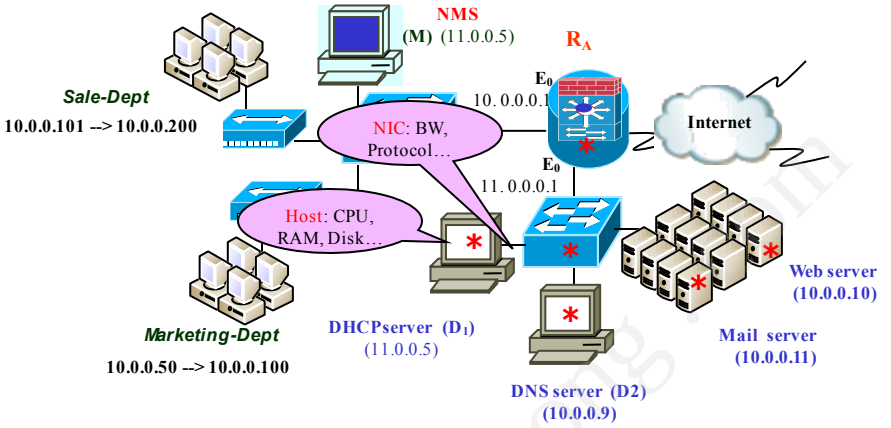
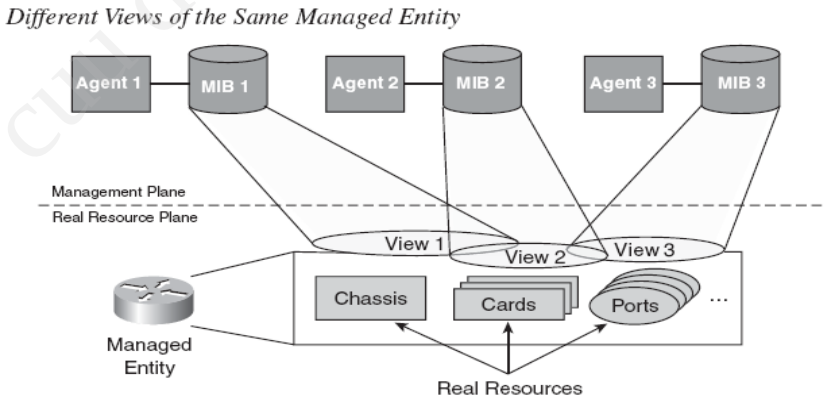
Chương 2 – Mô hình chức năng FCAPS

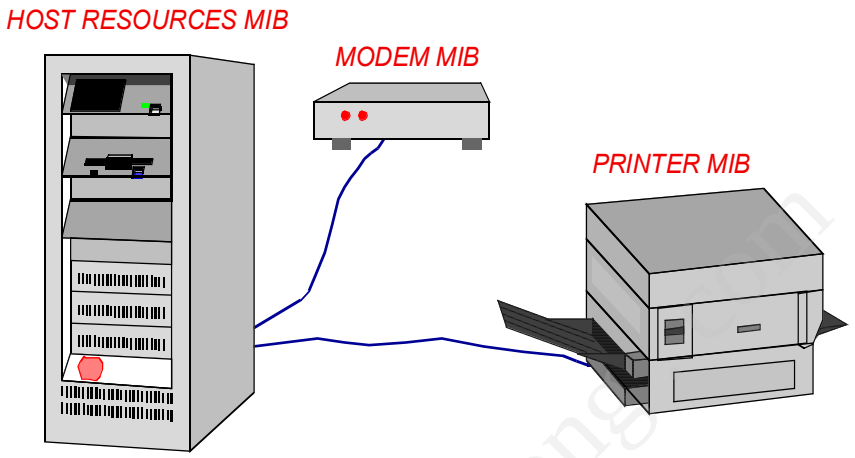
2.1 Các đối tượng cần quản lý



Management Information



Tài nguyên phần cứng của một hệ thống

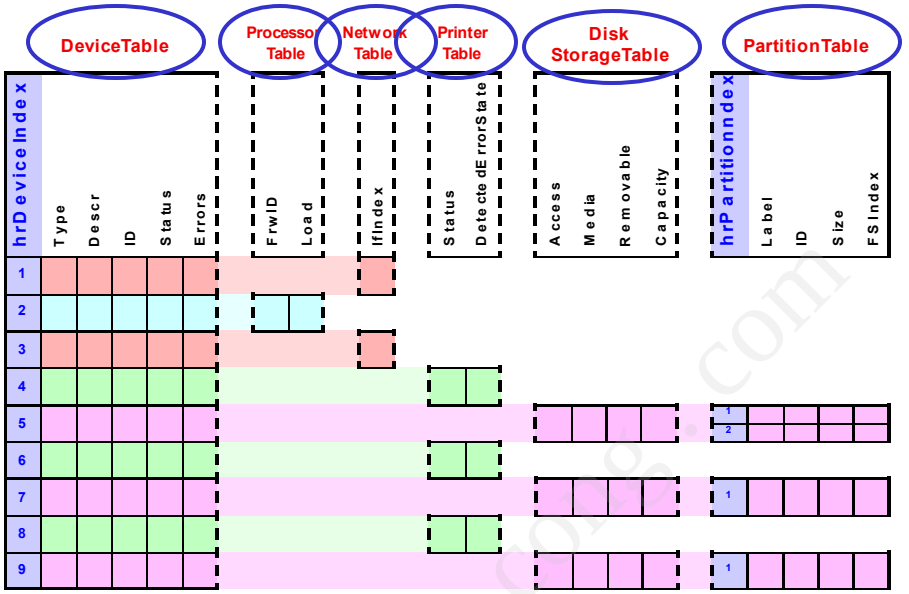


HARDWARE SPECIFIC MIBs

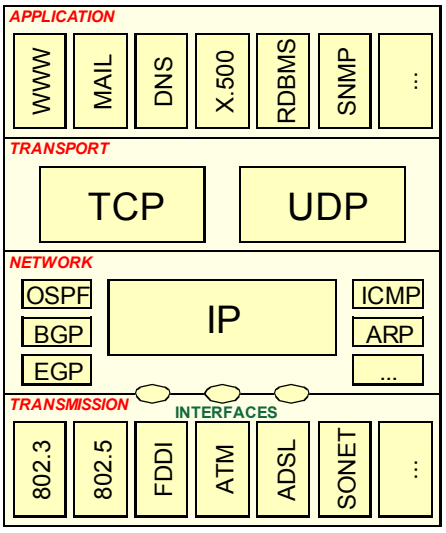
Title	RFC	STATUS
Host Resources MIB	**2790**	**D**
Entity MIB	**2737**	**P**
Job Monitoring MIB	**2707**	**I**
Printer	**1759**	**P**
Modem	**1696**	**P**
Parallel printer-like Hardware	**1660**	**D**
RS-232-like Hardware	**1659**	**D**
Character Stream Devices	**1658**	**D**
UPS	**1628**	**P**

