1. **网络管理概论**
   1. 什么是网络管理，网络管理的目标是什么？

计算机网络管理是指采用计算机软、硬件技术对由客户端计算机、服务器、存储和交换机、路由器等网络设备及相关软件组成的网络和信息系统进行管理的工作。

网络管理的根本目标是最大限度地满足网络管理者和网络用户对计算机网络的有效性、可靠性、开放性、综合性、安全性和经济性的要求。

* 1. 网络管理的标准有哪些？

网络管理的标准较多，其中主要的标准是OSI参考模式、TCP/IP参考模型、电信管理网（TMN）参考模型、IEEE LAN/MAN以及基于web的管理。

* 1. iso制定的网络管理标准有哪些文件？其内容是什么？

1989年，颁布了ISO/IRC 7498-4（x.700）文件，定义了网络管理的基本概念和总体框架。

1991年，ISO9595，定义公共管理信息服务。ISO9596，定义公共管理信息协议

1992年，ISO10164，规定系统管理功能。ISO10165,定义信息管理结构。

* 1. TCP/IP网络管理标准有哪些主要的RFC文件？其内容是什么？

1990年，RFC1155，公布管理信息结构。RFC1157公布了SNMP。RFC1212定义了MIB。RFC1213，定义了MIB-2规范。

1993年，RFC1441发布SNMPV2的简介。RFC 1902-1908规范了SNMPV2的结构。

1998年，RFC2271-2275，发布了SNMPv3。

* 1. 简述网络管理的基本模型以及各个组成部分的功能。

OSI参考模式、

TCP/IP参考模型、

电信管理网（TMN）参考模型、

IEEE LAN/MAN参考模型

web参考模型

* 1. 什么是管理站？什么是管理代理？管理代理可以向管理站发送消息吗？

管理站：管理站是一个逻辑的概念，通常由软件来实现，其安装实体可以是工作站，个人计算机等。

管理代理：与管理站对应的，被管实体担当代理角色代理负责提供被管对象的访问。

管理代理可以向管理站发送消息。

* 1. 在网络管理的基本模型中管理站的作用是什么？管理代理的作用是什么？

管理站：负责发出管理操作的指令，被管设备中的管理代理对这些指令进行响应，自动或按用户规定去收集管理代理管理的有关主机的运行状态、配置和性能信息。

管理代理：具有两个基本功能：一是从MIB中读取各种变量值；二是在MIB中修改各种变量值

* 1. 网络管理协议主要有哪些？

简单网络管理协议SNMP和公共管理信息服务与公共管理信息协议CMIS/CMIP

* 1. MIB中包括了哪些信息？p35

结构数据

动态数据

控制数据

* 1. 集中式网络管理和分布式网络管理有什么区别？各有什么优缺点？

集中式网络管理：由一个管理站队整个网络管理负责。

优点：管理集中，有专人负责，有利于从整个网络系统的全局对网络实施较为有效的管理。

缺点：管理信息集中汇总到网络管理中心节点上，导致网络信息流比较拥挤，管理不够灵活。管理节点如果发生故障有可能影响全网正常工作。

分布式网络管理：将局部管理任务、存储能力和部分数据库转移到被管设备中，使被管设备成为具有一定自我管理能力的自治单元。

优点：能容纳整个网络的增长和变化，既提供了很好的扩展性，同时也降低了管理的复杂性。

将管理任务都分布到各域的管理站，使网络管理更加稳定可靠，提高网络性能。

缺点：

* 1. 简述网络管理的软件结构。

用户接口软件

管理专用软件

管理支持软件

* 1. 网络管理的五大功能是什么？分别对每个功能进行简单的描述。p40

故障管理

配置管理

安全管理

性能管理

计费管理

* 1. 网络管理对于网络的正常运行有什么意义？

1、减少停机时间，2、改进响应时间，3、提高设备的利用率4、减少运行费用5、减少网络瓶颈6、提高运行效率

* 1. 局域网管理与网络管理有什么不同？试举出几种管理功能。
  2. 被管理的网络设备主要有哪些？

中继器、网桥、交换机、路由器和网关

数据库、中间件、备份软件

* 1. 网络管理系统分为哪些层次？

1、OSI/RM2、管理站3、代理系统

网络管理框架内容：各种网络管理应用工作的基础结构，1、管理功能分为管理站和代理2、为存储管理信息提供数据库支持3、提供用户接口和用户视图功能4、提供基本的管理操作

* 1. 网络管理框架的主要内容有哪些？在管理站和管理代理中应配置哪些软件实体。

主要内容：

管理站

管理代理

网络管理协议

管理信息库MIB

实体：

管理站：1、OS 2、通信3、NME(网络管理实体) 4、应用5、NMA(网络管理应用)

代理：1、OS 2、通信3、NME(网络管理实体) 4、应用

* 1. 什么是委托代理

有些设备不支持当前的网络管理标准，或无法完整实现NME全部功能，或不能运行附加软件，用来管理这些非标准设备的标准设备，称为委托代理。

* 1. 性能测试报告应包括哪些内容？

路由器性能。主要包括端口流量，温度，cpu利用率和内存余量等

实时性能监控。主要包括流量，丢包率，延迟，温度，内存余量和cpu利用率等。

统计分析。扫描数据文件，绘制性能分布图。

* 1. 故障管理可分为哪些功能模块？

故障检测和报警功能

故障预测功能

公章诊断和定位功能

* 1. 网络计费的管理有哪些？计费日志应包括哪些信息？

基于网络流量计费。

基于使用时间计费。

基于网络服务计费。

日志：

1. 用户标识符2、连接目标的标识符3、传送的分组数/字节数4、安全等级5、时间戳6、指示网络出错情况的状态码7、使用的网络资源
   1. 配置管理应包含哪些功能模块？设备的配置信息有哪些？

