

目 录

第 1 章 交换机管理	1-1
1.1 管理方式	1-1
1.1.1 带外管理	1-1
1.1.2 带内管理	1-5
1.2 CLI 界面	1-10
1.2.1 配置模式介绍	1-10
1.2.2 配置语法	1-13
1.2.3 支持快捷键	1-13
1.2.4 帮助功能	1-13
1.2.5 对输入的检查	1-14
1.2.6 支持不完全匹配	1-14
第 2 章 交换机基本配置	2-1
2.1 基本配置	2-1
2.2 远程管理	2-2
2.2.1 Telnet	2-2
2.2.2 SSH	2-4
2.3 配置交换机的 IP 地址	2-5
2.3.1 配置交换机的 IP 地址任务序列	2-6
2.4 SNMP 配置	2-7
2.4.1 SNMP 介绍	2-7
2.4.2 MIB 介绍	2-8
2.4.3 RMON 介绍	2-9
2.4.4 SNMP 配置	2-9
2.4.5 SNMP 典型配置举例	2-12
2.4.6 SNMP 排错帮助	2-14
2.5 交换机升级	2-14
2.5.1 交换机系统文件	2-14
2.5.2 BootROM 模式升级	2-15
2.5.3 FTP/TFTP 升级	2-17
第 3 章 文件系统操作	3-1
3.1 文件存储设备介绍	3-1

3.2 文件系统操作任务配置序列.....	3-1
3.3 典型应用	3-2
3.4 排错帮助	3-3
 第 4 章 集群网管配置.....	 4-1
4.1 集群网管介绍	4-1
4.2 集群网管基本配置	4-1
4.3 集群网管举例	4-4
4.4 集群网管排错帮助	4-5

第1章 交换机管理

1.1 管理方式

用户购买到交换机设备后，需要对交换机进行配置，从而实现对网络的管理。交换机为用户提供了两种管理方式：带外管理和带内管理。

1.1.1 带外管理

带外管理即通过 Console 进行管理，通常情况下，在首次配置交换机或者无法进行带内管理时，用户会使用带外管理方式。例如：用户希望通过远程 Telnet 来访问交换机时，必须首先通过 Console 给交换机配置一个 IP 地址。

用户用 Console 管理的步骤如下：

第一、搭建环境：

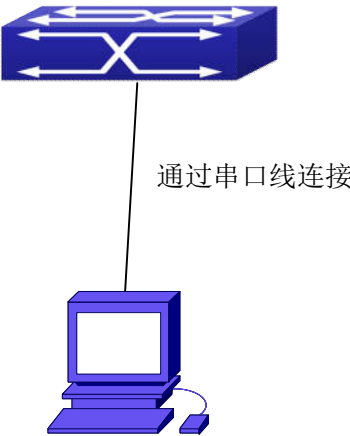


图 1-1 交换机 Console 管理配置环境

按照图 1-1 所示，将 PC 的串口（RS-232 接口）和交换机随机提供的串口线连接，下面是连接中用到的设备说明：

设备名称	说明
PC 机	有完好的键盘和 RS-232 串口，并且安装了终端仿真程序，如 Windows 系统自带超级终端等。
串口线	一端与 PC 机的 RS-232 串口相连；另一端与交换机的 Console 相连。
交换机	有完好的 Console。

