

【期末复习】2021-2022 南邮网络管理理论与实践复习题

计算机网络管理期末复习题

第一章 网络管理概述

01 网络管理对于网络的正常运行有什么意义？

答：P1。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

02 网络管理的主要标准有哪些？

答：P1。网络管理的主要标准分别是：(1) 基于 [OSI 参考模型](#)的 CMIS/CMIP；(2)基于 TCP/IP 参考模型的 [SNMP](#)。

03 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？

答：P3。区别：集中式的网络中，至少有一个结点（主机或路由器）担当管理站角色，所有代理都在管理站监视和控制下协同工作，实现集成的网络管理。而分布式的网络，是地理上分布的多台网络管理客户机与网络管理服务器交互作用，共同完成网络管理功能。

集中式优点：管理人员可以有效的控制整个网络资源，根据需要平衡网络负载，优化网络性能。集中式缺点：网络通信消耗大，管理站失效，将导致网络管理中断；对于大型网络则力不从心。

分布式优点：灵活性和可伸缩性，善于控制大型网络。缺点：不便于统一控制。

04 什么是委托代理？

答：P4。有些设备不支持当前的网络管理标准，或无法完整实现网络管理实体（NME）全部功能，用来管理这些非标准设备的标准设备，称为委托代理。

05 网络管理软件由哪些部分组成？它们的作用各是什么？

答：P5。1、用户接口软件：对网络资源实施本地配置、测试和排错，一定的信息处理能力，实现异构型网络连接

2、管理专用软件：支持多种网络管理应用，如配置管理、性能管理、故障管理

3、管理支持软件：保留管理所需要的相关信息，具有基本文件管理功能，支持节点之间的通信。

07 故障监视可分为哪些功能模块？

答：P13。

1、故障检测和报警功能 日志

1. 故障预测功能 门限值, 警报
2. 故障诊断和定位功能 线路测试

08 计算机网络的安全需求有哪些?

答: P17。

- 1、保密性(Secrecy): 计算机网络中的信息只能由授予访问权限的用户读取(包括显示、打印等, 也包含暴露“信息存在”这样的事实);
- 2、数据完整性(Integrity): 计算机网络中的信息资源只能被授予权限的用户修改;
- 3、可用性(Availability): 具有访问权限的用户在需要时可以利用计算机网络资源。

10 TCP/IP 网络管理标准有哪些主要的 RFC 文件? 各是什么内容?

答: P21。TCP/IP 网络管理在 1987 年 11 月提出的简单网关监控协议

(Simple Gateway Monitoring Protocol, SGMP), 并在此基础上发展为简单网络管理协议第一版 (Simple Network Management Protocol, SNMPv1), 陆续公布在 1990 和 1991 年的几个 RFC (Request For Comments) 文件中, 即

- 1、RFC1155(SMI)
- 2、RFC1157(SNMP)
- 3、RFC1212(MIB 定义)
- 4、RFC1213(MIB-2 规范)

11 什么是网络管理? 网络管理的目标是什么?

[答]:

网络管理是指对网络的运行状态进行监测和控制, 并能提供有效、可靠、安全、经济的服务。

网络管理的目标是使网络的性能达到最优化状态。通过网络管理, 要能够预知潜在的网络故障, 采取必要的措施加以预防和处理, 达到零停机; 通过监控网络性能, 调整网络运行配置, 提高网络性能; 借助有效的性能尺度和评估方法, 扩充和规划网络的发展。所以网络管理的根本目标就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。

12 . 简述网络管理的基本模型以及各个组成部分的功能。

[答] 在网络管理中, 一般采用“管理者—代理”的基本管理模型来构建网络管理系统, 进行实际的网络管理。

网络管理系统的基本模型包括 4 个要素组成, 分别是: 网络管理者、管理代理、管

理信息库和网络管理协议。

网络管理者通过网络管理协议从管理代理那里获取管理信息或向管理代理发送命令；管理代理也可以通过网络管理协议主动报告紧急信息。

管理信息库（Management Information Base, MIB）是一个信息存储库，是对于通过网络管理协议可以访问信息的精确定义，所有相关的被管对象的网络信息都放在 MIB 中。

