TRƯỜNG ĐẠI HỌC CẦN THƠ

KHOA CÔNG NGHỆ THÔNG TIN & TT

Chương 2

CÁC PHƯƠNG PHÁP VÀ CÔNG CỤ GIẢI QUYẾT SỰ CỐ MẠNG

Giảng viên: **Phạm Hữu Tài**

NỘI DUNG

2.1. Cách tiếp cận tổng quát để giải quyết sự cố

2.2. Căn cứ vào mô hình phân tầng để khắc phục sự cố

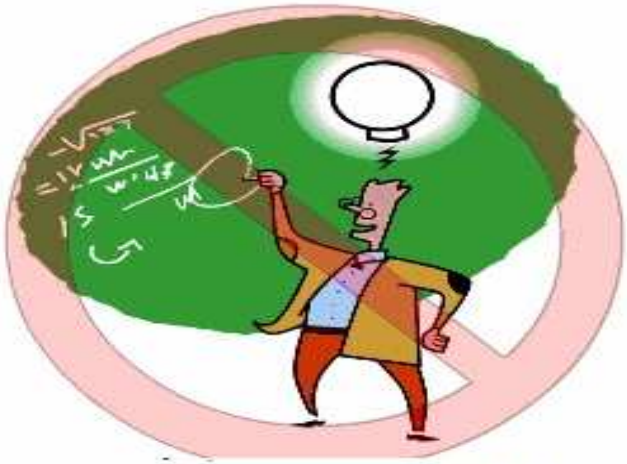
2.3. Tổng quát về các thủ tục xử lý sự cố

2.4. Các phương pháp và công cụ khắc phục sự cố

2.5. Các phần mềm hỗ trợ khắc phục sự cố

2.6. Giải quyết sự cố mạng

Cách tiếp cận tổng quát để giải quyết sự cố (1)



Cách tiếp cận của những nhà lý luận

Cách tiếp cận 'thử và sai'

Cách tiếp cận có hệ thống

Cách tiếp cận tổng quát để giải quyết sự cố (2)


Cách tiếp cận của những nhà lý luận

- Theo các tiếp cận **dựa vào lý thuyết** của các chuyên gia nghiên cứu lý thuyết
  - Thực hiện bằng cách: phân tích đi và phân tích lại một cách tỉ mỉ các tình trạng cho tới khi nguyên nhân chính xác nằm ở gốc của vấn đề đã được xác định và sửa chữa với độ chính xác đến từng chi tiết.
  - Quá trình thực hiện này là rất đáng tin cậy
  - Mất nhiều thời gian để khắc phục được vấn đề, đôi khi chỉ là những vấn đề đơn giản → *các công ty lại ít có khả năng chờ đợi hệ thống mạng của mình dừng chạy trong khoảng thời gian dài hàng giờ hay thậm chí hàng ngày để có thể phân tích toàn bộ các vấn đề liên quan đến hệ thống.*

Cách tiếp cận tổng quát để giải quyết sự cố (3)


Cách tiếp cận 'thử và sai'

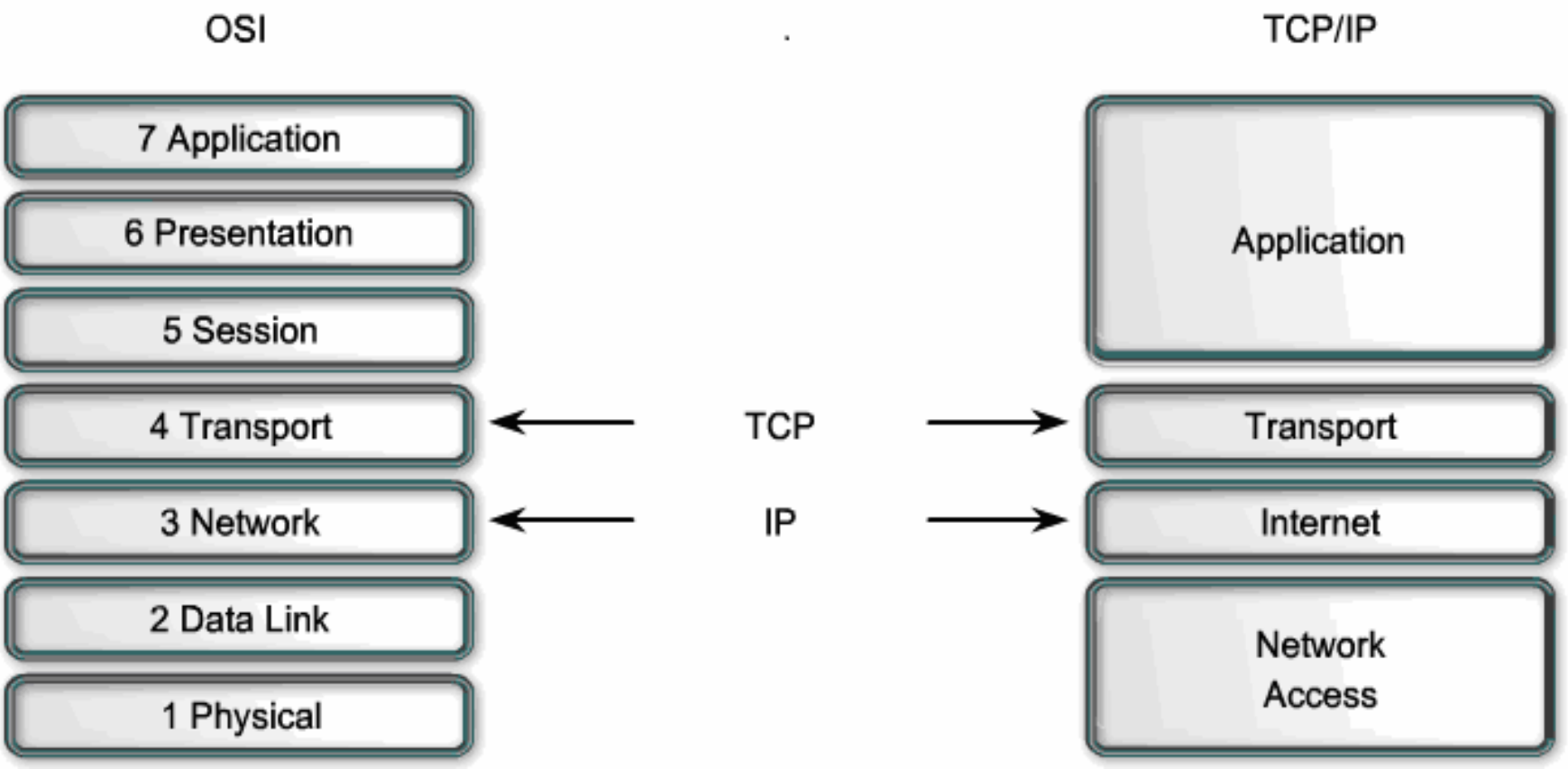
- Tiếp cập theo cách thức **'thử và sai'** sẽ hành xử 'thô bạo' trên các thiết bị của hệ thống để thực hiện thao tác tìm kiếm nguyên nhân gây ra sự cố.
  - Thực hiện theo cách tiếp cận này đơn giản là lần lượt thay thế tất cả các phần cứng, cài lại tất cả các phần mềm cho tới khi hệ thống hoạt động trở lại.
  - Việc thực hiện này có thể làm cho mạng có thể nhanh chóng vận hành trở lại nhưng điều này không có nghĩa là mạng đã hoạt động đúng cách như nó đã từng hoạt động.
  - Có thể đạt được một sự thay đổi trong việc xác định được vị trí của lỗi nhưng có thể không xác định được nguyên nhân gốc rễ của vấn đề → *hư hỏng tiềm tàng vẫn còn có thể tồn tại → đây không phải là cách tiếp cận đáng tin cậy.*

