Ipv4:

Tại khu vực trụ sở chính, toàn bộ hệ thống mạng sử dụng dải địa chỉ lớp B riêng là 172.27.0.0/16, cung cấp tới hơn 65.000 địa chỉ IP – hoàn toàn phù hợp cho một tổ chức quy mô trung bình đến lớn. Từ dải này, các subnet được chia riêng biệt cho từng VLAN dựa theo nhu cầu thực tế. Cụ thể, VLAN 10 cần 200 host nên được cấp subnet /24, VLAN 20 nhiều hơn với 300 host dùng /23, VLAN 30 chỉ cần 100 host sử dụng /25, còn VLAN 40, 50 và 60 lần lượt được cấp các subnet /26, /28 và /27 tùy theo số lượng thiết bị. Gateway trong mỗi mạng con luôn được đặt tại địa chỉ đầu tiên của dải usable – như 172.27.10.1 cho VLAN 10 – giúp quản lý nhất quán và thuận tiện. Cách phân chia này không chỉ đảm bảo tiết kiệm tài nguyên địa chỉ mà còn sẵn sàng cho việc mở rộng mạng trong tương lai.

Ipv6:

Việc phân bổ địa chỉ IPv6 cho các VLAN tại khu vực trụ x`sở chính (HQ) được thực hiện dựa trên khối địa chỉ được cấp là 2019:ABBA:CDDC::/48. Đây là một khối địa chỉ chuẩn trong IPv6, cho phép chia nhỏ thành rất nhiều subnet có độ dài /64 – là độ dài subnet tiêu chuẩn trong IPv6. Mỗi subnet /64 cung cấp tới 2⁶⁴ địa chỉ, giúp đáp ứng nhu cầu kết nối của hàng tỷ thiết bị, đồng thời hỗ trợ tốt cho các cơ chế tự động cấp phát địa chỉ như SLAAC. Trong mô hình này, các VLAN từ 10 đến 50 được cấp phát các subnet lần lượt là 2019:ABBA:CDDC:0::/64 cho VLAN 10, 2019:ABBA:CDDC:1::/64 cho VLAN 20, và tiếp tục tăng tuyến tính đến 2019:ABBA:CDDC:4::/64 cho VLAN 50. Việc đánh số tuyến tính như vậy giúp đơn giản hóa công tác quản lý, định tuyến và mở rộng hệ thống mạng trong tương lai.

Với mỗi subnet, địa chỉ gateway được đặt là địa chỉ đầu tiên trong dải, ví dụ như gateway của VLAN 10 là 2019:ABBA:CDDC:0::1. Bên cạnh địa chỉ toàn cục (global unicast), các interface của router còn được gán địa chỉ link-local như FE80::1, FE80::1:1, v.v... Đây là các địa chỉ chỉ có phạm vi hoạt động trong một liên kết nội bộ, không được định tuyến ra ngoài. Tuy nhiên, chúng đóng vai trò rất quan trọng trong việc thiết lập các quan hệ láng giềng và truyền thông tin định tuyến nội bộ giữa các router, đặc biệt là khi sử dụng các giao thức định tuyến như OSPFv3 hoặc EIGRP for IPv6.

**Lệnh kiểm tra để record:**

**Phần PPP:**

**PPP (Point-to-Point Protocol) là một giao thức lớp liên kết dữ liệu (Data Link Layer - tầng 2 trong mô hình OSI) được sử dụng để thiết lập kết nối trực tiếp giữa hai nút mạng. Nó thường được sử dụng trong các kết nối điểm-đến-điểm (point-to-point) như:**

**Giao thức gửi nhận gói tin xác thực PAP và CHAP**

**Quá trình chung:**

**Tạo username pass**

**Kích hoạt đóng gói ppp**

**Yêu câu xác thực pap hoặc chap**

**PAP: không mã hóa chỉ cần xác đúng username, password**

Trong bài thực hiện 2 chiều

đối với 2 chiều:

Ban đầu khi có ip thì nó vẫn ping bình thường, sau khi bật **encapsulation ppp** lên thì nó sẽ **down protocol cổng serial** và 2 thằng router nó sẽ không ping được nữa do yêu cầu xác thực không thành công

sau khi cấu hình xong pap và sent username password trên cả 2 thằng thì cổng sẽ up lên, cho thấy nó đã xác thực được với nhau và ping được.

2 chiều thì cả 2 thằng phải sent username password

đối với 1 chiều:

thì chỉ cần 1 thằng router thực hiện lệnh ppp pap sent-username để gửi xác thực

và thằng còn lại chỉ cần bật pap lên thôi chỉ thực hiện xác nhận xác thực.

show int se0/3/0 trên R6 và R7, R6 ping tới R7, Kiểm tra cổng up hết và encapsulation là PPP

**CHAP: sử dụng hàm băm md5 cho password**

showint se0/3/0 trên R8 và R7, R7 ping tới R8

Ban đầu khi có ip thì nó vẫn ping bình thường, sau khi bật **encapsulation ppp** lên thì nó sẽ **down cổng serial**

**User thì dùng tên hostname, mật mẩu user ban đầu trên 2 router phải giống,sau khi cấu hình chap thì** 2 cái mật khẩu ở 2 thằng phải tạo ra cùng 1 giá trị băm giống nhau thì nó mới xác thực thành công

