 - 16 = 2$. Số subnet = $2^2 = 4$.

5. Một host có IP `192.168.1.130/25`. Hãy xác định địa chỉ mạng và broadcast.

   Đáp án:
   /25 $\Rightarrow$ subnet mask = 255.255.255.128. Địa chỉ mạng: 192.168.1.128. Địa chỉ broadcast: 192.168.1.255.

6. Một tổ chức cần 500 host trong một mạng con. Hãy xác định prefix tối thiểu.

   Đáp án:
   $2^n - 2 \geq 500 \Rightarrow n = 9$. Prefix = $32 - 9 = 23 \Rightarrow$ /23. Mỗi subnet có 510 host khả dụng.

7. Một mạng có dải `192.168.5.0/24`. Nếu chia thành 4 subnet bằng nhau, hãy xác định prefix mới và số host khả dụng trong mỗi subnet.

   Đáp án:
   Cần chia 4 $\Rightarrow$ mượn 2 bit. Prefix mới = $24 + 2 = 26 \Rightarrow$ /26. Mỗi subnet có $2^6 - 2 = 62$ host khả dụng.

8. Một công ty có dải `10.0.0.0/8`. Nếu cần 1000 subnet, hãy xác định prefix cần dùng.

   Đáp án:
   $2^n \geq 1000 \Rightarrow n = 10$. Prefix = $8 + 10 = 18 \Rightarrow$ /18. Mỗi subnet có $2^{14} - 2 = 16,382$ host khả dụng.

9. Một gói dữ liệu có IP nguồn `192.168.1.10/24` và đích `192.168.2.20/24`. Hãy cho biết gói có cần đi qua router không.

   Đáp án:
   Mạng nguồn = 192.168.1.0/24. Mạng đích = 192.168.2.0/24. Hai mạng khác nhau $\Rightarrow$ cần qua router.

10. Một dải địa chỉ `192.168.100.0/24` được chia thành các subnet /28. Hãy tính số subnet tạo được và số host khả dụng trong mỗi subnet.

    Đáp án:
    Bit mượn = $28 - 24 = 4$. Số subnet = $2^4 = 16$. Mỗi subnet có $2^4 - 2 = 14$ host khả dụng.

11.9 Thuật ngữ cần nhớ

IPv4 Address Địa chỉ Internet Protocol phiên bản 4, dài 32 bit, được chia thành bốn octet và viết theo dạng thập phân chấm (ví dụ: 192.168.1.1).

Octet Nhóm 8 bit trong địa chỉ IPv4. Một địa chỉ IPv4 gồm 4 octet, mỗi octet có giá trị từ 0 đến 255.

Network Portion Phần địa chỉ xác định mạng hoặc subnet, giống nhau cho tất cả các host trong cùng một mạng con.

Host Portion Phần địa chỉ xác định thiết bị riêng lẻ (host) trong cùng một mạng con. Phần này phải duy nhất trong mạng.

Subnet Mask Dãy 32 bit đi kèm địa chỉ IPv4, dùng để phân biệt phần mạng và phần host. Thường viết ở dạng thập phân chấm, ví dụ: 255.255.255.0.

Prefix Length Cách viết rút gọn của subnet mask bằng CIDR (Classless Inter-Domain Routing), ví dụ: /24 tương ứng với 255.255.255.0.

Network Address Địa chỉ đầu tiên trong một subnet, tất cả các bit phần host bằng 0. Nó định danh chính subnet đó, không gán cho host.

Broadcast Address Địa chỉ cuối cùng trong subnet, tất cả các bit phần host bằng 1. Được dùng để gửi gói đến toàn bộ host trong subnet.

Unicast Address Địa chỉ IPv4 dùng để định danh một host duy nhất trong mạng. Gói unicast được gửi đến đúng thiết bị đích.

Private IPv4 Address Địa chỉ dành riêng cho mạng nội bộ, không định tuyến trực tiếp trên Internet. Các dải gồm:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

Public IPv4 Address Địa chỉ có thể định tuyến trên Internet toàn cầu, do các tổ chức quản lý địa chỉ (IANA, RIR) cấp phát.

Loopback Address Địa chỉ 127.0.0.0/8, thường dùng 127.0.0.1 để kiểm tra hoạt động TCP/IP cục bộ trên host.

Link-local Address Địa chỉ tự gán 169.254.0.0/16 khi host không nhận được IP từ DHCP. Chỉ hoạt động trong một liên kết cục bộ.

Classful Addressing Cách chia địa chỉ IPv4 theo lớp A, B, C, D, E dựa trên các bit đầu tiên. Ngày nay đã lỗi thời, được thay thế bởi CIDR.

CIDR (Classless Inter-Domain Routing) Phương pháp định tuyến không phân lớp, cho phép dùng prefix length linh hoạt để chia subnet hiệu quả hơn.

Subnetting Quá trình chia một mạng lớn thành các mạng con nhỏ hơn bằng cách mượn bit từ phần host để mở rộng phần mạng.

Variable Length Subnet Masking (VLSM) Kỹ thuật chia subnet với mặt nạ độ dài biến đổi, cho phép phân bổ không gian địa chỉ tối ưu hơn cho các mạng có quy mô khác nhau.

Address Block Một dải liên tục các địa chỉ IPv4 được gán hoặc cấp phát, thường được mô tả bằng địa chỉ mạng + prefix length.

Default Gateway Router trong mạng LAN có địa chỉ IP nội bộ, nơi host gửi gói khi đích nằm ngoài subnet của nó.

IPv4 Packet Header Phần đầu gói IPv4 chứa thông tin điều khiển, gồm các trường: địa chỉ IP nguồn, đích, TTL, protocol, checksum, v.v.

Address Exhaustion Hiện tượng cạn kiệt không gian địa chỉ IPv4 do số lượng host kết nối Internet ngày càng tăng.

NAT (Network Address Translation) Cơ chế cho phép nhiều thiết bị trong mạng riêng dùng một địa chỉ công cộng để truy cập Internet, giúp tiết kiệm IPv4 công cộng.

DHCP (Dynamic Host Configuration Protocol) Giao thức cấp phát tự động địa chỉ IPv4, subnet mask, default gateway, DNS cho host trong mạng.

Chương 12

Địa chỉ IPv6

Mục tiêu

Sau khi hoàn thành chương này, bạn sẽ có thể:

- Giải thích lý do cần IPv6 thay thế IPv4.
- Mô tả cấu trúc địa chỉ IPv6 (128 bit).
- Phân biệt các loại địa chỉ IPv6: unicast, multicast, anycast.
- Viết và rút gọn địa chỉ IPv6 đúng quy tắc.
- Cấu hình địa chỉ IPv6 trên thiết bị mạng.
- Hiểu cơ chế tự cấu hình SLAAC và DHCPv6.

Thuật ngữ chính

- IPv6 address
- Unicast / Multicast / Anycast
- Link-local
- Global unicast
- Unique local
- Loopback
- IPv6 prefix
- SLAAC
- DHCPv6
- ICMPv6 Neighbor Discovery

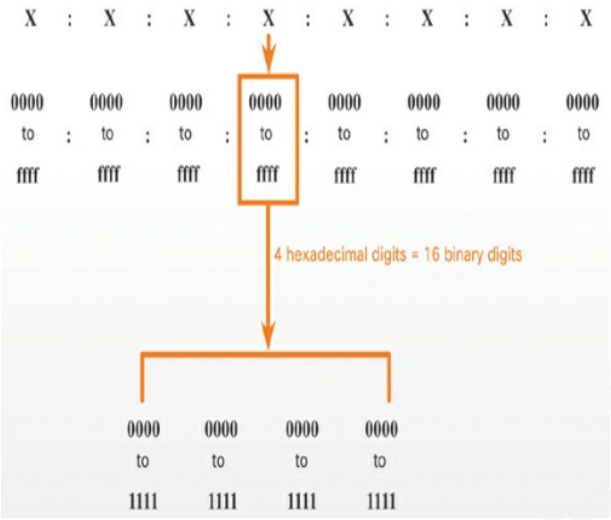
12.1 Giới thiệu

IPv4 chỉ có 32 bit địa chỉ, tức khoảng 4,3 tỷ địa chỉ. Với sự bùng nổ của Internet, con số này không còn đủ. IPv6 với địa chỉ 128 bit được phát triển để giải quyết vấn đề này, cung cấp không gian địa chỉ khổng lồ cùng nhiều cải tiến.

12.2 Cấu trúc địa chỉ IPv6

- Độ dài: 128 bit, viết dưới dạng thập lục phân, gồm 8 nhóm, mỗi nhóm 16 bit.
- Ví dụ: 2001:0db8:0000:0000:0000:ff00:0042:8329

- Có thể rút gọn: bỏ số 0 ở đầu mỗi nhóm, thay chuỗi nhóm 0 bằng "::" (chỉ dùng một lần).
- Ví dụ rút gọn: 2001:db8::ff00:42:8329



Hình 12.1: Cấu trúc địa chỉ IPv6.

12.3 Các loại địa chỉ IPv6

12.3.1 Unicast

Đại diện cho một giao diện duy nhất. Gồm:

- **Global unicast**: định tuyến toàn cầu trên Internet (2000::/3).
- **Link-local**: tự động tạo, bắt đầu bằng FE80::/10, dùng trong cùng liên kết.
- **Unique local**: tương tự địa chỉ riêng IPv4, không định tuyến toàn cầu (FC00::/7).

12.3.2 Multicast

Gửi đến nhiều nút cùng tham gia nhóm. Dải FF00::/8.

12.3.3 Anycast

Địa chỉ gán cho nhiều nút, gói tin sẽ đến nút gần nhất (theo định tuyến).

12.3.4 Địa chỉ đặc biệt

- ::1 – loopback
- :: – địa chỉ chưa xác định

12.4 Tiền tố và subnet IPv6

- IPv6 cũng dùng subnet prefix, viết dạng /n.
- Subnet mặc định cho LAN thường là /64.

12.5 Cấu hình địa chỉ IPv6

12.5.1 Thủ công

```
R1(config)# interface g0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
```

12.5.2 Tự động

- **SLAAC**: host tự cấu hình địa chỉ dựa trên prefix từ router advertisement.
- **DHCPv6**: cấp phát thêm thông tin như DNS, gateway.

12.6 Neighbor Discovery và ICMPv6

- Thay thế ARP trong IPv6.
- Sử dụng thông điệp Neighbor Solicitation và Neighbor Advertisement.
- Kiểm tra tính sẵn sàng của nút và phát hiện địa chỉ trùng lặp (DAD – Duplicate Address Detection).

Tóm tắt

- IPv6 được phát triển để thay thế IPv4 do thiếu địa chỉ.
- Địa chỉ dài 128 bit, viết dạng hex, có thể rút gọn.
- Các loại chính: global unicast, link-local, unique local, multicast, anycast.
- Subnet IPv6 thường dùng /64.
- Cấu hình thủ công, SLAAC hoặc DHCPv6.
- Neighbor Discovery thay ARP, dùng ICMPv6.

Câu hỏi ôn tập

1. **IPv6 có độ dài bao nhiêu bit? So với IPv4 thì khác thế nào?**
   - IPv6 có độ dài 128 bit, trong khi IPv4 dài 32 bit.
   - Không gian địa chỉ IPv6 lớn hơn rất nhiều so với IPv4.
2. **Các quy tắc rút gọn địa chỉ IPv6 là gì?**
   - Bỏ số 0 ở đầu trong mỗi nhóm 16 bit.
   - Thay chuỗi nhiều nhóm toàn 0 bằng ký hiệu `::` (chỉ dùng một lần trong địa chỉ).
3. **Phân biệt global unicast, link-local và unique local trong IPv6.**
   - **Global unicast**: có thể định tuyến toàn cầu trên Internet (bắt đầu bằng 2000::/3).
   - **Link-local**: tự động tạo (FE80::/10), chỉ dùng trong cùng liên kết.

- **Unique local**: dùng trong nội bộ tổ chức, không định tuyến toàn cầu (FC00::/7).

4. **SLAAC hoạt động như thế nào?**
   - Host nhận Router Advertisement (RA) từ router.
   - Dùng prefix trong RA kết hợp với địa chỉ MAC để tự cấu hình địa chỉ IPv6.
5. **Neighbor Discovery thay thế ARP ra sao trong IPv6?**
   - Neighbor Discovery (ND) dùng thông điệp ICMPv6 Neighbor Solicitation và Advertisement để phân giải địa chỉ.
   - Ngoài phân giải địa chỉ, ND còn phát hiện trùng lặp địa chỉ (Duplicate Address Detection).

12.7 Bài tập Chương 12

1. Viết rút gọn địa chỉ IPv6 sau: `2001:0db8:0000:0000:0000:0000:0000:1A2F`

   Đáp án:
   Bỏ số 0 thừa trong từng nhóm và dùng `::` cho chuỗi 0 liên tiếp. ⇒ `2001:db8::1a2f`.

2. Một địa chỉ IPv6 có prefix `/64`. Hãy tính số địa chỉ host khả dụng trong một mạng con.

   Đáp án:
   Host bit = 128 – 64 = 64. Tổng địa chỉ = $2^{64} \approx 1.84 \times 10^{19}$. Số lượng khả dụng cực kỳ lớn (không cần trừ như IPv4).

3. Một mạng IPv6 `2001:db8:acad::/48` được chia thành các subnet /64. Hãy tính số subnet tạo được.

   Đáp án:
   Bit mượn = 64 – 48 = 16. Số subnet = $2^{16} = 65,536$.

4. Địa chỉ IPv6 `FE80::1` thuộc loại nào? Có định tuyến toàn cầu được không?

   Đáp án:
   Bắt đầu bằng `FE80::/10` ⇒ là địa chỉ link-local. Không định tuyến toàn cầu, chỉ dùng trong cùng một liên kết.

5. Một tổ chức có prefix `2001:db8:acad::/48`. Nếu muốn chia thành các subnet `/56`, hãy tính số subnet có thể tạo.

   Đáp án:
   Bit mượn = 56 – 48 = 8. Số subnet = $2^8 = 256$.

6. Viết địa chỉ IPv6 đầy đủ (không rút gọn) cho: `2001:db8::abcd`.

   Đáp án:
   Điền đủ 8 nhóm 4 hex digit: `2001:0db8:0000:0000:0000:0000:0000:abcd`.

7. Một host tự động cấu hình SLAAC nhận prefix `2001:db8:acad:1::/64`. Địa chỉ MAC là `00:1A:2B:3C:4D:5E`. Hãy tính Interface ID theo định dạng EUI-64.

   Đáp án:
   MAC: 00-1A-2B-3C-4D-5E. Chèn `FFFE` giữa ⇒ 00-1A-2B-FF-FE-3C-4D-5E. Đảo bit U/L (bit thứ 7) của byte đầu: 00 ⇒ 02. Interface ID = `021A:2BFF:FE3C:4D5E`. Địa chỉ IPv6 đầy đủ: `2001:db8:acad:1:021a:2bff:fe3c:4d`

8. Một router quảng bá prefix `2001:db8:abcd::/64`. Nếu 100 host dùng SLAAC, hãy cho biết số lượng địa chỉ IPv6 được tạo.

   Đáp án:
   Mỗi host tự tạo một địa chỉ IPv6 duy nhất. Tổng số địa chỉ = 100 (khả thi vì không giới hạn).

9. Một địa chỉ IPv6 multicast bắt đầu bằng `FF02::1`. Hãy cho biết nhóm multicast này là gì.

   Đáp án:
   `FF02::1` là địa chỉ multicast all-nodes trên link-local. Tất cả các host trong liên kết sẽ nhận gói tin.

10. Một mạng `2001:db8:acad::/48` được chia thành `/64`. Nếu dùng hết các subnet, hãy tính số host lý thuyết tối đa mà mạng này có thể chứa.

    Đáp án:
    Số subnet /64 = $2^{16} = 65,536$. Mỗi subnet /64 có 2^{64} địa chỉ. Tổng số host lý thuyết = $65,536 \times 2^{64} = 2^{16} \times 2^{64} = 2^{80}$.

12.8 Thuật ngữ cần nhớ

IPv6 Address Địa chỉ Internet Protocol phiên bản 6, dài 128 bit, cung cấp không gian địa chỉ cực lớn. Viết dưới dạng thập lục phân, chia thành 8 nhóm cách nhau bởi dấu hai chấm (ví dụ: `2001:0db8:0000:0000:0000:ff00:0042:832`

Hexadecimal Notation Cách biểu diễn IPv6 bằng hệ thập lục phân để rút gọn độ dài, mỗi nhóm gồm 16 bit.

Zero Compression Quy tắc rút gọn trong IPv6: chuỗi các nhóm số 0 liên tiếp có thể thay bằng ký hiệu `::` (chỉ được dùng một lần trong địa chỉ).

IPv6 Prefix Phần đầu của địa chỉ IPv6 xác định mạng, tương tự như subnet trong IPv4. Được viết kèm độ dài (ví dụ: `/64`).

Interface ID Phần nhận dạng host trong địa chỉ IPv6, thường dài 64 bit. Có thể được sinh tự động từ địa chỉ MAC hoặc tạo ngẫu nhiên.

Global Unicast Address Địa chỉ công cộng toàn cầu trong IPv6, có phạm vi Internet, tương tự như địa chỉ công cộng IPv4. Thường bắt đầu bằng `2000::/3`.

Link-local Address Địa chỉ IPv6 tự động gán cho mọi giao diện, dùng để giao tiếp trong cùng một liên kết (không định tuyến). Tất cả đều bắt đầu bằng `FE80::/10`.

Unique Local Address (ULA) Địa chỉ IPv6 riêng, không định tuyến trên Internet toàn cầu, thường dùng trong mạng nội bộ (`FC00::/7`).

Multicast Address Địa chỉ IPv6 dùng để gửi gói đến nhiều thiết bị trong một nhóm, bắt đầu bằng `FF00::/8`.

Loopback Address Địa chỉ `::1`, tương đương 127.0.0.1 trong IPv4, dùng để kiểm tra TCP/IP cục bộ trên host.

Unspecified Address Địa chỉ `::`, được dùng khi một thiết bị chưa được gán địa chỉ IPv6.

Anycast Address Địa chỉ IPv6 được gán cho nhiều giao diện, gói tin được định tuyến đến giao diện gần nhất (theo định tuyến).

SLAAC (Stateless Address Autoconfiguration) Cơ chế cho phép host tự động cấu hình địa chỉ IPv6 dựa trên thông tin từ Router Advertisement (RA), không cần DHCPv6.

DHCPv6 Giao thức cấp phát địa chỉ IPv6 động, có thể hoạt động ở chế độ stateful (cấp địa chỉ đầy đủ) hoặc stateless (cấp thêm thông tin cấu hình).

Router Solicitation (RS) Bản tin ICMPv6 mà host gửi để yêu cầu router cung cấp thông tin mạng.

Router Advertisement (RA) Bản tin ICMPv6 mà router gửi, cung cấp prefix, default gateway, và thông tin cấu hình (SLAAC, DHCPv6).

Neighbor Discovery Protocol (NDP) Giao thức IPv6 thay thế ARP, cung cấp phân giải địa chỉ, phát hiện láng giềng, phát hiện trùng lặp địa chỉ (DAD), và quản lý thông tin router.

DAD (Duplicate Address Detection) Quá trình kiểm tra trùng lặp địa chỉ IPv6 trước khi một host sử dụng địa chỉ đó.

IPv6 Header Phần đầu gói IPv6, có độ dài cố định 40 byte, gồm các trường cơ bản: nguồn, đích, độ ưu tiên, Next Header, Hop Limit.

Extension Headers Các header bổ sung trong IPv6 cung cấp tính năng nâng cao như định tuyến mở rộng, phân mảnh, bảo mật (AH, ESP).

Tunneling Kỹ thuật bao gói gói IPv6 bên trong IPv4 để truyền qua hạ tầng chỉ hỗ trợ IPv4.

Dual Stack Phương pháp triển khai đồng thời cả IPv4 và IPv6 trên cùng thiết bị, cho phép hoạt động song song trong giai đoạn chuyển đổi.

Prefix Length Biểu diễn số bit thuộc phần mạng trong địa chỉ IPv6, ví dụ: `/64`, `/48`.

Aggregatable Global Unicast Address Cấu trúc địa chỉ IPv6 công cộng hỗ trợ phân cấp định tuyến, giúp giảm kích thước bảng định tuyến Internet.

Chương 13

Giao thức điều khiển thông điệp Internet (ICMP)

Mục tiêu

Sau khi hoàn thành chương này, bạn sẽ có thể:

- Giải thích vai trò của ICMP trong mạng IP.
- Mô tả các loại thông điệp ICMPv4 và ICMPv6.
- Hiểu ICMP hỗ trợ chẩn đoán mạng với lệnh ping và traceroute.
- So sánh sự khác biệt giữa ICMPv4 và ICMPv6.

Thuật ngữ chính

- ICMPv4
- ICMPv6
- Echo request / reply
- Destination unreachable
- Time exceeded
- Router advertisement / solicitation
- Neighbor solicitation / advertisement

13.1 Giới thiệu

ICMP (Internet Control Message Protocol) là giao thức hỗ trợ trong bộ TCP/IP. Nó cung cấp thông tin phản hồi về các vấn đề truyền gói tin, cũng như công cụ chẩn đoán như ping và traceroute.

