TRƯỜNG ĐẠI HỌC CẦN THƠ

KHOA CÔNG NGHỆ THÔNG TIN & TT

Chương 1

GIỚI THIỆU

Giảng viên: **Phạm Hữu Tài**

MỤC ĐÍCH YÊU CẦU

- **Mục đích:**

  Với một hệ thống mạng máy tính, tài liệu liên quan đến hệ thống thì rất quan trọng cho quá quá trình quản trị và giải quyết sự cố khi có xảy ra. Chương này sẽ giúp người đọc biết cách lập tài liệu của một hệ thống mạng theo một qui trình chuẩn mực và cách thiết lập đường cơ sở mạng, đây là trạng thái hoạt động ổn định trên hệ thống thực được người quản trị sử dụng để đánh giá tình trạng của hệ thống nếu có sự cố xảy ra.

- **Yêu cầu:**

  – Sinh viên nắm vững cách thức lập tài liệu của một hệ thống mạng

  – Nắm vững cách thức và sử dụng công cụ xây dựng được đường cơ sở mạng

NỘI DUNG

- 1.1. Lập tài liệu về hệ thống mạng
- 1.2. Bảng cấu hình mạng
- 1.3. Bảng cấu hình hệ thống đầu cuối
- 1.4. Sơ đồ hình trạng mạng
- 1.5. Qui trình lập tài liệu hệ thống mạng
- 1.6. Đường cơ sở của hệ thống mạng

Lập tài liệu cho hệ thống mạng (1)

- **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.

Lập tài liệu cho hệ thống mạng (2)

1. Bảng cấu hình mạng
2. Bảng thông tin cấu hình hệ thống đầu cuối
3. Sơ đồ hình trạng mạng

Bảng cấu hình mạng (1)

- Bảng cấu mạng phải 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

Bảng cấu hình mạng (2)

- Loại thiết bị, số hiệu mẫu (model)
- Tên thiết bị dùng trên mạng
- Tên phần mềm hệ thống (IOS)
- Vị trí lắp đặt của thiết bị (toà nhà, tầng, phòng, …)
- Nếu đó là một thiết bị mô-đun, bao gồm tất cả các kiểu của mô-đun và khe cắm mô-đun trên thiết bị.
- Các địa chỉ vật lý (đ/c MAC) của giao diện trên thiết bị
- Các địa chỉ luận lý (địa chỉ tầng Mạng) đặt trên giao diện mạng
- Thông tin quan trọng về mặt vật lý của thiết bị

Bảng cấu hình mạng (3)

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

Tên thiết bị, kiểu (model), địa chỉ quản trị	Tên giao diện	Tốc độ	Kiểu truyền	Trạng thái STP (Fwd / Block)	Port Fast (Yes / No)	Trunk	Ether Channel (L2 or L3)	VLANs	Ghi chú
S1, Cisco WS-C3550-24-SMI, 192.168.10.2 /24	fa0/1	100	Auto	Fwd	No	On	L2	1	Kết nối tới R1
	fa0/2	100	Auto	Fwd	No	On	L2	1	Kết nối tới máy 2
	fa0/3								Không kết nối
	fa0/4								Không kết nối

Bảng cấu hình hệ thống đầu cuối (1)

- Bảng cấu hình hệ thống đầu cuối chứa các bản ghi chuẩn về phần cứng và phần mềm được dùng trong thiết bị đầu cuối như máy chủ, máy quản trị và các 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.

Bảng cấu hình hệ thống đầu cuối (2)

- Tên thiết bị
- Hệ điều hành và phiên bản
- Địa chỉ IP / mặt nạ
- Cổng mặc định (default gateway), địa chỉ máy chủ DNS, và địa chỉ máy chủ WINS (nếu có)
- Các ứng dụng mạng yêu cầu băng thông cao mà các đầu cuối hệ thống đang sử dụng

Bảng cấu hình hệ thống đầu cuối (3)

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
PC_03 (demo)	Win7 Pro	192.168.30.10 /24	192.168.30.1 /24	192.168.30.2		VoIP/ Streaming Video	TR

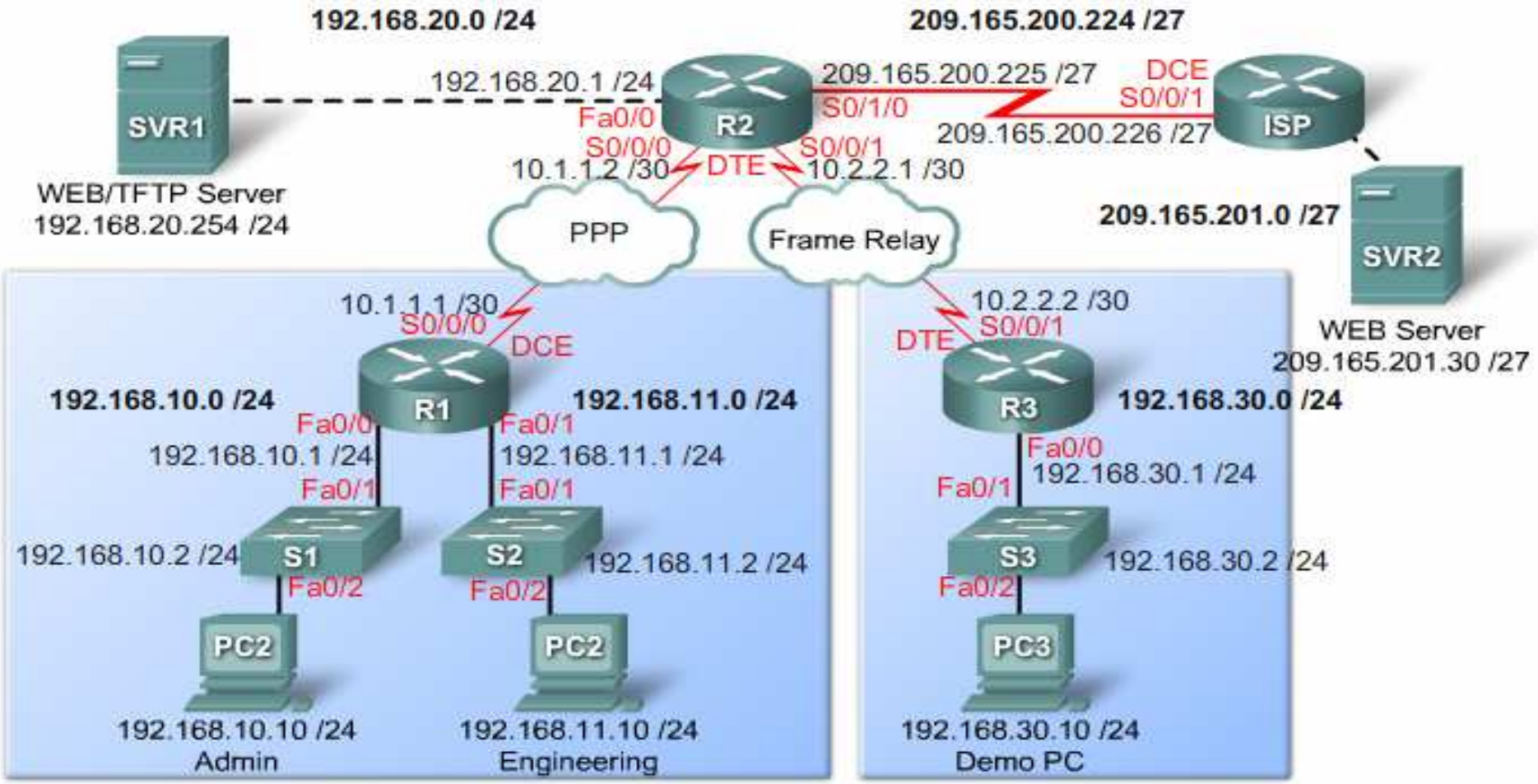
Sơ đồ hình trạng mạng (1)