LEGEND:
S = STANDARD
D = DRAFT STANDARD
P = PROPOSED STANDARD
I = INFORMATIONAL
E = EXPERIMENTAL

Tài nguyên phần cứng của một hệ thống
Host Resources Mib – RFC2790 (2/3)



Mibs liên quan bộ giao thức TCP/IP
PROTOCOL MIBS



TRANSMISSION MIBs -1

Title	RFC	STATUS
Ethernet-like Interface Types	2665	P
ADSL Lines	2662	P
SONET/SDH Interface Type	2558	P
ATM Management	2515	P
Frame Relay/ATM PVC Service Interworking Function	2955	P
DS3/E3 Interface Type	2496	P
DS1, E1, DS2 and E2 Interface Types	2495	P
DS0 and DS0 Bundle Interface Type	2494	P
Classical IP and ARP Over ATM (IPOA)	2320	P
IEEE 802.12 Repeater Devices	2266	P
Dial Control	2128	P
ISDN	2127	P
Frame Relay DTEs	2115	D

TRANSMISSION MIBs - 2

Title	RFC	STATUS
IEEE 802.3 Repeater Devices	2108	P
Data Link Switching	2024	P
IEEE 802.12 Interfaces	2020	P
IEEE 802.5 Station Source Routing	1749	P
IEEE 802.5	1748	D
SMDS	1694	D
Source Routing Bridges	1525	P
FDDI	1512	P
Bridges	1493	D
Bridge Network Control Protocol of PPP	1474	P
IP Network Control Protocol of PPP	1473	P
Security Protocols of PPP	1472	P
Link Control Protocol of PPP	1471	P

TRANSPORT LAYER MIBs

Title	RFC	STATUS
Real-Time Transport Protocol	2959	P
IP Version 6 MIB for the User Datagram Protocol	2454	P
IP Version 6 MIB for the Transmission Control Protocol	2452	P
User Datagram Protocol (UDP)	2013	P
Transmission Control Protocol (TCP)	2012	P

APPLICATION LAYER MIBs

Title	RFC	STATUS
MIB for the PINT Services Architecture	3055	P
Mail Monitoring MIB	2789	P
Network Services Monitoring	2788	P
RADIUS Accounting Server MIB	2621	I
RADIUS Accounting Client MIB	2620	I
RADIUS Authentication Server MIB	2619	P
RADIUS Authentication Client MIB	2618	P
Directory Server Monitoring MIB	2605	P
DNS Resolver MIB Extensions	1612	P
DNS Server MIB Extensions	1611	P
SNMPv2 MIB	1907	P
RDBMS MIB	1697	P

APPLICATION LAYER MIBs

Title	RFC	STATUS
DNS Resolver MIB Extensions	**1612**	**P**
DNS Server MIB Extensions	**1611**	**P**

2.2 Các chức năng quản trị

IETF sử dụng chuẩn mô hình chức năng của OSI:

1. Chức năng quản trị lỗi (Fault mgmt)
2. Chức năng quản trị khả năng thực thi (Performance mgmt).
3. Chức năng quản trị bảo mật (Security mgmt)
4. Chức năng quản trị tài nguyên (Accounting mgmt)
5. Chức năng quản trị cấu hình (Configuration mgmt)

2.2.1 Quản trị lỗi- Fault Management (1/3)

- Lỗi là các tình huống xẩy ra không đúng như thiết kế ban đầu
  - Baselines
  - Liên quan đến các giá trị thống kê và trạng thái của các thông số hoạt động của hệ thống và mạng.
- Các hoạt động:
  - Ngăn chặn lỗi xảy ra (prevent).
  - Phát hiện có lỗi xảy ra (detecting)
  - Định vị lỗi (locating)
  - Cách ly lỗi (isolating)
  - Thay thế / Sửa chửa

Quản trị lỗi- Fault Management (2/3)

- **Yêu cầu:**
  - Giám sát và thống kê được các loại lỗi tương ứng với đối tượng cần quản trị.
  - Nhận biết nguyên nhân gây ra lỗi và phục hồi lỗi.
  - Triển khai các giải pháp Fault-tolerance /Fail-over
- Quan tâm đến khả năng lỗi tại các điểm có thể làm tê liệt toàn bộ hệ thống : Single point of failure

Các loại lỗi (1/2)

- **Lỗi** truyền dữ **liệu.**
  - Nhận diện thông qua các lớp trong mô hình TCP/IP
    - TCP:
      - » Kết nối TCP
      - » Quá trình gởi và nhận các đoạn dữ liệu TCP
    - Gói IP và các lỗi liên quan
    - Tín hiệu xung clock tại lớp vật lý (dot3)
  - Nhận diện thông qua ICMP- source quench;
  - Trạng thái hoạt động hay không hoạt động tại interface (up / down)
- **Các** cảnh báo **về:**
  - nguồn điện
  - Đường truyền vật lý
  - Cháy nổ thiết bị

Các loại lỗi (2/2)

- Lỗi vi phạm QOS:
  - Số các gói lỗi trong 1 đơn vị thời gian
  - Số gói truyền lại
  - Thời gian tắc nghẽn hay suy giảm khả năng hoạt động của tài nguyên mạng.
    - » Quá tải: dẫn đến việc hủy gói gởi ra hay nhận vào
- Lỗi do phần mềm
- Lỗi do môi trường hoạt động
  - Độ ẩm
  - Nhiệt độ
  - Rung động
  - Vius …

Đánh giá và nhận diện lỗi

- Mức độ nghiệm trọng của lỗi.
  - Cảnh báo (Warning)
  - Lỗi nhỏ (Minor)
  - Lỗi quan trọng (Major)
  - Lỗi nghiêm trọng (Critical)
- Mức độ nhận diện được lỗi:
  - Nhận diện rõ ràng nguyên nhân gây ra lỗi (cleared).
  - Nhận diện không rõ ràng (indeterminate).
  - Thời gian , địa điểm đặt thiết bị và vị trí lỗi trên thiết bị.
- Hệ thống thẻ lỗi- Trouble Ticket

