QUẢN TRỊ MẠNG

# CHƯƠNG 1: Tổng quan về mạng máy tính

**Ghi chú:**

\_Những mục được đánh dấu đỏ là những mục chưa hiểu rõ.

**More:**

**1. Phân biệt địa chỉ MAC và địa chỉ IP**

|  |  |
| --- | --- |
| **MAC** | **IP** |
| \_Địa chỉ phần cứng cố định được gán cho mỗi card mạng | \_Địa chỉ tạm thời được gán cho mỗi thiết bị kết nối vào mạng |
| \_MAC có dải địa chỉ 48 bit nên vẫn sẽ đủ cho toàn bộ thiết bị trên thế giới | \_Có thể là địa chỉ **32bit/v4** hoặc **128bit/v6** |
| \_Chỉ dùng trong mạng LAN | \_Dùng cho mạng toàn cầu |

# I. Giới thiệu mạng máy tính

## Là gì?

Tập hợp các mạng máy tính độc lập được kết nối bằng cáp, theo một kiến trúc nhất định.

**More:** Hai máy tính kết nối với nhau cũng có thể coi là một mạng máy tính.

## Các thành phần của mạng máy tính?

### 1. Thiết bị mạng

Gồm hai thành phần chính:

**1. Thiết bị đầu cuối (end devices)**

**\_**Máy khách, máy chủ, …

**2. Thiết bị mạng:**

\_Kết nối các thành phần mạng lại với nhau

\_**Router, switch, brigde, …**

### 2. Phương tiện truyền dẫn vật lý

Gồm 2 phương tiện truyền dẫn chính:

**Hữu tuyến (có dây):** Cáp quang, đồng trục, cáp xoắn đôi.

**Vô tuyến (không dây)**: Wifi, di động, vệ tinh, sóng hồng ngoại, …

### 3. Kiến trúc mạng

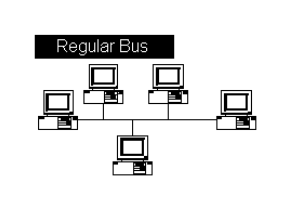
### Cách mà những thiết bị mạng được tổ chức.

### 4. Giao thức mạng

### Cách định nghĩa mà những thiết bị mạng trao đổi thông tin với nhau.

## Cấu trúc mạng máy tính(Topology)

### 1. Đường thẳng (Bus)

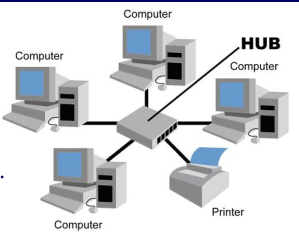


|  |  |
| --- | --- |
| **Ưu:** | **Nhược:** |
| \_Dễ cài đặt, mở rộng  \_Chi phí rẻ do cài đặt đơn giản  \_Một máy hỏng không ảnh hưởng tới đường truyền | \_Khó quản trị, tìm nguyên nhân lỗi (do một thiết bị có thể truyền dữ liệu cho nhiều thiết bị khác nhau nên việc tìm lỗi là do đâu sẽ rất khó)  \_Giới hạn chiều dài cáp và số lượng máy tính (trên một đường truyền chung nên muốn có nhiều máy tính hơn được kết nối vào mạng thì chiều dài cáp phải dài hơn)  \_Hiệu năng giảm khi có máy tính được thêm vào mạng (Khi một máy tính được thêm vào mạng thì khi đó cần tốn nhiều thời gian di chuyển và thời gian định tuyến hơn, dễ gây xung đột khi thực hiện truyền dữ liệu)  \_Một đoạn cáp backbone hỏng sẽ ảnh hưởng đến toàn mạng (do sử dụng chung một đường truyền mạng) |

### 2. Vòng tròn (Ring)

|  |  |
| --- | --- |
| Ưu: | **Nhược:** |
| \_Sự phát triển của hệ thống không tác động đáng kể đến hiệu năng (bởi vì việc thêm thiết bị vào hệ thống thì những máy tính còn lại vẫn có thể giao tiếp được với nhau thông qua vòng lặp)  \_Tất cả các máy tính có quyền truy cập như nhau bởi vì mạng liên kết theo hình tròn, nếu máy tính không có quyền truy cập như nhau thì làm thế nào để truyền được?  + Nó là ưu điểm bởi vì các máy tính có thể chia sẻ tại nguyên trên mạng, và việc truyền tải thông tin. | \_Chi phí thực hiện cao  \_Lắp đặt phức tạp  \_Khi một máy gặp sự cố thì có thể ảnh hưởng đến những máy khác. |

### 3. Hình sao (Star)



|  |  |
| --- | --- |
| **Ưu:** | **Nhược:** |
| \_Dễ dàng bổ sung hay bỏ bớt máy tính  \_Dễ dàng theo dõi và giải quyết sự cố (bởi vì đều đi qua một anh trung gian)  \_Phù hợp với nhiều loại cáp khác nhau (máy tính kết nối với máy chủ có thể có nhiều dạng kết nối khác nhau)  + Các loại mạng khác nếu sử dụng các dạng kết nối khác nhau có thể gây ra lổi bởi vì chúng được kết nối trên một đường truyền chung đòi hỏi phải có những loại cáp mạng phù hợp với đường truyền chung đó. | \_Khi hub/switch không làm việc, toàn mạng cũng sẽ không làm việc  \_Sử dụng nhiều cáp |

### 4. Phân cấp (Hierarchical)

**Mỗi một cấp sẽ được ứng với một chức năng nhất định**

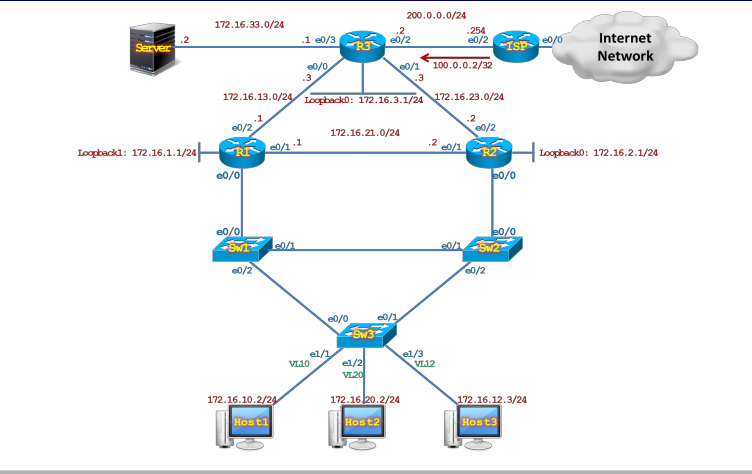
**VD:**

Thiết bị lớp 3(router) dùng để kết nối với thiết bị lớp 2(hub, switch) và các mạng khác.

Thiết bị lớp 2 được sử dụng để kết nối end devices và giao tiếp giữa chúng và lớp 3,...

### 5. Lưới (Mesh)

### 6. Hỗn hợp (Hybrid)



## Các dịch vụ mạng

### Dịch vụ chia sẻ tài nguyên:

**+ Print Services**: một máy in phục vụ cho nhiều người trong một mạng chia sẻ dùng chung

**+ File Services**: cung cấp truy cập tài nguyên mạng, mà chỉ có những người sử dụng đã được kiểm soát mới có thể truy cập được tài nguyên này

### Dịch vụ INTERNET:

**+ WWW**: Trang thông tin toàn cấu, người dùng sử dụng trình duyệt để truy cập vào những trang thông tin này. Và người dùng có thể đăng tải cho phép những người khác sử dụng được.

**+ FTP:** Cloud

**+ Email:**

\_Chương trình quản lý hộp thư là Mail Server

\_Máy Client cần có một chương trình Mail Client thích hợp để truyền nhận thư của mình tử hợp thư trên máy server.

### Các dịch vụ khác:

DNS, DHCP, IRC(trò chuyện trên mạng), **RAS**: Telnet (truy cập máy tính từ xa), …

# II. Phân loại mạng

**Mục đích:**

\_Dễ quản lý

## Theo phạm vi địa lý

### PAN – Personal Area Network

### LAN – Local Area Network

|  |  |
| --- | --- |
| **Đặc điểm** | **Nội dung** |
| Quy mô | nhỏ, giới hạn phạm vi khoảng vài km |
| Tốc độ truyền | từ 10Mbps đến hàng trăm Gbps, trễ thấp, độ tin cậy cao |
| Đơn vị quản lý | Do một tổ chức độc lập quản lý |
| Kĩ thuật sử dụng | Thường sử dụng kĩ thuật Ethernet, Token ring, EDM,… |
| Các thiết bị thường dùng | Repeater, Bridge, Hub, Switch, Router, … |
| Loại mạng LAN | Có dây và không dây |
| Phương thức kết nối mạng | **Broadcast** |

### MAN – Motropolitan Area Network

|  |  |
| --- | --- |
| **Đặc điểm** | **Nội dung** |
| Quy mô | \_lớn hơn **LAN**  **\_**thường trong phạm vi **một thành phố**  \_chứa nhiều mạng **LAN** |
| Tốc độ truyền | thấp hơn LAN do phạm vi rộng hơn |
| Đơn vị quản lý | Do một tổ chức độc lập quản lý |
| Kĩ thuật sử dụng | Cáp đồng trục, cáp quang |
| Các thiết bị thường dùng | Repeater, Bridge, Hub, Switch, Router, … |
| Loại mạng MAN | Có dây và không dây |
| Cách thức truyền tải | Broadcast |

### WAN – Wide Area Network

|  |  |
| --- | --- |
| **Đặc điểm** | **Nội dung** |
| Quy mô | \_lớn hơn **MAN**  **\_**kết nối giữa các thành phố hay một quốc gia, …  \_chung quy lại là lớn, không có giới hạn về địa lý |
| Tốc độ truyền | thấp hơn LAN do phạm vi rộng hơn |
| Đơn vị quản lý | Do nhiều tổ chức quản lý |
| Kĩ thuật sử dụng | Chuyển mạch kênh, chuyển mạch gói |
| Các thiết bị thường dùng | Repeater, Bridge, Hub, Switch, Router, … |
| Loại mạng MAN | Có dây và không dây |
| Cách thức truyền tải | Broadcast |

### GAN - Internet

Là tập hợp của các mạng **WAN**

## Theo kỹ thuật chuyển mạch

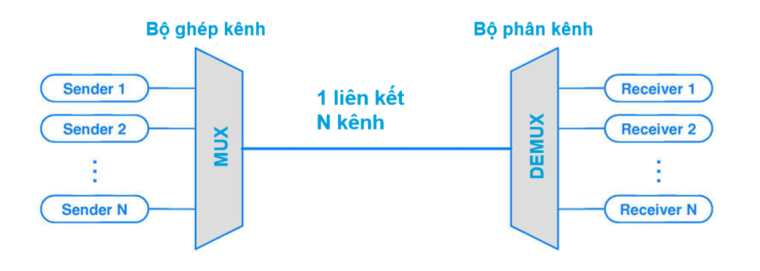
### Chuyển mạch kênh

\_Trước khi trao đổi thông tin hệ thống thiết lập kết nối giữa hai thực thể bằng một đường truyền vật lý. Thực thể đích nếu bận => hủy bỏ

\_Duy trì kết nối trong suốt quá trình trao đổi thông tin

\_Trao đổi xong thì kết nối được hủy bỏ, giải phóng tài nguyên bị chiếm dụng

|  |  |
| --- | --- |
| **Cơ chế dồn kênh:** | **Phân kênh:** |
| \_ghép nhiều kênh truyền thông khác nhau thành một kênh duy nhất để truyền thông tin  \_giúp cho việc truyền tải thông tin nhanh chóng do ghép kênh sử dụng nhiều kênh được ghép lại => tốc độ lớn | Quá trình dữ liệu được tách ra để truyền chính xác cho từng người dùng cụ thể |

Các phương pháp phổ biến là **FDM** và **TDM.**

### Chuyển mạch gói

\_Mỗi thông điệp truyền được chia thành các gói tin nhỏ (packet)

**Các cách thức để chuyển tiếp gói tin**

**Unicast**: tới một nút mạng cụ thể

**Multicast**: nhiều nút mạng

**Broadcast**: toàn bộ các nút trong mạng

### So sánh chuyển mạch kênh và chuyển mạch gói

|  |  |
| --- | --- |
| **Chuyển mạch kênh** | **Chuyển mạch gói** |
| \_Lãng phí nếu kênh rỗi  \_Truyền dẫn tin cậy hơn do thiết lập đường truyền liên tục giữa hai thiết bị mạng  \_Phù hợp cho ứng dụng thời gian thực (realtime, socket, …) | \_Chia sẻ dung lượng truyền dẫn tốt hơn  \_Không lãng phí  \_Tắc nghẽn có thể làm trễ, mất gói tin  \_Internet sử dụng chuyển mạch gói |

## Theo mô hình mạng phân cấp

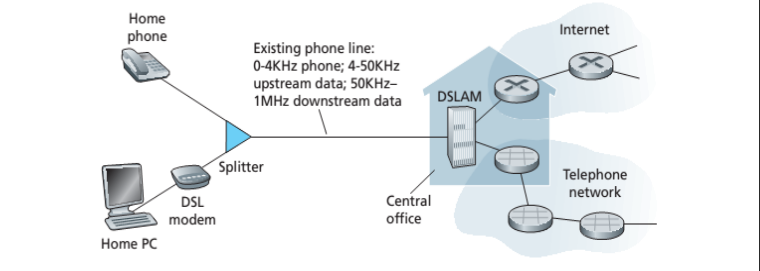
### Mạng biên và mạng lõi:

Biên là ở bên dìa, cạnh, có nghĩa là nó tương tác trực tiếp với thiết bị đầu cuối. Còn lõi tức là thành phần hỗ trợ giao tiếp giữa các mạng biên

## Theo phương thức truy cập

### 1. Truy cập gia đình

**+ DSL**



|  |  |
| --- | --- |
| **Đặc trưng** | **Nội dung** |
| Cơ chế truyền | \_dùng đường dây điện thoại |
| Tốc độ | upload **< 2.5 mbps**  downloads **< 24 mbps** |

**+ Cable**

|  |  |
| --- | --- |
| **Đặc trưng** | **Nội dung** |
| Cơ chế truyền | \_dùng loại cáp đặc trưng do ISP cung cấp, trên quãng đường từ trung tâm phân phối tới thiết bị đầu cuối thường sử dụng cáp đồng trục. |
| Tốc độ | upload **< 30.7 mbps**  downloads **< 42.8 mbps** |

**+ FTTH**

|  |  |
| --- | --- |
| **Đặc trưng** | **Nội dung** |
| Cơ chế truyền | \_chỉ sử dụng cáp quang cho toàn bộ tuyến đường từ trung tâm phân phối tới thiết bị đầu cuối. |
| Tốc độ | cao hơn **cable** |

**+ Ethernet**

|  |  |
| --- | --- |
| **Đặc trưng** | **Nội dung** |
| Cơ chế truyền | \_sử dụng dây cáp (đồng trục hoặc xoắn đôi) |
| Tốc độ | **\_**truy cập tới người dùng lên tới **100 Mbps**  **\_**truy cập tới server lên tới **1 Gbps,** thậm chí **10 Gbps** |

**+ Wifi** (công nghệ **802.11**)

|  |  |
| --- | --- |
| **Đặc trưng** | **Nội dung** |
| Cơ chế truyền | \_kết nối tới **router, 3G, 4G, …** thông qua Base Station (trạm thu phát sóng) còn được gọi là **Access point,** thường được dùng trong nội bộ gia đình, trường học, phạm vi vài chục mét với mục đích khuếch tại tín hiệu truyền và nhận của thiết bị di động. |
| Tốc độ | truy cập: **54Mbps** |

**+ Satelite**

### 2. Truy cập trong các tổ chức

**+ Ethernet**

**+ Wifi**

### 3. Truy cập không dây diện rộng

**+ 3G**

**+ LTE**

|  |  |
| --- | --- |
| **Đặc trưng** | **Nội dung** |
| Cơ chế truyền | \_sử dụng base station của các nhà mạng  \_phạm vi vài chục km |
| Tốc độ | **3G:**  + up/down = 6/42 Mbps  **LTE:**  **+** up/down = 50/300Mbps |

## Theo kiến trúc của ứng dụng

### Client/Server

\_Máy con gửi request cho máy chủ, máy chủ xử lý và trả về cho máy con

### Peer-to-peer

\_Các thiết bị trong mạng có chức năng và khả năng của các thiết bị đó là như nhau

### Boot room

\_Hệ thống mạng cho phép một số máy tính thành viên không gắn đĩa cứng mà vẫn có thể hoạt động như một máy tính thông thường.

## Theo topo mạng

Bus, star, ring, …

# III. Hiệu năng mạng

# IV. Mô hình OSI

## Mục đích phân tầng:

\_Có nhiều thiết bị khác nhau trong quá trình truyền thông mạng

\_Giúp giảm phức tạp trong thiết kế và cài đặt mạng

\_Tiêu chuẩn hóa các giao diện

\_Đảm bảo khả năng làm việc thống nhất giữa nhiều thiết bị

\_Dễ bảo trì, nâng cấp hệ thống nhờ cơ chế module hóa

## Nguyên tắc phân tầng:

\_Số lượng tầng là hạn chế, chức năng mỗi tầng là như nhau.

