Mạng cáp xoắn (twisted pair): Một hạ tầng truyền dẫn phổ biến được sử dụng trong mạng máy tính, sử dụng đôi dây đồng xoắn để truyền dữ liệu./- Tạo thành bằng cách quấn lẫn nhau hai sợi dây đồng để giảm nhiễu từ các nguồn tạp âm bên ngoài.- Cáp xoắn có thể chia làm hai loại: cáp xoắn đơn (unshielded twisted pair - UTP) và cáp xoắn chống nhiễu (shielded twisted pair - STP)./- Cáp xoắn được sử dụng trong các mạng LAN, như Ethernet và phân loại theo tốc độ truyền dữ liệu, từ 100Mbps đến 10Gbps.- Khoảng cách trung bình của các cáp xoắn là khoảng 100m
Mạng wireless LAN: Mạng không dây sử dụng sóng radio hoặc sóng hồng ngoại để kết nối các thiết bị trong mạng.- Mạng wireless LAN cho phép các thiết bị di động kết nối và truy cập vào mạng mà không cần sử dụng cáp vật lý.-Sử dụng các tiêu chuẩn như Wi-Fi (Wireless Fidelity) để đảm bảo tương thích giữa các thiết bị khác nhau.- Các thiết bị WLAN cần được kết nối với một (access point) để truyền và nhận dữ liệu.
Mạng cáp quang (fiber optics): Cáp truyền dẫn tín hiệu quang, có tốc độ truyền dữ liệu rất cao, khả năng chống nhiễu tốt và khoảng cách truyền dẫn xa. Cáp quang được sử dụng rộng rãi trong các mạng truyền dẫn dữ liệu dài hạn, như mạng truyền dẫn quốc tế, mạng truyền dẫn Internet và mạng cáp quang tốc độ cao (FTTH - Fiber to the Home), sử dụng cho các ứng dụng yêu cầu băng thông lớn và chất lượng cao, như truyền thanh, truyền hình, internet, camera quan sát,…Cáp quang có thể chia làm hai loại: Single-mode fiber (SMF) chi cho phép một chùm ánh sáng đi qua và Multi-mode fiber (MMF) cho phép nhiều chùm ánh sáng đi qua.
Data-Link Thuộc lớp thứ 2 trong mô hình OSI 7 lớp; Đóng vai trò truyền thông tin giữa 2 máy với nhau; Chức năng: Đóng khung; Kiểm soát luồng và lỗi; Kiểm soát nghẽn mạng. Data link layer **LLC** cung cấp một giao thức điều khiển liên kết dữ liệu duy nhất cho tất cả các mạng IEEE LAN. **MAC** - cung cấp các giao thức và cơ chế khác nhau cho các mạng LAN khác nhau nhằm tránh xung đột.
Chức năng chính IP: Phân đoạn và ghép nối dữ liệu, Định tuyến, Kiểm tra tổng hợp: Lớp IP sử dụng kiểm tra tổng hợp để phát hiện lỗi truyền tải dữ liệu.
Giao thức MAC nào được ứng dụng chóng xung đột mạng **3G/4G, CDMA (Code Division Multiple Access):** Sử dụng mã hóa để phân biệt các tín hiệu từ các thiết bị di động khác nhau. Mỗi thiết bị di động được gán một mã duy nhất, và tín hiệu của nó được mã hóa bằng mã này trước khi truyền. Khi nhiều thiết bị di động truyền cùng lúc, tín hiệu của chúng được cộng lại tại trạm gốc. Trạm gốc sau đó có thể giải mã tín hiệu bằng cách sử dụng mã tương ứng với mỗi thiết bị di động. **FDMA (Frequency Division Multiple Access):** Chia kênh truyền tin thành nhiều kênh con nhỏ hơn. Mỗi thiết bị di động được gán một kênh con riêng để truyền dữ liệu của mình. Điều này giúp ngăn chặn xung đột dữ liệu vì các thiết bị di động chỉ có thể truyền trên kênh con được gán cho chúng.
HDLC là gì? Protocol layer 2 (data link layer); Sử dụng để giao tiếp point-to-point và multipoint; Có thể truyền half-duplex và full-duplex; Sử dụng cơ chế ARQ để kiểm soát luồng; Sử dụng để nền tảng nhiều protocol phổ biến;Tiêu chuẩn sử dụng: ISO/IEC 13239:2000 **NRM:** Địa chỉ lúc nào cũng là một máy sơ cấp, dùng để phân biệt các máy sơ cấp **ABM**: Địa chỉ là địa chỉ máy cần được nhận dùng để phân biệt máy nhận frame
Frame relay là công nghệ mạch ảo (virtual-circuit) mạng WAN để đáp ứng nhu cầu lớn hơn về mạng WAN: Truyền dữ liệu tốc độ cao (1.544 Mbps và gần đây 44.376 Mbps); Cho phép truyền dữ liệu đồng loạt (bursty data); Chi phí thấp Tuy nhiên Frame Relay dần thay thế bởi mạng riêng ảo VPN vì Tốc độ cao hơn; Hỗ trợ làm việc từ xa; Tăng cường an ninh mạng
Giao thức MAC (truy cập ngẫu nhiên: ALOHA; CSMA; tcập có kiểm soát: Reservation; Polling; Token – passing; Phân kênh: FDMA;TDMA;CDMA)
Hãy mô tả các giao thức ALOHA, CSMA, CDMA và phân tích sự khác biệt của chúng. ALOHA: là một giao thức truyền thông không đồng bộ được sử dụng trong các mạng truyền thông không dây.
Pure ALOHA: các nút trong mạng có thể truyền dữ liệu vào bất kỳ thời điểm nào. Nếu hai hoặc nhiều nút truyền cùng một lúc và gây xung đột, thì các nút sẽ phát hiện xung đột và thực hiện việc truyền lại sau một khoảng thời gian ngẫu nhiên. Giao thức này đơn giản và dễ triển khai, nhưng hiệu suất truyền tải không cao. **Slotted ALOHA:** được thiết kế để cải thiện hiệu suất của Pure ALOHA. Trong Slotted ALOHA, các khung dữ liệu được chia thành các khe thời gian cố định và các nút chỉ truyền vào các khe thời gian cụ thể. Điều này giúp giảm xung đột và tăng hiệu suất truyền tải.
