



Summary

 Created By	
 Last Edited By	

Computer Networking

Basics of Computer Networking

Types of Computer Networks

Advanced Stuff

TCP 3-Way handshake

VLAN?

IP Address

IP Packet Header

IPV4

IPV6

Routing Protocols Types - Static, Dynamic

Address Resolution Protocol:

Các loại bản tin ARP

Các bước hoạt động của giao thức mạng ARP

MAC address and IP address

What is IP Routing? Types, Routing Table, Protocols, Commands

Các gói IP được định tuyến như thế nào trên Internet?

Giao thức mạng nào được sử dụng để định tuyến địa chỉ IP?

Subnetting: What is Subnet Mask?

Computer Network Differences

Modem vs Router – Difference Between Them

Modem

Cơ chế hoạt động

Vị trí kết nối

Chế độ kết nối

Chức năng của Modem

Ưu điểm

Nhược điểm

Router:

Hub vs Switch

IPv4 vs IPv6

SỰ KHÁC BIỆT CHÍNH

HTTP vs HTTPS

HTTP

HTTPS

SỰ KHÁC BIỆT CHÍNH

FTP vs SFTP

FTP

SFTP

SỰ KHÁC BIỆT CHÍNH

PUT vs POST

PUT

Kiểm tra một API với các yêu cầu PUT

POST

SỰ KHÁC BIỆT CHÍNH:

GET vs POST

Phương thức GET

Phương thức POST

Phân biệt POST và GET

SMB

DHCP

DNS

Computer Networking

Basics of Computer Networking

- Computer network là một nhóm gồm hai hoặc nhiều hệ thống máy tính được kết nối với nhau
- Computer networks giúp kết nối nhiều máy tính với nhau để gửi và nhận thông tin
- Switches hoạt động như một bộ điều khiển kết nối máy tính, máy in và các thiết bị phần cứng khác
- Routers giúp bạn kết nối với nhiều mạng. Nó cho phép bạn chia sẻ một kết nối internet duy nhất và tiết kiệm tiền
- Máy chủ - server là máy tính chứa các chương trình, tệp được chia sẻ và hệ điều hành mạng
- Khách hàng - clients là thiết bị máy tính truy cập và sử dụng mạng và chia sẻ dữ liệu mạng
- Hub là thiết bị chia kết nối mạng thành nhiều máy tính.
- Access points cho phép các thiết bị kết nối với mạng không dây mà không cần dây cáp

- Thẻ giao diện mạng gửi, nhận dữ liệu và kiểm soát luồng dữ liệu giữa máy tính và mạng
- protocol là tập hợp các quy tắc được xác định cho phép hai thực thể giao tiếp qua mạng
- Tên máy chủ, Địa chỉ IP, Máy chủ DNS và Máy chủ lưu trữ là các định danh duy nhất quan trọng của mạng máy tính.
- ARP là viết tắt của Address Resolution Protocol
- RAR Reverse Address Resolution Protocol cung cấp một địa chỉ IP của thiết bị với một địa chỉ vật lý đã cho làm đầu vào.
- Computer network giúp bạn chia sẻ cơ sở dữ liệu và phần mềm đắt tiền giữa những người tham gia mạng
- Hạn chế lớn nhất của việc cài đặt mạng máy tính là đầu tư ban đầu cho phần cứng và phần mềm có thể tốn kém cho việc thiết lập ban đầu

Types of Computer Networks

- Các loại kết nối trong mạng máy tính có thể được phân loại theo kích thước cũng như mục đích của chúng
- PAN là mạng máy tính thường bao gồm máy tính, thiết bị di động hoặc trợ lý kỹ thuật số cá nhân. PAN tương đối an toàn bảo mật, chỉ cung cấp giải pháp tầm 10m, hạn chế nghiêm ngặt trong một khu vực nhỏ.

Nó có thể thiết lập kết nối kém với các mạng khác ở cùng băng tần vô tuyến và giới hạn khoảng cách

- LAN (Mạng cục bộ) là một nhóm máy tính và thiết bị ngoại vi được kết nối trong một khu vực giới hạn (ít hơn 5000 thiết bị)

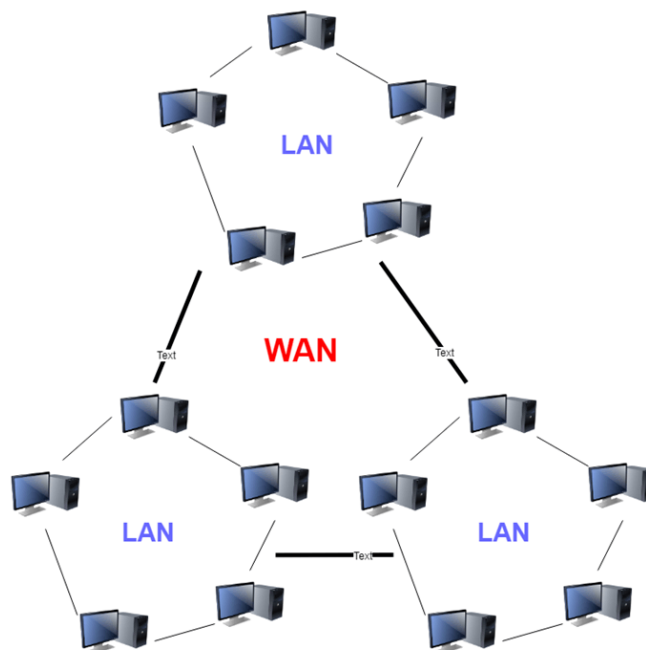
LAN là một mạng riêng, vì vậy một cơ quan quản lý bên ngoài không bao giờ kiểm soát được; mạng Lan hoạt động với tốc độ tương đối cao so với WAN; có nhiều loại phương pháp kiểm soát truy cập phương tiện khác

Các dữ liệu máy tính có thể chia sẻ mạng cục bộ; có thể sử dụng cùng 1 phần mềm qua mạng thay vì mua phần mềm được cấp phép cho từng máy khách trong mạng; Dữ liệu của tất cả người dùng mạng có thể được lưu trữ trên một đĩa cứng duy nhất của máy tính chủ; Có thể dễ dàng chuyển dữ liệu và tin nhắn qua các máy tính nối mạng; Dễ dàng quản lý dữ liệu tại một nơi duy nhất → an

toàn; Mạng cục bộ cung cấp cơ sở để chia sẻ một kết nối internet duy nhất giữa tất cả người dùng mạng Lan

Nhược: Chi phí cài đặt LAN ban đầu có thể cao; Người quản trị mạng LAN có thể kiểm tra các tệp dữ liệu cá nhân của mọi người dùng mạng LAN vì vậy nó không mang lại sự private; Người dùng trái phép có thể truy cập dữ liệu quan trọng của tổ chức trong trường hợp quản trị mạng LAN không thể bảo mật kho dữ liệu tập trung; Mạng cục bộ yêu cầu quản trị mạng LAN liên tục vì có các vấn đề liên quan đến thiết lập phần mềm và lỗi phần cứng

- WAN (Mạng diện rộng) là một mạng máy tính quan trọng khác được trải rộng trên một khu vực địa lý rộng lớn. Hệ thống mạng WAN có thể là kết nối của một mạng LAN kết nối với mạng LAN khác bằng đường dây điện thoại và sóng vô tuyến. Nó chủ yếu được giới hạn trong một doanh nghiệp hoặc tổ chức



- Mạng khu vực đô thị hoặc MAN bao gồm một mạng máy tính trên toàn bộ thành phố, khuôn viên trường đại học hoặc một khu vực nhỏ
- WLAN là mạng cục bộ không dây giúp bạn liên kết một hoặc nhiều thiết bị bằng cách sử dụng. Nó sử dụng giao tiếp không dây trong một khu vực hạn chế như nhà, trường học hoặc tòa nhà văn phòng.
- SAN là mạng khu vực lưu trữ là một loại mạng cho phép lưu trữ dữ liệu cấp khối, hợp nhất

- Mạng khu vực hệ thống cung cấp kết nối tốc độ cao trong các ứng dụng từ máy chủ đến máy chủ, mạng khu vực lưu trữ và các ứng dụng từ bộ xử lý đến bộ xử lý
- POLAN là một công nghệ mạng giúp bạn tích hợp vào hệ thống cáp có cấu trúc
- Mạng gia đình (HAN) luôn được xây dựng bằng cách sử dụng hai hoặc nhiều máy tính được kết nối với nhau để tạo thành mạng cục bộ (LAN) trong nhà
- Mạng doanh nghiệp mạng tư nhân (EPN) được xây dựng và sở hữu bởi các doanh nghiệp muốn kết nối an toàn các địa điểm khác nhau
- Mạng khu vực trường (CAN) được tạo thành từ sự kết nối với nhau của các mạng LAN trong một khu vực địa lý cụ thể
- VPN là mạng riêng tư sử dụng mạng công cộng để kết nối các trang web hoặc người dùng từ xa với nhau
- LAN là viết tắt của Local Area Network.
- Mạng LAN là mạng máy tính bao phủ một khu vực địa lý nhỏ, như nhà riêng, văn phòng hoặc nhóm tòa nhà, trong khi WAN là mạng máy tính bao phủ một khu vực rộng hơn.

Advanced Stuff

TCP 3-Way handshake

- TCP 3-way handshake hay 3-way handshake hoặc TCP 3-way handshake là một quá trình được sử dụng trong mạng TCP / IP để tạo kết nối giữa máy chủ và máy khách.
- Syn sử dụng để bắt đầu và thiết lập kết nối
- ACK giúp xác nhận với phía bên kia rằng nó đã nhận được SYN.
- SYN-ACK là một thông điệp SYN từ thiết bị cục bộ và ACK của gói trước đó.
- FIN được sử dụng để ngắt kết nối.
- Quá trình bắt tay TCP, một máy khách cần bắt đầu cuộc trò chuyện bằng cách yêu cầu một phiên giao tiếp với Máy chủ
- Trong bước đầu tiên, máy khách thiết lập kết nối với máy chủ

- Trong bước thứ hai này, máy chủ đáp ứng yêu cầu của khách hàng với bộ tín hiệu SYN-ACK
- Trong bước cuối cùng này, máy khách xác nhận phản hồi của Máy chủ
- TCP tự động ngắt kết nối giữa hai điểm cuối riêng biệt.

VLAN?