13.2 ICMPv4

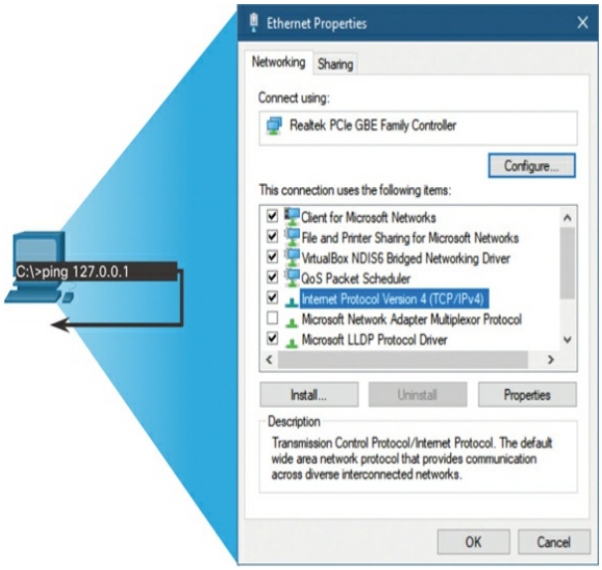
13.2.1 Các loại thông điệp chính

- **Echo request / reply**: dùng trong lệnh ping để kiểm tra kết nối.
- **Destination unreachable**: báo không thể đến đích (mạng, host, cổng, giao thức).
- **Time exceeded**: báo gói tin bị loại bỏ do TTL = 0 (dùng trong traceroute).

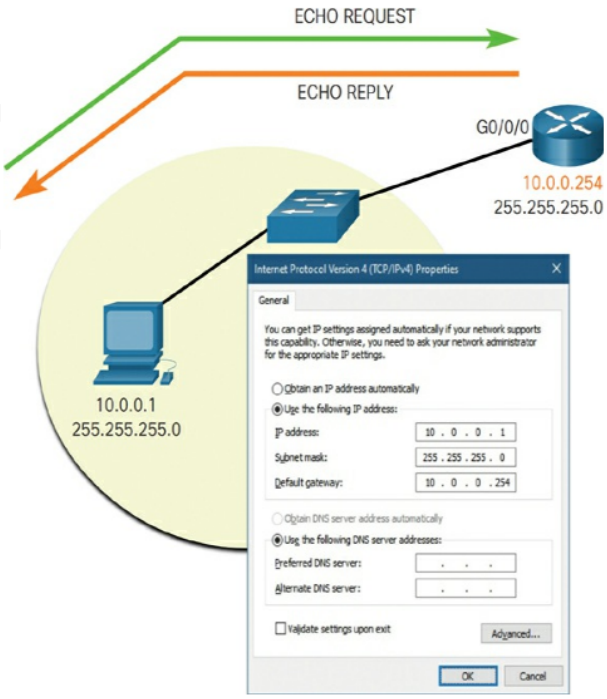
13.2.2 Ping với ICMPv4

- Ping gửi chuỗi echo request đến đích, nhận echo reply.
- Nếu nhận được phản hồi, đường đi kết nối là hoạt động.

Ping địa chỉ Loopback



Ping Default Gateway



13.2.3 Traceroute với ICMPv4

- Gửi gói với TTL tăng dần.
- Mỗi router giảm TTL, khi TTL = 0 thì trả ICMP time exceeded về nguồn.
- Giúp xác định đường đi qua các router trung gian.

13.3 ICMPv6

13.3.1 Các loại thông điệp chính

- **Echo request / reply**: tương tự ICMPv4.
- **Destination unreachable**, **Time exceeded**: tương tự ICMPv4.
- **Neighbor solicitation / advertisement**: dùng trong phân giải địa chỉ (thay ARP).
- **Router solicitation / advertisement**: hỗ trợ tự động cấu hình địa chỉ (SLAAC).

13.3.2 Ping và traceroute với ICMPv6

Hoạt động tương tự ICMPv4, nhưng dùng gói tin ICMPv6.

13.4 Sự khác biệt giữa ICMPv4 và ICMPv6

- ICMPv6 có thêm nhiều chức năng mới: Neighbor Discovery, hỗ trợ SLAAC.
- ICMPv6 bắt buộc trong IPv6; trong khi ICMPv4 thường chỉ dùng bổ trợ.

Tóm tắt

- ICMP cung cấp cơ chế phản hồi lỗi và chẩn đoán trong mạng IP.
- ICMPv4 hỗ trợ echo, unreachable, time exceeded.
- ICMPv6 ngoài các chức năng trên còn có Neighbor Discovery và Router Advertisement.
- Ping và traceroute là hai công cụ phổ biến dựa trên ICMP.

Câu hỏi ôn tập

1. **Vai trò chính của ICMP là gì?**
    - Cung cấp thông tin phản hồi về các vấn đề trong truyền dữ liệu IP.
    - Hỗ trợ chẩn đoán mạng thông qua các công cụ như `ping` và `traceroute`.
2. **Ping hoạt động dựa trên loại thông điệp ICMP nào?**
    - Dựa trên thông điệp **Echo Request** và **Echo Reply**.
3. **Traceroute sử dụng thông điệp ICMP gì?**

- Dựa vào thông điệp **Time Exceeded** để phát hiện các router trung gian trên đường đi.

4. **ICMPv6 bổ sung chức năng nào so với ICMPv4?**
   - Hỗ trợ Neighbor Discovery (thay ARP trong IPv4).
   - Hỗ trợ Router Solicitation/Advertisement cho SLAAC.
5. **Tại sao ICMPv6 được coi là bắt buộc trong IPv6?**
   - Vì nó không chỉ báo lỗi mà còn thực hiện các chức năng cốt lõi như phân giải địa chỉ, tự động cấu hình, phát hiện trùng lặp địa chỉ.
   - Nếu không có ICMPv6 thì IPv6 không thể hoạt động đầy đủ.

13.5 Bài tập Chương 13

1. Một PC gửi 4 gói ping (ICMP Echo Request), mỗi gói 64 byte, đến router. Nếu RTT trung bình là 20 ms, hãy tính tổng thời gian truyền và tổng số byte dữ liệu ICMP được gửi.

   Đáp án:
   Thời gian = $4 \times 20 = 80$ ms. Dữ liệu ICMP = $4 \times 64 = 256$ byte.

2. Một gói ICMP có TTL ban đầu = 8. Nó đi qua 10 router trước khi đến đích. Gói sẽ gặp vấn đề gì?

   Đáp án:
   Sau 8 router TTL = 0. Gói bị loại bỏ tại router thứ 8 và gửi ICMP Time Exceeded về nguồn.

3. Một lệnh traceroute gửi 3 probe đến mỗi hop. Nếu có 12 hop đến đích, hãy tính tổng số gói probe được gửi.

   Đáp án:
   $12 \times 3 = 36$ gói probe.

4. Một PC ping đích 10 lần. 7 lần trả lời, 3 lần timeout. Hãy tính tỷ lệ mất gói (packet loss).

   Đáp án:
   Tỷ lệ mất gói = $3 \uparrow 10 = 30\%$.

5. Một ICMPv4 Destination Unreachable có code = 3. Hãy giải thích ý nghĩa.

   Đáp án:
   Code 3 nghĩa là "Port Unreachable" – cổng đích không mở hoặc dịch vụ không lắng nghe.

6. Một host gửi Neighbor Solicitation trong IPv6. Nếu 50 host trong mạng, hãy tính bao nhiêu thiết bị nhận gói tin.

   Đáp án:
   Gói được gửi đến địa chỉ multicast nhóm đích, chỉ host mục tiêu nhận. $\Rightarrow$ chỉ 1 thiết bị nhận.

7. Một đường truyền có độ trễ lan truyền 2 ms. Nếu ping giữa hai thiết bị mất 12 ms RTT, hãy tính độ trễ xử lý/định tuyến trung gian.

   Đáp án:
   Tổng RTT = 12 ms. Lan truyền 2 chiều = $2 \times 2 = 4$ ms. Xử lý = $12 - 4 = 8$ ms.

8. Một PC gửi 100 gói ping, mỗi gói 32 byte. Nếu tốc độ đường truyền 1 Mbps, hãy tính tổng thời gian truyền toàn bộ dữ liệu ICMP (chỉ tính thời gian truyền).

   Đáp án:
   $100 \times 32 \times 8 = 25,600$ bit. Thời gian = $25,600 \uparrow 10^6 = 0.0256$ s = 25.6 ms.

9. Một router nhận được ICMP Redirect message. Hãy giải thích trường hợp xảy ra và ảnh hưởng đến bảng định tuyến của host.

   Đáp án:
   Redirect xảy ra khi host gửi gói qua router không tối ưu, nhưng router biết tuyến ngắn hơn. Router gửi Redirect để host cập nhật bảng định tuyến cục bộ.

10. Một host IPv6 thực hiện Duplicate Address Detection (DAD). Nó gửi Neighbor Solicitation cho chính địa chỉ của mình. Nếu nhận phản hồi, điều gì xảy ra?

    Đáp án:
    Địa chỉ đã bị trùng. Host không sử dụng địa chỉ đó và phải chọn địa chỉ khác.

13.6 Thuật ngữ cần nhớ

ICMP (Internet Control Message Protocol) Giao thức điều khiển Internet, được tầng Mạng sử dụng để gửi thông báo lỗi và chẩn đoán giữa các thiết bị mạng.

ICMPv4 Phiên bản ICMP dùng cùng với IPv4, hỗ trợ báo lỗi (Destination Unreachable, Time Exceeded) và chẩn đoán (Echo Request/Reply – ping).

ICMPv6 Phiên bản ICMP dùng cùng với IPv6, ngoài báo lỗi và chẩn đoán còn tích hợp Neighbor Discovery Protocol (NDP), Router Solicitation/Advertisement, Duplicate Address Detection (DAD).

Echo Request Bản tin ICMP gửi từ một thiết bị đến thiết bị khác để kiểm tra kết nối. Nếu đích nhận được, nó sẽ phản hồi bằng Echo Reply.

Echo Reply Bản tin ICMP trả lời cho Echo Request, xác nhận rằng thiết bị đích khả dụng và có thể giao tiếp.

Ping Lệnh chẩn đoán sử dụng ICMP Echo Request và Echo Reply để kiểm tra khả năng kết nối giữa hai thiết bị.

Traceroute Lệnh chẩn đoán sử dụng ICMP Time Exceeded (hoặc UDP/TCP tuỳ hệ điều hành) để xác định đường đi của gói tin qua các router trung gian.

Destination Unreachable Thông báo ICMP báo rằng gói tin không thể được chuyển đến đích vì một số lý do (không có tuyến, host không phản hồi, cổng không mở).

Time Exceeded Thông báo ICMP báo rằng TTL (IPv4) hoặc Hop Limit (IPv6) của gói tin đã giảm về 0, thường dùng trong traceroute để phát hiện router trung gian.

Redirect Thông báo ICMP từ router cho host, gợi ý sử dụng tuyến khác hiệu quả hơn để đến cùng đích.

Neighbor Solicitation (NS) Bản tin ICMPv6 yêu cầu địa chỉ MAC của một địa chỉ IPv6 đích trong cùng mạng.

Neighbor Advertisement (NA) Bản tin ICMPv6 trả lời NS, cung cấp địa chỉ MAC tương ứng với địa chỉ IPv6.

Router Solicitation (RS) Bản tin ICMPv6 do host gửi để yêu cầu router cung cấp thông tin mạng.

Router Advertisement (RA) Bản tin ICMPv6 do router gửi, cung cấp prefix, default gateway, và cơ chế cấu hình (SLAAC hoặc DHCPv6).

Duplicate Address Detection (DAD) Quá trình ICMPv6 sử dụng để đảm bảo địa chỉ IPv6 không bị trùng trên mạng.

Parameter Problem Thông báo ICMP báo lỗi khi trường trong header IP không hợp lệ hoặc không được hỗ trợ.

ICMP Type/Code Các trường trong header ICMP xác định loại bản tin (type) và chi tiết nguyên nhân (code). Ví dụ: Echo Request có type 8, code 0 trong ICMPv4.

Control Message Thông điệp ICMP dùng để quản lý và điều khiển mạng, không phải để vận chuyển dữ liệu người dùng.

Chương 14

Tầng Vận chuyển

Mục tiêu

Sau khi hoàn thành chương này, bạn sẽ có thể:

- Giải thích vai trò của tầng vận chuyển trong mô hình OSI.
- Phân biệt TCP và UDP, ưu nhược điểm của từng giao thức.
- Mô tả cơ chế port number và multiplexing/demultiplexing.
- Trình bày các cơ chế đảm bảo độ tin cậy: bắt tay ba bước, ACK, kiểm soát luồng.
- Hiểu ứng dụng thực tế của TCP và UDP trong các dịch vụ mạng.

Thuật ngữ chính

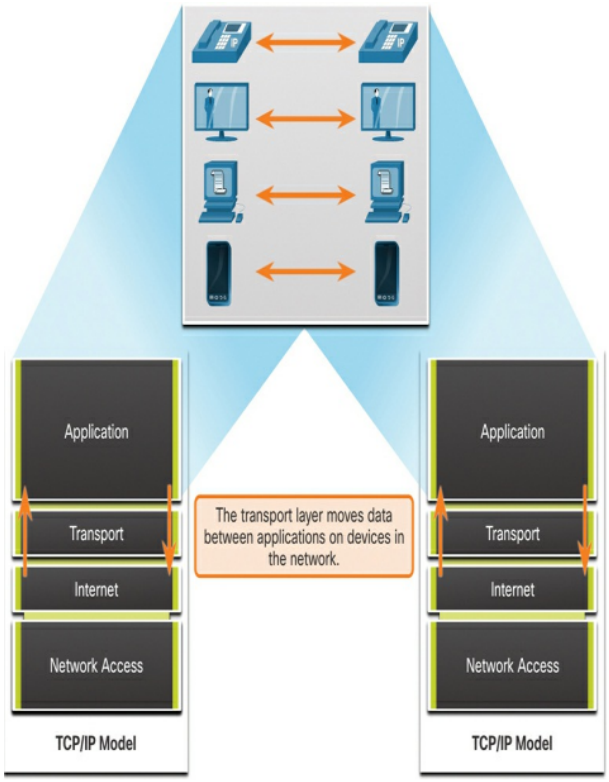
- Transport layer
- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)
- Multiplexing / Demultiplexing
- Port number
- Three-way handshake
- Acknowledgment (ACK)
- Flow control
- Window size
- Reliability

14.1 Giới thiệu

Tầng vận chuyển cung cấp dịch vụ truyền dữ liệu từ tiến trình nguồn đến tiến trình đích. Nó hoạt động trên tầng mạng, sử dụng địa chỉ IP, và bổ sung thông tin port để xác định ứng dụng cụ thể. Hai giao thức chính là **TCP** và **UDP**. Vị trí của tầng này trong mô hình TCP/IP được thể hiện trong Hình 14.1.

14.2 Chức năng của tầng vận chuyển

- **Multiplexing/Demultiplexing**: cho phép nhiều ứng dụng chia sẻ cùng một kết nối mạng, phân biệt bằng port number.
- **Độ tin cậy**: kiểm tra, xác nhận dữ liệu, sắp xếp lại nếu cần.



Hình 14.1: Tầng Vận chuyển trong mô hình TCP/IP.

- **Kiểm soát luồng**: điều chỉnh tốc độ gửi để tránh tràn bộ đệm.
- **Phát hiện lỗi**: dùng checksum để kiểm tra dữ liệu.

14.3 TCP

14.3.1 Đặc điểm

- Kết nối hướng (connection-oriented).
- Đảm bảo độ tin cậy (reliability).
- Thứ tự gói tin được duy trì.
- Có kiểm soát luồng và tắc nghẽn.

14.3.2 Quy trình bắt tay ba bước

1. SYN – Client gửi yêu cầu khởi tạo kết nối.
2. SYN-ACK – Server xác nhận và phản hồi.
3. ACK – Client xác nhận, kết nối được thiết lập.

14.3.3 Cơ chế đảm bảo độ tin cậy

- ACK: xác nhận dữ liệu đã nhận.

- Retransmission: gửi lại khi mất gói.
- Window size: kiểm soát lượng dữ liệu gửi chưa được ACK.

14.4 UDP

14.4.1 Đặc điểm

- Không kết nối (connectionless).
- Không đảm bảo độ tin cậy, không xác nhận, không sắp xếp.
- Ít overhead, nhanh, hiệu quả cho ứng dụng thời gian thực.

14.4.2 Ứng dụng

- DNS (Domain Name System)
- VoIP, video streaming
- Các giao thức cần tốc độ cao, chấp nhận mất gói.

14.5 Port number

- 16 bit, giá trị từ 0–65535.
- Các dải chính:
  - 0–1023: well-known ports (HTTP 80, HTTPS 443, FTP 21, SSH 22).
  - 1024–49151: registered ports.
  - 49152–65535: dynamic/private ports.

14.6 So sánh TCP và UDP

- TCP: tin cậy, có thứ tự, overhead cao hơn, dùng cho web, email, file transfer.
- UDP: không tin cậy, không thứ tự, overhead thấp, dùng cho thoại, video, game online.

Tóm tắt

- Tầng vận chuyển kết nối ứng dụng nguồn và ứng dụng đích qua port number.
- TCP đảm bảo tin cậy bằng bắt tay 3 bước, ACK, retransmission, flow control.
- UDP đơn giản, không đảm bảo tin cậy nhưng nhanh và hiệu quả.
- Port numbers cho phép nhiều dịch vụ chạy đồng thời trên một thiết bị.

Câu hỏi ôn tập

1. **Chức năng chính của tầng Vận chuyển là gì?**
   - Cung cấp truyền thông đầu cuối tới đầu cuối giữa các ứng dụng.
   - Thực hiện phân chia dữ liệu (segmentation), kiểm soát lỗi, kiểm soát luồng, và tái sắp xếp dữ liệu.
2. **Khác biệt chính giữa TCP và UDP?**
   - **TCP**: hướng kết nối, tin cậy, có đánh số thứ tự, có xác nhận (ACK), kiểm soát luồng.
   - **UDP**: không kết nối, không tin cậy, không đảm bảo thứ tự, ít overhead, tốc độ nhanh.
3. **Quy trình bắt tay ba bước của TCP là gì?**
   - Bước 1: Client gửi gói SYN đến server.
   - Bước 2: Server phản hồi bằng gói SYN-ACK.
   - Bước 3: Client gửi ACK, kết nối được thiết lập.
4. **Các loại port number và ví dụ?**
   - Well-known ports (0–1023): HTTP (80), HTTPS (443), FTP (21), SSH (22).
   - Registered ports (1024–49151): ứng dụng do các hãng đăng ký.
   - Dynamic/private ports (49152–65535): dùng tạm thời cho client.
5. **Ứng dụng thực tế thường dùng TCP và UDP?**
   - TCP: web (HTTP/HTTPS), email (SMTP, IMAP, POP3), FTP.
   - UDP: DNS, VoIP, video streaming, game trực tuyến.

14.7 Bài tập Chương 14

1. Một ứng dụng gửi 12.000 byte dữ liệu qua TCP. Nếu MSS (Maximum Segment Size) = 1460 byte, hãy tính số segment TCP được tạo ra.

   Đáp án:
   $12{,}000 \uparrow\uparrow 1460 \approx 8.22 \Rightarrow 9$ segment. (8 segment đầy đủ và 1 segment chứa phần dư).

2. Một segment TCP có payload 1000 byte, header TCP 20 byte, header IP 20 byte. Hãy tính kích thước toàn bộ gói IP và tỷ lệ overhead.

   Đáp án:
   Tổng = $1000 + 20 + 20 = 1040$ byte. Overhead = $40 \uparrow\uparrow 1040 \approx 3.85\%$.

3. Một client mở 500 kết nối TCP đồng thời, mỗi kết nối chiếm trung bình 64 byte thông tin trạng thái trong bộ nhớ. Hãy tính tổng dung lượng bộ nhớ cần thiết.

   Đáp án:
   $500 \times 64 = 32{,}000$ byte = 31.25 KB.

4. Trong quá trình bắt tay 3 bước (three-way handshake), có bao nhiêu segment TCP được trao đổi? Nếu mỗi segment dài 60 byte, hãy tính tổng dung lượng truyền trong quá trình này.

   Đáp án:
   3 segment (SYN, SYN-ACK, ACK). Tổng dung lượng = $3 \times 60 = 180$ byte.

5. Một kết nối TCP truyền file 4 MB. Nếu mất 2 segment, mỗi segment dài 1500 byte, hãy tính tổng số dữ liệu cần truyền lại.

   Đáp án:
   $2 \times 1500 = 3000$ byte cần truyền lại.

6. Một ứng dụng sử dụng UDP để gửi 800 gói tin, mỗi gói 512 byte dữ liệu + 8 byte UDP header + 20 byte IP header. Hãy tính tổng dung lượng được truyền.

   Đáp án:
   Kích thước 1 gói = $512 + 8 + 20 = 540$ byte. Tổng = $800 \times 540 = 432{,}000$ byte.

7. Một segment TCP có số thứ tự (Sequence Number) = 3001 và chứa 500 byte dữ liệu. Hãy tính số xác nhận (Acknowledgment Number) mong đợi từ phía nhận.

   Đáp án:
   ACK = $3001 + 500 = 3501$.

8. Một kết nối TCP có window size = 32 KB, MSS = 1460 byte. Hãy tính số segment tối đa có thể gửi mà không cần ACK.

   Đáp án:
   $32{,}768 \underset{\Uparrow}{} 1460 \approx 22.4 \Rightarrow 22$ segment đầy đủ.

9. Một ứng dụng thời gian thực gửi 100 gói UDP/giây, mỗi gói 1200 byte. Hãy tính tốc độ dữ liệu trung bình mà ứng dụng sử dụng.

   Đáp án:
   $100 \times 1200 \times 8 = 960{,}000$ bps = 960 Kbps.

10. Một kết nối TCP truyền file 10 MB trên đường truyền có băng thông 10 Mbps. Bỏ qua overhead, hãy tính thời gian truyền file.

    Đáp án:
    10 MB = $10 \times 8 \times 10^6 = 80 \times 10^6$ bit. Thời gian = $80 \times 10^6 \underset{\Uparrow}{} 10 \times 10^6 = 8$ giây.

