JXNET 甲信

甲信三层以太网交换机 SNMP 技术配置手册

配置指南(CLI)

(Rel_01)

北京甲信技术有限公司（以下简称“甲信”）为客户提供全方位的技术支持和服务。直接向甲信购买产品的用户，如果在使用过程中有任何问题，可与甲信各地办事处或用户服务中心联系，也可直接与公司总部联系。

读者如有任何关于甲信产品的问题，或者有意进一步了解公司其他相关产品，可通过下列方式与我们联系：

公司网址：　　www.jiaxinnet.com.cn

技术支持邮箱：　jxhelp@bjjx.cc

技术支持热线：　400-179-1180

公司总部地址：　北京市海淀区丹棱 SOHO 7 层 728 室

邮政编码:　　100080

声　明

目录

1.1 SNMP

1.1.1 简介

SNMP（Simple Network Management Protocol，简单网络管理协议）是由IETF（Internet Engineering Task Force，互联网工程任务组）为了解决Internet 中网络设备的管理问题而提出的一套网络管理协议。SNMP 可以使一个网管系统远程管理所有支持这种协议的网络设备，包括监视网络状态、修改网络设备配置、接收网络事件告警等。它是目前 TCP/IP 网络中应用最广泛的网络管理协议。

工作机制

SNMP 的结构分为代理 Agent 和网管系统两部分。代理和网管系统之间是通过 UDP 传送 SNMP 报文进行通信。SNMP 工作机制如图 10-1。

图 1-1 SNMP 工作机制示意图

甲信 NView NNM 网管系统能够提供友好的人机交互界面，方便网络管理员完成网络管理工作，主要可以实现以下功能：

- 向被管设备发送请求报文。
- 接收来自被管设备的响应报文和 Trap 报文，并显示结果。

代理是驻留在被管设备上的一个进程，主要实现以下功能：

- 接收、响应来自 NView NNM 网管系统的请求报文。
- 根据报文类型，对其进行读或写操作，并生成响应报文，返回给 NView NNM 网管系统。
- 根据各协议模块对触发条件进行定义，在达到触发条件后进入系统、退出系统、设备重新启动等，响应的模块通过代理向 NView NNM 网管系统发送 Trap 报文，报告设备的当前状态。

说明

代理可以同时配置多个版本，采用不同的版本与不同的网管系统交互。但是当代理和某个网管系统通信时，代理和该网管系统上的 SNMP 版本配置必须相同，才能正确互通。

协议版本

目前，SNMP 协议共有 v1、v2c 和 v3 三个版本。

- SNMPv1 采用共同体名（Community Name）认证机制。共同体名用来定义 SNMP 网管系统和 SNMP 代理之间的关系，起到了类似于密码的作用，用来限制 SNMP 网管系统对 SNMP 代理的访问。如果 SNMP 报文携带的共同体名在设备上没有认证通过，该报文将被丢弃。
- SNMPv2c 也采用共同体名认证机制。它在兼容 SNMP v1 的同时又扩充了 SNMP v1 的功能：支持更多的操作类型、数据类型和错误代码、能够更细致地区分错误。
- SNMPv3 采用了 USM（User-Based Security Model，基于用户的安全模型）和 VACM（View-based Access Control Model，基于视图的访问控制模型）安全机制。用户可以设置认证和加密功能，通过有无认证和有无加密等功能组合，可以为 SNMP 网管系统和 SNMP 代理之间的通信提供更高的安全性。认证用于验证报文发送方的合法性，避免非法用户的访问；加密则是对网管系统和代理之间的传输报文进行加密，以免被窃听。

设备同时支持 SNMP 的 v1、v2c、v3 三个版本。

MIB

MIB（Management Information Base，管理信息库）是网管系统能够管理的所有的对象的集合。它定义了被管理对象的一些属性：

- 名字
- 访问权限
- 数据类型

通过对这些数据项目的存取访问，就可以得到与设备相关的统计内容。每个代理都有自己的 MIB。MIB 可以看成是网管系统和代理之间的一个接口，通过这个接口，网管系统可以对代理中的每一个被管对象进行读/写操作，从而达到管理和监控设备的目的。

