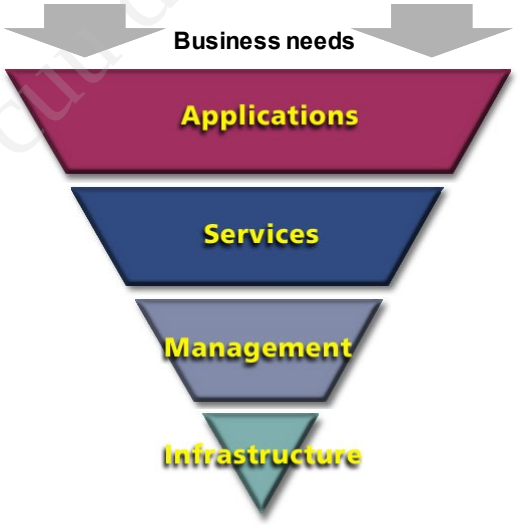
Chương 5: Trung Tâm quản lý mạng

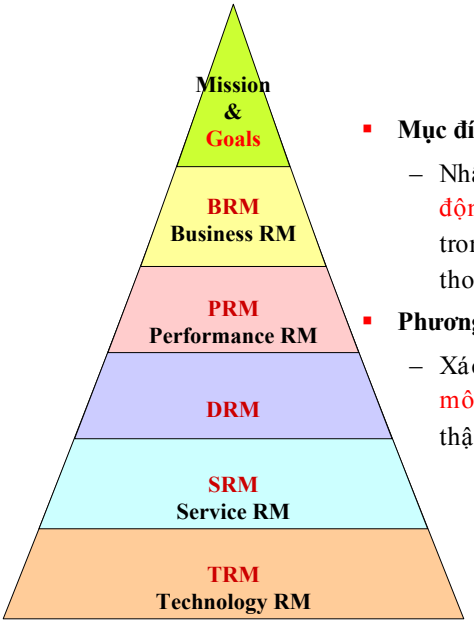
1. Trung tâm khai thác& quản lý mạng
2. Cấu trúc của hệ thống quản lý mạng
3. Giao diện quản trị người -máy
4. Hỗ trợ nhân viên khai thác
5. An toàn trong khai thác và quản lý mạng

Mục tiêu hoạt động của trung tâm NMS/NOC



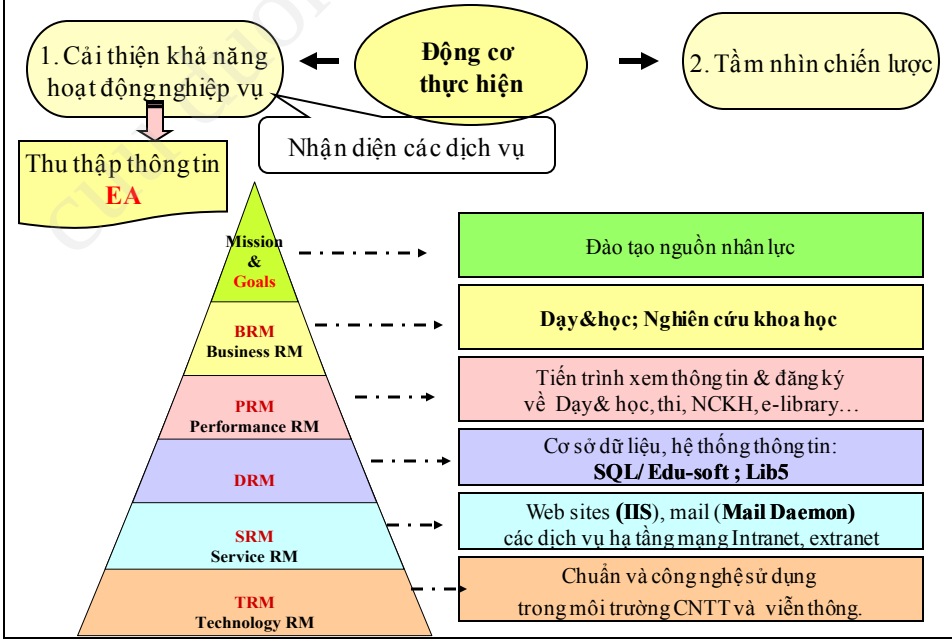
1. Cung cấp hạ tầng CNTT chất lượng để đáp ứng hoạt động hiệu quả cho các ứng dụng doanh nghiệp phục vụ các hoạt động nghiệp vụ của một tổ chức.

Mô hình kiến trúc doanh nghiệp- EA



- **Mục đích:**
  - Nhận diện được thực trạng quản lý và hoạt động của các thành phần nghiệp vụ cốt lõi trong môi trường ứng dụng công nghệ thong tin.
- **Phương pháp:**
  - Xác định kiến trúc doanh nghiệp với các mô hình tham chiếu liên quan cho phép thu thập thông tin chính xác và hiệu quả.

Cải thiện khả năng hoạt động nghiệp vụ



Mục tiêu hoạt động của trung tâm NMS/NOC

1. Cung cấp hạ tầng CNTT chất lượng để đáp ứng hoạt động hiệu quả cho các ứng dụng doanh nghiệp phục vụ các hoạt động nghiệp vụ của một tổ chức.
2. Đội ngũ quản trị mạng được giải phóng khỏi khối lượng công việc nặng nề bởi sự hỗ trợ hữu hiệu từ công cụ quản trị mạng và các giải pháp đảm bảo khả năng sẵn sàng của dịch vụ và thiết bị.
3. Hệ thống quản trị mạng được khai thác một cách đơn giản với nhiều chức năng phong phú cho mội trường mạng hội tụ.
4. Các sự cố cần được nhận diện, cô lập và xử lý nhanh chóng với thời gian sửa chửa (MTTR) qui ước.

Công tác quản lý mạng

- Triển khai và kết hợp tất cả nguồn lực, tài nguyên về con người, công cụ và qui trình hoạt động, để:
  1. Hoạch định
  2. Khai thác
  3. Quản trị:
     - Phân tích
     - Đánh giá
     - Cải thiện hoạt động và mở rộng mạng
- Đáp ứng các yêu cầu dịch vụ tại tất cả các thời điểm với chi phí và công sức hợp lý.