đối với 1 chiều : chỉ cần 1 router có lệnh ppp authentication chap

Sau khi cấu hình user R7 và R8 với pass giống nhau thì chỉ cần bật encap ppp thằng R7 lên thì nó đã up protocol cổng serial lên cho xác nhận được pass giống nhau rồi và ta bật thêm authentication chap vào

Đối với 2 chiều thì cần cả 2 router có lệnh ppp authentication chap

**Tunnel GRE:**

GRE (Generic Routing Encapsulation) là một giao thức đường hầm do Cisco phát triển, cho phép đóng gói nhiều loại gói tin (như IPv4, IPv6, IPX…) bên trong một gói IP để truyền qua mạng trung gian, thường là mạng WAN như Internet. Mục đích chính của GRE là tạo một kết nối ảo point-to-point giữa hai router qua WAN, giúp triển khai các giao thức định tuyến nội bộ (OSPF, EIGRP…) vốn yêu cầu liên kết trực tiếp. GRE cũng cho phép truyền tải các giao thức phi IP và có thể kết hợp với IPsec để mã hóa dữ liệu, đảm bảo an toàn khi truyền qua mạng WAN công cộng. Tuy nhiên, GRE không có sẵn cơ chế mã hóa hay xác thực, nên cần dùng kèm các giao thức bảo mật khác để bảo vệ dữ liệu.

Để thiết lập đường hầm GRE, địa chỉ mạng riêng 10.10.10.0/30 được sử dụng. R6 được gán địa chỉ IP 10.10.10.1/30 trên Tunnel0, còn R8 có địa chỉ 10.10.10.2/30.

Trên R6, giao diện Serial0/3/0 được cấu hình địa chỉ IP 200.0.100.2/30 làm địa chỉ nguồn vật lý, đảm bảo khả năng kết nối tới R8 qua mạng WAN. Sau đó, giao diện Tunnel0 được kích hoạt, gán IP 10.10.10.1/30, đồng thời chỉ định địa chỉ nguồn là Serial0/3/0 và địa chỉ đích là 200.0.100.6, tức địa chỉ serial của R8.

Trên R8, quá trình cấu hình tương tự được thực hiện. Giao diện Serial0/3/1 mang địa chỉ 200.0.100.6/30, và giao diện Tunnel0 được cấu hình IP 10.10.10.2/30. Địa chỉ nguồn tunnel là Serial0/3/1, còn địa chỉ đích là 200.0.100.2 – tức Serial của R6.

Việc cấu hình này cho phép tạo một đường hầm ảo giữa R6 và R8, từ đó các gói dữ liệu có thể được truyền qua tunnel như thể hai thiết bị nằm trong cùng một mạng nội bộ.

Kiểm tra bằng cách:

show ip route | include 10.10.10

ping địa chỉ 2 tunnel

traceroute ip tunnel còn lại

**Định tuyến:**

**Eigrp tại HQ**

EIGRP là một giao thức định tuyến động do Cisco phát triển, thuộc nhóm giao thức định tuyến nội bộ (IGP). EIGRP kết hợp ưu điểm của định tuyến distance vector và link-state, sử dụng thuật toán DUAL để tính toán đường đi tối ưu và đảm bảo không xảy ra vòng lặp định tuyến. Giao thức này hỗ trợ VLSM, CIDR, cập nhật định tuyến theo sự kiện thay vì định kỳ, giúp giảm tải mạng và tăng tốc độ hội tụ. Metric của EIGRP được tính dựa trên các yếu tố như băng thông, độ trễ, tải và độ tin cậy, trong đó bandwidth và delay là quan trọng nhất. EIGRP duy trì ba bảng thông tin: bảng láng giềng (Neighbor Table), bảng topo (Topology Table), và bảng định tuyến (Routing Table), đảm bảo quá trình chọn đường diễn ra hiệu quả và ổn định trong mạng nội bộ.

Đối với ipv4:

R4:

router eigrp 100

network 172.27.60.0 0.0.0.31

network 172.27.10.0 0.0.0.255

network 172.27.20.0 0.0.1.255

network 172.27.30.0 0.0.0.127

network 172.27.40.0 0.0.0.63

network 172.27.50.0 0.0.0.15

passive-interface default

no passive-interface GigabitEthernet0/0

no passive-interface GigabitEthernet0/0.60

end

Trong mô hình mạng tại khu vực HQ, các router R4, R5, R6, R7 và R8 được cấu hình sử dụng giao thức định tuyến động EIGRP ở chế độ classic với số hiệu hệ tự trị (AS) là 100. Mỗi router khai báo các dải mạng nội bộ thông qua lệnh network, cho phép EIGRP quảng bá và học các tuyến đường tương ứng. Để kiểm soát quá trình thiết lập láng giềng, lệnh passive-interface default được áp dụng nhằm vô hiệu hóa gửi/nhận gói Hello trên tất cả các cổng, ngoại trừ các cổng thực sự cần thiết như liên kết giữa các router – được bật lại bằng lệnh no passive-interface. Việc này giúp tối ưu hiệu năng và đảm bảo an toàn định tuyến. Các địa chỉ mạng được chia thành nhiều subnet phục vụ cho các VLAN và liên kết liên router, từ đó hình thành các bảng định tuyến động, hỗ trợ cập nhật nhanh và hiệu quả khi có thay đổi trong mạng.