14.8 Thuật ngữ cần nhớ

Transport Layer (Tầng Vận chuyển) Tầng 4 của mô hình OSI, cung cấp truyền thông tin cậy đầu cuối–đến–đầu cuối (end-to-end) giữa các ứng dụng, đảm bảo dữ liệu đến đúng tiến trình đích.

Multiplexing (Ghép kênh) Cơ chế cho phép nhiều ứng dụng cùng chia sẻ một kết nối mạng. Tầng Vận chuyển phân biệt các luồng dữ liệu bằng số cổng (port number).

De-multiplexing (Tách kênh) Quá trình ngược lại với multiplexing: tầng Vận chuyển nhận dữ liệu và phân phối cho ứng dụng thích hợp dựa trên cặp địa chỉ IP và số cổng.

Port Number Số hiệu định danh một ứng dụng hoặc dịch vụ trong tầng Vận chuyển. Ví dụ: HTTP (80), HTTPS (443), FTP (21).

Well-known Ports Các số cổng từ 0 đến 1023, được gán cho các dịch vụ tiêu chuẩn toàn cầu (HTTP, FTP, SMTP, DNS, SSH, . . .).

Registered Ports Các số cổng từ 1024 đến 49151, được đăng ký cho các ứng dụng hoặc dịch vụ cụ thể.

Dynamic/Private Ports Các số cổng từ 49152 đến 65535, được sử dụng tạm thời (ephemeral) cho các kết nối của client.

TCP (Transmission Control Protocol) Giao thức vận chuyển hướng kết nối, tin cậy, cung cấp cơ chế đánh số thứ tự, xác nhận (ACK), kiểm soát luồng và truyền lại khi mất gói.

UDP (User Datagram Protocol) Giao thức vận chuyển không kết nối, không tin cậy, ít overhead, thích hợp cho các ứng dụng thời gian thực như video/voice streaming, DNS.

Connection-oriented Communication Kiểu truyền thông yêu cầu thiết lập kết nối logic trước khi trao đổi dữ liệu. TCP là ví dụ điển hình.

Three-way Handshake Quá trình thiết lập kết nối TCP gồm 3 bước: SYN, SYN-ACK, ACK, đảm bảo đồng bộ giữa client và server.

Segmentation Quá trình tầng Vận chuyển chia dữ liệu ứng dụng lớn thành các segment nhỏ để truyền, và tái lắp ghép ở đầu nhận.

Sequence Number Trường trong header TCP đánh số byte dữ liệu, dùng để tái lắp ghép đúng thứ tự và phát hiện mất gói.

Acknowledgment Number Trường trong header TCP cho biết số thứ tự byte tiếp theo mà bên nhận mong đợi, xác nhận đã nhận dữ liệu.

Flow Control Cơ chế TCP điều chỉnh tốc độ gửi của bên phát dựa trên khả năng nhận (window size) của bên nhận.

Window Size Trường trong header TCP cho biết số byte dữ liệu mà bên nhận có thể tiếp nhận mà không cần ACK, dùng cho kiểm soát luồng.

Error Detection Quá trình phát hiện lỗi nhờ trường checksum trong header TCP và UDP.

Reliability Đặc tính của TCP đảm bảo dữ liệu đến đích chính xác, đầy đủ và theo đúng thứ tự.

UDP Datagram Đơn vị dữ liệu tại tầng Vận chuyển khi dùng UDP. Nó có header đơn giản (số cổng nguồn, số cổng đích, độ dài, checksum).

Low Latency Applications Ứng dụng yêu cầu độ trễ thấp (VoIP, video call, game online) thường sử dụng UDP để ưu tiên tốc độ hơn độ tin cậy.

Chương 15

Tầng Ứng dụng

Mục tiêu

Sau khi hoàn thành chương này, bạn sẽ có thể:

- Giải thích vai trò của tầng ứng dụng trong mô hình OSI và TCP/IP.
- Mô tả các giao thức phổ biến: HTTP, HTTPS, DNS, DHCP, FTP, SMTP, POP3, IMAP.
- Phân biệt dịch vụ client-server và peer-to-peer (P2P).
- Hiểu cơ chế hoạt động cơ bản của dịch vụ web và email.
- Liên hệ cách ứng dụng sử dụng port và giao thức tầng dưới.

Thuật ngữ chính

- Application layer
- Client-server
- Peer-to-peer (P2P)
- HTTP/HTTPS
- DNS
- DHCP
- FTP
- SMTP / POP3 / IMAP
- Port numbers

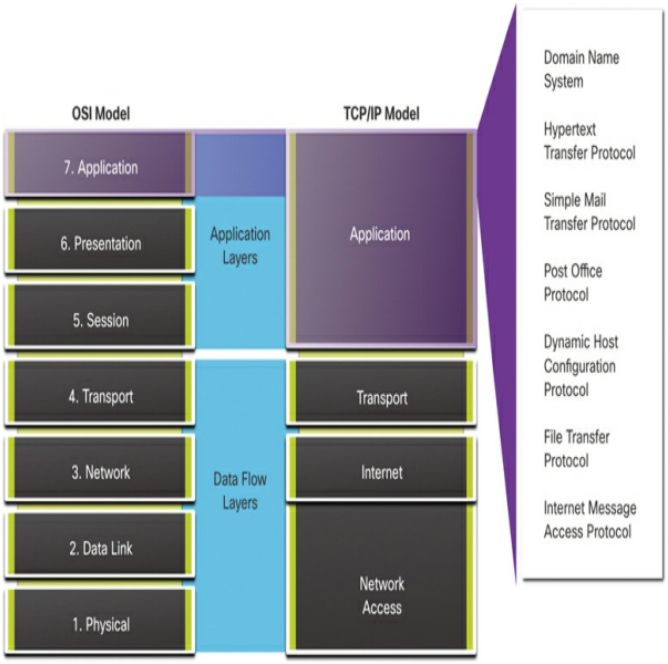
15.1 Giới thiệu

Tầng ứng dụng là tầng gần người dùng nhất. Nó cung cấp giao diện để ứng dụng trao đổi dữ liệu qua mạng. Các giao thức tầng ứng dụng trong Hình 15.1 định nghĩa cách ứng dụng định dạng, truyền và xử lý thông tin.

15.2 Mô hình client-server và P2P

15.2.1 Client-server

- Máy client gửi yêu cầu dịch vụ, server phản hồi.
- Ví dụ: duyệt web (client là trình duyệt, server là máy chủ web).



Hình 15.1: Các giao thức tầng ứng dụng.

15.2.2 Peer-to-peer

- Các thiết bị vừa là client vừa là server.
- P2P có thể là mạng trực tiếp (ad hoc) hoặc dựa trên ứng dụng (BitTorrent, Skype).

15.3 Các giao thức dịch vụ phổ biến

15.3.1 Web: HTTP và HTTPS

- **HTTP** (port 80): giao thức truyền siêu văn bản, nền tảng web.
- **HTTPS** (port 443): bổ sung mã hóa TLS/SSL, bảo mật hơn.

15.3.2 Tên miền: DNS

- DNS phân giải tên miền thành địa chỉ IP.
- Hoạt động dựa trên hệ thống máy chủ phân cấp.

15.3.3 Cấp phát địa chỉ: DHCP

- Cấp phát địa chỉ IP động cho thiết bị.
- Quy trình: Discover $\rightarrow$ Offer $\rightarrow$ Request $\rightarrow$ ACK.

15.3.4 Truyền tệp: FTP

- Dùng để tải lên/tải xuống tệp giữa client và server.
- Hoạt động ở port 20 (data) và 21 (control).

15.3.5 Email: SMTP, POP3, IMAP

- **SMTP** (port 25): gửi thư đi.
- **POP3** (port 110): tải thư về client, thường xóa khỏi server.
- **IMAP** (port 143): đồng bộ thư giữa client và server.

15.4 Ứng dụng và cổng dịch vụ

- Mỗi dịch vụ tầng ứng dụng dùng port cố định để phân biệt.
- Ví dụ: HTTP dùng 80, HTTPS dùng 443, DNS dùng 53, DHCP dùng 67/68.

Tóm tắt

- Tầng ứng dụng cung cấp giao diện giữa ứng dụng và mạng.
- Có hai mô hình dịch vụ chính: client-server và peer-to-peer.
- Các giao thức phổ biến: HTTP/HTTPS, DNS, DHCP, FTP, SMTP, POP3, IMAP.
- Port numbers giúp nhiều dịch vụ chạy song song trên cùng thiết bị.

Câu hỏi ôn tập

1. **Vai trò của tầng Ứng dụng là gì?**
   - Cung cấp giao diện giữa ứng dụng của người dùng và mạng.
   - Định nghĩa cách ứng dụng định dạng, truyền và xử lý dữ liệu.
2. **Khác biệt giữa client-server và peer-to-peer (P2P)?**
   - **Client-server**: client yêu cầu dịch vụ, server cung cấp dịch vụ. Ví dụ: trình duyệt web và máy chủ web.
   - **P2P**: các thiết bị vừa đóng vai trò client vừa là server. Ví dụ: BitTorrent, Skype.
3. **Giao thức nào dùng để phân giải tên miền?**
   - DNS (Domain Name System).
4. **Quy trình cấp phát địa chỉ DHCP gồm những bước nào?**
   - Discover → Offer → Request → Acknowledgment (DORA).
5. **Khác biệt POP3 và IMAP trong dịch vụ email?**
   - **POP3**: tải email về thiết bị và thường xóa khỏi server.
   - **IMAP**: giữ email trên server và đồng bộ giữa nhiều thiết bị.

15.5 Bài tập Chương 15

1. Một client gửi 50 yêu cầu HTTP, mỗi yêu cầu 800 byte dữ liệu, cộng với 40 byte header TCP/IP. Hãy tính tổng số byte được gửi từ client đến server.

   Đáp án:
   Mỗi yêu cầu = $800 + 40 = 840$ byte. Tổng = $50 \times 840 = 42{,}000$ byte.

2. Một email có kích thước 2 MB được gửi qua SMTP. Nếu mỗi segment TCP có payload 1460 byte, hãy tính số segment TCP cần thiết.

   Đáp án:
   $2 \times 10^6 \Uparrow 1460 \approx 1369.86 \Rightarrow 1370$ segment.

3. Một DNS query 60 byte và DNS reply 500 byte. Nếu client gửi 100 truy vấn, hãy tính tổng dung lượng dữ liệu DNS qua lại.

   Đáp án:
   Mỗi lượt = $60 + 500 = 560$ byte. Tổng = $100 \times 560 = 56{,}000$ byte.

4. Một client tải xuống file 25 MB từ FTP server. Nếu tốc độ đường truyền 10 Mbps, hãy tính thời gian tối thiểu cần thiết (bỏ qua overhead).

   Đáp án:
   $25 \times 8 = 200$ Mb. $200 \Uparrow 10 = 20$ giây.

5. Một host nhận cấu hình IP qua DHCP gồm: IP, subnet mask, default gateway, DNS. Nếu mỗi thông tin chiếm trung bình 20 byte, hãy tính kích thước dữ liệu cấu hình được gửi đến host.

   Đáp án:
   Tổng = $4 \times 20 = 80$ byte.

6. Một client duyệt web gửi 10 request HTTP, mỗi request 1000 byte. Server trả lời mỗi request bằng 50 KB dữ liệu. Hãy tính tổng lượng dữ liệu server gửi về.

   Đáp án:
   10×50 KB = 500 KB.

7. Một hệ thống NTP đồng bộ thời gian mỗi 64 giây bằng một gói 90 byte. Hãy tính tổng dữ liệu NTP trao đổi trong 1 giờ.

   Đáp án:
   1 giờ = 3600 giây. Số lần đồng bộ = $3600 \Uparrow 64 \approx 56.25 \Rightarrow 56$ lần. Tổng dữ liệu = $56 \times 90 = 5040$ byte.

8. Một host gửi 300 email trong ngày, mỗi email trung bình 100 KB. Hãy tính tổng lượng dữ liệu email được gửi đi.

   Đáp án:
   300×100 KB = 30,000 KB = 30 MB.

9. Một DNS server xử lý trung bình 500 query/giây. Nếu mỗi query 100 byte và reply 200 byte, hãy tính throughput dữ liệu DNS.

   Đáp án:
   Mỗi cặp query-reply = 300 byte. $500 \times 300 = 150{,}000$ byte/s ≈ 1.2 Mbps.

10. Một người dùng tải xuống video 200 MB qua HTTP streaming. Nếu tốc độ trung bình 8 Mbps, hãy tính thời gian tải.

Đáp án:
$200 \times 8 = 1600$ Mb. $1600 \overset{\uparrow\uparrow}{} 8 = 200$ giây ≈ 3 phút 20 giây.

15.6 Thuật ngữ cần nhớ

Application Layer (Tầng Ứng dụng) Tầng cao nhất trong mô hình OSI và TCP/IP, cung cấp giao diện trực tiếp giữa ứng dụng người dùng và mạng. Các giao thức tầng này hỗ trợ dịch vụ như web, email, chia sẻ tệp.

Client Thiết bị hoặc phần mềm khởi tạo yêu cầu dịch vụ mạng, ví dụ: trình duyệt web gửi yêu cầu HTTP đến máy chủ.

Server Thiết bị hoặc phần mềm cung cấp dịch vụ theo yêu cầu từ client, ví dụ: web server trả về trang HTML cho trình duyệt.

Client-Server Model Mô hình mạng trong đó client gửi yêu cầu và server phản hồi. Server có thể phục vụ nhiều client đồng thời.

Peer-to-Peer (P2P) Network Mạng trong đó các thiết bị vừa đóng vai trò client vừa làm server, chia sẻ trực tiếp tài nguyên mà không cần máy chủ trung tâm.

P2P Application Ứng dụng cho phép thiết bị vừa tải xuống vừa tải lên tài nguyên, ví dụ: BitTorrent, Skype.

DNS (Domain Name System) Giao thức phân giải tên miền (ví dụ: `www.example.com`) thành địa chỉ IP, giúp người dùng truy cập dịch vụ bằng tên dễ nhớ thay vì IP.

DHCP (Dynamic Host Configuration Protocol) Giao thức cấp phát tự động địa chỉ IP, subnet mask, default gateway và DNS cho host.

HTTP (Hypertext Transfer Protocol) Giao thức truyền tải dữ liệu web giữa trình duyệt và web server. Phiên bản an toàn (HTTPS) dùng TLS để mã hóa.

SMTP (Simple Mail Transfer Protocol) Giao thức dùng để gửi email từ client đến mail server hoặc giữa các mail server.

POP3 (Post Office Protocol version 3) Giao thức cho phép client tải email từ server về và thường xoá bản sao trên server.

IMAP (Internet Message Access Protocol) Giao thức quản lý email, cho phép đồng bộ email giữa client và server, giữ bản sao email trên server.

FTP (File Transfer Protocol) Giao thức truyền tệp tin giữa client và server. Có hai kênh: kênh điều khiển (port 21) và kênh dữ liệu.

SFTP (SSH File Transfer Protocol) Phiên bản FTP chạy trên giao thức SSH, hỗ trợ mã hóa để bảo mật dữ liệu.

TFTP (Trivial File Transfer Protocol) Phiên bản đơn giản của FTP, không xác thực, dùng UDP port 69. Thường dùng để tải firmware, file cấu hình.

Telnet Giao thức truy cập từ xa dòng lệnh không bảo mật (dữ liệu truyền ở dạng văn bản rõ ràng).

SSH (Secure Shell) Giao thức truy cập từ xa an toàn, thay thế Telnet, sử dụng mã hóa để bảo vệ dữ liệu và xác thực.

URL (Uniform Resource Locator) Địa chỉ định danh tài nguyên trên web, gồm giao thức (http/https), tên miền và đường dẫn (ví dụ: `https://www.example.com/page.html`).

FQDN (Fully Qualified Domain Name) Tên miền đầy đủ, xác định duy nhất một máy chủ trên Internet. Ví dụ: `mail.example.com`.

Resource Record Bản ghi DNS mô tả tài nguyên trong miền, ví dụ: A record (IP), MX record (mail server), CNAME (bí danh).

NTP (Network Time Protocol) Giao thức đồng bộ thời gian giữa các thiết bị mạng với độ chính xác cao.

SNMP (Simple Network Management Protocol) Giao thức quản lý mạng, cho phép giám sát và điều khiển thiết bị thông qua agent và trình quản lý.

Chương 16

Các nguyên tắc cơ bản về an ninh mạng

Mục tiêu

Sau khi hoàn thành chương này, bạn sẽ có thể:

- Giải thích các mối đe dọa an ninh mạng phổ biến.
- Mô tả các kiểu tấn công: malware, DoS, spoofing, phishing, social engineering.
- Hiểu khái niệm bảo mật: tính bí mật, toàn vẹn, khả dụng (CIA triad).
- Liệt kê biện pháp bảo mật cơ bản: tường lửa, ACL, VPN, mã hóa.
- Cấu hình bảo mật cơ bản trên router và switch (mật khẩu, SSH, banner).

Thuật ngữ chính

- CIA triad
- Malware
- Virus, Worm, Trojan
- DoS, DDoS
- Phishing
- Spoofing
- Social engineering
- Firewall
- ACL (Access Control List)
- VPN (Virtual Private Network)
- SSH (Secure Shell)

16.1 Giới thiệu

An ninh mạng là yếu tố quan trọng trong thiết kế và vận hành mạng. Các cuộc tấn công mạng ngày càng tinh vi, có thể gây mất dữ liệu, gián đoạn dịch vụ hoặc chiếm quyền điều khiển hệ thống. Quản trị viên cần hiểu các nguyên tắc cơ bản để bảo vệ hạ tầng.

16.2 Nguyên tắc CIA

- **Confidentiality** – Tính bí mật: dữ liệu chỉ được truy cập bởi người có quyền.

- **Integrity** – Tính toàn vẹn: dữ liệu không bị thay đổi trái phép.
- **Availability** – Khả dụng: dịch vụ luôn sẵn sàng cho người dùng hợp pháp.

16.3 Các mối đe dọa và tấn công

16.3.1 Malware

- **Virus**: lây nhiễm tệp, cần hành động của người dùng để kích hoạt.
- **Worm**: tự lây lan qua mạng, không cần người dùng.
- **Trojan**: giả dạng phần mềm hợp pháp để cài cửa hậu.

16.3.2 Tấn công DoS/DDoS

- Làm cạn kiệt tài nguyên hệ thống hoặc đường truyền, khiến dịch vụ ngừng hoạt động.

16.3.3 Spoofing và phishing

- **Spoofing**: giả mạo địa chỉ IP, MAC hoặc email để đánh lừa.
- **Phishing**: lừa đảo người dùng cung cấp thông tin nhạy cảm qua email/website giả mạo.

16.3.4 Social engineering

Khai thác yếu tố con người bằng cách lừa gạt, dụ dỗ để có quyền truy cập.

16.4 Biện pháp bảo mật cơ bản

16.4.1 Tường lửa và ACL

- **Firewall**: lọc lưu lượng giữa mạng tin cậy và không tin cậy.
- **ACL**: danh sách kiểm soát truy cập trên router, xác định lưu lượng cho phép/chặn.

16.4.2 Mã hóa và VPN

- **VPN**: tạo kênh bảo mật qua Internet bằng mã hóa.
- Đảm bảo dữ liệu bí mật và toàn vẹn khi truyền qua mạng công cộng.

16.4.3 Xác thực và mật khẩu

- Sử dụng mật khẩu mạnh, chính sách đổi mật khẩu định kỳ.
- Dùng SSH thay Telnet để bảo mật kết nối quản trị.

16.5 Bảo mật cơ bản trên thiết bị Cisco

16.5.1 Cấu hình mật khẩu

```
Router(config)# enable secret <MATKHAU_MANH>
Router(config)# line console 0
Router(config-line)# password <MATKHAU_CONSOLE>
Router(config-line)# login
Router(config)# line vty 0 4
Router(config-line)# password <MATKHAU_VTY>
Router(config-line)# login
```

16.5.2 Banner cảnh báo

```
Router(config)# banner motd #Truy cập trái phép bị cấm#
```

16.5.3 Bật SSH

```
Router(config)# ip domain-name example.com
Router(config)# crypto key generate rsa
Router(config)# username admin secret <MATKHAU>
Router(config)# line vty 0 4
Router(config-line)# transport input ssh
```

Tóm tắt

- An ninh mạng dựa trên nguyên tắc CIA: bí mật, toàn vẹn, khả dụng.
- Các mối đe dọa: malware, DoS/DDoS, spoofing, phishing, social engineering.
- Biện pháp cơ bản: firewall, ACL, VPN, mã hóa, xác thực.
- Thiết bị Cisco có thể cấu hình bảo mật: mật khẩu, SSH, banner.

Câu hỏi ôn tập

1. **Ba yếu tố trong nguyên tắc CIA là gì?**
   - Confidentiality (Bí mật).
   - Integrity (Toàn vẹn).
   - Availability (Khả dụng).
2. **Phân biệt virus, worm và trojan?**
   - **Virus**: gắn vào tệp, cần người dùng kích hoạt.
   - **Worm**: tự lây lan qua mạng mà không cần người dùng.
   - **Trojan**: giả dạng phần mềm hợp pháp, cài cửa hậu.
3. **Tấn công DoS/DDoS có mục đích gì?**
   - Làm cạn kiệt tài nguyên của hệ thống hoặc đường truyền.

- Khiến dịch vụ không thể phục vụ người dùng hợp pháp.

4. **SSH an toàn hơn Telnet ở điểm nào?**
   - SSH mã hóa dữ liệu truyền đi, bao gồm mật khẩu và lệnh.
   - Telnet gửi dữ liệu dạng plain text, dễ bị nghe lén.
5. **ACL dùng để làm gì?**
   - Xác định lưu lượng nào được phép hoặc bị chặn trên router hoặc switch.
   - Giúp kiểm soát truy cập, tăng cường bảo mật cho mạng.