MIB 采用树形结构进行存储，它的根在最上面，没有名字。树的节点表示被管理对象，它可以从根开始的一条路径唯一地识别（OID）。SNMP 协议报文通过遍历 MIB 树形目录中的节点来访问网络中的设备。

设备支持标准的 MIB 库和甲信自定义的 MIB 库。

1.1.2 配置准备

场景

当用户需要通过网管系统登录交换机设备时，应首先对设备配置 SNMP 基本功能。

前提

在配置 SNMP 之前，需完成以下任务：

- 配置路由协议，使设备和网管系统之间路由可达。

1.1.3 SNMP 的缺省配置

设备上 SNMP 的缺省配置如下。

功能	缺省值
SNMP 服务	缺省关闭，需要手动配置开启
SNMP 视图	缺省存在：internet 视图
SNMP 共同体	缺省存在：public、private 共同体
SNMP 访问组	缺省不存在
SNMP 用户	缺省不存在
SNMP 用户和访问组的映射关系	无
网管人员的标识和联系方法	support@JX.com
设备放置的物理位置	World China JX
Trap 状态	使能
SNMP 目标主机地址	无
SNMP 引擎 ID	800022B603000000111233

1.1.4 配置 SNMP v1/v2c 基本功能

SNMP Agent 为了保护自身及其管理的 MIB 不被非法访问，提出了共同体的概念。在某一个共同体内的管理站必须在所有对 Agent 的操作中使用该共同体的名字，否则其请求不被受理。

共同体名是用不同的字符串来标识不同的 SNMP 团体。不同的共同体可以具有只读（read-only）或读写（read-write）访问权限。具有只读权限的团体只能对设备信息进行查询，具有读写权限的团体除了可以对设备信息进行查询之外还可以对设备进行配置。

SNMP v1/v2c 采用共同体名认证方案，与设备认可的共同体名不符合的 SNMP 报文将被丢弃。

请在设备上进行以下配置。

步骤	配置	说明
1	`JX#configure`	进入全局配置模式。
2	`JX(config)#snmp server start`	启动 SNMP 服务端功能。

步骤	配置	说明
3	JX(config)#**snmp mib-view** *view-name* { **included** | **excluded** } *oid-tree* [**mask** *subtree-mask*]	创建SNMP视图，并配置访问的MIB变量范围。 缺省视图是 internet，范围包括 MIB 树中“1.3.6”节点以下的所有 MIB 变量。
4	JX(config)#**snmp community** { **read** | **write** } { **cipher** | **plain** } *community-name* [**mib-view** *view-name* |**acl-ipv4** *acl-ipv4-number* |**acl-ipv6** acl-ipv6-number]*	创建共同体名并配置对应的视图和访问权限。 如果没有填写 **mib-view** *view-name* 选项，则采用缺省视图 internet。

