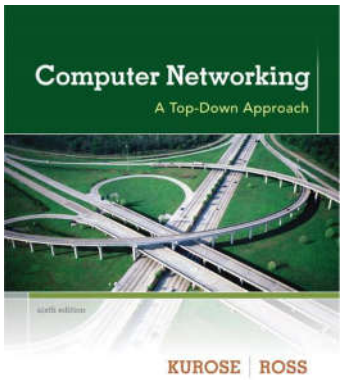
3 网络管理

中国科学技术大学
自动化系 郑烃



Computer Networking: A Top Down Approach
6th edition
Jim Kurose, Keith Ross
Addison-Wesley

3 :网络管理

- 网络管理引论
  - 动机
  - 功能和定义
  - 主要部件
- 互联网网络管理架构
  - SMI:管理信息结构
    - 命名:OID
    - 语法: ASN.1
    - 传输编码: BER
  - SNMP:互联网网络管理协议
  - 安全性

3 :网络管理

- 网络管理引论
  - 动机
  - 功能和定义
  - 主要部件
- 互联网网络管理架构
  - SMI:管理信息结构
    - 命名:OID
    - 语法: ASN.1
    - 传输编码: BER
  - SNMP:互联网网络管理协议
  - 安全性

网络管理的必要性

- 机构网络的现状
  - 设备数量多: 几百台
  - 设备种类多: 链路、交换机、路由器、主机、协议等
- 出现问题很正常
  - 设备本身故障
  - 配置问题
  - 对资源（例如链路带宽）过度使用
- 网络管理的必要性
  - 协助网管定位和解决问题
  - 提前发现问题，预警

设备管理的现实例子

- 飞机控制室、DCS控制系统
- 设备管理的功能
  - 监测系统各部件的运行状态（输入）
    - 管理人员查询设备(查询，定期)
    - 设备在异常时主动上报
  - 根据状态和目标，干涉系统的运行，发出执行动作（输出）
- 最终目的：监控各设备运行状态，保证系统的正常运行

希望网络管理达到的目标

- 监测网络（各部件）的运行状态
- 故障时异常时报警
- 允许管理人员干涉系统的运行（重启、配置参数等）
- 自动、远程

早期互联网的网络管理

- 人工ping设备，判断问题
- 远程电话让同事帮忙
- 自己去解决问题

网络管理的功能举例

- 检测主机或路由器的网卡故障（网卡发去的帧错误增加）
- 自动监测主机的活跃程度；
- 监测流量；
  - 某网段的流量增加，可以将服务器迁到另一个网段
  - 某网段的流量超过阈值，在用户感知之前，升级带宽
- 路由表格的快速变化,配置问题,在网络发生问题前发现并修复。
- SLA监测：掉线率，延迟，吞吐量,达到下限报警
- 入侵检测：攻击行为，检测和报警；

3 ：网络管理

- 网络管理引论
  - 动机
  - 功能和定义
  - 主要部件
- 互联网网络管理架构
  - SMI：管理信息结构
    - 命名：OID
    - 语法：ASN.1
    - 传输编码：BER
  - SNMP：互联网网络管理协议
  - 安全性

网络管理的5大功能

- 性能管理：
  - 性能（利用率、吞吐量）量化、测量、报告、分析和控制不同网络部件的性能
  - 涉及到的部件：单独部件（网卡，协议实体），端到端的路径
- 故障管理：记录、检测和响应故障；
  - 性能管理为长期监测设备性能
  - 故障管理：突然发生的强度大的性能降低，强调对故障的响应
- 配置管理：跟踪设备的配置，管理设备配置信息
- 账户管理：定义、记录和控制用户和设备访问网络资源
  - 限额使用、给予使用的收费，以及分配资源访问权限
- 安全管理：定义安全策略，控制对网络资源的使用

网络管理的定义

- 网络管理包括了硬件、软件和人类元素的设置、综合和协调，以便监测、测试、轮询、配置、分析、评价和控制网络和网元资源，用合理的成本满足实时性、运行能和服务质量的要求

3 ：网络管理

- 网络管理引论
  - 动机
  - 功能和定义
  - 主要部件
- 互联网网络管理架构
  - SMI：管理信息结构
    - 命名：OID
    - 语法：ASN.1
    - 传输编码：BER
  - SNMP：互联网网络管理协议
  - 安全性