16.6 Bài tập Chương 16

1. Một firewall kiểm tra trung bình 50.000 gói/giây. Nếu mỗi gói dài 800 byte, hãy tính throughput dữ liệu firewall xử lý.

   Đáp án:
   $50{,}000 \times 800 \times 8 = 320 \times 10^6$ bit/s = 320 Mbps.

2. Một tổ chức triển khai IPS phát hiện 2% gói tin bất thường trong tổng số 2 triệu gói/ngày. Hãy tính số gói bị đánh dấu.

   Đáp án:
   $2{,}000{,}000 \times 0.02 = 40{,}000$ gói.

3. Một hệ thống VPN tạo kết nối an toàn 200 Mbps. Nếu mỗi gói tin thêm 40 byte overhead bảo mật, hãy tính tỷ lệ overhead khi payload trung bình 1000 byte.

   Đáp án:
   Tổng = $1000 + 40 = 1040$ byte. Overhead ratio = $40 \over 1040 \approx 3.85\%$.

4. Một mật khẩu có độ dài 8 ký tự, gồm chữ cái thường (26). Hãy tính số khả năng tổ hợp mật khẩu.

   Đáp án:
   $26^8 \approx 2.09 \times 10^{11}$ khả năng.

5. Nếu thêm chữ hoa (26) và số (10), tổng ký tự = 62. Với mật khẩu dài 10 ký tự, hãy tính số tổ hợp.

   Đáp án:
   $62^{10} \approx 8.39 \times 10^{17}$ khả năng.

6. Một tấn công DDoS gửi 5 triệu gói/giây, mỗi gói 600 byte. Hãy tính băng thông cần thiết cho tấn công.

   Đáp án:
   $5{,}000{,}000 \times 600 \times 8 = 24 \times 10^9$ bit/s = 24 Gbps.

7. Một IDS giám sát 1 Gbps lưu lượng, với 5% là cảnh báo giả (false positive). Nếu trung bình 100.000 cảnh báo/ngày, hãy tính số cảnh báo giả.

   Đáp án:
   $100{,}000 \times 0.05 = 5000$ cảnh báo giả.

8. Một công ty có 500 nhân viên, mỗi nhân viên sử dụng VPN với băng thông trung bình 2 Mbps. Hãy tính tổng băng thông cần thiết.

   Đáp án:
   $500 \times 2 = 1000$ Mbps = 1 Gbps.

9. Một firewall xử lý 10 Gbps lưu lượng. Nếu cấu hình thêm tính năng mã hóa làm giảm hiệu năng 15%, hãy tính throughput tối đa còn lại.

   Đáp án:
   $10 \times 1 - 0.15 = 8.5$ Gbps.

10. Một hệ thống xác thực dùng OTP có thời gian hiệu lực 60 giây. Nếu người dùng nhập sai trung bình 3 lần trước khi đúng, hãy tính tổng thời gian trung bình để đăng nhập thành công.

    Đáp án:
    Mỗi lần sai + thử lại ≈ 60 giây. $3 \times 60 = 180$ giây (≈ 3 phút).

16.7 Thuật ngữ cần nhớ

Network Security Tập hợp các biện pháp nhằm bảo vệ dữ liệu, thiết bị và tài nguyên mạng khỏi truy cập trái phép, tấn công, hoặc thất thoát.

Confidentiality (Tính bí mật) Nguyên tắc bảo mật đảm bảo thông tin chỉ được truy cập bởi những người/thiết bị được ủy quyền. Biện pháp thường dùng: mã hóa dữ liệu.

Integrity (Tính toàn vẹn) Đảm bảo dữ liệu không bị thay đổi trái phép trong quá trình lưu trữ hoặc truyền tải. Thường áp dụng cơ chế băm (hashing) và chữ ký số.

Availability (Tính sẵn sàng) Đảm bảo hệ thống và dữ liệu luôn sẵn sàng cho người dùng hợp pháp. Tấn công từ chối dịch vụ (DoS/DDoS) đe dọa nguyên tắc này.

Threat (Mối đe dọa) Bất kỳ tình huống hay sự kiện nào có khả năng gây hại đến bảo mật mạng.

Vulnerability (Lỗ hổng) Điểm yếu trong hệ thống hoặc quy trình có thể bị khai thác bởi mối đe dọa để gây hại.

Attack (Cuộc tấn công) Hành động khai thác lỗ hổng nhằm gây thiệt hại, đánh cắp hoặc phá hoại dữ liệu/hệ thống.

Malware (Phần mềm độc hại) Chương trình được thiết kế để gây hại, bao gồm virus, sâu (worm), trojan, spyware, ransomware.

Social Engineering Hình thức tấn công khai thác yếu tố con người, dụ dỗ hoặc lừa gạt để lấy thông tin nhạy cảm (ví dụ: phishing, giả mạo email).

Phishing Tấn công giả mạo email/tin nhắn nhằm lừa người dùng cung cấp thông tin nhạy cảm như mật khẩu, tài khoản ngân hàng.

DoS (Denial of Service) Tấn công từ chối dịch vụ, làm tê liệt dịch vụ bằng cách gửi lượng lớn yêu cầu vượt quá khả năng xử lý.

DDoS (Distributed Denial of Service) Phiên bản DoS mở rộng, nhiều thiết bị bị chiếm quyền điều khiển (botnet) cùng tấn công một mục tiêu.

Firewall Thiết bị hoặc phần mềm kiểm soát lưu lượng vào/ra mạng dựa trên chính sách bảo mật, ngăn chặn truy cập trái phép.

Intrusion Detection System (IDS) Hệ thống giám sát mạng, phát hiện hành vi bất thường hoặc tấn công và đưa ra cảnh báo.

Intrusion Prevention System (IPS) Phiên bản nâng cao của IDS, có thể chủ động chặn hoặc giảm thiểu các mối đe dọa khi phát hiện.

VPN (Virtual Private Network) Mạng riêng ảo, tạo kênh truyền dữ liệu an toàn qua Internet bằng cách mã hóa và xác thực.

Authentication Quá trình xác minh danh tính của người dùng hoặc thiết bị (ví dụ: username/password, chứng chỉ số, OTP).

Authorization Quá trình xác định quyền truy cập của người dùng hoặc thiết bị sau khi đã xác thực.

Accounting (AAA) Ghi nhận và theo dõi hoạt động của người dùng (ai, làm gì, khi nào). Cùng với Authentication và Authorization tạo thành AAA.

Symmetric Encryption Phương pháp mã hóa dùng cùng một khóa cho cả mã hóa và giải mã. Nhanh nhưng cần cơ chế chia sẻ khóa an toàn.

Asymmetric Encryption Phương pháp mã hóa sử dụng cặp khóa công khai và khóa riêng tư. Thường dùng trong trao đổi khóa và chữ ký số.

Hash Function Hàm băm biến đổi dữ liệu thành chuỗi cố định, dùng để kiểm tra toàn vẹn dữ liệu. Ví dụ: MD5, SHA-256.

Public Key Infrastructure (PKI) Hệ thống quản lý khóa và chứng chỉ số, hỗ trợ xác thực và mã hóa dựa trên hạ tầng khóa công khai.

WPA2/WPA3 Các chuẩn bảo mật không dây thay thế WEP, cung cấp cơ chế mã hóa mạnh (AES) cho Wi-Fi.

Access Control List (ACL) Danh sách quy tắc trên router hoặc firewall để cho phép hoặc từ chối lưu lượng dựa trên tiêu chí như địa chỉ IP, giao thức, port.

Zero Trust Mô hình bảo mật hiện đại: "Không tin tưởng bất kỳ ai, xác thực mọi thứ", áp dụng xác thực liên tục và giới hạn quyền tối thiểu.

Chương 17

Xây dựng một mạng nhỏ

17.1 Giới thiệu

Trong các chương trước, chúng ta đã tìm hiểu về cách thức hoạt động của mạng, cách dữ liệu được truyền tải, vai trò của địa chỉ và các giao thức. Chương này tập trung vào việc kết hợp tất cả những kiến thức đó để xây dựng một mạng nhỏ hoàn chỉnh.

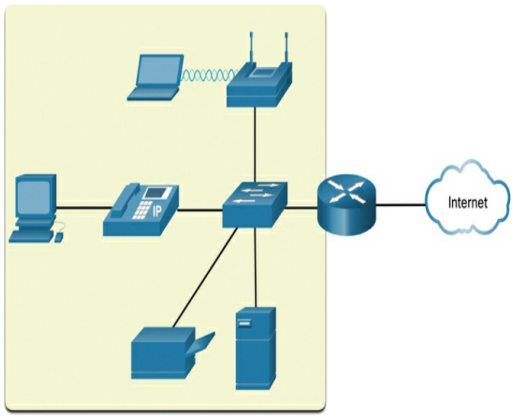
Một mạng nhỏ bao gồm các thiết bị đầu cuối (PC, laptop, điện thoại thông minh), các thiết bị mạng (switch, router, điểm truy cập không dây), và các dịch vụ mạng (DHCP, DNS). Việc thiết kế và triển khai mạng đòi hỏi sự hiểu biết về địa chỉ IP, cấu hình thiết bị, bảo mật cơ bản và cách khắc phục sự cố.

Sau khi hoàn thành chương này, bạn sẽ có thể:

- Mô tả các thành phần cần thiết để xây dựng một mạng nhỏ.
- Cấu hình cơ bản cho router, switch và thiết bị đầu cuối.
- Thiết lập kết nối có dây và không dây.
- Xác minh kết nối và khắc phục sự cố cơ bản.

17.2 Các thành phần của một mạng nhỏ

Một mạng nhỏ như Hình 17.1 thường bao gồm các loại thành phần sau:



Hình 17.1: Topology mạng của một doanh nghiệp nhỏ.

17.2.1 Thiết bị đầu cuối

Thiết bị đầu cuối là nơi dữ liệu được tạo ra hoặc nhận. Ví dụ: máy tính để bàn, máy tính xách tay, điện thoại thông minh, máy in mạng. Các thiết bị này cần địa chỉ IP hợp lệ để giao tiếp trên mạng.

17.2.2 Thiết bị trung gian

Thiết bị trung gian kết nối các thiết bị đầu cuối và điều khiển lưu lượng trong mạng.

- **Switch**: kết nối nhiều thiết bị trong cùng một mạng LAN.
- **Router**: kết nối nhiều mạng với nhau và định tuyến dữ liệu.
- **Access Point**: cung cấp kết nối không dây cho thiết bị di động.

17.2.3 Phương tiện truyền

Là đường dẫn để dữ liệu di chuyển. Có ba loại chính:

- Cáp đồng xoắn đôi (UTP).
- Cáp quang.
- Kết nối không dây (Wi-Fi).

17.2.4 Dịch vụ mạng (Network Services)

Dịch vụ mạng cung cấp chức năng cho người dùng và ứng dụng, ví dụ:

- **DHCP**: cấp phát địa chỉ IP động.
- **DNS**: phân giải tên miền thành địa chỉ IP.
- **Email, Web, File sharing**: cung cấp tiện ích cho người dùng.

17.3 Thiết kế và địa chỉ hóa mạng nhỏ

Khi xây dựng một mạng nhỏ, cần xem xét các yếu tố thiết kế và kế hoạch địa chỉ để đảm bảo mạng hoạt động hiệu quả và dễ quản lý.

17.3.1 Kế hoạch địa chỉ IP

Một sơ đồ địa chỉ IP hợp lý giúp quản trị viên dễ dàng quản lý và khắc phục sự cố.

- Sử dụng địa chỉ **IPv4 riêng** cho mạng nội bộ (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16).
- Phân chia địa chỉ cho các thiết bị theo nhóm: máy chủ, máy trạm, máy in, thiết bị di động.
- Đảm bảo gateway mặc định được cấu hình đúng trên mỗi subnet.

17.3.2 Địa chỉ IPv6

Khi triển khai IPv6, cần xác định prefix được ISP cung cấp và kế hoạch phân bổ cho từng mạng con.

- Dùng địa chỉ **Global Unicast** cho giao tiếp toàn cầu.
- Mỗi mạng LAN nên có một prefix /64.
- Dùng địa chỉ **Link-local** để router giao tiếp trong cùng liên kết.

17.3.3 Sơ đồ mạng

Một sơ đồ mạng trực quan thể hiện các thiết bị, kết nối và phạm vi địa chỉ. Điều này giúp quá trình triển khai và bảo trì dễ dàng hơn.

17.3.4 Cân nhắc về bảo mật

- Sử dụng VLAN để tách biệt lưu lượng trong mạng.
- Cấu hình mật khẩu mạnh và sử dụng SSH thay cho Telnet.
- Đảm bảo cập nhật phần mềm thiết bị thường xuyên.

17.4 Cấu hình thiết bị trong mạng nhỏ

Để một mạng nhỏ hoạt động, cần cấu hình cơ bản cho router, switch và thiết bị đầu cuối.

17.4.1 Cấu hình router

Router cung cấp kết nối giữa mạng LAN và Internet. Các bước cấu hình cơ bản gồm:

- Đặt tên cho thiết bị để dễ nhận diện.
- Cấu hình mật khẩu cho console, VTY và chế độ đặc quyền.
- Cấu hình địa chỉ IP trên các cổng giao diện.
- Thiết lập default route để truy cập Internet.

17.4.2 Cấu hình switch

Switch kết nối các thiết bị trong cùng LAN. Cấu hình cơ bản gồm:

- Đặt tên switch.
- Cấu hình mật khẩu truy cập.
- Cấu hình địa chỉ IP quản lý (SVI).
- Kích hoạt giao diện bằng lệnh `no shutdown`.

17.4.3 Cấu hình thiết bị đầu cuối

Máy tính, laptop, hoặc thiết bị di động cần có địa chỉ IP hợp lệ để tham gia mạng.

- Có thể cấu hình thủ công: nhập địa chỉ IP, subnet mask, default gateway, DNS.
- Hoặc dùng DHCP để tự động nhận cấu hình.

17.4.4 Kết nối không dây

Với mạng nhỏ có Wi-Fi, cần cấu hình Access Point:

- Đặt SSID cho mạng không dây.
- Bật chế độ mã hóa WPA2 hoặc WPA3 để bảo mật.
- Giới hạn hoặc lọc thiết bị dựa trên địa chỉ MAC (nếu cần).

17.5 Kiểm tra và khắc phục sự cố trong mạng nhỏ

Sau khi cấu hình xong, cần xác minh hoạt động của mạng và chuẩn đoán các vấn đề có thể xảy ra.

17.5.1 Các lệnh kiểm tra cơ bản

- `ping`: kiểm tra khả năng kết nối giữa hai thiết bị.
- `tracert` (Windows) hoặc `traceroute` (Linux/Cisco IOS): hiển thị đường đi của gói tin đến đích.
- `ipconfig` (Windows) hoặc `ifconfig` / `ip addr` (Linux): xem cấu hình IP của thiết bị đầu cuối.
- `show ip interface brief`: trên router/switch để kiểm tra trạng thái giao diện.

17.5.2 Các bước khắc phục sự cố

1. **Kiểm tra lớp vật lý**: đảm bảo cáp được cắm đúng, thiết bị bật nguồn.
2. **Kiểm tra cấu hình IP**: xác minh địa chỉ IP, subnet mask, gateway đúng.
3. **Kiểm tra định tuyến**: đảm bảo default gateway được cấu hình chính xác và router có route hợp lệ.
4. **Kiểm tra dịch vụ**: xác minh DHCP, DNS hoạt động nếu được sử dụng.

17.5.3 Công cụ hỗ trợ

Ngoài các lệnh cơ bản, có thể dùng công cụ:

- Packet Tracer hoặc Wireshark để mô phỏng và phân tích gói tin.
- Các phần mềm quản lý mạng để giám sát tình trạng thiết bị.

Câu hỏi ôn tập

1. **Liệt kê các thành phần chính của một mạng nhỏ.**
    - Thiết bị đầu cuối: máy tính, laptop, điện thoại, máy in.
    - Thiết bị trung gian: switch, router, access point.
    - Phương tiện truyền: cáp UTP, cáp quang, sóng vô tuyến.
    - Dịch vụ mạng: DHCP, DNS, email, web, chia sẻ tệp.
2. **Tại sao cần lập kế hoạch địa chỉ IP khi thiết kế mạng?**
    - Giúp sử dụng địa chỉ hiệu quả, tránh trùng lặp.
    - Dễ quản lý và mở rộng mạng.
    - Đảm bảo các thiết bị có cấu hình địa chỉ nhất quán và hợp lệ.
3. **Các bước cấu hình cơ bản cho switch và router trong mạng nhỏ là gì?**
    - Đặt tên thiết bị, cấu hình mật khẩu bảo mật.
    - Cấu hình địa chỉ IP trên router và SVI trên switch.
    - Kích hoạt giao diện bằng lệnh `no shutdown`.

- Thiết lập default route trên router để kết nối Internet.

4. **Những công cụ và lệnh nào có thể dùng để kiểm tra và khắc phục sự cố kết nối?**
   - `ping` để kiểm tra khả năng kết nối.
   - `tracert` hoặc `traceroute` để xem đường đi của gói tin.
   - `ipconfig`, `ifconfig`, `ip addr` để xem cấu hình IP.
   - `show ip interface brief` để kiểm tra trạng thái giao diện trên thiết bị Cisco.
5. **Nêu một biện pháp bảo mật cơ bản có thể áp dụng trong mạng nhỏ.**
   - Cấu hình mật khẩu mạnh và sử dụng SSH thay cho Telnet.
   - Bật mã hóa Wi-Fi bằng WPA2 hoặc WPA3.
   - Sử dụng VLAN để tách biệt lưu lượng.

17.6 Bài tập Chương 17

1. Một mạng nhỏ có 20 PC, 2 máy in và 1 server. Nếu dùng switch 24 cổng, hãy tính số cổng còn trống.

   Đáp án:
   Tổng thiết bị = $20 + 2 + 1 = 23$. Switch 24 cổng $\Rightarrow$ còn trống $24 - 23 = 1$ cổng.

2. Một router SOHO có uplink Internet 100 Mbps. Nếu 10 người dùng chia sẻ đều, mỗi người được trung bình bao nhiêu băng thông?

   Đáp án:
   $100 \Uparrow 10 = 10$ Mbps/người.

3. Một mạng dùng dải `192.168.1.0/27`. Hãy tính số host khả dụng và số subnet có thể chia từ dải này.

   Đáp án:
   /27 $\Rightarrow 2^5 - 2 = 30$ host khả dụng. Nếu từ dải /24 chia thành /27: $2^3 = 8$ subnet.

4. Một mạng có 3 VLAN, mỗi VLAN 50 host. Hãy tính số host tổng cộng và prefix tối thiểu cho mỗi VLAN.

   Đáp án:
   Mỗi VLAN: cần ≥ 50 host $\Rightarrow \Uparrow 26$ (62 host). 3 VLAN $\Rightarrow 3 \times 62 = 186$ host khả dụng.

5. Một access point hỗ trợ 300 Mbps. Nếu có 30 người dùng kết nối, hãy tính tốc độ trung bình mỗi người nhận được (giả sử chia đều).

   Đáp án:
   $300 \Uparrow 30 = 10$ Mbps/người.

6. Một mạng có 2 switch, mỗi switch 24 cổng, nối uplink với nhau. Hãy tính tổng số thiết bị đầu cuối tối đa có thể kết nối.

   Đáp án:
   Mỗi switch mất 1 cổng để uplink. Số cổng cho thiết bị $= 2 \times 24 - 1 = 46$.

7. Một dải `192.168.10.0/24` được chia thành các subnet /29. Hãy tính số subnet tạo được và số host khả dụng mỗi subnet.

   Đáp án:
   Mượn $29 - 24 = 5$ bit. Số subnet $= 2^5 = 32$. Mỗi subnet có $2^3 - 2 = 6$ host khả dụng.

8. Một server có 2 card mạng: NIC1 = 100 Mbps, NIC2 = 1 Gbps. Nếu cấu hình load balancing, hãy tính tổng băng thông server có thể đạt.

   Đáp án:
   100 + 1000 = 1100 Mbps = 1.1 Gbps.

9. Một mạng Wi-Fi có băng thông thực tế 150 Mbps. Nếu truyền video cần trung bình 5 Mbps/thiết bị, hãy tính số thiết bị tối đa có thể xem video cùng lúc.

   Đáp án:
   $150 \div 5 = 30$ thiết bị.

10. Một mạng nhỏ có 60 thiết bị cần cấp DHCP. Nếu mỗi lease DHCP kéo dài 8 giờ, trong 1 ngày DHCP server có thể cấp phát tối đa bao nhiêu lease (giả sử thiết bị ngắt kết nối và cấp phát lại liên tục)?

    Đáp án:
    1 ngày = 24 giờ. Mỗi thiết bị nhận tối đa $24 \div 8 = 3$ lease. Tổng lease = $60 \times 3 = 180$.

17.7 Thuật ngữ cần nhớ

Small Network Mạng quy mô nhỏ (SOHO, văn phòng nhỏ, lớp học) gồm các thiết bị đầu cuối, thiết bị trung gian (switch, router), phương tiện truyền (cáp, Wi-Fi) và dịch vụ cơ bản.

End Device Thiết bị đầu cuối như PC, laptop, smartphone, máy in mạng. Đây là nguồn phát hoặc đích đến của dữ liệu trong mạng.

Intermediary Device Thiết bị trung gian hỗ trợ truyền dữ liệu, ví dụ: switch, router, access point. Chúng định tuyến, chuyển mạch hoặc điều khiển lưu lượng.

IP Addressing Plan Kế hoạch địa chỉ IP cho mạng nhỏ, bao gồm phân bổ subnet, gán địa chỉ tĩnh/động, và xác định default gateway.

