Báo cáo thực thực tập công ty an ninh mạng viettel: Routing basic

Bùi Hoàng Dũng

February 2024

Mục lục

1 Basic router **2**

2 Router function **3**
2.1 Path determination 4

3 IP address **5**
3.1 IP address class 5

4 Subnet calculation **7**

5 IP public, IP private, NAT **8**
5.1 NAT 8

6 ACL(Access Controll List **11**

7 Link State Protocol và Distance Vector Protocol **12**
7.1 Link State Routing Protocol 12
7.2 Distance Vector Routing Protocol 12

8 RIP **12**

9 OSPF **13**
9.1 OSPF area 14
9.2 OSPF metric và OSPF neighbor 15
9.3 OSPF state 15

1 Basic router

mathptmx Encapsulaton IP packet: Việc đóng gói IP header vào gói tin nhằm giúp việc truyền đi của gói tin trở nên dễ dàng khi gói tin được chuyển qua mạng khác. Việc đóng gói sẽ được thực hiện ở bên phía người gửi còn việc mở gói sẽ được thực hiện ở bên người nhận. Dưới đây là mô tả quá trinh đóng gói: Khi dữ liệu được đóng gói một lớp được gọi là 'segment header' sau đó sẽ được truyền xuống dưới lớp network. Lớp network sẽ thực hiện đóng gói bằng cách thêm phần header vào gói tin lúc này ta được một IP packet.
Các thành phần của một **IP header**

Hình 1: Ip-header

- Trường đầu tiên là Version có chiều dài là 4 bits có tác dụng để xác định phiên bản IP sử dụng (Ipv4 = 0100, Ipv6 = 0110)
- Trường thứ hai là IHL (IP Header Length) có chiều dài là 4 bits dùng để xác định chiều dài của header với kết quả là bội của 4 bytes. (VD: giá trị của của này là 5 thì chiều dài của phần header sẽ là 20 bytes). Lưu ý giá trị tối thiểu của trường này là 5 (tức 20 bytes độ dài header) và giá trị tối đa của trường này là 15 (15.4=60 bytes).
- Trường tiếp theo là DSCP (Differentiated Services code point) và có chiều dài là 6 bit trường này được sử dụng cho mục đích QoS (Quality of Service) được sử dụng để ưu tiên cho những dữ liệu nhạy cảm với độ trễ (streaming voice, video, ...) trường này giúp cho việc xác định ra traffic nào nên được xử lý một cách ưu tiên
- Trường tiếp theo là ECN (Explicit Congestion Notification) có chiều dài 2 bits dùng để cung cấp thông báo về sự tắc nghẽn mạng ở kết nối end-to-end mà không phải drop packet. Tuy nhiên trường này lại là một trường optional yêu cầu về phần hạ tầng của các endpoint phải hỗ trợ nó.
- Trường tiếp theo là Total length có chiều dài 16 bits có tác dụng diễn tả tổng chiều dài của cả packet (bao gồm cả phần data và header) được diễn tả bằng bytes. Giá trị nhỏ nhất của trường này là 20 bytes(bằng với giá trị nhỏ nhất của Ipv4 header mà không phải đóng gói), giá trị lớn nhất là 65535 (maximum 16bit)
- Trường tiếp theo là Identification có chiều dài là 16 bits, trong trường hợp mà packet quá lớn và phải cần phân mảnh, trường này sẽ có tác dụng xác định xem phần phân mảnh này thuộc gói tin nào, nhớ đó mà gói tin có thể được lắp ráp lại như nguyên bản. Tất cả các phân đoạn thuộc cùng

một gói tin sẽ có một Ipv4 header riêng với giá trị giống nhau ở trường Identification. Packet được phân mảnh nếu nó lớn hơn MTU (Maximum Transmission Unit). Các phân đoạn sẽ được lắp ráp tại bên nhận.

- Trường tiếp theo là Flags Field có chiều dài là 3 bits được sử dụng để điều khiển và xác định các phân đoạn. Bit đầu tiên luôn luôn là bit 0, bit tiếp theo là Don't Fragment bit được sử dụng để chỉ ra một packet có nên được phân đoạn hay là không (nếu bit này có giá trị là 1 thì có nghĩa là packet này không nên được phân đoạn, còn 0 thì sẽ là ngược lại), bit cuối cùng là More Fragment bit được set là 1 nếu có nhiều phân đoạn khác trong packet được phân mảnh, được set là 0 nếu đó là fragment cuối cùng (Các paket mà không được phân mảnh thì MF bit luôn được set là 0)

- Trường tiếp theo là Fragment Offset Field có chiều dài là 13 bits có tác dụng là để chỉ ra vị trí của các phân đoạn trong packet nguyên bản, dựa vào trường này mà ta có thể lắp ráp lại các phân đoạn bất kể rằng các phân đoạn có đến đích theo thứ tự hay là không.

- Trường tiếp theo là Time to live có chiều dài là 8 bits. Một router sẽ drop một packet có giá trị TTL được set là 0, được sử dụng để ngăn chặn vòng lặp vĩnh viễn trong mạng.Trường này sẽ ngăn chặn loop trafic khi mà TTL = 0. Trường TTL được thiết kế với mục đích ban đầu là để chỉ ra thời gian sống bằng giây của một packet. Ngoài ra nó còn chỉ ra những chặng mà nó đã đi qua bằng cách khi qua mỗi 1 chặng thì TTL sẽ được trừ đi 1 (recommended Default TTL là 64)

- Trường tiếp theo là Protocol Field có chiều dài là 8 bits chỉ ra giao thức được sử dụng ở đóng gói lớp 4 (TCP = 6, UDP = 17, ICMP = 1 , OSPF = 89)

- Trường tiếp theo là Header checksum field có độ dài là 16 bits được sử dụng với mục đích kiểm tra lỗi trong Ipv4 header, khi mà một router nhận được một gói tin nó sẽ tính toán checksum của header và so sánh nó với giá trị trong checksum field, nếu nó không giống nhau thì router sẽ drop gói tin, IP sẽ dựa vào giao thức đóng gói được sử dụng để có thể phát hiện ra lỗi trong dữ liệu đã được đóng gói

- 2 Trường tiếp theo là địa chỉ IP nguồn và đích với mỗi địa chỉ có độ dài là 32 bits

- Trường cuối cùng là options có chiều dài từ 0 đến 320 bits thường hiếm khi được sử dụng, nếu trường IHL lớn hơn 5 tức là phần options của IP header đã được sử dụng