网络管理的实质

- 实质：远程（分布式）监测（查询、定期上报，以及异常异步报告）和控制
- 实例：集团和分支机构
  - 分支定期报告，产量等信息；
  - 分支主动报告异常；
  - 总部问分支：上报信息（指标）

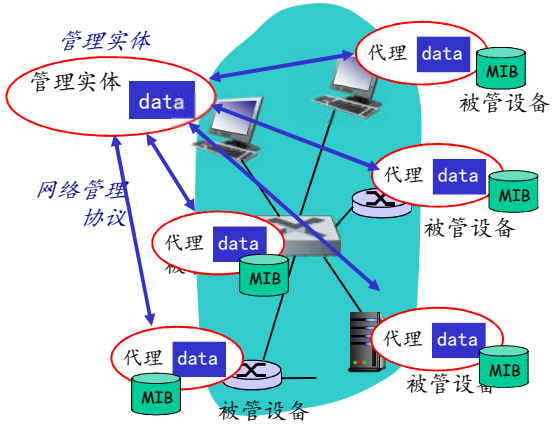
  分支向总部报告：主动或被动
  - 总部发出指令，让分支动作；

  总部向分支：发出指令

网络管理体系结构

- 管理实体：在NOC网络管理工作站上的应用程序（**老板**）
  - 执行网络管理动作：收集、处理、分析、显示
- 被管设备：主机、路由器、交换机、打印机、modem（**分支机构**）
  - 被管设备包括若干被管对象
    - 硬件的一个部分（网卡）
    - 某些硬件或软件的配置参数集合（RIP路由协议）
  - 被管对象的信息收集在：管理信息库MIB中
  - 被管设备中驻留**网络管理代理agent**，与管理实体通信，在被管设备上**执行本地动作**
- 网络管理协议
  - 在管理实体和被管设备之间
  - 允许实体查询设备的信息，报告异常事件
  - 通过代理对设备间接地采取动作

网络管理体系结构



目前已有的网络管理协议

- OSI：CMISE/CMIP
- 互联网：SNMP
  - SNMP仅仅是互联网网络管理体系中的一个组成部分

3 ：网络管理

- 网络管理引论
  - 动机
  - 功能和定义
  - 主要部件
- 互联网网络管理架构
  - SMI：管理信息结构
    - 命名：OID
    - 语法：ASN.1
    - 传输编码：BER
  - SNMP：互联网网络管理协议
  - 安全性

网管需要解决的问题

- 需要监视和控制被管设备的什么信息
  - 被管设备需要管理和维护的信息：被管对象
    - 例如：到目前为止接收到的错误分组个数，系统的描述信息等
  - 相关被管对象形成：模块
  - 被管设备中的被管模块形成本地存储：MIB库
- 被控信息什么形式进行定义和传输
  - 数据定义语言：SMI
    - MIB库中的所有对象和模块采用SMI（ASN.1）定义
  - BER：定义的被管对象和模块采用BER转换成标准码流进行数据交换
- 什么格式和时机进行管理信息的交换：SNMP协议

SNMP协议和MIB、SMI相互独立
便于独立演化

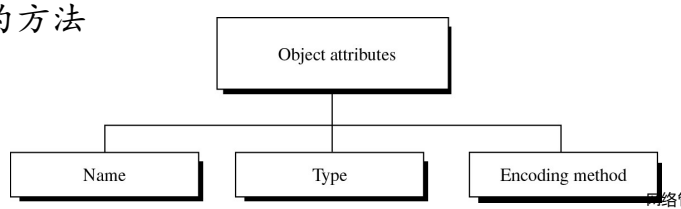
3 ：网络管理

- 网络管理引论
  - 动机
  - 功能和定义
  - 主要部件
- 互联网网络管理架构
  - SMI：管理信息结构
    - 命名：OID
    - 语法：ASN.1
    - 传输编码：BER
  - SNMP：互联网网络管理协议
  - 安全性

被管对象的属性

从最小的对象属性开始；
SMI的3个组成：
如何标示，如何定义，以及如何编码

- 名字：一个唯一的标示
  - MIB库由一堆对象构成，每个对象需要一个唯一标示
  - 需要一个标示方法，SMI的内容之一
- 语法：
  - 定义对象的数据类型（整数，字符串……），
  - ASN.1的子集和超集
- 编码方法：BER，定义编码从而在网络上进行传输的方法