Default Gateway Địa chỉ router trong mạng, nơi các host gửi gói khi đích nằm ngoài mạng con cục bộ.

Static IP Address Địa chỉ IP được cấu hình thủ công trên thiết bị, đảm bảo cố định và dễ quản trị cho server hoặc thiết bị hạ tầng.

Dynamic IP Address Địa chỉ IP được cấp phát tự động từ DHCP server hoặc router, thường dùng cho host trong mạng nhỏ.

DHCP (Dynamic Host Configuration Protocol) Giao thức cấp phát tự động địa chỉ IP, subnet mask, default gateway, và DNS cho các host.

DNS (Domain Name System) Dịch vụ phân giải tên miền sang địa chỉ IP, giúp truy cập dịch vụ dễ dàng qua tên thay vì số IP.

Switch Configuration Cấu hình cơ bản cho switch, ví dụ: hostname, mật khẩu, VLAN cho quản lý, địa chỉ IP cho VLAN 1.

Router Configuration Cấu hình cơ bản cho router, bao gồm hostname, mật khẩu, địa chỉ IP cho các cổng, và tuyến mặc định.

Wireless LAN (WLAN) Mạng cục bộ không dây dùng access point hoặc router Wi-Fi để kết nối thiết bị đầu cuối bằng sóng radio.

SSID (Service Set Identifier) Tên mạng không dây để phân biệt WLAN. Người dùng nhập SSID để kết nối Wi-Fi.

WPA2/WPA3 Các chuẩn bảo mật không dây dùng cho Wi-Fi, cung cấp cơ chế mã hóa mạnh (AES) và xác thực nâng cao.

Testing Connectivity Kiểm tra kết nối trong mạng bằng lệnh ping, traceroute, hoặc công cụ kiểm tra trạng thái giao diện.

Ping Lệnh sử dụng ICMP Echo Request/Reply để xác định host đích có khả dụng hay không.

Traceroute Lệnh hiển thị đường đi của gói tin qua các router trung gian từ nguồn đến đích.

Show ip interface brief Lệnh Cisco IOS hiển thị trạng thái giao diện mạng (địa chỉ IP, trạng thái vật lý và trạng thái đường truyền).

Troubleshooting Quá trình chẩn đoán và xử lý sự cố mạng, theo các bước: kiểm tra vật lý, kiểm tra địa chỉ IP, gateway, cấu hình thiết bị, giao thức.

Security Best Practices Các biện pháp bảo mật cơ bản cho mạng nhỏ: đặt mật khẩu mạnh cho thiết bị, dùng SSH thay vì Telnet, bật WPA3 cho Wi-Fi, và tách mạng khách ra khỏi mạng chính.

Phụ lục A

Bài kiểm tra số 1

Câu hỏi

1. Điều gì mô tả một mạng có khả năng phục hồi nhanh chóng sau sự cố và phụ thuộc vào nhiều đường dẫn giữa nguồn và đích?
    - Mạng chịu lỗi (Fault-tolerant network)
    - Mạng có thể mở rộng (Scalable network)
    - Mạng an toàn (Secure network)
    - Mạng chất lượng dịch vụ (QoS network)
2. Thiết bị nào sau đây kết nối các thiết bị đầu cuối riêng lẻ vào mạng và có thể kết nối nhiều mạng riêng lẻ để tạo thành một liên mạng?
    - Thiết bị trung gian (Intermediary device)
    - Thiết bị đầu cuối (End device)
    - Phương tiện mạng (Network media)
    - Thiết bị ngoại vi (Peripheral device)
3. Xu hướng nào cho phép người dùng cuối sử dụng các công cụ cá nhân của họ để truy cập thông tin và giao tiếp qua mạng của doanh nghiệp hoặc trường học?
    - Mang thiết bị của riêng bạn (BYOD)
    - Điện toán đám mây (Cloud computing)
    - Hợp tác trực tuyến (Online collaboration)
    - Mạng qua đường dây điện (Powerline networking)
4. Mạng WAN (Wide-Area Network) có đặc điểm nào sau đây?
    - Kết nối các mạng LAN qua các khu vực địa lý rộng lớn.
    - Thường được quản lý bởi một tổ chức hoặc cá nhân duy nhất.
    - Cung cấp băng thông tốc độ cao cho các thiết bị nội bộ.
    - Chỉ kết nối các thiết bị trong một khu vực giới hạn như tòa nhà văn phòng.
5. Trong các mối đe dọa bảo mật mạng, loại tấn công nào xảy ra vào ngày đầu tiên một lỗ hổng được biết đến?

- Tấn công zero-day (Zero-day attacks)
- Phần mềm gián điệp và quảng cáo (Spyware and adware)
- Tấn công từ chối dịch vụ (Denial-of-service attacks)
- Đánh cắp danh tính (Identity theft)

6. Hai chế độ lệnh nào được phần mềm Cisco IOS sử dụng để phân tách quyền truy cập quản lý?
   - User EXEC mode và Privileged EXEC mode
   - Global configuration mode và Interface configuration mode
   - Console mode và Telnet mode
   - Standard mode và Extended mode
7. Lệnh nào được sử dụng để chuyển từ chế độ User EXEC sang chế độ Privileged EXEC trên một thiết bị Cisco?
   - `enable`
   - `configure terminal`
   - `exit`
   - `show running-config`
8. Tệp cấu hình nào được lưu trữ trong NVRAM và chứa tất cả các lệnh sẽ được thiết bị sử dụng khi khởi động hoặc khởi động lại?
   - startup-config
   - running-config
   - vlan.dat
   - ios-image.bin
9. Phương thức truy cập nào sau đây là một phương thức trong băng tần (in-band) và được khuyến nghị để thiết lập một kết nối CLI an toàn từ xa qua mạng?
   - SSH (Secure Shell)
   - Console
   - Telnet
   - AUX
10. Lệnh nào được sử dụng để mã hóa tất cả các mật khẩu dạng văn bản thuần trong tệp cấu hình của thiết bị Cisco?
    - `service password-encryption`
    - `enable secret`
    - `line console 0`
    - `banner motd`
11. Để quản lý một switch từ xa qua mạng, địa chỉ IP và mặt nạ mạng con phải được cấu hình trên thành phần nào?
    - Giao diện ảo của switch (SVI)

- Cổng vật lý của switch
- Cổng console
- Cổng AUX

12. Mô hình phân lớp có lợi ích gì trong việc mô tả các giao thức và hoạt động của mạng?
    - Hỗ trợ thiết kế giao thức.
    - Thúc đẩy cạnh tranh vì các sản phẩm từ các nhà cung cấp khác nhau có thể hoạt động cùng nhau.
    - Ngăn chặn công nghệ ở một lớp ảnh hưởng đến các lớp khác.
    - Cung cấp một ngôn ngữ chung để mô tả các chức năng và khả năng của mạng.
13. Quá trình một thiết bị nhận đảo ngược quá trình đóng gói và gỡ bỏ các tiêu đề giao thức theo từng lớp được gọi là gì?
    - De-encapsulation (Mở gói)
    - Encapsulation (Đóng gói)
    - Segmentation (Phân đoạn)
    - Encoding (Mã hóa)
14. Tổ chức nào chịu trách nhiệm phát triển, cập nhật và duy trì các công nghệ Internet và TCP/IP, bao gồm cả việc phát hành các tài liệu Request for Comments (RFC)?
    - IETF (Internet Engineering Task Force)
    - IEEE (Institute of Electrical and Electronics Engineers)
    - ISO (International Organization for Standardization)
    - ICANN (Internet Corporation for Assigned Names and Numbers)
15. Ở lớp mạng (Network layer), PDU (Protocol Data Unit) được gọi là gì?
    - Packet (Gói tin)
    - Frame (Khung tin)
    - Segment (Phân đoạn)
    - Bits (Bit)
16. Địa chỉ nào chịu trách nhiệm gửi một khung liên kết dữ liệu (data link frame) từ một card mạng (NIC) đến một NIC khác trên cùng một mạng?
    - Địa chỉ lớp liên kết dữ liệu (Data link layer address)
    - Địa chỉ lớp mạng (Network layer address)
    - Địa chỉ cổng (Port address)
    - Địa chỉ đường phố (Street address)
17. Tùy chọn phân phối tin nhắn nào được sử dụng khi thông tin được truyền đến một thiết bị đầu cuối duy nhất?
    - Unicast
    - Multicast
    - Broadcast
    - Anycast

18. Các giao thức lớp vật lý mô tả những phương tiện nào để kích hoạt, duy trì và hủy kích hoạt các kết nối vật lý để truyền bit?

    - Cơ khí
    - Điện
    - Chức năng
    - Thủ tục

19. Ba loại phương tiện mạng chính được sử dụng trong các mạng hiện đại là gì?

    - Dây kim loại trong cáp (cáp đồng)
    - Sợi thủy tinh hoặc nhựa trong cáp (cáp quang)
    - Truyền dẫn không dây
    - Sóng âm thanh

20. Thuật ngữ nào mô tả thước đo lượng dữ liệu có thể sử dụng được truyền qua một khoảng thời gian nhất định (thông lượng trừ đi lưu lượng tiêu đề)?

    - Goodput
    - Throughput (Thông lượng)
    - Bandwidth (Băng thông)
    - Latency (Độ trễ)

21. Kỹ thuật nào được sử dụng trong cáp đồng đôi xoắn (twisted-pair) để chống lại nhiễu điện từ (EMI) và nhiễu tần số vô tuyến (RFI)?

    - Bọc trong lớp che chắn kim loại (shielding)
    - Xoắn các cặp dây đối diện với nhau
    - Sử dụng đầu nối được nối đất đúng cách
    - Sử dụng cáp đồng trục

22. Loại cáp quang nào có lõi rất nhỏ và sử dụng công nghệ laser đắt tiền để gửi một tia sáng duy nhất, phù hợp cho các ứng dụng đường dài?

    - Sợi đơn mode (Single-mode fiber - SMF)
    - Sợi đa mode (Multimode fiber - MMF)
    - Cáp đồng trục (Coaxial cable)
    - Cáp đôi xoắn không bọc giáp (UTP)

23. Trong các chuẩn không dây, chuẩn nào là một công nghệ Mạng cục bộ không dây (WLAN) sử dụng giao thức dựa trên tranh chấp được gọi là CSMA/CA?

    - Wi-Fi (IEEE 802.11)
    - Bluetooth (IEEE 802.15)
    - WiMAX (IEEE 802.16)
    - Zigbee (IEEE 802.15.4)

24. Chuẩn cáp UTP nào được khuyến nghị cho các công trình lắp đặt tòa nhà mới để hỗ trợ tốc độ Gigabit Ethernet?

- Category 6
- Category 3
- Category 5
- Coaxial

25. Địa chỉ IPv4 bao gồm bao nhiêu bit?
    - 32 bit
    - 64 bit
    - 128 bit
    - 16 bit
26. Hệ thống số nào sử dụng các chữ số từ 0 đến 9 và các chữ cái từ A đến F?
    - Hệ thập lục phân (Hexadecimal)
    - Hệ nhị phân (Binary)
    - Hệ thập phân (Decimal)
    - Hệ bát phân (Octal)
27. Trong địa chỉ IPv4 192.168.10.10, mỗi phần được phân cách bởi dấu chấm được gọi là gì?
    - Octet
    - Hextet
    - Bit
    - Byte
28. Địa chỉ IPv6 dài 128 bit, và mỗi 4 bit được biểu diễn bằng một ký tự thập lục phân. Thuật ngữ không chính thức nào được sử dụng để chỉ một đoạn 16 bit hoặc 4 ký tự thập lục phân trong địa chỉ IPv6?
    - Hextet
    - Octet
    - Quartet
    - Segment
29. Giá trị thập phân tương đương với số nhị phân 11010101 là gì?
    - 213
    - 187
    - 229
    - 205
30. Giá trị thập lục phân tương đương với số thập phân 210 là gì?
    - D2
    - C8
    - E6
    - B4

31. Lớp nào trong mô hình OSI chịu trách nhiệm giao tiếp giữa card mạng (NIC) này với card mạng khác?
    - Lớp liên kết dữ liệu (Data Link Layer)
    - Lớp vật lý (Physical Layer)
    - Lớp mạng (Network Layer)
    - Lớp vận chuyển (Transport Layer)
32. Hai lớp con của lớp liên kết dữ liệu theo chuẩn IEEE 802 LAN/MAN là gì?
    - Logical Link Control (LLC)
    - Media Access Control (MAC)
    - Network Control Protocol (NCP)
    - Physical Layer Control (PLC)
33. Kiểu topology mạng WAN nào bao gồm một liên kết cố định giữa hai điểm cuối?
    - Point-to-Point (Điểm-nối-Điểm)
    - Hub and Spoke (Trục và Nan hoa)
    - Mesh (Lưới)
    - Ring (Vòng)
34. Trong truyền thông dữ liệu, chế độ nào cho phép cả hai thiết bị có thể truyền và nhận đồng thời trên phương tiện chia sẻ?
    - Full-duplex (Song công toàn phần)
    - Half-duplex (Bán song công)
    - Simplex (Đơn công)
    - Multiplex (Ghép kênh)
35. Phương pháp kiểm soát truy cập nào được các mạng WLAN IEEE 802.11 sử dụng để cố gắng tránh xung đột bằng cách đợi trước khi truyền?
    - CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)
    - CSMA/CD (Carrier Sense Multiple Access/Collision Detection)
    - Token Passing
    - Polling
36. Ba phần cơ bản của một khung (frame) ở lớp liên kết dữ liệu là gì?
    - Header (Phần đầu)
    - Data (Dữ liệu)
    - Trailer (Phần cuối)
    - Preamble (Lời tựa)
    - Checksum (Tổng kiểm)
37. Trường nào trong khung Ethernet được sử dụng để phát hiện lỗi trong một khung bằng cách sử dụng kiểm tra dư thừa chu kỳ (CRC)?

- Frame Check Sequence (FCS)
- Preamble
- Source MAC Address
- Type/Length

38. Một địa chỉ MAC Ethernet bao gồm bao nhiêu bit?
    - 48 bit
    - 32 bit
    - 64 bit
    - 128 bit
39. 24 bit đầu tiên của một địa chỉ MAC được gọi là gì và do tổ chức nào cấp phát cho nhà sản xuất?
    - Organizationally Unique Identifier (OUI) do IEEE cấp.
    - Vendor Assigned ID (VAI) do ISO cấp.
    - Network Interface Code (NIC) do IETF cấp.
    - Physical Address Block (PAB) do IANA cấp.
40. Một switch Lớp 2 xây dựng bảng địa chỉ MAC của nó bằng cách nào?
    - Bằng cách kiểm tra địa chỉ MAC nguồn của các khung nhận được trên một cổng.
    - Bằng cách kiểm tra địa chỉ MAC đích của các khung nhận được.
    - Bằng cách gửi yêu cầu ARP đến tất cả các thiết bị.
    - Bằng cách được cấu hình thủ công bởi quản trị viên mạng.
41. Phương pháp chuyển tiếp khung nào của switch sẽ nhận toàn bộ khung và tính toán CRC trước khi chuyển tiếp?
    - Store-and-forward switching
    - Cut-through switching
    - Fragment-free switching
    - Fast-forward switching
42. Tự động MDIX (auto-MDIX) là một tính năng cho phép một thiết bị chuyển mạch thực hiện điều gì?
    - Tự động phát hiện loại cáp (thẳng hoặc chéo) được gắn vào cổng và cấu hình giao diện tương ứng.
    - Tự động thương lượng tốc độ và chế độ song công tốt nhất.
    - Tự động phát hiện và ngăn chặn các vòng lặp chuyển mạch.
    - Tự động gán địa chỉ IP cho các thiết bị được kết nối.
43. Địa chỉ MAC đích nào được sử dụng cho một khung quảng bá (broadcast) Ethernet?
    - FF-FF-FF-FF-FF-FF
    - 00-00-00-00-00-00
    - Địa chỉ MAC của cổng gateway mặc định
    - Một địa chỉ bắt đầu bằng 01-00-5E

44. Lớp mạng (Network Layer) thực hiện bốn hoạt động cơ bản nào?
    - Địa chỉ hóa các thiết bị cuối (Addressing)
    - Đóng gói (Encapsulation)
    - Định tuyến (Routing)
    - Mở gói (De-encapsulation)
    - Kiểm soát luồng (Flow Control)
45. Ba đặc điểm chính của Giao thức Internet (IP) là gì?
    - Connectionless (Không liên kết)
    - Best effort (Nỗ lực tối đa/Không đảm bảo)
    - Media independent (Độc lập với phương tiện)
    - Reliable (Đáng tin cậy)
    - Secure (An toàn)
46. Trường nào trong tiêu đề gói tin IPv4 được sử dụng để giới hạn vòng đời của một gói tin và giảm đi một mỗi khi gói tin được xử lý bởi một router?
    - Time-to-Live (TTL)
    - Header Checksum
    - Protocol
    - Version
47. Một trong những cải tiến chính của IPv6 so với IPv4 là gì?
    - Không gian địa chỉ lớn hơn nhiều (128 bit so với 32 bit).
    - Tiêu đề gói tin được đơn giản hóa để xử lý hiệu quả hơn.
    - Loại bỏ nhu cầu về NAT.
    - Tích hợp bảo mật (IPsec) là bắt buộc.
48. Trong tiêu đề gói tin IPv6, trường nào tương đương với trường Time-to-Live (TTL) của IPv4?
    - Hop Limit
    - Traffic Class
    - Flow Label
    - Next Header
49. Một thiết bị chủ xác định phải gửi một gói tin đến cổng mặc định (default gateway) khi nào?
    - Khi máy chủ đích nằm trên một mạng từ xa.
    - Khi máy chủ đích nằm trên cùng một mạng cục bộ.
    - Luôn luôn, đối với tất cả các gói tin gửi đi.
    - Khi không thể tìm thấy địa chỉ MAC của máy chủ đích.
50. Ba loại mục nhập tuyến đường nào được lưu trữ trong bảng định tuyến của một router?
    - Mạng được kết nối trực tiếp (Directly connected networks)

- Mạng từ xa (Remote networks)
- Tuyến đường mặc định (Default route)
- Tuyến đường tĩnh (Static route)
- Tuyến đường động (Dynamic route)

Hướng dẫn trả lời

1. **Đáp án đúng:** Mạng chịu lỗi (Fault-tolerant network)
   Giải thích: Mạng chịu lỗi được xây dựng để hạn chế số lượng thiết bị bị ảnh hưởng bởi một sự cố. Nó cho phép phục hồi nhanh chóng khi xảy ra lỗi bằng cách sử dụng các đường dẫn dự phòng hoặc nhiều đường dẫn giữa nguồn và đích.

2. **Đáp án đúng:** Thiết bị trung gian (Intermediary device)
   Giải thích: Các thiết bị trung gian như switch và router kết nối các thiết bị đầu cuối với mạng. Chúng cung cấp khả năng kết nối và đảm bảo rằng dữ liệu di chuyển qua mạng đến đúng đích.

3. **Đáp án đúng:** Mang thiết bị của riêng bạn (BYOD)
   Giải thích: BYOD là một xu hướng toàn cầu, cho phép người dùng cuối tự do sử dụng các thiết bị cá nhân như laptop, máy tính bảng, điện thoại thông minh để truy cập tài nguyên mạng của tổ chức.

4. **Đáp án đúng:** Kết nối các mạng LAN qua các khu vực địa lý rộng lớn.
   Giải thích: Mạng diện rộng (WAN) là một cơ sở hạ tầng mạng cung cấp quyền truy cập vào các mạng khác trên một khu vực địa lý rộng, chẳng hạn như giữa các thành phố, tiểu bang hoặc quốc gia.

5. **Đáp án đúng:** Tấn công zero-day (Zero-day attacks)
   Giải thích: Tấn công zero-day, còn gọi là tấn công zero-hour, là các cuộc tấn công xảy ra vào chính ngày đầu tiên một lỗ hổng bảo mật được phát hiện hoặc công bố, trước khi có bản vá lỗi.

6. **Đáp án đúng:** User EXEC mode và Privileged EXEC mode
   Giải thích: Phần mềm Cisco IOS phân tách quyền truy cập quản lý thành hai chế độ: User EXEC mode (chế độ người dùng, có giới hạn) và Privileged EXEC mode (chế độ đặc quyền, cho phép truy cập tất cả các lệnh).

7. **Đáp án đúng:** `enable`
   Giải thích: Lệnh `enable` được sử dụng để nâng cấp quyền từ chế độ User EXEC (được biểu thị bằng dấu >) lên chế độ Privileged EXEC (được biểu thị bằng dấu #).

8. **Đáp án đúng:** startup-config
   Giải thích: Tệp startup-config là tệp cấu hình đã lưu được lưu trữ trong bộ nhớ truy cập ngẫu nhiên không khả biến (NVRAM). Nó không bị mất nội dung khi thiết bị tắt nguồn.

9. **Đáp án đúng:** SSH (Secure Shell)
   Giải thích: SSH là một phương thức trong băng tần (yêu cầu các dịch vụ mạng đang hoạt động) để thiết lập một kết nối CLI an toàn, được mã hóa từ xa. Console là ngoài băng tần (out-of-band), còn Telnet không an toàn.

10. **Đáp án đúng:** `service password-encryption`
    Giải thích: Lệnh cấu hình toàn cục `service password-encryption` áp dụng một thuật toán mã hóa yếu cho tất cả các mật khẩu chưa được mã hóa trong tệp cấu hình, ngăn chặn việc xem mật khẩu dưới dạng văn bản thuần.

11. **Đáp án đúng:** Giao diện ảo của switch (SVI)
    Giải thích: Vì các cổng vật lý của switch Lớp 2 không hỗ trợ địa chỉ IP, một SVI phải được tạo trong phần mềm. Giao diện ảo này cho phép quản lý switch từ xa qua mạng bằng IPv4 và IPv6.