13 . 什么是网络管理者？什么是管理代理？管理代理可以向网络管理者发送信息吗？

[解答] 网络管理者是管理指令的发出者，它可以自动或按用户规定去轮询被管理设备中某些变量的值，被管设备中的管理代理对这些轮询进行响应，或在接收到被管理设备的告警信息后采取一定的措施。

管理代理负责管理指令的执行，并且以通知的形式向网络管理者报告被管对象发生的一些重要事件。

在有些情况下，管理代理也可以向网络管理者发送通知，管理者可根据报告的内容决定是否做出回答。

14 . 网络管理者，委托代理

- (1) 网络资源：集线器、网桥、路由器、传输设备。
- (2) 软件进程：程序、算法、协议功能、数据库。
- (3) 管理信息：相关人员记录、账号、密码等。

15 . 网络管理的 5 大功能是什么？并分别对每个功能进行简单的描述。

[答] 网络管理的 5 个功能域：

- 1. 故障管理（Fault Management）、
- 2. 配置管理（Configuration Management）、
- 3. 安全管理（Security Management）、
- 4. 性能管理（Performance Management）、
- 5. 计费管理（Accounting Management）。

16.网络管理的 5 大功能中哪些属于网络监视功能？哪些属于网络控制功能？简述其作用。

答：

- 1. **网络监视功能有：**故障管理（Fault Management）、性能管理（Performance

Management)、计费管理 (Accounting Management)

2. **网络控制功能有：**配置管理 (Configuration Management)、安全管理 (Security Management)

1. 网络监视：收集系统和子网的状态信息，分析被管理设备的行为，以便发现网络运行中存在的问题；

2、网络控制：修改设备参数或重新配置网络资源，以便改善网络的运行状态。

17.管理站与代理之间的基本的通信机制有那些？

(1) 轮询：轮询是一种请求---响应式的交互作用，即由管理站向代理发出请求，询问它所需要的信息数值，代理响应管理站的请求，从它所保存的管理信息库中取得请求的信息，返回给管理站。

(2) 事件报告：事件报告是由代理主动发送给管理站的信息。

19、什么是网络的可用性？怎么算

答：网络系统、元素或应用对用户可利用的时间的百分比。

20.什么是响应时间？，计算公式

答：从用户输入请求到系统在终端上返回计算结果的时间间隔。

21.网络的利用率 相对负载，相对利用率

第二章 抽象语法表示

01 表示层的功能是什么？抽象语法和传输语法各有什么作用？

答：见 P23。表示层的功能是提供统一的网络数据表示。抽象语法是用于应用协议构造协议数据单元，与对等系统进行通信。传输语法是将抽象数据变换成比特串的编码规则。

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

答：

L=18

0001 0010

L=180

1000 0001 1011 0100

L=1044

1000 0010 0000 0100 0001 0100

4.基本编码规则对下面的数据编码： 标签值=101 1001010， 长度=255.

答：

标签编码

xxx1 1111 1000 0101 0100 1010

长度编码

1000 0001 1111 1111

5.为什么要用宏定义？ 怎样由宏定义得到宏实例？

简化类型定义的方法

用一个已有的类型代替关键字 type 就可以得到一个宏实例。

02.计算机网络管理中提供统一的网络数据表示的形式语言是什么？

答： 见 P23。ASN.1。

03 . 为什么要用宏定义？ 怎样用宏定义得到宏实例？

[答] ASN.1 宏提供了创建“模板”的功能， 这也是引入 ASN.1 宏的原因。ASN.1 宏使得 ASN.1 语言具有良好的扩充性。

当用一个具体的值代替宏定义中的变量或参数时就产生了宏实例， 它表示一个实际的 ASN.1 类型（称为返回的类型）， 并且规定了该类型可取的值的集合（称为返回的值）。可见宏定义可以看做是类型的类型， 或者说是超类型。

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。

[答] 宏定义由：

- (1) 类型表示 (TYPE NOTATION)、
- (2) 值表示 (VALUE NOTATION)
- (3) 支持产生式 (supporting syntax)