- Sơ đồ hình trạng mạng là hình ảnh trình bày minh hoạ 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.

Sơ đồ hình trạng mạng (2)

- Yêu cầu tối thiểu cho các sơ đồ hình trạng mạng bao gồm các thông tin như sau:
  - Biểu tượng cho tất cả các thiết bị trong hệ thống và cách thức chúng được kết nối với nhau.
  - Kiểu các giao diện
  - Số hiệu của giao diện
  - Địa chỉ IP / mặt nạ mạng con

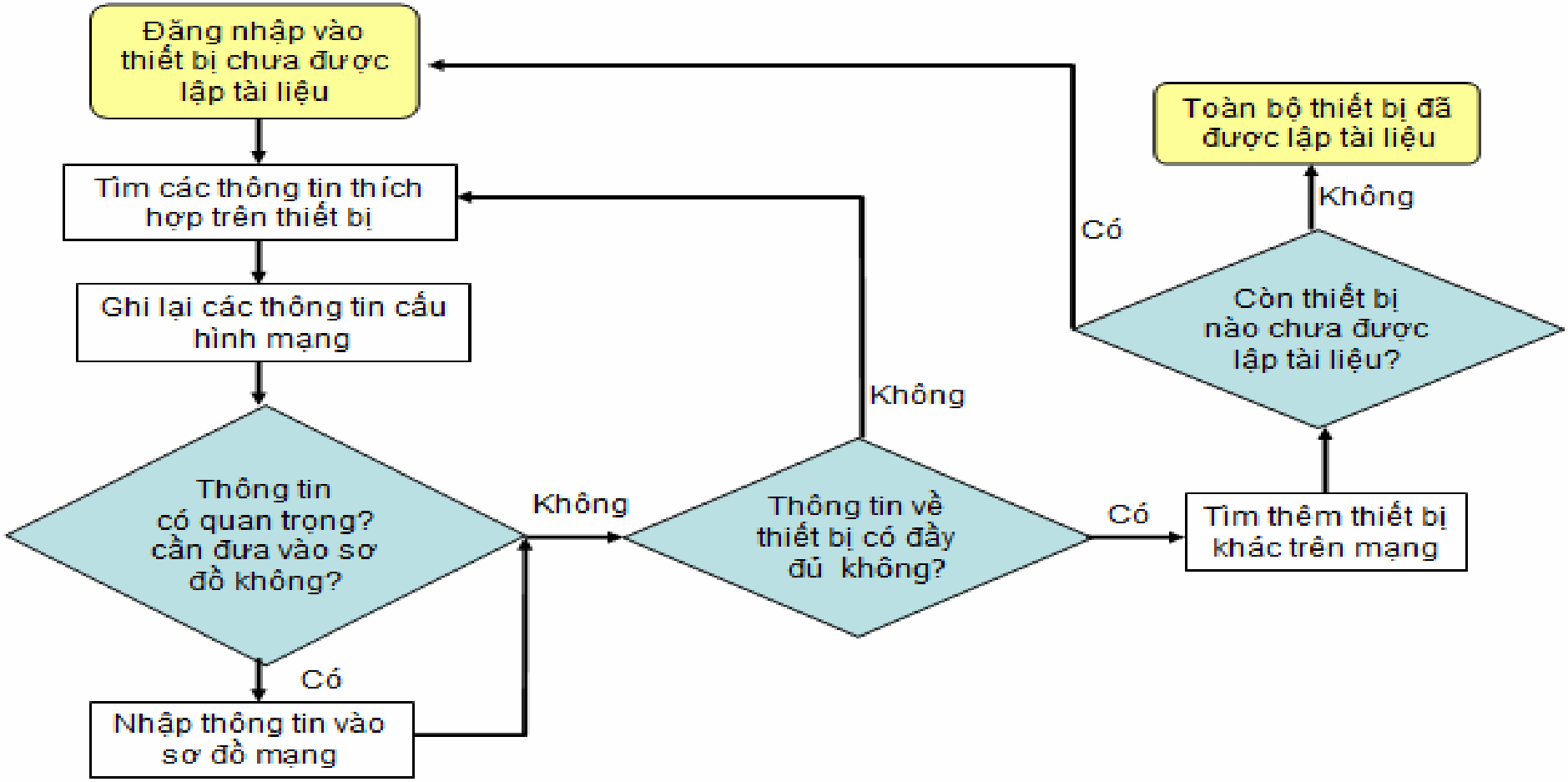
Sơ đồ hình trạng mạng (3)



