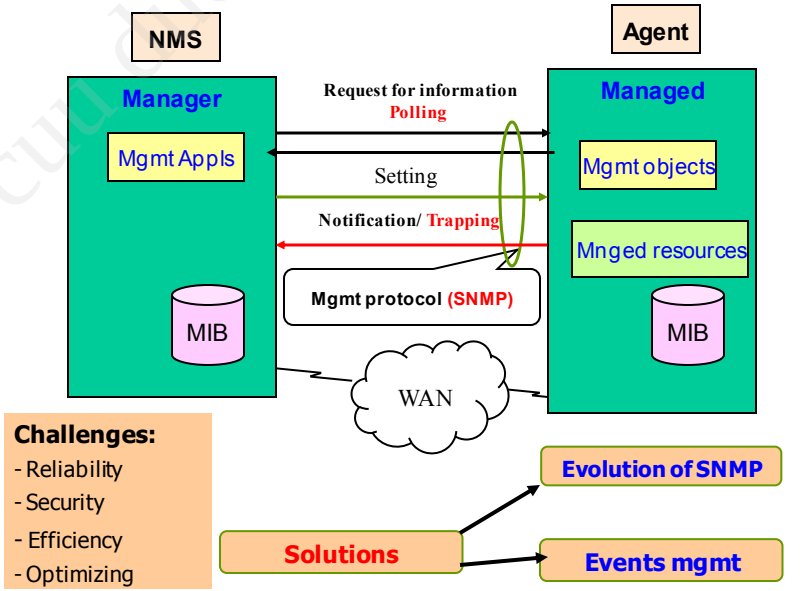
Chương 4. Mô hình truyền thông SNMP-IETF

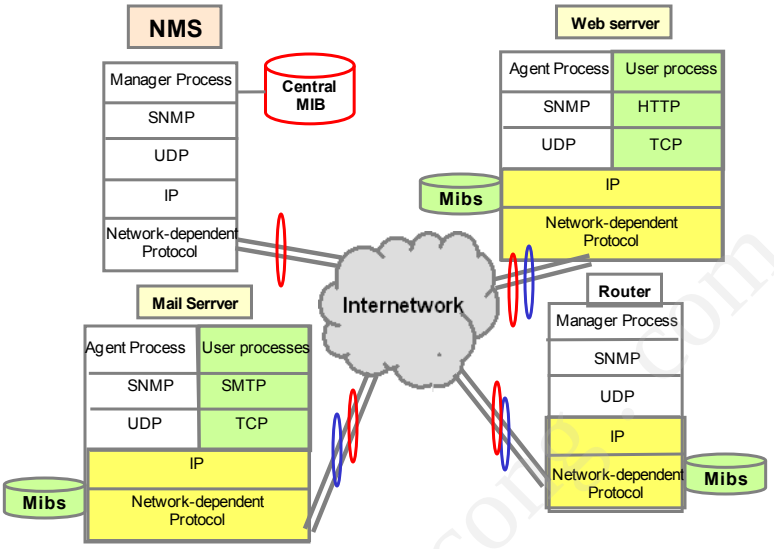
1. Mô hình truyền thông SNMP-IETF
2. Giới thiệu giao thức SNMP
3. Hoạt động của giao thức SNMPv1
4. Hoạt động của giao thức SNMPv2
5. Hoạt động của giao thức SNMPv3
6. Mối quan hệ điều khiển truyền thông
7. Quản trị sự kiện

Communication Model

Collection of management Information

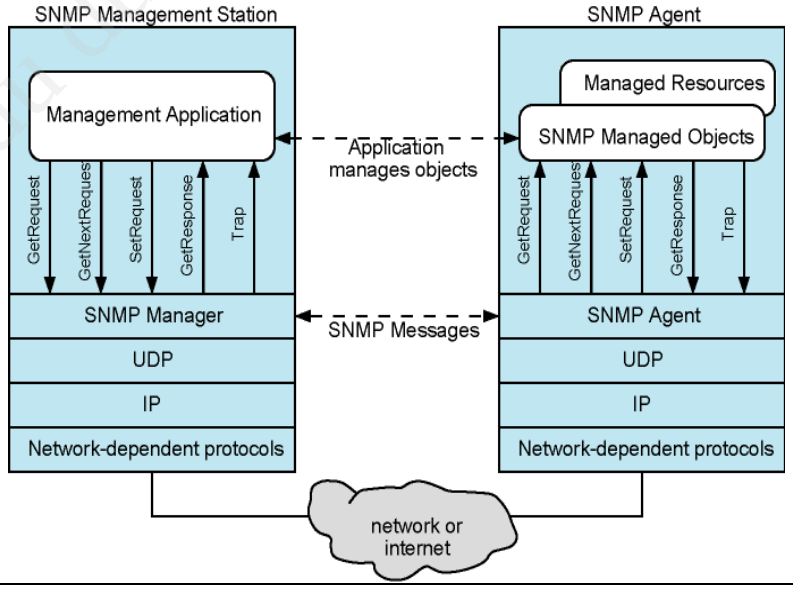


Mô hình tổ chức của SNMP/ IETF



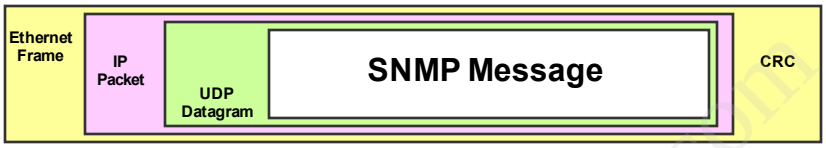
4.1 Mô hình truyền thông của SNMP/ IETF (1/2)

Ports & UDP



4.3 Mô hình truyền thông của SNMP/ IETF (1/2)
Ports & UDP

•SNMP uses User Datagram Protocol (UDP) as the transport mechanism for SNMP messages

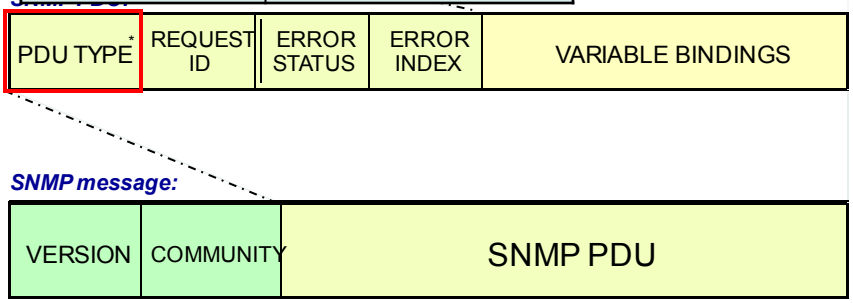


•Like FTP, SNMP uses two well-known ports to operate:

- •**UDP Port 161** – SNMP Get/ Getnext/GetBulk Messages
- •**UDP Port 162** - SNMP Trap Messages