CSMA là một giao thức truyền thông chia sẻ kênh, nơi các nút kiểm tra trạng thái của kênh trước khi truyền dữ liệu. **CSMA/CA**: trước khi truyền dữ liệu, các nút kiểm tra xem kênh truyền có sẵn hay không. Nếu kênh đang được sử dụng, nút sẽ đợi một khoảng thời gian ngẫu nhiên trước khi kiểm tra lại. Khi kênh trống, nút mới truyền dữ liệu. Thường được sử dụng trong mạng không dây, nơi xung đột không thể hoàn toàn tránh được. **CSMA/CD**: các nút kiểm tra trạng thái của kênh trước khi truyền dữ liệu, tuy nhiên, nếu hai nút truyền cùng một lúc và xảy ra xung đột, các nút sẽ phát hiện xung đột và ngừng truyền dữ liệu ngay lập tức. Sau đó, các nút sẽ chờ một khoảng thời gian ngẫu nhiên trước khi thử lại. Thường được sử dụng trong mạng Ethernet có cáp đồng trục.
CDMA (Code Division Multiple Access): CDMA sử dụng mã hóa để phân biệt các tín hiệu từ các thiết bị di động khác nhau. Mỗi thiết bị được gán một mã duy nhất, và tín hiệu của nó được mã hóa bằng mã này trước khi truyền. Khi nhiều thiết bị di động truyền cùng lúc, tín hiệu của chúng được cộng lại tại trạm gốc. Trạm gốc sau đó có thể giải mã tín hiệu bằng cách sử dụng mã tương ứng với mỗi thiết bị di động. CDMA được sử dụng trong mạng 3G CDMA2000 và 1xRTT.
FDMA(Frequency-Division Multiple Access): Đây là phương thức truy cập kênh trong đó băng thông của kênh được chia thành nhiều dải tần số cho nhiều người dùng. Mỗi người dùng được cấp một dải tần số riêng để truyền dữ liệu và dải tần số đó được giữ cho người dùng đó suốt thời gian kết nối. FDMA có thể được sử dụng với cả tín hiệu analog và số nhưng thường được sử dụng với tín hiệu analog. FDMA yêu cầu các bộ lọc hiệu suất cao trong phần cứng vô tuyến, khác với TDMA và CDMA. FDMA không bị ảnh hưởng bởi các vấn đề về đồng bộ hóa mà TDMA gặp phải.
TDMA(Time-Division Multiple Access): đây là phương thức truy cập kênh trong đó băng thông của kênh được chia thành nhiều khoảng thời gian cho nhiều người dùng. Mỗi người dùng chỉ có thể truyền dữ liệu trong khoảng thời gian được phân bổ cho họ. TDMA yêu cầu đồng bộ hóa giữa các người dùng để tránh xung đột. TDMA được sử dụng làm phương thức truy cập trong nhiều tiêu chuẩn điện thoại di động như GSM, D-AMPS và PDC. TDMA có ưu điểm là khả năng hỗ trợ nhiều người dùng trên cùng một kênh, khả năng giảm thiểu suy hao công suất và khả năng tương thích với các hệ thống analog.
Loop trên mạng Ethernet xảy ra khi có một kết nối vòng lặp trong hệ thống mạng, khiến các gói tin truyền đi trong vòng lặp liên tục và không thể đến được đích. Khi loop xảy ra, gói tin sẽ được sao chép và lan truyền trong vòng lặp, gây tăng đáng kể lưu lượng mạng và gây hiện tượng treo hoặc hóng hóc mạng. Vấn đề loop trong mạng nội bộ xảy ra khi có nhiều đường dẫn giữa các thiết bị mạng, và các gói dữ liệu bắt đầu lặp vô hạn trong mạng. Loop có thể dẫn đến nhiều vấn đề: mất mát dữ liệu; quá tải các phần tử mạng như Switch, router, giảm hiệu suất
Để khắc phục hiện tượng loop trên mạng Ethernet, có thể sử dụng các phương pháp sau:
1.Spanning Tree Protocol (STP): là một giao thức chống hiện tượng Loop tại lớp 2 trong mô hình OSI (Open Systems Interconnection). Nhiệm vụ chính của STP là phát hiện và loại bỏ các vòng lặp trong các mạng Ethernet, nhằm đảm bảo tính ổn định và hiệu suất của mạng. STP hoạt động bằng cách xác định các cổng trên các thiết bị mạng có liên quan đến mạng Ethernet và tạo ra một spanning tree duy nhất trong mạng đó. spanning tree sẽ loại bỏ các kết nối lặp lại và chỉ định một cổng chính để chuyển tiếp dữ liệu, trong khi các cổng khác được tắt (blocked).
Quá trình xây dựng spanning tree trong STP bao gồm các bước sau: => Chọn một switch làm root switch: Trong mạng Ethernet, một switch được chọn làm root switch. Các switch khác sẽ cung cấp thông tin về kết nối đến root switch. => Xác định đường đi ngắn nhất chọn ra root-port. Mỗi switch xác định đường đi ngắn nhất từ nó đến root switch. => Chọn destination port. => Chặn cổng trên các đường đi dư thừa: Các cổng không thuộc đường đi ngắn nhất được tắt (blocked) để loại bỏ vòng lặp. => Theo dõi sự thay đổi và cập nhật cây khung: STP liên tục kiểm tra sự thay đổi trong mạng và cập nhật spanning tree để đảm bảo tính ổn định và chống lại hiện tượng Loop.
2. Loop Guard: Loop Guard là một tính năng bổ sung cho STP, giúp phát hiện các vòng lặp ẩn (hidden loop) khi một cổng không nhận được thông báo từ các cây cầu khác. Nếu một cổng không nhận được thông báo trong khoảng thời gian nhất định, nó sẽ chuyển sang trạng thái loop- inconsistent và ngừng chuyển tiếp dữ liệu.
