MINH HỌA CÁC KHÁI NIỆM CCNA
CHO NGƯỜI MỚI DỄ HÌNH DUNG

Lưu ý ebook này dùng các ví dụ thực tế tương tự để giải thích các khái niệm về mạng, giúp người mới dễ hiểu, chứ không 100% khớp với các khái niệm về mạng.

Người học sau khi nắm khái niệm cần thực hành trên thiết bị (EVE-NG, GNS3, Packet tracer hoặc thiết bị thật) để hiểu rõ cách cấu hình và xử lí lỗi.

Tham gia nhóm Chia sẻ kiến thức, Xử lí lỗi quản trị mạng cho người mới bit.ly/lab-network

Mục Lục

1.Mô hình OSI 3
2. Vì sao cần chia Subnet 5
3. So sánh static route và dynamic route 6
4. So sánh IP private và IP public 7
5. NAT 8
6. Switch layer 2 và router 9
7. Telnet 11
8. Chia VLAN và Chia subnet liên quan gì tới nhau 12
9. OSPF (Thuật toán link state) 12
10. EIGRP (Thuật toán distance vector) 13
11. ACL (Access control list) 14
12. ARP 15
13. Quality of Service 16
14. Spanning Tree 16
15. Boardcast 18

1.Mô hình OSI

Xem video OSI dễ hiểu ở bài 1 (free) ở đây bit.ly/hai-ccna

Các thiết bị mạng hoạt động theo mô hình này để truyền tải thông tin sang host đầu xa. Ví dụ khi ta soạn 1 mail trong outlook để gửi.

Tầng application chính là phần mềm outlook. Khi ta mở outlook ra soạn mail, ta viết các text rồi paste hình ảnh vào mail, thì việc outlook chấp nhận các text , hình ảnh này do tầng presentation cho phép, tầng này bao gồm chữ và hình ảnh được sử dụng, ví dụ chữ có thể đậm, gạch dưới, in nghiêng, ảnh có thể dạng png, jpeg...Tầng này chưa liên quan đến kết nối mạng. Sau khi soạn xong email, chỉnh font chữ vừa ý rồi thì ta bấm nút send.

Sau khi bấm send, bản tin sẽ được đẩy xuống tầng session (session layer) , nó chuẩn bị các thông tin như ip đích của mail server, port(25,110,587.v.v...), kèm với nội dung mail. Sau đó gửi xuống tầng transport.

Lúc này tầng transport sẽ cắt nội dung mail thành các phần nhỏ và dán số port đích, port source(ngẫu nhiên), số thứ tự vào mỗi phần nhỏ đó (gọi là các gói tin), và chuyển xuống tầng network.

Tầng network thực hiện việc tìm nexthop để đẩy gói tin đi (dựa vào bảng routing-table). Sau khi tìm ra nexthop, gói tin được đẩy xuống tầng data link layer, tại đây thực hiện việc dán địa chỉ mác cổng thiết bị hiện tại và mác đích (mác của cổng router phía trước), dán xong thì packet được gọi là frame.

Frame sau đó được biến đổi thành tín hiệu điện tử và truyền đi trên dây mạng (phần điện tử kĩ sư mạng biết vậy thôi chứ không rõ biết cụ thể dạng tín hiệu như nào, vì nó thuộc phần công nghệ viễn thông, không cần nắm sâu)

Khi tín hiệu điện tử đến thiết bị đầu xa, nếu là router nó được phục hồi thành frame, rồi router sẽ remove mac source/mac đích đi; từ đó router check xem IP đích là gì và tiếp tục quy trình như trên để chuyển đến đích.

Nếu gặp thiết bị switch thì tín hiệu phục hồi thành frame, và switch check xem địa chỉ mác đích ở đâu, rồi tra trong bảng mac table, rồi forward frame đến mác đích.

Cứ như vậy tín hiệu đến được thiết bị đích và được phục hồi ngược lại thành frame—> packet —-> lắp lại thành segment—> thành bản tin dạng đọc được và hiển thị lên application.

2. Vì sao cần chia Subnet

Một cách hình dung đơn giản về việc cần chia subnet cho các bạn sinh viên mới học:

- Ta tưởng tượng 1 khu chung cư có 10 tầng

- Với mỗi tầng sẽ có các phòng => Cần đánh số cho nó (tương tự như gán địa chỉ IP cho các máy tính)

- Ta quy hoạch tầng 1 , các phòng sẽ bắt đầu từ 101 đến 198, còn số 100 được quy hoạch để chỉ toàn bộ các phòng của tầng 1, ta có thể gọi là"dãy 100"

Tương tự cho tầng 2 là 201 đến 299...Và khi nói "dãy 200" được dùng để chỉ các phòng thuộc tầng 2.

