Các câu hỏi của bài thu hoạch 5 6 7 Mạng máy tính

1. **Mô tả các kiểu WPA**
2. **Mô tả sự tiến triển của các công nghệ bảo mật trong WLAN**

Câu 1. Mô tả các kiểu WPA: bao gồm2 kiểu WPA và WPA

	WPA	WPA2
Enterprise mode (Kinh doanh, giáo dục, chính phủ)	Xác thực: IEEE 802.1X/EAP Mã hóa: TKIP/MIC	Xác thực : IEEE 802.1X/EAP Mã hóa: AES-CCMP
Personal mode (SOHO, sử dụng tại nhà hay cá nhân)	Xác thực: PSK Mã hóa: TKIP/MIC	Xác thực: PSK Mã hóa: AES-CCMP

Chuẩn WPA cung cấp khả năng xác thực được hỗ trợ thông qua chuẩn 802.1x và khóa chia sẻ (Pre-shared Key). WPA cung cấp khả năng mã hóa được hỗ trợ thông qua chuẩn TKIP. Chuẩn TKIP bao gồm MIC và PPK (Per-packet Keying) sử dụng thông qua "initialization vector hashing" và broadcast key rotation".

•Khi so sánh với WPA, quá trình xác thực của WPA2 thì vẫn không thay đổi nhưng quá trình mã hóa được thực hiện bởi AES với giao thức AES-CCMP (AES Counter with CBC MAC Protocol).

•Enterprise mode

"Enterprise mode" là thuật ngữ dành cho những sản phẩm đã được kiểm tra về khả năng liên vận hành ở cả 2 kiểu PSK và 802.1X/ EAP cho chức năng xác thực. Chuẩn 802.1X yêu cầu phải có một AAA server khi được sử dụng. "Enterprise mode" được đưa ra nhằm đáp ứng nhu cầu trong môi trường mạng doanh nghiệp.

•Personal mode

"Personal mode" là thuật ngữ được sử dụng cho những sản phẩm đã được kiểm tra về khả năng liên vận hành duy nhất kiểu PSK cho chức năng xác thực. Quá trình này yêu cầu cấu hình PSK bằng tay trên cả Access point và client. PSK xác thực người dùng thông qua mật mã hoặc mã định danh trên cả client và Access point. Trong trường hợp này không cần phải sử dụng đến server xác thực.

"Personal mode" được đưa ra nhằm đáp ứng nhu cầu trong môi trường SOHO

1. **WPA (Wi-Fi Protected Access):**
    - **Mục tiêu:** WPA được phát triển nhằm thay thế cho WEP (Wired Equivalent Privacy) do WEP có nhiều lỗ hổng bảo mật.
    - **Phương pháp bảo mật chính:**
        - Sử dụng giao thức bảo mật TKIP (Temporal Key Integrity Protocol) để thay đổi khóa mật khẩu theo thời gian.
        - Hỗ trợ chế độ chia sẻ khóa (PSK - Pre-Shared Key) và chế độ chứng nhận máy chủ (Enterprise).

- **Nhược điểm:**
    - TKIP đã bị phát hiện có một số vấn đề bảo mật, và WPA có thể dễ bị tấn công khi sử dụng PSK.

2. **WPA2 (Wi-Fi Protected Access 2):**
    - **Mục tiêu:** WPA2 được thiết kế để nâng cao bảo mật bằng cách sử dụng giao thức AES (Advanced Encryption Standard).
    - **Phương pháp bảo mật chính:**
        - Sử dụng giao thức AES để thực hiện mã hóa dữ liệu truyền qua mạng.
        - Hỗ trợ cả chế độ chia sẻ khóa (PSK) và chế độ chứng nhận máy chủ (Enterprise).
    - **Ưu điểm:**
        - AES được coi là một trong những phương pháp mã hóa mạnh nhất và an toàn nhất hiện nay.
        - Tăng cường đáng kể độ an toàn so với WPA.

Ngoài ra, WPA3 là một phiên bản mới hơn của WPA2, được thiết kế để cải thiện bảo mật, đặc biệt là trong việc bảo vệ trước các loại tấn công mới. WPA3 sử dụng cảm biến password-based authentication, forward secrecy, và cải tiến về khả năng chống lại các cuộc tấn công từ điển và brute-force.

Câu 2. Mô tả sự tiến triển của các công nghệ bảo mật trong WLAN

Hầu hết ngay khi các chuẩn bảo mật mới ra đời, các hacker sẽ cố gắng khai thác những điểm yếu trên những chuẩn này. Để chống lại quá trình đó, các chuẩn bảo mật lại liên tục được nâng cấp để tăng cường khả năng bảo mật. Chủ đề này sẽ mô tả quá trình phát triển của vấn đề bảo mật trong mạng WLAN.

•Ban đầu, bảo mật trong môi trường WLAN được định nghĩa dựa trên từ khóa WEP 64 bit cho cả 2 tiến trình mã hóa và xác thực. Từ khóa WEP 64bit bao gồm 40bit cho từ khóa thực sự và 24 bit cho Vector khởi tạo. Phương pháp xác thực này thực sự không mạnh và thậm chí có thể bị dàn xếp từ khóa giữa các người dùng. Bởi vì các từ khóa được quản lý một cách thủ công do vậy phương pháp này không thể mở rộng một các

linh động trên các hệ thống mạng lớn được. Các công ty cố gắng khắc phục yếu điểm này với một số kỹ thuật SSID và lọc địa chỉ MAC.

•SSID là tên dùng để xác định hệ thống mạng WLAN và là thông số có thể cấu hình được. Cả Client và Access point phải cùng sử dụng giống nhau giá trị SSID này để giao tiếp. Nếu Access point được cấu hình để broadcast giá trị SSID trên toàn hệ thống mạng, Client sẽ liên kết với Access point đó bằng giá trị SSID nhận được. Access point có thể được cấu hình để không broadcast giá trị SSID ra ngoài (SSID cloaking), điều này mang lại cấp độ bảo mật đầu tiên trên hệ thống mạng WLAN bởi các hacker sẽ gặp khó khăn hơn để xác định sự tồn tại của Access point này. được cấu hình bằng tay trên Access point để cho phép hoặc không cho phép dựa trên địa chỉ vật lý của các client. Tuy nhiên địa chỉ MAC có thể dễ dàng bị giả, do đó phương pháp lọc địa chỉ MAC không còn được xem là một đặc tính bảo mật nữa.

•Trong thời gian mà ủy ban 802.11 bắt đầu tiến trình nâng cấp khả năng bảo mật trên hệ thống WLAN, các hãng độc lập đã sớm triển khai các chuẩn bảo mật trên hệ thống mạng WLAN của họ. Cisco đã sớm phát triển chuẩn mã hóa WEP trên việc cải thiện thuật toán RC4. Cisco thực thi chuẩn TKIP (Temporal Key Integrity Protocol) để mã hóa trên từng gói dữ liệu và Cisco MIC (Message Integrity Check) để bảo vệ từ khóa WEP. Cisco cũng đã dùng chuẩn xác thực 802.11x từ môi trường dây dẫn sang môi trường không dây và tự động hóa các từ khóa sử dụng bằng Cisco LEAP (Lightweight Extensible Authentication Protocol) nhằm tập trung hóa cơ sở dữ liệu.

•Ngay sau khi Cisco triển khai các chuẩn bảo mật trên mạng WLAN, Wi-Fi Alliance đã đưa ra chuẩn WPA (Wi-Fi Protected Access) như một chuẩn tạm thời cho một phần của chuẩn bảo mật 802.11i đang được mong đợi dùng chuẩn xác thực 802.1x và cải thiện quá trình mã hóa WEP. Chuẩn TKIP mới ra đời tương tự như Cisco TKIP và Cisco MIC nhưng các chuẩn này không tương thích với nhau.

•Ngày nay, 802.11i đã được phê chuẩn và chuẩn bảo mật AES (Advanced Encryption Standard) đã thay thế WEP và được xem như một chuẩn bảo mật nhất để mã hóa dữ liệu. Những hệ thống IDS trên WLAN cũng được triển khai để xác định những cuộc tấn công và bảo vệ hệ thống mạng. Wi-Fi Alliance chứng nhận các thiết bị 802.11i dưới

Source ChatGPT: Sự tiến triển của công nghệ bảo mật trong mạng WLAN (Wireless Local Area Network) đã trải qua nhiều giai đoạn để đáp ứng với thách thức ngày càng cao về bảo mật thông tin và dữ liệu. Dưới đây là một mô tả tổng quan về sự phát triển của các công nghệ bảo mật trong WLAN:

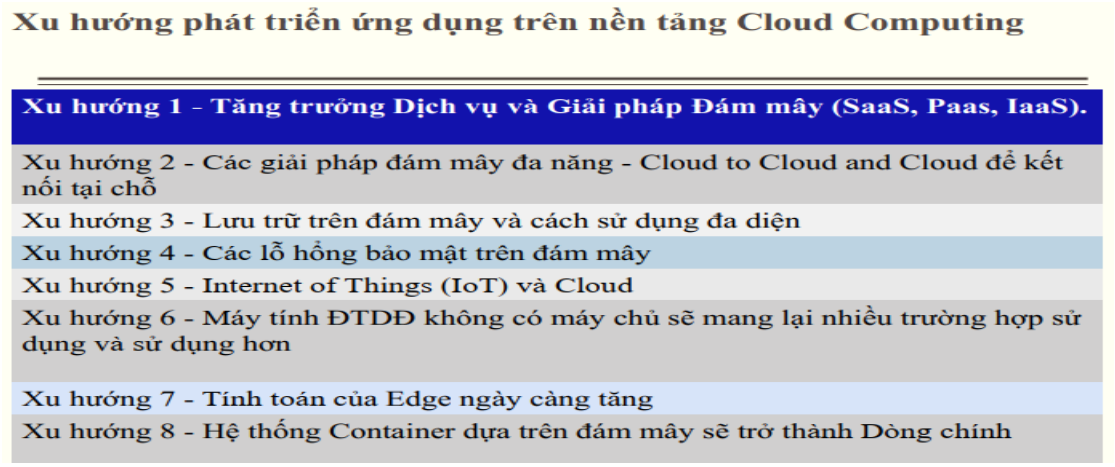
1. **WEP (Wired Equivalent Privacy):**

- **Thời kỳ:** WEP là phương thức bảo mật đầu tiên được sử dụng trong mạng WLAN.
- **Đặc điểm:**
  - Sử dụng thuật toán mã hóa RC4 để bảo vệ dữ liệu truyền qua mạng.
  - Tuy nhiên, WEP nhanh chóng trở nên không an toàn do những lỗ hổng bảo mật nổi bật, chẳng hạn như khả năng dễ dàng bị tấn công từ điển.

2. **WPA (Wi-Fi Protected Access):**
   - **Thời kỳ:** WPA đã ra đời như một giải pháp tạm thời để thay thế WEP khi WEP trở nên không an toàn.
   - **Đặc điểm:**
     - Sử dụng TKIP (Temporal Key Integrity Protocol) để thay đổi khóa mật khẩu theo thời gian.
     - WPA giúp cải thiện đáng kể độ an toàn so với WEP, nhưng vẫn có một số vấn đề bảo mật.
3. **WPA2 (Wi-Fi Protected Access 2):**
   - **Thời kỳ:** WPA2 tiếp tục phát triển từ WPA để cải thiện bảo mật.
   - **Đặc điểm:**
     - Sử dụng AES (Advanced Encryption Standard) thay vì TKIP, nâng cao đáng kể cường độ bảo mật của hệ thống.
     - WPA2 trở thành một tiêu chuẩn bảo mật cho nhiều hệ thống WLAN và được coi là rất an toàn.
4. **WPA3 (Wi-Fi Protected Access 3):**
   - **Thời kỳ:** WPA3 là một bước tiến mới nhất trong công nghệ bảo mật WLAN.
   - **Đặc điểm:**
     - Cung cấp nhiều cải tiến về bảo mật, bao gồm chống lại các cuộc tấn công từ điển và brute-force.
     - Sử dụng cảm biến password-based authentication và forward secrecy để cung cấp lớp bảo mật mạnh mẽ hơn.

Sự tiến triển của các công nghệ bảo mật WLAN đã làm cho mạng không dây trở nên an toàn hơn và đáp ứng được với những thách thức ngày càng phức tạp của môi trường mạng hiện đại.

Câu 1. Trình bày các xu hướng phát triển ứng dụng trên nền tảng Cloud computing.



1. Xu hướng 1 - Tăng trưởng Dịch vụ và Giải pháp Đám mây(SaaS, Paas, IaaS)

➢Với điện toán đám mây ngày càng tăng, chỉ có điều tự nhiên là các dịch vụ và giải pháp đám mây cũng sẽ phát triển.

➢Bain & Company dự đoán rằng phần mềm như một dịch vụ (SaaS), nơi phần mềm được cấp phép trên cơ sở đăng ký và được tổ chức tập trung, sẽ tăng trưởng ở mức 18% CAGR vào năm 2020. Các ứng dụng của Google Apps, Salesforce và Citrix GoToMeeting rất có thể tiếp tục đại diện cho thị trường điện toán đám mây lớn nhất.

➢Năm 2018 sẽ là năm mà sự chấp thuận của Enterprise Cloud Services được cải thiện; Dịch vụ Truyền thông xã hội sẽ tăng vọt, Dịch vụ Chia sẻ Tệp trên Điện toán đám mây sẽ gia tăng, Các Dịch vụ Hợp tác sẽ trở nên quen thuộc hơn, Dịch vụ Truyền thông xã hội sẽ nhận được sự dân chủ hóa và nhận được sự chấp nhận cao nhất.

2. Xu hướng 2 - Các giải pháp đám mây đa năng -Cloud to Cloud and Cloud để kết nối tại chỗ

➢ Cloud to Cloud Connectivity - Một số doanh nghiệp không đặc biệt thích gắn kết với nhà cung cấp đám mây duy nhất, đó là lý do tại sao nhiều nhà cung cấp đám mây đang mở API trên nền tảng để kết nối nhiều giải pháp. Mở API là cần thiết để đồng bộ quá trình và quản lý dữ liệu đa chức năng và đa chức năng cũng như tích hợp và kết nối với các hệ thống và công cụ.

➢ Cloud để kết nối tại chỗ - Hầu hết các doanh nghiệp sẽ giữ các giải pháp tại chỗ và kết nối với các giải pháp dựa trên đám mây với tùy chỉnh mạnh mẽ phù hợp nhất với nhu cầu kinh doanh của họ

3.Xu hướng 3-Lưutrữ trên đám mây và cách sử dụng đa diện

➢Lưu trữ đám mây đang trở nên rẻ hơn. Là do kinh tế của cung và cầu - cung cấp càng cao và nhu cầu thấp hơn, giá giảm.

➢Tuy nhiên, với lưu trữ đám mây không chỉ có một nguồn cung cấp đáng kể, nhưng cũng có nhu cầu cao. Do đó, lưu trữ đám mây không chỉ là giá rẻ mà còn được cung cấp miễn phí từ các nhà cung cấp đám mây nhất định để họ có thể giành được thị phần và thu thập dữ liệu người dùng có giá trị.

3. Xu hướng 3 - Lưu trữ trên đám mây và cách sử dụng đa diện

➢ Crowd Sourced Storage - Thay vì sử dụng lưu trữ đám mây truyền thống tốn kém, chậm và đôi khi không an toàn, việc lưu trữ đám đông sẽ trở thành lựa chọn cho những người muốn giữ cho chi phí thấp nhưng vẫn muốn tận dụng lợi ích của đám mây.

➢ Cloud Cost Wars - Cuộc chiến giá cả đám mây giữa Google và Amazon dựa trên nỗ lực của mỗi tổ chức để cung cấp dịch vụ rẻ nhất và chiếm lĩnh thị trường điện toán đám mây. Google giới thiệu Committed Use Discounts (CUD) hoặc theo định nghĩa của Google, "khả năng mua các hợp đồng sử dụng cam kết để đổi lấy giá chiết khấu sâu cho việc sử dụng máy chủ ảo".