3. BPDU Guard: BPDU Guard là một tính năng khác của STP, giúp ngăn chặn các thiết bị không chính thức (unauthorized devices) kết nối vào mạng và tạo ra các BPDU (Bridge Protocol Data Unit) giả mạo. Khi phát hiện BPDU giả mạo, cổng sẽ bị vô hiệu hóa để ngăn chặn nguy cơ tạo ra vòng lặp.
4. Portfast: Portfast là một tính năng trong STP cho phép cổng chuyển từ trạng thái Listening/Spanning-tree learning nhanh hơn thông thường. Điều này giúp giảm thời gian chờ đợi khi kết nối các thiết bị vào mạng và ngăn chặn việc hình thành các vòng lặp khi cổng chuyển từ trạng thái blocking sang forwarding.
5. Thiết kế mạng hợp lý: Thiết kế mạng Ethernet hợp lý và chia phân đoạn mạng thành các vùng cục bộ (VLANs) có thể giúp ngăn chặn và kiểm soát hiện tượng loop. Bằng cách sử dụng VLANs, các vòng lặp có thể được giới hạn trong một phân đoạn mạng cụ thể mà không ảnh hưởng đến toàn bộ mạng.
Tổng quan, sử dụng giao thức STP cùng với các tính năng bổ sung như Loop Guard, BPDU Guard, Portfast và thiết kế mạng hợp lý, có thể ngăn chặn và khắc phục hiện tượng loop trên mạng Ethernet.
VIRTUAL CIRCUIT (VC): là kỹ thuật lai giữa Circuit switching và Packet switching. Là đường dẫn từ nguồn tới đích, giống mạch điện thoại. Cắt thông tin thành nhiều packet vận chuyển cùng tuyến từ nguồn tới đích. VC bao gồm: đường dẫn(path) từ nguồn tới đích. VC numbers kỳ hiệu cho mỗi path. Table Forwarding trong Router kỳ hiệu cho paths. Packet được chuyển in path đã được routing. Packet mang VC numbers.
VC numbers can be changed for each link. Cơ chế: 1. Setup call 2.Cuộc gọi đến 3.accept call 4.call is connected 5.start data flow 6.recieve data
Circuit Switching, một kết nối vật lý được thiết lập giữa hai điểm trong thời gian truyền dữ liệu. Sử dụng toàn bộ băng thông của đường truyền ngay cả khi không có dữ liệu đang truyền, Khó mở rộng, sd gọi thoại truyền thống
Packet Switching, dữ liệu được chia thành các gói nhỏ trước khi được truyền. Chia sẻ băng thông giữa nhiều người dùng và chỉ sử dụng băng thông khi có dữ liệu cần truyền. Linh hoạt và có thể mở rộng tốt, Internet và các mạng dữ liệu
Hãy cho biết ý nghĩa của Subnet mask ? Khi nào thì cần phân chia mạng thành các mạng con có địa chỉ mạng khác nhau ? Hãy mô tả mạng lớp A, B, C
Subnet mask (hay còn gọi là mặt nạ mạng phụ) là một giá trị 32-bit được sử dụng để xác định phần mạng và phần máy trong một địa chỉ IP. Subnet mask định rõ phần mạng và phần host của địa chỉ IP, cho phép phân biệt các thiết bị trong mạng và quyết định liệu chúng có nằm trong cùng một mạng con hay không.
Mục đích phân chia mạng thành các mạng con có địa chỉ mạng khác nhau:
-Mạng cần được chia thành các mạng nhỏ hơn để tạo ra các mạng con riêng biệt với yêu cầu quản lý riêng. Việc phân chia mạng con cho phép quản lý dễ dàng hơn và cung cấp tính bảo mật cao hơn bằng cách giới hạn truy cập giữa các mạng con.
-Mạng cần hỗ trợ một số lượng lớn các thiết bị kết nối. Phân chia mạng con cho phép phân bổ địa chỉ IP hiệu quả hơn và giảm xung đột địa chỉ trong mạng.
-Mạng cần hỗ trợ các vùng địa lý khác nhau hoặc các phòng ban, bộ phận trong tổ chức cần được cấu hình riêng biệt.
Mô tả về mạng lớp A, B, C:
Mạng lớp A: Địa chỉ mạng lớp A bắt đầu từ 1.0.0.0 đến 126.0.0.0. Subnet mask mặc định của mạng lớp A là 255.0.0.0. Lớp A cho phép có tối đa 126 mạng con và mỗi mạng con có thể chứa tới 16.777.214 host.
Mạng lớp B: Địa chỉ mạng lớp B bắt đầu từ 128.0.0.0 đến 191.255.0.0. Subnet mask mặc định của mạng lớp B là 255.255.0.0. Lớp B cho phép có tối đa 16.384 mạng con và mỗi mạng con có thể chứa tới 65.534 host.
Mạng lớp C: Địa chỉ mạng lớp C bắt đầu từ 192.0.0.0 đến 223.255.255.0. Subnet mask mặc định của mạng lớp C là 255.255.255.0. Mạng lớp C cho phép có tối đa 2.097.152 mạng con và mỗi mạng con chỉ có thể chứa tối đa 254 host.Các mạng lớp A, B và C được sử dụng trong việc phân chia và quản lý địa chỉ IP trên Internet và các mạng nội bộ. sử dụng mạng lớp A, B hoặc C phụ thuộc vào quy mô và yêu cầu của mạng cụ thể.
NAT(Network Address Translation) là một kỹ thuật cho phép một hoặc nhiều địa chỉ IP nội miền chuyển sang một hoặc nhiều địa chỉ IP ngoại miền.
• Static NAT: kỹ thuật để thay đổi IP này thành một IP khác bằng cách sử dụng phương pháp cố định cụ thể từ địa chỉ IP cục bộ sang Public, được thực hiện thủ công. Static NAT hiệu quả nếu các thiết bị có địa chỉ cố định để truy cập internet từ bên ngoài.