\_Mỗi tầng có chức năng có thể thiết kế lại mà không gây ảnh hưởng đến những tầng khác

\_Mỗi tầng sử dụng dịch vụ của tầng dưới và cung cấp dịch vụ cho tầng trên

\_Chỉ có tầng vật lý giữa các hệ thống có thể giao tiếp trực tiếp với nhau.

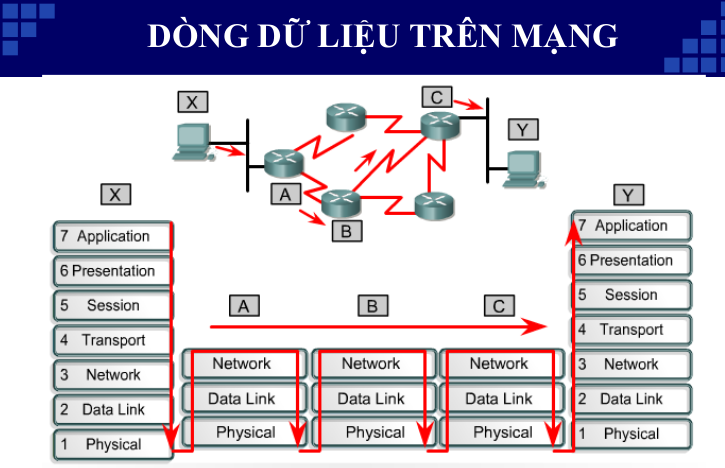
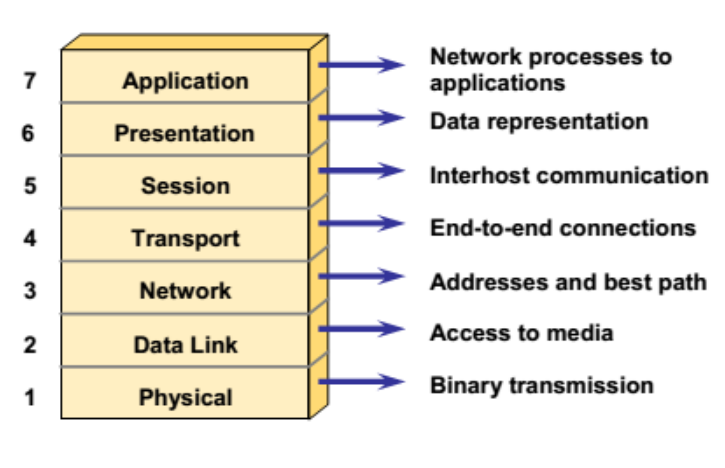
## Mô hình OSI

\_Là một mô hình theo nguyên tắc phân tầng trên do tổ chức OSI đưa ra năm 1970

\_Chia thành 7 tầng

\_Mỗi tầng có những giao thức khác nhau thực hiện các nhu cầu truyền thông cụ thể

## Chức năng của các tầng



|  |  |  |  |
| --- | --- | --- | --- |
| **Tầng** | **Chức năng** | **Protocol** | **Dạng dữ liệu**  **truyền tải**  **(***Được gọi chung là PDU***)** |
| Ứng dụng (application) | **\_cung cấp các dịch vụ ứng dụng** cho người dùng như email, truyền tệp, truyền thông đa phương tiện... | HTTP, FTP, SMTP, POP3, DHCP, DNS, Telnet, SSH | Messages |
| Trình diễn (presentation) | \_**định dạng và mã hóa dữ liệu** để tránh sự không tương thích giữa các thiết bị và các ứng dụng đảm bảo tính toàn vẹn. | MIME, SSL, TLS |  |
| Phiên (session) | \_t**hiết lập, quản lý và chấm dứt các phiên truyền thông** giữa các thiết bị, bao gồm việc quản lý đăng nhập, xác thực và đồng bộ hóa dữ liệu. | NetBIOS, NFS, RPC | Datagrams |
| Vận chuyển(Transport) | \_**cung cấp các dịch vụ truyền thông có độ tin cậy**, kiểm soát luồng dữ liệu và đảm bảo gói tin đến đúng địa chỉ đích. | TCP, UDP, | Segments |
| Mạng (network) | \_**quản lý việc chuyển dữ liệu giữa các mạng khác nhau**, điều khiển định tuyến (**routing**) và cung cấp các dịch vụ như chuyển mạch, định tuyến, giám sát lưu lượng... | IP, ICMP, OSPF, BGP, RIP | Packet |
| Liên kết dữ liệu (Datalink) | \_điều khiển truyền thông trên kết nối vật lý  \_đóng gói dữ liệu thành các khung (frames) và thêm thông tin định danh của các thiết bị trong mạng như địa chỉ MAC (đảm bảo truyền chính xác) | Ethernet, Wifi, ... | Frames |
| Vật lý (physical) | \_cung cấp các kết nối vật lý  \_chuyển đổi thành các tín hiệu để truyền dữ liệu qua các phương tiện truyền thông vật lý như cáp, sóng vô tuyến... | Ethernet, wifi | Bit |

## Một vài câu hỏi bổ sung

### Nêu các cổng dịch vụ của các protocol tiêu biểu tầng ứng dụng

|  |  |  |
| --- | --- | --- |
| **Giao thức** | **Port** |  |
| **HTTP/HTTPS** | **80/443** |  |
| **FTP** | **21**(control) **/ 20**(data) |  |
| **SMTP** | **25** |  |
| **POP3** | **110** |  |
| **DHCP** | **67** |  |
| **DNS** | **53** |  |
| **TELNET** | **23** |  |
| **SSH** | **22** |  |

# V. Mô hình TCP/IP

|  |  |  |  |
| --- | --- | --- | --- |
| **Tầng** | **Chức năng** | **Protocol** | **Dạng dữ liệu**  **truyền tải** |
| Ứng dụng (application) | **\_**kiểm soát các giao thức lớp cao  \_kiểm soát tính năng về định dạng dữ liệu, biểu diễn thông tin, mã hóa và điều khiển hội thoại  \_liên quan đến các chương trình ứng dụng | HTTP, FTP, SMTP, POP3, DHCP, DNS, Telnet, SSH | Messages |
| Vận chuyển(Transport) | \_đảm bảo việc vận chuyển dữ liệu từ nguồn tới đích | TCP, UDP, | Segments |
| Mạng (internet) | \_chọn đường đi tốt nhất xuyên qua mạng cho các gói dữ liệu di chuyển tới đích, liên quan đến địa chỉ IP | IP, ICMP, ARP, RARP | Packet |
| Truy cập mạng (Network access) | \_định ra những thủ tục giao tiếp với phần cứng mạng và truy nhập môi trường truyền | Ethernet, Fast Ethernet, … | Frames |

**Phân biệt hub, repeater, switch**

1. **Hub**

\_hoạt động tầng vật lý

\_khi một gói tin được gửi tới nó thì nó sẽ gửi tới tất cả các giao diện mà nó kết nối

1. **Repeater**

**\_**hoạt động tầng vật lý

\_tăng cường tín hiệu mạng

1. **Switch**

**\_**có bảng định tuyến các thiết bị trong mạng => truyền dữ liệu thông minh hơn

1. **Bridge**

\_Hoạt động ở tầng liên kết dữ liệu trong mô hình OSI

# VI. Đấu cáp mạng

\_Thiết bị cùng loại thì đấu chéo, khác loại thì đấu thẳng.

**Phân biệt cáp mạng STP và UTP**

STP có lớp bọc kim loại bảo vệ nên chống nhiễu tốt hơn UTP

# [QTM]-CHƯƠNG 1: TỔNG QUAN VỀ MẠNG

**Ghi chú:**

\_Những mục được đánh dấu đỏ là những mục chưa hiểu rõ.

**More:**

# II. Mô hình OSI và TCP/IP

## Cáp mạng



**Cáp đồng thì thường bao gồm 2 loại:**

|  |  |
| --- | --- |
| **Loại cáp** | **Đặc trưng** |
| Cáp đồng trục | \_Sử dụng một dây làm dây truyền tải tín hiệu  \_Có thêm vỏ kim loại để chống nhiễu  \_Và một lớp vỏ bọc bên ngoài  **Ưu:**  **\_**Độ chắc chắn cao và độ bền lâu dài  \_Tốc độ truyền tải tín hiệu cao  \_Khả năng chống nhiễu tốt hơn so với UTP/STP  **Nhược:**  \_Dày và cồng kềnh hơn so với UTP/STP  \_Chi phí cao hơn UTP/STP  \_Khó lắp đặt và sửa chữa |
| Utp/Stp | \_Sử dụng nhiều sợi dây xoắn với nhau  \_Khác biệt chính giữa hai loại này là stp có thêm một lớp bảo vệ chắn bên ngoài để giảm thiểu nhiễu  **Ưu:**  \_Dễ lắp đặt, sử dụng  \_Chi phí thấp  **Nhược:**  \_Tốc độ truyền tải tín hiệu thấp hơn so với cáp đồng trục  \_Khả năng chống nhiễu kém hơn so với cáp đồng trục |

## Cáp console

\_Là thiết bị được sử dụng để kết nối máy tính hoặc thiết bị mạng với một thiết bị mạng khác như **router, switch, …**

\_Cung cấp một kết nối trực tiếp giữa máy tính và thiết bị mạng và cho phép người dùng truy cập **giao diện dòng lệnh** để cấu hình và quản lý thiết bị mạng.

# III. Địa chỉ IPv4

## Đặc trưng

\_độ dài 32 bit

\_chia làm 4 octet

\_chia làm hai thành phần netwok và host

\_số bit cho network\_id và host\_id sẽ phụ thuộc vào cách cấu hình của người quản trị mạng

\_subnet mask là đơn vị dùng để xác định địa chỉ mạng của một địa chỉ IP.

## Một số những bài tập liên quan:

**Bài 1**: Mỗi công ty cần 2 mạng con, mỗi mạng 80 host. Vậy subnet mask là bao nhiêu?

*=> Dạng bài tính toán số lượng host*

\_Do mỗi mạng 80 host nên cần ít nhất cần 7 bit cho phần host vậy thì khi đó địa chỉ subnet mask sẽ là **255.255.255.128**

**Bài 2:** Cho địa chỉ IP của máy tính là 192.168.1.10/27, giá trị subnet mask dạng thập phân sẽ là.

*=> Dạng bài xác định địa chỉ subnet mask*

11111111.11111111.11111111.11100000 => **255.255.255.224**

**Bài 3:** Trong mạng máy tính giao thức **TCP/IP** và đều dùng subnet mask là **255.255.255.128** thì cặp máy tính nào là cặp máy tính có cùng mạng con.

*=> Dạng bài xác định mạng con từ địa chỉ* ***subnet mask*** *và địa chỉ* ***IP***

**Phương pháp làm:**

**TH1:**

\_Nếu địa chỉ subnet mask đều là 255 và 0 ví dụ: **255.255.0.0** thì chắc chắn địa chỉ mạng của một địa chỉ IP bất kì sẽ là phần ở trong địa chỉ IP tương ứng với những phần địa chỉ **255**

**VD: 192.168.1.10/16** => địa chỉ mạng **192.168.0.0**

**TH2:**

\_Nếu địa chỉ subnet mask dạng 255.255.128.0, ….

\_Thực hiện chuyển đổi thành phần khác 255 thành nhị phân sau đó thực hiện AND với thành phần tương ứng bên địa chỉ IP

VD: **192.168.15.1/25**

**=> 128 =>** 10000000

=> **1** => 00000001

=> địa chỉ mạng **192.168.15.0**

**Dạng bài chia mạng con:**

**Bài 1:** Chia mạng 139.12.0.0 với subnet-mask 255.255.0.0 thành 5 mạng con

=> Do chia thành 5 mạng con nên cần ít nhất 3 bit để có thể chia thành 5 mạng con. Bởi vì sử dụng 3 bit thì khi đó sẽ có ít nhất 8 địa chỉ IP, bỏ 2 địa chỉ đặc biệt là **địa chỉ mạng** và địa chỉ **broadcast**

**=> 5 mạng con sẽ là:**

|  |  |  |
| --- | --- | --- |
| **Địa chỉ mạng mới** | **Dải host** | **Broadcast** |
| 139.12.0.0/19 | 139.12.0.1/19-139.12.31.254/19  \_Tương ứng với 0000 0000 => 0001 1111 | 139.12.31.255/19 |
| 139.12.32.0/19 | 139.12.32.1/19-139.12.63.254/19  \_Tương ứng với 0010 0000 => 0011 1111 | 139.12.63.255/19 |
| 139.12.64.0/19 | 139.12.64.1/19-139.12.95.254/19 | 139.12.95.255/19 |
| 139.12.96.0/19 | 139.12.96.1/19-139.12.127.254/19 | 139.12.127.255/19 |
| 139.12.128.0/19 | 139.12.128.1/19-139.12.159.254/19 | 139.12.159.255/19 |

**Bài 2:** Chia mạng 139.12.0.0 với subnet-mask 255.255.192.0 thành 4 mạng con

Trường hợp này chúng ta đã có sẵn 2 bit phần subnet mask nên không cần phải mượn bit =>

|  |  |  |
| --- | --- | --- |
| **Địa chỉ mạng mới** | **Dải host** | **Broadcast** |
| 139.12.0.0/18 | 139.12.0.1/18-139.12.63.254/18 | 139.12.63.255/19 |
| 139.12.0.64/18 | 139.12.64.1/18-139.12.127.254/18 | 139.12.127.255/19 |
| 139.12.128.0/18 | 139.12.128.1/18-139.12.191.254/18 | 139.12.191.255/19 |
| 139.12.192.0/18 | 139.12.192.1/18-139.12.255.254/18 | 139.12.255.255/19 |

**Bài 3:** Chia mạng **172.16.32.0/19** thành 4 mạng con. Liệt kê dải host và địa chỉ Broadcast của các mạng

Mượn thêm 2 bit phần host => **172.16.32.0/21**

|  |  |  |
| --- | --- | --- |
| **Địa chỉ mạng mới** | **Dải host** | **Broadcast** |
| 172.16.32.0/21 | 172.16.32.1/21-172.16.39.254/21 | 172.16.39.255/21 |
| 172.16.40.0/21 | 172.16.40.1/21-172.16.47.254/21 | 172.16.47.255/21 |
| 172.16.48.0/21 | 172.16.48.1/21-172.16.55.254/21 | 172.16.55.255/21 |
| 172.16.56.0/21 | 172.16.56.1/21-172.16.63.254/21 | 172.16.63.255/21 |

**Bài 4:** Xác định địa chỉ mạng, dải host, địa chỉ broadcast của mạng khi biết địa chỉ IP: 150.64.128.236/20

Địa chỉ ip dạng bit AND subnet mask dạng nhị phân:

1001 0110.0100 0000.1000 0000. 1110 1100

1111 1111.1111 1111. 1111 0000. 0000 0000

--------------------------------------------------------

10010110.01000000.10000000.00000000

=> địa chỉ mạng: 150.64.240.0

=> dải host: 150.64.240.1/20 → 150.64.240.254/20

=> broadcast: 150.64.240.255/20

## Một số địa chỉ của IP v4

|  |  |
| --- | --- |
| **Loại địa chỉ** | **Chi tiết** |
| Network Address | Địa chỉ mạng |
| Host Addresses | Địa chỉ IP |
| Broadcast Addresses | Địa chỉ quảng bá |
| Unicast Addresses | Địa chỉ host đích |
| Multicast Addresses | Nhóm địa chỉ host đích |
| Public Addresses | Sử dụng toàn cầu |
| Private Addresses | Sử dụng trong LAN |

## Dải địa chỉ cho mạng riêng theo tiêu chuẩn RFC 1918

|  |  |
| --- | --- |
| **Địa chỉ mạng** | **Dải địa chỉ** |
| 10.0.0.0/8 | 10.0.0.0 – 10.255.255.255 |
| 172.16.0.0/12 | 172.16.0.0 – 172.31.255.255 |
| 192.168.0.0/16 | 192.168.0.0 - 192.168.255.255 |

## Chuyển đổi địa chỉ NAT

\_Là kĩ thuật để chuyển đổi địa chỉ private IPv4 sang địa chỉ public IPv4

\_Được sử dụng ở router biên kết nối internet

## Địa chỉ IPv4 đặc biệt

### Địa chỉ loopback:

\_127.0.0.0/8 (127.0.0.1 → 127.255.255.254)

\_Thường được xác định là chỉ 127.0.0.1

\_Được sử dụng trên host để kiểm tra xem TCP/IP có hoạt động hay không, và thường được sử dụng để sử dụng những dịch vụ ở trên host.

### Địa chỉ link-local:

\_169.254.0.0/16 (169.254.0.1/16 → 169.254.255.254/16)

\_Thường được gọi là địa chỉ IP riêng tư tự động hoặc địa chỉ tự gán

\_Được sử dụng bởi các máy khách DHCP của Windows để tự định cấu hình khi không có máy chủ DHCP.