Qui trình lập tài liệu hệ thống mạng (1)

- 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 qui 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.**

Qui trình lập tài liệu hệ thống mạng (2)



Qui trình lập tài liệu hệ thống mạng (3)

- Các lệnh cần thiết cho quá trình lập các tài liệu mạng này bao gồm:
- Lệnh ***ping*** được sử dụng để thử nghiệm kết nối đến các thiết bị ở xa trước khi đăng nhập vào chúng.
- Lệnh ***telnet*** được sử dụng để đăng nhập từ xa đến một thiết bị để truy cập thông tin hay cấu hình thiết bị.
- Lệnh ***traceroute*** (hay ***trace, tracert***) được sử dụng để xác định thông tin liên quan đến vấn đề đường đi từ nguồn đến đích của gói tin.
- Lệnh ***show ip interface brief*** được sử dụng đến sẽ hiển thị tình trạng *bật/tắt* và địa chỉ IP của tất cả các giao diện trên một thiết bị.
- Lệnh ***show ip route*** được sử dụng để hiển thị thông tin trong bảng định tuyến của một bộ định tuyến để học các nhánh mạng được kết nối trực tiếp với các bộ định tuyến láng giềng, từ các thiết bị khác ở xa (thông qua các tuyến đường được học) và các giao thức định tuyến đã được định cấu hình.
- Lệnh ***show cdp neighbor detail*** được dùng để lấy được thông tin chi tiết về các thiết bị (của hãng Cisco) láng giềng đang kết nối trực tiếp với bộ định tuyến đó.

Đường cơ sở của hệ thống mạng (1)

- Thiết lập được một đường cơ sở mạng là rất cần thiết để vận hành hệ thống mạng.
- Các câu trả lời cho những câu hỏi đặt ra khi giải quyết sự cố mạng sau đây:
  - *Làm thế nào để hệ thống mạng máy tính hoạt động như trong một ngày bình thường hoặc trung bình giữa các ngày?*
  - *Đâu là những vùng sử dụng cao hơn/thấp hơn mức trung bình (đường cơ sở mạng)?*
  - *Đâu là những vùng mà sai sót thường xảy ra nhất?*
  - *Những mức ngưỡng cần nào được đặt ra cho các thiết bị cần được giám sát?*
  - *Các chính sách của hệ thống mạng có thể được xác định?*

Đường cơ sở của hệ thống mạng (2)

- 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 thể mang lại đúng các 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

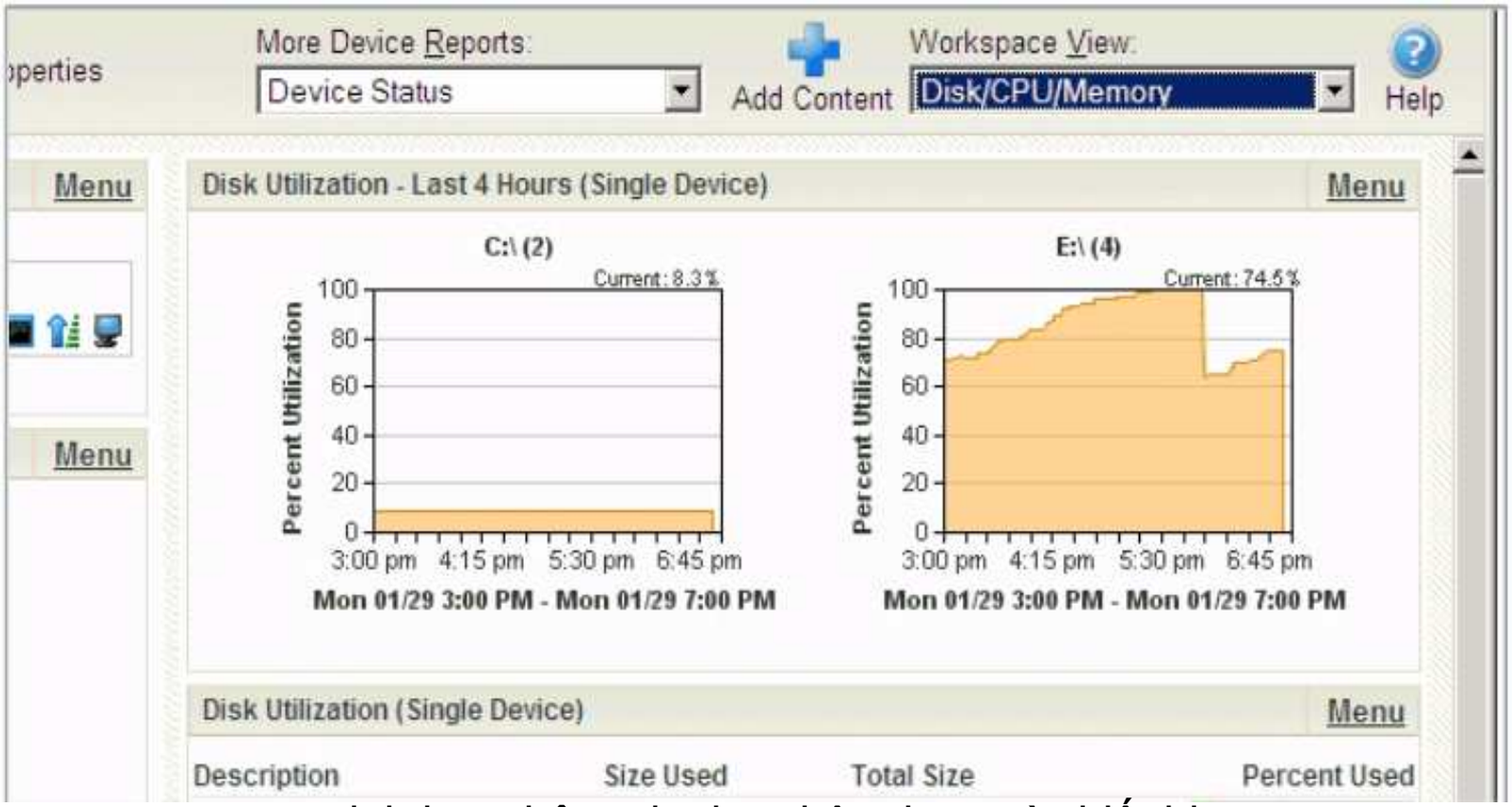
Các bước thiết lập đường cơ sở cho một hệ thống mạng (1)

