TRƯỜNG ĐẠI HỌC CẦN THƠ

KHOA CÔNG NGHỆ THÔNG TIN & TT

Chương 7

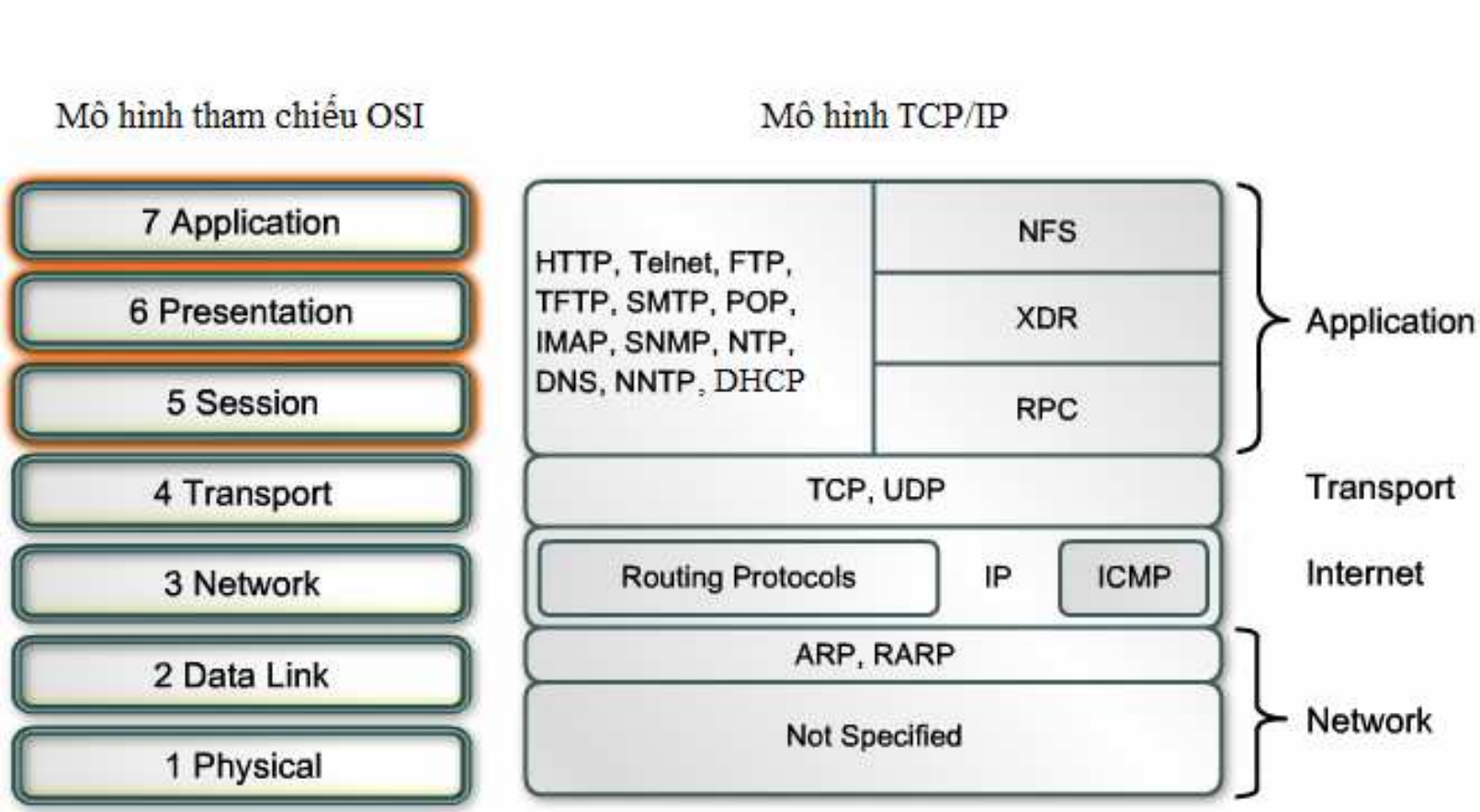
KHẮC PHỤC SỰ CỐ MẠNG Ở TẦNG ỨNG DỤNG

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 ứng dụng 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 ứng dụng của hệ thống mạng
  - Nắm được cách giải quyết sự cố mạng liên quan ở tầng ứng dụng
  - Nắm vững qui trình giải quyết sự cố mạng ở tầng ứng dụng

Tổng quan về tầng ứng dụng (1)



Tổng quan về tầng ứng dụng (2)