Cách tiếp cận tổng quát để giải quyết sự cố (4)


Cách tiếp cận có hệ thống

- **Tiếp cận có hệ thống**, đây là cách tiếp cận dung hoà các yếu tố giữa cả hai cách tiếp cận nêu trên.
- Điều quan trọng để phân tích và khắc phục sự cố mạng là căn cứ vào tổng thể hệ thống chứ không phải một phần nhỏ của một bộ phận nào đó.
- Một cách tiếp cận có hệ thống sẽ giảm thiểu được các sự nhầm lẫn và cắt giảm được thời gian chẩn đoán và khắc phục hơn là để lãng phí thời gian với thử và sai.

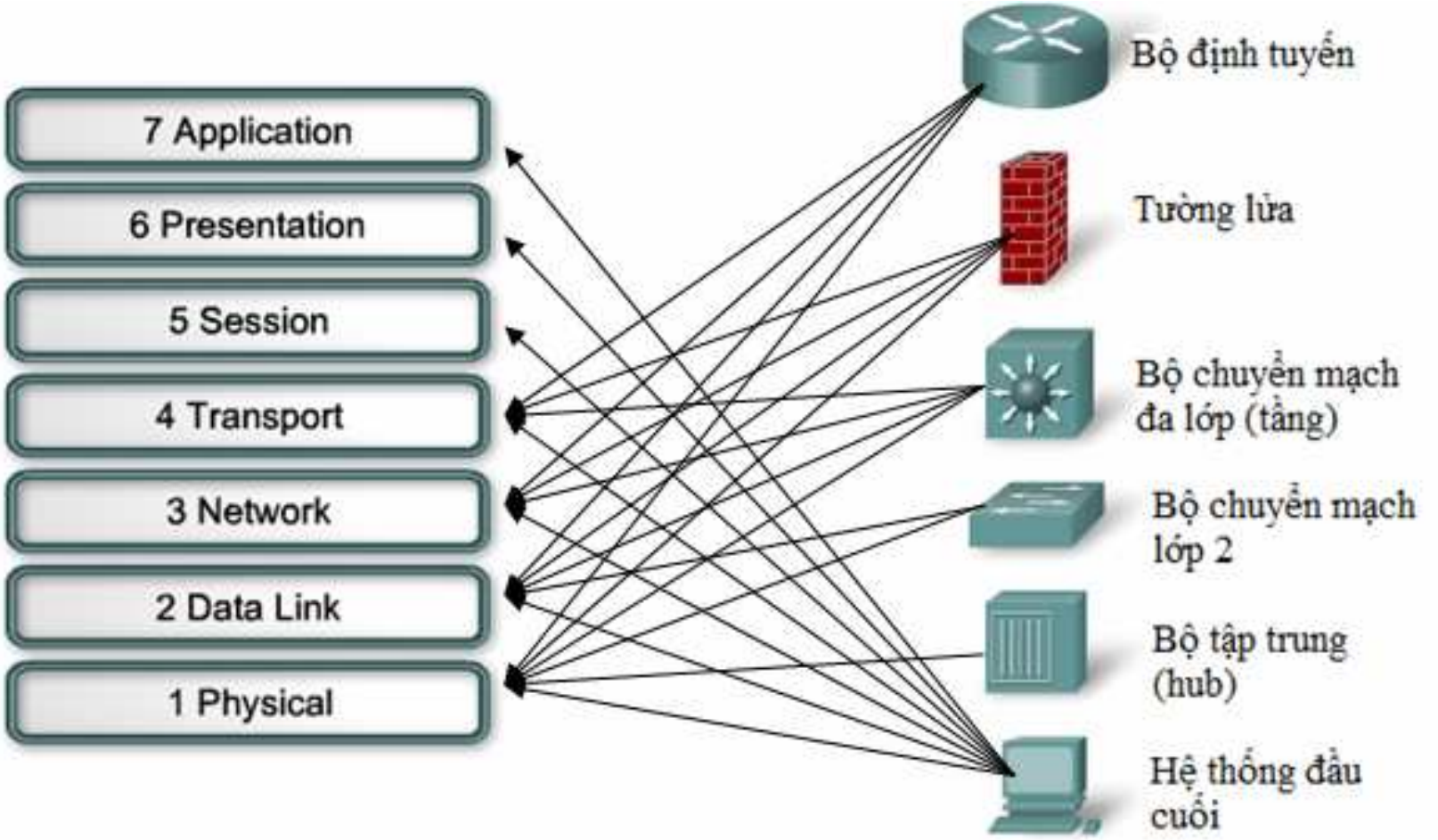
Căn cứ vào mô hình phân tầng để khắc phục sự cố (1)