## Phân lớp địa chỉ IPv4

Chuẩn RFC 790 (1981) chia địa chỉ IPv4 thành các lớp

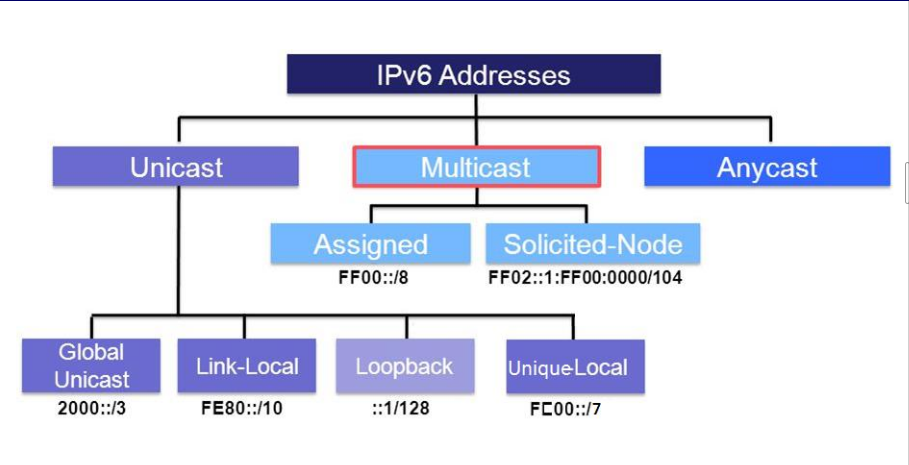
 Class A (0.0.0.0/8 to 126.0.0.0/8)

 Class B (128.0.0.0 /16 – 191.255.0.0 /16)

 Class C (192.0.0.0 /24 – 223.255.255.0 /24)

 Class D (224.0.0.0 to 239.0.0.0)

 Class E (240.0.0.0 – 255.0.0.0)



# IV. Địa chỉ IP v6

## Đặc trưng

\_Độ dài IPv6 gồm 128 bit

\_Chia thành 8 nhóm mỗi nhóm 16 bit

\_Phân cách nhau bằng ký hiệu hai chấm :

\_Biểu diễn bằng hệ 16 hexa

\_Cách biểu diễn rút gọn là các nhóm cạnh nhau bằng 0 thì có thể sử dụng dấu :: thay thế

VD:

2001:0ABC:00AB:000A:0000:0000:0000:1001 => 2001:0ABC:00AB:000A::1001

2001:0000:0000:0ABC:00AB:0000:0000:1001 => 2001:0:0:0ABC:00AB::1001 hoặc

2001::0ABC:00AB:0:0:1001 hoặc 2001:0:0:0ABC:00AB:0:0:1001

\_Cấu trúc IP v6 chia thành hai phần

+ Network prefix

+ Interface ID

VD: **2001:0000:0000:0001:: /64**

**Prefix Length IPv6** có thể nằm trong khoảng từ 0 đến 128

Tuy nhiên khuyến nghị hầu hết các loại mạng là 64

# V. Chuyển đổi IPv4-IPv6

### Các phương pháp chuyển đổi IPv4-IPv6:

|  |  |
| --- | --- |
| **Phương pháp** | **Chi tiết** |
| Dual stack | Các thiết bị mạng chạy song song giao thức IPv4-IPv6 |
| Phương pháp đường hầm (Tunneling) | Đóng gói tin IPv4 vào trong gói tin IPv4 |
| NAT-PT (Proxy and Translation) |  |

# VI. Cấu hình cơ bản thiết bị mạng

## Các phương pháp cấu hình thiết bị mạng

1. Trực tiếp thông qua cổng console
2. Từ xa sử dụng telnet
3. Từ xa sử dụng ssh

## Cấu trúc cơ bản của Router

1. ROM
2. CPU
3. Hệ điều hành (thiết lập cách hoạt động của router)
4. Interface
5. Running-config (lưu trữ cấu hình của thiết bị trong quá trình chạy)
6. Startup-config (lưu trữ cấu hình của thiết bị trong **NVRAM**~không mất khi khởi động lại)

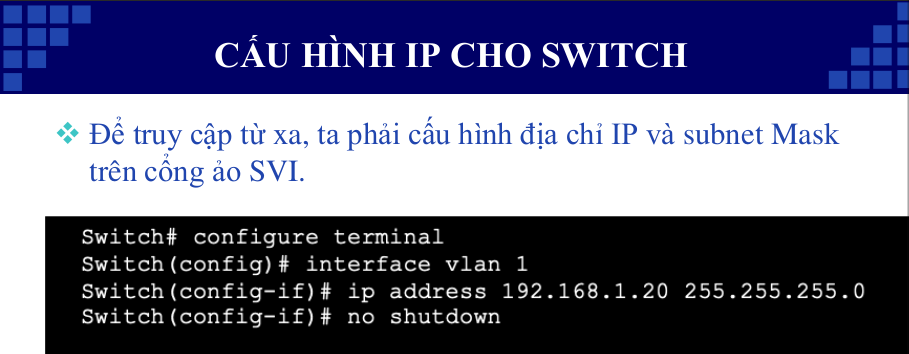
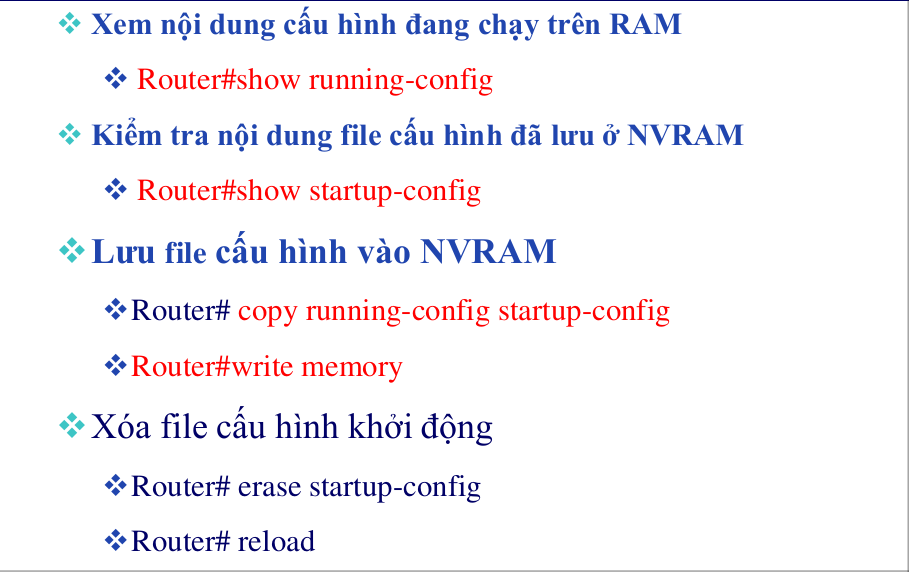
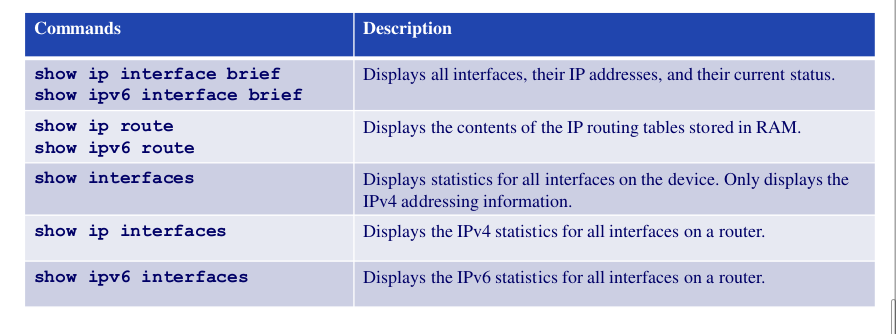
## Phân biệt các quyền

|  |  |  |
| --- | --- | --- |
| **Quyền** | **Chỉ thị** | **Thông tin** |
| Người dùng thông thường | > | Chỉ thực hiện được những lệnh cơ bản như kiểm tra kết nối, xem thông tin cấu hình |
| Global | # | Thực hiện được một vài lệnh cơ bản tuy nhiên nhiều chức năng hơn người dùng thông thường |
| Priviledge | config | Quyền cao nhất, có thể thực hiện những lệnh cấu hình router, … |
| Config interface | config-inf | Truy cập vào một interface cụ thể để cấu hình |
| … | | |

## Command:

### Cấu hình địa chỉ IPv4/v6:

|  |
| --- |
| Router(config)# interface type-and-number  Router(config-if)# description description-text  Router(config-if)# ip address ipv4-address subnet-mask  Router(config-if)# ipv6 address ipv6-address/prefix-length  Router(config-if)# no shutdown |



# CHƯƠNG 2: KĨ THUẬT ĐỊNH TUYẾN

## 1. Tổng quan về định tuyến

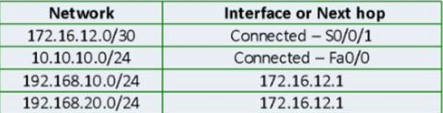
### Đặc trưng:

\_Giúp router giúp xác định **tìm đường đi** cho các gói tin để truyền dữ liệu từ nguồn tới đúng đích cần gửi.

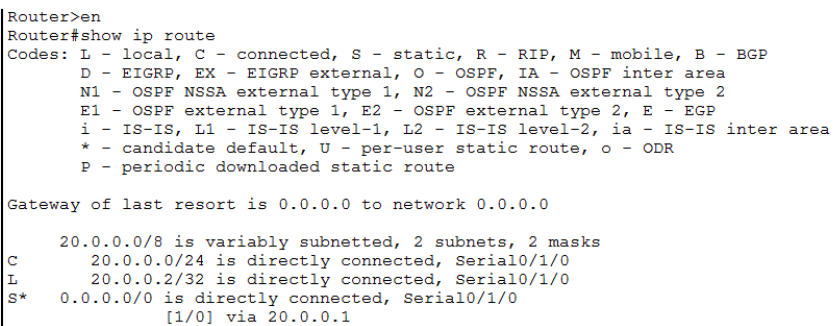
### Cơ chế:

\_Router dựa vào **địa chỉ IP đích (destination IP)** trong các gói tin và sử dụng bảng định tuyến (routing table) để xác định đường đi cho chúng.

\_Trong bảng này mỗi mạng mà router có thể truyền đi được thể hiện bằng một dòng, nó có thể là router được nối trực tiếp hoặc là router học được thông qua việc cấu hình định tuyến.



### Command:



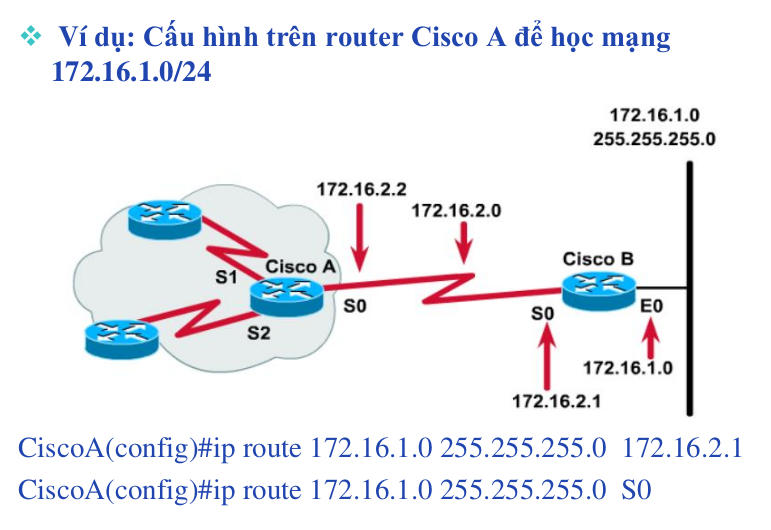
### Phân loại định tuyến:

|  |  |
| --- | --- |
| **Loại định tuyến** | **Nội dung** |
| Định tuyến tĩnh (Static route) | \_Loại định tuyến trong đó router sử dụng tuyến đường đi tĩnh để vận chuyển dữ liệu đi  \_Tuyến đường này do admin tự cấu hình thủ công |
| Định tuyến động (Dynamic route) | \_Router sử dụng các tuyến đường di động để vận chuyển dữ liệu đi  \_Những tuyến đường này do các router sử dụng các **giao thức định tuyến động** trao đổi thông tin định tuyến với nhau tạo ra.  \_Một số giao thức phổ biến: **RIP, OSPF, EIGRP**, … |

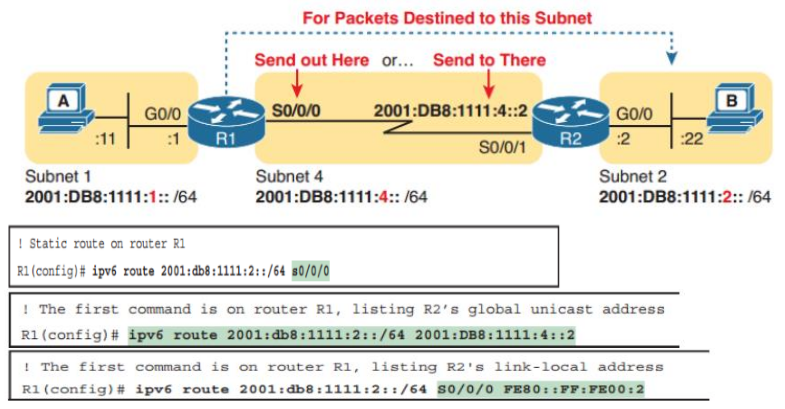
## 2. Định tuyến tĩnh

### Command:

|  |
| --- |
| **IPv4** |
| R(config)#**ip unicast-routing**  R(config)#**ip route <destination-network> <subnet-mask> <NextHop|OutPort>** |
| Trong đó:  + destination-network: Là địa chỉ mạng cần đi tới  + subnet-mask: subnet mask của destination-network  + next-hop: địa chỉ IP của router kế tiếp kết nối trực tiếp với router đang xét  địa chỉ next-hop là địa chỉ mà khi thiết bị mạng không truyền trực tiếp được tới đích thì sẽ truyền trực tiếp tới địa chỉ này. Xem ví dụ bên dưới.  + OutPort: cổng của router mà packet sẽ đi ra |



|  |
| --- |
| **IPv6** |
| R(config)#**ipv6 unicast-routing**  R(config)#ipv6 route prefix-network/prefix-length [OutGoing Interface | Next-Hop] |

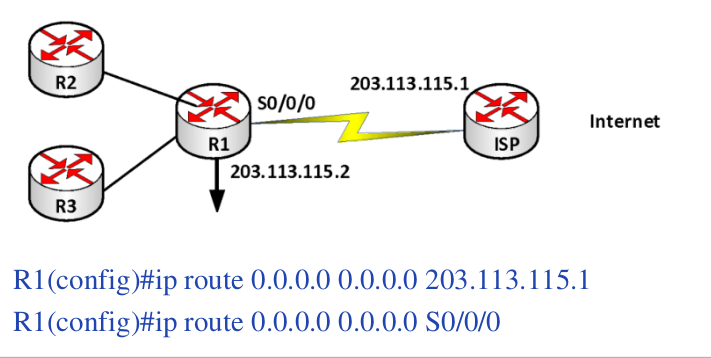


### DEFAULT ROUTE:

**IPv4:**

\_nằm ở cuối bảng định tuyến

\_được sử dụng để gửi các gói tin đi trong trường hợp mạng đích không tìm thấy trong bảng định tuyến

****

**IPv6:**

## 3. Định tuyến động

**Thuật ngữ:**

**+ Autonomous System:** hệ thống mạng độc lập có khả năng tự quản lý, thường được quản lý bởi một tổ chức độc lập.

### Phân loại định tuyến động

#### Theo phạm vi:

|  |  |
| --- | --- |
| **Tên loại định tuyến** | **Chi tiết** |
| Định tuyến ngoài **EGP** (Exterior Gateway Protocol) | \_là giao thức trao đổi thông tin giữa các AS khác nhau.  \_tiêu biểu là giao thức **BGP** |
| Định tuyến trong **IGP** (Interior Gateway Protocol)  ***Note:*** *Trong hay ngoài ở đây là biểu thị AS* | \_là giao thức định tuyến bên trong 1 AS như (**RIP, IGRP, EIGRP, OSPF**) |

#### Theo giải thuật định tuyến:

|  |  |
| --- | --- |
| **Tên loại định tuyến** | **Chi tiết** |
| Distance – vector | \_mỗi router gửi cho láng giềng của nó toàn bộ bảng định tuyến của nó theo định kì.  \_giao thức là **RIP**. |
| Link-state | \_mỗi router gửi bản tin trạng thái đường link LSA(*tóm tắt thông tin về đường đi tới các mạng của nó.*) cho các router khác.  \_các router sau khi xây dựng xong bảng định tuyến sẽ vẽ ra được một bản đồ mạng của toàn bộ hệ thống.  \_tiêu biểu là giao thức **OSPF** |
| Path-vector | \_định tuyến **BGP** trong mạng internet |

#### Phân loại theo các giao thức IGP:

|  |  |
| --- | --- |
| **Tên loại định tuyến** | **Chi tiết** |
| Các giao thức **Classfull** | \_router sẽ không gửi kèm subnet-mask trong bảng tin định tuyến của mình. Từ đó giao thức classfull không hỗ trợ sơ đồ VLSM và mạng gián đoạn (**Discontiguos networks**)  \_giao thức tiêu biểu là **RIPv1** |
| Các giao thức **Classless** | \_ngược lại với classfull  \_Router có thể gửi kèm **subnet-mask** trong bảng định tuyến. Từ đó các giao thức classless có hỗ trợ sơ đồ VLSM và mạng gián đoạn.  \_các giao thức tiêu biểu là **RIPv2, OSPF, EIGRP,** … |

## 4. Tham số định tuyến

|  |  |
| --- | --- |
| **Giá trị** | **Ý nghĩa** |
| AD (Administrative Distance) | \_là gía trị được sử dụng để chỉ **độ tin cậy** của các **giao thức định tuyến**  \_trong trường hợp router học được một mạng đích thông qua nhiều giao thức định tuyến khác nhau, thì tuyến của giao thức định tuyến nào có AD nhỏ nhất thì sẽ được lựa chọn và đưa vào bảng định tuyến.  \_giá trị AD này khác nhau theo từng Vendor quy định |
|  | |
| Metric | \_là giá trị định lượng **mức độ tối ưu** của một đường đi trong tính toán định tuyến  \_mỗi kĩ thuật routing sẽ có một **metric** khác nhau  + rip dựa vào số router trên đường đi đến đích gọi là **hop-count**  + ospf tính metric dựa vào băng thông (**bandwidth**) đường truyền  + eigrp tính metric dựa vào một bộ các thông số khác nhau trên đường đi đến đích như băng thông (**bandwidth**), độ trễ (**delay**), độ tin cậy (**reliability**), tải (**load**) của đường truyền |

## 5. Giao thức định tuyến OSPF

### Đặc trưng:

\_là giao thức định tuyến động thuộc nhóm **link-state**, là chuẩn do **IEEE** đưa ra

\_trên mỗi router đều có bản đồ mạng cả vùng (bảng định tuyến) thông qua việc đồng nhất bảng cơ sở dữ liệu trạng thái đường link (**LSDB - Link State Database**)

\_từ bản đồ mạng này Router sẽ tự tính toán ra đường đi ngắn nhất và xây dựng bảng định tuyến cho nó.

