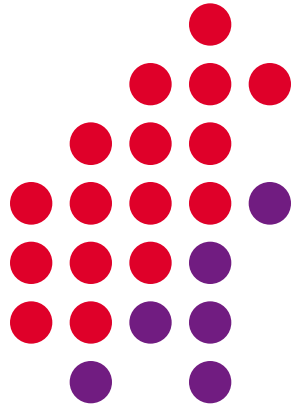


实验4
网络管理实验

主要内容

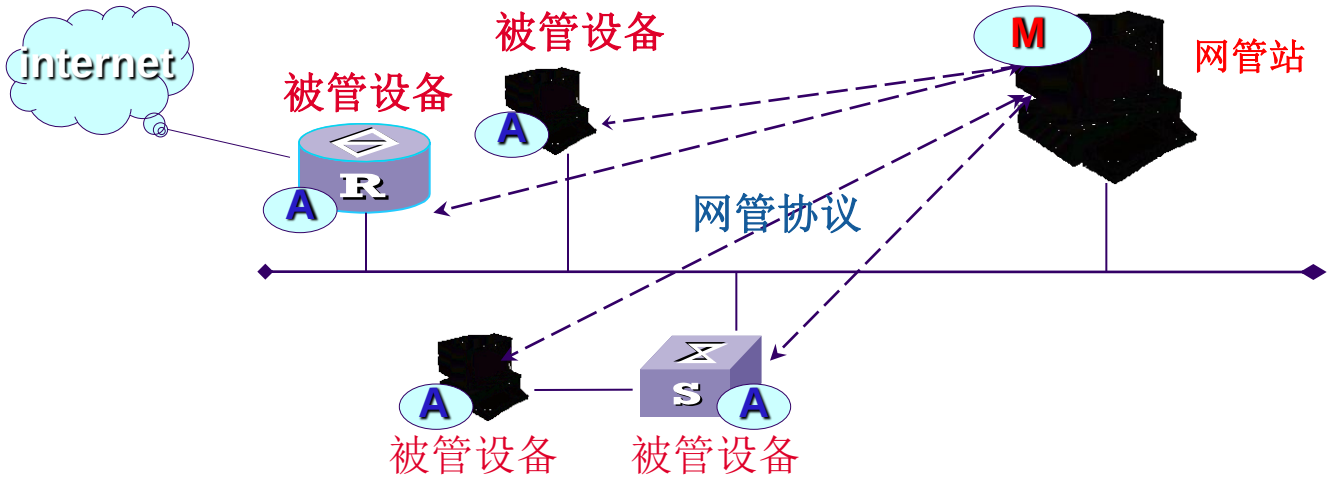
- 网管基本概念
- SNMP协议简介
- Quidview网管软件功能介绍
- 网络管理实验
  - 网管软件功能演示
  - SNMP协议分析
  - 网络拓扑发现

网络管理的基本概念

- 网络管理标准框架
  - OSI在其标准（ISO 7498-4）中提出了网络管理标准的框架，将网络管理分为：系统管理（管理整个OSI系统）、层管理（管理某一层次）、层操作（对一个层次中管理通信的一个实例进行管理）。
  - 系统管理中提出了五个功能域：故障管理、配置管理、计费管理、性能管理、安全管理。

网络管理的基本概念

◆网络管理的一般模型



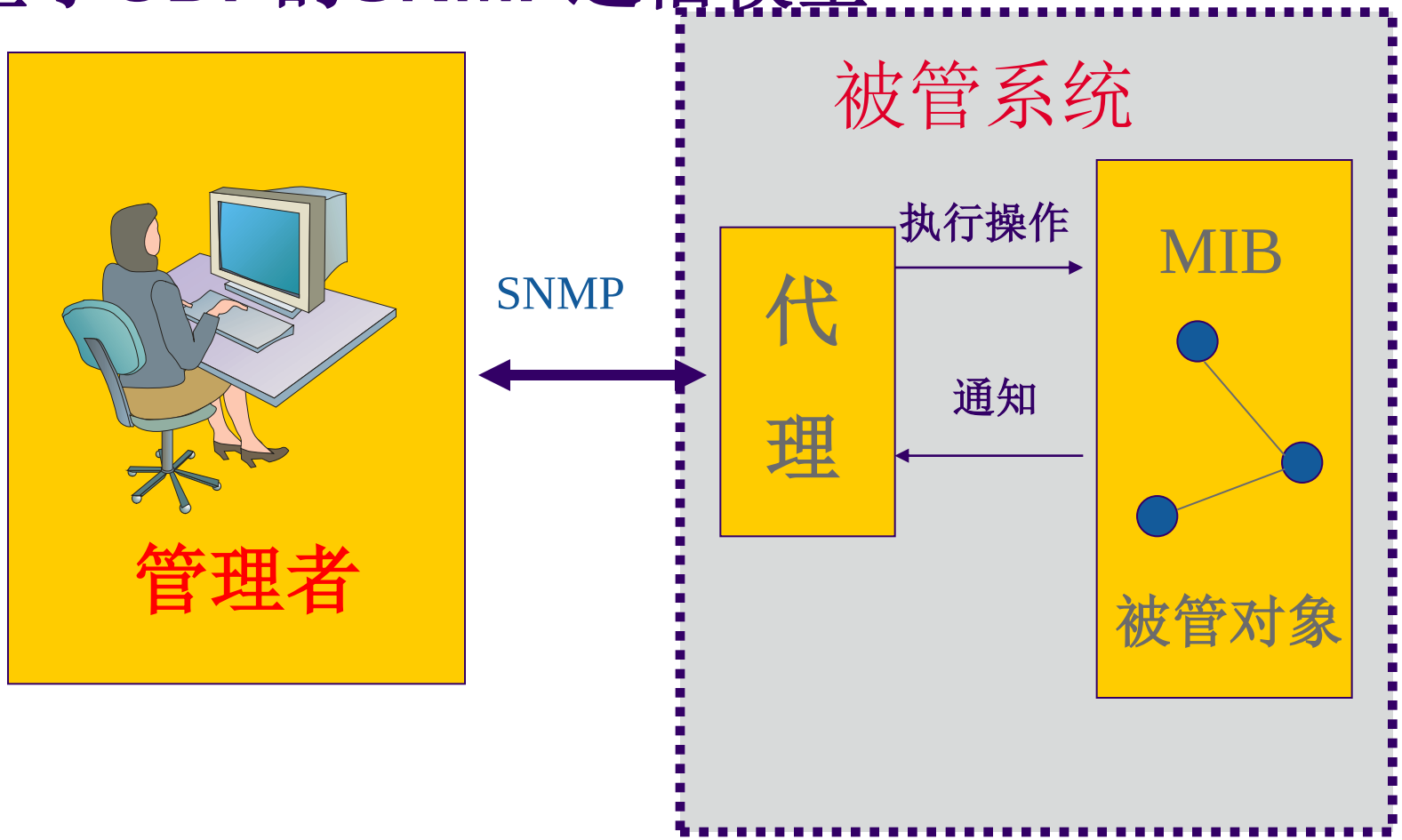
M——管理程序（运行SNMP客户程序）

A——代理程序（运行SNMP服务器程序）

- 网管站是整个网络管理系统的核心，所有向被管设备发送的命令都是从管理站发出的。
- 每一个被管设备中都要运行一个程序以便和管理站的管理程序进行通信。这些运行着的程序叫做网络管理代理程序，简称代理(agent)。

网络管理的基本概念

- 基于UDP的SNMP通信模型



RMON管理

- **RMON（Remote Monitoring，远程网络监视） 的基本思想：**
  - 把一部分原来在网管侧实现的功能放到设备上去进行，例如由网管侧配置设备Agent统计和计算某一个或几个监视对象的值，然后将这些值与设定的门限进行比较。只有当统计值超过门限时，设备侧才会向网管侧发出告警。
- **RMON的优点：**
  - 避免了网络上许多不必要的流量，在减轻网络负担的同时也有限降低了对网络带宽的要求。

主要内容

- 网管基本概念
- SNMP协议简介
- Quidview网管软件功能介绍
- 网络管理实验
  - 网管软件功能演示
  - SNMP协议分析
  - 网络拓扑发现

SNMP协议简介

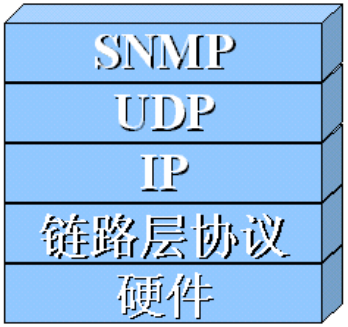
◆SNMP协议的设计依据:

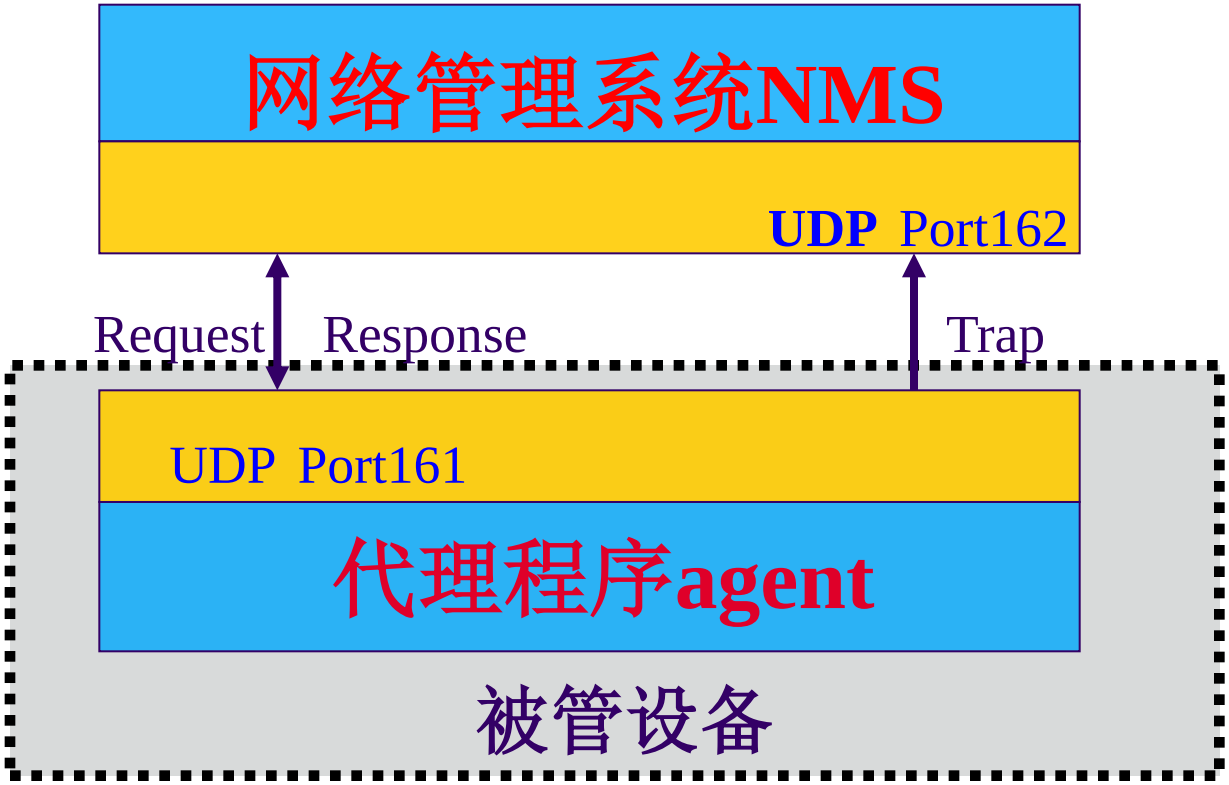
- 若要管理某个对象，就必然会给对象添加一些软件或硬件，但这种“添加”必须对原有对象的影响尽量小些。因此SNMP最重要的指导思想就是要尽可能简单。

