第3章 网络管理协议

本章学习目标

- 理解网络管理协议的作用
- 掌握SNMP协议的基本概念
- 了解WBM管理技术
- 了解公共管理协议

网络管理的标准化

- 如果每个厂商的网络设备都提供一套自己独特的网管方法和界面，网络管理的工作将很难进行。
- 网络管理的标准化
  - 每个的网络设备必须提供一致的网络管理的界面 (亦即相同的网络管理通信协议)。

3.1 简单网络管理协议(SNMP)

- SNMP:
  - Simple Network Management Protocol
  - 是管理TCP/IP 网络 (Internet)的事实上的标准
  - 所有TCP/IP网络设备都应该支持SNMP.

3.1 简单网络管理协议

3.1.1 SNMP的发展

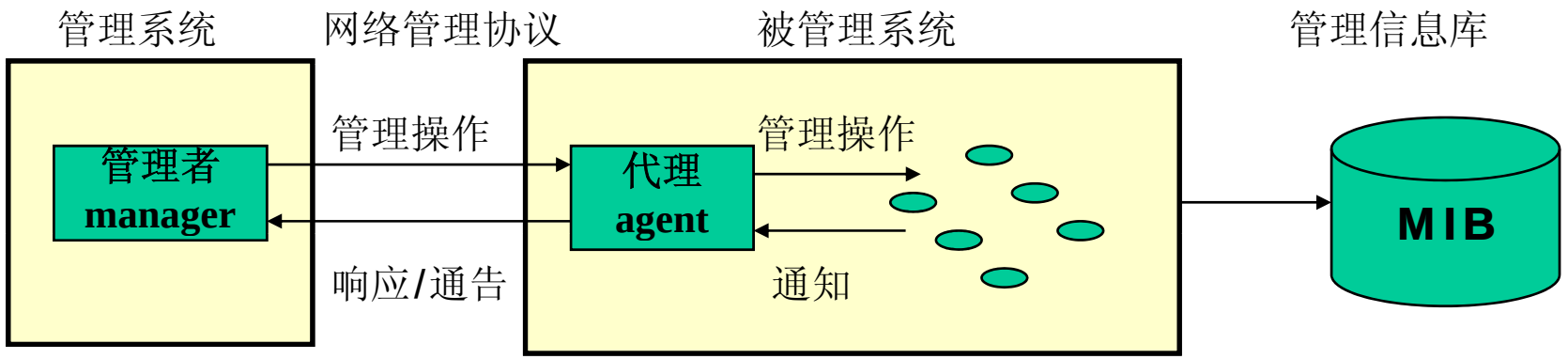
1. SNMP的发展

- 在TCP/IP的早期开发中，网络管理问题并未得到足够的重视，直到上世纪80后期，人们才意识到需要开发功能更强，并易于普通网络管理人员学习和使用的标准协议。
- 1987年11月发布的SGMP，成为提供专用网络管理工具的起点。
- 1988年，IAB确定了将SNMP作为近期解决方案进一步开发.
- 1992年7月发表了3个增强SNMP安全性的文件作为建议标准。 1993年安全版SNMPv2发布。
- 1996年SNMPv2的安全特性被取消了，报文格式也重新采用SNMPv1的基于“共同体(community)”概念的格式
- 1999年4月IETF SNMPv3工作组提出了RFC2571～RFC2576，形成了SNMPv3的建议。

2． SNMP的体系结构

1）网络管理体系结构

SNMP的网络管理模型包括以下关键元素：管理站、代理者、管理信息库、网络管理协议。

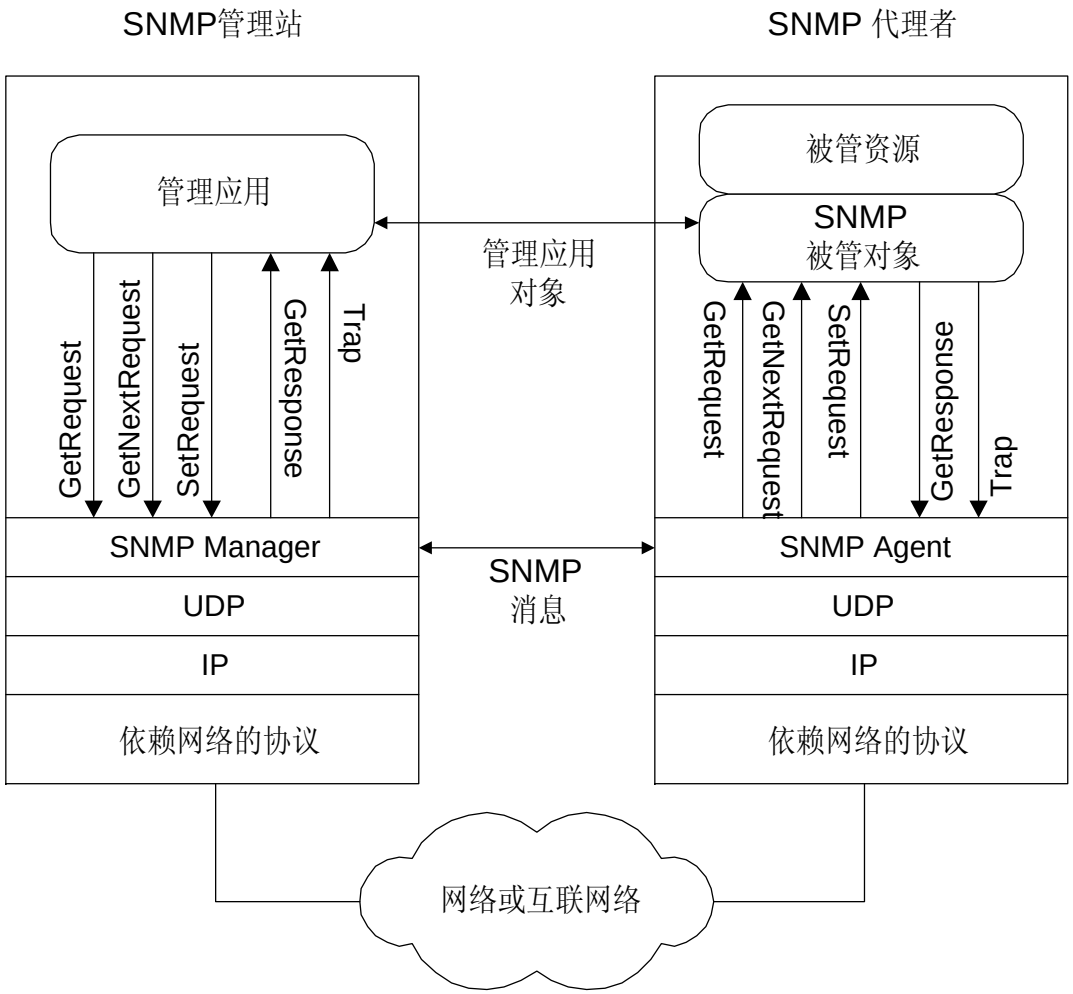


2. SNMP的体系结构

2）网络管理协议体系结构

SNMP为应用层协议，是TCP/IP协议族的一部分，它通过UDP来操作。

SNMP在UDP、IP及有关的特殊网络协议之上实现



2. SNMP的体系结构

3）陷阱引导轮询

- 管理站轮询所有知道关键信息的代理者
- 由每个代理者负责向管理站报告异常事件

4）代理

SNMP的代理者可以作为一个或多个其他设备的代理人。即管理站向代理者发出对某个设备的查询操作，代理者能够将查询转变为该设备使用的管理协议；当代理者收到对一个查询的应答时，将这个应答转发给管理站。

3.1.2 SNMPv1

1. SNMPv1支持的操作

SNMPv1是一种简单的请求/响应协议，使用管理者-代理模型，仅支持对管理对象值的检索和修改等简单操作。网络管理系统发出一个请求，管理器则返回一个响应。

- Get
- Set
- Trap。

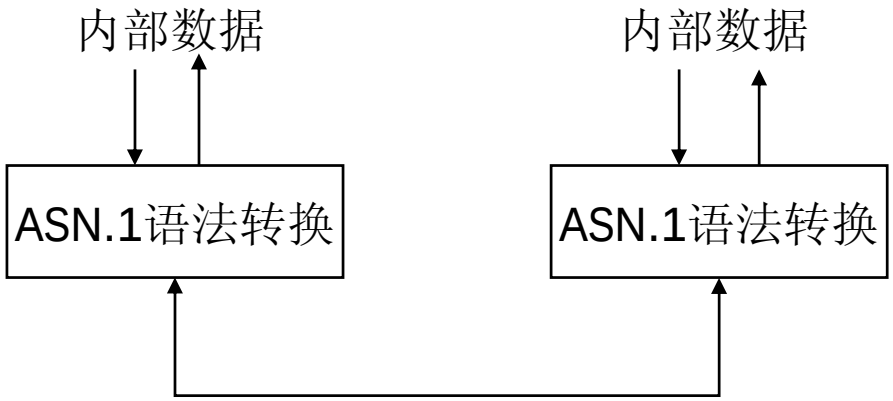
MIB的结构不能通过增加或减少对象实例被改变，并且，访问只能对对象标识树中的叶子对象进行。这些限制大大简化了SNMP的实现，但同时也限制了网络管理系统的能力。

复习几个概念

- ASN.1: 用于定义语法的正式语言。
- SMI（Structure of Management Information管理信息结构）：定义了一个ASN.1的子集，规定了SNMP使用到哪些ASN.1符号与元素，通过使用这些ASN.1子集的符号和元素描述SNMP。
- BER(Basic Encoding Rule基本编码规则)是一种编码规格，描述如何将ASN.1类型的值编码成字节串(string of octets)的方法。是ASN.1标准的一部分。SNMP使用BER编码将SNMP的操作请求和应答编码进行传输，并于接收端进行解码。

SNMPv1

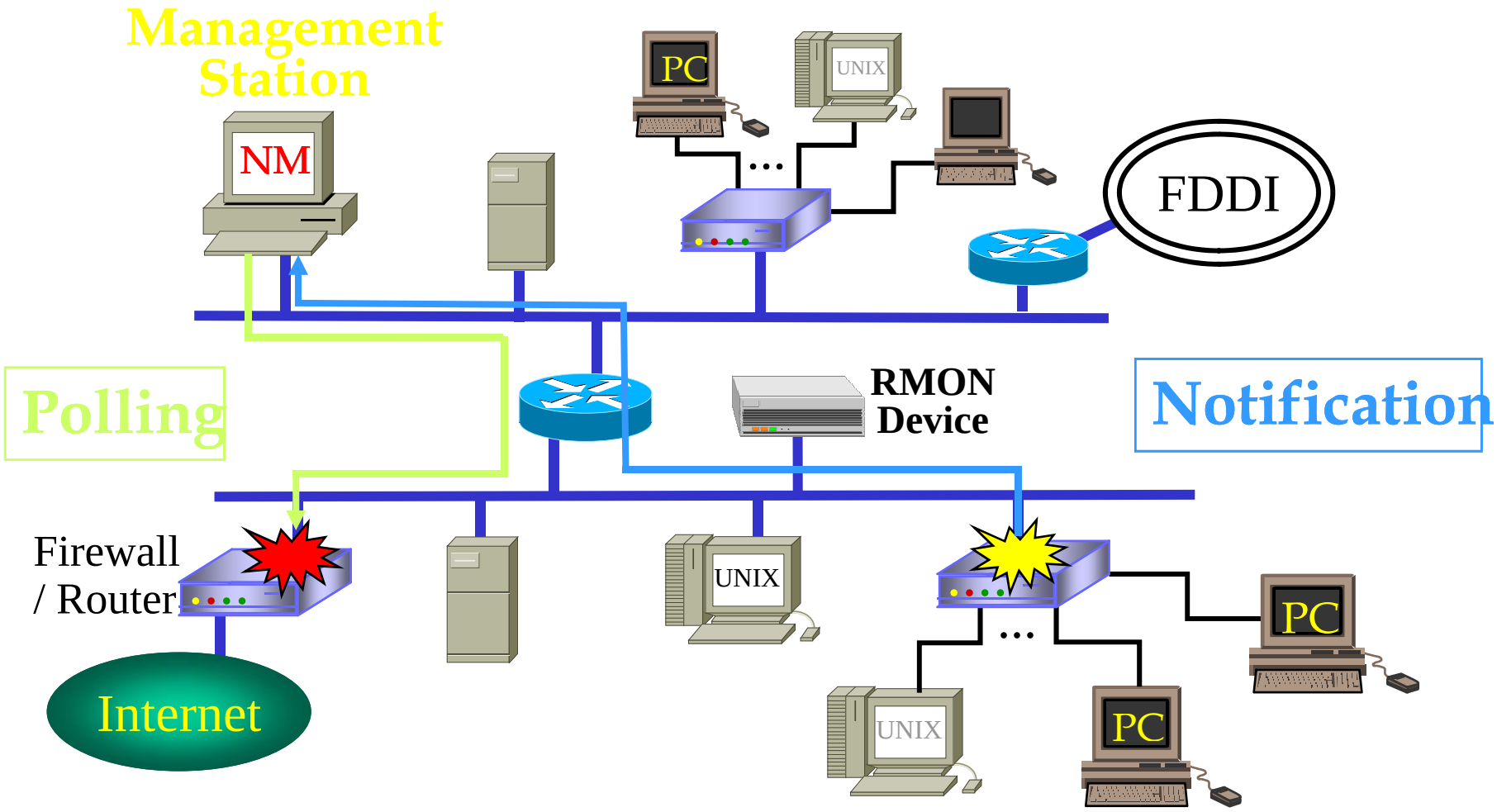
数据传输



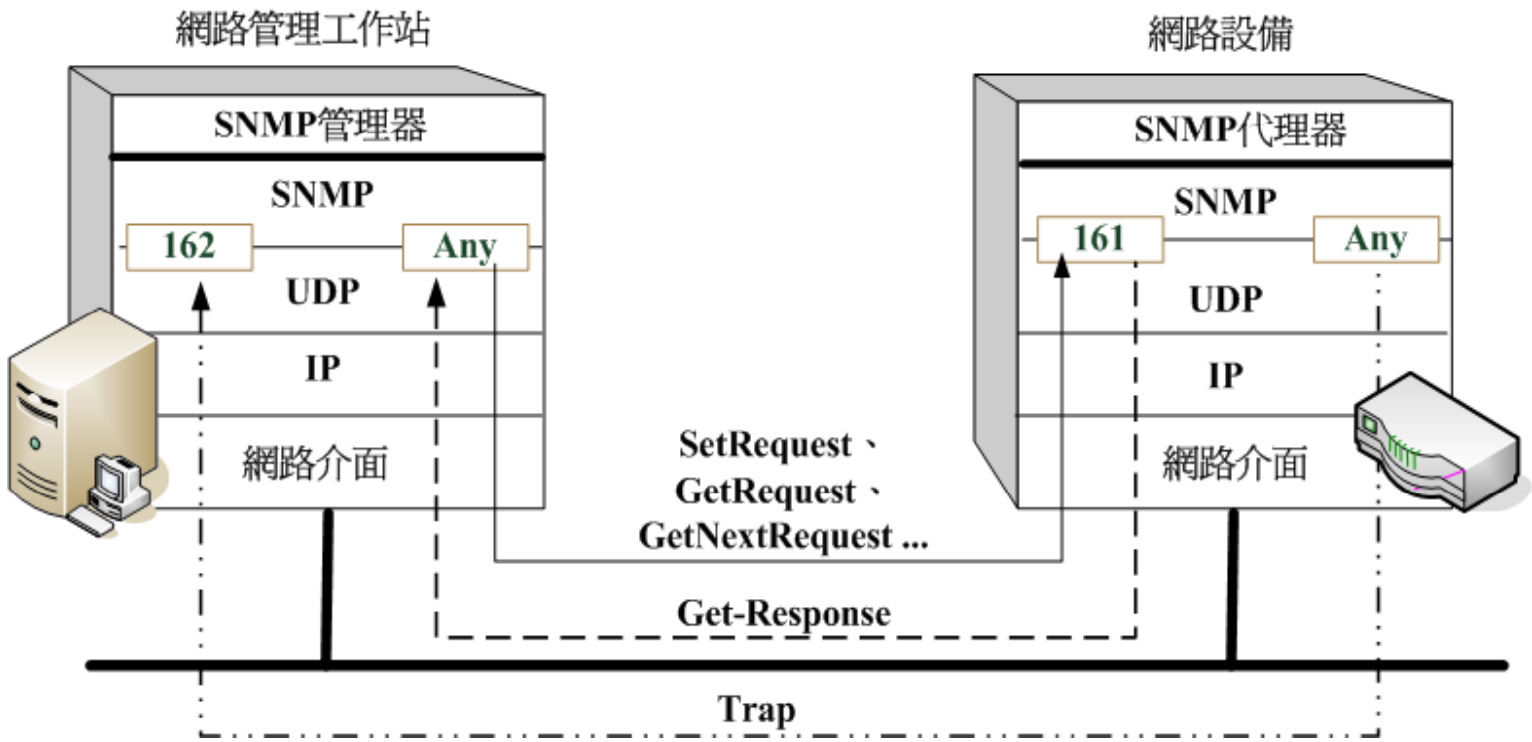
SNMPv1

SNMPv1操作

- get：获取特定的对象的管理信息值
- get-next：遍历MIB树获取对象的值
- set：修改对象的值
- trap：代理发送非请求性通知给网络管理系统，通报有重要事件发生了。


Management Station
NM
PC
UNIX
FDDI
Polling
RMON Device
Notification
Firewall / Router
Internet
UNIX
PC
UNIX
PC

SNMP通讯模式架构


網路管理工作站
SNMP管理器
SNMP
162
Any
UDP
IP
網路介面
網路設備
SNMP代理器
SNMP
161
Any
UDP
IP
網路介面
SetRequest、
GetRequest、
GetNextRequest ...
Get-Response
Trap

SNMP的相关概念

1. 团体名(community name)