\_giao thức OSPF được sử dụng rộng rãi trong các công ty hệ thống mạng lớn

\_sử dụng thuật toán dijkstra để tìm đường đi ngắn nhất

\_hoạt động ở nhóm classless(một địa chỉ IP có thể được phân thành nhiều mạng con khác nhau, hiệu quả hơn trong việc sử dụng không gian đĩa)

\_chạy trên nền giao thức IP, protocol-id = 89

\_trao đổi thông tin qua địa chỉ 224.0.0.5 và 224.0.0.6

### Tham số:

AD = 110

**Metric** phụ thuộc vào **bandwidth**

**Hoạt động của OSPF:**

|  |  |
| --- | --- |
| **Hoạt động** | **Nội dung** |
| Bầu chọn Router-id | \_Để chạy OSPF nó phải tạo ra 1 định danh để chạy gọi là Router-id (A.B.C.D, …)  \_Để tạo ra Router-id có hai cách  **1. Router tự động tạo**  \_Dựa vào interface có địa chỉ IP cao nhất trong các interface active và ưu tiên loopback để lấy IP đó là Router-id    **Giải thích:**  203…. đang không active  192.168.1.1/24 nhỏ hơn **192.168.2.1/24**  \_Nếu router có loopback tồn tại và cho tham gia định tuyến thì router-id ưu tiên cho loopback trước:    **2. Do admin tự tạo bằng cách config** |
| Thiết lập quan hệ láng giềng | \_Khi cả hai router liền kề đã chạy OSPF thì chúng bắt đầu gửi OSPF để thiết lập láng giềng.    Để có thể thiết lập làm láng giềng của nhau thì chúng phải có cùng một số những tham số sau:  **ĐIỀU KIỆN 1 (**Cùng Area\_id**)**  + **Backbone area**: có ít nhất một backbone area (phải có ít nhất 1 vùng) kí hiệu: 0 (khu vực trung tâm mà các non-backbone-area được kết nối cùng)  + **Non-backbone area:** phải kết nối trực tiếp với vùng backbone area. Kí hiệu: 1-2^52 => sẽ có 1 router đứng giữa 2 vùng.  + **Backbone router**: là router nằm trong vùng backbone-area  **+ Internal router:** là router nằm trong vùng non-backbone area  **+ Area border router (ABR):** router nằm giữa ranh giới backbone area và non-backbone area.  + **Autonomous system border router (ASBR)**: là router biên giới giữa định tuyến OSPF và 1 giao thức định tuyến khác (nghĩa là nó vừa chạy OSPF vừa chạy RIPv2 chẳng hạn)  **ĐIỀU KIỆN 2 (**2 router phải cùng subnet và subnet-mask**)**  **\_**2 router phải cùng **subnet** và **subnet-mask**      **ĐIỀU KIỆN 3 (**có cùng hello-time/die-timer (10s/40s))  **ĐIỀU KIỆN 4 (**cùng loại xác thực (Authentication)**)** |
| Trao đổi cơ sở dữ liệu LSDB | \_Sau khi ở trạng thái 2-way thì nó bắt đầu gửi thông tin cho nhau để hình thành lên 1 bảng database gọi là LSDB (Link-state database)  Theo 2 giai đoạn sau:  **Gđ1:**  **Router A** gửi 1 bản tin DBD (Database Description) để mô tả những thông tin mà nó có được cho router neighbor B.  **Gđ2**: Khi neighbor B nhận được DBD nếu nó thấy thông tin nào trong DBD mà nó không có thì nó sẽ gửi LSR (Link state request) cho router A để xin thông tin thiếu.  **Gđ3:** Khi router A nhận được LSR thì nó phải cho những thông tin thiếu cho router B bằng **LSA** (Link state Advertisement) nằm bên trong **LSU** (Link state update)  **Gđ4:** Khi router B nhận LSU thì nó lấy phần LSA bên trong LSU. Khi nhận xong thì nó phải trả lời lại là đã nhận được bằng LSACK (**link state acknowledgment**)  => Sau khi **LSDB** thì **router** có thể tự chọn được đường đi tốt nhất dựa vào thuật toán **Dijkstra** |
| Xây dựng bảng định tuyến |  |

### BẦU CHỌN DR/BDR

**+ DR**

\_Các router kết nối với nhau = interface **LAN**

\_Trước khi trao đổi thông tin thì các router sẽ bầu chọn ra 1 router đóng vai trò làm chủ đạo được gọi là **DR** có nhiệm vụ tiếp nhận các thông tin trao đổi và gửi qua cho các router khác.

**+ BDR**

\_Là router dự phòng cho DR

**+ DR other**

**\_**Những router còn lại. Những router không nói chuyện trực tiếp với nhau (vẫn giữ trạng thái **2-way**) mà không phải thông qua DR. Đồng thời DR này gửi thông tin copy cho BDR để backup.

#### Việc bầu chọn phải dựa vào một số thông tin:

**Priority:** Chỉ số ưu tiên của cổng. Có giá trị từ 0-255 (default = 1)

+ **Router** có priority cao nhất làm **DR**, cao thứ 2 làm **BDR**, còn lại **DR other**.

+ Khi đặt **priority = 0** cho **1 interface** thì router đó không bao giờ được làm **DR, BDR.**

**Router-id:** Khi xét quá trình chọn **DR** thì **router-id** sẽ không xét **loopback**

+ Riêng DR và BDR nói chuyện với nhau = 224.0.0.6 còn lại nói chuyện với nhau = 224.0.0.5

+ Trong OSPF có một quy luật **Non-preemptive**: nghĩa là không bầu chọn lại. Khi DR chết BDR thay nhưng sau đó DR sống lại thì nó sẽ không được bầu chọn lại làm DR lại như cũ.

### TÍNH COST

\_Trong **OSPF** không còn gọi là Metric mà gọi là Cost (Cost trên interface)

\_Cost được tính khi đi vào 1 cổng và đi ra không tính

\_Công thức tính cost như sau:

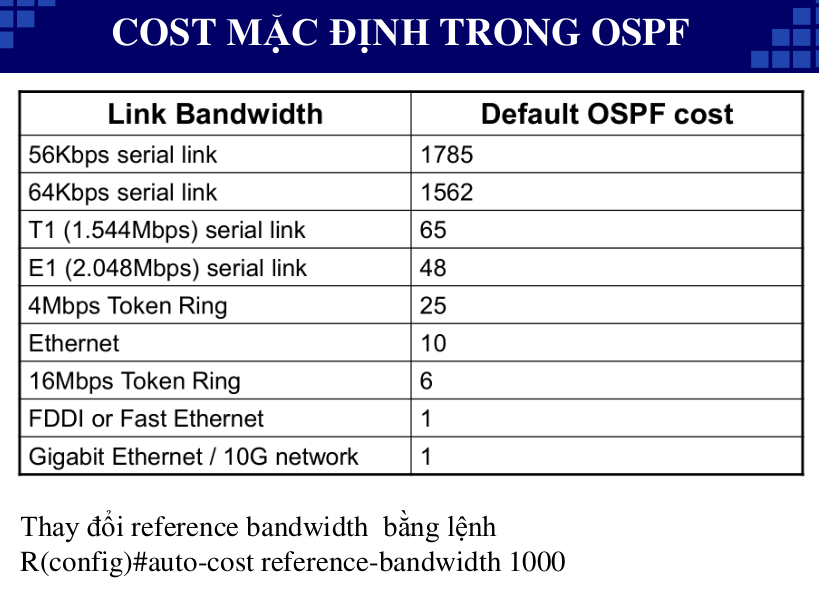
|  |
| --- |
| Cost = reference bandwidth / interface bandwidth |

Trong đó:

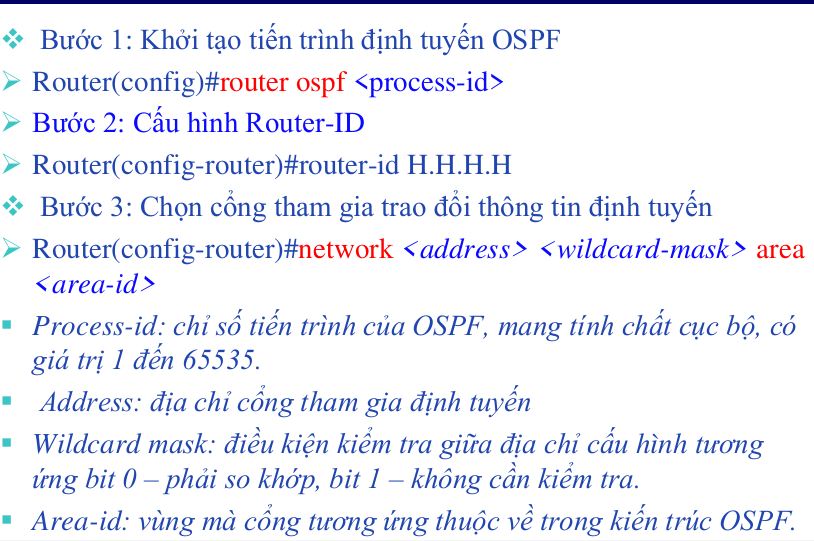
**reference bandwidth = 10^8**

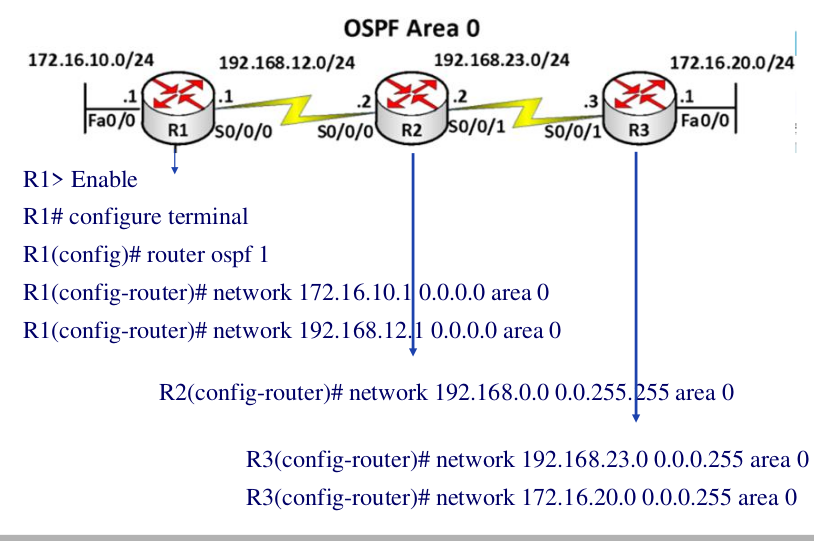
|  |
| --- |
| **Ethernet (10Mbps) → cost = 10 (**10^8 / 10 000 000 (10^7)**)**  **FastEthernet(100Mbps) --> cost=1**  **Serial(1,544Mbps) --> cost=64** |