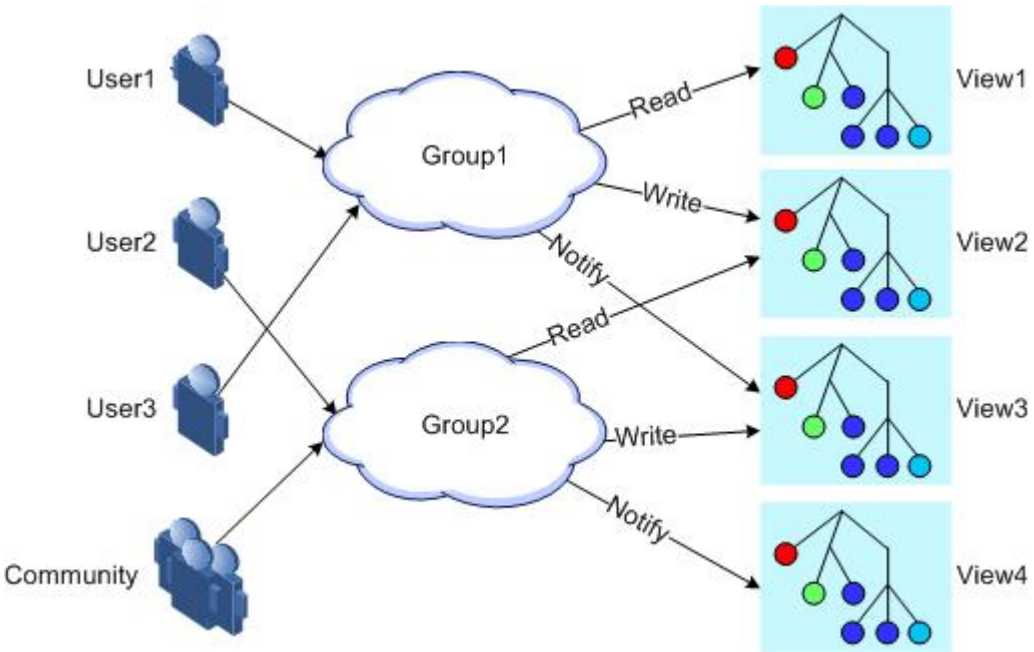
1.1.5 配置 SNMP v3 基本功能

SNMPV3 采用 USM 基于用户的认证机制。USM 提出了访问组（Group）的概念：一个或多个用户对应于一个访问组，每个访问组设定相应的读、写、通告视图，访问组中的用户拥有在该视图内的权限。发送 Get 和 Set 等请求的用户所在的访问组必须具有和其请求相应的权限，否则请求不被受理。

如图 10-2 所示，网管站采用 SNMP v3 对交换机正常的访问，需要进行的配置如下：

- 配置用户
- 确定用户属于哪个访问组
- 配置访问组拥有的视图权限
- 创建视图

图 1-2 SNMP v3 认证机制示意图



请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**snmp mib-view** *view-name* { **included** | **excluded** } *oid-tree* [**mask** *subtree-mask*]	创建 SNMP 视图，并配置访问的 MIB 变量范围。 缺省视图是 internet，范围包括 MIB 树中“1.3.6”节点以下的所有 MIB 变量。
3	JX(config)#**snmp group** *group-name* { **authentication** | **privacy** | **noauthentication** } [**read-view** *read-view-name* | **write-view** *write-view-name* | **notify-view** *notify-view-name*]*	配置访问组相关。
4	JX(config)#**snmp user** *user-name* **group** *group-name* **authentication** { **md5** | **sha** } *authpassword* **privacy** { **des** | **aes** } *privkeypassword*	创建用户并绑定组，并配置认证和加密。
5	JX(config)#**snmp user** *user-name* **group** *group-name* **authentication** { **md5** | **sha** } *authpassword*	创建用户并绑定组，并配置认证方式。
6	JX(config)#**snmp user** *user-name* **group** *group-name* [**acl-ipv4** *acl-ipv4-number* | **acl-ipv6** *acl-ipv6-number*]*	创建用户并绑定访问组。

1.1.6 配置 SNMP 其他信息

SNMP v1、v2c、v3 均支持以下信息的配置。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**snmp contact** *string*	配置联系方法。
3	JX(config)#**snmp location** *location-string*	配置设备当前所在地址信息。
4	JX(config)#**snmp auth-fail-reply** { **enable** | **disable** }	配置在认证失败时是否发送 SNMP 响应报文。
5	JX(config)#**snmp auth-trap** { **enable** | **disable** }	配置是否使能认证 Trap。
6	JX(config)#**snmp auth-fail-count** *fail-count-value*	配置 SNMP 认证失败次数。
7	JX(config)#**snmp reauth-interval** *reauth-interval-value*	配置 SNMP 重认证时间。
8	JX(config)#**snmp packet max-size** { *size-value*|**default** }	配置 SNMP 收发包最大长度。

步骤	配置	说明
9	JX(config)#**snmp reply-source-ip { enable | disable }**	配置将所输入的 IP 地址作为应答报文的源地址
10	JX(config)#**snmp udp-port** { *port-number* | **default** }	配置 SNMP 服务端口号。