Căn cứ vào mô hình phân tầng để khắc phục sự cố (2)

- Mô hình tham chiếu OSI
  - Mô hình tham chiếu OSI mô tả cách thức thông tin đi từ một phần mềm ứng dụng trên một máy tính di chuyển máy tính truyền qua một đường truyền mạng để đến và được xử lý trên một phần mềm ứng dụng trong máy tính khác.
  - Các tầng phía trên (các tầng từ 5-7) của mô hình OSI giải quyết với các vấn đề về ứng dụng của người dùng và thông thường chỉ được cài đặt trong phần mềm.
  - Các tầng bên dưới (các tầng từ 1-4) của mô hình OSI xử lý các vấn đề liên quan đến vận chuyển thông tin.
    - Tầng vận chuyển (tầng 4) và tầng mạng (tầng 3) thường thực hiện chỉ trong phần mềm.
    - Các tầng liên kết dữ liệu (tầng 2) và tầng vật lý (tầng 1) được thực hiện ở cả phần cứng và phần mềm.

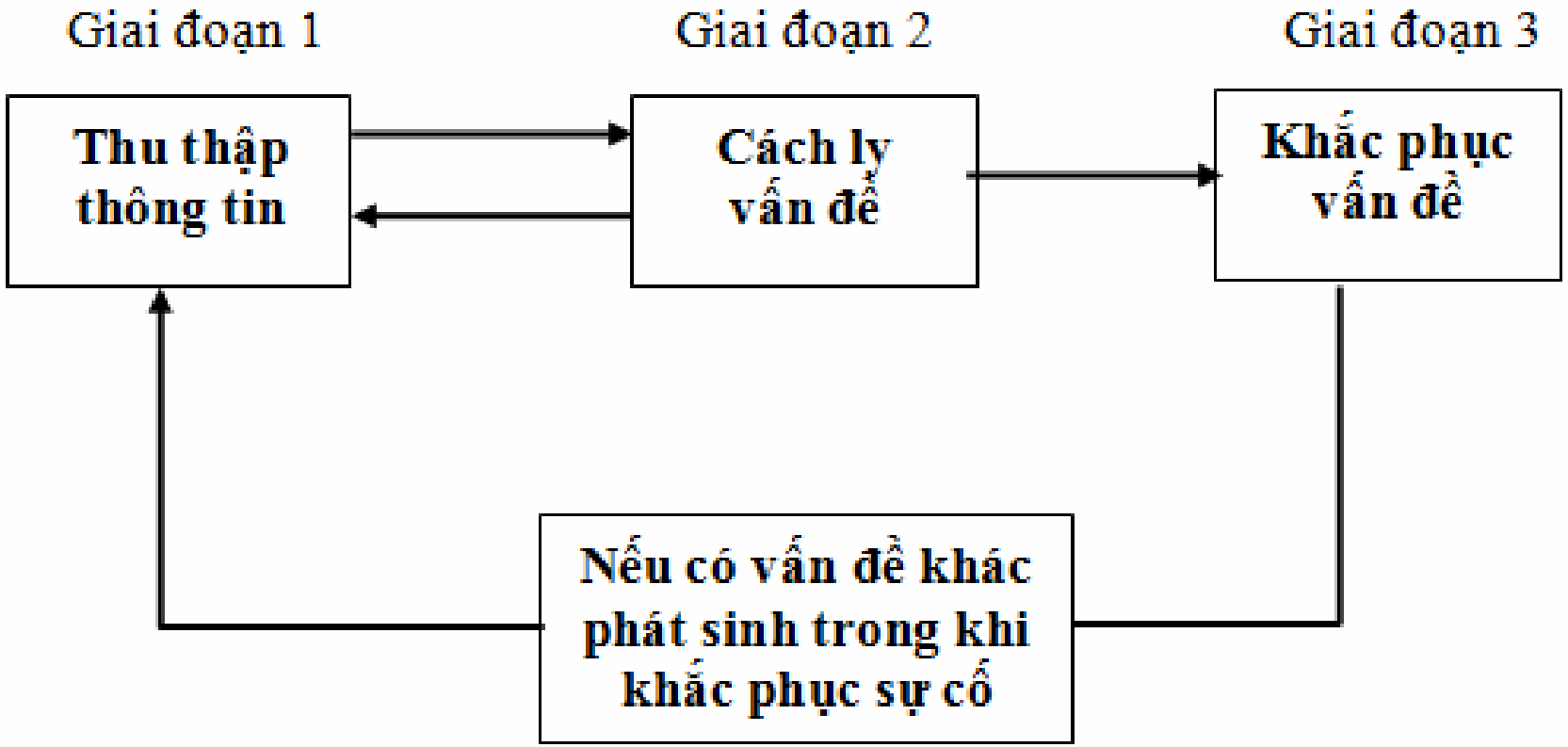
Căn cứ vào mô hình phân tầng để khắc phục sự cố (3)



Căn cứ vào mô hình phân tầng để khắc phục sự cố (4)

- Mô hình TCP / IP
  - **Tầng Ứng dụng** (Application) trong bộ giao thức TCP/IP thực sự kết hợp các chức năng của ba tầng trong mô hình OSI: tầng giao dịch, tầng trình bày và tầng ứng dụng, nó cung cấp truyền thông giữa ứng dụng như FTP, HTTP, SMTP,… trên các máy riêng biệt.
  - **Tầng Vận chuyển** (Transport) của giao thức TCP/IP có các chức năng tương ứng trực tiếp với các chức năng tầng vận chuyển trong mô hình OSI.
  - **Tầng Internet** trong bộ giao thức TCP/IP có các chức năng liên quan đến tầng mạng trong mô hình OSI.
  - **Tầng Truy cập mạng** (Network Access) trong bộ giao thức TCP/IP có các chức năng tương ứng với các chức năng của tầng vật lý và tầng liên kết dữ liệu trong mô hình OSI.

