TỔNG QUAN QUẢN TRỊ MẠNG

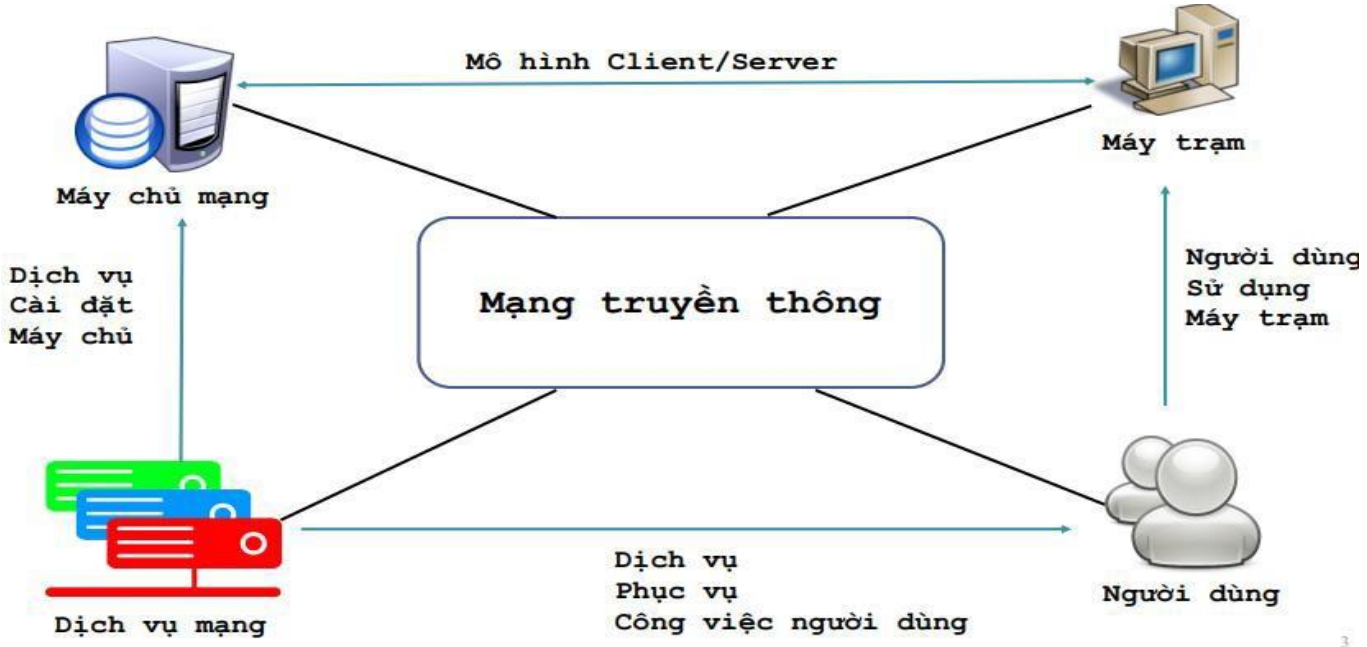
Nội dung

- Hệ thống máy tính là gì?
- Thành phần hệ thống mạng
- Nhiệm vụ quản trị hệ thống mạng
- Một số chức danh công việc quản trị hệ thống
- Kỹ năng cần có của quản trị hệ thống mạng
- Các công cụ quản trị mạng

Hệ thống máy tính là gì?

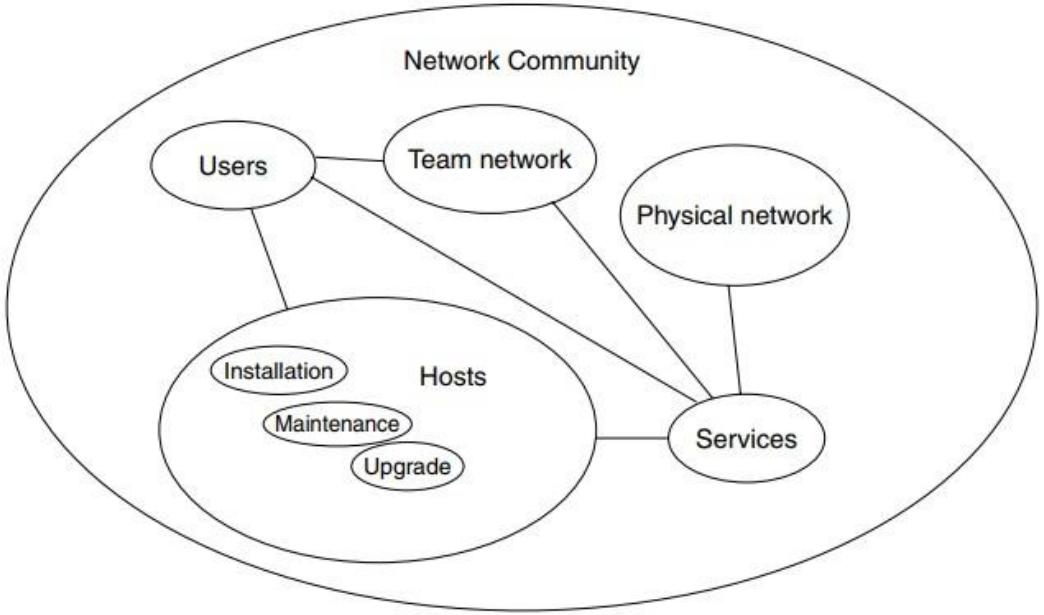
What is ‘the System’?

