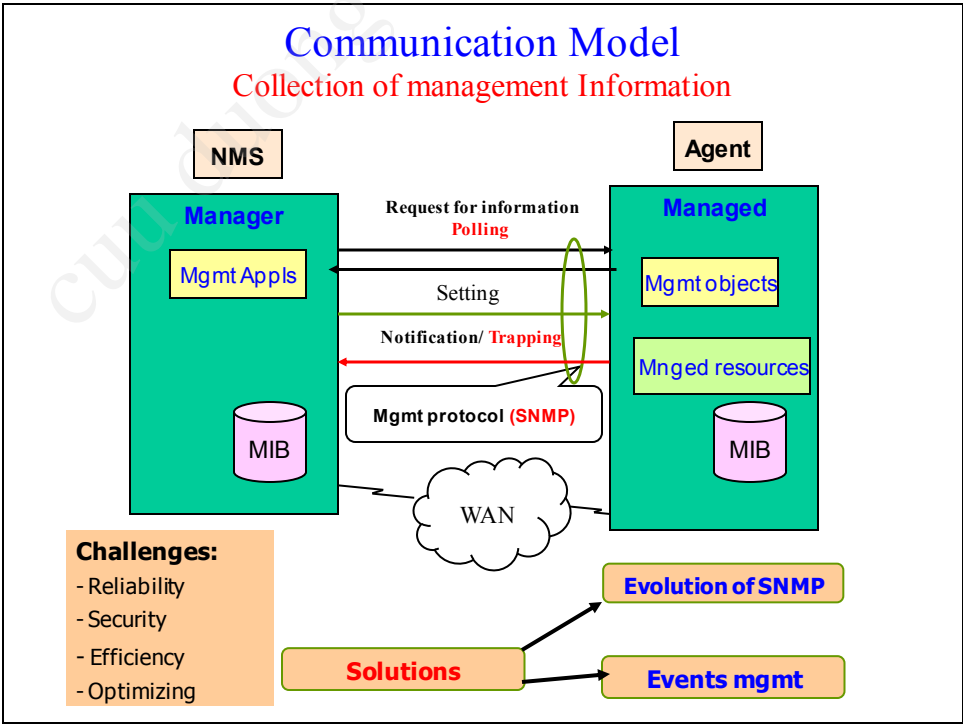
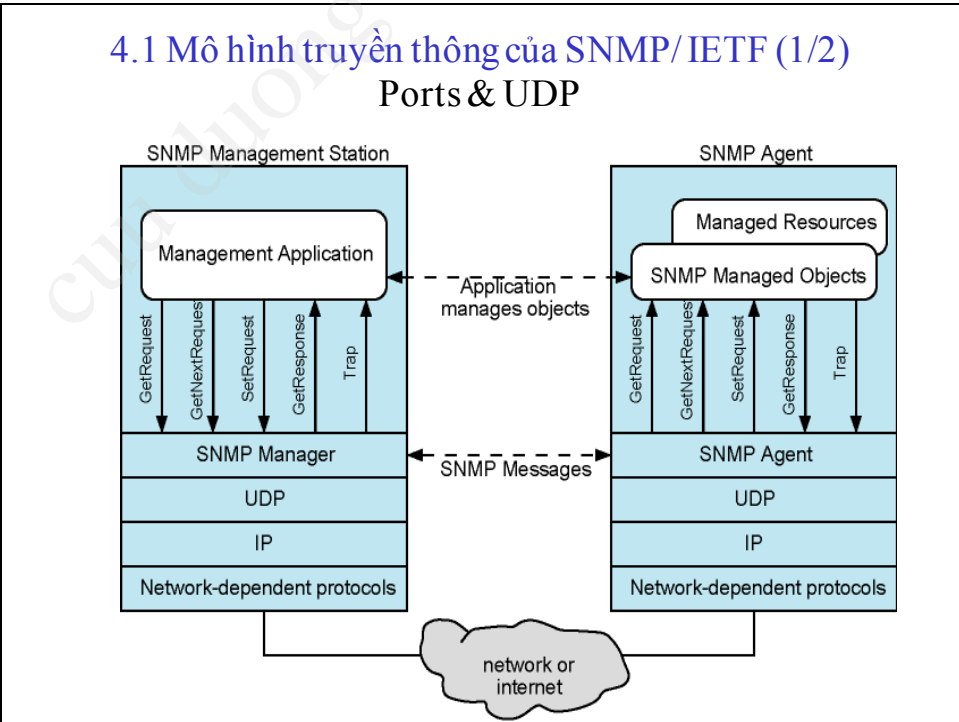
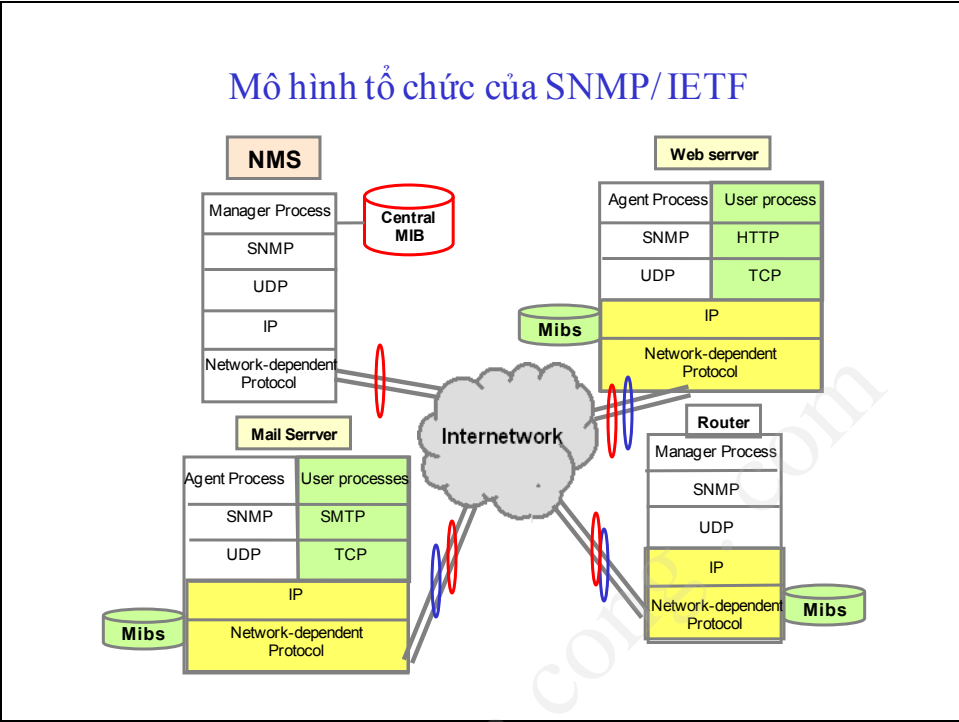