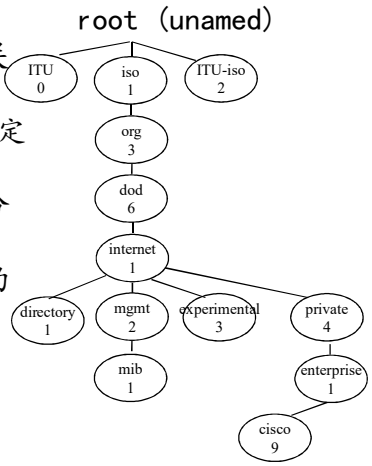


3 ：网络管理

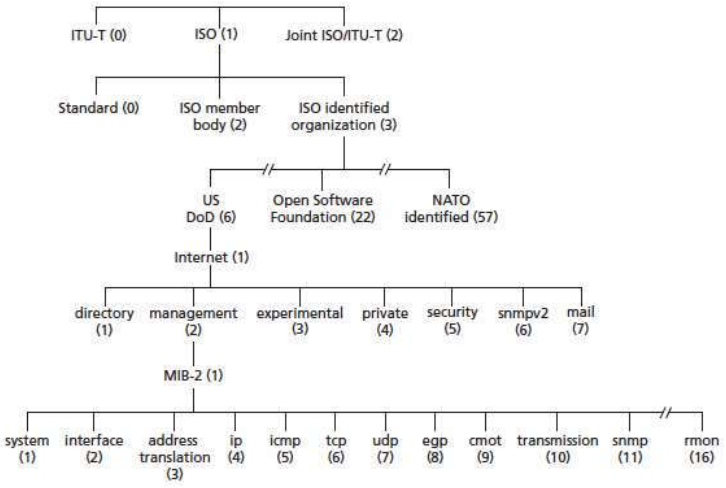
- 网络管理引论
  - 动机
  - 功能和定义
  - 主要部件
- 互联网网络管理架构
  - SMI:管理信息结构
    - 命名:OID
    - 语法：ASN.1
    - 传输编码：BER
  - SNMP:互联网网络管理协议
  - 安全性

对象的命名：OID和OID树

- 平面命名：重名（命名或者编号），不便于管理，也不携带对象之间的关系=>层次命名：像域名空间
- 一个对象的标示符（对象ID)唯一确定了在MIB层次结构中的一个被管对象
- 层次：一棵树，根不命名，一层层分配命名（有对应标号）
- OID:一个对象可以用从树根到树叶的节点名字（或者数字）来标示
  - iso.org.dod.internet.mgmt.mib <=>1.3.6.1.2.1
- MIB库就是一个按照层次组织起来的OID集合
  - 定义了被管对象的属性

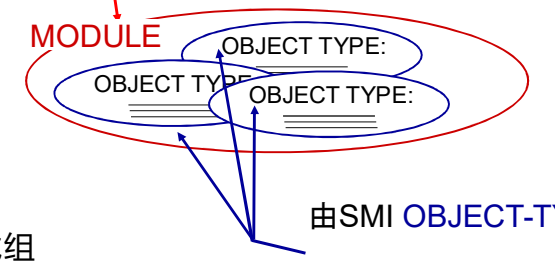


对象标识树



SNMP MIB

MIB模块被SMI规范
MODULE-IDENTITY
(100 标准MIBs, 更多生产厂商的规范)



由SMI OBJECT-TYPE 构造对象

对象 构成组
(组+对象）构成 模块
一些标准模块 形成:MIB库

MIB-I

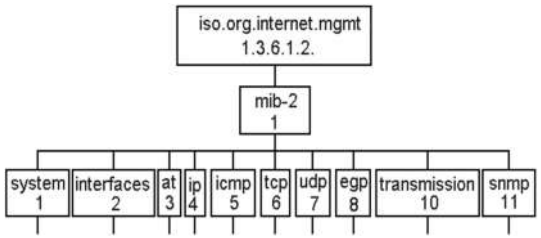
- MIB-I是一个标准模块，1988提出 (RFC1156 and RFC1212)
- 定义了100个被管对象
- 定义了8个对象组（group）
  - system object group (1.3.6.1.2.1.1)
  - Interface object group (1.3.6.1.2.1.2)
  - Address translation object group (1.3.6.1.2.1.3)
  - IP object group (1.3.6.1.2.1.4)
  - ICMP object group (1.3.6.1.2.1.5)
  - TCP object group (1.3.6.1.2.1.6)
  - UDP object group (1.3.6.1.2.1.7)
  - EGP object group (1.3.6.1.2.1.8)