Trouble Tickets – thuộc tính quản trị

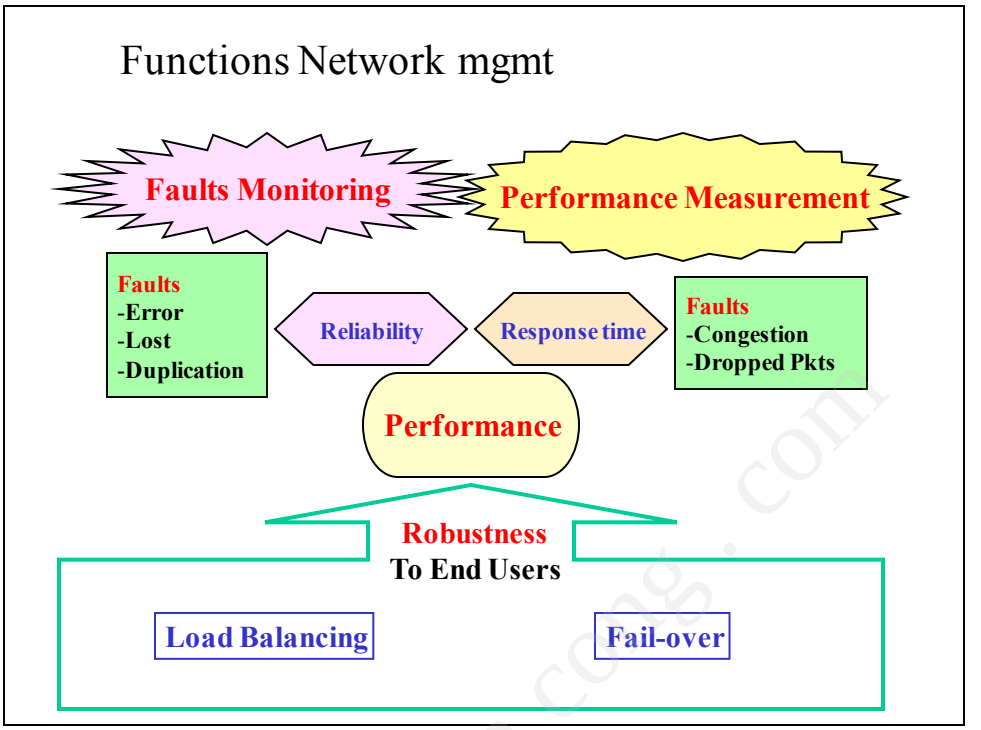
- Ngày, giờ hư hỏng xẩy ra
- Ngày, giờ hư hỏng được xử lý xong
- Thông tin người tiếp nhận báo hỏng
- Thông tin người xử lý hư hỏng
- Cơ sở nhận biết sự cố (thông tin thu thập được từ các Mibs so với baselines)
- Thông tin về nhận diện thiết bị hư hỏng
- Vị trí hư hỏng
- Tình trạng hư hỏng
- Loại lỗi gây ra sự cố
- Chẩn đoán nguyên nhân hư hỏng
- Phương pháp xử lý
- Kết quả xử lý

Trouble Tickets – Mục đích sử dụng

- Đánh giá và thống kê các loại lỗi
  - Khả năng nhận diện các loại sự kiện liên quan
  - Khả năng nhận diện các loại sự kiện tương quan
- Đánh giá tính đúng đắn trong xử lý hư hỏng
- Đánh giá tính hiệu quả trong công tác quản trị lỗi của quản trị viên.
- Đánh giá chất lượng sản phẩm hay chất lượng hậu mãi của nhà xản xuất, nhà cung cấp.

2.2.2 Chức năng quản trị khả năng thực thi (1/2)

- Qui trình Proactive
- Tập trung vào các đối tượng cần quản trị.
- **Các tiêu chí thực hiện:**
  - **Thời gian đáp ứng (Response time):**
    - Tắc nghẽn (congestion)
    - Mất gói-> truyền lại (Retransmission)
    - Yếu tố ảnh hưởng: Links/ Hosts (end systems + transition)
  - **Độ tin cậy (Reliability)-> truyền lại (ARQ)**:
    - Pkts Error; Duplication; Pkts loss
    - => ảnh hưởng đến: thời gian trễ và hiệu suất truyền
  - **Tính mạnh mẽ, bền bỉ (Robustness)**:
    - Cân bằng tải khi cần thiết (**Load Balancing**).



Thống kê dữ liệu và lỗi

- Đánh giá tính sẵn sàng của hệ thống :**Availability.**
  - Phần trăm thời gian tài nguyên mạng sẵn có đối với người dùng với tổng thời gian được đo.

Availability = MTBF/(MTBF+MTTR)

  - Downtime: thời gian hệ thống hay tài nguyên không sẵn sàng.

MTTRepair = MTTDiagnose + MTTRespond + MTTFix

- MTTDiagnose: Average number of minutes until the root cause is diagnosed (shows efficiency of NOC)
- MTTRespond: Average number of minutes until the service or vendor personnel arrives at location
- MTTFix: Average number of minutes until problem is fixed (shows efficiency of repair people)

- Ví dụ 1: số giờ mỗi tháng mà hệ thống hoạt động được chia với tổng giờ trong tháng (720 hours)
- Ví dụ 2: Xác định số giờ hoạt động nếu availability là:
  - 99% đến 99.5%
- Ví dụ 3: Nếu MTBF=10,000 và MTTR=4

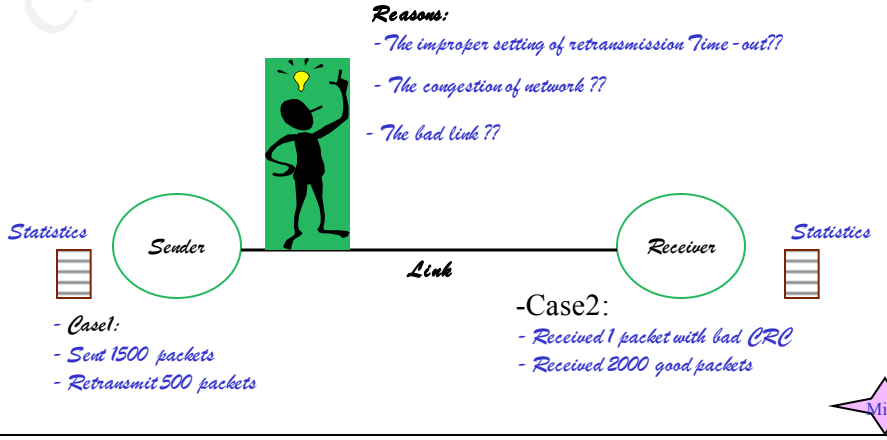
=> Availability = MTBF/(MTBF+MTTR)