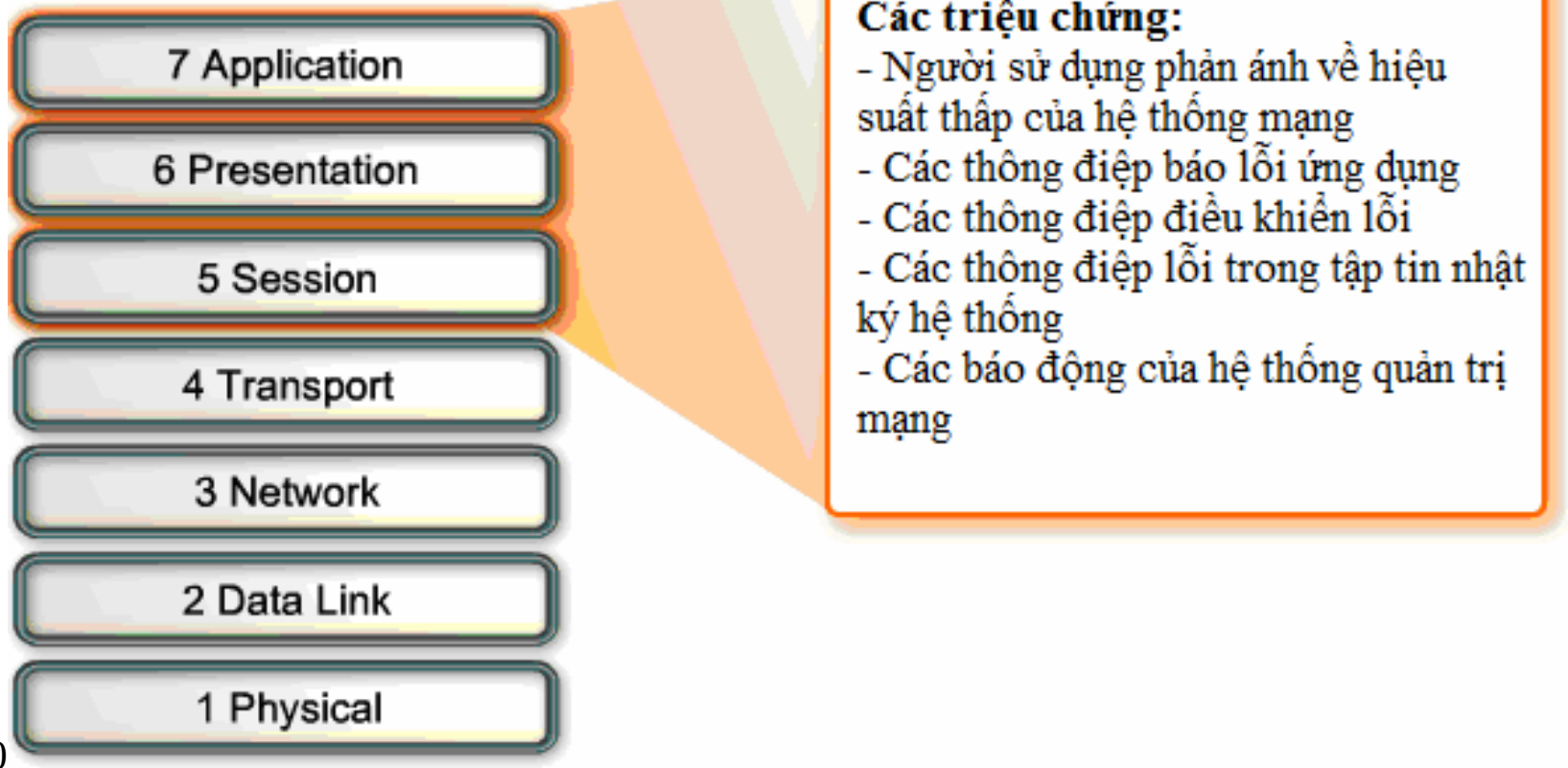
Các dịch phụ được sử dụng rộng rãi nhất trong bộ giao thức TCP/IP bao gồm:

- ***Telnet*** – Dịch vụ cho phép người dùng thiết lập phiên giao dịch kết nối với máy đầu cuối từ xa.
- ***HTTP (Hypertext Transfer Protocol)*** - Hỗ trợ việc trao đổi văn bản, hình ảnh đồ họa, âm thanh, hình ảnh truyền hình và các tập tin đa phương tiện khác trên web.
- ***FTP (File Transfer Protocol) -*** Thực hiện tương tác chuyển tập tin giữa các máy trên mạng theo mô hình máy phục vụ/máy trạm.
- ***TFTP (Trivial File Transfer Protocol)-*** Thực hiện tương tác cơ bản truyền tập tin thông thường giữa máy chủ và các thiết bị mạng. Thường được sử dụng để lưu dự phòng/phục hồi tập tin cấu hình, hệ điều hành của các thiết bị