MIB例子：UDP模块

Object ID	Name	Type	Comments
1.3.6.1.2.1.7.1	UDPInDatagrams	Counter32	total # datagrams delivered at this node
1.3.6.1.2.1.7.2	UDPNoPorts	Counter32	# underliverable datagrams: no application at port
1.3.6.1.2.1.7.3	UDInErrors	Counter32	# undeliverable datagrams: all other reasons
1.3.6.1.2.1.7.4	UDPOutDatagrams	Counter32	# datagrams sent
1.3.6.1.2.1.7.5	udpTable	SEQUENCE	one entry for each port in use by app, gives port # and IP address

MIB-II

- 1990定义 (RFC 1158 and RFC 1213)
- 11个对象组，包含171对象
  - MIB-1的超集
  - 定了一些SNMPv2所需要的功能性
- MIB-II中的新对象组
  - Transmission object group (1.3.6.1.2.1.10)
  - SNMP object group (1.3.6.1.2.1.11)



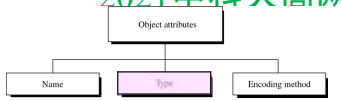
MIB对象细节

- 关键对象组（不包括其他5个对象组）
  - System Group 1.3.2.1.2.1.1：给出整个系统的信息
    - sysDesc, SysObjectID, sysUpTime, sysContact, sysName, SysLocation, sysService
  - Interface Group 1.3.2.1.2.1.2：给出接口信息
    - inNumber -> ifIndex, ifDescr … InOutLen, ifSpecific (total 22)
  - IP Group 1.3.2.1.2.1.4：定义了IP分组信息
    - ipForwarding, ipDefaultTTL, ipInReceive, ipInHdrErrors … ipFragCreates, ipRoutingDiscards (total 20) + ipAddrTable (5 sub varables)+ ipRouteTable (13 sub-variables)+ipNetMedia (3 sub variables)
  - ICMP Group 1.3.2.1.2.1.5：存储了有关ICMP包的信息
    - icmpInMsgs, icmpInErrors, … icmpOutAddrMaskReps (total 26)
  - TCP Group 1.3.2.1.2.1.6：存储了TCP段的一些信息
    - tcpRtoAlgroithm, tcpRtoMin, … tcpOutRsts (total 14)+ tcpConnState (5 sub-variables)
  - UDP Group 1.3.2.1.2.1.7：存储了UDP数据报的信息
    - udpInDatagram, UdpNoPorts, udpInErrors, udpOutDatagrams (total 4) + udpTables (2 sub variables)

3 ：网络管理

- 网络管理引论
  - 动机
  - 功能和定义
  - 主要部件
- 互联网网络管理架构
  - SMI:管理信息结构
    - 命名:OID
    - 语法：ASN.1
    - 传输编码：BER
  - SNMP:互联网网络管理协议
  - 安全性

SMI:语法



- 对象的第2个属性：数据类型
- SMI采用ASN.1的一些基本内容，另外增加了一些定义
  - Abstract Syntax Notation One (ASN.1)是一个数据定义语言，用于定义MIB中被管对象，可以使其在获得机器无关的表示一致性
  - ASN.1采用变量和声明，类似于编程语言
    - 而后面讲到的传输编码BER像机器语言
  - 提供供应商中立、跨平台、标准的语言，用于开发者来描述协议，系统和机器
  - 像ASN.1的一致性语言允许不同类型的计算机能够更有效的分享信息

ASN.1介绍

- ASN.1是SNMP用于创建实际MIB对象的数据表示格式
- ASN.1在SNMP之前很早就存在
- MIB的定义充分利用了ASN.1的优势
- ASN.1是OSI的标准： ISO 8824
- SNMP采用了ASN.1定义了交换报文的格式以及管理的对象

注：SNMP报文和被管对象（模块）都采用ASN.1定义；
BER进行编码

SMI中的基本数据类型

- 3种在ASN.1中定义的简单数据类型+4种SMI中定义的数据类型
  - Integers - 有符号整数，范围： -2,147,483,648 to 2,147,483,647.
  - Octet strings - 字符串（每位字符编码在0到65535）
  - Object IDs - These values are from the set of all object identifiers allocated according to the rules specified in ASN.1.
  - Network addresses - 网络地址代表一个特性协议族的地址.SNMPv1支持32为IP地址
  - Counters - 计数器值非负，可以增加一直到一个最大值，再增加到0. SNMPv1中,指定为32位计数器
  - Gauges - Gauges非负，可以增加或者减少，但是保持一个它曾经到达过的最大值
  - Time ticks - time tick代表从某个时间开始多少时间，以10ms为单位.