每个团体被赋予一个惟一的名字，管理者只能以代理认可的团体名行使其访问权。

使用get或get-next操作来读团体名

使用set操作来写团体名

有效范围：在定义它的代理系统中

缺省的 **‘Get’**团体名： public

SNMP的相关概念

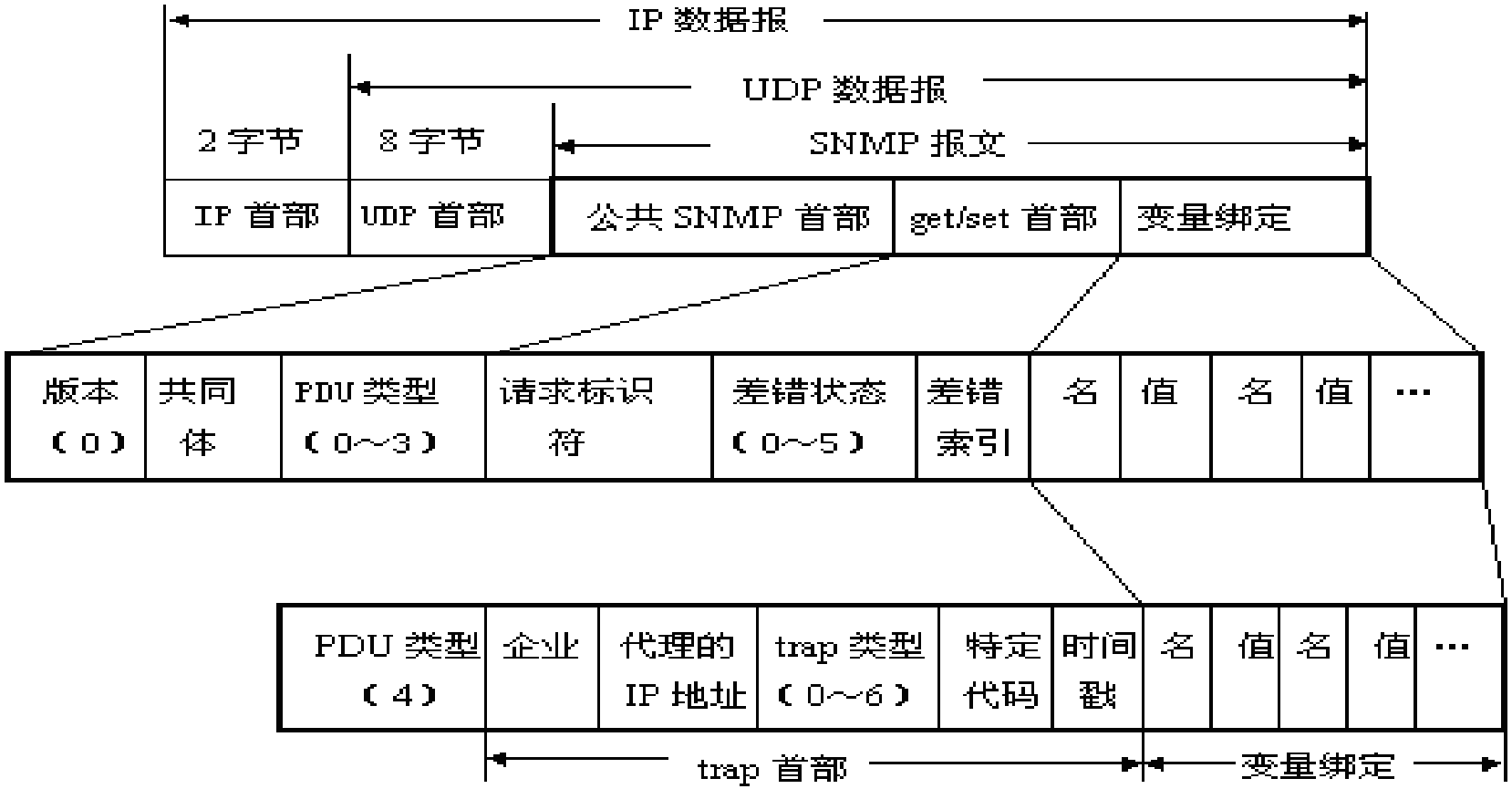
2. 变量绑定

指定要收集或修改的管理对象，是一个OBJECT IDENTIFIER值对应的列表。

对于get或get-next请求，将忽略该值部分。

3.SNMP报文格式

一个SNMP报文共有三个部分组成，即公共SNMP首部、get/set首部（trap首部）、变量绑定。



SNMPv1报文格式

- 版本号：指定SNMP的版本号，写入版本字段的是版本号减1
- 团体名：OCTET STRING类，用于身份认证，作为管理进程和代理进程之间的明文口令
- SNMP PDU：协议数据单元。包含5种类型：
  - GetRequest-PDU
  - GetNextquest-PDU
  - SetRequest-PDU
  - GetResponse-PDU
  - Trap-PDU

SNMPv1报文格式

1. 命令和响应的PDU格式

PDU 类型	请求标识符	差错状态	差错索引	变量绑定表

(1)PDU 类型： GetRequest-PDU，GetNextquest-PDU，SetRequest-PDU，GetResponse-PDU

(2)请求标识符(request ID)字段：赋予每个请求报文惟一的整数，用于区分不同请求。

(3)差错状态(error status)字段：代理处理管理者的请求时可能出现的各种错误。

- 只在GetResponse-PDU中使用，其他类型的PDU中为0。
- 6种差错状态：

SNMPv1报文格式

① noError(0)：成功处理该请求

② tooBig(1)：代理不能把该请求的结果放入到单个SNMP报文中

③ noSuchName(2)：在指定团体名的基础上指定了一个代理不知道的对象

④ badValue(3)：set操作试图把一个对象修改成无效的或不一致的值

⑤ readOnly(4)：指示一个set操作试图修改不能被写入的变量

⑥ genError(5)：任何其他错误

(4) 差错索引字段:当差错状态非0时指向变量绑定表中第一个导致差错的变量

(5)变量绑定列表:变量名和对应值的表,说明要检索或设置的所有变量及其值

SNMPv1报文格式

2. TrapPDU格式

PDU 类型	制造商ID	代理地址	通用陷阱	特殊陷阱	时间戳	变量绑定表

(1)PDU类型：TrapPD

(2)制造商ID：设备制

(3)代理地址：产生陷

(4)通用陷阱：SNMP定

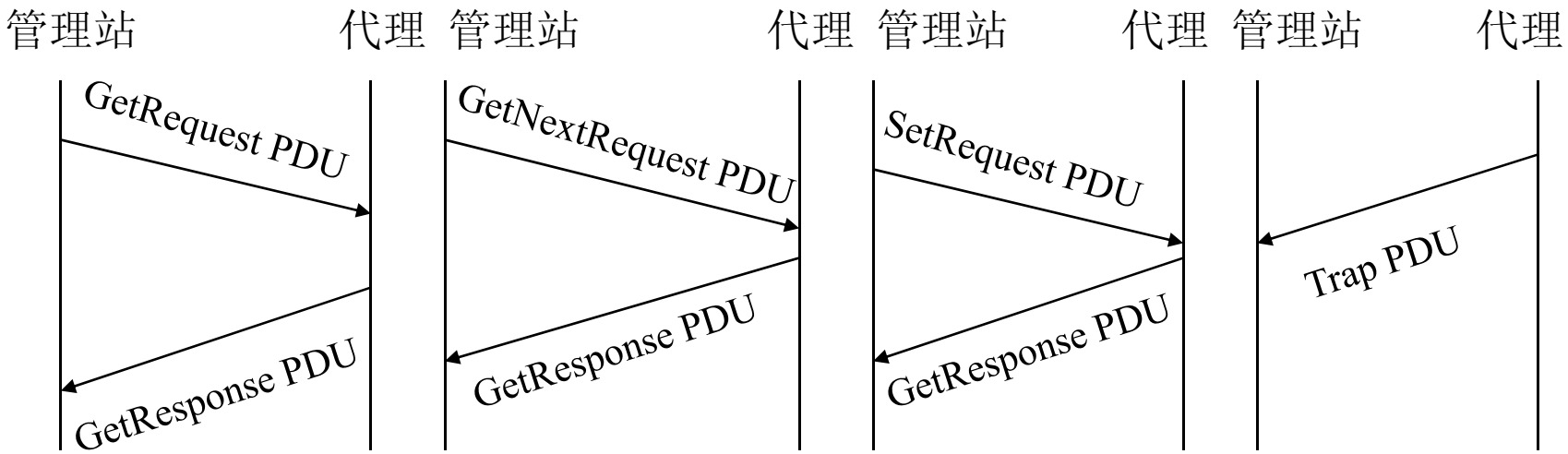
(5)特殊陷阱：与设备

(6)时间戳：代理发出

(7)变量绑定表：变量

t r a p类型	含 义
ColdStart (0)	设备正在重启或初始化，以致于代理和配置也许会改变，通常此消息表示系统崩溃或其他重启状态
WarmStart (1)	设备正在重启或初始化，但代理和配置不会改变，通常表示一个简单刷新或重新启动操作系统
LinkDown (2)	表示设备的一个通信接口连接失败
LinkUP (3)	表示设备的一个通信（接口）链路正在接通或运行
AuthenticationFailure (4)	设备发生了认证失败或其他安全问题，一般情况下是由于一个无效的S N M P团体名引起
EgpNeighorLoss (5)	表示与该设备对等的E G P邻居（external gateway protocol，外部网关协议）宕机或互通关系无效
EnterpriseSpecific (6)	表示一些厂商专用的事件发生了，在特殊陷入（specifc-trap）字段指明具体的陷入类型。

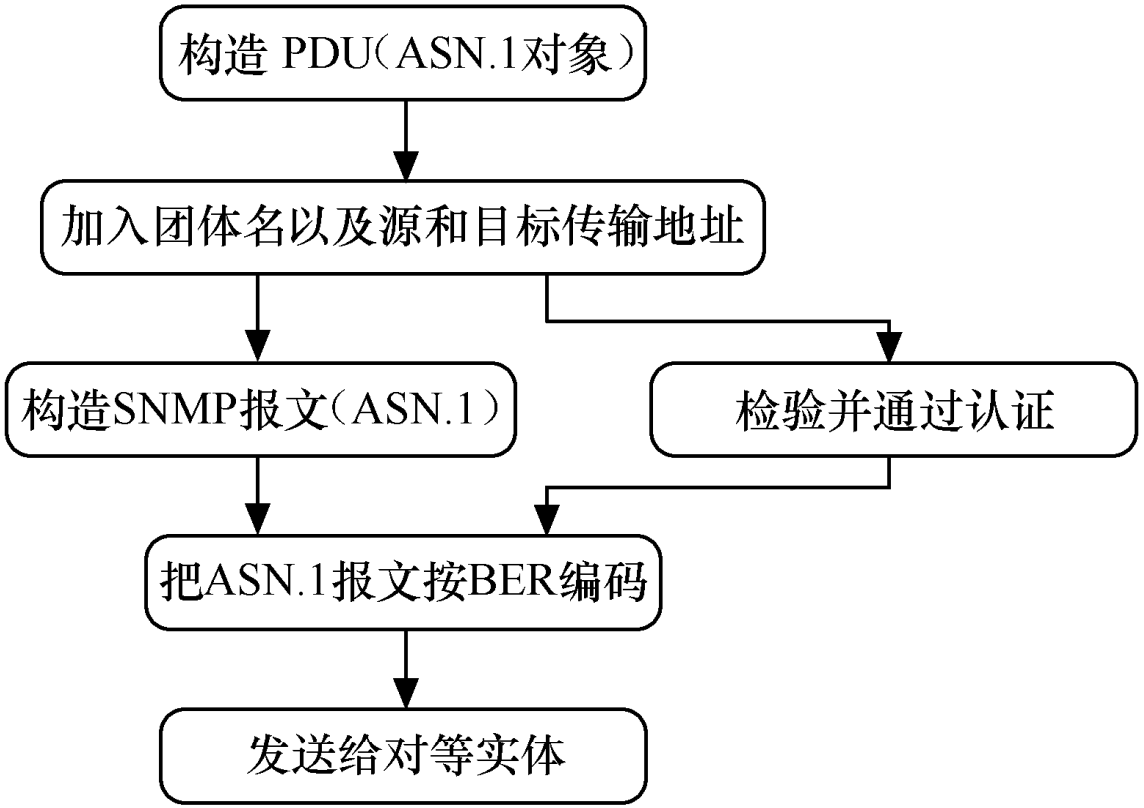
SNMP报文应答序列



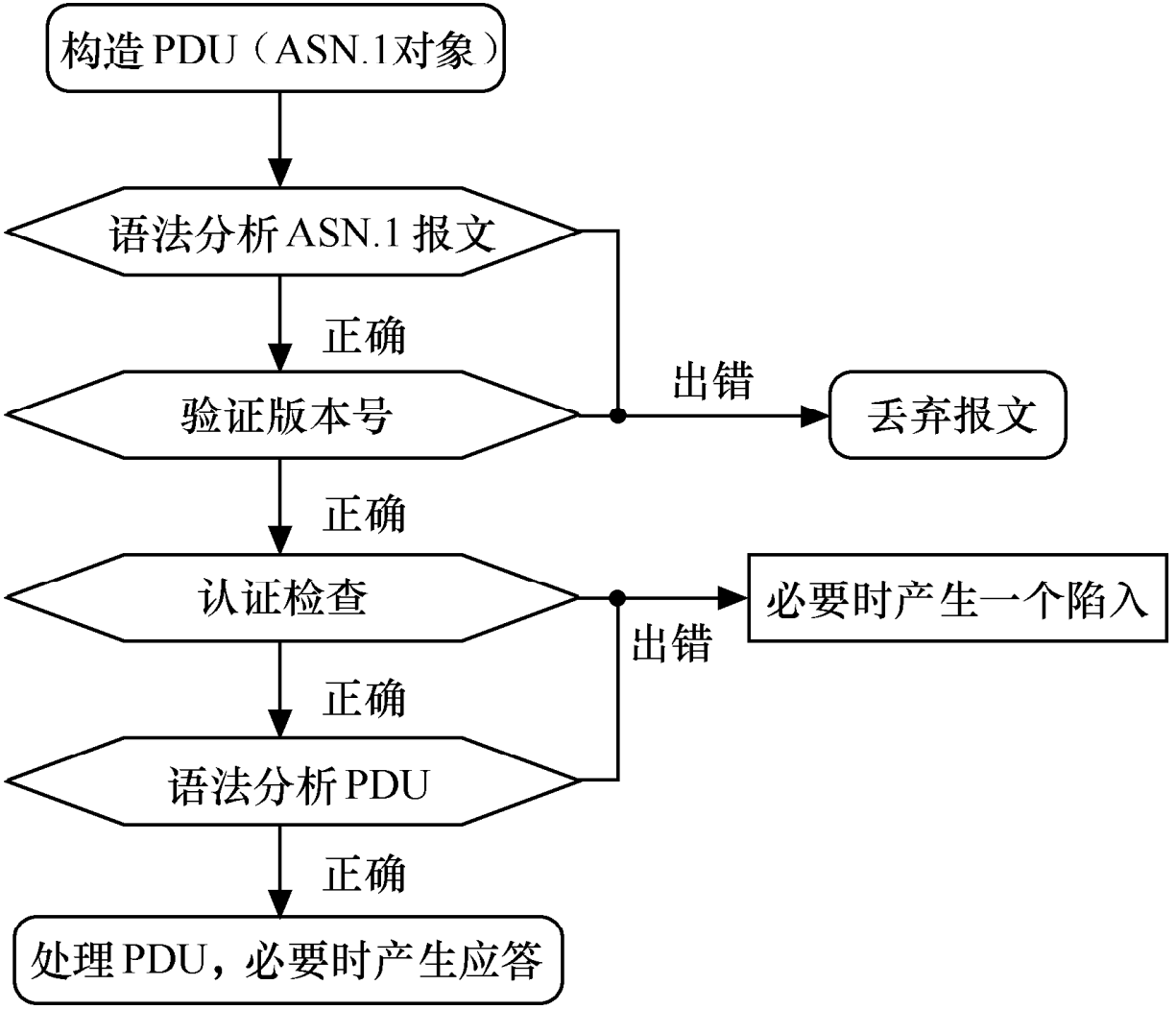
(a) Get　(b) Get-next　(c) Set　(a) Trap

- SNMP报文应答序列

报文发送与接收



生成和发送SNMP报文



接收和处理SNMP报文

SNMP报文应答序列

2. 响应的格式

0xA2	请求标识符	差错状态	差错索引	变量绑定表

- 0xA2：指示该SNMP是GetResponse。
- 请求标识符(reqid)：与原请求中的值相同。
- 差错状态(es)：指示该代理是否能成功处理该请求。
- 差错索引(ei)：非0则指示第一个变量在错误请求中的位置。
- 变量绑定：一个变量列表，每个变量包含一个对象标识符和一个值。

SNMP报文应答序列

3. 处理get和get-next请求：

请求	差错	GetResponse
get和 get-next	一个对象在指定团体名下不可用(对于get-next，如果下一个对象不存在)	差错状态：noSuchName 差错索引：该对象在变量绑定中的位置
	PDU太大	差错状态：tooBig
	由于其他原因不能获取一个值	差错状态：genErr 差错索引：该对象在变量绑定中的位置

SNMP报文应答序列

3. 处理set：

请求	差错	GetResponse
set	一个对象在指定团体名下不可用	差错状态：noSuchName 差错索引：该对象在变量绑定中的位置
	为该对象指定的值不一致	差错状态：badValue 差错索引：该对象在变量绑定中的位置
	PDU太大	差错状态： tooBig
	由于其他原因不能获取一个值	差错状态： genErr 差错索引：该对象在变量绑定中的位置

SNMP报文应答序列

- 一个SNMP响应信息包大小：至少484字节
- 一条484字节容纳的变量数：取决于对象标识符的长度和数据类型

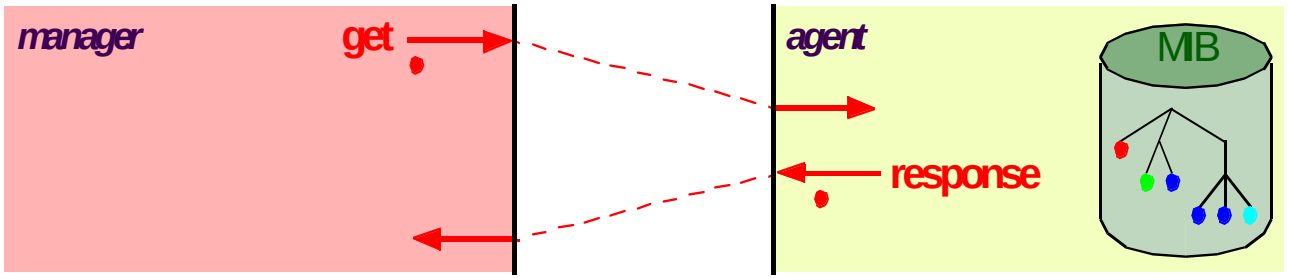
get操作

- 格式

PDU 类型	请求标识符	0	0	变量绑定表

PDU类型：0xA0

- 作用：获取特定的对象
- 可能的错误：
  - noSuchName 对象不存在或对象不是叶节点
  - tooBig PDU太大
  - genErr 其他错误



get操作

实例	ifIndex	ifDescr	ifType
1	1	Ethernet	6
2	2	Ethernet	6
3	3	serial	22
4	4	ppp	23
5	5	Ethernet	6
6	6	Ethernet	6

get-request {sysUpTime.0，ifIndex.1，ifDescr.2，ifType.4}

sysUpTime.0 287231 ifIndex.1 1
ifDescr.2 ethernet ifType.4 23
(ifIndex.1，ifDescr.2，ifType.7) ?

noSuchName 差错索引**3**

(ifTable) ?

noSuchName 差错索引**1**

get-next操作

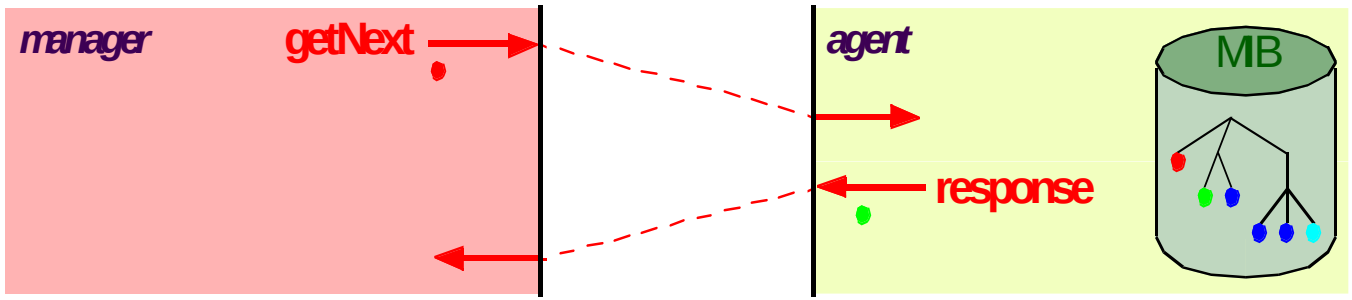
- 格式

PDU 类型	请求标识符	0	0	变量绑定表

PDU类型：0xA1

作用：对于变量绑定中指定的每个对象标识符执行一次MIB树遍历，获取下一个叶子对象，可用于检索未知对象和表对象。

- 可能的错误：
  - noSuchName　END OF MIB
  - tooBig PDU太大
  - genErr　其他错误



get-next操作

实例	ifInOctets	ifInUcastPkts	ifInNUcastPkts
1	200123	5601	912
2	4587213	8876	1790
3	735543	7268	
4	6537722	200211	3388
5	2987653211	101392199	46421
6	783101	53211	4241

get-next {ifInOctets，ifInUcastPkts，ifInNUcastPkts}

ifInOctets.1 200123

ifInUcastPkts.1 5601

ifInNUcastPkts.1 912

get-next操作

get-next {ifInOctets.1,
ifInOctets.2 45872
ifInUcastPkts.2 8876
ifInNUcastPkts.2 1790

