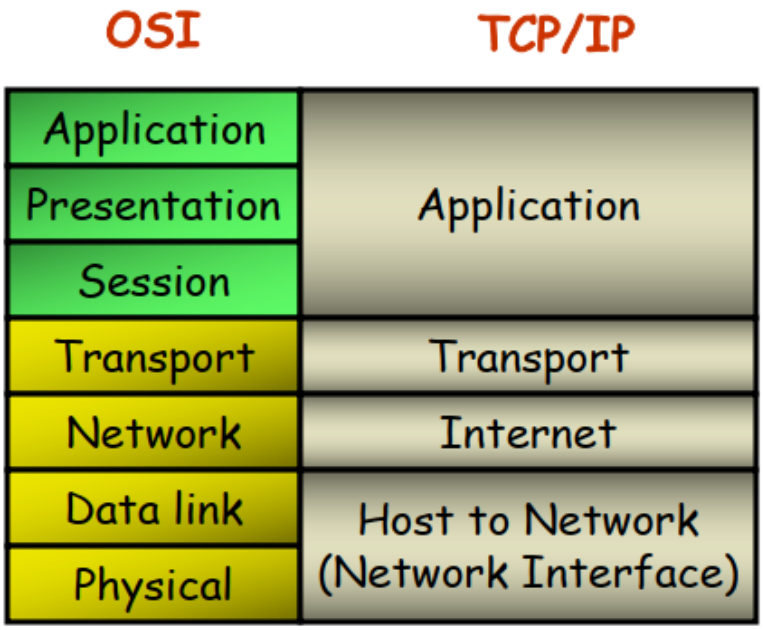
Ôn tập MMT nâng cao

I. Chương 1&2: Ôn lại MMT và chương IPv6

1. Địa chỉ IP là gì ?

Là định danh một máy tính khi giao tiếp trong mạng như địa chỉ nhà

2. Mô hình OSI khác giao thức TCP/IP như thế nào ? Hiện nay đa phần network được sử dụng mô hình nào ?



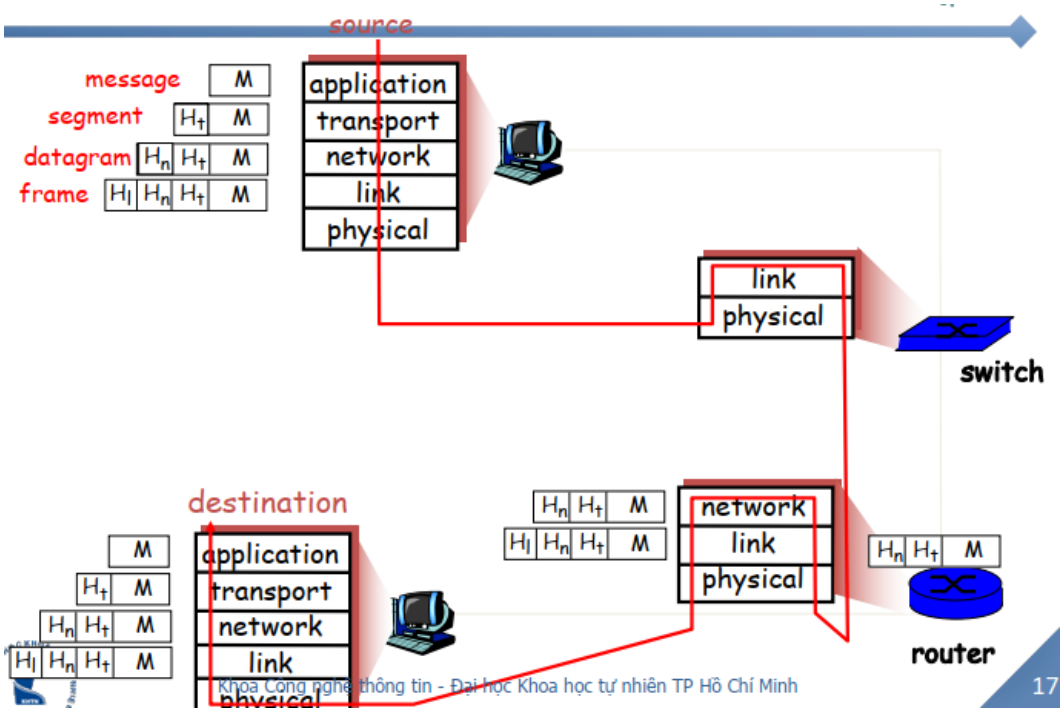
- Hiện nay đa phần network được sử dụng **giao thức TCP/IP**
- Điểm khác biệt lớn nhất giữa hai giao thức này có lẽ là sự kết hợp giữa các tầng với nhau. Đối với giao thức TCP/IP **thì tầng session và tầng presentation** được kết hợp với nhau trong **tầng ứng dụng**. Còn đối với mô hình OSI thì mỗi tầng khác nhau sẽ thực hiện một nhiệm vụ khác nhau.

