CHƯƠNG 3:

CHIẾN LƯỢC QUẢN TRỊ MẠNG

Trình bày: Bùi Minh Quân
Email: bmquan@cit.ctu.edu.vn

Nội dung

- **Chính sách bảo mật**
- **Giám sát - Monitoring**
- Hỗ trợ khách hàng- Hepldesks
- Dự phòng – Backup
- Khôi phục sau thảm họa – DisasterRecovery
- Nâng cấp và Bảo trì - Upgrades and Maintenance
- Trung tâm dữ liệu - Data center

Chiến lược là gì ?

Chiến lược là chương trình hành động, kế hoạch hành động được thiết kế để đạt được một mục tiêu cụ thể, là tổ hợp các mục tiêu dài hạn và các biện pháp, các cách thức, con đường đạt đến các mục tiêu đó.

Chính sách bảo mật

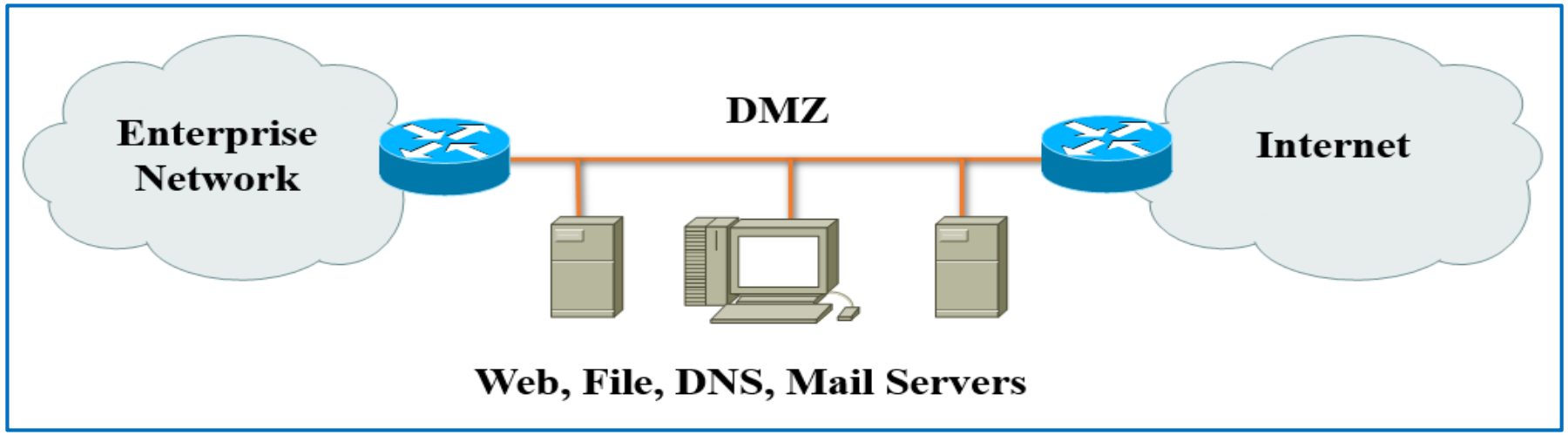
- An ninh mạng (security) bao gồm:
  - DMZ
  - Tường lửa (Firewall)
  - Hệ thống phát hiện xâm nhập (IDS)
  - Hệ thống ngăn chặn xâm nhập (IPS)
  - Phần mềm diệt virus
  - Hệ thống chứng thực người dùng
  - Mã hóa dữ liệu
  - Tài liệu bảo mật