实例	ifInOctets	ifInUcastPkts	ifInNUcastPkts
1	200123	5601	912
2	4587213	8876	1790
3	735543	7268	
4	6537722	200211	3388
5	2987653211	101392199	46421
6	783101	53211	4241

get-next {ifInOctets.2, ifInUcastPkts.2, ifInNUcastPkts.2}
ifInOctets.3 735543
ifInUcastPkts.3 7268
ifInNUcastPkts.4 3388

实例	ifInOctets	ifInUcastPkts	ifInNUcastPkts
1	200123	5601	912
2	4587213	8876	1790
3	735543	7268	
4	6537722	200211	3388
5	2987653211	101392199	46421
6	783101	53211	4241

-- ifInNUcastPkts.2空白，查找到下一个

get-next操作

例：查询一个设备所有接口的速率

{iso(1)org(3)dod(6)internet(1)mgmt(2)mib(1)
interfaces(2)ifNumber(1)}

命令：

GetRequest(1.3.6.1.2.1.2.1.0)

GetResponse(2)

GetRequest(1.3.6.1.2.1.2.2.1.5.1)

GetResponse(10000000)

GetRequest(1.3.6.1.2.1.2.2.1.5.2) ----或者用

GetNextRequest(1.3.6.1.2.1.2.2.1.5.1)

GetResponse(56000)

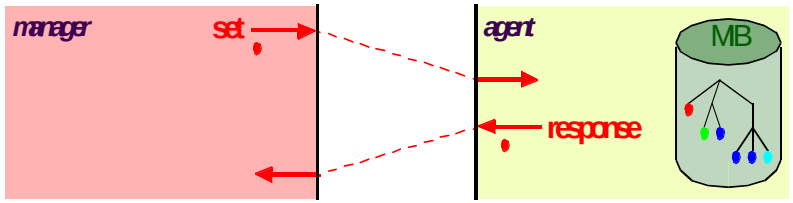
set操作

- 格式

PDU 类型	请求标识符	0	0	变量绑定表

PDU类型：0xA3

- 作用：修改或创建管理对象
- 如何工作？
  - 在set请求中提供的变量绑定定义了要设置的变量以及要设置的值
  - 在表中添加或删除行取决于表中对象的定义方式
- 可能的错误：
  - noSuchName 对象不存在或对象不是叶节点
  - tooBig PDU太大
  - badValue 为该对象指定的值不一致
  - genErr 其他错误



traps操作

0xA4	制造商ID	代理地址	通用陷阱	特殊陷阱	时间戳	变量绑定表

UDP端口：162

(1) 0xA4：trap
(2) 制造商ID：设备制造商标识
(3) 代理地址：产生陷阱的代理的IP地址
(4) 通用陷阱：SNMP定义的陷阱

值	含义
0 (ColdStart)	设备正在重启或初始化
1（WarmStart ）	设备正在重启或初始化，但代理和配置不会改变
2 （LinkDown ）	表示设备的一个通信接口连接失败
3 （LinkUP ）	表示设备的一个通信（接口）链路正在接通或运行
4 (AuthenticationFailure）	指示一条**SNMP**消息已接收到，鉴别失败
5（EgpNeighorLoss ）	指示一个**EGP**邻居过渡到**down**状态
6（EnterpriseSpecific ）	厂商用这一类型的**trap**表示其专用的一些**trap**情况

traps操作

(5) 特殊陷阱：与设备有关的特殊陷阱代码。通常为0，除非通用trap的值是enterpriseSpecific。

(6) 时间戳：代理发出陷阱的时间

(7) 变量绑定表：变量名和对应值的表

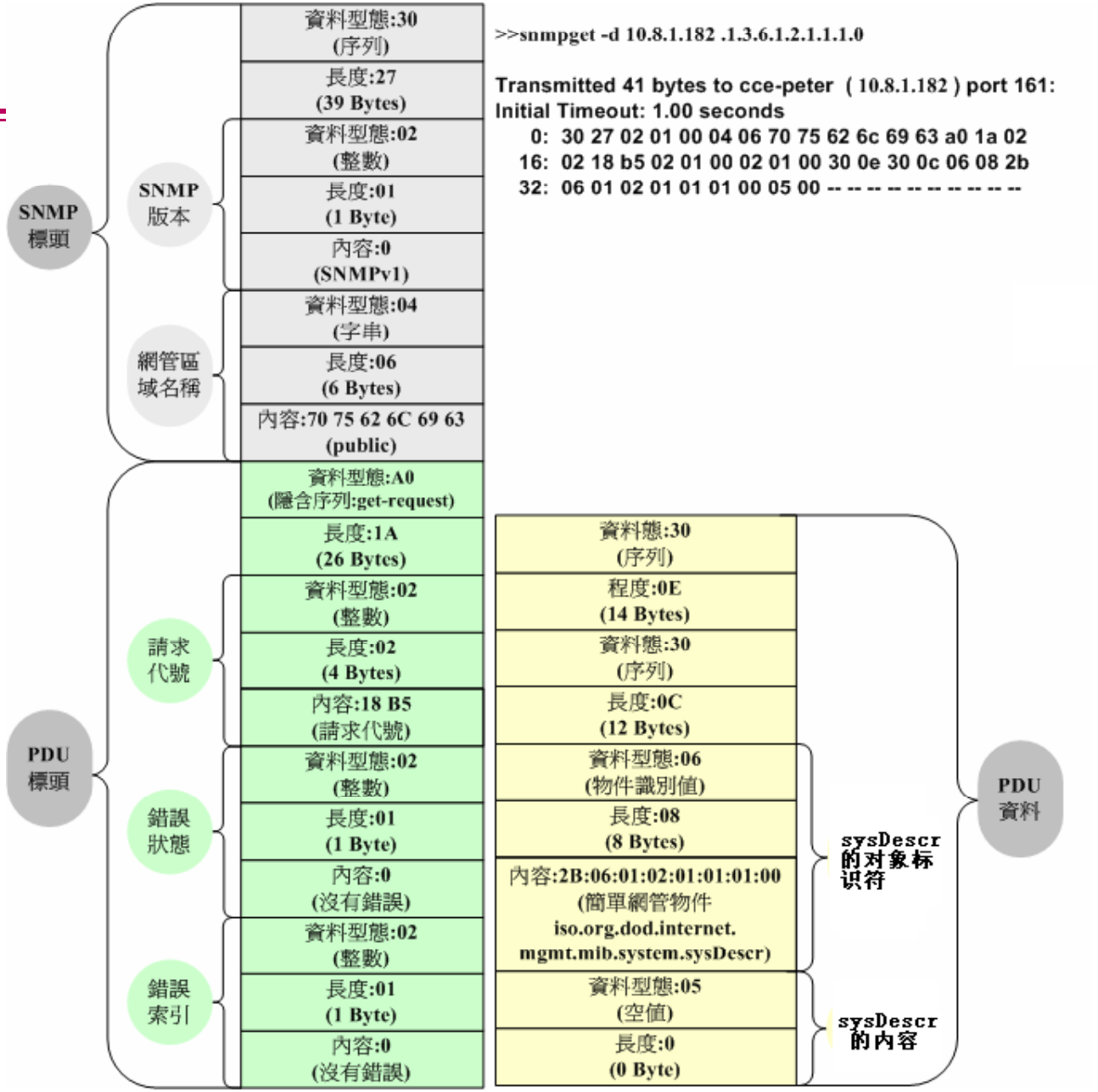
Generic-trap=0~5时 TRAP内容：ColdStart(0)
WarmStart (1)
LinkDown(2)
LinkUP(3)
AuthenticationFailure(4)
EgpNeighorLoss(5)

Generic-trap=6时 TRAP内容由各企业定义，并且用specific-trap号定义该trap

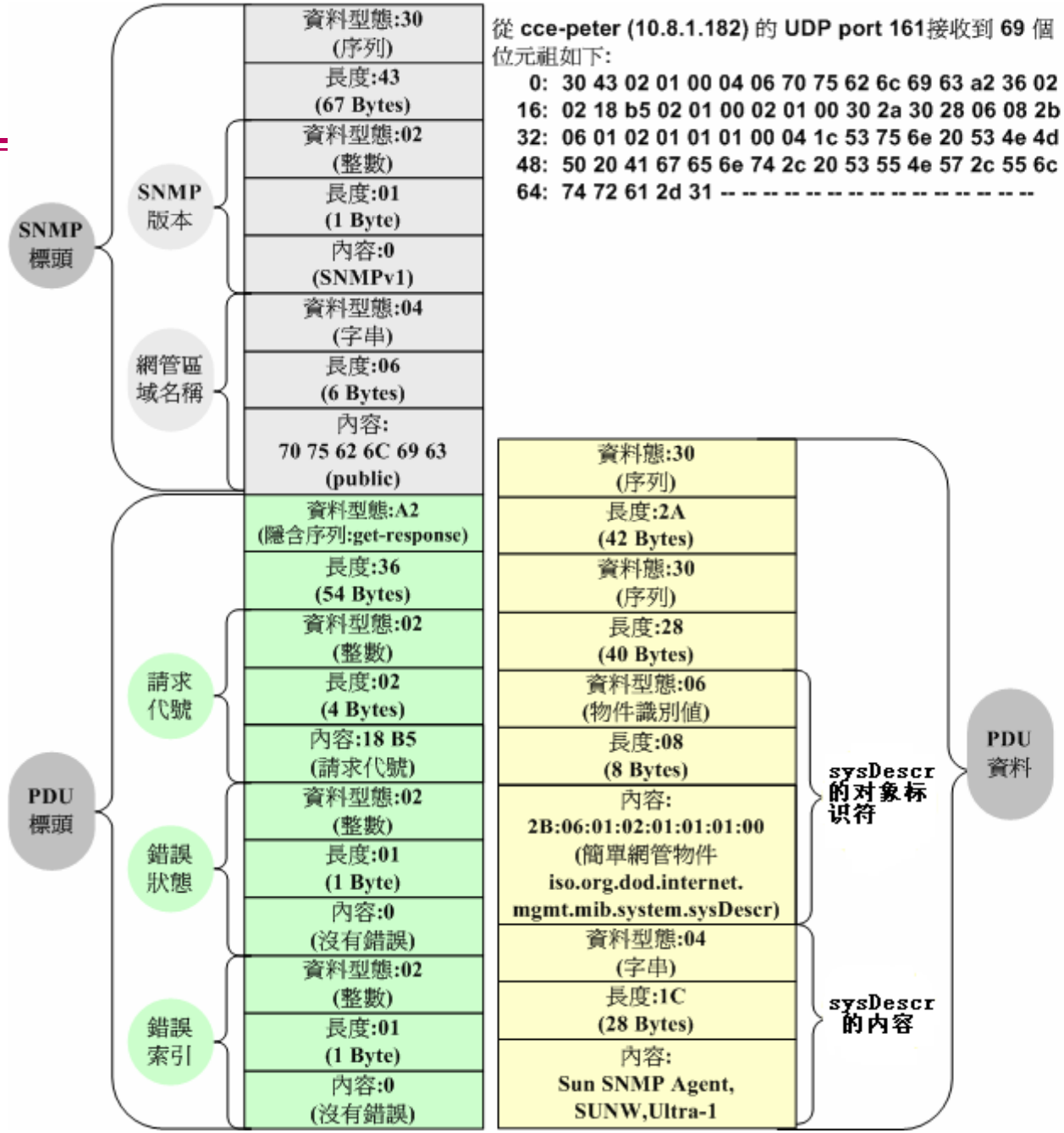
BER编码原则

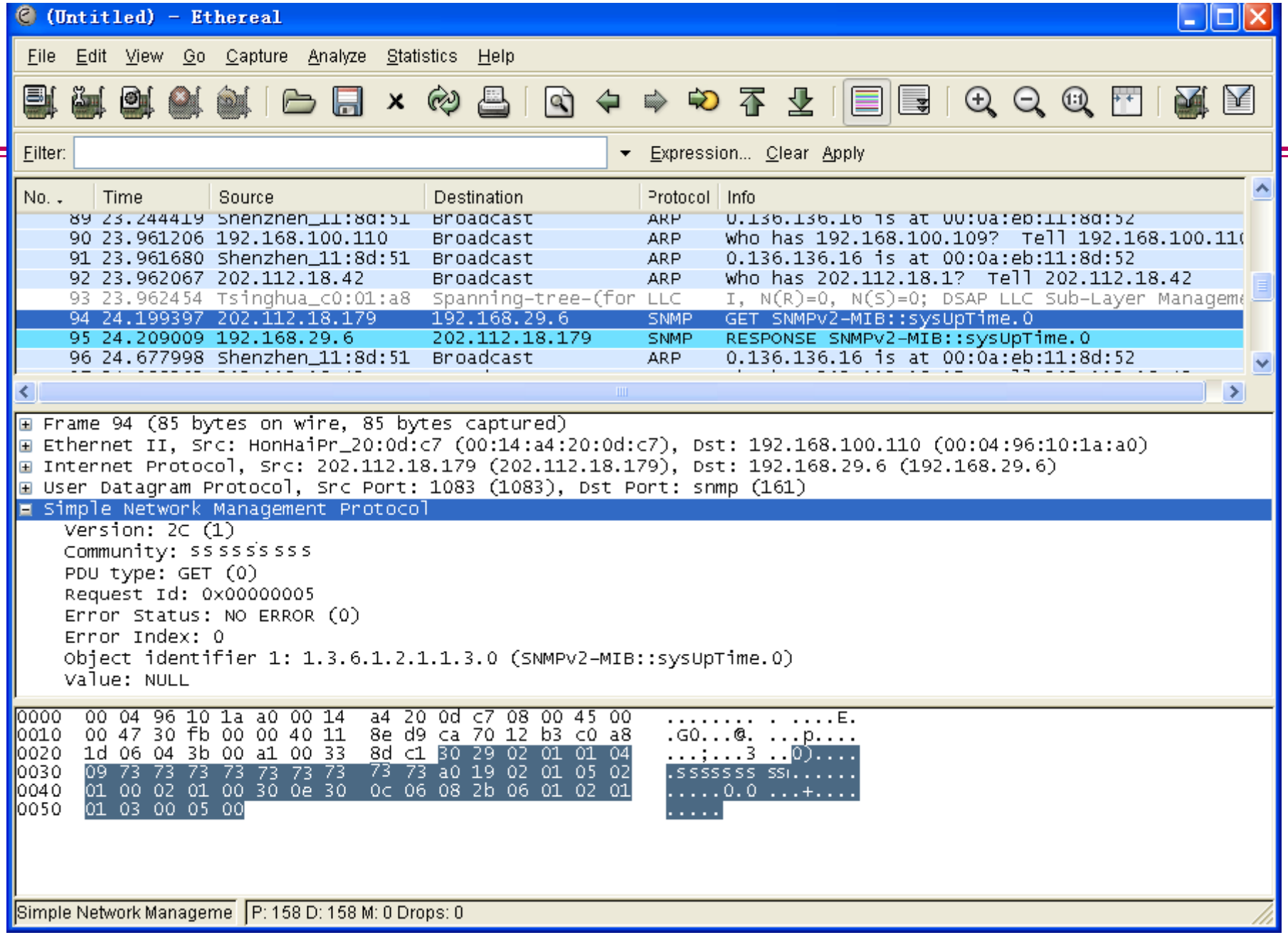
BER编码代号	类型	BER编码代号	PDU类型
02	INTEGER	A0	GetRequest-PDU
04	OCTET STRING	A1	GetNextRequest-PDU
06	OBJECT IDENTIFIER	A2	GetResponse-PDU
05	NULL	A3	SetRequest-PDU
16	SEQUENCE/ SEQUENCE OF	A4	Trap-PDU

