**Mục lục**

[Tuần 2 1](#_Toc142366544)

[1. Etherchannel 1](#_Toc142366545)

[1.1 Khái niệm 1](#_Toc142366546)

[1.2 Điều kiện cấu hình 1](#_Toc142366547)

[1.3 Mục đích 2](#_Toc142366548)

[1.4 Phân loại EtherChannel: 2](#_Toc142366549)

[1.5 Cân bằng tải trên EtherChannel: 2](#_Toc142366550)

[2. Inter Vlan routing 3](#_Toc142366551)

[2.1 Khái niệm 3](#_Toc142366552)

[2.2 Lợi ích 3](#_Toc142366553)

[3.3 Phân loại 3](#_Toc142366554)

[3. Sub interface 4](#_Toc142366555)

[3.1 Mục đích 4](#_Toc142366556)

[3.2 Khái niệm 4](#_Toc142366557)

[3.3 Vai trò 4](#_Toc142366558)

[4. Bảo mật trong mạng LAN 4](#_Toc142366559)

[4.1 ARP spoofing 4](#_Toc142366560)

[4.2 MAC spoofing 7](#_Toc142366561)

[4.3 DHCP spoofing 8](#_Toc142366562)

[5. Layer 3 Router 9](#_Toc142366563)

[6. Định tuyến 11](#_Toc142366564)

[6.1 Khái niệm 11](#_Toc142366565)

[6.2 Phân loại: 11](#_Toc142366566)

[7. Các giao thức định tuyến 14](#_Toc142366567)

[7.1 RIP(Routing Information Protocol) 14](#_Toc142366568)

[7.2 OSPF 15](#_Toc142366569)

[7.3 EIGRP 16](#_Toc142366570)

[7.4 So sánh 17](#_Toc142366571)

[8. VSS(Vitual Switching System) 18](#_Toc142366572)

[8.1 Khái niệm 18](#_Toc142366573)

[8.2 Mục đích 19](#_Toc142366574)

[9. vPC (virtual port channel) 20](#_Toc142366575)

[9.1 Khái niệm 20](#_Toc142366576)

[9.2 Đặc điểm 21](#_Toc142366577)

[10. Policy based routing 21](#_Toc142366578)

[10.1 Khái niệm 21](#_Toc142366579)

[10.2 Cách hoạt động 22](#_Toc142366580)

[10.3 Mục đích 23](#_Toc142366581)

[11. ACL 23](#_Toc142366582)

[11.1 Khái niệm 23](#_Toc142366583)

[11.2 Mục đích 24](#_Toc142366584)

[11.3 Phân loại 24](#_Toc142366585)

[11.4 Named ACL 24](#_Toc142366586)

[12. HSRP 25](#_Toc142366587)

[12.1 Khái niệm 25](#_Toc142366588)

[12.2 Chức năng 25](#_Toc142366589)

[12.3 Ưu nhược 26](#_Toc142366590)

[13. VRRP 26](#_Toc142366591)

[13.1 Khái niệm 26](#_Toc142366592)

[14. GLBP 27](#_Toc142366593)

[14.1 Khái niệm 27](#_Toc142366594)

# Tuần 2

## 1. Etherchannel

### 1.1 Khái niệm

Công nghệ EtherChannel của Cisco cho phép kết hợp các kết nối Ethernet thành một bó (bundle) để tăng băng thông. Mỗi bundle có thể bao gồm từ hai đến tám kết nối Fast Ethernet hay Gigabit Ethernet, tạo thành một kết nối luận lý gọi là FastEtherChannel hay Gigabit EtherChannel. Kết nối này cung cấp một băng thông lên đến 1600Mbps hoặc 16 Gbps.

Còn được gọi là Link Aggrengation Control Protocol (LACP), là 1 kỹ thuật được sử dụng trong các mạng máy tính để kết hợp nhiều liên kết vật lý giữa 2 thiết bị chuyển mạch mạng thành 1 liên kết logic duy nhật => cung cấp bang thông và dự phòng tang lên, cải thiện cân bằng tải.

### 1.2 Điều kiện cấu hình

Tất cả các cổng phải có:

-Cùng song công

-Cùng tốc độ

-Cùng 1 cấu hình VLAN (VLAN gốc và VLAN được phép phải giống nhau)

-Chuyển đổi chế độ cổng phải giống nhau (chế độ truy cập hoặc trung kế)

### 1.3 Mục đích

Etherchannel trên một Switch sẽ thực hiện "bó" nhiều đường đấu nối thành 1 đường duy nhất, coi các đường này chỉ như 1 đường .

### 1.4 Phân loại EtherChannel:

EtherChannel có thể được phân loại dựa trên số lượng liên kết vật lý được gom nhóm:

-**EtherChannel 2 cổng**: Còn được gọi là "Port Channel," loại này bao gồm gom nhóm hai liên kết vật lý thành một liên kết logic duy nhất.

-**EtherChannel 4 cổng**: Còn được gọi là "Fast EtherChannel," loại này bao gồm gom nhóm bốn liên kết vật lý.

-**EtherChannel 8 cổng**: Còn được gọi là "Gigabit EtherChannel," loại này bao gồm gom nhóm tám liên kết vật lý.

### 1.5 Cân bằng tải trên EtherChannel:

Cân bằng tải trong EtherChannel cho phép phân phối lưu lượng trên các liên kết được gom nhóm, tối ưu hóa việc sử dụng băng thông và giảm tắc nghẽn trên các liên kết cá nhân. Có nhiều phương pháp cân bằng tải khả dụng cho EtherChannel, và phương pháp cụ thể được sử dụng có thể thay đổi dựa trên nền tảng switch và cấu hình.

Một số phương pháp cân bằng tải thông thường cho EtherChannel bao gồm:

**Địa chỉ MAC nguồn**: Lưu lượng được phân phối dựa trên địa chỉ MAC nguồn của gói tin.

**Địa chỉ MAC đích**: Lưu lượng được phân phối dựa trên địa chỉ MAC đích của gói tin.

**Địa chỉ IP nguồn**: Lưu lượng được phân phối dựa trên địa chỉ IP nguồn của gói tin.

**Địa chỉ IP đích**: Lưu lượng được phân phối dựa trên địa chỉ IP đích của gói tin.

**Địa chỉ IP nguồn và đích**: Lưu lượng được phân phối dựa trên cả hai địa chỉ IP nguồn và đích của gói tin.

Thuật toán cân bằng tải nên được cấu hình trên cả hai đầu của EtherChannel để đảm bảo phân phối lưu lượng đúng trên các liên kết được gom nhóm. Phương pháp cân bằng tải cụ thể được chọn nên phụ thuộc vào các mẫu lưu lượng mạng và yêu cầu.

## 2. Inter Vlan routing

### 2.1 Khái niệm

Định tuyến Inter-VLAN có thể được định nghĩa là một cách để chuyển tiếp lưu lượng giữa các VLAN khác nhau bằng cách triển khai một bộ định tuyến trong mạng.

### 2.2 Lợi ích

-Bảo mật: tạo ra các vùng cấp độ bảo mật khác nhau cho người dùng hoặc ứng dụng khác nhau.