被管理对象的类型

- 简单类型：标量对象
  - 定义一个单个对象实例（类似于：C中的**变量**）
  - SMI的基本数据类型
    - Integer (4 bytes)，来自ANS.1
    - String (variable)，来自ANS.1
    - ObjectIdentifier (variable)，来自ANS.1
    - IPAddress (4 bytes)，SMI增加
    - Counter (4 bytes)，SMI增加
    - Gauge (4 bytes)，SMI增加
    - TimeTicks (4 bytes)，SMI增加

OBJECT-TYPE: ipInDelivers

```
ipInDelivers OBJECT TYPE
  SYNTAX      Counter32
  MAX-ACCESS  read-only
  STATUS      current
  DESCRIPTION
    "The total number of input
     datagrams successfully
     delivered to IP user-
     protocols (including ICMP)"
::= { ip  9}
```


被管理对象的类型

- 结构类型：
  - 简单类型和某些结构类型的组合
  - SMI定义了2中类型：sequence 和 sequence of
  - Sequence：1个*sequence数据类型是一些简单数据类型的组合*（c.f. C中的结构体）
  - Sequence of：1个*sequence of数据类型是简单类型的序列*（c.f. C中的数组）

模块

MODULE-IDENTITY: ipMIB

```
ipMIB MODULE-IDENTITY
  LAST-UPDATED "941101000Z"
  ORGANZATION "IETF SNPv2
          Working Group"
  CONTACT-INFO
    " Keith McCloghrie
    ....."
  DESCRIPTION
    "The MIB module for managing IP
    and ICMP implementations, but
    excluding their management of
    IP routes."
  REVISION "019331000Z"
  .....
::= {mib-2 48}
```


3 ：网络管理

- 网络管理引论
  - 动机
  - 功能和定义
  - 主要部件
- 互联网网络管理架构
  - SMI：管理信息结构
    - 命名：OID
    - 语法：ASN.1
    - 传输编码：BER
  - SNMP：互联网网络管理协议
  - 安全性

编码方法：BER

- SMI采用BER(Basic Encoding Rules)将SMI定义的被管对象值编码成传输的位串
- 使得不同机器获得语义上的一致性
  - 仅仅内存拷贝解决不了通信问题
  - 大端小端问题
- 每个被传输的数据(对象值和SNMP字段)都有：TLV
  - Type (1 byte) - 3子字段
    - class (2 bit), format (1 bit), and number (5 bit)
  - Length：1个或多个字节
  - Value：根据BER定义的规则编码数据的值

TLV 编码

思路： 被传输数据自说明

- T：数据类型，某个ASN.1定义的类型
- L：数据的字节长度
- V：数据的值，采用ASN.1编码标准编码

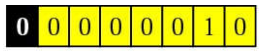
编码类型：T

- Type: 1 byte
  - Class (2bit) + format (1bit) + Number (5 bit)

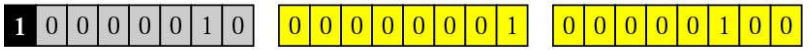
Data type	class	format	Number	Tag (bin)	Tag(Hex)
Integer	00	0	00010	00000010	02
String	00	0	00100	00000100	04
OID	00	0	00110	00000110	06
Sequence, sequence of	00	1	10000	00110000	30
IPAddress	01	0	00000	01000000	40
Counter	01	0	00001	01000001	41
Gauge	01	0	00010	01000010	42
TimeTics	01	0	00011	01000011	43

编码长度：L

- 长度字段1个或多个字节
  - 如果1字节，最高位为0，其他7个bits定义了数据的长度
  - 如果>1字节，最高位为1，其他7个bits定义了后面有几个字节用于表示长度L



a. The colored part defines the length (2)



b. The shaded part defines the length of the length (2 bytes); the colored bytes define the length (260 bytes)