**Cost mặc định trong OSPF:**

**Tính toán cost trong mạng:**

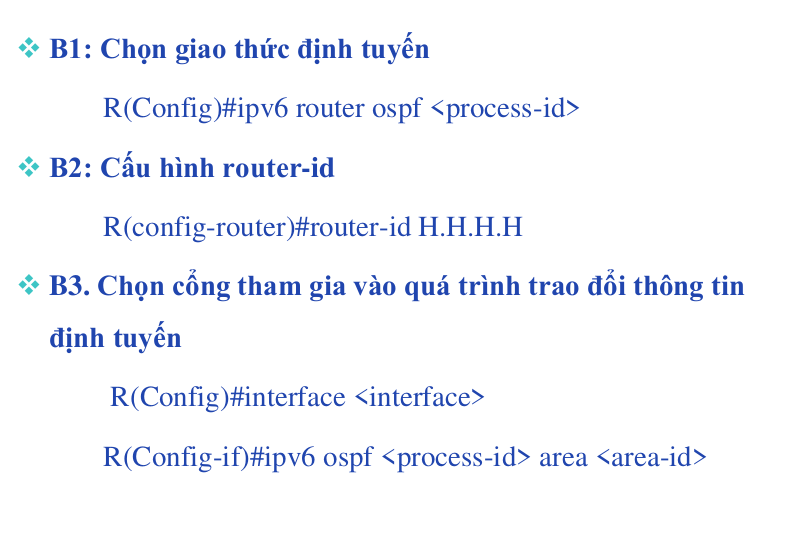
### COMMAND: CẤU HÌNH ĐỊNH TUYẾN OSPF

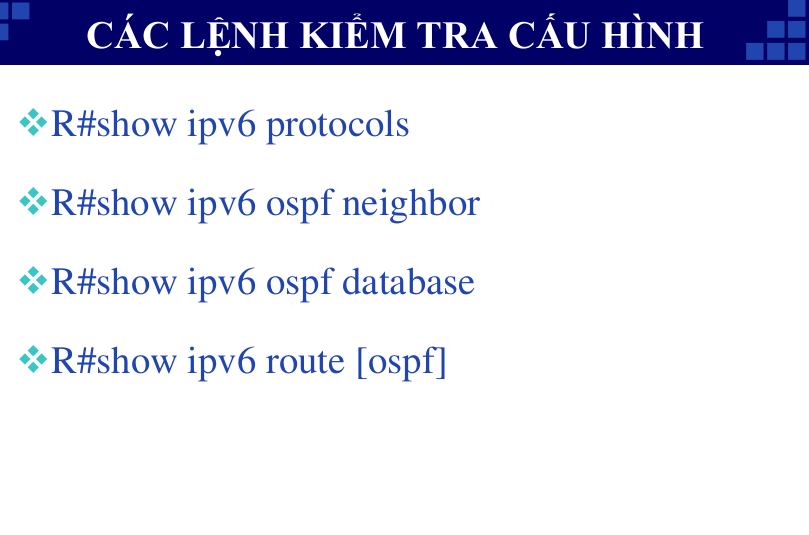


****

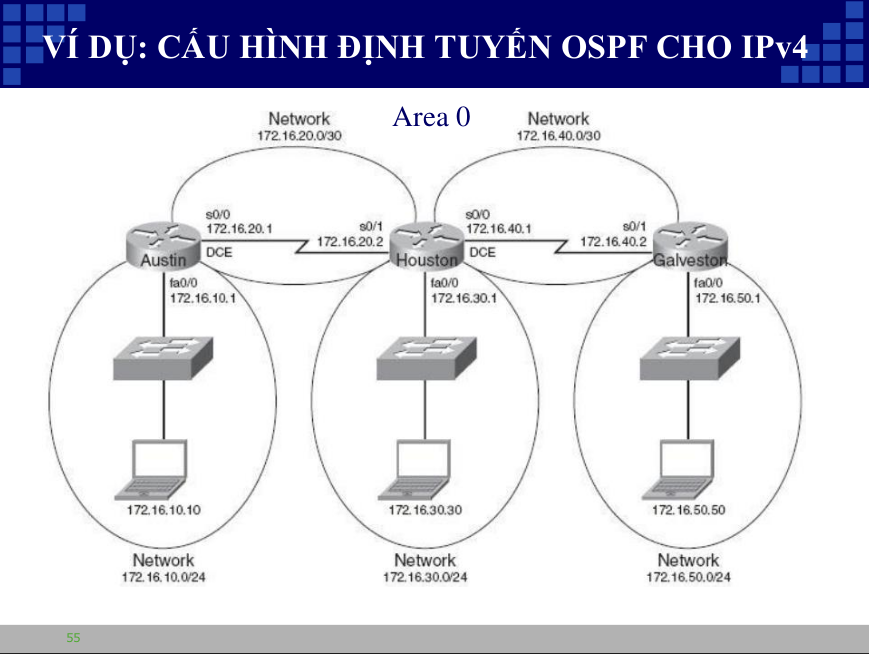
****

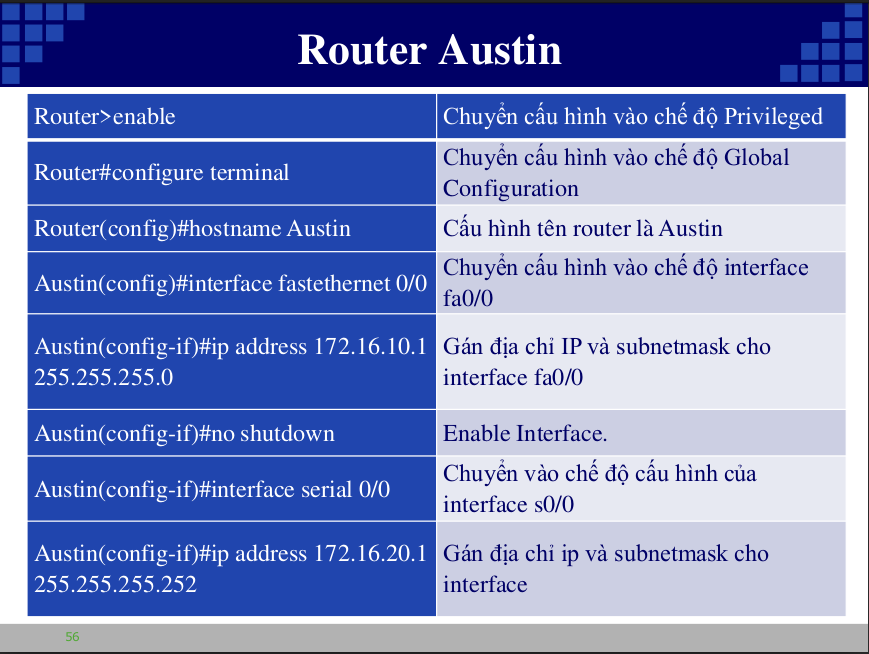
**Cấu hình cho IPv6:**

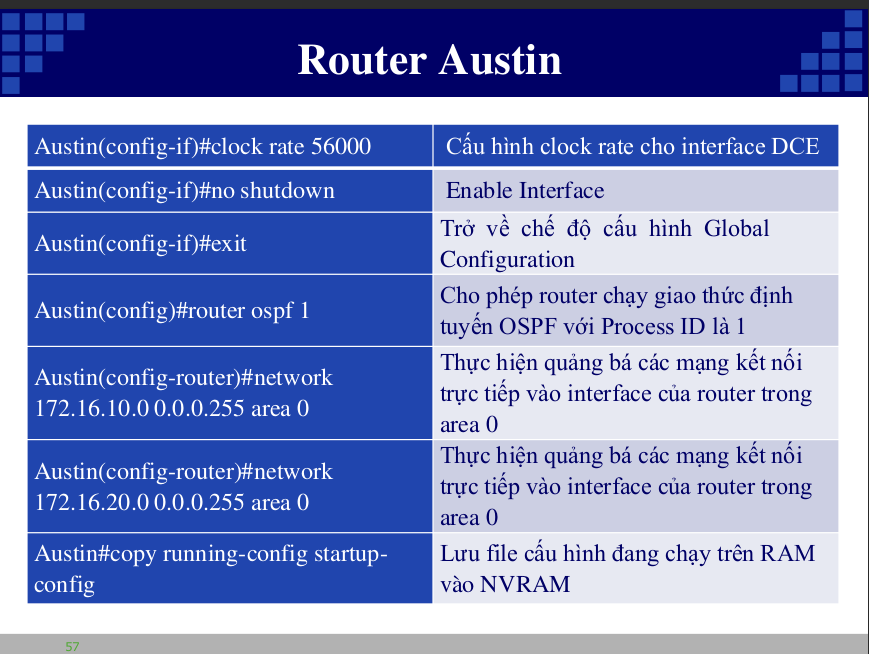
****

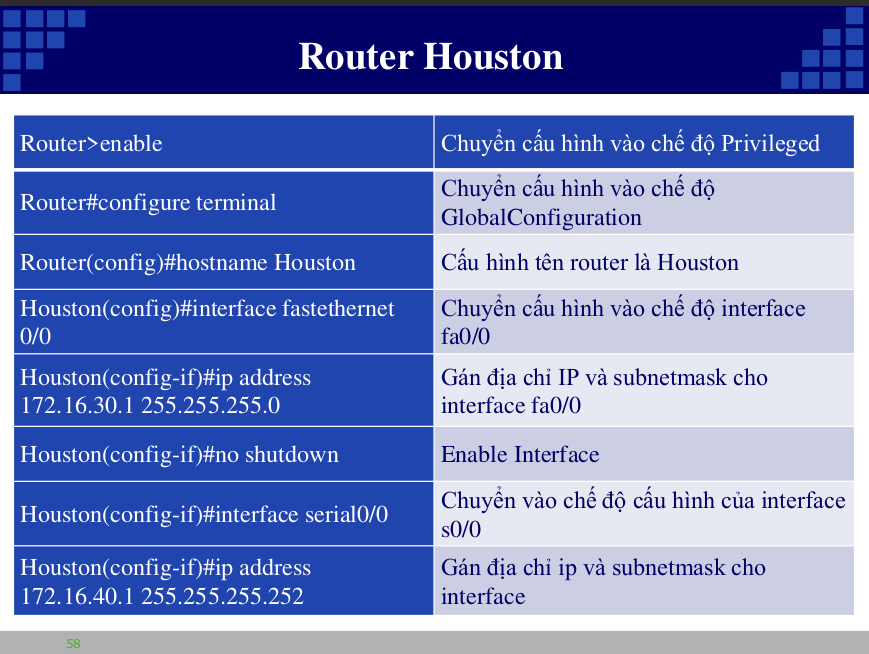
****

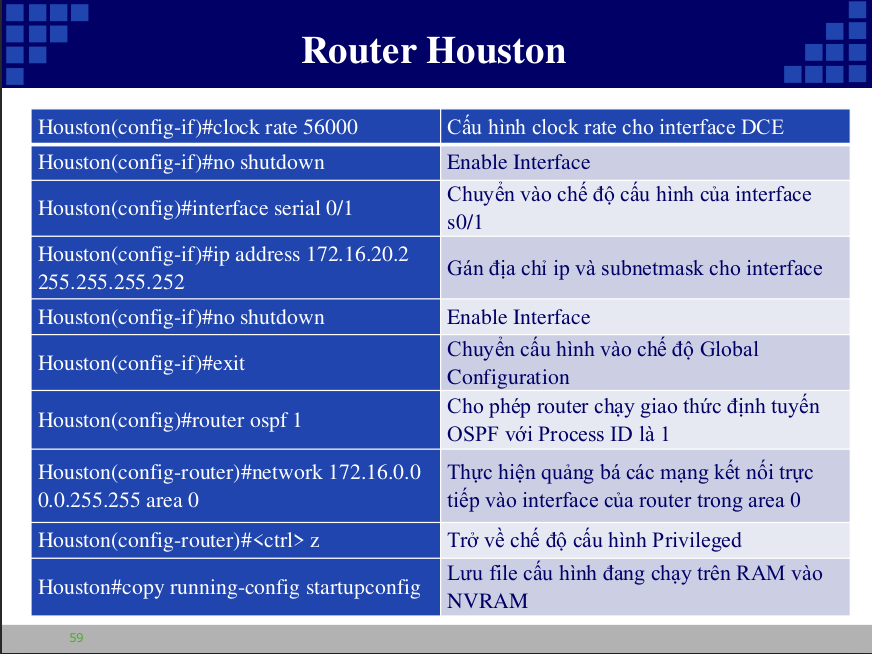
**Luyện tập:**

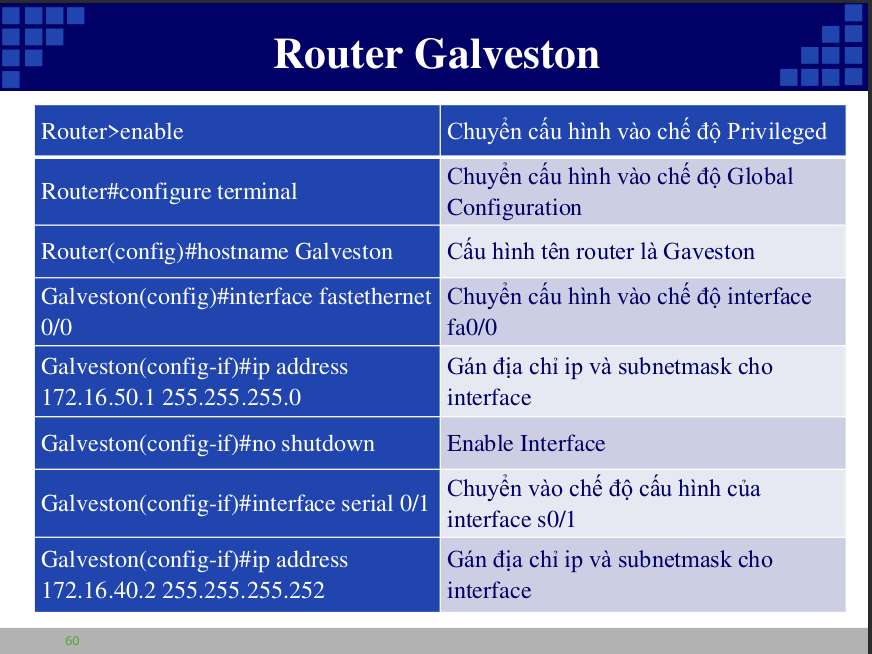
****

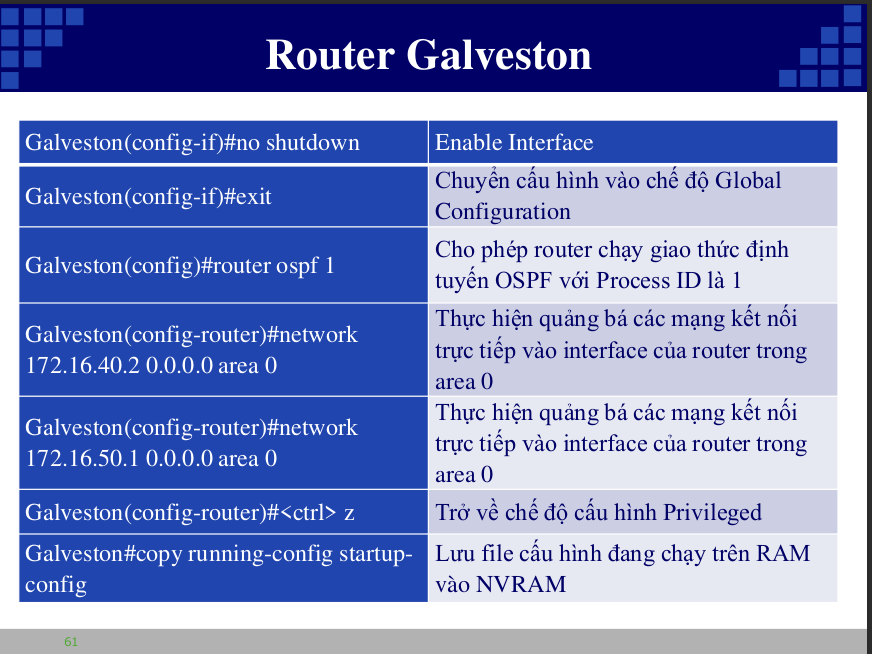
****

****

****

****

****

****

## 6. Dịch vụ DHCP

### Đặc trưng:

\_Cho phép host lấy địa chỉ IP động từ network server khi tham gia vào mạng

\_Có thể làm mới địa chỉ IP đang dùng

\_Có thể sử dụng lại các địa chỉ (chỉ giữ khi đang kết nối, còn sử dụng)

\_Cho phép thiết bị di động tham gia vào mạng (thời gian kết nối ngắn)

### Cơ bản về hoạt động của DHCP:

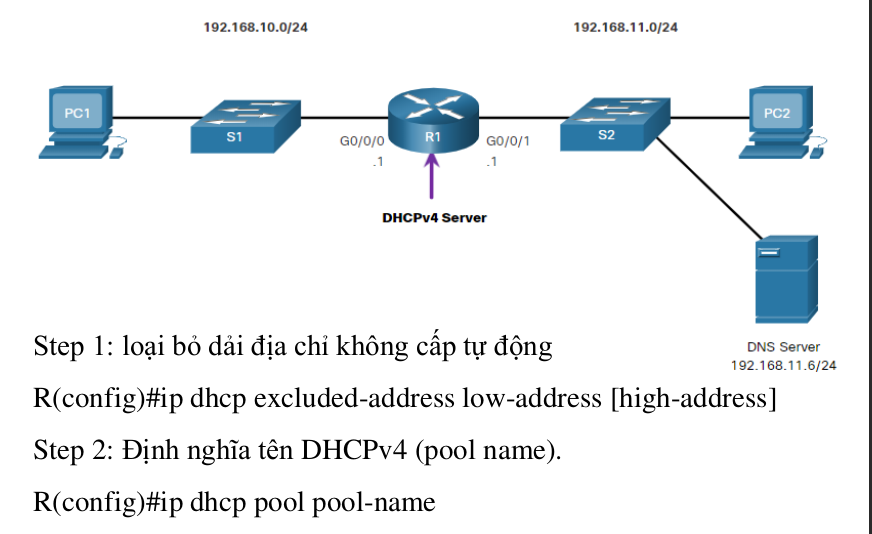
1. Host quảng bá bản tin **DHCP discover (**Xin cấp**)**

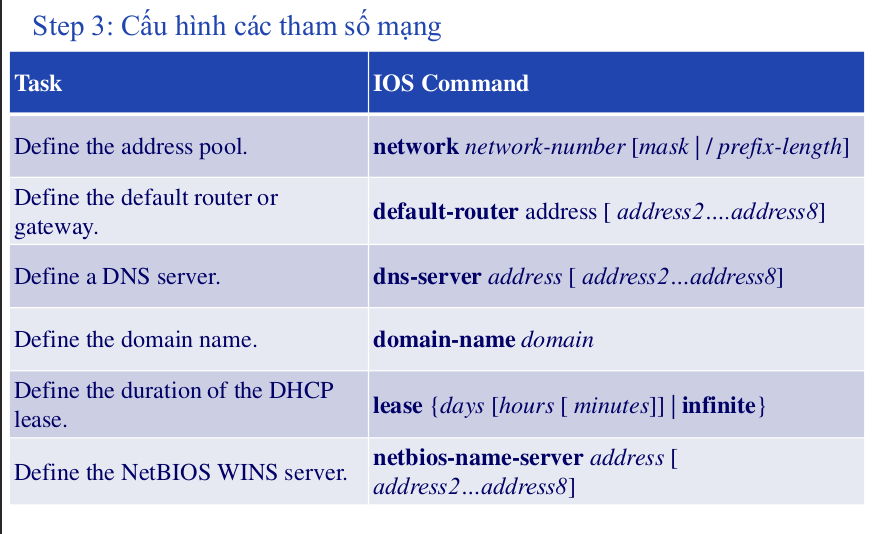
2. DHCP server trả lời bằng bản tin **DHCP offer (**Accept cấp**)**

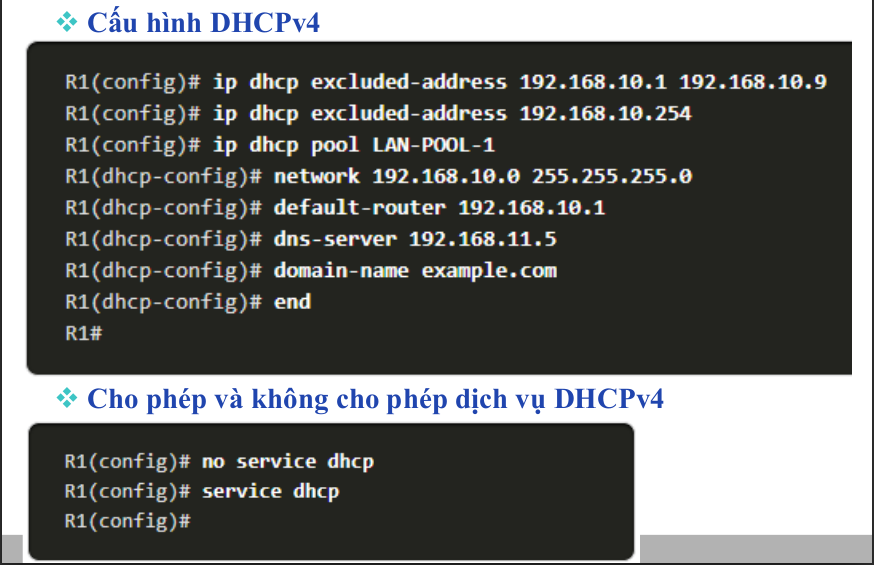
3. Host yêu cầu địa chỉ IP bằng bản tin **DHCP request (**yêu cầu địa chỉ IP**)**

