Slide 15: Fowarding table:  
- Đối với gói tin broadcast sẽ copy qua cả 2 cổng

* Bridge không lọc được broadcast packet

- Bridge dùng để chia nhỏ collisi

on domain

Slide 17:  
- kiểu chay cáp khác nhau nghĩa là khác topology

-Bridge chậm hơn repeater là chậm hơn ở quá trình xử lí do bridge xử lí trên frame còn repeater xử lí trên bit

Slide 18:   
- Switch khác với hub:

+ Gói tin trong hub được copy qua tất cả các cổng

+ Switch: Gởi thẳng qua máy cần gửi

* Switch làm đc do có fowarding table như bridge sẽ tra được nơi gửi

-Do đó 1 hub là một collision domain, còn mỗi một cổng của switch là một collision domain

Slide 18:  
-Full-duplex:

+mỗi một cổng vừa gửi và vừa nhận dữ liệu

+trong khi máy số 1 và máy số 2 truyền nhận dữ liệu với nhau thì máy số 3 và số 4 vẫn truyền được dữ liệu cho nhau

Slide 19:

-Switch và bridge có thể tự tạo fowarding table khác với routing table trong định tuyến router.

-Filtering để lọc gói tin đi qua những collision domain

- FCS: thông tin kiểm lỗi

- 2 loại switch:  
 + Hoạt động trong chế độ store-and-fowared (đắt tiền hơn):

+ Cut-through

-Khi nào dùng store-and-fowared và khi nào dùng cut-through:  
 + store-and-fowared: Dùng cho workgroup switch (switch nối các switch lại với nhau)

+ cut throught: Dùng cho segment switch( các switch nối đến workgroup switch)\

Slide 23:  
- Các switch nối với nhau cùng một mạng LAN

- Switch nối các mạng LAN ảo (VLAN):

+ Nhóm các cổng của switch thành các LAN nhỏ như LAN1, LAN2, LAN3

VD: 1 switch có 12 cổng nối đơn 12 máy tính muốn chia thành 3 LAN nhỏ thì sẽ chia LAN1 ( máy 1 đến máy 4), LAN2(máy 5-8), LAN3 ( máy 9-12).

Slide 25:  
- NIC: card mạng

Slide 26:

Nhớ Bộ thu và bộ phát

Slide 27:  
Nhớ bảng này để nhớ công việc từng thiết bị

Bridge dùng với BUS topylogy

Còn switch dùng với start topology

Slide 31:  
Số cổng của router là số broadcase domain

Số cổng của switch là số collision domain

Một hub là một collision domain

FIREWALL

1/ Kiến trúc dual-homed host:  
- Chỉ có một máy tính

-2 card mạng

- tắt bỏ tính năng định tuyến

=> Làm như vậy gói tin gửi đến máy từ bên ngoài lẫn bên trong sẽ đc bảo vệ

- Cài phần mềm proxy server để các máy trong mạng yêu cầu

- Cài các dịch vụ mạng bên ngoài vào như dns server, mail server, web server

=> Kiến trúc này có hạn chế là dễ quá tải ở máy dual-homed host và nếu như máy dual-homed host bị tấn công sẽ làm cho các máy trong mạng không được bảo vệ

2/ Kiến trúc Screened Host(screened ở đây là che chắn => dùng máy host để che chắn)

- Ưu điểm so với kiến trúc dual-homed host là giảm tải cho máy bastion host

-Có một router lọc gói tin (screening router)

-Có một máy bastion host có vai trò như máy dual-home hosted

=>Hạn chế: vẫn như kiến trúc số 1 bastion host chung mạng với các máy trong mạng mình nếu như bị tấn công vẫn sẽ như kiến trúc dual-homed host

3/ Screened Subnet(dùng 1 đường mảng để che chở)

-Tương tự như kiến trúc screened host có perimeter network tách ra

=> Ý tưởng khi máy bastion host bị tấn công, các máy trong mạng vẫn an toàn vì riêng đường mạng

=> Các kiến trúc hiện giờ đều là biến thể dựa trên screened subnet

Trong thuật ngữ firewal có thuật ngữ DMZ: dùng cho perimeter network

4/ Có 3 biến thể của screend Subnet

+ Biến thể 1 dùng nhìu máy bastion host

+ Biến thể 2 gom external và internal router thành 1 router có 3 cổng ( kết nối với internet, với bastion host và các máy trong

+ Biến thể 3 ( nghèo): cho bastion host làm chức năng của router ngoài

+ Biến thể 4( giàu): nối ra bên ngoài bằng nhiều đường, cứ một đường ra ngoài dùng một router

+ Biến thể 5(quá tốn kém): có nhiều đường ra ngoài với một đường ra ngoài dùng một perimeter network riêng

-Biến thể không nên dùng:  
+ Biến thể 1 : không dùng bastion host làm interal router vì nếu bị tấn công sẽ giống như kiến trúc screend host

+ Biến thể: Không cho nhiều router làm internal router vì làm vậy các gói tin giao tiếp bên trong sẽ lọt ra perimeter network và khi bastion host lọt ra sẽ đọc được

5/ Cách bảo vệ bastion host:  
- Tắt tất cả dịch vụ không cần trên máy bastion host

-Cấm các user accounts trên bastion host

- Thường xuyên vá lỗi trên bastion host

- Sử dụng system log để ghi lại lịch sử hoạt động các máy trên hệ thống

NỘI DUNG THI:  
- 90 phút

-Có 4 câu tương ứng với 4 tầng của TCP, mỗi một tầng ít nhất 1 câu:  
Application

TCP

IP

Data Link

Hỏi linh tinh bên ngoài như các thiết bị mạng, firewall