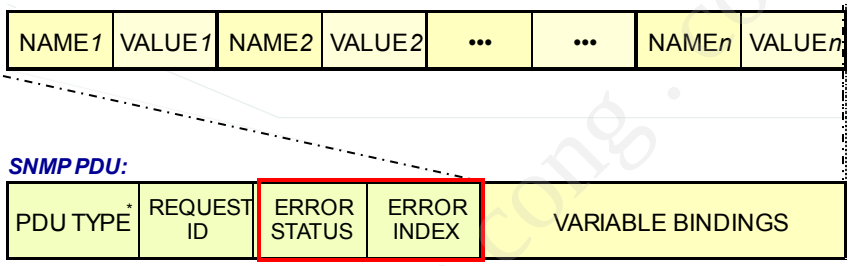
Định dạng thông điệp điều khiển SNMP

PDU	PDU Type Field Value
GetRequest	0
GetNextRequest	1
GetResponse	2
SetRequest	3
Trap	4

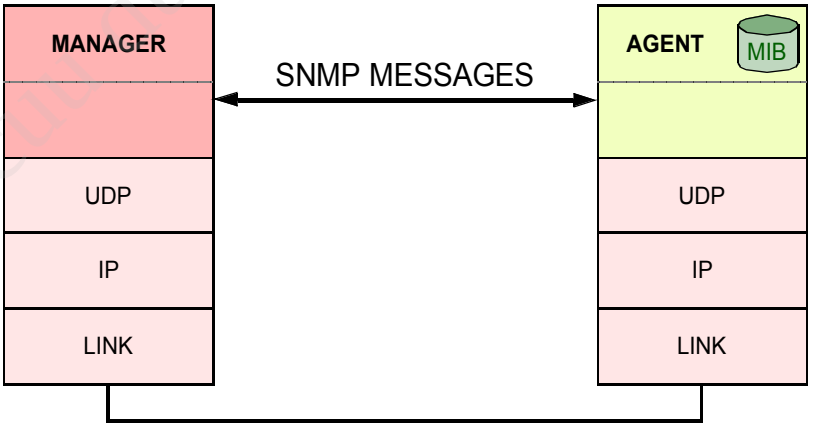


Định dạng thông điệp điều khiển SNMP

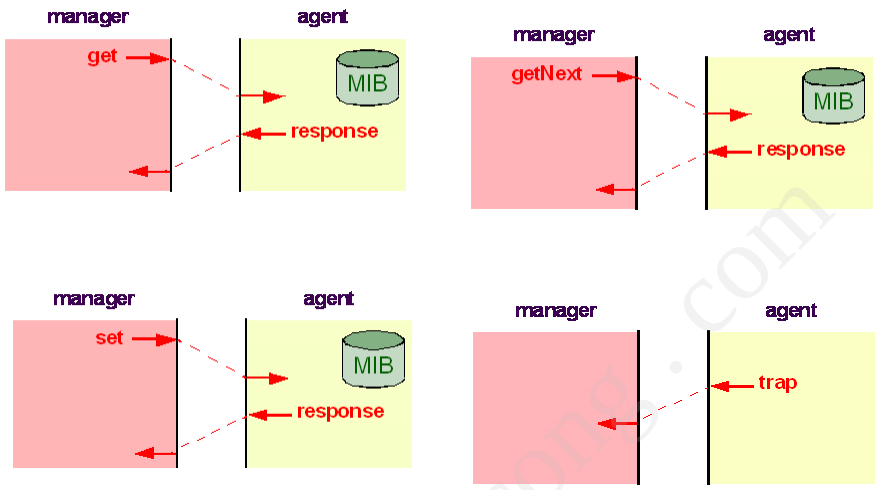
Status	*Name*	*Meaning*
0	noError	No error
1	tooBig	Response too big to fit in one message
2	noSuchName	Variable does not exist
3	badValue	The value to be stored is invalid
4	readOnly	The value cannot be modified
5	genErr	Other errors



4.2 Hoạt động của giao thức SNMPv1



Minh họa thông điệp điều khiển của SNMPv1



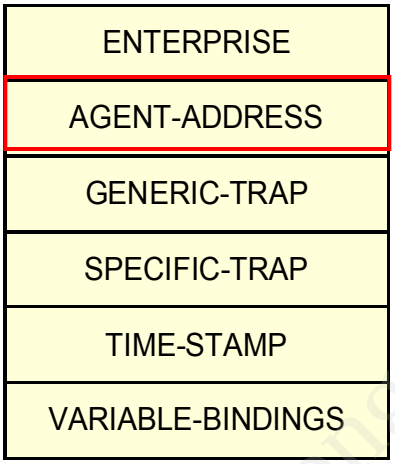
SET và yêu cầu trong cấu trúc MIB liên quan

- **ACCESS:**
  - READ-ONLY
    - Get, Trap, Set, Response
  - READ-WRITE.
    - Set

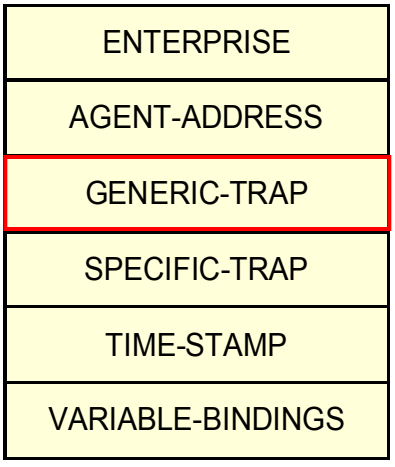
SysUpTime OBJECT-TYPE
SYNTAX Time-Ticks
ACCESS read-only
STATUS mandatory
DESCRIPTION
"Time since the network management portion of the system was last re-initialised.
::= {system 3}

ipDefaultTTL OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-write
STATUS mandatory
DESCRIPTION : "The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol."
::= { ip 2 }

TRAP - PDU FORMAT



TRAP - PDU FORMAT



Generic Trap

Trap	Value	Meaning
ColdStart	0	Reinitialized => **Agent's configuration** or entity implementation **may be altered.**
WarmStart	1	Reinitialized => but **neither** the **agent's configuration nor** the protocol entity implementation has been altered.
LinkDown	2	A communication link has failed--> name and value of the ***ifIndex* instance.**
LinkUp	3	A communication link has come up→ name and value of the *ifIndex* instance.
Authentication Failure	4	The **community name** was **incorrect**.
EgpNeighborLoss	5	An **EGP peer neighbor** is **down.**
EnterpriseSpecific	6	It's up to the Specific **Trap Type** field and Enterprise field.