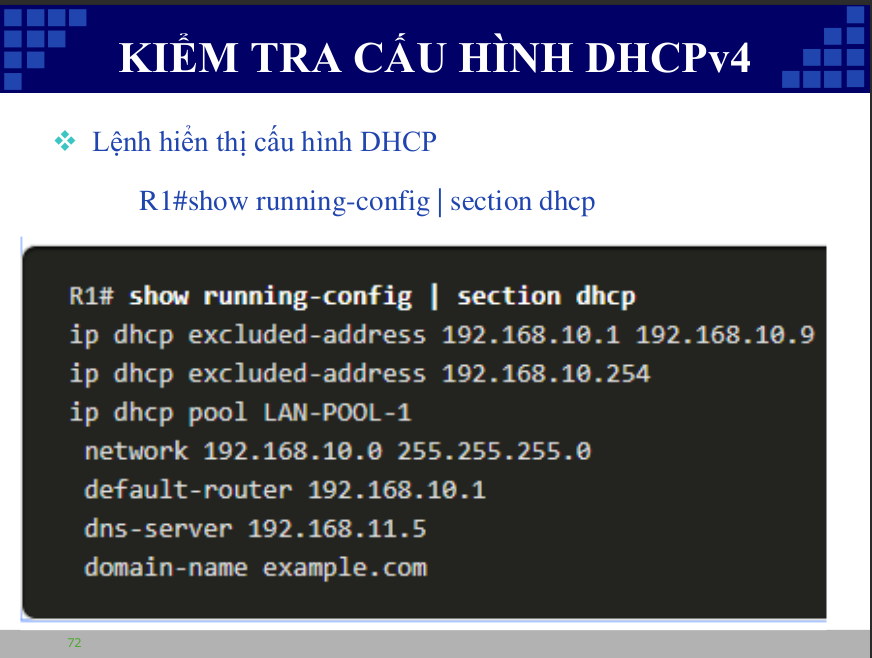
4. DHCP server gửi địa chỉ bản tin **DHCP ack (**Cấp**)**

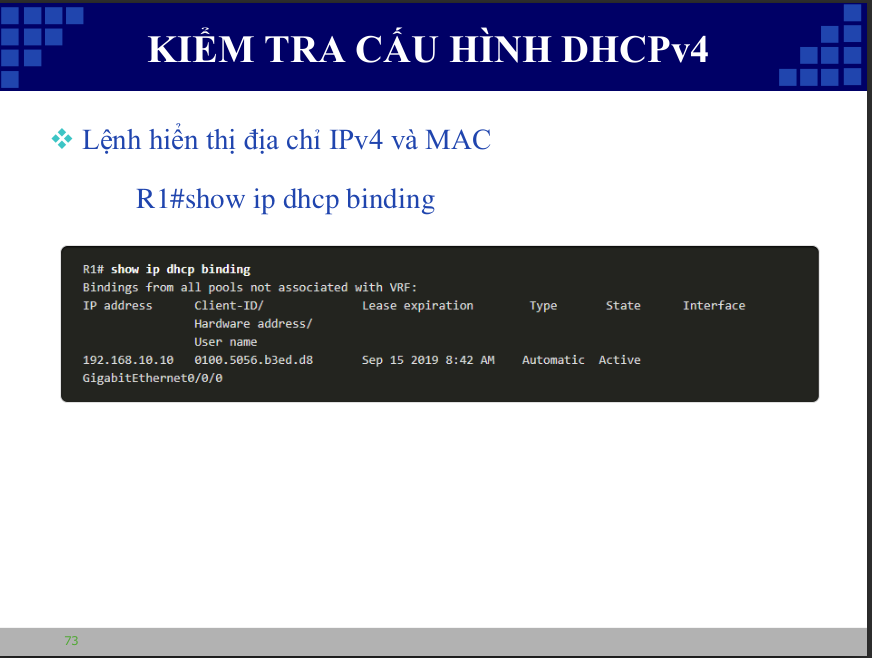
### Command: cấu hình dhcp v4

****

**VD:**

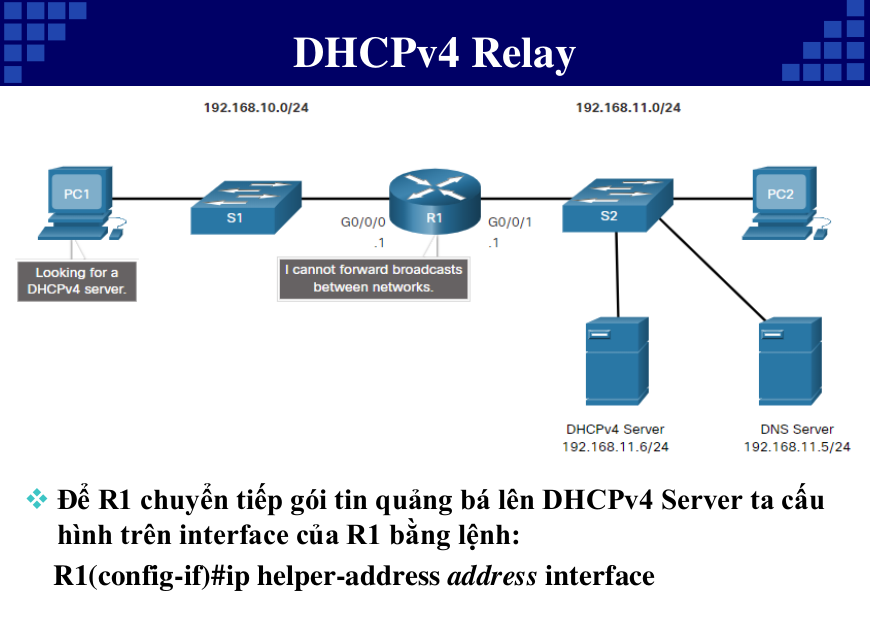


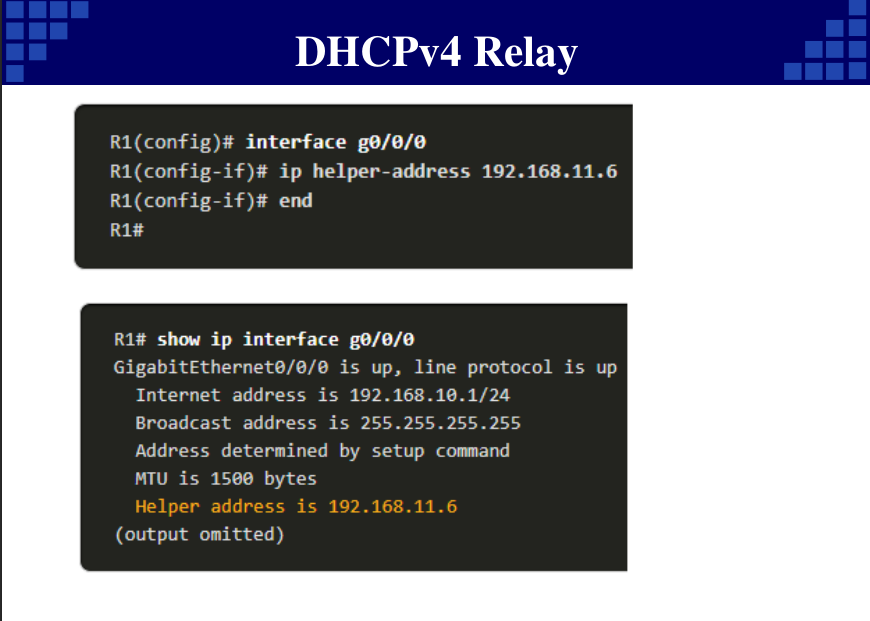


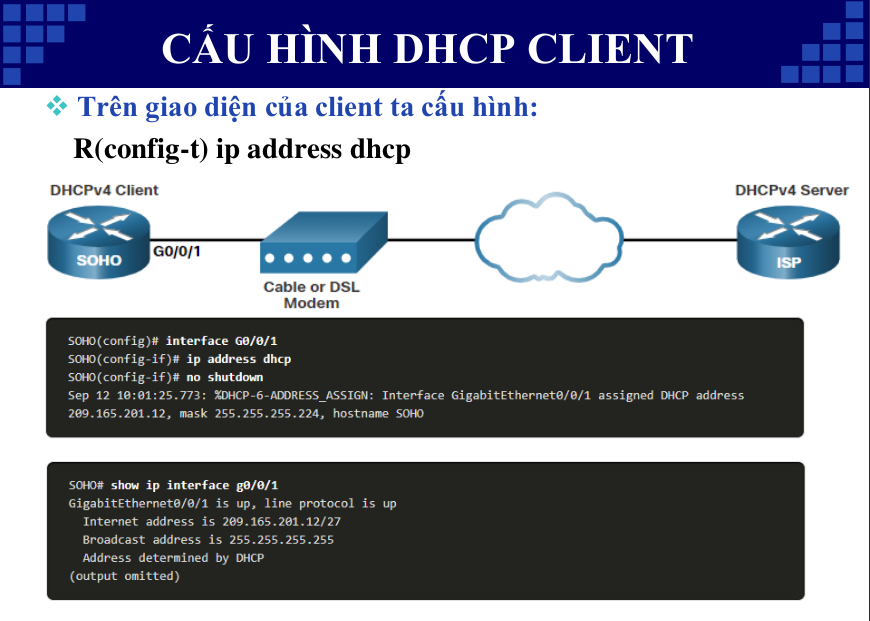


#### DHCPv4 Relay

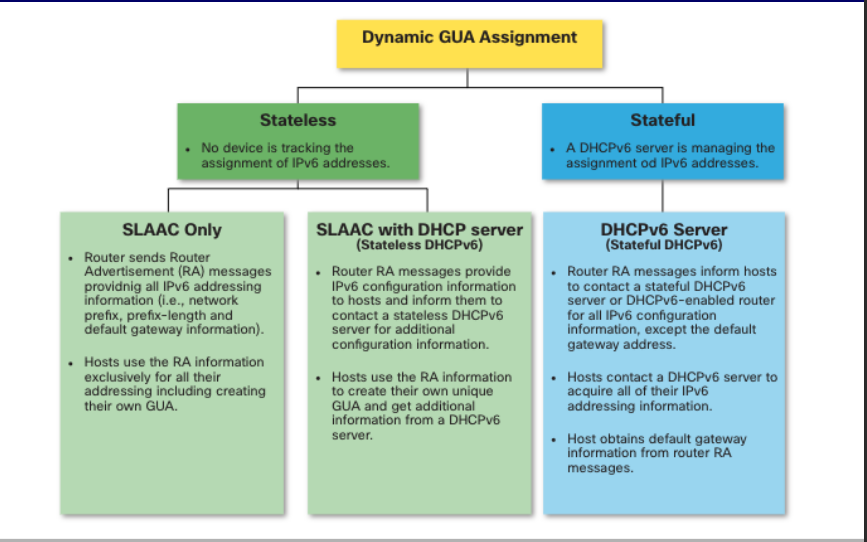
Nếu việc xin cấp địa chỉ IP đi qua router sẽ bị chặn nên cần phải cấu hình cho router chặn đó là nếu có yêu cầu nào xin cấp địa chỉ ip bằng dhcp thì có thể chuyển qua địa chỉ cụ thể

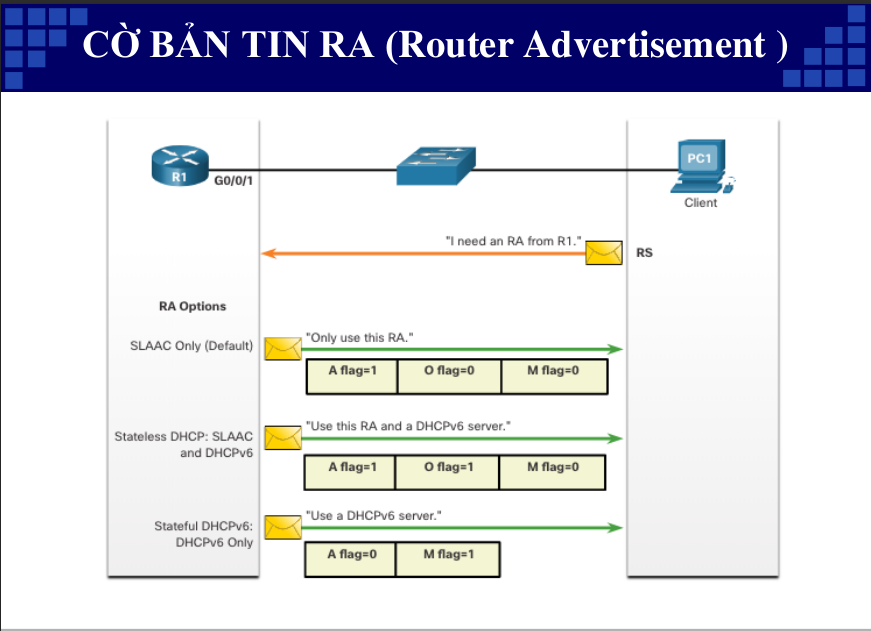






### Cấu hình DHCP v6





Có 3 options cấp địa chỉ IP cho host như sau:

|  |  |
| --- | --- |
| **Options** | **Thông tin** |
| SLAAC (stateless address autoconfiguration) | \_cho phép các máy host tạo địa chỉ GUA IPv6 duy nhất mà không cần các dịch vụ DHCPv6 Server  **Cơ chế triển khai:**  \_SLAAC gửi bản tin ICMPv6 RA định kỳ sau 200s cung cấp địa chỉ và thông tin cấu hình khác cho host để tự động cấu hình địa chỉ IPv6 dựa trên thông tin trong **RA.**  **Bao gồm những thông tin sau:**   |  |  | | --- | --- | | **Thông tin** | **Nội dung** | | **Prefix** | một địa chỉ IPv6 tiền tố được chia sẻ bởi các host trên mạng. | | **Default gateway** | một địa chỉ IPv6 của router được sử dụng làm gateway mặc định để gửi dữ liệu đến các đích ngoài mạng. | | **Lifetime** | thời gian sống của địa chỉ IPv6 được cấp phát cho host. | | **Miscellaneous** | bao gồm các tùy chọn khác như DNS server, time server, etc. |   \_Một máy host cũng có thể gửi một bản tin **RS (**Router Soclicitation**)** yêu cầu một **RA**  **\_SLAAC** có thể được triển khai dưới dạng **SLAAC** hoặc **SLAAC** với **DHCPv6**  **Command:**    Host sẽ nhận được **network-prefix, default-router, thiếu dns** |
| Stateless DHCPv6 | \_Có thể cấu hình thêm pool và DNS server  Command cấu hình **stateless DHCPv6 server**  Đầu tiên thực hiện lệnh **ipv6 unicast-routing** để thực hiện kích hoạt Ipv6 routing.  Stateless DHCPv6 is enabled using the **ipv6 nd other-config-flag** interface  configuration command setting the O flag to 1. |
| Statefull | Stateful DHCPv6 is enabled using the **ipv6 nd managed-config-flag** interface configuration  command setting the M flag to 1.  **Command:** |

# CHƯƠNG 3: CHUYỂN MẠCH TRONG MẠNG LAN

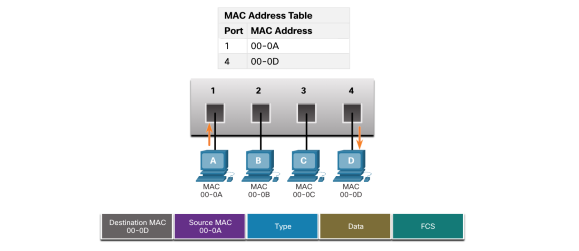
## 1. Khái niệm chung

### The MAC Address Table

\_Khi switch nhận các frame từ các thiết bị khác nhau, nó bằng cách kiểm tra địa chỉ MAC nguồn của mọi frame sau đó thực hiện cập nhật vảo trong bảng địa chỉ MAC

\_Khi bảng địa chỉ **MAC** của **switch** chứa địa chỉ MAC đích, nó có thể lọc khung và chuyển tiếp ra cổng tương ứng.

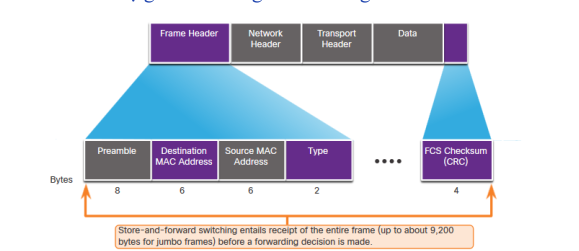
\_Khi không tìm thấy địa chỉ MAC bên trong bảng định tuyến của nó thì switch sẽ thực hiện gửi bản tin quảng ra tất cả các cổng ngoại trừ cổng nguồn (cổng mà bản tin được gửi tới switch). Sau đó nếu như host nào có địa chỉ MAC đích như địa chỉ mà switch gửi sẽ thực hiện gửi phản hồi lại cho switch. Switch nhận được bản tin sẽ thực hiện cập nhật bảng MAC của nó, cuối cùng thì thực hiện gửi gói tin tới địa chỉ đích.