= 10,000/(10,000+4) = **99,996%**

23

Nghiên cứu tình huống

- Thu thập thông tin thống kê cho phép đánh giá performance
- Ví dụ:



2.2.3 Quản trị tài nguyên - Accounting management (1/2)

- Đánh giá thực trạng đối với các thành phần tài nguyên mạng
  => tạo cơ sở hoạch định, phát triển hệ thống trong tương lai.
  - Giám sát, đo đạc và báo cáo thống kê từng loại tài nguyên.
    - Hàng ngày; Hàng tuần ; Hàng tháng; Hàng năm
    - Đo và báo cáo thống kê về số liệu sử dụng của người dùng cuối, về mức tiêu thụ, thời gian sử dụng.
      - Theo từng cá nhân
      - Theo nhóm
  - Phân tích-> xem xét -> đánh giá các thành phần liên quan
    - Khả năng thực thi
    - Mức khả dụng

Quản trị tài nguyên - Accounting management (2/2)

- Có giải pháp xử lý đúng đắn:
  - ✓ Tìm hiểu nguồn tiêu thụ tài nguyên:
    - Xác định được tài khoản sử dụng.
    - Xác định được máy truy cập sử dụng.
    - Không xác định được nguồn truy cập.
  - ✓ Đưa ra giải pháp thích hợp:
    - Phối hợp với các nhóm quản trị khác:
      - Nhóm quản trị khả năng thực thi
      - Nhóm quản trị bảo mật.
      - Nhóm quản trị cấu hình.
    - Nâng cấp hay mở rộng
- Đánh giá chi phí cụ thể cho từng loại tài nguyên được chia sẽ đối với chính sách sử dụng tài nguyên cụ thể.

Công cụ hỗ trợ cho quản trị tài nguyên

- Công cụ hỗ trợ cho quản trị tài nguyên thường được hỗ trợ thêm chức năng kiểm soát bảo mật như xác thực, cấp quyền và theo dõi (AAA).
- Một số công cụ được sử dụng phổ biến như: RADIUS, Diameter.
- Ví dụ: RADIUS có cấu trúc file quản lý các thông tin cơ sở như:
  - Danh sách người dùng cuối
  - Danh sách các thuộc tính mô tả người dùng cuối:
    - Rights
    - Permission
    - User profile
  - Nhật ký về chi tiết truy cập và sử dụng của từng tài khoản
  - Nhật ký lỗi…

IF Mibs

IP Mibs

- ipForwarding (1)
- ipDefaultTTL (2)
- ipInReceives (3)
- ipInHdrErrs (4)
- ipInAddrErrors (5)
- ipForwDatagrams (6)
- ipInUnknownProtos (7)
- ipInDiscards (8)
- ipInDelivers (9)
- ipOutRequests (10)
- ipOutDiscards (11)
- ipOutNoRoutes (12)
- ipReasmTimeout (13)
- ipReasmReqds (14)
- ipReasmOKs (15)
- ipReasmFails (16)
- ipFragOKs (17)
- ipFragFails (18)
- ipFragCreates (19)
- ipAddrTable (20)
  - ipAddrEntry (1)
    - ipAdEntAddr (1)
    - ipAdEntIfIndex (2)
    - ipAdEntNetMask (3)
    - ipAdEntBcastAddr (4)
    - ipAdEntReasmMaxSize* (5)

TCP Mibs

- tcpRtoAlgorithm (1)
- tcpRtoMin (2)
- tcpRtoMax (3)
- tcpMaxConn (4)
- tcpActiveOpens (5)
- tcpPassiveOpens (6)
- tcpAttemptFails (7)
- tcpEstabResets (8)
- tcpCurrEstab (9)
- tcpInSegs (10)
- tcpOutSegs (11)
- tcpRetransSegs (12)
- tcpConnTable (13)
  - tcpConnEntry (1)
    - tcpConnState (1)
    - tcpConnLocalAddress (2)
    - tcpConnLocalPort (3)
    - tcpConnRemAddress (4)
    - tcpConnRemPort (5)
- tcpInErrs* (14)
- tcpOutRsts* (15)

UDP Mibs

udpInDatagrams (1)
udpNoPorts (2)
udpInErrors (3)
udpOutDatagrams (4)
udpTable* (5)
  udpEntry* (1)
    udpLocalAddress* (1)
    udpLocalPort * (2)

EGP Mibs

egpInMsgs (1)
egpInErrors (2)
egpOutMessages (3)
egpOutErrors (4)
egpNeighTable (5)
  egpNeighEntry (1)
    egpNeighState (1)
    egpNeighAddr (2)
    egpNeighAs* (3)
    egpNeighInMsgs* (4)
    egpNeighInErrs* (5)
    egpNeighOutMsgs* (6)
    egpNeighOutErrs* (7)
    egpNeighInErrMsgs* (8)
    egpNeighOutErrMsgs* (9)
    egpNeighStateUps* (10)
    egpNeighStateDowns* (11)
    egpNeighIntervalHello* (12)
    egpNeighIntervalPoll* (13)
    egpNeighMode* (14)
    egpNeighEventTrigger* (15)
egpAs* (6)

Dot3StatsEntry

- **Dot3StatsEntry** ::= SEQUENCE { dot3StatsIndex InterfaceIndex,
  dot3StatsAlignmentErrors Counter32,
  - dot3Stats**FCSErrors** Counter32,
  - dot3Stats**SingleCollisionFrames** Counter32,
  - dot3Stats**MultipleCollisionFrames** Counter32,
  - dot3Stats**SQETestErrors** Counter32,
  - dot3Stats**DeferredTransmissions** Counter32,
  - dot3Stats**LateCollisions** Counter32,
  - dot3Stats**ExcessiveCollisions** Counter32,
  - dot3Stats**InternalMacTransmitErrors** Counter32,
  - dot3Stats**CarrierSenseErrors** Counter32,
  - dot3Stats**FrameTooLongs** Counter32,
  - dot3Stats**InternalMacReceiveErrors** Counter32,
  - dot3Stats**EtherChipSet** OBJECT IDENTIFIER,
  - dot3Stats**SymbolErrors** Counter32 }