- **Lập kế hoạch cho việc thiết lập đường cơ sở mạng lần đầu tiên**
  - *Bước 1. Xác định kiểu dữ liệu cần thu thập thông tin để xác lập hiệu suất chuẩn*
  - *Bước 2. Xác định các thiết bị và cổng giao diện cần thu thập thông tin*
  - *Bước 3. Xác định thời hạn cần ghi nhận hiệu suất mạng*

Các bước thiết lập đường cơ sở cho một hệ thống mạng (2)

- *Bước 1. Xác định kiểu dữ liệu cần thu thập thông tin để xác lập hiệu suất chuẩn*
  - *Chọn một số biến đại diện dựa trên các thông tin trong chính sách đã được xác định khi thiết kế hệ thống mạng.*
    - *Chọn nhiều biến đại diện để thu thập thông tin, số lượng thông tin có thể bị tràn ngập, làm cho phân tích các dữ liệu thu thập được gặp khó khăn.*
    - *Chọn ít số biến đại diện, thông tin thu được có thể không phản ánh hết được các thông số dùng để đánh giá hiệu suất một hệ thống mạng.*
  - *Cách tốt nhất là bắt đầu xác định các thông số từ các giao diện trên các thiết bị mạng và hiệu quả xử lý của CPU trên các thiết bị*

Các bước thiết lập đường cơ sở cho một hệ thống mạng (3)

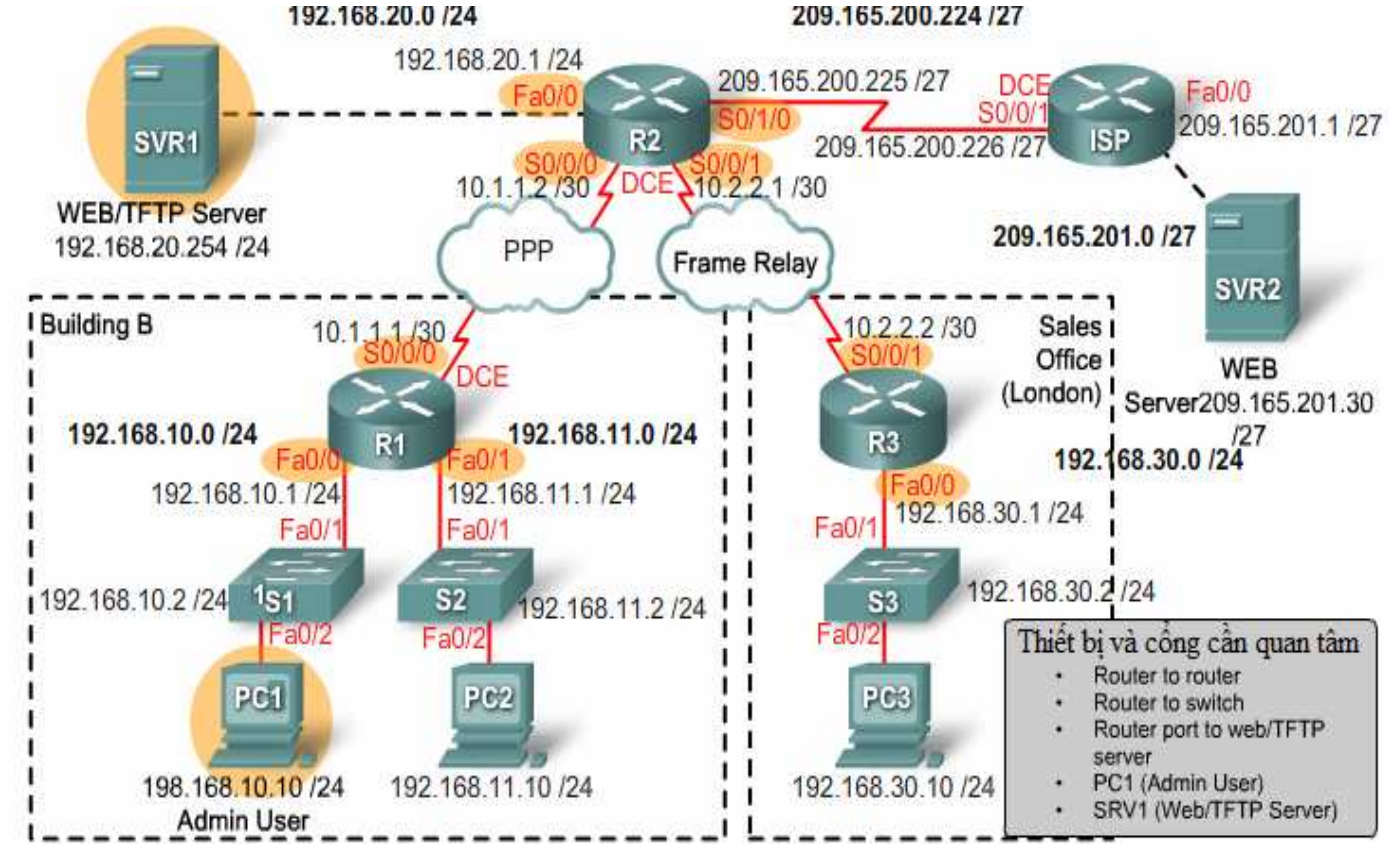


Minh hoạ thông tin thu nhận được từ thiết bị
(sử dụng phần mềm What's Up Gold)

Các bước thiết lập đường cơ sở cho một hệ thống mạng (4)

- *Bước 2. Xác định các thiết bị và cổng giao diện cần thu thập thông tin*
  - *Cổng của thiết bị mạng kết nối với các thiết bị mạng khác*
  - *Các máy chủ trên mạng*
  - *Các người dùng chủ chốt trong hệ thống*
  - *Các thông tin quan trọng khác liên quan đến hoạt động của hệ thống.*

Các bước thiết lập đường cơ sở cho một hệ thống mạng (5)

