第 6 章 SNMP

- 組成網路管理系統的元件
- SNMP封包的欄位
- SNMP協定的資料單元
- MIB樹的結構
- MIB-2物件及物件識別碼（object identifier）
- SNMP指令及參數
- SNMP指令示範
- SNMP的安全組件及用法
- NMS的MIB瀏覽器
- 使用NMS示範SNMP訊框的捕捉及分析

p. 6-3 Fig. 6.1

6.1 管理站／管理代理者之間的通訊

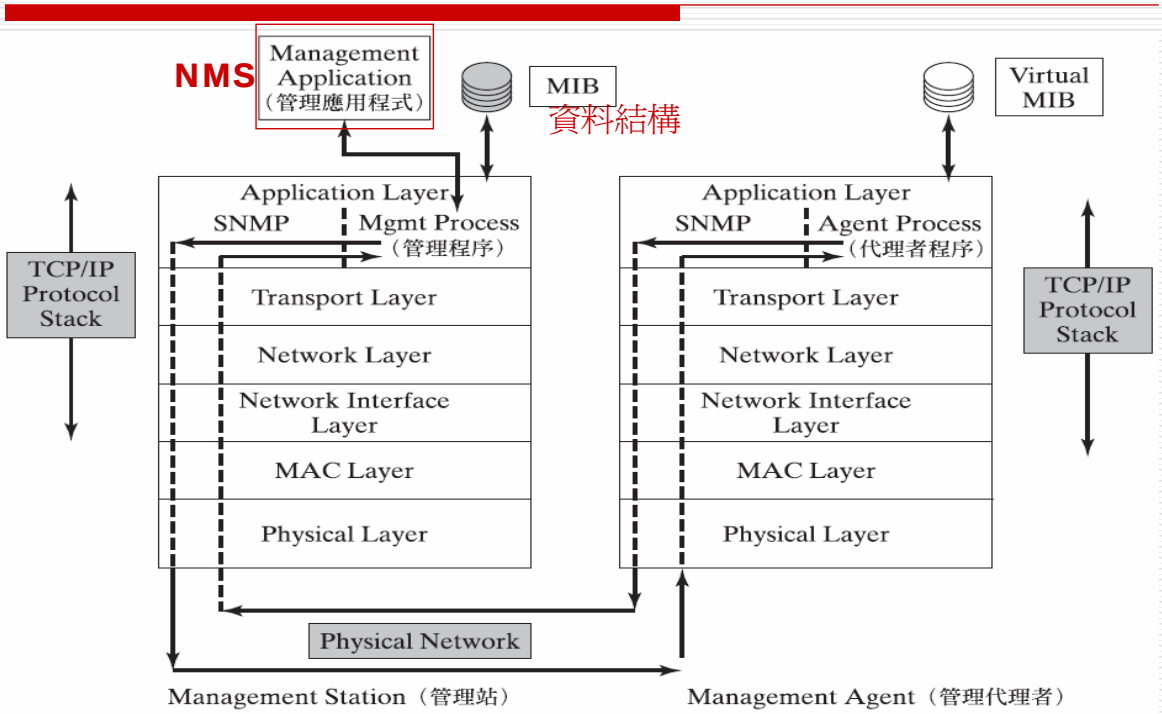
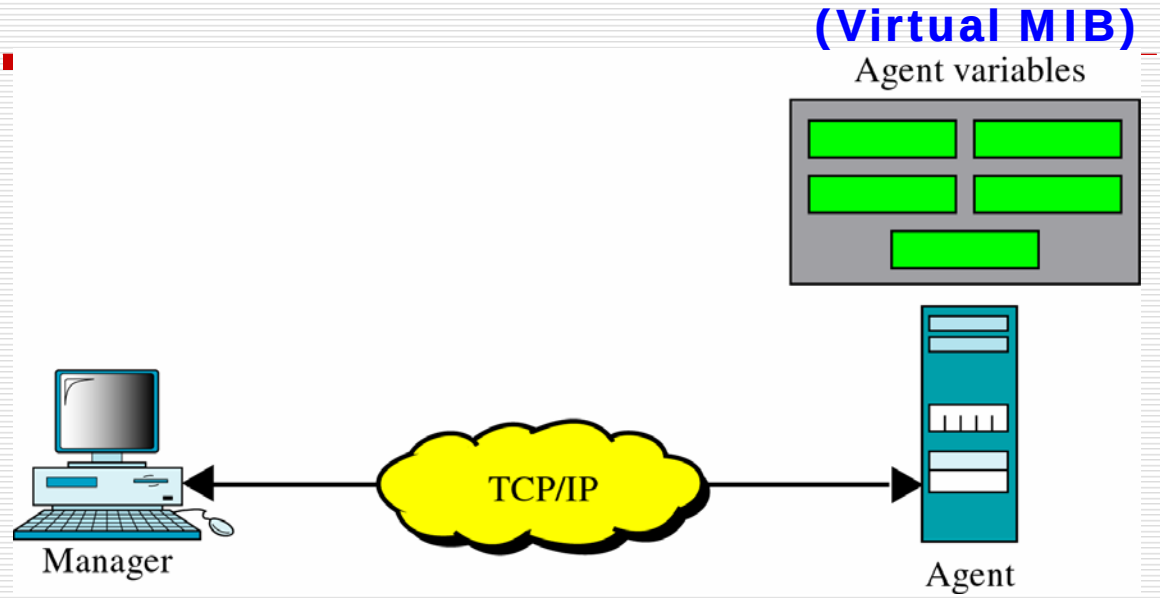


圖 6.1 TCP/IP 網路管理環境中的組件

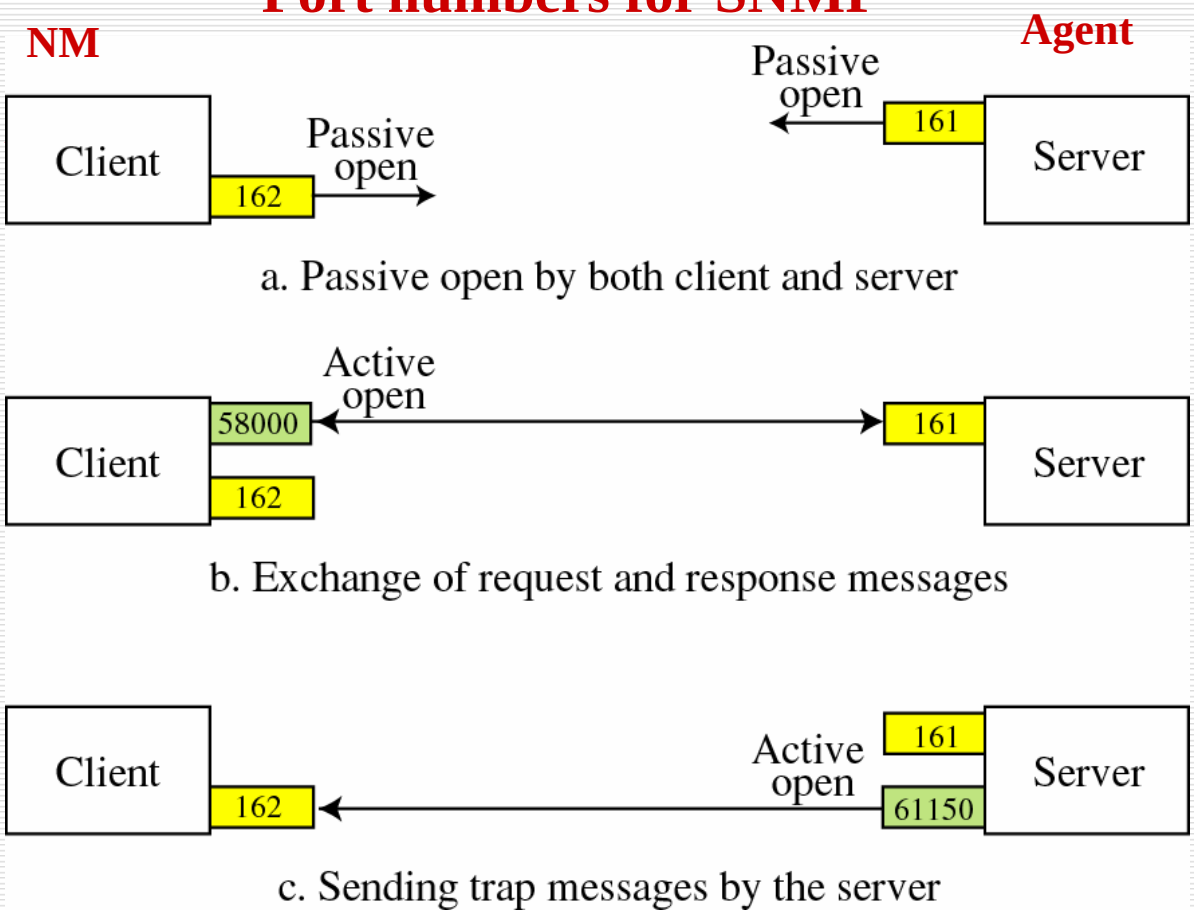
SNMP Concept



SNMP

- 簡單網路管理協定（Simple Network Management Protocol）
  - 「要求/回應」協定：GET，SET
- 遠端管理TCP/IP網路上的設備
  - 對不同網路節點進行讀取及寫入狀態資訊
- 在UDP上執行
  - Port 161：sending and receiving requests
  - Port 162: receiving traps from managed devices

Port numbers for SNMP



SNMP 標準 (RFC)

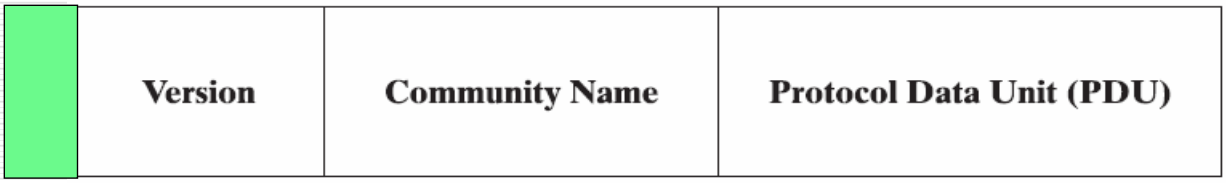
- Request for Comments (RFC) 是一系列的發展報告、通訊協定的建議及網際網路群區所使用的通訊協定標準。[簡單網路管理通訊協定 (SNMP)] 規格是由 Internet Engineering Task Force (IETF) 及其他工作群組發行的 RFC 所定義。

p. 6-4

6.1.3 管理站SNMP

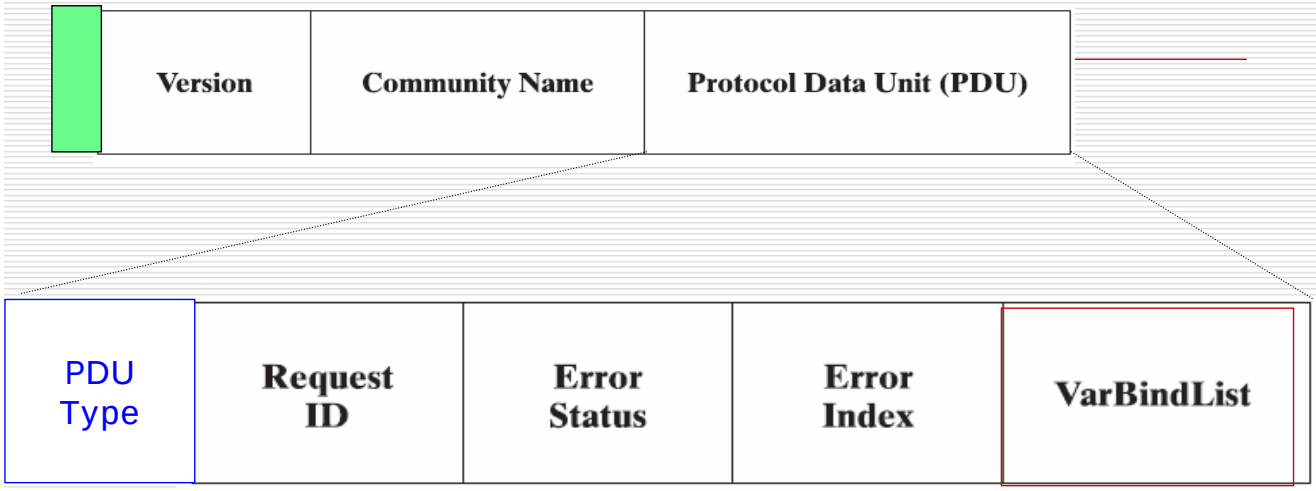
- SNMP封包包含：
  - 版本
  - 群體字串
  - SNMP指令
  - 傳送給TCP/IP協定堆疊傳輸層的一連串變數
- 傳輸層和較低的通訊層建立訊框標頭後，透過網路傳送訊框給管理代理者。