三部分组成， 而支持产生式部分是任选的， 是宏定义体中类型的详细语法说明。

第三章 管理信息库 MIB-2

01 Internet 网络管理框架由哪些部分组成？

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。

02 SNMP 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。

这种层次树结构有 3 个作用：

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

采用这种层次树结构的组织方式易于管理，易于扩充。

03.SNMP 属于的协议簇是什么？

答：TCP/IP

1. RFC1212 给出的宏定义由哪些部分组成？

答：

SYNTAX，表示对象类型的抽象语法

ACCESS，定义 SNMP 协议访问对象的方式

DescrPart，任选，用文字说明对象类型含义

RefValPart，任选，用文字说明可参考在其他 MIB 模块定义的对象

indexpart，用于定义表对象的索引项

defvalpart，定义了对象实例默认值，任选

value notation，指明对象的访问名

05.什么叫陷入（Trap）制导的轮询过程？

答：

管理站启动时、或每隔一定时间用 Get 操作轮询一遍所有代理，以便得到某些关键的信息，或基本的性能统计参数。一旦得到这些基本数据，管理站就停止轮询，而代理进程负责在必要时向管理站报告异常事件，由陷入操作传送给管理站。得到异常事件的报告后，管理站可以查询有关的代理，以便得到更具体的信息，对事件的原因做进一步的分析。

06. 为什么要使用陷入 (Trap) 制导的轮询过程？

答：为了使管理站能够及时而有效地对被管理设备进行监控，同时又不过分增加网络的通负载，必须使用陷入制导的轮询过程。

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。

08. SNMP 由哪些部分组成？

答：

1. 管理信息库结构的定义
2. 访问管理信息库的协议规范

09 . 什么是委托代理？它在网络管理中起什么作用。

[答] 一个委托代理可以管理若干台不支持 TCP/IP 的设备，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 通信，而与被管设备之间则按专用的协议通信。

10 . 什么是团体名？它的主要作用是什么？

[答] 团体名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。

11 . 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？

[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。

12 . 对象标识符是由什么组成的？为什么说对象的词典顺序对网络管理是很重要的？

[答] MIB 树中每个节点都有一个分层的编号。叶子节点代表实际的管理对象，从树根到树叶的编号串联起来，用圆点隔开，就形成了管理对象的对象标识符。对象标识符

有两种标识方法：数字形式和名字形式。例如，internet 的标识符是 1.3.6.1，或者写为 {iso (1) org (3) dod (6) 1}。数字形式更易存储和处理，实际上 SNMP 报文都是采用数字形式的对象标识符。

对象的顺序对网络管理是很重要的。因为管理站可能不知道代理提供的 MIB 的组成，所以管理站要用某种手段搜索 MIB 树，在不知道对象标识符的情况下访问对象的值。例如，为检索一个表项，管理站可以连续发出 Get 操作，按词典顺序得到预定的对象实例。

13 . 标量对象和表对象的实例如何标识？

[答]见习题答案

14 . 为什么不能访问表对象和行对象？

[答] 表和行对象（如 tcpConnTable 和 tcpConnEntry）是没有实例标识符的，因为它们不是叶子节点，SNMP 不能访问，其访问特性为“not-accessible（NA）”。这类对象叫做概念表和概念行。

15、对象 ifOperStatus 和 ifAdminStatus 的值分别为 1 和 2，这说明什么？

[答] ifAdminStatus 对象和 ifOperStatus 对象都返回整数，值 1 表示 Up，值 2 表示 Down。把这两个对象结合在一起，失效管理应用可以确定接口的当前状态。 11 正常 21 故障 22 停机 33 测试

17 ， 词典顺序

18 11 个功能组

• 简单网络管理协议

01 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
--------	--------	------	------	------	-----	-------

02 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。

05 如何更新和删除一个表对象？

答：见 P78--P79

更新：SetRequest (ipRouteMetric1.9.1.2.3=9)

GetResponse (ipRouteMetric1.9.1.2.3=9)

删除：SetRequest (ipRouteType.7.3.5.3=invalid)

GetResponse (ipRouteType.7.3.5.3=invalid)

06.SNMPv1 有哪些局限性？

答：

- (1)由于轮询的性能限制，snmp 不适合管理很大的网络。
- (2)snmp 不适合检索大量数据。
- (3)snmp 的陷入报文是没有应答的，管理站是否收到陷入报文，代理不得而知。可能丢掉重要的管理信息。
- (4)snmp 只提供简单的团体名认证，这样的安全措施是不够的。
- (5)snmp 并不直接支持向被管理设备发送命令。
- (6)snmp 的管理信息库 MIB-2 支持的管理对象是很有限的，不足以完成复杂的管理功能。
- (7)snmp 不支持管理站之间的通信，这一点在分布式网络管理中是很重要的。

07 SNMPv2 对 SNMPv1 进行了哪些扩充？

- 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

08 在表的定义中，AUGMENTS 子句的作用是什么？

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。

10.试描述 SNMPv2 的 3 种检索操作的工作过程。

答：1、GetRequestPDU

2、GetNextRequestPDU

3、GetBulkRequestPDU

14.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

拒绝服务 通信分析

21 . 与 SNMPv1 相比，SNMPv2 的操作有哪些改变？

[答]

SNMPv2 共有 6 种协议数据单元，分为 3 种 PDU 格式，GetRequest、GetNextRequest、SetRequest、InformRequest 和 Trap 等 5 种 PDU 与 Response PDU 有相同的格式，只是它们的错误状态和错误索引字段被置为 0。InformRequest 是管理站和管理站之间的请求/响应通信，这种方法是 SNMPv2 特有的，可以由一个管理站把有关管理信息告诉给另外一个管理站。

(1) GetRequest PDU：SNMPv2 对这种操作的响应方式与 SNMPv1 不同，SNMPv1 的响应是原子性的，即只要有一个变量的值检索不到，就不返回任何值；而 SNMPv2 的响应不是原子性的，允许部分响应。

(2) GetNextRequest PDU：在 SNMPv2 中，这种检索请求的格式和语义与 SNMPv1 基本相同，唯一的差别就是改变了响应的原子性。

(3) GetBulkRequest PDU：这是 SNMPv2 对原标准的主要增强，目的是以最少的交换次数检索大量的管理信息，或者说管理站要求尽可能大的响应报文。

(4) SetRequest PDU：这个请求的格式和语义与 SNMPv1 的相同，差别是处理响应的方式不同。SNMPv2 实体分两个阶段处理这个请求的变量绑定表，首先是检验操作的合法性，然后再更新变量，如果至少有一个变量绑定对的合法性检验没有通过，则不进行下一阶段的更新操作。

(5) Trap PDU：陷入是由代理发给管理站的非确认性消息，SNMPv2 的陷入采用与 Get 等操作相同的 PDU 格式，这一点也是与原标准不同的。

(6) InformRequest PDU：这是管理站发送给管理站的消息，PDU 格式与 Get 等操作相同，变量绑定表的内容与陷入报文一样。但是与陷入不同，这个消息是需要应答的。

22 简述 SNMPv3 体系结构的特点。

[答]

SNMPv3 通过简明的方式实现了加密和验证功能。SNMPv3 结构是由分布的、相互连接的 SNMP 实体组成。每一个实体可以作为一个代理节点、管理器节点或代理和管理器的混合节点。

SNMPv3 实体通常由一 SNMP 引擎和一个或多个相关联的应用组成。应用主要有：命令产生器、通知接收器、代理转发器、命令响应器、通知始发器和一些其他的应用。

作为 SNMP 实体核心的 SNMP 引擎用于发送和接受消息、鉴别消息、对消息进行解密和加密以及控制对被管对象的访问等功能。

23 . SNMPv3 在安全方面做了哪些改进？

[答]

SNMPv3 针对 SNMPv2 的最大改进主要在安全性和管理能力两个方面。SNMPv3 采用 User-based 安全模型和 View-based 访问控制模型提供 SNMP 网络管理的安全性，并利用加密的方式来避免信息的泄漏。

26.SNMPv3 不仅能与以前的标准 SNMPv1 和 SNMPv2 兼容，而且在 SNMPv2c 的基础上加上了什么内容？

答：见 P71

32.管理信息库 MIB-2 接口组中的对象可用于故障管理和性能管理。有关接口状态的对象有 ifAdminStatus 和 ifOperStatus。

- (1) ifAdminStatus 表示什么状态？管理状态
- (2) ifOperStatus 表示什么状态？接口的操作状态
- (3) 通过什么可以检测拥塞？检查进出接口
- (4) 若接口速率对象 ifSpeed 取值为 20000000，表示的数据传输率为多少？
- (5) 怎样判定接口状态正常？

33 snmp 引擎：调度器，报文处理子系统，安全子系统，访问控制子系统

第五章 远程网络监视

01 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。

02.RMON 对表对象的管理做出了什么改进？

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。

04.RMON 功能组在实现时的联带关系都有哪些？

答：见 P123

05. 捕获组的作用是什么？

答：储存从通道中捕获的分组

08.试写出产生上升警报的规则。

答：见 P130

报警机制：警报组定义了下面的警报机制。①如果行生效后的第一个采样值 \leq 上升门限，而后来一个采样值 \geq 上升门限，则产生一个上升警报。②如果行生效后的第一个采样值 \geq 上升门限，且 alarmStartupAlarm=1or 3，则产生一个上升警报。③如果行生效后的第一个采样值 \geq 上升门限，且 alarmStartupAlarm=2，则当采样值落回上升门限后，又变得采样值 \geq 上升门限时则产生一个上升警报。④产生一个上升警报后，除非采样值落回上升门限到达下降门限，并且又一次到达上升门限，将不再产生上升警报。对于下降警报的规则是类似的。

09.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。

10.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。

1. RMON 规范中的表结构的是哪两部分组成的？

答：控制表和数据表

1. 在 RMON 规范中，定义了两种新的数据类型，这两种数据类型是什么？

OwnerString EntryStatus

17.行增加：管理站用 Set 命令在 RMON 表中增加新行，并遵循下列规则，①管理站用

SetRequest 生成一个新行，如果新行的索引值与表中其他行的索引值不冲突，则代理生成一个新行，其状态对象的值为 createRequest (2)，②新行产生后，由代理把状态对象的值置为 underCreation(3)。③新行的状态值保持为 underCreation(3)，直到管理站产生了所有要生成的新行，这时由管理站置每一个新状态对象值为 valid(1)。④如果管理站要生成的新生行已经存在，则返回一个错误。

删除行：

只有行的所有者才能发出 SetRequest PDU，把状态对象的值置为 invalid(4)，这样就删除了行。这是否意味着物理删除，取决于具体的实现。

修改行：

首先置行状态对象的值为 invalid(4)，然后用 SetRequest PDU 改变行中其他对象的值。

18.管理站并发访问的解决方法：

RMON 控制表中的列对象 Owner 规定了表行的所属关系，所属关系有以下用法，可以解决多个管理并发地访问的问题。①管理站能认得自己所属的资源，也知道自己不再需要的资源。②网络操作员可以知道管理站占有的资源，并决定是否释放这些资源。③一个被授权的网络操作员可以单方面地决定是否释放其他操作员保有的资源。④如果管理站经过了重新启动过程，它应当首先释放不再使用的资源。

19.以太网的统计信息：

RFC1757 (Feb1995) 定义的 RMON MIB 主要包含以太网的各种统计数据，以及有关分组捕获、网络事件报警方面的信息。①统计组，提供了一个表，该表每一行表示一个子网的统计信息，其中大部分对象是计数器，记录监视器从子网上收集到的各种不同状态的分组数。②历史组，存储的是以固定间隔取样所获取的子网数据。由历史控制表和历史数据表组成。控制表定义被取样的子网接口编号，取样间隔大小，以及每次取样数据的多少，而数据表则用于存储取样期间获得的各种数据。③主机组，收集新出现的主机信息，其内容与接口组相同。由主机数据表和主机时间表组成。④最高 N 台主机组，记录某种参数最大的 N 台主机的有关信息，这些信息的来源是主机组。这个组包含一个控制表和一个数据表。⑤矩阵组，记录子网中一对主机之间的通信量，信息以矩阵的形式存储。由 3 个表组成。控制表一行指明发现主机对会话的子网接口；数据表分成源到目的 (SD) 和目的到源 (DS) 两表。