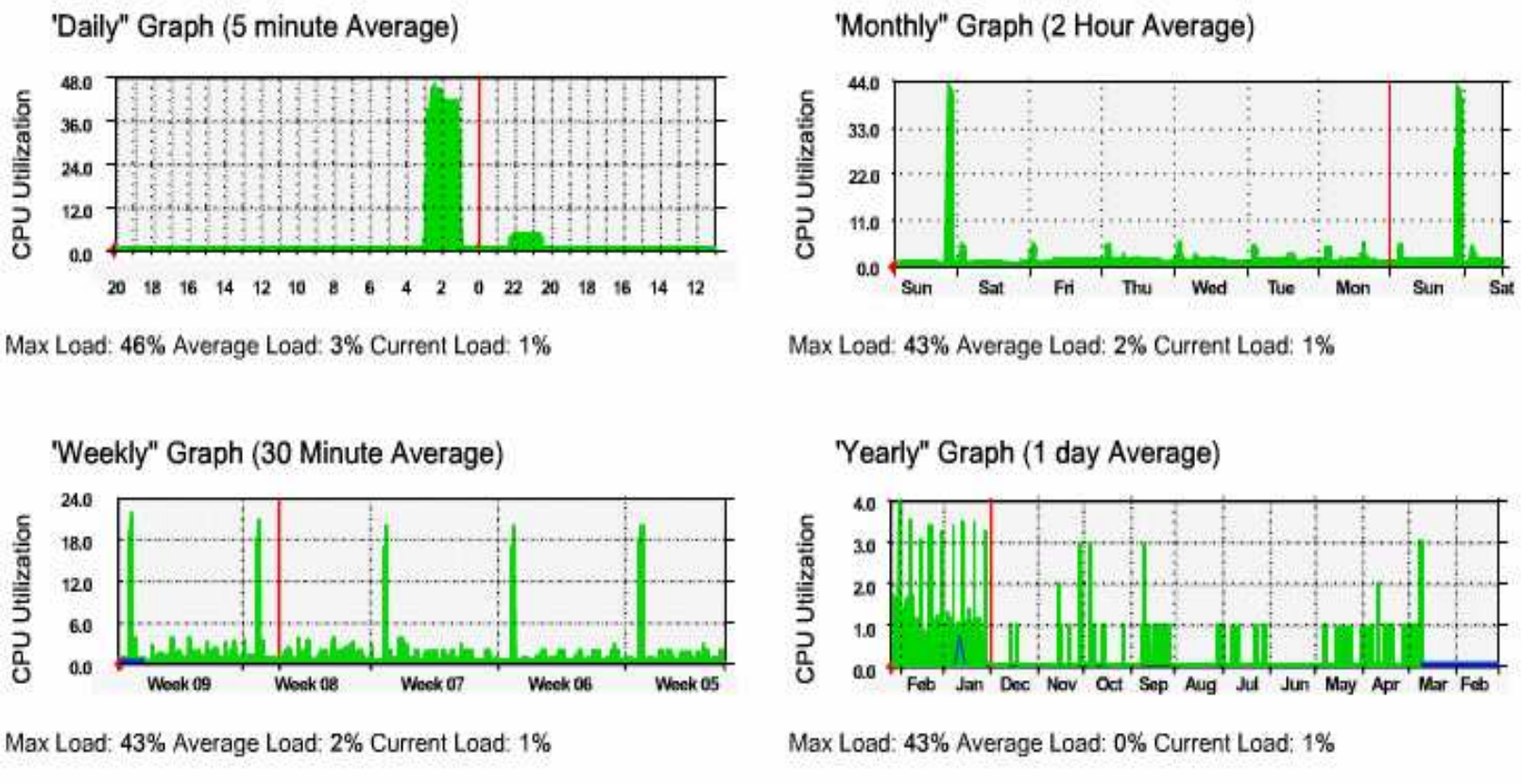


Hình trạng mạng với các thiết bị và các cổng cần thu thập thông tin

Các bước thiết lập đường cơ sở cho một hệ thống mạng (6)

- *Bước 3. Xác định thời hạn cần ghi nhận hiệu suất mạng*
  - *Để thu thập thông tin một cách chính xác và khách quan, cần phải xác định được khoảng thời gian cần thiết để lập mốc trong thông tin về đường cơ sở mạng.*
  - *Giai đoạn này cần được thực hiện lập lại ít nhất là bảy ngày để nắm bắt bất kỳ diễn biến thay đổi của hiệu suất mạng hàng ngày hay hàng tuần.*
  - *Các diễn biến thay đổi trong khoảng thời gian: hàng giờ, hàng ngày, hàng tuần, hàng tháng, hàng quý sẽ có giá trị tham khảo nhất định.*

Các bước thiết lập đường cơ sở cho một hệ thống mạng (7)



Mẫu các đường cơ sở mạng được ghi nhận theo các mốc thời gian

Các bước thiết lập đường cơ sở cho một hệ thống mạng (8)

- *Bước 3. Xác định thời hạn cần ghi nhận hiệu suất mạng (tt)*
  - *Việc ghi nhận hiệu xuất hàng tuần là quá ngắn để thấy được chính xác tính chất định kỳ của các sự việc xảy ra mỗi cuối tuần. Vào các ngày nghỉ cuối tuần hay các buổi không có người làm việc nhưng có thể có các hoạt động sử dụng nhiều băng thông của hệ thống mạng như: hoạt động lưu dự phòng cơ sở dữ liệu lớn, cập nhật các chương trình chống virus,…*
  - *Thông thường thì đánh giá đúng hiệu suất liên quan đến các hoạt động này nên được xem xét trên các mẫu biểu thị theo xu hướng hàng tháng.*
  - *Xu hướng hàng năm thì có thời hạn quá dài*
  - *Tổng quát, đường cơ sở mạng được xác lập dựa trên các thông số của hệ thống thu thập được từ hai đến bốn tuần là vừa đủ.*