4. Xu hướng 4 - Các lỗ hổng bảo mật trên đám mây

➢ Các vi phạm an ninh đang gia tăng. Theo Trung tâm Tài nguyên Tội phạm Cá nhân, số vụ vi phạm dữ liệu của Hoa Kỳ được theo dõi đến hết ngày 30 tháng 6 năm 2017 đã đạt mức kỷ lục 791 trong nửa năm, tăng đáng kể 29% so với cùng kỳ năm 2016. ITRC dự kiến rằng vào thời điểm này, có thể có sự gia tăng vi phạm hàng năm 37% vào năm 2017 so với năm 2016.

➢ Google đã thực hiện một số biện pháp bảo mật với key fob bảo mật của họ để đăng nhập vào các thiết bị bao gồm quy trình xác minh 2 bước. Fob chính này liên quan đến một mã được gửi đến điện thoại thông minh của bạn ngoài mật khẩu cố định của bạn để đảm bảo sự an toàn của tài khoản của bạn.

➢ Gartner dự kiến chi tiêu an ninh thông tin trên toàn thế giới sẽ đạt 93 tỷ đô la vào năm 2018 so với mức 86,4 tỷ đô la năm 2017 và IDC dự kiến doanh thu toàn cầu về công nghệ bảo mật sẽ đạt 101,6 tỷ đô la vào năm 2020.

➢ Các vấn đề bảo mật sẽ tiếp tục chiếm ưu thế vào năm 2018, có nghĩa là sẽ thấy nhiều công ty an ninh mạng hơn và sẽ có các lựa chọn bảo mật đám mây mới.

➢ Để thành công trong đám mây, IT và đội bảo mật cần phải nắm lấy một mô hình hoạt động mới. Đây chính là những gì mà công ty mới bắt đầu như Lacework đang tập trung vào. Bằng cách đưa tự động hóa, tốc độ và tích hợp với các dịch vụ bảo mật đám mây, công ty đã xác định lại cách tiếp cận bảo mật đám mây để thành công.

5. Xu hướng 5 - Internet of Things (IoT) và Cloud.

➢ Hầu hết các thiết bị IoT đều dựa vào đám mây để làm việc, đặc biệt là với các thiết bị được kết nối làm việc cùng nhau.

➢ Các thiết bị kết nối IoT như thiết bị gia dụng, ô tô và điện tử, có kết cuối dựa trên đám mây như một phương tiện để truyền thông và lưu trữ thông tin. Đám mây hỗ trợ các thiết bị này, và khi chúng ta thấy nhiều thiết bị IoT được sản xuất và bán thì việc sử dụng đám mây sẽ tiếp tục tăng lên.

6. Xu hướng 6 - Máy tính ĐTDĐ không có máy chủ sẽ mang lại nhiều trường hợp sử dụng và sử dụng hơn.

➢ Serverless Cloud Computing cho phép các nhà phát triển xây dựng, chạy các ứng dụng và dịch vụ mà không phải lo lắng về việc quản lý hoặc vận hành các máy chủ sẽ làm tăng việc sử dụng đám mây và các trường hợp sử dụng đám mây.

➢ Serverless Cloud Computing cũng cải thiện hiệu quả bằng cách cho phép các nhà phát triển kết nối và mở rộng các dịch vụ đám mây để dễ dàng giải quyết các ứng dụng và nhiều trường hợp sử dụng của họ. Cloud Computing Serverless đòi hỏi thời gian và công sức ít hơn, và nó đơn giản hoá việc phát hành các bản cập nhật mới.

7.Xu hướng 7 - Tính toán của Edge ngày càng tăng.

➢ Điện toán ranh giới là phương pháp tối ưu hoá hệ thống điện toán đám mây bằng cách xử lý tính toán dữ liệu tại vùng rìa (biên) của mạng, gần với nguồn dữ liệu nhất.

➢ Edge cần thiết và sẽ gia tăng vào năm 2018 bởi vì nó sẽ được yêu cầu để chạy các dịch vụ thời gian thực vì nó streamlines lưu lượng truy cập từ các thiết bị IoT và cung cấp phân tích dữ liệu địa phương thời gian thực và phân tích.

8. Xu hướng 8 -Hệ thống Container dựa trên đám mây sẽ trở thành dòng chính

➢Gói mây là một dịch vụ sẽ trở thành dòng chính vì nó có thể cung cấp một cơ sở hạ tầng an toàn tốt hơn. Ngoài ra, các hệ thống container dựa trên đám mây là một sự thay thế cho các máy ảo và cho phép các ứng dụng được triển khai một cách nhanh chóng, tin cậy, nhất quán và dễ hiểu cho phép chạy nhanh các tính năng.

Câu 2. Trình bày các chuẩn bảo mật không dây.

Các tổ chức định ra các chuẩn cho mạng WLAN

- ITU-R: International Telecommunication Union-Radiocommunication Sector. Chỉ ra các tần số sóng được sử dụng trong WLAN
- IEEE: Institute of Electrical and Electronic Engineers
  802.11 là tài liệu về các chuẩn kỹ thuật
- Wi-Fi Alliance: Tổ chức phi lợi nhuận. Thúc đẩy sự phát triển của WLAN qua các chứng nhận liên vận hành giữa các hang trên dòng sản phẩm cho WALN

•Có một vài băng tần radio không cần đăng ký tần số khi hoạt động. Chủ đề này mô tả 3 dãy băng tần không cần đăng ký được sử dụng cục bộ trong mạng không dây FCC của tổ chức ITU-R
•Có 3 băng tần không cần đăng ký tần số khi sử dụng: 900 MHz, 2.4 GHz và 5 GHz. Dãy băng tần 900 MHz và 2.4 GHz được biết đến như dãy băng tần dùng cho Công nghiệo, Khoa học và Y tế, trong khi đó dãy băng tần 5 GHz thì thường được biết đến như dãy băng tần UNII (Unlicensed National Information Infrastructure)

So sánh những sự khác biệt giữa những chuẩn trong IEEE 802.11

	802.11b	802.11a	802.11g	
Băng tần	2.4 GHz	5 GHz	2.4 GHz	
Số lượng kênh	3	Up to 23	3	
Truyền phát	Direct Sequence Spread Spectrum (DSSS)	Orthogonal Frequency Division Multiplexing (OFDM)	Direct Sequence Spread Spectrum (DSSS)	Orthogonal Frequency Division Multiplexing (OFDM)
Tốc độ [Mb/s]	1, 2, 5.5, 11	6, 9, 12, 18, 24, 36, 48, 54	1, 2, 5.5, 11	6, 9, 12, 18, 24, 36, 48, 54

•Các tiêu chuẩn của IEEE định nghĩa trên lớp vật lý và phân lớp MAC của lớp liên kết dữ liệu theo tham chiếu trong mô hình OSI. Những chuẩn không dây 802.11 nguyên gốc đã được hoàn tất vào năm 1997. Vào năm 1999 các chuẩn này đã được điều chỉnh lại để tạo ra chuẩn 802.11a/b và sau đó một lần nữa được xác nhận lại ở chuẩn 802.11g vào năm 2003.
•1 kênh truyền và trải dữ liệu qua tất cả các tần số được định nghĩa trên kênh truyền đó.
•Chuẩn IEEE 802.11 chia băng tần ISM 2.4 GHz thành 14 kênh truyền, tuy nhiên một số cơ quan quản lý như FCC sẽ chỉ định kênh truyền nào được sử dụng, ví dụ như việc sử dụng kênh truyền từ số 1 đến 11 tại Mỹ. Mỗi kênh truyền trong dãy băng tần 2.4 GHz có băng thông là 22 MHz và chỉ cách nhau 5 MHz trên phổ tần số, do đó phổ của một kênh truyền sẽ bị chồng một phần với phổ của các kênh truyền liền trước và sau nó. Vì vậy, các kênh truyền cần được cách nhau qua 5 kênh truyền khác đề không xảy ra hiện tượng chồng phổ này. Ví dụ, khi ta sử dụng 11 kênh truyền FCC, có 3 kênh truyền không trùng nhau là: 1, 6 và 11.
•Mạng không dây sử dụng cơ chế truyền bán song công (half-duplex), do vậy thông lượng truyền dẫn cơ bản chỉ vào khoản một nữa tốc độ dữ liệu. Do đó, muc tiêu chính của chuẩn 802.11b là nhằm đạt được tốc độ truyền cao hơn ở băng tần ISM 2.4 GHz để tăng thị phần khách hàng và khuyến khích sự chấo nhận của khách hàng của hệ thống chứng nhận Wi-Fi.
•Chuẩn 802.11b định nghĩa việc sử dụng DSSS với thuật toán điều chế mới CCK (Complementary Code Keying) cho một tốc độ truyền cao hơn là 5.5 và 11 Mbps

trong khi đó vẫn giữ kiểu điều chế cũ Barker ở tốc độ 1 và 2 Mbps. Chuẩn 802.11b vẫn dùng băng tần ISM 2.4 GHz như chuẩn 802.11 trước đo, mục tiêu nhằm đưa vào chuẩn 802.11b khả năng tương thích lùi với chuẩn cũ 802.11 ở tốc độ truyền liên quan là 1 và 2 Mbps.

•IEEE đã phát triển một chuẩn khác là 802.11a. Động cơ thúc đẩy 802.11a là sử dụng một kiểu trải phổ (OFDM – Ortogonal Frequency Division Multiplexing) và công nghệ điều chế tín hiệu khác. 802.11a sử dụng dãy tần số rộng hơn trên dãy tần 5 GHz UNII. Chuẩn 802.11a không được chấp nhận rộng rãi bởi vì các tài liệu để sản xuất các chip hỗ trợ chuẩn 802.11a ít phổ biến và điều này cũng tạo ra tiền đề dẫn đến giá thành cao trong việc phát triển hệ thống mạng sử dụng chuẩn 802.11a.

•Những chuẩn mới đây được phát triển bởi IEEE đều duy trì việc sử dụng chuẩn 802.11 MAC với tốc độ cao hơn trên băng tần ISM 2.4 GHz. IEEE 802.1g ra đời với sự cải thiện việc sử dụng kiểu trải phổ OFDM từ chuẩn 802.11a để đạt được tốc độ cao hơn và tương thích với chuẩn 802.11b sử dụng kiểu trải phổ DSSS. 802.11g hoạt động trên băng tần ISM 2.4 GHz. Tốc độ dữ liệu DSSS là 1, 2, 5.5 và 11Mbps và tốc độ dữ liệu OFDM là 6, 9, 12, 18, 24, 48 và 54Mbps đều được hỗ trợ bởi chuẩn 802.11g. IEEE chỉ yêu cầu trên 3 tốc độ dữ liệu bắt buộc là 6, 12 và 24Mbps mà sẽ không quan tâm đến các thiết bị hỗ trợ chuẩn 802.11a hay 802.11g OFDM.

Dưới đây là một số chuẩn bảo mật không dây quan trọng mà bạn có thể gặp trong lĩnh vực mạng máy tính:

1. **WEP (Wired Equivalent Privacy):**
    - **Mô tả:** WEP là chuẩn bảo mật không dây đầu tiên được sử dụng nhằm bảo vệ dữ liệu truyền qua mạng không dây.
    - **Đặc điểm:**
        - Sử dụng mã hóa RC4 để bảo vệ thông tin.
        - Mặc dù đã được thay thế do lỗ hổng bảo mật, nhưng vẫn có thể gặp trong một số môi trường cũ.
2. **WPA (Wi-Fi Protected Access):**
    - **Mô tả:** WPA được phát triển để thay thế WEP và nâng cao đáng kể tính bảo mật của mạng không dây.
    - **Đặc điểm:**
        - Sử dụng TKIP (Temporal Key Integrity Protocol) để thay đổi khóa mật khẩu theo thời gian.
        - Hỗ trợ chế độ chia sẻ khóa (PSK - Pre-Shared Key) và chế độ chứng nhận máy chủ (Enterprise).
3. **WPA2 (Wi-Fi Protected Access 2):**
    - **Mô tả:** WPA2 là một cải tiến so với WPA, sử dụng mã hóa AES (Advanced Encryption Standard).
    - **Đặc điểm:**

- Sử dụng mã hóa AES thay vì TKIP, nâng cao cường độ bảo mật.
- Hỗ trợ cả chế độ chia sẻ khóa (PSK) và chế độ chứng nhận máy chủ (Enterprise).

4. **WPA3 (Wi-Fi Protected Access 3):**
   - **Mô tả:** WPA3 là phiên bản mới nhất và được thiết kế để cung cấp bảo mật cao hơn so với các phiên bản trước đó.
   - **Đặc điểm:**
     - Chống lại các cuộc tấn công từ điển và brute-force.
     - Cung cấp chức năng chứng thực mạnh mẽ hơn với Simultaneous Authentication of Equals (SAE).
5. **802.11i:**
   - **Mô tả:** 802.11i là tiêu chuẩn chính đằng sau WPA và WPA2.
   - **Đặc điểm:**
     - Sử dụng mã hóa AES để cung cấp bảo mật mạnh mẽ hơn.
     - Được sử dụng trong chế độ WPA3-Personal.
6. **802.1X (WPA3-Enterprise):**
   - **Mô tả:** 802.1X là một tiêu chuẩn chứng thực mạng không dây, thường được sử dụng trong chế độ WPA3-Enterprise.
   - **Đặc điểm:**
     - Sử dụng các phương thức chứng thực như EAP (Extensible Authentication Protocol).
     - Cung cấp mô hình chứng thực mạnh mẽ và linh hoạt.
     -

<u>Câu hỏi 1. Giao thức PPP gồm mấy thành phần? Nêu rõ tên gọi và chức năng của từng thành phần?</u>

Trong mạng máy tính, **Point-toPointProtocol** (hoặc **PPP**) là một giao thức liên kết dữ liệu. Là một giao thức đóng gói ban đầu để mang gói IP trên kết nối điểm nối điểm.Thường được dùng để thiết lập một kết nối trực tiếp giữa 2 nút mạng.
• PPP cũng thiết lập một chuẩn để gán và quản lý IP địa chỉ, đóng gói đồng bộ hoặc bất đồng bộ, ghép kênh nhiều giao thức lớp mạng, cấu hình đường liên kết, kiểm tra chất lượng đường liên kết, phát hiện lỗi, thỏa thuận các tuỳ chọn như khã năng thỏa thuận địa chỉ lớp mạng và cơ chế nén.
PPP có hai thành phần:
• **Link Control Protocol (LCP):** thiết lập, tạo cấu hình, điều chỉnh cấu hình, và hủy bỏ một liên kết, kiểm tra kết nối dữ liệu.
•**Network Control Protocol (NCP):** làm nhiệm vụ thiết lập, điều chỉnh cấu hình và hủy bỏ việc truyền dữ liệu của các giao thức của lớp network khác nhau.
• Cả LCP và NCP đều hoạt động ở lớp 2 Chúng ta có thể cấu hình PPP trong các kiểu kết nối vật lý sau:

➢Asynchronous serial

➢Synchronous serial

➢High-Speed Serial Interface (HSSI)

Câu hỏi 2. Hãy nêu các ưu điểm và khuyết điểm của PSTN?

Public Switch Telephone Network (PSTN)

Mạng cung cấp dịch vụ điện thoại trên toàn cầu. Dùng modem tương tự loại truyền không đồng bộ hay truyền đồng bộ, để kết nối thiết bị mạng vào mạng điện thoại công cộng. Thỉnh thoảng, cần truyền dữ liệu với dung lượng thấp thì có thể sử dụng các modem bất đồng bộ và đường dây điện thoại.

• PSTN cung cấp kết nối theo nhu cầu, dung lượng thấp, thông qua các chuyển mạch dành riêng.

• Hệ thống này truyền tải các cuộc gọi điện thoại bằng tín hiệu analog bằng cáp đồng xoắn từ nhà và văn phòng đến tổng đài, thường được gọi là local loop (vòng lặp cục bộ).

• Khi gọi tín hiệu trong local loop là tín hiệu điện liên tục biến thiên để thể hiện âm thoại. Đường dây này không thích hợp để truyền dữ liệu, do đó một modem được sử dụng để đổi tín hiệu sang dạng có thể truyền trên local loop.

• Băng thông trên các kết nối này là giới hạn, khoảng 33kb/s là tối đa. Tốc độ có thể lên tới khoảng 56kb/s nếu kết nối tới một kết nối digital.