功能模块：

定义配置信息。

设置和修改设备属性

定义和修改网络元素的互连关系

启动和终止网络运行

发型软件

检查参数值、互联关系和报告配置现状

设备配置信息：

网络设备的拓扑关系：即存在性和连接关系

网络设备的域名、IP地址：即寻址信息

网络设备的运行特性：即运行参数

网络设备的备份操作参数：即是否备份、备份启用条件

网络设备的配置更改条件

* 1. 计算机网络的安全需求有哪些？

保密性

数据完整性

可用性

* 1. 对计算机网络的安全威胁有哪些？对网络管理的安全威胁有哪些？

计算机网络的安全威胁：

中断

窃取

窜改

假冒

网络管理的安全威胁：

伪装的用户

假冒的管理程序

侵入管理站和代理间的信息交换过程

* 1. 计算机网络的安全管理应包含哪些内容？

安全信息维护

资源访问控制

1. 抽象语法表示ASN.1

2-1 表示层的功能是什么？抽象语法和传输语法各有什么作用？

表示层的功能是提供统一的网络数据表示。

ASN.1( 抽象语法表示 )：一种形式语言，提供统一的网络数据表示，通常用于定义应用数据

的抽象语法和应用层协议数据单元的结构

传输语法：把抽象数据变换成比特串的编码规则

2-2 用ASN.1表示一个协议数据单元（例如，IEEE 802.3的帧）

GetRequest-PDU::=SEQUENCE{

request-id INTEGER,

error-status INTEGER,

error-index INTEGER,

variable-bindings VarBind

}

VarBind::=SEQUENCE{

name OBJECT IDENTIFIER,

value NULL

}

2-3 用基本编码规则对长度字段L编码：L=18，L=180，L=1044。

L=18，00010010；L=180，1000000110110100；L=1044，1000100010010100

2-4 用基本编码规则对下面的数据编码：标签值=1011001010,长度=255。

标签编码：×××111111000010111001010；长度编码：1000000111111111

2-5 为什么要用宏定义？怎样由宏定义得到宏实例？

使用宏定义的目的是为了简化类型定义的方法。

用具体的值代替宏定义中的变量可以产生宏实例

2-6 写出一个ASN.1的模块，该模块ENUMERATED数据类型定义了Months Of Year，它的值

从1到12.

monthsOfYear ::= ENUMERATED{

January (1),

Febryary(2),

March (3),

April (4),

May (5),

June (6),

July (7),

August(8),

Setember(9),

October(10),

November(11),

December(12)

}

2-7 写出一个ASN.1的模块，该模块以SEQUENCE数据类型指定Months Of Year,并以VisibleString类型指定一年中的每一个月（month1,month2...）。写出ASN.1对于结构的描述，并写出对于值的描述。

monthsOfYear ::= SEQUENCE{

Month1 VisibleString,

Month2 VisibleString,

Month3 VisibleString,

Month4 VisibleString,

Month5 VisibleString,

Month6 VisibleString,

Month7 VisibleString,

Month8 VisibleString,

Month9 VisibleString,

Month10 VisibleString,

Month11 VisibleString,

Month12 VisibleString,

}

2-8 子类型分为哪几种？分别举例说明。

子类型是由限制父类型的值集合而导出的类型，所以子类型的值集合是父类型的子集。子类型还可以产生子类型。产生子类型的方法有以下6种。

1. 单个值（single value）：列出子类型可取的各个值。例如，TestResule ::= INTEGER(0|1|2)
2. 值区间（value range）:这种方法只能用于整数和实数，指出子类型可取的区间，例如，EmployeeNumber::=INTEGER(1000...20000)
3. 允许字符（Permitted Alphabet）:允许字符只能用于字符串类型，限制字符集的取值范围。例如，House Size::=IA5STRING(FROM (“0”|“1”|“2”|“3”|“4”|“5”|“6”|“7”|“8”|“9”)SIZE(5))
4. 限制大小（Size Constrained）:可以限制5种类型（BIT STRING,OCTET STRING,CHARACTER STRING,SEQUENCE OF,SET OF）的规模大小，例如，WorkstationNumber::=OCTET STRING(SIZE(32))
5. 包含子类型（Contained Subtype）:从已有的子类型定义新的子类型，新子类型包含原子类型的全部可能的值。用关键字INCLUDES，说明被定义的类型包含了已有类型的所有的值。例如，First-quarter::=Months (January,February,March)
6. 内部子类型（Inner Subtype）适用于SEQUENCE,SEQUENCE OF,SET,SET OF 和CHOICE类型，主要用于对这些结构的元素项进行限制。例如，下面定义的协议数据单元（PDU）类型。

PDU::=SET{

alpha [0]INTEGER

Beta [1]IA5STRING OPTIONAL

Ganma [2]SEQUENCE OF parameter

Delta [3]BOOLEANi8

}

2-9 RFC 1212给出的宏定义由哪些部分组成？试按照这个宏定义产生一个宏实例。

宏定义由类型表示（TYPE NOTATION）、值表示（VALUE NOTATION）和支持产生式（supporting syntax）3部分组成，而最后部分是任选的，是关于宏定义中类型的详细语法说明。