Cơ chế bảo mật trong SNMP (1/2)

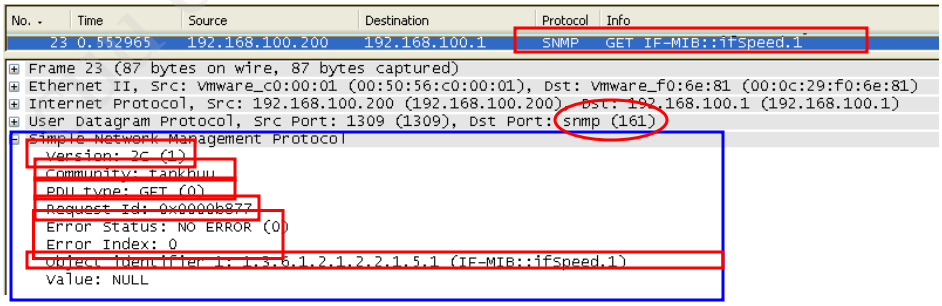
- SNMP sử dụng **Community Strings** như là passwords.
  - Được sử dụng để định nghĩa nơi mà một thông điệp SNMP được hướng đến.
- Cần thiết lập "community name" trên các tập tham biến của các đối tượng quản trị cụ thể đối với **từng nhóm quản trị** trong phân cấp quản trị.
- Thiết lập các các ứng dụng quản trị trong công tác giám sát và nhận cảnh báo (alert/ trapping)

Cơ chế bảo mật trong SNMP (2/2)

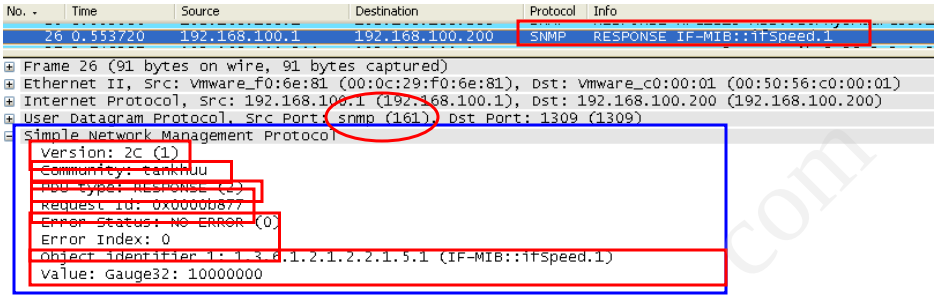
Có 3 loại chuỗi community chỉ định 3 mức quyền hạn khác nhau đối với việc truy xuất thông tin quản trị:

- READ-ONLY: được thực hiện bởi lệnh Get hay GetNext
- READ-WRITE: được thực hiện bởi lệnh Get, GetNext, và Set.
  - Nếu đối tượng quản trị có thuộc tính ACCESS mang gía trị là "read-write" thì lệnh Set mới được thực hiện
- TRAP: cho phép người quản trị nhóm các thành phần được quản trị vào trong một cộng đồng quản trị cụ thể.

