TRƯỜNG ĐẠI HỌC CẦN THƠ

KHOA CÔNG NGHỆ THÔNG TIN & TT

Chương 6

KHẮC PHỤC SỰ CỐ MẠNG Ở TẦNG VẬN CHUYỂN

Giảng viên: **Phạm Hữu Tài**

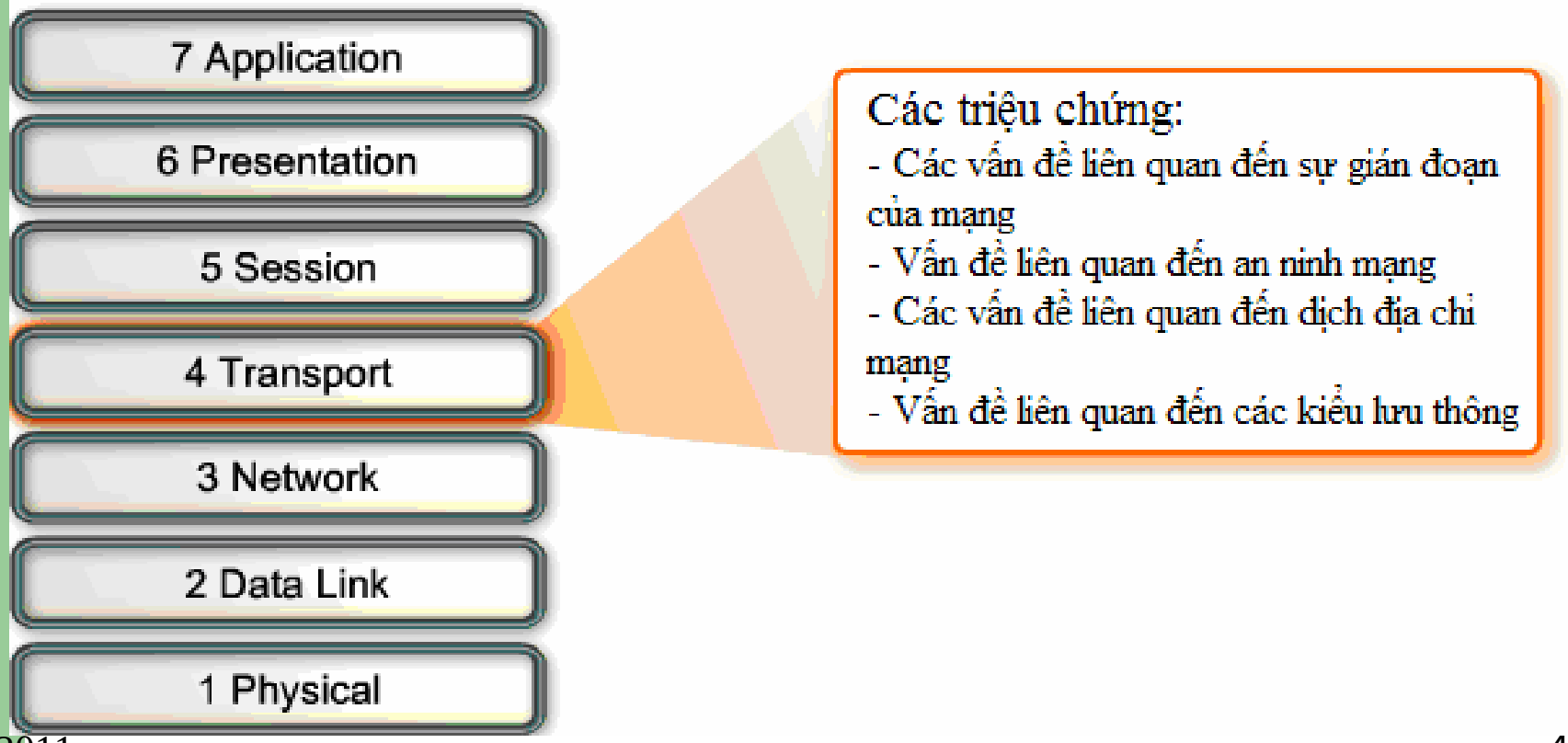
Mục đích – Yêu cầu

- **Mục đích:**
  - Cung cấp thông tin cho người đọc các triệu chứng cơ bản, các nguyên nhân và cách khắc phục liên quan đến các sự cố ở tầng vận chuyển trong mô hình OSI
- **Yêu cầu:**
  - Sinh viên xác định đúng các triệu chứng, xác định được các nguyên nhân liên quan đến sự cố ở tầng vận chuyển của hệ thống mạng
  - Nắm được cách giải quyết sự cố mạng liên quan ở tầng vận chuyển

Các triệu chứng của sự cố ở tầng vận chuyển (1)

- Phần lớn các triệu chứng có liên quan đến bộ định tuyến giữa mạng cục bộ với nhà cung cấp dịch vụ *(bộ định tuyến biên)*
  - Danh sách điều khiển truy cập (ACL)
  - Dịch địa chỉ mạng (NAT)