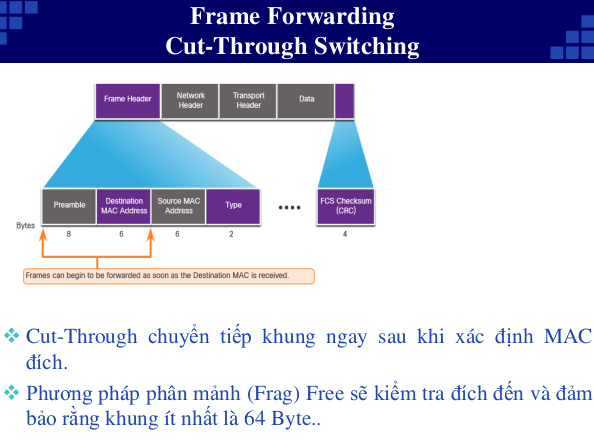


### Store and Forwarding Switching

\_Kiểm tra lỗi - **switch** sẽ kiểm tra **FCS checksum** để tìm lỗi **CRC.** Khung xấu sẽ bị loại bỏ

\_Bộ đệm - giao diện đầu vào sẽ đệm khung trong khi nó kiểm tra **FCS.** Điều này cũng cho phép switch điều chỉnh theo sự khác biệt tiềm ẩn về tốc độ giữa các cổng vào và cổng ra



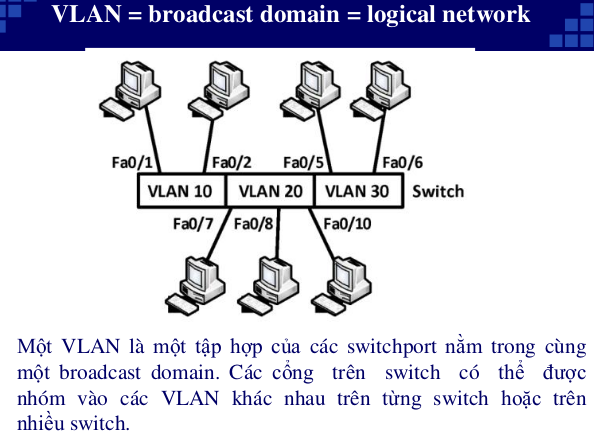


## 2. Mạng VLAN

\_**VLAN** là kỹ thuật sử dụng trên switch, dùng để chia một switch vật lý thành nhiều switch luận lý

\_mỗi một switch luận lý gọi là một VLAN (mạng ảo) hoặc có thể hiểu nó là một tập hợp các cổng mà trong đó chỉ có các cổng nằm trong một VLAN mới có thể giao tiếp được với nhau nếu không thực hiện config và được nằm trong cùng một miền quảng bá

\_các cổng trên switch có thể được nhóm vào các VLAN khác nhau trên một switch hoặc được triển khai trên nhiều switch



\_khi một gói tin quảng bá được gửi bởi một thiết bị nằm trong cùng VLAN đó, gói tin quảng bá sẽ không được chuyển tiếp đến các thiết bị thuộc VLAN khác.

### Ưu điểm:

+ Chia nhỏ miền quảng bá

+ Tăng bảo mật

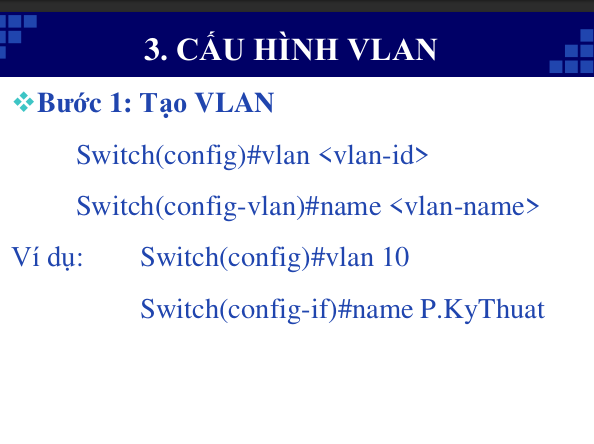
+ Giảm giá thành, dùng nhiều VLAN trên 1 switch vật lý

+ Dễ dàng trong quản trị

### Phân loại VLAN:

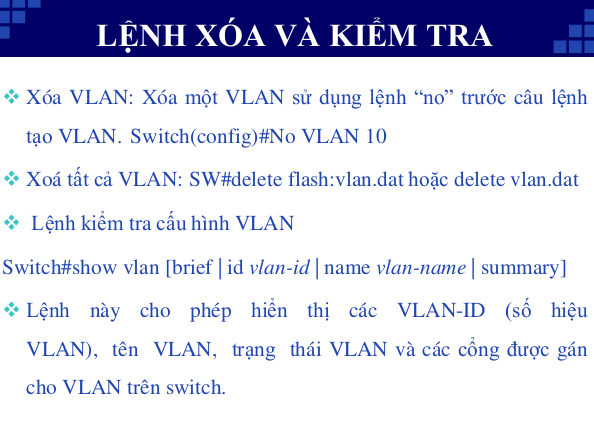
|  |  |
| --- | --- |
| **Phân loại** | **Chi tiết** |
| VLAN tĩnh | \_Các cổng switch được cấu hình thuộc về một VLAN nào đó  \_các thiết bị gắn vào cổng đó sẽ thuộc về VLAN đã định trước |
| VLAN động | \_Loại VLAN này sử dụng một server lưu trữ địa chỉ MAC của các thiết bị và quy định VLAN mà thiết bị đó thuộc về, khi một thiết bị gắn vào switch, switch sẽ lấy địa chỉ MAC của thiết bị và gửi cho server kiểm tra và cho vào VLAN định trước |
| Data VLAN | \_Dành riêng cho lưu lượng truy cập do người dùng tạo (email và lưu lượng truy cập web)  \_Phân chia mạng vật lý thành các phân đoạn nhỏ hơn  \_Giúp quản trị viên kiểm soát được lưu lượng mạng của từng ứng dụng  \_**Data vlan** là vlan dữ liệu mặc định vì tất cả các giao diện được gán cho vlan này |
| Default vlan (**VLAN 1**) |
| Native VLAN | \_Đây là VLAN được sử dụng cho các liên kết thân cây  \_Tất cả các khung được gắn thẻ trên liên kết trung kế **802.1Q** ngoại trừ những khung trên VLAN gốc |
| Management VLAN | \_Điều này được sử dụng cho lưu lượng  SSH/Telnet VTY và không được mang theo lưu lượng người  dùng cuối. Thông thường, Vlan là SVI cho Switch Lớp 2. |
| Voice Vlan | \_VLAN được sử dụng cho lưu lượng thoại  \_Đảm bảo băng thông  \_Ưu tiên cao hơn  \_Tránh tắc nghẽn  \_Độ trễ nhỏ  \_Toàn bộ mạng phải được thiết kế để hỗ trợ thoại |

### Command: Cấu hình VLAN









## 3. Trunking

### Đặc trưng:

Cách tổ chức để các thiết bị cùng VLAN nhưng ở trên nhiều switch khác nhau có thể liên lạc với nhau?

=> Dùng mỗi kết nối cho từng VLAN => Điều này gây ra lãng phí.

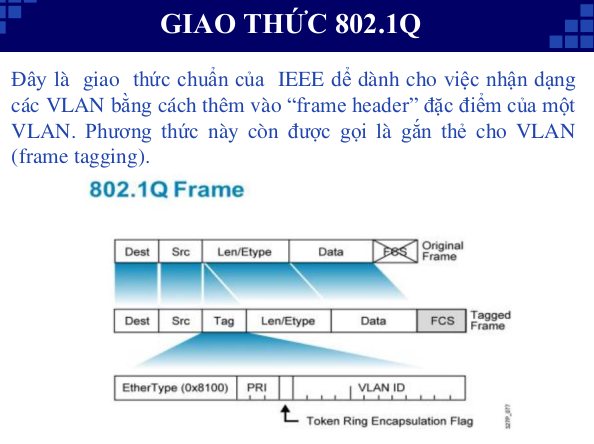
=> Sử dụng kết nối đường **trunking**

Một kỹ thuật khác để giải quyết vấn đề trên là dùng chỉ một kếtnối cho phép dữ liệu của các VLAN có thể cùng lưu thông qua đường này. Người ta gọi kết nối này là đường trunk.

=> Đường dây như thế gọi là **liên kết trunk lớp 2.**

### Tagging:

Vì kỹ thuật này cho phép dùng chung một kết nối vật lý cho dữ liệu của các VLAN đi qua nên để phân biệt được chúng là dữ liệu của VLAN nào, người ta gắn vào các gói tin một dấu hiệu gọi là “tagging”. Hay nói cách khác là dùng một kiểu đóng gói riêng cho các gói tin di chuyển qua đường “trunk” này. Giao thức được sử dụng là 802.1Q (dot1q).



### Command: Cấu hình trunk



**switchport trunk allowed vlan <vlan1>, <vlan2>, ...**

## 4. Giao thức VTP

\_VTP là giao thức hoạt động ở tầng liên kết dữ liệu trong mô hình **OSI**

\_giúp cho việc cấu hình VLAN luôn đồng nhất khi thêm, xóa, sửa thông tin về VLAN trong hệ thống mạng

\_hỗ trợ người quản trị thêm sửa xóa vlan nhanh chóng mà không cần phải thực hiện nhiều công việc. VD: Muốn thêm VLAN ở 3 switch thì chỉ cần cấu hình trên một switch sau đó thực hiện đồng bộ trên 2 vlan còn lại => giao thức **VTP**

### Điều kiện sử dụng giao thức VTP

+ Các switch phải cùng một **VTP domain**

### Giao thức vtp quy định 3 chế độ hoạt động

1. Chế độ **Server**

**\_**Tạo sửa xóa thông tin VLAN

\_Gửi thông tin quảng bá ra các cổng trunk

\_Đồng bộ thông tin VLAN

1. Chế độ **Client**

**\_Không** tạo, sửa, xóa thông tin của VLAN

**\_**Có đồng bộ mọi sự thay đổi của VLAN từ server

**\_**Có thể gửi các thông điệp bình thường qua các cổng trunk.

1. Chế độ **Transparent**

\_Có thể tạo các VLAN cục bộ

\_Có thể nhận và chuyển tiếp các thông điệp quảng bá VTP để cho các switch khác cấu hình

\_Không cập nhật vào cơ sở dữ liệu của nó (không cập nhật thông tin VTP)

### Cơ chế hoạt động

\_**VTP** thực hiện gửi thông điệp quảng bá qua **VTP domain** mỗi 5 phút một lần hoặc khi có sự thay đổi trong cấu hình của **VLAN.**

\_Mỗi thông điệp VTP bao gồm: “**revision number**” (số lần cấu hình), tên VLAN, số hiệu VLAN …

\_Mỗi lần VTP server điều chỉnh thông tin VLAN, nó tăng “revision number” lên 1 trước khi gửi thông tin quảng bá VTP đi. Và khi một switch nhận revision number cao hơn nó sẽ thực hiện cập nhật cấu hình VLAN.

## 5. Định tuyến giữa các VLAN

## 6. Giao thức STP

# CHƯƠNG 4: CÔNG NGHỆ MẠNG WAN

## 1. Mục đích mạng wan và một số khái niệm

### 1.1. Sự khác biệt giữa WAN là LAN

|  |  |
| --- | --- |
| **Local Area Networks (LANs)** | **Wide Area Networks (WANs)** |
| Cung cấp dịch vụ mạng trong một khu vực địa lý nhỏ. | Cung cấp dịch vụ mạng trong một khu vực địa lý rộng lớn. |
| Quản lý bởi một cơ quan, tổ chức hoặc người dùng gia đình. | Sở hữu và quản lý bởi các nhà cung cấp dịch vụ internet, điện thoại, cáp và vệ tinh |
| Ngoài chi phí đầu tư cơ sở hạ tầng mạng, sử dụng mạng LAN không mất phí. | Sử dịch vụ WAN có tính phí. |
| Cung cấp tốc độ băng thông cao sử dụng dịch vụ Ethernet và Wi-Fi có dây. | Các nhà cung cấp mạng WAN cung cấp tốc độ băng thông từ thấp đến cao, trên khoảng cách xa. |

### 1.2. Private và Public wans

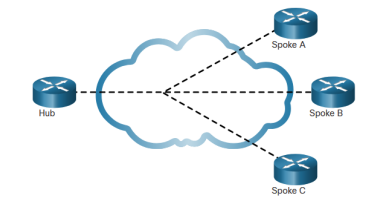
|  |  |
| --- | --- |
| **Private WANS** | **Public wans** |
| \_Dùng kết nối riêng cho một khách hàng  + Đảm bảo chất lượng dịch vụ  + Băng thông được đảm bảo  + Đảm bảo tính bảo mật | **\_**cung cấp bởi ISP  \_các chất lượng dịch vụ và băng thông có thể thay đổi, các kết nối được chia sẻ và không đảm bảo tính bảo mật. |

### 1.3. WAN TOPOLOGIES

1. **Point-to-Point Topology**

**\_**Hai thiết bị trực tiếp kết nối với nhau (**router, modem**)

1. **Hub-and-Spoke Topology**



**\_Hub** làphần trung tâm hỗ trợ giao tiếp giữa các spoke

1. **Dual-homed Topology**

\_Hai hub – nhiều spoke

**\_**Các spoke phải kết nối tới cả hai Hub

\_Một hub dùng dự phòng, cân bằng tải, xử lý phân tán.

\_Phức tạp hơn

1. **Fully Meshed Topology**

\_Tất cả các site được kết nối với nhau

\_Khả năng chịu lỗi cao nhất

1. **Partially Meshed Topology**

\_Các site có thể kết nối tới tất cả site còn lại hoặc không, ít nhất một kết nối.

### 1.4. KẾT NỐI VỚI ISP

\_Tổ chức có thiết lập **WAN** cũng có thể kết nối tới **Internet =>** Ký thỏa thuận cấp độ dịch vụ (**SLA**) với ISP.

\_**SLA** nêurõ các dịch vụ dự kiến và cam kết về độ tin cậy, tính khả dụng, hiệu suất của internet.

\_Có nhiều cách có thể kếtnối WAN tới ISP:

#### 1.4.1. Single-homed

\_Kết nối với 1 ISP, không dự phòng, ít tốn kém

#### 1.4.2. Dual-homed

\_Kết nối cùng 1 ISP bằng 2 liên kết. ~ cung cấp cả dự phòng và cân bằng tải

**1.4.3. Multi-homed**

\_Kết nối tới 2 ISP khác nhau

\_Tăng dự phòng, cân bằng tải => tốn kém

**1.4. Dual-multihomed**

**\_**Kết nối tới nhiều ISP bằng nhiều liên kết dự phòng => Đắt nhất

## 2. Hoạt động của mạng WAN

Tiêu chuẩn mạng WAN được xác định quản lý bởi nhiều tổ chức như: **TIA/EIA, ISO, IEEE**

### 2.1. WANS trong mô hình OSI

Hầu hết các tiêu chuẩn WAN đều tập trung vào lớp vật lý và lớp liên kết dữ liệu.

Dưới đây là một số giao thức và công nghệ được sử dụng trong các lớp này để xây dựng và vận hành các mạng **WAN.**

#### Lớp 1:

**+ SDH (Hệ thống truyền dẫn số đồng bộ).**

**+ SONET (Mạng quang đồng bộ)**

**+ DWDM (Ghép kênh phân chia theo bước sóng dày đặc)**

#### Lớp 2:

**+ Băng thông rộng (DSL và Cáp)**

**+ Không dây (Wireless)**

**+ Ethernet WAN**

**+ MPLS**

### 2.6. KỸ THUẬT CHUYỂN MẠCH KÊNH

\_Thiết lập kênh truyền ảo thông qua mạng của ISP trước khi có thể liên lạc.

\_Hai loại công nghệ phổ biến:

+ Mạng điện thoại chuyển mạch công cộng (PSTN)

+ Mạnh kĩ thuật số tích hợp dịch vụ kế thừa (ISDN)

### 2.7. KỸ THUẬT CHUYỂN MẠCH GÓI

\_Các loại công nghệ chuyển mạch gói phổ biến

+ Ethernet WAN

+ Nhãn đa giao thức (MPLS)

+ Chuyển mạch khung (Frame relay)

+ Chuyển mạch không đồng bộ (ATM)

## 3. Công nghệ mạng riêng ảo VPN

\_Tạo kết nối mạng riêng thông qua mạng WAN

\_Nó mang thông tin mạng riêng nhưng thông tin đó được truyền qua mạng công cộng (mã hóa)

\_Các site kết nối với nhau thông qua VPN gateways (mã hóa bảo mật, truyền dữ liệu, …)

\_Một remote-access VPN được tạo động để thiết lập kết nối an toàn giữa máy khách từ xa và thiết bị đầu cuối VPN.

# CHƯƠNG 5: BẢO MẬT MẠNG

## 1. Giới thiệu chung

### 1.1. Tường lửa – firewall

\_Nằm giữa hai hoặc nhiều mạng

\_Kiểm soát lưu lượng và chặn truy cập trái phép

\_Có thể cho người dùng bên ngoài truy cập có kiểm soát vào cách dịch vụ cụ thể

#### Các loại tường lửa

**Ngăn chặn hoặc cho phép truy cập dựa trên:**

\_Lọc gói bằng địa chỉ IP hoặc MAC

\_Lọc ứng dụng: cho phép ứng dụng cụ thể dựa trên số cổng

\_Lọc URL: Ngăn chặn vào những trang web dựa trên url, từ khóa cụ thể

\_Kiểm tra trạng thái gói:

## 2. Danh sách điều khiển truy cập ACL

### 2.1. ACL trên router cisco

\_Loạt lệnh theo chuẩn ISO

\_Lọc gói dựa trên thông tin tìm thấy trên tiêu đề gói

\_Mặc định Router không có bất kì ACL nào được cấu hình

\_ACL được áp dụng cho một giao diện cụ thể, mục đích đánh giá gói tin đi qua giao diện xem có chuyển tiếp được hay không.