Chương 4. Mô hình truyền thông SNMP-IETF

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. Môi quan hệ điều khiển truyền thông
7. Quản trị sự kiện





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

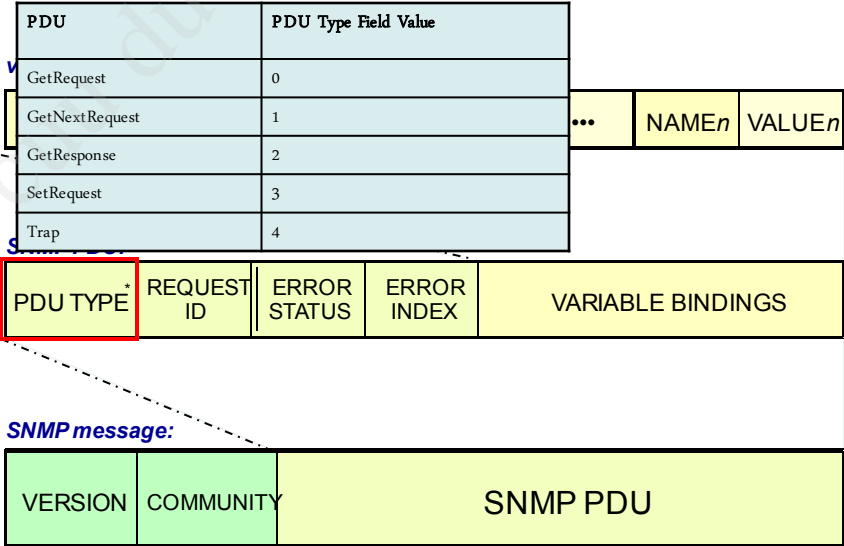
•SNMP uses User Datagram Protocol (UDP) as the transport mechanism for SNMP messages



•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



Định dạng thông điệp điều khiển SNMP

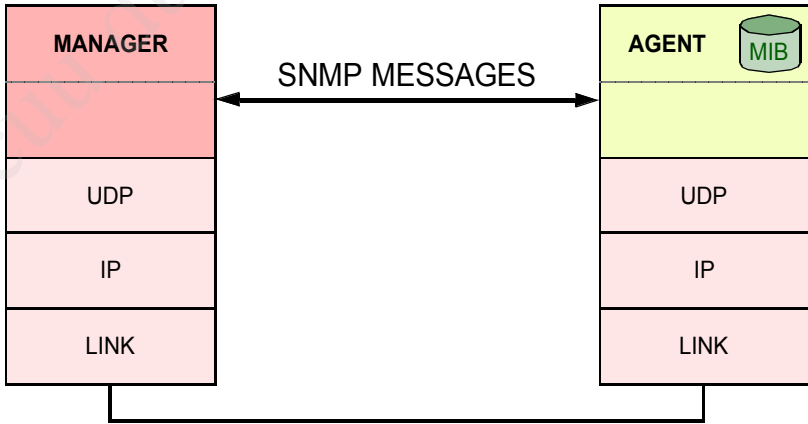
Status	Name	Meaning
0	noError	No error
1	tooBig	Response too big to fit in one message
2	noSuchName	Variable does not exist
3	badValue	The value to be stored is invalid
4	readOnly	The value cannot be modified
5	genErr	Other errors

NAME1	VALUE1	NAME2	VALUE2	NAME _n	VALUE _n
-------	--------	-------	--------	-----	-----	-------------------	--------------------

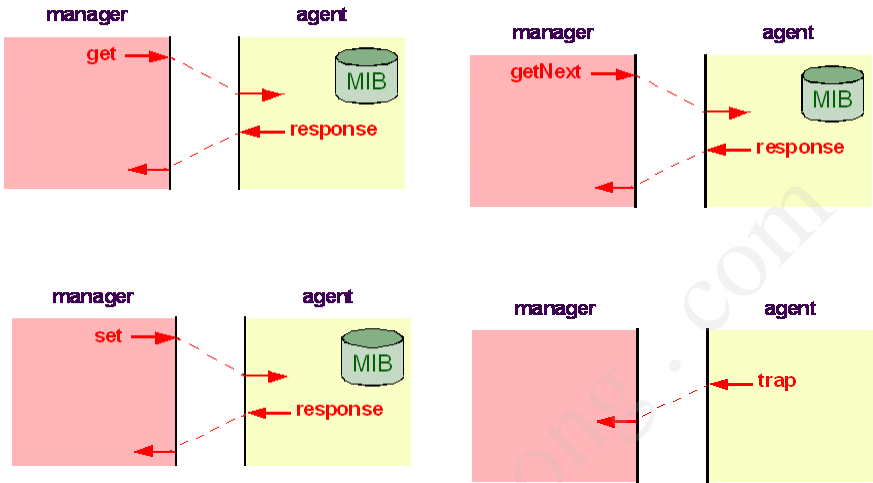
SNMP PDU:

PDU TYPE*	REQUEST ID	ERROR STATUS	ERROR INDEX	VARIABLE BINDINGS
-----------	------------	--------------	-------------	-------------------