đối với ipv6:

Tại site HQ, giao thức EIGRP for IPv6 được triển khai nhằm đảm bảo khả năng định tuyến động giữa các router R4, R5, R6, R7 và R8. Trước tiên, trên tất cả các router cần kích hoạt tính năng định tuyến IPv6 toàn cục bằng lệnh:

ipv6 unicast-routing

Sau đó, mỗi router được cấu hình tiến trình EIGRP riêng với một router-id duy nhất để định danh, ví dụ R4 là 4.4.4.4, R5 là 5.5.5.5, v.v. Tiến trình định tuyến cần được kích hoạt bằng lệnh no shutdown.

Khác với EIGRP cho IPv4, trong EIGRP cho IPv6, không cần sử dụng lệnh network để khai báo các mạng tham gia định tuyến. Thay vào đó, EIGRP được kích hoạt trực tiếp trên từng interface thông qua lệnh:

ipv6 eigrp 10

Lý do không cần khai báo network trong EIGRP IPv6 là bởi vì cơ chế hoạt động đã thay đổi: IPv6 EIGRP không tự động kích hoạt trên interface dựa vào network statements, mà yêu cầu người quản trị chỉ định rõ ràng từng interface nào sẽ tham gia EIGRP. Điều này giúp quản lý cấu hình linh hoạt, rõ ràng hơn, đồng thời tránh kích hoạt EIGRP ngoài ý muốn trên các interface không mong muốn.

Trên R4, các subinterface thuộc các VLAN (Gig0/0.10 đến Gig0/0.50) được gán địa chỉ IPv6 (global và link-local) và kích hoạt EIGRP. Các router còn lại như R5, R6, R7, R8 cũng được cấu hình tương tự trên các interface kết nối mạng nội bộ và liên router (Serial hoặc GigabitEthernet), đảm bảo toàn bộ site HQ đều có thể trao đổi bảng định tuyến thông qua EIGRP.

Ngoài ra, trên router R5 – đóng vai trò gateway ra ngoài – một tuyến mặc định (::/0) được thiết lập trỏ đến địa chỉ của router kết nối mạng ACCESS:

ipv6 route ::/0 2019:ABBA:AAAA:1::1

định tuyến vlan cho ipv6:

Tại router R4, các mạng LAN nội bộ tương ứng với các VLAN được triển khai thông qua các **subinterface** trên cổng GigabitEthernet0/0. Mỗi subinterface đại diện cho một VLAN riêng biệt, được định danh bằng số VLAN và cấu hình như sau:

interface Gig0/0.10

encapsulation dot1Q 10

ipv6 address 2019:ABBA:CDDC:0::1/64

ipv6 address FE80::1 link-local

ipv6 enable

ipv6 eigrp 10

Các dòng cấu hình thực hiện các chức năng:

* encapsulation dot1Q 10: Định danh subinterface thuộc VLAN 10, sử dụng chuẩn IEEE 802.1Q để gắn thẻ VLAN.
* ipv6 address .../64: Cấp địa chỉ IPv6 toàn cục (global unicast) cho interface.
* ipv6 address FE80::... link-local: Cấp địa chỉ IPv6 link-local để sử dụng trong giao tiếp nội bộ mạng (đặc biệt cần thiết cho hoạt động của các giao thức định tuyến như EIGRP).
* ipv6 enable: Kích hoạt IPv6 trên interface (cần thiết để EIGRP hoạt động).
* ipv6 eigrp 10: Kích hoạt tiến trình định tuyến EIGRP số 10 trên interface này.

Cấu hình tương tự được áp dụng cho các subinterface Gig0/0.20, Gig0/0.30, Gig0/0.40 và Gig0/0.50 tương ứng với VLAN 20, 30, 40 và 50, mỗi VLAN sử dụng một địa chỉ IPv6 mạng khác biệt:

Lệnh để kiểm tra:

Sh ip route eigrp

Sh ip eigrp nei

Sh ip eigrp topology

**OSPF tại khu vực Branch**

**OSPF (Open Shortest Path First)** là một giao thức định tuyến nội vùng (IGP) hoạt động theo thuật toán đường ngắn nhất (Dijkstra), được sử dụng phổ biến trong các mạng lớn nhờ khả năng hội tụ nhanh, phân cấp mạng hiệu quả và hỗ trợ định tuyến theo trạng thái liên kết. Mỗi router OSPF duy trì ba bảng dữ liệu quan trọng để đảm bảo việc định tuyến chính xác: (1) **Bảng láng giềng (Neighbor Table)** – lưu thông tin về các router lân cận đã thiết lập quan hệ; (2) **Bảng cơ sở dữ liệu liên kết trạng thái (Link-State Database - LSDB)** – chứa toàn bộ bản đồ mạng OSPF trong khu vực, đồng bộ giữa các router; (3) **Bảng định tuyến (Routing Table)** – chứa các tuyến đường tốt nhất đến các mạng đích, được tính toán dựa trên LSDB bằng thuật toán SPF.