### 3.3 Phân loại

Có ba loại định tuyến giữa các VLAN và đó là:

**Định tuyến Inter-VLAN kế thừa** Sử dụng bộ định tuyến có nhiều ổ cắm Ethernet, liên kết mỗi ổ cắm với một cổng chuyển mạch trong các VLAN khác nhau. Lưu lượng truy cập sau đó có thể định tuyến từ VLAN này sang VLAN khác thông qua bộ định tuyến.

**Bộ định tuyến trên thanh** Chỉ cần một giao diện Ethernet của bộ định tuyến và giao diện này được liên kết với bộ chuyển mạch dưới dạng kết nối trung kế. Mỗi VLAN được định nghĩa thông qua phần mềm như một giao diện con với lưu lượng truy cập được gắn thẻ tương ứng. Do đó, tất cả lưu lượng truy cập cho tất cả các VLAN được sắp xếp trong bộ định tuyến và có thể được gắn thẻ lại để di chuyển nó từ VLAN này sang VLAN khác.

**Giao diện ảo chuyển mạch (SVI)** Kỹ thuật này chạy trên switch Layer 3. Đây là phương pháp phổ biến nhất được sử dụng hiện nay và nó rất giống với phương pháp Router-on-a-Stick. Mỗi VLAN có một giao diện ảo trong switch và do đó lưu lượng truy cập có thể có các thẻ được hoán đổi trong thiết bị để di chuyển từ VLAN sang VLAN khác.

## 3. Sub interface

### 3.1 Mục đích

Giao tiếp với các VLAN

### 3.2 Khái niệm

Giao diện con là một giao diện ảo được tạo bằng cách chia một **[giao diện vật lý](https://www.omnisecu.com/cisco-certified-network-associate-ccna/different-types-of-interfaces-in-a-cisco-router.php" \t "_blank)** thành Nhiều giao diện logic. Giao diện phụ trong Bộ định tuyến Cisco sử dụng giao diện vật lý chính để gửi và nhận dữ liệu. (Nhiều card mạng được thiết kế trong router)

### 3.3 Vai trò

-Kết nối với nhiều mạng, kết nối với router khác để trao đổi thông tin.

## 4. Bảo mật trong mạng LAN

### 4.1 ARP spoofing

#### 4.1.1 Khái niệm

 ARP spoofing còn được gọi là ARP poisoning, là một cuộc tấn công Man in the Middle (MitM) cho phép những kẻ tấn công chặn giao tiếp giữa các thiết bị mạng.

#### 4.1.2 Cách tấn công

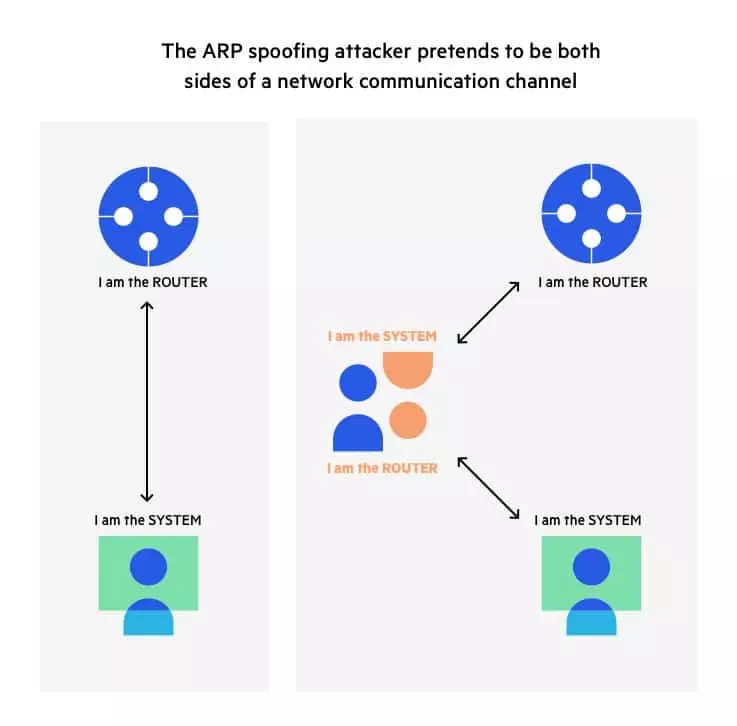
1. Kẻ tấn công phải có quyền truy cập vào mạng. Chúng quét mạng để xác định địa chỉ IP của ít nhất hai thiết bị⁠ — giả sử đây là một máy trạm và một bộ định tuyến.

2. Kẻ tấn công sử dụng một công cụ giả mạo, chẳng hạn như Arpspoof hoặc Driftnet, để gửi phản hồi ARP giả mạo.

3. Các phản hồi giả mạo thông báo rằng địa chỉ MAC chính xác cho cả hai địa chỉ IP, thuộc bộ định tuyến và máy trạm (workstation), là địa chỉ MAC của kẻ tấn công. Điều này đánh lừa cả bộ định tuyến và máy trạm kết nối với máy của kẻ tấn công, thay vì kết nối với nhau.

4. Hai thiết bị cập nhật các mục bộ nhớ cache ARP của chúng và từ thời điểm đó trở đi, giao tiếp với kẻ tấn công thay vì trực tiếp với nhau.

5. Kẻ tấn công hiện đang bí mật đứng giữa mọi liên lạc.



#### 4.1.3 Hậu quả

Tiếp tục định tuyến thông tin liên lạc như hiện tại, kẻ tấn công có thể đánh hơi (sniffing) các gói tin và đánh cắp dữ liệu, ngoại trừ trường hợp gói tin được truyền qua một kênh được mã hóa như HTTPS.

Thực hiện chiếm quyền điều khiển session⁠, nếu kẻ tấn công có được session ID, chúng có thể có quyền truy cập vào tài khoản mà người dùng hiện đang đăng nhập.

Thay đổi giao tiếp⁠ – ví dụ: đẩy một file hoặc trang web độc hại đến máy.

Tấn công DDoS – những kẻ tấn công có thể cung cấp địa chỉ MAC của server mà chúng muốn tấn công bằng DDoS, thay vì máy của chính chúng. Nếu làm điều này cho một số lượng lớn IP, server mục tiêu sẽ bị tấn công bởi lưu lượng truy cập.

#### 4.1.4 Cách phát hiện

Cách 1: Command line: arp -n

Ví dụ:

|  |  |
| --- | --- |
| IP Address | MAC Address |
| 192.168.5.1 | 00-14-22-01-23-45 |
| 192.168.5.201 | 40-d4-48-cr-55-b8 |
| 192.168.5.202 | 00-14-22-01-23-45 |

Nếu bảng chứa hai địa chỉ IP khác nhau có cùng địa chỉ MAC, chứng tỏ một cuộc tấn công ARP đang diễn ra. Vì địa chỉ IP 192.168.5.1 có thể được nhận dạng là bộ định tuyến nên IP của kẻ tấn công có thể là 192.168.5.202.

Cách 2: Sử dụng Wireshark để phát hiện và biết thêm thông tin về loại giao tiếp mà kẻ tấn công đang thực hiện.

#### 4.1.5 Cách phòng chống

Sử dụng **Mạng riêng ảo** (Virtual Private Network – [VPN](https://en.wikipedia.org/wiki/Virtual_private_network)) cho phép các thiết bị kết nối với Internet thông qua một tunnel được mã hóa. Điều này làm cho tất cả thông tin liên lạc được mã hóa và vô giá trị đối với kẻ tấn công ARP spoofing.