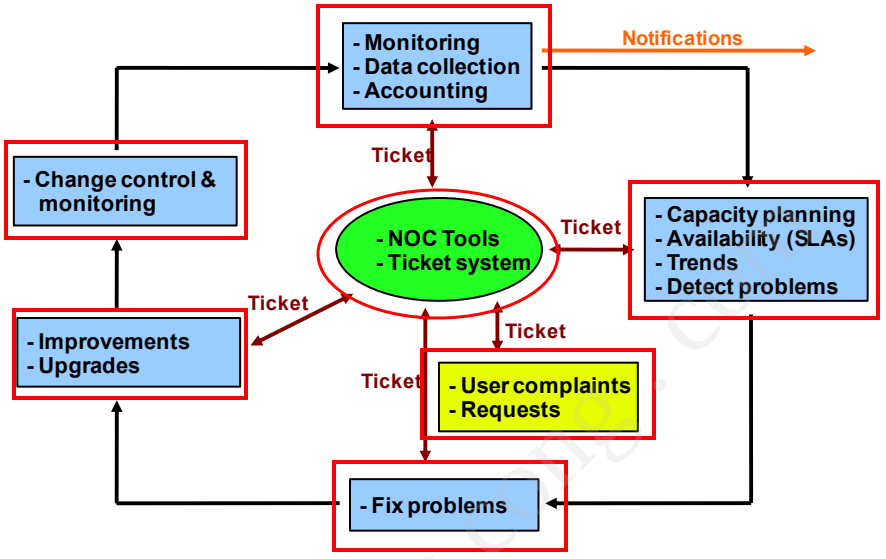
Các chức năng của một NOC (1/2)

1. Giám sát và đánh giá được khả năng thực thi của hệ thống & mạng
2. Giám sát, phát hiện và xử lý lỗi trước khi người dùng cuối nhận biết lỗi.
   - Hệ thống thẻ lỗi (trouble tickets)
3. Lưu trữ có hệ thống và cập nhật được các thay đổi về thông tin cấu hình của các thành phần được quản trị (changes control)
4. Hoạch định và quản lý tài nguyên mạng.
   - Phân tích và đánh giá khả năng hoạt động mạng
   - Nhận diện cơ hội để cải thiện khả năng hoạt động của hệ thống

Các chức năng của một NOC (2/2)

5. Hoạch định và quản lý bảo mật.
   - Giám sát, phân tích và kiểm toán các giải pháp bảo mật đang triển khai
   - Kiểm toán sự tuân thủ chính sách bảo mật
6. Quản lý được công tác quản trị:
   - Phân cấp quản trị
   - Kiểm soát truyền thông trong quản trị hệ thống & mạng

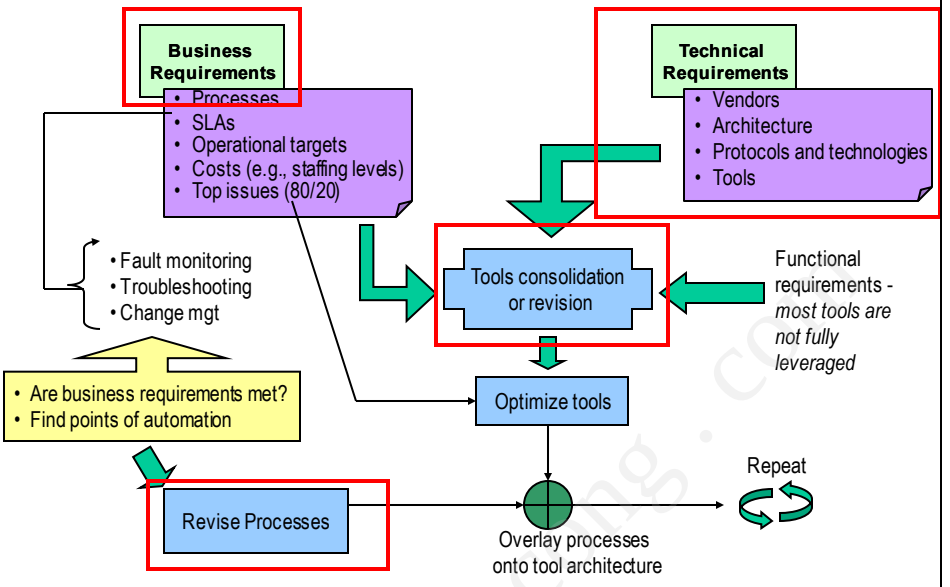
Khối chức năng của một NOC



Triển khai quản trị mạng

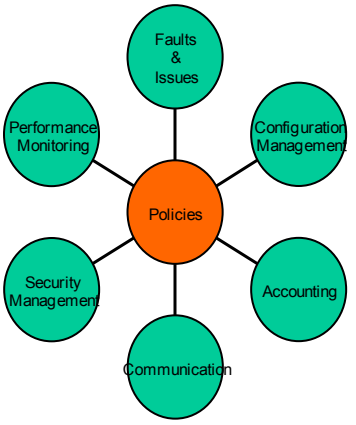
1. Giám sát hoạt động mạng
2. Thu thập thông tin quản trị mạng
   - Thu thập thông tin về các sự kiện quan tâm (polling)
   - Nhận các cảnh báo
   - Ghi nhận vào logfile các sự kiện xảy ra tại các hệ thống được quản trị.
3. Phân tích và đánh giá khả năng hoạt động mạng
4. Nhận diện cơ hội để cải thiện khả năng hoạt động của hệ thống.

Công tác quản trị mạng tại NOC



Hoạch định công tác quản trị mạng

1. Qui trình khai thác và quản trị phải được xây dựng và cập nhật để có thể quản lý được công tác quản trị tại cơ sở.
2. Xây dựng các chính sách quản trị liên quan đến các chức năng quản trị.
3. Xây dựng nền tảng thực hiện các các cơ chế quản lý mạng:
   - Quản trị dựa trên chính sách
   - Quản trị dựa trên thỏa thuận dịch vụ (LSA)
4. Hoạch định khả năng cung cấp tài nguyên mạng.



Quản trị dựa trên chính sách (Policy-based management)

- Chủ đầu tư hay người đứng đầu tổ chức phải xây dựng một chính sách chia sẽ tài nguyên và chính sách bảo mật
- Các chính sách được xây dựng trên cơ sở có sự tư vấn chuyên môn của các bộ phận liên quan:
  - Bộ phận quản lý nhân sự
  - Bộ phận quản lý tài chánh và đầu tư
  - Bộ phận CNTT
- Manager sẽ thiết lập mức ưu tiên cao nhất đối với lưu lượng videoconferencing trong khi đó mức ưu tiên sẽ thấp nhất đối với dịch vụ email.