Tổng quan về tầng ứng dụng (3)

- ***SMTP* (*Simple Mail Transfer Protocol*)**- Hỗ trợ cơ bản dịch vụ chuyển phát thông điệp.
- ***POP* (*Post Office Protocol*)**– Giao thức hỗ trợ kết nối với máy chủ email và tải e-mail.
- ***SNMP (Simple Network Management Protocol)*** - Thu thập thông tin quản trị từ các thiết bị mạng.
- ***DNS (Domain Name System)*** – Ánh xạ địa chỉ IP với các tên dạng tên miền được gán cho các thiết bị mạng.
- ***NFS (Network File System)*** - Cho phép các máy tính gắn kết các ổ đĩa trên các máy từ xa và hoạt động thư thể chúng đang được gắn kết trên các máy tính cục bộ. Ban đầu được phát triển bởi Sun Microsystems, nó kết hợp với hai giao thức tầng ứng dụng khác nhau là XDR (External Data Representation) and RPC (Remote-Procedure Call) để cho phép truy cập đến nguồn tài nguyên mạng từ xa

Các triệu chứng của sự cố ở tầng ứng dụng (1)



Các bước phát hiện sự cố ở tầng ứng dụng (1)

Các bước phát hiện sự cố ở tầng ứng dụng (2)

- Bước 1: Dùng lệnh ***ping*** <*gateway*> để kiểm tra kết nối đến cổng mặc định.
  - Nếu thành công, các dịch vụ ở tầng vật lý và tầng liên kết dữ liệu đang hoạt động đúng.
- Bước 2: Kiểm tra kết nối hai đầu cuối.
  - Sử dụng lệnh *ping* mở rộng từ bộ định tuyến đến các máy ở xa.
  - Nếu thành công, tầng mạng hoạt động tốt. Nếu tầng 1-3 hoạt động đúng, vấn đề phải tồn tại một tầng cao hơn.

Các bước phát hiện sự cố ở tầng ứng dụng (3)

- Bước 3: Kiểm tra hoạt động của danh sách điều khiển truy cập và hoạt động NAT (nếu có)

  Để giải quyết sự cố liên quan đến danh sách điều khiển truy cập, thực hiện các bước sau:

  – Trên bộ định tuyến, sử dụng các lệnh liệt kê các danh sách truy cập được thiết lập trên bộ định tuyến (trong bộ định tuyến của Cisco, dùng lệnh *show access-list)*. Có ACL nào có thể gây ra ngừng lưu thông mạng không? Ghi nhận các danh sách có khả năng gây dừng lưu thông mạng để xem xét sau.

  – Xóa bộ đếm của danh sách điều khiển truy cập và tiến hành thử cho kết nối trở lại để quan sát.

  – Ghi nhận lại bộ đếm danh sách điều khiển truy cập. Bộ đếm có tăng lên? Việc tăng đó có hợp lý?

Các bước phát hiện sự cố ở tầng ứng dụng (4)

- Bước 3: Kiểm tra hoạt động của danh sách điều khiển truy cập và hoạt động NAT (nếu có) (tiếp theo)