2 Router function

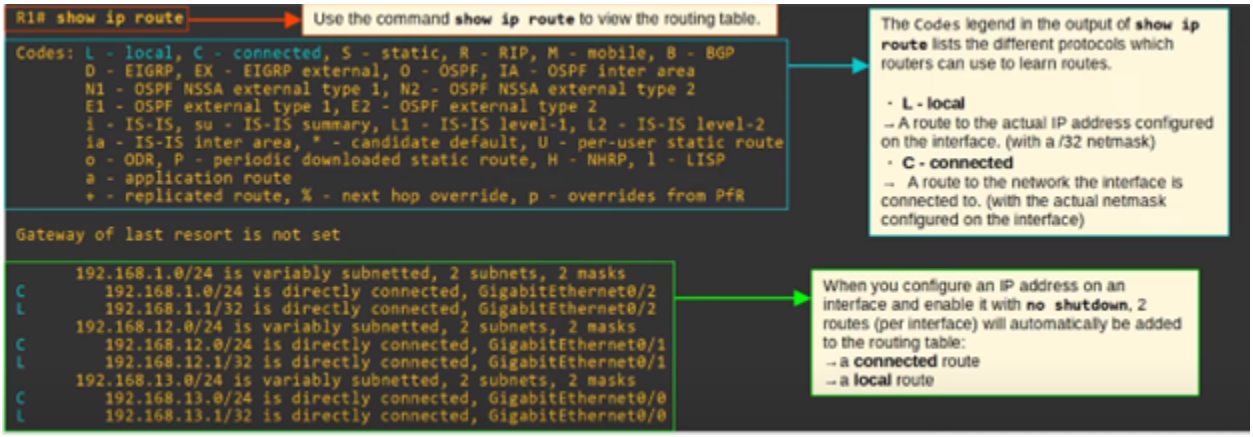
Chức năng của Router: thực hiện quá trình routing tức là xác định đongf đi mà IP packet sẽ đi trong mạng để đến được đích. Router sẽ lưu trữ một số đường đến với những đích mà nó biết trong routing tables. Khi mà một router nhận được gói tin nó sẽ nhìn vào trong routing tables của mình để tin tuyến đường tốt nhất để chuyển tiếp gói tin đó. Có hai cách routing được sử dụng hiện nay đó là:

- Dynamic Routing: Router sẽ sử dụng những dynamic routing protocol (OSPF) để chia sẻ thông tin định tuyến với các hop khác một cách tự động và xây dựng routing tables.

- Static Routing: Người quản trị mạng sẽ tự cấu hình tuyến đường đi cho gói tin.

Một tuyến đường sẽ chỉ cho router biết rằng là để gửi một gói tin đến một điểm đến X thì router nên gửi packet đó đến router nào tiếp theo. Nếu một router nhận được môt packet và nó không có đường đi nào khớp với địa chỉ đích của packet thì nó sẽ drop luôn packet (Khác với switch sẽ flood frames)

2.1 Path determination

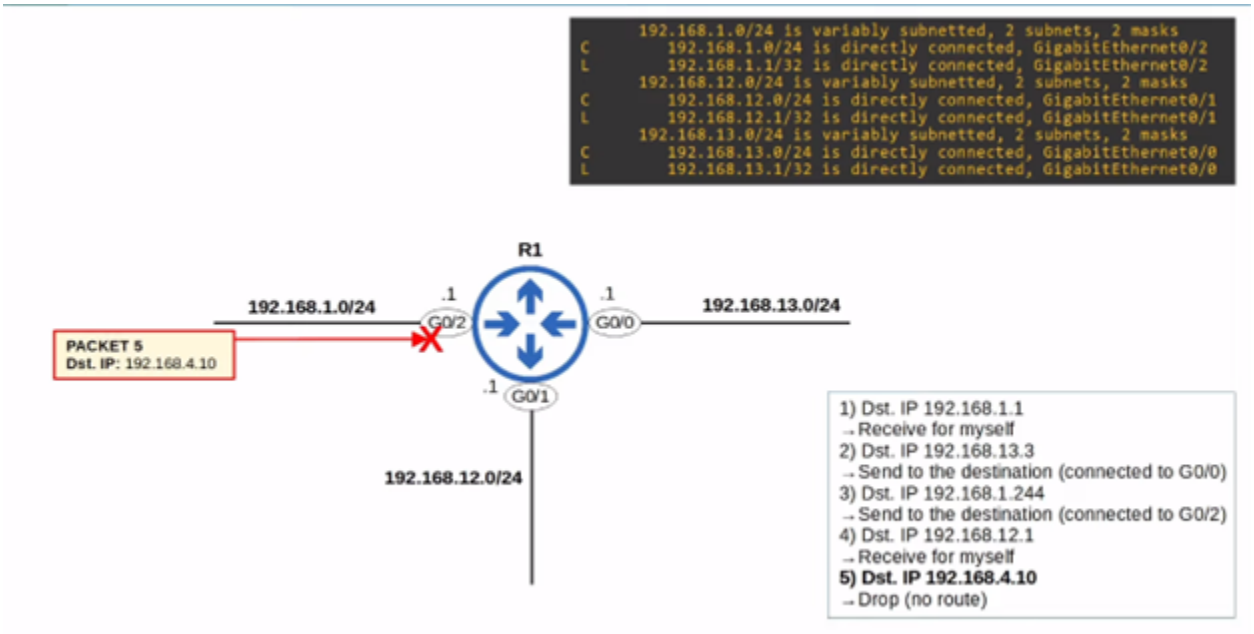


Hình 2: Path

Code sẽ thể hiện danh sách những protocol mà router sử dụng cho việc routing:

- L – local là đường đi đến chính interface của router.
- C – Connected là đường đi đến mạng mà interface của router được kết nối.

Dòng 192.168.1.0/24 is variably subnetted. 2 subnets, 2 masks có nghĩa là trong routing table có 2 đường đi đến cái subnet này với 2 netmask là /24 và /32.



Hình 3: Path

Khi packet thứ nhất có địa chỉ đích là **192.168.1.1** được gửi đến router R1 thông qua giao diện G0/2, đối chiếu với bảng định tuyến router 1 thấy được là **192.168.1.1** là local route vì vậy nó sẽ nhận packet đó cho mình luôn. Khi packet thứ 2 có địa chỉ đích là **192.168.13.3** được gửi đến router R1 qua

giao diện G0/2, đối chiếu với bảng định tuyến có tuyến đường connected với subnet là 192.168.13.0/24 thì router sẽ thực hiện forward gói tin thông qua giao diện G0/0.Khi packet thứ 4 có địa chỉ đích là 192.168.12.1 được gửi đến router R1 thông qua giao điện G0/2 đối chiếu với bảng dịnh tuyến có tuyến đường Local vì vậy R1 sẽ nhận packet cho mình luôn. Khi nhận được packet mà không xác định được địa chỉ đích R1 sẽ thực hiện drop luôn gói tin đó.

3 IP address

Địa chỉ IP là một logical address có độ dài là 32 bits là một địa chỉ ảo được gán cho một network interface của các network devices trong một mạng.

3.1 IP address class

Class	First octet	First octet numeric range
A	0xxxxxxx	0-127
B	10xxxxxx	128-191
C	110xxxxx	192-223
D	1110xxxx	224-239
E	1111xxxx	240-255