3. Các giao thức trong tầng của mô hình OSI cho ví dụ ?

- **Tầng ứng dụng:**
  - DHCP, DNS, FTP, HTTP
- **Tầng Transport:**
  - TCP, UDP
- **Tầng Network**
  - IP, ICMP
- **Tầng Data Link**
  - ARP (giữa tầng Data Link và tầng Network)
  - CSMA/CD, CSMA/CA, Ethernet

4. Gói tin trong mạng được truyền như thế nào ?

Gói tin trong mạng được truyền bằng cách đóng gói(escapsulation) sau đó phân rã, được truyền từ source nguồn tới đích(destination)



5. Có mấy loại địa chỉ mạng ?

Địa chỉ public và địa chỉ private

Địa chỉ public thì giao tiếp với nhau trên internet external mọi người đều thấy, địa chỉ private thì hoạt động trong internal chỉ trong tổ chức đó thấy ví dụ như hộ gia đình, cty,…

6. Địa chỉ IP classfull khác gì với IP classless

Các địa chỉ IPv4 từ classfull được chia nhỏ ra thành các subnet(classless)

Vấn đề phát sinh ra ip classless là do địa chỉ ip classfull nếu sử dụng quá lãng phí khó bảo trì

❑ Subnet mask mặc định:

- Lớp A: 255.0.0.0 (/8)
- Lớp B: 255.255.0.0 (/16)
- Lớp C: 255.255.255.0 (/24)

Table 2-4 Private IP Address Information

Class	Address (range)	Networks	Total Private Hosts
Class A	10.0.0.0	1	16,777,214
Class B	172.16.0.0–172.31.0.0	16	1,048,544
Class C	192.168.0.0–192.168.255.0	256	65,024

Cách tính 2^m -2 với m là số **host hợp lệ** ví dụ **lớp A (lấy 32 - 8) là 2^24 – 2 host vì có 1 network**

Còn class B là lấy (2^16-2)x16 vì có 16 network tương tự lớp C

Kích thước là 4byte tương đương 1 byte = 8bit sẽ có 32 bit tất cả

7. **IPv4 khác IPv6 như thế nào ? Tại sao phát sinh ra IPv6**

Sự khác biệt chính giữa IPv4 và IPv6

Chúng ta hãy xem sự khác biệt đáng kể giữa IPv4 và IPv6.