- VLAN được định nghĩa là một mạng tùy chỉnh được tạo từ một hoặc nhiều mạng cục bộ. LAN
- VLAN trong mạng được xác định bằng một số.
- VLAN ảo cung cấp cấu trúc để tạo các nhóm thiết bị ngay cả khi mạng khác nhau
- Làm giảm rủi ro bảo mật khi số lượng máy chủ được kết nối với broadcast domain giảm: thực hiện bằng cách định cấu hình một mạng LAN ảo riêng biệt chỉ dành cho các máy chủ có thông tin nhạy cảm
- Giảm traffic bằng cách chia sẻ lưu lượng truy cập khi các VLAN riêng lẻ hoạt động như một mạng LAN riêng biệt
- Phạm vi hợp lệ là 1-4094. Trên bộ chuyển mạch VLAN, bạn chỉ định các cổng với số VLAN thích hợp.
- Mạng LAN ảo cung cấp cấu trúc để tạo các nhóm thiết bị, ngay cả khi mạng của chúng khác nhau.
- Sự khác biệt chính giữa LAN và VLAN là Trong mạng LAN, gói mạng được quảng cáo đến từng thiết bị Trong khi trong VLAN, gói mạng chỉ được gửi đến một miền quảng bá cụ thể.
- Ưu điểm chính của VLAN là nó làm giảm kích thước của các miền quảng bá.
- Hạn chế của VLAN là một gói tin được đưa vào có thể dẫn đến một cuộc tấn công mạng.
- VLAN được sử dụng khi bạn có hơn 200 thiết bị trong mạng LAN của mình.

Aa LAN

☰ VLAN

Aa LAN	VLAN
<u>LAN có thể được định nghĩa là một nhóm máy tính và thiết bị ngoại vi được kết nối trong một khu vực giới hạn.</u>	VLAN có thể được định nghĩa là một mạng tùy chỉnh được tạo từ một hoặc nhiều mạng cục bộ.
<u>Dạng đầy đủ của mạng LAN là Mạng cục bộ.</u>	Dạng đầy đủ của VLAN là Mạng cục bộ ảo.
<u>Độ trễ của mạng LAN cao.</u>	Độ trễ của VLAN ít hơn.
<u>Chi phí của mạng LAN cao.</u>	Chi phí của một VLAN ít hơn.
<u>Trong mạng LAN, gói mạng được quảng cáo tới từng thiết bị.</u>	Trong VLAN, gói mạng chỉ được gửi đến một miền quảng bá cụ thể.

- VLAN là một mạng tùy chỉnh được tạo từ một hoặc nhiều Mạng cục bộ.
- VTP là một giao thức độc quyền của Cisco được sử dụng để trao đổi thông tin VLAN.
- Các thành phần quan trọng của VTP là

- **VTP Domain:**

Miền VTP giới hạn mức độ lan truyền thay đổi cấu hình trong mạng nếu xảy ra lỗi. Tại một thời điểm switch chỉ có thể là thành viên của một miền VTP tại một thời điểm. Cho đến khi tên miền VTP được chỉ định, không thể tạo hoặc sửa đổi các VLAN trên chế độ máy chủ VTP. Thông tin VLAN không được truyền qua mạng. Thành phần này bao gồm một hoặc nhiều công tắc được kết nối với nhau.

- **VTP Pruning:**

Thành phần này ngăn chặn sự tràn ngập thông tin quảng bá không cần thiết từ một VLAN trên tất cả các trunks trong miền VTP.

- **VTP Advertisements:**

Chế độ VTP này sử dụng một hệ thống phân cấp các quảng cáo để đồng bộ hóa và phân phối các cấu hình VLAN trong mạng. Thành phần này phân phối tên miền VTP và bộ cấu hình VLAN thay đổi thành các thiết bị chuyển mạch hỗ trợ VTP.

- Ba loại chế độ VTP là:
 - **VTP Server:** VTP servers help you to advertise the VTP domain VLAN information.

- **VTP Client:** VTP clients function in the same way as VTP servers. A VTP client also enables you to store the VLAN information for the entire domain when the Switch is on.
- **VTP Transparent:** Transparent switches help you to forward VTP to VTP clients and also to VTP servers. Whenever Switch is running in the transparent mode, you can create and modify VLANs on that Switch.
- Ưu điểm lớn nhất của VTP là nó giúp bạn phân chia mạng thành quản lý VLAN mạng nhỏ hơn.
- Điều quan trọng là phải kiểm tra các phiên bản VTP không tương thích và các vấn đề liên quan đến mật khẩu.
- Phiên bản V3 cung cấp khả năng tương thích ngược và cung cấp khả năng xử lý tài nguyên được tối ưu hóa và truyền thông tin hiệu quả hơn.

IP Address

Địa chỉ IP (viết tắt của Internet Protocol) có nghĩa là giao thức Internet. IP là một địa chỉ đơn nhất mà những thiết bị điện tử như điện thoại, laptop hiện nay đang sử dụng để **nhận diện và liên lạc với nhau trên mạng máy tính** bằng cách sử dụng giao thức Internet.


Địa chỉ IP **cung cấp danh tính của các thiết bị được kết nối mạng**, giúp các thiết bị trên mạng Internet phân biệt và nhận ra nhau, từ đó có thể giao tiếp với nhau.

Ưu điểm

- IP là giao thức kết nối, giao tiếp giữa các thiết bị mạng qua Internet.
- IP giúp truy cập Internet dễ dàng hơn.
- Địa chỉ IP giúp người dùng có thể quản lý hệ thống mạng đơn giản và chặt chẽ.
- IP ra đời là một sự phát triển vượt bậc của ngành công nghệ mạng.

Nhược điểm

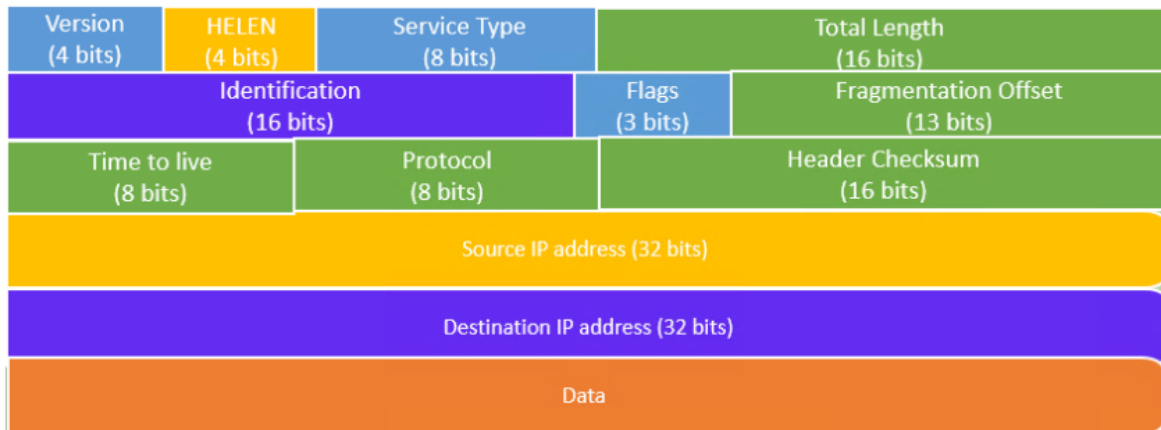
- Thông tin cá nhân dễ dàng bị khai thác nếu chẳng may bị ai đó xâm nhập và phá hoại.
- Hoạt động truy cập của người dùng sẽ bị lưu lại địa chỉ IP.

<u>Aa</u> Loại địa chỉ IP	 Sự mô tả
<u>Public IP</u>	Địa chỉ IP công cộng là địa chỉ mà nhà cung cấp dịch vụ internet sử dụng để chuyển đi các y/c trên internet đến một gia đình hoặc tổ chức cụ thể. Đây là địa chỉ mà mạng gia đình hay tổ chức sử dụng để kết nối với các thiết bị kết nối internet khác cho phép các thiết bị trong mạng truy cập mạng hay liên lạc trực tiếp với máy tính người dùng khác
<u>Private IP</u>	Địa chỉ IP private là địa chỉ riêng sử dụng trong nội bộ mạng LAN như mạng gia đình nhà trường công ty. Khác vs public IP private không thể kết nối với mạng internet mà chỉ có các thiết bị trong mạng mới có thể giao tiếp với nhau thông qua bộ định tuyến router. Địa chỉ Ip private được bộ định tuyến gán tự động hoặc có thể tự thiết lập lại thủ công
<u>Dynamic IP</u>	Địa chỉ IP động có thể thay đổi. Nếu không sử dụng các dịch vụ đặc biệt cần dùng IP tĩnh khách hàng thông thường chỉ đc ISP gán cho các IP khác nhau sau mỗi lần kết nối hoặc trong một phiên kết nối sẽ được đổi IP khác. Hành động cấp IP động của các ISP nhằm tiết kiệm nguồn địa chỉ IP đang cạn kiệt hiện nay. Khi một máy tính không được kết nối vào mạng thì nhà cung cấp sẽ sử dụng IP đó để cấp cho 1 người dùng khác
<u>Static IP</u>	Địa chỉ IP tĩnh cố định dành riêng cho một người hoặc nhóm sử dụng mà thiết bị kết nối đến internet của họ luôn được đặt một địa chỉ IP. thông thường ip tĩnh được cấp cho một máy chủ với một mục đích riêng như máy chủ web, mail... để nhiều người có thể truy cập mà không làm gián đoạn các quá trình đó

IP Packet Header

IP Header là thông tin meta ở đầu gói IP. Nó hiển thị thông tin như phiên bản IP, độ dài của gói, nguồn và đích.

Định dạng tiêu đề IPV4 có độ dài từ 20 đến 60 byte. Nó chứa thông tin cần thiết để định tuyến và phân phối. Nó bao gồm 13 trường như Phiên bản, Độ dài tiêu đề, tổng khoảng cách, nhận dạng, cờ, tổng kiểm tra, địa chỉ IP nguồn, địa chỉ IP đích. Nó cung cấp dữ liệu cần thiết để truyền dữ liệu



Sau đây là các thành phần / trường khác nhau của tiêu đề gói IP

- Version

Trường tiêu đề IP đầu tiên là chỉ báo phiên bản 4 bit. Trong IPv4, giá trị của bốn bit của nó được đặt thành 0100, cho biết 4 ở dạng nhị phân. Tuy nhiên, nếu bộ định tuyến không hỗ trợ phiên bản được chỉ định, gói tin này sẽ bị loại bỏ.