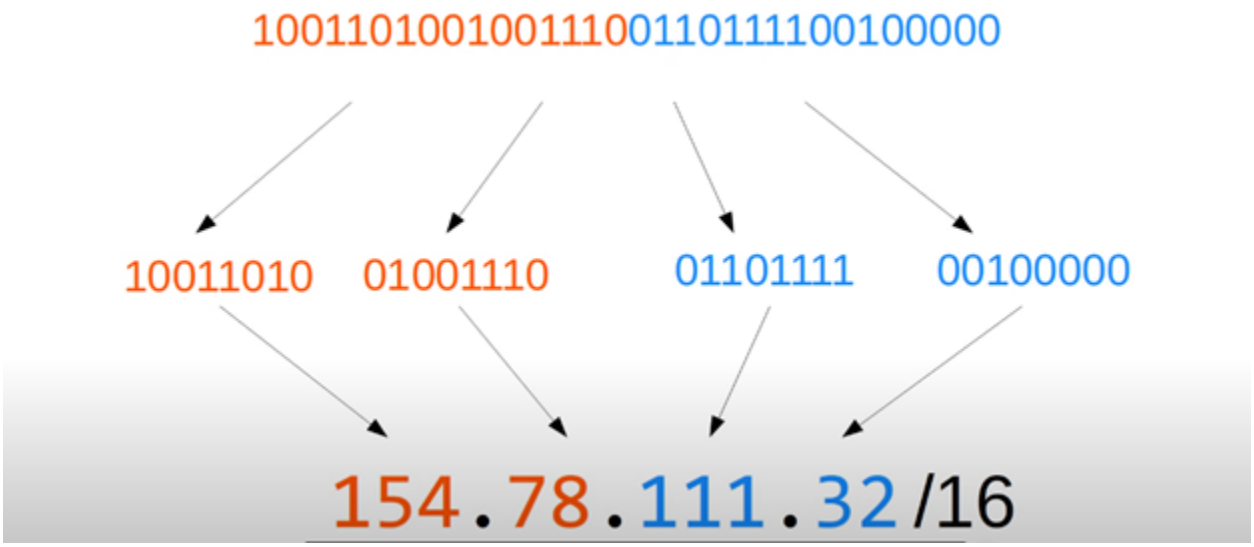
Hình 4: Ip class

Mỗi IP được phân vào các lớp dựa trên octet đầu tiên của từng địa chỉ IP. Tuy nhiên các lớp của địa chỉ IP sẽ chỉ được tập trung vào các class A, B, C. Class D sẽ được sử dụng để làm Multicast Address, class E sẽ được sử dụng cho các thí nghiệm và nghiên cứu. Ngoài cách chia class như trên ta có thể chia subnet hay là chia dải địa chỉ IP tùy theo mục đích sử dụng (trong mạng có bao nhiêu host cần kết nối) để tránh tình trạng lãng phí địa chỉ IP.

Class	First octet	First octet numeric range	Prefix Length
A	0xxxxxxx	0-127	/8
B	10xxxxxx	128-191	/16
C	110xxxxx	192-223	/24

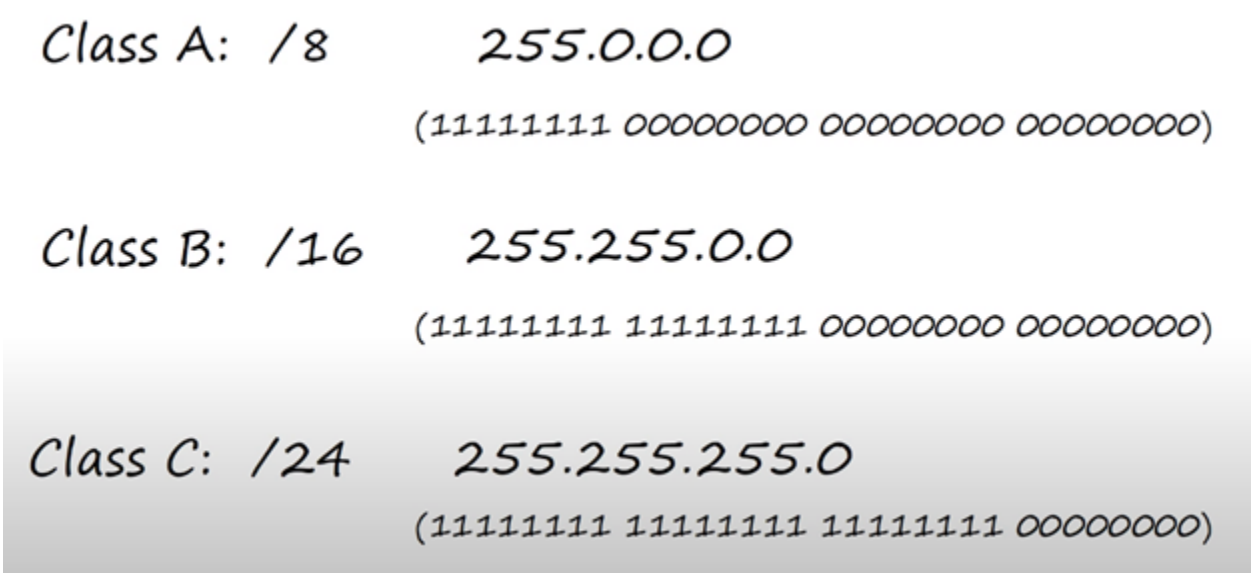
Hình 5: Ip-class

Mỗi class sẽ có tiền tố đặc trưng cho địa chỉ mạng và địa chỉ host. Ví dụ với Class A thì độ dài tiền tố sẽ là 8 bit đầu đặc trưng cho phần mạng còn 24 bit còn lại sẽ là đặc trưng cho phần host.



Hình 6: IP bit

Ngoài cách viết là /x ở đằng sau một địa chỉ IP để cho biết bao nhiêu bit là phần mạng bao nhiêu bit là phần host thì dựa vào địa chỉ netmask. Netmask có định dạng như là một địa chỉ IP với mỗi 8 bit sẽ được ngăn cách nhau bởi một dấu chấm. Tuy nhiên, ở netmask thì phần network sẽ được đánh dấu hết tất cả là 1 còn phần host sẽ được đánh đấu hết tất cả là 0. Dưới đây là netmask tương ứng với từng lớp địa chỉ IP.



Hình 7: Netmask

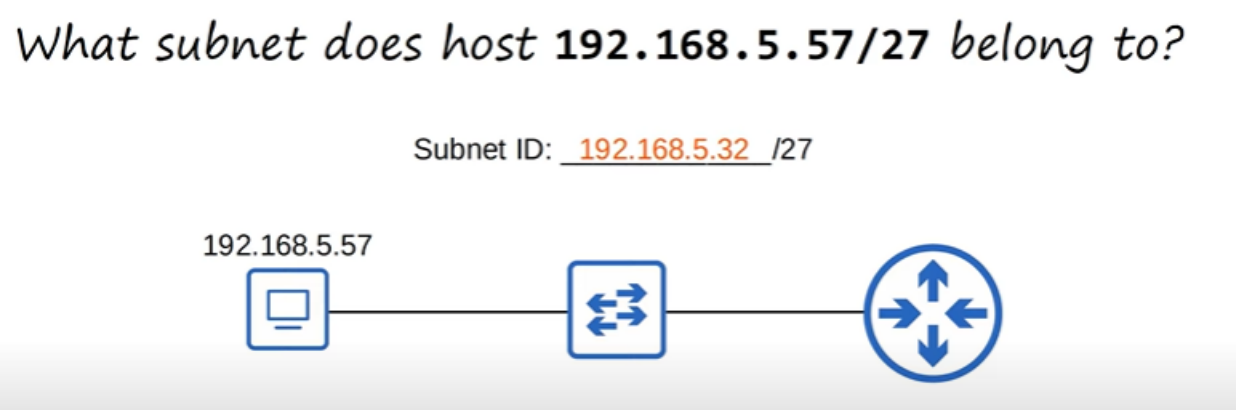
Thông thường, mỗi mạng sẽ có một địa chỉ riêng để xác định địa chỉ riêng của mạng thì ta giữ nguyên các bit phần mạng và tất cả các bit phần host sẽ được đặt là 0, ngoài ra mỗi mạng sẽ có một địa chỉ broadcast, ngược lại với địa chỉ mạng thì các bit phần host được đặt là 1. Ví dụ với gói tin có địa chỉ đích là 192.168.1.255 trong một mạng có địa chỉ mạng là 192.168.1.0/24 thì địa chỉ MAC tương ứng với gói tin này sẽ là **FFFF.FFFF.FFFF**.