宏实例（即ASN.1类型）的定义首先是对象名，然后是宏定义的名字，最后是宏定义规定的宏体部分、下面给出的对象定义的示例，对Internet控制报文协议流入的信息计数。

icmpIMSgs OBJECT-TYPE

SYNTAX Counter

ACCESS read-only

STATUS mandatory

::={icmp 1}

**第3章 管理信息结构**

**3.01Internet网络管理框架由哪些部分组成?支持SNMP的体系结构由哪些协议层组成？**

答：

1、RFC1155定义了管理信息结构(SMI)，即规定了管理对象的语法和语义

2、RFC1212说明了定义MIB模块的方法

3、RFC1213定义了MIB-2管理对象的核心集合，这些管理对象是任何SNMP系统必须实现的

4、RFC1157是SNMPV1协议的规范文件。

应用层协议，UDP协议，TCP/IP

**3.02SNMP环境中的管理对象是如何组织的？这种组织方式有什么意义？**

答：组织：分层的树结构。

意义：

1. 表示管理和控制关系
2. 提供了结构化的信息组织技术
3. 提供了对象命名机制。
4. 采用这种层次树结构的组织方式易于管理，易于扩充。

**3.03MIB-2中的应用类型有哪些？计数器类型和计量器类型有什么区别？**

答：

1、networkaddress::=choice{internet ipaddress}

2、internet object identifier::={iso(1)org(3)dod(6)1}

3、ipaddress::=[application 0] implict octet string(size(4))

4、counter::= [application 1] implict intrger(0..4 294 967 295)

5、gauge:= [application 2] intrger(0..4 294 967 295)

6、timeticks::= [application 3] intrger(0..4 294 967 295)

7、opaque::= [application 4] octet string—arbitrary ASN.1 value

区别：计量器与计数器不同的地方是计量器达到最大值后不回零，而是锁定在232-1

**3.04 RFC1212给出的宏定义由哪些部分组成？试按照这个宏定义产生一个宏实例。**

宏定义由类型表示（TYPE NOTATION）、值表示（VALUE NOTATION）和支持产生式（supporting syntax）3部分组成，而最后部分是任选的，是关于宏定义中类型的详细语法说明。

宏实例（即ASN.1类型）的定义首先是对象名，然后是宏定义的名字，最后是宏定义规定的宏体部分、下面给出的对象定义的示例，对Internet控制报文协议流入的信息计数。

icmpIMSgs OBJECT-TYPE

SYNTAX Counter

ACCESS read-only

STATUS mandatory

::={icmp 1}

**3.05MIB-2的管理对象分为哪几个组？**

答：1、系统组2、接口组3、地址转换组4、IP组5、ICMP组6、TCP组7、UDP组8、EGP组9、传输组

**3.06什么是标量对象？什么是表对象？标量对象和表对象的实例如何标识？**

 标量对象 指 SMI

中存储的简单对象和表中的列对象。

表对象是指 SMI

中存储的二维数组对象。

表的定义要使用

ASN.1 的序列类型和对象类型宏定义中的索引部分。表中的标量对象叫做

列对象， 列对象有唯一的对象标识符，

这对每一行都是一样的。

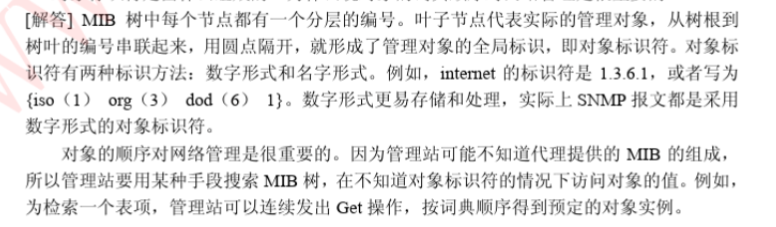
列对象的对象标识符与索引

对象的值组合起来就说明了列对象的一个实例。

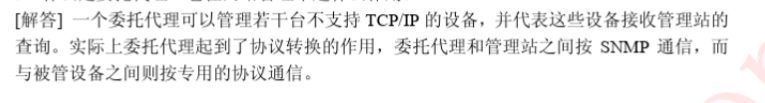
**3.07为什么不能访问表对象和行对象？**

答：表和行对象是没有实例标识符的，因为她们不是叶子节点，SNMP不能访问。

**3.08对象标识符是由什么组成的？为什么说对象的字典顺序对网络管理是很重要的？**



3-10 什么是委托代理？它在网络管理中起什么作用？



3-11 简述对不支持TCP/IP的设备如何进行SNMP管理。

SNMP要求所有的代理设备和管理站都必须实现TCP/IP协议，但这对于不支持TCP/IP的设备就不能直接用SNMP进行管理。为此，提出了委托代理的概念，一个委托代理设备可以管理多台非TCP/IP设备，并代表这些设备接收管理站的查询，实际上委托代理起到了协议转换的作用，委托代理和管理站之间按SNMP协议通信，而与被管理设备之间则按专门的协议通信。

3-12什么是团体名？它的主要作用是什么？

[解答 ] 每个代理管理若干管理对象， 并且与某些管理站建立团体 （community ）关系。 团体名作为团体的全局标识符， 是一种简单的身份认证手段。 一般来说代理进程不接受没有 团体名验证的报文， 这样可以防止假冒的管理命令， 同时在团体内部也可以实行专用的管理策略