Với mỗi số phòng này tương tự với 1 địa chỉ IP (ví dụ 192.168.1.101), còn khi ta nói "dãy 100" , "dãy 200" => tương đương với địa chỉ network 192.168.1.0, 192.168.2.0

Ở mỗi tầng sẽ dành ra số cuối (ví dụ 199, 299) để làm phòng truyền thông, có các phương tiện như loa phát thanh, khi BQL tòa nhà muốn thông báo gì đó đến toàn bộ các phòng; thì chỉ việc đến phòng đó và

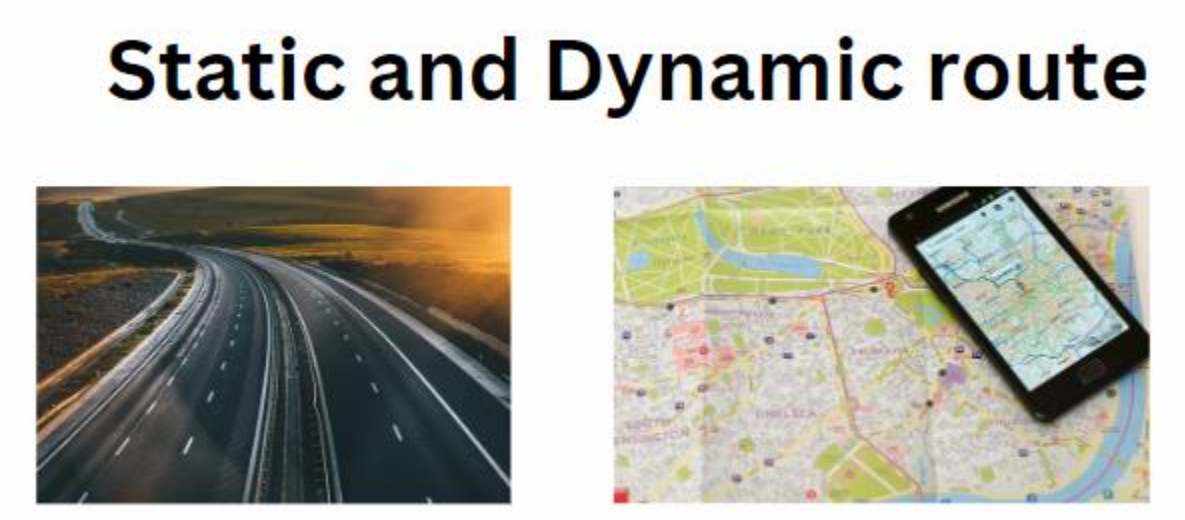
gọi loa => phòng 199 , 299... này giống như địa chỉ broadcast (ví dụ 192.168.1.255/24)

Như vậy ta thấy việc quy hoạch 1 khoảng số (cho mỗi tầng) làm việc quản lí dễ ràng hơn, dễ tìm địa chỉ phòng, ví dụ 215 là biết tầng 2., 110 là biết tầng 1... Ngoài ra tránh nguy cơ đánh địa chỉ sai, trùng lặp số phòng...

Tương tự việc phân chia 1 khối IP to thành nhiều phần, mỗi phần gán cho 1 phòng ban riêng sẽ giúp người quản trị dễ quản lí, ví dụ: dải 192.168.1.0/24 cho phòng KeToan, thì nhìn vào 1 IP 192.168.1.100 là biết user của phòng ketoan.

Ngoài ra còn có thể tăng tính bảo mật : ví dụ cấm các phòng khác nhau truy cập sang nhau....

3. So sánh static route và dynamic route

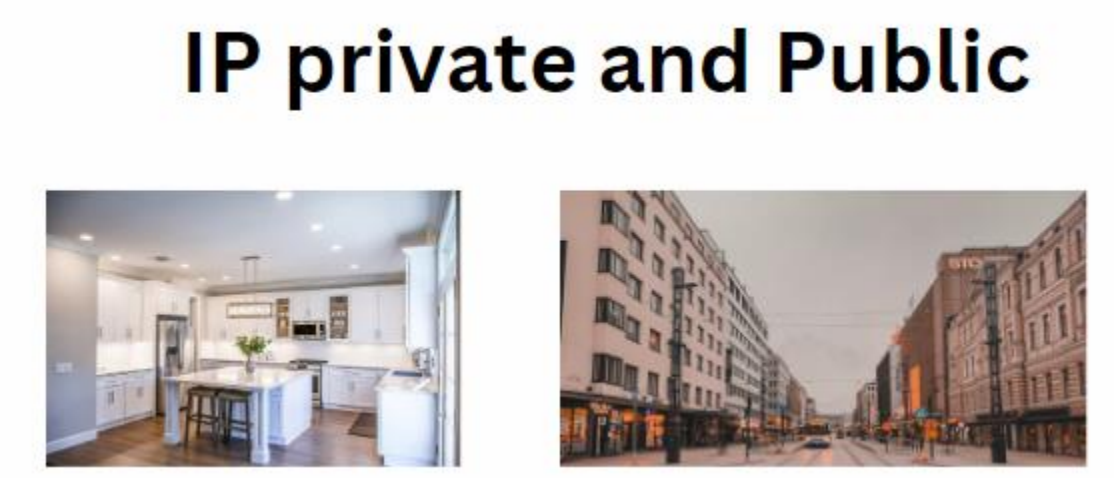


Khi bạn đi từ nhà tới nơi làm việc, bạn có thể đi 1 đường mình thích và quen thuộc nhất hoặc là bạn mở google map ra và xem đoạn đường nào tới công ty bị tắc nhất để tránh.