Sử dụng **ARP⁠ tĩnh** – giao thức ARP cho phép xác định mục nhập ARP tĩnh cho địa chỉ IP và ngăn thiết bị nghe phản hồi ARP cho địa chỉ đó. Ví dụ: nếu một máy tính luôn kết nối với cùng một bộ định tuyến, bạn có thể xác định một mục ARP tĩnh cho bộ định tuyến đó, điều này giúp ngăn chặn một cuộc tấn công.

Sử dụng **packet filtering**⁠ – các packet filtering⁠ có thể xác định các gói ARP bị nhiễm độc bằng cách phát hiện chúng chứa thông tin nguồn xung đột và ngăn chúng lại trước khi chúng đến được các thiết bị trên mạng của bạn.

Thực hiện một **cuộc tấn công ARP spoofing**⁠ – kiểm tra xem các hệ thống bảo mật hiện tại của bạn có đang hoạt động hay không bằng cách thực hiện một cuộc tấn công ARP spoofing với sự phối hợp của các nhóm Công nghệ thông tin và bảo mật. Nếu cuộc tấn công thành công, hãy xác định điểm yếu trong các biện pháp bảo mật của bạn và khắc phục chúng.

### 4.2 MAC spoofing

#### 4.2.1 Khái niệm

MAC spoofing là 1 kiểu tấn công được sử dụng để khai thác các lỗ hổng trong cơ chế xác thực được thực hiện bởi phần cứng mạng có dây hoặc không.

-Thường được coi là cuộc tấn công cũ và có thể được sử dụng để thực hiện nhiều payload.

-Được sử dụng để tạo 1 điểm truy cập trái phép hoặc nhiều điểm với cùng địa chỉ MAC như 1 điểm truy cập hợp pháp

-Còn được gọi là “Broadcast Spoofing”: kiểu tấn công này yêu cầu attacker phải nằm trong phạm vi vật lý của mạng mục tiêu hoặc có quyền truy cập vật lý vào nó, để loại tấn công này diễn ra.

VD: 1 loại của Broadcast Spoofing attack là 1 tấn công vét cạn, attacker thử liên tục cho đến khi có được quyền truy cập.

#### 4.2.2 Cách phòng chống

-Đảm bảo mạng không thể truy cập được thông qua các cổng không cần thiết nào (vô hiệu hóa các dịch vụ và các cổng không sử dụng) => ngăn chặn tấn công vét cạn.

-Cài tường lửa

-Sử dụng phương pháp xác thực mạnh hợn

-Cẩn thận sử dụng các công nghệ có Bluetooth (1 trong những công nghệ phổ biến nhất được sử dụng cho cá nhân và doanh nghiệp hiện nay, nhưng không cung cấp bảo vệ chống lại các lệnh MAC độc hoặc các cuộc tấn công giả mạo phát sóng)

### 4.3 DHCP spoofing

#### 4.3.1 Khái niệm

DHCP spoofing là kỹ thuật giả mạo DHCP Server trong mạng LAN. Kẻ tấn công có thể cài đặt một phần mềm DHCP trên máy tính của mình và cấp phát địa chỉ IP cho máy nạn nhân với các thông số giả mạo như default gateway, DNS. Từ đó, máy tính nạn nhân sẽ bị chuyển hướng truy cập theo ý đồ của kẻ tấn công.

#### 4.3.2 Cách tấn công

-Kịch bản:

**Bước 1**: Máy tính của kẻ tấn công sẽ vét cạn toàn bộ Pool IP của máy DHCP Server bằng cách liên tục gửi các yêu cầu xin cấp phát IP (DHCP Discover) tới máy DHCP Server. Mỗi yêu cầu DHCP Discover này đều chứa địa chỉ MAC giả mạo nhằm đánh lừa DHCP Server rằng đó là lời yêu cầu từ các máy tính khác nhau. Vì Pool IP cấp phát trên DHCP Server là hữu hạn nên sau khi đã cấp phát hết IP, DHCP Server không thể phục vụ các yêu cầu xin IP từ máy Client.

**Bước 2:** Kẻ tấn công cài đặt phần mềm DHCP Server trên máy của mình và cấp phát thông số IP giả mạo, điều hướng truy cập nạn nhân đến các Server do hắn kiểm soát nhằm đánh lừa và đánh cắp thông tin.

**-**Tấn công:

+Client gửi yêu cầu DHCP đến DHCP Server để nhận cấu hình IP

+DHCP Spoofing – cấu hình sai địa chỉ IP của Client

+DHCP Spoofing – Tất cả dữ liệu sẽ đi qua PC của hacker đến đích

#### 4.3.3 Cách phòng chống

-Xây dựng 1 bảng chứa thông tin liên quan giữa: địa chỉ MAC client – địa chỉ IP – số hiệu cổng -VLAN. Bảng này dùng để giám sát việc xin cấp phát địa chỉ IP của các máy client, tránh việc 1 máy client xin cấp phát nhiều địa chỉ IP.

-Quy định số lượng gói tin DHCP đến 1 cổng/đơn vị thời gian.

-Cấu hình các cổng trên switch thành 2 kiểu: trust và untrust

+Cổng trust là cổng có thể cho phép gửi đi tất cả các bản tin DHCP, là cổng nối với máy chủ DHCP.

+Cổng untrust là cổng chỉ có thể gửi đi bản tin xin cấp phát địa chỉ IP, thường là cổng nối với các thiết bị đầu cuối người dùng. Do vậy máy tính của attacker mặc dù là máy chủ DHCP, nhưng không thể gửi các bản tin DHCP cấp phát địa chỉ IP giả mạo.

## 5. Layer 3 Router

Router tầng 3, còn được gọi là router tầng mạng, là một thành phần cơ bản trong các mạng máy tính hiện đại. Chúng hoạt động tại tầng mạng (Tầng 3) của mô hình OSI (Open Systems Interconnection) và chịu trách nhiệm chuyển tiếp các gói dữ liệu giữa các mạng khác nhau. Dưới đây là một số thông tin cơ bản về router tầng 3:

**Chức năng**: Chức năng chính của router tầng 3 là định tuyến các gói dữ liệu qua nhiều mạng, cho phép giao tiếp giữa các thiết bị thuộc các mạng con hoặc mạng khác nhau. Chúng đưa ra quyết định về đường đi tốt nhất để dữ liệu đến điểm đích dựa trên địa chỉ IP và các giao thức định tuyến.

**Địa chỉ IP**: Router tầng 3 làm việc với địa chỉ IP (Internet Protocol) để định tuyến các gói dữ liệu. Chúng kiểm tra địa chỉ IP đích của các gói tin đến và sử dụng bảng định tuyến để xác định giao diện hoặc địa chỉ tiếp theo thích hợp để đến mạng đích.

**Bảng định tuyến**: Bảng định tuyến là một cấu trúc dữ liệu quan trọng được router sử dụng để lưu trữ thông tin về các mạng hiện có và các địa chỉ tiếp theo liên quan. Bảng định tuyến được xây dựng bằng tay bởi quản trị mạng hoặc tự động thông qua các giao thức định tuyến như OSPF (Open Shortest Path First), RIP (Routing Information Protocol), BGP (Border Gateway Protocol), v.v.