3-13 为什么MIB采用树状结构？在internet节点下定义了哪些子树？各起什么作用？

[解答 ] MIB 采用树状结构的组织方式易于管理，易于扩充。

在 internet 对象标识符下定义了如下 4 个子树，把 internet 节点划分为 4 个子树，为

SNMP 的试验和改进提供了非常灵活的管理机制。

（1）Directory （1）保留在将来使用，是为 OSI 的目录服务（ X.500 ）使用的。

（2）Mgmt （2）包括由 IAB 批准的所有管理对象，而 mib-2 （RFC 1213 ）是 mgmt （ 2）

的第一个子节点。

（3）Experimental （3）子树用来标识在互联网上实验的所有管理对象。在这个子树下的所

有对象的标识符都以整数 1.3.6.1.3 开始。

4）Private （4）子树是为私有用户管理信息准备的，目前这个子树只有一个子节点enterprise （1）。一个企业是一个注册了它的自定义 MIB 扩展的组织。该节点下的每个子树分配给一个企业，然后企业就可以在该子树下创建它的产品特有的属性。厂商自定义 MIB 都处于这个层次型结构的位置。

3-14 用ASN.1定义表对象tcpConnTable。

[解答 ] tcpConnTable OBJECT-TYPE

SYNTAX SEQUENCE OF tcpConnEntry

ACCESS not-accessible

STATUS mandatory

DESCRIPTION

"A table containing TCP connection-specific information"

： ：=｛tcp 13 ｝

tcpConnTable OBJECT-TYPE

SYNTAX TcpConnEntry

ACCESS not-accessible

STATUS mandatory

DESCRIPTION

＂Information about a particular TCP connection. An object of

this type is transient, in that it ceases to exist (or soon after)

the connection makes the transition to the CLOSED state. ＂

INDEX ｛tcpConnLocalAddress,

tcpConnLocalPort,

tcpConnRemAddress,

tcpConnRemPort ｝

： ：=｛tcpConnTrable 1 ｝

tcpConnEntry ： ：=SEQUENCE ｛

tcpConnState INTECER,

tcpConnLocalAddress IPAddress,

tcpConnLoc

alPort INTEGER(0..65535) ，

tcpConnLocalPort INTEGER(0..65535) ，

tcpConnRemAddress IPAddress,

tcpConnRemPort INTEGER （0..65535 ） ｝

tcpConnState OBJECT-TYPE

SYNTAX INTEGER ｛closed(1), listen(2), SynSent(3),

synReceived(4), established(5), finWaitl(6),

finWait2(7), closeWait(8), lastAck(9), closing(10),

timeWait(11), deleteTCB(12) ｝

ACCESS read-write

STATUS mandatory

DESCRIPTION

"The state of this TCP connection."

： ：=｛tcpConnEntry 1 ｝

tcpConnLocalAddress OBJECT-TYPE

SYNTAX IpAddress

ACCESS read-only

STATUS mandatory

DESCRIPTION

"The local IP address for this TCP connection."

： ：=｛tcpConnEntry 2 ｝

tcpConnLocalPort OBJECT-TYPE

syntax integer(0..65535)

ACCESS read-only

STATUS mandatory

DESCRIPTION

"The local port number for this TCP connection."

： ：=｛tcpConnEntry 3 ｝

tcpConnRemAddress OBJECT-TYPE

SYNTAX IpAddress

ACCESS read-only

STATUS mandatory

DESCRIPTION

"The remote Ipaddress for this TCP connection."

：

：=｛tcpConnEntry 4 ｝

： ：=｛tcpConnEntry 4 ｝

tcpConnRemPort OBJECT-TYPE

SYNTAX INTEGER(0..65535)

ACCESS read-only

STATUS mandatory

DESCRIPTION

"The remote port number for this TCP connection."

： ：=｛tcpConnEntry 5 ｝

3-16 如果某主机的对象sysServices的值为68，则该主机提供了哪些协议层服务？

68 对应的路由器返回值为 10001

00B ，对应的协议层为第三层和第七层。

3-17 对象ifOpenStatus的值分别为1和2，这说明什么？

在 MIB-2 功能组的接口组中，如果对象 ifAdminStatus 的值为 up(1) ，而 ifOperStatus

的值 down(2) ，则该接口处于故障状态。如果对象 if\_AdminStatus 、ifOperStatus 的值均

为 up(1) ， 则接口处于正常状态； 如果对象 ifAdminStatus 、 ifOperStatus 的值均为 down(2) ，

则接口处于停机状态；如果对象 ifAdminStatus 、ifOperStatus 的值均为 Testing(3) ，则接口处于测试状态

3-18如何计算接口的输入错误率，输出错误率，丢弃的输入包率和输出包率？

[解答 ] 接口的输入和输出错误率计算如下：

输入错误百分率 =ifInErrors/(ifInUcastPkts+ifInNUcastPkts)

输出错误百分率 =ifOutErrors/(ifOutUcastPkts+ifOutNUcastPkts)

丢弃的输入包率 =ifInDisscards/(ifInUcastPkts+ifInNUcastPkts)

丢弃的输出包率 =ifOutDiscards/(ifOutUcastPkts+ifOutNUcastPkts)

3-19 如何计算IP数据包的输入错误率、输出错误率、输入速率和转发速率？

IP 输入错误率 =(ipInDiscards + ipInHdrErrors + ipInAddrErrors)/ ipInReceives IP 输

出错误率 =(ipOutDiscards + ipOutNoRoutes)/ ipOutRequests

IP 输入速度 = (ipInReceivesy - ipInReceivesx)/(y -x)

ipForwDatagrams 告知设备对 IP 数据报转发的速率， 如果在时刻 x 和时刻 y 被两次查

询，则可得 IP 转发速度。

IP 转发速度 = (ipForwGatagramsy - ipForwDatagramsx)/(y-x)