编码值：V

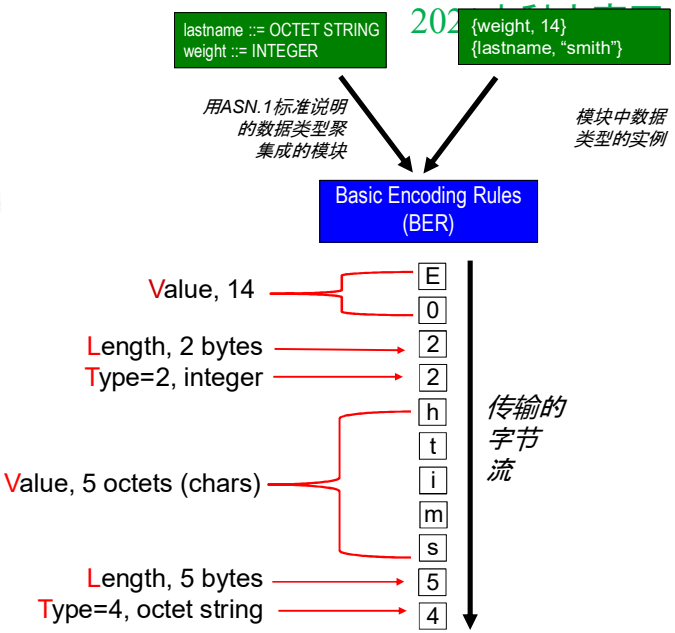
- 采用BER规则对传输的值（对象的值，字段的值）进行编码

BER编码的例子

- 例子：整数14
  - 02 | 02 | 0 | E　Integer + 2 byte value + 0 0 0 E
- 例子: 字符串 “smitch”
  - 04 | 05 | 48 | 49 | ‘l’ | ‘t’ | ‘h’ | | | |
- 格式：OID 1.3.6.1　String + 5 byte value + “s” + “m” + “i” + “t” + “h”
  - 06 | 04 | 01 | 03 | 06 | 01
- 格式: IPAddress 131.21.14.8
  - 40 | 04 | 83 | 15 | 0E | 08

tag　length　value

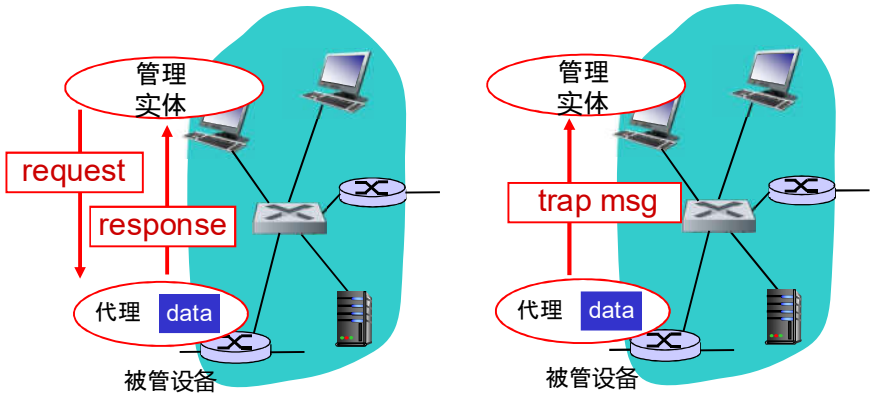
TLV编码:例子



3 ：网络管理

- 网络管理引论
  - 动机
  - 功能和定义
  - 主要部件
- 互联网网络管理架构
  - SMI：管理信息结构
    - 命名:OID
    - 语法：ASN.1
    - 传输编码：BER
  - SNMP:互联网网络管理协议
  - 安全性

SNMP协议

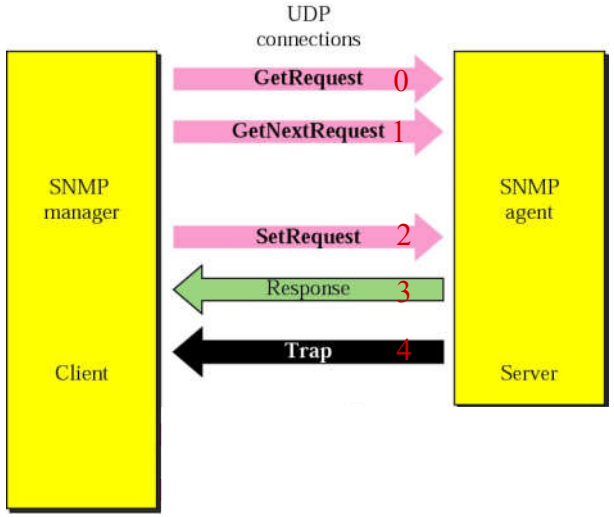


请求/响应模式　　陷阱模式

SNMP 协议：报文类型

报文类型	功能
GetRequest GetNextRequest GetBulkRequest	管理实体-代理：“给我数据” (instance, next in list, block)
InformRequest	实体-实体：给你MIB值
SetRequest	实体-代理：set MIB value
Response	代理-实体：值，对请求的响应
Trap	代理-实体：异常事件的报告