6.2 SNMPv1封包 p. 6-5 Fig. 6.2



- Version
  - 網路的管理站、以及管理代理者所使用的SNMP版本。
  - SNMP代表SNMPv1，版本欄位以“0”編碼表示SNMPv1。
- Community Name
  - 是SNMP的密碼。
  - 管理站及管理代理者必須使用相同的群體名稱，否則訊框會被棄置。
  - 管理站與管理代理者也必須使用相同的SNMP版本，否則訊框會被棄置。
  - SNMP的群體名稱沒有加密，所以沒有防止網路入侵的安全措施。SNMPv3則對此多所改良。

6.2 SNMPv1 PDU



- Request ID **p. 6-6 Fig. 6.3**
  - 整數，是管理站送到管理代理者的請求識別碼。
  - 管理代理者送出的回覆也使用此欄位，讓管理站的SNMP可以將請求及回覆建立關聯。

6.2 SNMP封包

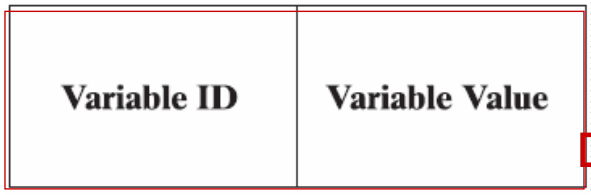
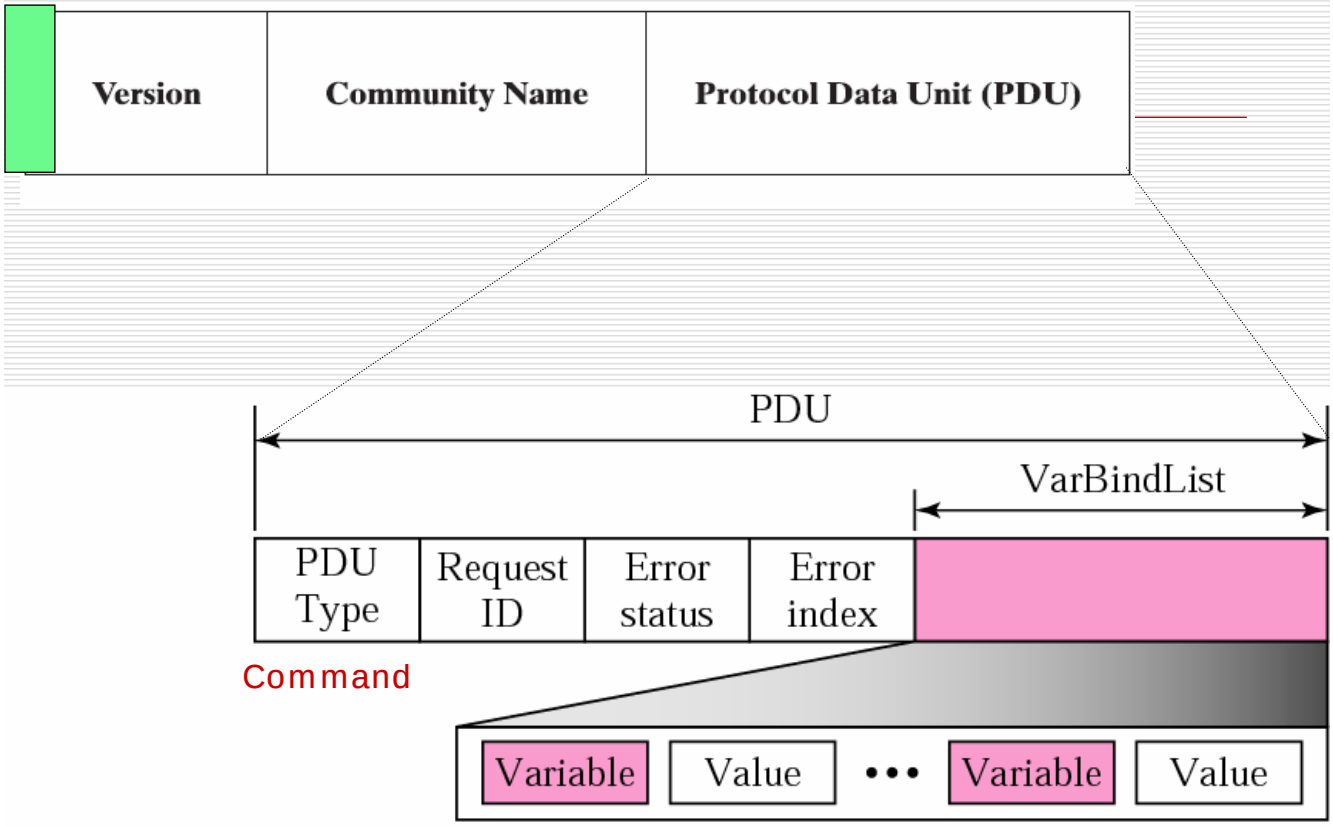


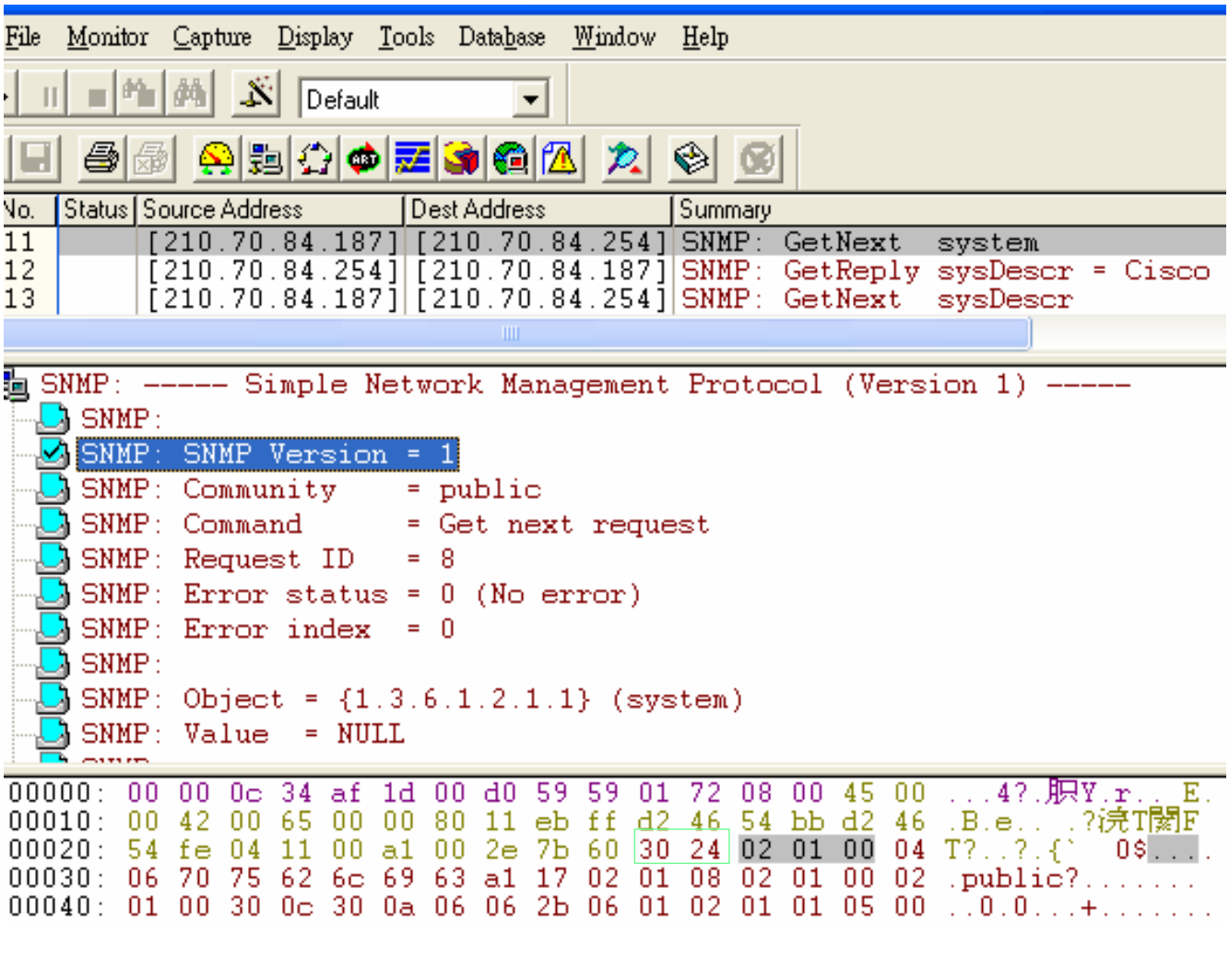
圖6.4 VarBindList 組合

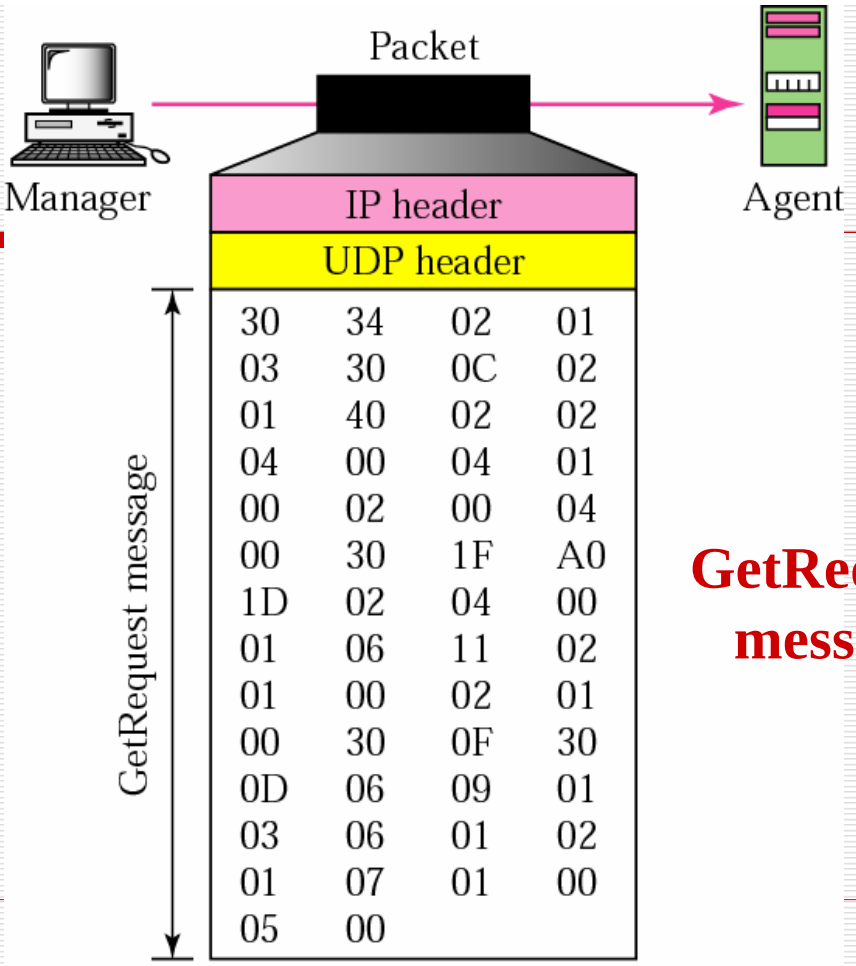
p. 6-7 Fig. 6.4

- Variable ID包含定義在管理資訊結構(SMI)規格中，變數的物件識別碼(OID)，物件識別碼則是定義MIB樹物件的路徑。
- Variable Value可能是整數、8進位字串或IP位址。
- 因爲管理站可以在一個請求封包中請求很多變數值，所以VarBindList可以包含若干欄位的組合。