Tôi hay đi đường nào quen thuộc nhất mà không cần xem google map (tương đương với static route), đi nhanh mà không phải nghĩ (đỡ tốn cpu) ,nhưng có thể gặp tắc đường hoặc đường đang sửa , hoặc sự cố…thì sẽ phải chấp nhận chờ hết tắc mới đi tiếp.

Nếu trước khi đi tôi dùng google map xem trước, tìm đoạn nào ngắn nhất, ít tắc nhất…tương ứng với định tuyến động, các thông tin về tắc, độ dài tương ứng với metric trong giao thức dùng để tính chi phí. Chi phí của tuyến nào nhỏ nhất sẽ được chọn. Tuy hơi tốn time tính toán nhưng bù lại tìm được đường ổn nhất.=> tương tự định tuyến động

4. So sánh IP private và IP public



IP private tương tự như địa chỉ của các đồ vật trong nhà riêng của bạn, chỉ các thành viên trong gia đình của bạn mới biết và có thể tìm được. Ví dụ cái tivi thì ở địa chỉ “phòng khách”, cái bàn ở địa chỉ ”trong bếp”, cái áo ở “trong tủ”. Những địa chỉ như này chỉ có người trong nhà biết, còn ví dụ khi bạn mua hàng trên shopee bạn không đặt địa chỉ

nhận hàng là “trong bếp” được. Vì “trong bếp” là quá chung chung, nhà nào cũng có bếp. Bạn phải chỉ rõ địa chỉ nhà trên bản đồ google map chả hạn.

Trong khi đó, IP public (ví dụ 203.112.1.1) giống như địa chỉ nhà của bạn trên bản đồ, để shiper mang hàng đến, là địa chỉ duy nhất, không nhà ai trùng nhà ai cả.

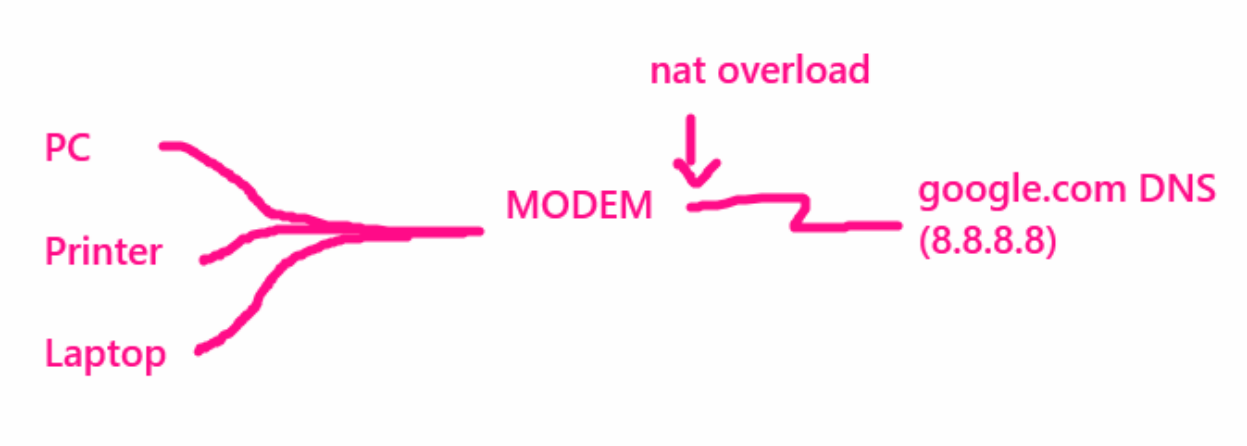
Khi bạn gửi đồ vật cho 1 người bạn của mình, bạn ra bưu điện chuyển phát cũng cần ghi địa chỉ nhận là đị chỉ public của họ, chứ không được ghi địa chỉ như “bếp nhà bạn A”, “phòng khách nhà bạn B”. Và địa chỉ gửi bạn cũng cần ghi địa chỉ public của nhà bạn. Tương tự khi các gói tin đi trên internet, cả địa chỉ gửi và nhận đều phải là ip public.

5. NAT

Trong ví dụ trên, khi ta gửi 1 đồ vật từ trong bếp (private address) đến nhà 1 người bạn ở xa. Thì ta cần điền địa chi gửi là địa chỉ public trên bản đồ của nhà ta, còn địa chỉ gửi cũng là địa chỉ public của nhà người bạn.