**Liên kết**: Router tầng 3 hoạt động như cổng kết nối giữa các mạng khác nhau, kết nối các mạng LAN (Local Area Networks) hoặc VLAN (Virtual Local Area Networks) trong một mạng doanh nghiệp lớn hoặc kết nối các mạng riêng biệt trên internet.

**Chuyển tiếp gói tin**: Khi router tầng 3 nhận được một gói dữ liệu, nó kiểm tra địa chỉ IP đích của gói tin đến, tìm kiếm trong bảng định tuyến để tìm kết hợp tốt nhất và chuyển tiếp gói tin đến giao diện hoặc địa chỉ tiếp theo phù hợp.

**NAT (Network Address Translation)**: Router tầng 3 thường thực hiện chức năng Network Address Translation, cho phép chuyển đổi địa chỉ IP riêng tư trong mạng cục bộ thành một địa chỉ IP công cộng duy nhất khi giao tiếp với các thiết bị ngoài mạng cục bộ. Điều này giúp tiết kiệm không gian địa chỉ IP công cộng và tăng cường tính bảo mật bằng cách ẩn các địa chỉ IP nội bộ.

**Bảo mật**: Router đóng vai trò trong bảo mật mạng bằng cách triển khai các tính năng như danh sách điều khiển truy cập (ACL), có thể lọc và kiểm soát luồng dữ liệu dựa trên các tiêu chí cụ thể như địa chỉ IP nguồn/đích hoặc các giao thức.

**QoS (Quality of Service)**: Router tầng 3 có thể hỗ trợ các tính năng Quality of Service, cho phép quản trị mạng ưu tiên một số loại dữ liệu (ví dụ: giọng nói hoặc video) hơn các loại khác, đảm bảo hiệu suất mạng hiệu quả và đáng tin cậy hơn.

**Định tuyến ảo**: Một số router hỗ trợ các phiên bản định tuyến ảo, cho phép chúng hoạt động như nhiều router độc lập chạy song song trên cùng một thiết bị vật lý. Tính năng này thường được sử dụng trong các mạng nhà cung cấp dịch vụ và môi trường doanh nghiệp quy mô lớn.

## 6. Định tuyến

### 6.1 Khái niệm

Định tuyến là chức năng của router giúp xác định quá trình tìm đường đi cho các gói tin từ nguồn tới đích thông qua hệ thống mạng.

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 định tuyến, mỗi mạng mà router có thể chuyển đi (mạng đích) thể hiện bằng một dòng. Mỗi mạng này có được có thể do chúng đang kết nối trực tiếp với router đang xét hay router học được thông qua việc cấu hình định tuyến.

### 6.2 Phân loại:

#### 6.2.1 Định tuyến tĩnh

Định tuyến tĩnh là loại định tuyến mà trong đó router sử dụng các tuyến đường đi tĩnh để vận chuyển dữ liệu đi. Các tuyến đường đi tĩnh này có được do người quản trị cấu hình thủ công vào các router.

Cấu hình: R(config)#ip route <destination-net> <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 -OutPort: cổng của router mà packet sẽ đi ra

**Default route** nằm ở cuối bảng định tuyến và được sử dụng để gửi các gói tin đi trong trường hợp mạng đích không tìm thấy trong bảng định tuyến. Nó rất hữu dụng trong các mạng dạng “stub network” như kết nối từ mạng nội bộ ra ngoài Internet.

#### 6.2.2 Định tuyến động

Định tuyến động là loại định tuyến mà trong đó router sử dụng các tuyến đường đi động để vận chuyển dữ liệu đi. Các tuyến đường đi động này có được 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 định tuyến động phổ biến: RIP, OSPF, BGP,…

Giao thức định tuyến động chia làm hai loại là **distance-vector** và **link-state**

##### 6.2.2.1 Distance-vector

Giao thức định tuyến thuộc loại này như RIP

Các router định tuyến theo Distance vector thực hiện gửi định kỳ toàn bộ bảng định tuyến của mình và chỉ gửi cho các router láng giềng kết nối trực tiếp với mình.

Các router định tuyến theo Distance vector không biết được đường đi đến đích một cách cụ thể, không biết về các router trung gian trên đường đi và cấu trúc kết nối giữa chúng.

##### 6.2.2.2 Link-state

Trong các giao thức định tuyến link-state, các router sẽ trao đổi các LSA (link state advertisement) với nhau để xây dựng và duy trì cơ sở dữ liệu về trạng thái các đường liên kết hay còn gọi là cơ sở dữ liệu về cấu trúc mạng (topology database). Các thông tin trao đổi được gửi dưới dạng multicast

=> mỗi router sẽ dùng thuật toán SPF để tính toán chọn đường đi tốt nhất đến từng mạng đích.

Khi các router định tuyến theo link-state đã hội tụ xong, nó không thực hiện cập nhật định tuyến định kỳ mà chỉ cập nhật khi nào có sự thay đổi xảy ra

=> thời gian hội tụ nhanh và ít tốn băng thông.

Giao thức định tuyến theo link-state có hỗ trợ CIDR, VLSM nên chúng là một chọn lựa tốt cho các mạng lớn và phức tạp. Nhưng đồng thời nó đòi hỏi dung lượng bộ nhớ lớn và khả năng xử lý mạnh của CPU của router.

Để đảm bảo là các database luôn cập nhật thông tin mới, trong các LSA này được đánh thêm chỉ số sequence. Chỉ số sequence được bắt đầu từ giá trị initial đến giá trị Maxage.

+Khi một router nào đó tạo ra một LSA, nó sẽ đặt giá trị sequence bằng initial. Mỗi khi router gửi ra một phiên bản LSA update khác, nó sẽ tăng giá trị đó lên 1 => giá trị sequence càng cao thì LSA update càng mới.

+Nếu giá trị sequence này đạt đến max-age, router sẽ flood LSA ra cho tất cả các router còn lại, sau đó router đó sẽ set giá trị sequence về initial.

##### 6.2.2.3 Classfull routing protocol

Các giao thức định tuyến nhóm classfull không quảng bá subnet-mask cùng với địa chỉ đích trong các gói tin cập nhật định tuyến (routing update). Do đó, khi router nhận được các update này, router phải lấy giá trị network-mask mặc định có cùng với địa chỉ lớp mạng của địa chỉ đích.

Nếu địa chỉ đích được kết nối trực tiếp với router, network-mask được lấy cùng với mask được cấu hình trên interface kết nối đến mạng đó. Nếu địa chỉ đích không nối trực tiếp (disconnected), router sẽ lấy địa chỉ subnetmask default của địa chỉ đích.

##### 6.2.2.4 Classless routing protocol

Các giao thức định tuyến thuộc nhóm classless sẽ quảng bá subnet –mask cùng với địa chỉ đích trong các gói tin cập nhật định tuyến.

Hai tham số quan trọng trong định tuyến: Metric và AD

-Metric:

+Là tham số được sử dụng để chọn đường tốt nhất cho việc định tuyến. Đây là giá trị mà bất kỳ giao thức định tuyến nào cũng phải dùng để tính toán đường đi đến mạng đích.

+Trong trường hợp có nhiều đường đi đến một mạng đích thì đường đi nào có metric thấp nhất sẽ được lựa chọn để đưa vào bảng định tuyến. Mỗi giao thức định tuyến có một kiểu metric khác nhau.