3-20如何计算ICMP分组的发送率和接收率？

计算 ICMP 分组的发送率和接收率，必须首先获得实体发送和接收的分组的总数，这

可以通过找出每个接口的输出分组和输入分组的总数完成，然后用 icmpOutMsgs 和

icmpInMsgs 去除以该和从而获得发送和接收 ICMP 分组的百分率。通过多次查询该对象，

可以找出 ICMP 分组发送和接收实体的速率。

3-21 通过哪些对象可以知道输入的ECHO消息个数、输入的EchoReply消息个数和输入的超时消息个数？

通过 icmpInEchos 可以知道输入的 Echo 消息个数；通过 icmpInEchoReps 可以知道输入的 EchoReply 消息个数；通过 icmpInTimeExcds 可以知道输入的超时消息个数。

3-22 如何计算TCP段的输入速率和输出速率？

让应用在不同的时间查询 tcpInSegs 和 tcpOutSegs 的值，可以检测 TCP 段的输入速率和输出速率。

3-23 如何计算UDP包的输入速率和输出速率？

查询 udpInDatagrams 和 udpOutDategrams 会产生数据报的输入速率和输出速率。

3-24 已知某一路由器某一端口的IP地址，如何用MIB-2查询该端口的物理地址？

IP-> IPAddressT able-> 端口编号 ->ifT able->MAC 地址

1. **简单网络管理协议**

4-1 SNMPv1支持哪些管理操作？对应的PDU格式如何？

答：

1. *GET*，管理站用于检索管理信息库中标量对象的值
2. *SET*，管理站用于设置管理信息库中标量对象的值
3. *TRAP*，代理用于向管理站报告管理对象的状态变化。

*GET,SET*的*PDU*格式：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *PDU*类型 | 请求标识 | 错误状态 | 错误索引 | 变量绑定表 |

*TRAP*格式：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| *PDU*类型 | 制造商*ID* | 代理地址 | 一般陷入 | 特殊陷入 | 时间戳 | 变量绑定表 |

4-2 SNMPv1报文采用什么样的安全机制？这种机制有什么优缺点？

答：*SNMPv1*的安全机制很简单，只是验证团体名。

优点：简单性。缺点：很不安全，团体名以明文形式传输，容易被第三者窃取。

4-3 举例说明如何检索一个简单对象？如何检索一个表对象？

答：*P76*

4-4 怎样利用GetNext命令检索未知对象？

答：发出命令：*GetNextRequest*（*udpInDatagrams.2*）

得到响应：*GetResponse*（*udpNoPorts.0*＝*1*）

4-5 如何更新和删除一个表对象？

答：更新：*SetRequest*（*ipRouteMetric 1.9.1.2.3=9*）

*GetResponse*（*ipRouteMetric1.9.1.2.3=9*）

删除：*SetRequest*（*ipRouteType.7.3.5.3=invalid*）

*GetResponse*（*ipRouteType.7.3.5.3=invalid*）

4-6 试描述数据加密、身份认证、数字签名消息摘要在网络安全中的作用，这些安全工具能对付哪些安全威胁？

答：

1. 数据加密：保密通信的基本手段
2. 身份认证：防止主动攻击的方法
3. 数字签名：防止否认的方法

*4*、消息摘要：验证消息的完整性

对付：窃取，假冒，篡改等安全威胁

4-7 SNMPv2对SNMPv1进行了哪些扩充？

答：*1*、管理信息结构的扩充*2*、管理站和管理站之间的通信*3*、新的协议操作

4-8 SNMPv2对计数器和计量器类型的定义做出了哪些改进？这些改进对网络管理有什么影响？

答：增加了两种新的数据类型，计数器没有定义的初始值，只有连续两次读计数器得到的增加值才有意义。规定了*Gauge32*的最大值可以设置为小于*232*的任意正数*MAX*。明确了当计数器到达最大值时可自动减少。

影响：这样规定更细致，应用更方便

4-9 举例说明不同类型的索引对象如何作用表项的索引。

4-10 在表的定义中，AUGMENTS字句的作用是什么？

答：*AUGMENTS*子句的作用是代替*INDEX*子句，标识概念行的扩展。

*SNMPv2*表的定义中必须包含*INDEX*或*AUGMENTS*子句，但是只能有一个。*INDEX*子句定义了一个基本概念行，而*INDEX*子句中的索引对象确定了一个概念行实例。

4-11 允许生成和删除的表与不允许生成和删除的表有什么区别？

答：*SNMPv2*把表分为两类：

*1*、禁止删除和生成行的表：这种表的最高访问级别是*read-write*。在很多情况下这种表由代理控制，表中只包含*read-only*型的对象。

*2*、允许删除和生成行的表：这种表开始时候可能没有行，由管理站生成和删除行。行数可由管理站或代理改变。

4-12 试描述生成表项的两种方法。

答：1、管理站通过事务处理产生和激活概念行2、管理站与代理协商生成概念行

生长概念行的4个步骤：1、选择实例标识符2、a管理站通过事务处理产生和激活概念行b管理站与代理协商生成概念行3、初始化非默认值对象4、激活概念行

4-13 SNMPv2管理信息库增加了哪些新的对象？

答：1、系统组：标量对象sysORLastChange、表对象sysORTable 2、SNMP组3、MIB对象组：子组（snmpTrap）snmpTrapOID，snmpTrapEnterprise 子组（snmpSet）：snmpSerialNo