Ưu điểm:

➢Đơn giản

➢Sẵn sàng

➢Chi phí

Khuyết điểm:

➢Tốc độ thấp

➢Thời gian thiết lập kết nối tương đối lâu

Ưu điểm của PSTN:

1. **Đơn giản:**
    - PSTN có cấu trúc đơn giản, điều này làm cho nó dễ triển khai và sử dụng cho người dùng cơ bản mà không cần kiến thức chuyên sâu về công nghệ.
    - Không yêu cầu cài đặt phức tạp, người dùng chỉ cần cắm điện thoại vào đường dây điện thoại và có thể sử dụng ngay lập tức.
2. **Sẵn sàng:**
    - PSTN đã tồn tại và phát triển từ rất lâu, do đó, nó có sẵn ở hầu hết mọi nơi trên thế giới. Người dùng có thể truy cập dịch vụ điện thoại mà không gặp khó khăn về cơ sở hạ tầng.

3. **Chi phí:**
    - So với một số giải pháp mới hơn như VoIP, việc triển khai PSTN có thể có chi phí thấp hơn, đặc biệt là trong các khu vực nơi hạ tầng đã được xây dựng sẵn.

Khuyết điểm của PSTN:

1. **Tốc độ thấp:**
    - Tốc độ truyền dữ liệu trên PSTN giới hạn, thường chỉ đạt tối đa khoảng 33kb/s, và thậm chí có thể thấp hơn đối với một số kết nối analog.
    - Điều này có thể tạo ra hạn chế đối với các ứng dụng đòi hỏi băng thông cao như video call hoặc truyền dữ liệu lớn.
2. **Thời gian thiết lập kết nối tương đối lâu:**
    - Quá trình thiết lập kết nối trên PSTN thường mất một khoảng thời gian đáng kể. Điều này làm cho quá trình kết nối không linh hoạt và đôi khi không hiệu quả đối với các yêu cầu kết nối ngay lập tức.
3. **Giới hạn băng thông:**
    - Băng thông trên các kết nối PSTN giới hạn, điều này có thể tạo ra rắc rối đối với các ứng dụng đòi hỏi băng thông cao như truyền video chất lượng cao hay truyền dữ liệu lớn qua mạng.

Câu 1. Trình bày cơ chế mặc định trên các máy chủ DNS

Phân giải tương tác là quá trình giải quyết tên miền thành địa chỉ IP thông qua sự tương tác giữa máy tính client và máy chủ DNS. Dưới đây là chi tiết về cơ chế mặc định của phân giải tương tác trên các máy chủ DNS:

1. **Yêu cầu Truy vấn:**
    - Khi máy tính (client) muốn biết địa chỉ IP của một tên miền, nó gửi một truy vấn DNS đến máy chủ DNS.
2. **Recursive DNS Query:**
    - Truy vấn thường được thiết lập dưới dạng truy vấn đệ quy, tức là máy chủ DNS sẽ thực hiện mọi bước để giải quyết truy vấn này. Nếu máy chủ DNS không biết câu trả lời, nó sẽ tiếp tục thực hiện truy vấn đệ quy đến khi nó có thể cung cấp câu trả lời hoặc đưa ra mã lỗi nếu không thể tìm thấy thông tin.
3. **Cache Kiểm Tra:**
    - Trước khi thực hiện truy vấn tương tác, máy chủ DNS thường kiểm tra trong cache xem có thông tin về tên miền được yêu cầu không. Nếu có, nó có thể trả lời trực tiếp từ cache mà không cần thực hiện truy vấn trên mạng.
4. **Chuyển Hướng Truy vấn:**

- Nếu cache không có thông tin hoặc nó quá cũ, máy chủ DNS sẽ thực hiện các bước sau:
    - Thực hiện truy vấn đệ quy bắt đầu từ máy chủ DNS gốc (Root DNS Server).
    - Máy chủ DNS gốc sẽ chuyển hướng truy vấn đến máy chủ DNS ở cấp cao hơn, chẳng hạn như Top-Level Domain (TLD) DNS Server.
    - Quá trình chuyển hướng tiếp tục cho đến khi máy chủ DNS cuối cùng có thể cung cấp câu trả lời.

5. **Phản Hồi Câu Trả Lời:**
    - Máy chủ DNS cuối cùng sẽ trả lời máy tính client với địa chỉ IP tương ứng của tên miền được yêu cầu hoặc thông báo rằng không thể tìm thấy thông tin.
6. **Cập Nhật Cache:**
    - Nếu máy chủ DNS cuối

cùng trả lời với thông tin mới, nó sẽ cập nhật cache của mình để lưu trữ thông tin này để sử dụng cho các truy vấn tương tự trong tương lai.

Tóm tắt quy trình:

- Máy chủ DNS client gửi một truy vấn tương tác đến máy chủ DNS.
- Máy chủ DNS kiểm tra cache để xem liệu có thông tin nào sẵn có không.
- Nếu không có trong cache hoặc cache quá cũ, máy chủ DNS thực hiện một truy vấn đệ quy qua nhiều máy chủ DNS từ gốc đến cuối.
- Máy chủ DNS cuối cùng cung cấp câu trả lời cho máy chủ DNS client.
- Máy chủ DNS client nhận câu trả lời và có thể sử dụng nó để thiết lập kết nối với địa chỉ IP tương ứng.
-

Câu 2. Qui trình hoạt động của kết nối HTTP bền vững và không bền vững

Kết nối HTTP: Có hai loại kết nối HTTP là kết nối không bền vững và kết nối bền vững.

- **Kết nối không bền vững:** sau khi, server gửi đi một đối tượng thì kết nối TCP sẽ được đóng. Như vậy, mỗi kết nối TCP chỉ truyền được duy nhất một yêu cầu từ client và nhận lại một thông điệp trả lời từ server.

- **Kết nối bền vững**: server sẽ duy trì kết nối TCP cho việc gửi nhiều đối tượng. Như vậy, sẽ có nhiều yêu cầu từ client được gửi đến server trên cùng một kết nối. Thông thường kết nối TCP này sẽ được đóng lại trong một khoảng thời gian định trước.

Quy trình hoạt động của kết nối HTTP không bền vững:
Bước 1: client khởi tạo kết nối TCP bằng việc gửi yêu cầu đến server. Server nhận được yêu cầu và chấp nhận kết nối bằng việc gửi trả lời về cho client. Nếu sau khoảng thời gian RTT mà không nhận được trả lời từ phía server thì client sẽ gửi lại yêu cầu.
- Bước 2: sau khi kết nối được thiết lập, client sẽ gửi thông điệp yêu cầu chứa tên đường dẫn của các đối tượng (ví dụ: www.hutech.edu.vn/homepage/index.php) đến server. Server nhận được thông điệp yêu cầu và tiến hành lấy ra các đối tượng được yêu cầu. Sau đó, các đối tượng được đóng gói thành thông điệp trả lời và gửi đến client
- Bước 3: server đóng kết nối TCP (Lưu ý: server chỉ đóng kết nối TCP khi chắc chắn rằng client nhận được thông điệp trả lời)
- Bước 4: client nhận thông điệp trả lời chứa tập tin HTML và hiển thị các đối tượng.
- Lưu ý: Trong kết nối HTTP không bền vững cần có một RTT (Round Trip Time) để khởi tạo kết nối TCP. Ngoài ra, cần có một RTT cho thông điệp HTTP yêu cầu và một vài byte đầu tiên của thông điệp HTTP trả lời được trả về.
Tổng thời gian truyền tập tin = 2RTT+ thời gian truyền.
Thời gian đáp ứng RTT là thời gian gửi một gói tin cơ bản từ client đến server rồi quay ngược lại. RTT bao gồm độ trễ truyền gói tin và hàng đợi, độ trễ trong các bộ định tuyến trung gian, chuyển mạch và xử lý gói tin Bước 5: lặp lại các bước từ 1-4 cho các đối tượng khác
Qui trình hoạt động của kết nối HTTP bền vững:
- Kết nối bền vững không có pipelining: Client phát ra yêu cầu mới, chỉ khi đáp ứng trước đó đã nhận xong. RTT cho mỗi đối tượng tham chiếu.
- Kết nối bền vững có pipelining: Mặc định có trong HTTP/1.1. Client gửi yêu cầu ngay sau khi gặp một đối tượng tham chiếu. Ít nhất 1 RTT cho tất cả đối tượng tham chiếu.
Qui trình hoạt động của kết nối HTTP bền vững:
1. Kết nối bền vững không có pipelining:

- **Client Phát Yêu Cầu Mới:**
    - Máy khách (client) gửi một yêu cầu HTTP đến máy chủ (server) qua kết nối TCP đã thiết lập.
- **Đợi Đáp Ứng Trước Đó:**
    - Máy khách chờ đợi đến khi nhận được phản hồi từ máy chủ cho yêu cầu trước đó trước khi gửi yêu cầu mới.
- **Round Trip Time (RTT) Cho Mỗi Đối Tượng Tham Chiếu:**

- Việc đợi đáp ứng từ mỗi yêu cầu gây mất thêm thời gian, còn được biết đến là Round Trip Time (RTT) cho mỗi đối tượng tham chiếu.

2. Kết nối bền vững có pipelining:

- **Pipelining Có sẵn Trong HTTP/1.1:**
  - Pipelining là một tính năng có sẵn trong phiên bản HTTP/1.1, cho phép máy khách gửi nhiều yêu cầu đến máy chủ trước khi nhận được phản hồi từ yêu cầu trước đó.
- **Client Gửi Yêu Cầu Ngay Khi Gặp Đối Tượng Tham Chiếu:**
  - Máy khách không cần phải đợi đến khi nhận được phản hồi từ yêu cầu trước đó, mà có thể tiếp tục gửi yêu cầu mới ngay khi gặp một đối tượng tham chiếu.
- **Ít Nhất 1 RTT Cho Tất Cả Đối Tượng Tham Chiếu:**
  - Mặc dù pipelining giúp giảm thời gian đợi, nhưng vẫn cần ít nhất một Round Trip Time (RTT) cho tất cả các đối tượng tham chiếu được gửi trong một "pipeline" (ống dẫn).

<u>Câu 3. DHCP là gì? Các bước thực hiện DHCP.</u>

- DHCP là giao thức được sử dụng để cấu hình địa chỉ IP cho thiết bị máy tính.
- Khi máy tính lần đầu tiên kết nối tới mạng nội bộ bằng dây cáp hoặc truy cập Wifi, điều đầu tiên nó làm chính là tìm địa chỉ IP, netmask, default gateway và DNS servers

DHCP server có thể có 3 phương thức cấp phát địa chỉ IP:

•**Cấp phát tĩnh:** DHCP server cấp phát một địa chỉ IP dựa trên một bảng với cặp địa chỉ MAC/ địa chỉ IP tương ứng, được điền thủ công và chỉ khi có yêu cầu từ client với địa chỉ MAC được liệt kê bên trong bảng mới được cấp IP.

•**Cấp phát động:** người quản trị mạng sẽ gán một dãy (range) địa chỉ IP tới DHCP, và mỗi máy tính client trong mạng LAN được cấu hình để request một địa chỉ IP từ DHCP server trong quá trình khởi tạo mạng.

•**Cấp phát tự động:** DHCP server gán vĩnh viễn địa chỉ IP tới request client từ dãy địa chỉ IP được quy định bởi người quản trị. Tương tự như cấp phát động, nhưng DHCP server giữ lại bảng chứa các địa chỉ IP được gán trước đó, để nó có thể gán cho client cùng địa chỉ IP mà họ đã request trước đó.

DHCP cung cấp tự động. Một DHCP server cung cấp thông tin này tới DHCP client thông qua 4 bước:

Bước 1: DHCP Discovery Máy tính client sẽ gửi thông điệp broadcast trên physical subnet để tìm server DHCP khả dụng. Máy tính client tạo ra một gói tin UDP đích đến mặc định 255.255.255.255 hoặc địa chỉ broadcast subnet cụ thể nếu được cấu hình.

Bước 2: DHCP offer DHCP server nhận được y/c cấp IP từ client, bảo lưu địa chỉ IP cho client và mở rộng địa chỉ IP sẽ gửi cho client message DHCPOFFER. Thông điệp này chứa địa chỉ MAC của client, địa chỉ IP mà server sẽ cung cấp, subnet mask,
Bước 3: DHCP request Client trả lời DHCP request, gửi tin unicast tới server địa chỉ nằm trong DHCP offser nhận được.
Bước 4: DHCP acknowledgement Khi DHCP server nhận được thông điệp DHCPREQUEST từ client, quá trình cấu bước vào giai đoạn cuối cùng.

Câu 1. Phương thức quản trị tín hiệu truyền trên mạng(CSMA/CD)

Tín hiệu Ethernet được phát từ mỗi máy nối vào mạng, dùng một tập các qui tắc đặc biệt để xác định trạm nào đang phát. Ethernet quản trị tín hiệu trên mạng bằng phương thức Carrier Sense Multiple Access with Collision Detection (CSMA/CD), hình trên minh họa tiến trình CSMA/CD thực hiện. Trong mạng Ethernet, trước khi phát tín hiệu, máy tính phải lắng nghe trên môi trường truyền. Nếu môi trường truyền đang ở trạng thái nghỉ, máy tính sẽ gửi dữ liệu. Sau khi tín hiệu được phát đi, tất cả các máy tính khác trên mạng sẽ cạnh tranh nhau tìm thời gian nghỉ kế tiếp để gửi frame khác. Quá trình cạnh tranh tìm thời gian nghỉ có nghĩa là không có trạm nào có ưu thế hơn các trạm còn lại. Các trạm trên mạng cục bộ CSMA/CD có thể truy cập mạng bất kỳ lúc nào. Trước khi gửi dữ liệu, các trạm CSMA/CD lắng nghe mạng để xác định xem mạng đã được sử dụng hay không. Nếu mạng đang được sử dụng các trạm sẽ phải đợi. Nếu mạng đang rảnh rỗi, các trạm sẽ phát dữ liệu. Đụng độ (collision) xãy ra khi 2 trạm cùng phát dữ liệu một lúc (xem hình). Trong trường hợp đó, cả hai tín hiệu đều bị hỏng, và các trạm phải gửi lại tín hiệu sau đó. Trạm CSMA/CD phải có khả năng phát hiện đụng độ để gửi lại tín hiệu khi cần thiết. Khi một trạm phát, tín hiệu được xem như là carrier. Card mạng sẽ nhận biết được carrier và tư kiềm chế việc phát tín hiệu lên mạng. Nếu không có carrier, một trạm đang đợi sẽ biết rằng đã sẵn sàng để phát tín hiệu. Chức năng này được gọi là nhận diện carrier (“carrier sense”). Toàn bộ phần mạng trên đó xảy ra đụng độ được gọi là miền đụng độ (collision domain). Kích thước miền đụng độ ảnh hưởng đến hiệu năng và thông lượng của mạng Ethernet. Trong tiến trình CSMA/CD, không có độ ưu tiên cho các trạm, vì thế tất cả các trạm trên mạng đều có quyền truy xuất như nhau, vì thế xuất hiện khả năng cùng truy cập (“multiple access”). Nếu có từ 2 trạm trở lên cố gắng phát dữ liệu cùng lúc đụng độ sẽ xảy ra. Khi xảy ra đụng độ các trạm sẽ thực hiện thuật toán backoff sinh ra thời gian chờ ngẫu nhiên trước khi phát lại tín hiệu. Cách làm này sẽ giúp ngăn chặn các máy tiếp tục cố gắng tín hiệu đồng thời đó là kỹ thuật giải quyết đụng độ “collision detection”

Câu 3. Cấu trúc Frame Ethernet:

Các bit nhị phân truyền trên mạng Ethernet được tổ chức thành từng frame. Frame là đơn vị dữ liệu trong ethernet bao gồm thông tin header, thông tin trailer, và nội dung thông tin cần truyền tải.

•**Preamble:** trường thông tin gồm 7 bytes chứa các bit 1, 0 liên tiếp, nó có tác dụng đồng bộ tín hiệu.

•**Bắt đầu frame (Start-of-frame - SOF chỉ có trong 802.3):** Trường thông tin gồm 1 byte có giá trị 10101011, dùng thông báo cho máy nhận biết điểm bắt đầu của Frame.

•**Địa chỉ đích (Destination address):** Trường địa chỉ đích chứa địa chỉ vật lý của card mạng máy nhận.

•**Địa chỉ nguồn (Source address):** Trường địa chỉ nguồn chứa địa chỉ vật lý của card mạng máy gửi.