12. **Đáp án đúng:** Hỗ trợ thiết kế giao thức., Thúc đẩy cạnh tranh vì các sản phẩm từ các nhà cung cấp khác nhau có thể hoạt động cùng nhau., Ngăn chặn công nghệ ở một lớp ảnh hưởng đến các lớp khác., Cung cấp một ngôn ngữ chung để mô tả các chức năng và khả năng của mạng.

Giải thích: Mô hình phân lớp giúp chia nhỏ các hoạt động phức tạp của mạng thành các lớp dễ quản lý. Điều này hỗ trợ thiết kế giao thức, cho phép các nhà cung cấp khác nhau tạo ra các sản phẩm tương thích, cô lập các thay đổi trong một lớp, và tạo ra một khuôn khổ chung để thảo luận.

13. **Đáp án đúng:** De-encapsulation (Mở gói)
Giải thích: De-encapsulation là quá trình được thiết bị nhận sử dụng để loại bỏ một hoặc nhiều tiêu đề giao thức. Dữ liệu được mở gói khi nó di chuyển lên chồng giao thức hướng tới ứng dụng người dùng cuối.

14. **Đáp án đúng:** IETF (Internet Engineering Task Force)
Giải thích: IETF là tổ chức phát triển, cập nhật và duy trì các công nghệ Internet và TCP/IP. Các tài liệu của họ, được gọi là RFC, định nghĩa các giao thức này.

15. **Đáp án đúng:** Packet (Gói tin)
Giải thích: Tại lớp mạng, đơn vị dữ liệu giao thức (PDU) được gọi là một gói tin (packet). Lớp mạng nhận một phân đoạn (segment) từ lớp vận chuyển và đóng gói nó vào một gói tin.

16. **Đáp án đúng:** Địa chỉ lớp liên kết dữ liệu (Data link layer address)
Giải thích: Địa chỉ lớp liên kết dữ liệu (ví dụ: địa chỉ MAC) chịu trách nhiệm phân phối khung dữ liệu từ một NIC đến một NIC khác trên cùng một mạng cục bộ.

17. **Đáp án đúng:** Unicast
Giải thích: Truyền thông unicast là quá trình truyền thông tin đến một thiết bị đầu cuối duy nhất.

18. **Đáp án đúng:** Cơ khí, Điện, Chức năng, Thủ tục
Giải thích: Các giao thức lớp vật lý mô tả các phương tiện cơ khí (đầu nối), điện (mức điện áp), chức năng (chức năng của các chân cắm) và thủ tục (trình tự các sự kiện) để truyền bit qua một kết nối vật lý.

19. **Đáp án đúng:** Dây kim loại trong cáp (cáp đồng), Sợi thủy tinh hoặc nhựa trong cáp (cáp quang), Truyền dẫn không dây
Giải thích: Các mạng hiện đại chủ yếu sử dụng ba loại phương tiện này để kết nối các thiết bị. Dữ liệu được mã hóa thành các xung điện đối với cáp đồng, xung ánh sáng đối với cáp quang và sóng điện từ đối với không dây.

20. **Đáp án đúng:** Goodput
Giải thích: Goodput là thước đo dữ liệu hữu ích thực tế được truyền đi, không bao gồm các tiêu đề giao thức, thông báo xác nhận và các bit truyền lại. Do đó, goodput luôn thấp hơn thông lượng (throughput).

21. **Đáp án đúng:** Bọc trong lớp che chắn kim loại (shielding), Xoắn các cặp dây đối diện với nhau
Giải thích: Cáp đồng sử dụng lớp che chắn kim loại (như trong cáp STP) để chống lại EMI và RFI. Việc xoắn các cặp dây lại với nhau (như trong UTP và STP) giúp loại bỏ nhiễu xuyên âm (crosstalk).

22. **Đáp án đúng:** Sợi đơn mode (Single-mode fiber - SMF)
Giải thích: SMF có lõi rất nhỏ, cho phép một tia sáng duy nhất truyền qua. Điều này làm giảm sự phân tán và cho phép tín hiệu đi xa hơn nhiều so với MMF, làm cho nó trở nên lý tưởng cho các ứng dụng đường dài.

23. **Đáp án đúng:** Wi-Fi (IEEE 802.11)
Giải thích: Wi-Fi là một công nghệ WLAN sử dụng CSMA/CA. Theo phương pháp này, NIC không dây phải lắng nghe để xác định xem kênh vô tuyến có trống không trước khi truyền để tránh xung đột.

24. **Đáp án đúng:** Category 6
Giải thích: Đối với các công trình xây dựng mới, Category 6 (Cat 6) là loại cáp được khuyến nghị vì nó được thiết kế để hỗ trợ tốc độ dữ liệu cao hơn, chẳng hạn như Gigabit Ethernet (1000 Mbps) và 10 Gigabit Ethernet trên khoảng cách ngắn hơn.

25. **Đáp án đúng:** 32 bit
Giải thích: Một địa chỉ IPv4 bao gồm một chuỗi 32 bit, được chia thành bốn phần 8-bit gọi là các octet.

26. **Đáp án đúng:** Hệ thập lục phân (Hexadecimal)
Giải thích: Hệ thập lục phân (cơ số 16) sử dụng 16 ký hiệu: các chữ số từ 0 đến 9 và sáu chữ cái từ A đến F để biểu diễn các giá trị.

27. **Đáp án đúng:** Octet
Giải thích: Mỗi địa chỉ IPv4 32 bit được chia thành bốn phần, mỗi phần chứa 8 bit. Một nhóm 8 bit được gọi là một octet.

28. **Đáp án đúng:** Hextet
Giải thích: Hextet là thuật ngữ không chính thức được sử dụng để chỉ một đoạn 16 bit (hoặc 4 ký tự thập lục phân) trong một địa chỉ IPv6. Một địa chỉ IPv6 đầy đủ bao gồm 8 hextet.

29. **Đáp án đúng:** 213
Giải thích: $11010101 = 1*128+1*64+0*32+1*16+0*8+1*4+0*2+1*1 = 128+64+16+4+1 = 213$.

30. **Đáp án đúng:** D2
Giải thích: Để chuyển đổi, trước tiên hãy chuyển 210 sang nhị phân: 11010010. Sau đó chia thành hai nhóm 4 bit: 1101 và 0010. 1101 trong hệ thập lục phân là D, và 0010 là 2. Do đó, kết quả là D2.

31. **Đáp án đúng:** Lớp liên kết dữ liệu (Data Link Layer)
Giải thích: Lớp liên kết dữ liệu chịu trách nhiệm truyền thông từ card mạng này đến card mạng khác trên cùng một mạng vật lý. Nó chuẩn bị dữ liệu mạng cho mạng vật lý.

32. **Đáp án đúng:** Logical Link Control (LLC), Media Access Control (MAC)
Giải thích: Lớp liên kết dữ liệu theo chuẩn IEEE 802 được chia thành hai lớp con: LLC, giao tiếp với các lớp trên, và MAC, chịu trách nhiệm đóng gói dữ liệu và kiểm soát truy cập phương tiện.

33. **Đáp án đúng:** Point-to-Point (Điểm-nối-Điểm)
Giải thích: Topology điểm-nối-điểm là dạng đơn giản nhất, bao gồm một liên kết duy nhất, cố định kết nối trực tiếp hai điểm cuối (nút).

34. **Đáp án đúng:** Full-duplex (Song công toàn phần)
Giải thích: Trong giao tiếp song công toàn phần, cả hai thiết bị có thể truyền và nhận dữ liệu đồng thời, cho phép luồng dữ liệu hai chiều cùng một lúc.

35. **Đáp án đúng:** CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)
Giải thích: Mạng không dây sử dụng CSMA/CA. Phương pháp này không phát hiện xung đột mà cố gắng tránh chúng bằng cách lắng nghe phương tiện trước khi truyền và sử dụng các cơ chế như bộ đếm thời gian ngẫu nhiên.

36. **Đáp án đúng:** Header (Phần đầu), Data (Dữ liệu), Trailer (Phần cuối)
Giải thích: Một khung ở lớp liên kết dữ liệu bao gồm một phần đầu (header) chứa thông tin điều khiển như địa chỉ, một phần dữ liệu (data) chứa gói tin từ lớp trên, và một phần cuối (trailer) chứa thông tin phát hiện lỗi.

37. **Đáp án đúng:** Frame Check Sequence (FCS)
Giải thích: Trường FCS nằm trong phần cuối (trailer) của khung Ethernet và chứa một giá trị kiểm tra dư thừa chu kỳ (CRC). Thiết bị nhận sẽ tính toán lại CRC và so sánh nó với giá trị trong FCS để kiểm tra xem khung có bị lỗi trong quá trình truyền hay không.

38. **Đáp án đúng:** 48 bit
Giải thích: Địa chỉ MAC (Media Access Control) là một địa chỉ 48-bit duy nhất được gán cho mỗi card giao diện mạng (NIC).

39. **Đáp án đúng:** Organizationally Unique Identifier (OUI) do IEEE cấp.
Giải thích: IEEE (Institute of Electrical and Electronics Engineers) cấp phát một OUI 24-bit (3-byte) duy nhất cho mỗi nhà sản xuất. OUI này tạo thành 24 bit đầu tiên của bất kỳ địa chỉ MAC nào do nhà sản xuất đó gán.

40. **Đáp án đúng:** Bằng cách kiểm tra địa chỉ MAC nguồn của các khung nhận được trên một cổng.
Giải thích: Khi một khung tin đến một cổng switch, switch sẽ đọc địa chỉ MAC nguồn của khung đó. Nếu địa chỉ này chưa có trong bảng MAC, switch sẽ thêm một mục mới, liên kết địa chỉ MAC đó với cổng mà khung tin đã đến.

41. **Đáp án đúng:** Store-and-forward switching
Giải thích: Chuyển mạch lưu-và-chuyển tiếp (store-and-forward) đợi cho đến khi toàn bộ khung được nhận vào bộ đệm của nó. Sau đó, nó thực hiện kiểm tra lỗi (CRC). Nếu khung không có lỗi, nó sẽ được chuyển tiếp đến cổng đích.

42. **Đáp án đúng:** Tự động phát hiện loại cáp (thẳng hoặc chéo) được gắn vào cổng và cấu hình giao diện tương ứng.
Giải thích: Auto-MDIX (automatic medium-dependent interface crossover) cho phép một cổng switch tự động cảm nhận kết nối dây cần thiết (thẳng hoặc chéo) và cấu hình lại chính nó cho phù hợp, loại bỏ nhu cầu sử dụng các loại cáp khác nhau cho các kết nối khác nhau.

43. **Đáp án đúng:** FF-FF-FF-FF-FF-FF
Giải thích: Địa chỉ MAC quảng bá là một địa chỉ đặc biệt bao gồm 48 bit đều là 1. Trong hệ thập lục phân, điều này được biểu diễn là FF-FF-FF-FF-FF-FF. Mọi thiết bị trên mạng LAN sẽ nhận và xử lý một khung có địa chỉ đích này.

44. **Đáp án đúng:** Địa chỉ hóa các thiết bị cuối (Addressing), Đóng gói (Encapsulation), Định tuyến (Routing), Mở gói (De-encapsulation)
Giải thích: Bốn hoạt động cơ bản của Lớp Mạng là: gán địa chỉ IP duy nhất cho các thiết bị cuối, đóng gói PDU của Lớp Vận chuyển vào các gói tin, chọn đường đi tốt nhất để chuyển tiếp các gói tin đến mạng đích, và mở gói tin khi nó đến thiết bị cuối đích.

45. **Đáp án đúng:** Connectionless (Không liên kết), Best effort (Nỗ lực tối đa/Không đảm bảo), Media independent (Độc lập với phương tiện)
Giải thích: Giao thức IP là "không liên kết"vì không có kết nối nào được thiết lập trước khi gửi dữ liệu. Nó là "nỗ lực tối đa"vì không đảm bảo việc phân phối gói tin. Và nó "độc lập với phương tiện"vì nó có thể hoạt động trên bất kỳ loại phương tiện lớp vật lý nào.

46. **Đáp án đúng:** Time-to-Live (TTL)
Giải thích: Trường TTL là một bộ đếm được đặt bởi nguồn và giảm đi một bởi mỗi router trên đường đi. Khi TTL về 0, router sẽ loại bỏ gói tin để ngăn nó lặp vô hạn trong mạng.

47. **Đáp án đúng:** Không gian địa chỉ lớn hơn nhiều (128 bit so với 32 bit)., Tiêu đề gói tin được đơn giản hóa để xử lý hiệu quả hơn., Loại bỏ nhu cầu về NAT.
Giải thích: IPv6 được tạo ra để giải quyết các hạn chế của IPv4, đặc biệt là sự cạn kiệt địa chỉ. Nó cung cấp một không gian địa chỉ khổng lồ, một tiêu đề hợp lý hơn để giảm tải xử lý của router, và loại bỏ nhu cầu về NAT, cho phép kết nối đầu cuối thực sự.

48. **Đáp án đúng:** Hop Limit
    Giải thích: Trong IPv6, trường Hop Limit 8-bit thực hiện cùng chức năng với trường TTL trong IPv4. Nó được giảm đi một ở mỗi hop (router), và gói tin sẽ bị loại bỏ khi giá trị này bằng không.

49. **Đáp án đúng:** Khi máy chủ đích nằm trên một mạng từ xa.
    Giải thích: Một thiết bị chủ sử dụng cổng mặc định của nó để gửi các gói tin có địa chỉ IP đích không nằm trong cùng mạng cục bộ (mạng từ xa). Cổng mặc định hoạt động như một cửa ngõ ra khỏi mạng cục bộ.

50. **Đáp án đúng:** Mạng được kết nối trực tiếp (Directly connected networks), Mạng từ xa (Remote networks), Tuyến đường mặc định (Default route)
    Giải thích: Một bảng định tuyến chứa thông tin về các mạng mà router được kết nối trực tiếp, các mạng từ xa mà nó đã học được (thông qua định tuyến tĩnh hoặc động), và thường là một tuyến đường mặc định để xử lý lưu lượng đến các mạng không xác định.

Phụ lục B

Bài kiểm tra số 2

Câu hỏi

1. Khi một máy chủ gửi một gói tin đến một máy chủ khác trên một mạng từ xa, địa chỉ MAC đích trong khung Ethernet là gì?

   a) Địa chỉ MAC của cổng gateway mặc định.
   b) Địa chỉ MAC của máy chủ đích.
   c) Địa chỉ IP của máy chủ đích.
   d) Địa chỉ MAC của switch.

2. Trong mạng IPv6, giao thức nào thực hiện chức năng tương tự như ARP trong IPv4 để phân giải địa chỉ lớp 3 thành địa chỉ lớp 2?

   a) Neighbor Discovery (ND)
   b) ARPv6
   c) DHCPv6
   d) ICMPv6

3. Một yêu cầu ARP (ARP request) được gửi dưới dạng nào?

   a) Broadcast ở Lớp 2
   b) Unicast ở Lớp 2
   c) Multicast ở Lớp 3
   d) Broadcast ở Lớp 3

4. Bảng ARP (ARP table) trên một thiết bị lưu trữ ánh xạ giữa các thông tin nào?

   a) Địa chỉ IPv4 và địa chỉ MAC
   b) Địa chỉ IP và số cổng
   c) Tên miền và địa chỉ IP
   d) Địa chỉ MAC và cổng switch

5. Kỹ thuật tấn công nào mà kẻ tấn công gửi các thông điệp ARP giả mạo vào mạng cục bộ?

   a) ARP spoofing (Giả mạo ARP)
   b) DNS spoofing
   c) MAC flooding
   d) IP spoofing

6. Hai thông điệp ICMPv6 nào được sử dụng để phân giải địa chỉ MAC trong mạng IPv6? (Chọn hai)

   a) Neighbor Solicitation
   b) Neighbor Advertisement
   c) Router Solicitation
   d) Router Advertisement
   e) Echo Request

7. Lệnh nào được sử dụng để mã hóa tất cả các mật khẩu dạng văn bản thuần (plaintext) trong tệp cấu hình của router?

a) service password-encryption
b) enable secret
c) encrypt all passwords
d) line console 0

8. Đặc điểm nào mô tả về gateway mặc định của một máy tính chủ?

a) Địa chỉ logic của giao diện router trên cùng mạng với máy tính chủ.
b) Địa chỉ vật lý của giao diện switch kết nối với máy tính chủ.
c) Địa chỉ logic được gán cho giao diện switch.
d) Địa chỉ vật lý của máy chủ DNS.

9. Lệnh nào hiển thị một bản tóm tắt ngắn gọn về trạng thái hiện tại của các giao diện, địa chỉ IP và trạng thái hoạt động của chúng trên router?

a) show ip interface brief
b) show running-config
c) show interfaces
d) show ip route

10. Tệp cấu hình nào được lưu trong NVRAM của router và được sử dụng khi router khởi động?

a) startup-config
b) running-config
c) IOS image
d) POST diagnostics

11. Mục đích của lệnh ‘banner motd‘ trên router là gì?

a) Cung cấp thông báo pháp lý hoặc cảnh báo cho bất kỳ ai đăng nhập vào router.
b) Cấu hình tên của router.
c) Mã hóa các mật khẩu.
d) Cấu hình giao diện loopback.

12. Để cho phép một switch Lớp 2 được quản lý từ xa từ một mạng khác, cần cấu hình thông tin nào sau đây?

a) Một địa chỉ IP gateway mặc định.
b) Một địa chỉ MAC.
c) Một VLAN trunking.
d) Một địa chỉ loopback.

13. Quá trình nào được sử dụng để xác định địa chỉ mạng từ một địa chỉ IPv4 và subnet mask của nó?

a) Phép toán AND logic
b) Phép toán OR logic
c) Phép toán XOR logic
d) Phép toán NOT logic

14. Địa chỉ IPv4 nào sau đây là một địa chỉ riêng (private address)?

a) 172.16.31.50
b) 172.32.5.2
c) 192.169.1.1
d) 100.64.10.10

15. Loại truyền thông nào gửi một gói tin đến tất cả các thiết bị trên một miền broadcast cụ thể?

a) Broadcast
b) Unicast
c) Multicast
d) Anycast

16. Một mạng có prefix là /27. Có bao nhiêu địa chỉ host hợp lệ trong mạng này?

a) 30
b) 32
c) 62
d) 14

17. Kỹ thuật nào cho phép chia một mạng thành các mạng con có kích thước khác nhau để tiết kiệm địa chỉ IP?

    a) Variable-Length Subnet Masking (VLSM)
    b) Classful Addressing
    c) Network Address Translation (NAT)
    d) Port Address Translation (PAT)

18. Trong địa chỉ IPv4 192.168.10.10/24, phần nào là địa chỉ mạng và phần nào là địa chỉ host?

    a) 192.168.10 là phần mạng, 10 là phần host.
    b) 192.168 là phần mạng, 10.10 là phần host.
    c) 192 là phần mạng, 168.10.10 là phần host.
    d) 192.168.10.0 là phần mạng, 0.0.0.10 là phần host.

19. Lợi ích chính của việc chia mạng (subnetting) là gì?

    a) Giảm kích thước của miền broadcast.
    b) Tăng tốc độ kết nối Internet.
    c) Tăng số lượng địa chỉ host trong một mạng.
    d) Đơn giản hóa việc gán địa chỉ IP.

20. Đâu là cách viết tắt hợp lệ cho địa chỉ IPv6 fe80:0000:0000:0000:02a0:c9ff:fe76:2434?

    a) fe80::2a0:c9ff:fe76:2434
    b) fe80:0:0:0:2a0:c9ff:fe76:2434
    c) fe80::02a0:c9ff:fe76:2434
    d) fe80:2a0:c9ff:fe76:2434

21. Loại địa chỉ IPv6 nào được yêu cầu cho mọi giao diện có bật IPv6 và chỉ được sử dụng để giao tiếp trên cùng một liên kết cục bộ?

    a) Link-local address (LLA)
    b) Global unicast address (GUA)
    c) Unique local address
    d) Anycast address

22. Một địa chỉ Global Unicast (GUA) của IPv6 bao gồm ba phần nào? (Chọn ba)

    a) Global Routing Prefix
    b) Subnet ID
    c) Interface ID
    d) Broadcast ID
    e) MAC Address

23. Phương pháp nào cho phép một thiết bị tự động cấu hình địa chỉ IPv6 GUA của mình bằng cách sử dụng thông tin từ thông điệp Router Advertisement (RA)?

    a) Stateless Address Autoconfiguration (SLAAC)
    b) Stateful DHCPv6
    c) Static configuration
    d) APIPA

24. Quá trình EUI-64 sử dụng địa chỉ nào của thiết bị để tạo ra Interface ID 64-bit cho địa chỉ IPv6?

    a) Địa chỉ MAC 48-bit
    b) Địa chỉ IPv4 32-bit
    c) Một số ngẫu nhiên 64-bit
    d) Địa chỉ Loopback

25. Địa chỉ IPv6 nào được sử dụng để gửi một gói tin đến tất cả các router IPv6 trên một liên kết cục bộ?

    a) ff02::2
    b) ff02::1
    c) fe80::1
    d) ::1

26. Lệnh ‘ping ::1‘ trên một máy chủ IPv6 có mục đích gì?

a) Kiểm tra xem chồng giao thức TCP/IP có được cài đặt và hoạt động chính xác trên máy chủ đó hay không.
b) Kiểm tra kết nối đến gateway mặc định.
c) Kiểm tra kết nối đến máy chủ DNS.
d) Gửi yêu cầu đến tất cả các máy chủ trên mạng.