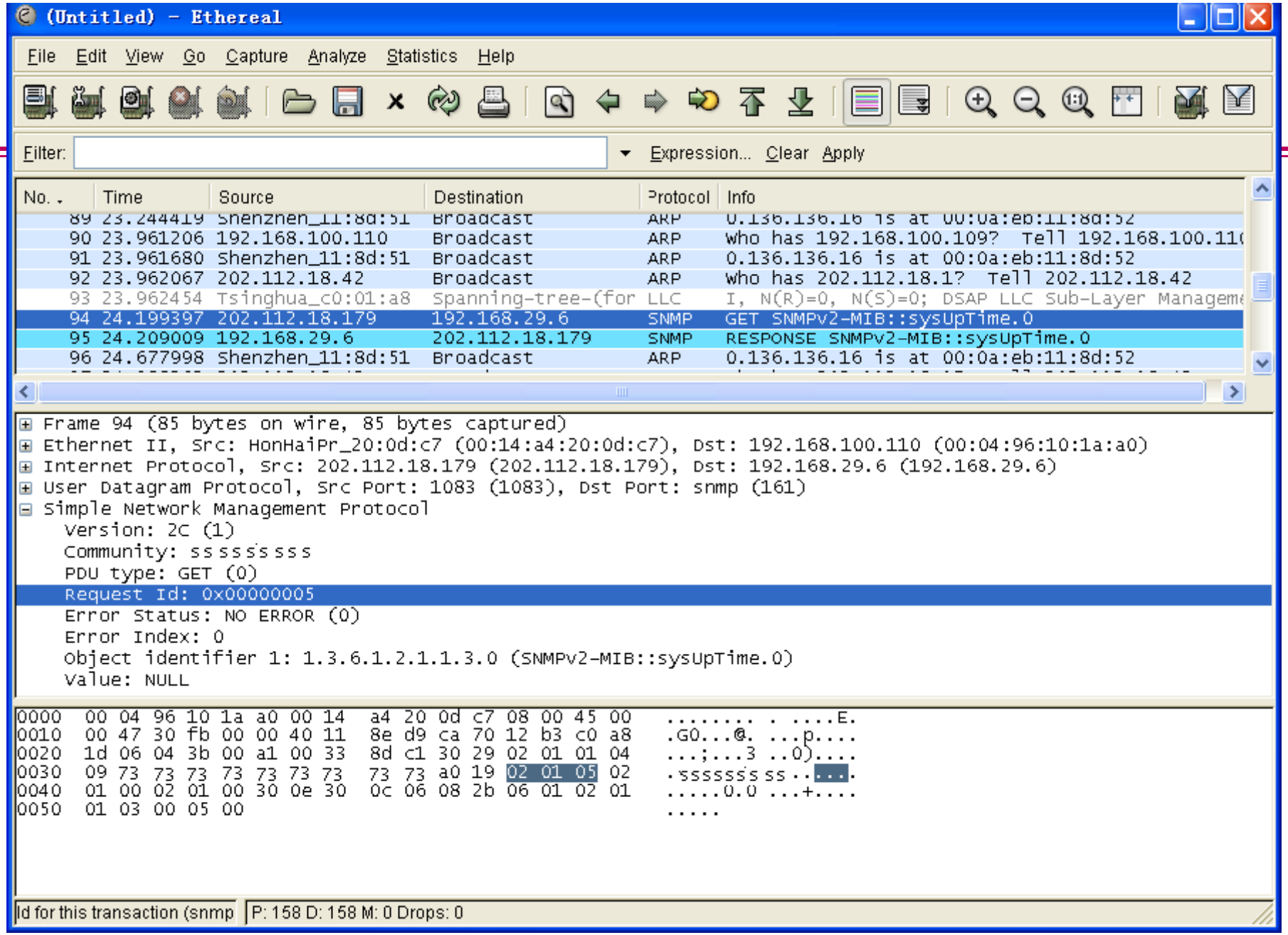
SNMP取得指令信息的应用实例

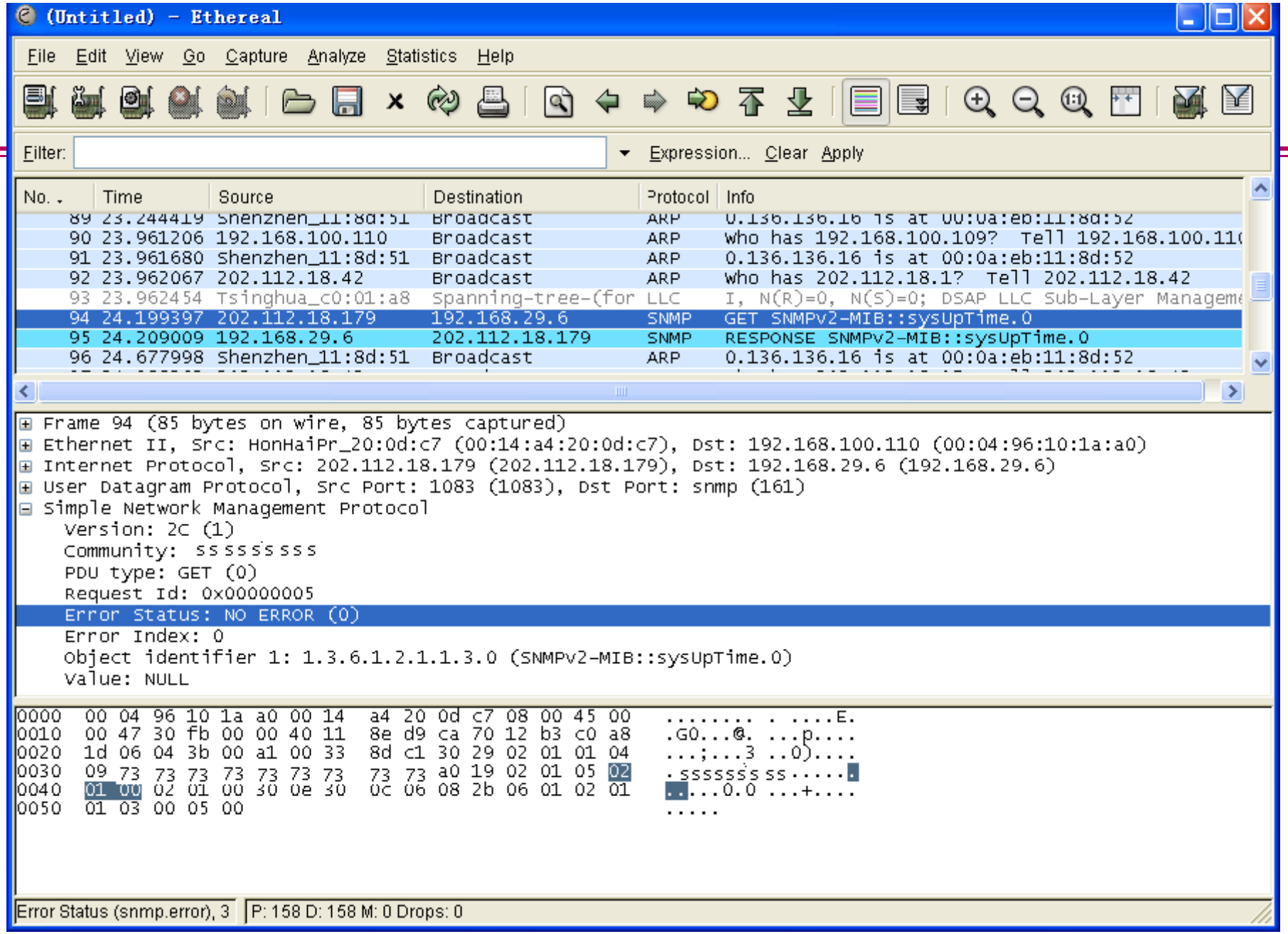


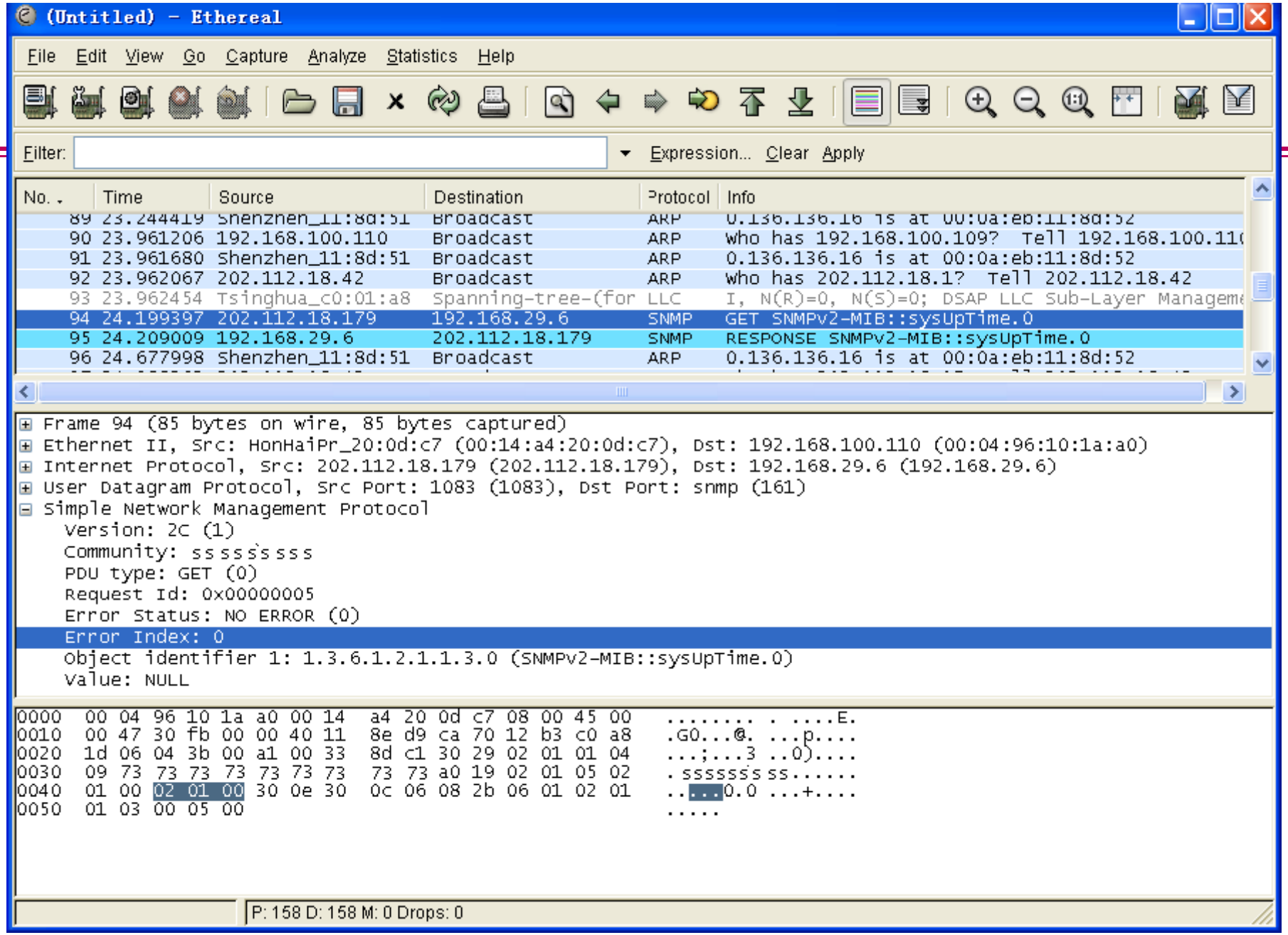
SNMP响应指令信息的应用实例

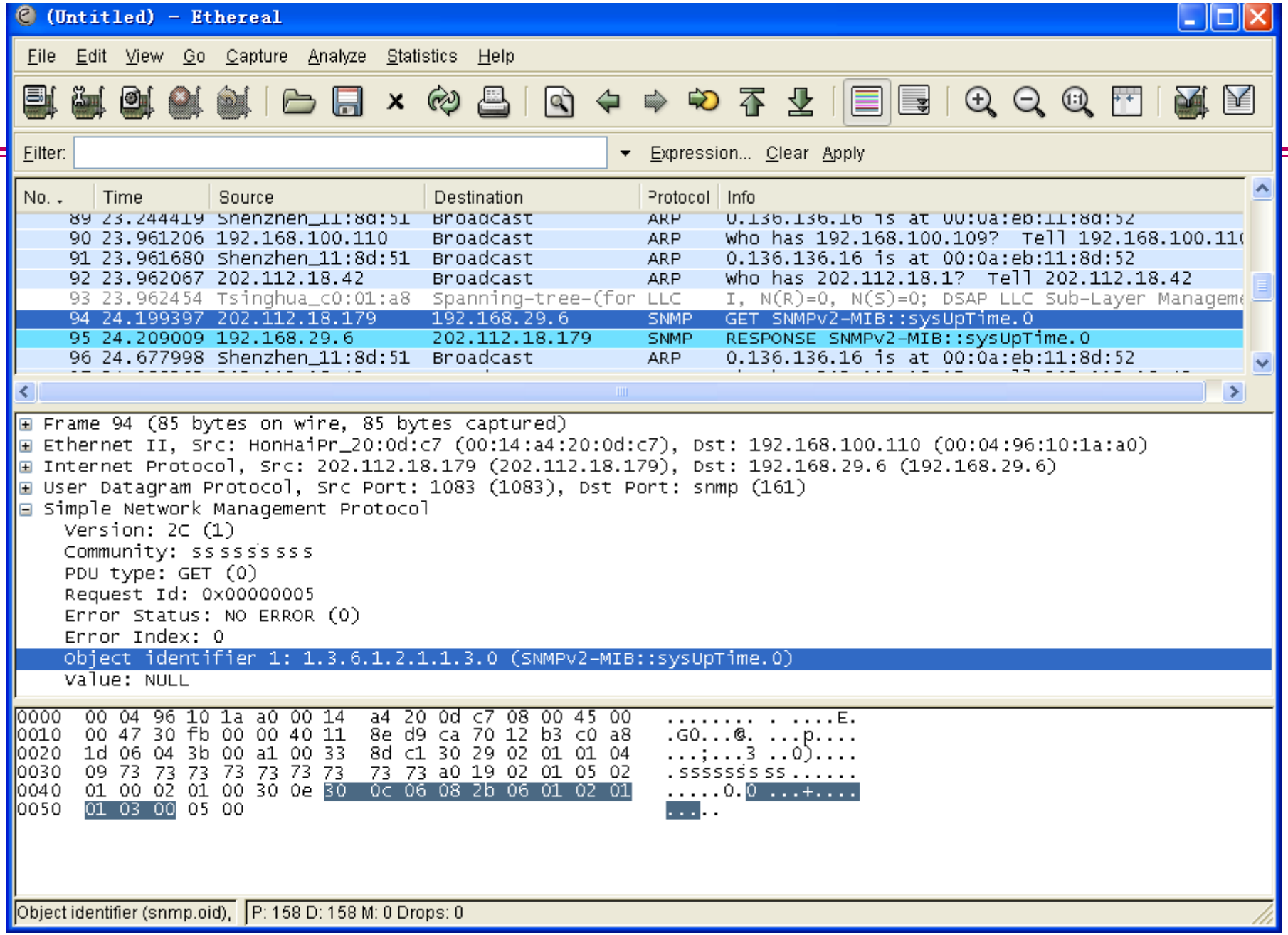


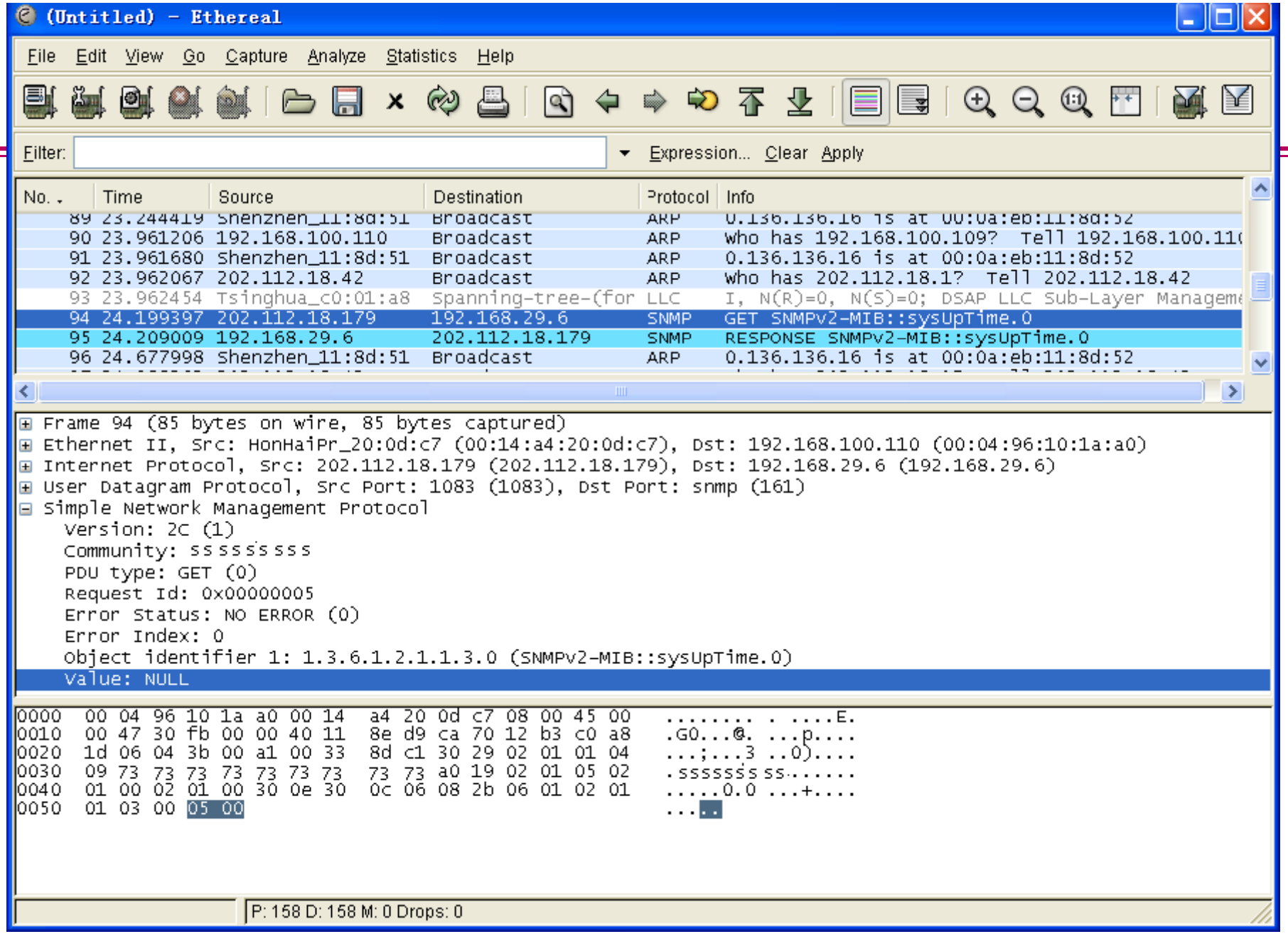

(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
90 23.961206 192.168.100.110 Broadcast ARP Who has 192.168.100.109? Tell 192.168.100.11
91 23.961680 Shenzhen_11:8d:51 Broadcast ARP 0.136.136.16 is at 00:0a:eb:11:8d:52
92 23.962067 202.112.18.42 Broadcast ARP Who has 202.112.18.1? Tell 202.112.18.42
93 23.962454 Tsinghua_c0:01:a8 Spanning-tree-(for LLC I, N(R)=0, N(S)=0; DSAP LLC Sub-Layer Manageme
94 24.199397 202.112.18.179 192.168.29.6 SNMP GET SNMPv2-MIB::sysUpTime.0
95 24.209009 192.168.29.6 202.112.18.179 SNMP RESPONSE SNMPv2-MIB::sysUpTime.0
96 24.677998 Shenzhen_11:8d:51 Broadcast ARP 0.136.136.16 is at 00:0a:eb:11:8d:52
Frame 94 (85 bytes on wire, 85 bytes captured)
Ethernet II, Src: HonHaiPr_20:0d:c7 (00:14:a4:20:0d:c7), Dst: 192.168.100.110 (00:04:96:10:1a:a0)
Internet Protocol, Src: 202.112.18.179 (202.112.18.179), Dst: 192.168.29.6 (192.168.29.6)
User Datagram Protocol, Src Port: 1083 (1083), Dst Port: snmp (161)
Simple Network Management Protocol
Version: 2C (1)
Community: ssssssss
PDU type: GET (0)
Request Id: 0x00000005
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: NULL
0000 00 04 96 10 1a a0 00 14 a4 20 0d c7 08 00 45 00
0010 00 47 30 fb 00 00 40 11 8e d9 ca 70 12 b3 c0 a8
0020 1d 06 04 3b 00 a1 00 33 8d c1 30 29 02 01 01 04
0030 09 73 73 73 73 73 73 73 73 73 a0 19 02 01 05 02
0040 01 00 02 01 00 30 0e 30 0c 06 08 2b 06 01 02 01
0050 01 03 00 05 00
Simple Network Manageme
P: 158 D: 158 M: 0 Drops: 0