- length header

tiêu đề Internet, gọi tắt là IHL, có kích thước 4 bit. Nó còn được gọi là HELEN (Độ dài tiêu đề). Thành phần IP này được sử dụng để hiển thị có bao nhiêu từ 32 bit trong tiêu đề.

- Service type

Loại dịch vụ còn được gọi là Điểm mã dịch vụ khác biệt hoặc DSCP. Trường này được cung cấp các tính năng liên quan đến chất lượng dịch vụ cho luồng dữ liệu hoặc cuộc gọi VoIP. 3 bit đầu tiên là các bit ưu tiên. Nó cũng được sử dụng để chỉ định cách bạn có thể xử lý Datagram.

- Total length

Tổng chiều dài được đo bằng byte. Kích thước tối thiểu của một sơ đồ IP là 20 byte và tối đa có thể là 65535 byte. HELEN và Tổng chiều dài có thể được sử dụng để tính toán kích thước của payload

Tất cả các máy chủ được yêu cầu để có thể đọc các biểu đồ dữ liệu 576 byte. Tuy nhiên, nếu một gói dữ liệu quá lớn đối với các máy chủ trong mạng, thì phương pháp phân mảnh được sử dụng rộng rãi.

- Identification

Nhận dạng là một gói được sử dụng để xác định các đoạn của một sơ đồ dữ liệu IP duy nhất. Một số đã khuyến nghị sử dụng trường này cho những việc

khác như thêm thông tin để theo dõi gói, v.v.

- **IP Flags:**

Flags là một trường ba bit giúp bạn kiểm soát và xác định các fragment.

Sau đây có thể là cấu hình khả thi của chúng:

Bit 0: được đặt trước và phải được đặt thành 0

Bit 1: nghĩa là không phân mảnh

Bit 2: có nghĩa là nhiều mảnh hơn.

- **Fragment offset - Phần bù phân mảnh:**

Phần bù phân mảnh biểu thị số byte dữ liệu phía trước phân đoạn cụ thể trong Sơ đồ dữ liệu cụ thể. Nó được chỉ định theo số lượng 8 byte, có giá trị tối đa là 65,528 byte.

- **TTL**

Đây là trường 8 bit cho biết thời gian tối đa Datagram sẽ tồn tại trong hệ thống internet. Khoảng thời gian được tính bằng giây và khi giá trị của TTL bằng 0, Datagram sẽ bị xóa.

Mỗi khi một sơ đồ dữ liệu được xử lý, giá trị TTL của nó sẽ giảm đi một giây. TTL được sử dụng để các sơ đồ dữ liệu không được phân phối và loại bỏ tự động. Giá trị của TTL có thể từ 0 đến 255.

- **Protocol**

Tiêu đề IPv4 này được dành riêng để biểu thị rằng giao thức internet được sử dụng trong phần sau của Sơ đồ dữ liệu. Ví dụ: chữ số 6 chủ yếu được sử dụng để biểu thị TCP và 17 được sử dụng để biểu thị giao thức UDP.

- **Header Checksum:**

Thành phần tiếp theo là trường tổng kiểm tra tiêu đề 16 bit, được sử dụng để kiểm tra tiêu đề xem có bất kỳ lỗi nào không. Tiêu đề IP được so sánh với giá trị tổng kiểm tra của nó. Khi tổng kiểm tra tiêu đề không phù hợp, thì gói tin sẽ bị loại bỏ.

- **Source address**

Địa chỉ nguồn là địa chỉ 32 bit của nguồn được sử dụng cho gói IPv4.

- **Destination Address**

Địa chỉ đích cũng có kích thước 32 bit lưu trữ địa chỉ của người nhận.

- IP options

Đây là trường tùy chọn của tiêu đề IPv4 được sử dụng khi giá trị của IHL (Độ dài tiêu đề Internet) được đặt thành lớn hơn 5. Nó chứa các giá trị và cài đặt liên quan đến bảo mật, tuyến bản ghi và dấu thời gian, v.v. Bạn có thể thấy rằng danh sách các thành phần tùy chọn kết thúc bằng End of Options hoặc EOL trong hầu hết các trường hợp.

- **Dữ liệu:**

Trường này lưu trữ dữ liệu từ lớp giao thức, lớp này đã chuyển giao dữ liệu cho lớp IP.

IPV4

IPv4 là phiên bản đầu tiên của IP. Nó đã được triển khai để sản xuất trong ARPANET vào năm 1983. Ngày nay nó là phiên bản IP được sử dụng rộng rãi nhất. Nó được sử dụng để xác định các thiết bị trên mạng bằng hệ thống định địa chỉ.

IPv4 sử dụng lược đồ địa chỉ 32 bit cho phép lưu trữ 2^{32} địa chỉ, tức là hơn 4 tỷ địa chỉ. Đến nay, nó được coi là Giao thức Internet chính và thực hiện 94% lưu lượng truy cập Internet.

IPV6

Đây là phiên bản mới nhất của Giao thức Internet. Internet Engineer Taskforce đã khởi xướng nó vào đầu năm 1994. Việc thiết kế và phát triển bộ ứng dụng đó bây giờ được gọi là IPv6.

Phiên bản địa chỉ IP mới này đang được triển khai để đáp ứng nhu cầu về nhiều địa chỉ Internet hơn. Nó nhằm mục đích giải quyết các vấn đề liên quan đến IPv4. Với không gian địa chỉ 128-bit, nó cho phép 340 triệu không gian địa chỉ duy nhất.

Routing Protocols Types - Static, Dynamic

Routing Protocols là tập hợp các quy tắc xác định được sử dụng bởi các bộ định tuyến để giao tiếp giữa nguồn và đích. Họ không di chuyển thông tin từ nguồn đến đích mà chỉ cập nhật bảng định tuyến có chứa thông tin.

Các giao thức của Bộ định tuyến mạng giúp xác định cách các bộ định tuyến giao tiếp với nhau. Nó cho phép mạng chọn các route giữa hai nodes bất kỳ trên mạng máy tính.

Static Routing Protocols được sử dụng khi quản trị viên chỉ định thủ công đường dẫn từ nguồn đến mạng đích. Nó cung cấp bảo mật hơn cho mạng.

Thuận lợi

- Không có bảng thông không sử dụng giữa các liên kết.
- Chỉ quản trị viên mới có thể thêm các route

Nhược điểm

- Quản trị viên phải biết từng bộ định tuyến được kết nối như thế nào.
- Không phải là một lựa chọn lý tưởng cho các mạng lớn vì nó tốn nhiều thời gian.
- Bất cứ khi nào liên kết không thành công, tất cả mạng sẽ bị gián đoạn, điều này không khả thi trong các mạng nhỏ.

Dynamic Routing Protocols là một loại giao thức định tuyến quan trọng khác. Nó giúp các bộ định tuyến tự động thêm thông tin vào bảng định tuyến của chúng từ các bộ định tuyến được kết nối. Các loại giao thức này cũng gửi các bản cập nhật cấu trúc liên kết bất cứ khi nào mạng thay đổi cấu trúc cấu trúc liên kết.

Thuận lợi:

- Dễ dàng cấu hình hơn ngay cả trên các mạng lớn hơn.
- Nó sẽ có thể tự động chọn một tuyến đường khác trong trường hợp nếu một liên kết bị trục trặc.
- Nó giúp load balancing giữa nhiều liên kết.

Bất lợi:

- Các bản cập nhật được chia sẻ giữa các bộ định tuyến, vì vậy nó tiêu tốn băng thông.
- Các giao thức định tuyến đặt một tải bổ sung lên CPU hoặc RAM của bộ định tuyến.

Address Resolution Protocol:

- ARP (viết tắt của cụm từ Address Resolution Protocol) là giao thức mạng được dùng để tìm ra địa chỉ phần cứng (địa chỉ MAC) của thiết bị từ một địa chỉ IP nguồn. Nó được sử dụng khi một thiết bị giao tiếp với các thiết bị khác dựa trên

nền tảng local network. Ví dụ như trên mạng Ethernet mà hệ thống yêu cầu địa chỉ vật lý trước khi thực hiện gửi packets.

- ARP cho phép một mạng quản lý các kết nối độc lập với những thiết bị vật lý cụ thể được gắn vào từng mạng. Điều này cho phép giao thức Internet vận hành hiệu quả hơn so với việc nó phải tự quản lý địa chỉ của các thiết bị phần cứng và mạng vật lý.

Cả hai trường hợp, đều thấy được là thiết bị phải gửi gói tin IP đến một thiết bị IP khác trên cùng mạng nội bộ. Chúng ta biết rằng việc gửi gói tin trong cùng mạng thông qua Switch là dựa vào địa chỉ MAC hay là địa chỉ phần cứng của thiết bị. Sau khi gói tin được đóng gói thì hệ thống mới bắt đầu được chuyển qua quá trình phân giải địa chỉ ARP và thực hiện chuyển đi.

ARP về cơ bản là một quá trình có 2 chiều request/response giữa các thiết bị trong cùng mạng nội bộ. Thiết bị nguồn request bằng cách gửi một bản tin local broadcast lên trên toàn mạng. Thiết bị đích response bằng một bản tin unicast để trả lại cho thiết bị nguồn.

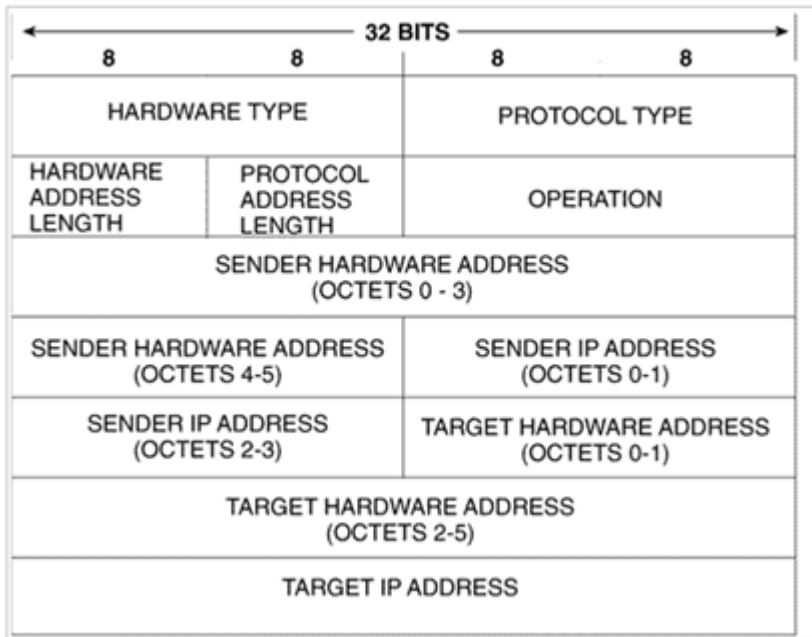
Các loại bản tin ARP

Có hai dạng bản tin trong ARP cơ bản nhất: một là được gửi từ nguồn đến đích, i từ đích tới nguồn.