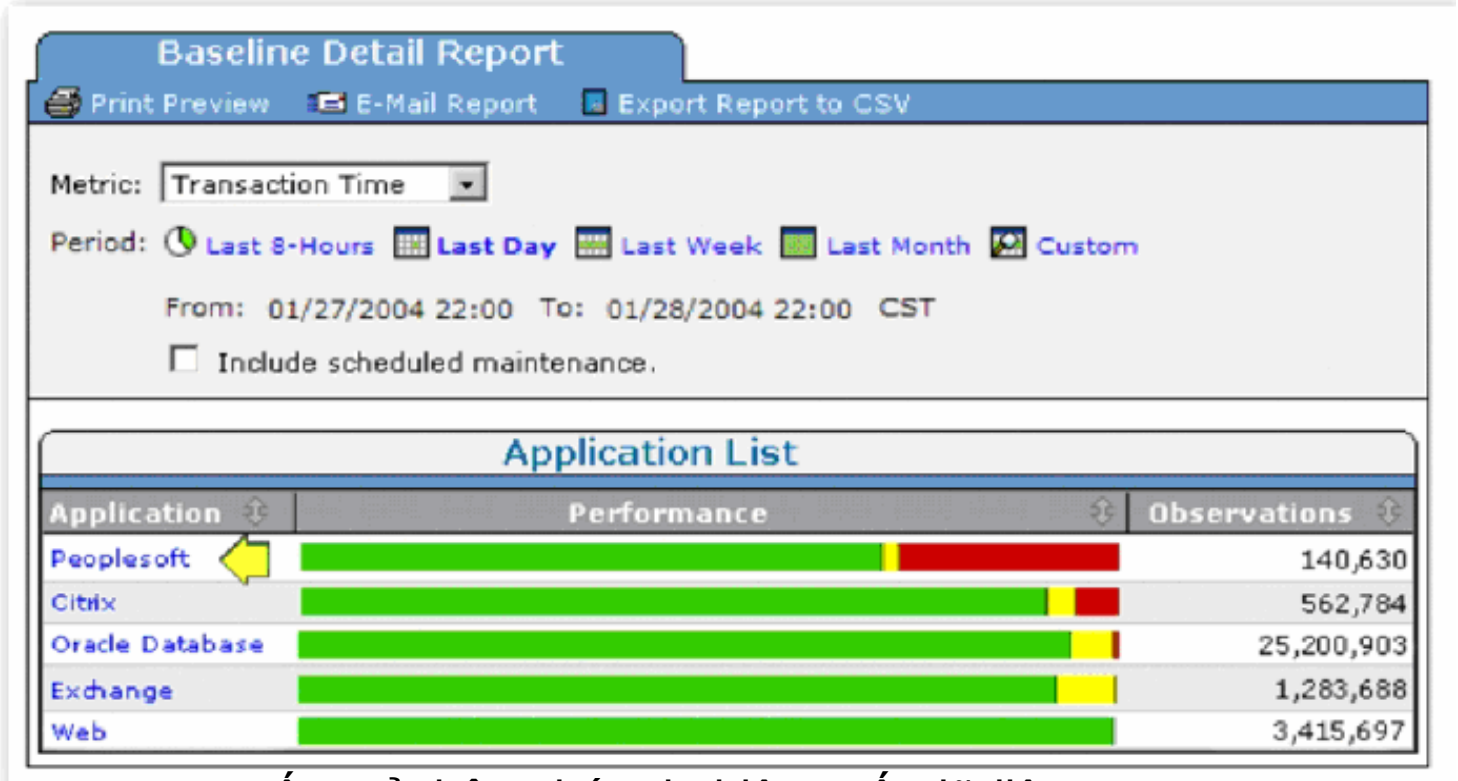
Các bước thiết lập đường cơ sở cho một hệ thống mạng (9)

- *Bước 3. Xác định thời hạn cần ghi nhận hiệu suất mạng (tt). Các lưu ý:*
  - *Thực hiện việc tính toán đường cơ sở mạng ở những thời điểm khi thông tin lưu thông trên mạng hoạt động ở trạng thái bình thường.*
  - *Việc phân tích hiệu suất chuẩn của mạng nên được tiến hành một cách thường xuyên.*

Các bước thiết lập đường cơ sở cho một hệ thống mạng (10)

- **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.

Các bước thiết lập đường cơ sở cho một hệ thống mạng (11)