Trong mạng máy tính, khi ta ping từ địa chỉ máy tính 192.168.1.10 (private) đến địa chỉ public , ví dụ 8.8.8.8. Thì việc biến đổi ip 192.168.1.10 thành ip public của nhà , gọi là NAT (network address translation)

Và do trong nhà có nhiều IP private như máy in, laptop, PC… nên khi đi ra ngoài internet, nó sẽ chung 1 IP public của nhà, đây gọi là NAT Overload (được thực hiện trên modem mạng của nhà)



6. Switch layer 2 và router

- Khi nhà bạn là một căn ở trong 1 tầng của chung cư, các nhà trong tầng đó ở 2 bên hành lang, bạn muốn đi sang các nhà khác chơi, bạn chỉ cần đi ra hành lang rồi vào gõ cửa nhà muốn vào, họ mở cửa cho bạn vào. Các nhà trong tầng này sẽ được đánh số liền nhau, với số 1 ở đầu, ví dụ nhà bạn là đầu xóm , đánh số 100, cho tới nhà cuối là 120. (đây gọi là dải số 1xx)

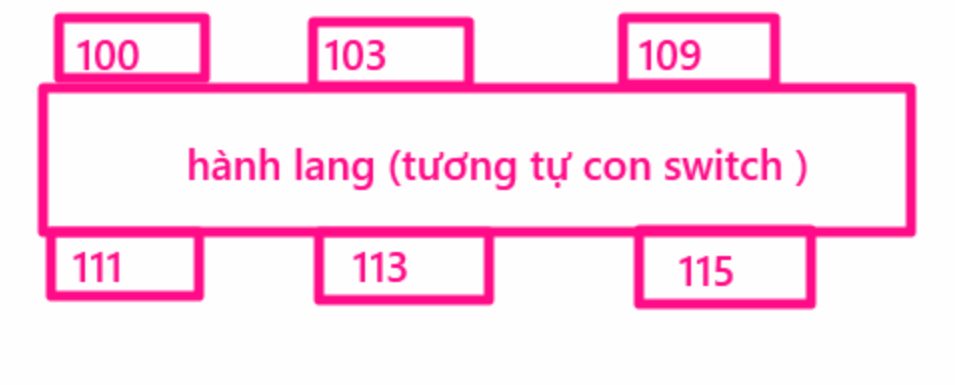
- Tương tự, các tầng khác cũng dùng dải số 2xx

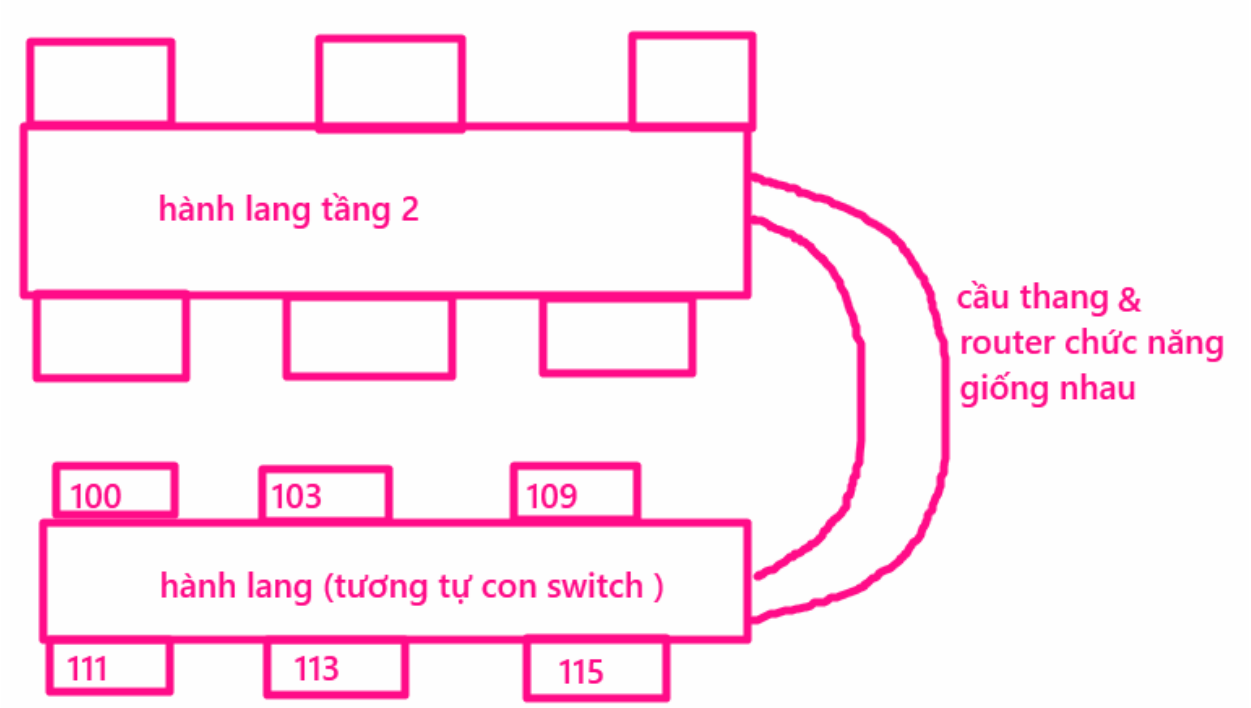
- Switch layer 2 cũng giống như cái hàng lang của mỗi tầng, các nhà trong tầng khi cần giao tiếp chỉ cần đi ra hành lang rồi có thể vào nhà khác.

