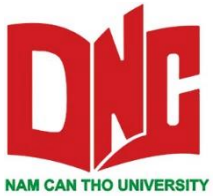
BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC NAM CẦN THƠ



QUẢN TRỊ MẠNG

Chương 6:

GIẢI QUYẾT SỰ CỐ MẠNG

Giảng viên: ThS. Nguyễn Minh Triết

Giải quyết sự cố mạng

6.1. Lập tài liệu về hệ thống mạng

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

6.3. Quá trình xử lý sự cố mạng tổng quát

6.4. Các phương pháp khắc phục sự cố

Giải quyết sự cố mạng

6.1. **Lập tài liệu về hệ thống mạng**

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

6.3. Quá trình xử lý sự cố mạng tổng quát

6.4. Các phương pháp khắc phục sự cố

Lập tài liệu về hệ thống mạng

- **Đường cơ sở mạng** (**Network baseline**): là một tập hợp các giá trị của các tham số được thu thập liên quan đến hoạt động thực tế của các thiết bị đang hoạt động trên hệ thống trong điều kiện hoạt động bình thường, ổn định.
- Đường cơ sở mạng gồm:
  - Bảng cấu hình mạng
  - Bảng thông tin cấu hình hệ thống đầu cuối
  - Sơ đồ hình trạng mạng

Lập tài liệu về hệ thống mạng (tt)

- *Bảng cấu hình mạng:*
  - Lưu thông tin chính xác, luôn cập nhật mới các hồ sơ liên quan đến phần cứng và phần mềm được dùng trong hệ thống mạng.
  - Các thông tin này sẽ được dùng để xác định chính xác các sự cố khi xảy ra trên hệ thống mạng.

Tên thiết bị	Tên giao diện	Địa chỉ MAC	Địa chỉ IP / Mặt nạ	Giao thức định tuyến động đang sử dụng
R1, Cisco 2611XM	fa0/0	0007 .8580.a159	192.168.10.1 /24	EIGRP 10
	fa0/1	0007 .8580.a160	192.168.11.1 /24	EIGRP 10
	s0/0/0	--- ---	10.1.1.1/30	OSPF
	s0/0/1	--- ---	Không kết nối	
R2, Cisco 2611XM	fa0/0	0007 .8580.a159	192.168.20.1 /24	EIGRP 10

Lập tài liệu về hệ thống mạng (tt)

- *Bảng thông tin cấu hình hệ thống đầu cuối:*
  - Chứa các bản ghi về phần cứng và phần mềm được dùng trong thiết bị đầu cuối như máy chủ, máy trạm trên hệ thống và các thiết bị đầu cuối khác (máy in, máy quét, điện thoại IP,…)
  - Một hệ thống đầu cuối bị cấu hình sai có thể tác động tiêu cực đối với hiệu suất tổng thể của một hệ thống mạng.