- Request: Khi hệ thống khởi tạo quá trình, gói tin được gửi từ máy nguồn tới thiết bị đích
- Reply: Khi quá trình đáp trả gói tin ARP request, được gửi từ thiết bị đích đến máy nguồn

Có 4 loại địa chỉ nằm trong một bản tin ARP đó là:

- Sender Hardware Address: Đây là địa chỉ lớp hai của thiết bị gửi bản tin
- Sender Protocol Address: Đây là địa chỉ lớp ba (hay còn gọi là địa chỉ logic) của thiết bị gửi bản tin
- Target Hardware Address: Địa chỉ lớp hai (hay còn được gọi là địa chỉ phần cứng) của thiết bị đích của bản tin
- Target Protocol Address: Địa chỉ lớp ba (hay gọi là địa chỉ logic) của thiết bị đích của bản tin



Các bước hoạt động của giao thức mạng ARP

1. Source Device Checks Cache: Trong bước này, thiết bị sẽ thực hiện kiểm tra cache (bộ đệm) của mình. Nếu đã có địa chỉ IP đích tương ứng với MAC nào đó rồi thì lập tức hệ thống chuyển sang bước 9.
2. Source Device Generates ARP Request Message: Hệ thống bắt đầu khởi tạo gói tin ARP Request với các trường địa chỉ như trên.
3. Source Device Broadcasts ARP Request Message: Thiết bị nguồn truyền gói tin ARP Request trên toàn mạng
4. Local Devices Process ARP Request Message: Các thiết bị trong mạng đều sẽ nhận được gói tin ARP Request. Gói tin được xử lý bằng cách đưa thiết bị vào trường địa chỉ Target Protocol Address. Nếu trùng với địa chỉ của mình thì tiếp tục xử lý, nếu không thì hủy gói tin
5. Destination Device Generates ARP Reply Message: Nếu Thiết bị với IP trùng với IP trong trường Target Protocol Address sẽ thực hiện quá trình khởi tạo gói tin ARP Reply. Đồng thời thiết bị sẽ lấy địa chỉ datalink của mình để tiến hành đưa vào trường Sender Hardware Address
6. Destination Device Updates ARP Cache: Thiết bị đích cập nhật bảng ánh xạ địa chỉ IP và MAC của thiết bị nguồn vào bảng ARP cache của mình để giảm bớt thời gian xử lý cho những lần sau.
7. Destination Device Sends ARP Reply Message: Thiết bị đích sẽ bắt đầu gửi gói tin Reply đã được khởi tạo đến thiết bị nguồn.

8. Source Device Processes ARP Reply Message: Thiết bị nguồn nhận được gói tin reply và tiến hành xử lý bằng cách lưu trường Sender Hardware Address trong gói reply như những địa chỉ phần cứng của thiết bị đích
9. Source Device Updates ARP Cache: Thiết bị nguồn update vào ARP cache giá trị tương ứng giữa địa chỉ network và cả địa chỉ datalink của thiết bị đích. Do đó, những lần tiếp theo sẽ không còn cần tới request.

MAC address and IP address

Địa chỉ MAC là số nhận dạng duy nhất được gán cho NIC (Thẻ / Bộ điều khiển giao diện mạng). Nó bao gồm một địa chỉ 48 bit hoặc 64 bit, được liên kết với bộ điều hợp mạng. Địa chỉ MAC có thể ở định dạng thập lục phân. Dạng đầy đủ của địa chỉ MAC là địa chỉ Kiểm soát truy cập phương tiện. Địa chỉ MAC thường có sáu bộ gồm hai chữ số / ký tự được phân tách bằng dấu hai chấm.

Địa chỉ IP là địa chỉ giúp bạn xác định kết nối mạng. Nó được gọi là 'Địa chỉ logic', được cung cấp cho một kết nối trong mạng. Địa chỉ IP giúp bạn kiểm soát cách các thiết bị trên Internet giao tiếp và xác định hành vi của bộ định tuyến internet..

Sự khác biệt chính

Địa chỉ MAC địa chỉ IP

là số nhận dạng phần cứng duy nhất được gán cho NIC (Thẻ / Bộ điều khiển giao diện mạng), trong khi

là địa chỉ giúp bạn xác định kết nối mạng.



Địa chỉ MAC được chỉ định bởi nhà sản xuất giao diện phần cứng trong khi địa chỉ IP được chỉ định bởi quản trị viên mạng hoặc Nhà cung cấp dịch vụ Internet (ISP).

Địa chỉ Mac xác định danh tính thiết bị, nhưng địa chỉ IP mô tả cách thiết bị được kết nối với mạng.

Địa chỉ MAC có thể được sử dụng để phát sóng, mặt khác, địa chỉ IP có thể được sử dụng để phát sóng hoặc phát đa hướng.

Địa chỉ MAC được thực hiện trong lớp Liên kết dữ liệu của mô hình tham chiếu OSI hoặc TCP / IP. Ngược lại, địa chỉ IP được thực hiện trong lớp Mạng của mô hình TCP / IP hoặc OSI.

Aa Địa chỉ MAC	≡ Địa chỉ IP
-----------------------	---------------------

 Địa chỉ MAC	 Địa chỉ IP
<u>Địa chỉ MAC là số nhận dạng duy nhất được gán cho Thẻ / Bộ điều khiển Giao diện Mạng.</u>	Địa chỉ IP được gán cho các thiết bị được kết nối với mạng máy tính sử dụng IP để giao tiếp. hoạt động như định danh cho một máy cụ thể trên một mạng cụ thể
<u>Dạng đầy đủ của địa chỉ MAC là Địa chỉ kiểm soát truy cập phương tiện.</u>	Dạng địa chỉ IP đầy đủ là Địa chỉ giao thức Internet.
<u>Nó được chỉ định bởi nhà sản xuất phần cứng giao diện.</u>	Nó được chỉ định bởi quản trị viên mạng hoặc nhà cung cấp dịch vụ internet (ISP).
<u>Thông tin được gửi bằng Ethernet sử dụng địa chỉ mac.</u>	Thông tin được gửi qua Internet bằng địa chỉ IP.
<u>Địa chỉ Mac được phân tách bằng dấu hai chấm.</u>	Địa chỉ Ip được phân tách bằng dấu chấm.
<u>Bạn không thể ẩn địa chỉ mac khỏi thiết bị.</u>	Có thể ẩn địa chỉ IP bằng bộ định tuyến hoặc VPN.
<u>Địa chỉ MAC không linh hoạt, có thể tự thay đổi</u>	Địa chỉ IP linh hoạt. Nó luôn được thay đổi bất cứ khi nào nó kết nối với một số mạng khác.
<u>Địa chỉ Mac giúp bạn xác định thiết bị trong mạng cục bộ.</u>	Địa chỉ IP giúp bạn xác định thiết bị trong mạng toàn cầu.

What is IP Routing? Types, Routing Table, Protocols, Commands

IP Routing là một quá trình gửi các gói từ một máy chủ trên một mạng đến một máy chủ khác trên một mạng từ xa khác. Nó giúp bạn kiểm tra địa chỉ IP đích của một gói tin, xác định địa chỉ bước tiếp theo và chuyển tiếp nó. Các bộ định tuyến IP sử dụng các bảng định tuyến để xác định địa chỉ bước tiếp theo mà gói tin sẽ được chuyển đến.

Trong định tuyến IP CISCO, dữ liệu được định tuyến từ nguồn đến đích thông qua bộ định tuyến và qua nhiều mạng. Các giao thức Định tuyến IP cho phép các bộ định tuyến xây dựng một bảng chuyển tiếp tương quan các điểm đến cuối cùng với các địa chỉ bước tiếp theo.

- Định tuyến IP là một quá trình gửi các gói từ một máy chủ trên một mạng đến một máy chủ khác trên một mạng từ xa khác.
- Các số liệu định tuyến khác nhau là: 1) Số lần truy cập 2) Bảng thông 3) Tải trọng 4) Chi phí và 5) Độ tin cậy.

- Cổng mặc định là một bộ định tuyến mà các máy chủ sử dụng để giao tiếp với các máy chủ khác trên các mạng từ xa.
- Bảng định tuyến được sử dụng bởi các bộ định tuyến để quyết định đường dẫn đến mạng đích.
- Một số giao thức định tuyến quan trọng là 1) Giao thức Internet 2) Giao thức mở đường dẫn ngắn nhất (OSPF) 3) RIP (Giao thức thông tin định tuyến) 4) Hệ thống trung gian từ hệ thống trung gian (ISIS) 5) Giao thức định tuyến cổng nội bộ nâng cao (EIGRP) và 5) Giao thức cửa khẩu biên giới (BGP).
- Định tuyến IP cung cấp các bản cập nhật định tuyến động của các đường dẫn mạng.
- Bộ định tuyến là thiết bị mạng máy tính phục vụ hai chức năng chính: 1) Tạo và duy trì mạng cục bộ, và 2) Quản lý dữ liệu ra vào mạng.
- Bộ định tuyến giúp xác định rằng thông tin có đến được đích đã định hay không.

Các gói IP được định tuyến như thế nào trên Internet?

Địa chỉ IP định tuyến các gói dữ liệu truyền từ máy tính này (Máy chủ / Máy chủ) sang máy tính khác cho đến khi nó đến đích trên Internet bằng thuật toán định tuyến.

Giao thức mạng nào được sử dụng để định tuyến địa chỉ IP?

Giao thức được sử dụng để định tuyến các địa chỉ IP được gọi là Giao thức Internet (IP), chỉ định nguồn gốc và điểm đến của mỗi gói dữ liệu. Các địa chỉ IP này định tuyến các gói dữ liệu từ một máy tính (hệ thống nguồn) đến một máy tính khác (hệ thống đích) trên Internet.

Subnetting: What is Subnet Mask?

Subnetting là thực tế chia một mạng thành hai hoặc các mạng nhỏ hơn. Nó làm tăng hiệu quả định tuyến, giúp tăng cường bảo mật của mạng và giảm kích thước của miền quảng bá.