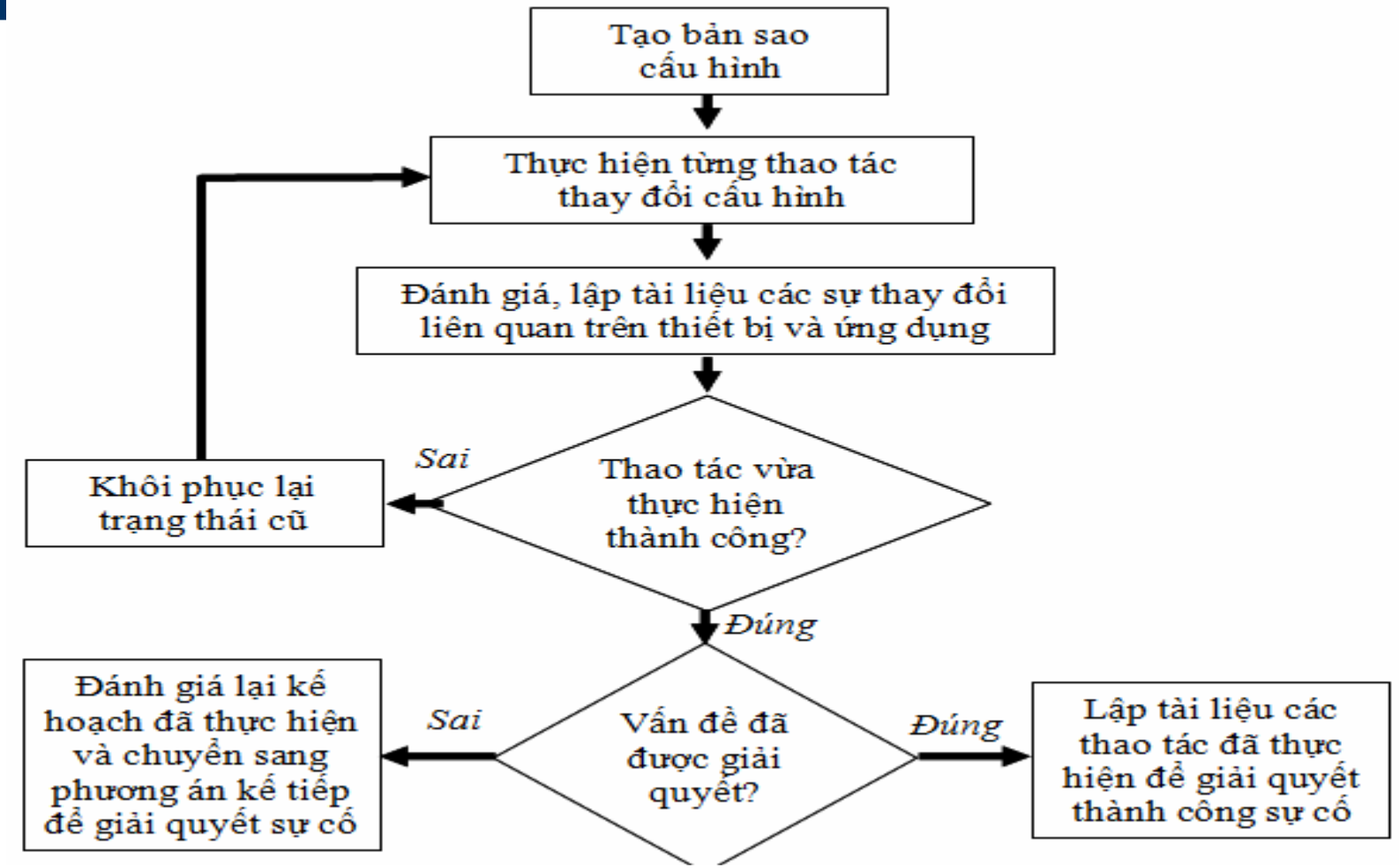
  Khắc phục sự cố khi dùng NAT, sử dụng các bước sau:

  - Sử dụng lệnh hiển thị quá trình dịch địa chỉ của NAT (Ví dụ lệnh *show ip nat translation* trong bộ định tuyến của Cisco). Ghi nhận xem có bản dịch nào được thực hiện không? Các bản dịch có như mong muốn?
  - Xóa bản dịch cũ của NAT và thử dùng một máy bên trong mạng truy cập đến nguồn tài nguyên bên ngoài mạng một số lần nữa để theo dõi quá trình dịch địa chỉ của NAT.
  - Sử dụng lệnh hỗ trợ gỡ rối NAT (ví dụ *debug ip nat*) để kiểm tra hoạt động dịch địa chỉ mạng của NAT.
  - Kiểm tra lại thông tin trong tập tin cấu hình xem các lệnh NAT bên trong và bên ngoài xem có đặt đúng giao diện trên bộ định tuyến hay không? Các dãy địa chỉ được thiết lập đúng không? Danh sách điều khiển được áp dụng cho NAT có đúng theo chính sách đặt ra không?
  - Nếu ACL và NAT có chức năng như mong đợi, vấn đề lỗi liên quan đến dịch mạng chắc chắn nằm trong một tầng cao hơn.

Các bước phát hiện sự cố ở tầng ứng dụng (5)

- Bước 4: Khắc phục sự cố ở các giao thức ở tầng trên
  - Mặc dù kết nối giữa nguồn và đích trong mạng đảm bảo hoạt động tốt thì các vấn đề liên quan đến sự cố mạng vẫn có thể tồn tại ở các tầng cao hơn, ví dụ như FTP, HTTP hoặc Telnet.
  - Các giao thức năm ở tầng ứng dụng nhưng khi hoạt động, nó có liên quan đến các giao thức ở tầng vận chuyển và chịu ảnh hưởng bởi bộ lọc hay bức tường lửa được thiết lập trên mạng.

Qui trình khắc phục các sự cố ở tầng ứng dụng



Hết chương 7!