第二、进入超级终端：

连接成功后，打开 Windows 系统自带超级终端。下面是打开 Windows XP 自带超级终端的示例。

1) 点击超级终端：

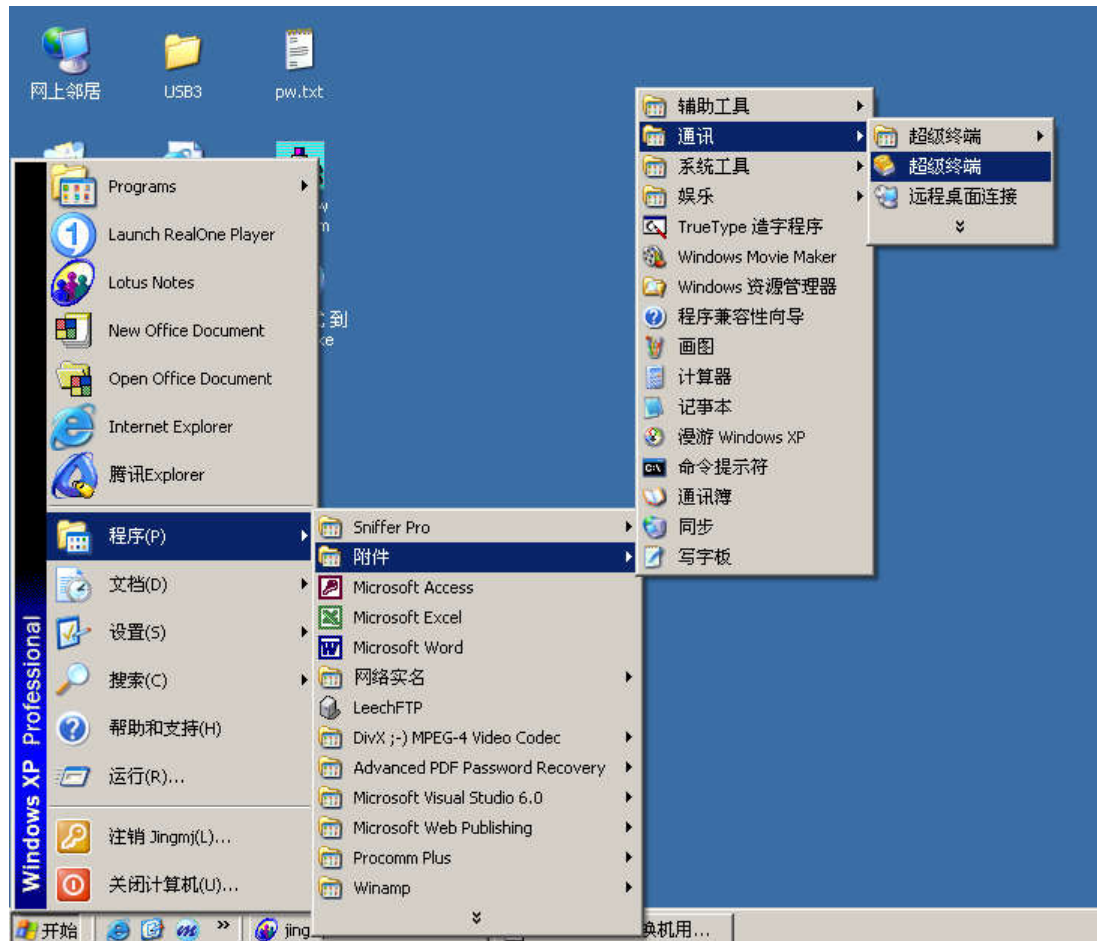


图 1-2 打开超级终端一

2) 在“名称”处填入打开超级终端的名称，例如把它定义为“Switch”：



图 1-3 打开超级终端二

3)在“连接时使用”处，选择PC机使用的RS-232串口，如连接的是串口1，则选择串口1，点击确定按钮：



图 1-4 打开超级终端三

4)出现COM1属性，波特率选择“115200”，数据位选择“8”，奇偶校验选择“无”，停止位选择“1”，数据流控制选择“无”；或者直接点击“还原默认值”后，点击确定按钮：