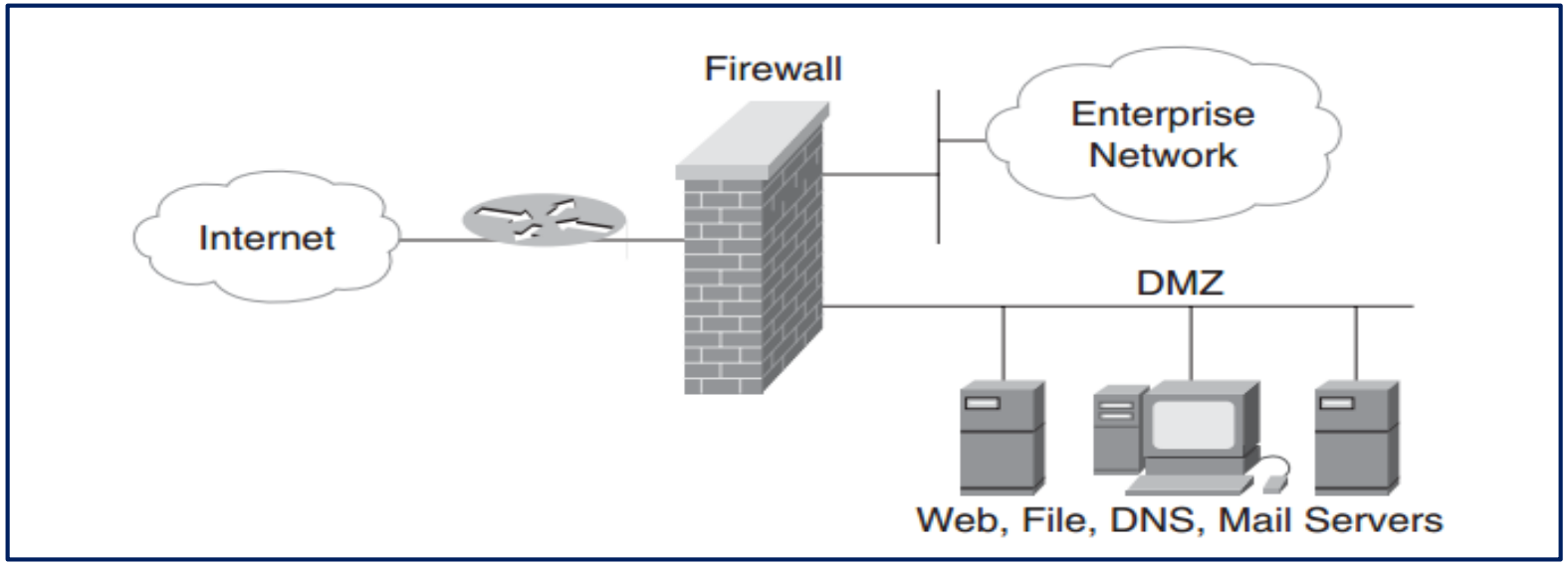
Chính sách bảo mật là các mô tả, các quy định, các quy trình đảm bảo an ninh mạng nhằm bảo vệ một mục tiêu cụ thể trong mạng

Chính sách bảo mật

- Phân tích rủi ro an ninh, xác định các mối đe dọa (bên trong, bên ngoài)
- Xây dựng các giải pháp bảo mật cần chú ý
  - Không làm gián đoạn khả năng kinh doanh
  - Bảo vệ được tài sản (mục tiêu bảo vệ)
  - Xác định chi phí thực hiện bảo mật
  - Xác định chi phí phục hồi sự cố
  - Phân tích chi phí liên quan đến sự cố an ninh làm gián đoạn công việc kinh doanh

Chính sách bảo mật: Mô hình mạng





Chính sách bảo mật - Firewall

- Tường lửa:
  - Hệ thống ngăn cách mạng bên trong và bên ngoài
  - Lọc gói tin theo :địa chỉ, giao thức, dung lượng, cổng
  - Đảm bảo chất lượng dịch vụ mạng QoS
- Hệ thống cảnh báo tấn công (IDS):
  - Quan sát mạng, quan sát gói tin trên mạng
  - Cảnh báo một số hoạt động tấn công mạng
  - Thông tin đến quản trị mạng khi có tấn công
  - Tích hợp với tường lửa để tự động đáp trả khi có tấn công

Chính sách bảo mật

- Phần mềm diệt virus
  - Cài đặt tại workstation
  - Phát hiện, tiêu diệt các loại virus
  - Phát hiện tiêu diệt các phần mềm độc hại
  - Bảo vệ Workstation trong quá trình liên lạc với hệ thống mạng
- Hệ thống chứng thực người dùng
  - Quản lý thông tin người dùng
  - Quản lý chính sách hoạt động người dùng
  - Quản lý quyền hạn sử dụng tài nguyên

Chính sách bảo mật

- Mục tiêu bảo mật là tiêu chí đầu tiên để tiến hành xây dựng chính sách bảo mật
  - Bảo vệ thông tin - dữ liệu lưu trữ
  - Đảm bảo chất lượng dịch vụ mạng
  - Chống chiếm dụng tài nguyên
  - Bí mật thương mại
  - Danh tiếng của một công ty

Chính sách bảo mật

- Phòng thủ theo chiều rộng
  - Xác định vành đai ngăn cách các phần tử cần bảo vệ - Firewall
  - Nhược điểm dễ bị xuyên qua ngoài ý muốn – thông qua Wireless, dùng chung máy tính Workstation
- Phòng thủ theo chiều sâu:
  - Định vị cụ thể mục tiêu bảo vệ
  - Dùng nhiều công cụ khác nhau trên cùng mục tiêu
  - Nhược điểm : tốn kém thời gian, tiền bạc, phức tạp khi sử dụng

Chính sách bảo mật: Lập tài liệu

- Người dùng căn cứ theo tài liệu bảo mật để làm việc
- Các loại tài liệu bảo mật:
  - Chính sách sử dụng tài nguyên
  - Chính sách giám sát – tính riêng tư
  - Chính sách truy xuất dịch vụ từ xa
  - Chính sách truy cập mạng
  - Chính sách lưu trữ thông tin trạng thái
- Các loại tài liệu phải trình bày rõ ràng, đầy đủ, phân cấp, mức độ bảo vệ cho từng mục.