Definition 1 (human–computer system). *An organized collaboration between humans and computers to solve a problem or provide a service. Although computers are deterministic, humans are non-deterministic, so human–computer systems are non-deterministic.*



Thành phần hệ thống mạng

- Cơ sở hạ tầng mạng (Network infrastructure)
  - Người dùng hệ thống
  - Máy tính: cố định hoặc thiết bị di động
  - Phần cứng mạng:
    - Router
    - Switch
    - Cables



Tầm quan trọng của quản trị mạng

- Mạng là một cấu trúc phức tạp đòi hỏi rất nhiều quản trị, cần phải có kế hoạch cận thận đảm bảo:
  - Cấu hình của các thiết bị mạng khi sửa đổi phải không gây ảnh hưởng xấu đến phần còn lại của mạng.
  - Các lỗi xảy ra trong hệ thống mạng phải được phát hiện, chẩn đoán và sửa chữa
  - Các dịch vụ phải luôn sẵn dùng và đảm bảo chất lượng dịch vụ cho người dùng cuối
  - Tiết kiệm chi phí: thiết kế, vận hành, bảo trì
  - Tăng doanh thu (Revenue)

Nhiệm vụ quản trị viên hệ thống

- Quản trị mạng (Network administrator) là người "biết mọi thứ" từ việc thiết kế LAN-WAN đến việc cấu hình, điều chỉnh chức năng hoạt động của một hệ thống mạng, vận hành, giải quyết sự cố, bảo mật và nhiều công việc liên quan khác.

Nhiệm vụ quản trị viên hệ thống

Một quản trị viên hệ thống (system administrator hoặc sysadmin) là người chịu trách nhiệm

- Bảo trì, cấu hình, và duy trì hoạt động tin cậy của hệ thống máy tính, máy chủ và thiết bị mạng.
- Xây dựng giải pháp đảm bảo hệ thống máy tính luôn hoạt động trơn tru.
- Đáp ứng nhu cầu của người dùng về thời gian hoạt động, chất lượng dịch vụ và tính bảo mật của hệ thống.
- Đảm bảo chi phí xây dựng giải pháp không được vượt quá ngân sách cho phép.

Nhiệm vụ quản trị viên hệ thống

- Trong một hệ thống nhỏ
  - Cài đặt và cấu hình phần cứng, hệ điều hành và phần mềm
  - Cập nhật các bản vá hệ điều hành và các ứng dụng
  - Bảo đảm an ninh máy tính (cài đặt phần mềm chống virus)
  - Kiểm tra thay thế, sửa chữa thiết bị
  - Sao lưu và phục hồi dữ liệu
  - Trả lời thắc mắc về kỹ thuật
  - Hỗ trợ người dùng.
  - .v.v.

Nhiệm vụ quản trị viên hệ thống

- **Trong hệ thống lớn**
  - Quản lý người dùng
  - Giám sát hoạt động của hệ thống
  - Phát hiện các sự cố và lập báo cáo về các sự cố này.
  - Phân tích nhật ký (logs) và xác định được nguyên nhân sự cố
  - Giải quyết và khắc phục các sự cố phát sinh
  - Tối ưu hóa hệ thống, cải thiện hiệu suất hoạt động
  - Lập kế hoạch bảo trì, nâng cấp hệ thống
  - Biên soạn các tài liệu phục vụ cho việc quản lý hệ thống.
  - Định kỳ thực hiện việc sao lưu và phục hồi
  - Thực hiện việc kiểm toán hệ thống.
  - .v.v.v

Một số chức danh công việc

- Trong một số tổ chức lớn, công việc của quản trị hệ thống có thể được chia nhỏ thành một số chức danh công việc riêng như:
  - Quản trị viên mạng máy tính (network administrator): bảo trì và khắc phục các sự cố về cơ sở hạ tầng mạng (ví dụ: router, switch)
  - Quản trị viên cơ sở dữ liệu (database administrator): vận hành và chăm sóc hệ thống máy chủ cơ sở dữ liệu
  - Quản trị máy chủ (server administrator): vận hành và chăm sóc máy chủ (các dịch vụ mạng như web, mail, dns .v.v.)