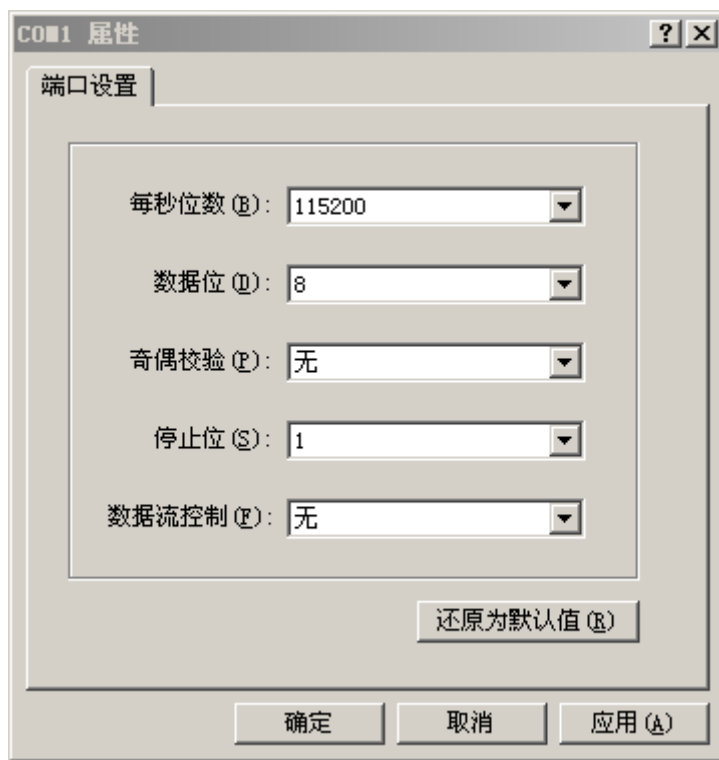


图 1-5 打开超级终端四

5) 出现超级终端的配置界面:

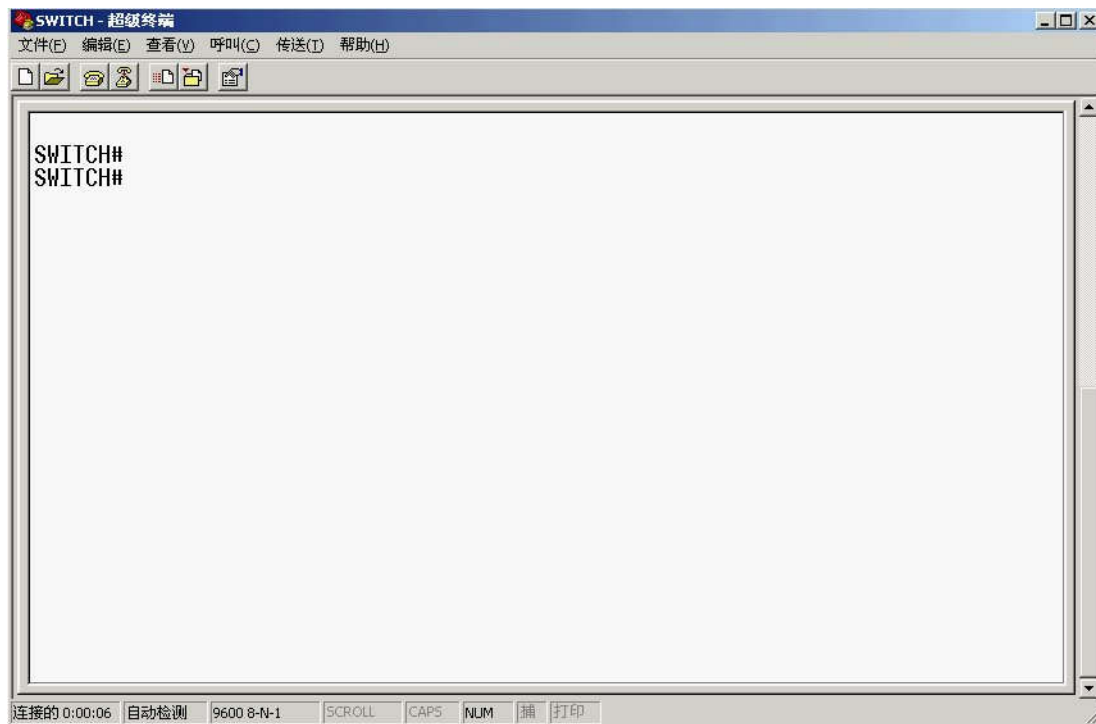


图 1-6 打开超级终端五

第三、进入交换机 CLI 界面：

打开交换机的电源开关。在超级终端的配置界面上出现了如下提示，进入到交换机的 CLI 配置方式：

```
switch>
```

接下来用户可以输入相关命令进行管理，命令详见具体章节。

1.1.2 带内管理

所谓带内管理（In-band management），包括通过 Telnet 程序登录到交换机，或者通过 HTTP 协议访问交换机，或者通过神州数码网络（北京）有限公司自主研发的 snmp 网管软件对交换机进行配置管理。交换机提供带内管理方式可以使连接到交换机中的某些设备具备管理交换机的功能。当交换机的配置出现变更，导致带内管理失效时，可以使用带外管理对交换机进行配置管理。