Chính sách bảo mật: Lập tài liệu

- Chính sách sử dụng tài nguyên: xác định danh tính, quyền hạn sử dụng tài nguyên của người dùng
- Chính sách giám sát - tính riêng tư: xác định quyền hạn giám sát máy tính, giám sát mạng, mức độ riêng tư của người dùng
- Chính sách truy xuất dịch vụ từ xa: xác định quy tắc truy cập máy tính, dịch vụ mạng từ xa.

Chính sách bảo mật: Lập tài liệu

- Chính sách truy cập mạng: xác định quyền hạn kết nối mạng giữa các máy tính, người dùng và các liên mạng
- Chính sách lưu trữ thông tin trạng thái: xác định nội dung lưu trữ, hạn mục lưu trữ, thời gian lưu trữ của các logfile, phục vụ việc truy vết cho các sự cố mạng.

Các chiến lược bảo mật

1. Vận hành và bảo trì thiết bị: cập nhật bản vá, hủy bỏ các hệ thống cũ
2. Theo dõi bên thứ ba: bên có chịu trách nhiệm công bố các lỗ hổng bảo mật, hướng dẫn chính sách bảo mật.
3. Phân chia mạng thành nhiều khu vực nếu có thể.
4. Suy nghĩ lại việc triển khai hệ thống mạng không dây
5. Mã hóa dữ liệu nhạy cảm

Các chiến lược bảo mật

6. Điều tra sự dị thường: quá trình đăng nhập quá nhiều, sự cố máy chủ, "tiếng ồn" từ thiết bị .v.v.
7. Khóa quyền truy cập của người dùng: hầu hết nhân viên không cần mức truy cập cao mà họ được cấp
8. Sử dụng xác thực đa năng: sử dụng công nghệ chứng thực khác ngoài chứng thực bằng mật khẩu
9. Thực hiện và theo dõi chu trình phát triển phần mềm
10. Đào tạo người dùng

SYSTEM MONITORING

Giám sát hệ thống - System Monitoring

- Tại sao phải giám sát
- Hệ thống giám sát thời gian thực
- Chiến lược xây dựng hệ thống giám sát
- Công cụ giám sát trên nền web

Giám sát hệ thống - System Monitoring

- Tại sao phải phải giám sát: nếu không giám sát không thể quản lý được
  1. Nhanh chóng phát hiện và khắc phục sự cố
  2. Xác định nguồn gốc của vấn đề
  3. Dự đoán và tránh các vấn đề trong tương lai
  4. Tài liệu vận hành hệ thống của SA

Lý do giám sát

- Lưu trữ dữ liệu giám sát trong thời gian dài
  - Thời gian hoạt động
  - Hiệu suất
  - Bảo mật
  - Mức độ sử dụng

  Ví dụ: thời gian hoạt động của máy chủ web là 99,99% vào năm ngoái, so với 99,9% năm trước.
  Mức sử dụng mạng tối đa là 8 MBps, tăng từ 5 MBps.

- Sử dụng
  - Lập kế hoạch năng lực.
  - Lập kế hoạch cải tiến độ tin cậy hoặc bảo mật

Hệ thống giám sát thời gian thực

- Cảnh báo SA những thất bại xảy ra
- Phát hiện các vấn đề trước khách hàng
- Thành phần hệ thống giám sát thời gian thực
  - Hệ thống giám sát (Poll hoặc alert)
  - Hệ thống cảnh báo (Email hoặc SMS)

Kỹ thuật giám sát thời gian thực

- Polling
  - Thực hiện các phép đo theo khoảng thời gian đều đặn
  - Lưu trữ liệu đo lường
  - Vẽ biểu đồ dữ liệu
  - Tham dò trạng thái hệ thống và dịch vụ

  Ví dụ: cứ 5 phút ping server
- Alerting
  - Hệ thống có thể gửi cảnh báo đến hệ thống giám sát khi phát hiện vấn đề.