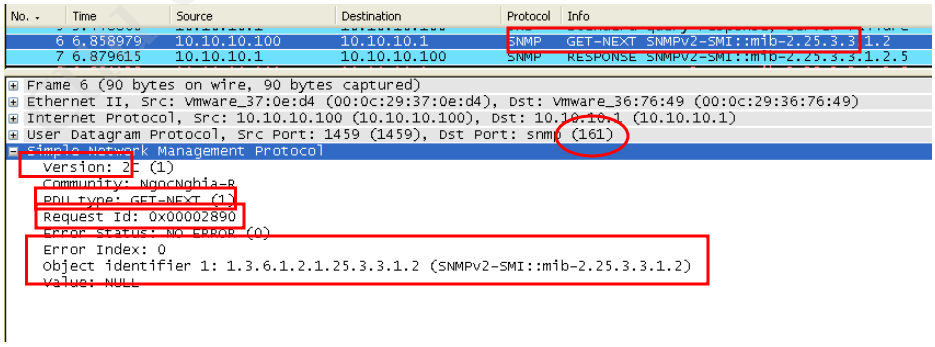
Polling-> Get Request SNMP



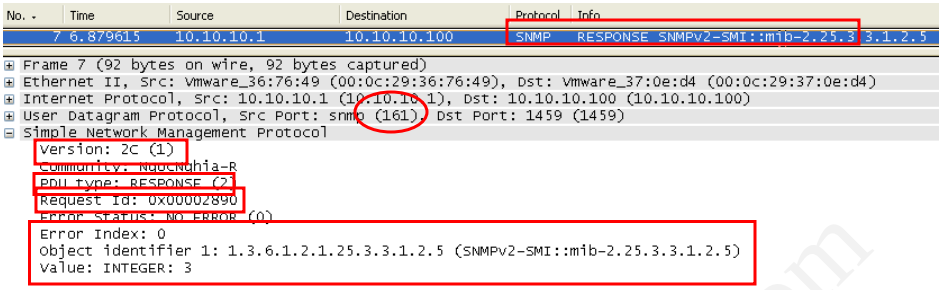
Polling-> Get Response SNMP



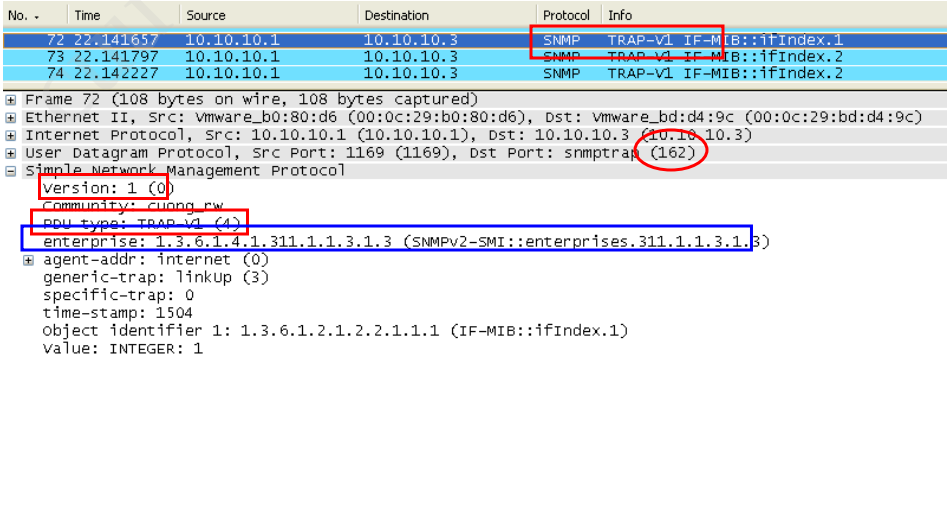
Polling-> GetNext Request SNMP



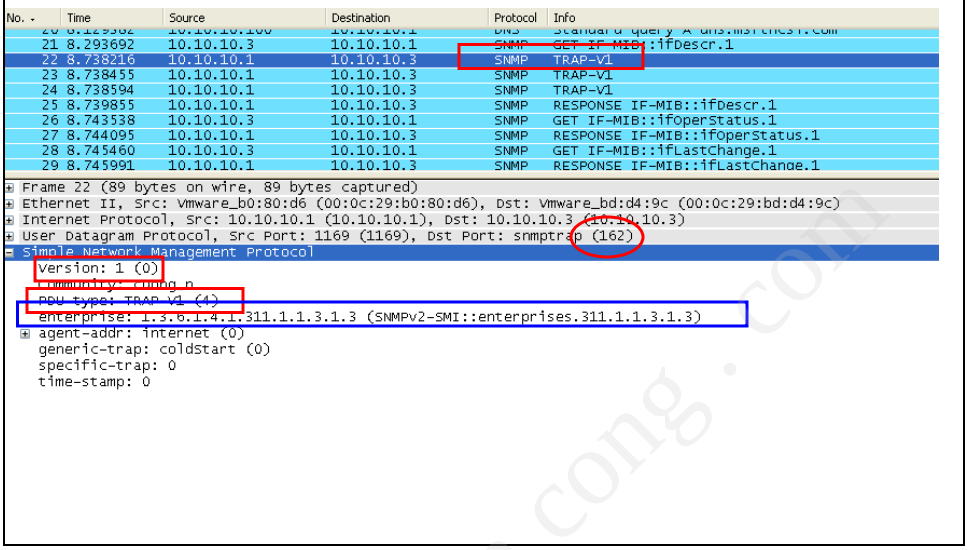
Polling-> GetNext Response SNMP



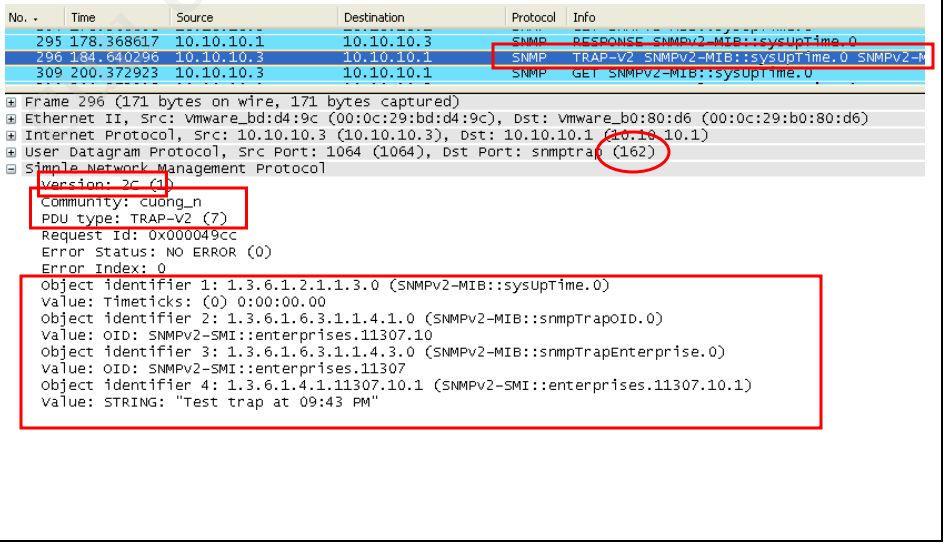
Trapping -> Trap SNMPv1



Trapping -> Trap SNMPv1



Trapping -> Trap SNMPv2



Các giới hạn của SNMPv1

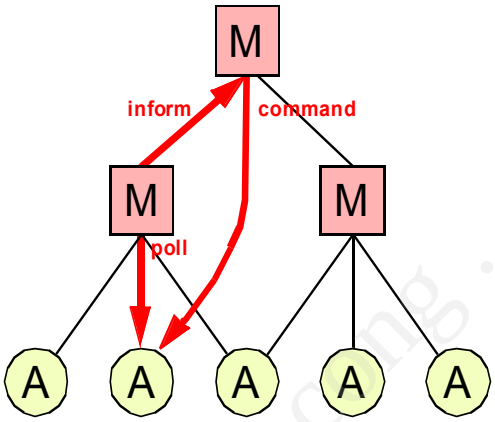
- Không định nghĩa rõ các luật
- Còn hạn chế về:
  - Các mã lỗi.
  - Kiểu dữ liệu.
  - Các thông báo sự kiện.
  - Khả năng thu thập lượng lớn thông tin quản trị.
- Sự lệ thuộc vào độ tin cậy của môi trường truyền, đặc biệt đối với TRAP.
- Chưa hỗ trợ kiến trúc phân tán.
- Hạn chế về bảo mật trong truyền thông SNMP

4.3 Phiên bản SNMPv2

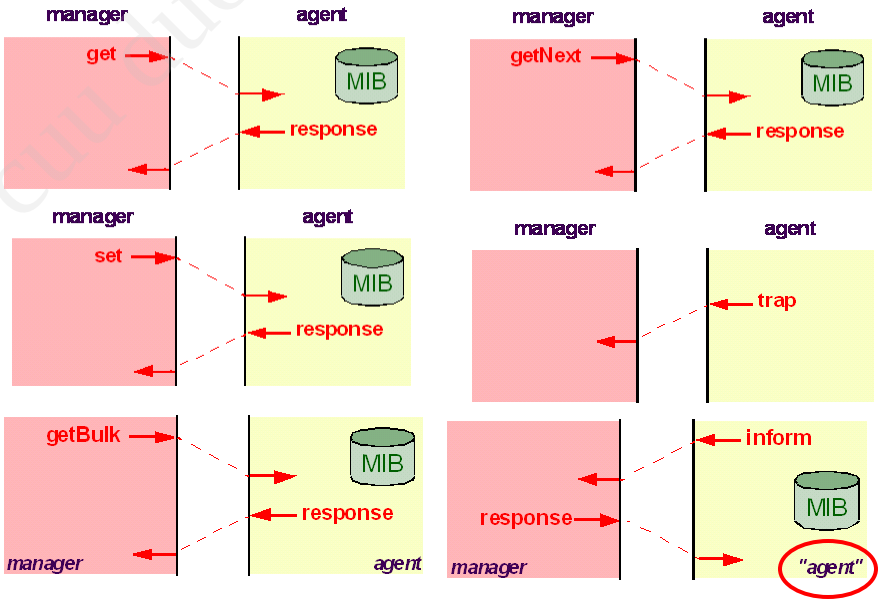
- **Đặc điểm:**
  - Triển khai mô hình hoạt động quản trị phân cấp M2M
  - Cải thiện mô hình bảo mật.
  - Cải thiện hoạt động thu thập lượng lớn thông tin (Getbulk)
  - Cải thiện độ tin cậy trong hoạt động cảnh báo TRAPPING bởi Inform và Report.
  - Cải thiện khả năng chỉ báo lỗi trong hoạt động của SNMP.

Mô hình quản trị phân cấp trong SNMPv2

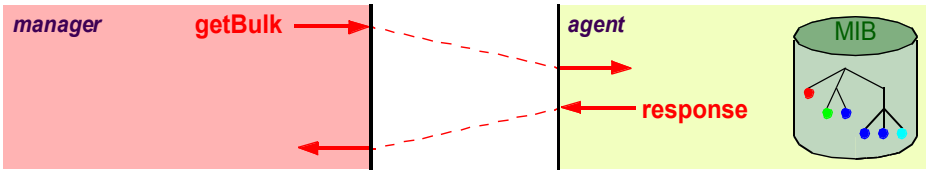
- Mô hình quản trị MANAGER TO MANAGER (M2M)



Hoạt động cơ bản của SNMPv2



GET-BULK



- Chức năng mới trong SNMPv2
  - Dùng để thu thập **lượng lớn** thông tin quản trị.
  - Cải thiện khả năng hoạt động của SNMP