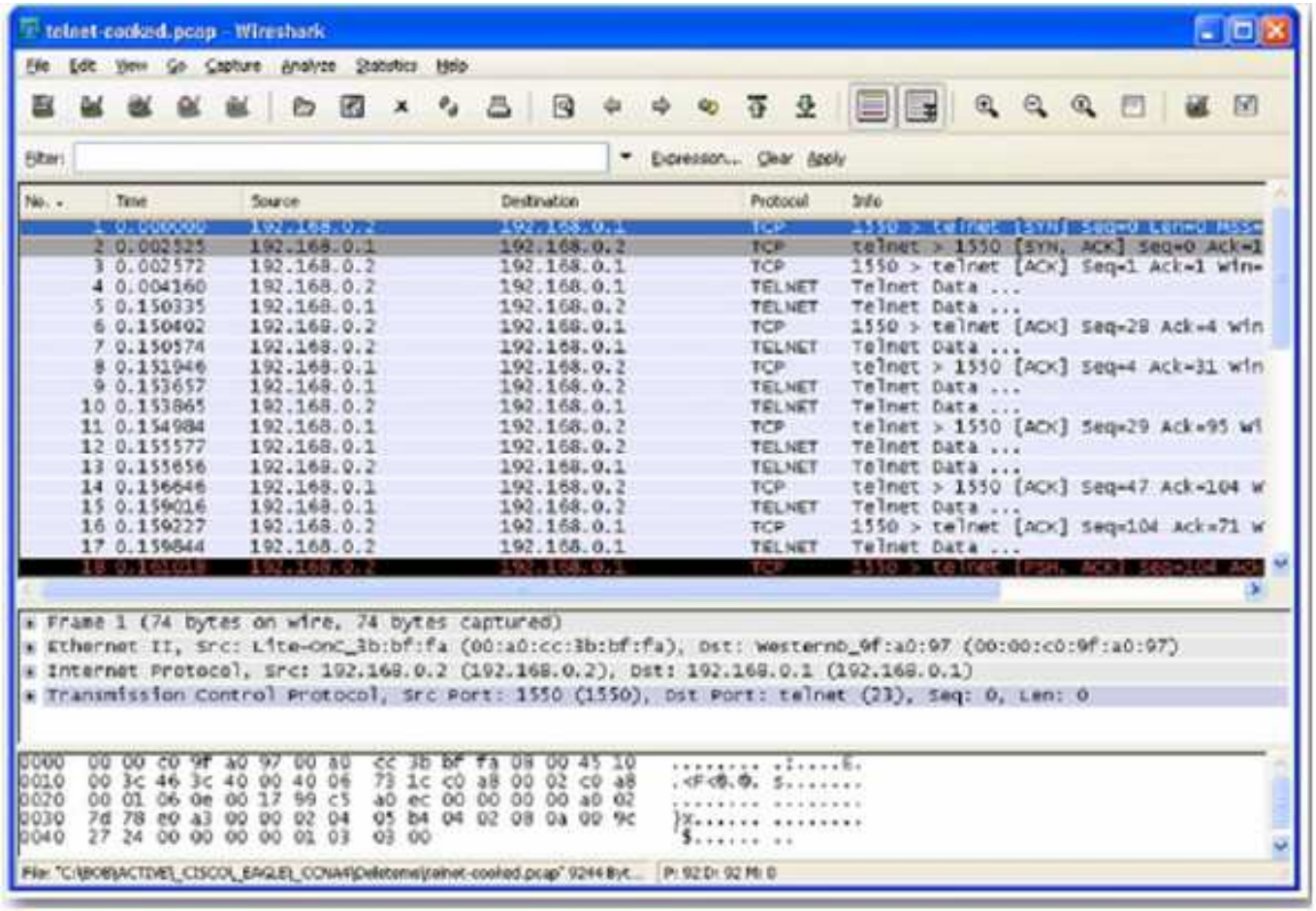


Kết quả thông báo đo hiệu suất dữ liệu mạng
(phần mềm Fluke Network SuperAgent)

Các bước thiết lập đường cơ sở cho một hệ thống mạng (12)

- **Các công cụ hỗ trợ xây dựng đường cơ sở mạng**
  - Công cụ xây dựng đường cơ sở mạng: phần mềm *SolarWinds* hay *CyberGauge*
  - Công cụ phân tích giao thức mạng: *Wireshark*

Các bước thiết lập đường cơ sở cho một hệ thống mạng (1)



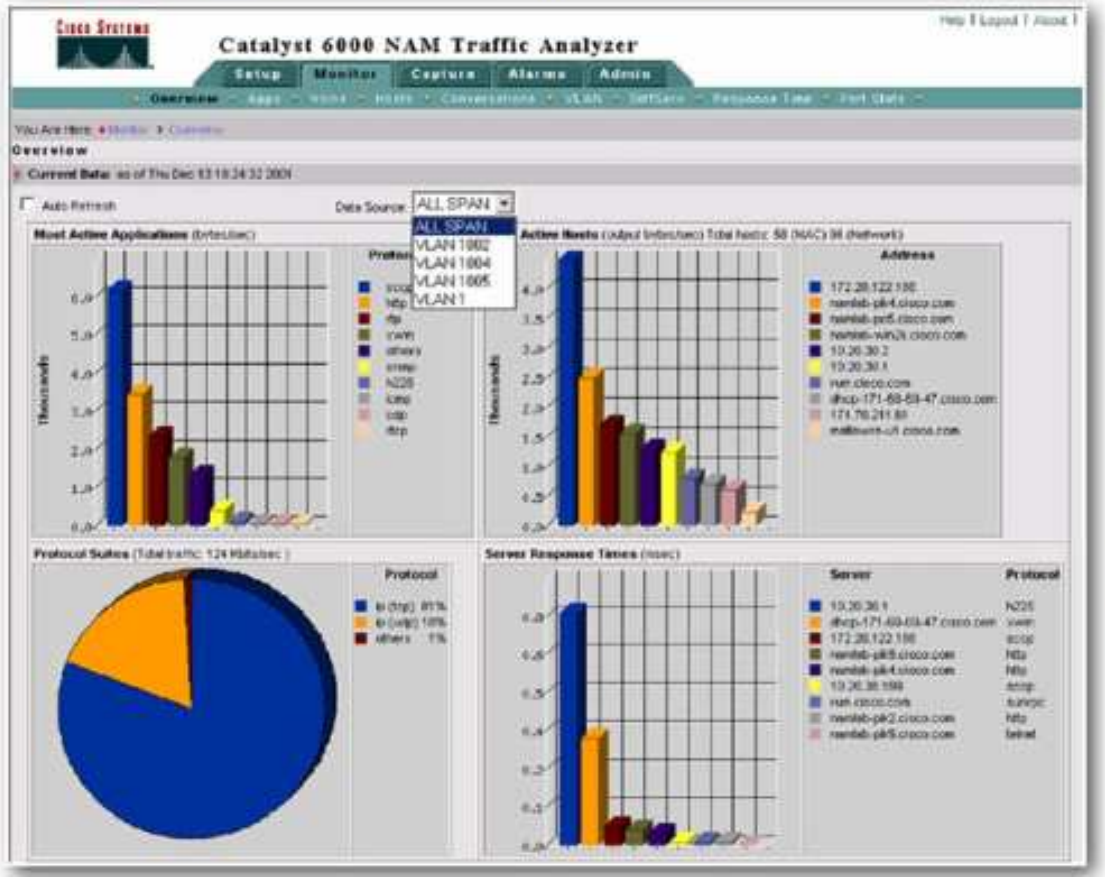
Minh họa phần mềm phân tích giao diện mạng *WireShark*

Phần cứng hỗ trợ khắc phục sự cố mạng (1)

- **Mô-đun phân tích mạng**
  - **Mô-đun phân tích mạng (Network Analysis Module - NAM):** là một thiết bị phần cứng được sử dụng để giám sát thông tin lưu thông qua đó.
  - **Thông tin được thu thập qua các mô-đun phân tích mạng:**
    - Sẽ được tổng hợp, phân tích và hiển thị lên máy của người quản trị thông qua một giao diện đồ họa của phần mềm phân tích mạng chuyên dụng được kèm theo hay thông qua một trình duyệt web.
    - Thu thập và giải mã các gói, lần theo vết các lần đáp ứng cho các yêu cầu liên quan đến các ứng dụng được nghi ngờ có sự cố liên quan đến các máy chủ trên mạng.