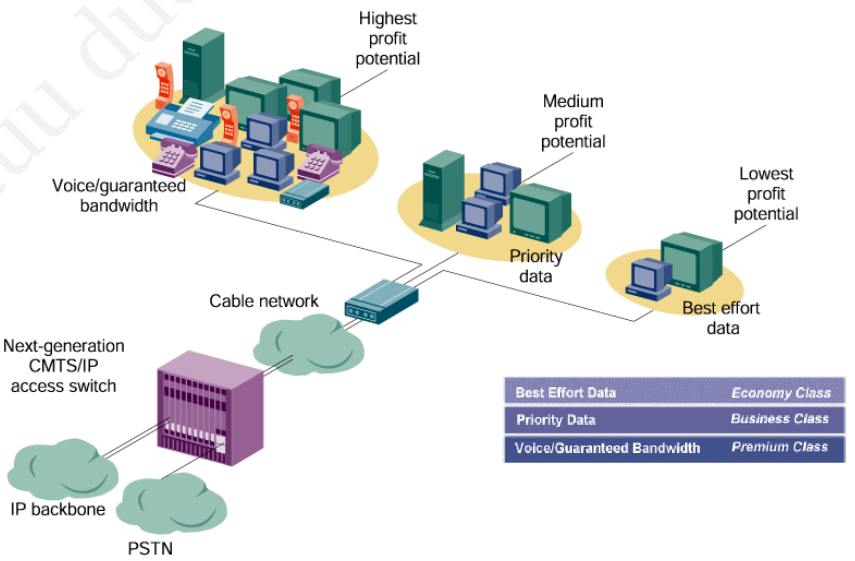
Quản trị dựa trên mức thỏa thuận dịch vụ 1/2) (Service-level agreements)

- Xây dựng các bảng biểu chi tiết về các mức thỏa thuận dịch vụ mạng liên quan.
- Mức thỏa thuận dịch vụ mạng được tập trung vào việc chỉ rõ mức độ cụ thể của các tiêu chuẩn về chất lượng dịch vụ truyền thông và mức độ xảy ra lỗi.
  - Băng thông truyền
  - Độ trễ lớn nhất cho phép
  - Tỉ lệ mất gói
  - Thời gian gián đoạn downtime hay MTBF và MTTR

Quản trị dựa trên mức thỏa thuận dịch vụ (2/2) (Service-level agreements)

- Hoàn cảnh áp dụng:
  - Thuê bao dịch vụ ứng dụng hay dịch vụ truyền thông giữa tổ chức đầu cuối và nhà cung cấp dịch vụ công cộng.
    - Các mức độ bồi thường cũng được nêu rõ trong bảng thỏa thuận dịch vụ này.
  - Áp dụng cho việc phân loại và đánh giá mức độ rủi ro và yêu cầu về khả năng sẵn sàng của hệ thống này.
- ví dụ về mức thỏa thuận dịch vụ về giá trị MTBF yêu cầu nhỏ nhất 99% cho đường thuê kênh riêng T1 trong thời gian 4 tháng.

Phân loại LSA cho từng loại tài nguyên mạng



Xác định các thông số quản trị và baseline liên quan (1/2)

Liên quan đến việc đo và ghi nhận vào hồ sơ kỹ thuật về trạng thái hay giá trị cụ thể của tham biến quản trị tại thời điểm đối tượng được quản trị hoạt động đạt mức yêu cầu (trong thiết kế)

Giá trị baseline có thể được sử dụng để đánh giá thực trạng mạng hiện tại và giúp cho người quản trị mạng có thể hoạch định cho việc cải thiện hoạt động mạng trong tương lai.

Việc xác định và cập nhật baseline liên quan được thực hiện ngay sau khi có các thay đổi về cấu hình thành phần của hệ thống mạng.

Xác định các thông số quản trị và baseline liên quan (2/2)

- Baseline của các tham biến quản trị (Mibs):
  - Phân tích các thông tin quản trị được thu thập từ một số các tham biến quản trị theo các chức năng quản trị tại nhiều hệ thống liên quan, bao gồm các loại server, các thiết bị nối mạng như routers, bridges, switches, hubs...

- Baseline về cấu trúc mô hình mạng:
  - Các sơ đồ kết nối mạng:
    - sơ đồ cấu trúc cable
    - sơ đồ kết nối vật lý
    - sơ đồ logic…

Qui trình thực hiện quản trị khả năng thực thi (1/2)

1. Nhận diện các tham biến quản trị và giá trị baselines.
2. Giám sát và thu thập thông tin (polling/ trapping):
   - Chỉ định tập tham biến cần thu thập
   - Chỉ định giá trị ngưỡng cho các cảnh báo cần thiết
   - Thu thập thông tin
3. Phân tích thông tin.
   - Thông tin thu thập được online và offline
   - Các sự kiện tương quan (Correlation events)
   - Các thông tin quản trị có được trước đó (Historical data)
   - Nhận diện xu hướng và đánh giá khả năng thực thi của hệ thống mạng.

Qui trình thực hiện quản trị khả năng thực thi (2/2)

4. Thực hiện điều khiển (Controlling):
   - Xử ký từng bước:
     - » Nhận diện được các thành phần gây nên sự suy giảm khả năng thực thi.
     - » Cách ly nguồn gây giảm sút khả năng thực thi
   - Có thể liên quan đến các chức năng quản trị khác.
   - Điều chỉnh giá trị một số thông số cấu hình liên quan.
   - Hoạch định lại tài nguyên
     - » nâng cấp
     - » mở rộng.

Công tác quản lý lỗi:

- Đội ngũ quản trị mạng có nhiệm vụ phân tích các sự kiện thu thập được để có thể chẩn đoán và phối hợp với các cộng sự để giải quyết sự cố
  - Sự cố có khả năng xảy ra
  - Sự cố đã xảy ra.
- NOC kiểm tra, lần vết và truy cứu để giải quyết triệt để các sự cố xảy ra.
- Các sự cố không được giải quyết triệt để phải lập báo cáo cụ thể cho người có trách nhiệm.