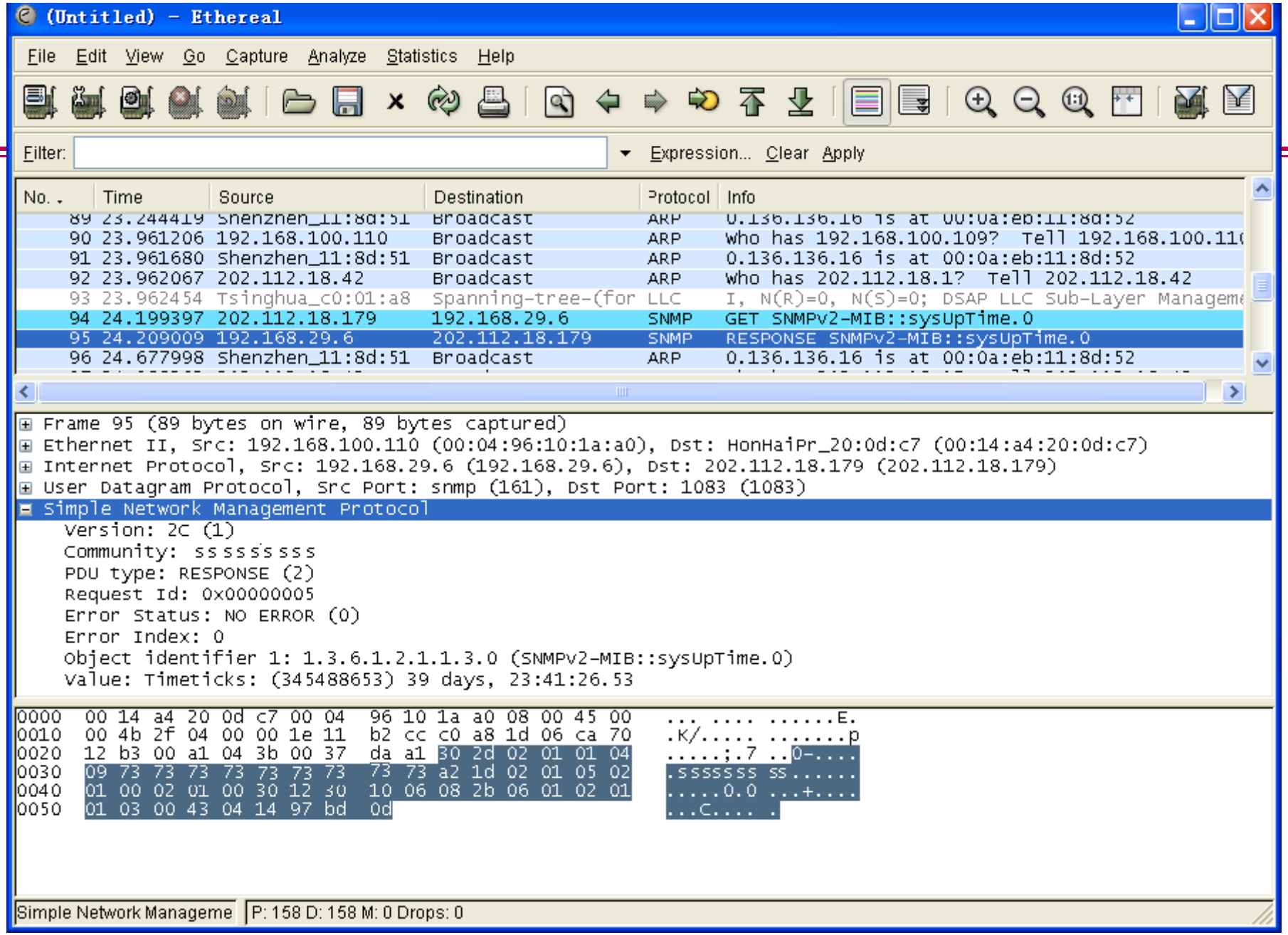

(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
89 23.244419 Shenzhen_11:8d:51 Broadcast ARP 0.136.136.16 is at 00:0a:eb:11:8d:52
90 23.961206 192.168.100.110 Broadcast ARP who has 192.168.100.109? Tell 192.168.100.11
91 23.961680 Shenzhen_11:8d:51 Broadcast ARP 0.136.136.16 is at 00:0a:eb:11:8d:52
92 23.962067 202.112.18.42 Broadcast ARP who has 202.112.18.1? Tell 202.112.18.42
93 23.962454 Tsinghua_c0:01:a8 Spanning-tree-(for LLC I, N(R)=0, N(S)=0; DSAP LLC Sub-Layer Manageme
94 24.199397 202.112.18.179 192.168.29.6 SNMP GET SNMPv2-MIB::sysUpTime.0
95 24.209009 192.168.29.6 202.112.18.179 SNMP RESPONSE SNMPv2-MIB::sysUpTime.0
96 24.677998 Shenzhen_11:8d:51 Broadcast ARP 0.136.136.16 is at 00:0a:eb:11:8d:52
Frame 94 (85 bytes on wire, 85 bytes captured)
Ethernet II, Src: HonHaiPr_20:0d:c7 (00:14:a4:20:0d:c7), Dst: 192.168.100.110 (00:04:96:10:1a:a0)
Internet Protocol, Src: 202.112.18.179 (202.112.18.179), Dst: 192.168.29.6 (192.168.29.6)
User Datagram Protocol, Src Port: 1083 (1083), Dst Port: snmp (161)
Simple Network Management Protocol
Version: 2C (1)
Community: ssssssss
PDU type: GET (0)
Request Id: 0x00000005
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: NULL
0000 00 04 96 10 1a a0 00 14 a4 20 0d c7 08 00 45 00 ....E.
0010 00 47 30 fb 00 00 40 11 8e d9 ca 70 12 b3 c0 a8 .G0...@. ...p....
0020 1d 06 04 3b 00 a1 00 33 8d c1 30 29 02 01 01 04 ...;...3 ..0)....
0030 09 73 73 73 73 73 73 73 73 73 a0 19 02 01 05 02 .ssssssss ......
0040 01 00 02 01 00 30 0e 30 0c 06 08 2b 06 01 02 01 .....0.0 ...+....
0050 01 03 00 05 00 .....
Id for this transaction (snmp
P: 158 D: 158 M: 0 Drops: 0

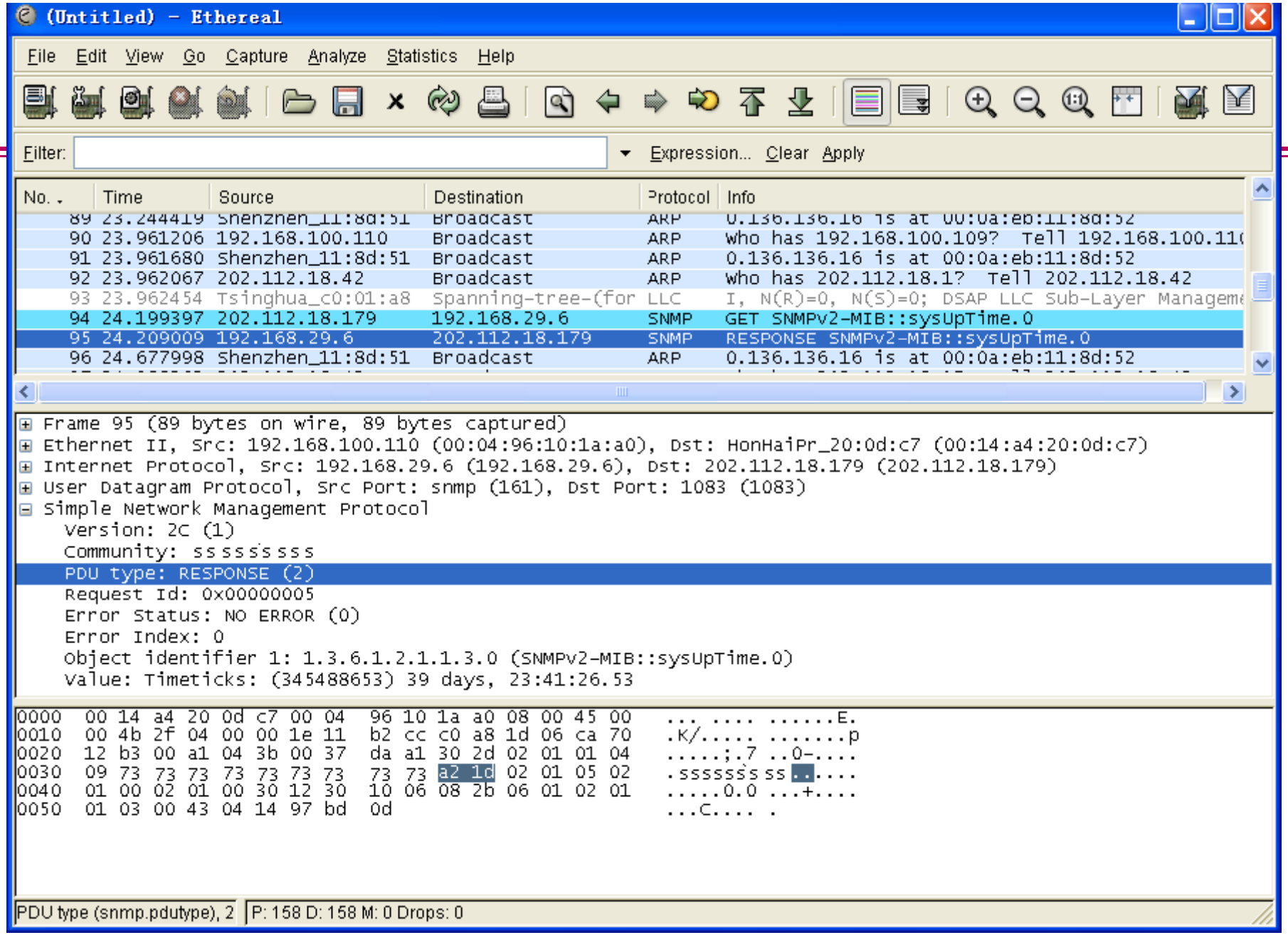

(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
89 23.244419 Shenzhen_11:8d:51 Broadcast ARP 0.136.136.16 is at 00:0a:eb:11:8d:52
90 23.961206 192.168.100.110 Broadcast ARP Who has 192.168.100.109? Tell 192.168.100.11
91 23.961680 Shenzhen_11:8d:51 Broadcast ARP 0.136.136.16 is at 00:0a:eb:11:8d:52
92 23.962067 202.112.18.42 Broadcast ARP Who has 202.112.18.1? Tell 202.112.18.42
93 23.962454 Tsinghua_c0:01:a8 Spanning-tree-(for LLC I, N(R)=0, N(S)=0; DSAP LLC Sub-Layer Manageme
94 24.199397 202.112.18.179 192.168.29.6 SNMP GET SNMPv2-MIB::sysUpTime.0
95 24.209009 192.168.29.6 202.112.18.179 SNMP RESPONSE SNMPv2-MIB::sysUpTime.0
96 24.677998 Shenzhen_11:8d:51 Broadcast ARP 0.136.136.16 is at 00:0a:eb:11:8d:52
Frame 94 (85 bytes on wire, 85 bytes captured)
Ethernet II, Src: HonHaiPr_20:0d:c7 (00:14:a4:20:0d:c7), Dst: 192.168.100.110 (00:04:96:10:1a:a0)
Internet Protocol, Src: 202.112.18.179 (202.112.18.179), Dst: 192.168.29.6 (192.168.29.6)
User Datagram Protocol, Src Port: 1083 (1083), Dst Port: snmp (161)
Simple Network Management Protocol
Version: 2C (1)
Community: ssssssss
PDU type: GET (0)
Request Id: 0x00000005
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: NULL
0000 00 04 96 10 1a a0 00 14 a4 20 0d c7 08 00 45 00 ....E.
0010 00 47 30 fb 00 00 40 11 8e d9 ca 70 12 b3 c0 a8 .G0...@. ...p....
0020 1d 06 04 3b 00 a1 00 33 8d c1 30 29 02 01 01 04 ...;...3 ..0)....
0030 09 73 73 73 73 73 73 73 73 73 a0 19 02 01 05 02 .sssssss ss......
0040 01 00 02 01 00 30 0e 30 0c 06 08 2b 06 01 02 01 .....0.0 ...+....
0050 01 03 00 05 00 .....
Error Status (snmp.error), 3
P: 158 D: 158 M: 0 Drops: 0

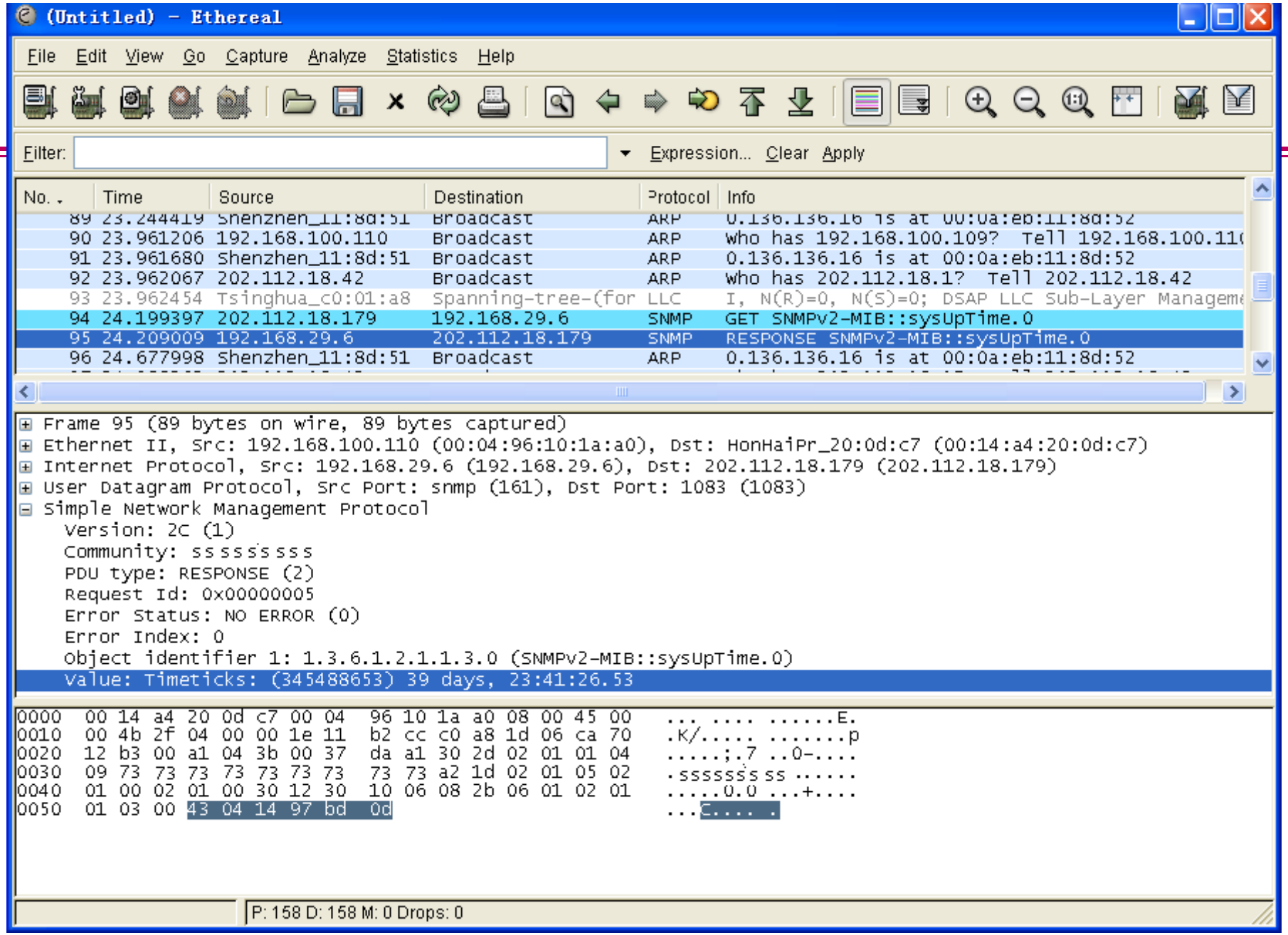

(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
89 23.244419 Shenzhen_11:8d:51 Broadcast ARP 0.136.136.16 is at 00:0a:eb:11:8d:52
90 23.961206 192.168.100.110 Broadcast ARP Who has 192.168.100.109? Tell 192.168.100.11
91 23.961680 Shenzhen_11:8d:51 Broadcast ARP 0.136.136.16 is at 00:0a:eb:11:8d:52
92 23.962067 202.112.18.42 Broadcast ARP Who has 202.112.18.1? Tell 202.112.18.42
93 23.962454 Tsinghua_c0:01:a8 Spanning-tree-(for LLC I, N(R)=0, N(S)=0; DSAP LLC Sub-Layer Manageme
94 24.199397 202.112.18.179 192.168.29.6 SNMP GET SNMPv2-MIB::sysUpTime.0
95 24.209009 192.168.29.6 202.112.18.179 SNMP RESPONSE SNMPv2-MIB::sysUpTime.0
96 24.677998 Shenzhen_11:8d:51 Broadcast ARP 0.136.136.16 is at 00:0a:eb:11:8d:52
Frame 94 (85 bytes on wire, 85 bytes captured)
Ethernet II, Src: HonHaiPr_20:0d:c7 (00:14:a4:20:0d:c7), Dst: 192.168.100.110 (00:04:96:10:1a:a0)
Internet Protocol, Src: 202.112.18.179 (202.112.18.179), Dst: 192.168.29.6 (192.168.29.6)
User Datagram Protocol, Src Port: 1083 (1083), Dst Port: snmp (161)
Simple Network Management Protocol
Version: 2C (1)
Community: ssssssss
PDU type: GET (0)
Request Id: 0x00000005
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: NULL
0000 00 04 96 10 1a a0 00 14 a4 20 0d c7 08 00 45 00 ....E.
0010 00 47 30 fb 00 00 40 11 8e d9 ca 70 12 b3 c0 a8 .G0...@. ...p....
0020 1d 06 04 3b 00 a1 00 33 8d c1 30 29 02 01 01 04 ...;...3 ..0)....
0030 09 73 73 73 73 73 73 73 73 73 a0 19 02 01 05 02 .ssssssss ss......
0040 01 00 02 01 00 30 0e 30 0c 06 08 2b 06 01 02 01 .....0.0 ...+....
0050 01 03 00 05 00 .....
P: 158 D: 158 M: 0 Drops: 0


(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
89 23.244419 Shenzhen_11:8d:51 Broadcast ARP 0.136.136.16 is at 00:0a:eb:11:8d:52
90 23.961206 192.168.100.110 Broadcast ARP Who has 192.168.100.109? Tell 192.168.100.11
91 23.961680 Shenzhen_11:8d:51 Broadcast ARP 0.136.136.16 is at 00:0a:eb:11:8d:52
92 23.962067 202.112.18.42 Broadcast ARP Who has 202.112.18.1? Tell 202.112.18.42
93 23.962454 Tsinghua_c0:01:a8 Spanning-tree-(for LLC I, N(R)=0, N(S)=0; DSAP LLC Sub-Layer Manageme
94 24.199397 202.112.18.179 192.168.29.6 SNMP GET SNMPv2-MIB::sysUpTime.0
95 24.209009 192.168.29.6 202.112.18.179 SNMP RESPONSE SNMPv2-MIB::sysUpTime.0
96 24.677998 Shenzhen_11:8d:51 Broadcast ARP 0.136.136.16 is at 00:0a:eb:11:8d:52
Frame 94 (85 bytes on wire, 85 bytes captured)
Ethernet II, Src: HonHaiPr_20:0d:c7 (00:14:a4:20:0d:c7), Dst: 192.168.100.110 (00:04:96:10:1a:a0)
Internet Protocol, Src: 202.112.18.179 (202.112.18.179), Dst: 192.168.29.6 (192.168.29.6)
User Datagram Protocol, Src Port: 1083 (1083), Dst Port: snmp (161)
Simple Network Management Protocol
Version: 2C (1)
Community: ssssssss
PDU type: GET (0)
Request Id: 0x00000005
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: NULL
0000 00 04 96 10 1a a0 00 14 a4 20 0d c7 08 00 45 00 ....E.
0010 00 47 30 fb 00 00 40 11 8e d9 ca 70 12 b3 c0 a8 .G0...@. ...p....
0020 1d 06 04 3b 00 a1 00 33 8d c1 30 29 02 01 01 04 ...;...3 ..0)....
0030 09 73 73 73 73 73 73 73 73 73 a0 19 02 01 05 02 .sssssssss......
0040 01 00 02 01 00 30 0e 30 0c 06 08 2b 06 01 02 01 .....0.0 ...+....
0050 01 03 00 05 00 ...
Object identifier (snmp.oid), P: 158 D: 158 M: 0 Drops: 0