◆SNMP协议的组成:

- 管理信息库MIB（网络中所有的对象都存放在一个叫管理信息库的数据结构中）
- 管理信息结构SMI（定义了SNMP的数据结构）
- SNMP协议本身

SNMP协议栈及操作模型





SNMP操作模型

- 网管系统
  - 网管程序所要做的就是定期请求被管设备的信息，这个功能通过探询操作来实现，它通过周期性的用一个UDP数据报给被管设备的IP地址发送一个SNMP请求报文（Request）来完成，同时接收被管设备的响应和Trap报文。
- 网管代理程序（agent）
  - 处理来自网管工作站的请求报文，然后从设备上的相关模块取出管理变量（OID）的数值，形成响应报文，回送网管站。紧急情况下，主动发出trap报文

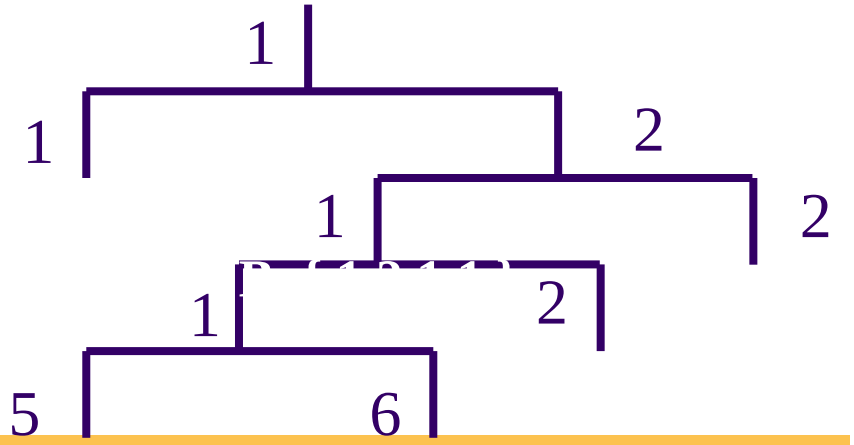
SNMPv1定义的PDU

- SNMPv1定义的协议数据单元PDU有五种类型

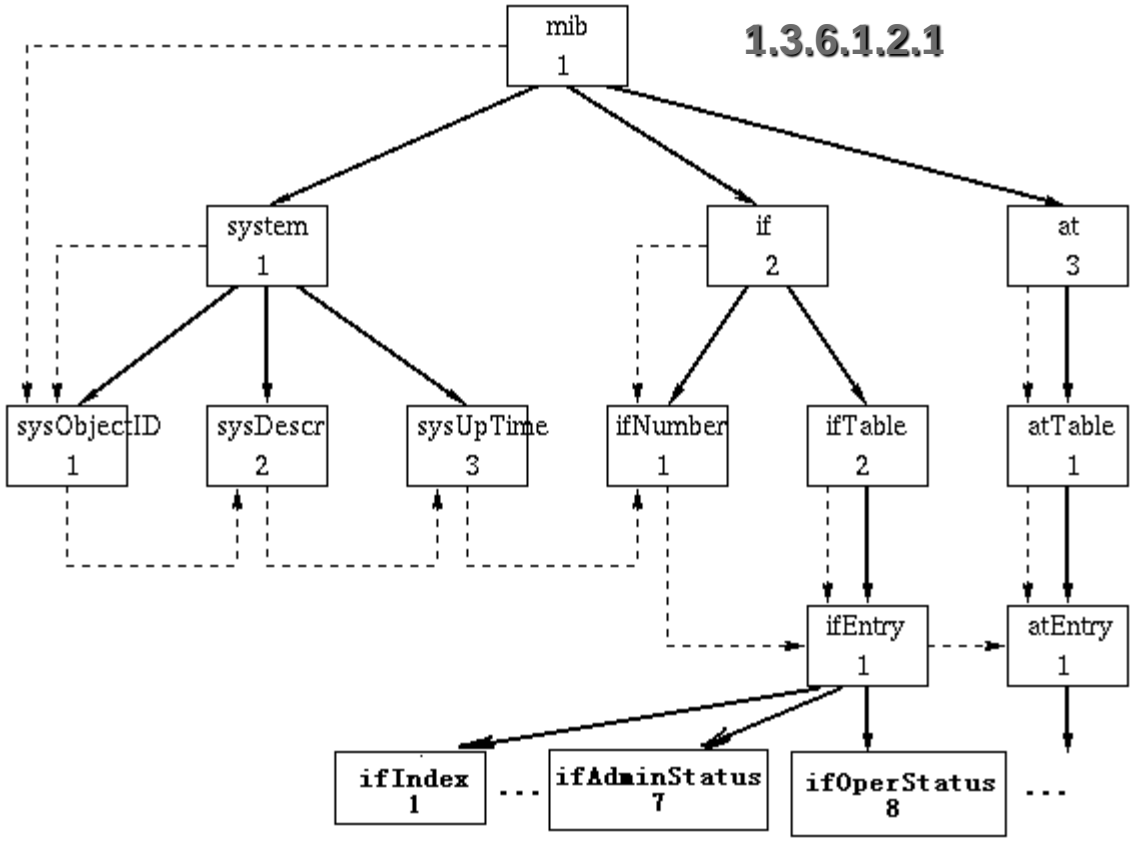
PDU编号	PDU名称	用途
0	get-request	用来查询一个或多个变量的值
1	get-next-request	允许在一个MIB树上检索下一个变量，此操作可反复进行
2	get-response	对get/set报文作出响应，并提供差错码、差错状态等信息
3	set-request	对一个或多个变量的值进行设置
4	Trap	向管理进程报告代理中发生的事件

管理信息库 MIB

- **MIB（Management Information Base）是所监控的网络设备的标准变量定义的集合。**
- **每个被管对象对应树型结构的一个叶子节点，称为一个object或一个MIB**
  - **SNMP的管理信息库采用和域名系统DNS相似的树形结构**



MIB树结构



MIB树结构

管理信息结构SMI

- SMI（structure of management information）用来定义SNMP数据结构。
- 是SNMP的一个重要组成部分（RFC1155）
- SMI标准规定了所有的MIB变量必须使用抽象语法记法1（ASN.1）来定义。

ASN. 1——抽象语法记法1

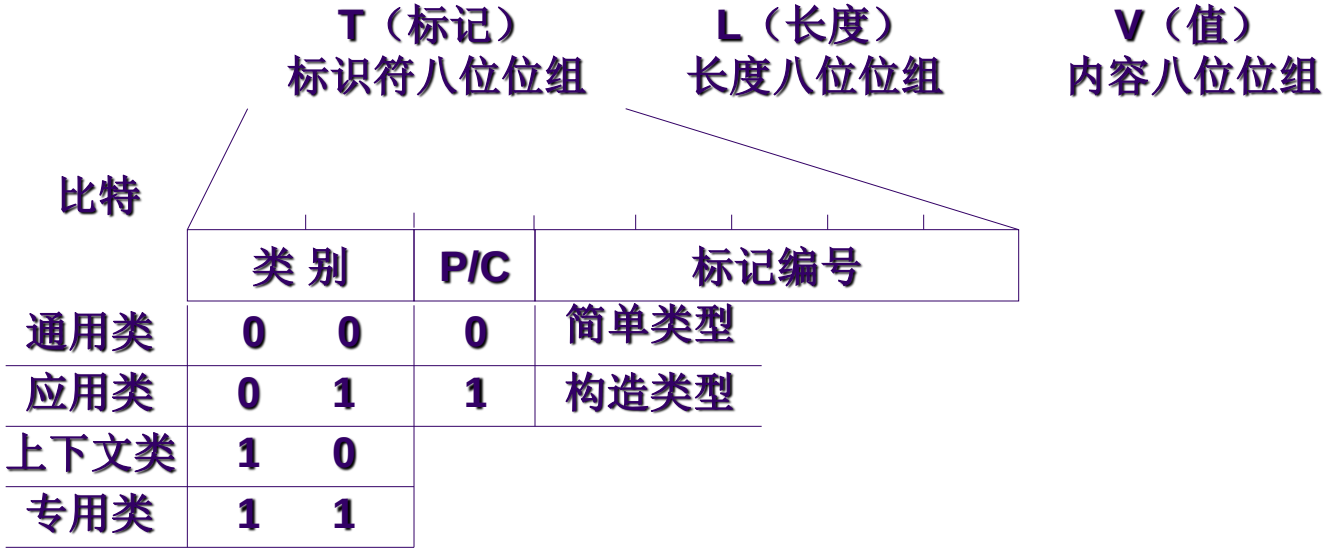
- ASN.1的产生
  - 为了使多个制造商设备之间的通信成为可能，用一种标准而与制造商无关的方式来定义这些对象是十分必要的。
  - 另外还需要用标准方式来编码以用于网络传输。
- ASN.1是SNMP所使用的标准对象定义语言和编码规则。

ASN. 1——抽象语法记法1

- ASN.1转换语法
  - 定义了ASN.1类型的值如何明确地转换为适合于传输的字节序列（在另一端也能被明确地解码）
- 基本编码规则BER（basic encoding rules）
  - 定义了ASN.1类型的值如何明确地转换为适合于传输的字节序列（在另一端也能被明确地解码）。