4-14 试描述SNMPv2的3种检索操作的工作过程。

答：1、GetRequestPDU

2、GetNextRequestPDU

3、GetBulkRequestPDU

4-15 SNMPv2的操作管理框架由哪些部分组成？它们对管理操作的安全有什么作用？

答：主要涉及4个基本概念：参加者、上下文、MIB视图和访问控制策略

参加者：是否可以成为某次协议操作的参加者是需要进行认证的

4-16 管理站之间的通信有什么意义？需要哪些管理信息的支持？

答：意义：管理站之间的通信机制是分布式网络管理所需要的功能特征。

需要通知报文和管理站数据库支持。

4-17 试描述SNMPv2加密报文的发送和接收过程。

答：发送：发送实体首先构造管理通信消息SNMPMGMTCOM,这需要查找本地数据库，发现合法的参加者和上下文，然后如果需要认证协议，则在snmpmgmtcom前面加上认证信息authinfo，构成认证报文snmpauthmsg，否则把authinfo置为长度为0的字符串。若参加者的认证协议为v2md5authprotocol，则由本地实体按照md5算法计算产生16个字节的消息摘要，作为认证信息中的authdigest。第三步是检查目标参加者的私有协议，如果需要加密，则采用指定的加密协议对snmpauthmsg加密，生成privdata。最后置privdst＝dstparty，组成完整的SNMPV2报文，并经过BER编码发送出去。

接收：目标方实体接收到snmpprivmsg后首先检查报文格式。如果通过，则查找本地数据库，发现需要的验证信息。根据本地数据库的记录，可能需要使用私有协议对报文解密，对认证码进行验证，检查源方参加者的访问特权和上下文是否符合要求等。一旦检查全部通过，就可以支行协议请求的操作了。

4-18 SNMP引擎是由哪些部分组成的？各部分的作用是什么？

答：1、一个调度器：a向/从网络中发送/接收报文b确定SNMP报文的版本，并交给相应的报文处理模块处理c为接收PDU的SNMP应用提供一个抽象的接口d为发送PDU的SNMP应用提供一个抽象的接口

2、一个报文处理子系统：按照预订的格式准备要发送的报文，或者从接收的报文中提取数据

3、一个安全子系统：提供安全服务，例如，报文的认证和加密

4、一个访问控制子系统：确定是否允许访问一个管理对象，或者是否可以对某个管理对象实施特殊的管理操作

4-19 基于用户的安全模型可以防护哪些安全威胁？

答：两种主要威胁：1、修改信息2、假冒

两种次要威胁：1、修改报文流2、消息泄露

4-20 时间序列检验的工作原理是什么？这种检验不能防止哪些安全威胁？

答：为防止报文被重发和故意延迟，每次通信有一个SNMP引擎被指定为有权威的，而通信对方是无权威的。当SNMP报文要求响应时，该报文的接收者是有权威的。反之，当SNMP报文不要求响应时，该报文的发送者是有权威的。有权威的SNMP引擎维持一个时间值，无权威的SNMP引擎跟踪这个时钟值，并保持与之松散同步。

不能防止：窃取，假冒，中断

4-21 HMAC-MDS-96认证协议是怎样计算报文摘要的？试对其安全性进行分析。

答：p111

4-22 SNMPv3怎样进行秘钥管理？

答：通过密钥局部化来管理，也就是把用户的口令字变换成他/她与一个有权威的SNMP引擎共享的密钥。

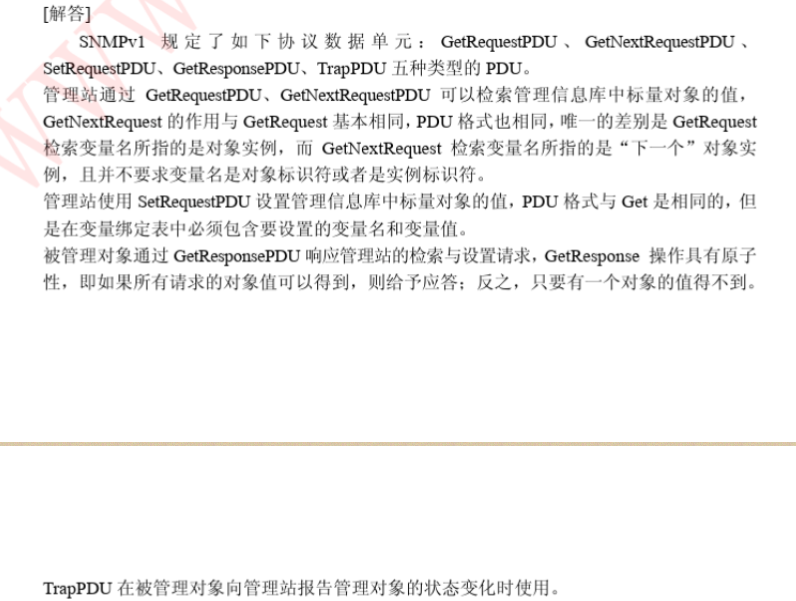
密钥局部化过程的主要思想是把口令字和相应的SNMP引擎标识作为输入，运行一个散列函数，得到一个固定长度的伪随机序列，作为加密密钥。

4-23 视图是怎样定义的？在处理一个访问请求时怎样进行访问呢控制决策？

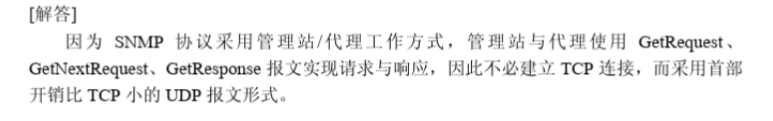
答：为了安全，我们需要把某些组的访问权限制在一个管理信息的子集中，提供这种能力的机制就是MIB视图。