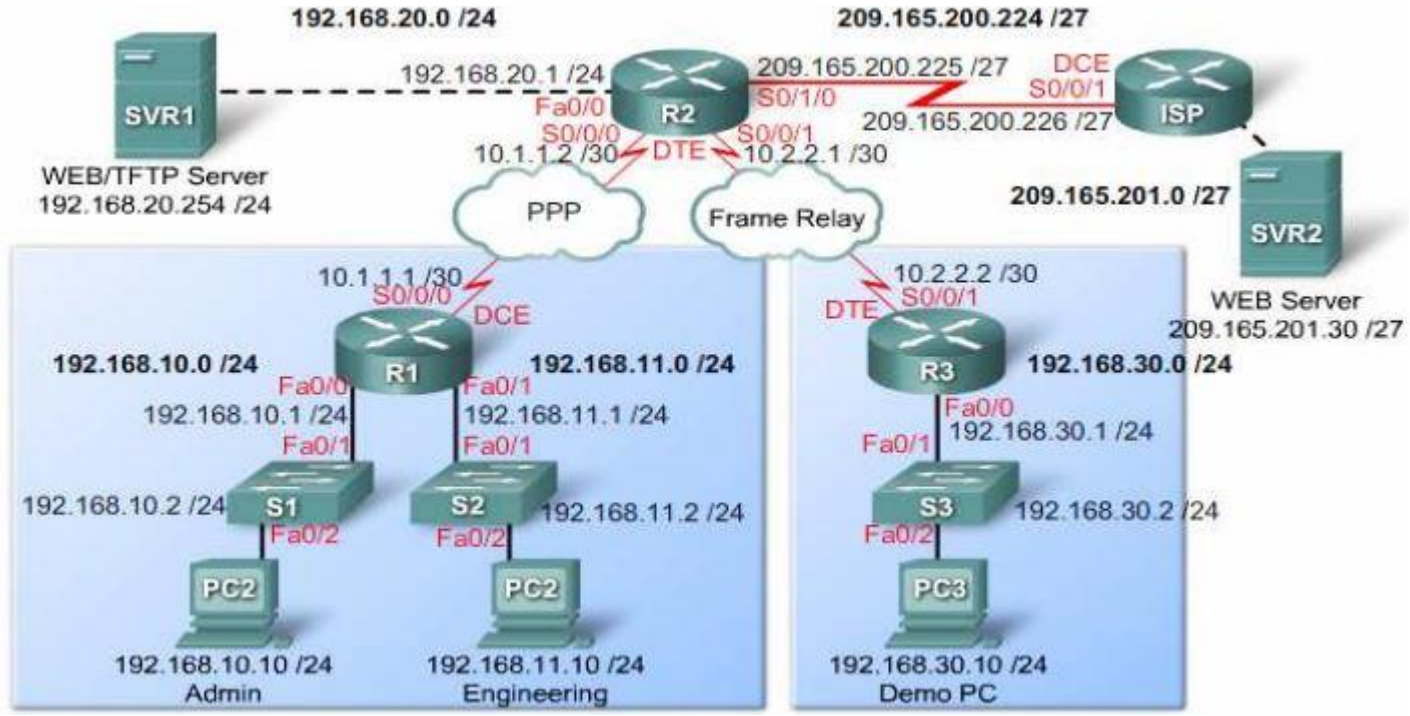
Tên thiết bị /	Hệ điều hành / phiên bản	Địa chỉ / mặt nạ	Địa chỉ gateway	Địa chỉ DNS server	Ứng dụng mạng	Ứng dụng yêu cầu băng thông cao	Vị trí lắp đặt
SRV_01 (Intranet Web/FTP)	UNIX	192.168.20.254 /24	192.168.20.1 /24	192.168.20.2	HTTP/ FTP		AR
SRV_02 (Internet Web)	UNIX	209.165.201.30 /27	209.165.201.1 /27	203.162.4.190	HTTP/ HTTPS		AR
PC_01 (Admin)	UNIX	192.168.10.10 /24	192.168.10.1 /24	192.168.20.2	FTP/ Telnet	VoIP	AR
PC_02	WinXP Pro-SP3	192.168.11.10 /24	192.168.11.1 /24	192.168.20.2		VoIP	SR

Lập tài liệu về hệ thống mạng (tt)

- *Sơ đồ hình trạng mạng:*
  - Là hình ảnh trình bày minh họa cho một hệ thống mạng, cách thức các thiết bị trong hệ thống kết nối với nhau và kiến trúc luận lý của hệ thống. Mỗi thiết bị mạng cần được trình bày trên sơ đồ với các ký hiệu hay biểu tượng tuân theo quy ước chuẩn.
  - Mỗi kết nối vật lý hay luận lý nên được biểu diễn bằng một đường đơn giản, hoặc ký hiệu thích hợp khác.
  - Các giao thức định tuyến được sử dụng trong hệ thống cũng có thể hiển thị.

Lập tài liệu về hệ thống mạng (tt)

- Sơ đồ hình trạng mạng (tt)



Lập tài liệu về hệ thống mạng (tt)