GET-BULK

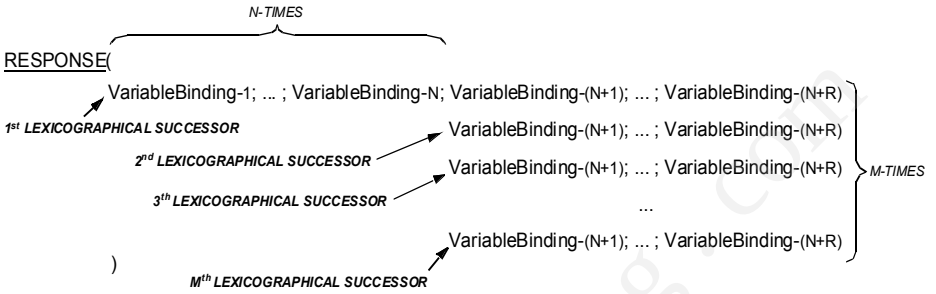
- GetBulk REQUEST có 2 thông số được thêm vào:
  - N: non-repeators: không lặp lại
  - M: max-repetitions: lặp lại với số lần tối đa

• Thông số non-repeators chỉ ra N phần tử của các tham biến quản trị trong danh sách cần được xử lý như hoạt động thông thường của getnext

• Thông số max-repeators chỉ ra số M các phần tử kế tiếp của danh sách các tham biến được xử lý như là các hoạt động getnext được lặp lại cần thiết.

Minh họa của cú pháp GET-BULK

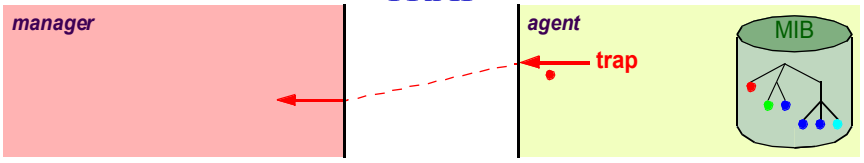
REQUEST(non-repeaters = N; max-repetitions = M;
VariableBinding-1; ... ; VariableBinding-N; VariableBinding-(N+1); ... ; VariableBinding-(N+R)
)



Các mã lỗi được định nghĩa mới

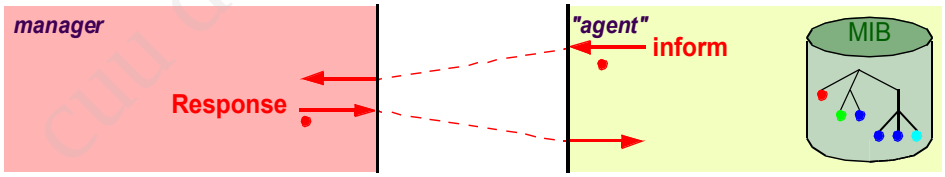
	SNMPv1	SNMPv2
PHASE 1:	badValue	wrongValue
	badValue	wrongEncoding
	badValue	wrongType
	badValue	wrongLength
	badValue	inconsistentValue
	noSuchName	noAccess
	noSuchName	notWritable
	noSuchName	noCreation
	noSuchName	inconsistentName
	genErr	resourceUnavailable
	genErr	genErr
PHASE 2:	genErr	CommitFailed
	genErr	undoFailed

TRAP



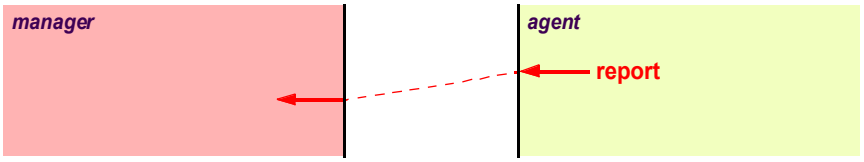
- **Đối với SNMPv1:**
  - COLD START
  - WARM START
  - LINK DOWN
  - LINK UP
  - AUTHETICATION FAILURE
  - EGP NEIGHBOR LOSS
- **Đối với SNMPv2:**
  - MIBs có thể được bao gồm các Macro về thông báo NOTIFICATION
  - Có 2 tham biến: sysUptime và snmpTrapOID
  - Sử dụng cùng định dạng với các PDU khác.

INFORM



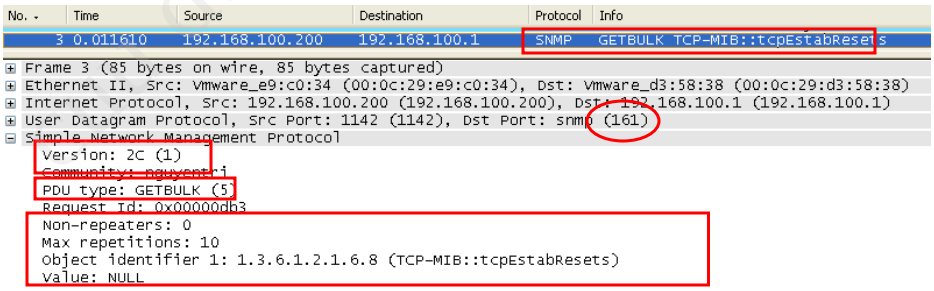
- Dùng để xác nhận đã nhận được cảnh báo TRAP
  - Đây là giải pháp để khắc phục sự hạn chế về độ tin cậy của môi trường truyền thông.
  - Định dạng dữ liệu tương tự định dạng của TRAP
- Mã lỗi : tooBig

REPORT

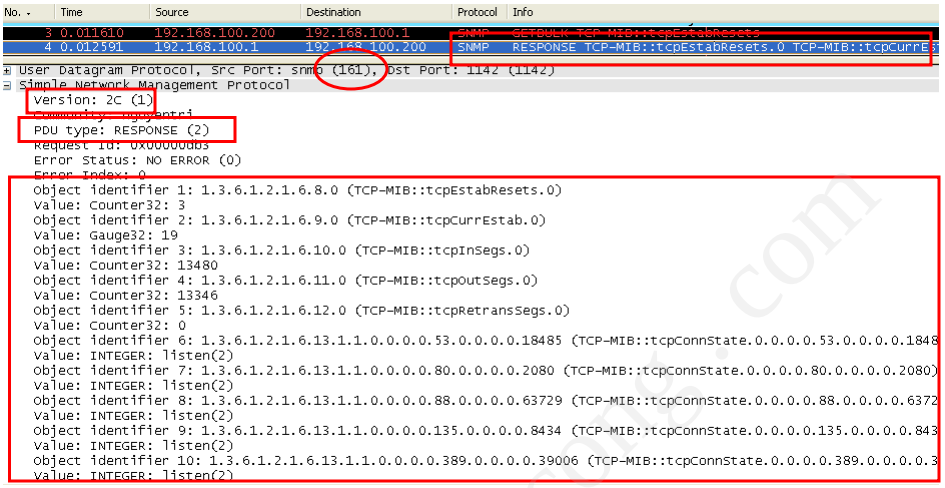


- Chức năng mới của SNMPv2 sử dụng cho M2M
- Dùng để báo cáo chi tiết các trường hợp ngoại lệ xảy ra.