Tại khu vực Branch, OSPF được triển khai theo mô hình đa khu vực để tối ưu hóa định tuyến và giảm tải cho backbone. Mạng 10.28.1.0/24 kết nối vật lý các router R1, R2, R3 qua switch và được cấu hình trong Area 0 – vùng backbone trung tâm của OSPF, đảm bảo trao đổi thông tin định tuyến giữa các area khác nhau.

Loopback là một địa chỉ logic trên router, không gắn với cổng vật lý nào, thường dùng để định danh router và phục vụ quản lý mạng. Việc gán loopback vào các area này giúp phân tách mạng theo chức năng, giảm tải cho backbone. Nếu ta kh cấu hình router id thủ công thì nó sẽ chọn địa chỉ loopback cao nhất làm router id

Backbone là **một vùng mạng diện rộng**, nơi các router trong các area khác phải “đi qua” để trao đổi thông tin định tuyến với nhau. Vì thế, backbone là khu vực trung tâm, có vai trò làm xương sống của mạng OSPF

Area 0 là backbone nên các interface trên router tham gia vào backbone thường dùng địa chỉ cố định với wildcard mask 0.0.0.0 trong câu lệnh OSPF để chỉ định chính xác từng địa chỉ IP, đảm bảo kết nối ổn định giữa các router trong backbone.

Các router là ABR vì đều kết nối giữa Area 0 và 1 area khác ,có nhiệm vụ kết nối, chuyển tiếp thông tin định tuyến giữa backbone và các khu vực con. Cấu hình passive-interface mặc định giúp giảm lưu lượng OSPF không cần thiết, chỉ giữ interface vật lý liên kết router được hoạt động OSPF.

Test:

Sh ip route ospf

Sh ip ospf nei

**Định tuyến mặc định từ router R5 đến Access**

Ở phần này thực hiện lệnh ip route 0.0.0.0 0.0.0.0 200.0.100.10. Lệnh này định nghĩa rằng mọi gói tin không biết đích sẽ được chuyển tiếp đến địa chỉ IP 200.0.100.10 – tức router ACCESS. Tuyến mặc định này sau đó sẽ được phân phối (redistribute) vào các giao thức định tuyến đang chạy trên R5 như OSPF và EIGRP, để các router khác trong hệ thống cũng biết cách đi ra ngoài mạng.

**Redistribution giữa OSPF và EIGRP trên R5:**

⎯ Redistribute từ EIGRP sang OSPF: Trên R5, tiến trình OSPF được khởi tạo với router-id là 5.5.5.5. R5 đưa mạng kết nối về backbone (10.28.1.4) vào OSPF Area 0 thông qua lệnh network 10.28.1.4 0.0.0.0 area 0. Để chia sẻ các route học được từ tiến trình EIGRP, lệnh redistribute eigrp 100 subnets được sử dụng. Tùy chọn subnets đảm bảo rằng các subnet có độ dài khác nhau đều được tái phân phối, thay vì chỉ các route classful.

Bên cạnh đó, tuyến mặc định đã được cấu hình trên R5 (ip route 0.0.0.0 0.0.0.0 200.0.100.10) sẽ được quảng bá vào OSPF bằng lệnh default-information originate. Điều này cho phép các router khác trong OSPF biết đường đi ra Internet thông qua R5.

Để kiểm soát việc gửi bản tin OSPF Hello, R5 cấu hình passive-interface default để tắt chế độ gửi nhận OSPF trên tất cả các interface, và chỉ mở lại trên những cổng cần thiết như GigabitEthernet0/0, GigabitEthernet0/1 và Serial0/3/0.

⎯ Redistribute từ OSPF sang EIGRP: Ở chiều ngược lại, trong tiến trình EIGRP (AS 100), R5 đưa các mạng nội bộ 172.27.60.0/27 vào định tuyến bằng các lệnh network. Để chia sẻ các route học được từ OSPF, lệnh redistribute ospf 1 metric 10000 100 255 1 1500 được sử dụng. Lệnh này yêu cầu bắt buộc cung cấp các thông số metric vì OSPF không sử dụng các thành phần metric tương tự như EIGRP. redistribute static chèn các tuyến tĩnh (static routes) vào trong bảng định tuyến của giao thức định tuyến này .

Cụ thể, các tham số metric trong lệnh redistribute ospf là các giá trị cấu hình metric cho EIGRP theo thứ tự sau:

* **Bandwidth**: 10000 (tính bằng kilobits/giây) — băng thông giả định của đường đi.
* **Delay**: 100 (tính bằng micro giây) — độ trễ giả định.
* **Reliability**: 255 (giá trị từ 0 đến 255, 255 là tốt nhất).
* **Load**: 1 (giá trị từ 0 đến 255, càng nhỏ càng tốt).
* **MTU**: 1500 (Maximum Transmission Unit) — kích thước gói tối đa.

Sh ip route trên router r5 và r7 r1 để check

**Định tuyến ipv6 eigrp tại khu vực HQ**

**Switch và vlan:**

Mục đích chính của VLAN là giới hạn phạm vi broadcast trong từng nhóm riêng biệt, tránh broadcast lan rộng khắp toàn mạng, từ đó giảm tắc nghẽn và tăng hiệu suất mạng.

Để quản lý thống nhất cơ sở dữ liệu VLAN tại khu vực HQ, hệ thống sử dụng giao thức VTP với vtp domain là tdtu và vtp password là tdtuvn.