4.2 Hoạt động của giao thức SNMPv1



Mình 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

ENTERPRISE
AGENT-ADDRESS
GENERIC-TRAP
SPECIFIC-TRAP
TIME-STAMP
VARIABLE-BINDINGS

TRAP - PDU FORMAT

ENTERPRISE
AGENT-ADDRESS
GENERIC-TRAP
SPECIFIC-TRAP
TIME-STAMP
VARIABLE-BINDINGS

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 <i>ifIndex</i> instance.
LinkUp	3	A communication link has come up → name and value of the <i>ifIndex</i> 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 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 giá 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

No. -	Time	Source	Destination	Protocol	Info
23	0.552965	192.168.100.200	192.168.100.1	SNMP	GET IF-MIB::ifSpeed.1

Frame 23 (87 bytes on wire, 87 bytes captured)

Ethernet II, Src: Vmware_c0:00:01 (00:50:56:c0:00:01), Dst: Vmware_f0:6e:81 (00:0c:29:f0:6e:81)

Internet Protocol, Src: 192.168.100.200 (192.168.100.200), Dst: 192.168.100.1 (192.168.100.1)

User Datagram Protocol, Src Port: 1309 (1309), Dst Port: snmp (161)

Simple Network Management Protocol

Version: 2c (1)

Community: Fapkhui

PDU type: GET (0)

Request Id: 0x00000077

Error Status: NO ERROR (0)

Error Index: 0

Object Identifier 1: 1.3.6.1.2.1.2.1.5.1 (IF-MIB::ifSpeed.1)

Value: NULL

Polling-> Get Response SNMP

No. -	Time	Source	Destination	Protocol	Info
26	0.553720	192.168.100.1	192.168.100.200	SNMP	RESPONSE IF-MIB::ifSpeed.1
Frame 26 (91 bytes on wire, 91 bytes captured)					
Ethernet II, Src: vmware_f0:6e:81 (00:0c:29:f0:6e:81), Dst: Vmware_c0:00:01 (00:50:56:c0:00:01)					
Internet Protocol, Src: 192.168.100.1 (192.168.100.1), Dst: 192.168.100.200 (192.168.100.200)					
User Datagram Protocol, Src Port: snmp (161), Dst Port: 1309 (1309)					
Simple Network Management Protocol					
Version: 2C (1)					
Community: tankhuu					
PDU type: RESPONSE (0)					
Request id: 0x00000877					
Error status: NO ERROR (0)					
Error Index: 0					
Object identifier 1: 1.3.6.1.2.1.2.2.1.5.1 (IF-MIB::ifSpeed.1)					
Value: Gauge32: 10000000					

Polling-> GetNext Request SNMP

No. -	Time	Source	Destination	Protocol	Info
6	6.858979	10.10.10.100	10.10.10.1	SNMP	GET-NEXT SNMPV2-SMI::mib-2.25.3.3.1.2
7	6.879615	10.10.10.1	10.10.10.100	SNMP	RESPONSE SNMPV2-SMI::mib-2.25.3.3.1.2.5
Frame 6 (90 bytes on wire, 90 bytes captured)					
Ethernet II, Src: vmware_37:0e:d4 (00:0c:29:37:0e:d4), Dst: vmware_36:76:49 (00:0c:29:36:76:49)					
Internet Protocol, Src: 10.10.10.100 (10.10.10.100), Dst: 10.10.10.1 (10.10.10.1)					
User Datagram Protocol, Src Port: 1459 (1459), Dst Port: snmp (161)					
Simple Network Management Protocol					
Version: 2 (1)					
Community: wpcnghia-8					
PDU type: GET-NEXT (1)					
Request id: 0x00002890					
Error status: NO ERROR (0)					
Error Index: 0					
Object identifier 1: 1.3.6.1.2.1.25.3.3.1.2 (SNMPV2-SMI::mib-2.25.3.3.1.2)					
Value: NULL					

Polling-> GetNext Response SNMP

No. -	Time	Source	Destination	Protocol	Info
7	6.879615	10.10.10.1	10.10.10.100	SNMP	RESPONSE SNMPv2-SMI::mib-2.25.3.3.1.2.5
[+] Frame 7 (92 bytes on wire, 92 bytes captured)					
[+] Ethernet II, Src: Vmware_36:76:49 (00:0c:29:36:76:49), Dst: Vmware_37:0e:d4 (00:0c:29:37:0e:d4)					
[+] Internet Protocol, Src: 10.10.10.1 (10.10.10.1), Dst: 10.10.10.100 (10.10.10.100)					
[+] User Datagram Protocol, Src Port: snmp (161), Dst Port: 1459 (1459)					
[+] Simple Network Management Protocol					
Version: 2C (1)					
Community: nccccchia-r					
PDU type: RESPONSE (2)					
Request id: 0x00002890					
ERROR STATUS: NO ERROR (0)					
Error Index: 0					
Object identifier 1: 1.3.6.1.2.1.25.3.3.1.2.5 (SNMPv2-SMI::mib-2.25.3.3.1.2.5)					
Value: INTEGER: 3					

Trapping -> Trap SNMPv1

No. -	Time	Source	Destination	Protocol	Info
72	22.141657	10.10.10.1	10.10.10.3	SNMP	TRAP-V1 IF-MIB::ifIndex.1
73	22.141797	10.10.10.1	10.10.10.3	SNMP	TRAP-V1 IF-MIB::ifIndex.2
74	22.142227	10.10.10.1	10.10.10.3	SNMP	TRAP-V1 IF-MIB::ifIndex.2
[+] Frame 72 (108 bytes on wire, 108 bytes captured)					
[+] Ethernet II, Src: Vmware_b0:80:d6 (00:0c:29:b0:80:d6), Dst: Vmware_bd:d4:9c (00:0c:29:bd:d4:9c)					
[+] Internet Protocol, Src: 10.10.10.1 (10.10.10.1), Dst: 10.10.10.3 (10.10.10.3)					
[+] User Datagram Protocol, Src Port: 1169 (1169), Dst Port: snmptrap (162)					
[+] Simple Network Management Protocol					
Version: 1 (0)					
Community: cccccrww					
PDU type: TRAP-V1 (4)					
enterprise: 1.3.6.1.4.1.311.1.1.3.1.3 (SNMPv2-SMI::enterprises.311.1.1.3.1.3)					
agent-addr: internet (0)					
generic-trap: linkup (3)					
specific-trap: 0					
time-stamp: 1504					
Object identifier 1: 1.3.6.1.2.1.2.2.1.1.1 (IF-MIB::ifIndex.1)					
Value: INTEGER: 1					