• Dynamic NAT: kỹ thuật dùng để ánh xạ một địa chỉ IP này sang địa chỉ IP khác bằng phương pháp tự động. Dynamic NAT sẽ chuyển đổi từ IP mạng cục bộ sang địa chỉ IP được đăng ký hợp lệ.
• NAT Overload(PAT: Port Address Translation): biến thể của Dynamic NAT. Kiểu chuyển dịch địa chỉ PAT là dạng many to one và dùng các chỉ số cổng khác nhau để phân biệt cho từng chuyển đổi
Định tuyến là quá trình xác định đường đi tốt nhất trên một mạng máy tính để gói tin tới được đích theo một số thủ tục nhất định nào đó thông qua các nút trung gian là các bộ định tuyến (router).
Link Cost: Là một giá trị số được gán cho mỗi liên kết (kết nối) trong mạng, dung Đo lường chất lượng của một liên kết để tìm đường đi tối ưu
Link State: Giao thức Định trạng Liên kết (Link State Routing Protocol - LSRP) là một loại giao thức định tuyến sử dụng thông tin về trạng thái của các liên kết trong mạng để xác định đường dẫn tốt nhất giữa hai nút bất kỳ. LSRP là một giao thức định tuyến phân tán, có nghĩa là mỗi bộ định tuyến trong mạng duy trì bảng định tuyến của riêng mình. Bộ định tuyến trao đổi thông tin về trạng thái liên kết của chúng với các bộ định tuyến lân cận và thông tin này được sử dụng để tính toán đường dẫn ngắn nhất giữa hai nút bất kỳ. Ưu điểm của LSRP: **Hội tụ nhanh chóng**: LSRP hội tụ nhanh chóng với những thay đổi trong cấu trúc mạng. Điều này có nghĩa là nó có thể nhanh chóng tìm thấy đường dẫn tốt nhất giữa hai nút bất kỳ, ngay cả khi cấu trúc mạng thay đổi thường xuyên. **Định tuyến không vòng lặp**: LSRP là một giao thức định tuyến không vòng lặp. Điều này có nghĩa là nó sẽ không tạo ra các vòng lặp định tuyến, có thể khiến lưu lượng mạng bị kẹt trong vòng lặp. **Khả năng mở rộng**: LSRP là một giao thức định tuyến có thể mở rộng. Điều này có nghĩa là nó có thể được sử dụng trong các mạng lớn với nhiều nút. Nhược điểm của LSRP: **Chi phí:** LSRP có thể tạo ra nhiều lưu lượng, đặc biệt là trong các mạng lớn. Điều này là do mỗi bộ định tuyến định kỳ gửi LSA đến các bộ định tuyến lân cận của nó. **Độ phức tạp:** LSRP là một giao thức định tuyến phức tạp. Điều này có nghĩa là nó có thể khó cấu hình và khắc phục sự cố. Nên sử dụng linkState khi: Mạng lớn và phức tạp, cần độ tính cậy cao, hiệu suất cao, mạng sử dụng MPLS hoặc VPN, mạng yêu cầu tính linh hoạt cao.
Distance Vector: (Distance Vector Routing Protocol) là một loại giao thức định tuyến được sử dụng để tìm đường dẫn tốt nhất để gửi gói tin đến một đích cụ thể. Nó hoạt động dựa trên thông tin về khoảng cách (cost) được quảng cáo bởi các bộ định tuyến lân cận. Cách thức hoạt động: **Quảng cáo Vectơ Khoảng Cách**: Mỗi bộ định tuyến định kỳ gửi bảng vectơ khoảng cách của mình đến các bộ định tuyến lân cận. Bảng này chứa thông tin về khoảng cách đến các mạng khác, **Cập nhật Bảng Định tuyến:** Mỗi bộ định tuyến sử dụng thông tin nhận được từ các bộ định tuyến lân cận để cập nhật bảng định tuyến của riêng mình. **Lặp lại:** Quá trình quảng cáo và cập nhật bảng định tuyến diễn ra liên tục. Điều này cho phép các bộ định tuyến học về các mạng khác trong mạng và cập nhật thông tin định tuyến của chúng. So với Giao thức Định trạng Liên kết (LSRP), Giao thức Vectơ Khoảng cách đơn giản hơn để thiết lập nhưng có một số nhược điểm. LSRP hội tụ nhanh hơn, tránh được vấn đề về vòng lặp định tuyến và hiệu quả hơn trong các mạng lớn. Tuy nhiên, LSRP phức tạp hơn để thiết lập và cấu hình. Sử dụng giải thuật khi mạng nhỏ, chi phí thấp (ít lưu lượng mạng, băng thông, tài nguyên máy), cần triển khai mạng nahnh chóng, Mô trường mạng ổn định, ít thay đổi.
RIP (Routing Information Protocol) Đây là một giao thức vectơ khoảng cách phổ biến được sử dụng trong các mạng nhỏ.