27. Tiện ích ‘traceroute‘ (hoặc ‘tracert‘) sử dụng thông điệp ICMP nào để xác định đường đi đến một đích?

a) Time Exceeded
b) Echo Request
c) Destination Unreachable
d) Echo Reply

28. Khi bạn ping một địa chỉ không tồn tại trên mạng cục bộ, loại thông điệp ICMP nào bạn có thể nhận lại từ gateway?

a) Destination Unreachable
b) Time Exceeded
c) Echo Reply
d) Redirect

29. Giao thức ICMPv6 bao gồm các chức năng mới không có trong ICMPv4, như là một phần của Neighbor Discovery Protocol. Các chức năng này bao gồm:

a) Phân giải địa chỉ và tự động cấu hình địa chỉ.
b) Báo cáo lỗi và kiểm tra kết nối.
c) Phân mảnh và tái hợp gói tin.
d) Điều khiển luồng và quản lý phiên.

30. Hai tiện ích dòng lệnh nào sử dụng thông điệp ICMP để kiểm tra kết nối mạng? (Chọn hai)

a) ping
b) traceroute
c) ipconfig
d) netstat
e) arp

31. Giá trị Time-to-Live (TTL) trong gói tin IPv4 có chức năng gì?

a) Ngăn các gói tin lặp vô hạn trong mạng.
b) Đo thời gian trễ của mạng.
c) Xác định mức độ ưu tiên của gói tin.
d) Đảm bảo gói tin được gửi đến đúng đích.

32. Đặc điểm nào sau đây mô tả đúng nhất về giao thức TCP (Transmission Control Protocol)?

a) Hướng kết nối và đảm bảo tin cậy.
b) Không hướng kết nối và nhanh.
c) Sử dụng cho các ứng dụng thời gian thực.
d) Có overhead thấp.

33. Một socket trong giao tiếp mạng được xác định bởi sự kết hợp của những yếu tố nào?

a) Địa chỉ IP và số cổng.
b) Địa chỉ MAC và địa chỉ IP.
c) Số thứ tự và số xác nhận.
d) Địa chỉ IP và tên miền.

34. Quá trình bắt tay ba bước (three-way handshake) của TCP sử dụng các cờ (flag) nào? (Chọn hai)

a) SYN
b) ACK
c) FIN
d) RST
e) PSH

35. Giao thức nào ở tầng Vận chuyển phù hợp nhất cho các ứng dụng như thoại qua IP (VoIP) và streaming video trực tiếp?

a) UDP (User Datagram Protocol)
b) TCP (Transmission Control Protocol)
c) ICMP (Internet Control Message Protocol)
d) ARP (Address Resolution Protocol)

36. Chức năng của số thứ tự (sequence number) trong header của TCP là gì?

a) Để sắp xếp lại các segment theo đúng thứ tự tại đích.
b) Để xác định ứng dụng đích.
c) Để kiểm tra lỗi trong segment.
d) Để điều khiển luồng dữ liệu.

37. Khoảng số cổng nào được định nghĩa là các cổng nổi tiếng (well-known ports)?

a) 0 đến 1023
b) 1024 đến 49151
c) 49152 đến 65535
d) 0 đến 255

38. Cơ chế nào của TCP được sử dụng để ngăn việc làm quá tải bộ đệm của thiết bị nhận?

a) Điều khiển luồng (Flow Control)
b) Bắt tay ba bước
c) Số thứ tự
d) Xác nhận

39. Giao thức nào được sử dụng để chuyển đổi tên miền (ví dụ: www.google.com) thành địa chỉ IP?

a) DNS (Domain Name System)
b) DHCP (Dynamic Host Configuration Protocol)
c) HTTP (Hypertext Transfer Protocol)
d) SMTP (Simple Mail Transfer Protocol)

40. Khi một máy khách web gửi yêu cầu để lấy một trang web, nó sử dụng phương thức HTTP nào?

a) GET
b) POST
c) PUT
d) HEAD

41. Giao thức nào được sử dụng để gửi email từ một máy khách đến một máy chủ mail?

a) SMTP (Simple Mail Transfer Protocol)
b) POP3 (Post Office Protocol 3)
c) IMAP (Internet Message Access Protocol)
d) HTTP (Hypertext Transfer Protocol)

42. Sự khác biệt chính giữa POP3 và IMAP là gì?

a) IMAP giữ lại bản sao email trên máy chủ, trong khi POP3 thường xóa chúng sau khi tải về.
b) POP3 an toàn hơn IMAP.
c) IMAP chỉ dùng để gửi mail, POP3 dùng để nhận mail.
d) POP3 nhanh hơn IMAP.

43. Giao thức nào cho phép cấp phát địa chỉ IP và các thông tin cấu hình mạng khác một cách tự động cho các thiết bị trong mạng?

a) DHCP (Dynamic Host Configuration Protocol)
b) DNS (Domain Name System)
c) FTP (File Transfer Protocol)
d) SNMP (Simple Network Management Protocol)

44. Trong mô hình client-server, vai trò của client là gì?

a) Yêu cầu thông tin hoặc dịch vụ.
b) Cung cấp thông tin hoặc dịch vụ.
c) Quản lý lưu lượng mạng.
d) Lưu trữ dữ liệu lâu dài.

45. Giao thức chia sẻ tệp nào là chủ đạo trong các mạng của Microsoft và cũng được hỗ trợ trên Linux (thông qua SAMBA) và macOS?

    a) SMB (Server Message Block)
    b) FTP (File Transfer Protocol)
    c) NFS (Network File System)
    d) TFTP (Trivial File Transfer Protocol)

46. Loại phần mềm độc hại nào tự nhân bản và lây lan qua mạng mà không cần sự tương tác của người dùng?

    a) Worm (Sâu)
    b) Virus
    c) Trojan horse
    d) Spyware

47. Ba thành phần của framework bảo mật AAA là gì? (Chọn ba)

    a) Authentication (Xác thực)
    b) Authorization (Ủy quyền)
    c) Accounting (Kiểm toán)
    d) Access (Truy cập)
    e) Administration (Quản trị)

48. Giao thức nào cung cấp kết nối quản lý từ xa an toàn bằng cách mã hóa dữ liệu?

    a) SSH (Secure Shell)
    b) Telnet
    c) HTTP
    d) FTP

49. Loại tấn công nào có mục đích làm cho một dịch vụ mạng không khả dụng đối với người dùng hợp pháp?

    a) Denial-of-Service (DoS)
    b) Reconnaissance
    c) Man-in-the-middle
    d) Access Attack

50. Một bức tường lửa (firewall) hoạt động ở tầng nào của mô hình OSI?

    a) Chủ yếu ở Tầng 3 (Network) và Tầng 4 (Transport).
    b) Chỉ ở Tầng 2 (Data Link).
    c) Chỉ ở Tầng 7 (Application).
    d) Chỉ ở Tầng 1 (Physical).

51. Một trong những cách hiệu quả nhất để giảm thiểu tác động của một cuộc tấn công worm là gì?

    a) Tải xuống các bản cập nhật bảo mật và vá lỗi cho các hệ điều hành.
    b) Cài đặt nhiều chương trình diệt virus.
    c) Thay đổi mật khẩu thường xuyên.
    d) Sử dụng tường lửa phần cứng.

52. Một cuộc tấn công mà kẻ tấn công cố gắng đoán mật khẩu bằng cách thử tất cả các kết hợp có thể được gọi là gì?

    a) Brute-force attack
    b) Social engineering
    c) Phishing
    d) Spoofing

53. Yếu tố nào sau đây là quan trọng nhất khi lựa chọn thiết bị cho một mạng nhỏ có dự báo tăng trưởng lớn?

    a) Khả năng mở rộng (Modularity/Expandability)
    b) Chi phí thấp nhất
    c) Mật độ cổng cố định
    d) Giao diện quản lý đơn giản nhất

54. Việc tạo một "baseline"cho hiệu suất mạng có mục đích gì?

a) Để có một điểm tham chiếu cho hiệu suất bình thường, giúp xác định các vấn đề trong tương lai.
b) Để sao lưu cấu hình mạng.
c) Để kiểm tra kết nối mạng lần đầu.
d) Để tự động cấu hình các thiết bị mạng.

55. Lệnh nào trên router Cisco được sử dụng để khám phá các thiết bị Cisco được kết nối trực tiếp?

a) show cdp neighbors
b) show ip route
c) show interfaces
d) show arp

56. Khi một máy tính Windows không thể nhận được địa chỉ IP từ máy chủ DHCP, nó sẽ tự gán cho mình một địa chỉ IP từ dải nào?

a) 169.254.0.0/16 (APIPA)
b) 192.168.1.0/24
c) 10.0.0.0/8
d) 127.0.0.0/8

57. Yếu tố thiết kế nào giúp loại bỏ các điểm lỗi đơn (single points of failure) trong mạng?

a) Redundancy (Dự phòng)
b) Scalability (Khả năng mở rộng)
c) Cost (Chi phí)
d) Security (Bảo mật)

58. Trong việc khắc phục sự cố, bước đầu tiên và quan trọng nhất là gì?

a) Xác định vấn đề.
b) Thực hiện giải pháp.
c) Tài liệu hóa các phát hiện.
d) Kiểm tra giả thuyết.

59. Lệnh nào trên router Cisco sẽ hiển thị các thông điệp gỡ rối (debug messages) trên một phiên Telnet hoặc SSH từ xa?

a) terminal monitor
b) debug all
c) show logging
d) logging console

Hướng dẫn trả lời

1. **Đáp án:** A. Địa chỉ MAC của cổng gateway mặc định.
   Giải thích: Khi đích nằm trên một mạng khác, khung dữ liệu phải được gửi đến router (gateway mặc định) để được định tuyến. Do đó, MAC đích của khung là MAC của giao diện router trên cùng mạng cục bộ với máy chủ gửi.

2. **Đáp án:** A. Neighbor Discovery (ND)
   Giải thích: IPv6 sử dụng Giao thức Khám phá Láng giềng (ND), một phần của ICMPv6, để thực hiện các chức năng như phân giải địa chỉ (tương đương ARP), khám phá router và tự động cấu hình địa chỉ.

3. **Đáp án:** A. Broadcast ở Lớp 2
   Giải thích: Yêu cầu ARP được gửi đến địa chỉ MAC broadcast (FF:FF:FF:FF:FF:FF) để tất cả các thiết bị trên mạng cục bộ đều nhận và xử lý nó, nhưng chỉ thiết bị có địa chỉ IP tương ứng mới trả lời.

4. **Đáp án:** A. Địa chỉ IPv4 và địa chỉ MAC
   Giải thích: Bảng ARP (còn gọi là ARP cache) duy trì một bảng ánh xạ động giữa địa chỉ IP (Lớp 3) và địa chỉ MAC (Lớp 2) tương ứng của các thiết bị trên mạng cục bộ.

5. **Đáp án:** A. ARP spoofing (Giả mạo ARP)
   Giải thích: ARP spoofing là một kỹ thuật tấn công trong đó kẻ tấn công gửi các gói tin ARP giả mạo để liên kết địa chỉ MAC của mình với địa chỉ IP của một thiết bị khác, thường là gateway mặc định, nhằm mục đích chặn hoặc sửa đổi dữ liệu.

6. **Đáp án:** A, B. Neighbor Solicitation, Neighbor Advertisement
   Giải thích: Trong IPv6, một thiết bị gửi thông điệp Neighbor Solicitation (tương tự ARP request) để hỏi địa chỉ MAC của một địa chỉ IPv6 cụ thể. Thiết bị đích sẽ trả lời bằng một thông điệp Neighbor Advertisement (tương tự ARP reply) chứa địa chỉ MAC của nó.

7. **Đáp án:** A. service password-encryption
   Giải thích: Lệnh này áp dụng một phương pháp mã hóa yếu cho tất cả các mật khẩu chưa được mã hóa trong tệp cấu hình, chẳng hạn như mật khẩu console, vty, để chúng không hiển thị dưới dạng văn bản thuần.

8. **Đáp án:** A. Địa chỉ logic của giao diện router trên cùng mạng với máy tính chủ.
   Giải thích: Gateway mặc định là thiết bị (thường là router) mà một máy chủ sử dụng để gửi lưu lượng truy cập đến các thiết bị trên các mạng khác. Địa chỉ của nó phải nằm trên cùng một mạng con logic với máy chủ.

9. **Đáp án:** A. show ip interface brief
   Giải thích: Lệnh này cung cấp một đầu ra súc tích, hiển thị trạng thái của từng giao diện (up/down), địa chỉ IP được cấu hình và trạng thái của giao thức trên giao diện đó.

10. **Đáp án:** A. startup-config
    Giải thích: Tệp ‘startup-config‘ được lưu trữ trong bộ nhớ truy cập ngẫu nhiên không khả biến (NVRAM) và chứa cấu hình được tải vào router mỗi khi nó khởi động hoặc khởi động lại.

11. **Đáp án:** A. Cung cấp thông báo pháp lý hoặc cảnh báo cho bất kỳ ai đăng nhập vào router.
    Giải thích: Lệnh ‘banner motd‘ (Message of the Day) được sử dụng để hiển thị một thông điệp cho tất cả người dùng khi họ cố gắng kết nối và đăng nhập vào thiết bị, thường dùng cho mục đích cảnh báo truy cập trái phép.

12. **Đáp án:** A. Một địa chỉ IP gateway mặc định.
    Giải thích: Mặc dù switch Lớp 2 không cần địa chỉ IP để chuyển mạch các khung, nó cần một địa chỉ IP trên

một SVI (Switch Virtual Interface) và một gateway mặc định để có thể giao tiếp với các thiết bị ở mạng khác, cho phép quản lý từ xa.

13. **Đáp án:** A. Phép toán AND logic
Giải thích: Một thiết bị thực hiện phép toán AND logic từng bit một giữa địa chỉ IPv4 của nó và subnet mask để xác định địa chỉ mạng mà nó thuộc về.

14. **Đáp án:** A. 172.16.31.50
Giải thích: Theo RFC 1918, dải địa chỉ riêng lớp B là 172.16.0.0 đến 172.31.255.255. Địa chỉ 172.16.31.50 nằm trong dải này.

15. **Đáp án:** A. Broadcast
Giải thích: Truyền thông broadcast gửi một gói tin từ một nguồn đến tất cả các đích khác trong cùng một mạng hoặc miền broadcast.

16. **Đáp án:** A. 30
Giải thích: Một prefix /27 có nghĩa là 27 bit dành cho mạng và 32 - 27 = 5 bit dành cho host. Số lượng địa chỉ có thể có là 2^5 = 32. Trừ đi một địa chỉ cho mạng và một địa chỉ cho broadcast, ta còn lại 32 – 2 = 30 địa chỉ host hợp lệ.

17. **Đáp án:** A. Variable-Length Subnet Masking (VLSM)
Giải thích: VLSM cho phép các quản trị viên mạng sử dụng các subnet mask khác nhau cho các mạng con khác nhau trong cùng một mạng lớn, giúp tối ưu hóa việc sử dụng không gian địa chỉ.

18. **Đáp án:** A. 192.168.10 là phần mạng, 10 là phần host.
Giải thích: Với prefix /24 (tương đương subnet mask 255.255.255.0), 24 bit đầu tiên (3 octet đầu) là phần mạng, và 8 bit cuối cùng (octet cuối) là phần host.

19. **Đáp án:** A. Giảm kích thước của miền broadcast.
Giải thích: Khi một mạng lớn được chia thành các mạng con nhỏ hơn (subnet), các router sẽ ngăn chặn lưu lượng broadcast lan truyền từ subnet này sang subnet khác, do đó làm giảm kích thước của mỗi miền broadcast và cải thiện hiệu suất mạng.

20. **Đáp án:** A. fe80::2a0:c9ff:fe76:2434
Giải thích: Quy tắc viết tắt IPv6 cho phép loại bỏ các số 0 đứng đầu trong mỗi hextet (0000 thành 0) và thay thế một chuỗi các hextet toàn số 0 liên tiếp bằng dấu hai chấm đôi (::).

21. **Đáp án:** A. Link-local address (LLA)
Giải thích: Địa chỉ link-local (bắt đầu bằng fe80::/10) được tự động cấu hình trên mọi giao diện IPv6 và được sử dụng cho giao tiếp trong phạm vi liên kết cục bộ, chẳng hạn như khám phá láng giềng và làm gateway mặc định. Chúng không thể được định tuyến.

22. **Đáp án:** A, B, C. Global Routing Prefix, Subnet ID, Interface ID
Giải thích: Một địa chỉ GUA được cấu trúc thành ba phần: Global Routing Prefix (phần mạng do ISP cấp), Subnet ID (phần để tạo các mạng con trong tổ chức), và Interface ID (phần định danh thiết bị trên mạng con).

23. **Đáp án:** A. Stateless Address Autoconfiguration (SLAAC)
Giải thích: SLAAC là một phương pháp cho phép thiết bị tự tạo địa chỉ GUA của mình bằng cách kết hợp prefix mạng (64 bit) nhận được từ thông điệp RA của router với một Interface ID (64 bit) do chính nó tạo ra (thường từ địa chỉ MAC qua EUI-64 hoặc ngẫu nhiên).

24. **Đáp án:** A. Địa chỉ MAC 48-bit
Giải thích: Quá trình EUI-64 lấy địa chỉ MAC 48-bit của giao diện, chèn giá trị ‘FFFE‘ vào giữa, và đảo ngược bit thứ 7 để tạo ra một Interface ID 64-bit duy nhất.

25. **Đáp án:** A. ff02::2
    Giải thích: ff02::2 là địa chỉ multicast all-routers với phạm vi link-local. Tất cả các router IPv6 trên một liên kết sẽ lắng nghe địa chỉ này. Ví dụ, các máy chủ gửi thông điệp Router Solicitation đến địa chỉ này.

26. **Đáp án:** A. Kiểm tra xem chồng giao thức TCP/IP có được cài đặt và hoạt động chính xác trên máy chủ đó hay không.
    Giải thích: Ping đến địa chỉ loopback (::1 cho IPv6 hoặc 127.0.0.1 cho IPv4) là một bài kiểm tra nội bộ để xác nhận rằng ngăn xếp giao thức mạng của hệ điều hành đang hoạt động, mà không cần gửi bất kỳ lưu lượng nào ra mạng bên ngoài.

27. **Đáp án:** A. Time Exceeded
    Giải thích: ‘traceroute‘ hoạt động bằng cách gửi các gói tin với giá trị TTL (Time-to-Live) hoặc Hop Limit tăng dần. Mỗi router trên đường đi giảm giá trị này đi một. Khi giá trị về 0, router sẽ gửi lại một thông điệp ICMP "Time Exceeded", cho phép ‘traceroute‘ xác định được địa chỉ của router đó.

28. **Đáp án:** A. Destination Unreachable
    Giải thích: Khi một router hoặc máy chủ nhận được một gói tin mà nó không thể chuyển tiếp hoặc không có đường đi đến đích, nó sẽ gửi lại một thông điệp ICMP "Destination Unreachable"cho nguồn.

29. **Đáp án:** A. Phân giải địa chỉ và tự động cấu hình địa chỉ.
    Giải thích: ICMPv6 tích hợp các chức năng của Giao thức Khám phá Láng giềng (NDP), bao gồm các thông điệp như Neighbor Solicitation/Advertisement (để phân giải địa chỉ) và Router Solicitation/Advertisement (hỗ trợ tự động cấu hình địa chỉ).

30. **Đáp án:** A, B. ping, traceroute
    Giải thích: ‘ping‘ sử dụng ICMP Echo Request và Echo Reply để kiểm tra sự tồn tại và thời gian phản hồi của một máy chủ. ‘traceroute‘ sử dụng ICMP Time Exceeded để xác định các chặng đường đi của gói tin.

31. **Đáp án:** A. Ngăn các gói tin lặp vô hạn trong mạng.
    Giải thích: Mỗi router trên đường đi sẽ giảm giá trị TTL đi một. Nếu TTL về 0 trước khi đến đích, gói tin sẽ bị hủy. Điều này ngăn chặn các gói tin đi lạc hoặc bị kẹt trong một vòng lặp định tuyến làm tắc nghẽn mạng.

32. **Đáp án:** A. Hướng kết nối và đảm bảo tin cậy.
    Giải thích: TCP thiết lập một kết nối logic (phiên) trước khi truyền dữ liệu, và sử dụng các cơ chế như số thứ tự và xác nhận để đảm bảo rằng tất cả dữ liệu được gửi đi đều đến đích một cách chính xác và theo đúng thứ tự.

33. **Đáp án:** A. Địa chỉ IP và số cổng.
    Giải thích: Một socket là điểm cuối của một kết nối hai chiều, được xác định duy nhất bởi sự kết hợp của một địa chỉ IP và một số cổng. Cặp socket (nguồn và đích) xác định một kết nối mạng duy nhất.

34. **Đáp án:** A, B. SYN, ACK
    Giải thích: Quá trình bắt tay ba bước bắt đầu bằng một gói tin có cờ SYN (synchronize). Máy chủ trả lời bằng một gói tin có cả cờ SYN và ACK (acknowledgment). Cuối cùng, máy khách hoàn tất kết nối bằng một gói tin có cờ ACK.

35. **Đáp án:** A. UDP (User Datagram Protocol)
    Giải thích: Các ứng dụng thời gian thực như VoIP và streaming video ưu tiên tốc độ và độ trễ thấp hơn là độ tin cậy tuyệt đối. UDP có overhead thấp và không có cơ chế bắt tay hay truyền lại, phù hợp với các yêu cầu này.

36. **Đáp án:** A. Để sắp xếp lại các segment theo đúng thứ tự tại đích.
Giải thích: Vì các segment có thể đến đích không theo thứ tự, bên nhận sử dụng số thứ tự trong mỗi segment để sắp xếp chúng lại thành luồng dữ liệu ban đầu trước khi chuyển lên tầng ứng dụng.

37. **Đáp án:** A. 0 đến 1023
Giải thích: IANA định nghĩa dải số cổng từ 0 đến 1023 là các cổng nổi tiếng, được dành riêng cho các dịch vụ và giao thức mạng phổ biến (ví dụ: HTTP port 80, FTP port 21).