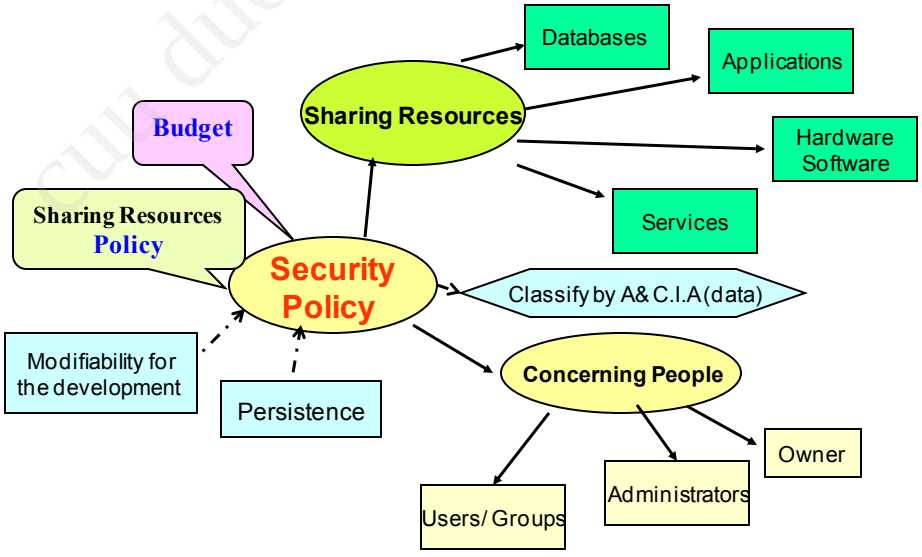
ICMP Mibs

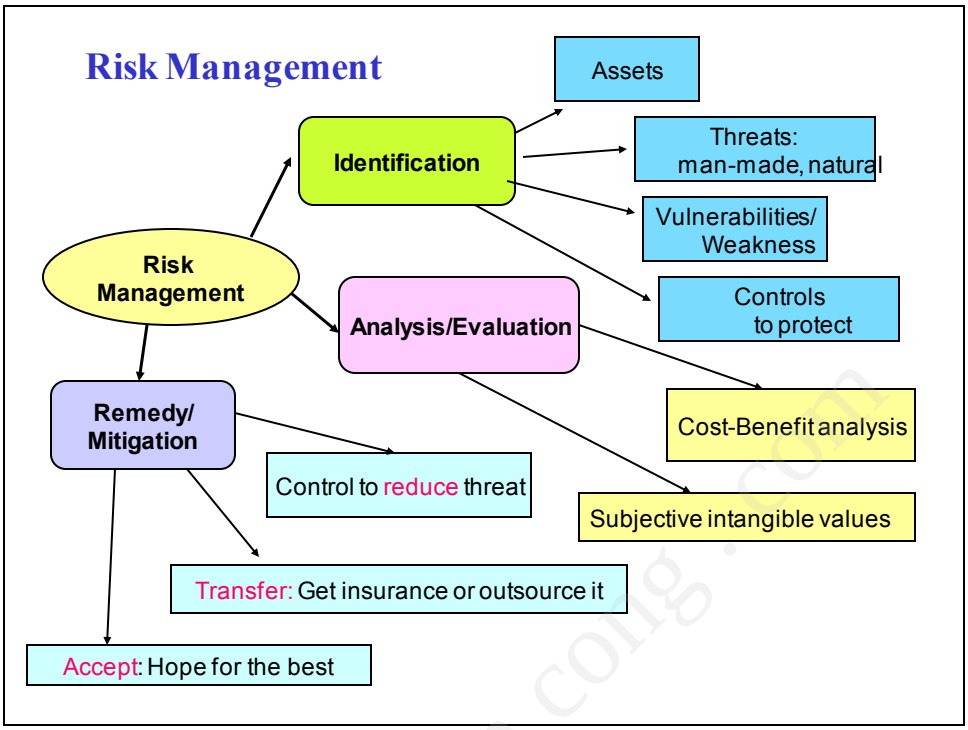
icmpInMsgs (1)
icmpInErrors (2)
icmpInDestUnreachs (3)
icmpInTimeExcds (4)
icmpInParmProbs (5)
icmpInSrcQuenchs (6)
icmpInRedirects (7)
icmpInEchos (8)
IcmpInEchoReps (9)
icmpInTimeStamps (10)
icmpInTimestampReps (11)
icmpInAddrMasks (12)
icmpInAddrMaskReps (13)
icmpOutMsgs (14)
icmpOutErrors (15)
icmpOutDestUnreachs (16)
icmpOutTimeExcds (17)
icmpOutParmProbs (18)
icmpOutSrcQuenchs (19)
icmpOutRedirects (20)
icmpOutEchos (21)
icmpOutEchoReps (22)
icmpOutTimeStamps (23)
icmpOutTimestampReps (24)
icmpOutAddrMasks (25)
icmpOutAddrMaskReps (26)

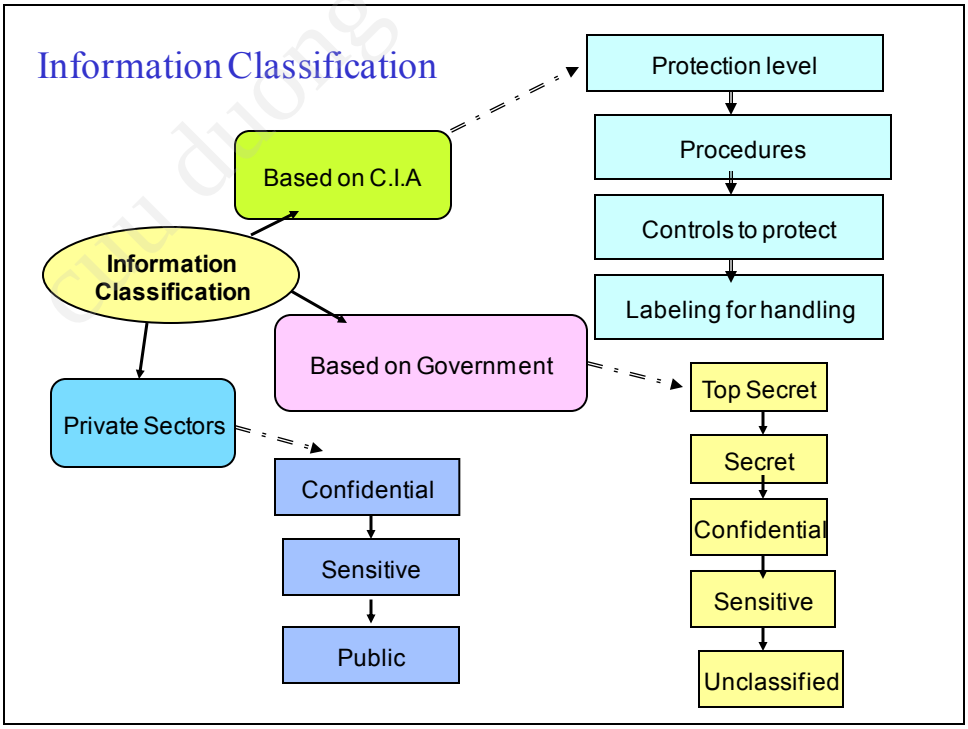
2.2.4 Quản trị bảo mật-Security Management (1/2)