Kết nối: TCP thiết lập một kết nối hướng giữa hai thiết bị trước khi truyền dữ liệu. Điều này đảm bảo rằng dữ liệu được truyền theo đúng thứ tự và không bị mất. UDP không thiết lập kết nối, dữ liệu được truyền dưới dạng các gói tin độc lập. **Độ tin cậy:** TCP có độ tin cậy cao hơn UDP nhờ các cơ chế như kiểm tra lỗi, xác nhận nhận gói tin và retransmission (gửi lại dữ liệu bị mất). UDP không có các cơ chế này, do đó dữ liệu có thể bị mất hoặc bị hỏng trong quá trình truyền tải. **Sắp xếp:** TCP đảm bảo dữ liệu được truyền theo đúng thứ tự, ngay cả khi các gói tin đến đích không theo thứ tự. UDP không sắp xếp dữ liệu, các gói tin có thể đến đích theo thứ tự bất kỳ. **Kiểm soát lỗi:** TCP kiểm tra lỗi dữ liệu bằng cách sử dụng checksum. Nếu lỗi được phát hiện, gói tin sẽ được gửi lại. UDP không kiểm tra lỗi dữ liệu, do đó dữ liệu bị hỏng sẽ không được sửa chữa. **Độ trễ:** Do các cơ chế kiểm soát lỗi, sắp xếp và kiểm soát lưu lượng, TCP có độ trễ cao hơn UDP. UDP có độ trễ thấp hơn vì nó không có các cơ chế này. **Tốc độ:** Do độ tin cậy cao hơn, TCP có tốc độ truyền dữ liệu thấp hơn UDP. UDP có tốc độ truyền dữ liệu cao hơn vì nó không có các cơ chế kiểm soát lỗi, sắp xếp và kiểm soát lưu lượng. **Chi phí:** Do độ phức tạp cao hơn, TCP có chi phí triển khai và sử dụng cao hơn UDP. UDP có chi phí triển khai và sử dụng thấp hơn. TCP được sử dụng cho:Email Web FTP SSH Telnet
UDP được sử dụng cho: Video theo thời gian thực (streaming) Âm thanh theo thời gian thực (streaming) VoIP (gọi điện thoại qua internet)DNS (Hệ thống tên miền) DHCP (Giao thức cấu hình máy khách động)

POP3 (viết tắt của Post Office Protocol version 3) là một giao thức mạng được sử dụng để tải email từ máy chủ email đến máy tính cá nhân. Nó hoạt động ở lớp ứng dụng của mô hình OSI và thường được sử dụng với các ứng dụng email. Cách thức hoạt động của POP3: **Kết nối:** Máy tính của bạn kết nối với máy chủ email thông qua cổng 110 (hoặc 995 cho kết nối SSL/TLS). **Xác thực:** Máy tính của bạn xác thực với máy chủ email bằng tên người dùng và mật khẩu email của bạn. **Danh sách thư**: Máy chủ email gửi danh sách các hộp thư đến cho máy tính của bạn. **Tải xuống email:** Máy tính của bạn tải xuống các email từ hộp thư đến

được chọn. **Xóa email:** Theo mặc định, POP3 sẽ xóa email khỏi máy chủ email sau khi tải xuống. Tuy nhiên, bạn có thể cấu hình để lưu trữ email trên máy chủ. **Ngắt kết nối:** Máy tính của bạn ngắt kết nối với máy chủ email. trường hợp bạn có thể sử dụng POP3: Nếu bạn chỉ sử dụng một thiết bị để kiểm tra email. Nếu bạn không cần tìm kiếm email cũ. Nếu bạn không quan tâm đến bảo mật email của mình.
IMAP (viết tắt của Internet Message Access Protocol) là một giao thức mạng được sử dụng để truy cập và quản lý email trên máy chủ email. Nó là một giao thức tiên tiến hơn so với POP3 (Post Office Protocol version 3) và mang lại nhiều ưu điểm: đồng bộ hóa, tìm kiếm, bảo mật. Trường hợp bạn có thể sử dụng IMAP: Nếu bạn sử dụng nhiều thiết bị để kiểm tra email, chẳng hạn như điện thoại thông minh, máy tính bảng và máy tính xách tay. Nếu bạn cần tìm kiếm email cũ. Nếu bạn quan tâm đến bảo mật email của mình.
Mã CRC là một mã kiểm tra lỗi sử dụng một đa thức sinh để tạo ra một số dư (remainder) từ dữ liệu gốc. Số dư này được gửi kèm với dữ liệu để bên nhận có thể kiểm tra tính toàn vẹn của dữ liệu. Nếu số dư của dữ liệu nhận được chia cho đa thức sinh bằng 0, có nghĩa là dữ liệu không có lỗi. Nếu không, có nghĩa là dữ liệu bị hỏng hoặc mất mát. Mã CRC hoạt động dựa trên phép chia modulo-2, trong đó phép cộng và trừ được thực hiện bằng phép XOR (phép loại trừ đôi). Mã CRC có khả năng phát hiện các lỗi đơn bit, lỗi kép bit, lỗi burst và lỗi chèn/xóa bit. Mã CRC được sử dụng rộng rãi trong các giao thức tầng liên kết dữ liệu và tầng vận chuyển, ví dụ như Ethernet, HDLC, PPP, ATM, Bluetooth, USB và TCP.
Internet checksum là một mã kiểm tra lỗi sử dụng phép cộng để tính tổng các từ (word) trong dữ liệu gốc. Tổng này được lấy bù hai để tạo ra giá trị checksum. Giá trị checksum này được gửi kèm với dữ liệu để bên nhận có thể kiểm tra tính toàn vẹn của dữ liệu. Nếu tổng của các từ trong dữ liệu nhận được cộng với giá trị checksum bằng 0, có nghĩa là dữ liệu không có lỗi. Nếu không, có nghĩa là dữ liệu bị hỏng hoặc mất mát. Internet checksum hoạt động dựa trên phép cộng modulo-1, trong đó nếu có nhớ (carry) thì nhớ sẽ được cộng lại vào kết quả. Internet checksum có khả năng phát hiện các lỗi đơn bit và lỗi kép bit, nhưng không phát hiện được các lỗi burst và lỗi chèn/xóa bit. Internet checksum được sử dụng trong các giao thức tầng mạng và tầng vận chuyển, ví dụ như IP, ICMP, UDP và TCP3.
Mô tả các chế độ hoạt động của giao thức HDLC.
Asynchronous Balanced Mode (ABM): Đây là chế độ hoạt động phổ biến nhất của HDLC. Trong chế độ này, hai thiết bị trao đổi dữ liệu với nhau mà không có vai trò chủ động hoặc bị động. Cả hai thiết bị đều có khả năng gửi và nhận dữ liệu. Gói tin dữ liệu được chia thành các khung (frames) và được đánh dấu để đồng bộ hóa và kiểm tra lỗi. Asynchronous Response Mode (ARM): Đây là chế độ trong đó một thiết bị được coi là "chủ" và thiết bị còn lại là "nhân viên". Thiết bị chủ động gửi yêu cầu (command) và thiết bị nhân viên phản hồi (response) theo yêu cầu đó. Chế độ này thường được sử dụng trong các ứng dụng điều khiển từ xa.