Một số chức danh công việc

- Quản trị hệ thống an ninh (Security Systems Administrator): duy trì hoạt động của hệ thống an ninh, xây dựng các giải pháp an ninh hệ thống, giám sát hệ thống, sao lưu dữ liệu; thiết lập, xóa và duy trì các tài khoản người dùng cá nhân.
- Nhà lập kế hoạch (Network planner): thiết kế hệ thống mạng, lựa chọn thiết bị mạng.
- Nhân viên hỗ trợ kỹ thuật (technical support): người xử lý các sự cố không thể được khắc phục từ xa.
- Nhân viên trực hỗ trợ (IT HelpDesk): hỗ trợ khách hàng
- v.v…

Kỹ năng cần có của quản trị hệ thống

- Kiến thức về hệ điều hành và các ứng dụng đang sử dụng
- Kiến thức về an toàn và bảo mật thông tin
- Kỹ năng giải quyết sự cố là kỹ năng quan trọng nhất
- Khả năng chịu đựng áp lực và bình tĩnh
- Kỹ năng giao tiếp tốt và làm việc theo nhóm
- Khả năng trình bày và viết tài liệu
- Khả năng tự học
- Kiến thức đạt được tương đương các chứng chỉ: Microsoft, Cisco (CCNA, CCNP), LPI (Linux Professional Institute)

CÔNG VIỆC CHÍNH CỦA QUẢN TRỊ MẠNG

Công việc chính của quản trị mạng

- Quản trị người dùng.
- Quản trị phần cứng.
- Quản trị phần mềm
- Dự phòng
- Giải quyết sự cố
- Quan sát hệ thống.
- Ghi dấu bảo mật.
- Hướng dẫn, giúp đỡ người dùng.
- Truyền thông, và giao tiếp

Quản trị người dùng

- Tạo mới người dùng
- Cập nhật thông tin người dùng
- Xóa người dùng
- Quản lý không gian tên – (Usernames and UIDs)
- Quản lý không gian lưu trữ dữ liệu cá nhân

Quản trị phần cứng – thiết bị

- Lắp đặt, vận hành, bảo trì thiết bị
  - Cấu hình, kết nối dây, cài driver phần cứng .v.v
- Quản lý vòng đời thiết bị: đánh giá lựa chọn công nghệ
  - Xây dựng kế hoạch bảo trì
  - Xây dựng kế hoạch mua sắp thiết bị hằng năm
  - Xây dựng kế hoạch mua sắp thiết bị nâng cấp hệ thống.
    - Số lượng máy chủ, số lượng người dùng, số lượng dịch vụ
    - Băng thông truyền tải, không gian lưu trữ

Quản trị phần cứng – thiết bị

- Quản lý phòng máy chủ
  - Nguồn điện chính, nguồn điện dự phòng
  - Tủ kỹ thuật
  - Môi trường: hệ thống làm mát, hệ thống báo cháy, hệ thống chống sét, .v.v.

Quản trị phần mềm

- Cài đặt – cấu hình phần mềm
- Quản lý tiến trình cài đặt phần mềm
- Cập nhập, vá lỗi phần mềm
- Đánh giá phần mềm
- Lịch biểu bảo trì phần mềm
- Lịch biểu nhắc nhở người dùng
- Quản lý phần mềm: version, nâng cấp, thay thế .v.v.

Dự phòng

- Xây dựng chiến lược và quy tắc dự phòng
  - Xác định đối tượng: tập tin, CSDL, Server .v.v.
  - Lập lịch biểu: thời điểm, tần suất?
  - Sức chứa
  - Định vị lưu trữ: online hay offline
- Cài đặt phần mềm, công cụ thực hiện dự phòng
- Quản lý tiến trình lưu dự phòng
  - Quan sát quá trình dự phòng
    - Ghi nhận quá trình thực hiện
    - Kiểm tra không gian lưu trữ
- Phục hồi khi có yêu cầu

Giải quyết sự cố

- Xác định sự cố
  - Thông qua cảnh báo người dùng
  - Thông qua ghi nhận của phần mềm, phần mềm quan sát
- Truy vết và xác định vấn đề
- Xác định nguyên nhân sự cố - giải quyết sự cố
  - Cung cấp giải pháp dự phòng trước khi giải quyết
  - Khắc phục sự cố

Quan sát hệ thống

- Thiết lập hệ thống giám sát và cảnh báo tự động
  - Problems (disk full, error logs, security)
  - Performance (CPU, mem, disk, network)
  - Giám sát lưu lượng, băng thông qua thiết bị switch, router
  - Giám sát trạng thái thiết bị và dịch vụ mạng
- Lưu trữ thông tin log và dữ liệu dự phòng
- Cung cấp dữ liệu cho kế hoạch nâng cấp hệ thống

Hỗ trợ người dùng

- Xây dựng danh sách công việc hỗ trợ IT
- Hướng dẫn người dùng cung cấp thông tin sự cố.
- Thông báo kết quả khắc phục sự cố
- Đào tạo nhân viên hỗ trợ
- Giám sát và đánh giá hiệu quả hoạt động hỗ trợ
- Sử dụng công cụ vào hoạt động hỗ trợ

Tạo lập tài liệu

- **Tạo lập tài liệu hướng dẫn**
  - Tài liệu về quy tắc sử dụng hệ thống
  - Tài liệu sử dụng phần mềm
  - Tài liệu sử dụng phần cứng
  - Đào tạo người dùng nâng cao nhận thức an toàn thông tin