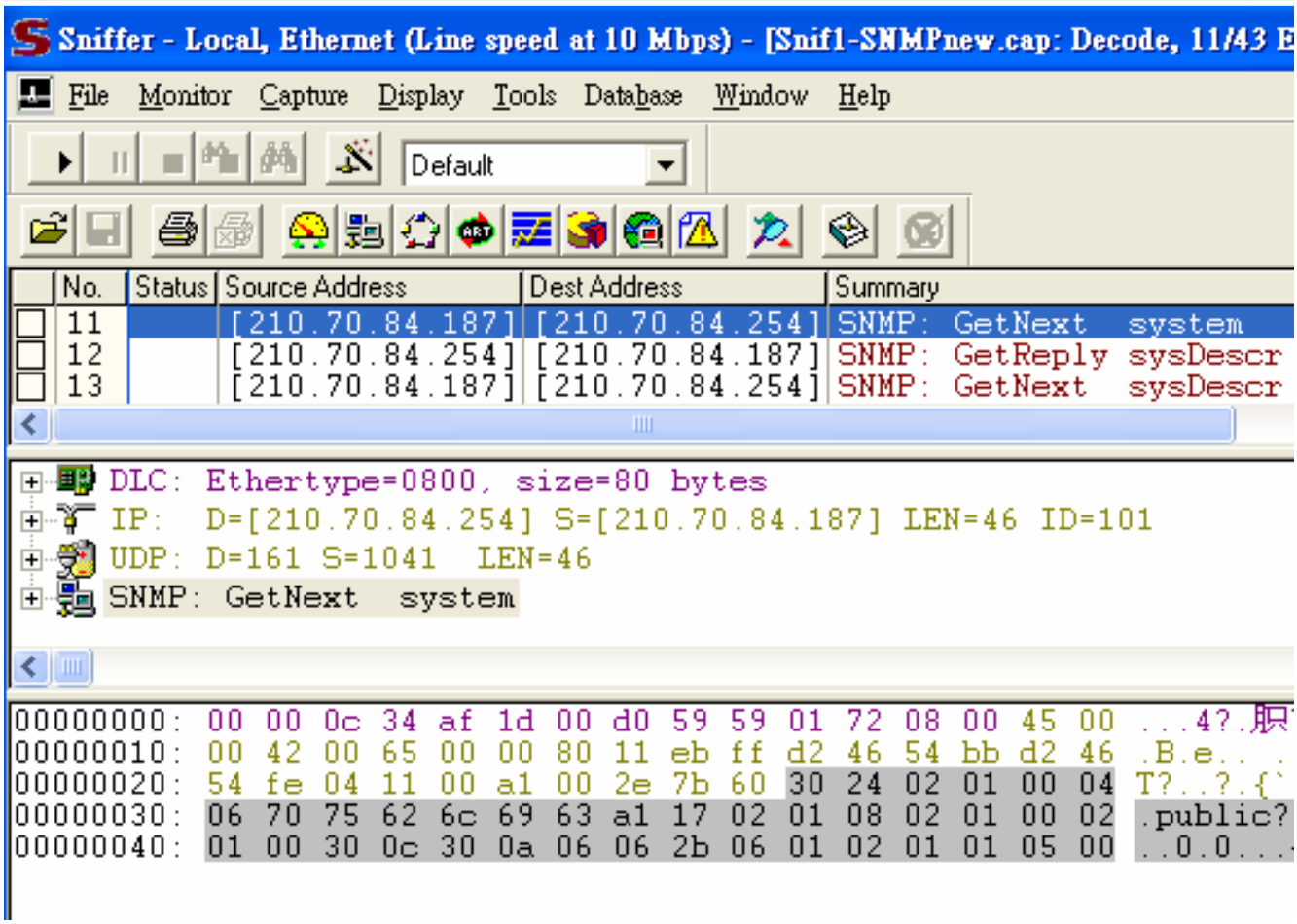
SNMP PDU format

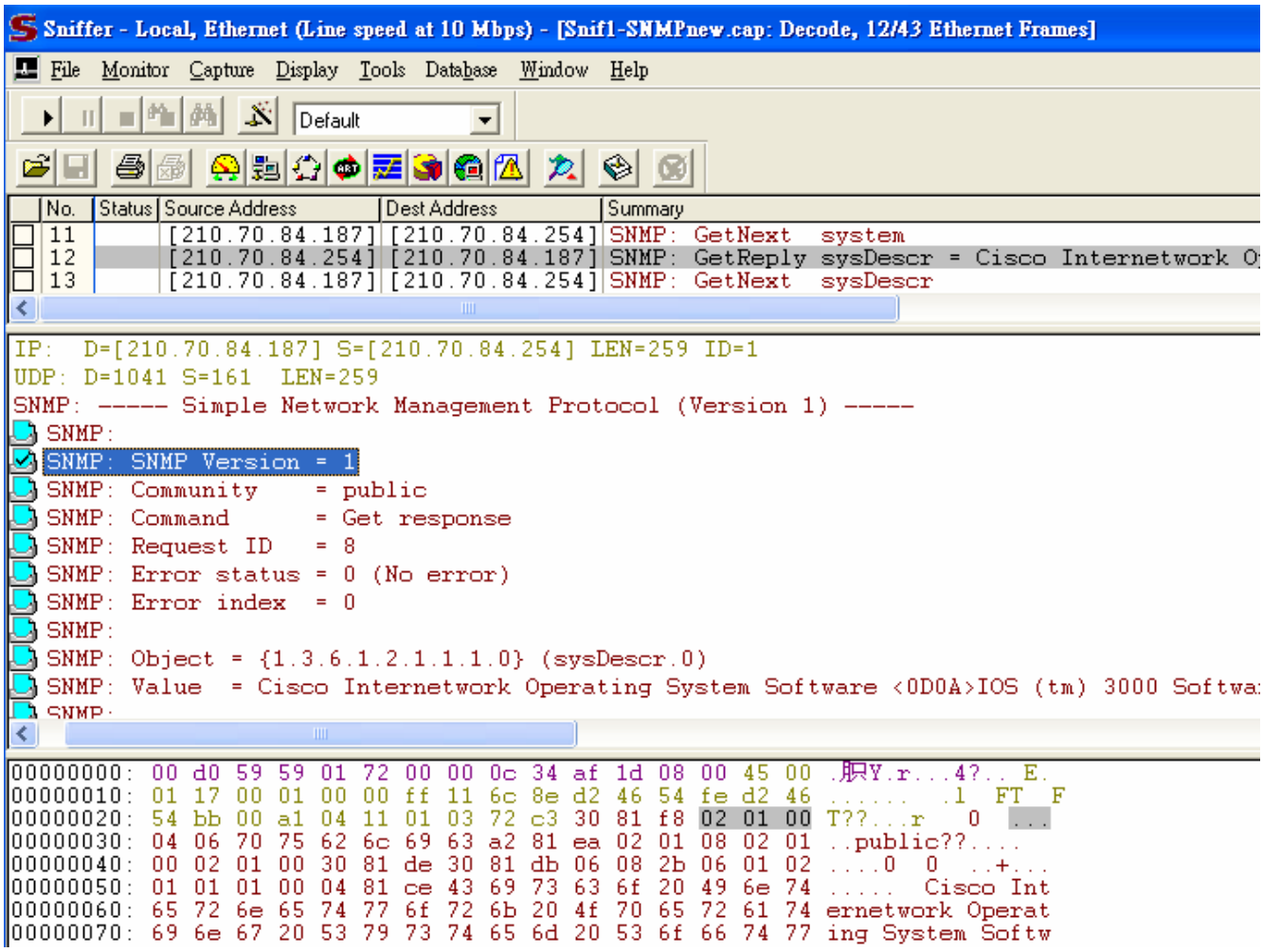






GetRequest message

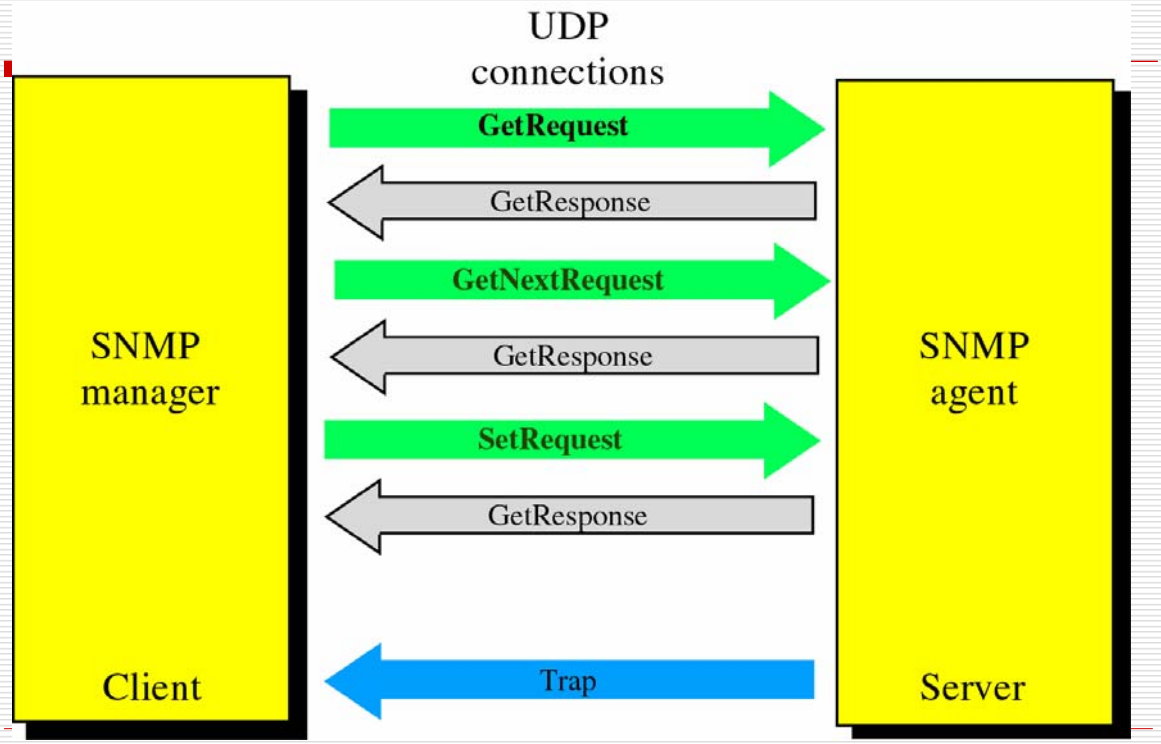




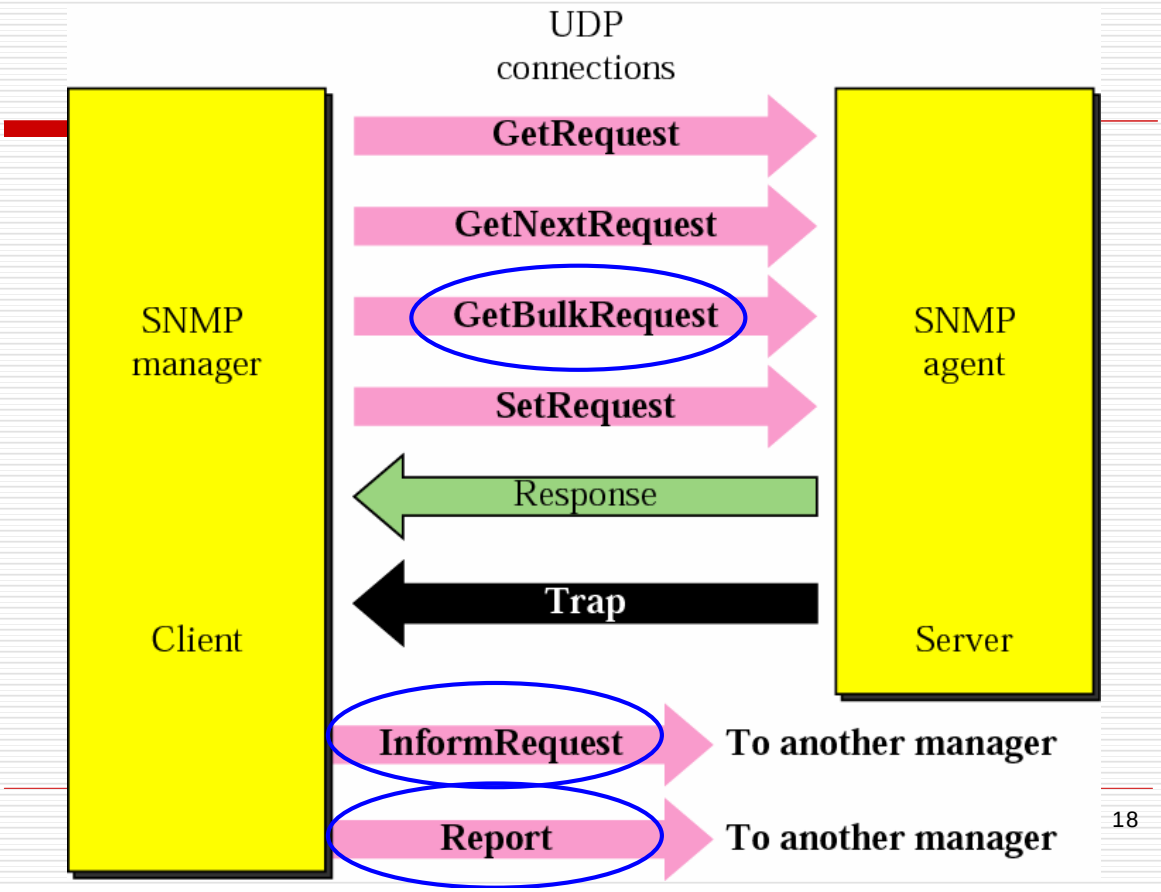
6.3 SNMP指令 p. 6-7

- SNMP定義有5種指令，括號中的數字有其相關的PDU種類。
  - Get-Request（0）：請求管理代理者的MIB，提供一個值或一組值。
  - Get-Next-Request（1）：請求提供MIB樹中，比現有的物件識別碼的詞彙順序更大的下一個物件識別碼值。管理站不斷使用這個指令後，可以“走”過全部的MIB樹，得到所有變數的值。
  - Get-Response（2）：代理者將請求值回覆給管理站
  - Set-Request（3）：設定（或更改）管理代理者MIB中的值，例如：在關閉設備時發出警告。
  - Trap（4）：管理代理者主動傳送給管理站的訊息。警告訊息由管理代理者的警報／事件組合（pair）來啓動。警告的目的是通知管理站，此時可能需要網路管理員採取行動的事件。

SNMPv1 Messages



SNMPv2 PDUs



6.3 SNMP Trap指令 p. 6-7

Enterprise	Agent Address	Generic Trap Number	Specific Trap Number	Time Stamp	VarBindList