P118

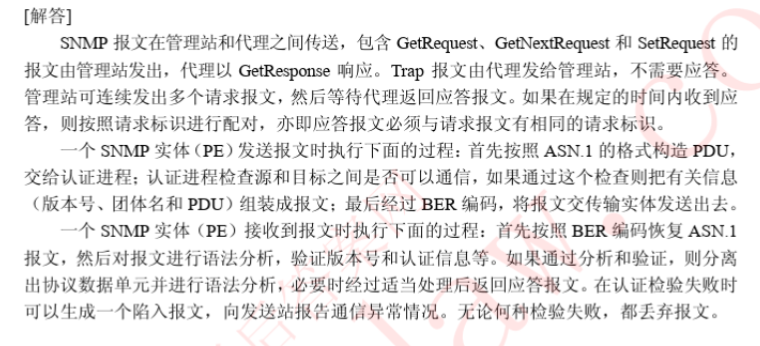
4-24 SNMPv1规定了哪些协议数据单元？分别有什么作用？



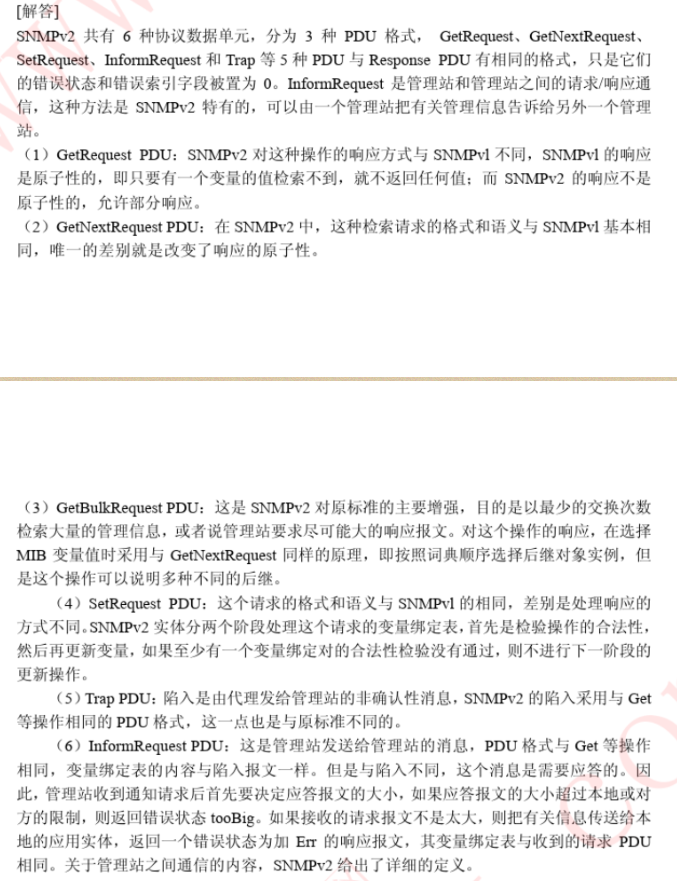
4-25 SNMP为什么不使用TCP传送报文？



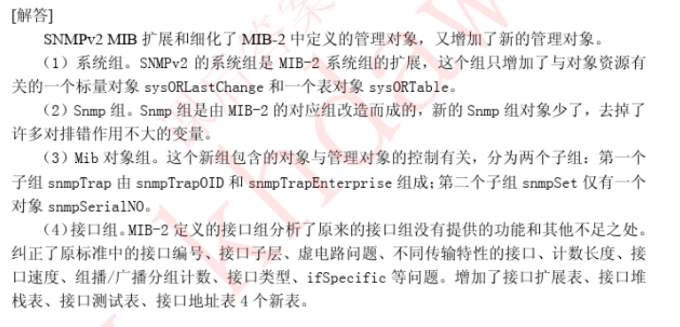
4-26 简述SNMP报文的发送和接收过程。



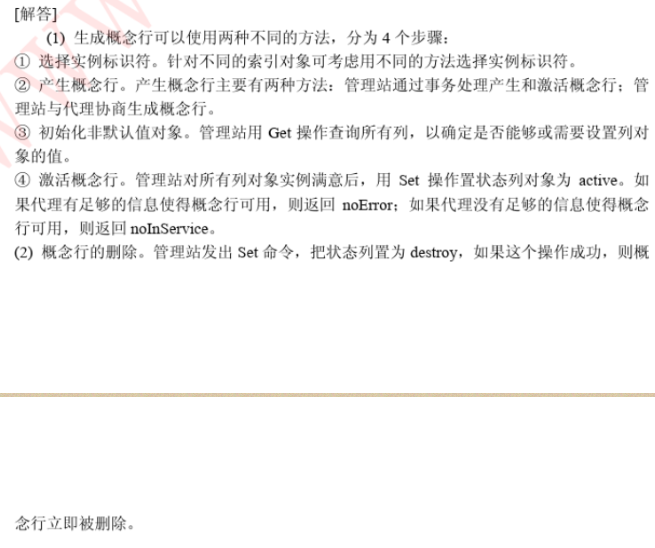
4-27 与SNMPV1相比，SNMPv2在操作上有哪些改变？



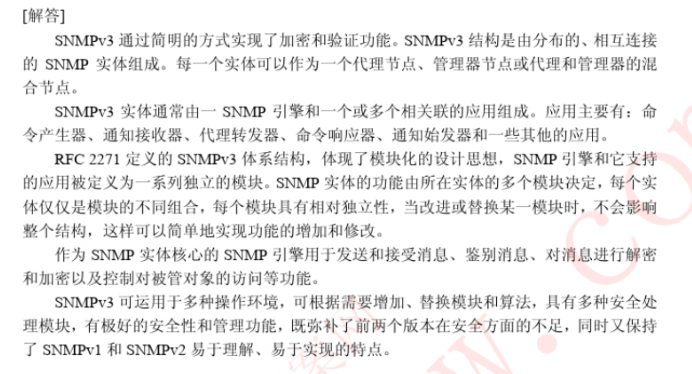
4-28 SNMPv2对MIB-2的扩展包括哪些方面？



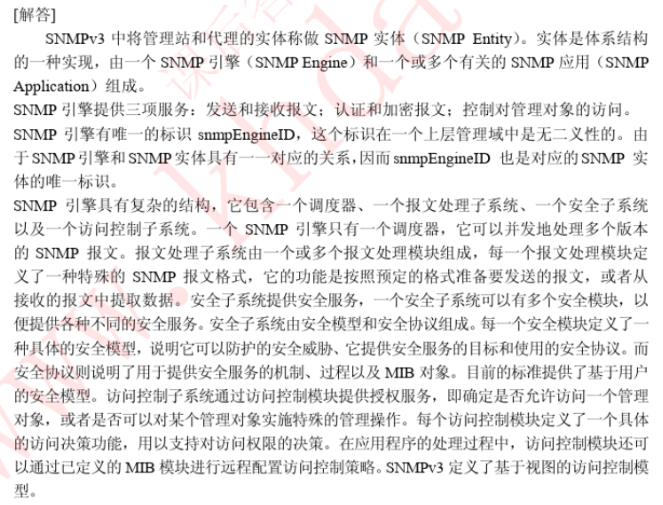
4-29 SNMPv2中，如何进行行的创建和删除？



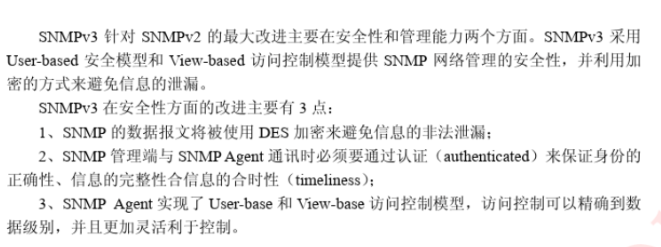
4-30 简述SNMPV3体系结构的特点。



4-31 SNMPv3引擎有什么功能？包括哪几部分？



4-32 SNMPv3在安全方面做了哪些改进？



1. **远程网络监视**

5-1 为什么需要RMON？网络监视器能提供哪些管理信息？

答：因为RMON是对SNMP标准的重要补充，是简单网络管理向互联网管理过渡的重要步骤。RMON扩充了SNMP的管理信息库MIB-2，可以提供有关互联网管理的主要信息，在不改变SNMP协议的条件下增强了网络管理的功能。

提供：出错统计数据，性能统计数据等。

5-2 RMON扩充了哪些功能组？它们的作用是什么？

答：1、协议目录组：提供了各种网络协议的标准方法。