Tổng quát về các thủ tục xử lý sự cố (1)



Tổng quát về các thủ tục xử lý sự cố (2)

- Giai đoạn 1: *Thu thập thông tin liên quan đến các triệu chứng*
  - Khắc phục sự cố mạng bắt đầu với quá trình thu thập và ghi lại các triệu chứng được ghi nhận từ mạng, hệ thống đầu cuối và những người dùng.
  - Xác định các thành phần mạng bị ảnh hưởng và cách thức mà các chức năng của mạng đã thay đổi so với đường cơ sở mạng.
    → *Các triệu chứng có thể xuất hiện dưới nhiều hình thức khác nhau như: các cảnh báo từ các hệ thống quản trị mạng, các thông điệp điều khiển hay các phản ánh của người dùng.*
  - Sử dụng các câu hỏi phỏng vấn người dùng trực tiếp như là một phương thức để định vị vấn đề, từ đó khoanh vùng được phạm vi nhỏ hơn mà sự cố có thể xảy ra

Tổng quát về các thủ tục xử lý sự cố (3)

- Giai đoạn 2: *Cách ly vấn đề*
  - Vấn đề gây ra sự cố là chưa được xem là đã được cách ly cho đến khi nó chỉ còn là một vấn đề riêng rẽ duy nhất hoặc một tập hợp các vấn đề liên quan được xác định.
  - Thực hiện kiểm tra các đặc tính của các vấn đề tại các tầng luận lý của mạng để xác định các nguyên nhân có khả năng gây ra sự cố nhiều nhất.
  - Có thể thu thập thông tin và xem xét tài liệu các triệu chứng khác liên quan dựa vào các đặc tính vấn đề được xác định.

Tổng quát về các thủ tục xử lý sự cố (4)

- Giai đoạn 3: *Khắc phục những vấn đề đã được xác định*
  - Phải thực hiện cách ly và xác định đúng nguyên nhân của vấn đề
  - Nếu nhà quản trị mạng xác định rằng những hành động vừa thực hiện đã tạo nên một vấn đề khác, các giải pháp đã thử phải được ghi nhận lại, các thay đổi đã thực hiện phải bị loại bỏ → *quay lại giai đoạn thu thập thông tin liên quan các triệu chứng và cách ly các vấn đề*.

Tổng quát về các thủ tục xử lý sự cố (5)

- Những giai đoạn này không được loại trừ lẫn nhau.
- Khi thử khắc phục một vấn đề, một vấn đề khác có thể được tạo ra → *cần thu thập thêm các triệu chứng, cách ly và khắc phục được vấn đề mới.*
- Một chính sách khắc phục sự cố phải được thiết lập cho từng giai đoạn:
  - Chính sách cung cấp một cách nhất quán các trình tự thực hiện cho mỗi giai đoạn.
  - Chính sách bao gồm cả việc lập tài liệu cho mỗi phần của thông tin quan trọng.

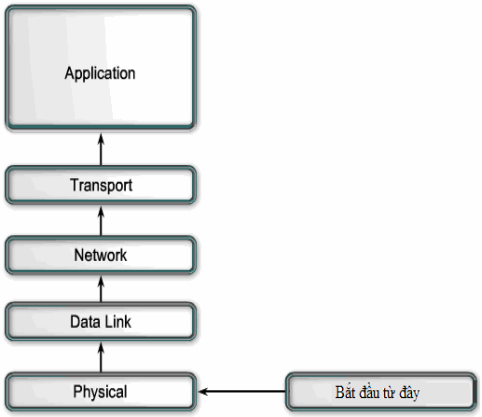
Các phương pháp và công cụ khắc phục sự cố (1)

- Các phương pháp khắc phục sự cố

  Có ba phương pháp tiếp cận chủ yếu để khắc phục sự cố mạng:

  – ***Tiếp cận từ dưới lên*** *(Bottom-up)*
  – ***Tiếp cận từ trên xuống*** *(Top-down)*
  – ***Chia để trị*** *(Divide and conquer)*

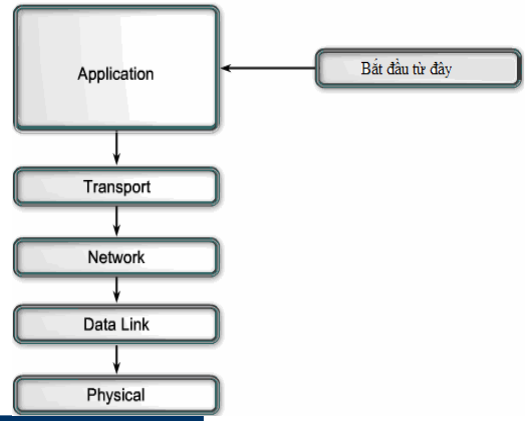
Các phương pháp và công cụ khắc phục sự cố (2)



- Phương pháp khắc phục sự cố **tiếp cận từ dưới lên**
  - Bắt đầu khắc phục sự cố với các thành phần vật lý của mạng và di chuyển lên qua các tầng trên của mô hình OSI cho đến khi nguyên nhân của vấn đề được xác định.
  - Xử lý sự cố theo cách từ dưới lên là một phương pháp tốt để thực hiện khi vấn đề được nghi ngờ nằm ở tầng vật lý.
  - Hầu hết các vấn đề về mạng nằm ở các tầng bên dưới

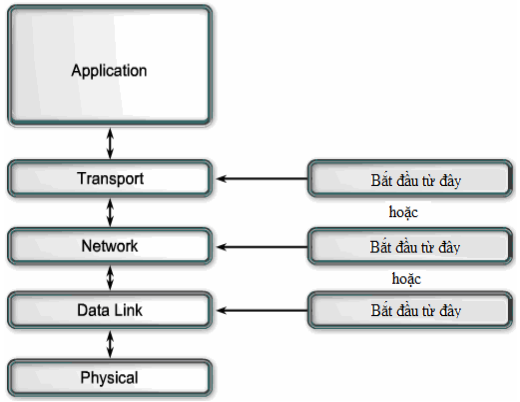
  → *thực hiện phương pháp tiếp cận từ dưới lên thường được kết quả cao hơn so với các phương pháp tiếp cận khác.*
  - Bất lợi:
    - Yêu cầu phải kiểm tra tất cả các thiết bị cùng với các giao diện kết nối mạng của nó cho đến khi nguyên nhân gây ra sự cố được tìm thấy.
    - Thách thức đầu tiên là việc quyết định nên bắt đầu việc xử lý sự cố với thiết bị nào.