Các triệu chứng của sự cố ở tầng vận chuyển (2)



Các vấn đề liên quan đến danh sách điều khiển truy cập (ACL) (1)

Các vấn đề phổ biến của ACL:
- Áp dụng không đúng lưu thông
- Thứ tự các câu lệnh
- Câu lệnh ẩn "*deny any any*"
- Địa chỉ và mặt nạ ký tự đại diện
- Chọn giao thức TCP hay UDP
- Cổng nguồn / cổng đích
- Dùng tham số trong ACL
- Giao thức không phổ biến

Các vấn đề liên quan đến danh sách điều khiển truy cập (ACL) (2)

- *Lựa chọn các luồng giao thông*
  - Đây là lỗi phổ biến liên quan đến ACL
  - Lưu thông qua bộ định tuyến *là có hướng*

  ➔ Hướng giải quyết đề nghị: Mỗi ACL khi áp dụng vào bộ định tuyến cần phải xác định đúng giao diện cần áp dụng, đúng hướng lưu thông.

Các vấn đề liên quan đến danh sách điều khiển truy cập (ACL) (3)

- *Thứ tự của các câu lệnh trong ACL*
  - Các câu lệnh thành phần trong một ACL nên có thứ tự từ các trạng thái cụ thể tổng quát.
  - ➔ Hướng giải quyết đề nghị: Kiểm tra cẩn thận thứ tự các câu lệnh trong một chương trình soạn thảo văn bản trước khi áp dụng vào trong một danh sách điều khiển truy cập trên thiết bị

Các vấn đề liên quan đến danh sách điều khiển truy cập (ACL) (4)

- *Mặc định ẩn từ chối tất cả (deny any)*
  - Trong cấu hình ACL, mặc định cuối danh sách có một câu lệnh được hiểu mặc định là *từ chối tất cả (deny any)*

  → câu lệnh mặc định này sẽ ngăn cản mọi lưu thông qua bộ định tuyến theo hướng lưu thông được thiết lập trên giao diện của bộ định tuyến.

  ➔ Hướng giải quyết đề nghị: Tùy theo cấu hình chính sách an ninh trong hệ thống mạng mà người quản trị có thể để nguyên mặc định này thực thi hay không. Nếu muốn vô hiệu hóa câu lệnh này, người quản trị thêm vào câu lệnh *cho phép tất cả (permit any)* vào dòng cuối trước khi đóng lại danh sách.

Các vấn đề liên quan đến danh sách điều khiển truy cập (ACL) (5)

- *Mặt nạ mạng (Netmask) và mặt nạ ký tự đại diện (Wildcard mask)*

  Nếu bộ định tuyến đang được cài đặt để chạy cả ACL và NAT, chú ý:

  – Luồng lưu thông trên mạng đi vào bộ định tuyến từ mạng bên ngoài (từ ISP) vào: xử lý ACL *trước khi* NAT (outside-to-inside NAT) dịch địa chỉ từ địa chỉ công cộng sang địa chỉ mạng riêng.

  – Ngược lại, với gói tin đi từ mạng cục bộ thông qua bộ định tuyến ra ngoài ISP: xử lý ACL *sau khi* NAT (inside-to-outside NAT) dịch địa chỉ từ địa chỉ mạng riêng sang địa chỉ công cộng

  ➔ Hướng giải quyết đề nghị: Hiểu rõ vai trò của mặt nạ ký tự đại diện dùng trong ACL và áp dụng đúng

Các vấn đề liên quan đến danh sách điều khiển truy cập (ACL) (6)

- *Lựa chọn giao thức tầng vận chuyển*
  - Khi cấu hình các danh sách điều khiển truy cập, điều quan trọng là chỉ có các giao thức tầng vận chuyển cần thiết sẽ được chỉ định trong danh sách → *cấu hình một cổng TCP hoặc một cổng UDP, thậm chí họ cấu hình cả hai* → tạo lỗ hổng an ninh mạng
  - Thêm vào đó, khi thêm một câu lệnh thành phần cho một giao thức trong ACL, ACL của mất thêm thời gian để xử lý → *tăng độ trễ khi tuyền thông → làm giảm hiệu suất lưu thông mạng*.

  ➔ Hướng giải quyết đề nghị: khi sử dụng ACL mở rộng, cần xác định đúng giao thức ở tầng vận chuyển để đạt được chính sách an ninh phù hợp mà không ảnh hưởng đến hiệu suất mạng.

Các vấn đề liên quan đến danh sách điều khiển truy cập (ACL) (7)

- *Vấn đề liên quan đến cổng nguồn và cổng đích*
  - Kiểm soát chính xác lưu thông giữa hai máy → *thông tin về địa chỉ và cổng dịch vụ được phát trả lại từ máy nhận là phản chiếu lại địa chỉ và cổng dịch vụ nhận được yêu cầu từ máy gửi.*

  ➔ Hướng giải quyết đề nghị: Cần xác định chính xác thông tin liên quan đến các các giao dịch có thể có giữa hai đầu cuối trên mạng để cấu hình hoạt động của ACL hiệu quả mà không ảnh hưởng đến truyền thông trên mạng.