CÁC CÔNG CỤ QUẢN TRỊ MẠNG

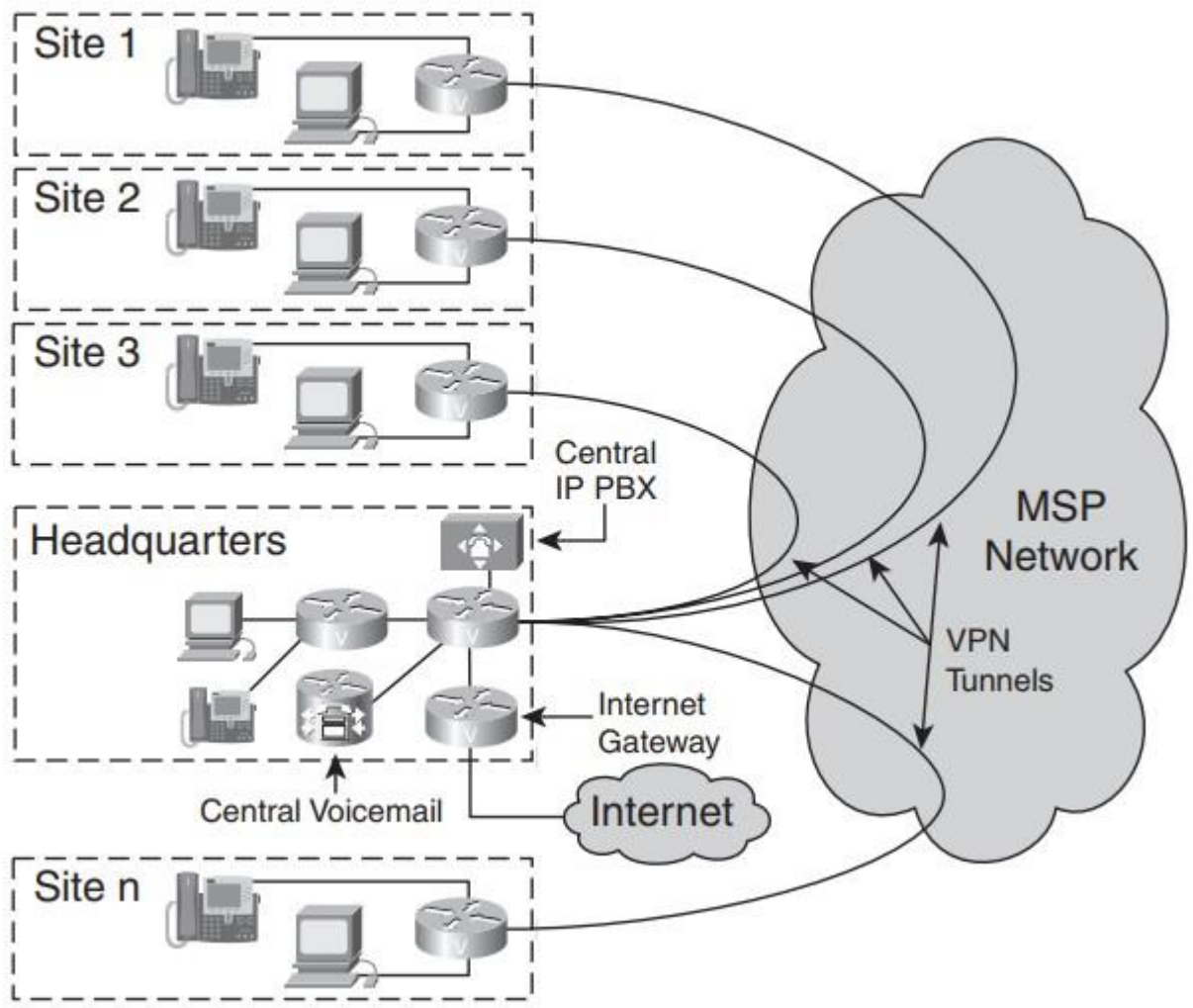
Công cụ quản trị mạng

- Device managers
- Network analyzers
- Collectors (probes)
- Intrusion Detection System (IDS)
- Performance analysis systems
- Alarm management systems
- Trouble ticket systems

Công cụ quản trị mạng

- Work order systems
- Workflow management systems
- Service provisioning systems
- Service-order management systems
- Element managers
- Management platform
- Billing systems