Qui trình quản trị lỗi

1. Nhận diện tham biến quản trị của đối tượng liên quan.
2. Giám sát và phát hiện lỗi:
   - *Polling*
   - *Alarms/ trapping*
3. Nhận diện các sự kiện tương quan
4. Định vị và cách ly lỗi
5. Thay thế hay phục hồi
   - *Phục hồi tự động.*
   - *Phục hồi nhân công*
   - *Sửa chửa*
   - *Mua mới*

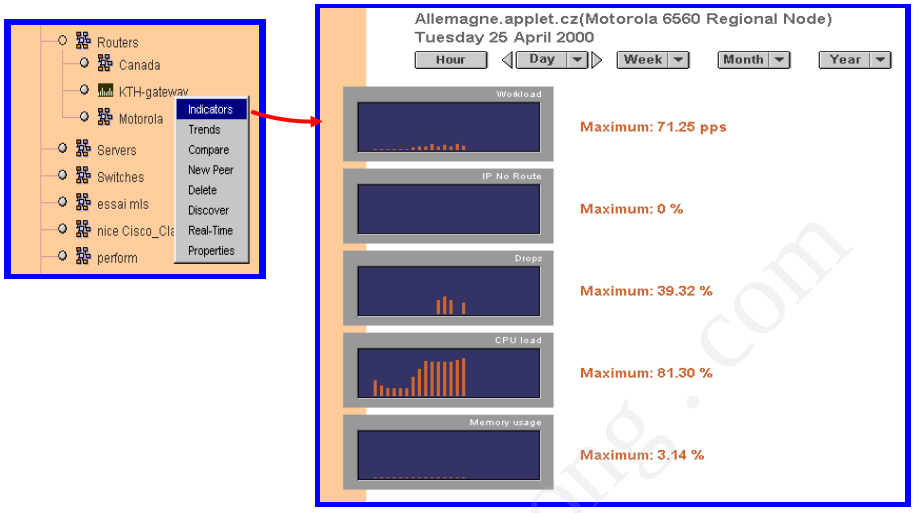
Trouble Tickets

- Hệ thống thẻ lỗi cho phép thống kê và báo cáo các lỗi xảy ra trên hệ thống mạng.
  - Có thể tự động tạo ra nhờ các phần mềm chuyên dụng
  - Tạo bằng nhân công bởi bộ phận khai thác mạng NOC
- Mục đích sử dụng trouble tickets
  - Theo dõi và thống kê các sự cố xảy ra
    - Thống kê các loại lỗi theo các thuộc tính cần thiết.
  - Hỗ trợ các giải pháp xử lý hư hỏng theo mức độ ưu tiên khác nhau.

Thống kê hằng ngày với dữ liệu về lưu lượng mạng:

- Đánh giá chất lượng mạng:
  - Tổng số gói/ byte với cái loại lỗi trên mỗi interface
  - Thông lượng truyền trung bình, thấp nhất, cao nhất
- Đánh giá lỗi trên hệ thống và hạ tầng mạng.
  - Thống kê các loại lỗi theo các tiêu chí:
    - Loại thiết bị
    - Loại phần mềm
    - Nhà sản xuất
    - Khu vực xảy ra lỗi
- Thống kê công tác xử lý lỗi:
  - Theo thời gian (ngày, tháng, năm)
  - Theo nhân viên xử lý
  - Nhận định được nguyên nhân gây ra lỗi
  - Kết quả cuối cùng

Thống kê hằng giờ, ngày, tháng, năm



Mục đích thống kê lưu lượng mạng

- Đánh giá mức sử dụng tài nguyên các loại
  - Thống kê theo từng loại tài nguyên
  - Thống kê theo cá nhân người dùng hay nhóm người dùng
- Nhận diện nhu cầu sử dụng tài nguyên chính đáng từ người dùng
- Đánh giá xu hướng hoạt động mạng bằng các số liệu cụ thể và biểu đồ cần thiết.
- Nhận diện được nguy cơ tiềm ẩn các vị trí có thể sẽ bị nghẽn cổ chai
- Lập các phương án cải thiện khả năng cung cấp tài nguyên:
  - Nâng cấp hay mở rộng mạng,
  - Giải pháp cân bằng tải và fail-over