ASN. 1基本编码规则

- ASN.1规定了各种数据值都采用TLV法进行编码。
  - 这种方法把一个数据元素表示为由下面三个字段组成的八位位组序列：



ASN. 1数据类型

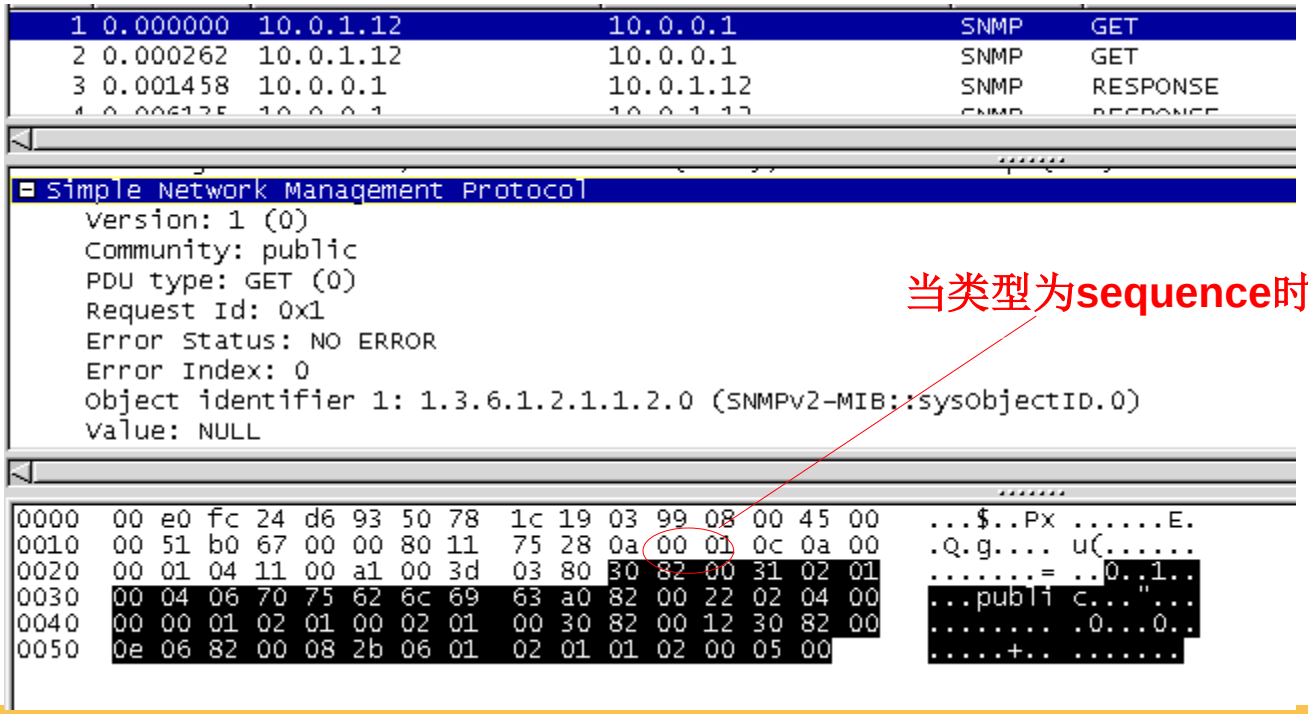
◆SNMP中允许使用的ASN.1的一些原始数据类型

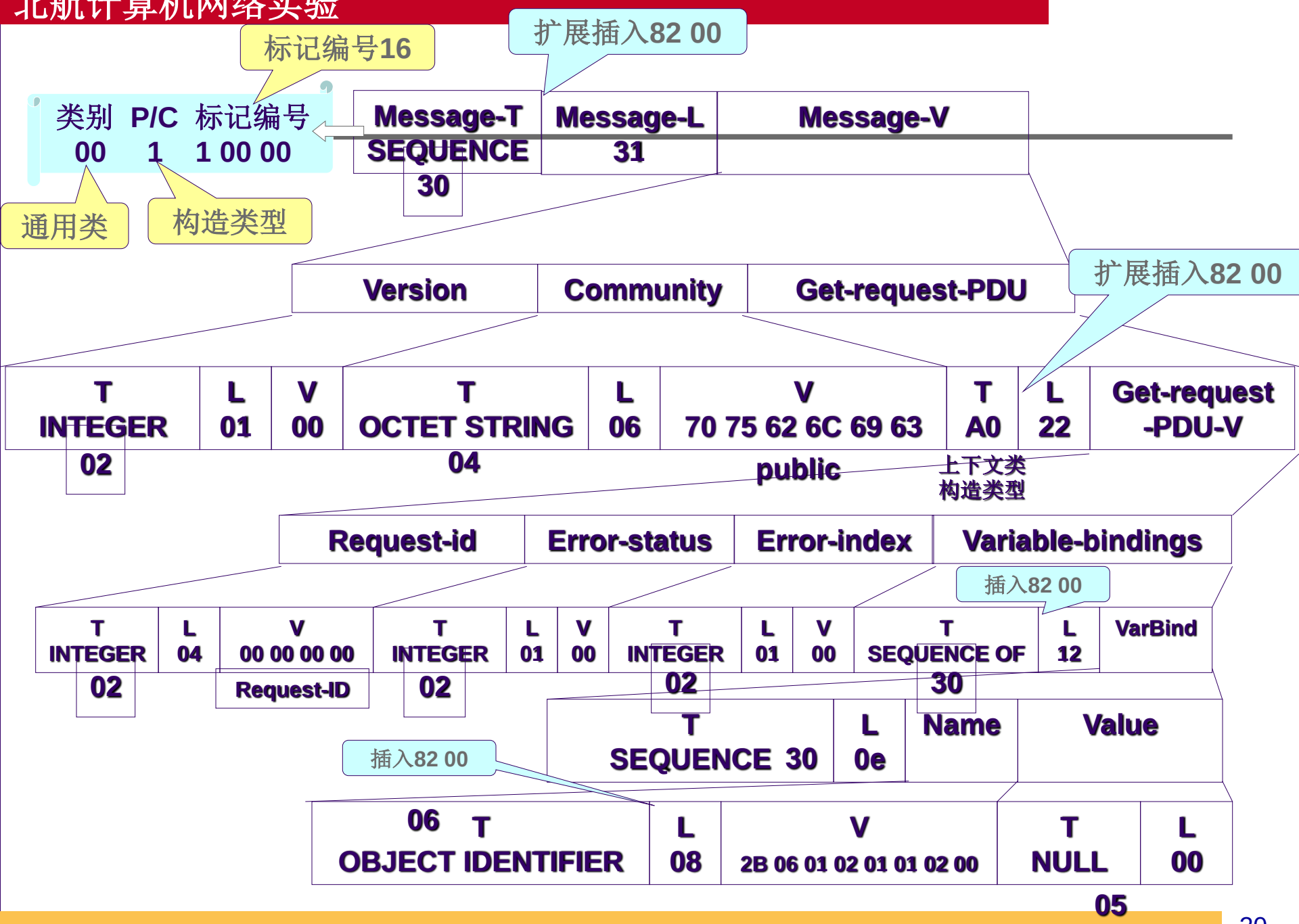
分类	标记	类型名称	主要特点
简单类型	UNIVERSAL 2	INTEGER	取整数值数据类型
	UNIVERSAL 4	OCTET STRING	取八位位组序列值的数据类型
	UNIVERSAL 5	NULL	只取空值的数据类型（用于尚未获得数据的情况下）
	UNIVERSAL 6	OBJECT IDENTIFIER	与信息对象相关联的值的集合
构造类型	UNIVERSAL 16	SEQUENCE	取值为多个数据类型的按序组成的值
	UNIVERSAL 16	SEQUENCE -OF	取值为同一数据类型的按序组成的值
	无标记	CHOICE	可选择多个数据类型中的某一个数据类型
	无标记	ANY	可描述事先还不知道的任何类型的任何值

使用ASN.1编码过程简介

- 实际截获的报文在编码过程中，与教材中有些不同，在T字段类型为Object Identifier、Sequence、sequence of、上下文类型时，在T与L字段中插入了82 00两个字节。
- 可以理解为L字段扩展了82 00两个字节。
  - 82 00 31为L字段。 82（1000 0010）最高的1bit代表扩展，0000010=2代表后面的两个字节表示长度，即00 31为0x31字节

实际截获的报文可能如图所示




标记编号16
扩展插入82 00
类别 P/C 标记编号
00 1 1 00 00
通用类
构造类型
Message-T
SEQUENCE
30
Message-L
31
Message-V
Version
Community
Get-request-PDU
扩展插入82 00
T
INTEGER
02
L
01
V
00
T
OCTET STRING
04
L
06
V
70 75 62 6C 69 63
public
T
A0
上下文类
构造类型
L
22
Get-request
-PDU-V
Request-id
Error-status
Error-index
Variable-bindings
插入82 00
T
INTEGER
02
L
04
V
00 00 00 00
Request-ID
T
INTEGER
02
L
01
V
00
T
INTEGER
02
L
01
V
00
T
SEQUENCE OF
30
L
12
VarBind
T
SEQUENCE 30
L
0e
Name
Value
插入82 00
06 T
OBJECT IDENTIFIER
L
08
V
2B 06 01 02 01 01 02 00
T
NULL
05
L
00

使用ASN.1编码过程简介

- 最后得到用十六进制表示的编码
  - 这些编码和实际截获的报文相吻合，并作为UDP用户数据报的数据部分的一个完整的SNMP报文发送。

主要内容

- 网管基本概念
- SNMP协议简介
- Quidview网管软件功能介绍
- 网络管理实验
  - 网管软件功能演示
  - SNMP协议分析
  - 网络拓扑发现

网管软件Quidview概述

- HUAWEI Quidview网络管理软件
  - HUAWEI Quidview网络管理软件是华为公司针对数据通信设备如路由器、交换机、接入服务器、视频设备等进行统一管理和维护的网管产品，位于网络解决方案的管理层次，能够实现网元管理和网络管理的功能。
- 实验中主要使用的网管软件
  - Quidview 面向华为3Com IP设备
  - 简单网络管理协议（SNMP）

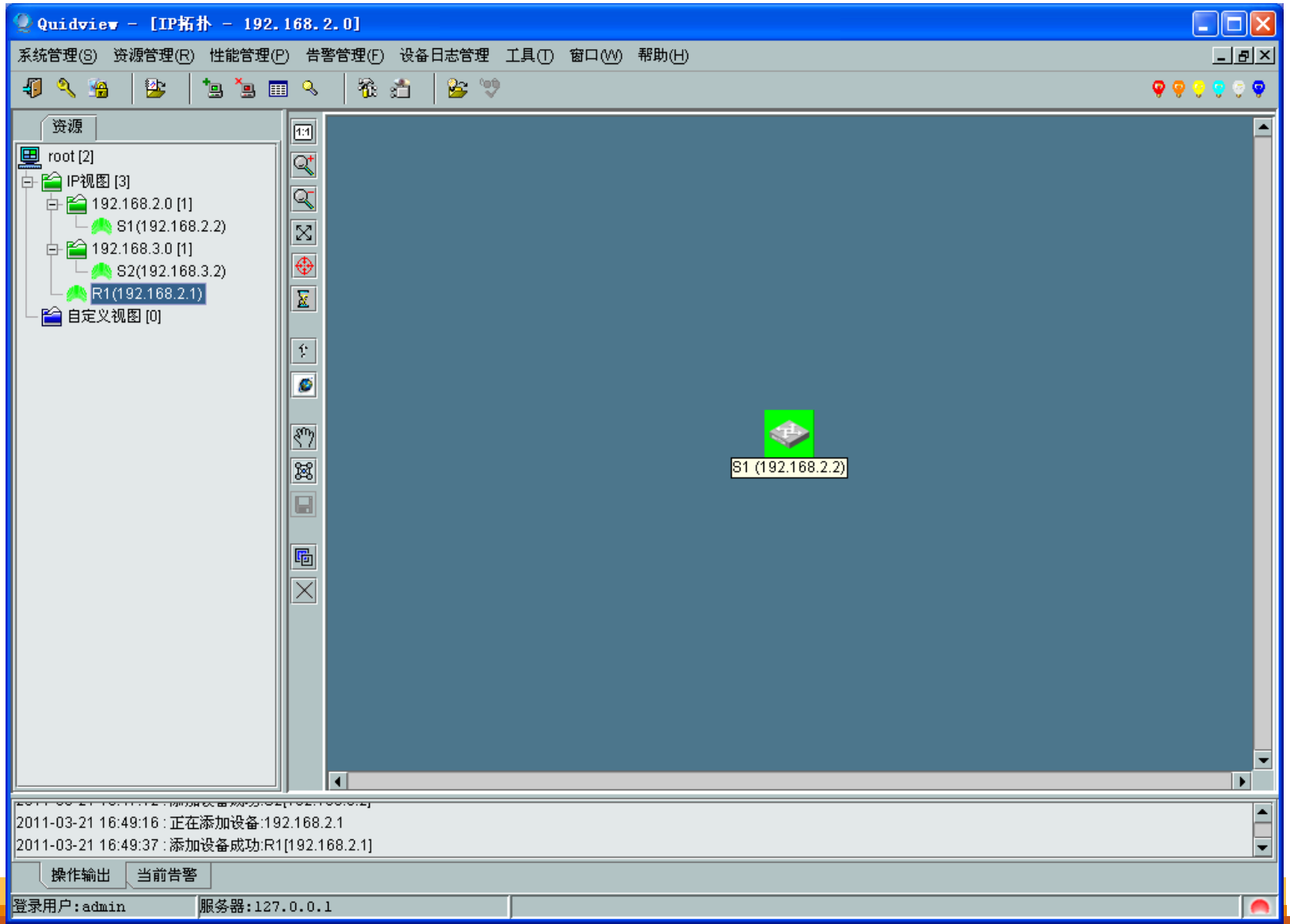
Quidview3.10功能

- 采用灵活的组件化结构，实现以下功能：
  - 网络拓扑管理
  - 设备管理
  - **Traffic View**
  - 资源管理系统
  - **Easy Config**