4 Subnet calculation

Classless Inter-Domain Routing (CIDR): với CIDR các khái niệm như các class sẽ bị loại bỏ. Nó cho phép các mạng lớn sẽ được chia thành nhiều class nhỏ hơn để có thể tận dụng được tối ưu tránh lãng phí địa chỉ IP. Số host có thể trong một subnet được tính là $2^n - 2 vin Øccoilsbithost.$
$Variable - lengthsubetMask(VLSM)lqutrnhtonnccsubnetcsizekhcnhauØtndngtiØakhnggianØach.$

Ta sẽ thấy được rằng để có được 45 host mỗi subnet cần các subnet có 6 bit host. Lưu ý rằng mỗi bit mượn đằng sau sẽ được coi là 2 mũ x bit mượn subnet. Ta thực hiện chia như sau:

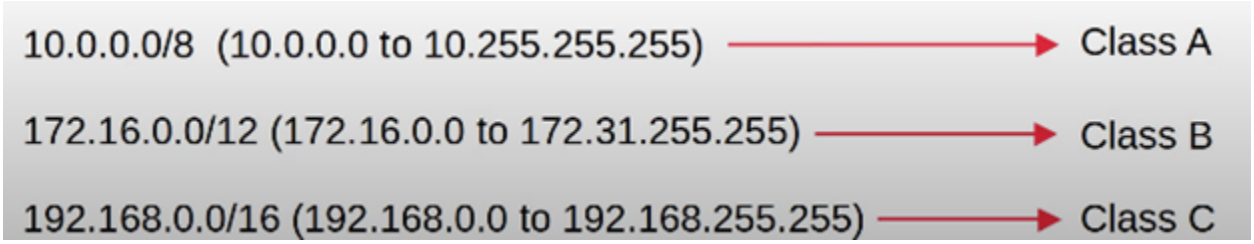
- Subnet 1: 192.168.1.0/26 (11000000.10101000.00000001.**00**000000)
- Subnet 2: 192.168.1.64/26 (11000000.10101000.00000001.**01**000000)
- Subnet 3: 192.168.1.128/26 (11000000.10101000.00000001.**10**000000)
- Subnet 4: 192.168.1.192 (11000000.10101000.00000001.**11**000000)



Hình 9: Subnet calculation

5 IP public, IP private, NAT

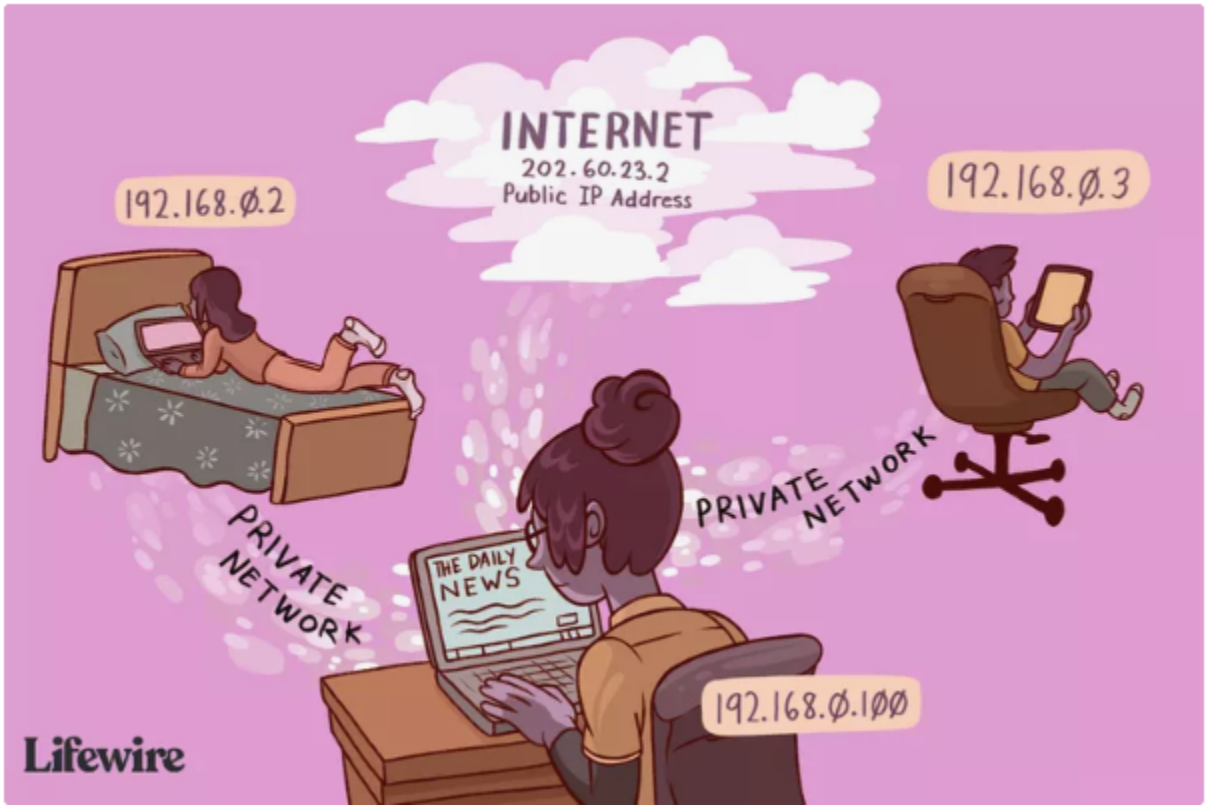
Public Ip là hay còn là địa chỉ IP công cộng thường được cấp bởi các ISP cho router ở nhà hay công ty hay là cho server để host một website có thể giúp các thiết bị kết nối với internet. Public IP là một địa chỉ độc nhất và không được trung với bất kì địa chỉ IP nào.
Private IP là một đại chỉ IP được gán cho các thiết bị phía sau một router. Với private IP thì các thiết bị trong nhà của mình cũng có thể có private Ip giống với các thiét bị ở trong nhà hàng xóm hay trong một công ty,....Đó là bởi vì Private IP là các địa chỉ non-routable. Các thiết bị phần cứng trên mạng được lập trình để ngăn chặn các thiết bị có private IP thực hiện kết nối, giao tiếp trực tiếp với các IP ngoài router mà router được kết nối đến. Bởi vì các private IP bị hạn chế việc kết nối với internet đó đó mà ta cần phải cần một địa chỉ để kết nối với thế giới bên ngoài đó chính là Public IP.
Một cái nhìn khác ta có thể coi router như là môt 'ISP' cung cấp các private IP cho các thiết bị trong nhà mà có kêt nối đến với router, ISP thật sự sẽ cấp cho router đó một public IP để giúp cho các thiết bị trong nhà có thể kết nối được internet thông qua cơ chế NAT. Theo RFC 1918, các địa chỉ IP thuộc dải sau được coi là IP private:



Hình 10: IP private

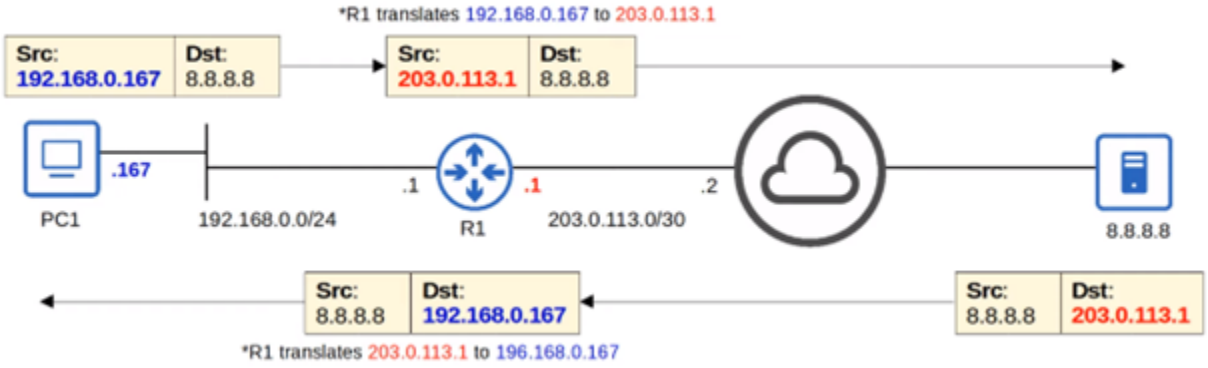
5.1 NAT

NAT (Network Address Translation) được sử dụng để điều chỉnh địa chỉ IP nguồn và địa chỉ IP đích của gói tin. Mục đích của việc sử dụng NAT là để cho phép các host với địa chỉ private IP có thể giao tiếp với host khác qua internet, qua đó ta có thể cho nhiều host bên trong mạng nội bộ có thể cùng share một địa chỉ IP public riêng.