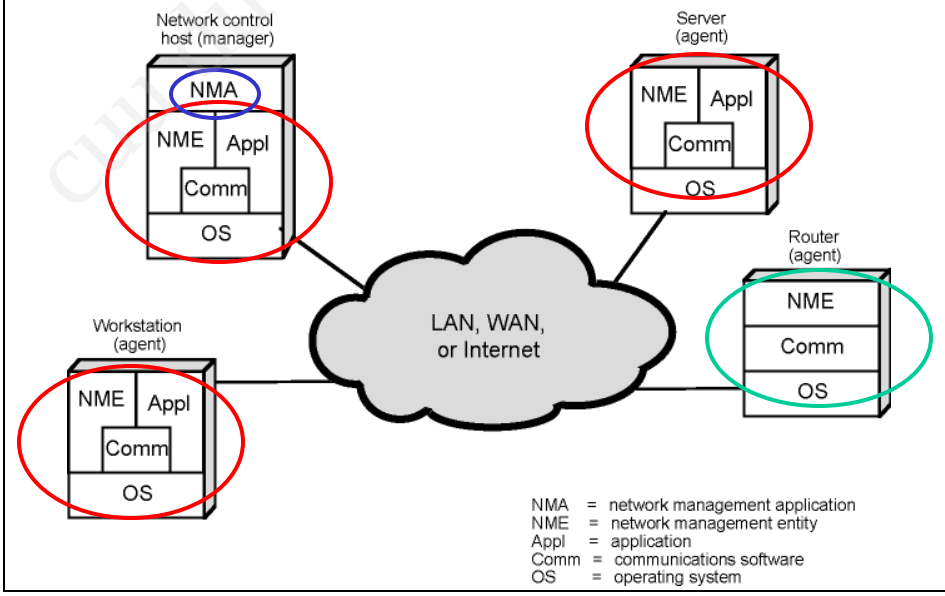
Qui trình quản lý thay đổi cấu hình

1. Thiết lập giá trị baseline
2. Nhận diện các thay đổi và hoàn tất yêu cầu thay đổi
3. Đệ trình thay đổi cấu hình

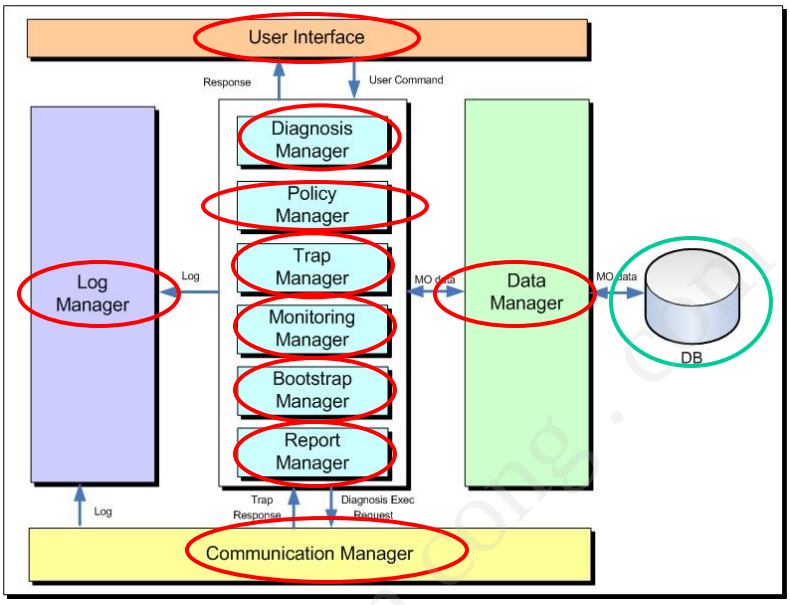
4. Đánh giá yêu cầu thay đổi
5. Xem xét và phân tích các ảnh hưởng liên quan
6. Phê duyệt cuối cùng: *đồng ý, không đồng ý, bổ sung, ...*

7. Thực hiện kiểm soát, theo dõi các thay đổi cấu hình liên quan
8. Kiểm định và kiểm toán hoạt động thay đổi cấu hình

5.2 Cấu trúc của hệ thống quản lý mạng



Cấu trúc cụ thể của hệ thống quản trị (1/3)



Các yêu cầu về tài nguyên

- Tài nguyên phần cứng của hệ thống: RAM, CPU, Hard-disk
  - Tùy thuộc vào lượng thông tin cần thu thập
  - Số máy cần quản trị
  - Thời khoảng polling/ interval
  - Độ lớn dữ liệu thu thập trong một kỳ polling / sample size
  - Phần mềm quản trị được sử dụng
- Yêu cầu về băng thông truyền
  - Tính liên tục
  - Tốc độ
  - Độ tin cậy
  - Thông lượng

5.3 Giao diện người- máy

- Công nghệ giao diện quản trị Desktop (DMI)
- Quản trị mạng với giao diện Web (HTTP & CGI)

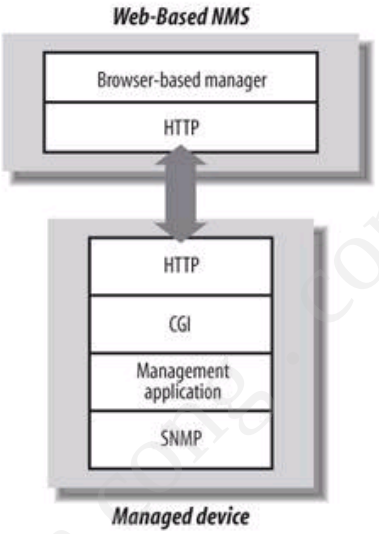
Desktop Management Interface (DMI)- 1992

- Gồm Digital Equipment, Hewlett-Packard, IBM, Intel, Microsoft, Novell, SunSoft, và SynOptics Communications (Bay Networks).
- -> phát triển tập các chuẩn cho lập trình ứng dụng APIs:
  - cho phép truy cập và quản trị các máy Desktop (HW& SW & I/O)
  - cho phép quản trị mạng LAN
  - độc lập với việc khai thác và hệ điều hành trên máy Desktop cần quản trị.
- DMI được thiết kế tích hợp với tất cả các giao thức quản trị mạng như SNMP hay CMIP.

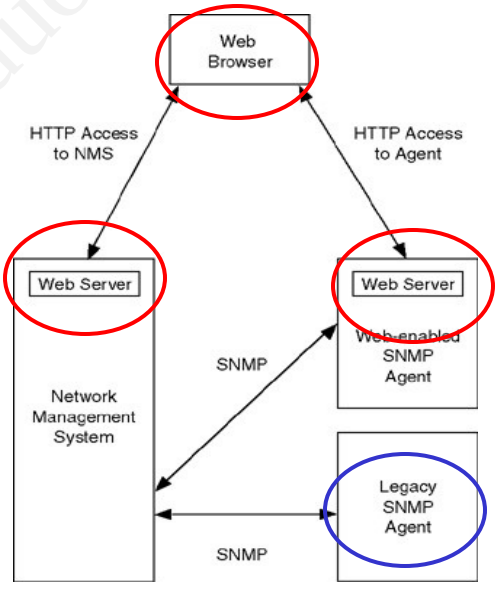
Quản trị mạng với giao diện Web (1/2)

- Sử dụng giao thức HTTP và Giao diện CGI
- Sử dụng ngôn ngữ XML cho việc trao đổi cấu trúc dữ liệu quản trị.

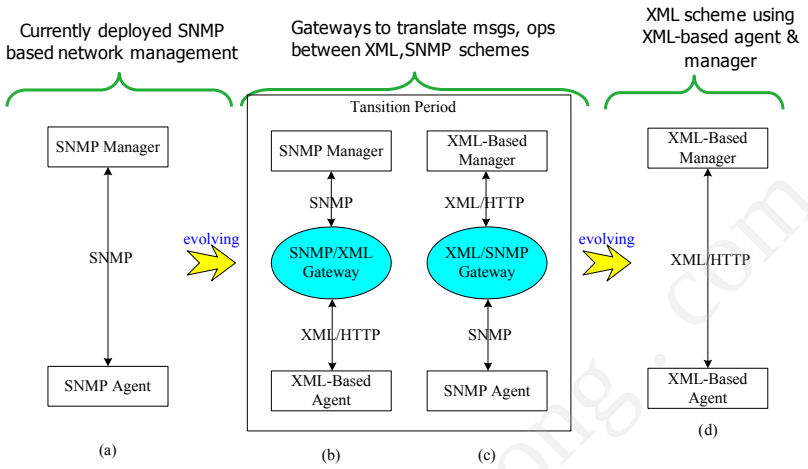
- Nhúng Web server vào thiết bị tương thích cùng với công cụ CGI để chuyển đổi các thông điệp điều khiển SNMP thành dạng thích hợp và ngược lại.