Hệ thống giám sát

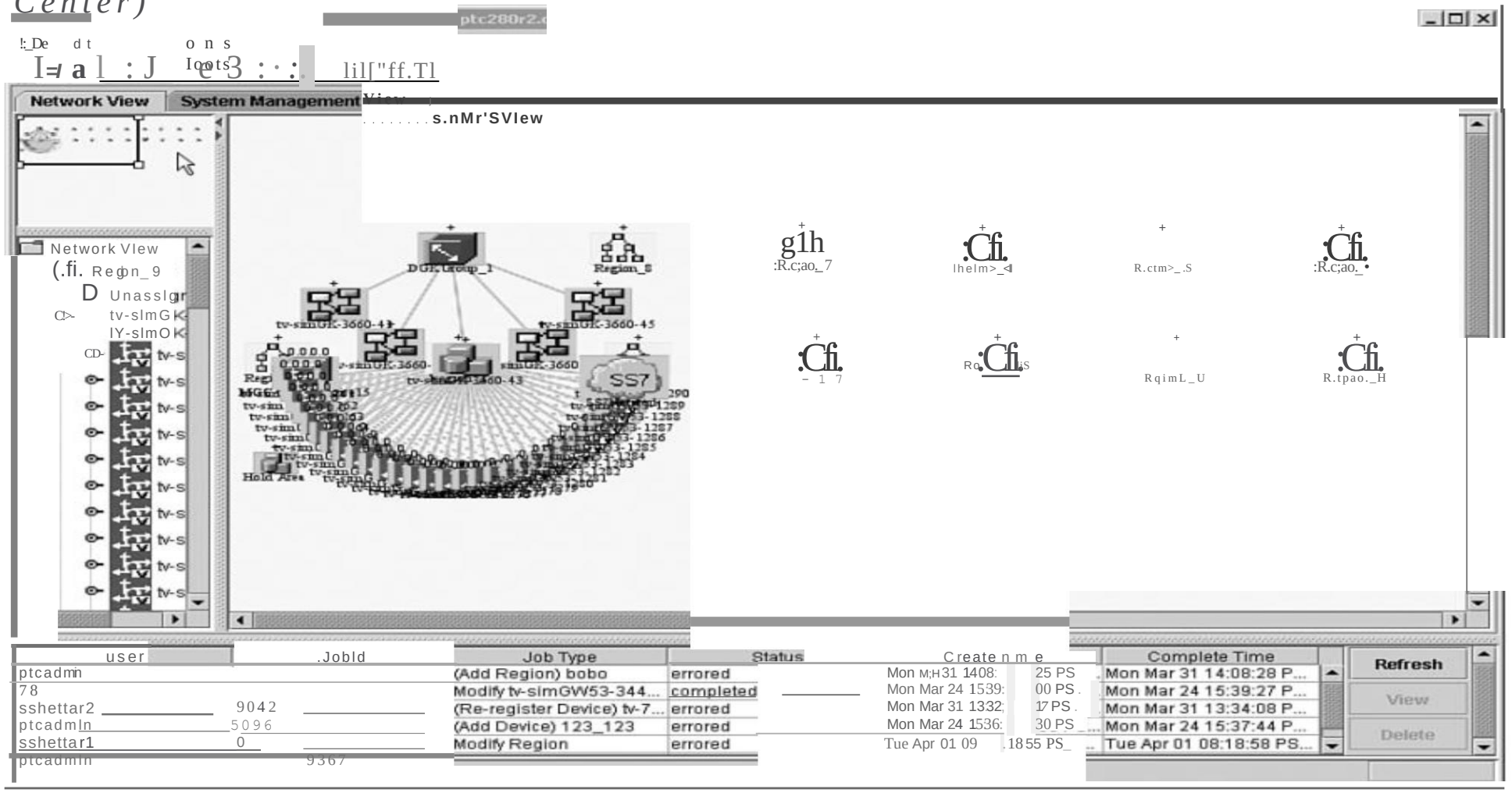


- Mỗi router được biểu diễn dưới dạng một biểu tượng trên màn hình màu xanh, vàng, cam hoặc đỏ, tùy thuộc vào trạng thái báo động của nó.
- Mã màu này cho phép nhìn thấy mọi thứ đang hoạt động và chạy