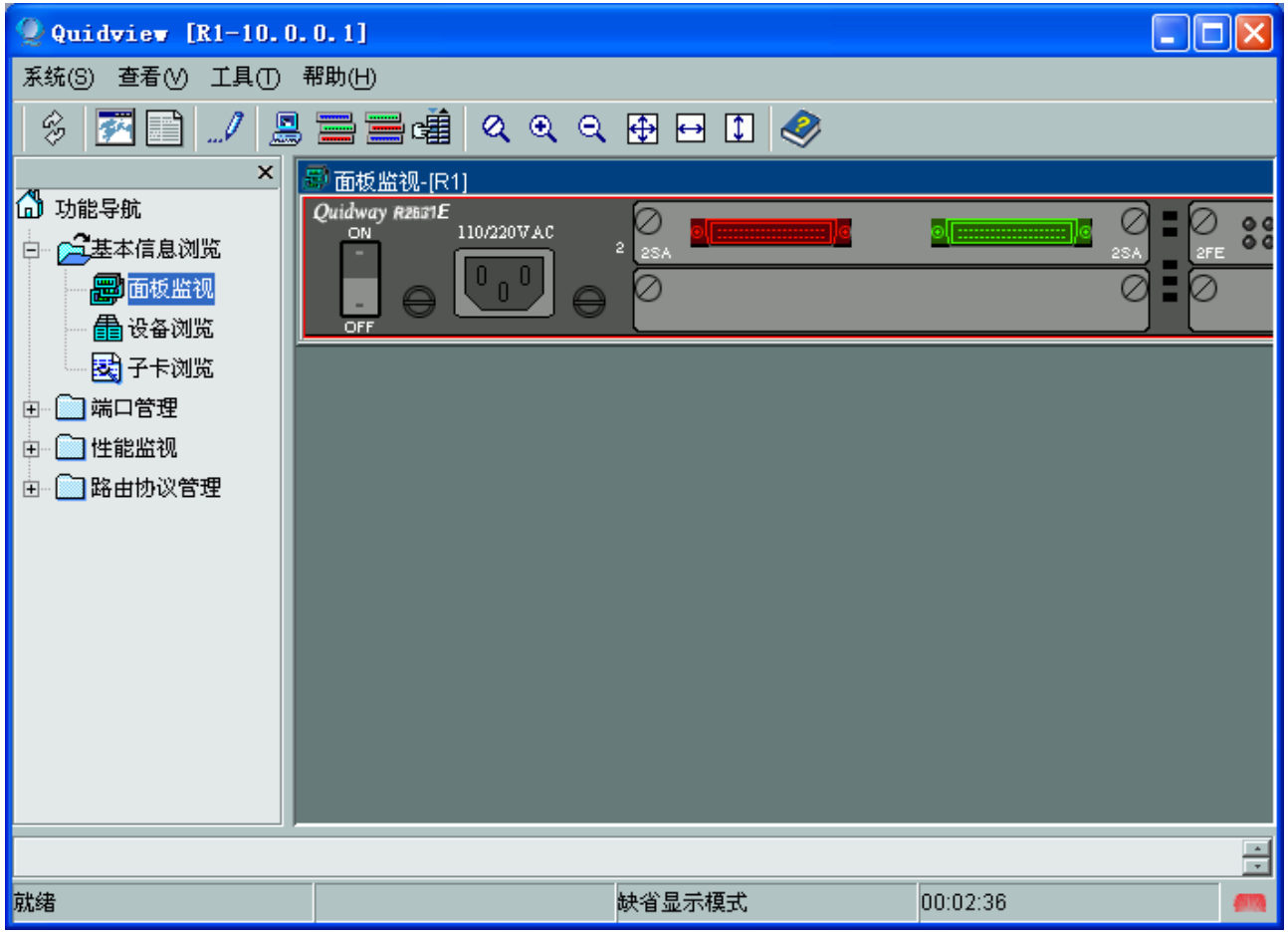
网络拓扑管理

- 主要体现在以下方面：
  - 网络拓扑的自动发现
  - IP网络的网络层拓扑显示，同时提供子图的浏览树
  - 拓扑图的自动排列和按比例缩放
  - 使用不同的位图标识不同设备，不同颜色标识不同状态
  - 支持手工增加/删除子网、设备节点和链路
  - 定期轮询、更新子网、设备节点和链路状态
  - 网络对象的属性浏览
  - Ping、Telnet设备、浏览设备的MIB信息的快捷方式

Quidview软件主界面

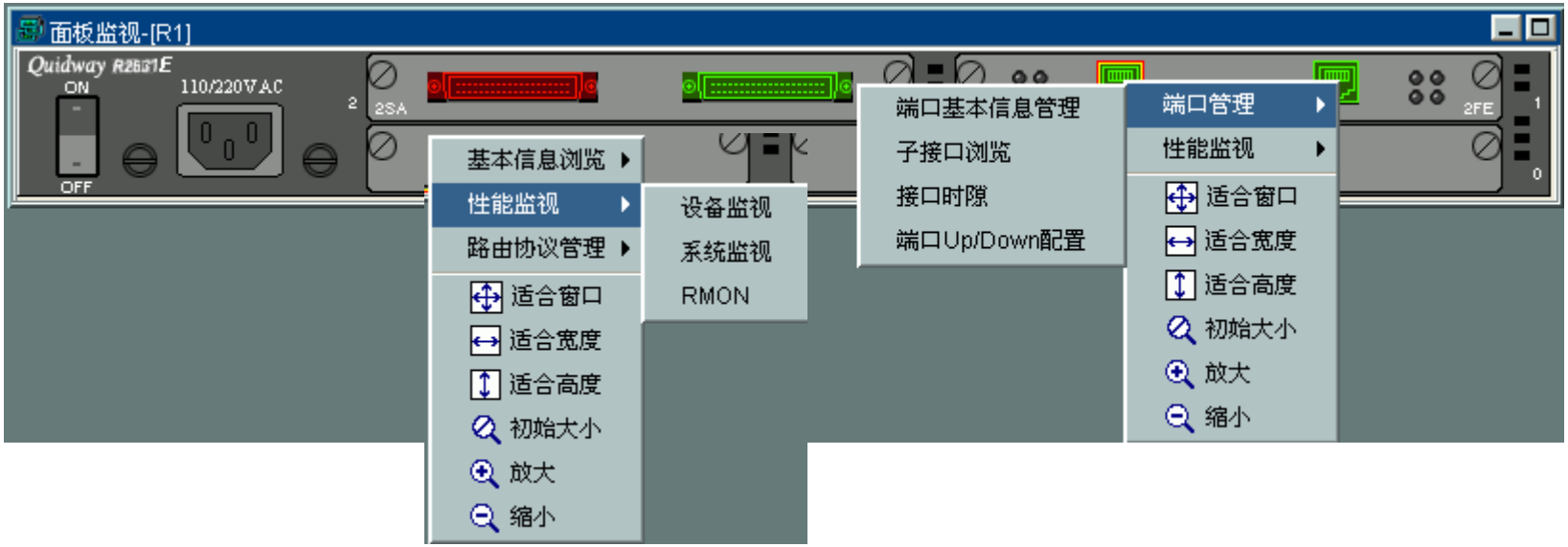


路由器设备管理功能



◆主要有：基本信息浏览、端口管理、性能监视和路由协议管理四个功能部件。

基本信息浏览——面板监视

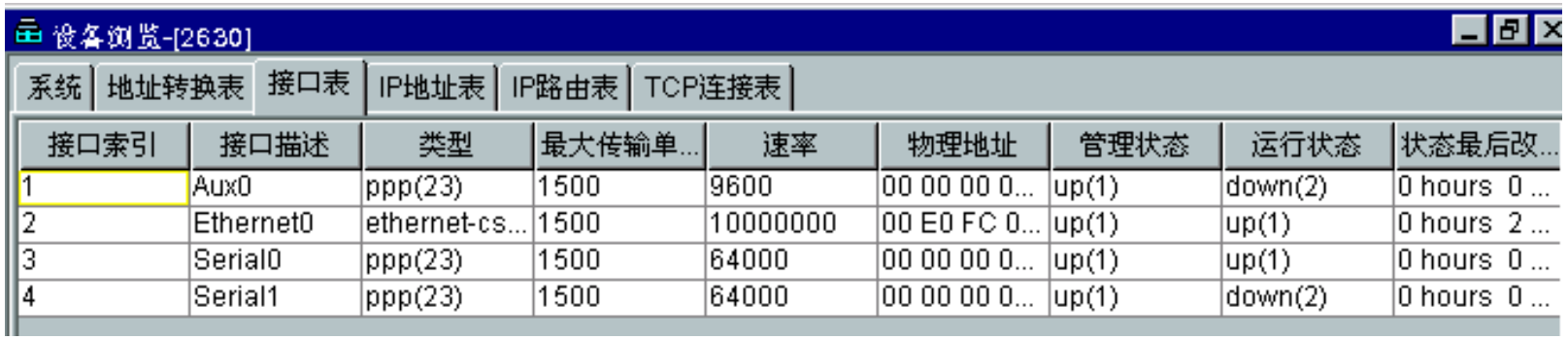


- 在设备面板上提供右击设备接口或设备接口之外部分可以观察有关设备和接口的一些信息和对它们进行管理。
- 这些功能也可以在功能导航菜单中找到。我们将以功能导航菜单为例介绍Quidview功能。

基本信息浏览——设备浏览

◆系统信息：是所有设备都具备的，它描述了设备端最基本、最重要的信息。

基本信息浏览——设备浏览



接口索引	接口描述	类型	最大传输单...	速率	物理地址	管理状态	运行状态	状态最后改...
1	Aux0	ppp(23)	1500	9600	00 00 00 0...	up(1)	down(2)	0 hours 0 ...
2	Ethernet0	ethernet-cs...	1500	10000000	00 E0 FC 0...	up(1)	up(1)	0 hours 2 ...
3	Serial0	ppp(23)	1500	64000	00 00 00 0...	up(1)	up(1)	0 hours 0 ...
4	Serial1	ppp(23)	1500	64000	00 00 00 0...	up(1)	down(2)	0 hours 0 ...