-AD (administrative distance)

+AD là giá trị quy ước dùng để chỉ độ tin cậy của các giao thức định tuyến, giao thức nào có AD nhỏ hơn sẽ được xem là đáng tin cậy hơn.

+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.

## 7. Các giao thức định tuyến

### 7.1 RIP(Routing Information Protocol)

#### 7.1.1 Khái niệm

RIP là một giao thức định tuyến theo kiểu distance-vector. Hop count được sử dụng làm metric cho việc chọn đường. Nếu có nhiều đường đến cùng một đích thì RIP sẽ chọn đường nào có số hop-count (số router) ít nhất.

Nếu hop-count lớn hơn 15 thì packet bị loại bỏ. Mặc định thời gian update là 30 giây. Administrative Distance là 120.

#### 7.1.2 Phân loại

RIP có hai phiên bản là RIPv1 và RIPv2

|  |  |  |
| --- | --- | --- |
| Đặc điểm | RIPv1 | RIPv2 |
| Loại định tuyến | Classfull; distance-vector | Classless |
| Hỗ trợ VLSM và mạng không liên tục | Không | Có |
| Gửi kèm Subnet-mask trong bản tin cập nhật định tuyến | Không | Có |
| Quảng bá thông tin định tuyến | Broadcast | Multicast |
| Hỗ trợ tóm tắt các tuyến thủ công | Không | Có |
| Hỗ trợ chứng thực | Không | Có |
| Định nghĩa trong RFC | RFC 1058 | RFC 1721, 1722, 2453 |

**RIPv1:**

Metric của RIP là hop-count. Cập nhật định tuyến theo chu kỳ mặc định là 30 giây. Hop-count tối đa để chuyển gói là 15.

**RIPv2:**

-RIPv2 cập nhật định tuyến dạng multicast, sử dụng địa chỉ lớp D 224.0.0.9

-RIPv2 sử dụng metric là hop-count

-Chứng thực:

Chứng thực trong định tuyến là cách thức bảo mật trong việc trao đổi thông tin định tuyến giữa các router. Nếu có cấu hình chứng thực thì các router phải vượt qua quá trình này trước khi các thông tin trao đổi định tuyến được thực hiện. RIPv2 hỗ trợ hai kiểu chứng thực là: “Plain text” và “MD5”

+Chứng thực dạng “Plain Text”: còn gọi là “Clear text”

Quá trình chứng thực chỉ đơn giản là các router được cấu hình một khóa (password) và trao đổi chúng để so khớp. Các khóa này được gửi dước dạng không mã hóa trên đường truyền

+Chứng thực dạng MD5

Dạng chứng thực này sẽ gửi thông tin về khóa đã được mã hóa giúp các thông tin trao đổi được an toàn hơn. Các bước cấu hình tương tự như dạng “Plain Text”, chỉ có khác ở bước 3 phải thêm 1 lệnh sau:

Router(config-if)#ip rip authentication mode md5

### 7.2 OSPF

#### 7.2.1 Khái niệm

OSPF (Open Shortest Path First) là một giao thức định tuyến dạng link-state, sử dụng thuật toán Dijkstra “ Shortest Path First (SPF)” để xây dựng bảng định tuyến

OSPF mang những đặc điểm của giao thức link-state. Nó có ưu điểm là hội tụ nhanh, hỗ trợ được mạng có kích thước lớn và không xảy ra routing loop.

Là giao thức định tuyến dạng classless nên hỗ trợ VLSM và mạng không liên tục (discontigous network).

OSPF sử dụng địa chỉ multicast 224.0.0.5 và 224.0.0.6 (DR và BDR router) để gửi các thông điệp hello và update.

Sử dụng area để giảm yêu cầu về CPU, memory của OSPF router cũng như lưu lượng định tuyến.

OSPF còn có khả năng hỗ trợ chứng thực dạng plaintext và dạng MD5.

7.2.2 Metric của OSPF

OSPF sử dụng metric là cost. Cost của toàn tuyến được tính theo cách cộng dồn cost dọc theo tuyến đường đi của packet. Cách tính cost được IETF đưa ra trong RFC 2328.

Cost được tính dựa trên băng thông sao cho tốc độ kết nối của đường link càng cao thì cost càng thấp dựa trên công thức 108 /bandwidth với giá trị bandwidth được cấu hình trên mỗi interface và đơn vị tính là bps.

Tuy nhiên, chúng ta có thể thay đổi giá trị cost. Nếu router có nhiều đường đến đích mà cost bằng nhau thì router sẽ cân bằng tải trên các đường đó (tối đa là 16 đường). Những tham số bắt buộc phải giống nhau trong các router chạy OSPF trong một hệ thống mạng đó là Hello/dead interval, Area – ID, authentication password (nếu có), stub area flag.

#### 7.2.2 Các loại môi trường OSPF

Multiple access (ethernet)

Point-to-point

NBMA (Non-Broadcast Multiple Access)

### 7.3 EIGRP

**Enhanced Interior Gateway Routing Protocol (EIGRP)** là giao thức định tuyến do Cisco tạo ra, chỉ hoạt động trên các thiết bị của Cisco. EIGRP là một giao thức định tuyến lai, nó vừa mang những đặc điểm của “distance vector” vừa mang một số đặc điểm của ”link-state”. EIGRP là dạng định tuyến “classless”.

EIGRP hỗ trợ VLSM và CIDR nên sử dụng hiệu quả không gian địa chỉ, sử dụng địa chỉ multicast (224.0.0.10) để trao đổi thông tin cập nhật định tuyến

Những xử lý cơ bản của EIGRP trong việc học các mạng đích:

● Các router phát hiện các láng giềng của nó, danh sách các láng giềng được lưu giữ trong “neighbor table”.

● Mỗi router sẽ trao đổi các thông tin về cấu trúc mạng với các láng giềng của nó.

● Router đặt những thông tin về cấu trúc hệ thống mạng học được vào cơ sở dữ liệu về cấu trúc mạng (topology table).

● Router chạy thuật toán DUAL với cơ sở dữ liệu đã thu thập được ở bước trên để tính toán tìm ra đường đi tốt nhật đến mỗi một mạng trong cơ sở dữ liệu.

● Router đặt các đường đi tốt nhất đến mỗi mạng đích vào bảng định tuyến.

● Trong EIGRP có hai tuyến ta cần quan tâm là “successor route” và “fessible successor route”.

✓ Successor route: là tuyến đường đi chính được sử dụng để chuyển dữ liệu đến đích, được lưu trong bảng định tuyến. EIGRP cho phép chia tải tối đa trên 16 đường (mặc định là 4 đường) đến mỗi mạng đích.