Lệnh vtp domain tdtu dùng để thiết lập tên miền VTP, giúp các switch thuộc cùng domain có thể trao đổi và đồng bộ thông tin VLAN với nhau. Trong khi đó, vtp password tdtuvn thiết lập mật khẩu xác thực nhằm đảm bảo chỉ những switch có cùng mật khẩu mới được phép tham gia trao đổi dữ liệu VTP. Việc cấu hình cả domain và password giúp đảm bảo tính đồng bộ và bảo mật trong quản lý VLAN trên toàn hệ thống mạng.

Switch S1 được cấu hình ở chế độ VTP server thông qua lệnh vtp mode server để tạo và phân phối VLAN, còn các switch còn lại (S2, S3, S4) được cấu hình là VTP client thông qua lệnh vtp mode client, giúp tự động đồng bộ VLAN từ server mà không cần cấu hình thủ công. Trên VTP Server S1, các VLAN sau được tạo ra để phục vụ cho các đơn vị và mục đích riêng biệt:

**STP và root brigde:**

**Rapid PVST+** là phiên bản cải tiến của giao thức STP (Spanning Tree Protocol) truyền thống, giúp tăng tốc quá trình hội tụ mạng khi có sự thay đổi topology. Khác với STP thường, Rapid PVST+ cho phép mỗi VLAN có một cây spanning riêng (giống PVST+), nhưng hội tụ nhanh hơn nhờ các cơ chế như edge port (portfast), link-type, và handshake nhanh. Việc chuyển sang Rapid PVST+ giúp giảm thời gian chuyển trạng thái của cổng (port), từ đó rút ngắn thời gian khôi phục kết nối khi có sự cố.

Trong cấu hình, việc đặt **S1 làm Root Bridge cho VLAN 10, 20, 30** và **S2 làm Root Bridge cho VLAN 40, 50, 60** bằng cách thiết lập priority 4096 giúp xác định rõ switch nào sẽ đóng vai trò trung tâm trong từng cây spanning tree. Điều này giúp kiểm soát đường đi của dữ liệu, tối ưu hóa lưu lượng mạng và tránh hiện tượng loop.

Để kiểm tra cấu hình Root Bridge, có thể dùng lệnh show spanning-tree vlan [vlan-id] trên các switch. Nếu switch đang xét là Root Bridge, dòng kết quả sẽ hiển thị “**This bridge is the root**”; ngược lại, sẽ hiển thị thông tin Root Bridge là switch khác cùng với địa chỉ MAC của nó.

VLAN quản lý và truy cập SSH

Để hỗ trợ quản trị tập trung và an toàn, tất cả các switch đều được gán địa chỉ IP trong VLAN 60 (vùng quản lý) với subnet /27 là 172.27.60.0/27 Mỗi switch sử dụng default-gateway là 172.27.60.1 để có thể kết nối ra ngoài, đồng thời cho phép truy cập SSH từ xa. Các bước cấu hình SSH gồm:

Việc cấu hình SSH giúp bảo mật phiên làm việc từ xa, tránh truy cập trái phép và nâng cao tính bảo mật hệ thống mạng

**Định tuyến vlan Router-on-a-Stick – Kết nối giữa các VLAN**

Router-on-a-Stick là phương pháp cấu hình định tuyến liên VLAN bằng cách sử dụng một cổng vật lý trên router để xử lý nhiều VLAN khác nhau thông qua các sub-interface. Mỗi sub-interface tương ứng với một VLAN, được gán địa chỉ IP làm gateway cho VLAN đó và sử dụng giao thức encapsulation dot1Q để phân biệt lưu lượng từng VLAN. Trong bài này, router R4 được cấu hình các sub-interface cho VLAN 10 đến 60, với VLAN 60 là native VLAN (không gắn thẻ VLAN tag khi truyền qua trunk).

Để các sub-interface này hoạt động, switch kết nối với router (ở đây là SW1, cổng fa0/6) phải được cấu hình ở chế độ trunk, cho phép truyền lưu lượng của nhiều VLAN trên cùng một đường truyền. Đồng thời, vì trên R4 có một sub-interface là native VLAN 60, nên phía switch cũng phải cấu hình switchport trunk native vlan 60 để đảm bảo sự khớp giữa hai thiết bị. Nếu không cấu hình đúng native VLAN ở cả hai phía, việc giao tiếp qua VLAN 60 sẽ không thành công, ảnh hưởng đến việc ping, cấp DHCP, hoặc truy cập liên VLAN.

Tóm lại, Router-on-a-Stick giúp tiết kiệm cổng vật lý trên router, trunk đảm bảo truyền dữ liệu nhiều VLAN qua một cổng, và native VLAN đóng vai trò truyền lưu lượng không gắn thẻ giữa các thiết bị một cách chính xác và đồng bộ.

Sh ip int br trên R4 để check vlan trên sub

**Etherchannel với LACP**

Nhằm tăng băng thông và nâng cao khả năng dự phòng mạng, các kết nối giữa các switch trong hệ thống được thiết lập dưới dạng EtherChannel, sử dụng giao thức thương lượng LACP (Link Aggregation Control Protocol). Giao thức này cho phép các switch tự động thương lượng để gộp nhiều cổng vật lý thành một kênh logic duy nhất, được gọi là Port-Channel. Việc sử dụng EtherChannel không chỉ giúp tăng tổng băng thông giữa các switch, mà còn cải thiện độ ổn định của mạng khi một trong các liên kết vật lý gặp sự cố.