Quản trị mạng với giao diện Web (2/2)

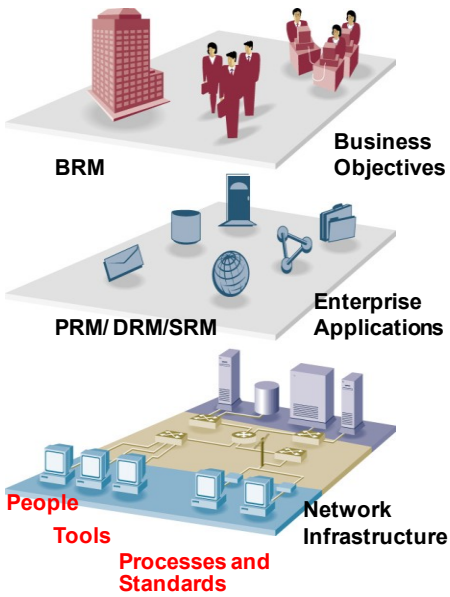


Kiến trúc quản trị mạng dựa trên web với XML



5.4 Hỗ trợ nhân viên khai thác

- 3 yếu tố quan trọng trong công tác khai thác và quản lý mạng:
  - Con người
  - Công cụ và phương tiện
  - Qui trình quản lý mạng
- Công cụ và phương tiện
  - Hồ sơ kỹ thuật mạng
  - Các công cu quản trị mạng
- Qui trình:
  - Qui trình khai thác
  - Qui trình thực hiện các chức năng quản trị lỗi và quản trị khả năng thực thi.
  - Quản trị thay đổi và quản trị cấu hình



Công tác đào tạo và huấn luyện

- Tham gia huấn luyện và đào tạo các loại hình:
  - Huấn luyện tập trung (In-class): huấn luyện chuyên sâu
  - Huấn luyện trực tiếp: one to one
  - Huấn luyện gián tiếp thông qua tài liệu hướng dẫn
- Cập nhật được kiến thức về công nghệ hiện đại về máy tính, thiết bị nối mạng, các phần mềm ứng dụng và sự tiến hóa của IP.
- Cập nhật được kiến thức về công nghệ viễn thông trong môi trường mạng IP và các tiến hóa của mạng LAN, MAN
- Tham mưu được cho lảnh đạo hiểu được về lợi ích chiến lược trong việc hỗ trợ hoạt động nghiệp vụ thông qua việc phát triển các ứng dụng trong môi trường CNTT.

Công tác của nhân viên quản trị

- Thực hiện công tác bảo dưỡng định kỳ và khai thác mạng hàng ngày
- Hỗ trợ người dùng cuối:
  - Xử lý sự cố
  - Huấn luyện và tư vấn
- Xử lý được sự cố xảy ra trên các hệ thống chia sẽ và thiết bị mạng
- Tuân thủ đúng các qui trình khai thác, bảo dưỡng và xử lý sự cố.
- Bảo đảm mạng hoạt động thông suốt
- Đánh giá được chất lượng hoạt động mạng
- Triển khai chiến lược quản trị proactive-> đáp ứng các yêu cầu nghiệp vụ của tổ chức.tiết kiệm được chi phí quản trị cho tổ chức.

Các nguyên tắc cần tuân thủ

1. Tự động hóa tất cả các công tác quản trị nếu có thể
2. Lập hồ sơ kỹ thuật mọi đối tượng liên quan
3. Thực hiện truyền thông tất cả các đối tượng quản trị đến người hay bộ phận liên quan ngay khi có thể
4. Nhận biết rõ về tài nguyên mạng
5. Nhận biết rõ về người dùng mạng
6. Nhận biết rõ về yêu cầu nghiệp vụ của tổ chức
7. Phải có kế hoạch và giải pháp trong vấn đề bảo mật.
8. Hoạch định chiến lược và qui trình quản trị cụ thể .

Các tiến trình then chốt trong quản trị mạng

- Định nghĩa nguyên tắc và phương pháp để các thành viên trong đội quản trị có thể làm việc được với nhau và khai thác công cụ quản trị.
- Định nghĩa phương pháp được triển khai để đáp ứng được yêu cầu nghiệp vụ trong môi trường hệ thống mạng.
- Giám sát và đánh giá được tính hiệu quả của kế hoạch **triển khai công cụ** và **chiến lược quản trị sự kiện**.

Công cụ và phương tiện hỗ trợ

- Hồ sơ kỹ thuật mạng và công cụ hỗ trợ
- Công cụ chẩn đoán và giám sát
- Công cụ đánh giá khả năng thực thi
- Công cụ kiểm thử chủ động và thụ động

Công cụ quản lý mạng mạng.
Công cụ lập sơ đồ mạng

Windows Diagramming Software

- Visio:
  http://office.microsoft.com/en-us/visio/FX100487861033.aspx
- Ezdraw:
  http://www.edrawsoft.com/

Open Source Diagramming Software

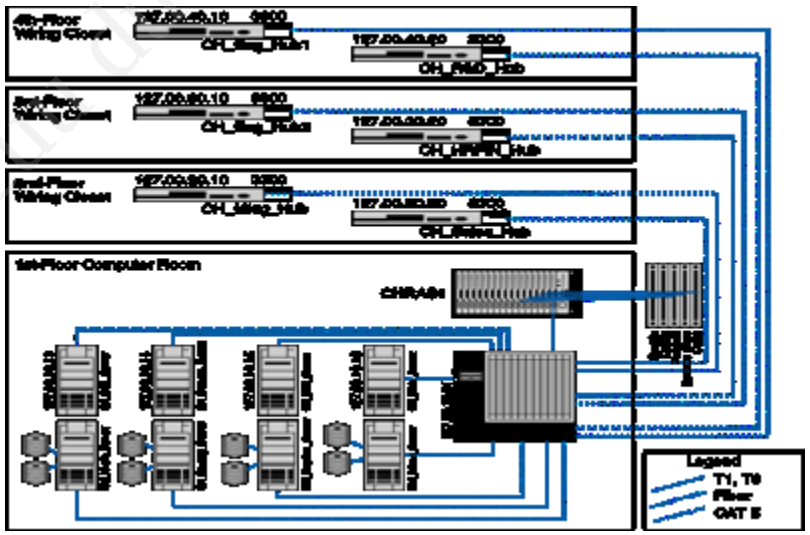
- Dia:
  http://live.gnome.org/Dia
- Cisco reference icons:
  http://www.cisco.com/web/about/ac50/ac47/2.html
- Nagios Exchange:
  http://www.nagiosexchange.org/