✓ Fessible successor route: là đường đi dự phòng cho đường đi chính và được lưu trong bảng cấu trúc mạng (topology table)

### 7.4 So sánh

|  |  |  |  |
| --- | --- | --- | --- |
| Nội dung | RIP | EIGRP | OSPF |
| Loại giao thức định tuyến | Distance-vector | Distance-vector; Link-state | Link-state |
| Tốc độ hội tụ | Tương đối chậm  -RIPv1: cập nhật chỉ diễn ra sau mỗi 30s  -RIPv2: mỗi 30s cho các cập nhật thường xuyên; 90s cho các cập nhật kích hoạt | Nhanh chóng thích ứng với các thay đổi trong cấu trúc mạng | Nhanh, cho phép cấc router có cái nhìn chi tiết và cập nhật mạng thường xuyên |
| Khả năng mở rộng | Phù hợp cho các mạng nhỏ, trung bình | Xử lý các mạng lớn 1 cách hiêu quả | Xử lý các mạng lớn , phức tạp hơn và khả năng mở rộng cao. |
| Ngăn chặn vòng lặp | Sử dụng split,route poisoning và bộ đếm giữ nút để ngăn chặn các vòng lặp định tuyến, không hiệu quả trong mạng lớn | Sử dụng thuật toán DUAL, cung cấp các đường đi không lặp lại, hội tụ nhanh chóng. | Sử dụng thuật toán Dijkstra để tính toán các đường đi ngắn nhất, đảm bảo định tuyến không lặp lại. |
| Hỗ trợ VLSM | Không  =>Cấp phát địa chỉ ko hiểu quả | Có | Có |

## 8. VSS(Vitual Switching System)

### 8.1 Khái niệm

Một Hệ thống Chuyển mạch Ảo (VSS) là một công nghệ mạng được sử dụng chủ yếu trong các thiết bị Cisco để tạo một chuyển mạch logic duy nhất bằng cách kết hợp hai chuyển mạch vật lý. Thông thường, nó được triển khai trong các kịch bản có tính sẵn sàng cao để nâng cao tính khả dụng của mạng, đơn giản hóa quản lý và tăng cường khả năng mở rộng.

Công nghệ VSS cho phép hai chuyển mạch Cisco Catalyst hoạt động như một chuyển mạch ảo duy nhất, cung cấp một mặt bằng kiểm soát và mặt bằng dữ liệu thống nhất. Từ góc nhìn của các thiết bị mạng bên ngoài cặp VSS, toàn bộ chuyển mạch ảo xuất hiện như một thiết bị duy nhất với một địa chỉ IP và địa chỉ MAC duy nhất. Sự kết hợp này giảm bớt sự phức tạp trong mạng, cải thiện hiệu suất mạng và đơn giản hóa thiết kế mạng.

### 8.2 Mục đích

1. Sẵn sàng cao: VSS cung cấp tính dự phòng và khả năng chịu lỗi, đảm bảo thời gian không hoạt động của mạng được giảm thiểu. Nếu một chuyển mạch trong cặp VSS gặp sự cố, chuyển mạch còn lại tiếp tục hoạt động một cách liền mạch, mà không cần các giao thức bên ngoài như Spanning Tree Protocol (STP) để hồi phục lại.

2. Phân chia tải: VSS cho phép phân phối tải trên hai chuyển mạch vật lý, phân chia lưu lượng mạng một cách đồng đều giữa chúng. Tính năng này đảm bảo sử dụng tối ưu các tài nguyên và tăng khả năng sẵn có của băng thông.

3. Quản lý đơn giản: Quản lý VSS dễ dàng hơn quản lý hai chuyển mạch riêng biệt vì tất cả các cấu hình, chính sách và giám sát được thực hiện trên chuyển mạch ảo thay vì xử lý từng chuyển mạch một cách riêng lẻ.

4. Khả năng mở rộng: Bằng cách kết hợp hai chuyển mạch thành một VSS, bạn có thể tăng mật độ cổng và tổng dung lượng của mạng mà không tăng thêm sự phức tạp.

5. Địa chỉ IP duy nhất: Cặp VSS trình bày chính nó cho mạng như một chuyển mạch duy nhất với một địa chỉ IP duy nhất, đơn giản hóa việc định địa chỉ và định tuyến trong mạng.

6. Chuyển đổi nhanh có trạng thái (SSO): VSS cung cấp chuyển đổi nhanh giữa chuyển mạch hoạt động và chuyển mạch dự phòng, giảm thiểu sự gián đoạn mạng trong các sự kiện chuyển đổi khẩn cấp.

Lưu ý quan trọng là VSS là một công nghệ độc quyền của Cisco và chỉ áp dụng cho một số chuyển mạch Cisco cụ thể, chẳng hạn như dòng Cisco Catalyst 6500. Các nhà cung cấp khác có thể cung cấp các chức năng tương tự dưới tên gọi khác hoặc sử dụng các tiêu chuẩn mở như Virtual Router Redundancy Protocol (VRRP) hoặc Shortest Path Bridging (SPB). Nếu bạn đang xem xét triển khai VSS hoặc các công nghệ tương tự trong mạng của mình, hãy đảm bảo kiểm tra tính tương thích và yêu cầu của các thiết bị mạng của bạn và tìm hiểu tài liệu hướng dẫn hoặc hỗ trợ từ nhà cung cấp phù hợp.

## 9. vPC (virtual port channel)

### 9.1 Khái niệm

vPC (Virtual Port-Channel), còn được gọi là multichassis EtherChannel (MEC) là một tính năng trên các thiết bị chuyển mạch Cisco Nexus cung cấp khả năng định cấu hình Port-Channel trên nhiều thiết bị chuyển mạch (tức là các đồng nghiệp vPC).

vPC tương tự như Hệ thống chuyển mạch ảo (VSS) trên Catalyst 6500s. Tuy nhiên, sự khác biệt chính giữa vPC và VSS là VSS tạo ra một switch logic duy nhất. Điều này dẫn đến một mặt phẳng điều khiển duy nhất cho cả mục đích quản lý và cấu hình. Trong khi với vPC, mỗi switch được quản lý và cấu hình độc lập.

Điều quan trọng cần nhớ là với vPC, cả hai thiết bị chuyển mạch đều được quản lý độc lập. Điều này có nghĩa là bạn sẽ cần tạo và cho phép các VLAN của mình trên cả hai thiết bị chuyển mạch Nexus

Virtual Port Channel (vPC) là một công nghệ mạng của Cisco được sử dụng để kết hợp hai switch vật lý thành một chuyển mạch logic duy nhất, cung cấp tính sẵn sàng cao, khả năng chịu lỗi và hiệu suất tối ưu cho mạng.

Với vPC, hai switch hoạt động như một cặp đồng thời, tạo thành một môi trường mạng ảo và liên kết các cổng vật lý của chúng thành một Port Channel (được gọi là vPC Peer Link). Các thiết bị ngoài mạng thấy cặp switch này như một chuyển mạch duy nhất, với một địa chỉ MAC duy nhất và một địa chỉ IP duy nhất. Việc kết hợp các cổng vật lý thành một Port Channel giúp cải thiện hiệu suất mạng và cân bằng tải lưu lượng.

### 9.2 Đặc điểm

Một số điểm chính về vPC bao gồm:

Tính sẵn sàng cao và khả năng chịu lỗi: Với vPC, nếu một trong hai switch trong cặp gặp sự cố, các thiết bị ngoài mạng vẫn có thể kết nối đến mạng thông qua switch hoạt động khác. Điều này giảm thiểu thời gian chết và đảm bảo tính sẵn sàng cao cho mạng.

Phân chia tải: Khi được kết nối đến vPC, các thiết bị ngoài mạng có thể truy cập cả hai switch trong cặp, cho phép phân chia tải trên hai switch và cân bằng lưu lượng mạng.

Eliminate Spanning Tree Protocol (STP): Với vPC, không cần sử dụng STP truyền thống để tránh vòng lặp trong mạng. Thay vào đó, vPC sử dụng vPC Peer Link để tránh vòng lặp và cung cấp tính sẵn sàng cao hơn.