•**Loại/chiều dài (Type/length):** Trong chuẩn Ethernet II, trường này chứa mã số xác định giao thức lớp mạng. Trong chuẩn 802.3, trường này chứa chiều dài của trường dữ liệu (data). Thông tin về giao thức lớp network chứa trong trường 802.2, lớp LLC chứa 802.2 header và trường dữ liệu.

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

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

Câu 4. Địa chỉ vật lý MAC được ghi trong ROM của card mạng và một số nhà cung cấp cho phép sửa đổi lại giá trị này để phù hợp với nhu cầu cục bộ. Địa chỉ MAC 48-bit gồm 2 thành phần như sau :

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

Broadcast hay multicast bit — Locally administered address bit

•24-bit vendor-assigned end station address

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

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

Câu 2. Mô tả sự khác biệt giữa việc thực thi mạng WLAN và LAN

- Môi trường WLAN, sóng radio được sử dụng tại lớp vật lý (trong mô hình OSI).
- WLAN sử dụng phương thức truy nhập CSMA/CA thay vì CSMA/CD trong mạng LAN Ethernet. Khả năng phát hiện xung đột không được trang bị trong hệ thống WLAN bởi vì một máy khi gởi sẽ không đồng thời nhận tín hiệu vào tại thời điểm đó. Thay vào đó, hệ thống WLAN sử dụng tín hiệu RTS (Ready to send – sẵn sàng gởi) và CTS (Clear to send – sẵn sàng nhận) để tránh xung đột trong quá trình truyền dẫn.
- Định dạng khung dữ liệu mà hệ thống WLAN sử dụng khác định dạng khung dữ liệu trong hệ thống Ethernet LAN. WLANs có thêm một số yêu cầu trên phần định dạng khung lớp 2. Sóng radio sẽ tạo ra một số vấn đề không gặp như trong môi trường LAN.
- Vấn đề kết nối trong mạng WLAN xảy ra thường là liên quan đến vấn đề tầm phủ sóng, quá trình truyền sóng radio, méo dạng sóng và nhiễu từ những dịch vụ không dây hay những hệ thống WLANs khác.
- Vấn đề đảm bảo sự riêng tư cũng là một thử thách bởi sóng radio có thể lọt ra ngoài tầm kiểm soát vật lý. Trong môi trường WLAN, những người dùng di động kết nối với hệ thống mạng thông qua điểm truy cập (Access Point), được xem như tương tự với HUB trong môi trường Ethernet LAN
- Người dùng di động không có kết nối vật lý vào môi trường mạng.
- Những thiết bị di động thường sử dụng pin làm nguồn năng lượng chính.
- WLAN phải tuân theo một số quy định về tần số ở nước sở tại.
- Mục tiêu của việc chuẩn hóa để đưa ra các tiêu chuẩn nhằm giúp mạng WLAN có mặt rộng khắp trên toàn thế giới. Bởi vì mạng WLAN sử dụng tần số radio, do vậy phải tuân theo quy định về tần số và công suất phát ở nước sở tại. Yêu cầu này không xảy ra trong hệ thống mạng LAN có dây.

Câu 1: IPv6 bao gồm bao nhiêu loại? nêu các loại đó?
IPv6 gồm 3 loại: Unicast, Multicast và Anycast.
1. Unicast: Địa chỉ Unicast được sử dụng để phân biệt các host đơn lẻ trên một mạng. Trong mô hình định tuyến,
các gói tin có địa chỉ đích là địa chỉ unicast chỉ được gửi tới một giao diện duy nhất. Địa chỉ unicast được sử dụng trong giao tiếp một – một.
2. Multicast: Đia chỉ Multicast lại sử dụng để phân biệt một nhóm các giao diện mạng cư trú điển hình trong các máy tính phức hợp. Khi một gói dữ liệu được gửi đến địa chỉ multicast thì gói đó được gửi đến tất cả các giao diện mạng trong nhóm Multicast. Địa chỉ multicast được sử dụng trong giao tiếp một – nhiều.
3. Anycast: Giống như các địa chỉ Multicast, các địa chỉ Anycast cũng phân biệt một nhóm cụ thể các giao diện mạng thường cư trú trong các máy tính phức hợp. Địa chỉ anycast cũng xác định tập hợp nhiều giao diện. Tuy nhiên, trong mô hình định tuyến, gói tin có địa chỉ đích anycast chỉ được gửi tới một giao diện duy nhất trong tập hợp. Giao diện đó là giao diện "gần nhất" theo khái niệm của thủ tục định tuyến.
Câu 2:Trình bày các dạng địa chỉ thuộc loại unicast?
Địa chỉ unicast bao gồm năm dạng sau đây: Địa chỉ đặc biệt; Địa chỉ Link-local; Địa chỉ Site-local; Địa chỉ định danh toàn cầu (Global unicast address); Địa chỉ tương thích(Compatibility address).
1. Định dạng địa chỉ Global unicast addresses: GUA là địa chỉ IPv6 toàn cầu (tương tự như địa chỉ public của IPv4). Phạm vi định vị của GUA là toàn hệ thống IPv6 trên thế giới.
- 001: 3 bit đầu luôn có giá trị là 001 (Prefix=2000::/3)
- Global Routing Prefix: gồm 45 bit. Là địa chỉ được cung cấp cho công ty, cơ quan, tập đoàn hay một tổ chức nào đó khi đăng ký địa chỉ IPv6 public.
- Subnet ID: Gồm 16bit, là địa chỉ do các tổ chức tự cấp.
- Interface ID: Gồm 64 bit, là địa chỉ của các interface trong subnet.
2. Link-Local Address (LLA): LLA được sử dụng cho những node trên 1 link duy nhất. Tự động cấu hình, tìm kiếm neighbor. Router không được chuyển tiếp gói tín có địa chỉ nguồn hoặc đích là link-local ra khỏi phạm vi liên kết. Bao gồm các địa chỉ dùng cho các host trong cùng 1 link và quy trình xác định các node (Neighbor Discovery Process), qua đó các node trong cùng link cũng có thể liên lạc với nhau. Phạm vi sử dụng của LLA là trong cùng 1 link (do đó có thể trùng nhau ở link khác). Khi dùng HĐH Windows, LLA được cấp tự động như sau:

- 64 bit đầu có giá trị FE80 là giá trị cố định (Prefix=FE80::/64)
- Interface ID: gồm 64 bit kết hợp cùng địa chỉ MAC.

3. Site Local Addresses (SLA): Một site có thể là một tổ chức hoặc một phần của tổ chức. Một mạng được cấu hình với SLA không đến được các vị trí bên ngoài site. Router biên của site phải giữ lưu lượng sitelocal trong nội bộ site và có trách nhiệm kiểm soát việc quảng bá router. Ngoài site-local FP và interface ID, SLA còn có một trường gọi là subnet ID, và trong SLA không tồn tại TLA hay NLA ID. Những địa chỉ này được thiết kế chỉ trong một site duy nhất, không yêu cầu prefix toàn cầu, và có thể sử dụng lặp lại ở các site khác nhau. Định dạng của SLA được định nghĩa với FP 1111 11011 và theo sau là 38 bit 0, 16 trường subnet, và 64 bit interface ID.

- 1111 1110 11: 10 bit đầu là giá trị cố định (Prefix=FEC0/10).
- Subnet ID: gồm 54 bit dùng để xác định các subnet trong cùng site.
- Interface ID: Gồm 64 bit là địa chỉ của các interface trong subnet.

4. Unique-Local Addresses (ULA): Đối với các tổ chức có nhiều Site, Prefix của SLA có thể bị trùng lặp. Có thể thay thế SLA bằng ULA (RFC 4193), ULA là địa chỉ duy nhất của một Host trong hệ thống có nhiều Site với cấu trúc:

- 1111 110: 7 bit đầu là giá trị cố định FC00/7. L=0: Local. → Prefix = FC00/8.
- Global ID: Địa chỉ site. Có thể gán thêm tuỳ ý.
- Subnet ID: Địa chỉ subnet trong site

5. Địa chỉ đặc biệt: IPv6 sử dụng hai địa chỉ đặc biệt sau đây trong giao tiếp:

- 0:0:0:0:0:0:0:0 hay còn được viết "::" là loại địa chỉ “không định danh” được IPv6 node sử dụng để thể hiện rằng hiện tại nó không có địa chỉ. Địa chỉ “::” được sử dụng làm địa chỉ nguồn cho các gói tin trong quy trình hoạt động của một IPv6 node khi tiến hành kiểm tra xem có một node nào khác trên cùng đường kết nối đã sử dụng địa chỉ IPv6 mà nó đang dự định dùng hay chưa. Địa chỉ này không bao giờ được gắn cho một giao diện hoặc được sử dụng làm địa chỉ đích.
- 0:0:0:0:0:0:0:1 hay "::1" được sử dụng làm địa chỉ xác định giao diện loopback, cho phép một node gửi gói tin cho chính nó, tương đương với địa chỉ 127.0.0.1 của IPv4. Các gói tin có địa chỉ đích ::1 không bao giờ được gửi trên đường kết nối hay chuyển tiếp đi bởi router. Phạm vi của dạng địa chỉ này là phạm vi node.

TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP
THÀNH PHỐ HỒ CHÍ MINH

ĐỀ THI CUỐI KỲ

Lớp/HP: DHTMT15A,B,C/42030010580(1,2,3)

Ngày thi: 20/12/2021

Thời gian làm bài: 05 ngày
(Không kể thời gian phát đề)

Họ và tên thí sinh ……

Đề tiểu luận 1

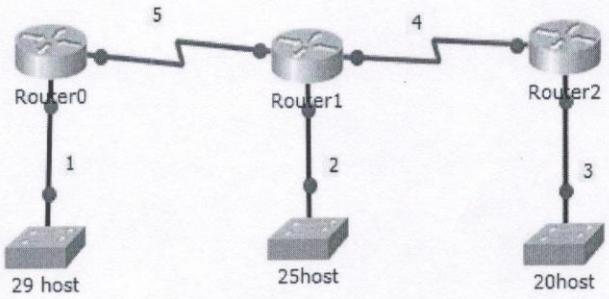
Nội dung: Sinh viên tự thiết kế thống mạng máy tính theo yêu cầu của một tổ chức như: Trường học, doanh nghiệp, cửa hàng, cơ quan ...

Yêu cầu: Sinh viên nộp file pdf đúng hạn.

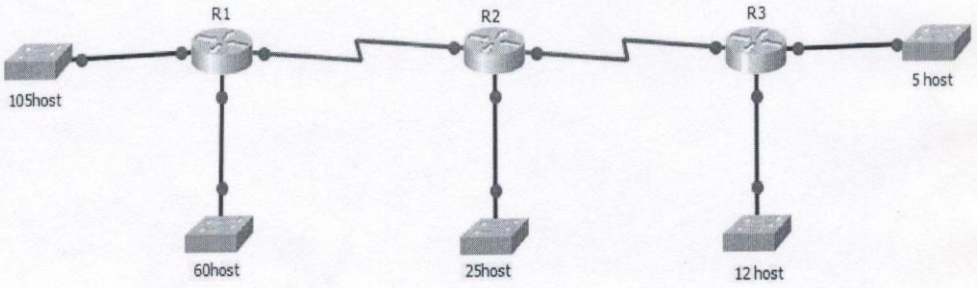
+ Mô tả quá trình phân phối gói tin từ máy đến máy, cho ví dụ minh họa *(2 điểm)*

+ Nêu Cấu trúc Frame Ethernet *(2 điểm)*

+ Sơ đồ mạng và IP như sau: IP 10.10.10.0/24 thực hiên chia IP cho các mạng 1,2,3,4,5 *(2 điểm)*



+ Tổ chức có sơ đồ mạng như sau: có IP : 172.16.100.0/24 *(3 điểm)*



+ Hãy tóm tắt các địa chỉ mạng sau đây về thành một địa chỉ mạng đại diện: *(1điểm)*

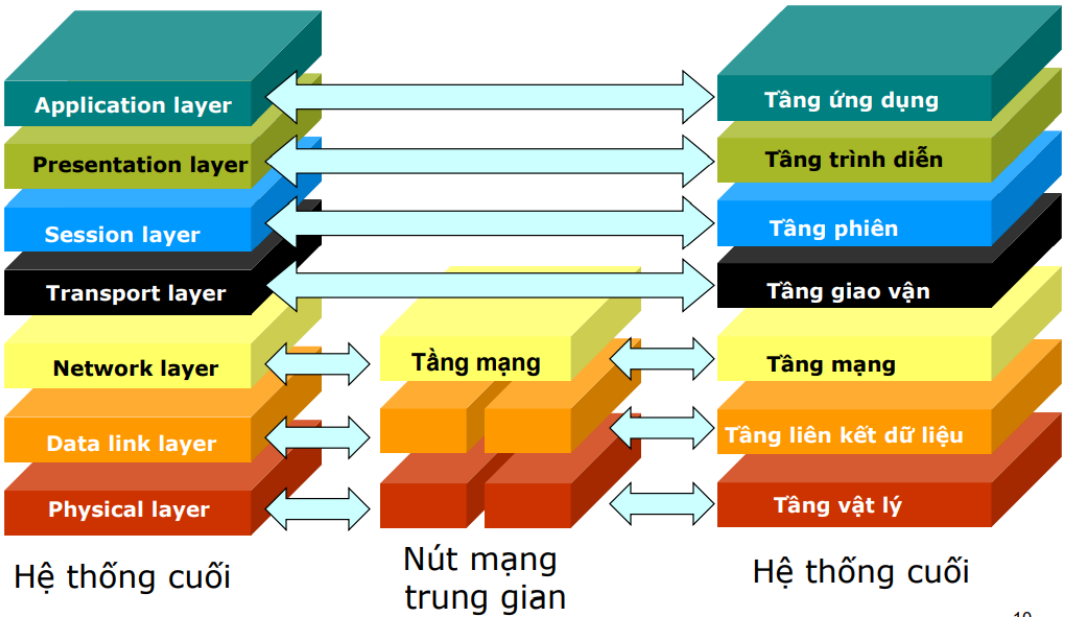
172.16.16.0/24
172.16.20.0.24
172.16.30.0/24
172.16.28.0/24

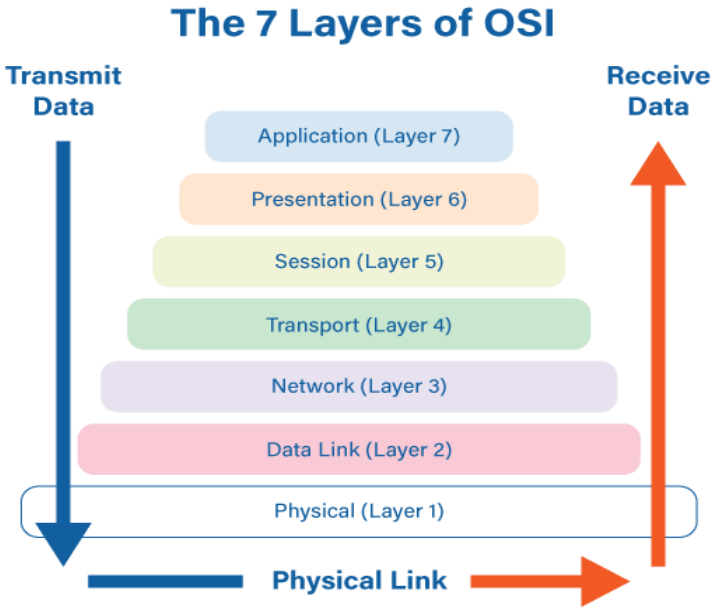
---------- Hết ----------

Lưu ý: - Giáo viên ra đề và trưởng bộ môn ký duyệt vào mặt sau của đề.

BÀI 1: MÔ TẢ QUÁ TRÌNH PHÂN PHỐI GÓI TIN TỪ MÁY ĐẾN MÁY

1.Phân phối gói tin trong mô hình OSI





Sơ lược về mô hình OSI. Mô hình OSI gồm 7 tầng được đánh số thứ tự từ dưới lên trên. Quy trình truyền (Transmit Data) và nhận (Receive Data) trong hình thể hiện khi truyền một gói tin đi, gói tin sẽ đi từ tầng 7 xuống tầng 1 và ngược lại.