Hình 11: NAT

Source NAT (SNAT):



Hình 12: SNAT

Khi một gói tin có địa chỉ nguồn là 192.168.0.167 và địa chỉ đích là 8.8.8.8 thì nhờ cơ chế SNAT R1 đã đổi địa chỉ nguồn của gói tin thành địa chỉ IP public 203.0.113.1 qua internet để đến server có địa chỉ IP là 8.8.8.8. Sau khi server nhận được gói tin, server gửi một gói tin hồi đáp với địa chỉ nguồn là 8.8.8.8 và địa chỉ đích là 203.0.113.1 qua internet để đến với R1. R1 thực hiện quá trình dịch địa chỉ IP 203.0.113.1 thành 192.168.0.167 để chuyển tiếp gói tin cho PC1.

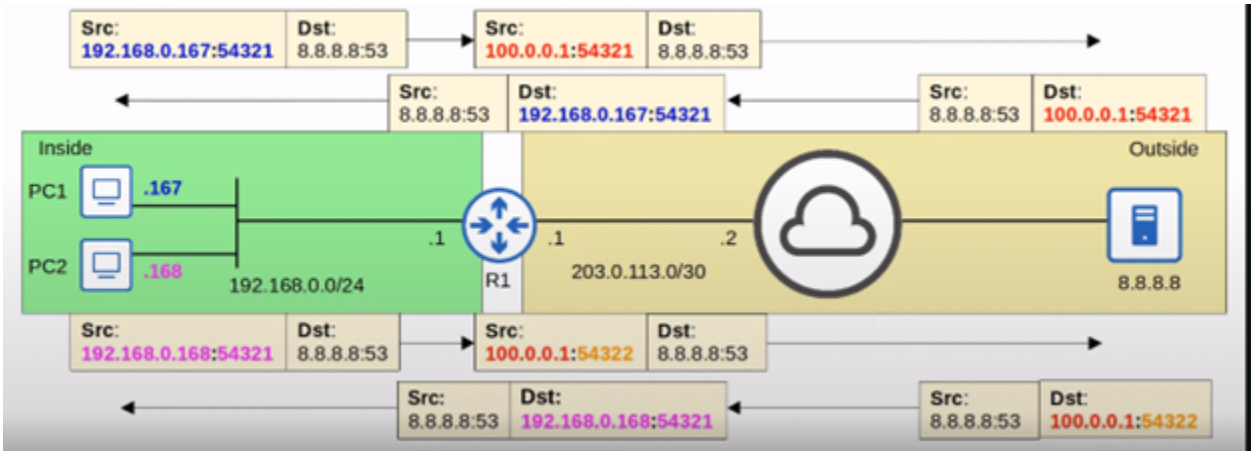
Static NAT: là cách cấu hình thủ công NAT bằng cách mapping 1-1 địa chỉ IP private và địa chỉ IP public. Một inside local IP address được mapped tới một inside global IP address. Inside local là địa chỉ IP ở trong mạng nội bộ thường là địa chỉ IP private còn inside global là địa chỉ IP ở host nhưng địa chỉ

này được sử dụng ở bên ngoài mạng thường là địa chỉ IP public. Static NAT sẽ cho phép thiết bị với một IP private có thể kết nối được với internet tuy nhiên việc yêu cầu mapping 1-1 sẽ khiến cho không còn địa chỉ IP public để sử dụng nữa.

Destination NAT: là được sử dụng để thay đổi địa chỉ đích trong IP header của packet. DNAT thường thay đổi port đích trong TCP/UDP header, thường được sử dụng để chuyển hướng incoming packet với một đích có địa chỉ hoặc port public thành địa chỉ private IP hoặc port bên trong mạng.

Dynamic NAT: router sẽ thực hiện mapping 'động' các inside local address thành các inside global address khi cần. Khi thực hiện Dynamic NAT thì sẽ phải cần ACL để xác định xem traffic nào sẽ được NAT. Nếu source IP address được cho phép bởi ACL thì source IP sẽ được NAT, còn nếu không thì sẽ không được NAT. NAT pool sẽ được sử dụng để chứa những inside global address dùng cho việc NAT. Mặc dù việc gán địa chỉ được thực hiện tự động nhưng Dynamic NAT vẫn là mapping 1-1 -> gây tốn địa chỉ public hoặc không NAT được nếu địa chỉ public trong pool được sử dụng hết. Nếu một gói tin từ một host trong mạng nội bộ cần NAT mà trong khi không có sẵn địa chỉ IP trong NAT pool thì router sẽ drop gói tin đó, và host đó sẽ không thể kết nối với internet cho đến khi có sẵn địa chỉ IP trong NAT pool.

PAT (Port address Translation) hay có thể gọi là NAT overload khi nó thực hiện dịch cả địa chỉ IP và địa chỉ cổng nếu cần thiết. Băng cách sử dụng một địa chỉ port đọc nhất cho mỗi phiên truyền dữ liệu, một public IP có thể được sử dụng bởi nhiều host thông qua các địa chỉ port khcs nhau (port number có 16 bits độ dài) .