- 接口表记录了接口当前运行状况一些重要的数据，它能帮助管理员在接口出现异常时快速定位故障、分析查找原因。

基本信息浏览——设备浏览

接口索引	接口描述	接口IP地址	接口IP掩码	接口IP广播地址
2	Ethernet0	10.0.0.1	255.255.255.0	1
3	Serial0	10.0.1.1	255.255.255.0	0
5	NULL	127.0.0.1	255.0.0.0	0

- IP地址表描述了与设备接口相关的IP地址等信息，它可帮助管理员了解设备接口地址的情况。

基本信息浏览——设备浏览

目的地址	端口	掩码	跳数	下一跳地址	路由协议	路由类型	路由建立时...
10.0.0.0	2	255.255.25...	-1	0.0.0.0	other(1)	direct(3)	0
10.0.0.1	5	255.255.25...	-1	127.0.0.1	other(1)	indirect(4)	0
10.0.1.0	3	255.255.25...	-1	0.0.0.0	other(1)	direct(3)	0
10.0.1.1	5	255.255.25...	-1	127.0.0.1	other(1)	indirect(4)	0
10.0.1.2	3	255.255.25...	-1	0.0.0.0	other(1)	direct(3)	0
10.0.2.0	3	255.255.25...	-1	10.0.1.2	other(1)	indirect(4)	0
127.0.0.0	5	255.0.0.0	-1	0.0.0.0	other(1)	direct(3)	0
224.0.0.5	5	255.255.25...	-1	0.0.0.0	other(1)	direct(3)	0
224.0.0.6	5	255.255.25...	-1	0.0.0.0	other(1)	direct(3)	0

- **IP路由表描述了设备所有接口当前的路由信息，它是设备在转发包时的主要依据。**

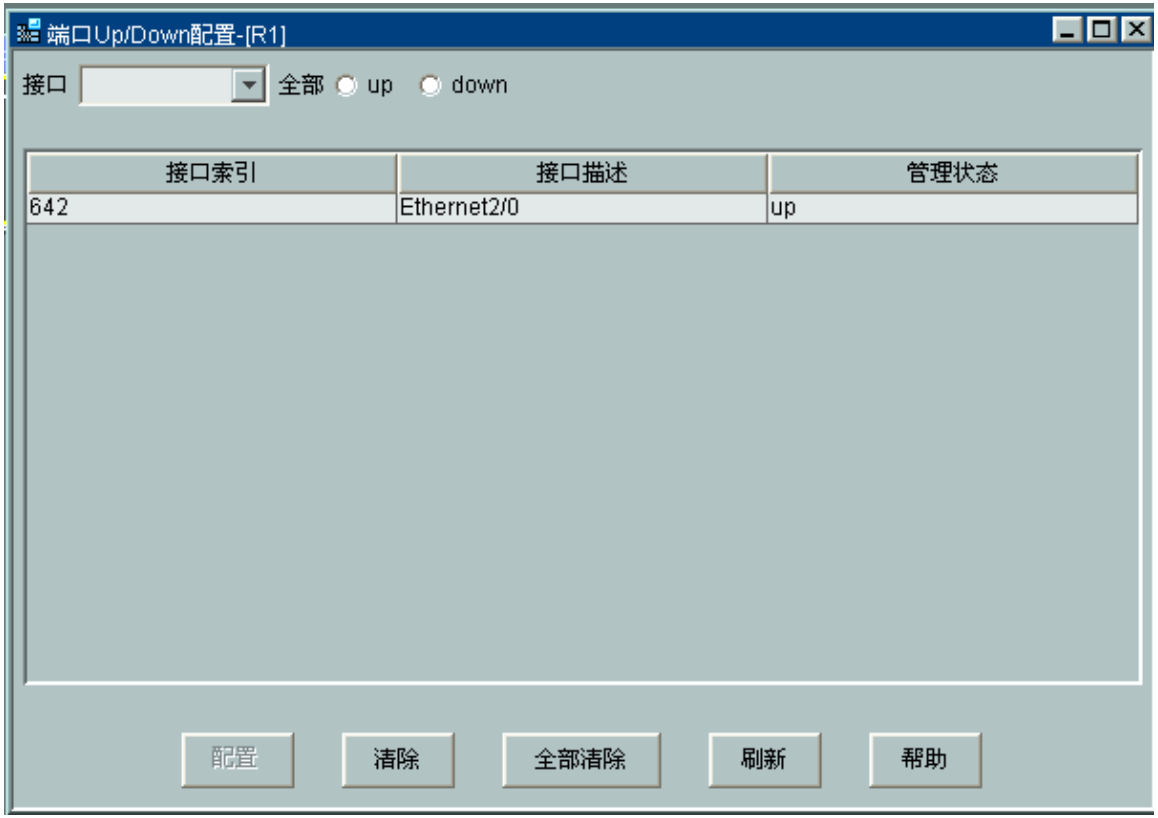
基本信息浏览——设备浏览

◆TCP连接表显示设备当前有哪些TCP连接，显示了这些连接发起者的IP地址、端口号及连接状态。

端口管理——端口基本信息管理

◆端口基本信息显示与接口有关的配置信息，隔一定的时间自动刷新。通过改变接口索引的值，用户可浏览到各个接口的配置信息。

端口管理——端口UP/DOWN配置

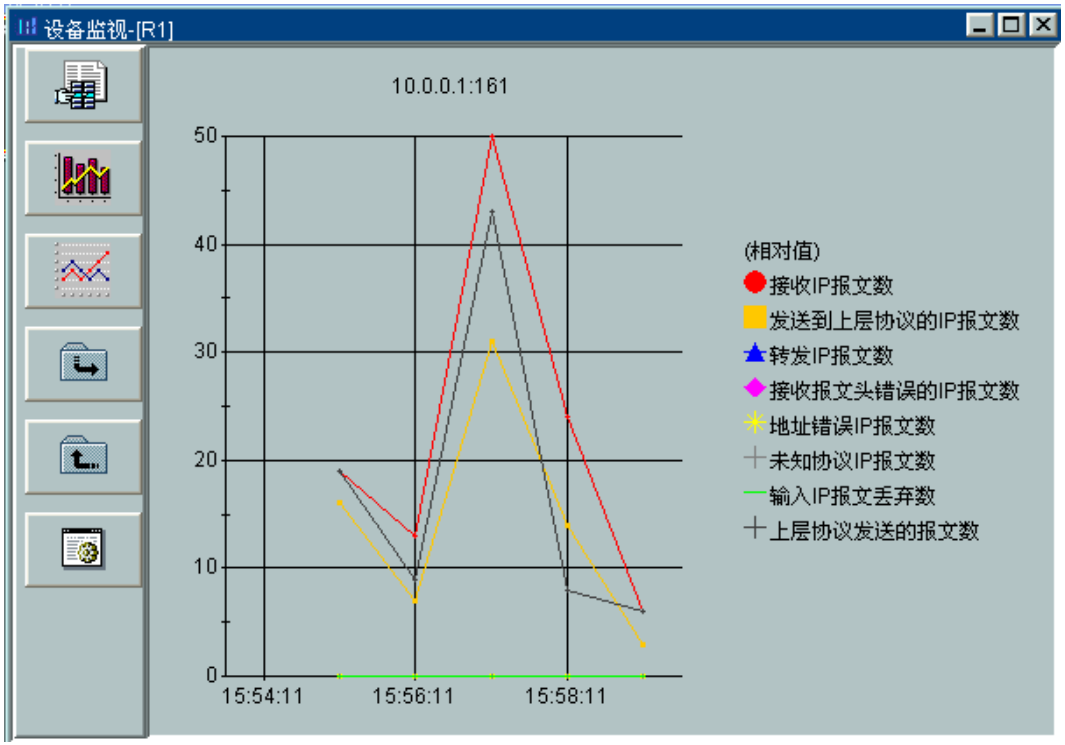


◆端口UP/DOWN配置：通过选择单选框框将端口状态配置为UP或者DOWN状态

性能监视功能

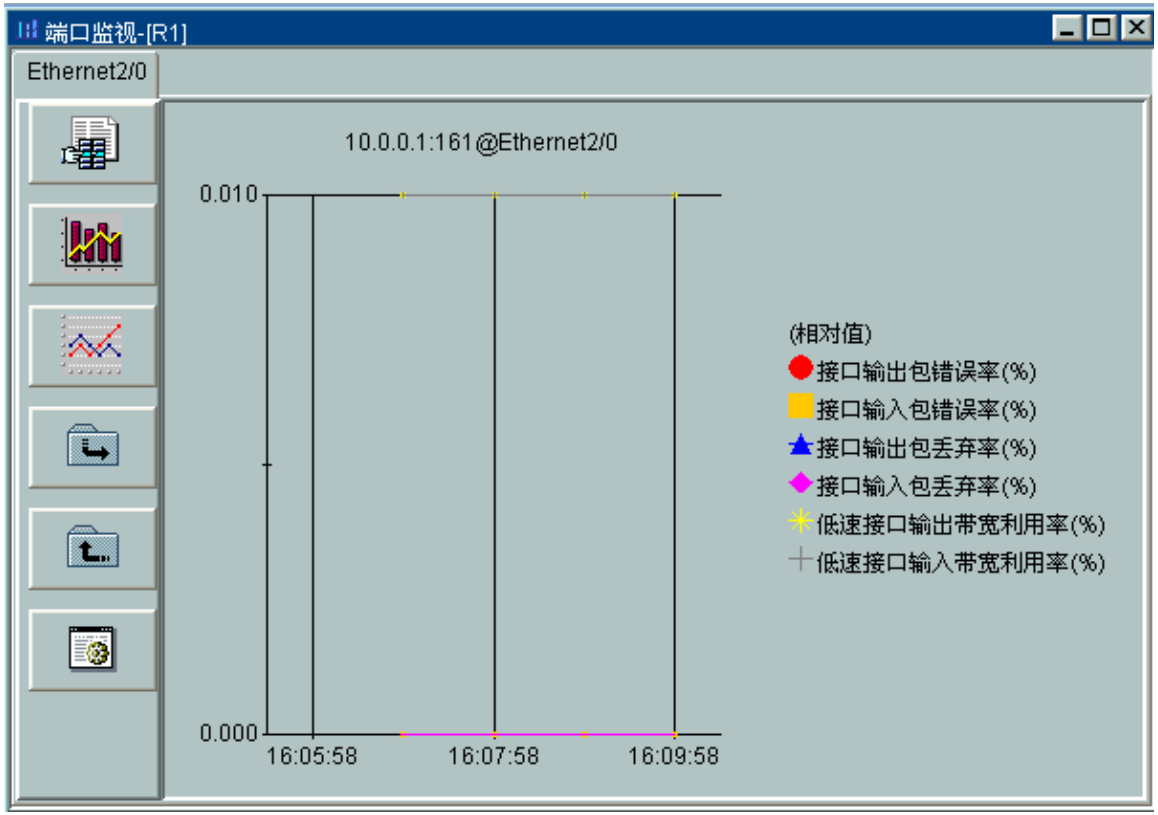
- 性能监视主要是通过图表形式将设备或设备的某个接口的性能显示出来，帮助网络管理员了解设备或接口的运行状况，以便网络管理员在紧急情况下采取必要措施。
- 性能监视主要有如下几个功能：
  - 设备监视
  - 端口监视
  - 系统监视
  - **RMON**