Các kết nối trên được cấu hình ở chế độ trunk, cho phép truyền tải nhiều VLAN qua lại giữa các switch trong toàn bộ hệ thống.

Lệnh channel-group <số> mode active: đưa các cổng vật lý vào nhóm EtherChannel sử dụng chế độ **active**, tức là **chạy LACP** để tự động thương lượng liên kết.

Lệnh interface port-channel <số> cùng với switchport mode trunk: cấu hình kênh logic thành trunk để truyền tải **nhiều VLAN**, như VLAN 10, 20, 30... qua lại giữa các switch.

Tất cả các port-channel đều tuân theo chuẩn **trunking 802.1Q**, đảm bảo khả năng hoạt động đồng bộ giữa các VLAN toàn hệ thống.

Test:

show etherchannel summary

vi du

 Po1(SU): Port-channel 1 đang hoạt động (S: Layer 2, U: Up).

 LACP: Giao thức được sử dụng là LACP.

 Fa0/2(P), Fa0/3(P): Các cổng vật lý đang ở trạng thái **Participating (P)** trong EtherChannel.

**NAT va DHCP**

NAT (Network Address Translation) là kỹ thuật cho phép các thiết bị trong mạng nội bộ sử dụng địa chỉ IP riêng (private IP) để truy cập Internet thông qua việc chuyển đổi sang một địa chỉ IP công cộng. Trong cấu hình này, chúng ta sử dụng NAT Overload, hay còn gọi là PAT (Port Address Translation), cho phép nhiều thiết bị chia sẻ cùng một địa chỉ IP công cộng bằng cách gán các cổng khác nhau.

**Xác định các giao diện inside và outside:**

Đầu tiên, chúng ta xác định đâu là phía "trong" (inside) và đâu là phía "ngoài" (outside) của NAT:

* Giao diện **GigabitEthernet0/0** được gán IP công cộng 203.0.113.254, kết nối đến ISP, nên ta đánh dấu là **ip nat outside**.
* Giao diện **Serial0/3/0**, IP 200.0.100.10, kết nối về nội bộ (HQ và Branch), ta đánh dấu là **ip nat inside**.

**Để NAT hoạt động**, router cần biết những địa chỉ IP nào trong nội bộ cần được chuyển đổi. Ta sử dụng **Access List 1** để cho phép NAT cho 2 dải mạng nội bộ:

* 172.27.0.0/16 cho khu vực **HQ**
* 10.28.0.0/16 cho khu vực **Branch**

Lệnh cấu hình:

access-list 1 permit 172.27.0.0 0.0.255.255

access-list 1 permit 10.28.0.0 0.0.255.255

**Áp dụng NAT Overload (PAT):**

Sau khi xác định dải IP nội bộ, ta cấu hình NAT Overload để tất cả các thiết bị trong HQ và Branch có thể chia sẻ **IP công cộng 203.0.113.254** khi truy cập Internet. Câu lệnh thực hiện:

ip nat inside source list 1 interface GigabitEthernet0/0 overload

Câu lệnh này nói với router: “Hãy lấy tất cả các gói từ những IP trong access-list 1 và dịch chúng thành địa chỉ của G0/0 (IP công cộng), đồng thời sử dụng các cổng để phân biệt từng kết nối”.

**Định tuyến mặc định về ISP:**

Để gói tin ra Internet được gửi đúng, ta thêm một **default route** trỏ đến địa chỉ IP của router ISP là 203.0.113.1:

ip route 0.0.0.0 0.0.0.0 203.0.113.1

Router Access đóng vai trò như **cổng ra Internet duy nhất** cho toàn bộ hệ thống mạng nội bộ của tổ chức. Việc sử dụng NAT Overload không chỉ giúp tiết kiệm địa chỉ IP công cộng, mà còn góp phần tăng tính bảo mật, vì địa chỉ IP nội bộ không được lộ ra bên ngoài.

Test kiểm tra bằng show running config và xem cổng se0/3/0 và gi0/0 trên access

**Cấu hình Port Forwarding cho HTTPS và HTTP**

Port forwarding là kỹ thuật cho phép **các yêu cầu từ bên ngoài Internet (IP công cộng)** được **chuyển tiếp tới một máy chủ nội bộ (IP private)**. Trường hợp này, chúng ta chuyển tiếp:

* **HTTP (port 80)**
* **HTTPS(port443)**  
  từ IP công cộng của router Access là 203.0.113.254 đến **máy chủ web nội bộ tại địa chỉ 172.27.50.10** (ví dụ: máy chủ trong VLAN 50 của HQ).

**Câu lệnh cấu hình cụ thể**

ip nat inside source static tcp 172.27.50.10 80 203.0.113.254 80

ip nat inside source static tcp 172.27.50.10 443 203.0.113.254 443

**Giải thích:**

* ip nat inside source static tcp: chỉ định kiểu NAT tĩnh và giao thức TCP.
* 172.27.50.10 80: IP nội bộ và cổng đích trên server web.
* 203.0.113.254 80: IP công cộng và cổng bên ngoài để truy cập từ Internet.  
  => Khi người dùng truy cập [**http://203.0.113.254**](http://203.0.113.254) hoặc [**https://203.0.113.254**](https://203.0.113.254), router sẽ tự động **chuyển tiếp yêu cầu** đến máy chủ nội bộ tại 172.27.50.10.