Normal Response Mode (NRM): Chế độ này tương tự như ARM, tuy nhiên, có sự khác biệt là thiết bị nhân viên có khả năng gửi yêu cầu (command) đến thiết bị chủ và thiết bị chủ sẽ phản hồi (response) theo yêu cầu đó. Chế độ này thường được sử dụng trong các ứng dụng mạng phân tán.
Phân tích vai trò của Root DNS và mô tả các chế độ truy vấn DNS (DNS query)
Root DNS (Domain Name System) là một tầng quan trọng trong hệ thống DNS và chịu trách nhiệm cung cấp thông tin về các máy chủ DNS cấp cao nhất trên Internet. Root DNS đóng vai trò quan trọng trong việc định vị TLD (Top-Level Domain) và máy chủ DNS cấp trên. Cụ thể, vai trò của Root DNS bao gồm: Định vị TLD: Root DNS cung cấp thông tin về các máy chủ DNS quản lý các TLD như .com, .org, .net, .edu, Khi một truy vấn DNS được thực hiện cho một tên miền cụ thể, Root DNS sẽ chỉ định máy chủ DNS cho TLD tương ứng. Định vị máy chủ DNS cấp trên: Root DNS giúp xác định địa chỉ IP của các máy chủ DNS cấp trên, cung cấp thông tin để truy cập đến các máy chủ DNS cấp cao hơn. Điều này cho phép các truy vấn DNS được chuyển tiếp từ máy chủ DNS gốc tới máy chủ DNS cấp cao hơn để lấy thông tin liên quan đến tên miền.
DNS query là quá trình gửi yêu cầu từ máy khách (client) tới máy chủ DNS để lấy thông tin về một tên miền cụ thể. Có ba chế độ truy vấn DNS phổ biến:
-Recursive Query (Truy vấn đệ quy): Máy khách gửi yêu cầu truy vấn DNS tới máy chủ DNS. Máy chủ DNS nhận yêu cầu và truy vấn các máy chủ DNS khác trong hệ thống để lấy thông tin cần thiết. Sau đó, nó trả về kết quả cho máy khách. Quá trình này diễn ra theo hướng từ máy chủ DNS cấp cao hơn xuống đến máy chủ DNS cấp thấp hơn cho đến khi tìm thấy thông tin được yêu cầu.
-Iterative Query (Truy vấn lặp lại): Máy khách gửi yêu cầu truy vấn DNS tới máy chủ DNS. Máy chủ DNS trả lời bằng cách cung cấp thông tin về máy chủ DNS cấp cao hơn, nhưng không thực hiện truy vấn thay mặt cho máy khách. Máy khách tiếp tục gửi các truy vấn cho các máy chủ DNS cấp cao hơn cho đến khi tìm thấy thông tin cần thiết. Quá trình này yêu cầu máy khách phải gửi nhiều yêu cầu truy vấn để lấy được thông tin hoàn chỉnh.
-Reverse Query (Truy vấn ngược): Reverse query là quá trình truy vấn DNS ngược lại, trong đó máy khách yêu cầu xác định tên miền dựa trên địa chỉ IP. Máy khách gửi yêu cầu tới máy chủ DNS và máy chủ DNS trả lời bằng cách cung cấp tên miền tương ứng với địa chỉ IP được yêu cầu.

Hãy mô tả giao thức HTTP và HTTPS? hãy cho biết sự khác biệt giữa HTTP và HTTPS? HTTP là giao thức truyền tải dữ liệu phổ biến nhất trên Internet. Nó được sử dụng để truyền tải các trang web, tài liệu và các tài nguyên khác qua mạng. Giao thức HTTP hoạt động dựa trên mô hình yêu cầu/phản hồi giữa máy khách (client) và máy chủ (server).
Mô tả giao thức HTTP:
-Giao thức HTTP hoạt động bằng cách sử dụng các yêu cầu và phản hồi giữa máy khách và máy chủ. Quá trình truyền tải dữ liệu thông qua giao thức HTTP bao gồm các bước sau:
-Máy khách gửi yêu cầu HTTP đến máy chủ. Yêu cầu này bao gồm một phương thức (GET, POST, PUT, DELETE, vv.) và một URL (Uniform Resource Locator) xác định tài nguyên được yêu cầu
-Máy chủ nhận yêu cầu và xử lý nó. Nếu yêu cầu hợp lệ, máy chủ sẽ trả về một mã phản hồi HTTP, cùng với dữ liệu tương ứng (nếu có).
-Máy khách nhận phản hồi từ máy chủ và xử lý dữ liệu nhận được. Dữ liệu này có thể là trang web, tài liệu hoặc các tài nguyên khác, được truyền từ máy chủ đến máy khách.
Quá trình truyền tải kết thúc và kết nối có thể được đóng hoặc duy trì để thực hiện các yêu cầu và phản hồi tiếp theo.
HTTPS là phiên bản bảo mật của giao thức HTTP. Nó sử dụng lớp bảo mật SSL/TLS để đảm bảo tính bảo mật trong quá trình truyền tải dữ liệu trên mạng.
Quá trình hoạt động của giao thức HTTPS bao gồm các bước sau:
Giao tiếp ban đầu: Khi máy khách (client) kết nối đến máy chủ (server), máy khách gửi yêu cầu kết nối HTTPS. Điều này thông qua việc yêu cầu máy chủ cung cấp chứng chỉ SSL/TLS để xác minh danh tính của nó.
-Xác thực chứng chỉ: Máy chủ gửi lại chứng chỉ SSL/TLS cho máy khách. Máy khách sẽ kiểm tra tính hợp lệ của chứng chỉ này, bao gồm xác minh xem chứng chỉ được ký bởi một tổ chức chứng chỉ đáng tin cậy và chưa hết hạn.
-Thiết lập kết nối an toàn: Sau khi chứng chỉ được xác minh, máy khách và máy chủ sử dụng quy trình mã hóa để thiết lập kết nối an toàn. Quá trình này bao gồm thỏa thuận về phiên mã hóa, cung cấp khóa bí mật và thiết lập một kênh truyền tải an toàn giữa hai bên.