性能监视——设备监视



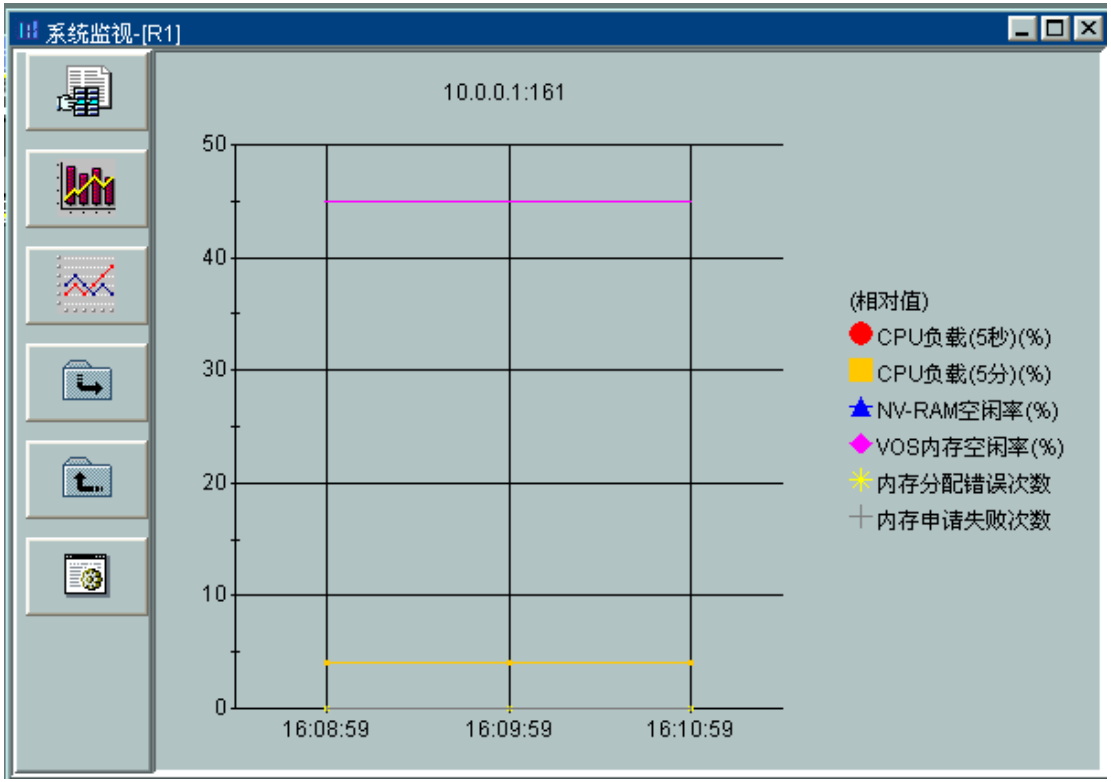
- “设备监视”窗口中以直方图、折线图的形式显示所选择监视项的性能。
- 通过属性按钮设置轮询间隔和最大显示条数

性能监视——端口监视



◆该功能主要是将接口的某些重要参数定期采样后，将统计数据绘制成折线图，以此来观察接口在一定时间间隔内的变化趋势，它可为网络管理员发现、定位和解决网络问题提供参考。