  Ví dụ: ghi nhận mạng Raid của HDD bị lỗi

Các loại giám sát

- Độ sẵn dùng
  - Theo dõi xác sự cố trong mạng, server và ứng dụng

  Ví dụ: không truy cập máy chủ web
- Sức chứa
  - Kiểm tra các ngưỡng cho CPU, Mem, Disk, Network

  Ví dụ: mức độ sử dụng CPU là 95%

Giám sát chủ động (Active Monitoring)

- Hệ thống giám sát chủ động có thể khắc phục các vấn đề.
  - Phản ứng nhanh hơn con người.
  - Thông thường chỉ có thể thực hiện sửa chữa tạm thời.
  - Không thể khắc phục được các vấn đề: đĩa xấu, tràn bộ nhớ
- Rủi ro
  - Độ tin cậy: Kiểm tra phản ứng tích cực trước khi triển khai.
  - Bảo mật: giám sát chủ động thường cần quyền quản trị viên truy cập vào toàn hệ thống giám sát.

Mức độ kiểm tra

- Kiểm tra máy chủ bằng ping: chỉ kiểm tra nối kết
- Kiểm tra xem ứng dụng đã được kích hoạt chưa
  - Thực hiện nối kết TCP với cổng dịch vụ
  - Kiểm tra danh sách dịch vụ
- Kiểm tra đầu cuối
  - Thực hiện toàn bộ các giao dịch như khách hàng

  Ví dụ: gửi và nhận một email

Chiến lược xây dựng hệ thống giám sát hiệu quả

- Thành phần cơ bản của hệ thống giám sát:
  1. **Collect**
  2. **Baseline**
  3. **Alert**
  4. **Report**
  5. **Analyze**
  6. **Share**

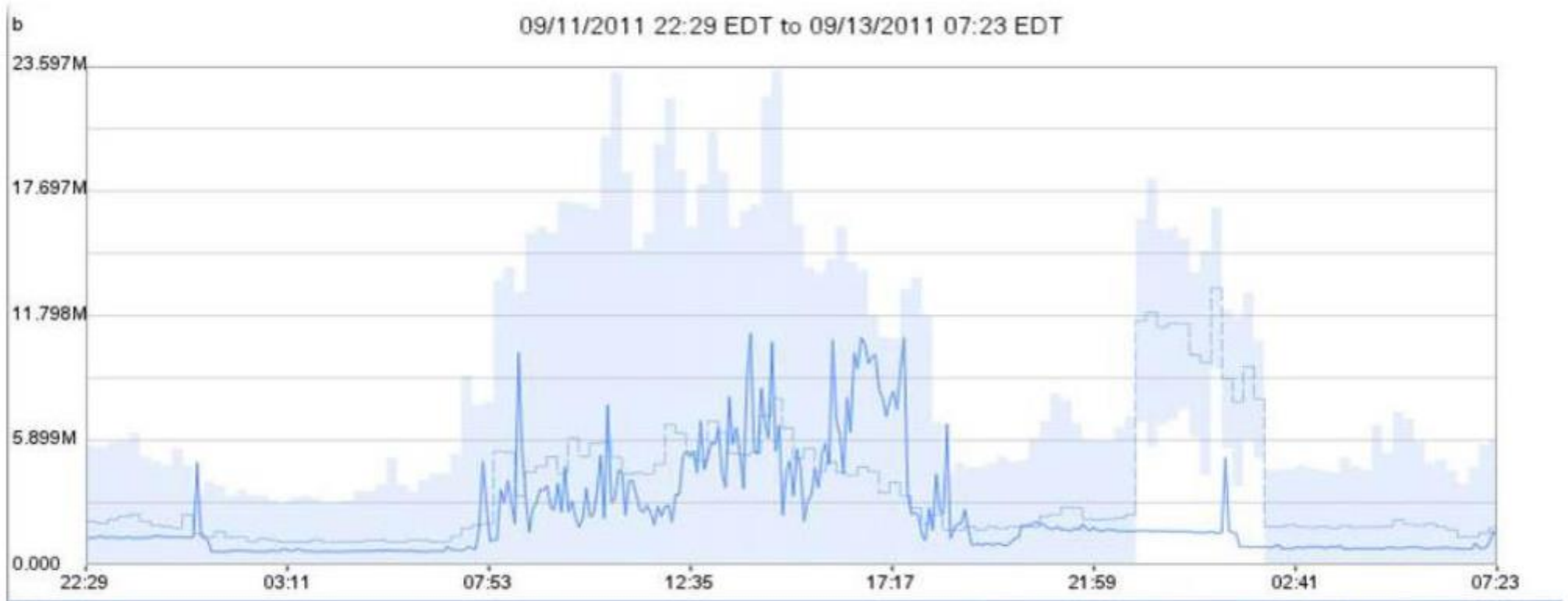
Chiến lược xây dựng hệ thống giám sát hiệu quả

- **Collect: chiến lược thu thập thông tin**
  - Nền tảng hỗ trợ thu thập dữ liệu thông qua: SNMP, NetFlow, IP SLA, WMI, JMX, NBAR, Syslog .v.v
  - Khả năng duy trì dữ liệu thời gian dài
  - Nền tảng giám sát phải có khả năng mở rộng theo nhu cầu thu thập dữ liệu