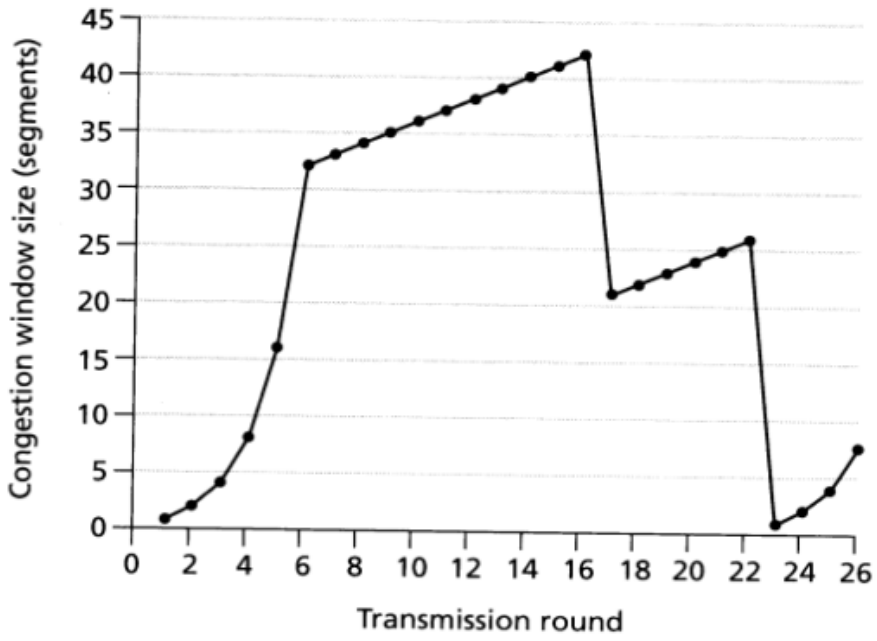
- IPv4 có độ dài địa chỉ 32 bit trong khi IPv6 có độ dài địa chỉ 128 bit.
- Địa chỉ IPv4 đại diện cho số nhị phân theo số thập phân. Mặt khác, địa chỉ IPv6 thể hiện số nhị phân ở dạng thập lục phân.
- IPv6 sử dụng phân mảnh đầu cuối trong khi IPv4 yêu cầu bộ định tuyến trung gian để phân đoạn bất kỳ datagram nào quá lớn.
- Độ dài tiêu đề của IPv4 là 20 byte. Ngược lại, độ dài tiêu đề của IPv6 là 40 byte.
- IPv4 sử dụng trường tổng kiểm tra ở định dạng tiêu đề để xử lý kiểm tra lỗi. Ngược lại, IPv6 loại bỏ trường tổng kiểm tra tiêu đề.
- Trong IPv4, tiêu đề cơ sở không chứa trường cho độ dài tiêu đề và trường độ dài tải trọng 16 bit thay thế nó trong tiêu đề IPv6.
- Các trường tùy chọn trong IPv4 được sử dụng làm tiêu đề mở rộng trong IPv6.
- Trường thời gian để sống trong IPv4 được gọi là giới hạn Hop trong IPv6.
- Trường độ dài tiêu đề có trong IPv4 bị loại bỏ trong IPv6 vì độ dài của tiêu đề được cố định trong phiên bản này.
- IPv4 sử dụng phát sóng để truyền các gói đến các máy tính đích trong khi IPv6 sử dụng đa tuyến và phát sóng.
- IPv6 cung cấp xác thực và mã hóa, nhưng IPv4 không cung cấp nó.

Vấn đề phát sinh ra IPv6 là do địa chỉ IPv4 là 32bit ta tính đơn giản 2^32-2 ~ 4,3 tỉ mà vấn đề thiết bị tham gia môi trường mạng ngày càng tăng nên ko thể đáp ứng đủ nhu cầu nên phải phát sinh ra địa chỉ IPv6

8. **Chia subnet cơ bản xem lại bài tập của thầy**
9. **Phần về gói tin truyền từ nguồn tới đích gồm những gì các bạn tự xem. Đại khái là sẽ mang theo MAC và IP khi qua các router/modem/switch sẽ có sự thay đổi phần ví dụ của thầy có nếu bạn chép bài**

II. Chương 3: TCP congestion control(Kiểm soát tắt nghẽn)

TCP reno



a) **Xác định các khoảng thời gian mà TCP slow-start đang hoạt động**

Slow-start ta xem cột transmission round

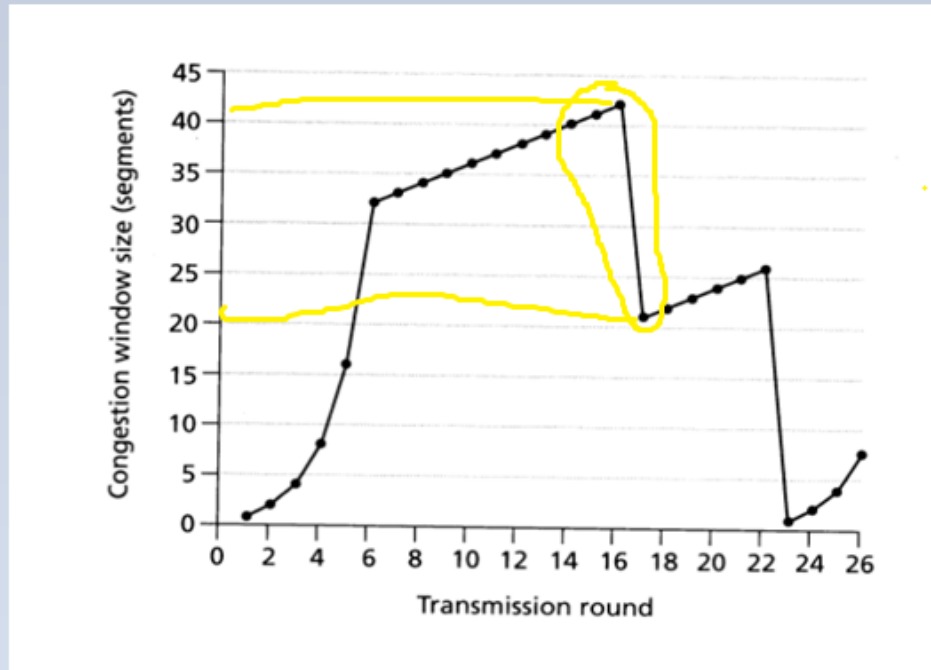
Vậy ta có là [1,6] và [23,26] vì nó đi nhanh dần đều lên