1.1.7 配置 Trap

说明

SNMP v1、v2c 和 v3 的 Trap 配置步骤除了目标主机的配置，其余都是一样的，请根据需要进行选择。

Trap 是设备主动向网管系统发送的未经请求的信息，用于报告一些紧急的重要事件。

在配置 Trap 功能之前，需完成以下任务：

- 配置 SNMP 的基本功能。如果使用 SNMP v1 和 v2c 版本需要配置共同体名；如果使用 SNMP v3 版本需要配置用户名和 SNMP 视图。
- 配置路由协议，使设备和网管系统之间路由可达。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**snmp server { start | stop }**	启动 SNMP 服务端功能。
3	JX(config)#**snmp trap-host** *ip-address* **{ v1 | v2 } [port** *port-id* **| securityname** *security-name* **| vpn-instance** *vpn-name* **]***	配置基于 SNMP v1 和 SNMP v2c 的 Trap 目标主机(IPV4)。
4	JX(config)#**snmp-ipv6 trap-host** *ipv6-address* **{ v1 | v2 } [port** *port-id* **| securityname** *security-name* **| vpn-instance** *vpn-name* **]***	配置基于 SNMP v1 和 SNMP v2c 的 Trap 目标主机(IPV6)。
5	JX(config)#**snmp trap-host** *ip-address* **v3 { authentication | privacy } securityname** *security-name* **[port** *port-id* **| vpn-instance** *vpn-name* **]**	配置基于 SNMP v3 的 Trap 目标主机(IPV4)。
6	JX(config)#**snmp-ipv6 trap-host** *ipv6-address* **v3 { authentication | privacy } securityname** *security-name* **[port** *port-id* **| vpn-instance** *vpn-name* **]***	配置基于 SNMP v3 的 Trap 目标主机IPV6)。

1.1.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

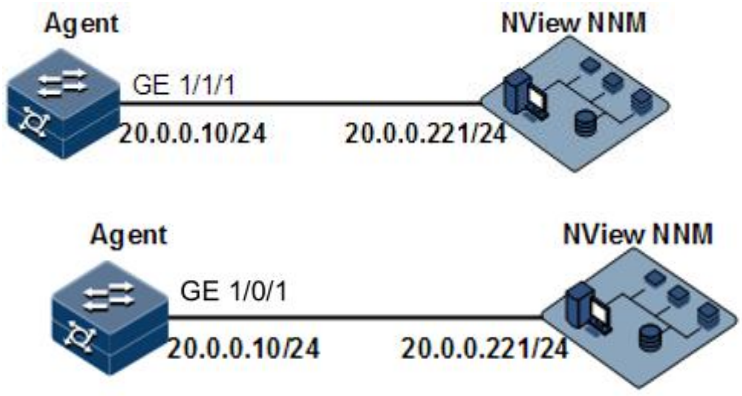
序号	检查项	说明
1	JX#show snmp information	查看 SNMP 全局的信息。 包含本地 SNMP 引擎 ID，网管人员的标识及联系方法，设备所在位置，Trap 开关状态信息，SNMP 服务开启状态，服务端口号。
2	JX#show snmp group	查看 SNMP 访问组的信息。
3	JX#show snmp community	查看 SNMP 共同体的配置信息。
4	JX#show snmp config	查看 SNMP 的基本配置信息。
5	JX#show snmp trap-host	查看 Trap 目标主机信息。
6	JX#show snmp statistics	查看 SNMP 的统计信息。
7	JX#show snmp user	查看 SNMP 用户信息。
8	JX#show snmp mib-view	查看 SNMP 的视图信息。

1.1.9 配置 SNMP v1/v2c 和 Trap 示例

组网需求

如图 10-3 所示，NView NNM 网管系统与交换机设备之间路由可达，NView NNM 通过 SNMP v1/v2c 可以查看远程交换机的对应视图下的 MIB，交换机出现紧急情况时可以主动向 NView NNM 发送 Trap。

图 1-3 SNMP v1/v2c 组网示意图



配置步骤

步骤 1 配置交换机设备的 IP 地址。

```
JX#config
JX(config)#interface meth 0/0/0
JX(config-meth-0/0/0)#ip address 192.168.62.100/24
JX(config-meth-0/0/0)#quit
```

步骤 2 启动 SNMP 服务端功能。

```
JX(config)#snmp server start
```

步骤 3 配置 Trap 告警。

```
JX(config)#snmp trap-host 192.168.62.1 v2
```

检查结果

通过 **show ip interface** 查看 IP 地址配置是否正确。

```
JX#show ip interface
Total number: 2
 Interface         State(a/o) Addr/Prefix       Role     Type
Vpn-instance
------------------------------------------------------------
--------------------------------------
 loopback-0        up/up     127.0.0.1/8       primary   auto
N/A
 meth-0/0/0        up/up     192.168.62.100/24  primary
static    N/A
------------------------------------------------------------
--------------------------------------
```