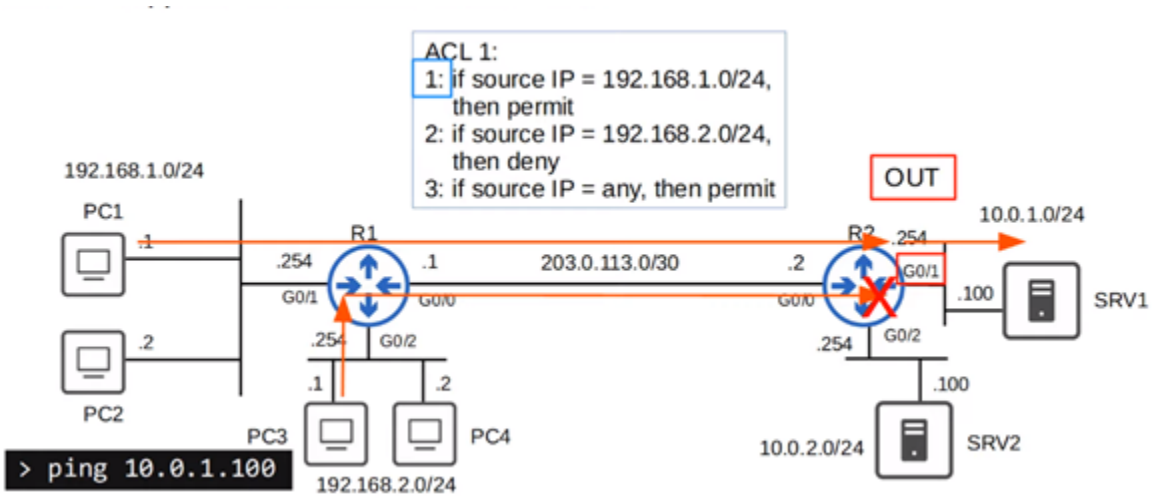


Hình 13: PAT

PC1 thực hiện gửi một gói tin với địa chỉ nguồn là 192.168.0.167:54321 và địa chỉ đích là 8.8.8.8:53, trong khi đó PC2 cũng thực hiện gửi một gói tin với địa chỉ nguồn là 192.168.0.168:54321 và địa chỉ đích là 8.8.8.8:53. Khi 2 gói tin này đến R1, R1 sẽ thực hiện dịch địa chỉ nguồn của gói tin đến từ PC1 là 100.0.0.1:54321 và thực hiện dịch địa chỉ nguồn của gói tin đến từ PC2 là 100.0.0.1:54322 (Sở dĩ có sự khác nhau về port là để khi mà server thực hiện phản hồi lại với một gói tin thì R1 sẽ biết được rằng là server thực hiện gửi gói tin cho PC1 hay là PC2). Khi nhận được gói tin thì server sẽ thực hiện gửi lại gói tin hồi đáp đến R1 và R1 sẽ thực hiện gửi về lại cho PC1 và PC2.

6 ACL(Access Controll List

Được coi như là một packet filter, chỉ dẫn cho router thực hiện cho phép hay không cho phép loại traffic nào đi qua. ACL có thể lọc được những traffic dựa trên địa chỉ IP đích và địa chỉ IP nguồn, địa chỉ port đích địa chỉ port nguồn. ACL được hình thảnh bởi các ACE(Access Control Entries) entries. ACL có thể được apply cho cả outbound vào inbound của một interface. Router sẽ check ACL theo thứ tự từ trên xuống dưới, nếu một packet mà match với một trong các ACE entries trong ACL thì router sẽ take action ngay lập tức và bỏ quả các etries còn lại.



Hình 14: ACL

Nếu một packet mà không match với entry nào trong ACL thì router sẽ deny luôn packet đó -> Implicit deny. Các loại ACL:

- Standard ACLs: Match based on **Source IP address** only
  - → Standard Numbered ACLs
  - → Standard Named ACLs

- Extended ACLs: Match based on **Source/Destination IP, Source/Destination port,** etc.
  - → Extended Numbered ACLs
  - → Extended Named ACLs

Hình 15: ACL2

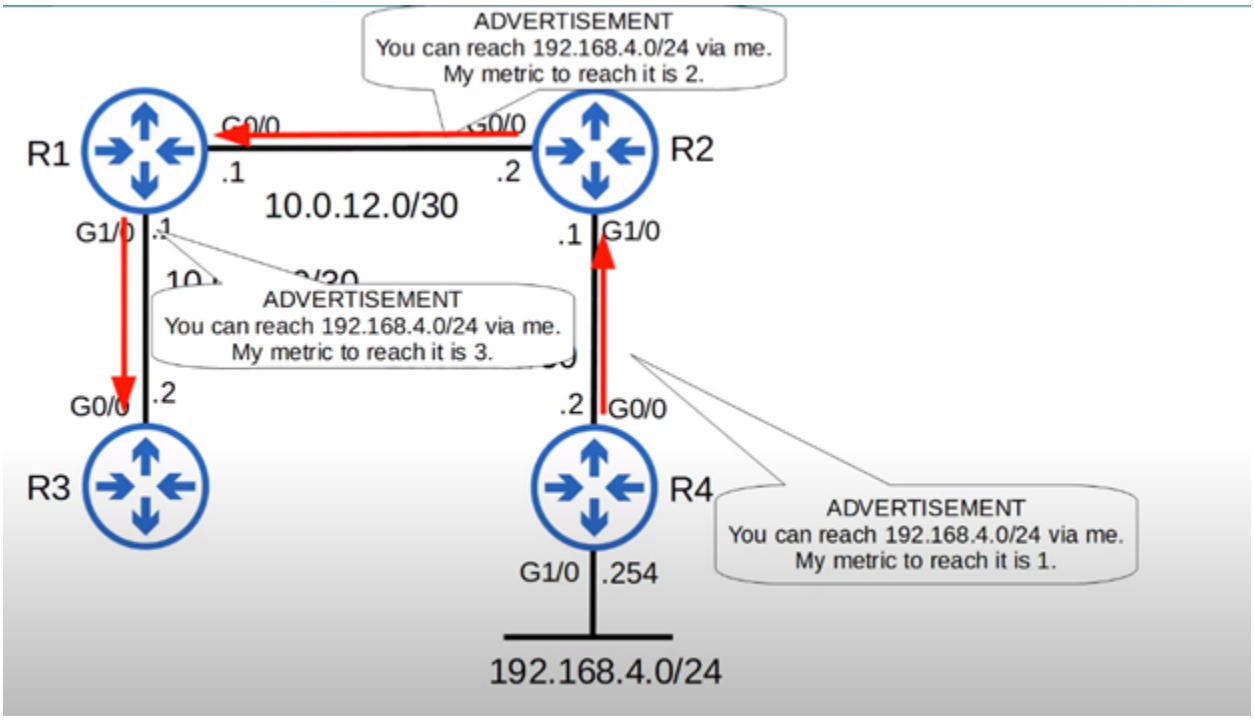
7 Link State Protocol và Distance Vector Protocol

7.1 Link State Routing Protocol

Khi sử dụng một link state routing protocol, mỗi một router cần tạo một 'connectivity map' của mạng, để cho phép điều đó, mỗi router sẽ quảng bá thông tin về interfaces nối với các nút lân cận của nó. Thông tin quảng bá này sẽ được đưa qua các router khác cho đến khi tất cả các router trong mạng đều phát triển được một mạng giống như nhau. Dựa vào mạng đó mỗi router sẽ tự tính toán đường đi tối ưu nhất để đi được đến đích. Linkstate sẽ tiêu tốn nhiều tài nguyên tính toán hơn do nhiều thông tin được chia sẻ. Tuy nhiên link state protocol lại có phản ứng nhanh hơn với bất kỳ những thay đổi nào trong mạng

7.2 Distance Vector Routing Protocol

Distance Vector protocol (RIP, EIRGP) được thực hiện bằng cách gửi những metrics routing (những mạng mà router đó đã biết và đặc điểm của đường đi để tới được mạng đó) tới trực tiếp những hop lân cận. Phương pháp này thực hiện chia sẻ route information cho các nút lân cận bởi lẽ router bình thường sẽ không thể nào biết được route information của các nút bên cạnh nếu các nút lân cận không nói cho nó biết. Được gọi là distance vector bởi vi router sẽ chi học khoảng cách và hướng (hướng tới next-hop) của mỗi route.