- Chính sách bảo mật.
  - Thiết lập các nguyên tắc, điều khoản, mức chế tài, xử phạt áp dụng cho các đối tượng liên quan đến việc triển khai, quản lý, sử dụng và phát triển tài nguyên được chia sẽ trên mạng.
  - Chính sách bảo mật được xây dựng phù hợp với yêu cầu và chính sách chung của tổ chức.
- Quản trị bảo mật:
  - Kiểm toán việc tuân thủ chính sách bảo mật của các đối tượng liên quan.
  - Đánh giá được tính hiệu quả của các giải pháp bảo mật được triển khai.

Quản trị bảo mật-Security Management




Risk Management
Assets
Identification
Threats: man-made, natural
Vulnerabilities/ Weakness
Risk Management
Analysis/Evaluation
Controls to protect
Remedy/ Mitigation
Cost-Benefit analysis
Control to reduce threat
Subjective intangible values
Transfer: Get insurance or outsource it
Accept: Hope for the best


Information Classification
Protection level
Procedures
Based on C.I.A
Controls to protect
Information Classification
Labeling for handling
Based on Government
Top Secret
Private Sectors
Secret
Confidential
Confidential
Sensitive
Sensitive
Public
Unclassified

Chính sách bảo mật- Đối với chủ đầu tư

❖ Đối với chủ đầu tư: xác định rõ tài sản hữu hình và vô hình của tổ chức. Từ đó đưa ra các qui định cho các đối tượng liên quan.

❖ Xây dựng chính sách bảo mật:

1. Nhận diện các nguồn tài nguyên, thiết bị cần bảo mật (Assets)
2. Phân tích rủi ro bảo mật (Risks)
3. Phân tích các yêu cầu bảo mật và các thách thức phải đối diện (Requirements & tradeoffs)
4. Phát triển một kế hoạch bảo mật (Security plan)
5. Định nghĩa các nguyên tắc, yêu cầu tuân thủ , yêu cầu thực hiện trong chính sách (Define a security policy)
6. Phát triển thủ tục, qui trình áp dụng chính sách bảo mật (Procedures)

Đánh giá các tài nguyên trên hệ thống

- Hardware
- Software
- Ứng dụng nghiệp vụ (Applications)
- Dữ liệu (Data)
- Sở hữu trí tuệ (Intellectual property)
- Bí mật thương mại (Trade secret)
- Danh tiếng của công ty (Company's reputation)

Chính sách bảo mật- Đội ngũ quản trị mạng và users

• Đội ngũ quản trị mạng/ IT staff: người tham gia phát triển và quản lý tài nguyên:

- Thiết kế và triển khai đúng đắn giải pháp bảo mật cho các tài nguyên dùng chung.
- Giám sát và đánh giá được tính hiệu quả của các giải pháp bảo mật được triển khai.
- Thực hiện kiểm tóan các hoạt động quản trị và khai thác tài nguyên -> nhanh chóng phát hiện các khiếm khuyết trong hoat động bảo mật mạng
- Xây dựng và triển khai chính sách bảo mật đối với USERs

•Đối với users: hiểu được quyền lợi và trách nhiệm trong việc sử dụng và bảo vệ tài nguyên dùng chung.

Các thách thức về bảo mật (Security Tradeoffs)

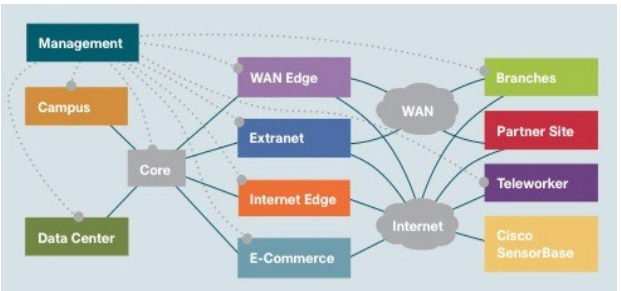
- Affordability
- Usability
- Performance
- Availability
- Manageability

Đối với bộ phận quản lý mạng

1. Triển khai được các giải pháp về kỹ thuật bảo mật phù hợp (Technical Solutions)
2. Kiểm sóat được sự tuân thủ chính sách bảo mật chung của tất cả các đối tượng liên quan (Achieve buy-in)
3. Huấn luyện thường kỳ (Training users, managers, and technical staff)
4. Triển khai các chiến lược và thủ tục bảo mật (Implement security strategy and procedures)
5. Giám sát, Kiểm thử và cập nhật, điều chỉnh nếu cần thiết
6. Kiểm tóan thường kỳ bởi bộ phận độc lập

Thiết kế bảo mật theo modules

- Internet connections
- Public servers and e-commerce servers
- Remote access networks and VPNs
- Network services and network management
- Server farms
- User services
- Wireless networks



Các giải pháp bảo mật cơ sở (1/3)

- Giữ cho hệ thống và mạng được an toàn đối với các truy cập trái phép.
  - Đảm bảo tính sẵn sàng của tài nguyên, hệ thống quản trị tài nguyên.
  - Triển khai các hệ thống bảo vệ vòng ngoài:
    - tường lửa: firewall (packet filter; proxy)
    - phát hiện thâm nhập IDS/ IPS

Ref-1 Ref-2 Back ...