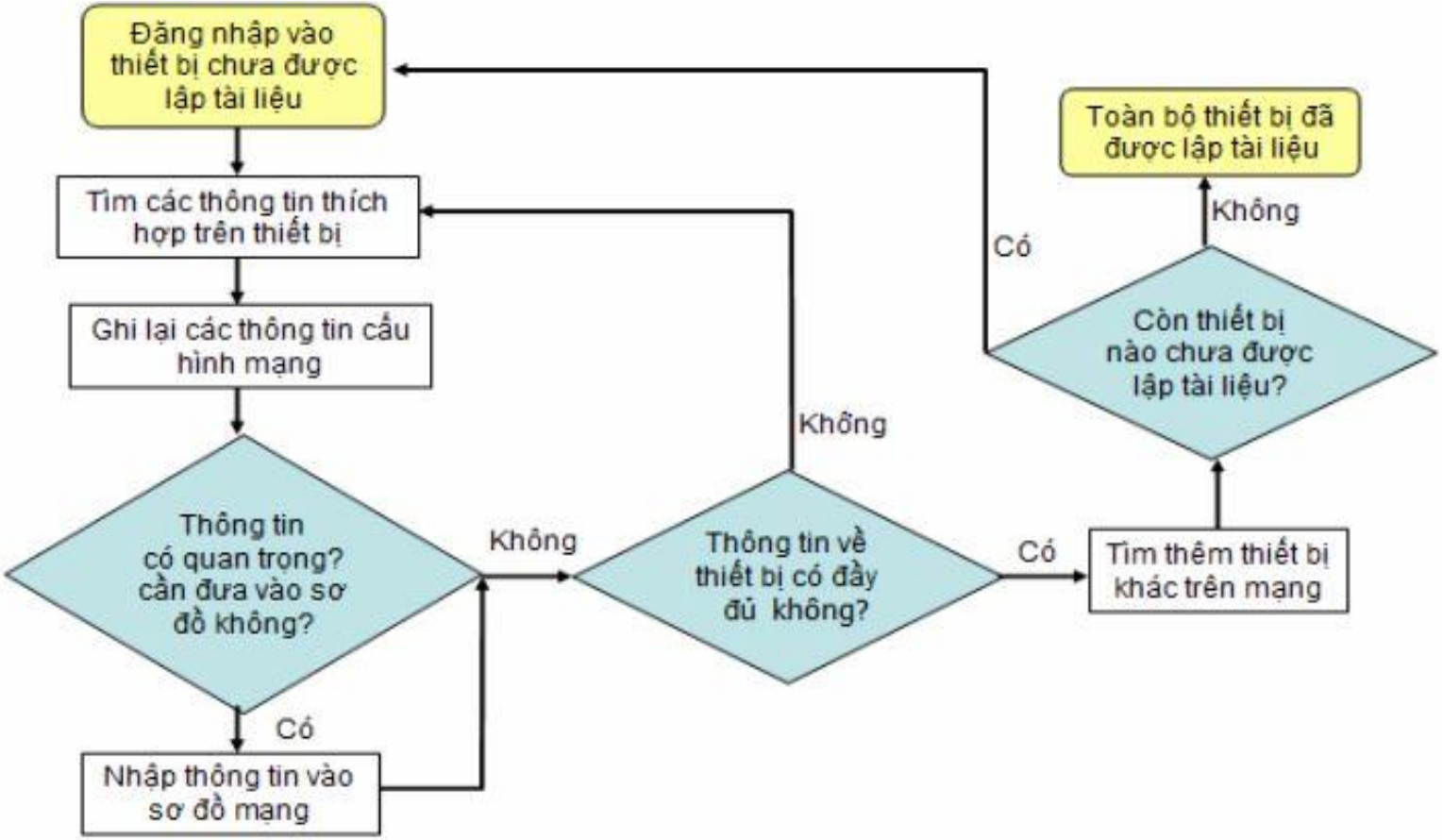
- Tài liệu hệ thống mạng "*phải*" được hoàn tất trong giai đoạn thiết kế, lắp đặt trước khi đưa vào sử dụng chính thức. Thực tế, có nhiều hệ thống mạng được thiết kế và đưa vào sử dụng không tuân theo đầy đủ các bước trong quy trình thiết kế.

→ Phải nhanh chóng lập tài liệu cho hệ thống mạng.

- Tài liệu là một phần không thể thiếu giúp cho quá trình giải quyết sự cố mạng được thực hiện một cách nhanh chóng, hiệu quả.