性能监视——系统监视

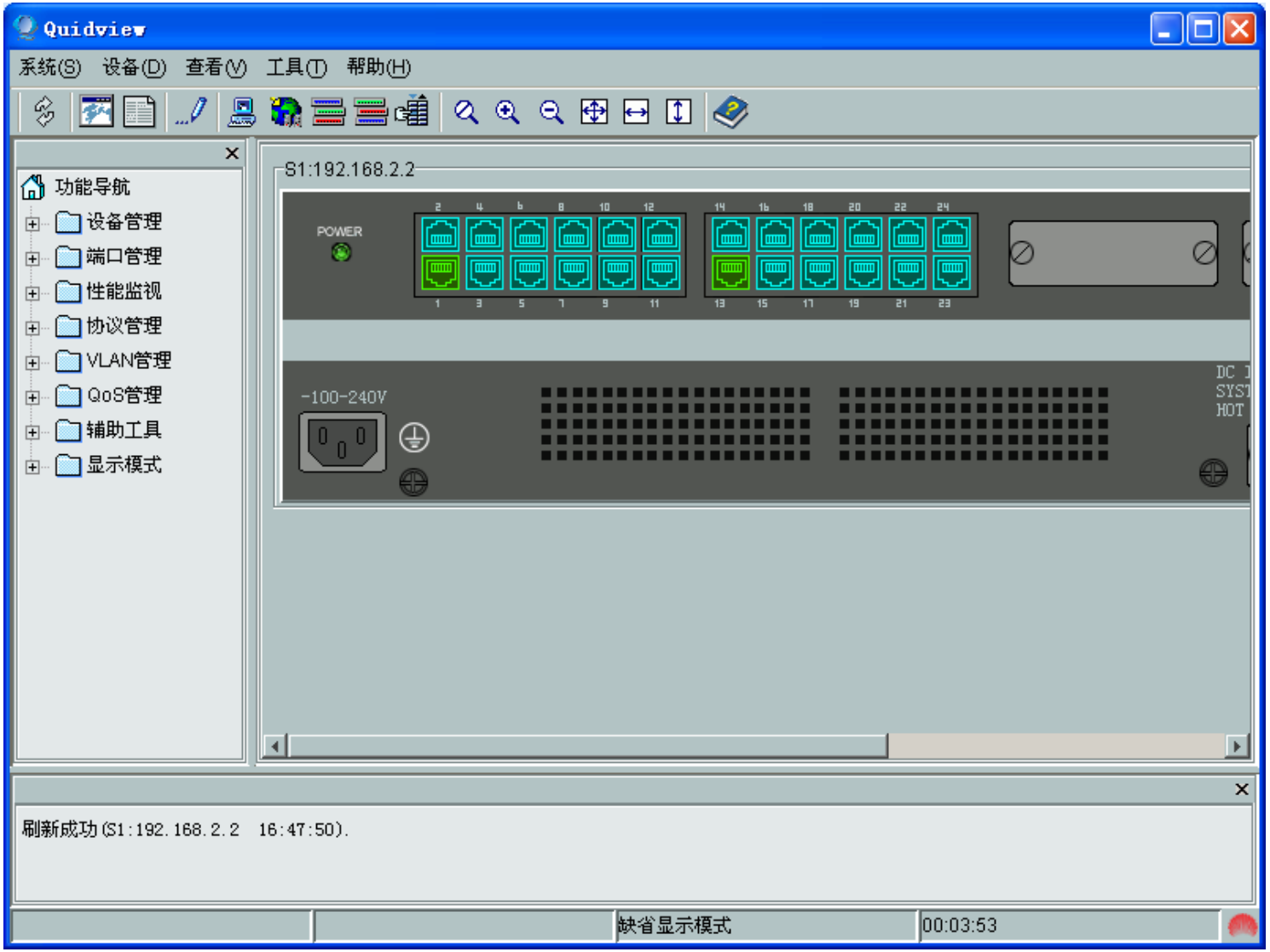


◆该功能主要针对NE系列路由器，并以折线图方式显示NE系列路由器板卡的已用内存数、剩余内存数、内存最大空闲、缓存失败、缓存无内存等信息。

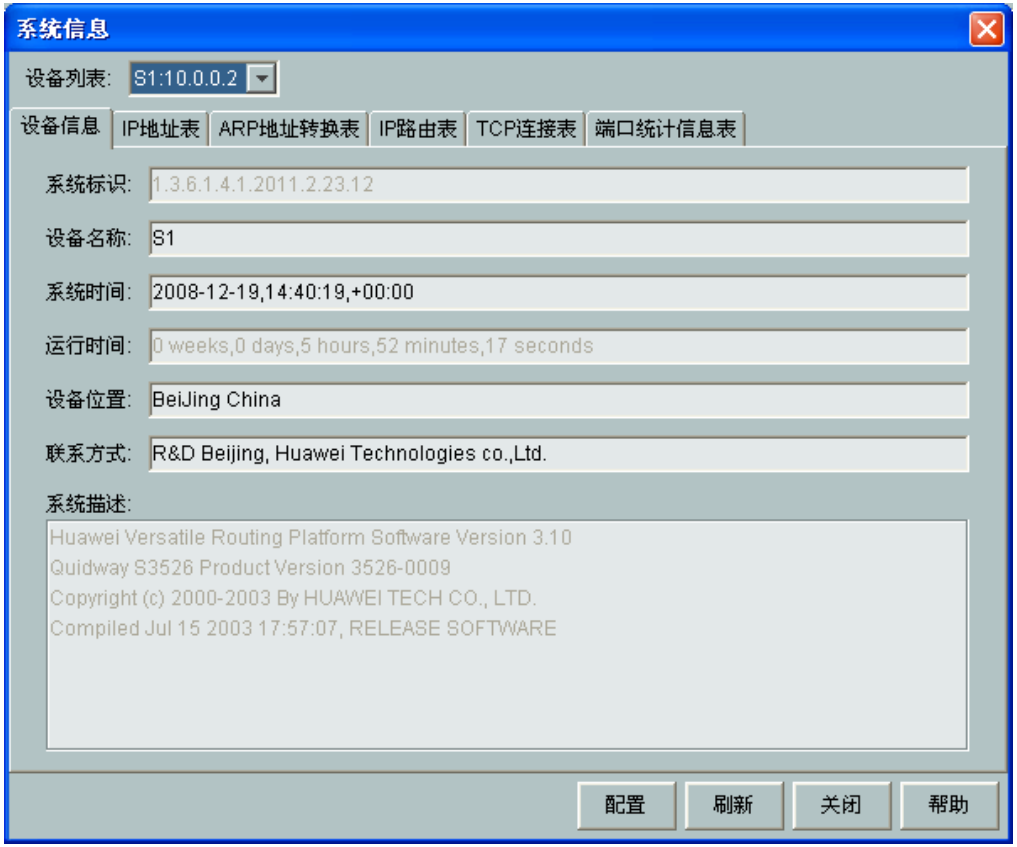
交换机设备管理

- 交换机的设备管理功能主要包括：
  - 设备管理
  - 端口管理
  - 性能监视
  - 协议管理
  - **VLAN管理**

Quidview网管软件的交换机设备主界面



设备管理-系统信息

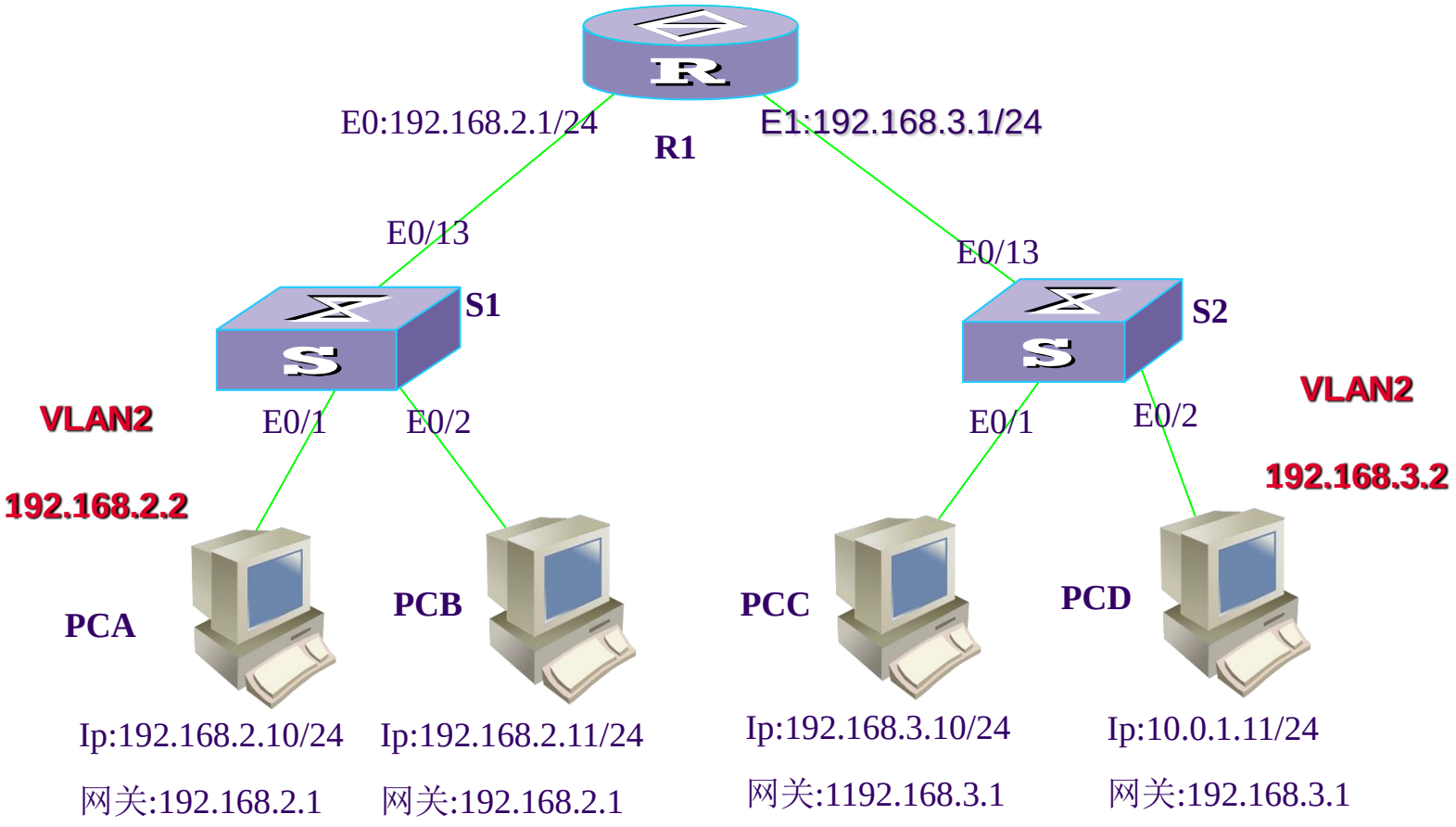


- 系统信息浏览功能给出了关于该设备的最基本的管理信息

主要内容

- 网管基本概念
- SNMP协议简介
- Quidview网管软件功能介绍
- 网络管理实验
  - 网管软件功能演示
  - SNMP协议分析
  - 网络拓扑发现

网管软件功能演示



注：交换机S1和S2的E0/1到E0/20都划分到VLAN2

网络管理软件安装

- 执行 **D:\常用工具\网管软件\install\installw.exe**
- 按照默认选项进行，除了
  - 路径 定位**E:\quidview**
  - 最后，不要选择重新启动
- **步骤1：给交换机S1和S2配置静态路由，使全网互通；**
- 注：交换机S1和S2的E0/1到E0/20都划分到VLAN2

网络管理软件的使用

- “资源管理”—〉“添加设备”—〉输入要添加的网络设备IP地址和子网掩码—〉查看资源面板的IP视图
- “资源管理”—〉“设置SNMP参数”，可对SNMP参数进行设置
- 双击添加的设备，即可打开该设备
- 在设备管理界面，选择“系统”—〉“系统参数…”，可对系统参数进行设置
  - 面板刷新间隔：5秒（默认为5分）
  - 实时监视刷新间隔：60秒（默认）

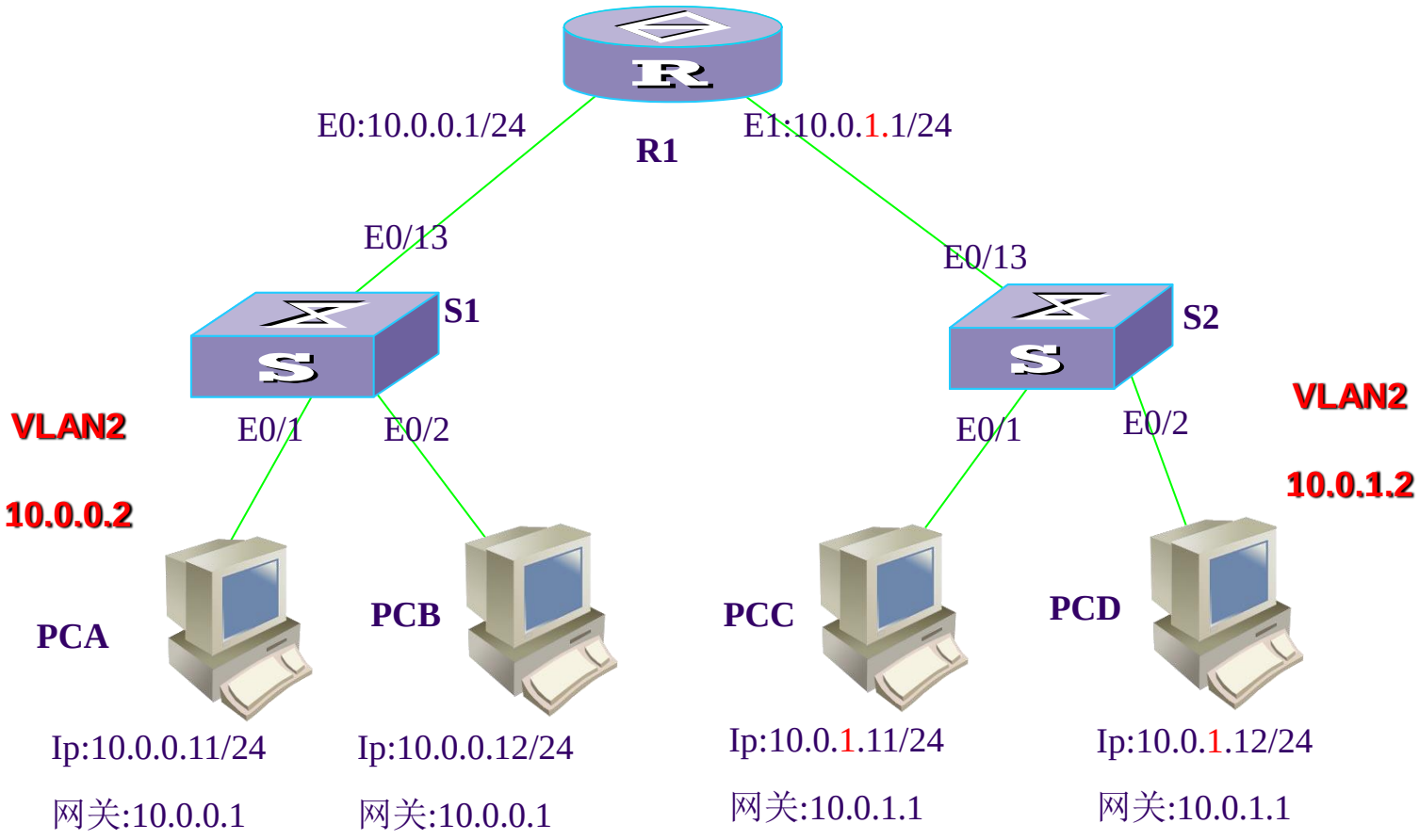
主要内容

- 网管基本概念
- SNMP协议简介
- Quidview网管软件功能介绍
- 网络管理实验
  - 网管软件功能演示
  - SNMP协议分析
  - 网络拓扑发现

SNMP协议分析

- 实验目的
  - 了解SNMP协议的工作过程
  - 理解SNMP报文格式以及管理信息库MIB的结构
  - 理解管理信息结构SMI及抽象语法记法1(ASN.1)
- 实验环境
  - Quidway 26 系列路由器 1 台，S3526以太网交换机1 台，PC机 4 台，标准网线6 根；
  - 每组4名同学，各操作1台PC协同进行实验。

实验组网图



注：交换机S1和S2的E0/1到E0/20都划分到VLAN2

实验步骤

- 按照上面的组网连接各实验设备，并正确配置IP地址
- 在每台交换机及路由器上配置SNMP代理
- 在PC机上安装Quidview网管软件，每组每次最好一台PC来管理网络，按照实验步骤轮流进行实验
- 分析截获的报文
- 注意：若网管软件不能关闭路由器的端口，可用网管软件管理交换机来实现。

网管软件关闭交换机端口

- 启动抓包软件，准备截获报文；
- 在交换机S2上配置trap

```
[S2]snmp trap enable
[S2]snmp target-host trap address udp-domain 10.0.0.11 params securityname public
```

注：路由器AR2811 trap 命令配置与此相同。

- 进入以太网交换机网管系统，选定S2；
- 选定端口，鼠标右键，弹出菜单->端口配置->将选定端口状态由up改为down；
- 分析截获报文，重点分析“set”和“trap”报文。