圖6.5 SNMP Trap 的PDU

- Enterprise：包含物件的識別碼。該識別碼是由授權廠商爲發出警告訊息的設備子系統所定義。
- Agent Address：網路設備的IP位址。
- Generic Trap Number：以整數代表SNMP RFC 1157所定義7種警告。
- Specific Trap Number：代碼；管理站需爲設備建立專用MIB，以了解此碼含意。
- Time Stamp：設備代理者自啓動後的經過時間，精確度可達0.01秒。
- VarBindList：包含圖6.4中的全部或部份資訊，以及其他可以用來解決問題的資訊，例如：物件的識別碼、以及識別特定錯誤的相關值。

6.4 管理資訊結構 p. 6-8

- ASN.1界定了需定義物件的型別，並定義物件的格式。(**Appendix B**)
- 格式包括物件名稱、型別，例如：
  - 其中無論管理站是否可以存取；
  - 若可存取，其型別就可能是唯讀、可讀-寫、或不可存取。
- RFC 1155（管理訊息結構）介紹定義MIB的語言，而SMI規範如何在TCP/IP網路上管理資訊。
- SMI使用部分的ASN.1來正式定義MIB物件。

SMI Object Tree (p. 6-9)

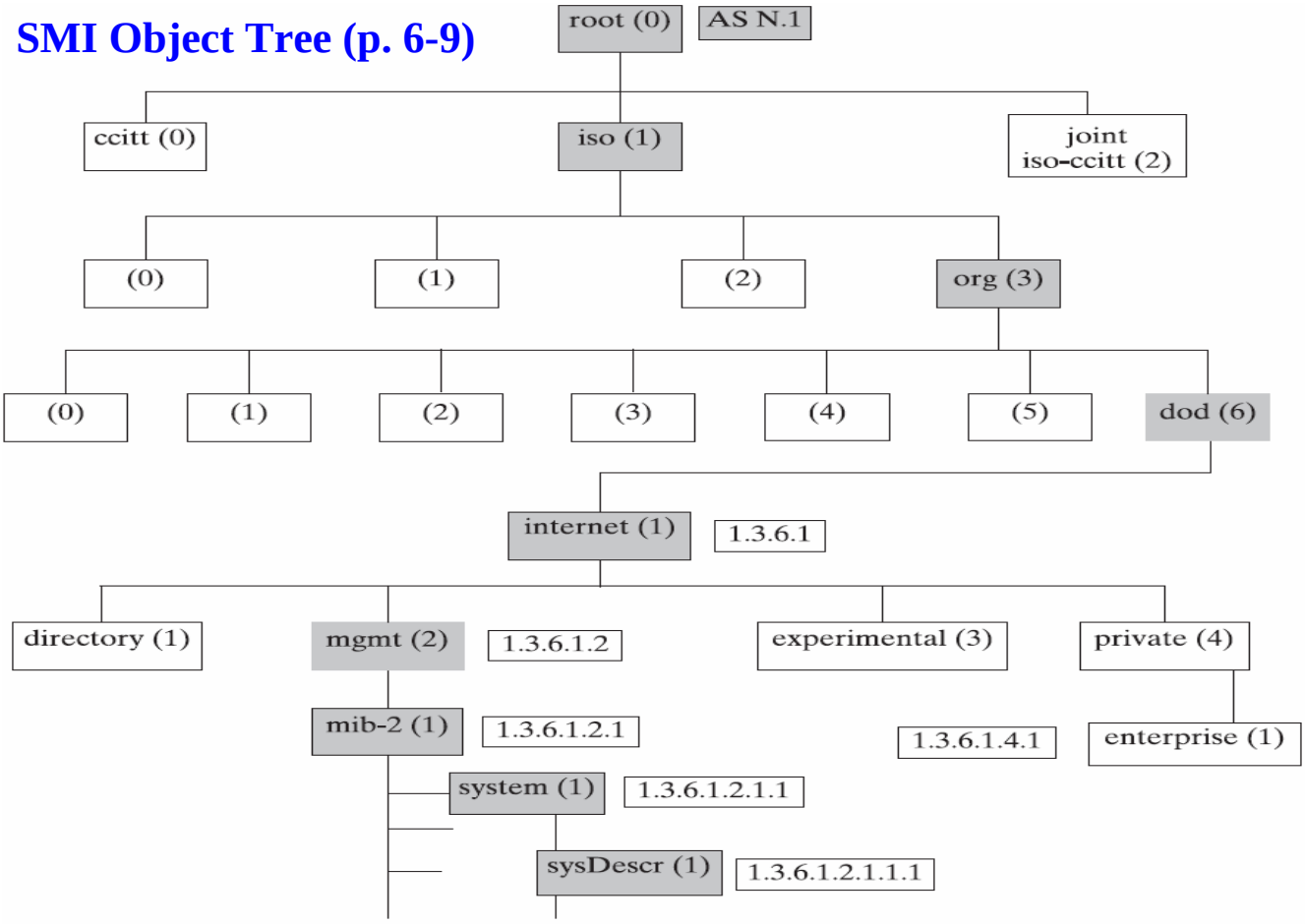
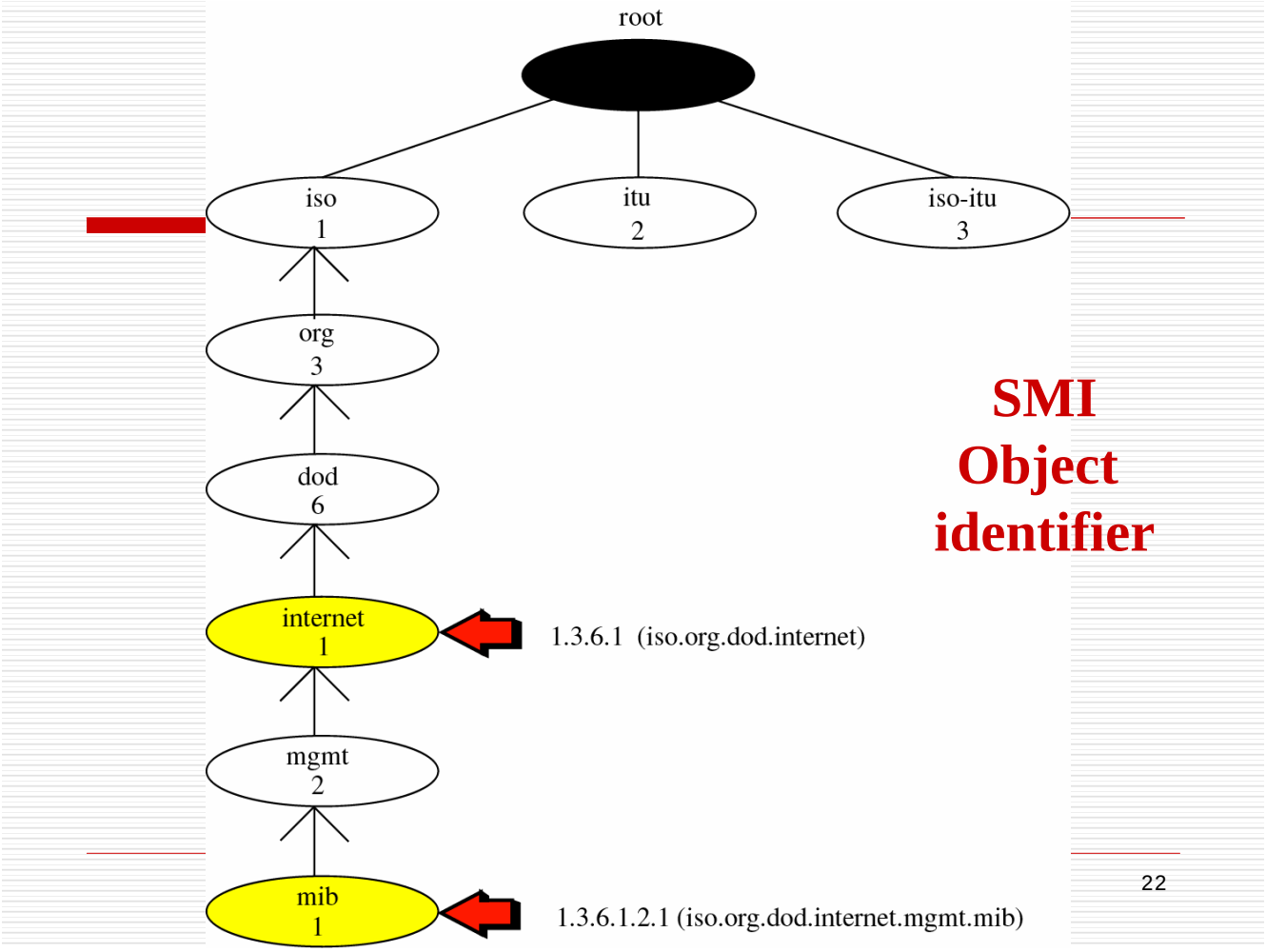
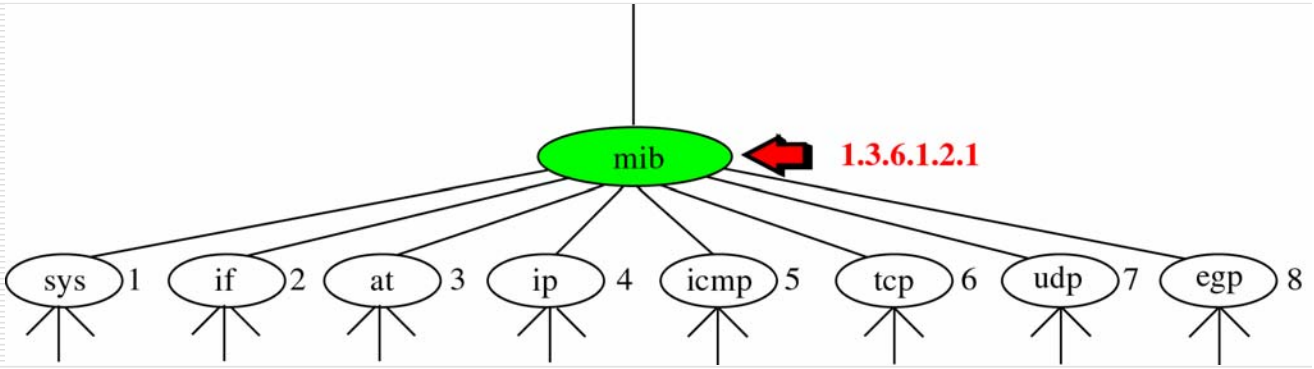