Lập tài liệu về hệ thống mạng (tt)

- Quy trình lập tài liệu hệ thống



Lập tài liệu về hệ thống mạng (tt)

- Đường cơ sở mạng là cơ sở cho phép nhà quản trị mạng xác định sự khác biệt giữa các hành vi bất thường khi so sánh với đường cơ sở mạng.
  - Xảy ra khi nâng cấp, phát triển hoặc thay đổi các mẫu lưu thông trên mạng.
  - Cung cấp cái nhìn vào bên trong của hệ thống để xem các thiết kế hệ thống hiện tại có chính xác với chính sách theo yêu cầu hay không.
  - Tồn tại một chuẩn mực để đo tính chất tối ưu của lưu lượng mạng và các mức nghẽn trên mạng nếu nó xảy ra.
  - Giúp nhà thiết kế hay người quản trị mạng phát hiện được những vấn đề tiềm ẩn.
  - Giúp nhà quản trị phát hiện các khu vực trong mạng hoạt động dưới mức hiệu suất chuẩn.

Lập tài liệu về hệ thống mạng (tt)

- Xác định dữ liệu cần thiết cho đường cơ sở mạng:
  - Phần mềm quản trị mạng thường được sử dụng vào các mạng lớn và phức tạp.
  - Trong các hệ thống mạng đơn giản, thiết lập đường cơ sở mạng có thể yêu cầu một sự kết hợp của các công việc: thu thập dữ liệu bằng thao tác thủ công và sử dụng các giao thức quản trị mạng đơn giản.

Lập tài liệu về hệ thống mạng (tt)

- Một số phần mềm quản trị mạng phổ biến:
  - Fluke Networks SuperAgent
  - SolarWinds
  - CyberGauge
  - Wireshark

Giải quyết sự cố mạng

6.1. Lập tài liệu về hệ thống mạng

6.2. **Cách tiếp cận tổng quát để giải quyết sự cố**

6.3. Quá trình xử lý sự cố mạng tổng quát

6.4. Các phương pháp khắc phục sự cố

Cách tiếp cận tổng quát để giải quyết sự cố

- **Tiếp cận dựa vào lý thuyết:**
  - 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 (tt)

- **Tiếp cận theo cách thức "thử và sai":**
  - 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 (tt)

- **Tiếp cận có hệ thống:**
  - Đây là cách tiếp cận dung hòa 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.