Trapping -> Trap SNMPv1

No. -	Time	Source	Destination	Protocol	Info
21	8.293692	10.10.10.3	10.10.10.1	SNMP	GET IF-MIB::ifDescr.1
22	8.738216	10.10.10.1	10.10.10.3	SNMP	TRAP-V1
23	8.738455	10.10.10.1	10.10.10.3	SNMP	TRAP-V1
24	8.738594	10.10.10.1	10.10.10.3	SNMP	TRAP-V1
25	8.739855	10.10.10.1	10.10.10.3	SNMP	RESPONSE IF-MIB::ifDescr.1
26	8.743538	10.10.10.3	10.10.10.1	SNMP	GET IF-MIB::ifOperStatus.1
27	8.744095	10.10.10.1	10.10.10.3	SNMP	RESPONSE IF-MIB::ifOperStatus.1
28	8.745460	10.10.10.3	10.10.10.1	SNMP	GET IF-MIB::ifLastChange.1
29	8.745991	10.10.10.1	10.10.10.3	SNMP	RESPONSE IF-MIB::ifLastChange.1

Frame 22 (89 bytes on wire, 89 bytes captured)

Ethernet II, Src: vmware_b0:80:d6 (00:0c:29:b0:80:d6), Dst: vmware_bd:d4:9c (00:0c:29:bd:d4:9c)

Internet Protocol, Src: 10.10.10.1 (10.10.10.1), Dst: 10.10.10.3 (10.10.10.3)

User Datagram Protocol, Src Port: 1169 (1169), Dst Port: snmptrap (162)

Simple Network Management Protocol

Version: 1 (0)

Community: cuong_n

PDU type: TRAP-V1 (4)

Enterprise: 1.3.6.1.4.1.311.1.1.3.1.3 (SNMPv2-SMI::enterprises.311.1.1.3.1.3)

agent-addr: internet (0)

generic-trap: coldStart (0)

specific-trap: 0

time-stamp: 0

Trapping -> Trap SNMPv2

No. -	Time	Source	Destination	Protocol	Info
295	178.368617	10.10.10.1	10.10.10.3	SNMP	RESPONSE SNMPv2-MIB::sysUpTime.0
296	184.640296	10.10.10.3	10.10.10.1	SNMP	TRAP-V2 SNMPv2-MIB::sysUpTime.0 SNMPV2-MIB::sysUpTime.0
309	200.372923	10.10.10.3	10.10.10.1	SNMP	GET SNMPv2-MIB::sysUpTime.0

Frame 296 (171 bytes on wire, 171 bytes captured)

Ethernet II, Src: vmware_bd:d4:9c (00:0c:29:bd:d4:9c), Dst: vmware_b0:80:d6 (00:0c:29:b0:80:d6)

Internet Protocol, Src: 10.10.10.3 (10.10.10.3), Dst: 10.10.10.1 (10.10.10.1)

User Datagram Protocol, Src Port: 1064 (1064), Dst Port: snmptrap (162)

Simple Network Management Protocol

Version: 2c (3)

Community: cuong_n

PDU type: TRAP-V2 (7)

Request ID: 0x00049cc

Error Status: NO ERROR (0)

Error Index: 0

Object identifier 1: 1.3.6.1.2.1.1.3.0 (SNMPv2-MIB::sysUpTime.0)

Value: Timeticks: (0) 0:00:00.00

Object identifier 2: 1.3.6.1.6.3.1.1.4.1.0 (SNMPv2-MIB::snmpTrapOID.0)

Value: OID: SNMPv2-SMI::enterprises.11307.10

Object identifier 3: 1.3.6.1.6.3.1.1.4.3.0 (SNMPv2-MIB::snmpTrapEnterprise.0)

Value: OID: SNMPv2-SMI::enterprises.11307

Object identifier 4: 1.3.6.1.4.1.11307.10.1 (SNMPv2-SMI::enterprises.11307.10.1)

Value: STRING: "Test trap at 09:43 PM"

Các giới hạn của SNMPv1

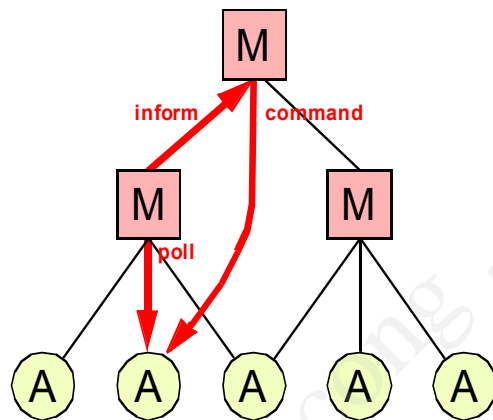
- Không định nghĩa rõ các luật
- Còn hạn chế về:
 - Các mã lỗi.
 - Kiểu dữ liệu.
 - Các thông báo sự kiện.
 - Khả năng thu thập lượng lớn thông tin quản trị.
- Sự lệ thuộc vào độ tin cậy của môi trường truyền, đặc biệt đối với TRAP.
- Chưa hỗ trợ kiến trúc phân tán.
- Hạn chế về bảo mật trong truyền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