b) **Xác định các khoảng thời gian mà TCP congestion-avoidance đang hoạt động**

Slow-start ta xem cột transmission round

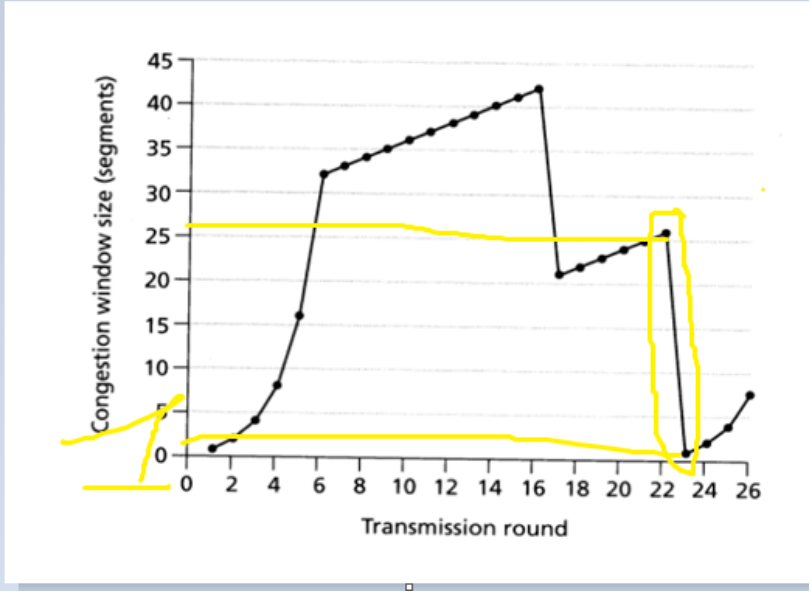
Vậy ta có là [6,16] và [17,22] vì nó đi thẳng lên sẽ

c) **After the 16th transmission round, is segment loss detected by a triple duplicate ACK or by a timeout event?(Sau 16 chỗ transmission round nó hỏi là mất dữ liệu cập nhật hay 3 ACK)**



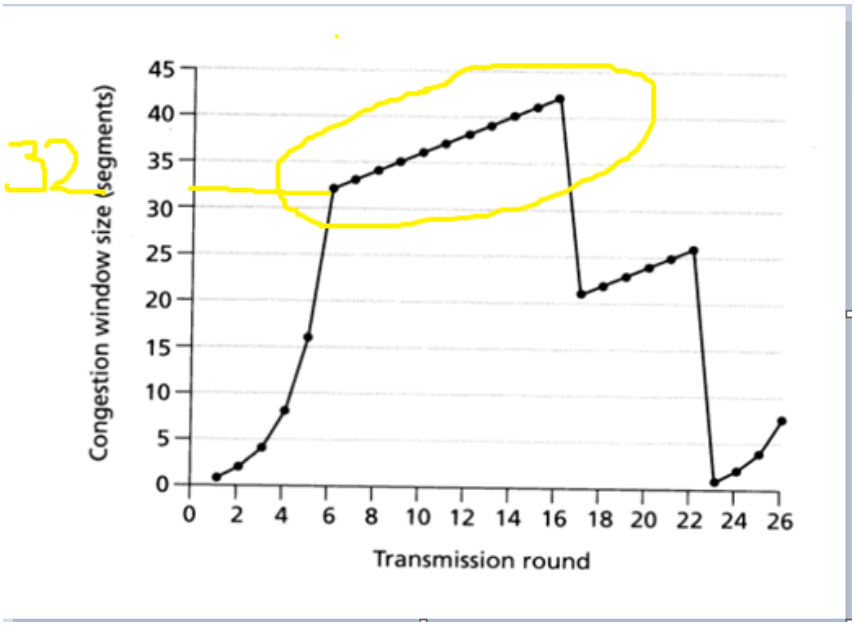
⇨ Vì chỗ 16 ta thấy đi xuống nhưng ko về đến 1 nên nó là mất do **3 ACK**