**3. Kiểm tra Port Forwarding bằng mô phỏng**

Để kiểm tra hoạt động port forwarding, bạn cần **mô phỏng người dùng ngoài Internet** truy cập dịch vụ web trên mạng nội bộ thông qua IP công cộng.

**Cách làm:**

* Tạo một PC giả lập **nằm ngoài mạng nội bộ**, gán IP 192.168.1.10.
* Kết nối PC này với router **ISP**, router này gán IP 192.168.1.1 cho interface kết nối PC.
* Cấu hình định tuyến từ ISP về router Access:

ip route 0.0.0.0 0.0.0.0 203.0.113.254

* Trên PC giả lập, mở trình duyệt web và nhập:
  + http://203.0.113.254 (kiểm tra HTTP)
  + https://203.0.113.254 (kiểm tra HTTPS)

Nếu cấu hình đúng, bạn sẽ thấy giao diện web của máy chủ nội bộ tại 172.27.50.10.

**DHCP ipv4:**

Router R4 được cấu hình làm DHCP server nội bộ cho các VLAN trong mạng, cụ thể là các VLAN 10, 20, 30 và 40. DHCP server sẽ tự động cấp phát địa chỉ IP cho các thiết bị trong các VLAN tương ứng, giúp giảm công sức cấu hình thủ công và đảm bảo quản lý địa chỉ IP hiệu quả.

Cách hoạt động của DHCP trên R4

R4 giữ các pool địa chỉ IP riêng biệt cho từng VLAN, dựa trên subnet của VLAN đó.

Trong mỗi pool DHCP:

network xác định dải địa chỉ IP cấp phát cho VLAN.

default-router là gateway mặc định của VLAN, chính là địa chỉ IP của interface router trên VLAN đó.

dns-server cung cấp địa chỉ server DNS để các thiết bị trong VLAN có thể phân giải tên miền.

Ngoài ra, các địa chỉ IP bị loại trừ (excluded-address) như địa chỉ gateway của từng VLAN sẽ không được DHCP cấp phát cho các thiết bị khác, tránh trùng lặp.

Ví dụ cấu hình trên R4:

bash

CopyEdit

ip dhcp excluded-address 172.27.10.1

ip dhcp excluded-address 172.27.20.1

ip dhcp excluded-address 172.27.30.1

ip dhcp excluded-address 172.27.40.1

ip dhcp pool VLAN10

network 172.27.10.0 255.255.255.0

default-router 172.27.10.1

dns-server 172.27.50.10

ip dhcp pool VLAN20

network 172.27.20.0 255.255.254.0

default-router 172.27.20.1

dns-server 172.27.50.10

ip dhcp pool VLAN30

network 172.27.30.0 255.255.255.128

default-router 172.27.30.1

dns-server 172.27.50.10

ip dhcp pool VLAN40

network 172.27.40.0 255.255.255.192

default-router 172.27.40.1

dns-server 172.27.50.10

Giải thích bổ sung: Đây là loại DHCP nào?

Loại DHCP trên R4 là DHCP server nội bộ (Router-based DHCP server).

Router R4 thực hiện chức năng cấp phát địa chỉ IP động trực tiếp, không cần một server DHCP riêng biệt (như Windows DHCP Server hay Linux DHCP Server).

Khi một thiết bị trong VLAN gửi yêu cầu DHCP (DHCP Discover), router R4 sẽ phản hồi và cấp phát địa chỉ IP theo pool tương ứng dựa trên VLAN/subnet của thiết bị đó.

Đây là một cách phổ biến và hiệu quả để quản lý DHCP cho các mạng VLAN nhỏ và vừa, tận dụng luôn router làm DHCP server mà không cần thiết bị riêng.

Tóm lại:

R4 là DHCP server, cung cấp IP động cho các VLAN.

Các địa chỉ IP được chia thành pool riêng theo VLAN.

Địa chỉ IP gateway được loại trừ không bị cấp cho thiết bị.

Router đảm bảo thiết bị trong từng VLAN được cấp IP đúng dải và cấu hình gateway, DNS phù hợp.

Đây là DHCP server tích hợp trong router (router-based DHCP server).

**DHCP ipv6:**

Trong mô hình mạng tại site HQ, do packet tracer không hỗ trợ chức năng DHCPv6 relay agent, nên không thể triển khai DHCPv6 theo kiểu phân tán. Vì vậy, toàn bộ quá trình cấp phát thông tin DNS và domain name được thực hiện tập trung tại router R4 thông qua cơ chế DHCPv6 stateless. Cụ thể, các pool DHCPv6 tương ứng với từng VLAN (10, 20, 30, 40) được tạo trên R4, trong đó khai báo các tham số như DNS server và domain name. Trên mỗi subinterface, lệnh ipv6 nd other-config-flag được bật để thông báo cho thiết bị đầu cuối rằng cần dùng DHCPv6 để nhận các thông tin cấu hình bổ sung. Lệnh ipv6 dhcp server <pool> được sử dụng để gán pool tương ứng với từng interface. Cơ chế này không cấp phát địa chỉ IPv6 – các thiết bị tự động sinh địa chỉ qua SLAAC dựa trên Router Advertisement từ router R4 – mà chỉ cung cấp thông tin bổ sung, đảm bảo các máy trạm trong từng VLAN có thể cấu hình đầy đủ thông tin mạng một cách tự động.