(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
90 23.961206 192.168.100.110 Broadcast ARP Who has 192.168.100.109? Tell 192.168.100.11
91 23.961680 Shenzhen_11:8d:51 Broadcast ARP 0.136.136.16 is at 00:0a:eb:11:8d:52
92 23.962067 202.112.18.42 Broadcast ARP Who has 202.112.18.1? Tell 202.112.18.42
93 23.962454 Tsinghua_c0:01:a8 Spanning-tree-(for LLC I, N(R)=0, N(S)=0; DSAP LLC Sub-Layer Manageme
94 24.199397 202.112.18.179 192.168.29.6 SNMP GET SNMPv2-MIB::sysUpTime.0
95 24.209009 192.168.29.6 202.112.18.179 SNMP RESPONSE SNMPv2-MIB::sysUpTime.0
96 24.677998 Shenzhen_11:8d:51 Broadcast ARP 0.136.136.16 is at 00:0a:eb:11:8d:52
Frame 94 (85 bytes on wire, 85 bytes captured)
Ethernet II, Src: HonHaiPr_20:0d:c7 (00:14:a4:20:0d:c7), Dst: 192.168.100.110 (00:04:96:10:1a:a0)
Internet Protocol, Src: 202.112.18.179 (202.112.18.179), Dst: 192.168.29.6 (192.168.29.6)
User Datagram Protocol, Src Port: 1083 (1083), Dst Port: snmp (161)
Simple Network Management Protocol
Version: 2C (1)
Community: ssssssss
PDU type: GET (0)
Request Id: 0x00000005
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: NULL
0000 00 04 96 10 1a a0 00 14 a4 20 0d c7 08 00 45 00
0010 00 47 30 fb 00 00 40 11 8e d9 ca 70 12 b3 c0 a8
0020 1d 06 04 3b 00 a1 00 33 8d c1 30 29 02 01 01 04
0030 09 73 73 73 73 73 73 73 73 73 a0 19 02 01 05 02
0040 01 00 02 01 00 30 0e 30 0c 06 08 2b 06 01 02 01
0050 01 03 00 05 00
P: 158 D: 158 M: 0 Drops: 0


(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
89 23.244419 Shenzhen_11:8d:51 Broadcast ARP 0.136.136.16 is at 00:0a:eb:11:8d:52
90 23.961206 192.168.100.110 Broadcast ARP Who has 192.168.100.109? Tell 192.168.100.11
91 23.961680 Shenzhen_11:8d:51 Broadcast ARP 0.136.136.16 is at 00:0a:eb:11:8d:52
92 23.962067 202.112.18.42 Broadcast ARP Who has 202.112.18.1? Tell 202.112.18.42
93 23.962454 Tsinghua_c0:01:a8 Spanning-tree-(for LLC I, N(R)=0, N(S)=0; DSAP LLC Sub-Layer Manageme
94 24.199397 202.112.18.179 192.168.29.6 SNMP GET SNMPv2-MIB::sysUpTime.0
95 24.209009 192.168.29.6 202.112.18.179 SNMP RESPONSE SNMPv2-MIB::sysUpTime.0
96 24.677998 Shenzhen_11:8d:51 Broadcast ARP 0.136.136.16 is at 00:0a:eb:11:8d:52
Frame 95 (89 bytes on wire, 89 bytes captured)
Ethernet II, Src: 192.168.100.110 (00:04:96:10:1a:a0), Dst: HonHaiPr_20:0d:c7 (00:14:a4:20:0d:c7)
Internet Protocol, Src: 192.168.29.6 (192.168.29.6), Dst: 202.112.18.179 (202.112.18.179)
User Datagram Protocol, Src Port: snmp (161), Dst Port: 1083 (1083)
Simple Network Management Protocol
Version: 2C (1)
Community: ssssssss
PDU type: RESPONSE (2)
Request Id: 0x00000005
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: (345488653) 39 days, 23:41:26.53
0000 00 14 a4 20 0d c7 00 04 96 10 1a a0 08 00 45 00 ... .E.
0010 00 4b 2f 04 00 00 1e 11 b2 cc c0 a8 1d 06 ca 70 .K/..... ....p
0020 12 b3 00 a1 04 3b 00 37 da a1 30 2d 02 01 01 04 .....;.7 ..0-....
0030 09 73 73 73 73 73 73 73 73 73 a2 1d 02 01 05 02 .ssssssss ss......
0040 01 00 02 01 00 30 12 30 10 06 08 2b 06 01 02 01 .....0.0 ...+....
0050 01 03 00 43 04 14 97 bd 0d ...C.... .
Simple Network Manageme
P: 158 D: 158 M: 0 Drops: 0


(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
89 23.244419 Shenzhen_11:8d:51 Broadcast ARP 0.136.136.16 is at 00:0a:eb:11:8d:52
90 23.961206 192.168.100.110 Broadcast ARP Who has 192.168.100.109? Tell 192.168.100.11
91 23.961680 Shenzhen_11:8d:51 Broadcast ARP 0.136.136.16 is at 00:0a:eb:11:8d:52
92 23.962067 202.112.18.42 Broadcast ARP Who has 202.112.18.1? Tell 202.112.18.42
93 23.962454 Tsinghua_c0:01:a8 Spanning-tree-(for LLC I, N(R)=0, N(S)=0; DSAP LLC Sub-Layer Manageme
94 24.199397 202.112.18.179 192.168.29.6 SNMP GET SNMPv2-MIB::sysUpTime.0
95 24.209009 192.168.29.6 202.112.18.179 SNMP RESPONSE SNMPv2-MIB::sysUpTime.0
96 24.677998 Shenzhen_11:8d:51 Broadcast ARP 0.136.136.16 is at 00:0a:eb:11:8d:52
Frame 95 (89 bytes on wire, 89 bytes captured)
Ethernet II, Src: 192.168.100.110 (00:04:96:10:1a:a0), Dst: HonHaiPr_20:0d:c7 (00:14:a4:20:0d:c7)
Internet Protocol, Src: 192.168.29.6 (192.168.29.6), Dst: 202.112.18.179 (202.112.18.179)
User Datagram Protocol, Src Port: snmp (161), Dst Port: 1083 (1083)
Simple Network Management Protocol
Version: 2C (1)
Community: ssssssss
PDU type: RESPONSE (2)
Request Id: 0x00000005
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: (345488653) 39 days, 23:41:26.53
0000 00 14 a4 20 0d c7 00 04 96 10 1a a0 08 00 45 00 ... .E.
0010 00 4b 2f 04 00 00 1e 11 b2 cc c0 a8 1d 06 ca 70 .K/..... ....p
0020 12 b3 00 a1 04 3b 00 37 da a1 30 2d 02 01 01 04 .....;.7 ..0-....
0030 09 73 73 73 73 73 73 73 73 73 a2 1d 02 01 05 02 .ssssssss ss......
0040 01 00 02 01 00 30 12 30 10 06 08 2b 06 01 02 01 .....0.0 ...+....
0050 01 03 00 43 04 14 97 bd 0d ...C.... .
PDU type (snmp.pdutype), 2
P: 158 D: 158 M: 0 Drops: 0


(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
89 23.244419 Shenzhen_11:8d:51 Broadcast ARP 0.136.136.16 is at 00:0a:eb:11:8d:52
90 23.961206 192.168.100.110 Broadcast ARP Who has 192.168.100.109? Tell 192.168.100.11
91 23.961680 Shenzhen_11:8d:51 Broadcast ARP 0.136.136.16 is at 00:0a:eb:11:8d:52
92 23.962067 202.112.18.42 Broadcast ARP Who has 202.112.18.1? Tell 202.112.18.42
93 23.962454 Tsinghua_c0:01:a8 Spanning-tree-(for LLC I, N(R)=0, N(S)=0; DSAP LLC Sub-Layer Manageme
94 24.199397 202.112.18.179 192.168.29.6 SNMP GET SNMPv2-MIB::sysUpTime.0
95 24.209009 192.168.29.6 202.112.18.179 SNMP RESPONSE SNMPv2-MIB::sysUpTime.0
96 24.677998 Shenzhen_11:8d:51 Broadcast ARP 0.136.136.16 is at 00:0a:eb:11:8d:52
Frame 95 (89 bytes on wire, 89 bytes captured)
Ethernet II, Src: 192.168.100.110 (00:04:96:10:1a:a0), Dst: HonHaiPr_20:0d:c7 (00:14:a4:20:0d:c7)
Internet Protocol, Src: 192.168.29.6 (192.168.29.6), Dst: 202.112.18.179 (202.112.18.179)
User Datagram Protocol, Src Port: snmp (161), Dst Port: 1083 (1083)
Simple Network Management Protocol
Version: 2C (1)
Community: ssssssss
PDU type: RESPONSE (2)
Request Id: 0x00000005
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: (345488653) 39 days, 23:41:26.53
0000 00 14 a4 20 0d c7 00 04 96 10 1a a0 08 00 45 00 ... .E.
0010 00 4b 2f 04 00 00 1e 11 b2 cc c0 a8 1d 06 ca 70 .K/..... ....p
0020 12 b3 00 a1 04 3b 00 37 da a1 30 2d 02 01 01 04 .....;.7 ..0-....
0030 09 73 73 73 73 73 73 73 73 73 a2 1d 02 01 05 02 .sssssss ss ......
0040 01 00 02 01 00 30 12 30 10 06 08 2b 06 01 02 01 .....0.0 ...+....
0050 01 03 00 43 04 14 97 bd 0d ...C.... .
P: 158 D: 158 M: 0 Drops: 0

3.1.3 SNMPv2

- SNMPv1简单易实现，但没有实质性的安全措施，无数据源认证功能，不能防止被偷听。为弥补SNMP的安全缺陷，1992年发布S-SNMP，该协议增强了以下安全方面的功能：用报文摘要算法MD5保证数据完整性和进行数据源认证；用时间戳对报文排序；用DES算法提供数据加密功能。
- 但S-SNMP没有改进SNMP功能和效率方面的缺点。于是又提出SMP协议，该协议在使用范围、复杂程度、速度和效率、安全措施、兼容性等方面对SNMP进行了扩充。1993年发布SNMPv2，它以SMP为基础，放弃了S-SNMP。
- 1996年1月发布SNMPv2C

SNMPv2

SNMPv2 SMI对SNMPv1 SMI进行了扩充，提供了更严格的规范，规定了新管理对象和MIB文件，是SNMPvl SMI的超集。

SNMPv2相对于SNMPv1的改进：

(1) 加强了数据定义语言，改进了SMI，定义扩充了对象类型宏，增强对象表达能力，扩展了数据类型

(2) 提供了更完善的表操作能力，支持分布式管理

(3) 定义了新MIB功能组，丰富了故障处理能力

(4) 引入两种新PDU，用于大数据块的传送和管理者之间的通信。

SNMPv2中对象的定义

- SNMPv2的对象定义的变化

(1) 数据类型：

① 增加了两种数据类型Unsigned32和Counter64

② 规定计数器没有已定义的“初始值”

③ 计量器类型达到最大值时保持其最大值，并可随信息的减少而减少，计量器最大值可以设置为小于$2^{32}-1$

SNMPv2中对象的定义

(2) Units Part：增加了UNITS子句

这个子句用文字说明与对象有关的度量单位。比如时间，示例如下：　　UNITS　“seconds”

(3) MAX-ACCESS子句：去掉write-only，增加read-create和accessible-for-notify。

访问级别(由低到高)：

- not-accessible(不可访问)
- accessible-for-notify(通报访问，通报访问对象只有在网络管理器或其他代理进行通告时才有效，直接查询该对象是不允许的)
- read-only(只读)
- read-write(读写)
- read-create(读-创建)

SNMPv2中对象的定义

(4) STATUS子句：指明对象状态

SNMPv2标准去掉了SNMPvl中的optional和mandatory，只有3种可选状态。

① current:表示在当前的标准中是有效的

② obsolete:表示对象已经过时了，不必实现这种对象

③ deprecated:表示对象已经过时了，但是为了兼容旧版本实现互操作，实现时还要支持这种对象。

SNMPv2中表的操作

- 表的类型

(1) 禁止管理者进行行生成和行删除的表

这种表的最高的访问级别是read-write。在很多情况下这种表由代理控制，表中只包含read-ouly型的对象。

(2) 允许管理者进行行生成和行删除的表

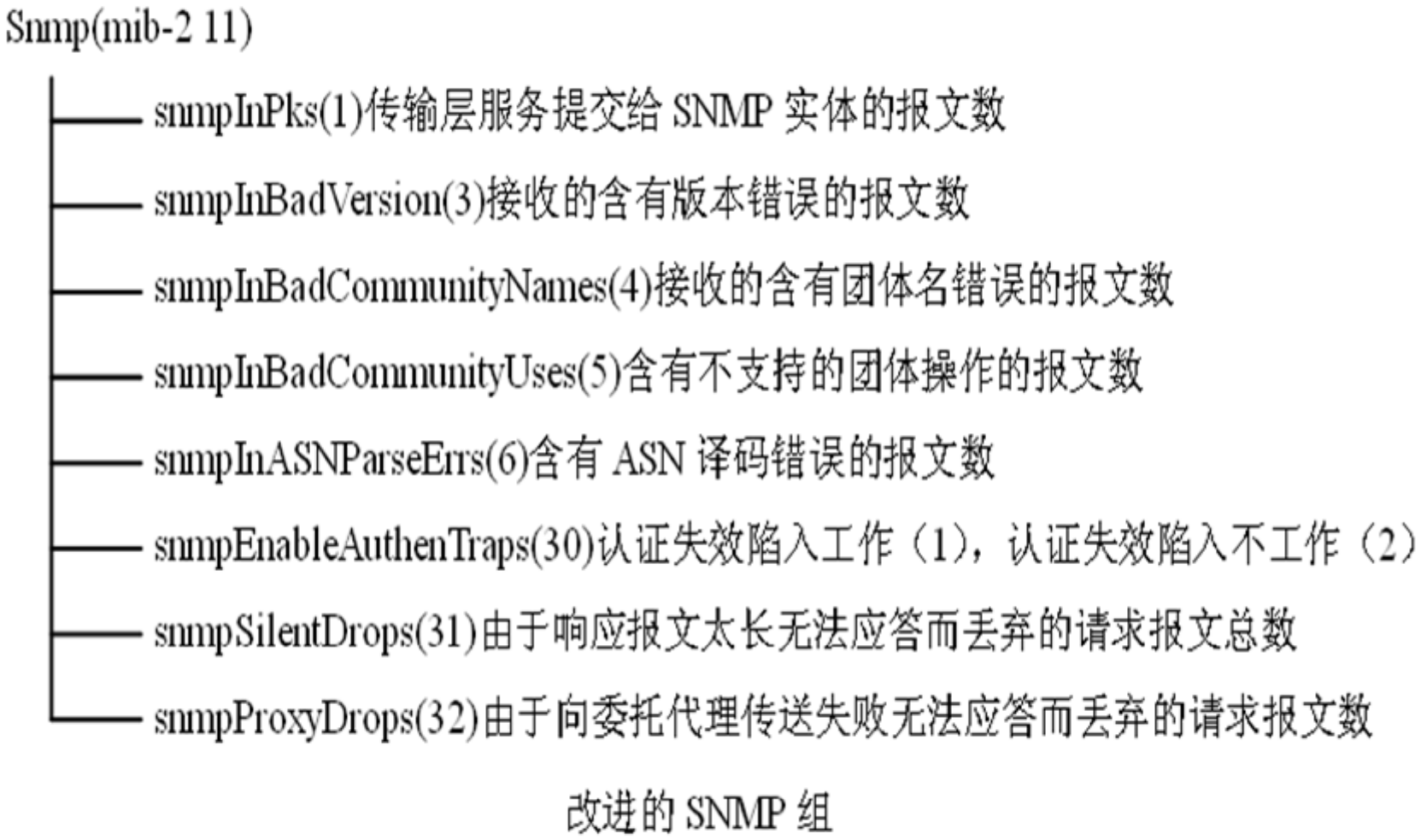
这种表开始时可能没有行，由管理站生成和删除行。行数可由管理站或代理改变。

SNMPv2管理信息库

- Snmp组

  Snmp组是由MIB-2的对应组改造而成的，有些对象被删除，同时又增加了一些新对象，新的Snmp组对象少了，去掉了许多对排错作用不大的变量。

SNMPv2管理信息库



改进的 SNMP 组

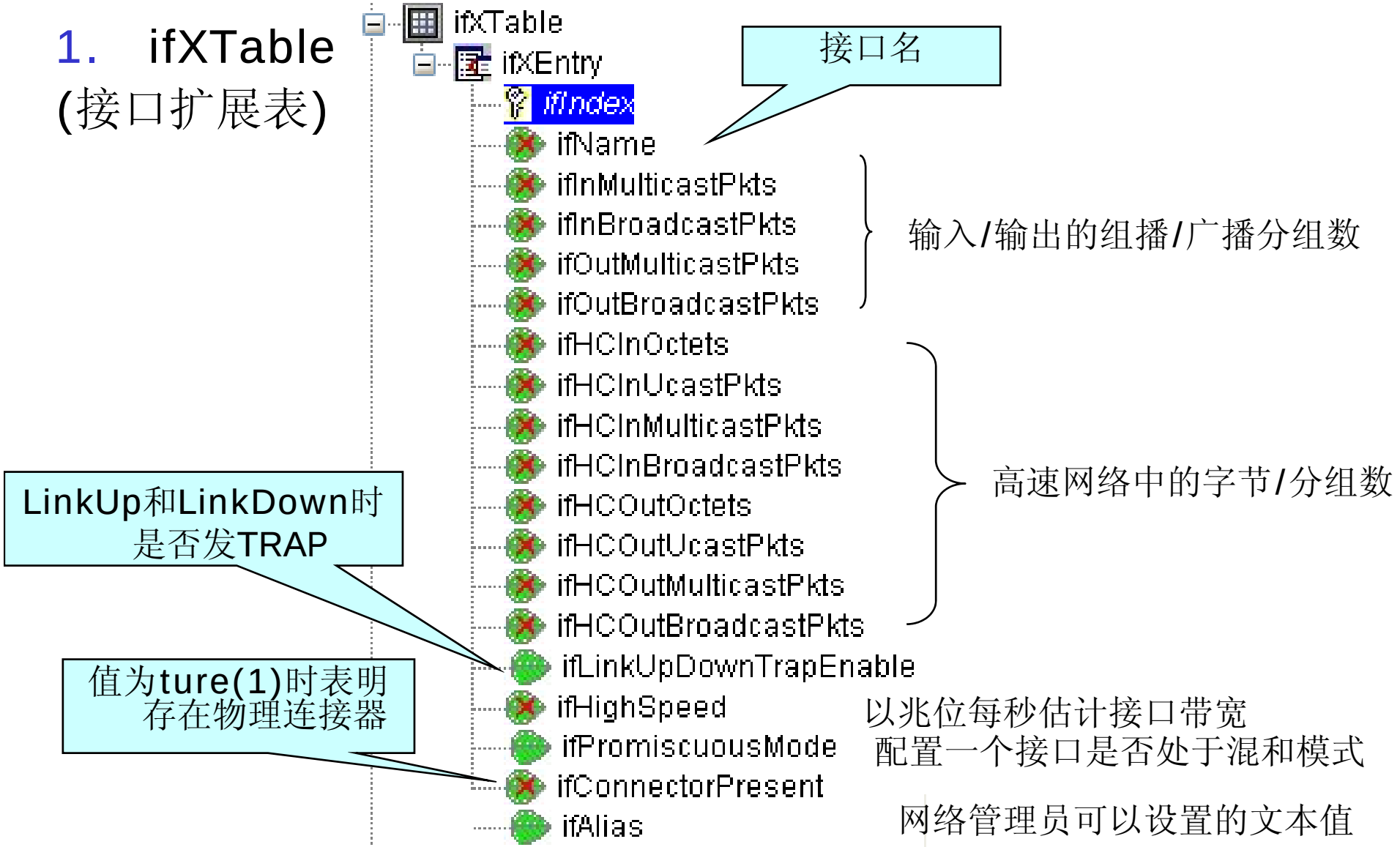
SNMPv2管理信息库

接口组

- 新引入4个表
  - ifXTable
  - ifStackTable
  - ifTestTable
  - ifRcvAddressTable
- 改进的几个地方:
  - 广播包和多点发送包分开计数
  - 使用64位计数器替换32位计数器
  - 接口可以大于2.2G
  - 提供在物理接口之上映射虚拟接口的方法
  - 去掉ifInNucastPkts, ifOutNucastPkts, ifSpecific, ifOutQLen