Các phương pháp và công cụ khắc phục sự cố (3)



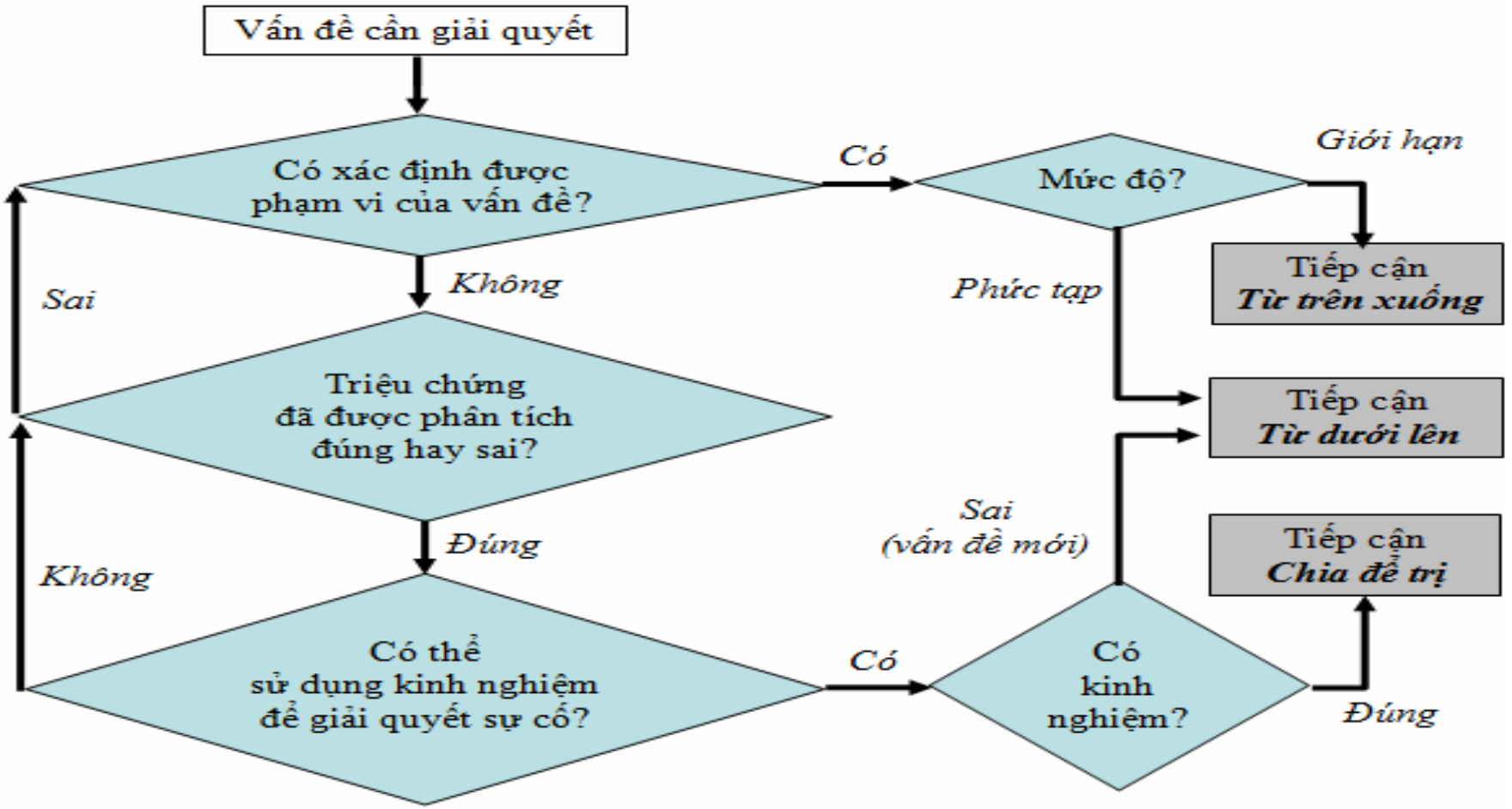
- Phương pháp khắc phục sự cố **tiếp cận từ trên xuống**
  - Bắt đầu với các ứng dụng của người dùng và di chuyển xuống thông qua các tầng của mô hình OSI cho đến khi nguyên nhân của vấn đề đã được xác định.
  - Các ứng dụng của người dùng một hệ thống cuối được thử nghiệm trước khi giải quyết các phần cụ thể khác của mạng.
  - Sử dụng cách tiếp cận này cho những vấn đề đơn giản hoặc khi chúng ta xác định rằng vấn đề xảy ra liên quan đến phần mềm.
  - Khuyết điểm:
    - Yêu cầu kiểm tra tất cả các ứng dụng mạng cho đến khi nguyên nhân có thể có của vấn đề được tìm thấy.
    - Ứng dụng nào được kiểm tra đầu tiên?