Các vấn đề liên quan đến danh sách điều khiển truy cập (ACL) (8)

- *Sử dụng tham số trong danh sách điều khiển truy cập*
  - Việc sử dụng từ khóa trong danh sách điều khiển truy cập (ví dụ như *established*) làm tăng tính bảo mật cho ACL → Nhưng trong một số trường hợp, các từ khóa được sử dụng không phù hợp có thể nhận được các kết quả không mong muốn.

  ➔ Hướng giải quyết đề nghị: Cần nắm rõ ý nghĩa của từng tham số được sử dụng trong ACL.

Các vấn đề liên quan đến danh sách điều khiển truy cập (ACL) (9)

- *Các giao thức không phổ biến*
  - Các ACL bị cấu hình nhầm lẫn thường sẽ gây ra các vấn đề cho các giao thức ít phổ biến hơn so với các giao thức TCP và UDP.
  - Các giao thức không phổ biến được biết như các giao thức được dùng trong VPN.

  ➔ Hướng giải quyết đề nghị: Khi sử dụng các giao thức không phổ biến (như các giao thức trong VPN), cần tham khảo các chỉ dẫn trong các tài liệu liên quan để có thể nắm bắt được các vấn đề tiềm ẩn khi sử dụng các giao thức không phổ biến đó.

Các vấn đề thường gặp với dịch địa chỉ mạng (NAT) (1)

- BOOTP và DHCP: Cả hai giao thức quản lý việc cung cấp địa chỉ IP tự động cho các máy khách trên mạng.
- NAT đòi hỏi gói tin được dịch địa chỉ phải có địa chỉ nguồn và đích hợp lệ, BOOTP và DHCP có thể gặp phải khó khăn hơn khi một bộ định tuyến chạy NAT tĩnh hoặc động.

➔ Hướng giải quyết đề nghị: Cấu hình tính năng *IP helper* trên các giao diện của bộ định tuyến có thể giúp giải quyết vấn đề này.

Các vấn đề thường gặp với dịch địa chỉ mạng (NAT) (2)

- DNS và WINS: Bởi vì một bộ định tuyến đang được thiết lập chạy NAT động đang thực hiện sự thay đổi mối quan hệ giữa các địa chỉ bên trong (địa chỉ riêng) và địa chỉ bên ngoài (địa chỉ công cộng) theo qui tắc như một bảng mục hết hạn và được tái tạo, một máy chủ DNS hay WINS bên ngoài bộ định tuyến đang cài đặt NAT không có một địa chỉ chính xác của mạng bên trong bộ định tuyến.
- SNMP: một trạm quản lý SNMP trên một phía của một bộ định tuyến có thiết lập NAT có thể không thể liên hệ với các tác nhân SNMP trên phía còn lại của bộ định tuyến cài đặt NAT đó.

➔ Hướng giải quyết đề nghị: Cấu hình tính năng *IP helper* trên các giao diện của bộ định tuyến có thể giúp giải quyết vấn đề này.

Các vấn đề thường gặp với dịch địa chỉ mạng (NAT) (3)

- Các giao thức đường hầm (tunneling) và mã hóa trong VPN: thông thường khi lưu thông trên mạng với cổng nguồn có thể thuộc UDP hay TCP hay một giao thức ở tầng vận chuyển mà NAT trên bộ định tuyến không thể xử lý được. Ví dụ, các giao thức đường hầm IPSec và giao thức đóng gói loại định tuyến tổng quát được sử dụng bởi VPN không thể được xử lý bởi NAT.

➔ Hướng giải quyết đề nghị: tạo ra một mục NAT tĩnh cho cổng cần thiết cho một địa chỉ IP duy nhất vào bên trong của bộ định tuyến NAT

Các vấn đề thường gặp với dịch địa chỉ mạng (NAT) (4)

- NAT ảnh hưởng đến lưu thông cả mạng bên trong và mạng bên ngoài → Cấu hình NAT sai có thể dẫn đến những hành vi không mong muốn hoặc hoạt động dưới mức so với đường cơ sở mạng.
- Cấu hình không đúng các bộ định thời cũng có thể dẫn đến hành vi không mong muốn và hoạt động dưới chuẩn của NAT động.
  - Nếu bộ định thời của NAT là **quá ngắn**, các mục trong bảng NAT có thể hết hạn trước khi nhận được các trả lời, do đó, các gói tin bị bỏ đi.
  - Nếu bộ định thời được xác lập với thời gian **quá dài,** mục có thể ở lại trong bảng NAT dài hơn cần thiết, tiêu thụ các địa chỉ công cộng được định nghĩa trong dãy → đầy bảng NAT

➔ Hướng giải quyết đề nghị: Cẩn trọng khi cấu hình bộ định thời khi sử dụng NAT.

Hết chương 6!