d) After the 22nd transmission round, is segment loss detected by a triple duplicate ACK or by a timeout event?(Sau 22 thì mất do 3 ACK hay time out)



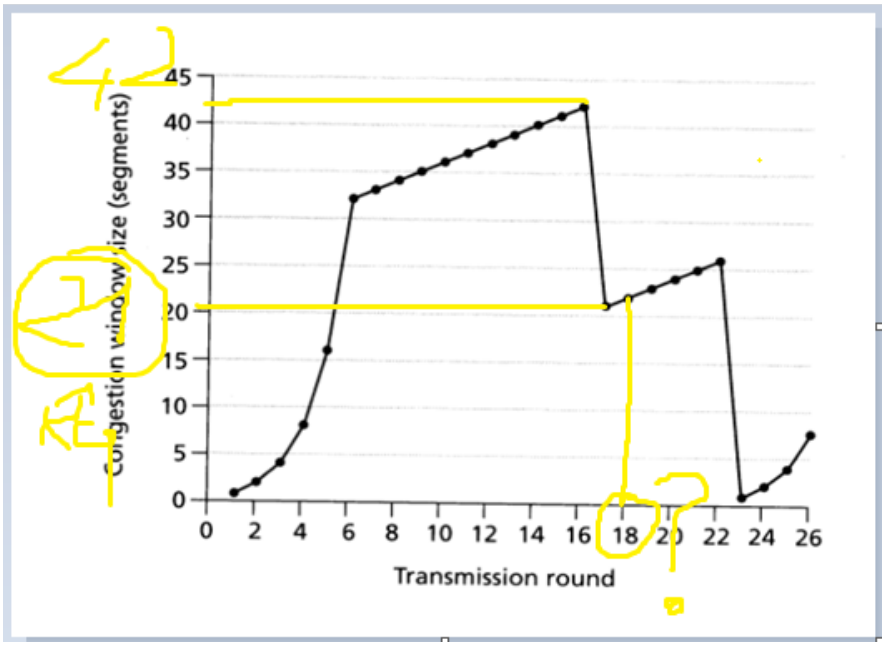
⇨ Vì nhìn vào hình ta thấy mất do **timeout** do ta thấy nó xuống 1

e) What is the *ssthreshold* value at the first transmission round? (Đại khái nó hỏi giá trị threshold đầu tiên là bao nhiêu)



⇨ Nhìn vào hình ta thấy từ **32** chỗ đường thẳng nhìn qua cột dọc

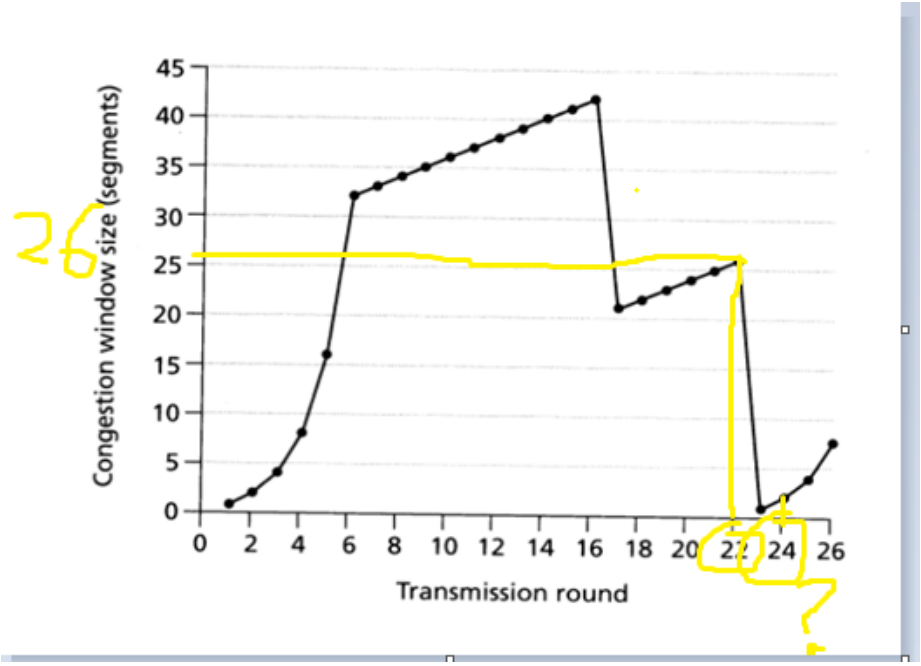
f) What is the *ssthreshold* value at the 18th transmission round?(Nó hỏi chỗ cột ngang á là 18 thì giá trị threshold là bao nhiêu)