Các phương pháp và công cụ khắc phục sự cố (4)

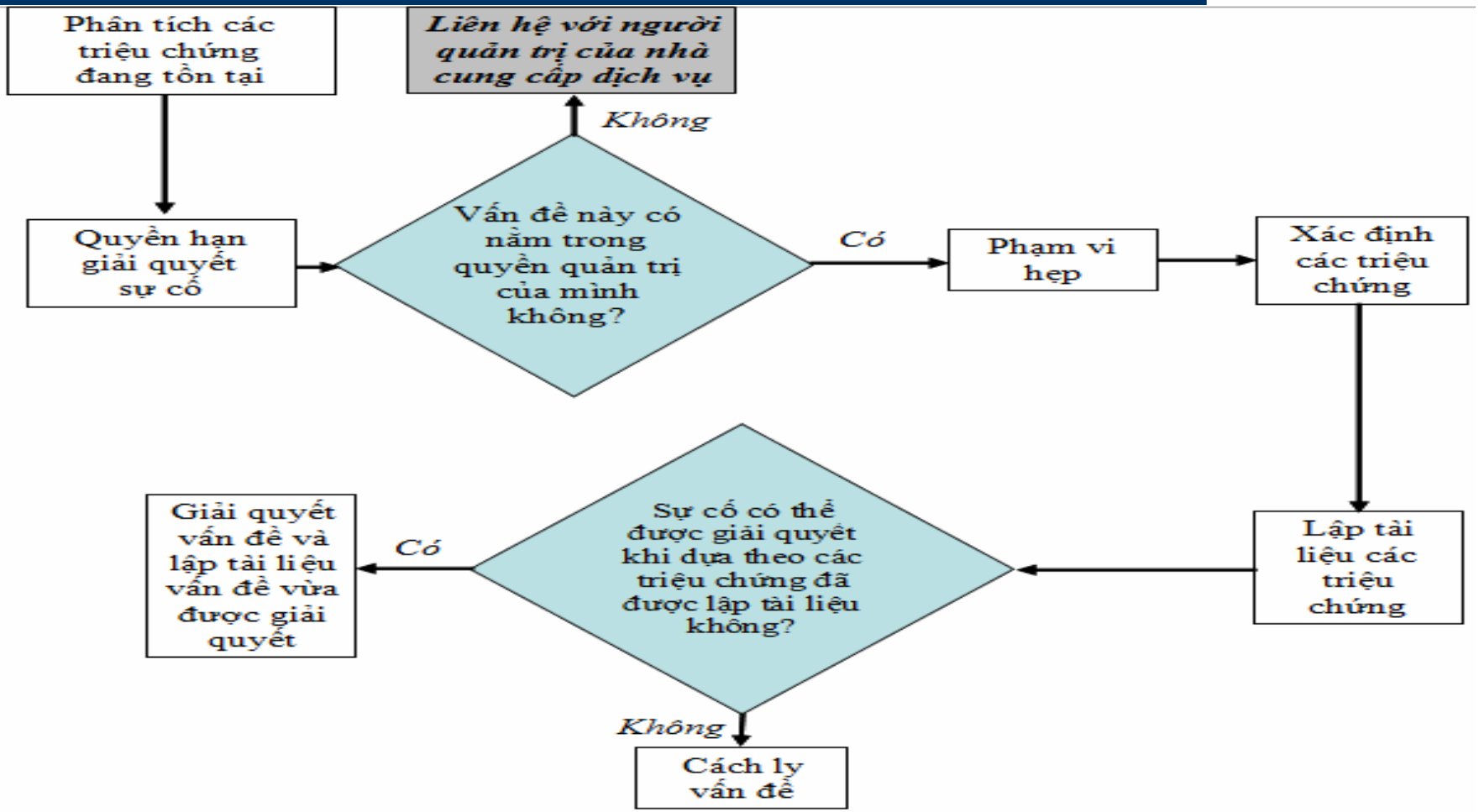


- Phương pháp khắc phục sự cố **tiếp cận chia để trị**
  - Bắt đầu bằng việc thu thập kinh nghiệm người dùng về vấn đề này, các tài liệu liên quan đến các triệu chứng
  - Tiến hành một chẩn đoán với tầng liên quan trong mô hình OSI mà ta bắt đầu điều tra.
  - Một khi ta đã xác minh rằng một tầng được hoạt động đúng thì ta giả sử rằng:
    - Các tầng bên dưới đã hoạt động tốt và tiến hành xem xét đến một tầng bên trên kế tiếp trong mô hình OSI.
    - Nếu một tầng trong mô hình OSI không hoạt động đúng, thì thực hiện kiểm tra xuống các tầng bên dưới của mô hình tầng OSI.

Hướng dẫn lựa chọn một phương pháp khắc phục sự cố



Thu thập các triệu chứng (1)



Thu thập các triệu chứng (2)

- Bước 1. *Phân tích các triệu chứng đang tồn tại*
  - Phân tích các triệu chứng thu thập được:
    - Từ các nhật ký đã được ghi nhận
    - Từ những người dùng trực tiếp sử dụng hay điều hành
    - Từ hệ thống đầu cuối bị ảnh hưởng

Thu thập các triệu chứng (3)

- Bước 2. *Xác định quyền hạn giải quyết sự cố*
  - Nếu vấn đề là ở ngoài sự kiểm soát của người quản trị

    → Liên hệ và thông báo vấn đề đến quản trị của nơi cung cấp dịch vụ để nhận được sự hỗ trợ trước khi tiếp tục thu thập các triệu chứng bổ sung.
  - Nếu vấn đề xảy ra trong hệ thống thuộc quyền quản lý, điều hành của người quản trị

    → Di chuyển đến bước tiếp theo.

Thu thập các triệu chứng (4)

- Bước 3. *Thu hẹp phạm vi*
  - Vấn đề xảy ra nằm ở tầng lõi, tầng phân phối hay tầng truy cập mạng?
  - Tại tầng xác định được → *tiến hành phân tích các triệu chứng hiện tại để có thể xác định những bộ phận nào của hệ thống các thiết bị có khả năng gây ra sự cố nhiều nhất.*

Thu thập các triệu chứng (5)

- Bước 4. *Thu thập các triệu chứng từ thiết bị nghi ngờ*
  - Sử dụng cách tiếp cận xử lý sự cố ở từng tầng, thu thập các triệu chứng của phần cứng và phần mềm trong các thiết bị nghi ngờ.
  - Bắt đầu với những bộ phận có nhiều khả năng gây lỗi nhất
  - Tiếp theo là vận dụng kiến thức và kinh nghiệm có được để xác định được các nguyên nhân gây sự cố nếu vấn đề liên quan đến cấu hình của phần cứng hay phần mềm.