SNMP报文类型

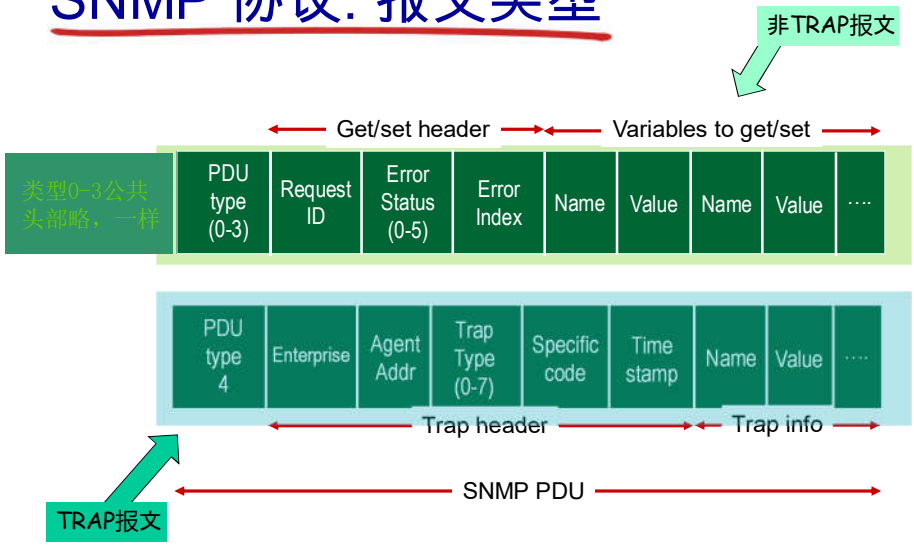


SNMP报文格式

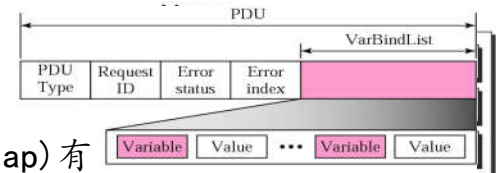
非trap报文的类型，0,1,2,3
TYPE见52页：A0-A3

代表trap报文
TYPE类型：A7

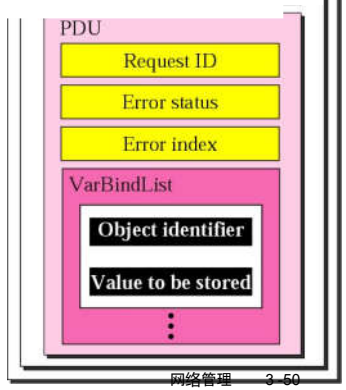
SNMP 协议: 报文类型



SNMP PDU



- 每个SNMP PDU（除了trap）有以下格式：
  - PDU type: SNMP 非TRAP报文类型
  - request id - 请求序号
  - error status - 如无错0；否则不为0
  - error index - 如果不为0则指示哪一个PDU中的OID导致错误
  - variable bind-列表
    - variable name - OIDs
    - values - get报文和get next报文，该字段为null



SNMP PDU格式(trap)

- enterprise - 导致陷阱报文的对象类型标示
- agent address - 发送此trap报文的agent IP地址
- generic trap id - 标准traps标识
- specific trap id - 私有或者企业定义的trap
- time stamp - trap发生的时间ticks
- variable bind-list
  - variable name - OIDs
  - values - get或者get next报文时，值为空