圖6.6　管理資訊結構（SMI）的MIB

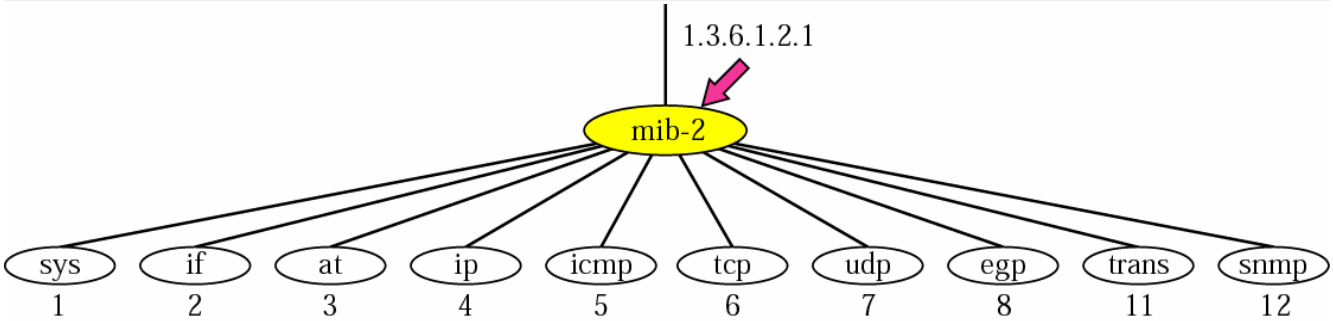


SMI Object identifier

MIB


mib
1.3.6.1.2.1
sys 1
if 2
at 3
ip 4
icmp 5
tcp 6
udp 7
egp 8

MIB-II

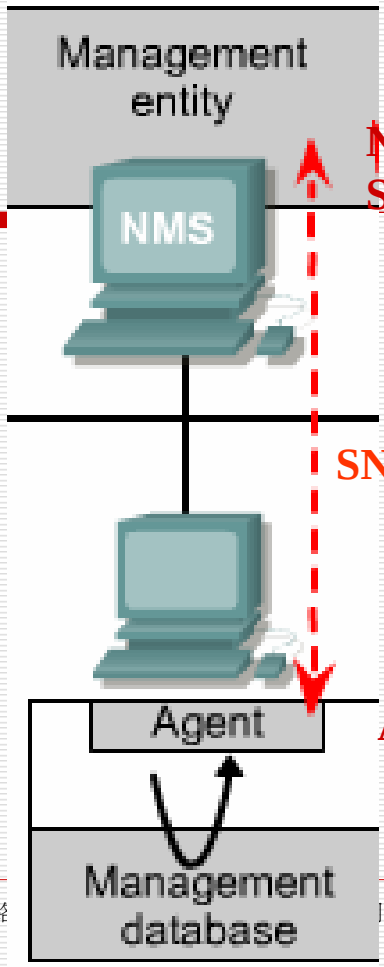

1.3.6.1.2.1
mib-2
sys 1
if 2
at 3
ip 4
icmp 5
tcp 6
udp 7
egp 8
trans 11
snmp 12

MIB – Management Information Base

- 定義網路設備各種資訊的儲存結構
  - Name (OID)
  - Type and syntax
  - encoding
- MIB-II
  - 所有網路設備皆提供的MIB標準
  - 各家廠商也會提供proprietary MIB

6.4 管理資訊結構 p. 6-10

- MIB-2原本包括10個群組：系統、介面、位址翻譯（at）、網際網路協定（ip）、網際網路控制管理協定（icmp）、傳輸控制協定（tcp）、不可靠資料片協定（udp）、外部閘道協定（egp）、傳輸、及簡易網路管理協定（snmp）。
- 後來又新增了13個群組，稱爲延伸。是由遠端監視（RMON）標準所提供。RMON的物件包含網路區段的流量資訊。
- MIB-2的物件無法滿足所有使用者及廠商的需求。所以很多廠商爲其設備建立專用的MIB。
- 這些MIB列在Enterprise節點之下。如圖6.6所示，Enterprise節點是private(4)節點的子節點。
- 在使用者取得廠商提供的MIB後，會編譯該物件並載入管理站中，以存取設備中的更多物件。



Network Management System

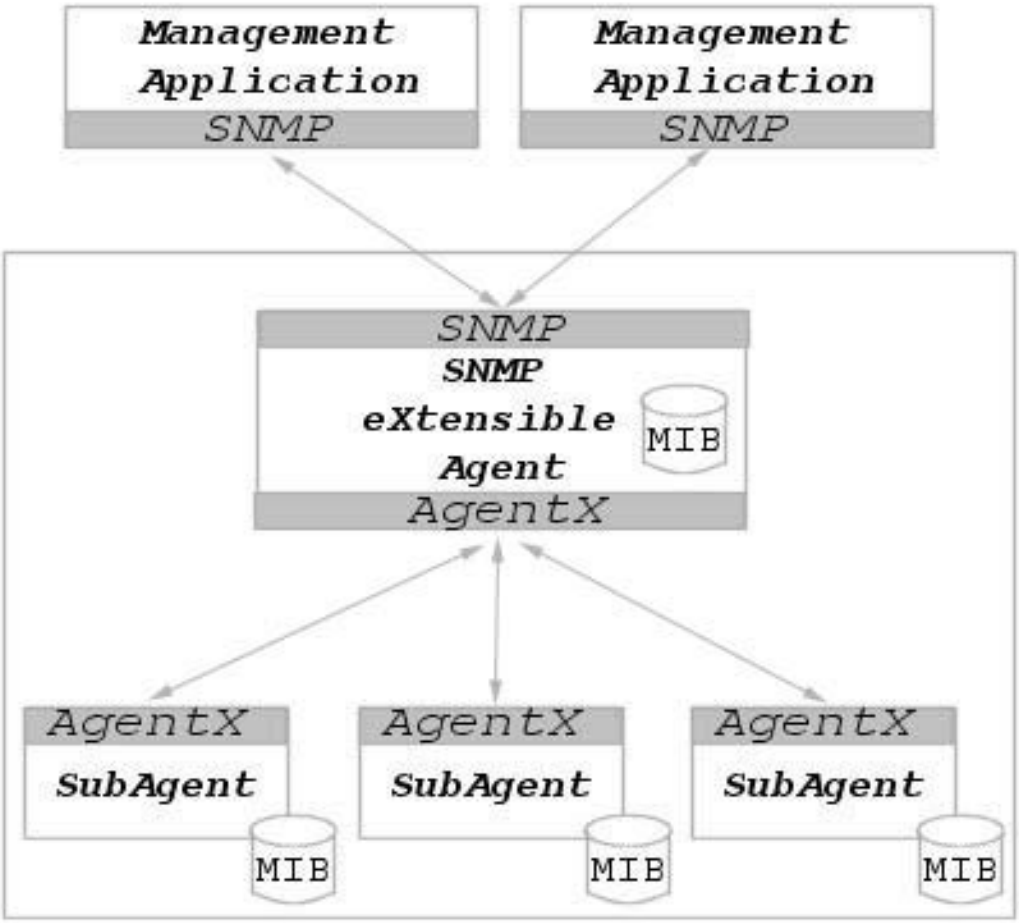
SNMP

Agent

MIB

Picture sources by Cisco Systems, Inc.

2741 Agent Extensibility (AgentX) Protocol Version 1 (Obsoletes: 2257)



p. 6-11

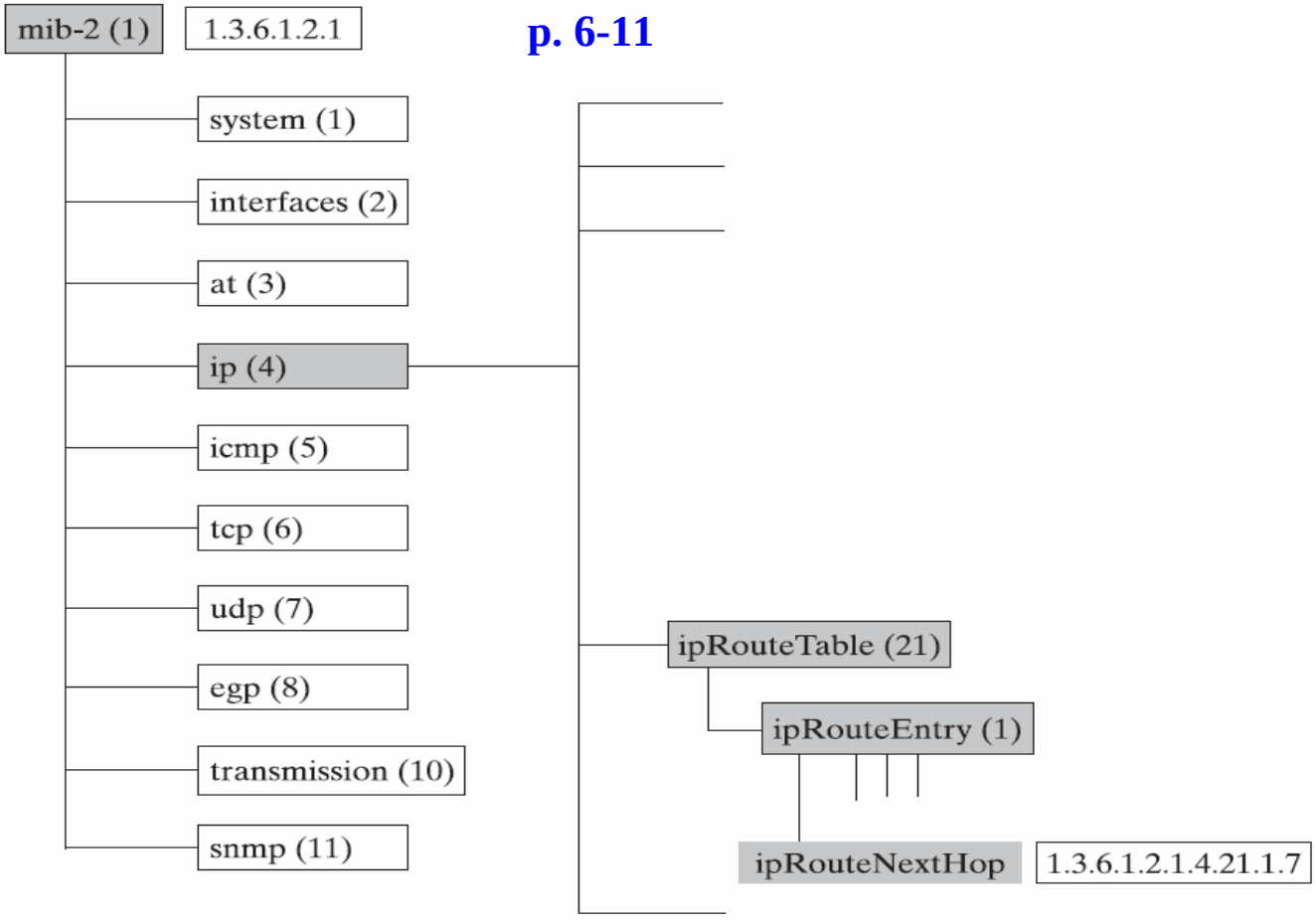


圖 6.7　mib-2 物件（左邊）以及 ip(4) 物件（右邊）

p. 6-19

6.6　安全- 1. authentication（認證）

- 在SNMP中，authentication（認證）爲安全保護的第一道防線。
- **community** name認證管理站及代理者之間的訊息。
- 接收器的資料庫中必須有傳送器使用的community name ，否則訊息將會棄置。
- 數個管理站可以存取一個管理代理者的訊息。同理，一個管理代理者可傳送警告訊息給數個管理站。

p. 6-19

6.6 安全- 2. authorization（授權）

- authorization（授權）爲安全保護提供有第二道防線。授權決定管理站對於MIB物件的使用權限。
- SNMP access mode（SNMP存取模式）決定一組權限。管理代理者爲MIB物件選擇唯讀或讀-寫存取模式。
- 另一組權限是由MIB view指定所決定。MIB view是一組MIB物件，可以限制管理站使用SNMP存取模來存取物件。
- SNMP community profile定義爲SNMP存取模式及MIBview的組合。
- **SNMP access policy**定義爲**SNMP Community**及SNMP Community Profile的組合。

p. 6-19 管理代理者必須維護SNMP 存取政策表(Access Policy)