- Các thiết bị cắm vào cùng 1 switch layer 2 chỉ cần đặt địa chỉ IP thuộc cùng 1 dải là giao tiếp được với nhau

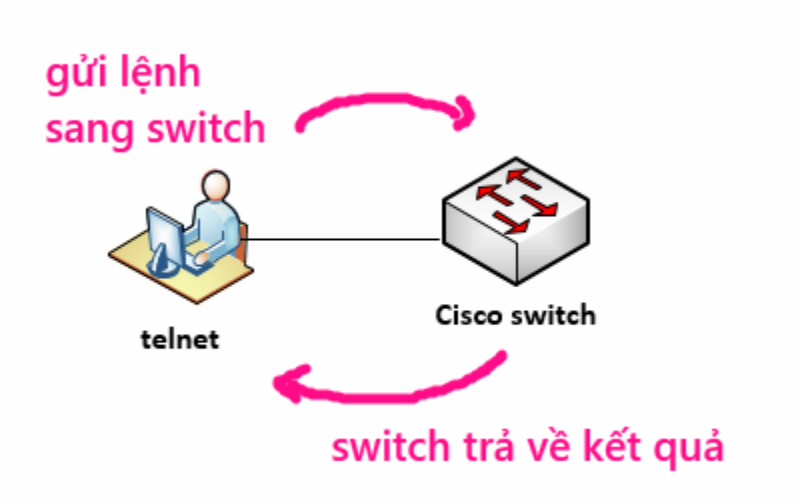
- Khi bạn từ tầng 1 muốn lên căn phòng có địa chỉ 205, thuộc tầng 2. => thì bạn phải ra thang máy hoặc (cầu thang bộ) để chuyển lên hành lang tầng 2, rồi mới tìm đến phòng 205.

=> Router giống với cái cầu thang (hoặc thang bộ), dùng để di chuyển giữa các IP của dải mạng khác nhau, ví dụ từ 192.168.1.10 lên 192.168.2.20


100
103
109
hành lang (tương tự con switch)
111
113
115


hành lang tầng 2
cầu thang &
router chức năng
giống nhau
100
103
109
hành lang (tương tự con switch)
111
113
115

7. Telnet



Telnet là giao thức truy cập từ xa, ví dụ có 1 người ngồi từ xa với 1 máy tính thông mạng với thiết bị, Người đó dùng giao thức telnet để gửi các lệnh tới thiết bị, ví dụ lệnh show run, show ip int brief… Sau đó switch trả về kết quả của các lệnh, hiển thị trên màn hình máy tính của người đó.

Tương tự với việc 2 người nói chuyện ở nơi công cộng, người A hỏi gì và người B trả lời nấy. Tuy nhiên giao tiếp kiểu này có 1 nhược điểm là các thông tin nhạy cảm sẽ bị xung quanh nghe thấy, ví dụ người A hỏi người B mật khẩu vào máy tính là gì, để người A mượn 1 lúc…Để an toàn thì người A và B có thể chuyển sang nhắn tin bằng điện thoại, xung quanh sẽ không nghe được họ trao đổi gì.

Tương tự thì các bản tin trao đổi bằng giao thức telnet sẽ ở dạng thuần text, và các phương tiện bắt gói như wireshark sẽ nhìn thấy toàn bộ nội dung trao đổi. Vì vậy nên dùng SSH để đảm bảo an toàn, vì thông tin SSH đã được mã hóa trên đường truyền, có bắt được gói thì cũng không hiểu được nội dung.

8. Chia VLAN và Chia subnet liên quan gì tới nhau

Khi công ty có nhiều phòng ban thì mỗi phòng ban sẽ được chia ra thành 1 VLAN nào đó, ví dụ ketoan vlan 100, NhanSu vlan 200,…

mục đích để thu nhỏ miền broadcast , ví dụ như 1 máy trong vlan bị virus, nó auto lây sang toàn bộ vlan đó thì các máy cùng vlan sẽ bị nhiễm, còn các máy khác vlan thì khả năng bị nhiễm khó hơn.

Mỗi vlan sẽ gồm các port trên switch, ví dụ các máy Ketoan cắm vào port 10,11,12,15 sẽ cho vào vlan 100.