Giải quyết sự cố mạng

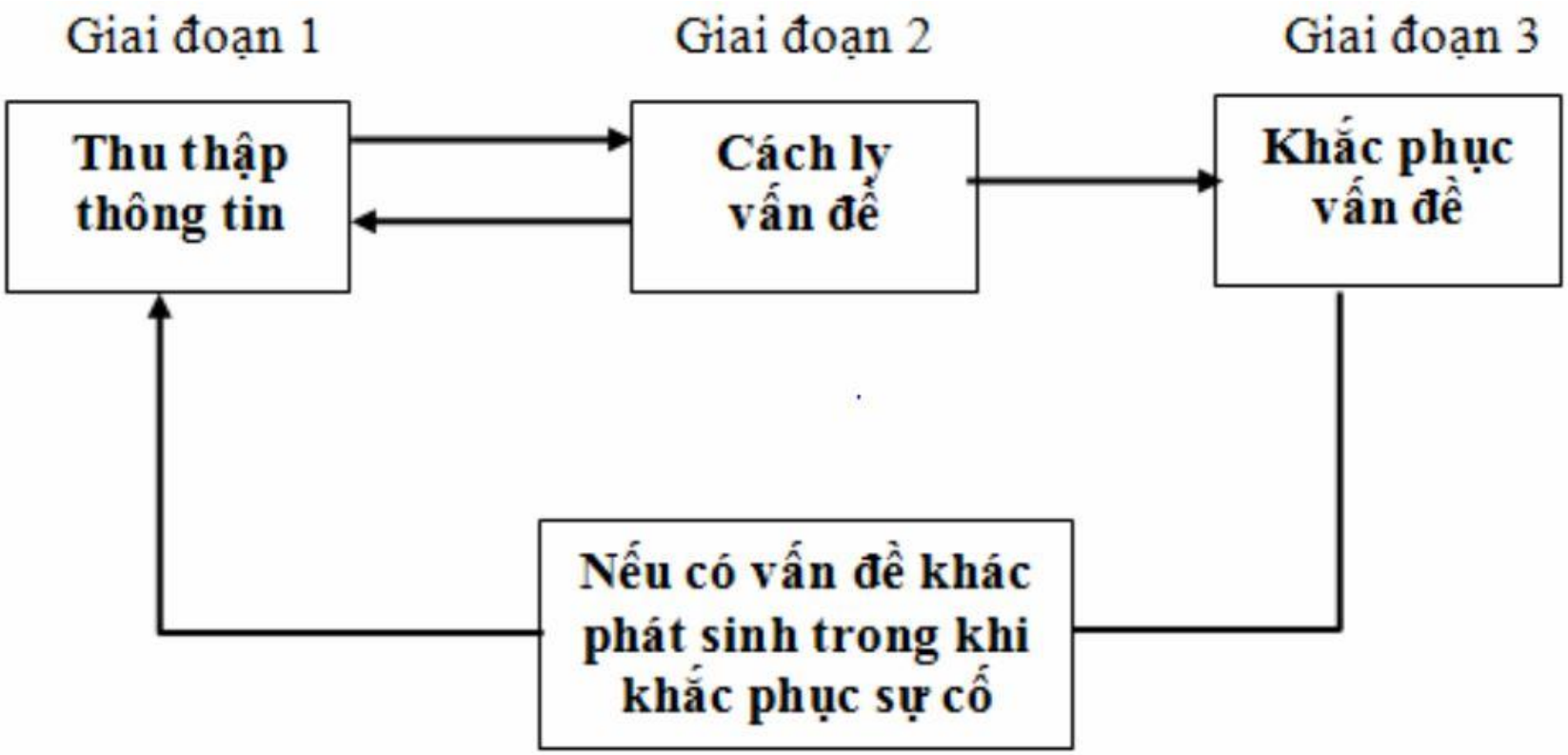
6.1. Lập tài liệu về hệ thống mạng

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

6.3. **Quá trình xử lý sự cố mạng tổng quát**

6.4. Các phương pháp khắc phục sự cố

Quá trình xử lý sự cố mạng tổng quát



Quá trình xử lý sự cố mạng tổng quát (tt)

- **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.

Quá trình xử lý sự cố mạng tổng quát (tt)

- **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.

Quá trình xử lý sự cố mạng tổng quát (tt)

- **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.
  - Tiến hành xử lý vấn đề đã xác định.

Quá trình xử lý sự cố mạng tổng quát (tt)

- 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.

Giải quyết sự cố mạng

6.1. Lập tài liệu về hệ thống mạng

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

6.3. Quá trình xử lý sự cố mạng tổng quát

6.4. **Các phương pháp khắc phục sự cố mạng**

Các phương pháp khắc phục sự cố mạng

- Mô hình tham chiếu OSI
  - Mô tả cách thức thông tin đi từ một phần mềm ứng dụng trên một máy tính, di chuyển dần xuống các tầng dưới rồi truyền qua một đường truyền mạng để đến và được xử lý trên một phần mềm ứng dụng trong máy tính khác.

Các phương pháp khắc phục sự cố mạng (tt)

- Các tầng phía trên (các tầng 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 1-4) của mô hình OSI xử lý các vấn đề liên quan đến vận chuyển thông tin.

Các phương pháp khắc phục sự cố mạng (tt)

- 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 khắc phục sự cố mạng (tt)

- **Phương pháp 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.

Các phương pháp khắc phục sự cố mạng (tt)

- Ưu điểm: 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 khắc phục sự cố mạng (tt)

- **Phương pháp 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.

Các phương pháp khắc phục sự cố mạng (tt)