Quy trình xử lý dữ liệu trong mô hình OSI

Phía máy gửi:

Ở tầng Application (tầng 7), người dùng tiến hành đưa thông tin cần gửi vào máy tính. Các thông tin này thường có dạng như: hình ảnh, văn bản, v.v…

Sau đó thông tin dữ liệu này được chuyển xuống tầng Presentation (tầng 6) để chuyển các dữ liệu thành một dạng chung để mã hóa dữ liệu và nén dữ liệu.

Dữ liệu tiếp tục được chuyển xuống tầng Session (Tầng 5). Tầng này là tầng phiên có chức năng bổ sung các thông tin cần thiết cho phiên giao dịch (gửi- nhận) này. Các bạn có thể hiêu nôm na là tâng phiên cũng giống như các cô nhân viên ngân hàng làm nhiệm vụ xác nhận, bổ sung thông tin giao dịch khi bạn chuyển tiền tại ngân hàng.

Sau khi tầng Session thực hiện xong nhiệm vụ, nó sẽ tiếp tục chuyển dữ liệu này xuống tầng Transport (Tầng 4). Tại tầng này, dữ liệu được cắt ra thành nhiều Segment và cũng làm nhiệm vụ bổ sung thêm các thông tin về phương thước vận chuyển dữ liệu để đảm bảo tính bảo mật, tin cậy khi truyền trong mô hình mạng.

Tiếp đó, dữ liệu sẽ được chuyển xuống tầng Network (Tầng 3). Ở tầng này, các segment lại tiếp tục được cắt ra thành nhiều gói Package khác nhau và bổ sung thông tin định tuyến. Tầng Network này chức năng chính của nó là định tuyến đường đi cho gói tin chứa dữ liệu.

Dữ liệu tiếp tục được chuyển xuống tầng Data Link (tầng 2). Tại tầng này, mỗi Package sẽ được băm nhỏ ra thành nhiều Frame và bổ sung thêm các thông tin kiểm tra gói tin chứa dữ liệu để kiểm tra ở máy nhận.

Cuối cùng, các Frame này khi chuyển xuống tầng Physical (Tầng 1) sẽ được chuyển thành một chuỗi các bit nhị phân (0 1….) và được đưa lên cũng như phá tín hiệu trên các phương tiện truyền dẫn (dây cáp đồng, cáp quang,…) để truyền dữ liệu đến máy nhận.

Mỗi gói tin dữ liệu khi được đưa xuống các tầng thì được gắn các header của tầng đó, riêng ở tầng 2 (Data Link), gói tin được gắn thêm FCS.

Phía máy nhận:

Tầng Physical (tầng 1) phía máy nhận sẽ kiểm tra quá trình đồng bộ và đưa các chuỗi bit nhị phân nhận được vào vùng đệm. Sau đó gửi thông báo cho tầng Data Link (Tầng 2) rằng dữ liệu đã được nhận.

Tiếp đó tầng Data Link sẽ tiến hành kiểm tra các lỗi trong frame mà bên máy gửi tạo ra bằng cách kiểm tra FCS có trong gói tin được gắn bên phía máy nhận. Nếu có lỗi xảy ra thì frame đó sẽ bị hủy bỏ. Sau đó kiểm tra địa chỉ lớp Data Link (Địa chỉ MAC Address) xem có trùng với địa chỉ của máy nhận hay không. Nếu đúng thì lớp Data Link sẽ thực hiện gỡ bỏ Header của tầng Data Link để tiếp tục chuyển lên tầng Network.

Tầng Network sẽ tiến hành kiểm tra xem địa chỉ trong gói tin này có phải là địa chỉ của máy nhận hay không. (Lưu ý: địa chỉ ở tầng này là địa chỉ IP). Nếu đúng địa chỉ máy nhận, tầng Network sẽ gỡ bỏ Header của nó và tiếp tục chuyển đến tầng Transport để tiếp tục qui trình.

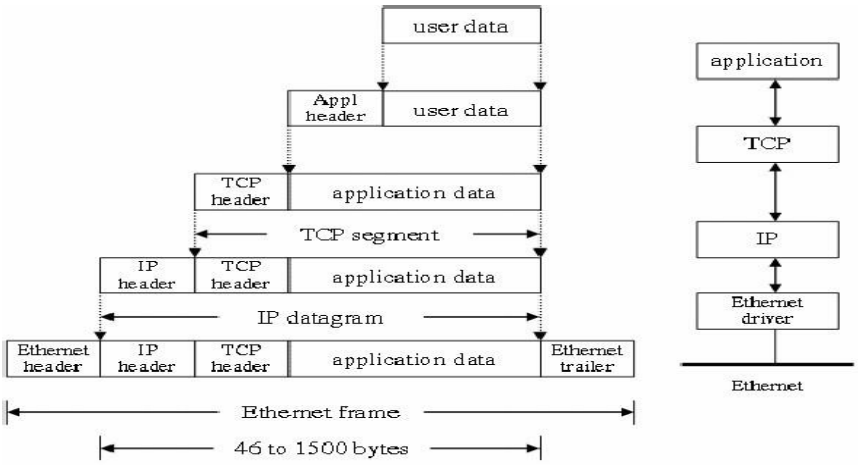
Ở tầng Transport sẽ hỗ trợ phục hồi lỗi và xử lý lỗi bằng cách gửi các gói tin ACK, NAK (gói tin dùng để phản hồi xem các gói tin chứa dữ liệu đã được gửi đến máy nhận hay chưa?). Sau khi phục hồi sửa lỗi, tầng này tiếp tục sắp xếp các thứ tự phân đoạn và đưa dữ liệu đến tầng Session.

Tầng Session làm nhiệm vụ đảm bảo các dữ liệu trong gói tin nhận được toàn vẹn. Sau đó tiến hành gỡ bỏ Header của tầng Session và tiếp tục gửi lên ầng Presentation.

Tầng Presentation sẽ xử lý gói tin bằng cách chuyển đối các định dạng dữ liệu cho phù hợp. Sau khi hoàn thành sẽ tiến hành gửi lên tầng Application.

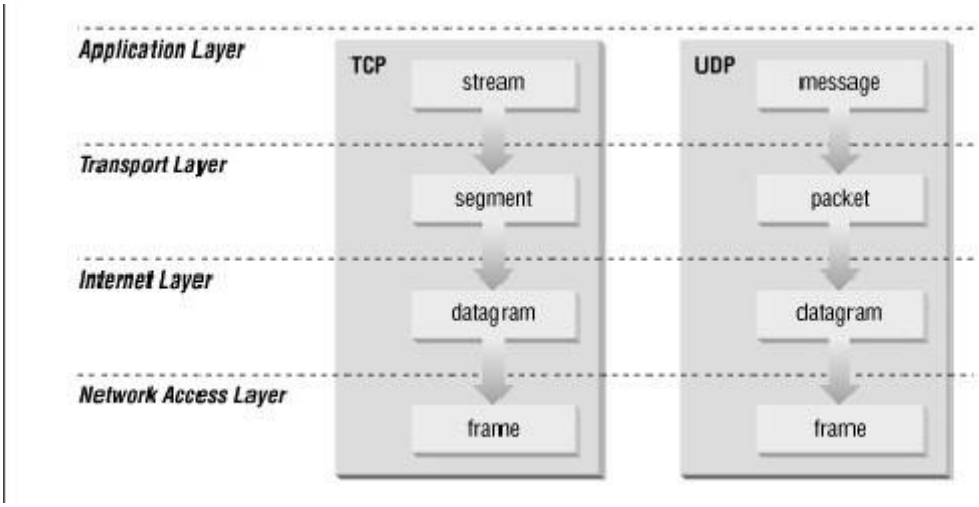
Cuối cùng, tầng Application tiến hành xử lý và gỡ bỏ Header cuối cùng. Khi đó ở máy nhận sẽ nhận được dữ liệu của gói tin được truyền đi.

2.Phân phối gói tin trong mô hình TCP/IP



Quá trình đóng gói dữ liệu trong mô hình TCP/IP

Cũng tương tự như trong mô hình OSI, khi truyền dữ liệu , quá trình tiến hành từ tầng trên xuống tầng dưới, qua mỗi tầng dữ liệu được them vào thông tin điều khiển gọi là Header. Khi nhận dữ liệu thì quá trình xảy ra ngược lại. dữ liệu được truyền từ tấng dưới lên và qua mỗi tầng thì phần header tương ứng sẽ được lấy đi và khi đến tầng trên cùng thì dữ liệu không còn phần header nữa.



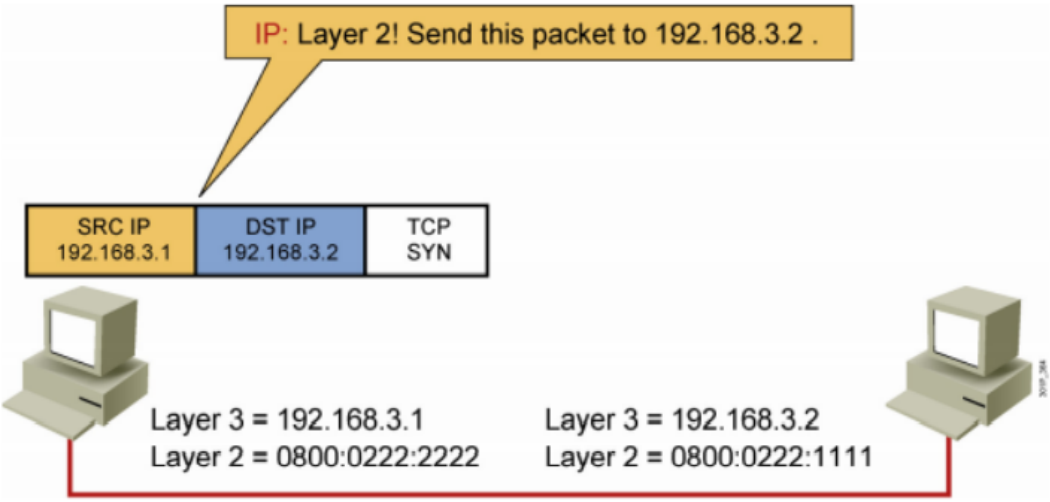
Cấu trúc dữ liệu trong TCP/IP

Hình trên cho ta thấy lược đồ dữ liệu qua các tầng. Trong hình ta thấy tại các tầng khác nhau dữ liệu được mang những thuật ngữ khác nhau o Trong tầng ứng dụng: dữ liệu là các luồng được gọi là stream. o Trong tầng giao vận: đơn vị dữ liệu mà TCP gửi xuống gọi là TCP segment. o Trong tầng mạng, dữ liệu mà IP gửi xuống tầng dưới gọi là IP Datagram o Trong tầng liên kết, dữ liệu được truyền đi gọi là frame

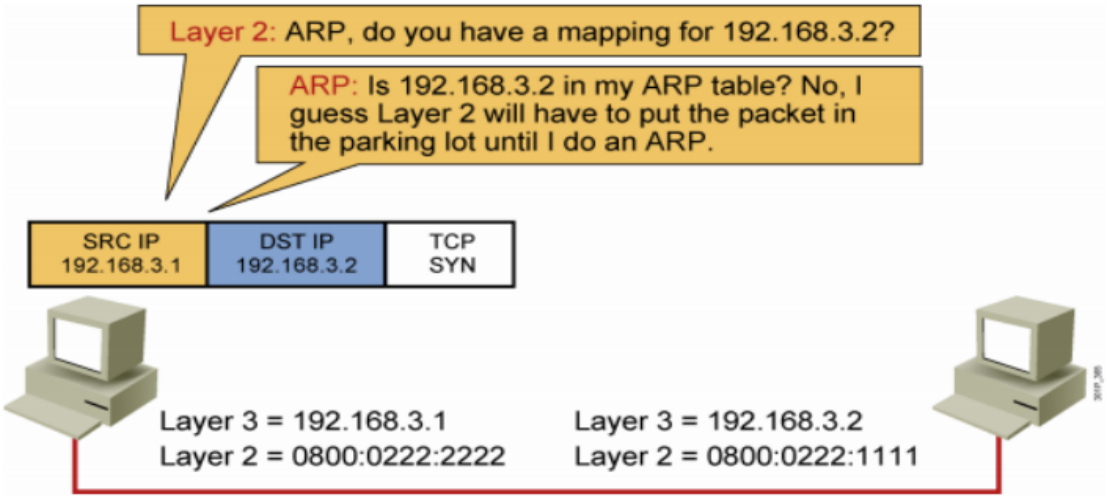
3. Ví dụ về phân phối gói tin từ máy đến máy

VD: Một ứng dụng trên máy tính 192.168.3.1 muốn gửi dữ liệu qua máy có địa chỉ là 192.168.3.2

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

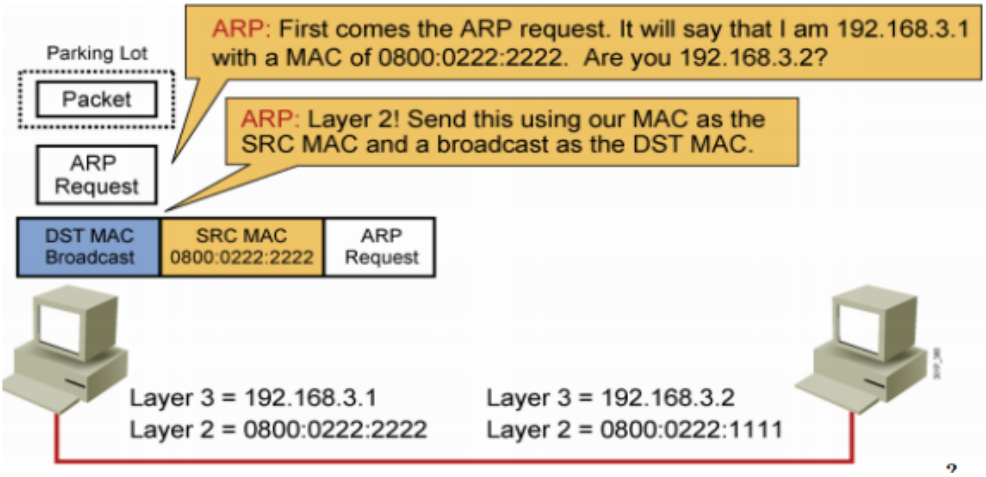


- Lớp IP đóng gói dữ liệu SYN của TCP vào gói tin bằng cách gắn thêm vào phía trước dữ liệu TCP địa chỉ lớp 3 của máy gửi sau đó gửi qua lớp 2 để xử lý tiếp.



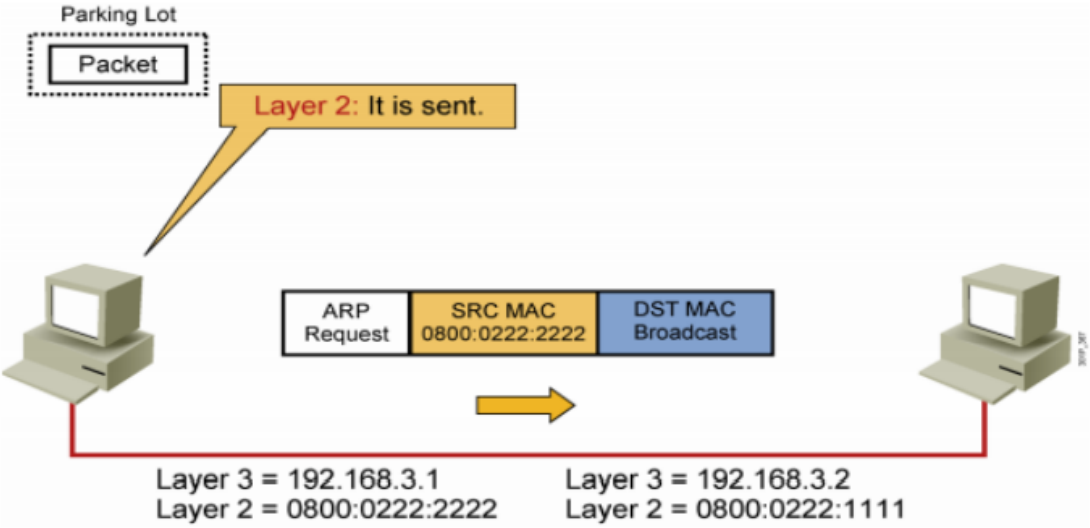
- Lớp 2 đóng gói dữ liệu lớp 3 (IP packet) vào trong Frame lớp 2. Lớp 2 gửi yêu cầu đến ARP để ánh xạ địa chỉ IP – MAC của máy đích.