Nhưng câu hỏi đặt ra là chia subnet và chia VLAN có liên quan gì nhau không? => Câu trả lời là nó ĐI ĐÔI VỚI NHAU. Chẳng hạn như sau khi quy hoạch vlan 100 cho KeToan, vlan 200 cho NhanSu, thì bạn đặt IP cho mỗi phòng ban như nào, chả lẽ lại chung 1 subnet là 10.0.0.0/8 ? (thực tế là không đặt chung subnet được)

=> Câu trả lời là mỗi phòng ban vừa cần 1 VLAN khác nhau, vừa cần dải IP phải khác nhau.

Ví dụ ketoan , vlan 100, dải IP là 10.0.1.0/24

vlan 200, Nhan Su, dải IP là 10.0.2.0/24

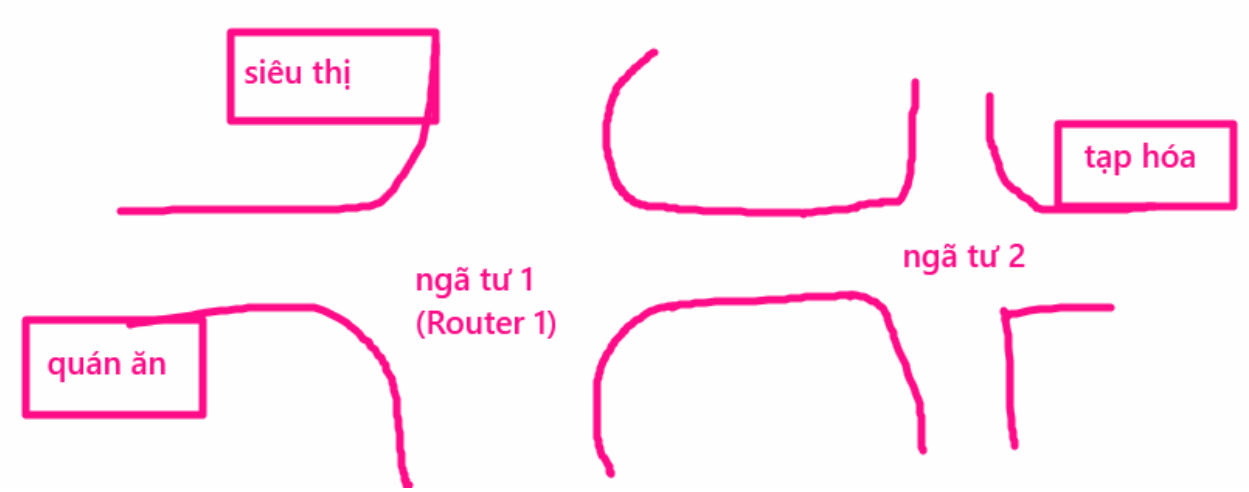
9. OSPF (Thuật toán link state)

Ta có thể coi mạng máy tính như 1 thành phố, gồm các ngã tư, tại mỗi ngã tư có thiết bị chỉ đường cho các thiết bị có thể đến đích (thiết bị này tương tự router). Đích ở đây có thể là các nhà hàng, quán ăn, siêu thị ở 2 bên đường.

Các thiết bị tại ngã tư sẽ gửi cho nhau các mảnh nhỏ thông tin , nội dung là về khoảng cách từ ngã tư tới các đích như nhà hàng, siêu thị…ở trên đoạn đường nối trực tiếp với ngã tư đó. (Tương tự như LSA trong OSPF, chứa các cost từ router tới các dải mạng LAN connected trực tiếp với nó, và IP của các port router, area…)

> Kết quả là mọi thiết bị ở ngã tư đều có các mảnh thông tin giống nhau. (Trong OSPF gọi là LSDB database)

Dựa vào các mảnh thông tin đã được đồng bộ, các router sẽ tính đường đi tốt nhất đến mọi đích trên bản đồ mạng.



Lưu ý là OSPF tuy gọi là thuật toán link-state, nhưng các mảnh thông tin nó gửi cho nhau không chứa các state như đường nào đang nghẽn, băng thông đang dùng là bao nhiêu, từ đó việc chọn đường nhiều khi không thực sự tối ưu khi nhiều đường cao tải giờ cao điểm, nhưng vẫn được chọn=> Đây là 1 nhược điểm của các thuật toán định tuyến truyền thống, và được cải thiện trong công nghệ SDWAN.

10. EIGRP (Thuật toán distance vector)

Trong một mạng gồm các node chạy định tuyến distance vector, mỗi node sẽ tim đường đi ngắn nhất tới mọi đích trên bản đồ. Sau đó nó sẽ gửi kết quả tốt nhất đó sang hàng xóm, giả sử A gửi sang hàng xóm B, báo là đường đi ngắn nhất từ tôi sang “quán nhậu X” có chi phí đi lại là 100k VND, đồng thời B cũng nhận được thông tin từ C gửi sang với nội dung “ tôi đi sang X chỉ mất 50k VND”.

Khi đấy B sẽ chọn đi theo C, vì chi phí nhỏ hơn.