Giám sát sơ đồ và trạng thái hệ thống mạng

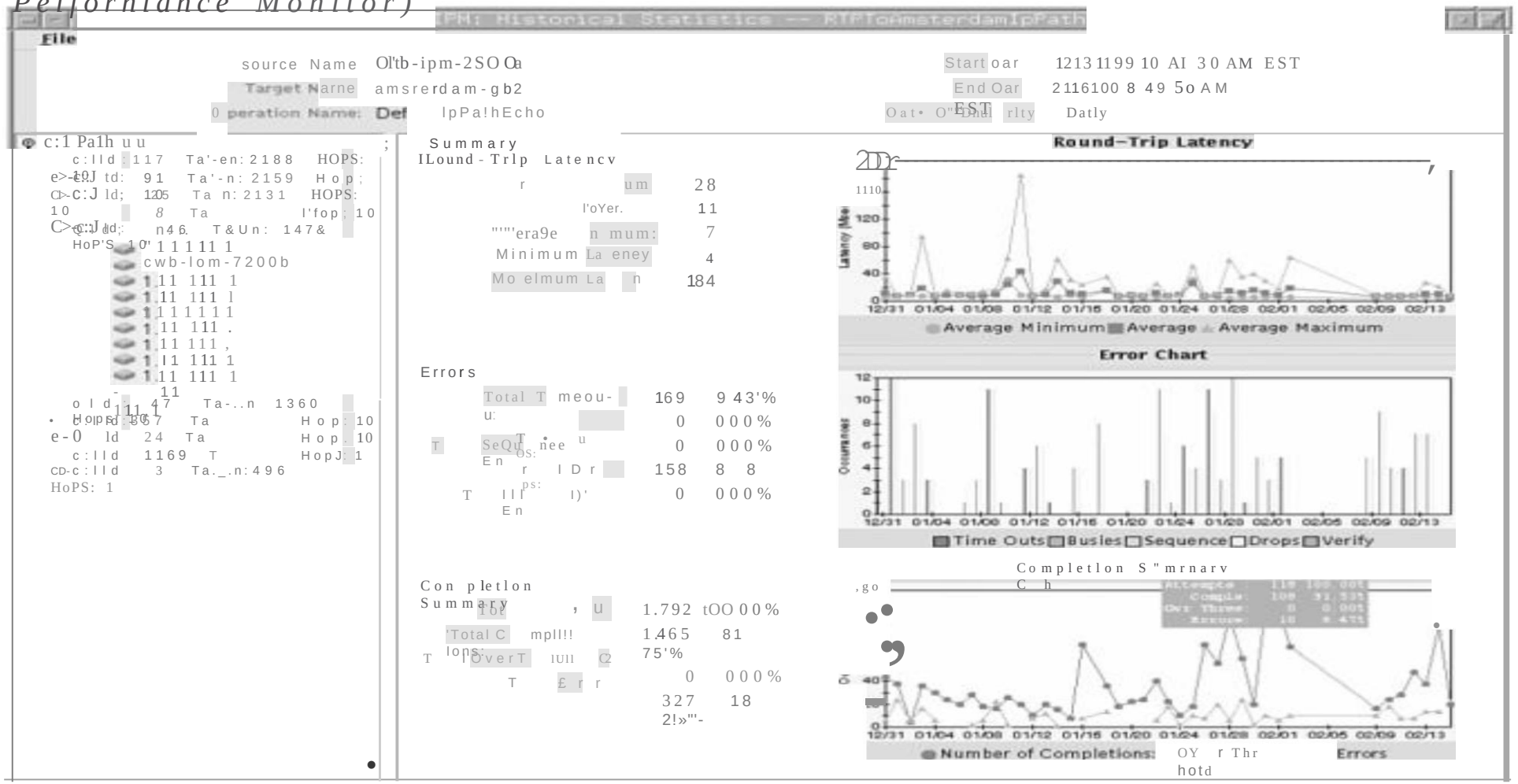
Sử dụng phần mềm giám sát

A Typical Management Application Screen (Cisco Packet Telephony Center)



Giám sát hệ thống

SaFnple Screen of a ManLlgeJnent Application 1-vith Peiforrnance (Cisco IP Graph Work Peifornlance Monitor)