表6.2 SNMP 的安全參數

Authentication	Authorization (Rights)	MIB Access
• Community Name	• SNMP Access Mode ❑ Read-Only ❑ Read-Write	• read-only • read-write • write-only • not-accessible
	• MIB View ❑ Object ❑ Object 2 • • ❑ Object N	

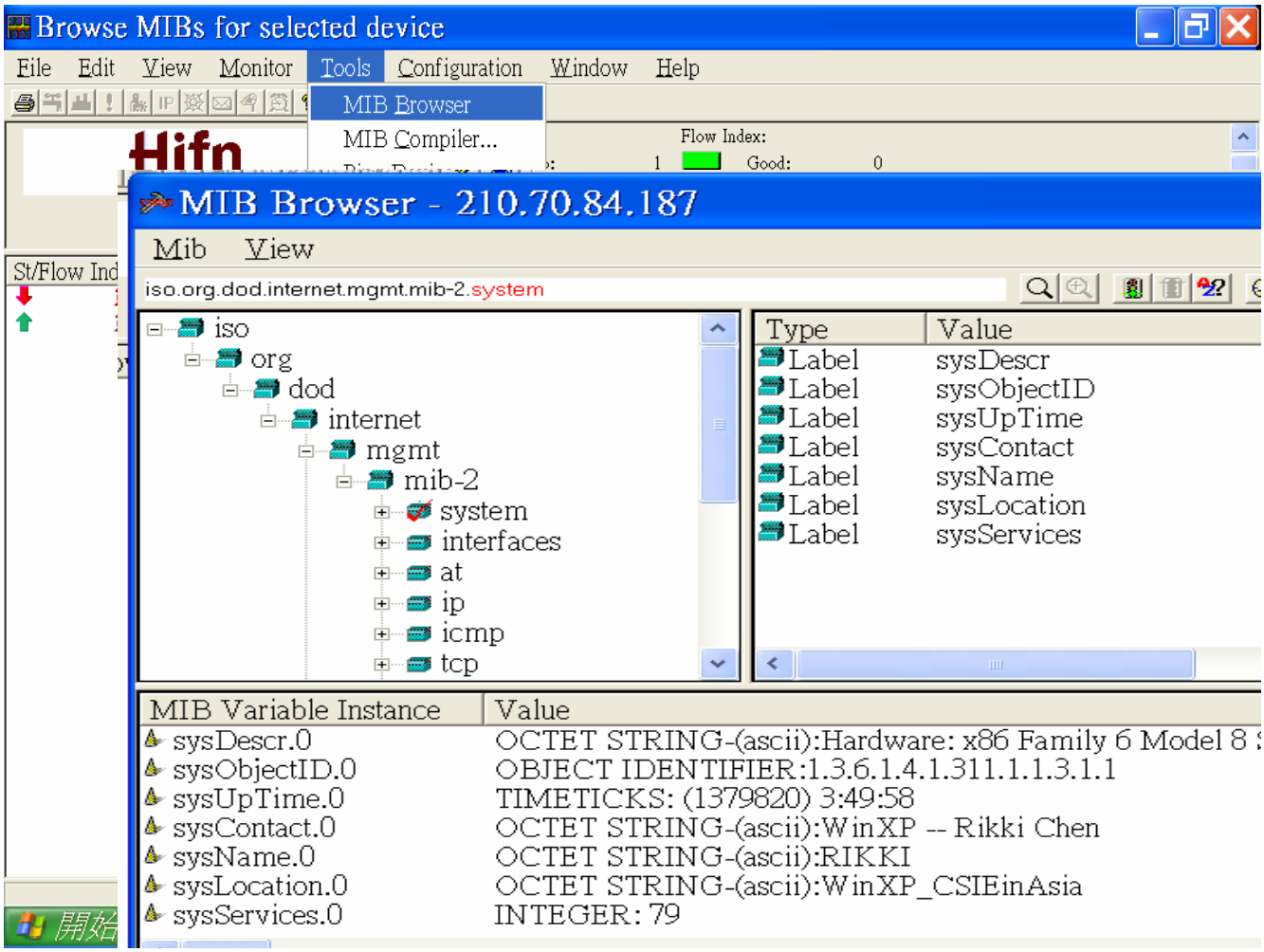
SNMP Community Profile = MIB View + SNMP Access Mode

SNMP Access Policy = SNMP Community + SNMP Community Profile

6.7 SNMP NMS應用程式- Hifn Analyzer

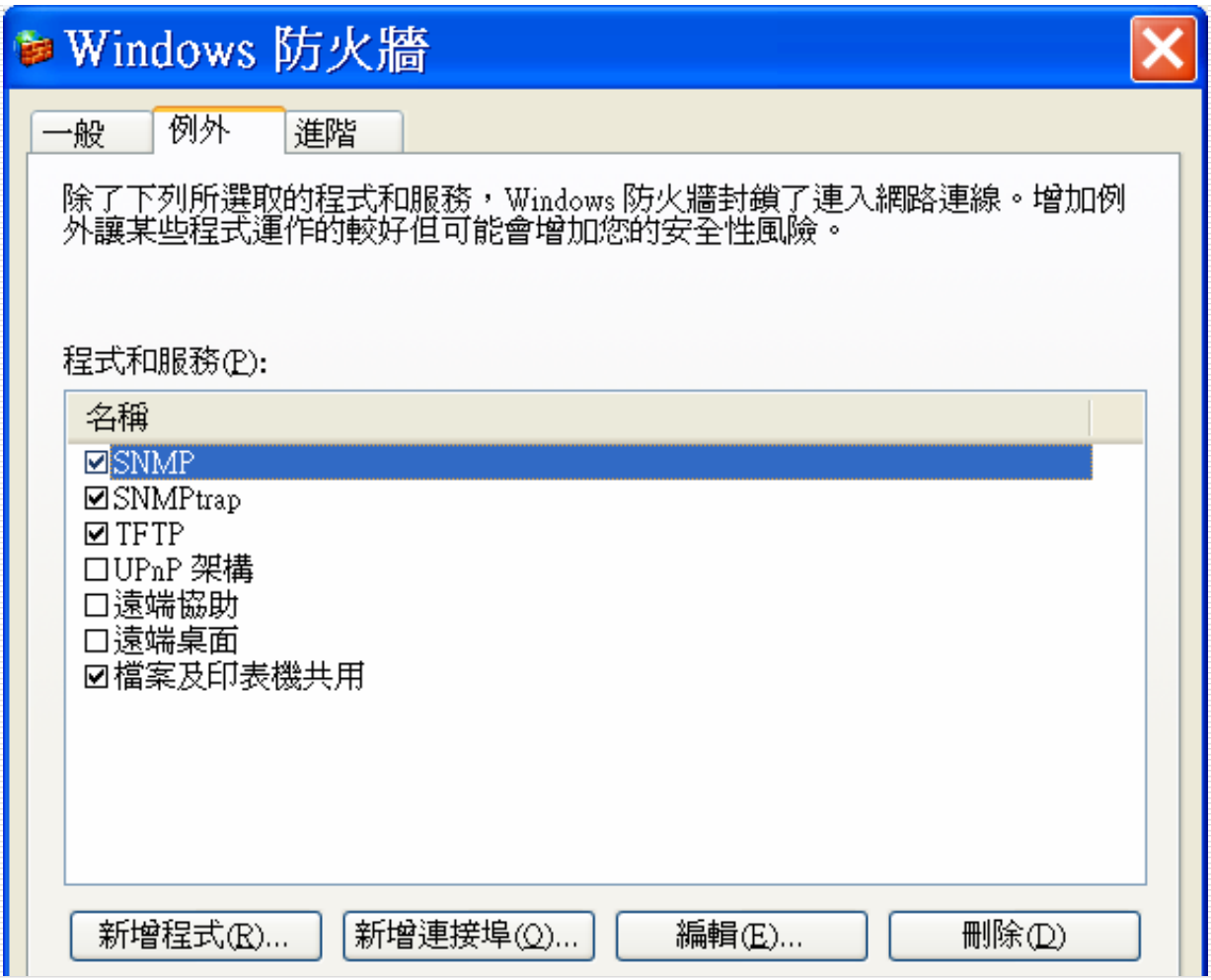
- 大多數NMS都包含瀏覽MIB的應用程式。這個程式提供MIB的圖形化外觀，可以輕易地清楚顯示回覆的物件值。
- 反白顯示物件後，再點選“Get”按鈕，就可以建立“Get-Request”或“Get-Next-Request”指令。
- “Set”按鈕可以更改MIB物件值。

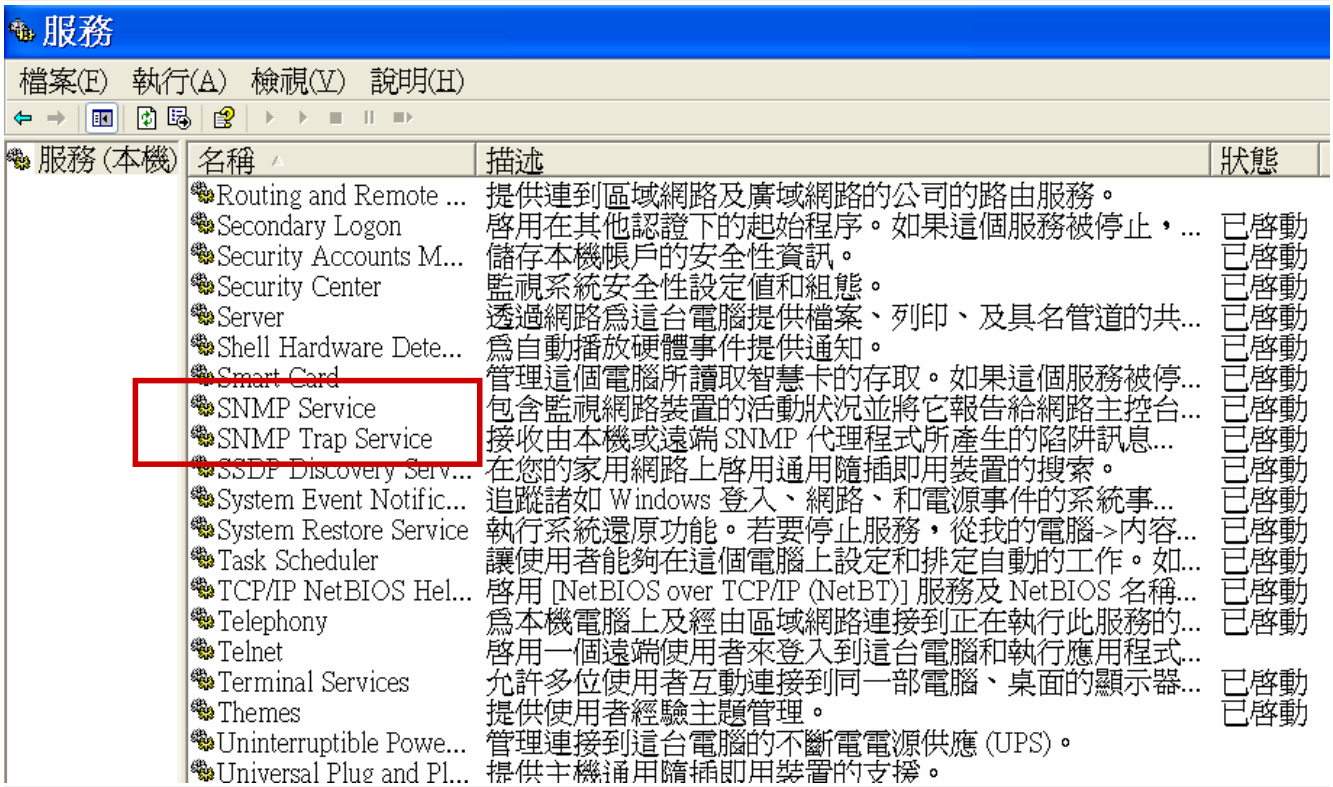

Hifn Analyzer
File Edit View Monitor Tools Configuration Window Help
Hifn
Intelligent Secure Networking
Summary Information
Status:
Up: 1
Down: 1
Unknown: 0
Flow Index:
Good: 0
Fair: 0
Poor: 0
St/Flow Index/Alarm Name IP Address Media Type SNMP Lvl Type Status
CiscoRouter * 210.70.84.254 Ethernet * MIB II Router Down/Trap
WinXP * 210.70.84.187 Unknown * MIB II Other Up/Trap