Hình 16: Distance Vector Protocol example

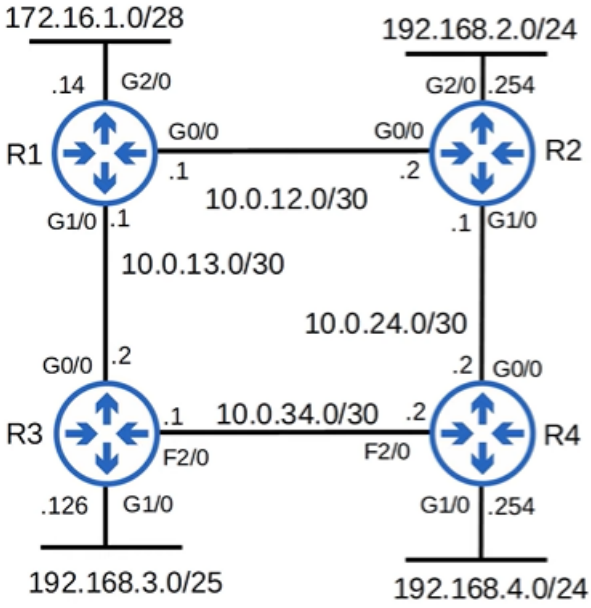
8 RIP

RIP (Routing Information Protocol) là distance vector protocol (sử dụng routing-by-rumor để học cũng như là share routes). RIP sử dụng hop count như là một metric của nó, một router sẽ được coi như là

một hop và không liên quan đến về băng thông. Ví dụ như kết nối 10Gb hay là 10Mb cũng chỉ được coi như là một hop. **Số lượng hop count tối đa là 15** (nhiều hơn thì sẽ được coi là không thể truy cập được và RIP sẽ không insert route đó vào routing table. Trong thực tế thì RIP thường không được sử dụng nhiều, nhưng có thể được sử dụng trong các mạng nhỏ. RIP có 2 version: RIPv1, RIPv2 được sử dụng cho Ipv4 ngoài ra thì còn có RIPng được sử dụng cho Ipv6. RIP sử dụng 2 loại message đó là:

- Request: Để yêu cầu RIP-enabled neighbor routers gửi routing table của nó
- - Response: để gửi routing table của các router đến với các neighbor router

RIP-enabled router sẽ gửi routing table của nó trong 30s/1 lần. Điều này có thể gây ra vấn đề khi mạng có nhiều routers bởi vì những update này có thể làm cho mạng bị chậm.
RIPv1: chỉ quảng bá các địa chỉ phân lớp (class A, class B, class C), không hỗ trợ CIDR, VLSM, không bao gồm thông tin quảng bá về subnet mask ở response message do chỉ quảng bá các địa chỉ phân lớp mà thôi (A/8, B/16, C/24), địa chỉ IP đía là địa chỉ broadcast: 255.255.255.255.
RIPv2: hỗ trợ VLSM, CIDR, bao gồm thông tin quảng bá về subnetmask. Các bản tin trong RIPv2 là bản tin multicast đến địa chỉ 224.0.0.9 (Multicast message là bản tin được gửi đi và chỉ được nhận bởi các thiết bị tham gia vào một multicast group nào đó mà thôi).



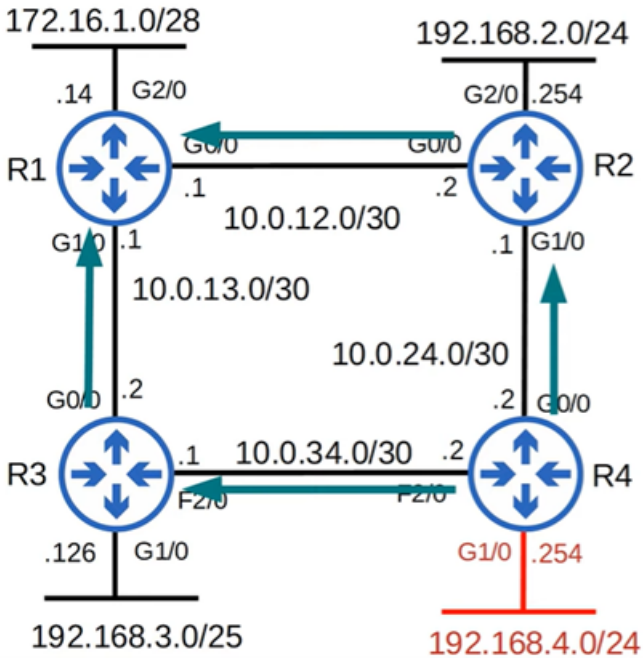
Hình 17: RIP

Một điểm lưu ý nữa là trong topo mạng trên thì khi G0/0 và G1/0 của R1 được kích hoạt RIP thì nó sẽ quảng bá routing table đến các router lân cận là R2 và R3. Tuy nhiên nếu như G2/0 cũng được kích hoạt RIP nhưng lại không có router lân cận thì nó vẫn sẽ gửi routing table. Điều này sẽ tạo ra những traffic 'useless' ta phải configure interface đó là **passive interface** để ngăn chặn.

9 OSPF

OSPF (Open Shortest Path First) là một thuật toán link state sử dụng thuật toán Dijkstra để tìm đường đi ngắn nhất. Router sẽ lưu thông tin về mạng trong LSAs (Link State Advertisements) được tổ

chức ở trong Link State Database. Router sẽ **flood** LSAs cho đến khi tất cả router trong khu vực sử dụng OSPF khám phá và tạo được một mô hình mạng giống nhau.



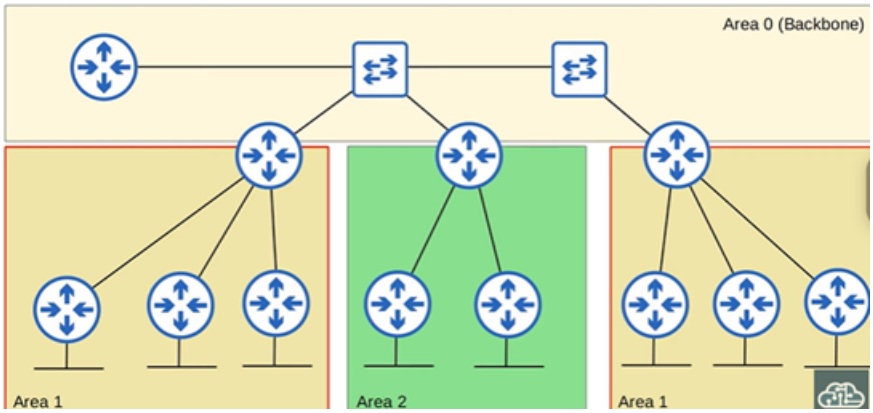
Hình 18: OSPF

Diễn tả về LSA flooding ta có mô hình mạng như sau: Để thêm một kết nối mới với G1/0 của R4 thì R4 sẽ tạo ra một LSA để nói với các router lân cận về đoạn mạng ở interface R4. LSA sẽ được flood trong mạng cho đến khi tất cả router đều nhận được nó. Kết quả là các router đều share chung một LSBD. Mỗi router sẽ sử dụng thuật toán Shortest Path First để tìm được đường đi tốt nhất đến subnet 192.168.4.0/24. Mỗi LSA sẽ có thời gian sống tối đa vào khoảng 30 min, LSA sẽ được flood lại nếu như hết khoảng thời gian trên.

9.1 OSPF area

OSPF sử dụng 'area' để chia mạng. Trong một mạng lớn có khoảng hàng trăm router thì việc chia nhỏ ra thành từng vùng mạng nhỏ sẽ giúp router tránh khỏi việc mất nhiều thời gian để tính toán đường đi cũng như flood LSA.

Area trong OSPF được định nghĩa là một danh sách các router và các đường dẫn cùng chia sẻ một LSDB. **Backbone area** là một vùng mà tất cả các area khác phải kết nối vào. Router với tất cả interface được đặt trong cùng một area thì được gọi là **internal router**. Còn router có interface nằm ở nhiều area thì được gọi là **area border routers (ABRs)** . Mỗi ABR sẽ lưu giữ LSDB cho mỗi area mà interface của chúng được kết nối đến. Router mà kết nối với backbone area được gọi là **backbone router**. Một **intra-area route** là một route đến một đích nằm trong cùng một OSPF area, **interarea route** là một route đến đích nằm ở OSPF area khác. Lưu ý trong OSPF thì các area phải contigous . Tức là tất cả các router phải cùng chung một vùng và chỉ có 1 kết nối đến backbone area mà thôi. Ngoài ra OSPF có interface nằm cùng trong một subnet thì phải ở cùng một area.