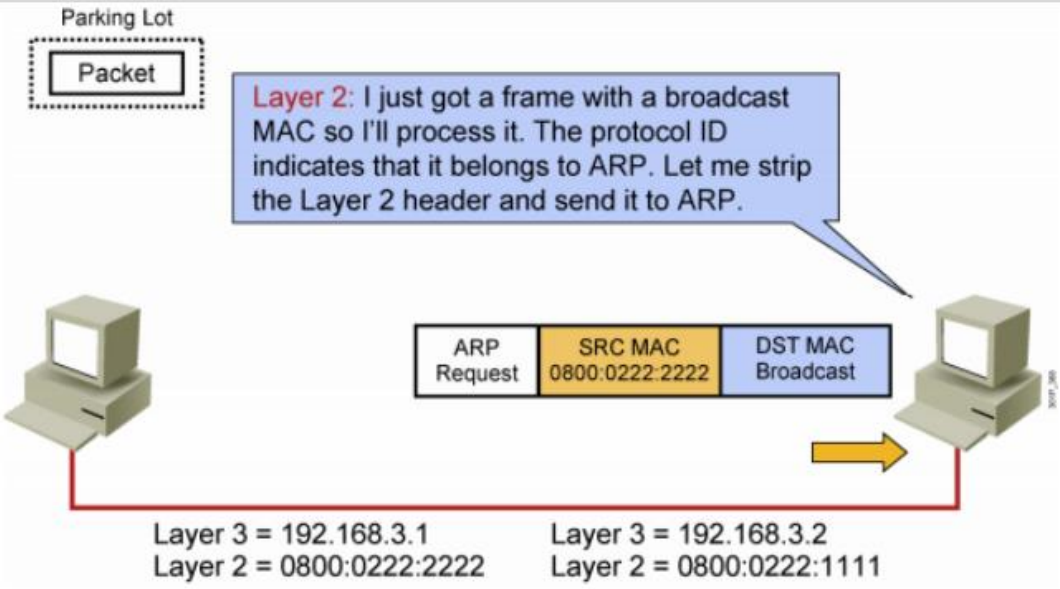
- ARP kiểm tra cache của mình. Nếu máy này chưa bao giờ giao tiếp với máy khác thì lớp 2 sẽ giữ lại gói tin đến khi ánh xạ ARP được tạo ra vì ARP hiện tại đang rỗng.



- ARP xây dựng gói tin ARP Request và chuyển cho lớp 2, yêu cầu lớp 2 gửi lại thông tin với địa chỉ đích boardcast.

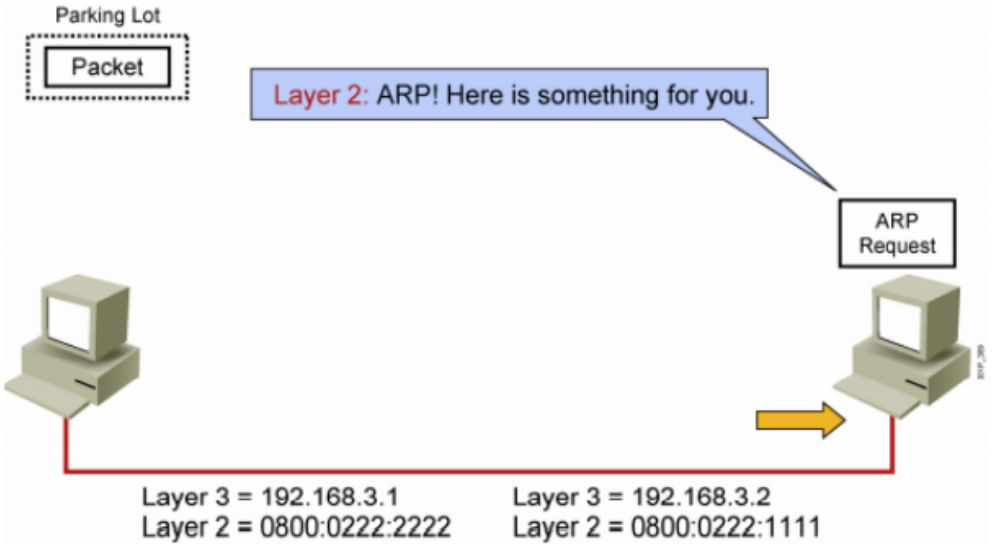
- Lớp 2 đóng gói ARP Request trong frame lớp 2 dùng địa chỉ MAC đích là boardcast, và địa chỉ MAC nguồn của máy yêu cầu phân giải.

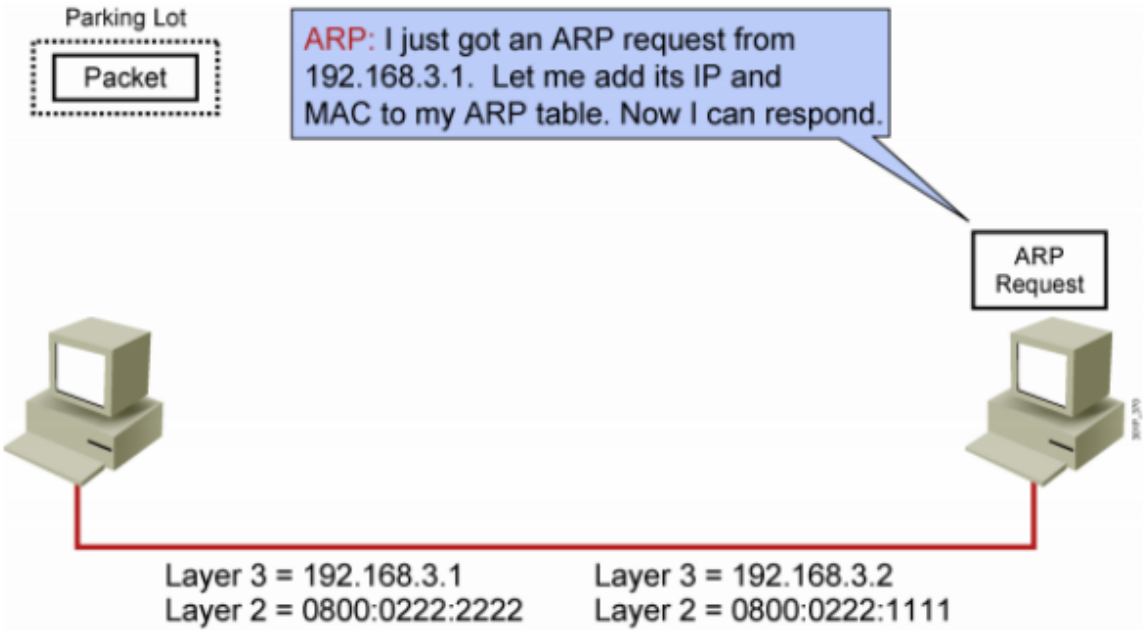




- Khi máy 192.168.3.2 nhận được frame, nó sẽ lưu ý địa chỉ boardcast và thực hiện đóng gói frame lớp 2.

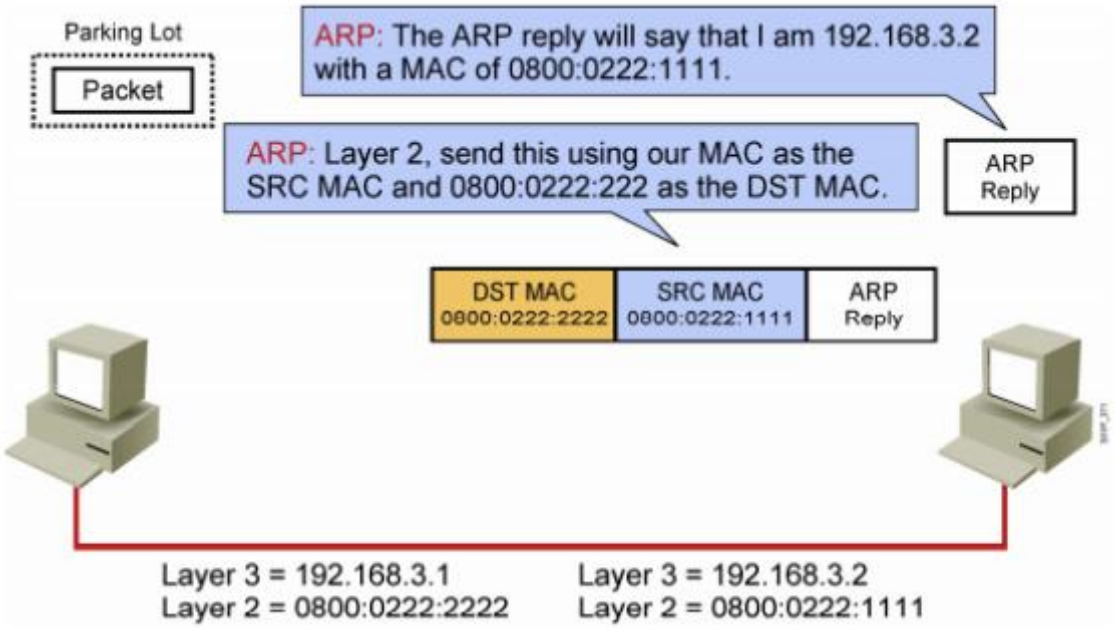
- Thông tin ARP Request được chuyển đến cho chương trình ARP.

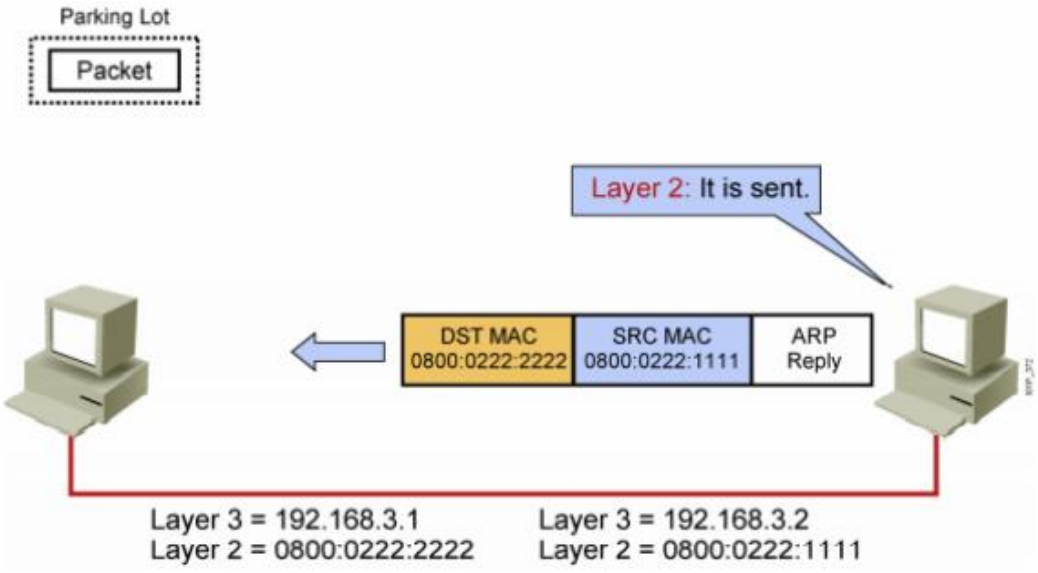




- Sử dụng thông tin ARP Request, chương trình ARP cập nhật bảng cache của nó.

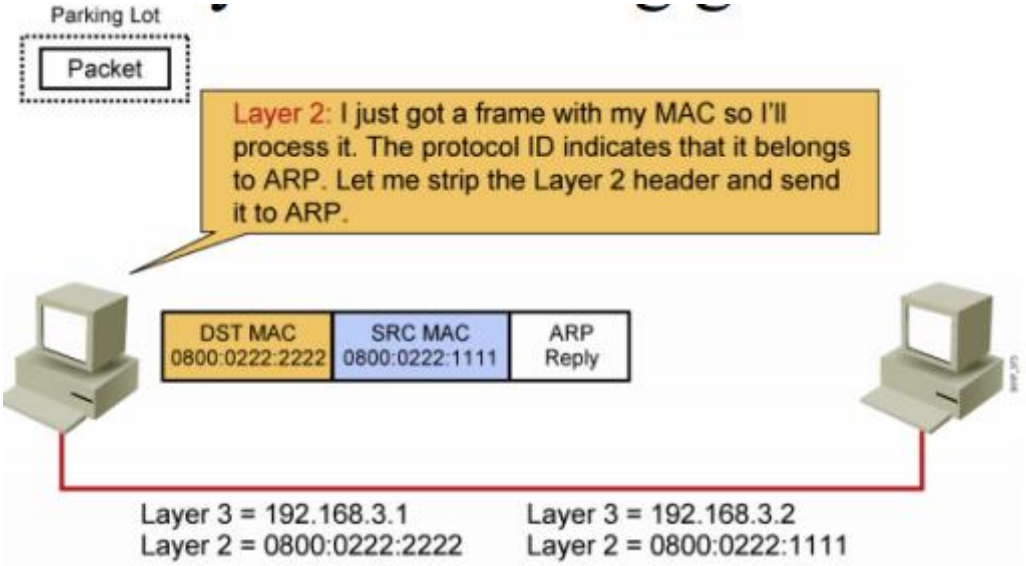
- Chương trình ARP xây dựng gói tin ARP Reply và gửi cho lớp 2, yêu cầu lớp 2 gửi đến địa chỉ MAC 0800:0222:2222 (IP: 192.168.3.1)

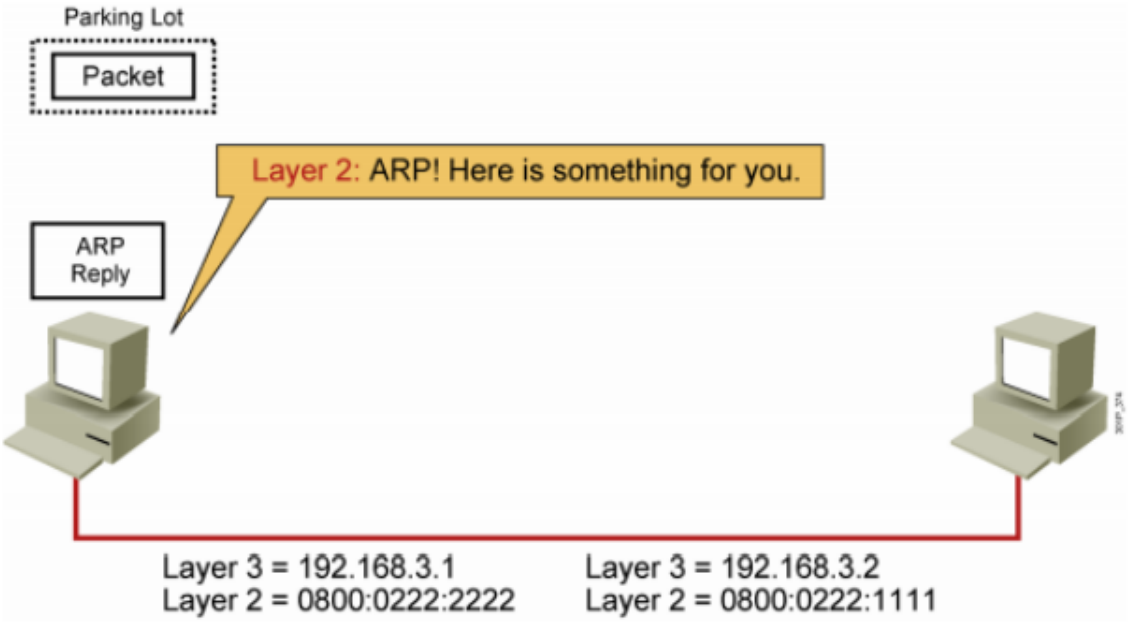




- Lớp 2 đóng gói ARP Reply vào frame lớp 2 với địa chỉ MAC đích cung cấp bởi bảng ARP và địa chỉ nguồn máy gửi.