IP Subnetting chỉ định các bit bậc cao từ máy chủ lưu trữ như một phần của tiền tố mạng. Phương pháp này chia một mạng thành các mạng con nhỏ hơn.

Nó cũng giúp giảm kích thước của các bảng định tuyến, được lưu trữ trong các bộ định tuyến. Phương pháp này cũng giúp mở rộng cơ sở địa chỉ IP hiện có và cấu trúc lại địa chỉ IP.

- Mạng con IP là hoạt động chia một mạng thành hai hoặc các mạng nhỏ hơn.
- Mạng con giúp bạn tối đa hóa hiệu quả địa chỉ IP.
- Mặt nạ mạng con là một địa chỉ 32 bit được sử dụng để phân biệt giữa địa chỉ mạng và địa chỉ máy chủ lưu trữ trong địa chỉ IP.
- Mặt nạ mạng con được bộ định tuyến sử dụng để che địa chỉ mạng. Nó cho thấy những bit nào được sử dụng để xác định mạng con.

Computer Network Differences

Modem vs Router – Difference Between Them

Modem

Modem (viết tắt của Modulator and Demodulator – Bộ điều giải) là một thiết bị điều chế sóng tín hiệu tương tự để mã hóa dữ liệu số, và giải điều chế tín hiệu mạng để giải mã tín hiệu số.

biến đổi thông tin kỹ thuật số từ các thiết bị kết nối mạng (máy tính, điện thoại) thành tín hiệu analog có thể truyền qua dây dẫn, và ngược lại, modem dịch các tín hiệu analog thành dữ liệu số mà những thiết bị như máy tính có thể hiểu được.

Cơ chế hoạt động

- **Modem:** Chuyển đổi tín hiệu kỹ thuật số của máy tính, điện thoại... thành tín hiệu analog.
- **Router:** Kiểm tra gói thông tin và xác minh đường dẫn của gói đó để truyền thành công đến thiết bị đích.

Tóm lại, router là để phân luồng các gói thông tin, gán IP cho các thiết bị trong hệ thống mạng. Tuy nhiên các thông tin truyền tải (trong cáp đồng, cáp quang) là analog (nó là dạng thông tin liên tục), nó khác với định dạng mà máy tính, điện thoại xử lý là digital (0 và 1) nên cần một thiết bị để đổi giữa hai thứ này. Các gói thông tin gửi đi sẽ được modem chuyển từ digital sang analog để truyền đi trong internet; khi các gói thông tin truyền từ internet về máy bạn thì ngược lại, modem chuyển từ analog sang digital để máy tính, điện thoại đọc được thông tin.

Vị trí kết nối

- **Modem:** Modem được kết nối trực tiếp với nhà mạng thông qua đường dây cáp quang, dây đồng... (hoặc cũng có thể không dây).
- **Router:** Router được đặt giữa modem và hệ thống mạng. Mạng có thể là một tập hợp các máy tính hoặc một tập hợp gồm máy tính và switch, v.v... Modem và router được kết nối vật lý với nhau. Do đó, các thiết bị được kết hợp với router có thể truy cập Internet qua modem. Router có cổng Gigabit và Ethernet để kết nối với các thiết bị và hệ thống mạng khác. Các router phổ biến hiện nay cũng có WiFi để kết nối không dây.
- Đôi khi Modem và Router được tích hợp chung vào một thiết bị, đó là cái “cục Wi-Fi” có thể cắm trực tiếp cáp quang vào mà nhà mạng trang bị cho bạn. Nhưng thường những “cục” này khá hạn chế về khả năng phát Wi-Fi, vì vậy các bạn cũng nên sắm thêm một Router riêng để tận dụng tối đa băng thông.

Chế độ kết nối

- **Modem:** Modem có các chế độ kết nối vật lý sau: Bán song công (Half Duplex), song công toàn phần (Full Duplex), 4 dây và 2 dây.
- **Router:** Các chế độ kết nối của Router là: User Execution, Administrative, Global Configuration.

Tuy có sự khác biệt nhưng đôi khi modem và router được tích hợp chung vào một thiết bị. Đây là modem được chứa trong một bộ định tuyến, cho phép nhiều máy tính / thiết bị kết nối trong một mạng cục bộ (mạng LAN) và cả mạng diện rộng Internet. Đây là công nghệ khá phổ biến hiện nay vì nó giúp việc thiết lập mạng không còn phức tạp bởi quá nhiều thiết bị bao gồm modem và router riêng biệt. Dưới đây là hình ảnh thiết bị tích hợp cả modem và router.

Chức năng của Modem

Với các thông tin ở bản ở mục 1 có lẽ phần nào bạn đã hiểu được chức năng chính của modem rồi phải không nào? Bên cạnh chức năng chính là điều chế tín hiệu mạng, modem còn có một số chức năng sau:

- Nén dữ liệu: Chức năng này nhằm giảm lượng thời gian gửi dữ liệu và giảm lượng lỗi trong tín hiệu..
- Kiểm soát lưu lượng mạng
- Truyền dữ liệu và sao lưu
- Quản lý từ xa

- Sửa lỗi: Khi thông tin được truyền giữa các modem, đôi khi nó có thể bị hỏng – nghĩa là các phần của dữ liệu bị thay đổi hoặc mất. Trong trường hợp này, modem cần sử dụng đến tính năng sửa lỗi để khắc phục nó.

Ưu điểm

Modem là con đường giao tiếp dữ liệu được sử dụng rộng rãi nhất bởi các ưu điểm mà nó mang lại như sau:

- Chuyển đổi tín hiệu hiệu quả, nhanh chóng
- Tốc độ truyền mạng cao
- Cung cấp nhiều gói cước internet linh hoạt về giá cả, phù hợp với nhiều mục đích sử dụng khác nhau
- Một số modem hoàn toàn tương thích với công nghệ fax. Tin nhắn fax có thể được gửi và nhận ngay lập tức bằng modem.

Nhược điểm

Bên cạnh các ưu điểm nêu trên thì Modem cũng có 1 số nhược điểm sau:

- Một nhược điểm lớn của việc kết nối modem là nó có thể khiến máy tính của bạn dễ bị tin tặc và phần mềm độc hại tấn công. Tuy nhiên, để chống lại điều này, hầu hết các modem và bộ định tuyến đều có tường lửa tích hợp. Ngoài tường lửa, phần mềm bảo mật có thể được sử dụng cho mục đích này.
- Khó khăn trong việc nâng cấp, phụ thuộc rất nhiều vào nhà cung cấp dịch vụ mạng ISP
- Các dòng Modem bên ngoài thiếu tính di động.
- Các dòng Modem DSL không khả dụng ở các vùng nông thôn hoặc vùng sâu vùng xa.

Router:



Bộ định tuyến là một thiết bị mạng máy tính phục vụ hai chức năng chính: (1) tạo và duy trì mạng cục bộ và (2) quản lý dữ liệu ra vào mạng cũng như dữ liệu di chuyển bên trong mạng. Nó cũng giúp bạn xử lý nhiều mạng và định tuyến lưu lượng mạng giữa chúng. Trong mạng gia đình của bạn, bộ định tuyến của bạn có một kết nối với Internet và một kết nối với mạng nội bộ riêng của bạn. Hơn nữa, hầu hết các bộ định tuyến cũng chứa các công tắc tích hợp cho phép bạn kết nối nhiều thiết bị có dây.

- Tạo mạng cục bộ (LAN).
- Nó cho phép bạn chia kết nối internet của mình cho tất cả các thiết bị của bạn.
- Kết nối các phương tiện / thiết bị khác nhau với nhau
- Chạy tường lửa.
- Bộ định tuyến xác định nơi gửi thông tin từ máy tính này sang máy tính khác
- Chuyển tiếp gói, Chuyển và lọc.
- Bộ định tuyến cũng đảm bảo rằng thông tin sẽ đến đích đã định.
- Kết nối với VPN

Một bộ định tuyến kết nối nhiều mạng và theo dõi lưu lượng mạng giữa chúng. Nó có một kết nối với internet và một kết nối với mạng nội bộ riêng của bạn.

Hơn nữa, nhiều bộ định tuyến cũng chứa các công tắc tích hợp cho phép bạn kết nối nhiều thiết bị có dây. Nhiều bộ định tuyến cũng chứa radio không dây cho phép bạn kết nối các thiết bị Wi-Fi.

so sánh


 Modem	 Bộ định tuyến
<u>Một Modem điều chế và giải điều chế tín hiệu.</u>	Bộ định tuyến là một thiết bị mạng cho phép bạn kết hợp nhiều mạng với nhau cho mạng LAN và WAN.
<u>Nó được sử dụng để truy cập Internet vì nó kết nối máy tính của bạn với ISP.</u>	Bạn có thể truy cập Internet mà không cần modem.
<u>Modem hoạt động trên lớp Datalink.</u>	Bộ định tuyến có thể được vận hành ở Lớp liên kết dữ liệu, Lớp mạng và Lớp vật lý.
<u>Modem không giúp kiểm tra gói dữ liệu. Do đó, mối đe dọa an ninh luôn hiện hữu.</u>	Bộ định tuyến kiểm tra tất cả gói dữ liệu trước khi chuyển tiếp nó, giúp xác định mối đe dọa.
<u>Nó được đặt giữa đường dây điện thoại và bộ định tuyến hoặc trực tiếp đến máy tính.</u>	Nó được đặt giữa mạng máy tính và modem.

Hub vs Switch

Hub là một thiết bị mạng cho phép bạn kết nối nhiều PC với một mạng duy nhất. Nó được sử dụng để kết nối các phân đoạn của mạng LAN. Một trung tâm lưu trữ các

cổng khác nhau, vì vậy khi một gói tin đến một cổng, nó sẽ được sao chép sang nhiều cổng khác. Hub hoạt động như một điểm kết nối chung cho các thiết bị trong mạng.

Switch là một thiết bị mạng máy tính kết nối nhiều thiết bị với nhau trên một mạng máy tính duy nhất. Nó cũng có thể được sử dụng để định tuyến thông tin dưới dạng dữ liệu điện tử được gửi qua mạng. Vì quá trình liên kết các phân đoạn mạng còn được gọi là bắc cầu, các thiết bị chuyển mạch thường được gọi là thiết bị bắc cầu.