通过 **show snmp config** 查看 SNMP 配置是否正确。

```
JX#show snmp config
Software Version: SNMP_VL3.00.00.00
!
snmp server start
snmp trap-host 192.168.62.1 securityname
AJ35Grrnpx3xRv_UdbJBiGsl3Dwxp932il5pfsKvs8X-GN6R49ihEydRaxBXk
M5V-w
```

通过 **show snmp trap-host** 查看目标主机配置是否正确。

```
JX#show snmp trap-host
Trap-host : 192.168.62.1
------------------------------------------------------------
------------------
Status             : ACTIVE
Udp Port           : 162
MP Modle           : V2
Security Level      : None
Security Name       :
AJ35Grrnpx3xRv_UdbJBiGsl3Dwxp932il5pfsKvs8X-GN6R49ihEydRaxBXk
M5V-w
Vpn Instance Name    : public
------------------------------------------------------------
------------------
```

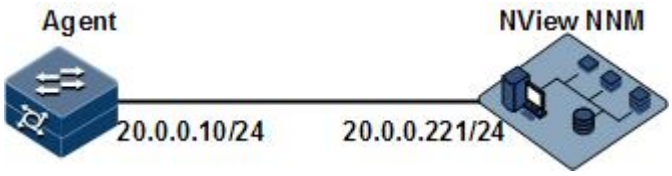
1.1.10 配置 SNMP v3 和 Trap 示例

组网需求

如图 10-4 所示，NView NNM 网管系统与 Agent 之间有可达路由，NView NNM 通过 SNMP v3 对 Agent 进行监控，Agent 出现紧急情况时可以主动向 NView NNM 发送 Trap。

缺省情况下，交换机设备上存在 VLAN 1，所有物理接口属于 VLAN 1。

图 1-4 SNMP v3 和 Trap 组网示意图



配置步骤

步骤 1 配置交换机设备的 IP 地址。

```
JX#config
JX(config)#interface meth 0/0/0
JX(config-meth-0/0/0)#ip address 192.168.62.100/24
JX(config-meth-0/0/0)#quit
```

步骤 2 配置 SNMP v3 访问。

启动 SNMP 服务端功能。

```
JX(config)#snmp server start
```

创建 g1 的访问组，安全等级为认证但不加密。

```
JX(config)#snmp group g1 authentication
```

创建用户 u1 为认证但不加密，绑定访问组 g1，采用 md5 鉴别算法，口令为 JX。

```
JX(config)#snmp user u1 group g1 authentication md5 JX
```

步骤 3 配置 Trap 告警，配置的 trap-host 类型必须与 user 的认证类型一致，不存在包含关系。

```
JX(config)#snmp trap-host 192.168.62.1 v3 authentication
securityname u1
```

检查结果

通过 **show snmp group** 查看 SNMP 访问组信息配置是否正确。

```
JX#show snmp group
Group                          Security     ReadView
WriteView                       NotifyView
```

```
------------------------------------------------------------
------------------------------------------------------------
---
g1                            authNoPriv    internet
-                             -
------------------------------------------------------------
------------------------------------------------------------
---
```

通过 **show snmp user** 查看用户和访问组的映射关系配置是否正确。

```
JX#show snmp user
User                          Group                          Auth
Priv    Filter
------------------------------------------------------------
--------------------------------------
u1                            g1                             MD5
no-priv  N/A
------------------------------------------------------------
--------------------------------------
```

通过 **show snmp trap-host** 查看 Trap 目标主机配置是否正确。

```
JX#show snmp trap-host
Trap-host : 192.168.62.1
------------------------------------------------------------
-------------------
Status             : ACTIVE
Udp Port           : 162
MP Modle           : V3
Security Level      : Auth
Security Name       : u1
Vpn Instance Name    : public
------------------------------------------------------------
-------------------
```

通过 **show snmp config** 查看所有配置信息是否正确。

```
JX#show snmp config
Software Version: SNMP_VL3.00.00.00
!
snmp server start
snmp trap-host 192.168.62.1 v3 authentication securityname u1
snmp group g1 authentication
snmp user u1 group g1 authentication md5
ACs87nMCx4RbzvvPS5lo3zDtbzu5xyzSZaDGmHOuqsc0
```