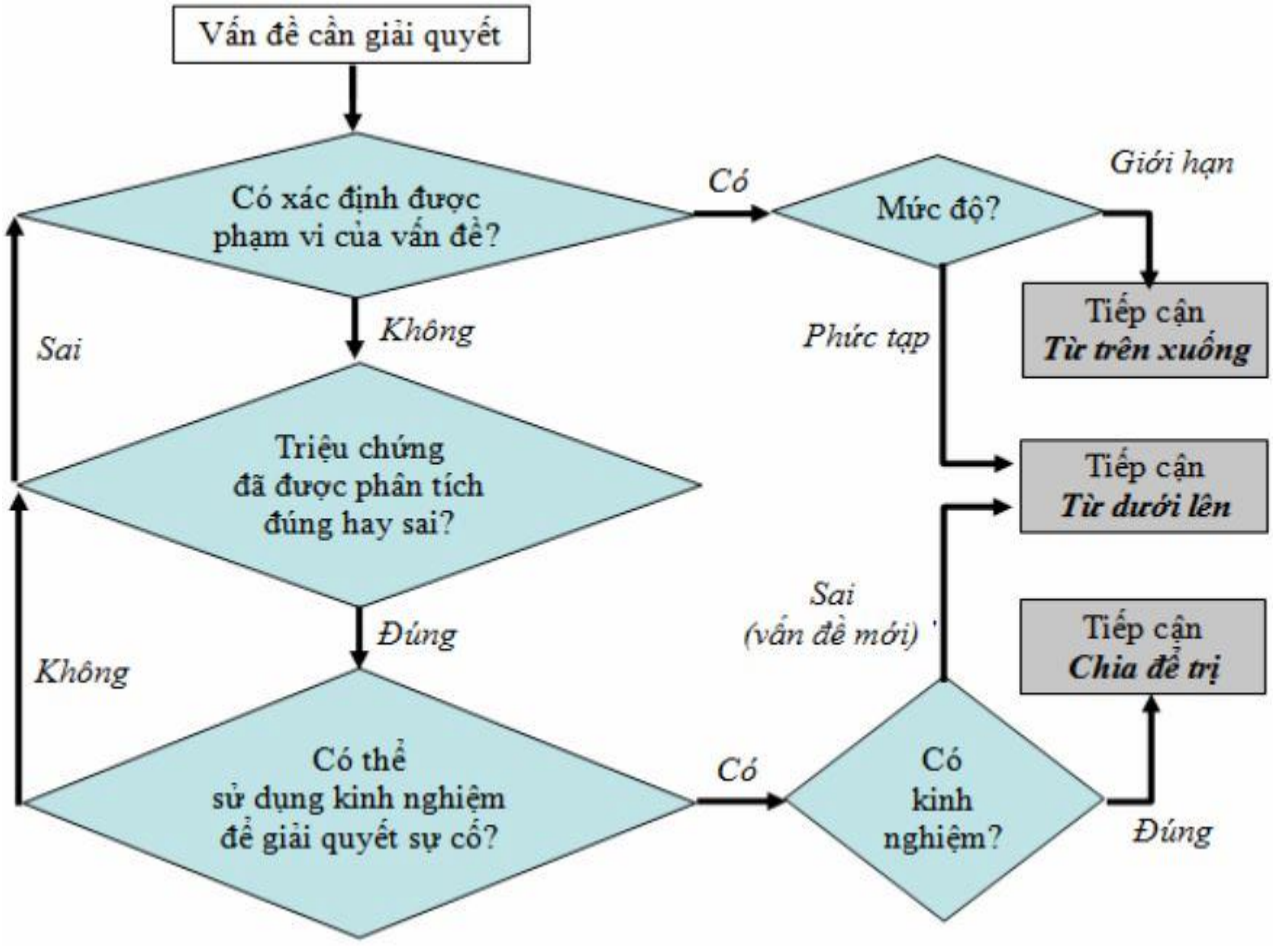
- Ưu điểm: sử dụng cách tiếp cận này rất tốt cho những vấn đề đơn giản hoặc khi xác định rằng vấn đề xảy ra liên quan đến phần mềm.
- Khuyết điểm:
  - Yêu cầu kiểm tra tất cả các ứng dụng mạng cho đến khi nguyên nhân có thể có của vấn đề được tìm thấy.
  - Ứng dụng nào được kiểm tra đầu tiên?

Các phương pháp khắc phục sự cố mạng (tt)

- **Phương pháp chia để trị:**
  - Bắt đầu bằng việc thu thập kinh nghiệm người dùng về vấn đề cần xử lý, các tài liệu liên quan đến các triệu chứng.
  - Tiến hành chẩn đoán với tầng liên quan trong mô hình OSI.
  - Một khi đã xác minh rằng một tầng được hoạt động đúng thì 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.

Các phương pháp khắc phục sự cố mạng (tt)

- Hướng dẫn lựa chọn một phương pháp khắc phục sự cố



Các phương pháp khắc phục sự cố mạng (tt)

- Phương pháp đặt câu hỏi cho người dùng 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.
  - 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 phương pháp khắc phục sự cố mạng (tt)

- 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, What's Up Gold,...