<u>Aa</u> Hub	 switch
<u>Một trung tâm hoạt động trên lớp vật lý.</u>	Một công tắc hoạt động trên lớp liên kết dữ liệu.
<u>Chỉ một miền va chạm đơn lẻ hiện diện trong một trung tâm.</u>	Các cổng khác nhau có các miền xung đột riêng biệt.
<u>Transmission mode is Half-duplex</u>	Transmission mode is Full duplex
<u>Hubs operates as a Layer 1 devices per the OSI model.</u>	Network switches help you to operate at Layer 2 of the OSI model.
<u>Để kết nối một mạng máy tính cá nhân nên được tham gia thông qua một central hub.</u>	Cho phép kết nối nhiều thiết bị và port.
<u>Có xảy ra xung đột</u>	Không có xung đột
<u>Hub is a passive device</u>	A switch is an active device
<u>A network hub can't store MAC addresses.</u>	Bộ chuyển mạch sử dụng CAM (Content Accessible Memory- Bộ nhớ có thể truy cập nội dung) có thể được truy cập bằng ASIC (Bộ chip tích hợp dành riêng cho ứng dụng).
<u>Không phải là một thiết bị thông minh</u>	Thiết bị thông minh
<u>Tốc độ của nó lên đến 10 Mbps</u>	10/100 Mbps, 1 Gbps, 10 Gbps
<u>Không sử dụng phần mềm</u>	Có phần mềm để quản trị

Ưu điểm của HUB

- Cung cấp khả năng mở rộng Internet được chia sẻ
- Cho phép giám sát mạng

- Cung cấp khả năng tương thích ngược
- Giúp bạn mở rộng tổng khoảng cách của mạng

Nhược điểm của HUB

- Nó chủ yếu là half-Duplex
- Không cung cấp băng thông chuyên dụng
- Nó không thể chọn Network's Best Path.
- Không có bất kỳ cơ chế nào để giảm lưu lượng mạng.

Ưu điểm của Switch

- Nó giúp bạn giảm số lượng broadcast domains
- Hỗ trợ VLAN có thể giúp logical segmentation of port
- Các thiết bị chuyển mạch có thể sử dụng bảng CAM để ánh xạ Cổng đến MAC

Nhược điểm của Switch

- Không tốt như một bộ định tuyến để hạn chế broadcast
- Giao tiếp giữa các VLAN yêu cầu định tuyến giữa các VLAN, nhưng ngày nay, có rất nhiều thiết bị chuyển mạch Đa lớp có sẵn trên thị trường.
- Xử lý các gói Multicast đòi hỏi khá nhiều cấu hình và thiết kế phù hợp.

IPv4 vs IPv6

IPv4 là phiên bản IP được sử dụng rộng rãi để xác định các thiết bị trên mạng bằng hệ thống định địa chỉ. Đây là phiên bản IP đầu tiên được triển khai để sản xuất trong ARPANET vào năm 1983. Nó sử dụng lược đồ địa chỉ 32 bit để lưu trữ 2^{32} địa chỉ, tức là hơn 4 tỷ địa chỉ. Nó được coi là Giao thức Internet chính và thực hiện 94% lưu lượng truy cập Internet.

- Giao thức không kết nối
- Cho phép tạo một lớp giao tiếp ảo đơn giản trên các thiết bị đa dạng
- Nó yêu cầu ít bộ nhớ hơn và dễ nhớ địa chỉ
- Giao thức đã được hỗ trợ bởi hàng triệu thiết bị
- Cung cấp thư viện video và hội nghị

IPv6 là phiên bản mới nhất của Giao thức Internet. Phiên bản địa chỉ IP mới này đang được triển khai để đáp ứng nhu cầu về nhiều địa chỉ Internet hơn. Nó nhằm

giải quyết các vấn đề liên quan đến IPv4. Với không gian địa chỉ 128-bit, nó cho phép 340 triệu không gian địa chỉ duy nhất. IPv6 còn được gọi là IPng (Giao thức Internet thế hệ tiếp theo).

- Cơ sở hạ tầng định tuyến và địa chỉ phân cấp
- Cấu hình trạng thái và không trạng thái
- Hỗ trợ chất lượng dịch vụ (QoS)
- Một giao thức lý tưởng cho tương tác nút lân cận

SỰ KHÁC BIỆT CHÍNH

- IPv4 là địa chỉ IP 32-Bit trong khi IPv6 là địa chỉ IP 128-Bit.
- IPv4 là một phương pháp đánh địa chỉ số trong khi IPv6 là một phương pháp đánh địa chỉ chữ và số.
- Các bit nhị phân IPv4 được phân tách bằng dấu chấm (.) Trong khi các bit nhị phân IPv6 được phân tách bằng dấu hai chấm (:).
- IPv4 cung cấp 12 trường tiêu đề trong khi IPv6 cung cấp 8 trường tiêu đề.
- IPv4 supports broadcast whereas IPv6 doesn't support broadcast.
- IPv4 has checksum fields while IPv6 doesn't have checksum fields
- Khi so sánh IPv4 và IPv6, IPv4 hỗ trợ VLSM (Variable Length Subnet Mask-Mặt nạ mạng con có độ dài thay đổi) trong khi IPv6 không hỗ trợ VLSM.
- IPv4 sử dụng ARP (Giao thức phân giải địa chỉ) để ánh xạ tới địa chỉ MAC trong khi IPv6 sử dụng NDP (Neighbour Discovery Protocol) để ánh xạ tới địa chỉ MAC.

HTTP vs HTTPS

HTTP

Dạng đầy đủ của HTTP là Hypertext Transfer Protocol- Giao thức truyền siêu văn bản. HTTP cung cấp bộ quy tắc và tiêu chuẩn chi phối cách bất kỳ thông tin nào có thể được truyền trên World Wide Web. HTTP cung cấp các quy tắc tiêu chuẩn để trình duyệt web và máy chủ giao tiếp.

HTTP là một giao thức mạng lớp ứng dụng được xây dựng trên TCP. HTTP sử dụng văn bản có cấu trúc Siêu văn bản thiết lập liên kết logic giữa các nút chứa văn

bản. Nó còn được gọi là “giao thức không trạng thái” vì mỗi lệnh được thực thi riêng biệt, không sử dụng tham chiếu của lệnh chạy trước đó.

- HTTP có thể được triển khai với giao thức khác trên Internet hoặc trên các mạng khác
- Các trang HTTP được lưu trữ trên bộ nhớ cache của máy tính và internet, vì vậy nó có thể truy cập nhanh chóng
- Nền tảng độc lập cho phép chuyển nhiều nền tảng
- Không cần bất kỳ hỗ trợ Runtime nào
- Có thể sử dụng qua tường lửa! Các ứng dụng toàn cầu có thể
- Không định hướng kết nối; vì vậy không cần mạng để tạo và duy trì trạng thái phiên và thông tin

—

- Không có quyền riêng tư vì bất kỳ ai cũng có thể xem nội dung
- Tính toàn vẹn của dữ liệu là một vấn đề lớn vì ai đó có thể thay đổi nội dung. Đó là lý do tại sao giao thức HTTP là một phương pháp không an toàn vì không có phương pháp mã hóa nào được sử dụng.
- Not Connection Oriented; Bất kỳ ai chặn được yêu cầu đều có thể lấy tên người dùng và mật khẩu.

HTTPS

là viết tắt của Hyper Text Transfer Protocol Secure. Đây là phiên bản HTTP cao cấp và an toàn. Nó sử dụng cổng số. 443 để Truyền dữ liệu. Nó cho phép các giao dịch an toàn bằng cách mã hóa toàn bộ thông tin liên lạc với SSL. Nó là sự kết hợp của giao thức SSL / TLS và HTTP. Nó cung cấp nhận dạng được mã hóa và bảo mật của một máy chủ mạng.

HTTP cũng cho phép bạn tạo kết nối được mã hóa an toàn giữa máy chủ và trình duyệt. Nó cung cấp bảo mật hai chiều của Dữ liệu. Điều này giúp bạn bảo vệ thông tin nhạy cảm có khả năng bị đánh cắp.



Trong giao thức HTTPS, các giao dịch SSL được thương lượng với sự trợ giúp của thuật toán mã hóa dựa trên khóa. Khóa này thường có cường độ 40 hoặc 128 bit.

- Trong hầu hết các trường hợp, các trang web chạy qua HTTPS sẽ có một chuyển hướng tại chỗ. Do đó, ngay cả khi bạn nhập HTTP: // nó sẽ chuyển hướng đến https qua kết nối bảo mật

- Nó cho phép người dùng thực hiện giao dịch thương mại điện tử an toàn, chẳng hạn như ngân hàng trực tuyến.
- Công nghệ SSL bảo vệ mọi người dùng và xây dựng lòng tin
- Một cơ quan độc lập xác minh danh tính của chủ sở hữu chứng chỉ. Vì vậy, mỗi Chứng chỉ SSL chứa thông tin xác thực, duy nhất về chủ sở hữu chứng chỉ.
- —
- HTTPS protocol can't stop stealing confidential information from the pages cached on the browser
- Dữ liệu SSL chỉ có thể được mã hóa trong quá trình truyền trên mạng. Vì vậy, nó không thể xóa văn bản trong bộ nhớ trình duyệt
- HTTPS có thể tăng tổng chi phí tính toán cũng như tổng chi phí mạng của organization

SỰ KHÁC BIỆT CHÍNH

- HTTP thiếu cơ chế bảo mật để mã hóa dữ liệu trong khi HTTPS cung cấp Chứng chỉ số SSL hoặc TLS để bảo mật giao tiếp giữa máy chủ và máy khách.
- HTTP hoạt động ở Lớp ứng dụng trong khi HTTPS hoạt động ở Lớp truyền tải.
- HTTP theo mặc định hoạt động trên cổng 80 trong khi HTTPS theo mặc định hoạt động trên cổng 443.
- HTTP truyền dữ liệu ở dạng văn bản thuần túy trong khi HTTPS truyền dữ liệu ở dạng văn bản mật mã (mã hóa văn bản).
- • HTTP is fast as compared to HTTPS because HTTPS consumes computation power to encrypt the communication channel.

<u>Aa</u> Tham số	 HTTP	 HTTPS
<u>Giao thức</u>	Nó là giao thức truyền siêu văn bản.	Nó là giao thức truyền siêu văn bản với an toàn.
<u>Bảo vệ</u>	Nó kém an toàn hơn vì dữ liệu có thể dễ bị tấn công bởi tin tặc.	Nó được thiết kế để ngăn chặn tin tặc truy cập thông tin quan trọng. Nó an toàn trước các cuộc tấn công như vậy.