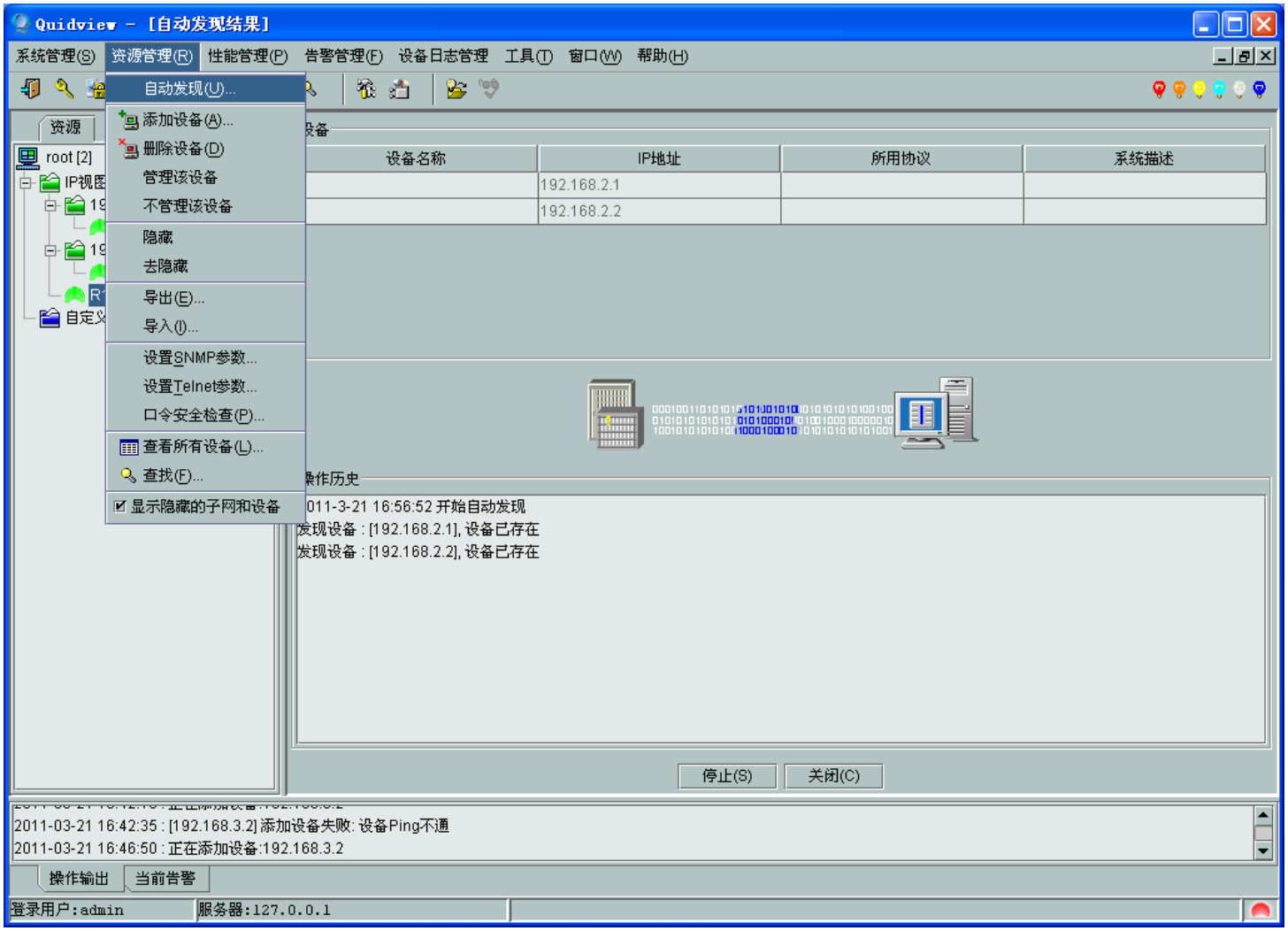
主要内容

- 网管基本概念
- SNMP协议简介
- Quidview网管软件功能介绍
- 网络管理实验
  - 网管软件功能演示
  - SNMP协议分析
  - 网络拓扑发现

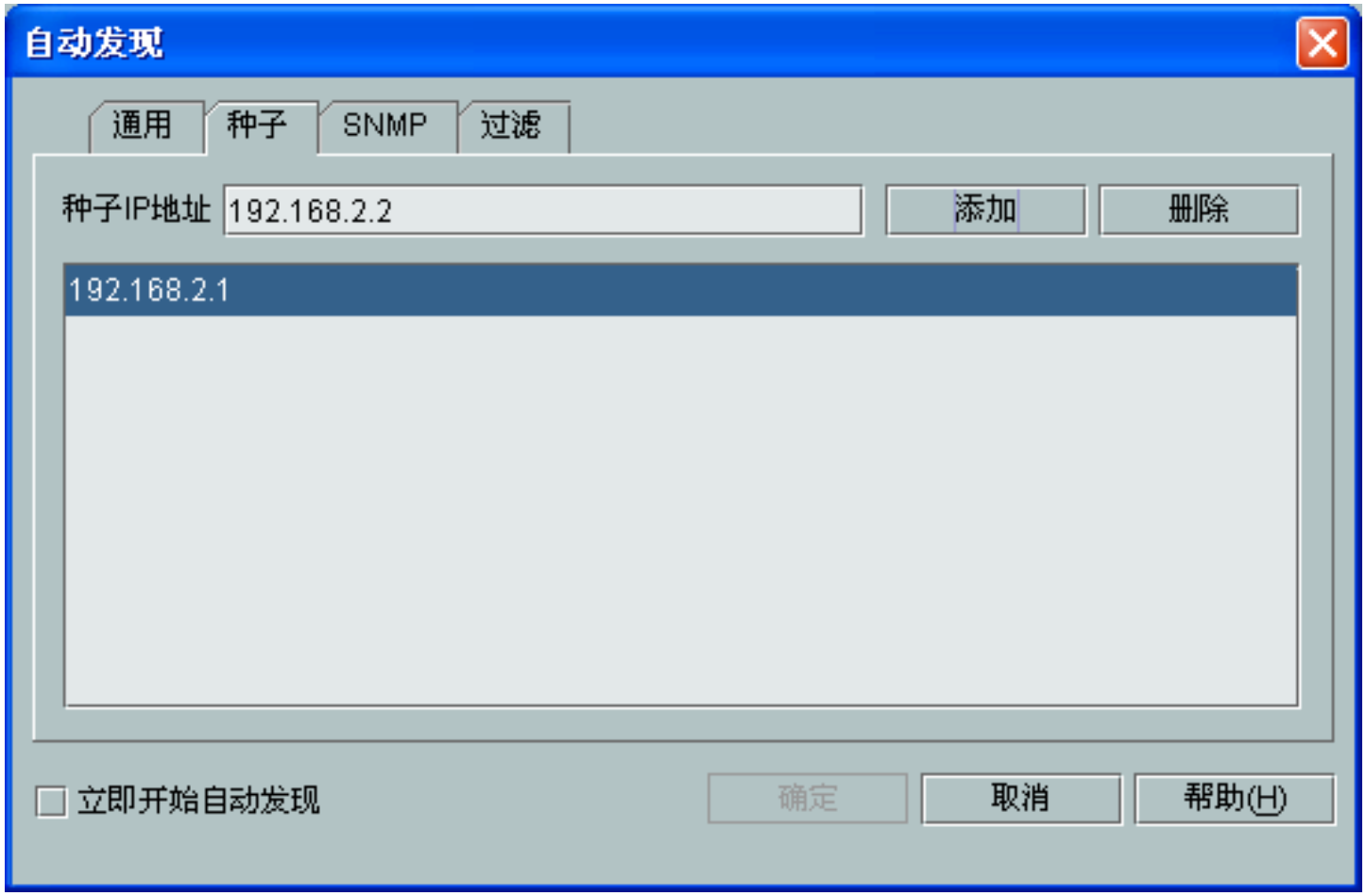
网络拓扑发现

- 发现原理
  - 拓扑管理平台选择种子节点（Seed）；
  - NMS首先读取种子节点（Seed）的路由表，通过分析路由表确定网络上有哪些已存在的子网；
  - 通过发ping或broadcast报文来确定子网中的设备；
  - 根据学习到的网络信息及设备和主机的信息，按一定的算法形成拓扑结构。
- 种子节点设置的基本经验
  - Seed节点位置比较居中、路由信息较为丰富的设备；
  - 一般平台支持多种子节点。

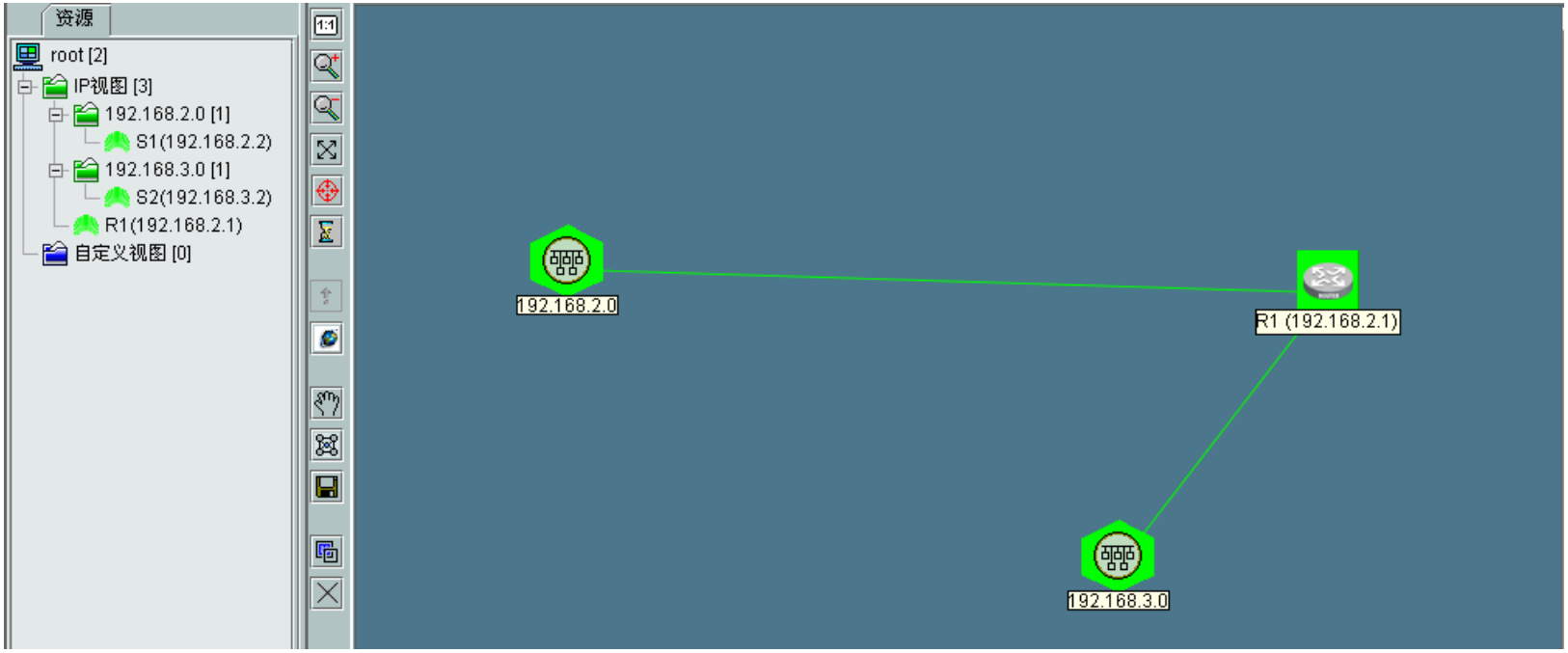
网络拓扑自动发现


Quidview - [自动发现结果]
系统管理(S)
资源管理(R)
性能管理(P)
告警管理(F)
设备日志管理
工具(T)
窗口(W)
帮助(H)
自动发现(U)...
添加设备(A)...
删除设备(D)
管理该设备
不管理该设备
隐藏
去隐藏
导出(E)...
导入(I)...
设置SNMP参数...
设置Telnet参数...
口令安全检查(P)...
查看所有设备(L)...
查找(F)...
显示隐藏的子网和设备
资源
root [2]
IP视图
自定义
设备名称
IP地址
所用协议
系统描述
192.168.2.1
192.168.2.2
操作历史
011-3-21 16:56:52 开始自动发现
发现设备 : [192.168.2.1], 设备已存在
发现设备 : [192.168.2.2], 设备已存在
停止(S)
关闭(C)
2011-03-21 16:42:35 : [192.168.3.2] 添加设备失败: 设备Ping不通
2011-03-21 16:46:50 : 正在添加设备:192.168.3.2
操作输出
当前告警
登录用户:admin
服务器:127.0.0.1

网络拓扑自动发现


自动发现
通用
种子
SNMP
过滤
种子IP地址
192.168.2.2
添加
删除
192.168.2.1
立即开始自动发现
确定
取消
帮助(H)

网络拓扑自动发现


资源
root [2]
IP视图 [3]
192.168.2.0 [1]
S1(192.168.2.2)
192.168.3.0 [1]
S2(192.168.3.2)
R1(192.168.2.1)
自定义视图 [0]
192.168.2.0
R1 (192.168.2.1)
192.168.3.0

谢谢！