Thu thập các triệu chứng (6)

- Bước 5. *Lập tài liệu các sự cố*
  - Đôi khi các vấn đề có thể giải quyết một cách dễ dàng bằng việc tham khảo lại các tài liệu giải quyết sự cố đã thực hiện trước đó.
  - Nếu sự cố chưa có trong tài liệu (vấn đề mới chưa được xử lý trước đó), chúng ta hãy bắt đầu giai đoạn cách ly vấn đề của qui trình xử lý sự cố tổng quát.
- *Chú ý: Sử dụng các lệnh debug, ping, telnet, traceroute*, các lệnh *show*,…

Đặt câu hỏi cho các người dùng đầu cuối

- Các câu hỏi nên đi thẳng vào vấn đề
- Sử dụng mỗi câu hỏi như là phương tiện để loại trừ hay khám phá được vấn đề của sự cố
- Dùng các thuật ngữ ở mức kỹ thuật sao cho người dùng có thể hiểu được
- Hỏi người dùng để biết được thời điểm đầu tiên xuất hiện sự cố
- Cái gì đã không xuất hiện kể từ khi lần cuối cùng nó vận hành
- Hỏi xem người dùng có thể tạo lại sự cố đã xảy ra
- Xác định đúng trình tự của các sự kiện trước khi sự cố xảy ra

Các phần mềm hỗ trợ khắc phục sự cố

- Phần mềm được sử dụng để thu thập và phân tích các triệu chứng liên quan đến sự cố.
- Các công cụ này còn cung cấp các chức năng giám sát và báo cáo để người quản trị mạng dựa vào các thông tin đó để thiết lập đường cơ sở mạng.
- Phần mềm hệ thống quản trị mạng (Network Management System - NMS) bao gồm các giám sát mức phần cứng, cấu hình và các công cụ quản trị lỗi của thiết bị → *giao diện đồ họa, dễ sử dụng*
- Các phần mềm quản trị thường được sử dụng *là CiscoView, HP Openview, Solar Winds* và *What's Up Gold*

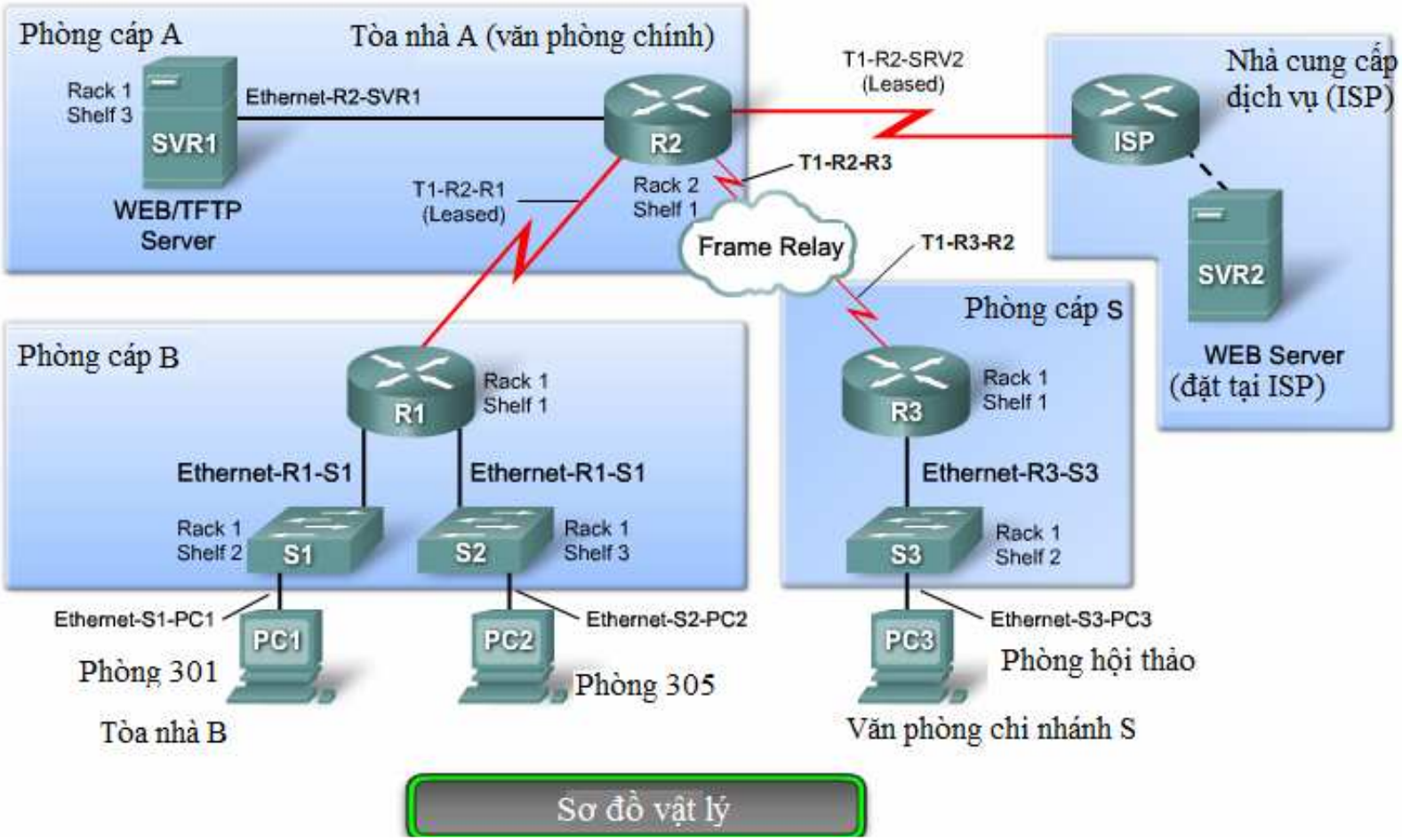
Giải quyết sự cố mạng

- Giải thích các sơ đồ mạng để nhận diện các sự cố mạng
  - Các sơ đồ mạng mô tả các địa chỉ IP của các giao diện mạng, các giao thức định tuyến IP, các thiết bị như tường lửa, chuyển mạch,...
  - Người chịu trách nhiệm khắc phục sự cố mạng cần có cả sơ đồ vật lý và luận lý để hỗ trợ cho quá trình khắc phục sự cố.