2、协议分布组：提供每个协议产生的通信统计数据。

3、地址映像组：建立网络层地址(IP地址)与MAC地址的映像关系。

4、网络层主机组：类似于RMON1的主机组，收集网上主机的信息。

5、网络层矩阵组：记录主机对(源/目标)之间的通信情况。

6、应用层主机组：记录有关主机发送/接收的分组/字节数等，使用户了解每个主机上的每个应用协议的通信情况。

7、应用层矩阵组：统计一对应用层协议之间的各种通信情况，以及各种选定的参数最大的一对应用层协议之间的通信情况。

8、用户历史组：按照用户定义的参数，周期的收集统计数据。

9、监视器配置组：定义了监视器的标准参数集合

5-3 RMON对表对象的管理作出了什么改进？

答：1、增加了两种新的数据类型，增强规范的可读性2、RMON规范中的表结构由控制表和数据表两部分组成。控制表定义数据表结构，数据表存储数据。

5-4 试根据矩阵组定义的管理对象设计一个显示网络会话的工具。

5-5 举例说明RMON进行状态过滤的逻辑。

5-6 试描述警报组，过滤组、事件组和包捕获组的关系。

答：1、实现警报组时必须实现事件组。

2、实现最高N台主机组时必须实现主机组。

3、实现捕获组时必须实现过滤组。

5-7 为什么要使用外部对象作为表的索引？

答：为了把数据表与对应的控制表结合起来。

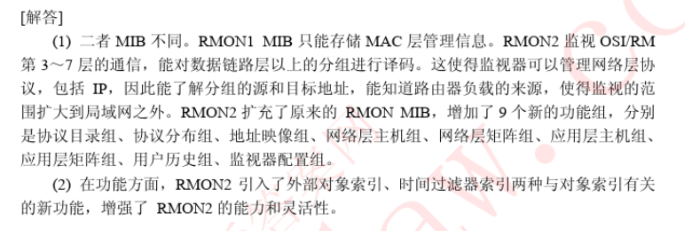
5-8 RMON2如何标识协议之间的关系？

答：用协议标识符和协议参数共同标识一个协议以及该协议与其他协议之间的关系。

5-9 RMON监视器如何配置？

5-10 试把RMON对象划分到各个管理功能域。

5-11 RMON1和RMON2的区别和联系是什么？



5-12 RMON2新增了哪些功能？它们的作用是什么？