编码SNMP报文

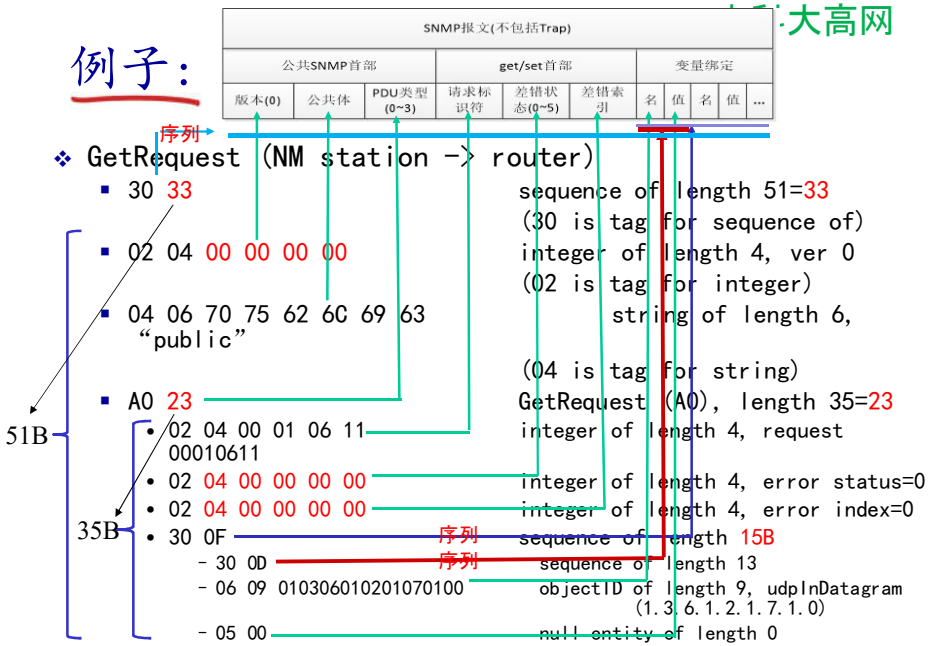
- 也采用BER编码SNMP报文
- 用tags(PDU Type)定义报文,Type字段包括3个子字段
  - class
  - format
  - number => for different type of message

Data	class	format	Number	Tag (bin)	Tag(Hex)	类型
GetRequest	10	1	00000	10100000	A0	0
GetNextRequest	10	1	00001	10100001	A1	1
GetResponse	10	1	00010	10100010	A2	2
SetRequest	10	1	00011	10100011	A3	3
Trap	10	1	00111	10100111	A7	4

GetRequest 报文例子

- 一个管理工作站(snmp client，管理实体)采用GetRequest 报文读取一个路由器接收到了UDP数据报的数量
- 路由器中的agent(SNMP server)用GetResponse报文来应答

例子：



例子：编码GetResponse

- GetResponse (router->NM Station)
  - 30 37 — sequence of length 37(hex), 55(dec)
  - 02 04 00 00 00 00 — integer of length 4, ver 0
  - 04 06 70 75 62 6C 69 63 — string of length 6, "public"
  - A2 27 — GetResponse (A2), length 39=27h
    - 02 04 00 01 06 11 — integer of length 4, request 00010611
    - 02 04 00 00 00 00 — integer of length 4, error status=0
    - 02 04 00 00 00 00 — integer of length 4, error index=0
    - 30 13 — sequence of length 19=13(hex)
      - 30 11 — sequence of length 17=11(hex)
      - 06 09 010306010201070100 — objectID of length 9, udpInDatagram (1.3.6.1.2.1.7.1.0)
      - 41 04 00 00 12 11 — counter of length 04 with value 12 11

3 ：网络管理

- 网络管理引论
  - 动机
  - 功能和定义
  - 主要部件
- 互联网网络管理架构
  - SMI：管理信息结构
    - 命名:OID
    - 语法：ASN.1
    - 传输编码：BER
  - SNMP:互联网网络管理协议
  - 安全性

SNMPv3中增加的安全性

- 在SNMPv3中增加了以下安全特性：
  - ✓ • 报文完整性
    - 保证报文在传输中不被修改
  - ✓ • 可认证性
    - 能够判断报文是不是一个有效的源发送的
  - ✓ • 加密
    - 保证私密性，即使被截获无法得知发送的到底是什么
  - ✓基于视图的访问控制：
    - SNMP实体维护着不同用户的访问权限，策略的数据库
    - 是否可访问的LCD数据库可以作为被管对象**访问**

2021中科大高网

总结

- 网络管理主要功能是方便网络管理员监控网络运行状态
  - 获取被管设备的状态，报告故障等信息，控制被管设备的运行
  - 分布、自动
- 网络管理的体系结构：管理实体、agent、MIB、SNMP
- SMI:管理信息结构
  - 对象、组、模块（MIB库）命名：树形层次型对象（及模块）OID
  - ASN.1数据语言定义（跨平台）定义对象、模块
  - BER编码规则定义将SMI定义的对象编码成传输码流（机器无关，保持语义上的一致性），也可用于编码SNMP PDU
- SNMP：管理实体和agent间传输网管报文的协议
- 安全性