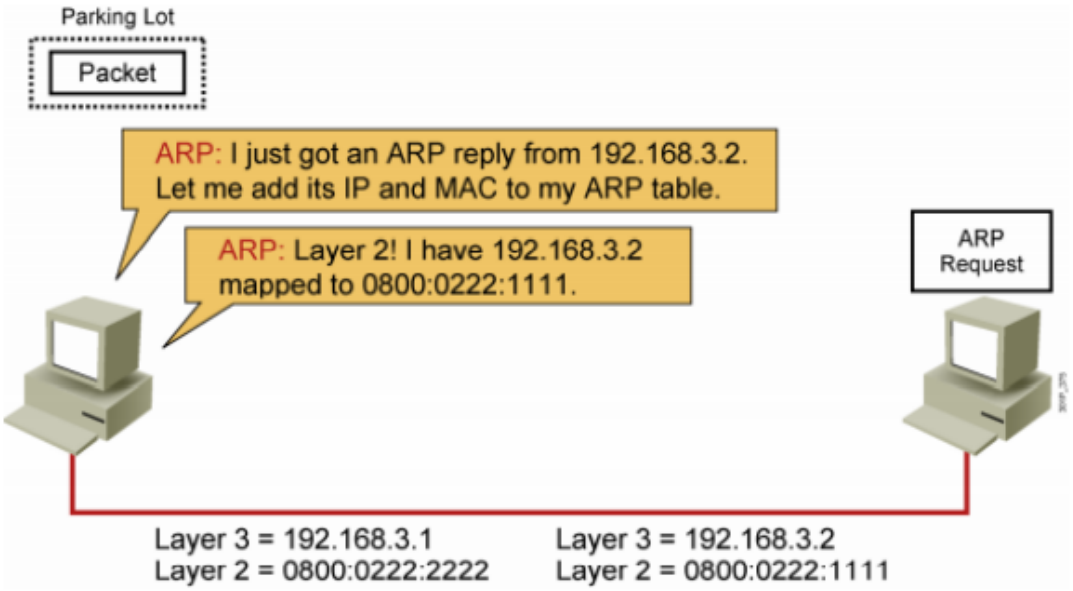
- Khi máy 192.168.3.1 nhận được frame, nó lưu ý đến địa chỉ MAC đích của nó. Máy đích sẽ đóng gói frame lớp 2.

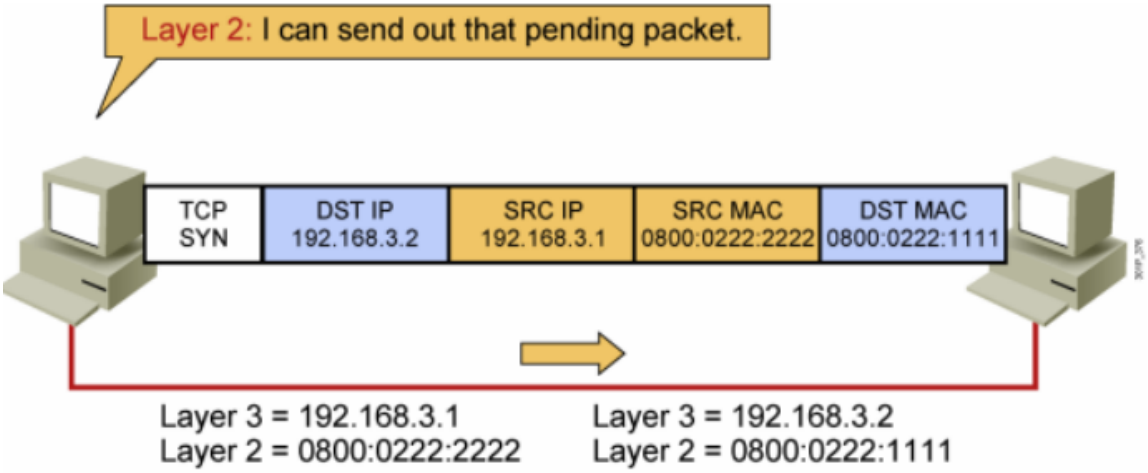




- Phần thông tin ARP reply sẽ được chuyển đến cho chương trình ARP.

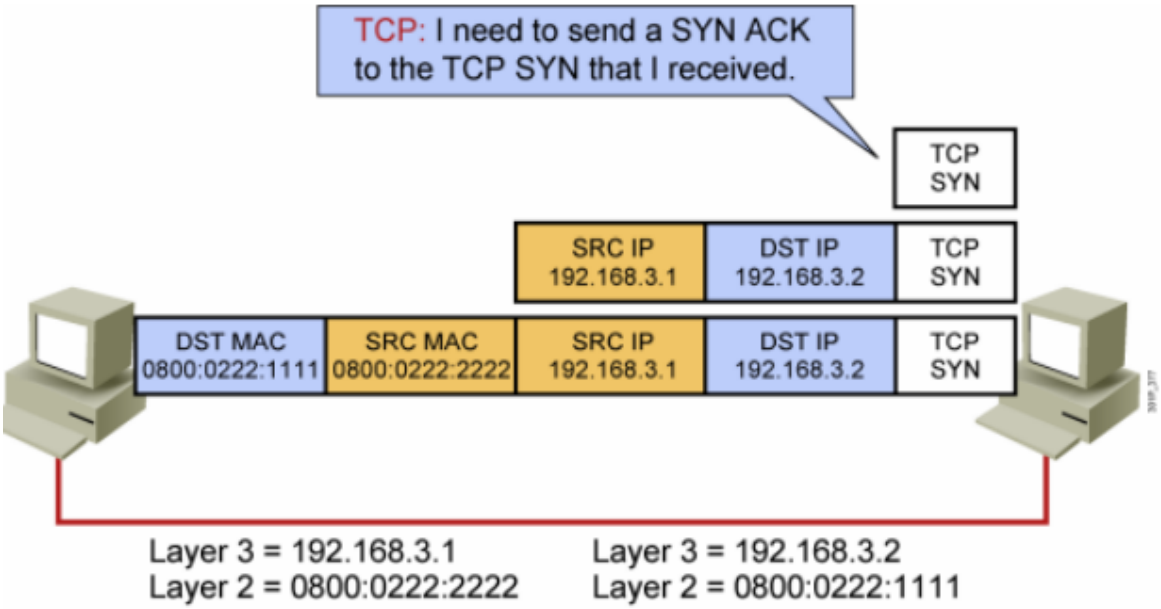
- ARP thực hiện cập nhật bảng cache ánh xạ IP – MAC tương ứng.

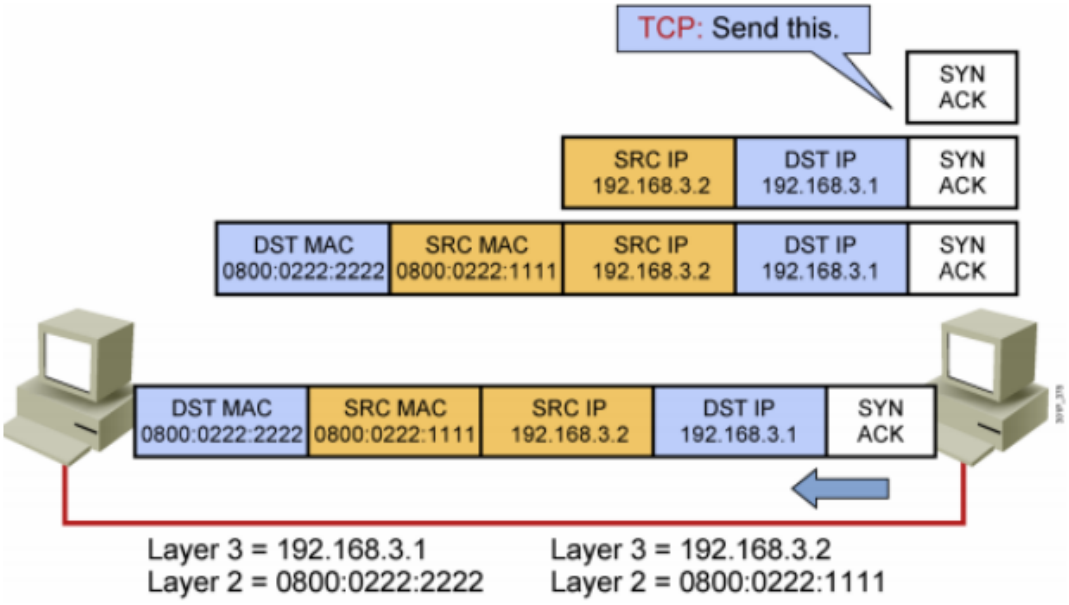




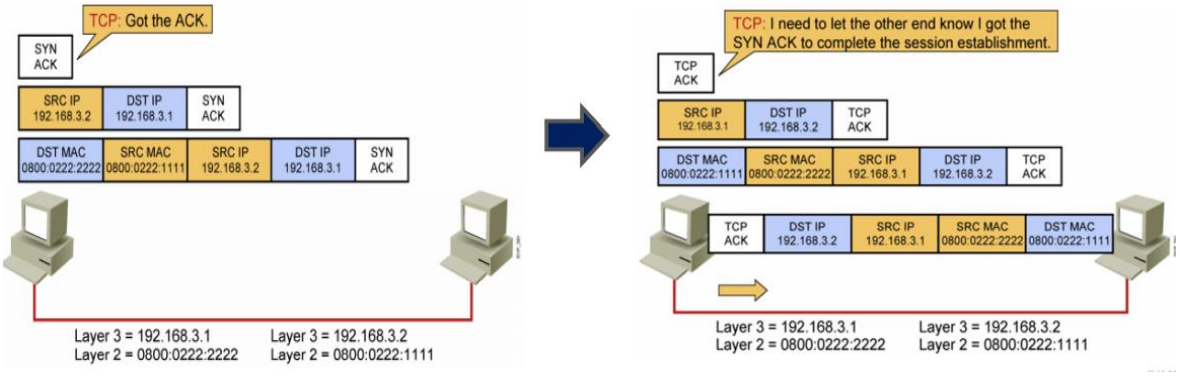
- Lớp 2 giờ có thể gửi gói tin treo lúc nãy.

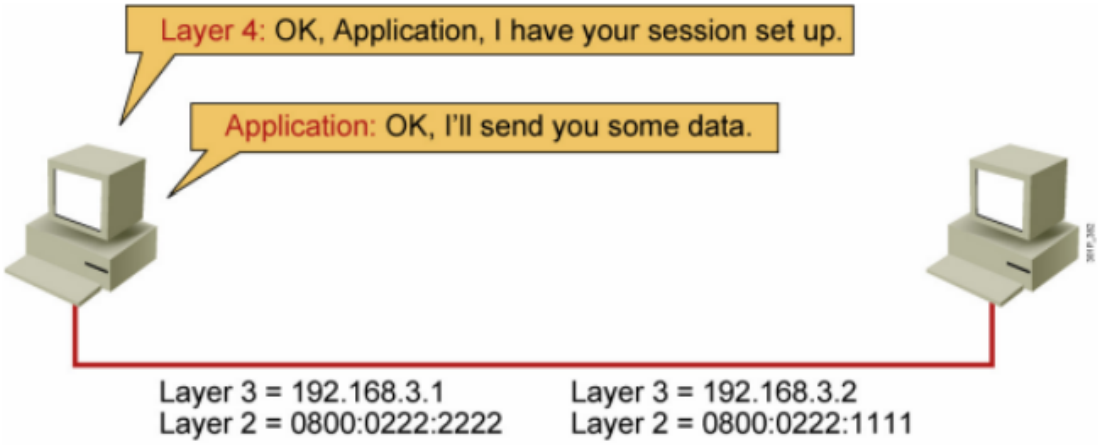
- Ở máy 192.168.3.2, frame được chuyển lên cho các lớp phía trên (giải đóng gói dữ liệu). Phần PDU tương ứng còn lại được chuyển cho TCP.





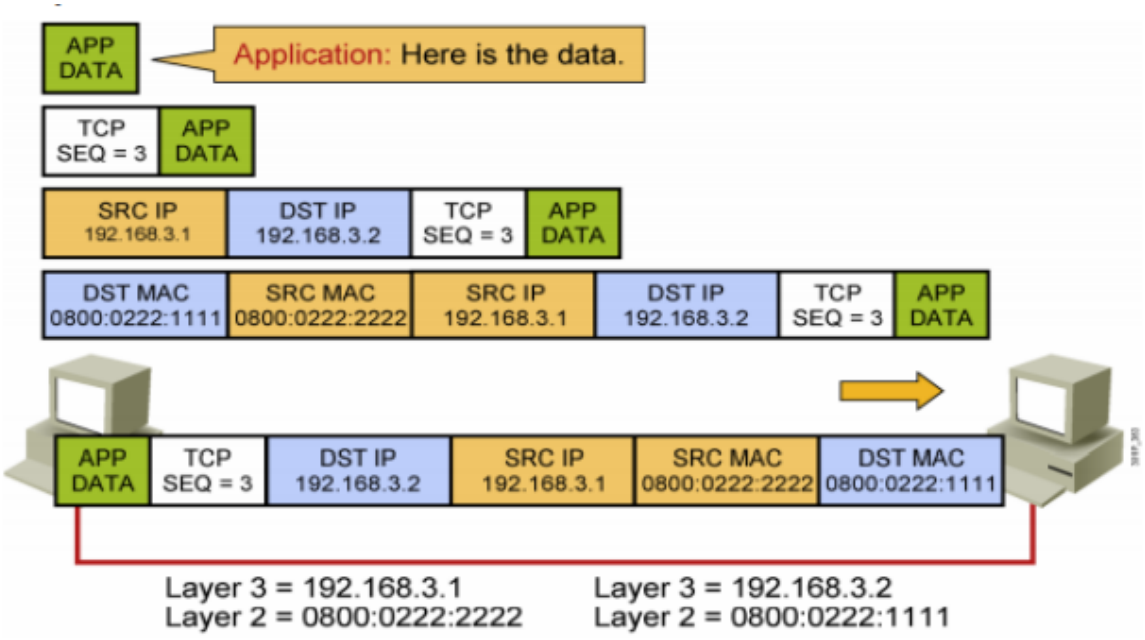
- Để trả lời cho SYN, TCP chuyển dữ liệu SYN ACK xuống cho các lớp bên dưới thực hiện việc đóng gói.



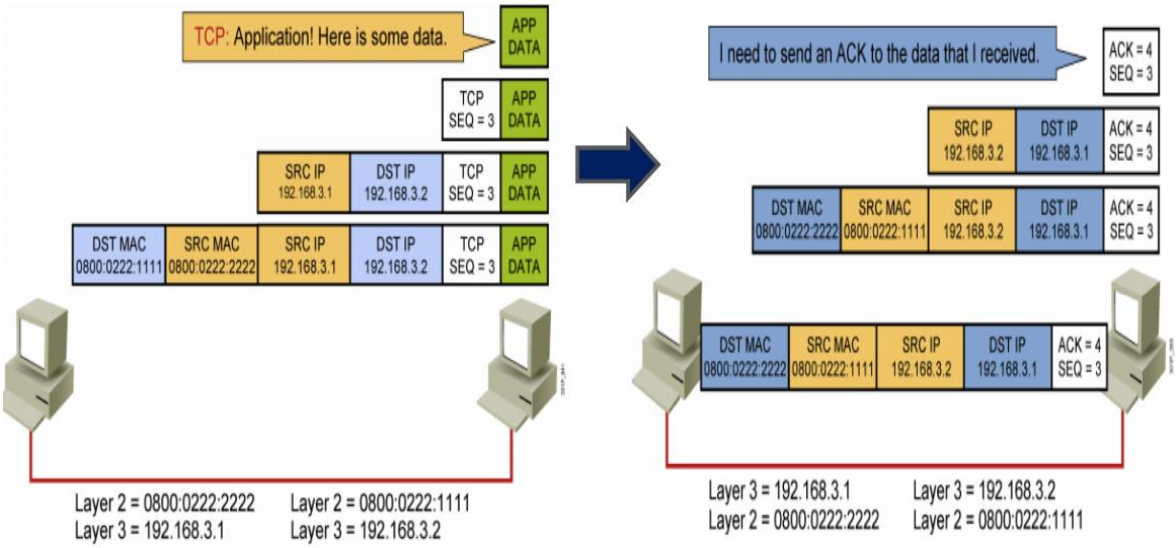


- Khi quá trình bắt tay 3 bước (three – way handshake), TCP có thể báo cho ứng dụng biết rằng phiên truyền thông (session) đã được thiết lập.