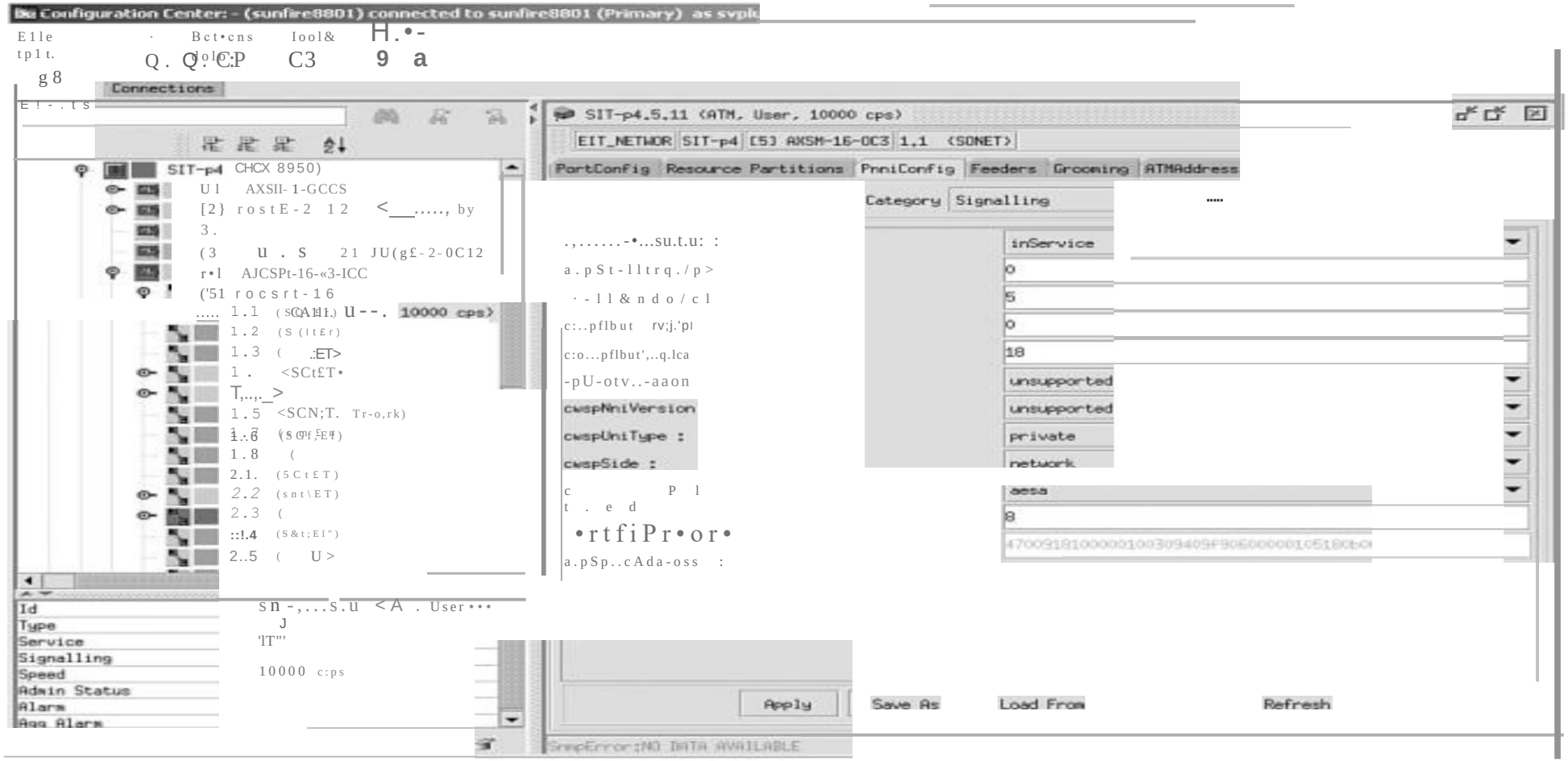


Cấu hình thiết bị từ xa qua giao diện

Santple Screen of a Manage nent Application WAN Manager 15..1)

That Allo-...vs the Configuration of Port

(Cisco



Device Managers - Network Analyzers - Collectors và Probes

- Quản trị các thiết bị mạng: cấu hình thiết bị, backup/restore cấu hình thiết bị
  - Telnet
  - SSH
  - Console
- Phân tích mạng: bao gồm packet sniffers, packet analyzers, và traffic analyzers
- Thu gom thông tin và thăm dò (Collectors và Probes): thu thập dữ liệu từ mạng. Ví dụ: thông tin lưu lượng đi qua router, hệ thống thu thập syslog messages

Intrusion Detection Systems (IDS)

- Hệ thống phát hiện xâm nhập
  - Giúp nhanh chóng phát hiện những truy cập nghi ngờ, có thể là dấu hiệu của một cuộc tấn công đang diễn ra.
- IDS sử dụng rất nhiều kỹ thuật:
  - Phân tích lưu lượng truy cập trên mạng
  - Lắng nghe cảnh động
  - Kiểm tra hoạt động nhật ký
  - Quan sát mẫu tải (observing load patterns)
- Việc nhanh chóng nhận ra các mối đe dọa sẽ giảm nhẹ tác động của chúng. Ví dụ: bằng cách tắt các cổng mạng thông qua các cuộc tấn công xảy ra.

Performance Analysis Systems

- Hệ thống phân tích hiệu năng
  - Cho phép người dùng phân tích lưu lượng và hiệu suất
  - Xác định xu hướng mô hình lưu lượng truy cập
  - Dự đoán khả năng bổ sung năng lực mạng cần thiết
  - Điều chỉnh hiệu suất mạng để tránh tắc nghẽn

Trouble Ticket Systems

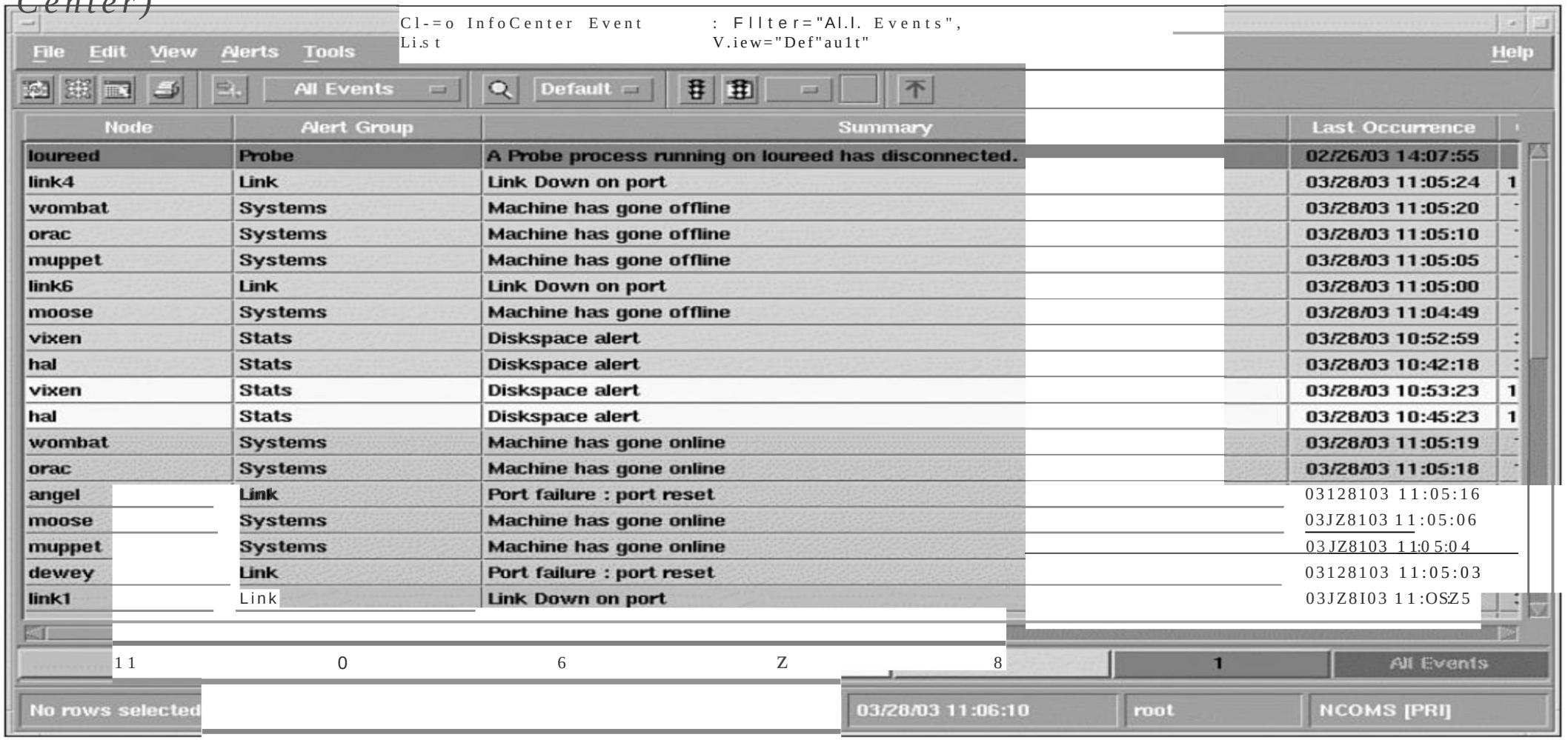
- Hệ thống định danh sự cố:
  - Được sử dụng để theo dõi các sự cố trong mạng
  - Thu thập thông tin về vấn đề phát sinh, giúp xác định nguyên nhân và cách giải quyết vấn đề.
  - Sự cố được phát hiện bởi: người dùng kinh nghiệm hoặc ứng dụng giám sát
  - Hệ thống có hỗ trợ cách giải quyết vấn đề
    - Gửi cảnh báo
    - Hệ thống chuyển vấn đề đến người có tránh nhiệm trả lời
    - Nâng cao mức cảnh báo khi thời gian xử lý quá lâu
    - Theo dõi quá trình xử lý vấn đề (khi áp dụng qui trình xử lý)