-Truyền tải dữ liệu an toàn: Khi kết nối an toàn đã được thiết lập, các yêu cầu và phản hồi HTTP được truyền tải thông qua kênh truyền tải an toàn đã được mã hóa. Điều này đảm bảo rằng dữ liệu không bị nội dung bị thay đổi hoặc bị đánh cắp trong quá trình truyền tải.
Với HTTPS, thông tin nhạy cảm như thông tin cá nhân, thông tin thanh toán và mật khẩu được bảo vệ bởi mã hóa, ngăn chặn người thứ ba không có quyền truy cập hoặc đánh cắp dữ liệu. Điều này tạo ra một môi trường an toàn cho việc truyền tải thông tin trên Internet và làm tăng tính bảo mật và tin cậy cho người dùng.
Sự khác biệt giữa HTTP và HTTPS có thể được tóm tắt như sau:
HTTP: Không có cơ chế bảo mật để mã hóa dữ liệu; Hoạt động ở tầng ứng dụng; Sử dụng cổng 80 mặc định; Hiển thị http:// trước URL của trang web; Không yêu cầu chứng chỉ số cho máy chủ web; Không ảnh hưởng đến xếp hạng SEO của trang web
HTTPS: Cung cấp chứng chỉ số SSL hoặc TLS để bảo mật truyền thông giữa máy chủ và máy khách; Hoạt động ở tầng vận chuyển; Sử dụng cổng 443 mặc định; Hiển thị https:// và biểu tượng khóa an toàn; Yêu cầu máy chủ web phải có chứng chỉ số được cấp bởi một tổ chức có uy tín; Là một yếu tố SEO tích cực và có thể cải thiện xếp hạng của trang web
Thuật toán quản lý luồng và quản lý nghẽn là hai phương pháp điều khiển lưu lượng truyền dữ liệu trong mạng.
Quản lý luồng là kỹ thuật điều chỉnh tốc độ truyền dữ liệu từ bên gửi đến bên nhận để tránh việc bên nhận bị quá tải dữ liệu quá nhanh. Mục tiêu của quản lý luồng là ngăn chặn tràn bộ đệm, có thể dẫn đến mất gói tin và hiệu suất mạng kém.
Quản lý nghẽn là kỹ thuật ngăn ngừa tình trạng nghẽn trọng mạng. Nghẽn xảy ra khi có quá nhiều dữ liệu được gửi qua mạng, và mạng bị quá tải, dẫn đến mất gói tin và hiệu suất mạng kém.
Một số thuật toán quản lý luồng và quản lý nghẽn phổ biến là:
Quản lý luồng: Giao thức cửa sổ trượt (Sliding Window Protocol), Giao thức điều khiển truyền (Transmission Control Protocol - TCP), Giao thức điều khiển truyền nhiều đường (Multipath Transmission Control Protocol - MPTCP).
Quản lý nghẽn: Thuật toán tăng liên kết (Linked-Increases Algorithm - LIA), Thuật toán Reno, thuật toán Tahoe, Thuật toán Vegas,…
Thuật toán Tahoe: sử dụng ba kỹ thuật khởi động chậm, tránh tắc nghẽn và phục hồi nhanh
Khi bắt đầu kết nối, cửa sổ tắc nghẽn (congestion window) được thiết lập bằng một giá trị nhỏ. Cửa sổ tắc nghẽn sẽ tăng theo cấp số nhân trong giai đoạn khởi động chậm cho đến khi gặp một gói tin bị mất hoặc đạt được ngưỡng tắc nghẽn (congestion threshold). Sau đó, cửa sổ tắc nghẽn sẽ tăng theo cấp số cộng trong giai đoạn tránh tắc nghẽn cho đến khi gặp một gói tin bị mất. Khi xảy ra mất gói tin, thuật toán Tahoe sẽ giảm cửa sổ tắc nghẽn xuống một nửa và quay lại giai đoạn khởi động chậm. Ưu điểm là khôi phục được từ tình trạng sụp đổ của mạng (congestion collapse) Nhược điểm là không khai thác được toàn bộ băng thông của mạng và phản ứng chậm với các thay đổi của mạng.
Thuật toán TCP Reno là một biến thể tiếp theo của giao thức TCP, được phát triển từ TCP Tahoe. Bổ sung thêm một cơ chế gọi là Fast Recovery vào TCP Tahoe để cải thiện hiệu suất của quá trình truyền tải dữ liệu. Khi xảy ra mất mát gói tin, TCP Reno sẽ chuyển từ trạng thái Slow Start sang trạng thái Congestion Avoidance, trong đó cửa sổ cửa truyền sẽ tăng tuyến tính theo thời gian.
Nếu TCP Reno nhận được thông báo ACK lặp lại (duplicate ACK) cho cùng một gói tin, nó sẽ kích hoạt cơ chế Fast Recovery. Cơ chế này giảm bớt cửa sổ cửa truyền một lượng nhất định và sau đó chuyển sang trạng thái Fast Retransmit để gửi lại gói tin bị mất.
Sau khi gửi lại gói tin bị mất, TCP Reno sẽ tiếp tục quá trình tăng tốc bằng cách sử dụng cơ chế additive increase.
Ứng dụng của TCP Reno tương tự như TCP Tahoe, nhưng nó cung cấp hiệu suất tốt hơn trong việc xử lý sự mất mát gói tin và khôi phục nhanh chóng.
Thuật toán Vegas là một phiên bản cải tiến của thuật toán Tahoe, sử dụng ba kỹ thuật khởi động chậm, tránh tắc nghẽn và phục hồi nhanh, nhưng có một số khác biệt quan trọng, không chỉ dựa vào việc phát hiện mất gói tin để điều chỉnh cửa sổ tắc nghẽn, mà còn dựa vào việc ước tính thời gian trễ của các gói tin để phát hiện sớm dấu hiệu của tình trạng nghẽn.
Khác biệt giữa mã CRC và Internet checksum:
-Mã CRC tính toán giá trị băm bằng cách sử dụng đa thức nhị phân và phép chia modulo 2, trong khi Internet checksum tính toán giá trị checksum bằng cách cộng các từ 16-bit liên tiếp.