Easy Management (Quản lý dễ dàng): VPC được quản lý như một thực thể duy nhất, giúp giảm bớt công việc quản lý và giữ cho cấu hình của hai switch đồng bộ hóa với nhau.

## 10. Policy based routing

### 10.1 Khái niệm

PBR là quá trình sử dụng bản đồ tuyến đường (route map) để chỉ định một thuộc tính khác với điểm đến và sau đó xác định đường dẫn ra khỏi Router dựa trên các điều kiện đó.  
 Với PBR, quản trị viên mạng có thể chọn các chính sách theo các thông số cụ thể, chẳng hạn như:

+Địa chỉ IP của nguồn hoặc đích

+Cổng của nguồn hoặc đích

+Loại traffic

+Giao thức mạng

+Kích thước của gói dữ liệu

+Một ACL

Khi các tham số như thế này được thiết lập, các gói dữ liệu sẽ được định tuyến tương ứng. Điều này cho phép bạn tăng cường độ linh hoạt của mạng.  
 Bởi vì bạn có thể xác định chiến lược định tuyến của mình bằng cách sử dụng các thuộc tính của ứng dụng, bạn có thể thực thi các chính sách quản lý lưu lượng cụ thể để kiểm soát cách các gói được chuyển tiếp.  
 Bằng cách này, bạn có thể tối ưu hóa cách băng thông được sử dụng bởi các ứng dụng quan trọng.

### 10.2 Cách hoạt động

PBR được coi là một ngoại lệ đối với cơ sở thông tin định tuyến (RIB) và được xem xét trước khi kiểm tra RIB. Điều này cho phép nhiều tùy chọn định tuyến hơn.  
 Ví dụ: trong route map được sử dụng cho PBR, bạn có thể đối sánh trên danh sách kiểm soát truy cập (ACL) sau đó đối sánh trên nguồn, đích, loại giao thức và/hoặc số cổng.  
 Bạn cũng có thể kết hợp trên:  
 Đánh giá chất lượng dịch vụ (QoS), chẳng hạn như mức độ ưu tiên của Giao thức Internet (IP) hoặc dịch vụ khác biệt (DSCP). Kích thước của các gói, cho phép bạn gửi dữ liệu đến nơi bạn muốn một cách hiệu quả dựa trên mức độ lớn hay nhỏ của các gói.  
 Khi bạn có kết quả phù hợp, bạn có thể đặt địa chỉ và/hoặc cổng đầu ra của thiết bị kế tiếp. Bạn cũng có thể đặt các giá trị QoS cùng lúc, điều này cho phép bạn đảm bảo ứng dụng nhận được tài nguyên cần thiết để hoạt động tốt như bạn cần.  
 Route map có thể có nhiều statements, các statements này thường được sắp xếp theo số gia là 10. Điều này cho phép bạn kiểm soát để so khớp trên nhiều tập hợp các điều kiện so khớp.  
 Route map cũng có thể có câu lệnh “deny”. (Mặc định, nếu không được chỉ định, là “permit”.) Chúng cũng có thể được sử dụng để hoạt động như một bộ lọc. Khi Route map khớp với một ACL, nếu nó khớp với lệnh deny, nó sẽ thoát ra khỏi câu lệnh đó của Route map và tiếp tục đến câu lệnh tiếp theo trong map. Việc deny hoặc drop được xác định bởi Route map, không phải ACL được tham chiếu bởi Route map.  
 Nếu không có kết quả phù hợp nào trong route map hoặc bạn thêm vào một route map mà không có sự cho phép, thì nó được chỉ định là “chính sách bị từ chối”. Nếu bạn bị từ chối chính sách, thì lưu lượng được chuyển tiếp bình thường dựa trên RIB.  
 Khi bạn sử dụng lệnh show ip route hoặc sh ipv6 route, bạn sẽ không thấy rằng PBR đang được sử dụng. Bạn có thể sử dụng lệnh show ip policy hoặc show ipv6 policy. Điều này sẽ cho bạn thấy rằng có một chính sách được xác định cho PBR, nhưng không phải là chính sách liên minh. Để xem nó được áp dụng cho một cổng, hãy sử dụng show ip int. Tất nhiên, nếu bạn có quyền truy cập, bạn có thể chỉ cần xem cấu hình.

### 10.3 Mục đích

Mục đích chính của Virtual Port Channel (vPC) là cung cấp tính sẵn sàng cao, khả năng chịu lỗi và hiệu suất tối ưu cho mạng thông qua việc kết hợp hai switch vật lý thành một chuyển mạch logic duy nhất.

## 11. ACL

### 11.1 Khái niệm

ACL là một danh sách các điều kiện được áp đặt vào các cổng của router để lọc các gói tin đi qua nó. Danh sách này chỉ ra cho router biết loại dữ liệu nào được cho phép (allow) và loại dữ liệu nào bị hủy bỏ (deny). Sự cho phép và huỷ bỏ này có thể được kiểm tra dựa vào địa chỉ nguồn, địa chỉ đích, giao thức hoặc chỉ số cổng

### 11.2 Mục đích

Sử dụng ACL để quản lý các lưu lượng mạng, hỗ trợ ở mức độ cơ bản về bảo mật cho các truy cập mạng, thể hiện ở tính năng lọc các gói tin qua router.

### 11.3 Phân loại

#### 11.3.1 Standard ACL

Sử dụng “Standard CL” 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.

“Standard CL” kiểm tra điều kiện dựa vào địa chỉ nguồn trong các gói tin và thực hiện hành động cấm hoặc cho phép tất cả các lưu lượng từ một thiết bị hay một mạng xác định nào đó

Dùng “Standard ACL” để điều khiển telnet:

+Trên router có các “virtual terminal port” được dùng để cấu hình cho mục đích cho phép telnet vào router. Telnet cũng là một cách thức cho phép người quản trị cấu hình hay theo dõi thiết bị từ xa. Ta có thể lọc các địa chỉ truy xuất vào các cổng này bằng “Standard ACL”.

#### 11.3.2 Extended ACL

“Extended ACL” cung cấp sự điều khiển linh hoạt hơn “Standard ACL”. Nó kiểm tra cả địa chỉ nguồn, địa chỉ đích, giao thức, chỉ số cổng ứng dụng. “Extended ACL” thực hiện hành động cấm hay cho phép ở một số ứng dụng xác định.

### 11.4 Named ACL

“Extended ACL” cung cấp sự điều khiển linh hoạt hơn “Standard ACL”. Nó kiểm tra cả địa chỉ nguồn, địa chỉ đích, giao thức, chỉ số cổng ứng dụng. “Extended ACL” thực hiện hành động cấm hay cho phép ở một số ứng dụng xác định.