Phần cứng hỗ trợ khắc phục sự cố mạng (2)

Thông tin hiển thị của bộ phân tích mạng trên Cisco Catalyst 6000



Mô-đun phân tích mạng cho bộ chuyển mạch Cisco Catalyst 6000

Phần cứng hỗ trợ khắc phục sự cố mạng (3)

- **Bộ đo đa năng kỹ thuật số**
  - Bộ đo đa năng kỹ thuật số (Digital MultiMeters-DMMs) là bộ công cụ kiểm tra mạng được sử dụng để đo lường trực tiếp các giá trị điện áp, dòng điện và trở kháng của đường truyền.
  - Trong xử lý sự cố mạng, hầu hết các bộ kiểm tra đa năng liên quan đến việc kiểm tra các mức của nguồn điện cung cấp và kiểm tra thiết bị mạng đang được cung cấp điện ổn định và chính xác

Phần cứng hỗ trợ khắc phục sự cố mạng (4)

Hình ảnh về bộ đo đa năng Fluke 179

Phần cứng hỗ trợ khắc phục sự cố mạng (5)

- **Bộ kiểm tra cáp mạng**
  - Cáp kiểm tra cáp mạng là một thiết bị được thiết kế đặc biệt để cầm tay, được dùng để thử nghiệm các loại cáp dữ liệu truyền thông.
  - Có thể sử dụng để phát hiện dây cáp mạng bị hỏng, cáp bị chạm chập, ngắt mạch và các cặp dây được kết nối không đúng.
  - Các bộ kiểm tra có thể có các chức năng từ đơn giản đến phức tạp với chi phí đầu tư từ thấp đến cao.

Phần cứng hỗ trợ khắc phục sự cố mạng (6)

Bộ kiểm tra
Fluke Networks LinkRunner Pro

Bộ kiểm tra
Fluke Networks CableIQ Qualification

Hình ảnh về bộ kiểm tra cáp mạng đa năng

Phần cứng hỗ trợ khắc phục sự cố mạng (7)

- **Bộ phân tích cáp mạng**
  - Bộ phân tích cáp là thiết bị cầm tay đa chức năng được sử dụng kiểm tra và xác nhận các loại cáp đồng hay cáp quang cho các dịch vụ khác nhau, theo các tiêu chuẩn khác nhau.
  - Có thể kiểm tra, chẩn đoán được các lỗi trên đường truyền cũng như khoảng cách xuất hiện lỗi so với một đầu mút đang gắn thiết bị kiểm tra, ví dụ như các lỗi gây ra bởi nhiễu, xác định những hành động sửa lỗi cần thiết, hiển thị đồ họa thông tin về các loại nhiễu có trong đường truyền và hành vi của trở kháng trên đường truyền.
  - Dữ liệu thu thập được từ thiết bị cầm tay này có thể được cập nhật vào phần mềm trên máy tính để thông báo các thông tin về các cáp mạng mà thiết bị đo được.

Phần cứng hỗ trợ khắc phục sự cố mạng (8)

Hình ảnh bộ phân tích cáp mạng Fluke DTX

Phần cứng hỗ trợ khắc phục sự cố mạng (9)

- **Bộ phân tích mạng cầm tay**
  - Là thiết bị được sử dụng để xử lý sự cố mạng trên các bộ chuyển mạch và VLAN trên các bộ chuyển mạch đó.
  - Bằng cách cắm vào bất cứ vị trí nào trên một bộ chuyển mạch, người quản trị có thể nhận biết được các các thông số của bộ chuyển mạch đó, hiệu suất sử dụng trung bình và mốc cao điểm sử dụng tài nguyên của thiết bị.
  - Được sử dụng để phát hiện các VLAN có trên bộ chuyển mạch, cấu hình của các VLAN, phân tích lưu lượng mạng và hiển thị thông tin chi tiết của các giao diện trên bộ chuyển mạch.
  - Có thể được kết nối với máy tính hay các bộ phân tích mạng để người quản trị mạng có thể phân tích và xử lý sự cố khi đã xảy ra.

Phần cứng hỗ trợ khắc phục sự cố mạng (10)

Hình ảnh bộ phân tích mạng cầm tay
Fluke Network
Optiview Series III

Phần cứng hỗ trợ khắc phục sự cố mạng (11)

- **Các trang thông tin hỗ trợ**
  - **Công cụ phần mềm**
    - Hệ thống quản trị mạng và các tài liệu liên quan
      - http://www.ipswitch.com/products/whatsup/index.asp?t=demo
      - http://www.solarwinds.com/products/network_tools.aspx
      - http://h20229.www2.hp.com/products/cvnnm/ds/cvnnm_ds.pdf
    - Công cụ xây dựng đường cơ sở mạng cho hệ thống mạng
      - http://www.networkuptime.com/tools/enterprise/
      - http://www.neon.com/Tutorials/index.html?drawyournetworkmap.htm
    - Kiến thức cơ bản về mạng và thiết bị mạng máy tính
      - http://www.cisco.com
    - Các bộ phân tích mạng và giao thức mạng
      - http://www.flukenetworks.com/fnet/en-us/products/OptiView+Protocol+Expert/

Phần cứng hỗ trợ khắc phục sự cố mạng (12)

- **Các trang thông tin hỗ trợ**
  - **Phần cứng hỗ trợ giải quyết sự cố mạng**
    - Cisco Network Analyzer Module (NAM):
      - http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_software/3.5/user/guide/user.html
    - Thông tin về các bộ kiểm tra cáp mạng
      - http://www.flukenetworks.com/fnet/en-us/products/CableIQ+Qualification+Tester/Demo.htm
    - Thông tin về bộ phân tích cáp mạng
      - http://www.flukenetworks.com/fnet/en-us/products/DTX+CableAnalyzer+Series/Demo.htm
    - Bộ phân tích mạng
      - http://www.flukenetworks.com/fnet/en-us/products/OptiView+Series+III+Integrated+Network+Analyzer/Demos.htm