4.3 Phiên bản SNMPv2

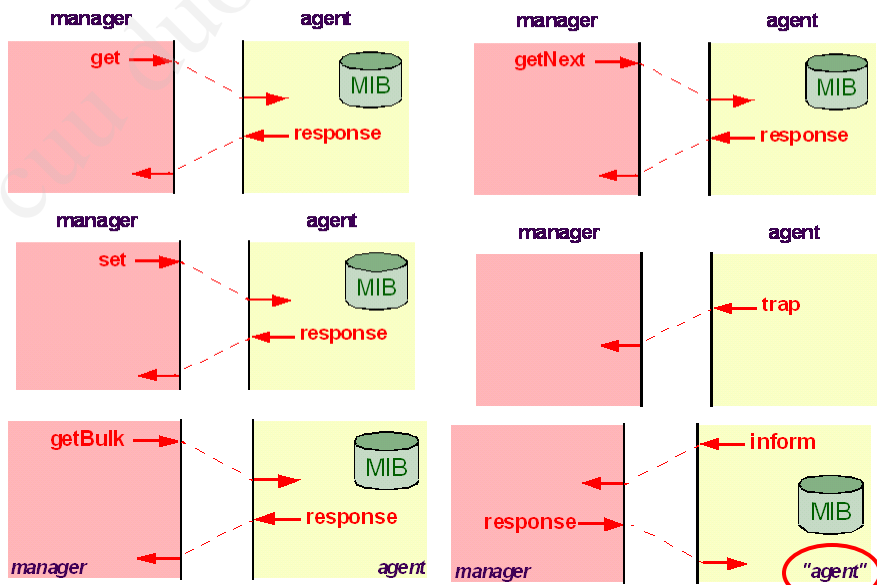
- **Đặc điểm:**
 - Triển khai mô hình hoạt động quản trị phân cấp **M2M**
 - Cải thiện mô hình **bảo mật**.
 - Cải thiện **hoạt động thu thập lượng lớn thông tin (Getbulk)**
 - Cải thiện **độ tin cậy** trong hoạt động cảnh báo TRAPPING bởi **Inform** và **Report**.
 - Cải thiện khả năng **chỉ báo lỗi**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

Mô hình quản trị phân cấp trong SNMPv2

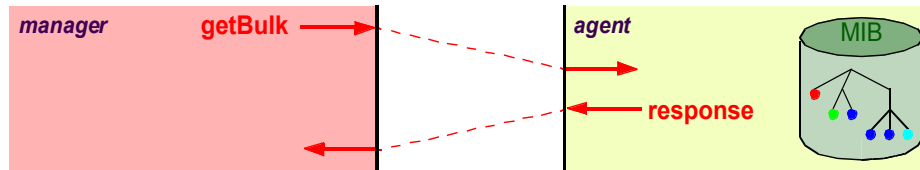
- Mô hình quản trị MANAGER TO MANAGER (M2M)



Hoạt động cơ bản của SNMPv2



GET-BULK



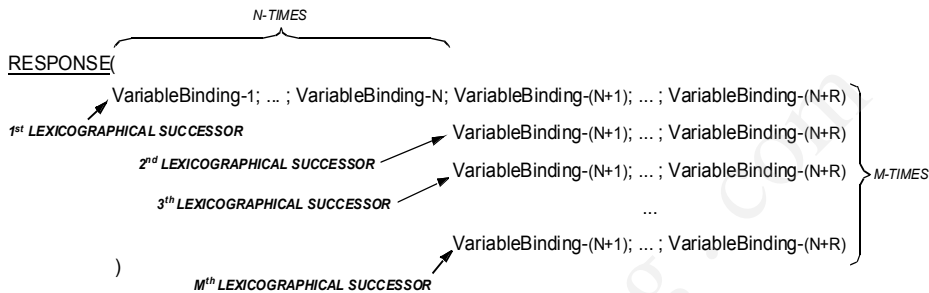
- Chức năng mới trong SNMPv2
 - Dùng để thu thập **lượng lớn** thông tin quản trị.
 - Cải thiện khả năng hoạt động của SNMP

GET-BULK

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

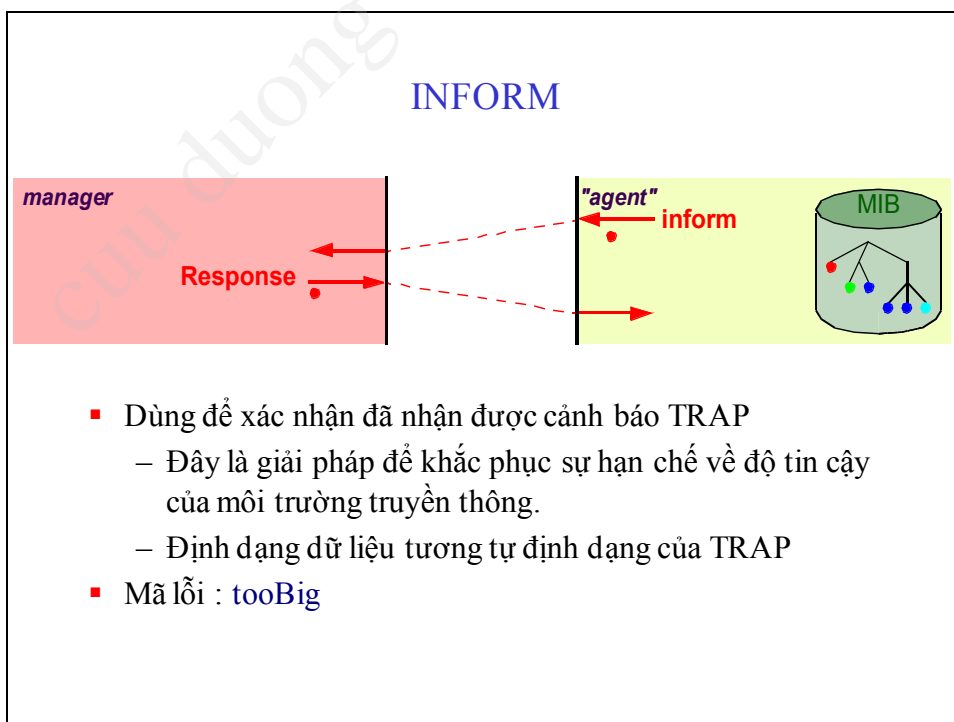
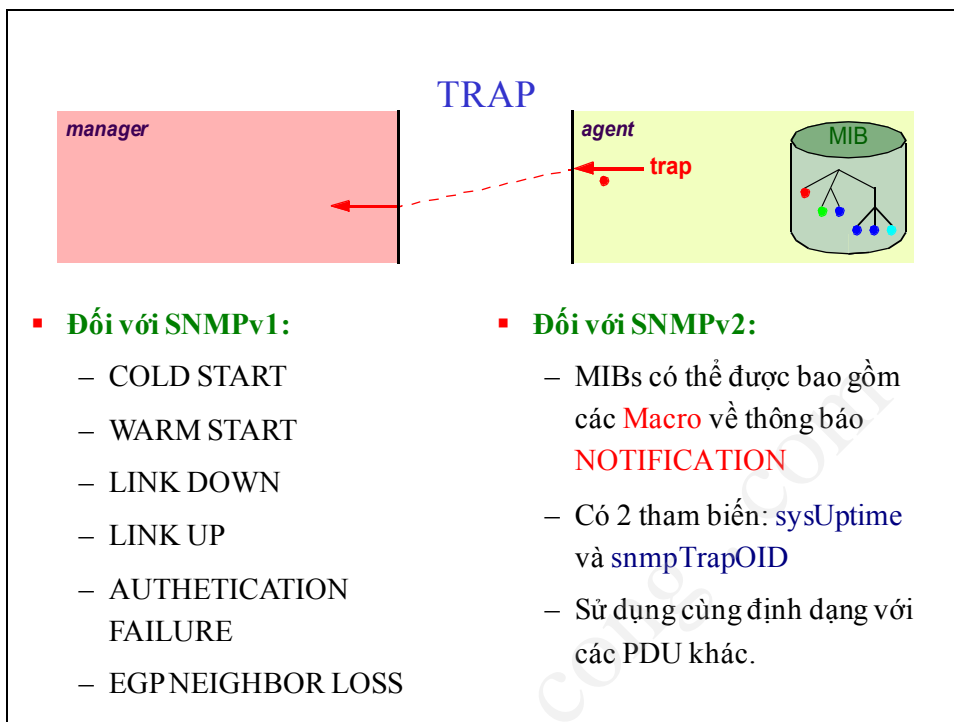
badValue
badValue
badValue
badValue
badValue
noSuchName
noSuchName
noSuchName
noSuchName
genErr
genErr