⇨ Ta lấy từ chỗ mà nó bị 3 ACK là lúc nó chưa mất là giá trị 42 sau khi mất nó sẽ giảm 1 nửa(3 ACK là luôn luôn giảm 1 nửa)

⇨ **Vậy kq sẽ là 21**

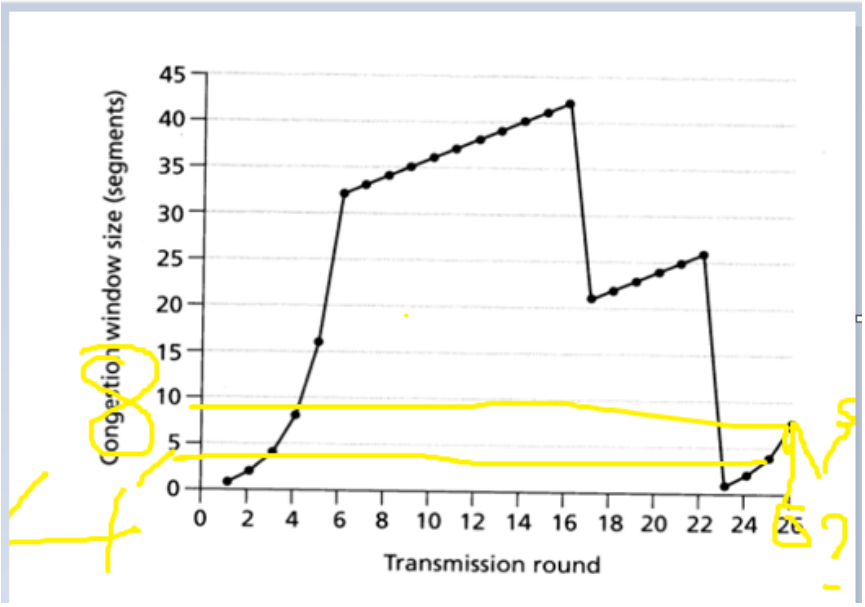
g) What is the *ssthreshold* value at the 24th transmission round?(Giá trị chỗ cột nằm ngang 24 là bao nhiêu)



⇨ Tương tự như câu trên ta thấy lúc mà chưa bị mất gói chỗ cột nằm ngang là 22 giá trị qua bên cột dọc là 26 ta chia 2 ra

⇨ **Kết quả bằng 13**

h) What will be the values of *cwind* and *ssthreshold* if packet loss is detected after the 26th round by receipt of triple duplicate ACKs?(Đại khái nó hỏi giả sử sau giá trị của cột ngang là 26 nó giả sử mất gói do 3 ACK thì điểm threshold đi lên sẽ là bao nhiêu)



⇨ Đơn giản thôi nhìn vào note ta thấy mất do 3 ACK thì từ threshold giảm một nửa mà threshold lúc đó là 4 thôi