Polling-> GetBulk Request SNMP



Polling-> GetBulk Response SNMP



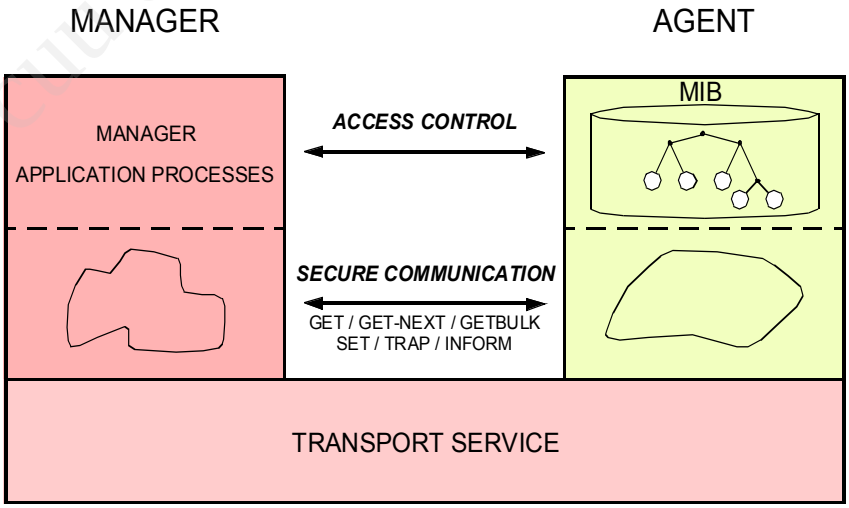
Các chuẩn RFCs liên quan SNMPv2

- Mô hình truyền thông:
  - DRAFT STANDARD
  - RFC 1905, RFC1906
- Mô hình bảo mật - SNMPv2**C**:
  - **COMMUNITY BASED** SNMP
  - SAME 'SECURITY MECHANISMS' AS SNMPv1
  - EXPERIMENTAL STATUS
  - RFC 1901
- Mô hình bảo mật - SNMPv2**U**:
  - **USER BASED** SECURITY (AUTHENTICATION / ENCRYPTION / ACCESS CONTROL)
  - EXPERIMENTAL STATUS
  - RFC 1909, RFC1910
- Mô hình thông tin:
  - STANDARD, RFC2578, RFC2579, RFC2580

4.4 Phiên bản SNMPv3

- Giới thiệu.
- Những quyết định thiết kế SNMPv3
- Kiến trúc SNMPv3
- Cấu trúc thông điệp SNMPv3
- Bảo mật trong truyền thông SNMPv3
  - Mô hình bảo mật dựa trên người dùng- **USM**/ USER SECURITY MODEL
- Điều khiển truy cập
  - Mô hình điều khiển truy cập dựa vào MIB View
    - VIEW BASED **ACCESS CONTROL** MODEL (VACM)
- Các chuẩn RFCs liên quan

Bảo mật truyền thông vs điều khiển truy cập



Mức bảo mật sử dụng

- **snmpSecurityLevel**
  - no authentication or privacy (noAuthNoPriv).
    - Vẫn sử dụng "securityName"
  - Authentication and no privacy (authNoPriv).
  - Authentication and privacy (authPriv).

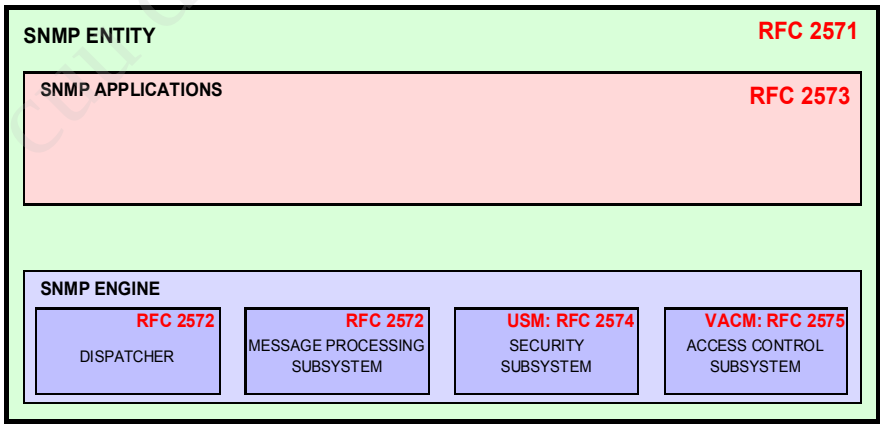
ACCESS CONTROL TABLES

MIB VIEW	ALLOWED OPERATIONS	ALLOWED MANAGERS	REQUIRED LEVEL OF SECURITY
Interface Table	SET	John	Authentication Encryption
Interface Table	GET / GETNEXT	John, Paul	Authentication
Systems Group	GET / GETNEXT	George	None
•••	•••	•••	•••
•••	•••	•••	•••
•••	•••	•••	•••
•••	•••	•••	•••

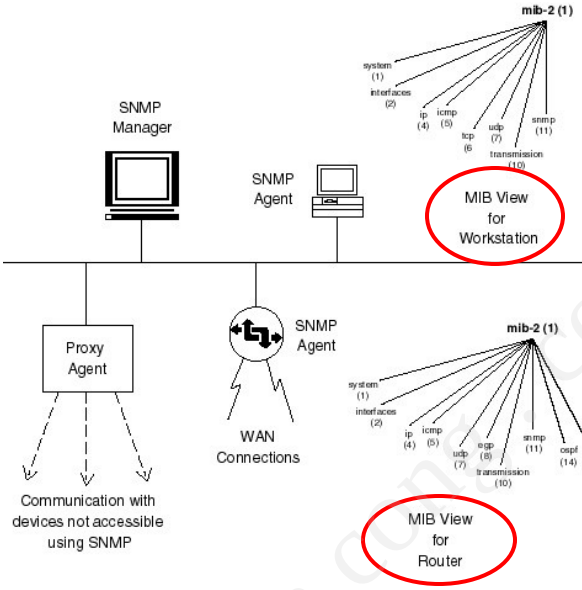
Các bước cấu hình bảo mật cho SNMPv3

- **Username** :Mô tả dạng text về người chịu trách nhiệm cho thực thể SNMP cần được quản trị (security name)
- **Security level:** noAuthNoPriv, authNoPriv, và authPriv.
  - Chú ý: không thể có privacy mà không "authentication", nhưng vẫn có thể " authentication" mà không cần "privacy"
- **Authentication protocol**: MD5 và SHA1
  - **Authentication passphrase**: *passphrase* sử dụng tương ứng với giao thức xác thực liên quan.
- **Privacy protocol: được sử dụng để mã hóa dữ liệu của gói SNMP** (DES)
  - **Privacy passphrase:** được sử dụng với thuật tóan mã hóa liên quan

Các RFCs liên quan SNMPv3



4.5 Quản lý các mối quan hệ của các thành phần kiến trúc quản trị (1/5)



Các mối quan hệ trong kiến trúc quản trị (2/5)

- Giao thức quản trị cho phép hệ thống quản trị NMS và các thành phần được quản trị tương tác với nhau.
  - Sử dụng SNMP hay CMIP
- MIB View là tập các đối tượng quản trị đặc trưng cho thiết bị được quản trị.
- Cặp giá trị giống như mật khẩu gọi là "The SNMP community " được lưu trử tại SNM và hệ thống được quản trị phục vụ cho xác thực quyền quản trị của một đối với mib-view nào đó.
- Phương thức xác thực- Authentication protocol: được chỉ ra trong giao thức SNMP (sử dụng trong phiên bản v.3)