**Các yêu cầu khác ở ipv4:**

**Chặn truy cập nội bộ từ VLAN GUEST**

Trong hệ thống mạng, VLAN 40 được cấu hình làm VLAN GUEST — phục vụ người dùng không thuộc tổ chức, chẳng hạn như khách đến thăm. Để đảm bảo tính bảo mật và phân vùng truy cập, cần giới hạn khả năng truy cập của VLAN GUEST vào toàn bộ mạng nội bộ của HQ và Branch. Tuy nhiên, VLAN này vẫn phải được phép nhận địa chỉ IP qua DHCP và truy cập ra Internet.

Để thực hiện điều này, chúng tôi cấu hình Access Control List (ACL) mở rộng có tên là BLOCK\_GUEST\_ACCESS trên router R4. ACL này được gắn vào subinterface GigabitEthernet0/0.40 (tương ứng với VLAN 40) ở chiều in — tức là chặn ngay tại điểm đầu ra khỏi VLAN GUEST.

Cấu hình chi tiết

R4(config)# ip access-list extended BLOCK\_GUEST\_ACCESS

R4(config-ext-nacl)# deny ip 172.27.40.0 0.0.0.63 172.27.0.0 0.0.255.255

R4(config-ext-nacl)# deny ip 172.27.40.0 0.0.0.63 10.28.0.0 0.0.255.255

R4(config-ext-nacl)# permit udp 172.27.40.0 0.0.0.63 any eq bootpc

R4(config-ext-nacl)# permit udp any any eq bootps

R4(config-ext-nacl)# permit ip 172.27.40.0 0.0.0.63 any

Giải thích:

deny ip 172.27.40.0 0.0.0.63 172.27.0.0 0.0.255.255: chặn VLAN GUEST truy cập toàn bộ mạng nội bộ HQ.

deny ip 172.27.40.0 0.0.0.63 10.28.0.0 0.0.255.255: chặn VLAN GUEST truy cập mạng nội bộ Branch.

permit udp 172.27.40.0 any eq bootpc: cho phép gói tin DHCP Discover từ client gửi đi.

permit udp any any eq bootps: cho phép gói tin DHCP Offer từ server trả về.

permit ip 172.27.40.0 0.0.0.63 any: cho phép các gói IP còn lại (đặc biệt là ra Internet).

Gắn ACL vào interface VLAN GUEST

R4(config)# interface GigabitEthernet0/0.40

R4(config-subif)# ip access-group BLOCK\_GUEST\_ACCESS in

Lệnh này đảm bảo các gói tin từ VLAN 40 bị kiểm soát ngay khi rời khỏi subinterface.

**Giới hạn truy cập SSH vào các switch ngoại trừ VLAN SERVERS**

Cơ chế thực hiện

Trên từng switch, ta tạo một danh sách kiểm soát truy cập (ACL) dạng chuẩn với tên gọi SSH\_ONLY\_SERVERS. ACL này cho phép các kết nối từ dải IP VLAN SERVERS và chặn tất cả các kết nối SSH đến từ các VLAN khác.

ACL sau đó được áp dụng trực tiếp vào dòng điều khiển từ xa line vty 0 4 qua lệnh access-class, nhằm kiểm soát quyền truy cập SSH.

Ngoài ra, để tăng cường bảo mật, ta chỉ cho phép giao thức SSH được sử dụng cho kết nối điều khiển từ xa, đồng thời từ chối các giao thức không an toàn như Telnet bằng câu lệnh transport input ssh.

Cấu hình chi tiết

Switch(config)# ip access-list standard SSH\_ONLY\_SERVERS

Switch(config-std-nacl)# permit 172.27.50.0 0.0.0.15

Switch(config-std-nacl)# exit

Switch(config)# line vty 0 4

Switch(config-line)# access-class SSH\_ONLY\_SERVERS in

Switch(config-line)# transport input ssh

Switch(config-line)# exit

Giải thích:

ip access-list standard SSH\_ONLY\_SERVERS tạo ACL chuẩn tên SSH\_ONLY\_SERVERS.

permit 172.27.50.0 0.0.0.15 chỉ cho phép IP trong dải VLAN SERVERS truy cập.

access-class SSH\_ONLY\_SERVERS in áp dụng ACL cho các kết nối SSH đến qua line vty.

transport input ssh giới hạn chỉ cho phép giao thức SSH, chặn Telnet và các giao thức không an toàn khác.

Kết quả kiểm thử

Khi thực hiện kết nối SSH từ thiết bị trong VLAN SERVERS (ví dụ dùng lệnh ssh -l admin <ip-switch>), kết nối được thiết lập thành công.

Các thiết bị từ các VLAN khác (ví dụ VLAN 10) không thể thiết lập kết nối SSH đến switch.

Điều này đảm bảo rằng chỉ người dùng trong VLAN SERVERS mới được quyền truy cập từ xa vào các thiết bị mạng, tăng cường an ninh hệ thống.