❖ **NOTE**

– **Nếu mất gói do timeout thì kênh truyền nghẽn để an toàn sẽ xuống 1**

– **Nếu do 3 ACK thì từ threshold(giá trị lúc mất giảm đi 1 nửa) đi lên**

Bài này ko hiểu có thể contact mình

1. **So sánh flow control và congestion control ?**
   - Kiểm soát luồng là người nhận kiểm soát mức độ mà người gửi đưa vào mạng
   - Kiểm soát tắc nghẽn là người gửi cảm nhận tắc nghẽn trên mạng bằng cách định thời gian ACK và kiểm soát tốc độ gửi của nó.
2. Các dữ liệu mất gói do
   - 3 ACK
   - Timeout
3. TCP reno vs TCP Tahoe
   - TCP: reno
     + Mất gói do 3 ACK
     + Sequence từ threshold đi lên
   - TCP Tahoe
     + Mất gói do timeout
     + Đi từ 1 đi lên
4. TCP vs UDP
   - UDP:
     + Bỏ qua các kết nối lỗi
     + Không thiết lập kết nối
     + Kích thước header nhỏ
   - TCP:
     + Truyền tin cậy
     + Kiểm soát luồng
     + Kiểm soát tắt nghẽn
     + Thiết lập kết nối

Kiểm soát lưu lượng(flow control):

- Nó đảm bảo rằng người gửi không quá tải người nhận.
- Đó là một hiện tượng cục bộ, không giống như kiểm soát tắc nghẽn.

- **Nó thường được khởi xướng bởi người gửi.**

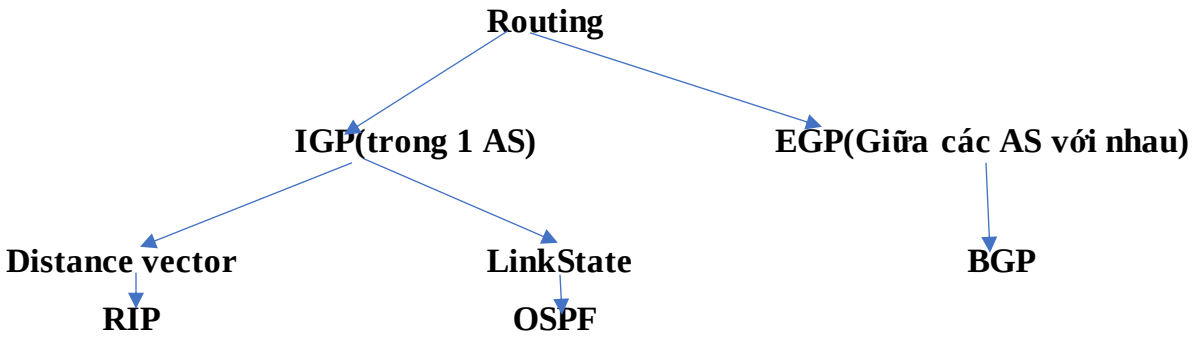
Điều khiển tắc nghẽn(congestion control):

- Nó đảm bảo rằng mạng có thể xử lý tải các gói.
- Đó là một hiện tượng toàn cầu và ảnh hưởng đến mọi Máy chủ được kết nối với mạng đó.
- **Nó được điều khiển bởi bộ định tuyến(router).**

III. Chương 4 & 5: Internet routing

- Định tuyến: là tìm đường đi từ nguồn tới đích
- Có 2 loại định tuyến
    + Tĩnh: Do ta tự cấu hình
    + Động:
        - Distance vector: gởi theo định kì, gởi toàn bộ bảng định tuyến, vd: RIP,IGRP,
        - Link state: Gửi khi có thay đổi, gửi tình trạng kết nối vd: OSPF, ISIS,

Sơ đồ Routing



a) RIP khác gì so với OSPF(hay distance vector khác gì so với linkstate)

- **RIP(distance vector): lựa chọn đường đi tốt nhất dựa vào số hop đi qua, nếu số hop lớn hơn 15 sẽ ko đi được, cập nhật bằng việc gửi broadcast**
    + Xác định hướng tới mạng đích
    + Cập nhật định kì các router khi có thay đổi
    + Xác định khoảng cách tới mạng đích
- **OSPF(linkstate): lựa chọn đường đi ngắn nhất theo thuật toán dikjstra, mỗi router sẽ nhận tất cả đường đi tới các router khác sau đó chọn đường đi ngắn nhất**

+ Trạng thái của từng link
+ Biết được topo của mạng hiện hành
+ Không cập nhật định kì

NOTE: So với distance vector thì linkstate sẽ tốt hơn nếu xảy ra sự cố 1 router không tham gia vào đường mạng

b) Các mạng hiện nay giao tiếp với nhau thông qua giao thức nào ? với BGP nó tìm cách nào đi từ nguồn tới đích

BGP(path vector), BGP sẽ tuân thủ theo policy việc chọn tuyến đường tốt nhất dựa trên các thuộc tính của tuyến đường(xem slide về BGP)

c) BGP định tuyến theo cách nào ?