Các mối quan hệ trong kiến trúc quản trị (3/5)

- Application management entity: thực thể ứng dụng quản trị quản trị thực hiện các chức năng truyền thông của SNMP.
- SNMP access mode chỉ định kiểu thao tác đối với tham biến quản trị được lưu trử tại thành phần được quản trị, do thực thể ứng dụng quản trị quản lý.
  - read-only hay read-write.
- Kết hợp SNMP community string và SNMP access mode cho phép xác thực người có quyền hạn truy cập vào tham biến quản trị được lưu trử tại thành phần được quản trị.
  - Authentication & Authorization

Các mối quan hệ trong kiến trúc quản trị (4/5)

- Kết hợp Mib-view, SNMP community string và SNMP access mode cho phép thực hiện phân cấp quản trị cụ thể theo chức năng quản trị.
  - Community profile là giá trị tạo bởi SNMP access mode và SNMP MIB View cho phép xác định đặc quyền truy xuất vào tập tham biến quản trị trong một MIB view.
  - SNMP access policy : chính sách truy cập là cặp giá trị giữa SNMP community với SNMP community profile.

Các mối quan hệ trong kiến trúc quản trị (5/5)

- SNMP proxy agent cung cấp các chức năng quản trị đại diện cho các thực thể mạng không thể truy cập trực tiếp vào được do không sử dụng cùng giao thức quản trị hay mô hình tổ chức.

4.6. Quản lý sự kiện

- Công tác quản lý sự kiện
- Các kiểu thu thập thông tin quản trị
  - Chức năng báo cáo cảnh báo (trapping/ alert; events report)
  - Chức năng báo cáo thường kỳ (polling)
  - Chức năng báo cáo nhật ký (logfile/ syslog)

Công tác quản lý sự kiện

- Xây dựng và phát triển chiến lược quản trị sự kiện
- Tối ưu công tác quản trị sự kiện
- Tận dụng tất cả các loại công cụ quản trị có sẵn
  - Tích hợp các công cụ để đạt được sự thuận tiện trong chiến lượt quản trị sự kiện
- Nhận biết sự cố xảy ra
- Triển khai Các chuẩn cảnh báo và xác nhân được
  - Syslog
  - Polling
  - Trapping/ alert

Các yêu cầu đối với thu thập thong tin

- Thỏa mản về chất lượng thông tin quản trị thu thập được.
  - Có thể phân tích.
    - Đủ thông tin để phản ảnh được thực trạng hoạt động mạng.
    - Tính đồng nhất của thông tin nhận được.
    - Độ tin cậy của thông tin nhận được.
  - Các dạng thức chỉ báo/ kết xuất ra màn hình hay file
    - Dạng biểu đồ
    - Dạng văn bản
    - Dạng cơ sở dữ liệu
- Hiệu suất tài nguyên mạng.
  - Bandwidth , CPU, Memory

Loại thông tin cần thu thập

- Chi tiết của lưu lượng thông tin được thống kê trên một link hay trên một interface.
  - Addresses (Src-Addr, Dst-Addr)
  - Application (port numbers)
  - QoS (DSCP)
  - Time stamps (ICMPs)
  - Routing and peering
- Thông tin điều khiển (header) hay chi tiết nội dung dữ liệu người dùng (payload)
- Thông tin thô (thông tin lớp 2), thông tin lớp cao (lớp 3, lớp 4...)

Xây dựng và phát triển chiến lược quản trị sự kiện (1/2)

- Nhận diện các sự kiện đặc trưng của hệ thống cần quản trị
  - Xác định thông số quản trị tương ứng .
  - Mib view
- Nhận diện nguồn liên kết với các sự kiện.
- Xác định luồng các sự kiện và công cụ quản trị liên quan sẽ đảm trách việc giám sát và thu thập sự kiện.
- Hợp nhất mọi sự kiện đến hệ thống quản lý sự kiện chung->DB
- Nhận diện các tình huống đặc biệt và các phương án xử lý kịp thời.

Xây dựng và phát triển chiến lược quản trị sự kiện (2/2)

- Nhận diện sự kiện theo đặc trưng hoạt động của thiết bị:
  - Nhận diện đối với thiết bị Hub
    - Vấn đề coliision
  - Nhận diện đối với thiết bị Switch
    - Broadcast storm
  - Nhận diện đối với thiết bị router
    - Fragment/ reassembly
    - Routing
  - Nhận diện đối với hệ thống web server
    - Efficiency
    - Error codes
    - Retransmission

Tối ưu công tác quản trị sự kiện (1/2)

- Loại trừ được các sự kiện không cần thiết: luật 20/80.
  - ➢ Tập trung vào việc xử lý 20% sự kiện quan trọng mà chúng gây nên 80% lỗi.
  - Thống kê lỗi (trouble tickets)
  - Phát triển các luật để bẩy sự kiện- (rules)
  - Sử dụng các bộ lọc phù hợp (Apply filters)
  - Hoạch định sự kiện với phương pháp chỉ báo:
    - Gởi ngay cảnh báo (alert/ trapping)
    - Ghi vào nhật ký (log file)

Tối ưu công tác quản trị sự kiện (2/2)

- Sử dụng sự tích hợp các sự kiện tương quan (event correlation)
- Tổ chức sự kiện theo phân nhóm .
  - Phân cấp quản trị
  - Phân nhóm quản trị
    - theo chức năng quản trị,
    - theo loại hệ thống,
    - hay khu vực

Tận dụng tất cả các loại công cụ quản trị có sẵn

- Công cụ quản trị khả năng thực thi (Performance management tools)
  - Nhận diện các thông số quản trị và baselines liên quan.
  - Nhận diện các thông số quản trị cần cảnh báo và ngưỡng liên quan.
  - Chuyển tiếp các sự kiên xảy ra cho thực thể quản trị sự kiện liên quan.
- Công cụ quản trị hệ thống (host resources Mibs).
  - Xác định các thông số và baselines liên quan đến các thành phần: CPU, RAM, Disk…
  - Giám sát và thu thập thông tin.
- Phân tích nhật ký tự động (parsing logs).

Cần tránh các lỗi thường gặp:

- Không quản trị tất cả các hệ thống, thiết bị đang nối vào mạng.
  - Ví dụ: Không quản trị các hệ thống không cần thiết như laptop, máy in…
- Phải bảo đảm hệ thống DNS và các cơ sở dữ liệu liên quan DNS được chính xác và hoạt động đúng đắn.
- Tận dụng tối đa các hợp đồng, thỏa thuận duy trì, bảo dưỡng hệ thống, phần mềm ứng dụng.