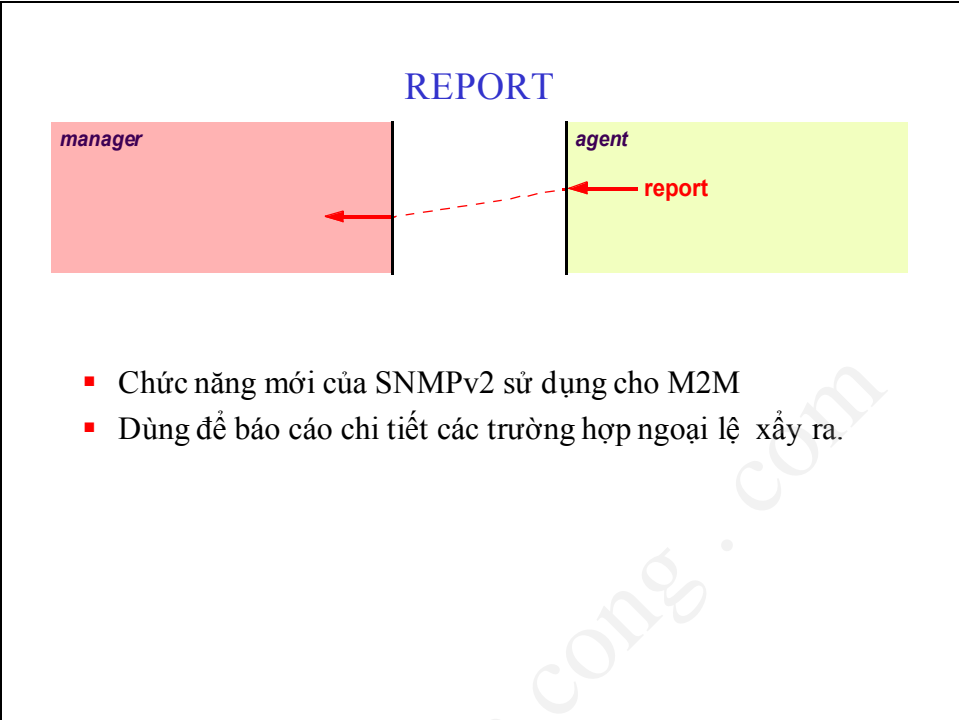
wrongValue
wrongEncoding
wrongType
wrongLength
inconsistentValue
noAccess
notWritable
noCreation
inconsistentName
resourceUnavailable
genErr

PHASE 2:

genErr
genErr

CommitFailed
undoFailed





Polling-> GetBulk Request SNMP

The image shows a Wireshark packet capture of an SNMP GetBulk Request. The packet is sent from 192.168.100.200 to 192.168.100.1. The packet details are as follows:

No.	Time	Source	Destination	Protocol	Info
3	0.011610	192.168.100.200	192.168.100.1	SNMP	GETBULK TCP-MIB::tcpEstabResets

Frame 3 (85 bytes on wire, 85 bytes captured)

- Ethernet II, Src: vmware_e9:c0:34 (00:0c:29:e9:c0:34), Dst: vmware_d3:58:38 (00:0c:29:d3:58:38)
- Internet Protocol, Src: 192.168.100.200 (192.168.100.200), Dst: 192.168.100.1 (192.168.100.1)
- User Datagram Protocol, Src Port: 1142 (1142), Dst Port: snmp (161)
- Simple Network Management Protocol
 - Version: 2c (1)
 - Community: agent-1
 - PDU type: GETBULK (5)
 - Request id: 0x00000db3
 - Non-repeaters: 0
 - Max repetitions: 10
 - Object identifier 1: 1.3.6.1.2.1.6.8 (TCP-MIB::tcpEstabResets)
 - Value: NULL

Polling-> GetBulk Response SNMP

No.	Time	Source	Destination	Protocol	Info
3	0.011610	192.168.100.200	192.168.100.1	SNMP	GETBULK-REQ-MIB::tcpestabResets
4	0.012391	192.168.100.1	192.168.100.200	SNMP	RESPONSE-TCP-MIB::tcpestabResets.0 TCP-MIB::tcpCurrEstab.0