Chiến lược xây dựng hệ thống giám sát hiệu quả

- **Baseline (đường cơ sở)**
  - Dựng biểu đồ từ dữ liệu giám sát (phần mềm)
  - Cung cấp các tham khảo lịch sử giám sát: 15 phút, 1 ngày, 1 tuần, 1 tháng, 1 năm.
    - Giám sát hiệu suất hạ tầng mạng: thế nào là bình thường, thế nào là bất thường.
    - Các yếu tố ảnh hưởng
  - Cơ sở thiết lập chính sách cảnh báo

Performance baselines



Indicator	Freq	Last	Average	Peak	Total	Units
Core_Switch_6509.sevone.com - Vl254 - Vlan 264 - Internet Connection - Total HC Octets	300s	1.393M	2.242M	11.005M	266.224G	b
Baseline	300s	-	3.458M	13.173M	410.752G	b
Standard Deviation	-	-	3.434M	23.597M	-	b

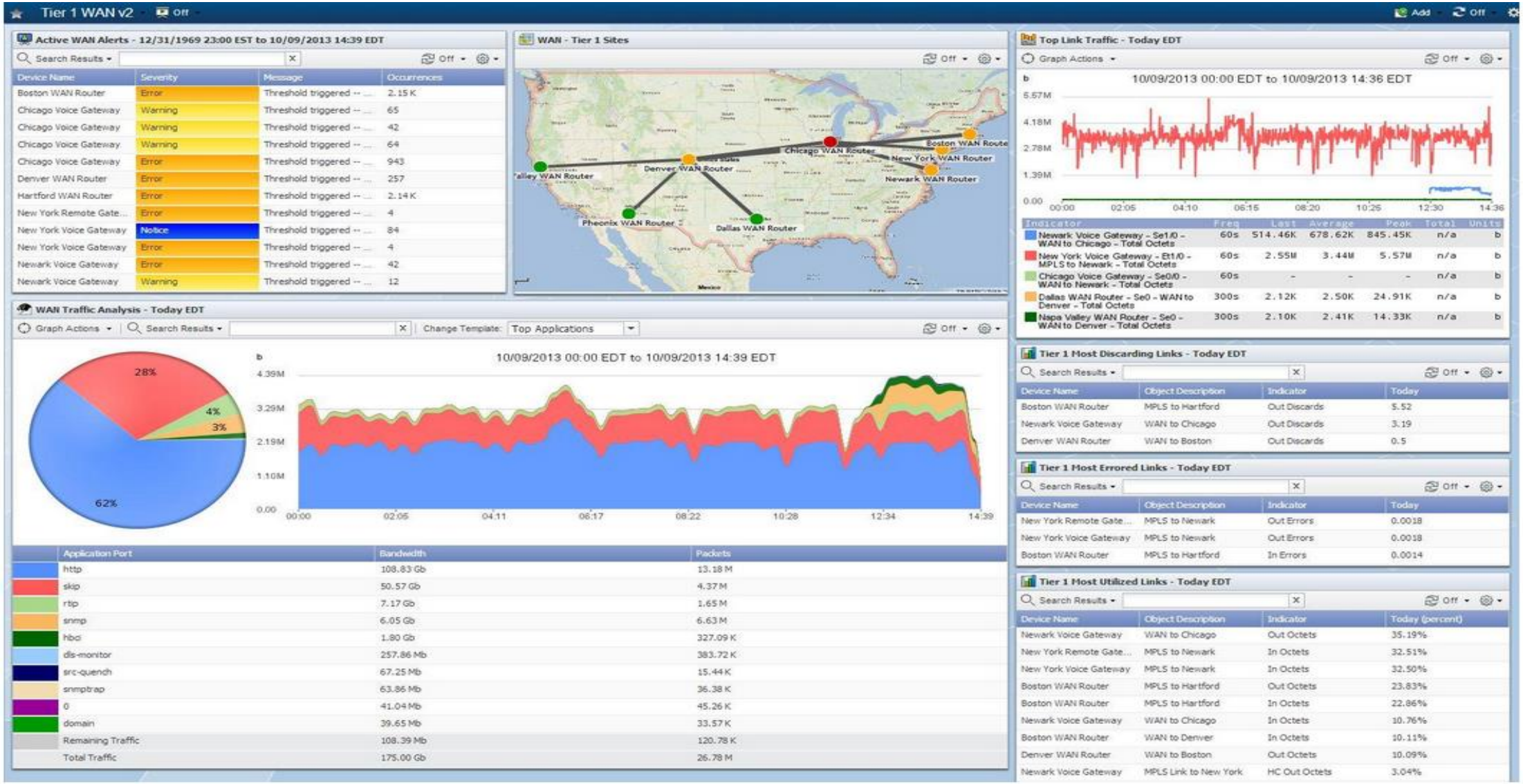
Chiến lược xây dựng hệ thống giám sát hiệu quả