38. **Đáp án:** A. Điều khiển luồng (Flow Control)
Giải thích: TCP sử dụng một cơ chế gọi là cửa sổ trượt (sliding window). Thiết bị nhận sẽ thông báo kích thước cửa sổ (window size) của nó, cho biết lượng dữ liệu nó có thể nhận trước khi cần xử lý. Điều này giúp bên gửi điều chỉnh tốc độ truyền để không làm quá tải bên nhận.

39. **Đáp án:** A. DNS (Domain Name System)
Giải thích: DNS là hệ thống phân giải tên miền, hoạt động như một "danh bạ"của Internet, cho phép người dùng sử dụng các tên dễ nhớ để truy cập các trang web, trong khi máy tính sử dụng các địa chỉ IP số để giao tiếp.

40. **Đáp án:** A. GET
Giải thích: Phương thức GET được sử dụng để yêu cầu một tài nguyên cụ thể (như một trang HTML, hình ảnh) từ máy chủ web. Đây là phương thức phổ biến nhất khi bạn truy cập một trang web.

41. **Đáp án:** A. SMTP (Simple Mail Transfer Protocol)
Giải thích: SMTP được sử dụng cho quá trình gửi email. Máy khách email sử dụng SMTP để gửi thư đến máy chủ mail của mình, và các máy chủ mail cũng sử dụng SMTP để chuyển tiếp thư cho nhau.

42. **Đáp án:** A. IMAP giữ lại bản sao email trên máy chủ, trong khi POP3 thường xóa chúng sau khi tải về.
Giải thích: IMAP được thiết kế để quản lý email trực tiếp trên máy chủ, cho phép truy cập từ nhiều thiết bị và đồng bộ hóa trạng thái. POP3 được thiết kế để tải email về một thiết bị duy nhất và thường xóa bản gốc trên máy chủ.

43. **Đáp án:** A. DHCP (Dynamic Host Configuration Protocol)
Giải thích: DHCP tự động hóa quá trình cấu hình IP cho các thiết bị. Khi một thiết bị kết nối vào mạng, nó có thể gửi yêu cầu đến máy chủ DHCP để nhận địa chỉ IP, subnet mask, gateway mặc định và địa chỉ máy chủ DNS.

44. **Đáp án:** A. Yêu cầu thông tin hoặc dịch vụ.
Giải thích: Trong mô hình client-server, client là bên chủ động khởi tạo kết nối và gửi yêu cầu đến server để nhận về dữ liệu hoặc sử dụng một dịch vụ mà server cung cấp.

45. **Đáp án:** A. SMB (Server Message Block)
Giải thích: SMB là giao thức chính được sử dụng trong các mạng Windows để chia sẻ tệp, máy in và các tài nguyên mạng khác. Nó cho phép các ứng dụng và người dùng truy cập các tệp trên một máy chủ từ xa như thể chúng đang ở trên máy cục bộ.

46. **Đáp án:** A. Worm (Sâu)
Giải thích: Worm là một loại phần mềm độc hại có khả năng tự nhân bản và lây lan độc lập qua các kết nối mạng, thường khai thác các lỗ hổng bảo mật để xâm nhập vào các hệ thống khác mà không cần tệp tin chủ.

47. **Đáp án:** A, B, C. Authentication (Xác thực), Authorization (Ủy quyền), Accounting (Kiểm toán)
Giải thích: AAA là một framework bảo mật: Authentication xác minh danh tính người dùng (bạn là ai?), Authorization xác định quyền hạn của người dùng (bạn được làm gì?), và Accounting ghi lại các hành động của người dùng (bạn đã làm gì?).

48. **Đáp án:** A. SSH (Secure Shell)
    Giải thích: SSH cung cấp một kênh giao tiếp được mã hóa qua một mạng không an toàn, cho phép đăng nhập và thực thi lệnh từ xa một cách bảo mật, không giống như Telnet truyền dữ liệu dưới dạng văn bản thuần.

49. **Đáp án:** A. Denial-of-Service (DoS)
    Giải thích: Mục tiêu của tấn công DoS là làm cạn kiệt tài nguyên của một hệ thống (như CPU, bộ nhớ, băng thông), khiến nó không thể phục vụ các yêu cầu hợp lệ từ người dùng, gây gián đoạn dịch vụ.

50. **Đáp án:** A. Chủ yếu ở Tầng 3 (Network) và Tầng 4 (Transport).
    Giải thích: Tường lửa packet-filtering và stateful hoạt động ở tầng 3 và 4, kiểm tra các địa chỉ IP nguồn/đích và số cổng nguồn/đích. Các tường lửa thế hệ mới (Next-Gen) có thể kiểm tra sâu hơn ở tầng ứng dụng (Tầng 7).

51. **Đáp án:** A. Tải xuống các bản cập nhật bảo mật và vá lỗi cho các hệ điều hành.
    Giải thích: Worm thường khai thác các lỗ hổng đã biết trong hệ điều hành hoặc phần mềm. Việc áp dụng các bản vá bảo mật mới nhất sẽ đóng các lỗ hổng này, ngăn chặn worm lây lan hiệu quả.

52. **Đáp án:** A. Brute-force attack
    Giải thích: Tấn công brute-force là một phương pháp thử-và-sai, sử dụng các công cụ tự động để thử mọi tổ hợp ký tự có thể cho đến khi tìm ra mật khẩu đúng.

53. **Đáp án:** A. Khả năng mở rộng (Modularity/Expandability)
    Giải thích: Với dự báo tăng trưởng lớn, việc chọn các thiết bị có thể mở rộng (ví dụ: switch modular có thể thêm cổng, router có thể thêm module) là rất quan trọng để mạng có thể phát triển cùng doanh nghiệp mà không cần thay thế toàn bộ phần cứng.

54. **Đáp án:** A. Để có một điểm tham chiếu cho hiệu suất bình thường, giúp xác định các vấn đề trong tương lai.
    Giải thích: Một baseline ghi lại các chỉ số hiệu suất của mạng (như độ trễ, băng thông sử dụng) trong điều kiện hoạt động bình thường. Khi có sự cố, quản trị viên có thể so sánh các chỉ số hiện tại với baseline để nhanh chóng xác định sự bất thường.

55. **Đáp án:** A. show cdp neighbors
    Giải thích: Giao thức Khám phá của Cisco (CDP) hoạt động ở Lớp 2 và cho phép các thiết bị Cisco trao đổi thông tin về mình với các thiết bị được kết nối trực tiếp. Lệnh ‘show cdp neighbors‘ hiển thị thông tin về các thiết bị láng giềng này.

56. **Đáp án:** A. 169.254.0.0/16 (APIPA)
    Giải thích: Automatic Private IP Addressing (APIPA) là một tính năng của Windows. Khi một máy tính được cấu hình để nhận IP tự động nhưng không tìm thấy máy chủ DHCP, nó sẽ tự gán một địa chỉ trong dải 169.254.0.0 đến 169.254.255.254.

57. **Đáp án:** A. Redundancy (Dự phòng)
    Giải thích: Dự phòng là việc triển khai các thành phần (thiết bị, liên kết) dự phòng để nếu một thành phần chính bị lỗi, thành phần dự phòng có thể tiếp quản, đảm bảo tính liên tục của hoạt động mạng và loại bỏ các điểm lỗi đơn.

58. **Đáp án:** A. Xác định vấn đề.
    Giải thích: Theo các phương pháp khắc phục sự cố có cấu trúc, bước đầu tiên luôn là thu thập thông tin và xác định rõ ràng vấn đề là gì (ví dụ: "Người dùng X không thể truy cập máy chủ Y", thay vì "mạng chậm"). Điều này định hướng toàn bộ quá trình xử lý sau đó.

59. **Đáp án:** A. terminal monitor
Giải thích: Theo mặc định, các thông điệp hệ thống như debug chỉ hiển thị trên phiên console. Để xem chúng trên một phiên kết nối từ xa (Telnet/SSH), bạn phải sử dụng lệnh ‘terminal monitor‘ ở chế độ privileged EXEC.

Phụ lục C

Bài kiểm tra tổng hợp

Câu hỏi

1. Mạng máy tính mang lại lợi ích nào?
    a) Liên lạc và chia sẻ thông tin
    b) Làm việc và học tập từ xa
    c) Giải trí trực tuyến
    d) Tất cả các đáp án trên
2. Điểm khác biệt chính giữa mạng gia đình và mạng doanh nghiệp là gì?
    a) Quy mô và số lượng người dùng
    b) Mức độ bảo mật và độ tin cậy
    c) Dịch vụ mạng triển khai
    d) Loại card mạng sử dụng
3. Internet là gì?
    a) Một mạng LAN
    b) Tập hợp nhiều mạng con kết nối toàn cầu
    c) Một loại kết nối không dây
    d) Chỉ là mạng doanh nghiệp lớn
4. Địa chỉ IPv4 có độ dài bao nhiêu bit?
    a) 16
    b) 32
    c) 64
    d) 128
5. Địa chỉ IPv6 có độ dài bao nhiêu bit?
    a) 32
    b) 64
    c) 128
    d) 256
6. Giao thức nào dùng để phân giải tên miền?
    a) DHCP
    b) FTP
    c) DNS
    d) SSH
7. Giao thức nào cấp phát địa chỉ IP động?
    a) SMTP
    b) DHCP
    c) POP3
    d) IMAP
8. Giao thức nào dùng để gửi email đi?
    a) SMTP
    b) POP3
    c) IMAP
    d) FTP
9. Giao thức nào hỗ trợ truyền tệp tin?
    a) HTTP
    b) FTP
    c) IMAP
    d) DNS
10. Trong mô hình OSI, tầng nào chịu trách nhiệm định tuyến gói tin?
    a) Tầng Vật lý

b) Tầng Liên kết dữ liệu

c) Tầng Mạng

d) Tầng Ứng dụng

11. Tầng nào cung cấp dịch vụ đầu cuối-đến-đầu cuối?

a) Tầng Vận chuyển

b) Tầng Mạng

c) Tầng Liên kết dữ liệu

d) Tầng Vật lý

12. TCP là gì?

a) Giao thức không kết nối

b) Giao thức hướng kết nối, tin cậy

c) Giao thức tầng ứng dụng

d) Giao thức vật lý

13. UDP thường được dùng trong ứng dụng nào?

a) Email

b) Truyền video trực tuyến

c) FTP

d) HTTPS

14. Địa chỉ MAC có độ dài bao nhiêu bit?

a) 32

b) 48

c) 64

d) 128

15. Giao thức nào dùng để phân giải IPv4 sang MAC?

a) DNS

b) ARP

c) ICMP

d) DHCP

16. IPv6 thay thế ARP bằng cơ chế nào?

a) ICMPv4

b) DNS

c) NDP (Neighbor Discovery)

d) SLAAC

17. Lệnh `ping` dùng để làm gì?

a) Hiển thị bảng MAC

b) Kiểm tra kết nối giữa hai thiết bị

c) Cấu hình địa chỉ IP

d) Sao chép cấu hình

18. Lệnh `show ip interface brief` trên router dùng để?

a) Kiểm tra trạng thái các giao diện

b) Hiển thị bảng định tuyến

c) Hiển thị bảng MAC

d) Hiển thị ARP cache

19. Quy trình bắt tay ba bước (3-way handshake) thuộc về giao thức nào?

a) UDP

b) TCP

c) ICMP

d) HTTP

20. Địa chỉ broadcast trong IPv4 là gì?

a) Địa chỉ đầu tiên trong subnet

b) Địa chỉ cuối cùng trong subnet

c) Địa chỉ mặc định của router

d) Địa chỉ DNS

21. Các dải địa chỉ IPv4 riêng là gì?

a) 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16

b) 128.0.0.0/8

c) 169.254.0.0/16

d) 224.0.0.0/4

22. Địa chỉ loopback của IPv4 là gì?

a) 0.0.0.0

b) 127.0.0.1

c) 255.255.255.255

d) 169.254.1.1

23. SLAAC trong IPv6 có chức năng gì?

a) Tự động cấu hình địa chỉ IPv6 cho host

b) Phân giải tên miền

c) Gán địa chỉ MAC

d) Thiết lập VPN

24. ICMP dùng cho mục đích gì?

a) Mã hóa dữ liệu
b) Báo lỗi và chẩn đoán kết nối
c) Cấp phát IP động
d) Truyền email

25. ICMPv6 hỗ trợ chức năng gì mà ICMPv4 không có?
a) Echo Request/Reply
b) Neighbor Discovery
c) Time Exceeded
d) Destination Unreachable

26. ACL dùng để làm gì?
a) Sao chép cấu hình
b) Lọc và kiểm soát lưu lượng mạng
c) Chia subnet
d) Tăng tốc độ mạng

27. Giao thức nào truyền dữ liệu dạng mã hóa, thay thế cho Telnet?
a) FTP
b) SSH
c) HTTP
d) SMTP

28. Tường lửa (firewall) có chức năng gì?
a) Tăng tốc độ truyền dữ liệu
b) Ngăn chặn và lọc truy cập trái phép
c) Sao lưu dữ liệu
d) Quản lý địa chỉ MAC

29. Một subnet /26 cung cấp bao nhiêu địa chỉ host khả dụng?
a) 62
b) 126
c) 254
d) 512

30. Địa chỉ IPv6 link-local luôn bắt đầu bằng?
a) FE80::/10
b) FF00::/8
c) 2000::/3
d) ::1

31. Router có chức năng chính là gì?
a) Kết nối các mạng khác nhau và định tuyến gói tin
b) Lọc khung dữ liệu trong LAN
c) Cấp phát địa chỉ IP
d) Chuyển đổi tín hiệu

32. Switch xây dựng bảng MAC bằng cách nào?
a) Dùng ARP
b) Học địa chỉ MAC nguồn từ khung đi vào
c) Dựa vào DNS
d) Nhờ router cung cấp

33. VLAN dùng để?
a) Tăng băng thông vật lý
b) Tách biệt logic lưu lượng trong mạng LAN
c) Mã hóa dữ liệu đầu cuối
d) Tự động cấp phát IP

34. Một địa chỉ IPv6 ::1 có ý nghĩa gì?
a) Địa chỉ link-local
b) Địa chỉ loopback
c) Địa chỉ multicast
d) Địa chỉ anycast

35. Giao thức nào hoạt động ở tầng Liên kết dữ liệu?
a) IP
b) Ethernet
c) HTTP
d) ICMP

36. CRC trong khung dữ liệu dùng để?
a) Mã hóa dữ liệu
b) Phát hiện lỗi khi truyền
c) Định tuyến gói tin
d) Phân giải tên miền

37. Lớp nào trong mô hình OSI đảm bảo dữ liệu có thể đọc được cho người dùng?
a) Trình bày (Presentation)
b) Ứng dụng (Application)

c) Vận chuyển (Transport)

d) Phiên (Session)

38. Các cổng well-known nằm trong phạm vi nào?

a) 0–1023

b) 1024–49151

c) 49152–65535

d) 0–65535

39. Port mặc định của HTTPS là gì?

a) 21

b) 25

c) 80

d) 443

40. Port mặc định của DNS là gì?

a) 20

b) 21

c) 53

d) 110

41. Port mặc định của FTP (control) là gì?

a) 20

b) 21

c) 22

d) 23

42. Port mặc định của SSH là gì?

a) 20

b) 21

c) 22

d) 23

43. Port mặc định của Telnet là gì?

a) 22

b) 23

c) 25

d) 110

44. Port mặc định của SMTP là gì?

a) 25

b) 53

c) 80

d) 143

45. Port mặc định của POP3 là gì?

a) 25

b) 53

c) 110

d) 143

46. Port mặc định của IMAP là gì?

a) 25

b) 53

c) 110

d) 143

47. Một khung broadcast trong Ethernet được gửi đến?

a) Một host cụ thể

b) Một nhóm host

c) Tất cả host trong LAN

d) Router gần nhất

48. Dải địa chỉ multicast IPv4 nằm trong phạm vi nào?

a) 169.254.0.0/16

b) 224.0.0.0 – 239.255.255.255

c) 240.0.0.0/4

d) 10.0.0.0/8

49. Thiết bị nào làm việc chủ yếu ở tầng Liên kết dữ liệu?

a) Router

b) Switch

c) Hub

d) Firewall

50. Thiết bị nào làm việc chủ yếu ở tầng Mạng?

a) Router

b) Switch

c) Hub

d) Access Point

51. ICMP thông điệp “Destination Unreachable” có ý nghĩa gì?

a) Host đích không phản hồi

b) Không thể định tuyến đến đích

c) Router bị tắt

d) Kết nối đã hết TTL

52. TTL trong gói IPv4 có ý nghĩa gì?

a) Tốc độ truyền tải

b) Thời gian tồn tại gói tin, giảm dần khi qua router

c) Tổng số hop cố định

d) Thời gian đáp ứng

53. Giao thức nào cung cấp độ tin cậy với cơ chế ACK?

a) UDP

b) TCP

c) ICMP

d) ARP

54. Công cụ nào dùng để phân tích gói tin chi tiết?

a) Telnet

b) Wireshark

c) FTP

d) SSH

55. Một mạng nhỏ thường dùng dịch vụ nào để cấp phát địa chỉ IP?

a) DNS

b) DHCP

c) FTP

d) ICMP

56. WPA2/WPA3 được dùng trong?

a) Mạng LAN có dây

b) Mạng không dây Wi-Fi

c) VPN

d) VLAN

57. Một trong các biện pháp bảo mật cơ bản cho thiết bị Cisco là?

a) Cấu hình mật khẩu console và VTY

b) Bỏ qua banner cảnh báo

c) Sử dụng Telnet thay SSH

d) Không cần enable secret

58. Địa chỉ APIPA (Automatic Private IP Addressing) thuộc dải nào?

a) 10.0.0.0/8

b) 169.254.0.0/16

c) 172.16.0.0/12

d) 192.168.0.0/16

59. Địa chỉ IPv6 ::/0 biểu thị gì?

a) Default route

b) Loopback

c) Link-local

d) Multicast

60. Bước đầu tiên trong xử lý sự cố kết nối là gì?

a) Kiểm tra lớp vật lý (cáp, nguồn điện, kết nối)

b) Cấu hình lại DNS

c) Thay router

d) Xóa toàn bộ cấu hình

Hướng dẫn trả lời

1. d. Tất cả lợi ích đều đúng (liên lạc, học/làm từ xa, giải trí)
2. a,b,c. Khác biệt về quy mô, bảo mật/độ tin cậy, dịch vụ triển khai
3. b. Internet = tập hợp nhiều mạng con kết nối toàn cầu
4. b. IPv4 dài 32 bit
5. c. IPv6 dài 128 bit
6. c. DNS phân giải tên miền
7. b .DHCP cấp phát IP động
8. a .SMTP gửi email đi
9. b .FTP truyền tệp tin
10. c. Định tuyến nằm ở tầng Mạng (Network)
11. a. Dịch vụ đầu cuối-đến-đầu cuối là tầng Vận chuyển (Transport)
12. b. TCP là giao thức hướng kết nối, tin cậy
13. b. UDP hay dùng cho streaming/thời gian thực
14. b. MAC địa chỉ 48 bit
15. b. ARP phân giải IPv4 -> MAC
16. c. IPv6 dùng NDP thay ARP
17. b. ping để kiểm tra kết nối
18. a. show ip interface brief: xem nhanh trạng thái giao diện
19. b. 3-way handshake thuộc TCP
20. b. Địa chỉ broadcast = địa chỉ cuối của subnet
21. a. Dải IPv4 private: 10/8, 172.16/12, 192.168/16
22. b. Loopback IPv4: 127.0.0.1
23. a. SLAAC tự cấu hình IPv6 cho host
24. b. ICMP dùng báo lỗi/chẩn đoán
25. b. ICMPv6 có Neighbor Discovery
26. b. ACL dùng lọc/kiểm soát lưu lượng
27. b. SSH mã hóa, thay Telnet
28. b. Firewall lọc/ngăn truy cập trái phép
29. a. /26 có 62 host khả dụng (64-2)
30. a. Link-local IPv6: FE80::/10
31. a. Router kết nối mạng và định tuyến
32. b. Switch học MAC nguồn để lập bảng MAC
33. b. VLAN tách biệt logic lưu lượng trong LAN
34. b. ::1 là loopback IPv6
35. b. Ethernet là giao thức tầng Liên kết dữ liệu
36. b. CRC phát hiện lỗi khi truyền
37. a. Presentation định dạng/biểu diễn dữ liệu
38. a. Well-known ports: 0–1023
39. d. HTTPS dùng cổng 443
40. c. DNS dùng cổng 53
41. b. FTP control dùng cổng 21
42. c. SSH dùng cổng 22
43. b. Telnet dùng cổng 23
44. a. SMTP dùng cổng 25
45. c. POP3 dùng cổng 110
46. d. IMAP dùng cổng 143
47. c. Broadcast Ethernet đến tất cả host trong LAN
48. b. IPv4 multicast: 224.0.0.0–239.255.255.255
49. b. Switch hoạt động chủ yếu ở Layer 2 (Data Link)
50. a. Router hoạt động chủ yếu ở Layer 3 (Network)
51. b. Destination Unreachable: không thể đến đích
52. b. TTL: thời gian tồn tại, giảm qua mỗi router
53. b. TCP cung cấp độ tin cậy với ACK
54. b. Wireshark phân tích gói tin
55. b. DHCP thường cấp phát IP cho mạng nhỏ
56. b. WPA2/WPA3 dùng trong Wi-Fi
57. a. Bảo mật cơ bản: đặt mật khẩu console & VTY
58. b. APIPA: 169.254.0.0/16
59. a. ::/0 là default route IPv6
60. a. Bước đầu: kiểm tra lớp vật lý (cáp/nguồn/kết nối)