Các giải pháp bảo mật cơ sở (2/3)

- Thực hiện được yêu cầu bảo đảm tính riêng tư, tính toàn vẹn dữ liệu trong truyền thông và lưu trữ dữ liệu.
  - Tính riêng tư (privacy) hay tính bí mật (confidentiality)
  - Tính toàn vẹn dữ liệu (integrity)
    - Triển khai các hệ thống xác thực, cấp quyền: AAA
      - Authentication
      - Authorization
      - Accounting

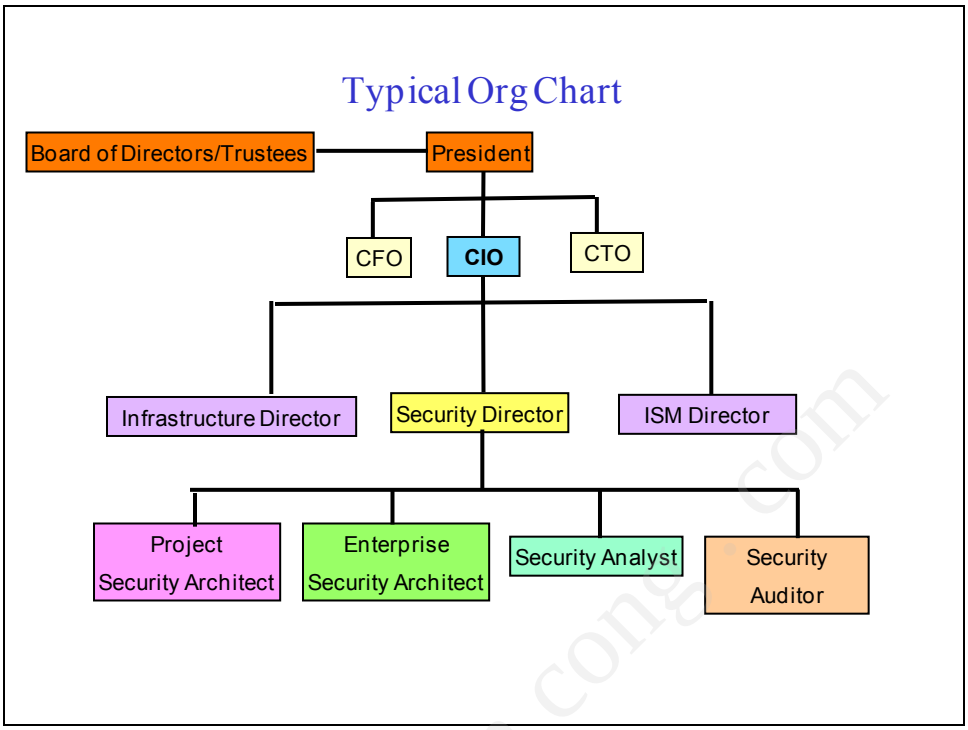
Ref-1 Ref-2 Back ...

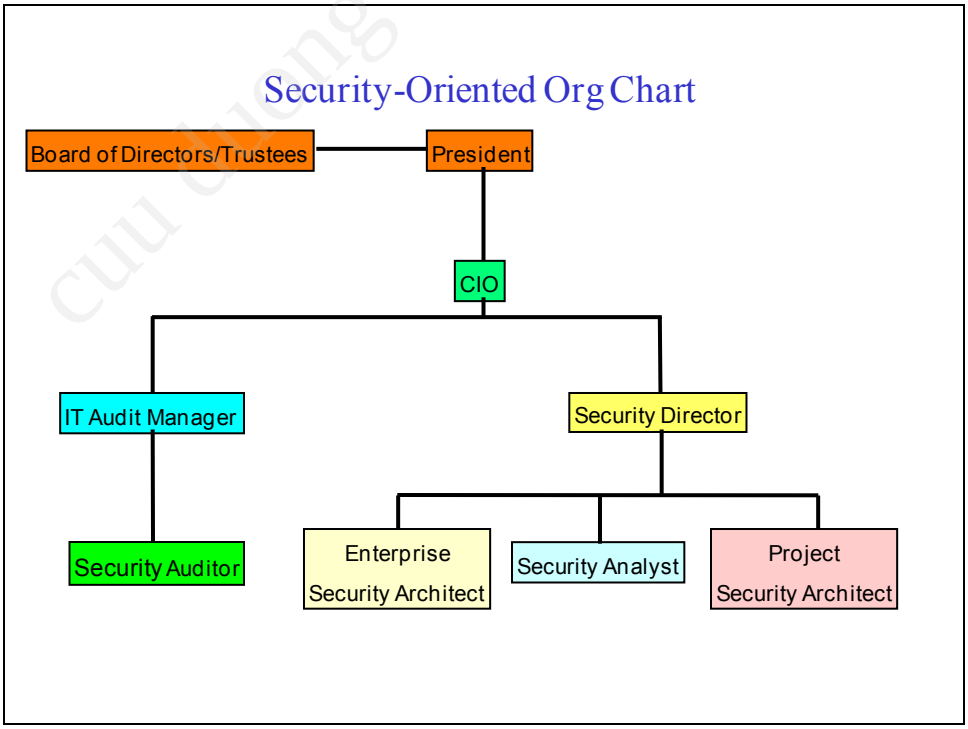
Các giải pháp bảo mật cơ sở (3/3)

- Cung cấp được phương tiện thực hiện trao đổi dữ liệu an toàn cho người dùng cuối:
  - Sử dụng mật khẩu (theo chính sách mật khẩu)
  - Sử dụng khóa đối xứng- symmetry key hay khóa bí mật (secret key)
  - Sử dụng khóa bất đối xứng: asymmetry key
    - Khóa công khai (public key):
    - Khóa riêng (private key)
- Đánh giá và phân loại độ nhạy cảm, tầm quan trọng dữ liệu truyền thông và lưu trử theo tiêu chí CIA
  - Confidentiality, Integrity , Availability