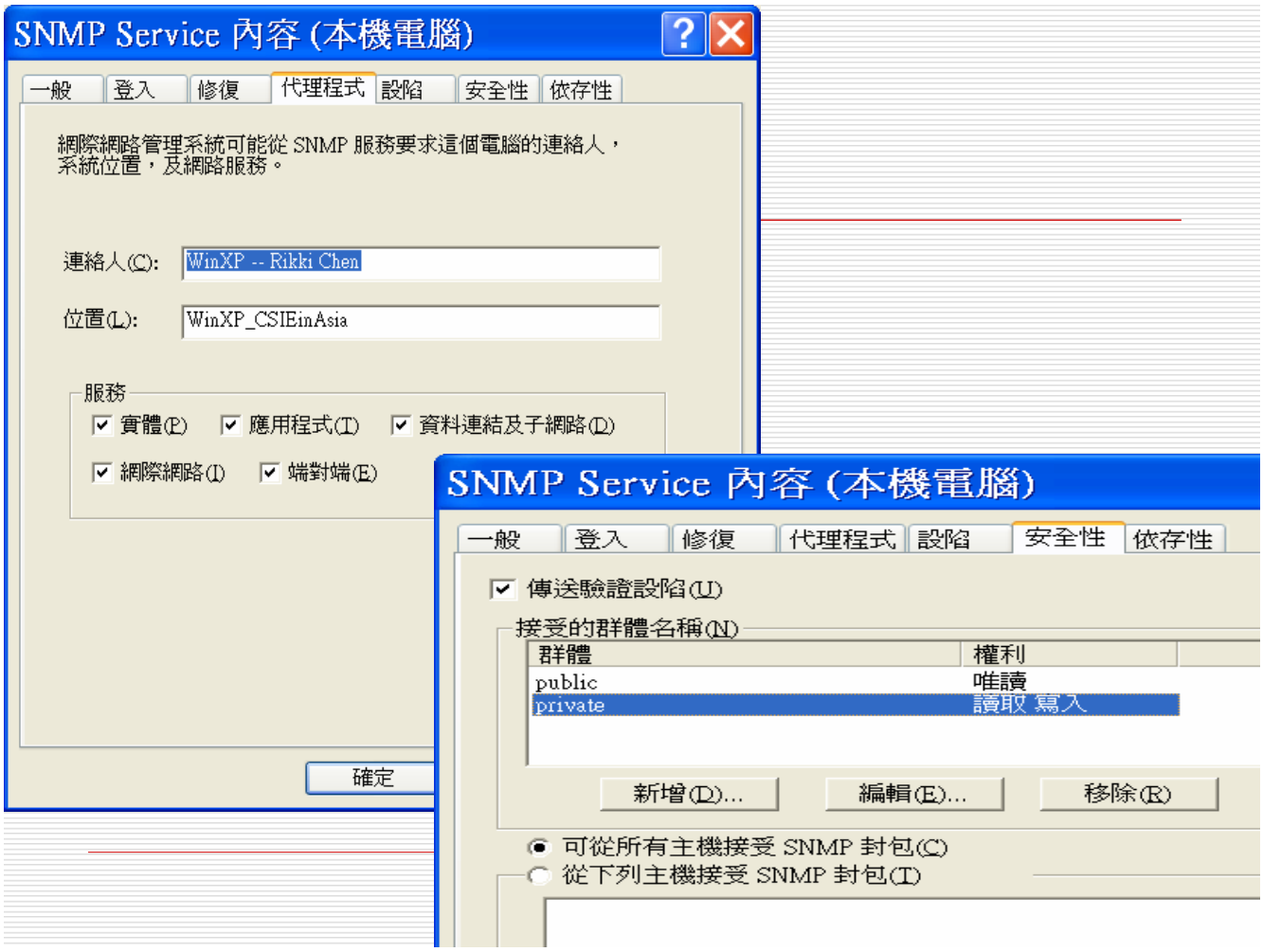

Browse MIBs for selected device
File Edit View Monitor Tools Configuration Window Help
MIB Browser
MIB Compiler...
MIB Browser - 210.70.84.187
Mib View
iso.org.dod.internet.mgmt.mib-2.system
iso
org
dod
internet
mgmt
mib-2
system
interfaces
at
ip
icmp
tcp
Type Value
Label sysDescr
Label sysObjectID
Label sysUpTime
Label sysContact
Label sysName
Label sysLocation
Label sysServices
MIB Variable Instance Value
sysDescr.0 OCTET STRING-(ascii):Hardware: x86 Family 6 Model 8
sysObjectID.0 OBJECT IDENTIFIER:1.3.6.1.4.1.311.1.1.3.1.1
sysUpTime.0 TIMETICKS: (1379820) 3:49:58
sysContact.0 OCTET STRING-(ascii):WinXP -- Rikki Chen
sysName.0 OCTET STRING-(ascii):RIKKI
sysLocation.0 OCTET STRING-(ascii):WinXP_CSIEinAsia
sysServices.0 INTEGER: 79