Alarm Management Systems

- Hệ thống quản lý cảnh báo:
  - Thu thập và giám sát các cảnh báo từ mạng
  - Giúp người dùng nhanh chóng sàng lọc và hiểu được vấn đề từ khối các sự kiện và tin cảnh báo
  - Cung cấp khả năng chẩn đoán giúp xác định nguyên nhấn gốc của vấn đề cảnh báo
  - Tổng hợp và giải thích các sự kiện phát hiện
  - Đóng vai trờ tiền xử lý cho các ứng dụng khác

Alarm Management Systems

Sample Screen of an Alarm Management Application (Cisco Info Center)



Work Order Systems

- Hệ thống lập kế hoạch: được sử dụng phân công và theo dõi công việc bảo trì hệ thống mạng.
  - Lập kế hoạch và lên lịch công việc cho công tác bảo trì
    - Xác định độ ưu tiên công việc
    - Trình tự thực hiện các công việc
    - Đảm bảo các công việc được thực hiện đúng lúc đúng thời điểm
    - Đảm bảo độ tin cậy và khả năng sẵn sàng của thiết bị.

Workflow Management Systems

- Hệ thống quản lý qui trình làm việc: xây dựng quy trình, chuẩn hóa các giai đoạn vận hành hệ thống
- Những quy trình thường áp dụng:
  - Qui trình lập kế hoạch bảo trì hệ thống (work order systems)
  - Qui trình truy vết sự cố (Trouble Ticket Systems)
  - Quy trình xử lý sự cố (Incident Management)
  - Quy trình xử lý vấn đề (Problem Management)
- Tài liệu nguyên cứu xây dựng qui trình

Inventory Systems

- ❖ Hệ thống thống kế thiết bị tồn: thống các thiết bị, card
  - mở rộng, phần mềm-phiên bản.
  - ❑ Khai thác và sử dụng thiết bị hiệu quả
  - ❑ Gắn kết thiết bị với kế hoạch bảo trì hệ thống (work order
    - systems)

Những thách thức của quản trị hệ thống

- Quản trị hệ thống không chỉ là cài đặt hệ điều hành, mà còn đảm nhận các công việc như lập kế hoạch, thiết kế hệ thống mạng hiệu quả cho người dùng:
- Các thách thức thường gặp:
  - Thiết kế một hệ thống mạng hợp lý và hiệu quả.
  - Triển khai một lượng lớn máy tính: sau cho có thể dễ dàng nâng cấp và quản lý sau đó.
  - Quyết định những dịch vụ nào là cần thiết
  - Lập kế hoạch và thực hiện các giải pháp bảo mật
  - Cung cấp một môi trường thoải mái cho người sử dụng
  - Phát triển cách sửa lỗi và các vấn đề phát sinh.

Tài liệu tham khảo

1. Principles of Network and System Administration, Mark Burgess, Oslo University College, Norway, Second Edition
2. Network Management Fundamentals, Alexander Clemm Ph.D., Copyright© 2007 Cisco Systems, Inc.
3. Priscilla Oppenheimer, Top-Down Network Design Second Edition, Cisco Press, 2011
4. Maintenance Planning and Scheduling Handbook.
5. https://www.sokanu.com/careers/computer-systems-administrator/