\_Sử dụng một danh sách tuần tự các câu lệnh cho phép hoặc từ chối được gọi là **ACE (**mục kiểmsoát truy cập**)**

**\_**Sựcho phép dựa vào địa chỉ nguồn, địa chỉ đích, giao thức hoặc chỉ số cổng.

### 2.2. Hoạt động của ACLs

\_So sánh lần lượt với từng rule, match thì đi tiếp không thì chặn.

\_Nếu tất cả không match thì mặc định có một cái deny ở cuối.

\_Việc kiểm tra sẽ có thể đặt ở cả interface đầu vào và interface đầu ra.

### 2.3. Phân loại ACL

+ Chia thành 2 loại:

\_ **Standard ACL**

**\_ Extended ACL**

### 2.4. Cấu hình ACL

#### Có hai phương pháp cấu hình ACL:

**\_**Dựa vào số (**numbered ACL** ~ mỗi quy tắc được đặt thành một con số duy nhất)

\_Dựa vào tên (**named ACL** ~ mỗi quy tắc được đặt thành một tên duy nhất)

+ Các bước thiết lập **ACL:**

**Bước 1:**

**\_**Xác địnhloại ACL dựa vào số hiệu ACL (**numbered ACL**) **hoặc** tên **(named ACL)**

**\_**Lựa chọn hành động cho từng điều kiện “permit” hay “deny” theo yêu cầu cụ thể

**Bước 2**:

\_Gán ACL được gán vào một hoặc nhiều cổng và có thể lọc theo chiều vào hoặc ra.

+ Một só thuật ngữ

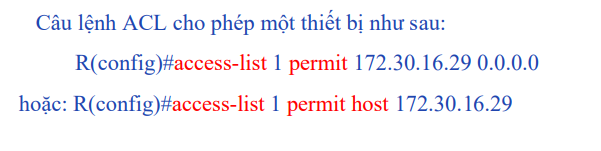
#### Một số thuật ngữ

1. **Wildcard mask**

**\_**Với tiêu chuẩn **ACL,** nếu không thêm **wildcard-mask** trong câu lệnh tạo ACL thì mặc định wildcard-mask là 0.0.0.0

1. **Wildcard-host**

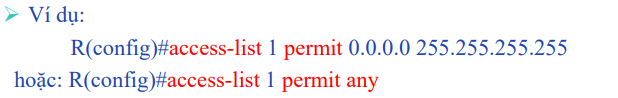
**\_Wildcard-mask** dùng cho một thiết bị hay còn gọi là wildcard-host. Ví dụ: host **172.30.26.29**



1. **Wildcard-any**

Cho tất cả các thiết bị được gọi là wildcard “any” có dạng 255.255.255.255 (không kiếm tra tất cả các bit)

* Chấp nhận tất cả các địa chỉ



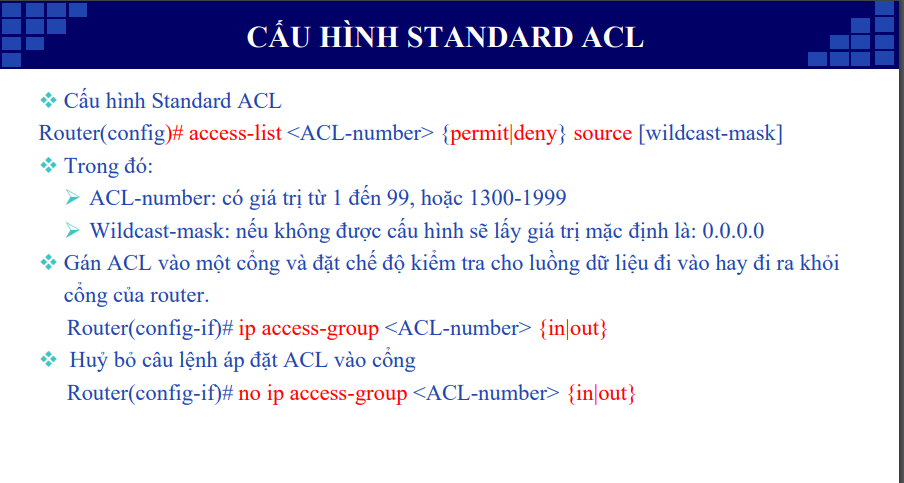
1. **Inbound và outbound**

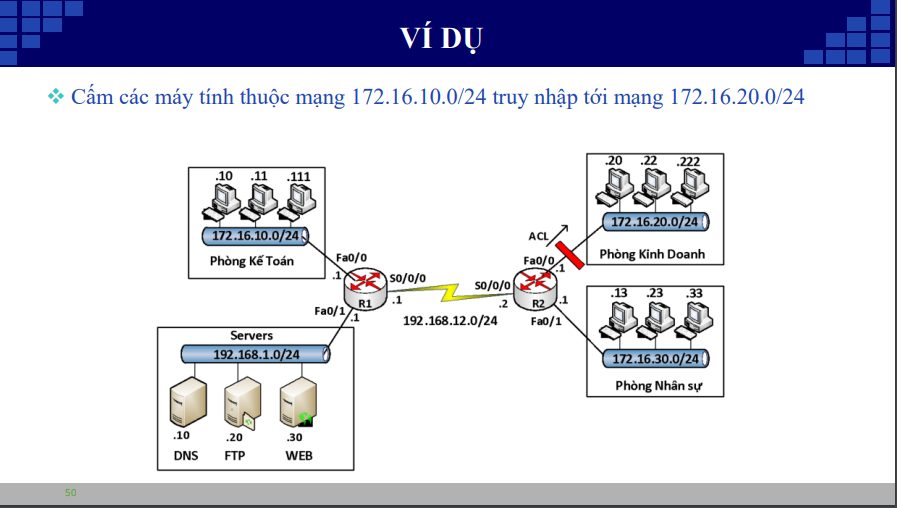
**\_**Xác định chiều kiểm tra là kiểm tra đầu vào hay đầu ra

#### Cấu hình standard acl

\_Sử dụng khi ta muốn cấm hay cho phép tất cả các luồng dữ liệu từ một thiết bị hay một mạng xác định trên toàn bộ giao thức.

**\_**Kiểm tra điều kiện dựa vào địa chỉ nguồn gói tin





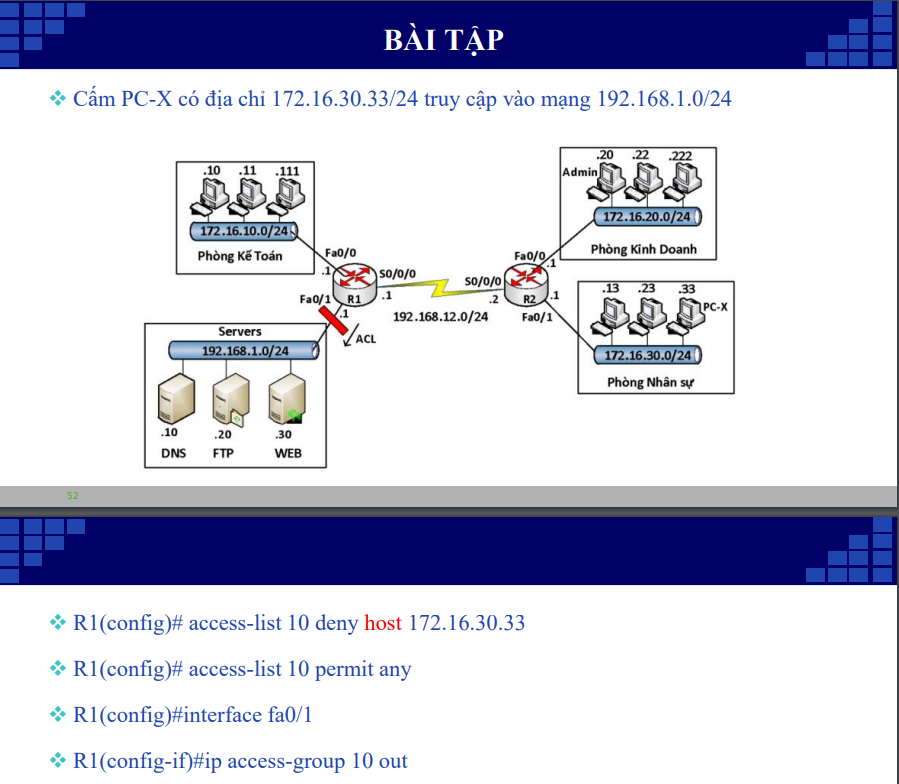


**Giải thích:**

\_Cấm địa chỉ với đầu là **172.16.10.0**

**\_**Các địa chỉ khác thì được **permit**

**\_**Truy cập vào **interface fa0/0** sau đó cấp acl cho interface này với đầu ra bởi vì nếu thực hiện cấm đầu vào thì ip phòng kế toán không truy cập được vào bên trong của phòng nhân sự.



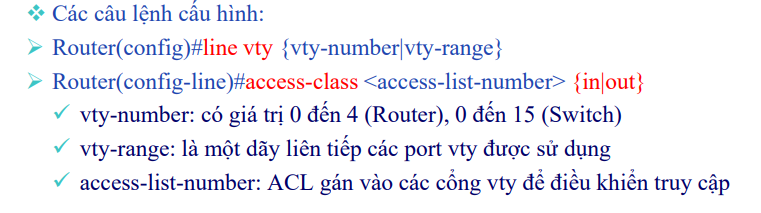
#### Cấu hình điều khiển telnet sử dụng standard acl

\_Trên router có các port được dùng để cấu hình cho mục đích cho phép telnet vào router

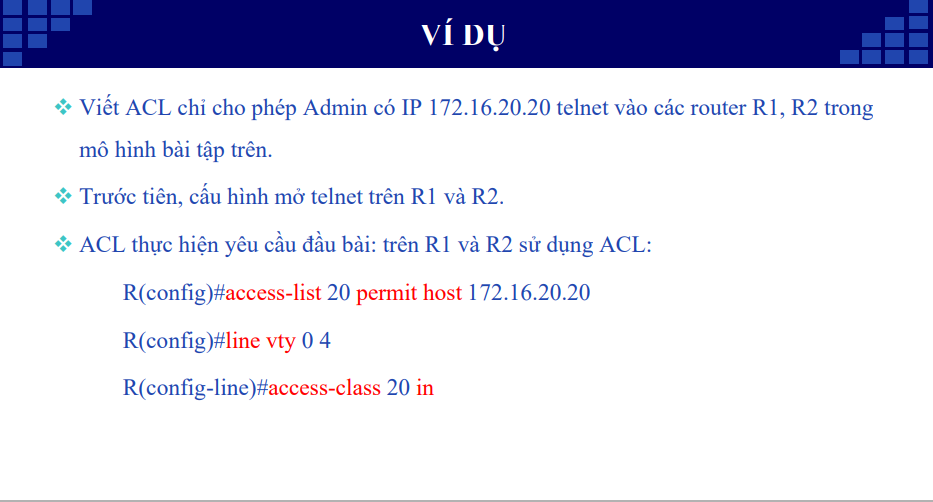
**Hai bước chính:**

+ Truy cập vào trong các port ảo để cấu hình

+ Cấu hình acl

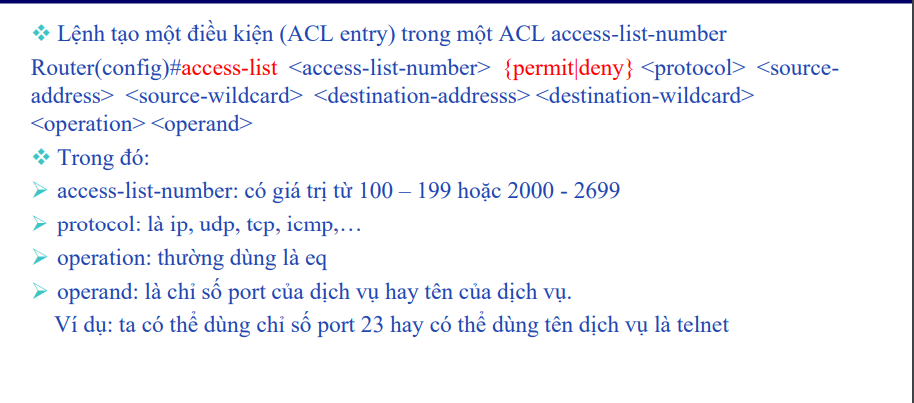


**Access-class** sử dụng cho kết nối **telnet** hoặc **ssh**

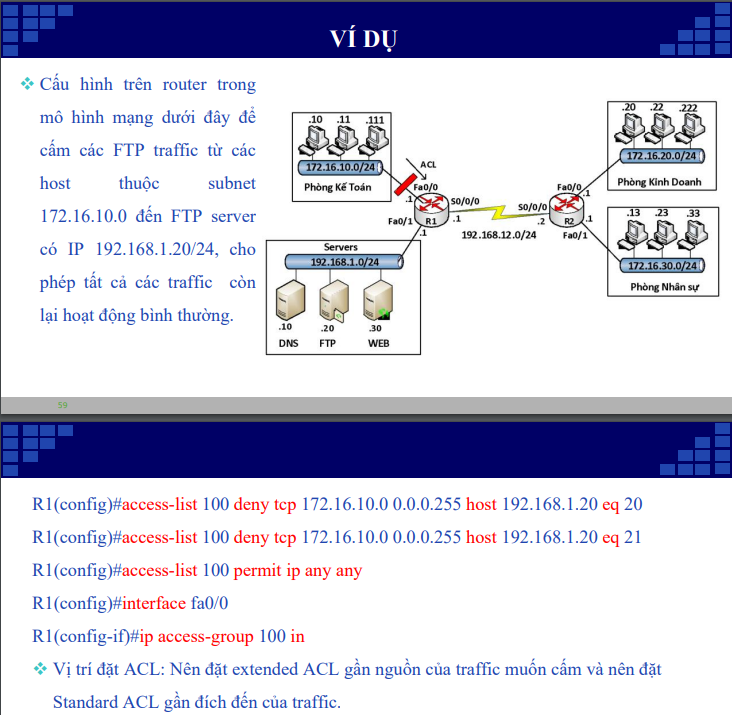


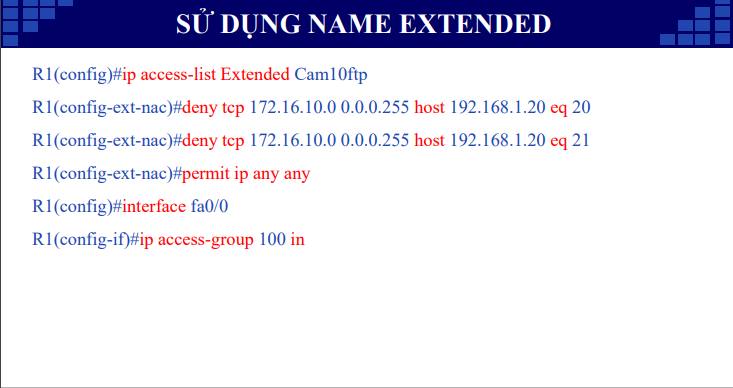
#### Cấu hình extended acl

\_Ngoài kiểm tra cả địa chỉ nguồn, còn kiểm tra địa chỉ đích, giao thức, chỉ số cổng ứng dụng.





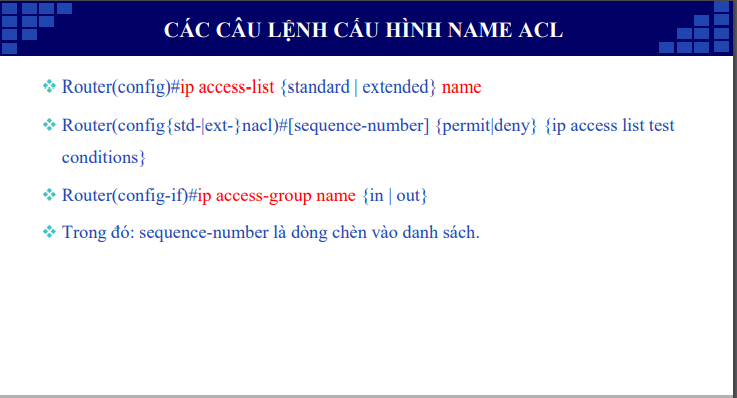




#### Named acl

\_Cho phép xóa một số dòng điều kiện cấu hình

\_Không tương thích Cisco IOS phiên bản trước 11.2



# ÔN TẬP

**I. Lý thuyết**

Kiểm tra trắc nghiệm 25 câu => all

**II. Bài tập**

1. Chia mạng

a. Chia mạng con đều:

\_\_\_xác định mạng con, dải IP, địa chỉ broadcast khi biết địa chỉ IP

b. Chia không đều

192.168.1.0/24

→

+ Chia thành 4 mạng và gán cho các mạng trong sơ đồ

B1: chia mạng trên thành 2 mạng con

|  |
| --- |
| mạng 1: 192.168.1.0/25 |
| mạng 2: 192.268.1.128/25  Tiếp tục chia đôi thành hai mạng con  → 192.168.1.128/26 → mạng 2 |

+ Cấu hình cơ bản

+ Cấu hình định tuyến

2.