Hồ sơ kỹ thuật

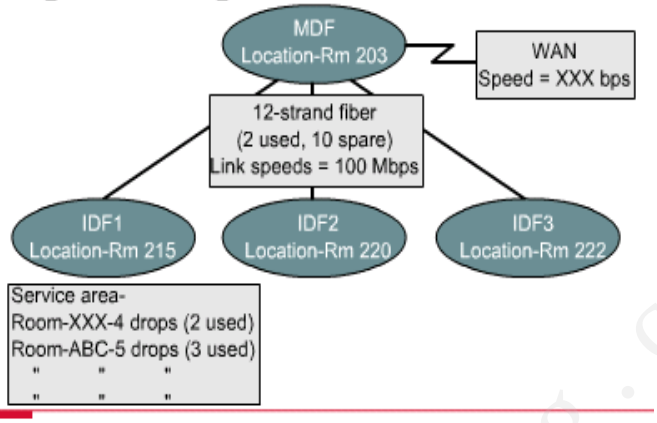
- Hồ sơ về kế hoạch đánh nhản cables, nhản patch panel.

- Hồ sơ cấu trúc cables.
  - Loại cables
    - Chiều dài cables
    - Loại connector

Network Configuration Diagram



Layer 1 Documentation - Logical Diagram

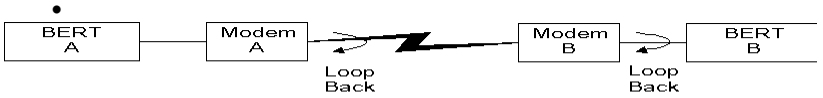


- Logical diagram is a snapshot view of all LAN implementation
- Useful in troubleshooting problems and implementing expansion in the future

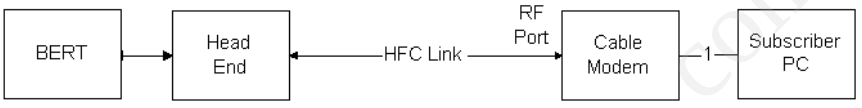
Cut Sheet

Connection	Cable ID	Cross Connection Paired#/Port#	Type of Cable	Status
IDF1 to Rm 203	203-1	HCC1/Port 13	Category 5 UTP	Used
IDF1 to Rm 203	203-2	HCC1/Port 14	Category 5 UTP	Not used
IDF1 to Rm 203	203-3	HCC2/Port 3	Category 5 UTP	Not used
IDF1 to MDF	IDF1-1	VCC1/Port 1	Multimode fiber	Used
IDF1 to MDF	IDF1-2	VCC1/Port 2	Multimode fiber	Used

Công cụ quản lý mạng mạng.
Công cụ kiểm thử lớp vật lý



Bit Error Rate Tester (BERT)



HFC Testing Using BERT

Công cụ quản lý mạng mạng.
Công cụ kiểm thử lớp vật lý

- Giám sát tại lớp vật lý
- BERT:
  - Phát chuỗi bit và phát hiện lỗi: so sánh BER nhận được với chuỗi bit mẫu được phát
    - Bit error rate (BER)
  - Sử dụng cho kiểm thử cục bộ (Loop back) hay kiểm thử link giữa 2 modem hay CPE.
    - Customer Premises Equipment- CPE

- VAM :Bộ công cụ kiểm tra điện tử -Electrical testers (voltage, ampere, etc.)
- Cable testers Bộ công cụ kiểm tra cáp - (open circuits, etc.)

Phần mềm quản trị mạng

- Yêu cầu tài nguyên:
- Phần cứng:
  - CPU, RAM, free Disk space, BW...
- Phần mềm:
  - Hệ điều hành
  - Cac gói phần mềm hỗ trợ xử lý thông tin và truyền thông
- Dịch vụ hỗ trợ:
  - Web services: IIS/ Apache
  - Database: SQL, MySQL, Oracle ...
  - Kết xuất đồ họa: RRD

Phần mềm quản trị mạng

- Các thành phần chức năng:
  - Giao diện người dùng:
    - Giao diện dòng lệnh- CLI
    - Giao diện đồ họa- Graphical User Interface (GUI)
  - Cơ sở thông tin quản trị:
    - MIB-II, RMON 1- RMON 2
    - Host Resources Mib
    - hay các thành phần tương đương
  - Cơ chế và giao thức thu thập thông tin quản trị:
    - Polling
    - Trapping
    - Log file/ syslog
    - SNMP; HTTP; XML-RPC
  - Cơ chế quản lý sự kiện

Phần mềm quản trị mạng

- Một số thành phần phụ trợ:
  - Thành phần biểu diễn đồ họa
  - Thành phần lưu trữ và kết xuất thông tin quản trị thu thập được (cơ sở dữ liệu).
  - Công cụ lập trình ứng dụng mạng (API) cho phép phát triển thêm các tiện ích khác.
  - Thành phần thực hiện truyền thông.

Công cụ quản trị
Phân loại công cụ quản trị

- Công cụ giám sát hệ thống
  - Kiểm tra so sánh với baselines
- Giám sát trạng thái & cấu hình
- Giám sát lưu lượng
- Công cụ hỗ trợ bảo mật
- Công cụ kiểm thử
  - Kiểm thử tải workload
  - Kiểm thử khả năng thực thi so với baselines
- Công cụ tích hợp cùng hệ điều hành
- Bộ công cụ độc lập

Phân loại công cụ phần mềm quản trị mạng (1/3)

1. Các gói phần mềm luôn được hỗ trợ sẵn với hệ điều hành.
   - Thuận tiện cho các hoạt động kiểm thử đơn giản.
   - Ping, tracert, route, arp, etherfind…
2. Bộ công cụ độc lập.
   - Các bộ công cụ được thiết kế tích hợp nhiều chức năng quản trị và có cơ sở dữ liệu về thong tin quản trị cho phép phân tích và đánh giá được xu hướng hoạt động của hệ thống và mạng.
   - Phân loại theo sản phẩm thương mại và sản phẩm mã nguồn mở, miễn phí.