⚠ User Datagram Protocol, Src Port: snmp (161), Dst Port: 1142 (1142)
⚠ Simple Network Management Protocol
Version: 2C (1)
Community: public
PDU type: RESPONSE (2)
Request ID: 0x00000003
Error Status: NO ERROR (0)
Error Index: 0

Object identifier 1: 1.3.6.1.2.1.6.8.0 (TCP-MIB::tcpEstabResets.0)
value: Counter32: 3
Object identifier 2: 1.3.6.1.2.1.6.9.0 (TCP-MIB::tcpCurrEstab.0)
value: Gauge32: 19
Object identifier 3: 1.3.6.1.2.1.6.10.0 (TCP-MIB::tcpInSegs.0)
value: Counter32: 13480
Object identifier 4: 1.3.6.1.2.1.6.11.0 (TCP-MIB::tcpOutSegs.0)
value: Counter32: 13346
Object identifier 5: 1.3.6.1.2.1.6.12.0 (TCP-MIB::tcpRetransSegs.0)
value: Counter32: 0
Object identifier 6: 1.3.6.1.2.1.6.13.1.1.0.0.0.0.53.0.0.0.18485 (TCP-MIB::tcpConnState.0.0.0.0.53.0.0.0.18485)
value: INTEGER: listen(2)
Object identifier 7: 1.3.6.1.2.1.6.13.1.1.0.0.0.0.80.0.0.0.2080 (TCP-MIB::tcpConnState.0.0.0.0.80.0.0.0.2080)
value: INTEGER: listen(2)
Object identifier 8: 1.3.6.1.2.1.6.13.1.1.0.0.0.0.88.0.0.0.63729 (TCP-MIB::tcpConnState.0.0.0.0.88.0.0.0.63729)
value: INTEGER: listen(2)
Object identifier 9: 1.3.6.1.2.1.6.13.1.1.0.0.0.0.135.0.0.0.8434 (TCP-MIB::tcpConnState.0.0.0.0.135.0.0.0.8434)
value: INTEGER: listen(2)
Object identifier 10: 1.3.6.1.2.1.6.13.1.1.0.0.0.0.389.0.0.0.39006 (TCP-MIB::tcpConnState.0.0.0.0.389.0.0.0.39006)
value: INTEGER: listen(2)

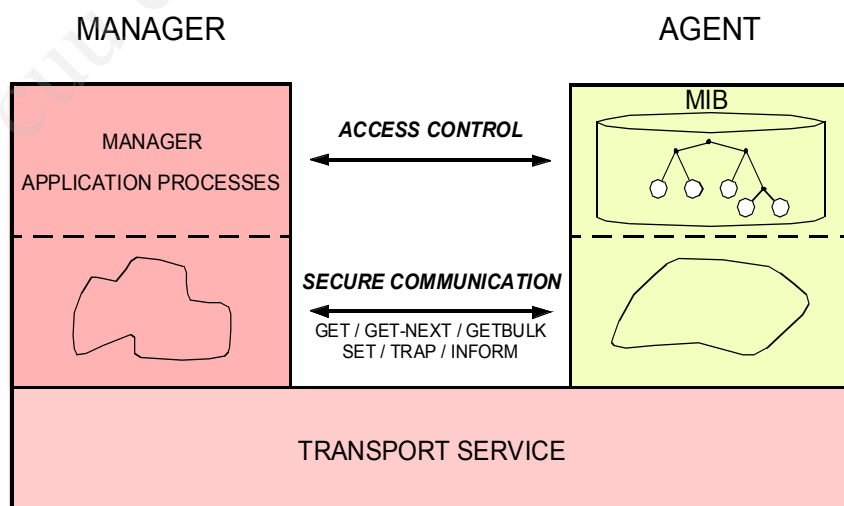
Các chuẩn RFCs liên quan SNMPv2

- Mô hình truyền thông:
 - DRAFT STANDARD
 - RFC 1905, RFC 1906
- Mô hình bảo mật - SNMPv2C:
 - COMMUNITY BASED SNMP
 - SAME 'SECURITY MECHANISMS' AS SNMPv1
 - EXPERIMENTAL STATUS
 - RFC 1901
- Mô hình bảo mật - SNMPv2U:
 - USER BASED SECURITY (AUTHENTICATION / ENCRYPTION / ACCESS CONTROL)
 - EXPERIMENTAL STATUS
 - RFC 1909, RFC 1910
- Mô hình thông tin:
 - STANDARD, RFC 2578, RFC 2579, RFC 2580

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).

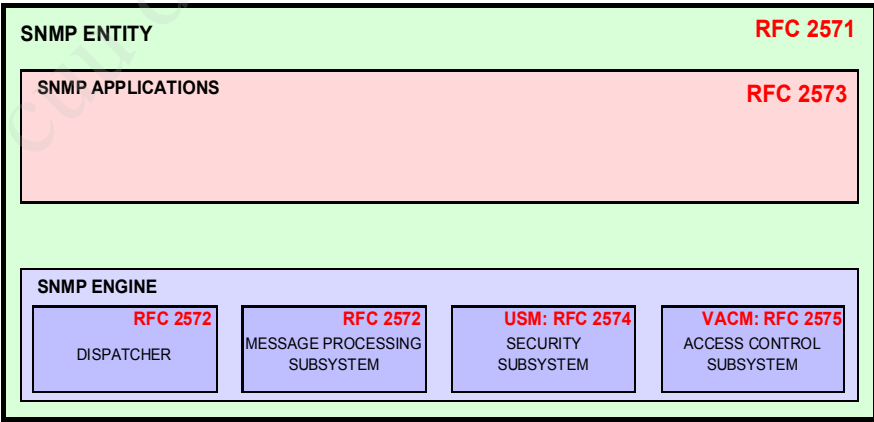
ACCESS CONTROL TABLES

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
...
...
...
...