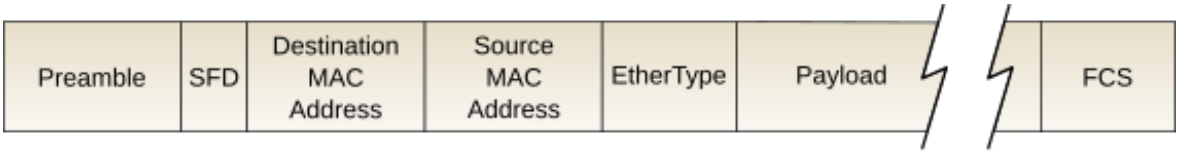
- Bây giờ ứng dụng có thể gửi dữ liệu thông qua phiên truyền thông dựa trên TCP để sửa các lỗi nếu có.



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



Câu 2: Nêu cấu trúc Frame Ethernet



1. Packet Ethernet – tầng vật lý

Preamble và start frame delimiter

Một packet Ethernet bắt đầu bởi một preamble dài 7 octet và một *start frame delimiter* (SFD) dài một octet.

Preamble chứa một pattern bit dài 56– bit (bảy– byte) gồm các bit 1 và 0 xen kẽ nhau, cho phép các thiết bị trên mạng dễ dàng đồng bộ clock receiver của chúng, cung cấp đồng bộ hóa ở mức bit. Nó được theo sau bởi SFD để cung cấp đồng bộ hóa ở mức byte và để đánh dấu một frame mới đang đến. Đối với các phương án Ethernet truyền các bit tuần tự thay vì các symbol lớn hơn, pattern bit trên– đường– dây (không được mã hóa) dành cho preamble cùng với phần SFD của frame là 10101010 10101010 10101010 10101010 10101010 10101010 10101010 10101011; bởi vì các bit được truyền với thứ tự từ trái sang phải, biểu diễn hexadecimal tương ứng là 0xAA 0xAA 0xAA 0xAA 0xAA 0xAA 0xAA 0xAB.

SFD là giá trị 8– bit (một byte) đánh dấu kết thúc của preamble, trường đầu tiên của một packet Ethernet, và chỉ ra điểm bắt đầu của một frame Ethernet. SFD được thiết kế để phá vỡ pattern bit của preamble và đánh tín hiệu sự bắt đầu của một frame thực sự. Địa chỉ MAC của đích theo ngay sau SFD. Đây là trường đầu tiên của một frame Ethernet. SFD có giá trị 171 (10101011 ở dạng nhị phân), được truyền với least– significant bit đi trước tiên như 213 (0xD5 hexadecimal).

Physical layer transceiver circuitry (viết tắt: PHY) cần phải kết nối Ethernet MAC với medium vật lý. Kết nối giữa một PHY và MAC độc lập với medium vật lý và sử dụng một bus từ họ giao diện độc lập media (MII, GMII, RGMII, SGMII, XGMII). Các chip transceiver Fast Ethernet sử dụng bus MII, một bus rộng 4– bit (một

nibble), do đó preamble được biểu diễn bởi 14 lần 0x5, và SFD là 0x5 0xD (như các nibble). Các chip transceiver Gigabit Ethernet sử dụng bus GMII, một giao diện rộng 8– bit, vì thế chuỗi preamble theo sau bởi SFD sẽ là 0xAA 0xAA 0xAA 0xAA 0xAA 0xAA 0xAA 0xAB (như các byte).

2. Frame – Tầng liên kết dữ liệu

Header

Header gồm có địa chỉ MAC nguồn và đích (mỗi địa chỉ dài 6 octet), trường EtherType và một tag IEEE 802.1Q tùy chọn.

Trường EtherType dài hai octet và có thể dùng cho nhiều mục đích khác nhau. Giá trị nhỏ hơn hoặc bằng 1500 có nghĩa là nó được dùng để chỉ kích thước của payload bằng octet, còn giá trị lớn hơn hoặc bằng 1536 có nghĩa là nó được dùng để chỉ kiểu EtherType, xác định procol nào được đóng gói trong payload của frame. Khi được dùng với tư cách là EtherType, chiều dài của frame được xác định bởi vị trí của interpacket gap và frame check sequence (FCS) hợp lệ.

Tag IEEE 802.1Q, nếu có, là một trường dài 4– octet chỉ thành viên mạng virtual LAN (VLAN) và quyền ưu tiên IEEE 802.1p.

Payload

Payload minimum là 42 octet khi có một tag 802.1Q và 46 octet khi không có tag. Payload maximum là 1500 octet. Các jumbo frame (frame ngoại cỡ) phi tiêu chuẩn cho phép kích thước payload lớn hơn kích thước maximum.

Frame check sequence

Frame check sequence (FCS, chuỗi kiểm tra frame) là một cyclic redundancy check (CRC) dài 4 octet cho phép phát hiện dữ liệu bị hỏng bên trong toàn bộ frame khi nhận ở phía receiver. Giá trị FCS được tính như một hàm số của các trường frame MAC được bảo vệ: địa chỉ nguồn, địa chỉ đích, trường độ dài/kiểu, dữ liệu client MAC và padding (có nghĩa là, tất cả các trường trừ FCS).

Chạy thuật toán CRC trên dữ liệu frame đã nhận được bao gồm mã CRC sẽ luôn có kết quả là một giá trị 0 nếu như dữ liệu nhận được không có lỗi, bởi vì CRC là số dư

của dữ liệu chia bởi đa thức. Tuy nhiên, kĩ thuật này có thể có kết quả là các "false negative" (phủ định sai), trong đó dữ liệu với các trailing zero cũng sẽ có kết quả trong số dư cùng zero. Để tránh trường hợp này, FCS được complement (bổ sung) (dự trữ cho mỗi bit) bởi sender trước khi nó gắn vào đuôi của dữ liệu payload. Nếu làm theo cách này thì thuật toán sẽ luôn luôn có kết quả là một *magic number* (số huyền bí) hoặc *CRC32 residue* của 0xC704DD7B khi dữ liệu được nhận một cách chính xác. Điều này cho phép nhận frame và xác nhận FCS mà không cần biết trường FCS thực sự bắt đầu ở đâu.

3. End of frame – tầng vật lý

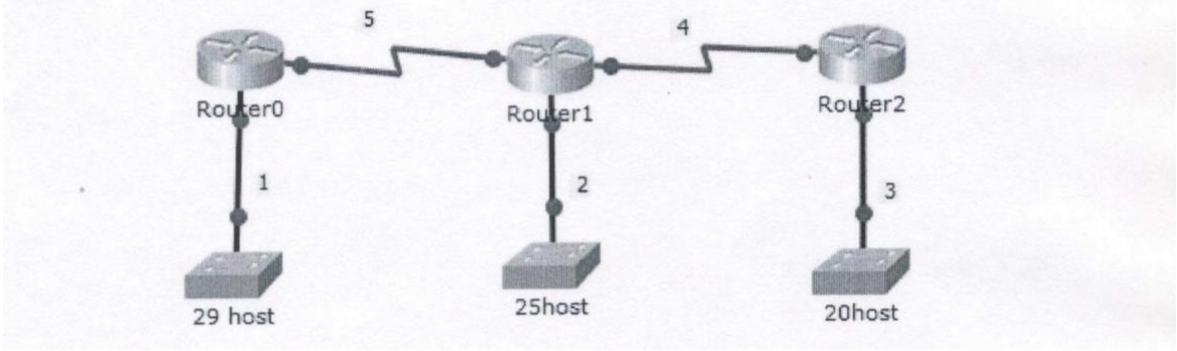
End of a frame (kết thúc frame) thường được biểu thị bằng một symbol (kí hiệu) end– of– data– stream ở tầng vật lý hoặc bởi sự mất mát của tín hiệu mang (carrier signal); một ví dụ là 10BASE–T, trong đó station nhận phát hiện được kết thúc của một frame đã gửi. Sau đó tầng vật lý sử dụng một symbol *end of data* rõ ràng hoặc một symbol/chuỗi *end of stream* để tránh sự mơ hồ về nghĩa, đặc biệt khi carrier được gửi liên tục giữa các frame; một ví dụ là Gigabit Ethernet với sơ đồ mã (encoding scheme) 8b/10b, các sơ đồ này sử dụng các symbol đặc biệt được truyền đi trước và sau khi một frame được truyền.

4. Interpacket gap – tầng vật lý

Interpacket gap là khoảng thời gian nhàn rỗi giữa hai packet. Sau khi một packet đã được gửi đi, các transmitter cần phải truyền ít nhất 96 bit (12 octet) của idle line state (trạng thái dây rảnh) trước khi truyền packet tiếp theo.

Câu 3:

- Sơ đồ mạng và IP như sau: IP 10.10.10.0/24 thực hiên chia IP cho các mạng 1,2,3,4,5 *(2 điểm)*



Ta có tất cả 5 mạng, mạng nhiều host nhất là mạng có 30 host (cộng thêm địa chỉ cổng router). Gọi số bit mượng là n, số bit host là m. Ta có hệ sau:

$2^n >= 5$ (số mạng chia ra tối thiểu phải bằng 5)

$2^m - 2 >= 30$ (nếu mỗi mạng con đáp ứng được về số host của mạng 30 host, nó sẽ đáp ứng được yêu câu về số host của tất cả các mạng con còn lại trên sơ đồ)

m + n = 8

⇨ m = 5, n = 3 là phù hợp. Vậy ta có tất cả $2^3 = 8$ mạng và mỗi mạng này có $2^5 - 2 = 30$ host đáp ứng như câu trên.

M1: 10.10.10.0/27 → 10.10.10.31/27

M2: 10.10.10.32/27 → 10.10.10.63/27

M3: 10.10.10.64/27 → 10.10.10.95/27

M4: 10.10.10.96/27 → 10.10.10.127/27

M5: 10.10.10.128/27 → 10.10.10.159/27

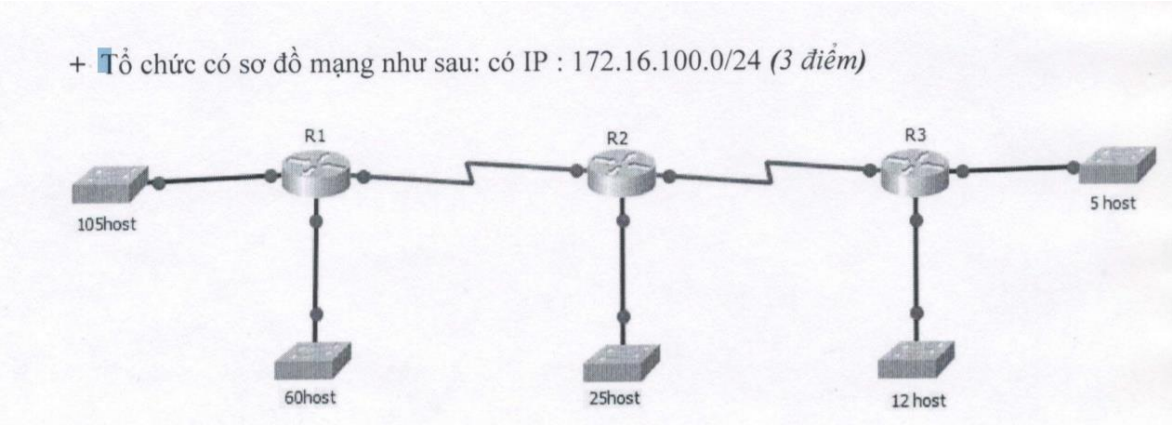
M6: 10.10.10.160/27 → 10.10.10.191/27

M7: 10.10.10.192/27→10.10.10.223/27

M8: 10.10.10.224/27 → 10.10.10.255/27

Vậy ta chọn các mạng M1, M2, M3, M4, M5 để gán cho các mạng 1, 2, 3, 4, 5 trên sơ đồ

Câu 4 :



› xét mạng 105 host

$2^m - 2 >= 106$

m + n = 8 (với m: số bit host, n: số bit mượn)

m = 7, n = 1 vậy ta mượn 1 bit sẽ chia 172.16.100.0/24 thành 2 con

//Các mạng m đều thiếu kí hiệu mạng 1: 172.16.100.0/25 → 172.16.100.127/25

// chứ không phải để không không v 172.16.100.0/25 → 172.16.100.127/25 nhớ sửa ở dưới hết luôn kí hiệu ở mạng 1: 172.16.100.0/25 → 172.16.100.127/25 phải giống với kí hiệu chỗ kết luận chọn mạng để gán => đặt tên cho địa chỉ mạng

1: 172.16.100.0/25 → 172.16.100.127/25

2: 172.16.100.128/25 → 172.16.100.255/25

► **Vậy ta chọn mạng 1 để gán cho mạng 105 host**

› xét mạng 60 host

$2^m - 2 >= 61$

m + n = 8 (với m: số bit host, n: số bit mượn)

m = 6, n = 2 vậy ta mượn 2 bit sẽ chia 172.16.100.0/24 thành 4 con

1: 172.16.100.0/26 → 172.16.100.63/26

2: 172.16.100.64/26 → 172.16.100.127/26

3: 172.16.100.128/26 → 172.16.100.191/26

4: 172.16.100.192/26 → 172.16.100.255/26

► **Vậy ta chọn mạng 3 để gán cho mạng 60 host**

› xét mạng 25 host

$2^m - 2 >= 26$

m + n = 8 (với m: số bit host, n: số bit mượn)

m = 5, n = 3 vậy ta mượn 3 bit sẽ chia 172.16.100.0/24 thành 8 con

1: 172.16.100.0/27 → 172.16.100.31/27

2: 172.16.100.32/27 → 172.16.100.63/27

3: 172.16.100.64/27 → 172.16.100.95/27

4: 172.16.100.96/27 → 172.16.100.127/27

5: 172.16.100.128/27 → 172.16.100.159/27

6: 172.16.100.160/27 → 172.16.100.191/27

7: 172.16.100.192/27→ 172.16.100.223/27

8: 172.16.100.224/27 → 172.16.100.255/27

► Vậy ta chọn mạng 7 để gán cho mạng 25 host

› xét mạng 12 host

$2^m – 2 >= 13$

m + n = 8 (với m: số bit host, n: số bit mượn)

m = 4, n = 4 vậy ta mượn 4 bit sẽ chia 172.16.100.0/24 thành 16 con

1: 1172.16.100.0/28 → 172.16.100.15/28

…….

15: 172.16.100.224/28 → 172.16.100.239/28

16: 172.16.100.240/28 → 172.16.100.255/28

► Vậy ta chọn mạng 15 để gán cho mạng 12 host

› Xét mạng có 5 host

$2^m – 2 >= 6$

m + n = 8 (với m: số bit host, n: số bit mượn)

m =3 n =5 vậy ta mượn 5 bit sẽ chia 172.16.100.0/24 thành 32 mạng con

1: 172.16.100.0/29 → 172.16.100.7/29

…….

31: 172.16.100.240/29 → 172.16.100.247/29

32: 172.16.100.248/29 → 172.16.100.255/29

► Vậy ta chọn mạng 31 để gán cho mạng 5 host

› Xét mạng có 2 host

$2^m - 2 >= 2$

m + n = 8 (với m: số bit host, n: số bit mượn)

m =2 n =6 vậy ta mượn 6 bit sẽ chia 172.16.100.0/24 thành 64 mạng con

1: 172.16.100.0/30 → 172.16.100.3/30

…………

63: 172.16.100.248/30 → 172.16.100.251/30

64: 172.16.100.252/30 → 172.16.100.255/30

► Vậy ta chọn mạng 63, mạng 64 để gán cho 2 mạng 2 host

Câu 5:

+ Hãy tóm tắt các địa chỉ mạng sau đây về thành một địa chỉ mạng đại diện: *(1điểm)*

172.16.16.0/24

172.16.20.0.24

172.16.30.0/24

172.16.28.0/24

------------------------ Hết -----------------------------

172.16.16.0/24 → 172.16.00010000.0/24

172.16.20.0/24 → 172.16.00010100.0/24

172.16.30.0/24 → 172.16.00011110.0/24

172.16.28.0/24 → 172.16.00011100.0/24

– –

172.16.00010000.0/20

Ta thấy tại octet thứ 3 có thêm 4 bit giống nhau. Vậy ta có mạng tóm tắt là 172.16.0.0/20 → subnet 255.255.240.0

Kiểm tra:

172.16.16.0/24 → 172.16.00010000.0

AND 172.16.11110000.0

– – – – – – – – – – – – – – – – – – –

172.16.00010000.0