Phân loại công cụ phần mềm quản trị mạng (2/3)

- Chức năng quản trị:
  - Khả năng thực thi;
  - Cấu hình;
  - Lỗi;
  - Tài nguyên và người sử dụng
  - Hỗ trợ quản trị bảo mật:
- Đối tượng quản trị:
  - Lưu lượng mạng LAN
  - Lưu lượng mạng LAN/ WAN
  - Các ứng dụng; dịch vụ
  - Cấu hình phần cứng của servers; thiết bị nối mạng

Phân loại công cụ phần mềm quản trị mạng (3/3)

- Cơ chế thực hiện:
  - SNMP
  - Ping
  - HTTP/ CGI
- Môi trường hoạt động:
  - DOS
  - Windows Server; Windows XP/ Server
  - Linux/Unix/ SUN
- Chi phí trang bị công cụ:
  - Miễn phí tòan bộ
  - Miễn phí phần lõi
  - Bản quyền thương mại

Một số bộ công cụ quản trị hoạt động mạng

- Tính năng giám sát mạng:
  - Sun's SunNet Manager
  - HP's OpenView
  - IBM's Netview for AIX
  - Solarwind
- Equipments/ link status
  - Nagios & Intermapper
- Traffic & services
  - NTOP; Nagios; Argus; Zennos
- Traffic:
  - MRTG; Cricket
- Configuration
  - Rancid

Công cụ hỗ trợ bảo mật

- Some security tools to consider:
  - NetFilter IP Tables – Firewall
  - WireShark – Protocol analyzer
  - Snort – Intrusion detection
  - Netcat – Feature rich tool. Great for debugging.
  - Nessus – Vulnerability scanner
  - Many many more…

Các công cụ giám sát trạng thái

Công cụ tiện ích của HDH- trạng thái & cấu hình

Tên công cụ	Hệ điều hành	Mô tả
Ifconfig	Unix	Sử dụng để chỉ định hay truy vấn thông tin địa chỉ đối với một interface.
Ping	Unix; Windows	Kiểm tra trạng thái của một node/ host
Nslookup	Unix; Windows	Truy vấn thong tin tên miền và địa chỉ của một host từ DNS server
Dig	Unix/ Linux	Truy vấn DNS server (Domain Name Groper)
Host	Unix/ Linux	Truy vấn thong tin của một host

Các công cụ giám sát trạng thái
Công cụ tiện ích của HDH- Giám sát đường đi

Tên công cụ	Hệ điều hành	Mô tả
netstat	Unix; Windows	Truy vấn thông tin về trạng thái hoạt động truyền thông hiện tại
Arp Rarp	Unix; Windows	Chỉ định hay truy vấn thông tin ARP cache
Route	Unix; Windows	Thay đổi hay truy vấn thong tin định tuyến tại một host
Traceroute Tracert	Unix; Windows	Truy vết các lộ trình đường đi từ nguồn đến đích, quan tâm đến độ trễ truyền thông.

A few Open Source solutions…

Performance
- Cricket
- IFPFM
- flowc
- mrtg
- netflow
- NfSen
- ntop
- pmacct
- rrdtool
- SmokePing

SNMP/Perl/ping

Ticketing
- RT, Trac, Redmine

Change Mgmt
- Mercurial
- Rancid (routers)
- RCS
- Subversion

Security/NIDS
- Nessus
- OSSEC
- Prelude
- Samhain
- SNORT
- Untangle

Net Management
- Big Brother
- Big Sister
- Cacti
- Hyperic
- Munin
- Nagios*
- Netdisco
- Netdot
- OpenNMS
- Sysmon
- Zabbix

5.5. An toàn trong khai thác và quản lý mạng

1. Vấn đề tĩnh điện (Static)
2. Bụi và chất gây ô nhiễm (contaminants)
3. Vấn đề nhiệt độ
4. Vấn đề độ ẩm
5. Sự chấn động (rung động/ Vibration)
6. Điều kiện về nguồn cung cấp
7. Software viruses

1. Vấn đề tĩnh điện (Static)

- Cẩn trọng trước khi tiếp xúc với các thành phần linh kiện và mạch điện tử bên trong thiết bị:
  - Vấn đề tiếp đất (grounding strap)
  - Vấn đề phóng điện (discharge)

2. Vấn đề bụi và chất ô nhiễm

- Tránh được bụi và bẩn ra khỏi các bộ phận bàn phím, ổ đĩa, cánh quạt tỏa nhiệt và lỗ thông khí trong thiết bị…
- Giữ cho môi trường nơi thiết bị được lưu giữ được sạch và không bị ô nhiễm bởi các chất như khói thuốc (nhựa thuốc lá và chất nicotine) .

3. Vấn đề nhiệt độ

- Nhiệt độ bên trong thiết bị:
  - Quạt gió gắn bên trong (built-in fans)
  - Khe thông gió
  - Tấm tỏa nhiệt
- Nhiệt độ môi trường:
  - Phòng đặt thiết bị
  - Hệ thống thông gió (quạt hút)
  - Hệ thống điều hòa

4. Vấn đề độ ẩm

- Vấn đề độ ẩm:
  - Ảnh hưởng hoạt động ổn định của linh kiện điện tử
  - Tuổi thọ của linh kiện, thiết bị

5. Vấn đề rung động (Vibration)

- Sự rung động và va chạm đột ngột dẫn đến sự lỏng lẻo của các thành phần linh kiện trong thiết bị.
- Cần tránh sự rung động và va chạm từ các nguồn như lưu lượng xe cộ bên ngoài, sấm sét, giông bảo
- Giải pháp:
  - Cần xiết chặt tất cả các linh, phụ kiện trong thiết bị.
  - Sử dụng các hệ thống cố định thiết bị như:
    - Racks / Cabins gắn chặt xuống đất
    - Các kệ rack với các khe cắm hay hệ thống bắt ốc, vít chắc chắn cho các thiết bị như:
      - Servers; switches, UPS; back panel… =>racks/ cabins
    - Sử dụng các chấu cắm hay gen chuyên dụng nối và ràng tại các Sockets/ connectors.

6. Vấn đề nguồn điện

- Vấn đề nhiễu điện từ (Electro-Magnetic Interference -EMI)
- Vấn đề nhiễu sóng vô tuyến điện (Radio Frequency Interference -RFI)
- Biến động của nguồn cung cấp.
  - Ổn áp (Electrical irregularities)

7 Vấn đề lây và nhiễm viruses

- **Boot virus** (boot sector /master boot record)
- **File virus** (.EXE, .COM,)
  - DLL, OCX (machine codes)
  - DOC, XLS (macro)
  - HTM, RTF, PDF (script, OLE).
- **Trojan Horse:** Seven, Girl Friend, The Thing...
- **Worms**