接口组

1. ifXTable (接口扩展表)



接口组

2. ifStackTable(接口堆栈表)

- 显示了网络接口的不同子层之间的关系。
- 包含关于哪些子层运行在其他哪些子层上的信息
- 相关对象

(1) ifStackHigherLayer：相应于关系的高子层的ifIndex值。

(2) ifStackLowerLayer：相应于关系的低子层的ifIndex值。

(3) ifStackStatus：RowStatus对象，可能是active、notInService 或destroy，用于在该表中添加/删除行

例：ifStackStatus.0.133:-->active(1)

接口组

3. ifTestTable(接口测试表)

作用：由管理站指示代理系统测试接口的故障。

（1）ifTestId：每个测试的唯一标识符

（2）ifTestStatus：测试是否正在进行，可以是notInUse和inUse

（3）ifTestType：测试类型，如noTest，test-to-run

（4）ifTestResult： none(1), success(2),inProgress(3), notSupported(4), unAbleToRun(5), aborted(6), failed(7)

（5）ifTestCode：测试结果代码

（6）ifTestOwner：管理站标识符

接口组

4. ifRcvAddressTable(接口地址表)

包含每个接口对应的各种地址：广播地址、多播地址和单播地址

（1）ifRcvAddressAddress：接口接收分组的地址

（2）ifRcvAddressStatus：RowStatus对象，用于行的删除和修改

（3）ifRcvAddressType：地址的类型，可能是other(1), volatile(2),nonVolatile(3)

SNMPv2的协议操作

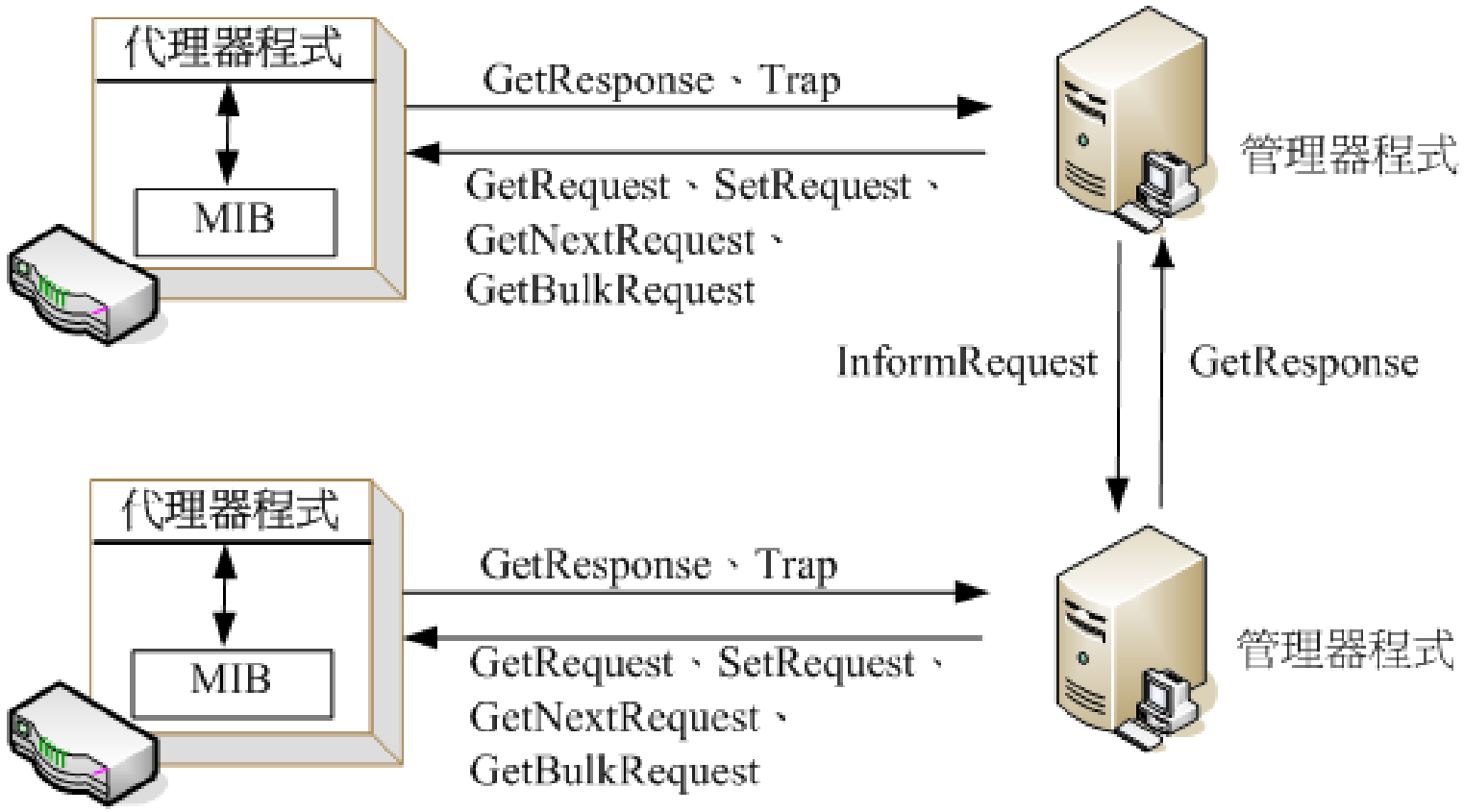
- SNMPv2访问管理信息的方法

(1) 管理者和代理之间请求/响应通信

(2) 管理者之间

(3) 代理向管理者发送陷阱报文

SNMPv2的协议操作



SNMPv2协议数据单元

1．SNMPv2报文

SNMPv2报文的结构分为3部分：版本号、团体名和作为数据传送的PDU。这个格式与SNMPvl一样。版本号取值0代表SNMPvl，取值1代表SNMPv2。团体名提供简单的认证功能，与SNMPvl的用法一样。

SNMPv2协议数据单元

SNMPv2实体发送报文一般要经过下面4个步骤。

（1）根据要实现的协议操作构造PDU。

（2）把PDU、源和目标端口地址以及团体名传送给认证服务，认证服务产生认证码或对数据进行加密，返回结果。

（3）加入版本号和团体名，构造报文。

（4）进行BER 编码，产生0/1比特串，发送出去。

SNMPv2协议数据单元

SNMPv2实体接收到一个报文后要完成下列动作。

（1）对报文进行语法检查，丢弃出错的报文。

（2）把PDU部分、源和目标端口号交给认证服务。如果认证失败，发送一个陷入，丢弃报文。

（3）如果认证通过，则PDU转换成ASN.1 形式。

（4）协议实体对PDU做句法检查，如果通过，根据团体名和适当的访问策略作相应的处理。

SNMPv2协议数据单元

SNMPv2 报文

(a) GetRequest、GetNextRequest、SetRequest、InformRequest 和 Trap

PDU 类型	请求标识	0	0	变量绑定表

(b) ResponsePDU

PDU 类型	请求标识	错误标志	错误索引	变量绑定表

(c) GetBulkRequest PDU

PDU 类型	请求标识	非重复数 N	最大后继数 M	变量绑定表

图 5-25　SNMPv2 PDU 格式

SNMPv2的协议操作

1. SNMPv2 Traps

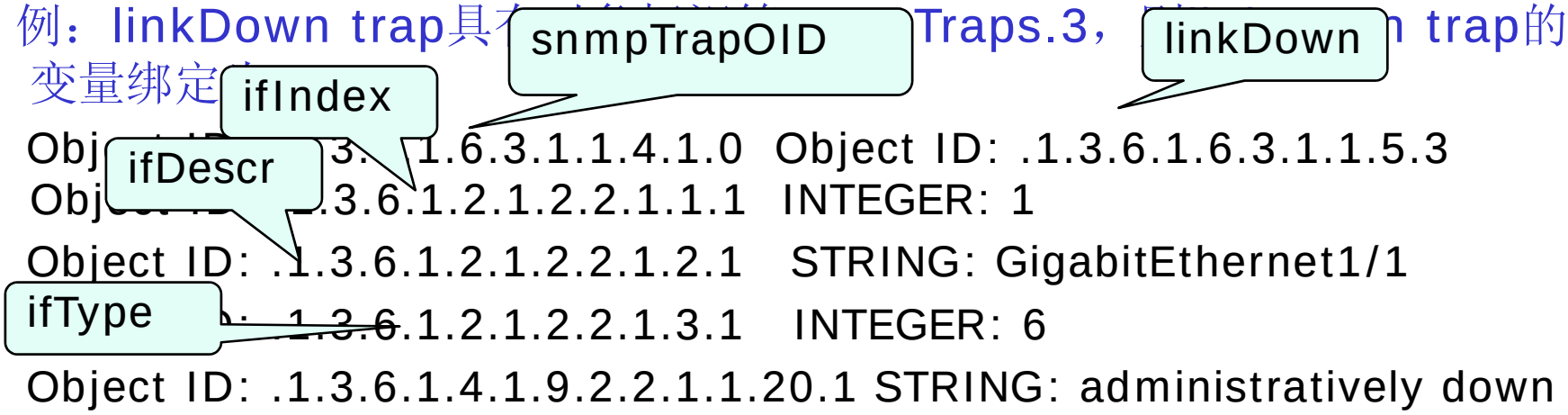
0xA7	请求标识符	0	0	变量绑定表

SNMPv2 traps的特点：

(1) 关于trap的信息被嵌入在变量绑定中

(2) SNMPv1定义的通用trap具有与SNMPv2定义的对象标识符相同的值

例：linkDown trap具有[illegible]Traps.3，[illegible] trap的变量绑定[illegible]



SNMPv2的协议操作

2. InformRequest

- Inform：仅仅是一个需要得到响应的SNMPv2 Trap。
- InformRequest-PDU格式

0xA6	请求标识符	0	0	变量绑定表

引入inform是为了解决trap丢失的问题，但是它不能完全解决问题，还可能使问题恶化。

SNMPv2的协议操作

3. Get-Bulk

在概念上与通过重复的get-next命令遍历一个表的逻辑类似。

优点：改善了性能，当响应太大而不能在一条消息中容纳时，它将被截断以发送尽可能大的消息。

作用：允许用户获取表的一部分

PDU格式

0xA5	请求标识符	n	m	变量绑定表

n是non-repeaters，m是max-repetitions

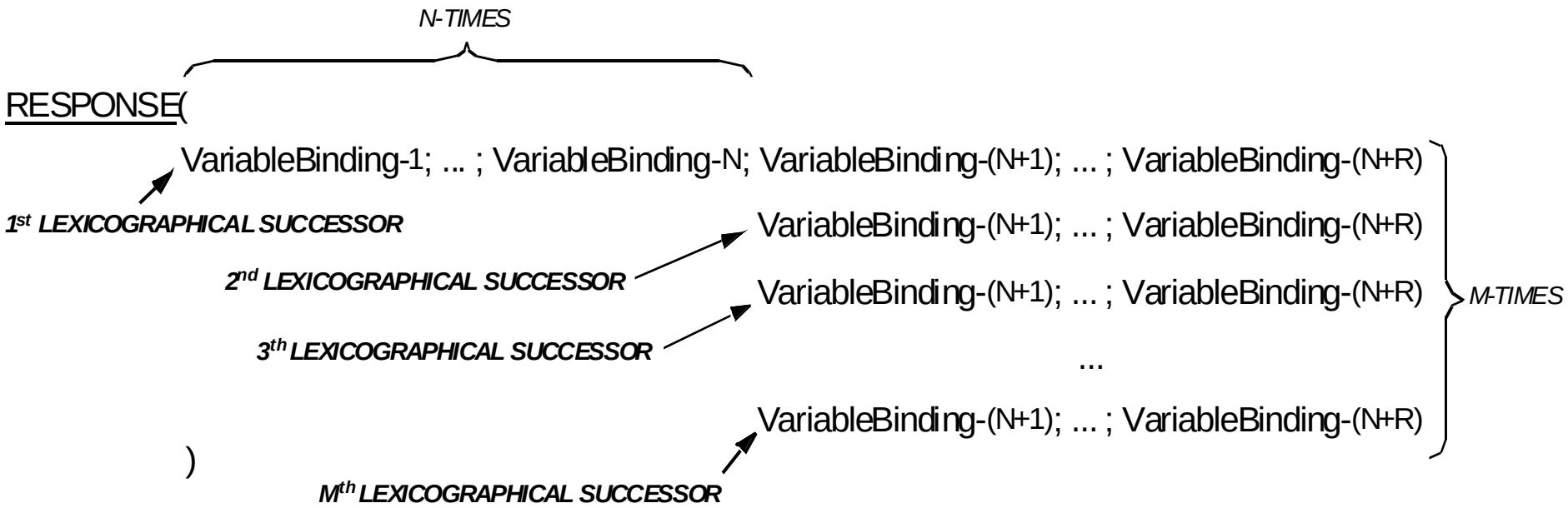
SNMPv2的协议操作

3. Get-Bulk

REQUEST(non-repeaters = N; max-repetitions = M;

VariableBinding-1; ... ; VariableBinding-N; VariableBinding-(N+1); ... ; VariableBinding-(N+R)

)



SNMPv2的协议操作

例：

getBulkRequest{non-repeaters=1,max-repetitions=3,
varbindlist={sysUpTime,ifInOctets,ifInErrors}}

响应：

sysUpTime.0 12432
ifInOctets.1 34543
ifInErrors.1 11
ifInOctets.2 222
ifInErrors.2 33
ifInOctets.3 44346
ifInErrors.3 0

SNMPv2的协议操作

4. 其他差错状态

(1) noAccesss(6)：试图设置一个不可访问的变量

(2) wrongType(7)：试图把一个变量设置成与它所要求类型不一致的值

(3) wrongLength(8)：试图把一个变量设置成与它所要求长度不一致的值

(4) wrongEncoding(9)：试图把一个变量设置成其ASN.1编码与该字段的ASN.1标记不一致的值

(5) wrongValue(10)：试图把一个变量设置成不正确的值

(6) noCreation(11)：试图修改或创建一个不存在并且不能创建的变量

(7) inconsistent Value(12)：试图把一个变量设置成与当前值不一致的值

SNMPv2的协议操作

(8) resourceUnavailable(13)：试图把一个变量设置成要求收集不存在的资源的值

(9) commitFailed(14)：一个set操作失败

(10) undoFailed(15)：一个set操作失败并且有些赋值不能恢复

(11) authorizationError(16)：get、get-next、set或inform请求没有通过认证

(12) notWritable(17)：试图修改一个当前存在但是不能被修改的变量

(13) inconsistentName(18)：试图修改一个当前不存在并且当前不能创建的变量

SNMPv2的协议操作

5. get与get-next的改进

- SNMPv1与SNMPv2的get和get-next的区别：当指定的变量之一无法获取时，响应的处理方式不同。

例：发送对象{ifIndex.5, ifDescr.20, protocolDistStatsPkts.1}的SNMPv2 get请求，该设备没有索引为20的接口或不支持RMONv2