- **Alert (thiết lập cảnh báo)**
  - Thiết lập các ngưỡng tĩnh
  - Thời điểm gia tăng mức độ sử dụng
  - Xác định độ lệnh so với đường cơ sở, xây dựng phương pháp dự đoán tin cậy

Chiến lược xây dựng hệ thống giám sát hiệu quả

- Report (báo cáo)
  - Báo cáo theo mẫu hoặc tùy chỉnh theo yêu cầu
  - Cung cấp thông tin: tỷ lệ mất gói, các chỉ số quan trọng khác
  - Không hỗ trợ cho phép điều khiển và gỡ rối
- Lựa chọn nền tảng: đáp ứng các yêu cầu
  - Hiển thị trạng thái của thiết bị, cấu hình, khung thời gian, hình ảnh và tóm tắt các thông tin quan trọng.
  - Cho phép hiển thị nhiều điểm dữ liệu khác nhau ?
  - Có giới hạn số lượng đối tượng trong một báo cáo không ?
  - Có thể nối kết các dạng biểu đồ báo cáo khác nhau không ?

Report (báo cáo dữ liệu giám sát)



Chiến lược xây dựng hệ thống giám sát hiệu quả

- Analyze (phân tích dữ liệu):
  - Mục đích: có cái nhìn sâu sắc về dữ liệu
    - Chủ động phát hiện và tránh các sự kiện về hiệu suất
    - Giúp tinh chỉnh cơ sở hạ tầng và đưa ra nhiều quyết định dự báo về cơ sở hạ tầng
    - Chìa khóa để phân tích đúng dữ liệu hiệu suất là phải có tất cả dữ liệu ở cùng một nơi.

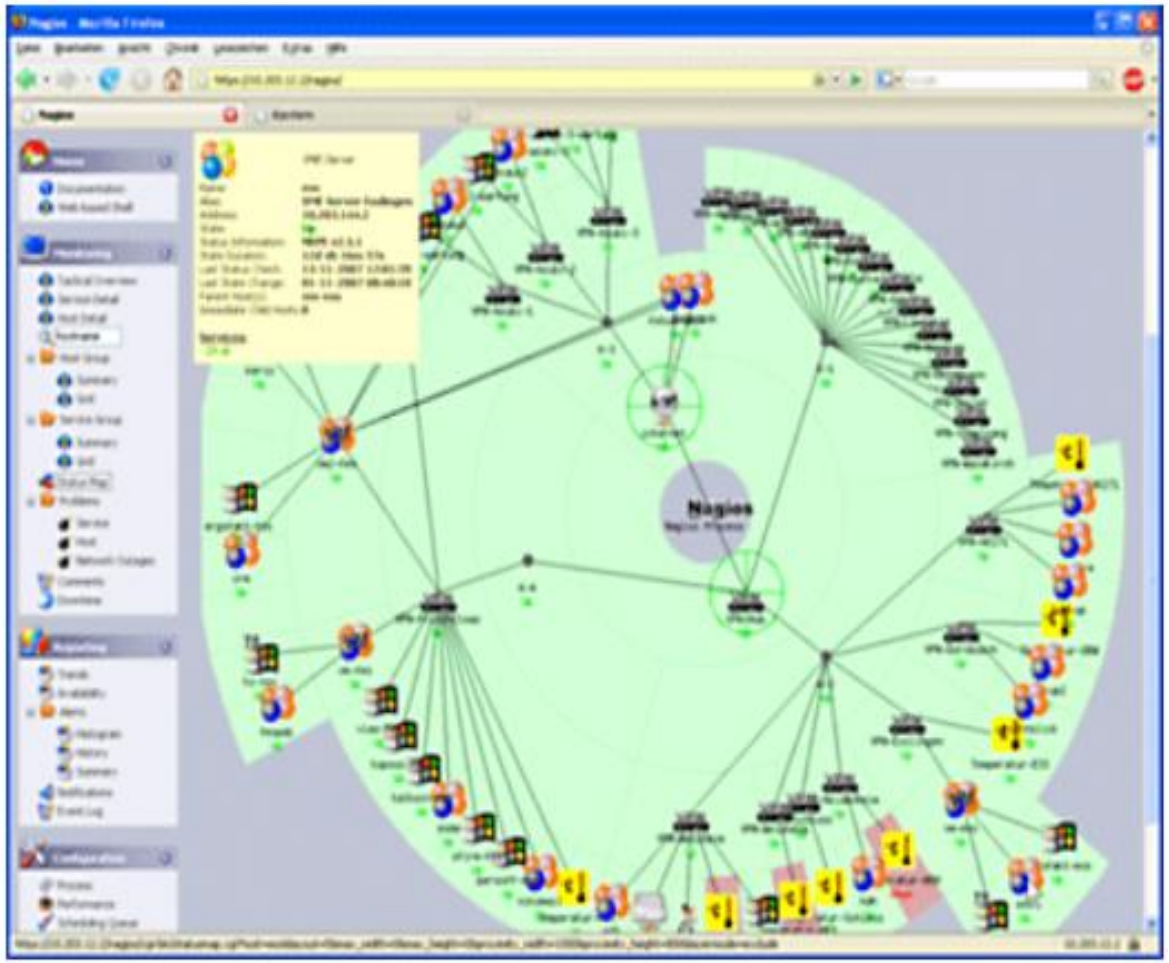
Chiến lược xây dựng hệ thống giám sát hiệu quả