Tích hợp các công cụ

- Tích hợp các công cụ quản trị khả năng thực thi vào trong cùng môi trường quản trị để đạt được sự thuận tiện trong chiến lược quản trị sự kiện
- Tích hợp các công cụ quản trị bảo mật vào chung cấu trúc quản trị sự kiện.
- Tích hợp các sự kiện từ các điều khiển tình huống cụ thể.
- Sử dụng công cụ quản trị sự kiện MoA (Manager to Agents) ; MoM (Manager to Manager) để quản lý sự kiện:
  - RMON
  - SNMPv2.
- Chuyển các sự kiện quan trọng đến hệ thống quản lý trouble tickets.

Nhận biết sự cố xảy ra

- Dựa vào các cơ chế quản lý sự kiện:
  - SNMP Traps/Informs
  - SYSLOG
  - Polling
  - Help Desk
- Cơ sở dữ liệu lưu trử các thông tin quản trị được thu thập trước đó.

Phương cách thu thập thông tin Polling

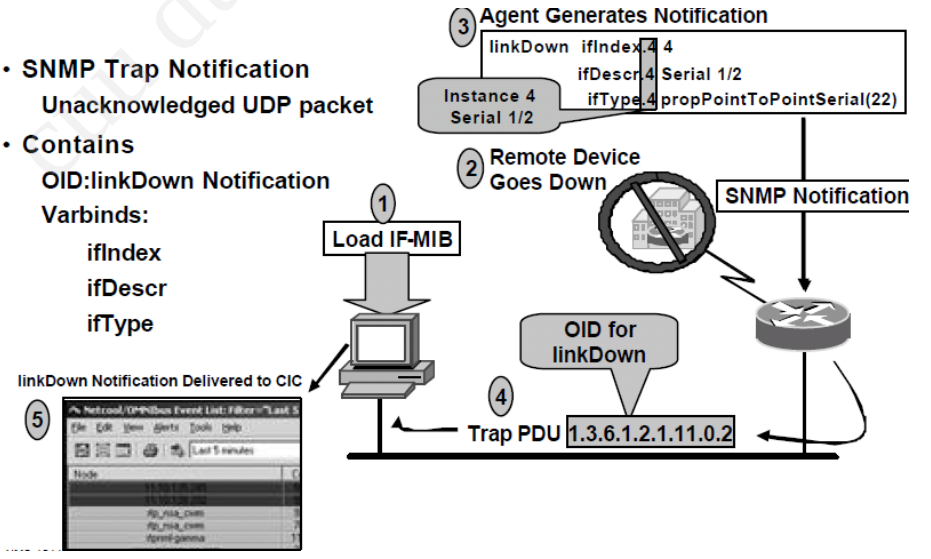
- Nhận diện các tham biến quản trị trên thiết bị được quản trị cần thu thập.
  - Ví dụ:
    - Số octects hay gói trên một interface nào đó
    - Độ khả dụng của một tài nguyên mạng nào đó (utilization of CPU)
- ➢ Quyết định chi tiết của thông tin quản trị thu thập được.
  - Chọn thời khoảng thu thập thông tin (Collection interval)
  - Quan tâm đến mức độ lấy mẫu thông tin quản trị (sample size).
- Ưu điểm: độ tin cậy cao
- Hạn chế: ảnh hưởng hiệu suất mạng

Phương cách thu thập thông tin Trapping

- Xác định tham biến và ngưỡng cần thiết lập
  - Cơ sở lựa chọn.
  - Ứng dụng trong các chức năng quản trị
  - Xây dựng các tình huống điển cứu (case study)
- Ưu điểm.
  - Thời gian thực/ real-time
  - Hiệu suất mạng cao/ efficiency
- Hạn chế: độ tin cậy kém

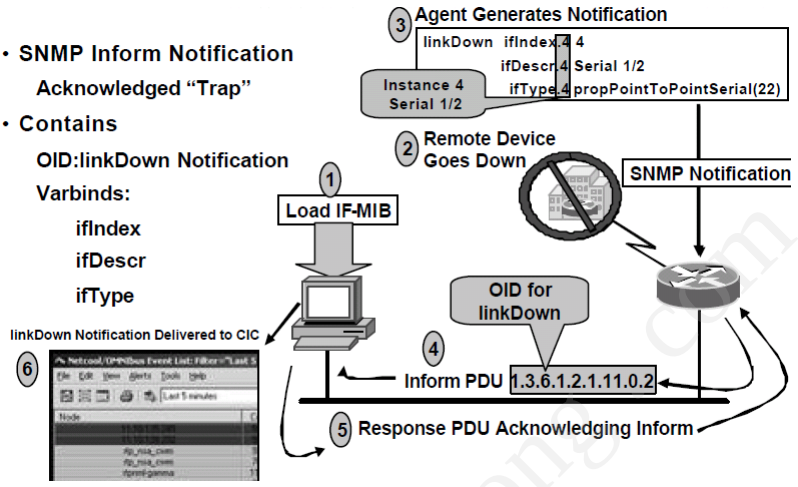
Gởi cảnh báo lỗi

- SNMP Trap Notification
  Unacknowledged UDP packet
- Contains
  OID:linkDown Notification
  Varbinds:
  ifIndex
  ifDescr
  ifType



Thông báo đã nhận được cảnh báo lỗi

- SNMP Inform Notification
  Acknowledged "Trap"
- Contains
  OID:linkDown Notification
  Varbinds:
    ifIndex
    ifDescr
    ifType

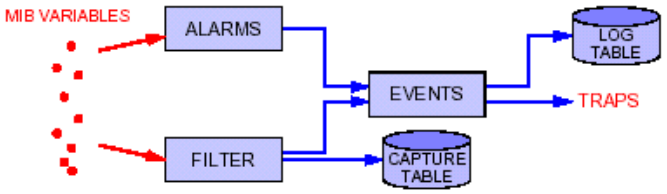


Các dạng báo cáo về thông tin quản trị

- Báo cáo các ngoại lệ (Exceptions)
  - Chỉ báo vượt ngưỡng tại một thời điểm cụ thể trên các tham biến quản trị đã được quan tâm trước đó.
  - Báo cáo về xu hướng hoạt động(Trends)
    - Short term dựa trên thông tin thu được trong 15 ngày gần nhất
    - Long term dựa trên thông tin thu được trong 3 tháng gần nhất
- Tính khả dụng bị xâm phạm (Points to Watch)
  - Nhận diện được một số tài nguyên có mức sử dụng quá cao, đe dọa tính sẵn sàng của hệ thống.
- Thống kê các hệ thống/ máy đầu cuối sử dụng quá cao (Matrix/ RMON2)
- Chẩn đoán lỗi (Diagnostics)
  - Phân tích, truy tìm nguyên nhân về các lỗi xảy ra hay sự giảm sút khả năng hoạt động của hệ thống.

▪Ứng dụng trong RMON

OTHER GROUPS



- FILTER GROUP
  - TO COUNT PACKETS THAT CARRY A SPECIFIC BIT-PATTERN
- PACKET CAPTURE GROUP
  - TO STORE SPECIFIC PACKETS
- EVENT GROUP
  - TO DEFINE THE VARIOUS EVENTS
  - TO DETERMINE ON LOGGING AND / OR TRANSMISSION OF TRAPS

▪Ứng dụng trong RMON

Chức năng và các mối quan hệ giưa các đối tượng