Named-ACL không tương thích với các Cisco IOS phiên bản trước 11.2 và không thể sử dụng cùng một tên cho nhiều ACL. ACL của các loại giao thức khác nhau không thể có cùng một tên

## 12. HSRP

### 12.1 Khái niệm

HSRP là một giao thức mạng được sử dụng để tạo khả năng dự phòng và độ tin cậy trong việc sử dụng các bộ định tuyến trong mạng máy tính. Giao thức này cho phép nhiều bộ định tuyến trong mạng con hoạt động cùng nhau và tạo thành một nhóm. Giao thức này sẽ hoạt động theo phương thức Active – Standby. Nếu bộ định tuyến chính bị lỗi, bộ định tuyến dự phòng sẽ tự động đảm nhận vai trò của bộ định tuyến chính mà không cần can thiệp thủ công.. Cụm từ viết tắt của HSRP là **Hot Standby Router Protocol**

### 12.2 Chức năng

-Tính khả dụng:

HSRP được sử dụng để tăng tính khả dụng của mạng bằng cách cung cấp giải pháp chuyển đổi dự phòng tự động và nhanh chóng. Nếu bộ định tuyến chính bị lỗi, bộ định tuyến dự phòng có thể ngay lập tức tiếp quản và duy trì kết nối mạng.

-Khắc phục tính dư thừa:

HSRP được sử dụng để tăng tính khả dụng của mạng bằng cách cung cấp giải pháp chuyển đổi dự phòng tự động và nhanh chóng . Nếu bộ định tuyến chính bị lỗi, bộ định tuyến dự phòng có thể ngay lập tức tiếp quản và duy trì kết nối mạng.

-Cân bằng tải:

HSRP cho phép chia sẻ tải lưu lượng giữa bộ định tuyến chính và bộ định tuyến dự phòng. Nó giúp tối ưu hóa việc sử dụng tài nguyên mạng và cải thiện hiệu suất mạng.

-Gateway an toàn:

HSRP cho phép các thiết bị trong mạng giao tiếp với các mạng bên ngoài bằng cùng một gateway mặc định, ngay cả khi bộ định tuyến chính thay đổi.

### 12.3 Ưu nhược

**Ưu điểm**

Tính khả dụng cao, tính dự phòng, khả năng cân bằng tải, cấu hình đơn giản và khả năng tương thích với hầu hết các thiết bị mạng.

**Nhược điểm**

Cần có thời gian hội tụ khi xảy ra thay đổi trạng thái mạng giữa router active và router standby.

HSRP hoạt động ở lớp 2 trong mô hình tham chiếu OSI. Do đó, để triển khai HSRP hiệu quả, tất cả các bộ định tuyến trong một nhóm phải được kết nối với cùng một phân đoạn mạng ở lớp 2.

## 13. VRRP

### 13.1 Khái niệm

Virtual Router Redundancy Protocol (VRRP) là một giao thức quản lý mạng được sử dụng để tăng sự sẵn có của host phục vụ gateway mặc định trên cùng một subnet. VRRP cải thiện độ tin cậy và hiệu suất của các mạng máy chủ bằng cách cho phép một router ảo để hoạt động như các cổng mặc định cho mạng đó.

Dưới đây là một số thông tin cơ bản về VRRP:

**Mục tiêu**: Mục tiêu chính của VRRP là cung cấp khả năng chuyển đổi tự động giữa các router để đảm bảo tính khả dụng và độ tin cậy cao cho mạng.

Virtual IP (VIP): Trong một nhóm VRRP, có một địa chỉ IP ảo được gọi là Virtual IP (VIP) hoặc Virtual Router IP. Các thiết bị trong mạng gửi dữ liệu đến VIP thay vì đến các địa chỉ IP cụ thể của các router.

Router Chính (Master):Là thiết bị trong nhóm VRRP được chọn làm router chính, có trách nhiệm xử lý dữ liệu được gửi đến VIP. Nếu router chính gặp sự cố, một router backup sẽ tiếp tục xử lý dữ liệu.

Router Backup: Là các thiết bị trong nhóm VRRP ở chế độ chờ, sẵn sàng thay thế router chính nếu cần. Router backup liên tục kiểm tra tình trạng của router chính để biết khi nào cần tiến hành chuyển đổi.

Priority: Mỗi router trong nhóm VRRP có một giá trị ưu tiên (priority). Router có ưu tiên cao hơn sẽ trở thành router chính. Nếu có nhiều router có cùng ưu tiên, router có địa chỉ IP cao hơn sẽ trở thành router chính.

Advertisement Interval: Là khoảng thời gian mà router chính gửi các thông báo VRRP cho các router backup để thông báo về tình trạng của mình. Khi router backup không nhận được thông báo trong khoảng thời gian này, nó có thể giả định rằng router chính đã gặp sự cố.

Preemption: Chức năng cho phép router có ưu tiên cao hơn có thể đẩy router chính hiện tại ra khỏi vị trí và tiếp tục trở thành router chính khi nó trở lại sau một sự cố.

Authentication: VRRP cung cấp khả năng xác thực giữa các router trong nhóm bằng cách sử dụng mật khẩu chia sẻ.

## 14. GLBP

### 14.1 Khái niệm

Gateway Load Balancing Protocol (GLBP) là một giao thức mạng cung cấp tính sẵn sàng cao và cân bằng tải trong môi trường mạng. Giống như VRRP, GLBP cũng cho phép nhiều router hoạt động như một định tuyến ảo duy nhất, nhưng GLBP cung cấp tính năng cân bằng tải giữa các router chính trong mạng.

Dưới đây là một số thông tin cơ bản về GLBP:

**Mục tiêu**: GLBP được thiết kế để cung cấp khả năng cân bằng tải đồng đều cho các router trong mạng, đồng thời cũng giữ tính sẵn sàng và độ tin cậy cao.

Virtual IP (VIP): Tương tự như VRRP, GLBP cũng sử dụng địa chỉ IP ảo gọi là Virtual IP (VIP) để đại diện cho gateway mặc định của mạng. Các thiết bị trong mạng sẽ gửi dữ liệu đến VIP.

Active Virtual Gateway (AVG): Trong một nhóm GLBP, có một router được chọn làm Active Virtual Gateway, có trách nhiệm phân phối các yêu cầu ARP từ các thiết bị trong mạng đến các router thực tế (Active Virtual Forwarder - AVF).

Active Virtual Forwarder (AVF): Mỗi router trong nhóm GLBP sẽ hoạt động như một AVF. AVF thực hiện vai trò định tuyến thực tế của các gói dữ liệu trong mạng và sẽ nhận lưu lượng từ AVG để xử lý.

Weighted Load Balancing: GLBP sử dụng một hệ số gọi là Weight để cân bằng tải giữa các AVF. Trong cấu hình mặc định, các AVF có cùng Weight, nhưng bạn có thể tùy chỉnh để thay đổi tỷ lệ phân phối lưu lượng.

Round Robin Load Balancing: Khi AVG nhận được yêu cầu ARP từ các thiết bị trong mạng, nó sẽ phản hồi với địa chỉ MAC của các AVF theo cách tuần tự (round robin). Điều này giúp phân chia lưu lượng mạng đến các router chính.

Tracking: GLBP hỗ trợ theo dõi trạng thái của các router chính. Nếu một router chính gặp sự cố hoặc không còn khả dụng, AVG có thể ngừng gửi yêu cầu ARP đến router đó và chỉ gửi đến các router còn lại.

Authentication: Tương tự như VRRP, GLBP cung cấp tính năng xác thực bằng cách sử dụng mật khẩu chia sẻ giữa các router.

GLBP thường được sử dụng trong môi trường mạng có yêu cầu cao về tính sẵn sàng, độ tin cậy và cân bằng tải, như các trung tâm dữ liệu, mạng doanh nghiệp, và các mạng có nhiều lưu lượng.