<u>Aa</u> Tham số	☰ HTTP	☰ HTTPS
<u>Port</u>	Nó sử dụng cổng 80 theo mặc định	Nó được sử dụng cổng 443 theo mặc định.
<u>Bắt đầu với</u>	URL HTTP bắt đầu bằng http://	Các URL HTTP bắt đầu bằng https://
<u>Được dùng cho</u>	Nó rất phù hợp cho các trang web được thiết kế để tiêu thụ thông tin như blog.	Nếu trang web cần thu thập thông tin cá nhân như số thẻ tín dụng, thì đó là một giao thức an toàn hơn.
<u>Scrambling</u>	HTTP không xáo trộn dữ liệu được truyền. Đó là lý do tại sao tin tặc có khả năng cao hơn thông tin được truyền đi.	HTTPS xáo trộn dữ liệu trước khi truyền. Ở đầu thu, nó giải mã để khôi phục dữ liệu ban đầu. Do đó, thông tin được truyền đi được bảo mật và không thể bị tấn công.
<u>Giao thức</u>	Nó hoạt động ở cấp <u>TCP / IP</u> .	HTTPS không có bất kỳ giao thức riêng biệt nào. Nó hoạt động bằng HTTP nhưng sử dụng kết nối TLS / SSL được mã hóa.
<u>Xác thực tên miền</u>	Trang web HTTP không cần SSL.	HTTPS yêu cầu chứng chỉ SSL.
<u>Mã hóa dữ liệu</u>	Trang web HTTP không sử dụng mã hóa.	Các trang web HTTPS sử dụng mã hóa dữ liệu.
<u>Xếp hạng Tìm kiếm</u>	HTTP không cải thiện thứ hạng tìm kiếm.	HTTPS giúp cải thiện xếp hạng tìm kiếm.
<u>Tốc độ, vận tốc</u>	Nhanh	Chậm hơn HTTP
<u>Tính dễ bị tổn thương</u>	Dễ bị tấn công bởi tin tặc	Nó có tính bảo mật cao vì dữ liệu được mã hóa trước khi nó được nhìn thấy trên mạng.

FTP vs SFTP

FTP

là viết tắt của “File Transfer Protocol”. Đây là một dịch vụ internet được thiết kế để thiết lập kết nối với máy chủ hoặc máy tính cụ thể. Do đó, người dùng có thể chuyển tệp (download) hoặc truyền dữ liệu / tệp vào máy tính của họ hoặc máy chủ FTP.

Giao thức FTP cũng bao gồm các lệnh mà bạn có thể sử dụng để thực hiện các hoạt động trên bất kỳ máy tính từ xa nào. Ví dụ: để thay đổi thư mục, hiển thị nội dung thư mục, tạo thư mục hoặc xóa tệp. Nó được xây dựng trên kiến trúc máy khách-máy chủ. FTP cho phép bạn sử dụng các kết nối dữ liệu và điều khiển riêng

biệt giữa các ứng dụng máy khách và máy chủ. Nó giúp giải quyết vấn đề của các cấu hình máy chủ lưu trữ cuối khác nhau.

- Danh sách thư mục là thống nhất và machine-readable
 - Quá trình chuyển có thể được tiếp tục và có thể được lên lịch
 - Không giới hạn kích thước đối với một lần chuyển
 - FTP cho phép các tệp có quyền sở hữu và hạn chế quyền truy cập
 - Nó giúp bạn ẩn thông tin trên các hệ thống máy tính cá nhân
 - Nhiều ứng dụng khách FTP cung cấp khả năng viết kịch bản
 - Hầu hết các máy khách FTP đều có tiện ích đồng bộ hóa
 - Ứng dụng khách FTP cho phép bạn chuyển nhiều tệp & thư mục
-
- Lọc các kết nối FTP đang hoạt động là một công việc khó khăn trên máy cục bộ của bạn
 - Máy chủ có thể bị giả mạo để gửi dữ liệu đến một cổng ngẫu nhiên không xác định trên bất kỳ máy tính trái phép nào
 - Khó lập kịch bản các công việc bằng giao thức FTP
 - FTP không phải là một cách truyền dữ liệu không an toàn
 - Tuân thủ có thể là một vấn đề khi sử dụng FTP để gửi tệp
 - Không cho phép sao chép từ máy chủ đến máy chủ và hoạt động xóa thư mục đệ quy

SFTP

(full form SSH File Transfer Protocol-giao thức truyền tệp SSH dạng đầy đủ) là một phần của bộ giao thức SSH. Nó cung cấp truyền tệp an toàn qua SSH để cung cấp quyền truy cập vào tất cả các tài khoản shell trên máy chủ SFTP từ xa.

SSH là một giao thức để truy cập từ xa một cách an toàn vào một máy tính qua các mạng không đáng tin cậy. SSH là sự thay thế cho telnet, rsh, rlogin. SFTP xác minh danh tính của khách hàng và khi kết nối an toàn được thiết lập, thông tin sẽ được trao đổi.

- Kết nối luôn được bảo mật
- Các cổng TCP / IP

không được thông tin có thể được chuyển hướng qua kênh được mã hóa theo cả hai hướng



- Giao thức SFTP chạy trên một kênh an toàn, vì vậy không có mật khẩu văn bản rõ ràng hoặc dữ liệu tệp nào được truyền.
- Bạn có thể cài đặt phần mềm và sử dụng với chức năng hạn chế ngay cả khi không có quyền root

-
- Giao tiếp là nhị phân và không thể đăng nhập
 - Khóa SSH không dễ quản lý và xác thực
 - Các tiêu chuẩn xác định những điều cụ thể là tùy chọn hoặc khuyến nghị. Nó có thể dẫn đến sự cố tương thích giữa các phần mềm khác nhau do các nhà cung cấp khác nhau phát triển.

SỰ KHÁC BIỆT CHÍNH

- FTP không cung cấp một kênh an toàn để truyền tệp giữa các máy chủ trong khi SFTP cung cấp một kênh an toàn để truyền tệp giữa các máy chủ.
- FTP là viết tắt của "File Transfer Protocol" trong khi SFTP là viết tắt của "SSH File Transfer Protocol".
- FTP sử dụng 2 kênh để truyền dữ liệu trong khi SFTP sử dụng 1 kênh để truyền dữ liệu.
- FTP cho phép kết nối đến trên cổng 21 trong khi SFTP cho phép kết nối đến trên cổng 22.
- FTP không cung cấp mã hóa trong khi SFTP cung cấp mã hóa để gửi dữ liệu.
- FTP sử dụng kiến trúc Máy khách-máy chủ trong khi SFTP sử dụng kiến trúc SSH.
- • FTP has a direct transfer method whereas SFTP has a tunneling transfer method.

<u>Aa</u> Tham số	 FTP	 SFTP
<u>Người sáng lập</u>	Bởi Abhay Bhushan năm 1971	Tatu Ylönen với sự hỗ trợ của Sami Lehtinen vào năm 1997

<u>Aa</u> Tham số	 FTP	 SFTP
<u>Full Form</u>	Giao thức truyền tập tin.	Giao thức FTP an toàn.
<u>Basic</u>	FTP không cung cấp một kênh an toàn để truyền tệp giữa các máy chủ.	SFTP cung cấp một kênh an toàn để truyền tệp giữa các máy chủ.
<u>Encryption</u>	FTP có thể truy cập ẩn danh và trong hầu hết các trường hợp, nó không được mã hóa.	SFTP mã hóa dữ liệu trước khi gửi đến một máy chủ khác.
<u>Kiến trúc được sử dụng</u>	Client-server	SSH
<u>Giao thức</u>	FTP là giao thức TCP / IP.	Giao thức SFTP là một phần của giao thức SSH là một chương trình ứng dụng đăng nhập từ xa.
<u>Số kênh được sử dụng</u>	2	1
<u>Thường được sử dụng</u>	Đúng	KHÔNG
<u>Transfer method</u>	Direct transfer (truyền trực tiếp)	Tunneling
<u>Inbound Port</u>	Cho phép kết nối đến trên cổng 21	Cho phép các kết nối đến trên cổng 22
<u>Outbound Port</u>	Cho phép kết nối ra ngoài tới cổng 21.	Cho phép các kết nối đi đến cổng 22.

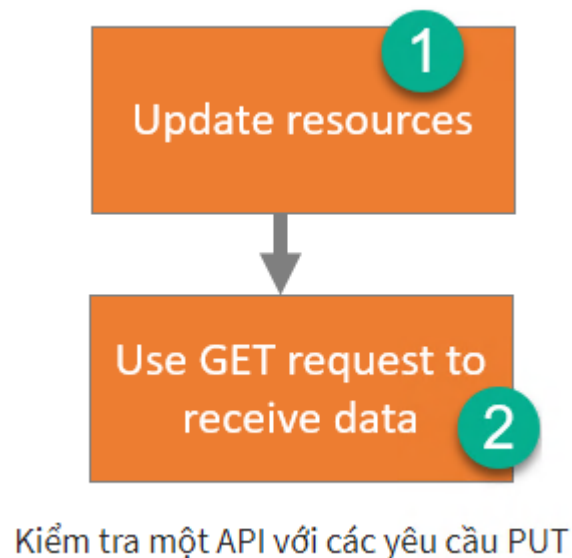
PUT vs POST

PUT

Phương thức PUT được sử dụng để cập dữ liệu có sẵn trên máy chủ. Thông thường, nó thay thế bất kỳ thứ gì tồn tại tại URL đích bằng một thứ gì đó khác. Có thể sử dụng nó để tạo dữ liệu mới hoặc ghi đè dữ liệu hiện có. PUT yêu cầu thực thể kèm theo phải được lưu trữ theo URI (Định danh tài nguyên đồng nhất) được yêu cầu cung cấp.

Kiểm tra một API với các yêu cầu PUT

Dưới đây là các bước để kiểm tra API với các yêu cầu PUT:



Bước 1) Cập nhật dữ liệu với yêu cầu PUT.

Bước 2) Sử dụng phương thức GET cho dữ liệu. Nếu yêu cầu PUT thành công, bạn sẽ nhận được dữ liệu mới. Phương pháp này sẽ không thành công nếu dữ liệu được cung cấp trong yêu cầu không hợp lệ. Do đó, nó sẽ không cập nhật bất cứ điều gì.

- Nó giúp bạn lưu trữ entity được cung cấp trong URI được cung cấp
- Nếu entity được cung cấp đã tồn tại, → thực hiện thao tác cập nhật hoặc có thể tạo bằng URI đó.
- có thể tạo một dữ liệu nhiều lần
- Tạo một dữ liệu với phương pháp PUT rất dễ dàng.
- Không cần phải kiểm tra xem người dùng đã nhấp vào nút gửi nhiều lần hay chưa.
- Nó có thể xác định thực thể kèm theo yêu cầu.