- Share (chia sẻ thông tin)
  - Điều này đòi hỏi cần phải biết: đối tượng cần chia sẻ, đối tượng quan tâm của đối tương chia sẻ là gì?
  - Chia sẻ dữ liệu với các nền tảng khác: như lỗi hoặc các giải pháp quản lý cấu hình.
  - Dễ dàng xuất dữ liệu

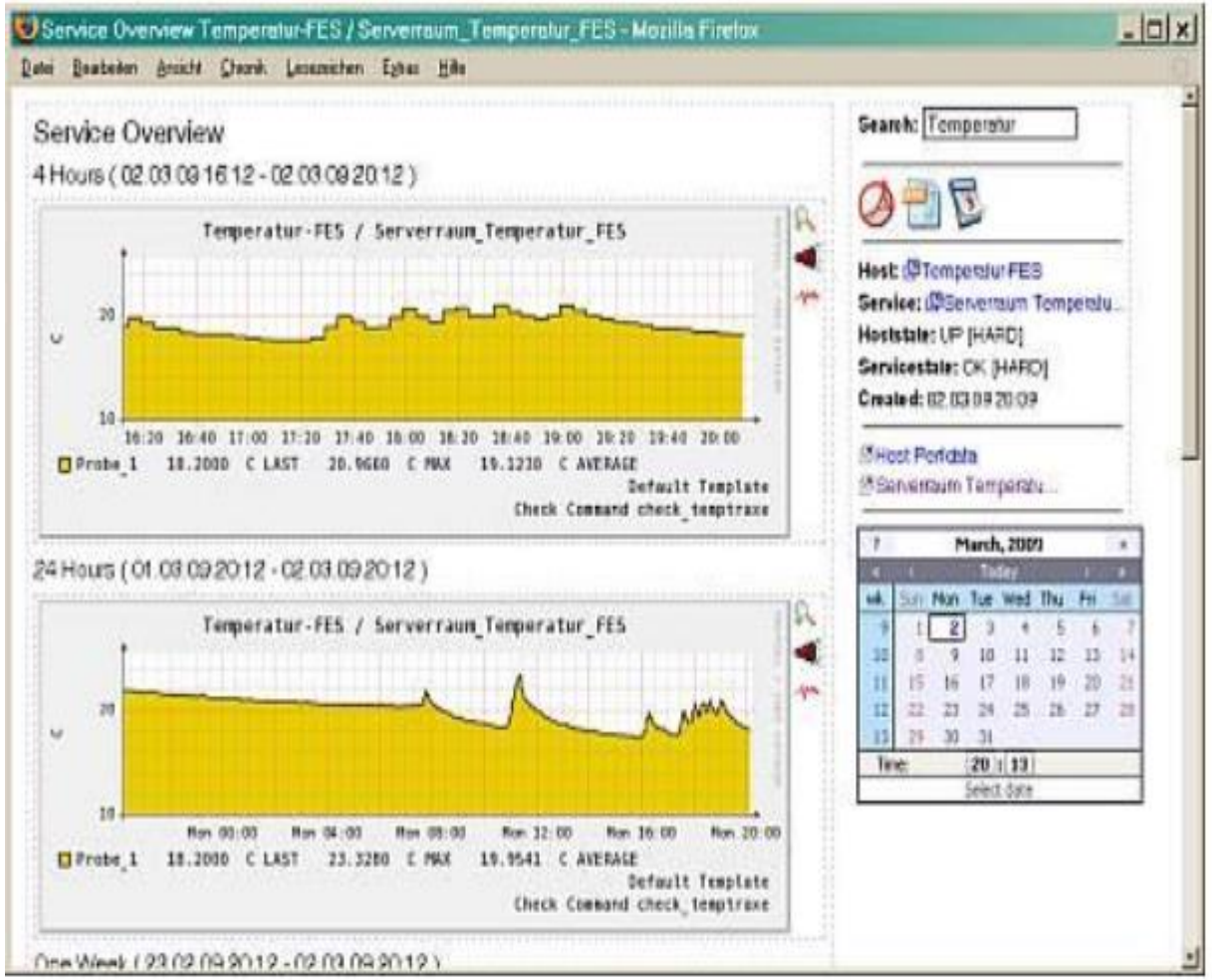
Các công cụ giám sát