Sơ đồ vật lý mạng (1)

- Một sơ đồ mạng vật lý của hệ thống mạng cho biết vị trí và cách bố trí vật lý của các thiết bị kết nối vào mạng.
- Đối với thiết bị, thông tin ghi trên sơ đồ vật lý thường bao gồm:
  - Loại thiết bị
  - Nhà sản xuất, kiểu
  - Phiên bản hệ điều hành
  - Loại cáp loại được sử dụng
  - Đặc điểm kỹ thuật của cáp
  - Kiểu đầu nối
  - Thiết bị đầu cuối cáp

Sơ đồ vật lý mạng (2)

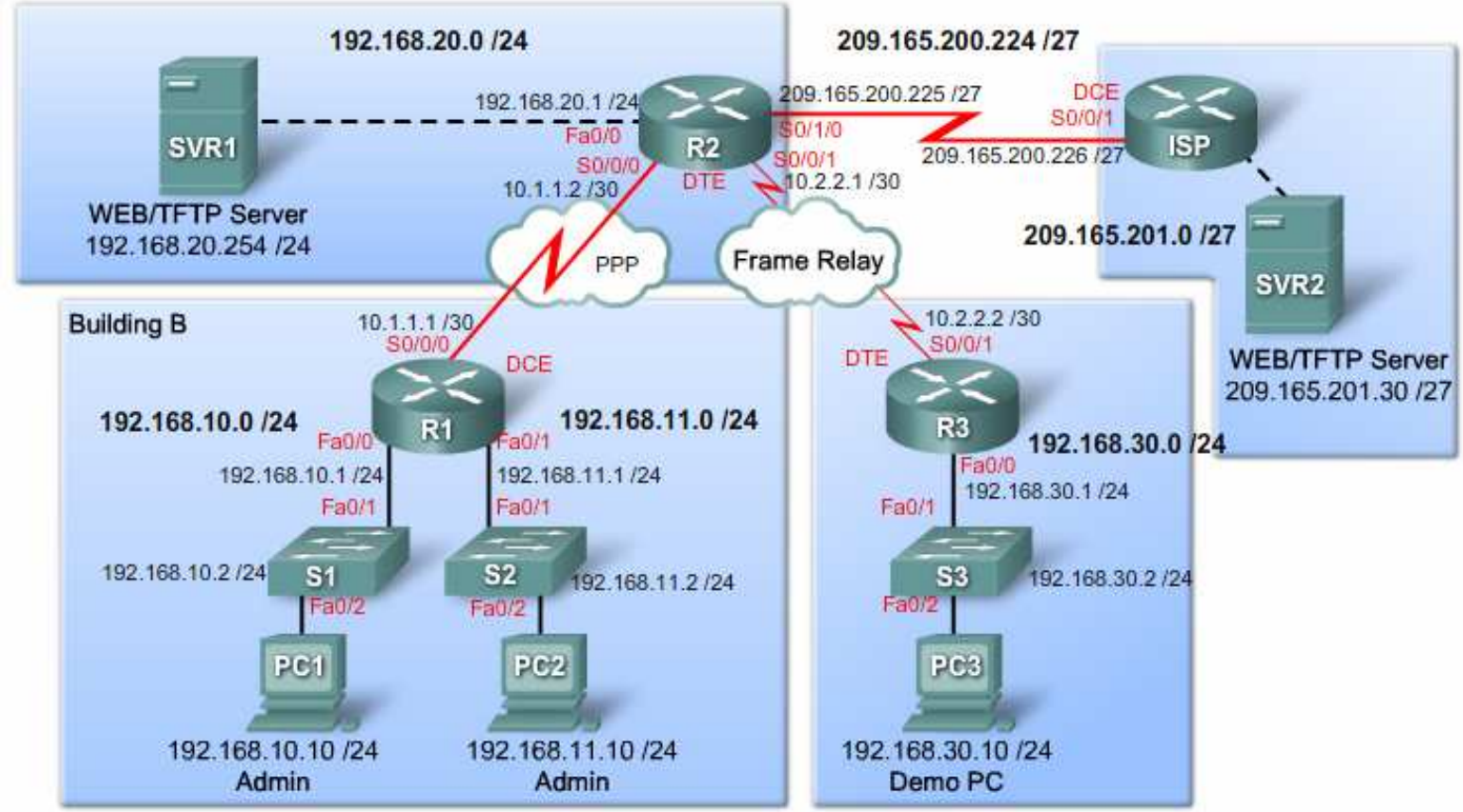


Sơ đồ vật lý

Sơ đồ luận lý của hệ thống mạng (1)

- Một sơ đồ luận lý của hệ thống mạng cho thấy cách thức dữ liệu được truyền trên mạng.
- Thông tin ghi trên một sơ đồ luận lý mạng có thể bao gồm:
  - Định danh thiết bị
  - Địa chỉ IP và mặt nạ mạng con
  - Định danh giao diện mạng
  - Kiểu kết nối
  - Số nhận dạng kênh cho mạch ảo
  - Các giao thức định tuyến (nếu có)
  - Các định tuyến tĩnh
  - Giao thức tầng liên kết dữ liệu được sử dụng cho các liên kết
  - Công nghệ WAN được sử dụng

Sơ đồ luận lý của hệ thống mạng (2)



Sơ đồ luận lý

Hết chương 2!