POST

là một phương thức được hỗ trợ bởi HTTP và mô tả rằng một máy chủ web chấp nhận dữ liệu được bao gồm trong nội dung của thư, được yêu cầu. POST thường được World Wide Web sử dụng để gửi dữ liệu do người dùng tạo đến máy chủ web hoặc khi bạn tải tệp lên.



Kiểm tra một API với các yêu cầu POST

Bước 1) Tạo một dữ liệu bằng cách sử dụng yêu cầu POST và đảm bảo rằng nó trả về mã trạng thái 200.

Bước 2) Thực hiện yêu cầu GET cho dữ liệu đó và lưu dữ liệu ở định dạng chính xác.

Bước 3) ADD tests đảm bảo yêu cầu POST không thành công với dữ liệu không chính xác.

- Phương pháp này giúp bạn xác định resource URI.
- Việc chỉ định resource location header mới rất dễ dàng bằng cách sử dụng location header.
- can send user-generated data to the web server.
- POST là một phương pháp an toàn vì các yêu cầu của nó không còn trong lịch sử trình duyệt.
- Bạn có thể dễ dàng truyền một lượng lớn dữ liệu bằng cách sử dụng post
- Bạn có thể giữ dữ liệu ở chế độ riêng tư.
- This method can be used to send binary as well as ASCII data.

SỰ KHÁC BIỆT CHÍNH:

- Phương thức PUT được gọi khi phải sửa đổi single resource trong khi phương thức POST được gọi khi phải thêm child resource.
 - Phản hồi của phương thức PUT có thể được lưu vào bộ nhớ cache nhưng không thể lưu vào bộ nhớ cache các phản hồi của phương thức POST.
 - Có thể sử dụng truy vấn UPDATE trong PUT trong khi có thể tạo truy vấn trong POST.
 - Trong phương thức PUT, máy khách quyết định URI resource nào nên có và trong phương thức POST, máy chủ quyết định URI resource nào nên có.
 - Phương thức PUT là Idempotent trong khi phương thức POST không phải là Idempotent.
-

Sum:

- Bảo toàn dữ liệu là dữ liệu cuối cùng và dữ liệu ban đầu là không đổi → phương thức bảo toàn dữ liệu là phương thức thực hiện bao nhiêu lần đi chăng nữa thì kết quả cũng chỉ giống thực hiện 1 lần
- PUT là phương thức bảo toàn dữ liệu (khi ấn submit bao nhiêu lần thì dữ liệu cũng chỉ tính như 1 lần submit)
- POST sẽ cho các kết quả khác nhau
- Khi tạo dữ liệu mới nên để hệ thống tự tạo id cho dữ liệu đó để tránh trùng lặp id dẫn đến thay đổi dữ liệu. POST để làm việc này tốt hơn PUT. Vì tạo mới PUT sẽ đi kèm với id để hệ thống sẽ tạo id của dữ liệu theo id đó nên sẽ có thể trùng lặp mà dữ liệu bị thay đổi

GET vs POST

Phương thức GET

Dữ liệu của phương thức này gửi đi thì hiện trên thanh địa chỉ (URL) của trình duyệt.

```
/test/demo_form.php?user=itplus&password=admin
```

Đặc điểm:

- HTTP GET có thể được cache bởi trình duyệt
- HTTP GET không được sử dụng nếu trong form có các dữ liệu nhạy cảm như là password, tài khoản ngân hàng
- HTTP GET bị giới hạn số trường độ dài data gửi đi

Phương thức POST

Dữ liệu được gửi đi với METHOD POST thì không hiển thị trên thanh URL.

Đặc điểm:

- HTTP POST không cache bởi trình duyệt
- HTTP POST không thể duy trì bởi lịch sử
- HTTP POST không giới hạn dữ liệu gửi đi

Phân biệt POST và GET

Điểm chung: là các HTTP method dùng để trao đổi dữ liệu giữa client và server.

Điểm khác nhau:

- POST: Bảo mật hơn GET vì dữ liệu được gửi ngầm, không xuất hiện trên URL
- GET: Dữ liệu được gửi tường minh, chúng ta có thể nhìn thấy trên URL, đây là lý do khiến nó không bảo mật so với POST.
- GET thực thi nhanh hơn POST vì những dữ liệu gửi đi luôn được webbrowser cached lại.
- Khi dùng phương thức POST thì server luôn thực thi và trả về kết quả cho client, còn phương thức GET ứng với cùng một yêu cầu đó webbrowser sẽ xem trong cached có kết quả tương ứng với yêu cầu đó không và trả về ngay không cần phải thực thi các yêu cầu đó ở phía server.
- Đối với những dữ liệu luôn được thay đổi thì chúng ta nên sử dụng phương thức POST, còn dữ liệu ít thay đổi chúng ta dùng phương thức GET để truy xuất và xử lý nhanh hơn.

SMB

SMB là một giao thức chia sẻ file phổ biến hiện nay khi người sử dụng hệ điều hành Windows. SMB sẽ được sử dụng ở chế độ mặc định trên các nền tảng như Win 7 8 10 khi chia sẻ file

Trong mô hình OSI, SMB được gọi là giao thức ở tầng App hoặc Presentation.

SMB có khả năng sử dụng mà không cần sự hỗ trợ của một giao thức truyền tải khác bằng việc kết hợp SMB với NBT để đảm bảo sự tương thích với nhiều phiên bản hệ điều hành Win khác nhau. Giao thức SMB dùng trên Win buộc phải sử dụng transport thông qua NetBT với các cổng 137, 138 (UDP), 139 (TCP). từ win 2000 nó đã nâng cấp chạy trực tiếp trên TCP/IP, chỉ sử dụng TCP

Chức năng của giao thức SMB

Một điểm mạnh mà nhiều công cụ khác không có được của SMB là hỗ trợ cả Unicode. và:

- Hỗ trợ tìm kiếm các máy chủ sử dụng giao thức SMB khác
- Hỗ trợ in qua mạng
- Cho phép thực hiện xác thực file và thư mục được chia sẻ
- Thông báo ngay lại sự thay đổi của file và thư mục
- Xử lý các thuộc tính mở rộng của file
- Hỗ trợ Unicode
- Cho phép lập tức khóa file đang truy cập tùy theo y/c

DHCP

Dynamic Host Configuration Protocol (giao thức cấu hình máy chủ): có nhiệm vụ giúp quản lý nhanh tự động và tập trung việc phân phối địa chỉ IP bên trong 1 mạng. Ngoài ra DHCP còn giúp đưa thông tin đến các thiết bị hợp lý hơn cung như việc cấu hình subnetmask hay gateway default

Hoạt động: Khi một thiết bị yêu cầu địa chỉ IP từ một router thì ngay sau đó router sẽ gán một địa chỉ IP khả dụng cho phép thiết bị đó có thể giao tiếp trên mạng.

Hoặc khi một thiết bị muốn kết nối với mạng thì nó sẽ gửi 1 y/c tới máy chủ, y/c này gọi là DHCP DISCOVER, sau khi y/c này đến máy chủ DHCP thì ngay tại đó máy chủ sẽ tìm một địa chỉ IP có thể sử dụng trên thiết bị đó rồi cung cấp cho thiết bị đặc chỉ cung với gói DHCP OFFER.

Khi nhận được IP thì thiết bị tiếp tục phản hồi lại máy chủ DHCP gói mang tên DHCP REQUEST. Lúc này là lúc chấp nhận y/c thì máy chủ sẽ gửi báo nhận ACK để xác định thiết bị đó đã có IP đồng thời xác định rõ thời gian sử dụng IP vừa cấp đến khi có địa chỉ IP mới

Ưu điểm:

- Máy tính hay bất cứ thiết bị nào phải cấu hình đúng cách thì mới có thể kết nối với mạng được. DHCP cho phép cấu hình tự động nên dễ dàng cho các thiết bị máy tính, điện thoại, các thiết bị smart khác có thể kết nối mạng nhanh
- Vì DHCP thực hiện theo kiểu gán địa chỉ IP nên sẽ không xảy ra trường hợp trùng IP
- Quản lý mạng mạnh hơn vì các cài đặt mặc định và thiết lập tự động lấy địa chỉ sẽ cho mọi thiết bị kết nối mạng đều có thể nhận được địa chỉ IP.
- Các thiết bị có thể di chuyển tự do từ mạng này sang mạng khác và nhận địa chỉ IP tự động mới vì các thiết bị này có thể tự nhận IP

Nhược:

- Không nên sử dụng địa chỉ IP động, địa chỉ IP thay đổi đối với các thiết bị cố định và cần truy cập liên tục. như máy in và file server

DNS

DNS là từ viết tắt trong tiếng Anh của Domain Name System, là Hệ thống phân giải tên, chỉ một hệ thống cho phép thiết lập tương ứng giữa địa chỉ IP và tên miền.

Hệ thống tên miền DNS là một hệ thống đặt tên theo thứ tự cho máy tính, dịch vụ hoặc bất cứ j trong internet. Nó liên kết nhiều thông tin đa dạng với tên miền được gán cho nhưng người tham gia.

Nó chuyển tên miền có ý nghĩa cho con người vào định danh (nhị phân) liên kết với các trang thiết bị mạng cho các mục đích định vị và địa chỉ hóa các thiết bị khắp thế giới

hệ thống tên miền phân phối trách nhiệm gán tên miền và lập bản đồ những tên tới địa chỉ IP bằng cách định rõ những máy chủ có thẩm quyền cho mỗi tên miền.

Những máy chủ có tên thẩm quyền được phân công chịu trách nhiệm đối với tên miền riêng của họ và lần lượt có thể chỉ định tên máy chủ khác độc quyền của họ cho các tên miền phụ

Chức năng: Mỗi website có một tên và một địa chỉ IP. Địa chỉ IP gồm 4 nhóm số cách nhau bằng dấu chấm (IPv4). Khi mở một trình duyệt Web và nhập tên Website, trình duyệt sẽ đến thẳng website mà không cần phải thông qua việc nhập IP của web đó. Quá trình dịch tên miền thành IP để cho trình duyệt hiểu và truy cập được là công việc của DNS server. Các DNS trợ giúp qua lại để dịch IP thành tên và ngược lại → chỉ cần nhớ tên