Vậy distance vector là mỗi router sẽ quảng cáo tuyến đường ngắn nhất từ mình đến đích sang hàng xóm, từ đó hàng xóm cân nhắc đi theo đường nào tốt nhất.

11. ACL (Access control list)

Ví dụ, giả sử một tòa nhà có nhiều tầng và mỗi tầng có một số phòng khác nhau. Để đảm bảo an ninh, các nhân viên bảo vệ sẽ đứng canh ở các cửa, họ sẽ có danh sách những ai được vào, và thời gian được vào. Những người không có tên trong danh sách này sẽ không được phép vào tòa nhà hoặc chỉ được phép vào một số phòng không quan trọng.

Tương tự, trong mạng máy tính, ACL được áp dụng tại các điểm khác nhau trên mạng(các cổng của router) để quản lý quyền truy cập vào các tài nguyên mạng, ví dụ như địa chỉ IP nào sẽ được cho phép hoặc bị chặn, tùy thuộc vào các quy tắc được cấu hình trên router.

Ví dụ cấu hình chặn ip 10.1.2.3 không cho truy cập server 192.168.1.100

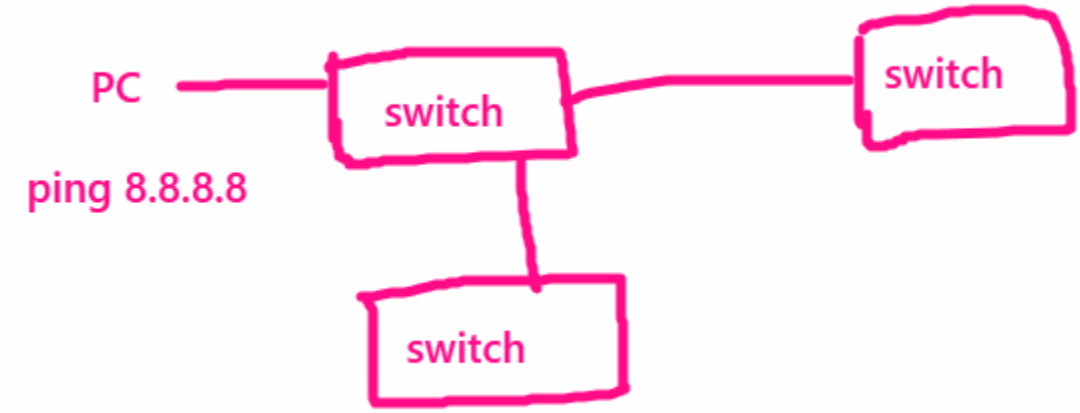
```
ip access-list standard
deny ip host 10.1.2.3 host 192.168.1.100
permit ip any any
exit
int e0/0
```

```
ip access-group 1 in
```

12. ARP

Khi ta đi vào cửa hàng sách cần tìm mua 1 cuốn sách, ta sẽ viết tên sách muốn tìm và đưa cho cô nhân viên tìm hộ, từ đó nhân viên sẽ tìm xem sách đó ở kệ số mấy, nếu biết thì cô sẽ đi đến kệ đó và lấy sách ra, còn nếu nhân viên (mới vào làm việc) không biết thì cô ta sẽ hỏi các nhân viên khác xem sách này ở đâu, từ đó nhân viên nào biết sẽ đi lấy và mang ra đưa cho người mua.

Tương tự trong sơ đồ dưới:



Khi PC ping 8.8.8.8, nó sẽ gửi gói arp , hỏi địa chỉ mác của 8.8.8.8 là gì (MAC tương tự như địa chỉ của kệ sách). Switch1 sẽ gửi gói tin arp (tương tự phiếu ghi sách cần tìm) ra toàn bộ 2 switch còn lại để hỏi xem có ai biết MAC của 8.8.8.8 là gì không. (Switch tương tự nhân viên thư viện)

Nếu có switch nào gắn với 1 PC có IP là 8.8.8.8 thì nó sẽ biết MAC tương ứng, và trả lời lại cho PC ban đầu, ví dụ: MAC của 8.8.8.8 là AAA-BBB-CCC.

Trên switch để show mác , ta dùng lệnh show mac address-table

13. Quality of Service

Giả sử ta có 2 con đường trong thành phố giao cắt tại ngã tư. Nếu xe cộ ít thì không cần cảnh sát đứng phân luồng. Tuy nhiên vào giờ tan tầm, lượng traffic đổ ra đường rất nhiều. Nếu không ai nhường ai sẽ dẫn đến ùn tắc kéo dài. Giả sử có 1 xe cấp cứu đang cần đi gấp cũng sẽ không thể lách lên trên mà đi được.
Tình trạng traffic chạy trong mạng cũng như giao thông giờ cao điểm, gói tin nào cũng muốn để đi nhanh nhất có thể. Khi lượng gói tin đi vào quá khả năng xử lí của router thì sẽ bị nghẽn. Vai trò của CSGT và đèn giao thông giống như các lệnh QoS trong router, switch.