ifIndex.5	5
ifDescr.20	noSuchInstance
protocolDistStatsPkts.1	noSuchObject

3.1.4 SNMPv3

SNMPv3特点：

(1) 适应性强

(2) 扩充性好

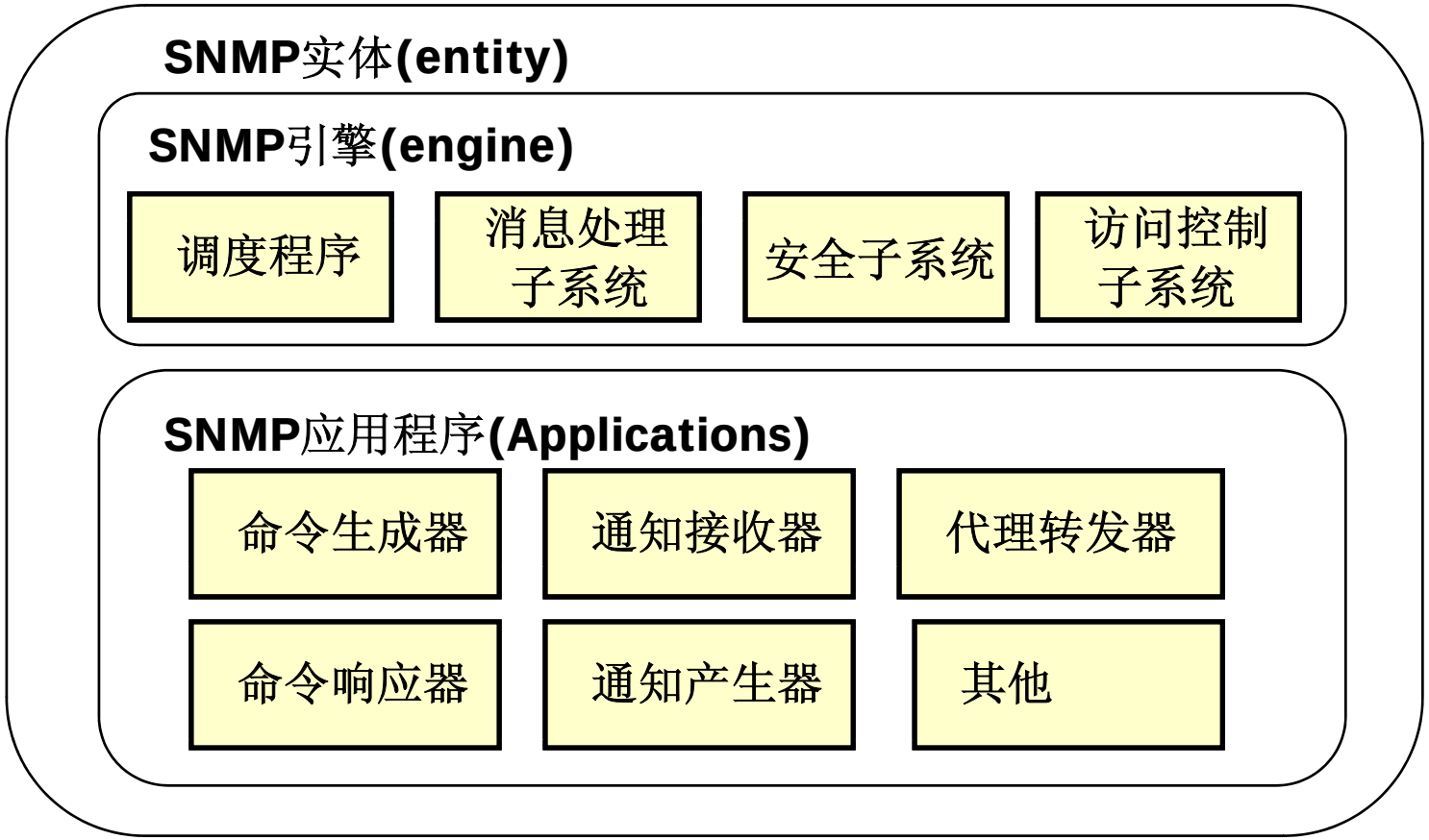
(3) 安全性好

SNMPv3体系结构

- SNMP实体：以前的SNMP代理和SNMP管理者的统称。
- 组成：SNMP引擎和SNMP应用程序

SNMPv3体系结构

- SNMP实体



SNMPv3体系结构

1. SNMP引擎

SNMP引擎提供三项服务：发送和接收报文；认证和加密报文；控制对管理对象的访问。

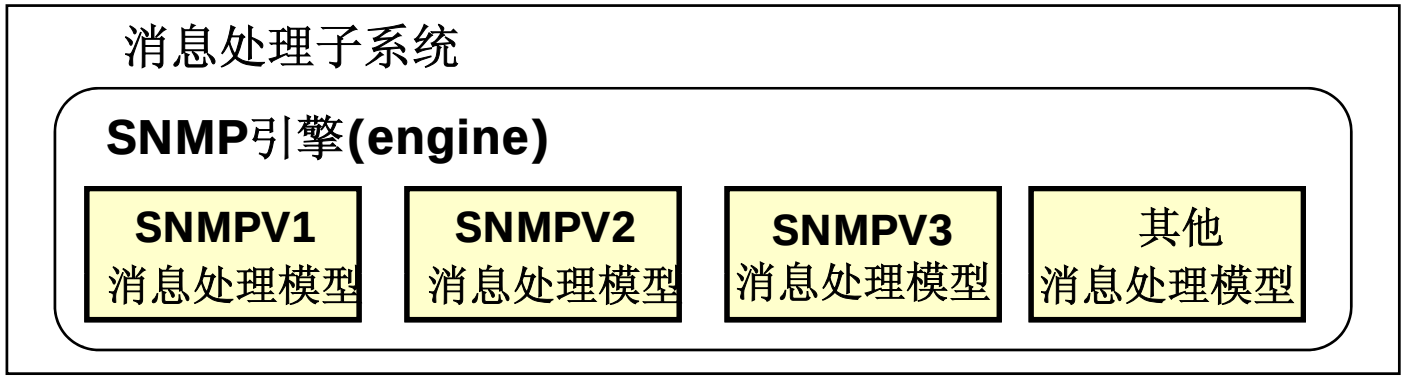
(1) 调度程序

负责发送和接收消息。确定SNMP报文的版本，并交给相应的报文处理模块处理。

(2) 消息处理子系统

由一个或多个消息处理模型组成。

功能：按照预定的格式准备要发送的消息或者从接收到的消息中提取数据。

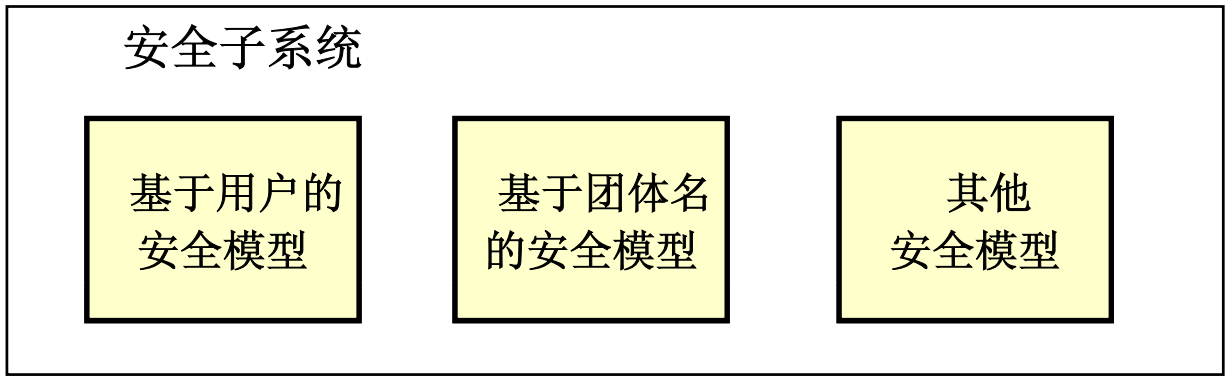


SNMPv3体系结构

1. SNMP引擎

(3) 安全子系统

提供验证消息和加/解密消息的安全服务



① 基于用户的安全模型：提供身份验证和数据保密服务

② 基于团体的安全模型

③ 其他安全模型：企业待定的；将来的标准

SNMPv3体系结构

1. SNMP引擎

(4) 访问控制子系统

确定是否允许访问管理对象，或者是否可以对某个管理对象实施特殊的管理操作

SNMPv3体系结构

1. SNMP引擎

(4) 访问控制子系统

用于确定是否允许访问管理对象：

① 当处理一个**SNMPGet，Get-Next，Get-Bulk**或**SetPDU**时调用它以确认在变量绑定中所指定的**MIB**对象允许访问。

② 当生成一个通知时调用它以确保在变量绑定中所指定的**MIB**对象允许访问。

SNMPv3体系结构

2. 应用程序

类型：

(1) 命令生成器:生成收集或设置管理数据的SNMP命令

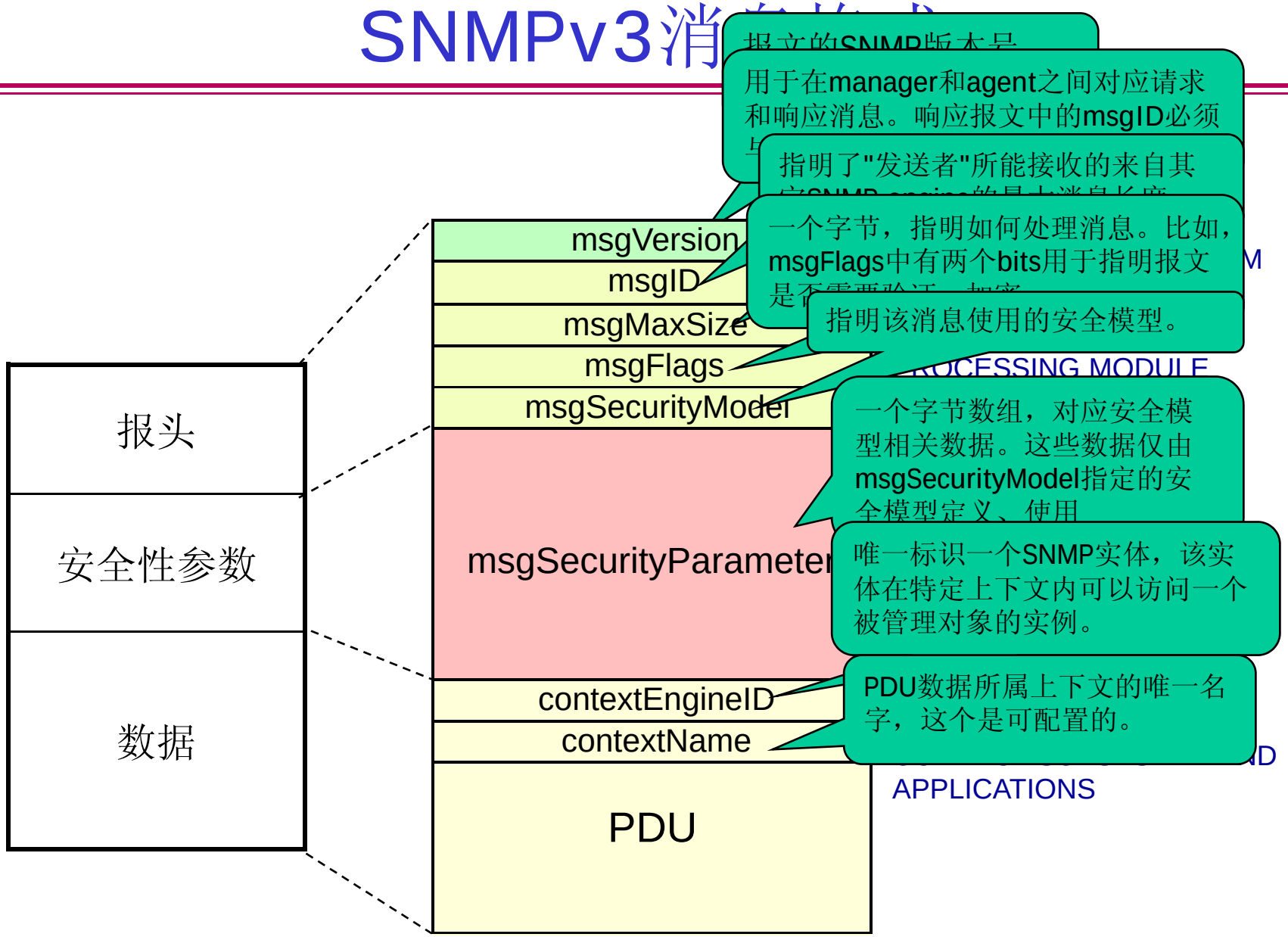
(2) 命令应答器:接收SNMP Read/Write请求，对管理数据进行访问，并按照协议规定的操作产生响应报文，返回给读/写命令的发送者。

(3) 通知产生器:监控系统中出现的特殊事件，产生Trap或Inform消息

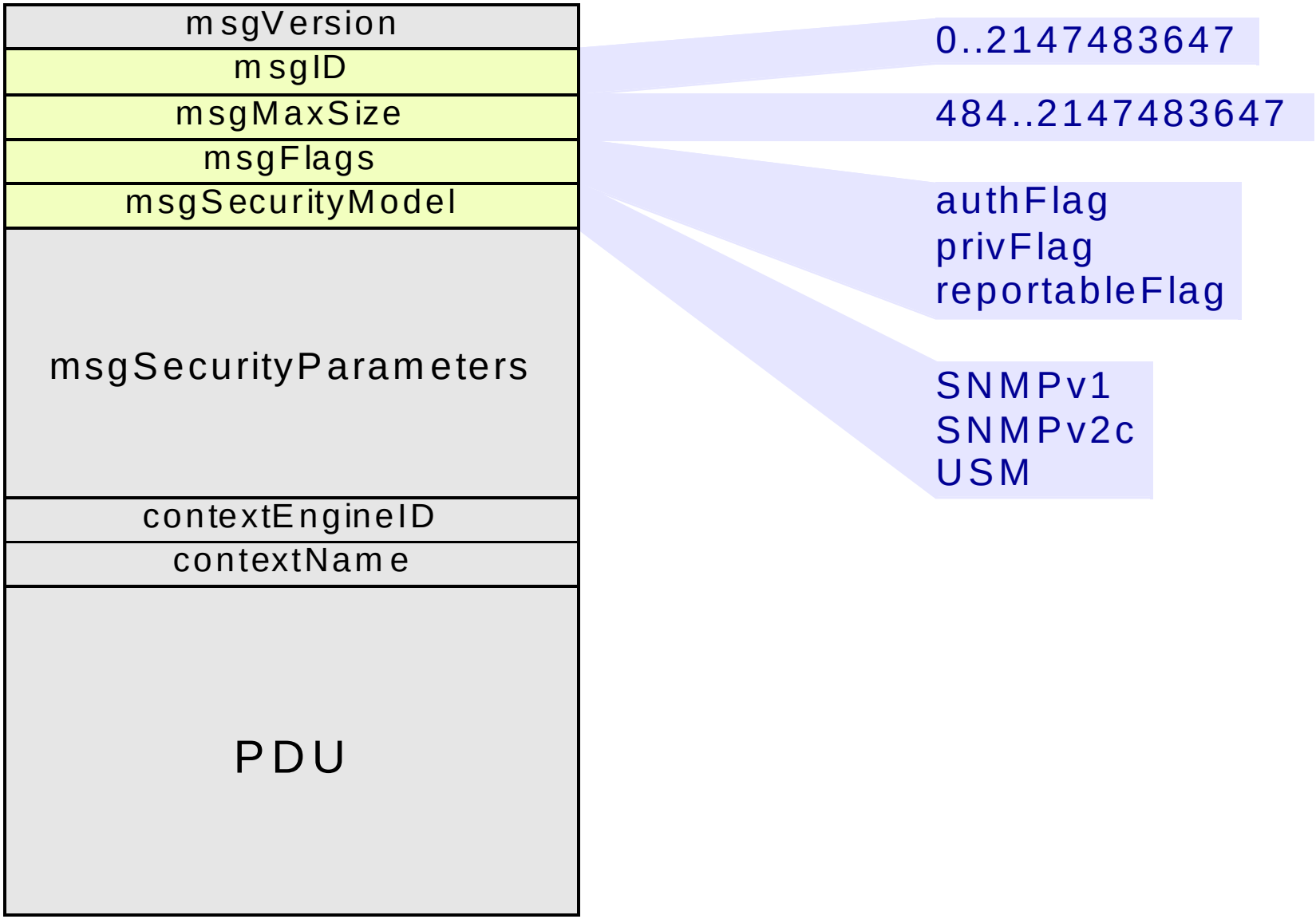
(4) 通知接收器:接收并处理Trap或Inform消息

(5) 代理转发器:转发SNMP实体之间的消息

SNMPv3消


报头
安全性参数
数据
msgVersion
msgID
msgMaxSize
msgFlags
msgSecurityModel
msgSecurityParameter
contextEngineID
contextName
PDU
用于在manager和agent之间对应请求和响应消息。响应报文中的msgID必须
指明了"发送者"所能接收的来自其
一个字节，指明如何处理消息。比如，msgFlags中有两个bits用于指明报文
指明该消息使用的安全模型。
一个字节数组，对应安全模型相关数据。这些数据仅由msgSecurityModel指定的安全模型定义、使用
唯一标识一个SNMP实体，该实体在特定上下文内可以访问一个被管理对象的实例。
PDU数据所属上下文的唯一名字，这个是可配置的。
APPLICATIONS

SNMPv3 PROCESSING MODULE PARAMETERS



3.2公共管理信息协议

3.2.1CMIP/CMIS概述

公共管理信息协议（Common Management Information Protocol，CMIP）协议是在OSI制订的网络管理框架中提出的网络管理协议，所提供的服务是公共管理信息服务（Common Management Information Service，CMIS）。CMIP包含以下组成部分：一套用于描述协议的模型，一组用于描述被管对象的注册、标识和定义的管理信息结构，被管对象的详细说明以及用于远程管理的原语和服务。CMIP与SNMP一样，也是由被管代理和管理者、管理协议与管理信息库组成。在CMIP中，被管代理和管理者没有明确的指定，任何一个网络设备既可以是被管代理，也可以是管理者。

3.3基于WEB的管理技术

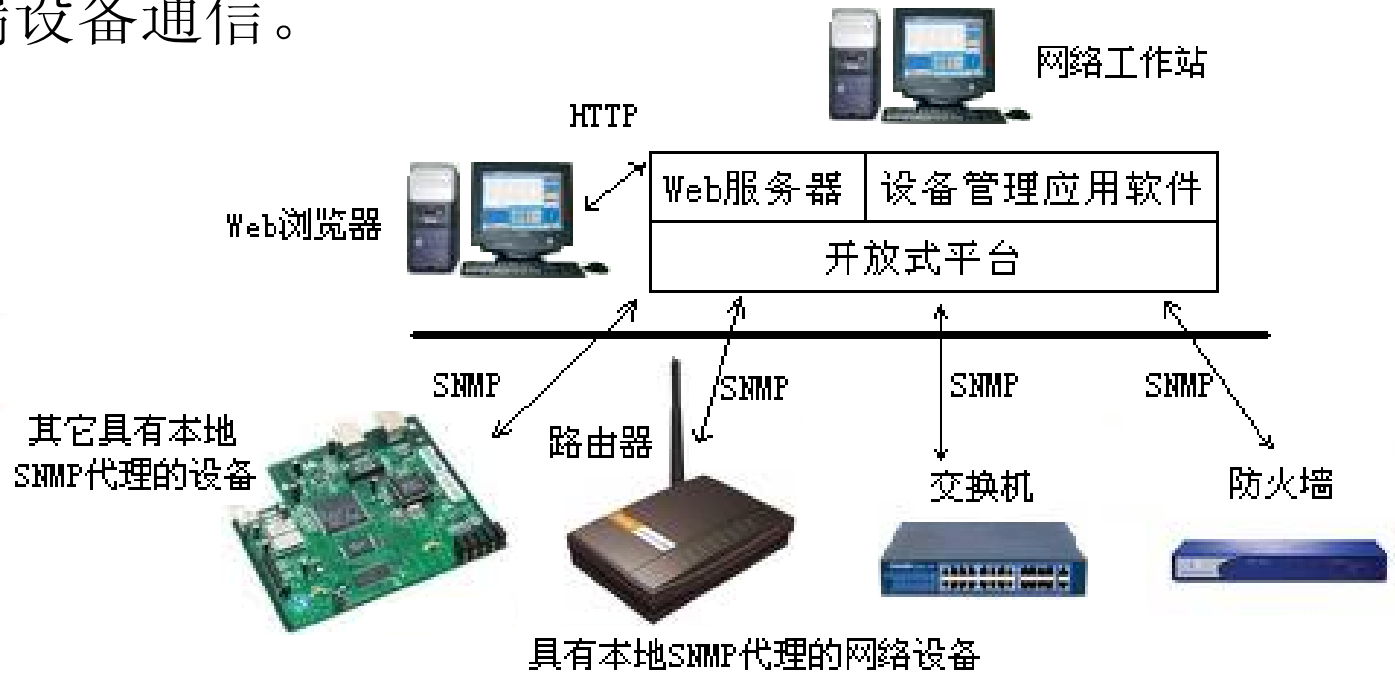
3.3.1 WBM概述

- WBM（Web-Based Management）技术允许网络管理人员用任何一种Web 浏览器，在网络任何节点上方便迅速地配置、控制以及存取网络和它的各种部分。WBM是网管方案的一次革命，它将使网络用户管理网络的方式得以改善。
- WBM融合了Web功能与网管技术，从而为网管人员提供了比传统工具更强有力的能力。管理人员应用WBM能够通过任何Web浏览器、在任何站点监测和控制企业网络，而不再只拘泥于网管工作站，并且由此能够解决很多由于多平台结构产生的互操作性问题。
- WBM的结果降低了管理信息系统全体培训的费用又促进了更多的用户去利用网络运行状态信息。

3.3.2 WBM的实现方法

- 1．代理方式

代理方式也就是将一个Web服务器加到一个内部工作站（代理）上，这个工作站轮流与端设备通信，浏览器用户通过HTTP协议与代理通信，同时代理通过SNMP协议与端设备通信。



2．嵌入方式

嵌入方式将Web能力真正地嵌入到网络设备中，每个设备有它自己的Web地址，管理人员可轻松地通过浏览器访问到该设备并且管理它。

图 3-10　基于 Web 管理的嵌入方式

3.3.3 WBM的标准

- 有两项WBM标准正处于考虑之中。
  - 一个是WBEM（Web-Based Enterprise Management）标准，于1996年7月推出，是Microsoft最先提出的，包括3Com在内的60多个提供商都支持此项标准。此项标准是面向对象的，能够将从多来源（设备、系统、应用程序）以多协议（例如SNMP，DMI）获得的数据抽象化，它加强了管理能力并且使它们通过单一的协议出现。WBEM “兼容和扩展”了当前的标准，如SNMP、DMI和CMIP，并不是取而代之。但它的真正目标是强化对于网络元素和系统的管理。WBEM的关键是一个新的协议HMMP（Hypermedia Management Protocol），这个传输协议处理包括重发功能、分组速率、传送证实以及允许一个报文拆成一个或几个分组等功能。
  - 一个WBM标准是（Java-Management Application Program Interface），它被作为Sun的Java标准扩展API结构的一部分。JMAPI其实是一个完整的网络管理应用程序开发环境，它提供了一个厂商当今不得不收集到的完全的特性清单，包括生成资源清单表格、图像的用户接口、SNMP的网络API、远程过程调用主机、数据库访问方法以及式样向导。

3.4本章小结

- 本章主要介绍了SNMP的发展、基本框架、格式、通信机制等内容。首先介绍了SNMP演化的过程，并对其基本结构框架、协议环境、基本应用配置等基础知识进行了介绍。接着分别介绍了SNMPv1、SNMPv2、SNMPv3的基本特点，最后介绍了基于WBM的网络管理思想。
- SNMP采用了基于Client/Server形式的管理者--代理模型，网络的管理与维护是通过管理者与代理间的交互工作完成的。目前，SNMP有3 种：SNMPV1、SNMPV2、SNMPV3。第1版和第2版没有太大差距，但SNMPV2是增强版本，包含了其它协议操作。与前两种相比，SNMPV3则包含更多安全和远程配置。为了解决不同SNMP版本间的不兼容问题，RFC3584中定义了三者共存策略。
- 本章的重点是掌握不同版本SNMP的功能和特点，理解其通信的机制和应用。