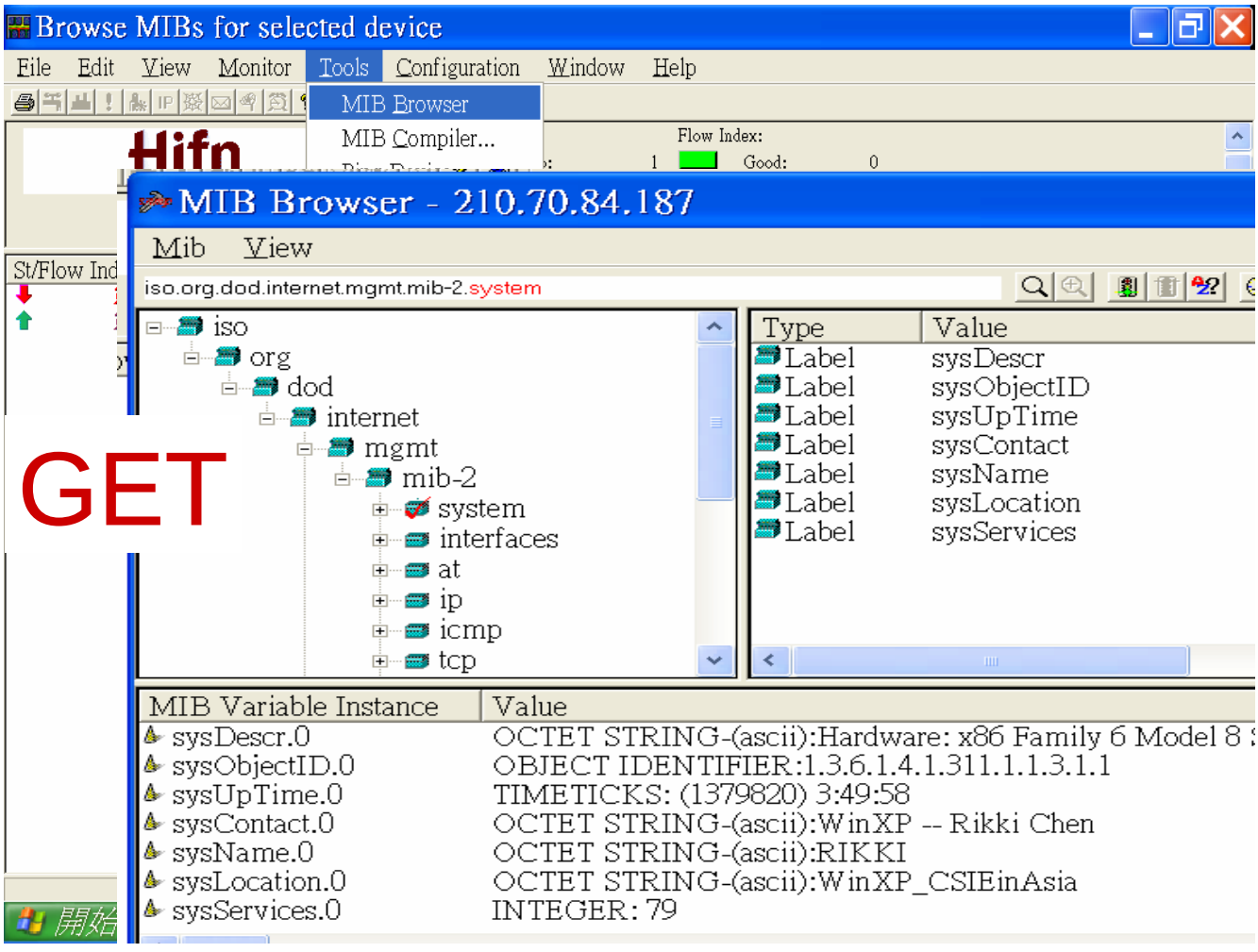
SNMP for Windows XP

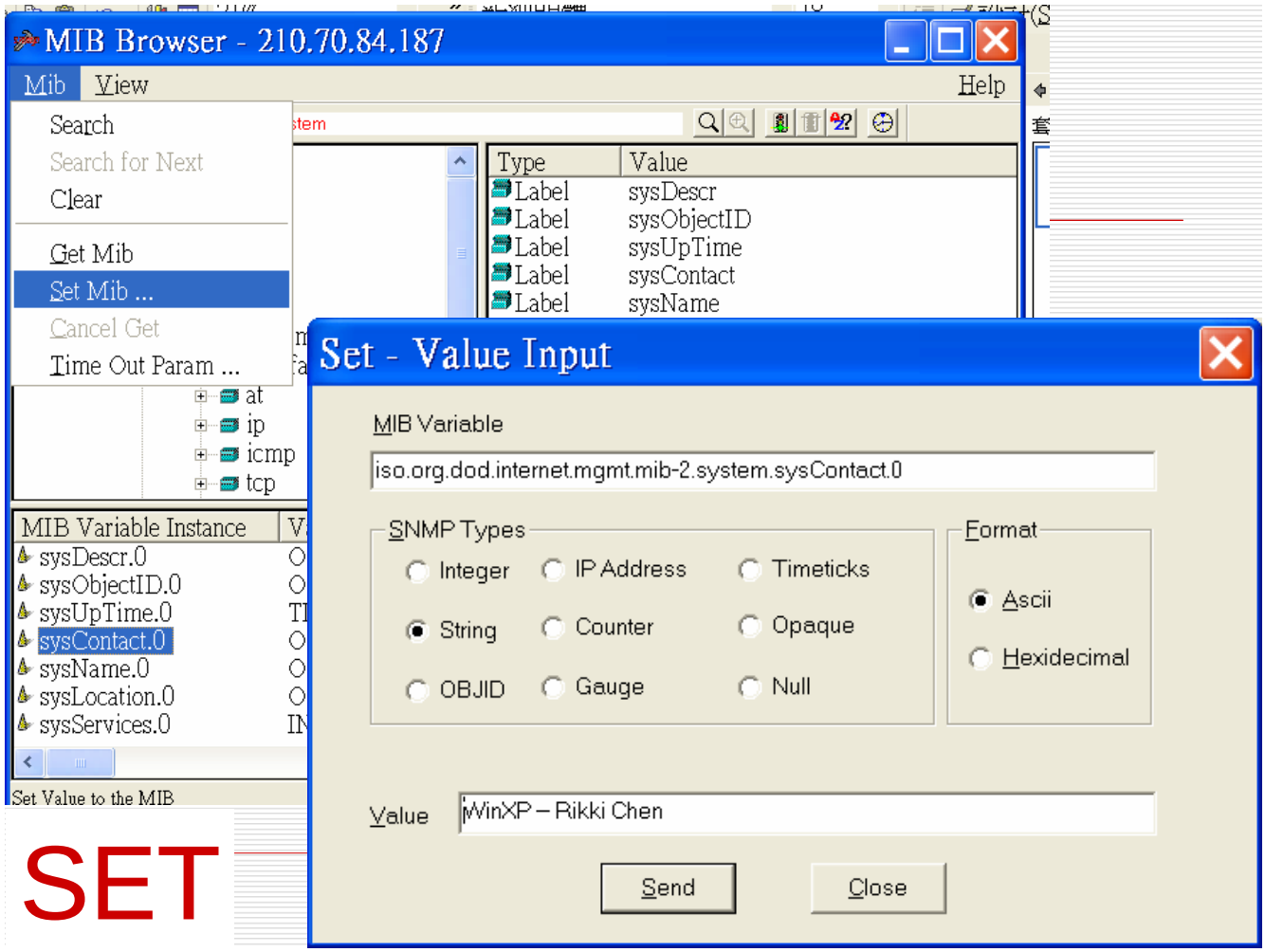
- 安裝 SNMP 服務
  - [開始]、[控制台]、[新增或移除程式] 及 [新增/移除 Windows 元件]➔開啓 [Windows 元件精靈]。
  - 在 [元件] 中按一下 [Management and Monitoring Tools] (但不選取或清除其核取方塊)，再按 [詳細資料]。
  - 選取 [Simple Network Management Protocol] 核取方塊，再按一下 [確定]。
- 必須以系統管理員或 Administrators 群組的成員身分登入，才能完成這項程序。
- 如果電腦已連線到網路，則網路原則設定值也可能會讓您無法完成這項程序。
- SNMP 會在安裝之後自動啓動。


Windows 防火牆
一般
例外
進階
除了下列所選取的程式和服務，Windows 防火牆封鎖了連入網路連線。增加例外讓某些程式運作的較好但可能會增加您的安全性風險。
程式和服務(P):
名稱
SNMP
SNMPtrap
TFTP
UPnP 架構
遠端協助
遠端桌面
檔案及印表機共用
新增程式(R)...
新增連接埠(O)...
編輯(E)...
刪除(D)


服務
檔案(F) 執行(A) 檢視(V) 說明(H)
服務 (本機)
名稱
描述
狀態
Routing and Remote ... 提供連到區域網路及廣域網路的公司的路由服務。
Secondary Logon 啓用在其他認證下的起始程序。如果這個服務被停止，... 已啓動
Security Accounts M... 儲存本機帳戶的安全性資訊。 已啓動
Security Center 監視系統安全性設定值和組態。 已啓動
Server 透過網路爲這台電腦提供檔案、列印、及具名管道的共... 已啓動
Shell Hardware Dete... 爲自動播放硬體事件提供通知。 已啓動
Smart Card 管理這個電腦所讀取智慧卡的存取。如果這個服務被停... 已啓動
SNMP Service 包含監視網路裝置的活動狀況並將它報告給網路主控台... 已啓動
SNMP Trap Service 接收由本機或遠端 SNMP 代理程式所產生的陷阱訊息... 已啓動
SSDP Discovery Serv... 在您的家用網路上啓用通用隨插即用裝置的搜索。 已啓動
System Event Notific... 追蹤諸如 Windows 登入、網路、和電源事件的系統事... 已啓動
System Restore Service 執行系統還原功能。若要停止服務，從我的電腦->內容... 已啓動
Task Scheduler 讓使用者能夠在這個電腦上設定和排定自動的工作。如... 已啓動
TCP/IP NetBIOS Hel... 啓用 [NetBIOS over TCP/IP (NetBT)] 服務及 NetBIOS 名稱... 已啓動
Telephony 爲本機電腦上及經由區域網路連接到正在執行此服務的... 已啓動
Telnet 啓用一個遠端使用者來登入到這台電腦和執行應用程式...
Terminal Services 允許多位使用者互動連接到同一部電腦、桌面的顯示器... 已啓動
Themes 提供使用者經驗主題管理。 已啓動
Uninterruptible Powe... 管理連接到這台電腦的不斷電電源供應 (UPS)。
Universal Plug and Pl... 提供主機通用隨插即用裝置的支援。


SNMP Service 內容 (本機電腦)
一般
登入
修復
代理程式
設陷
安全性
依存性
網際網路管理系統可能從 SNMP 服務要求這個電腦的連絡人，系統位置，及網路服務。
連絡人(C):
WinXP -- Rikki Chen
位置(L):
WinXP_CSIEinAsia
服務
實體(P)
應用程式(T)
資料連結及子網路(D)
網際網路(I)
端對端(E)
確定
SNMP Service 內容 (本機電腦)
一般
登入
修復
代理程式
設陷
安全性
依存性
傳送驗證設陷(U)
接受的群體名稱(N)
群體
權利
public
唯讀
private
讀取 寫入
新增(D)...
編輯(E)...
移除(R)
可從所有主機接受 SNMP 封包(C)
從下列主機接受 SNMP 封包(T)

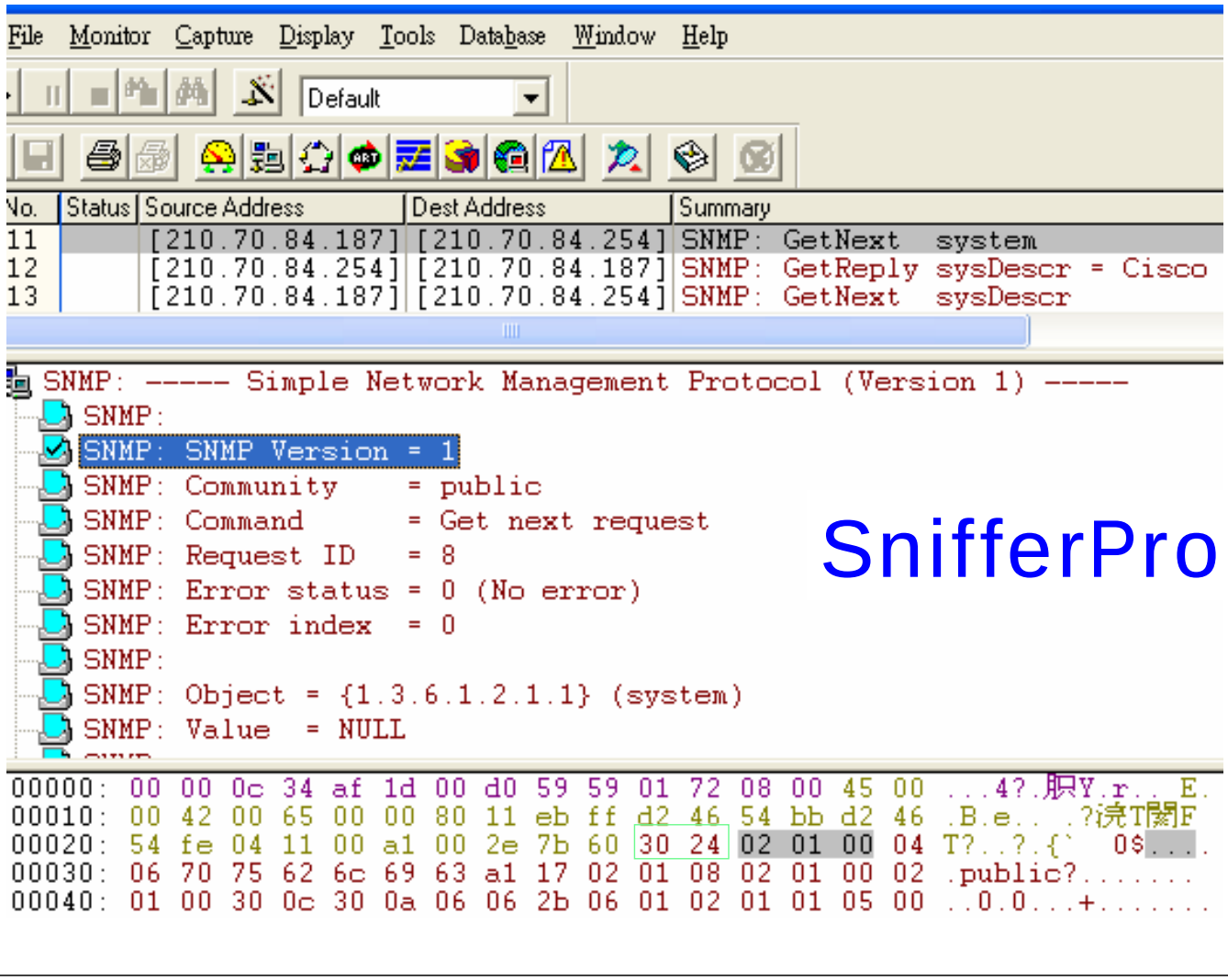

Browse MIBs for selected device
File
Edit
View
Monitor
Tools
Configuration
Window
Help
MIB Browser
MIB Compiler...
Flow Index:
Good:
0
Hifn
MIB Browser - 210.70.84.187
Mib
View
iso.org.dod.internet.mgmt.mib-2.system
iso
org
dod
internet
mgmt
mib-2
system
interfaces
at
ip
icmp
tcp
Type
Value
Label
sysDescr
Label
sysObjectID
Label
sysUpTime
Label
sysContact
Label
sysName
Label
sysLocation
Label
sysServices
GET
MIB Variable Instance
Value
sysDescr.0
OCTET STRING-(ascii):Hardware: x86 Family 6 Model 8
sysObjectID.0
OBJECT IDENTIFIER:1.3.6.1.4.1.311.1.1.3.1.1
sysUpTime.0
TIMETICKS: (1379820) 3:49:58
sysContact.0
OCTET STRING-(ascii):WinXP -- Rikki Chen
sysName.0
OCTET STRING-(ascii):RIKKI
sysLocation.0
OCTET STRING-(ascii):WinXP_CSIEinAsia
sysServices.0
INTEGER: 79



p. 6-22

6.8 SNMP訊息的捕捉

- 封包有三種型別：IP、UDP及SNMP。
- SNMP使用UDP做爲傳輸層協定，以減少管理訊框的經常成本。
- 表6.4列出“Get-Next-Request”訊息的解碼以供比較，這些資料也顯示在圖6.13的SNMP部份，其中的欄位則如圖6.2及圖6.3所示。



SnifferPro

p. 6-23 p. 6-24 Fig. 6.13

Meterware

6.8 SNMP訊息的捕捉

表6.4 圖6.2 及圖6.3 ，與圖 6.13 的SNMP 訊息解碼的比較

圖6.2 及6.3	圖6.13 的SNMP 訊息解碼
SNMP Version	0
Community String	public
PDU Tag*	GetNextRequest (161)
Request ID	3891
Error Status	No Error (0)
Error Index	0
VarBindList	sysName/Null 0

* 圖6.13 標示的PDU Type

p. 6-23　　p. 6-25 Fig. 6.14

6.8　SNMP訊息的捕捉

表6.5　圖6.2 及圖6.3 ，與圖 6.14 的SNMP 訊息解碼的比較

圖6.2 及6.3	圖6.14 的SNMP 訊息解碼
SNMP Version	0
Community String	public
PDU Tag*	Get-Response(162)
Request ID	3891
Error Status	No Error (0)
Error Index	0
VarBindList	sysName.0/SERVER

* 圖6.14 標示的PDU Type

結論

- Question?
- Thank you!