Ví dụ QoS sẽ set cho traffic voice được ưu tiên chuyển mạch trước các trafic https, hoặc ưu tiên cho gói tin từ 1 IP cụ thể nào đó được đi trước…v.v
Trong router, mỗi cổng sẽ có bộ nhớ đệm (RX ring) để chứa gói tin đi vào và chờ, sau đó gói tin đi vào input queue, và được chuyển mạch. Nếu không có QoS thì gói nào đến trước được chuyển mạch trước. Kể cả các gói critical nếu đến sau cũng phải chờ gói không quan trọng nếu nó đến trước. QoS sẽ giúp nhặt các gói quan trọng hơn và cho lên input queue trước. (Tương tự với chiều out thì là TX ring và output queue).

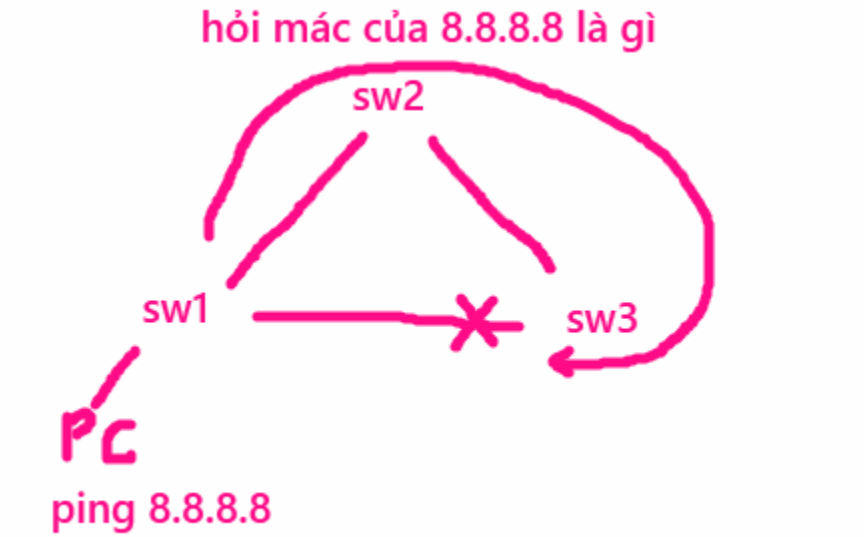
14. Spanning Tree

Tưởng tượng bạn vào 1 nhà sách và tìm sách bằng cách hỏi nhân viên sách X ở chỗ nào, sau đó cô ấy sẽ đi lấy cho bạn.
Giả sử cửa hàng sách có 3 cô nhân viên 1,2,3. Nếu cô NV1 biết chỗ cuốn sách X thì cô ta sẽ lấy ra đưa cho bạn.
Nếu cô NV1 này không biết ở đâu thì hỏi cô NV2.
Nếu cô NV2 cũng không biết, sẽ hỏi cô NV3
Nếu cô NV3 không biết, có khả năng cô sẽ lại hỏi cô NV1 ban đầu.

Cứ như vậy sẽ gây ra vòng lặp mà không có hiệu quả. (Trong network gọi là LOOP)
Vì vậy người quản lí sẽ chọn ra 1 cô giỏi nhất, giả sử là NV3, khi cô này không biết cuốn sách ở đâu thì việc tìm kiếm kết thúc, và xác nhận là KO có cuốn sách đó.

Khách hàng hỏi NV1
NV1 ko biết====>Hỏi NV2 ,
NV2 ko biết ====>Hỏi NV3,
NV3 không biết, KẾT THÚC, CHỨ KHÔNG QUAY LẠI HỎI NV1

Tương tự trong spanning tree, khi các switch nối với nhau thành vòng kín, thì mỗi vòng kín sẽ chắc chắn bị khóa 1 cổng, để cắt đứt vòng, tránh tình trạng hỏi nhau mãi mãi (gọi là LOOP). Ví dụ có 3 switch như dưới:



Bản tin ARP (hỏi MAC của 8.8.8.8) sẽ bị dừng tại switch 3.
Điểm khác của mô hình so với ví dụ 3 cô nhân viên trên ở chỗ là: các switch bầu chọn dựa trên {MAC,priority} của cổng nào nhỏ nhất sẽ làm root switch và không bị block, chứ không dựa vào “ai giỏi nhất”

15. Boardcast

Broadcast tương tự như khi loa phát ra âm thanh, tất cả mọi người trong 1 phòng cùng nghe thấy.
Tương tự trong mạng máy tính, broadcast là 1 địa chỉ IP mà khi 1 PC có IP 192.168.0.100/24 muốn truyền tin ra mọi máy khác cùng dải IP, thay vì gửi thủ công tới từng IP của các máy, thì nó sẽ gửi tới địa chỉ IP broadcast của dải, (192.168.0.255), thì các host dải 192.168.0.0/24 sẽ đều nhận được.
Ở đây 192.168.0.255 là địa chỉ broadcast của dải mạng 192.168.0.0/24