Hình 19: OSPF area

9.2 OSPF metric và OSPF neighbor

OSPF metric được gọi là **cost** . Nó được tự động tính toán dựa vào speed của interface
OSPF neighbor: khi mà một router trở thành OSPF neighbor, nó sẽ tự động làm những việc như chia sẽ thông tin về mạng, tính toán đường đi,....Khi OSPF được activated ở interface thì router sẽ bắt đầu gửi OSPF hello message ra interface đó trong một khoảng thời gian được định nghĩa bởi hello timer. Điều này để khiến cho router có thể tìm được các OSPF neighbor, bằng cách trao đổi messages các router sẽ kiểm tra xem router này hay router kia có thể trở thành OSPF neighbor được không. Hello messages là một bản tin multicast đến 224.0.0.5 (địa chi multicast của tất cả OSPF router). OSPF message là một bản tin được đóng gói bởi IP header có giá trị 89 ở trường Protocol. Trong bản tin Hello có 2 trường quan trọng là router ID và neighbor ID

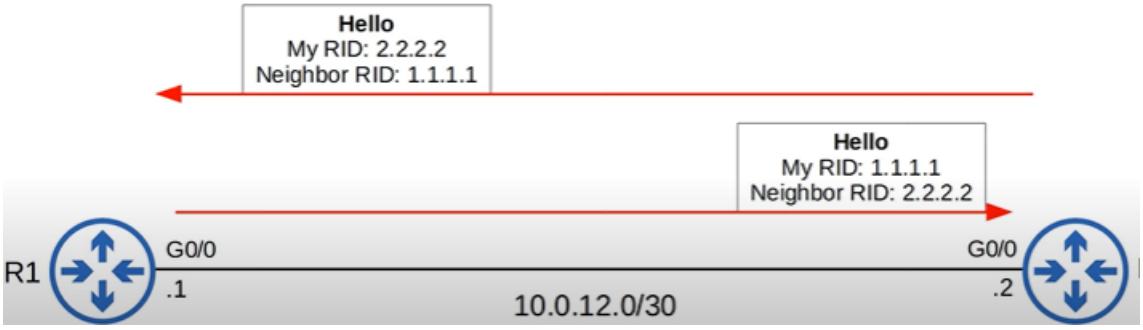
9.3 OSPF state

Để OSPF router trở thành neighbor thì nó phải trải qua nhiều trạng thái:

1. Down là trạng thái mà router không biết rằng xung quanh mình có OSPF router nào khác hay không

2. Init state: là trạng thái mà OSPF router đã nhận được hello message từ router và thêm một entry cho router đó vào OSPF neighbor table.

3. 2-way state là trạng thái mà router sẽ nhận được một bản tin mà có RID của chính nó trong đó. Sau trạng thái này các router sẽ được coi là OSPF neighbor của nhau và có thể share LSA để xây dựng được một LSDB.



Hình 20: 2 way state

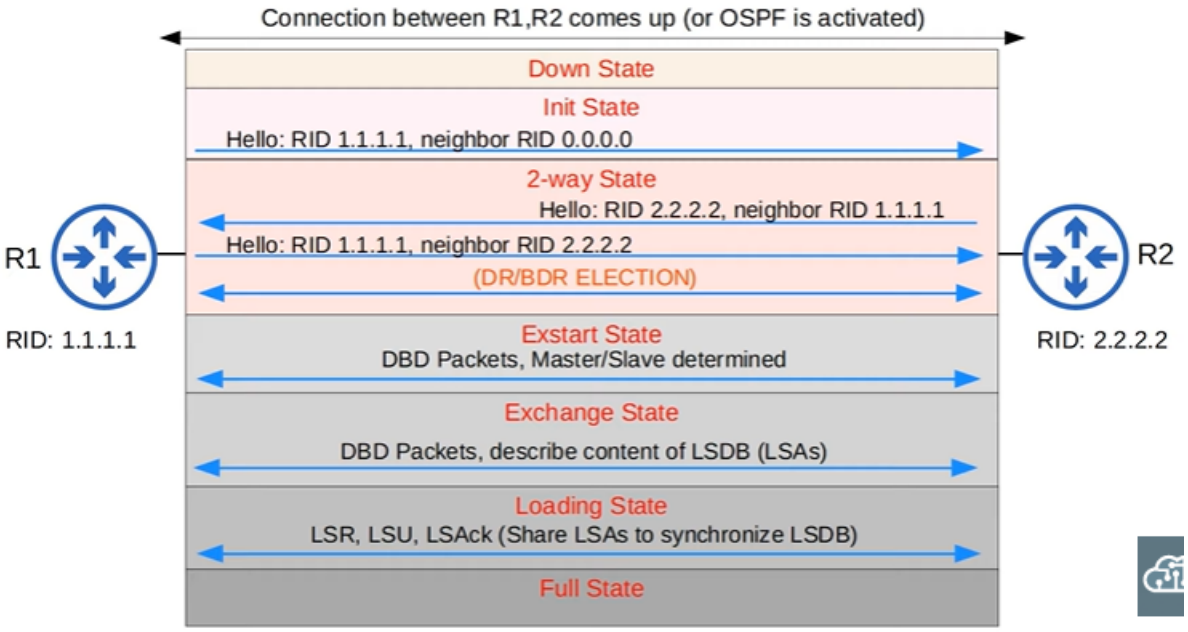
4. Sau bước trên, 2 router sẽ chuẩn bị để trao đổi thông tin về LSDB. Trước khi trao đổi thông tin thì nó phải chọn đâu là router thực hiện trao đổi trước. 2 router sẽ thực hiện điều này ở trạng thái Exstart state. Router với RID cao hơn sẽ trở thành Master và khởi tạo phiên trao đổi, router có RID bé hơn sẽ trở thành Slave. Để quyết định xem ai là Master ai là Slave 2 router thực hiện trao đổi bản tin DBD (Database Description).

5. Ở trạng thái tiếp theo là exchange thì router sẽ trao đổi DBDs (chứa một danh sách LSA trong LSDB, DBD chỉ chứa những thông tin cơ bản của LSA chứ không bao gồm thôm tin chi tiết) để nói cho neighbor rằng nó đang có LSA nào. Router nhận được DBD và sẽ thực hiện so sánh thông tin LSDB của chính nó và xác định xem LSA nào nó nên nhận từ neighbor.

6. Trạng thái tiếp theo là Loading state, router gửi Link State Request (LSR) message để request cho các neighbor của nó gửi LSA nào mà nó chưa có. LSAs được gửi thông qua LSU (Link State Update) message. Router nhận được sẽ gửi lại LSAck message đê thông báo rằng nó đã nhận được LSAs.

Hình 21: Loading State

7. Trạng thái cuối cùng là Full state, trong trạng thái này các router đã thực hiện xây dựng xong LSDB của nó. Tuy nhiên các router vẫn sẽ tiếp tục gửi và nghe Hello packet (10s một lần) để giữ các neighbor lân cận. Mỗi khi Hello packet được nhận thì 'Dead' timer (default 40s) sẽ được reset khi mà timer được đếm hết thì neighbor sẽ bị remove. Router sẽ tiếp tục trao đổi LSA để hoàn thiện được LSDB.



Hình 22: All state