-Mã CRC thường được sử dụng trong các giao thức truyền tải dữ liệu và lưu trữ, trong khi Internet checksum được sử dụng trong các giao thức mạng Internet như IPv4, UDP và TCP.
-Mã CRC có khả năng phát hiện lỗi cao hơn so với Internet checksum, do cách tính toán khác nhau. CRC có thể phát hiện được các lỗi như bit đảo ngược, bit bị mất và một số lỗi khác, trong khi Internet checksum chỉ có thể phát hiện các lỗi đơn giản hơn. Tuy nhiên, cả hai đều không thể khắc phục lỗi.
-Mã CRC tốn nhiều thời gian tính toán hơn Internet checksum do sử dụng phép chia modulo 2, trong khi Internet checksum tương đối nhanh chóng và đơn giản hơn.
1. TCP/IP (Transmission Control Protocol/Internet Protocol):Bộ giao thức chính cho Internet. TCP quản lý việc truyền dữ liệu một cách tin cậy qua mạng, trong khi IP quản lý địa chỉ và định tuyến.
2. HTTP (Hypertext Transfer Protocol): Sử dụng để truyền tải dữ liệu siêu văn bản, thường được sử dụng trong trình duyệt web.
3. HTTPS (Hypertext Transfer Protocol Secure):Là phiên bản bảo mật của HTTP, sử dụng SSL/TLS để mã hóa dữ liệu giữa trình duyệt và máy chủ.
4. FTP (File Transfer Protocol):Sử dụng để truyền tải tệp tin giữa các hệ thống qua mạng.
5. SSH (Secure Shell):Dùng để thiết lập kết nối bảo mật qua mạng và cung cấp môi trường dòng lệnh an toàn.
6. DNS (Domain Name System):Dịch địa chỉ IP thành tên miền và ngược lại, giúp người dùng dễ nhớ và sử dụng các tên miền.
7. SMTP (Simple Mail Transfer Protocol):Sử dụng để gửi email từ máy chủ email nguồn đến máy chủ email đích.
8. POP3 (Post Office Protocol version 3):Dùng để tải email từ máy chủ đến máy tính cá nhân và xóa chúng khỏi máy chủ.
9. IMAP (Internet Message Access Protocol):Cho phép quản lý email trực tiếp trên máy chủ mà không cần tải về máy tính.
10. SNMP (Simple Network Management Protocol): Sử dụng để quản lý và giám sát các thiết bị mạng từ xa.
11. ARP (Address Resolution Protocol): Dùng để ánh xạ địa chỉ IP thành địa chỉ MAC trong mạng LAN.
12. DHCP (Dynamic Host Configuration Protocol):Cung cấp cấu hình IP tự động cho các thiết bị trong mạng.
13. BGP (Border Gateway Protocol): Sử dụng trong quá trình định tuyến giữa các hệ thống mạng trên Internet.

Go-back-N là thuật toán truyền lại gói tin được sử dụng trong giao thức truyền thông dữ liệu để đảm bảo dữ liệu được truyền đi chính xác và theo đúng thứ tự. Nó hoạt động dựa trên việc theo dõi số sê-ri của các gói tin và sử dụng bộ đếm thời gian để phát hiện lỗi mất gói. Cơ chế: **Gửi khung dữ liệu:** Máy phát gửi khung dữ liệu đến máy thu. Khung này bao gồm dữ liệu cần truyền và số sê-ri để theo dõi thứ tự. **Xác nhận:** Máy thu gửi khung xác nhận (ACK) cho máy phát để xác nhận nhận được khung dữ liệu thành công. Số sê-ri của ACK bằng số sê-ri của khung dữ liệu đã nhận. **Bộ đếm thời gian:** Máy phát giả định khung dữ liệu bị mất và thực hiện: Gửi lại khung dữ liệu bị mất: Khung dữ liệu bị mất và tất cả các khung dữ liệu tiếp theo (từ N trở đi) được gửi lại. Bỏ qua ACK: Máy phát bỏ qua bất kỳ ACK nào nhận được cho các khung dữ liệu đã được gửi lại. **Loại bỏ bản sao:** Khi máy thu nhận được khung dữ liệu đã nhận trước đó, nó sẽ loại bỏ bản sao.
Selective Repeat: Cơ chế hoạt động: **Gửi khung dữ liệu:** Máy phát gửi khung dữ liệu đến máy thu. Khung này bao gồm dữ liệu cần truyền và số sê-ri để theo dõi thứ tự. **Xác nhận:** Máy thu gửi khung xác nhận (ACK) cho máy phát để xác nhận nhận được khung dữ liệu thành công. Số sê-ri của ACK bằng số sê-ri của khung dữ liệu đã nhận. **Bộ đếm thời gian:** Máy phát đặt bộ đếm thời gian cho mỗi khung dữ liệu được gửi đi. **Hết hạn**: Nếu bộ đếm thời gian hết hạn trước khi nhận được ACK, máy phát giả định khung dữ liệu bị mất và thực hiện: Gửi lại khung dữ liệu bị mất: Chỉ khung dữ liệu bị mất được gửi lại. Lưu ý ACK: Máy phát lưu ý số sê-ri của các ACK đã nhận được cho các khung dữ liệu chưa được xác nhận. **Loại bỏ bản sao**: Khi máy thu nhận được khung dữ liệu đã nhận trước đó, nó sẽ loại bỏ bản sao.
Cơ chế hoạt động của TCP: 1. Thiết lập kết nối 2. Truyền dữ liệu 3. Kiểm soát lỗi 4. Kiểm soát lưu lượng 5. Đóng kết nối: Hiệu quả hơn: Hiệu quả hơn khi mất nhiều gói tin, Giảm tắc nghẽn mạng, Hỗ trợ truyền dữ liệu theo luồng, Độ tin cậy cao hơn (TCP sử dụng nhiều cơ chế kiểm soát lỗi và kiểm soát lưu lượng để đảm bảo dữ liệu được truyền đi chính xác và không bị lỗi)