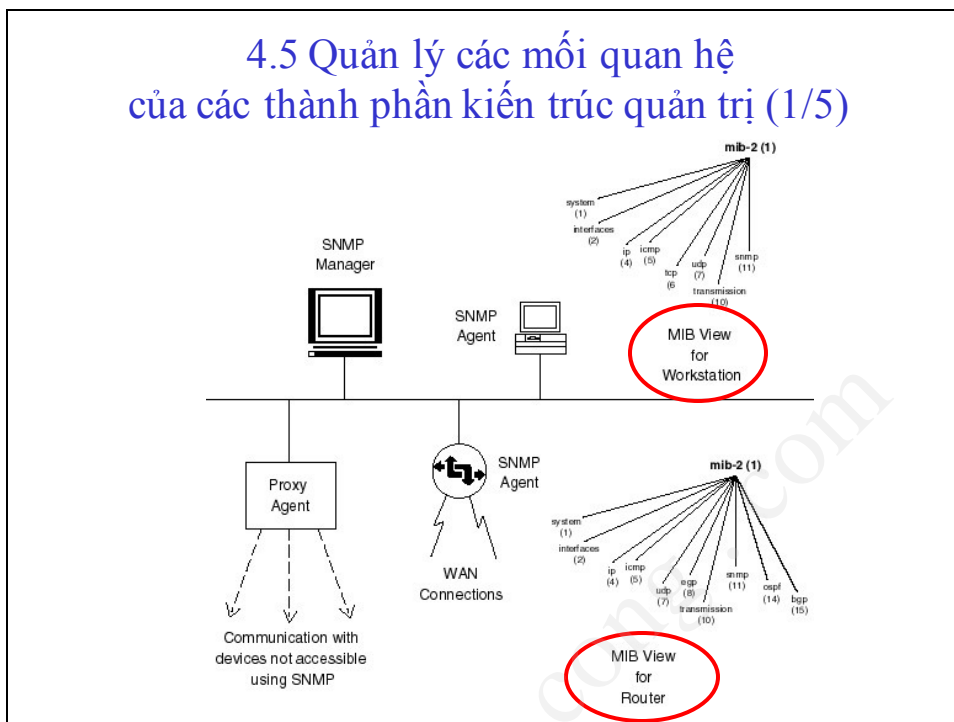
Các bước cấu hình bảo mật cho SNMPv3

- **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 toán 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 trữ 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 trữ 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 trữ 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 lược quản trị sự kiện
- Nhận biết sự cố xảy ra
- **Triển khai** Các chuẩn cảnh báo và xác nhận được
 - Syslog
 - Polling
 - Trapping/ alert

Các yêu cầu đối với thu thập thông tin

- Thỏa mãn về **chất lượng thông tin** quản trị thu thập được.
 - Có thể phân tích.
 - **Đủ thông tin** để phản ánh 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 collision
 - 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 bẫy sự kiện- (rules)
 - Sử dụng các **bộ lọc** phù hợp (Apply filters)
 - **Hoạch định** sự kiện với phương pháp chỉ báo:
 - Gửi 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 kiện 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 trữ 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 octets 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

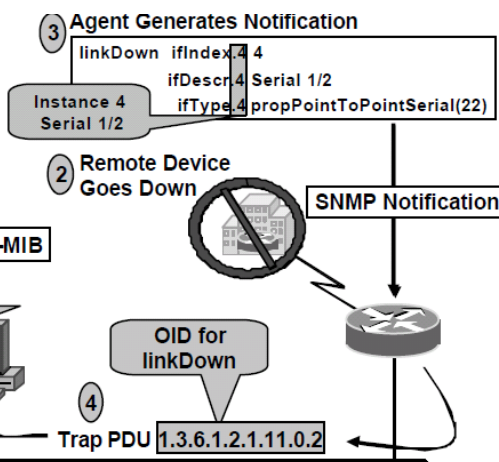
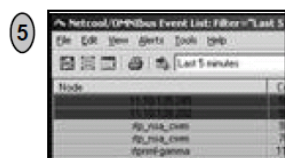
- Xác định tham biến và ngưỡng cần thiết lập
 - Cơ sở lựa chọn.
 - Ứng dụng trong các chức năng quản trị
 - Xây dựng các tình huống điển cứu (case study)
- Ưu điểm.
 - Thời gian thực/ real-time
 - Hiệu suất mạng cao/ efficiency
- Hạn chế: độ tin cậy kém

Gửi cảnh báo lỗi

- **SNMP Trap Notification**
Unacknowledged UDP packet

- **Contains**
OID: linkDown Notification
Varbinds:
ifIndex
ifDescr
ifType

linkDown Notification Delivered to CIC



Thông báo đã nhận được cảnh báo lỗi

• SNMP Inform Notification

Acknowledged "Trap"

• Contains

OID: linkDown Notification

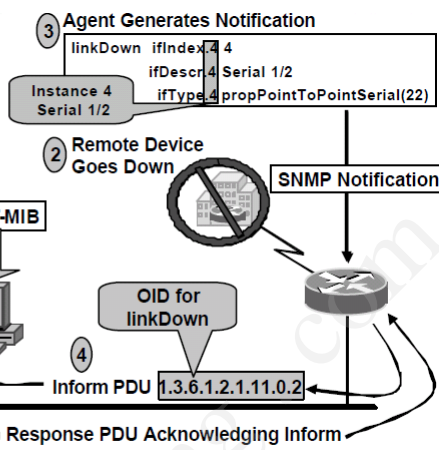
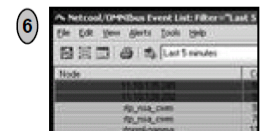
Varbinds:

ifIndex

ifDescr

ifType

linkDown Notification Delivered to CIC

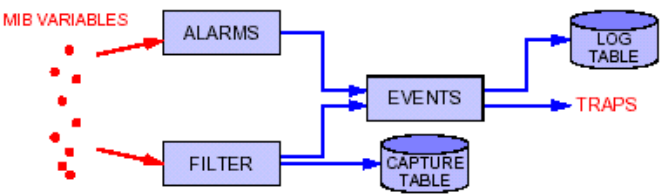


Các dạng báo cáo về thông tin quản trị

- 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 giữa các đối tượng