- Ganglia
- Cacti
- Nagios
- Zabbix
- Hyperic HQ
- Munin
- ZenOSS
- OpenNMS
- GroundWork

Nagios

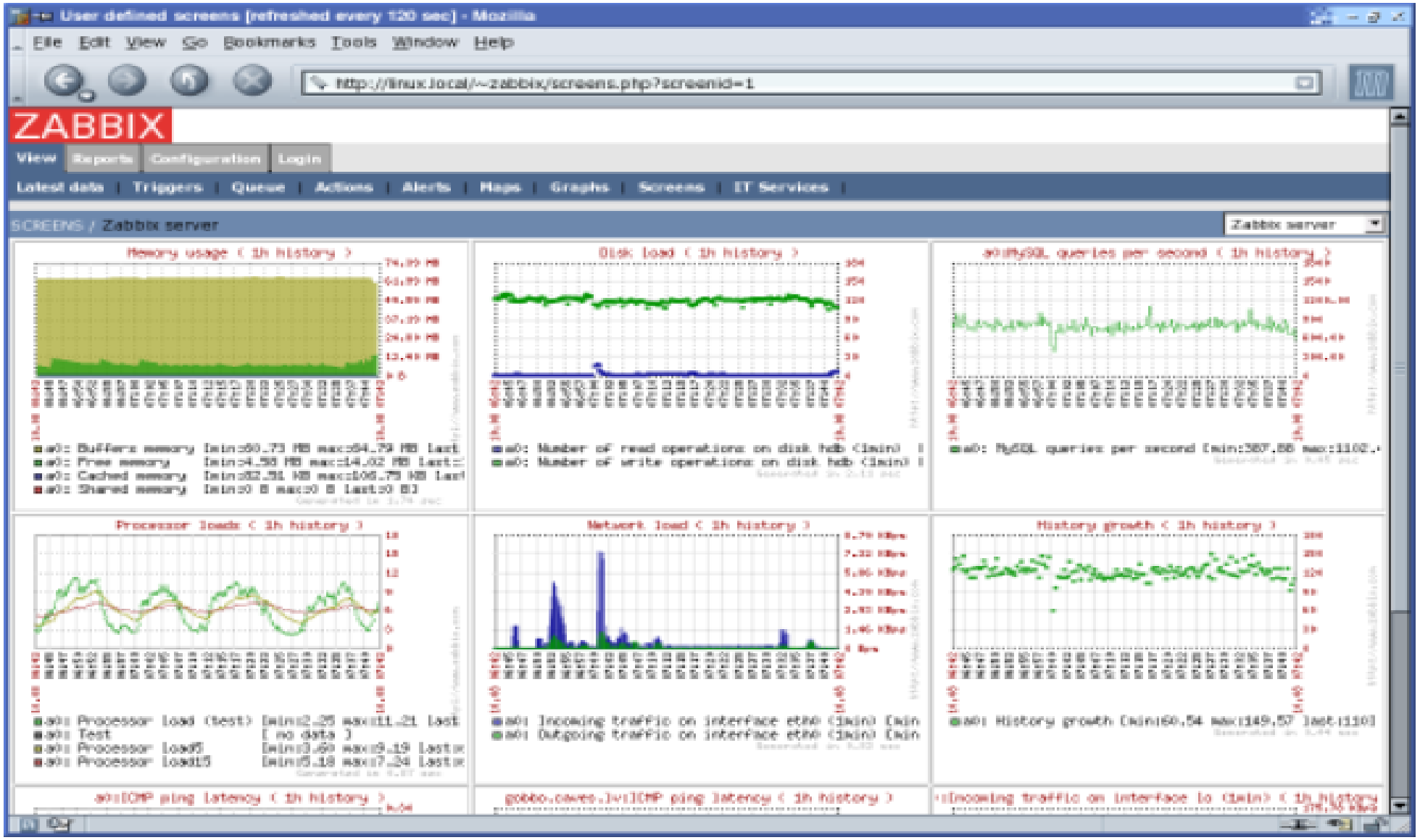


Nagios Network Maps



Nagios Graphs

Zabbix Graphs



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. http://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems