网络管理配置

目 录

第 1 章　网络管理配置

1.1　配置SNMP

1.1.1　概述

SNMP 系统包括下面 3 个部分：

- SNMP 管理端 (NMS)
- SNMP 代理 (AGENT)
- 管理信息库 （MIB）

SNMP 是应用层协议。它提供了在 SNMP 管理端和代理之间进行通信的报文格式。

SNMP 管理端可以是网络管理系统（NMS，如 CiscoWorks）的一部分。代理和 MIB 驻留在系统上。配置系统上的 SNMP，需要定义管理端和代理间的关系。

SNMP 代理包含 MIB 变量，SNMP 管理端可以查询或改变这些变量的值。管理端可以从代理处得到变量值，或者把变量值存储到代理处。代理从 MIB 收集数据。MIB 是设备参数和网络数据的信息库。代理也能响应管理端的读取或设置数据的请求。SNMP 代理可以主动向管理端发送陷阱（trap）。陷阱是针对网络的某一条件而向 SNMP 管理端报警的消息。陷阱能指出不正确的用户认证、重启、链路状态（启动或关闭）、TCP 连接的关闭、与邻近系统连接的丢失或其它重要的事件。

1. SNMP 通告

特殊事件发生时系统能向 SNMP 管理端发送通知(inform)。例如，当代理系统遭遇一个错误条件时，它可能向管理端发送一个消息。

SNMP 通告可以作为陷阱（trap）或通知请求（inform request）来发送。由于接收方收到一个陷阱时不发送任何应答，导致发送方不能确定是否陷阱已经被接收，所以陷阱不可靠。与此相对的是，接收通知请求的 SNMP 管理端用 SNMP 响应 PDU 作为这个消息的应答。如果管理端没有收到一个通知请求，也不会发送响应。如果发送方没有收到应答，那么可以重新发送通知请求。这样，通告更可能到达它们计划中的目的地。

因为通知请求更加可靠，所以它们消耗了系统和网络的更多的资源。陷阱只要一发出便被丢弃。与此不同的是，通知请求必须保留在内存中，直到收到响应或者请求超时。另外，陷阱只发送一次，而通知请求可以重新发送多次。重新发送增加了网络通信量并在网络上产生更多的负荷。因此，陷阱和通知请求在可靠性和资源间提供了平衡。如果 SNMP 管理端非常需要收到每个通知，可使用通知请求；如果关心网络的通信量或系统的内存，并且不必收到每个通知，可使用陷阱。

本公司系统目前支持陷阱，但提供了对通知请求的扩充。

2. SNMP 的版本

本公司系统现支持下面的 SNMP 版本：

- SNMPv1---简单网络管理协议，一个完全的 Internet 标准，在 RFC1157 中定义。
- SNMPv2C--- SNMPv2 的基于团体的管理框架，Internet 试验协议，在 RFC1901 中定义。

本公司三层交换机还支持下面版本的 SNMP：

- SNMPv3--- 简单网络管理协议版本 3，在 RFC3410 中定义。

SNMPv1 使用基于团体的安全形式。能访问代理 MIB 的管理端团体用 IP 地址访问控制列表和口令来定义。

SNMPv3 通过对 SNMP 报文进行认证和加密操作来提供对设备访问的安全性。

SNMPv3 提供了下列安全特性：

- 消息完整性：保证消息在传输过程中没有被篡改
- 认证：确保消息的来源地的合法性
- 加密：对消息题进行加密，未经认证的主机即使窃取到消息也无法解密阅读

SNMPv3 提供安全模型和安全级别。安全模型是指一种认证策略，通过配置用户名和该用户所属的组来实现。安全级别是指安全模型中支持的不同的认证方式。SNMPv3 基于用户的安全模型支持三种安全级别，按照从高到低的顺序排列分别是认证并加密、认证不加密和不认证；通过使用 MD5 或 SHA 散列算法计算认证密钥的摘要值在网络间传送并在 SNMP 引擎比对来实现密码不被泄漏，使用 DES 加密算法对报文进行加密保证设备不被第三者窃听。通过配置用户/密码对和用户所属的组来实现管理者对设备的身份认证，通过配置组和视图决定组内的用户不同操作对于管理信息库的访问权限；组同时限制了组内用户的最低安全级别。

必须把 SNMP 代理配置为管理工作站支持的 SNMP 版本。代理能与多个管理端通信。

3. 所支持的 MIB

本公司系统的 SNMP 支持所有的 MIB II 变量（在 RFC 1213 中讲述）和 SNMP 陷阱（RFC 1215 中讲述）。

本公司系统为每个系统提供了自己私有的 MIB 扩充。

1.1.2 SNMP 配置任务

SNMP 配置任务有：

- 配置 SNMP 视图

- 为 SNMP 团体创建或修改访问控制
- 设置该系统管理员的联系方法和系统所在位置
- 定义 SNMP 代理数据包的最大长度
- 监视 SNMP 状态
- 配置 SNMP 本地引擎
- 配置 SNMP 陷阱
- SNMP 绑定源地址
- SNMP 配置侦听端口
- 配置 SNMPv3 组
- 配置 SNMPv3 用户
- 配置共同体密文显示
- 配置陷阱源地址
- 配置陷阱发送超时时间
- 配置陷阱绑定主机名称
- 配置将陷阱发送记录为 log
- 配置 snmp 饱和攻击防御
- 配置发送心跳 trap
- 配置设备网元编码
- 配置陷阱事件列表
- 配置 getbulk 请求的最大处理时间
- 配置 getbulk 请求的 cpu 间歇时间
- 显示 snmp 运行信息
- 显示 snmp 调试信息

1. 配置 SNMP 视图

SNMP 视图用于规定管理信息库的访问权限：允许访问和拒绝访问。使用下面的命令配置 SNMP 视图

命令	说明

snmp-server view *name oid* [**excluded** | **included**]	将oid指定的管理信息库叶子或表加入SNMP视图name中，并指定SNMP视图name中oid指定的对象标示符的访问权限，excluded为拒绝访问，included为允许访问

SNMP 视图中可以访问的子集为所有配置了允许访问的管理信息库的对象除去所有配置了拒绝访问的对象；未配置的对象默认权限为不可访问。

配置了 SNMP 视图后，可以将 SNMP 视图应用到 SNMP 团体名的配置中，用以限定该团体名的可访问对象的子集。

2. 为 SNMP 团体创建或修改访问控制

使用 SNMP 团体字符串定义 SNMP 管理端和代理的关系。团体字符串类似于允许访问系统上代理的口令。可选的是，可以指定下面一个或多个与团体字符串相关联的特性：

允许使用团体字符串获得代理访问权的 SNMP 管理端的 IP 地址访问列表。

定义对指定团体有访问权的所有 MIB 对象子集的 MIB 视图。

指定团体对有访问权的 MIB 对象的读写权限。

在全局配置模式下使用下面的命令来配置团体字符串：

命令	目的
snmp-server community [0|7] *string* [**view** *view-name*] [**ro | rw**] [*word*]	定义团体访问字符串。

可以配置一个或多个团体字符串。使用 no snmp-server community 命令除去给定的团体字符串。

关于配置团体字符串的示例，参见"SNMP 命令”一章。

3. 设置该系统管理员的联系方法和系统所在位置

sysContact 和 sysLocation 都是 MIB 中 system 组中的管理变量，分别定义了被管理该节点（系统）的联系人标识和实际位置。这些信息可以通过配置文件进行访问。在全局配置模式下使用下面的一个或多个命令：

命令	目的
snmp-server contact *text*	设置节点联系人字符串。
snmp-server location *text*	设置节点位置字符串。

4. 定义 SNMP 代理数据包的最大长度

当 SNMP 代理接收请求或发出响应时，可以设置数据包的最大许可长度。在全局配置模式下使用下面的命令：

命令	目的
snmp-server packetsize *byte-count*	设定数据包的最大许可长度。

5. 监视 SNMP 状态

在全局配置模式下使用下面的命令，监视 SNMP 输入和输出统计，包括非法团体字符串条目，错误和请求变量的数量。

命令	目的
show snmp	监视SNMP状态。

6. 配置 SNMP 本地引擎

在全局模式下使用下面命令，配置 SNMP 本地引擎。

命令	目的
snmp-server engineID local *engineID*	配置SNMP本地引擎

7. 配置 SNMP 陷阱

使用下面的命令配置系统发送 SNMP 陷阱（第二个任务是可选的）：

- 配置系统发送陷阱

  在全局配置模式下使用下面的命令配置系统向一个主机发送陷阱。

命令	目的
snmp-server host|hostv6 host community-string [trap-type]	指定陷阱消息的接收者。
snmp-server host|hostv6 *host* **[vrf** *word***] [udp-port** *port-num***] [permit|deny** *event-id***] {{version [v1 | v2c | v3]} | {[informs | traps] | [auth |noauth]}}** *community-string/user* **[authentication | configure| snmp]**	指定陷阱消息的接收者，以及陷阱信息的版本号和用户名等

  系统开机后，SNMP 代理自动启动，所有类型的陷阱被激活。使用 snmp-server host 命令指定哪个主机将要接收哪些类型的陷阱。

  有些陷阱需要通过其它命令来控制。例如，如果要在接口打开或关闭时会发送 SNMP 链路陷阱，需在接口配置模式下使用 snmp trap link-status 激活链路陷阱。使用接口配置命令 no snmp trap link-stat 关闭这些陷阱。

  为了使主机收到陷阱，必须为该主机配置 snmp-server host 命令。

- 改变陷阱运行参数

  作为可选项，可以指定产生陷阱的源接口，为每个主机指定消息（数据包）队列长度或重发间隔的值。

  在全局配置模式下使用下面可选命令改变陷阱运行参数：

命令	目的
snmp-server trap-source *interface*	指定产生陷阱消息的源接口。该命令为信息也设置源IP地址。
snmp-server queue-length *length*	为每个陷阱主机建立消息队列长度。 缺省为10。
snmp-server trap-timeout *seconds*	定义重发队列中重发陷阱消息的频率。 缺省为30秒。

8. SNMP 绑定源地址

在全局配置模式下使用下面的命令，设置 SNMP 报文的源地址功能。

命令	目的
snmp source-addr *ipaddress*	设置SNMP报文的源地址

9. snmp 配置侦听端口

在全局模式下使用下面命令，配置 snmp 代理的侦听端口号。

命令	目的
snmp-server udp-port *portnum*	设置SNMP代理的侦听端口号

10. 配置 SNMPv3 组

通过下面的命令配置组

命令	目的
snmp-server group [*groupname* { **v3** [**auth | noauth | priv**]}][**read** readview][**write** writeview] [**notify** notifyview] [**access** access-list]	配置一个SNMPv3组。默认情况下可以读internet子树下所有叶子，不可以写任何叶子。

11. 配置 SNMPv3 用户

通过下面的命令配置一个本地用户，管理者访问设备时，必须使用设备上配置的用户名和密码进行访问。用户的安全级别不能低于用户所属的组的安全级别，否则用户不能通过认证

命令	目的
snmp-server user *username groupname* **{v3 [encrypted|auth] [md5|sha]** *auth-password***}**	配置一个本地SNMPv3用户

12. 配置共同体密文显示

使用全局配置模式命令 **snmp-server encryption** 使已经配置的 snmp 共同体，SHA 加密密码和 MD5 加密密码密文显示， 该命令为一次性命令，不做保存，不可用 NO 命令取消。命令格式如下

命令	目的
snmp-server encryption	使snmp共同体，SHA加密密码和MD5加密密码密文显示。用于保证密码安全性

13. 配置陷阱源地址

使用全局配置模式命令 snmp-server trap-source 指定一个接口用于所有陷阱的源地址。使用该命令的 no 形式除去这样一个接口。

命令	目的
snmp-server trap-source *interface*	当从 SNMP 服务器发出 SNMP 陷阱时，无论当时在哪个接口发出，它都有一个的陷阱地址。如果想用该陷阱地址进行跟踪，可使用该命令。

14. 配置陷阱发送超时时间

使用全局配置模式命令 snmp-server trap-timeout 定义重发陷阱消息的超时值。

命令	目的
snmp-server trap-timeout *seconds*	在交换机软件试图发送陷阱之前，它查找到目标地址的路由。如果没有路由，陷阱存入重发队列中。命令 server trap-timeout 决定了重发的间隔。

15. 配置陷阱绑定主机名称

该设置用于 snmp 发送 trap 时在绑定变量中添加 hostname 信息

命令	目的
snmp-server trap-add-hostname	在特定的时候，网管主机需要定位 trap 来自哪个主机，这来命令可以起到很大的帮助。

16. 配置将陷阱发送记录为 log

设置设备把 trap 的发送记录记为 logs。

命令	目的
snmp-server trap-logs	启用 snmp trap 的发送 log 记录后，可以向 log

	服务器发送，设备的 trap 发送记录，可以增加对设备运行状态的了解

17. 配置 snmp 饱和攻击防御

设置开启 snmp 遭受不断尝试密码时的防护功能，设置 snmp sever 在五分钟内错误 commuity 登录的重复次数

命令	目的
snmp-server set-snmp-dos-max *retry times*	启用 snmp trap 的发送 log 记录后，可以向 log 服务器发送，设备的 trap 发送记录，可以增加对设备运行状态的了解

需要配合 snmp-server host 使用

18. 配置发送心跳 trap

使用全局配置模式命令 **snmp-server keep-alive** 配置设备定时的发送心跳 trap。时间间隔为 *times*

命令	目的
snmp-server keep-alive *times*	定期向指定 trap host 发送心跳 trap

19. 配置设备网元编码

使用全局配置模式命令 snmp-server necode 设置管理节点的信息（设备唯一标识符）。使用 no 形式除去设备标识信息。

命令	目的
snmp-server necode *text*	与 snmp 私有 MIB 变量的值对应。

20. 配置陷阱事件列表

使用全局配置模式命令 snmp-server event-id 创建和设置 event 列表，使用 no 命令删除

命令	目的
snmp-server event-id *number* **trap-oid** *oid*	在 host 配置中使用，用于发送 trap 时的过滤。

21. 配置 getbulk 请求的最大处理时间

使用全局配置模式命令 snmp-server getbulk-timeout 设置 getbulk 请求的最大处理时间，若超过此时间无法处理完成所有的 getbulk 请求，则直接返回现有结果。使用 no 命令删除。

命令	目的
snmp-server getbulk-timeout *seconds*	设置 getbulk 请求的最大处理时间，若超过此时间无法处理完成所有的 getbulk 请求，则直接返回现有结果。

22. 配置 getbulk 请求的 cpu 间歇时间

使用全局配置模式命令 snmp-server getbulk-delay 设置 snmp 代理在处理 getbulk 请求时，为防止 snmp 占用过多 cpu 设置 snmp 任务挂起的时间。单位为百分之一秒。使用 no 命令删除。

命令	目的
snmp-server getbulk-delay *ticks*	snmp 代理在处理 getbulk 请求时，为防止任务占用过多 cpu 设置 snmp 任务挂起时间，单位为百分之一秒。

23. 显示 snmp 运行信息

使用命令 **show snmp** 监视 SNMP 输入和输出统计，包括非法团体字符串条目，错误和请求变量的数量。使用命令 **show snmp engineID** 显示 SNMP 引擎信息。使用命令 **show snmp host** 显示 SNMP 陷阱主机信息。使用命令 **show snmp view** 显示 SNMP 视图信息。使用命令 **show snmp mibs** 显示 mib 注册信息。使用命令 **show snmp group** 显示 SNMP 组信息。使用命令 **show snmp user** 显示 SNMP 用户信息。

命令	目的
show snmp *engineID*	显示SNMP 引擎信息。
show snmp *host*	显示SNMP 陷阱主机信息。
show snmp *view*	显示SNMP视图信息。
show snmp *mibs*	显示SNMP MIB注册的信息。
show snmp *group*	显示SNMP组信息。
show snmp *user*	显示SNMP用户信息。

24. 显示 snmp 调试信息

显示 SNMP 事件、报文发送、接收过程和出错信息。

命令	目的
debug snmp *error*	打开SNMP出错信息的调试开关。
debug snmp *event*	打开SNMP事件的调试开关。
debug snmp *packet*	打开SNMP输入输出报文的调试开关。

1.1.3 配置实例

1. 例一

snmp-server community public RO
snmp-server community private RW
snmp-server host 192.168.10.2 public

在这个例子中配置了对所有 MIB 变量有读权限的团体字符串 public 与对所有 MIB 变量有读写权限的团体字符串 private。用户可以用团体字符串 public 读系统中 MIB 变量，用 private 读系统中的 MIB 变量与写系统中可写的 MIB 变量。它还指定了当系统需要发送陷阱消息时，用团体字符串 public 向 192.168.10.2 发送陷阱消息。例如当系统的某个端口 down 时，系统会向 192.168.10.2 发送一条 linkdown 的陷阱消息。

2. 例二

snmp-server group getter v3 auth
snmp-server group setter v3 priv write v-write
snmp-server user get-user getter v3 auth sha 12345678
snmp-server user set-user setter v3 encrypted auth md5 12345678
snmp-server view v-write internet included

使用 SNMPv3 对设备进行管理。组 getter 可以对设备信息进行浏览，组 setter 可以对设备进行设置操作。用户 get-user 属于组 getter，安全级别为认证不加密，口令为 12345678，时用 sha 算法进行口令摘要；用户 set-user 属于组 setter，安全级别为认证并加密，口令为 12345678，使用 md5 算法进行口令摘要。

1.2 配置RMON

1.2.1 RMON 配置任务

RMON 配置任务有：

- 配置交换机 rMon 告警功能
- 配置交换机 rMon 事件功能
- 配置交换机 rMon 统计功能
- 配置交换机 rMon 历史功能
- 显示交换机 rMon 配置

1. 配置交换机 rMon 告警功能

可以通过命令行或 SNMP 网管配置 rMon 告警功能；如果通过 SNMP 网管配置，还需要对交换机的 SNMP 进行配置。告警功能配置完成后，设备可以监控系统中某些统计值。配置 rMon 告警功能步骤如下：

命令	目的
config	进入全局配置模式。
rmon alarm index variable *interval* {**absolute** | **delta**} **rising-threshold** *value* [*eventnumber*] **falling-threshold** *value* [*eventnumber*] [**owner** *string*] **[repeat]**	增加一个rMon告警表项。 index为该表项的索引，有效范围1~65535 。 variable为被监测MIB中对象，必须是系统中一个有效的MIB对象，并且只有类型为INTEGER、Counter、Gauge或TimeTicks的对象才能被检测。 interval为取样的间隔时间，以秒为单位，有效范围1~2147483647。 使用absolute来直接监测MIB对象的取值；使用delta来监测两次取样之间MIB对象值的变化。 value用于表示产生告警的阈值，对应的eventnumber表示到达该阈值时产生的事件的索引；eventnumber是可选的。 owner string可以用来描述该告警的一些描述性信息。 repeat用来控制允许重复触发事件。
exit	退回到管理模式。
write	保存配置 。

配置完成一条告警表项后，设备会每隔 interval 秒获取 variable 指定的 oid 的值，并根据告警类型（absolute 或 delta）与前次值进行比较，如果本次统计值比前次大并且超出 rising-threshold 指定的阈值则会引发索引为 eventnumber 的事件（如果 eventnumber 为零或事件表不存在索引为 eventnumber 的事件则不引发），下降亦然；如果无法获取 variable 指定的 oid，则本行告警表项状态被设置为 invalid。当使用 rmon alarm 命令多次配置相同 index 的告警表项时，只有最后一次配置的参数有效；使用 no rmon alarm index 命令删除索引为 index 的告警表项。

2. 配置交换机 rMon 事件功能

配置 rMon 事件步骤如下：

步骤	命令	目的
1.	**config**	进入全局配置模式。
2.	**rmon event index** [**description** *string*] [**log**] [**owner** *string*] [**trap** community] [**ifctrl** *interface*]	增加一个rMon事件表项。 index为该表项的索引，有效范围1~65535 。 description表示该事件的描述信息 。

		log表示该事件被引发时在log表中增加一条信息 。 trap表示该事件被引发时产生一条trap，community为团体名称。 ifctrl interface配置事件控制关闭的端口。 owner string可以用来描述该事件的一些描述性信息。
3.	**exit**	退回到管理模式。
4.	**write**	保存配置 。

配置 rMon 事件后，当触发 rMon 告警时，首先更新本事件表项的 eventLastTimeSent 域为当时的 sysUpTime；如果该事件配置了 log 属性，则向 log 表中增加一条信息；如果配置了 trap 属性，则以 community 为团体名称发出一条 trap。当使用 rmon event 命令多次配置相同 index 的事件表项时，只有最后一次配置的参数有效；使用 no rmon event index 命令删除索引为 index 的事件表项。

3. 配置交换机 rMon 统计功能

rMon 统计组用于监测设备上每一个接口上的统计信息。rMon 统计功能配置步骤如下：

步骤	命令	目的
1.	**config**	进入全局配置模式。
2.	**interface iftype ifid**	进入端口模式。 iftype为端口的类型 。 ifid为接口的id。
3.	**rmon collection stats index** [**owner** *string*]	在该接口上使能统计功能。 index为统计表项索引 。 owner string可以用来描述该统计表的一些描述性信息。
4.	**exit**	退回到全局模式 。
5.	**exit**	退回到管理模式 。
6.	**write**	保存配置 。

当使用 rmon collection stats 命令多次配置相同 index 的事件表项时，只有最后一次配置的参数有效；使用 no rmon collection stats index 命令删除索引为 index 的统计表项。

4. 配置交换机 RMON 历史功能

RMON 历史组用于收集设备上一个接口上的不同时间段的统计信息。rMon 统计功能配置步骤如下：

步骤	命令	目的
1.	**config**	进入全局配置模式

2.	**interface** iftype ifid	进入端口模式 iftype为端口的类型 ifid为接口的id
3.	**rmon collection history index** [buckets bucket-number] [interval second] [owner owner-name]	在该接口上使能历史功能 index为该历史表项索引 在所有该历史记录控制表项收集的数据中，最近bucket-number条表项需要保留，用户可以浏览以太网历史记录表获取这些统计值；默认值为50条 second为每两次获取统计数据的间隔时间，默认值为1800秒（半小时） owner string可以用来描述该历史控制表的一些描述性信息
4.	**exit**	退回到全局模式
5.	**exit**	退回到管理模式
6.	**write**	保存配置

增加一个历史控制表项后，设备会每隔 second 秒从指定的接口上获取一次统计值，将结果作为表项增加到以太网历史记录表中。当使用 rmon collection history index 命令多次配置相同 index 的历史表项时，只有最后一次配置的参数有效；使用 no rmon history index 命令删除索引为 index 的历史控制表项。注意 bucket-number 过大和 interval second 过小都会过多占用系统资源。

5. 显示交换机 RMON 配置

使用 show 命令显示交换机 RMON 配置。

命令	目的
show rmon [alarm] [event] [statistics] [history]	显示rmon配置信息 alarm表示显示告警表项配置 event表示显示事件表项配置，同时显示由于事件被引发而导致log表中包含的表项 statistics表示显示统计表项配置，同时显示设备收集到的该接口上的统计值 history表示显示历史表项配置，同时显示设备收集到的该接口上最近指定个数时间间隔内的统计值