20.警报：定义了一组网络性能的门限值，超过门限值时向控制台产生报警事件。必须和事件组同时实现。警报组由一个表组成，该表的一行定义了一种警报：监视的变量、采样区间和门限值。

25.过滤组：过滤组提供一种手段，使监视器可以观察接口上的分组，通过过滤选择出某种指定的特殊分组。定义了两种过滤器：数据过滤器是按位模式匹配，即要求分组的一部分匹配或不匹配指定的位模式；而状态过滤器是按状态匹配，即要求分组具有特

定的错误状态(有效, CRC 错误等)。

26.通道: 各种过滤器可以用逻辑运算来组合, 形成复杂的测试模式。一组过滤器的组合叫通道。可以对通过通道测试的分组统计数据, 也可以配置通道使得通过的分组产生事件(由事件组定义), 或者使得通过的分组被捕获(由捕获组定义)。

27.过滤组结构: 过滤组由两个控制表组成。过滤表 filterTable 定义了一组过滤器, 每一行定义一对数据过滤器和状态过滤变量 filterChannelIndex 说明该过滤器所属的通道; 通道表 channelTable 定义由若干过滤器组成的通道, 每一行定义一个通道。

28.包捕获组: 建立一组缓冲区, 用于存储从通道中捕获的分组。由控制表和数据表组成。

29.事件组: 作用是管理事件。事件是由 MIB 中其他地方的条件触发的, 事件也能触发其他地方的作用。产生事件的条件在 RMON 其他组定义。事件不能使得这个功能组存储有关信息, 甚至引起代理进程发送陷入消息。分为两个表, 事件表, 定义事件的作用; log 表记录事件出现的顺序和时间。

30.RMON2 MIB 的作用: RMON2 监视 OSI/RM 第 3 层至第 7 层的通信, 能对数据链路层以上分组进行译码。这使得监视器可以管理网络层协议, 包括 IP 协议。因而能了解分组的源和目的地址, 能知道路由器负载的来源, 使得监视的范围扩大到局域网以外。监视器也能监视应用层协议, 这样监视器就可以记录主机应用活动的数据, 可以显示各种应用活动的图表。

31.RMON2 新增功能:

RMON2 引入了两种与对象索引的有关的新功能, 增强了 RMON2 的能力和灵活性。①外部对象索引, RMON2 采用了新的表结构, 经常使用外部对象索引数据表, 以便把数据表与对应的控制表结合起来。②时间过滤器索引, 网络管理应用需要周期的轮询监视器, 以便得到被管理对象的最新状态信息。为了提高效率, 使用时间过滤器索引, 使监视器每次只返回那些自上次查询以来改变了的值。

32. RMON2 在网络管理中的应用:

①协议的标识, RMON2 用协议标识符和协议参数共同表示一个协议以及该协议与其它协议之间的关系。协议标识符是由字节串组成的分层的树结构, 类似于 MIB 对象组成的树。RMON 赋予每个协议层 32 位的字节串, 编码为 4 个十进数, 表示为[a.b.c.d.]的形式, 这是协议标识符树的结点。链路层协议字节串是协议标识符树的根, 下面每个直接相连的结点是链路层协议直接支持的上层协议, 或者说是直接包装在数据链路帧中的协议。整个协议标识符树就是这样逐步构造的。

②协议目录表, 协议标识符和协议参数作为表项的索引, 另外还为表项指定了一个唯一的索引, 可由 RMON2 的其它组引用该表项。

③用户定义的数据收集机制，关于历史数据收集在 RMON1 中是预选定义的，在 RMON2 中可以由用户定义。

④监视器的标准配置法，为了增强管理站台票监视器之间的互操作性，RMON2 在监视器配置组中定义了远程配置监视器的标准化方法。由一些标题对象和 4 个表组成。4 个表是串行配置表、网络配置表;陷入定义表和串行连接表。