BGP định tuyến bằng cách sử dụng các thuộc tính của các tuyến đường. Mỗi tuyến đường là danh sách các AS cần phải đi qua.

d) Bản tin BGP có 4 loại thông điệp?

+ **Open:** Thiết lập kết nối với hàng xóm
+ **Keep Alive:** Bắt tay thường xuyên với hàng xóm
+ **Notif:** Thông báo với hàng xóm
+ **Update:** Thông báo tuyến đường mới hoặc hủy 1 tuyến đường đã quảng bá trước đó

e) Routing loop là gì ? Nguyên nhân và tác hại ? Cách ngăn ngừa

- Routing loop là tình trạng gói tin đi qua nhiều router mà không đến đích
- Nguyên nhân do cấu hình sai, hội tụ chậm,
- Tác hại: Tiêu tốn bandwidth, mạng không hội tụ, thông tin cập nhật định tuyến bị mất hoặc ko xử lý kịp
- Cách chống loop: với distance vector thì thiết lập giá trị metric lớn nhất để xác định đường đi đó không khả dụng, sử dụng **hold down timer** giúp router ko thay đổi đường đi trong TG nhất định, sử dụng **split horizon rule** router sẽ không quảng bá đường mạng mà nó chỉ nhận thông tin về đường mạng đó

f) Fdsf

g) Fsdf

h) Dfsf

i) **Sfsdf**

j) **Dsfsd**

k)

IV. Chương 7: Ảo hóa & cloud

Phần ảo hóa này các nhóm đã làm nên mình ko note nhiều, nếu ko chỗ nào có câu hỏi cần hỏi mình ,mình sẽ trả lời trong sự hiểu biết và kinh nghiệm làm việc của mình

- Virtual machine(VM): hoạt động như một hệ điều hành mà trong đó các phần cứng sẽ chia sẻ các tài nguyên với nhau, ta có thể dễ dàng snapshort,clone,…
- Có các loại ảo hóa: Ảo hóa server, ảo hóa desktop, ảo hóa về memory, disk, network,..
- Ảo hóa sử dụng KVM, VMWare
  - ⇨ Tóm lại ảo hóa khác gì so với cloud

    Máy ảo khi request 1 VPS thì thời gian có thể lâu còn khi cloud chúng ta có thể tạo trực tiếp trên đó mà ko cần thông qua trung gian nào, có thể chia sẻ resource pool dễ dàng
- Các tính năng của máy ảo khác với máy thật

  + Có thể tạo nhiều VM trên đó sử dụng nhiều services

  + Tiết kiệm chi phí hơn so với mỗi hardware sử dụng 1 distro (OS)
- Ảo hóa
  - + Được cô lập
  - + Bảo mật nâng cao
  - + Dễ dàng mô phỏng kiến trúc khác nhau và cùng tồn tại

V. Chương 8: Container

Phần này cũng ko có gì nhiều tùy cơ ứng biến

- Khác với ảo hóa và cloud container hoạt động độc lập không dựa vào các tài nguyên như cpu,ram,disk,…
- Không sử dụng kernel
- Có thể dễ dàng di chuyển qua các máy khác nhau
- Hạn chế của máy ảo

+ Máy ảo vẫn yêu cầu cpu,ram,disk

+ Chạy nhiều máy ảo thì càng nhiều tài nguyên

+ Sử dụng hđh ko sử dụng hết gây lãng phí

+ Tính di động ko được đảm bảo

- Docker image & container

+ Image:

  - Chỉ đọc để tạo ra container
  - Được sử dụng bởi mình hoặc docker ng khác tạo
  - Được lưu trữ trong docker hub

+ Container:

  - Chứa mọi thứ cần thiết để chạy ứng dụng
  - Dựa trên 1 hoặc nhiều image

VI. Các bài các nhóm khác seminar có thể tham khảo

https://www.dropbox.com/sh/zwm8gpnkr5xetue/AABPjDJNGVu2guiEDzkA1Lz2a?dl=0&fbclid=IwAR1zK7VMVu5uX_HEicpymTcZD4hC6iJhzYFzO4XpyT2zPA7m1OuzpHnkQUY