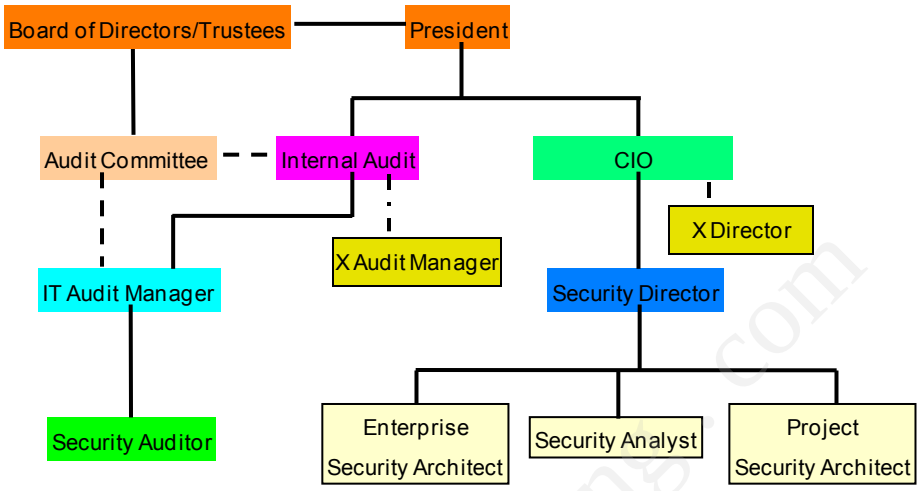
Bảo mật trong công tác quản trị mạng

- Phân cấp quyền quản trị cụ thể theo đối tượng quản trị.
  - Xác định mức độ cần xác thực và mã hóa khi truy cập vào cơ sở thông tin quản trị trên thiết bị được quản trị.
  - Chỉ định cụ thể nhóm đối tượng quản trị đối với người có quyền quản trị.
  - Quyền hạn đối với nhóm thông tin quản trị.
- Yêu cầu mã hóa thông tin quản trị trong truyền thông giữa hệ thống quản trị và hệ thống được quản trị.
- Sử dụng các đường truyền VPN cần thiết.





The best security-Oriented Org Chart



2.2.5 Quản trị cấu hình - Configuration management (1/2)

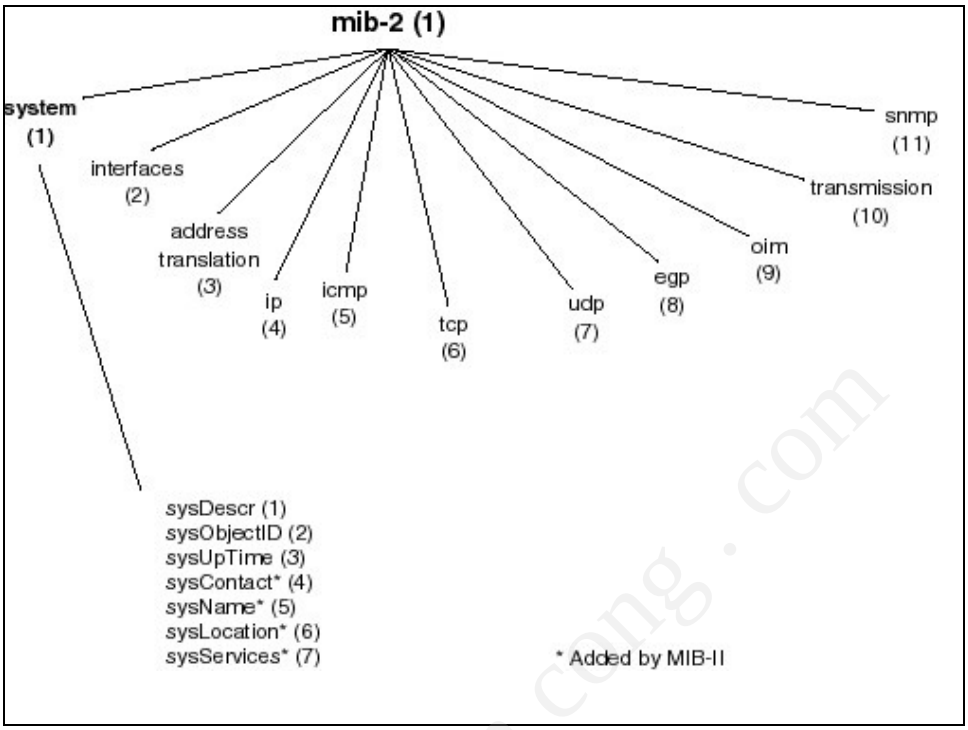
- Quản trị cấu hình.
  - Thiết lập và cập nhật được các hồ sơ kỹ thuật một cách có hệ thống nhằm mục đích:
    - Nhận diện các thành phần nối mạng, thành phần tài nguyên mạng và người dùng cuối.
    - Lưu trữ thông tin chi tiết:
      - Chính sách chia sẽ tài nguyên
      - Chính sách bảo mật
      - Hồ sơ thiết kế, triển khai và kiểm thử
      - Cấu hình phần cứng & phần mềm và thiết lập ban đầu của thiết bị.
      - Quá trình xử lý và thay đổi trên một thiết bị.

Quản trị cấu hình - Configuration management (2/2)

- Mục đích: Triển khai thành công các hoạt động quản lý sự thay đổi cấu hình một cách chặc chẻ và nhất quán.
  - Thiết lập được các giá trị cơ sở (baseline) của các đối tượng quản trị được kiểm thử cuối cùng trước khi đưa vào sử dụng.
  - Duy trì được sự toàn vẹn các số đo về năng lực hoạt động của hệ thống trong suốt chu kỳ sống của các hệ thống nối mạng.
  - Theo dõi và truy vấn được các thay đổi về cấu hình, các giá trị thiết lập hoạt động của hệ thống trên mạng LAN, WAN, cho phép quản trị rủi ro một cách hiệu quả.

Các loại thông tin cấu hình

- Thông tin cấu hình về:
  - Phần cứng và phần mềm của các thành phần thiết bị và hệ thống (systems)
  - Các đường kết nối vào thiết bị/ hệ thống
    - NIC->Media -BW
- Các thông tin nhận dạng thành phần mạng
  - ID/ Addresses/ Name...
- Các thông tin về baselines:
  - Các thông tin về yêu cầu thiết kế, kết quả thiết kế và triển khai, kiểm thử
  - Sơ đồ mạng (Topology; diagrams, cable structure, ...)
  - Các giá trị cài đặt ban đầu (setting up)
  - Các giá trị ở mức được chấp nhận của các thông số điều khiển hoạt động mạng



Các mối quan hệ giữa các chức năng quản trị

- Mối quan hệ giữa quản trị khả năng thực thi và quản trị lỗi
- Mối quan hệ giữa quản trị khả năng thực thi và quản trị cấu hình.
- Mối quan hệ giữa quản trị khả năng thực thi và quản trị bảo mật.
- Mối quan hệ giữa quản trị lỗi và quản trị cấu hình.
- Mối quan hệ giữa quản trị lỗi và quản trị bảo mật.
- Mối quan hệ giữa quản trị tài nguyên mạng và quản trị cấu hình.
- Mối quan hệ giữa quản trị tài nguyên mạng và quản trị bảo mật.