1.1.2.1 通过 Telnet 管理交换机

通过 Telnet 管理交换机要具备的条件：

- 1) 交换机配置 IPv4/IPv6 地址；
- 2) 作为 Telnet 客户端的主机 IP 地址与其所属交换机的 VLAN 接口的 IPv4/IPv6 地址在相同网段；
- 3) 若不满足 2)，则 Telnet 客户端可以通过路由器等设备到达交换机某个 IPv4/IPv6 地址。

本交换机是三层交换机，可以配置多个 IPv4/IPv6 地址，配置方法见配置交换机的 IP 地址相关章节。下面以交换机出厂时的情况举例，系统只有 VLAN1 存在。

以下是 Telnet 客户端 Telnet 到交换机的 VLAN1 接口的步骤（以 IPv4 地址为例）：

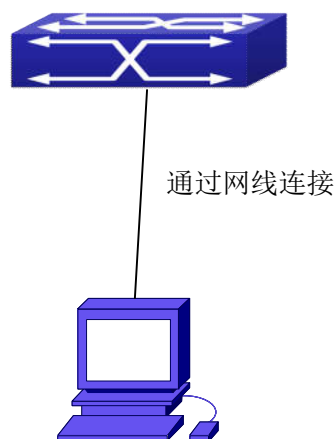


图 1-7 通过 Telnet 管理交换机

第一：配置交换机 IP 地址，并且启动交换机的 Telnet Server 功能。

首先配置主机的 IP 地址，要与交换机的 VLAN1 接口 IP 地址在同一个网段。如交换机的 VLAN1 接口 IP 地址为 10.1.128.251/24，则可以设置主机的 IP 地址为 10.1.128.252/24。在主机上执行“ping 10.1.128.251”命令，显示是否 ping 通；若 ping 不通，则检查原因。

下面简单介绍交换机 VLAN1 接口的 IP 地址配置命令，在进行带内管理之前，必须通过带外管理即 Console 方式配置交换机的 IP 地址，配置命令如下（以后如不特殊说明，所有的交换机配置时的提示符均采用 Switch）：

```
Switch>
```

```
Switch>enable
```

```
Switch#config
```

```
Switch(config)#interface vlan 1
```

```
Switch(Config-if-Vlan1)#ip address 10.1.128.251 255.255.255.0
```

```
Switch(Config-if-Vlan1)#no shutdown
```

然后在 Console 的全局配置模式下使用命令 **telnet-server enable** 启动 Telnet Server 功能。配置如下：

```
Switch>enable
```

```
Switch#config
```

```
Switch(config)# telnet-server enable
```

第二：运行 Telnet 客户端程序。

运行 Windows 自带的 Telnet 客户端程序，并且指定 Telnet 的目的地址。



图 1-8 运行 Windows 自带的 telnet 客户端程序

第三：登录交换机。

登录到 Telnet 的配置界面，需要输入正确的用户名和口令，否则交换机将拒绝该 Telnet 用户的访问。该项措施是为了保护交换机免受非授权用户的非法操作。若交换机没有设置授权 Telnet 用户，则任何用户都无法进入交换机的 Telnet 配置界面。因此在允许 Telnet 方式配置管理交换机时，必须在 Console 的全局配置模式下使用命令 **username <username> privilege <privilege> [password (0 | 7) <password>]** 为交换机设置 Telnet 授权用户和口令并使用命令 **authentication line vty login local** 打开本地验证方式，其中 privilege 选项必须存在且为 15。如交换机的授权用户名为 test，口令为明文的 test，设置方式如下：

```
Switch>enable
```

```
Switch#config
```

```
Switch(config)#username test privilege 15 password 0 test  
Switch(config)#authentication line vty login local
```

在 Telnet 配置界面上输入正确的用户名和口令，Telnet 用户就可成功的进入到交换机的 CLI 配置界面。Telnet 登录后与通过 Console 进入后使用的命令完全一致。

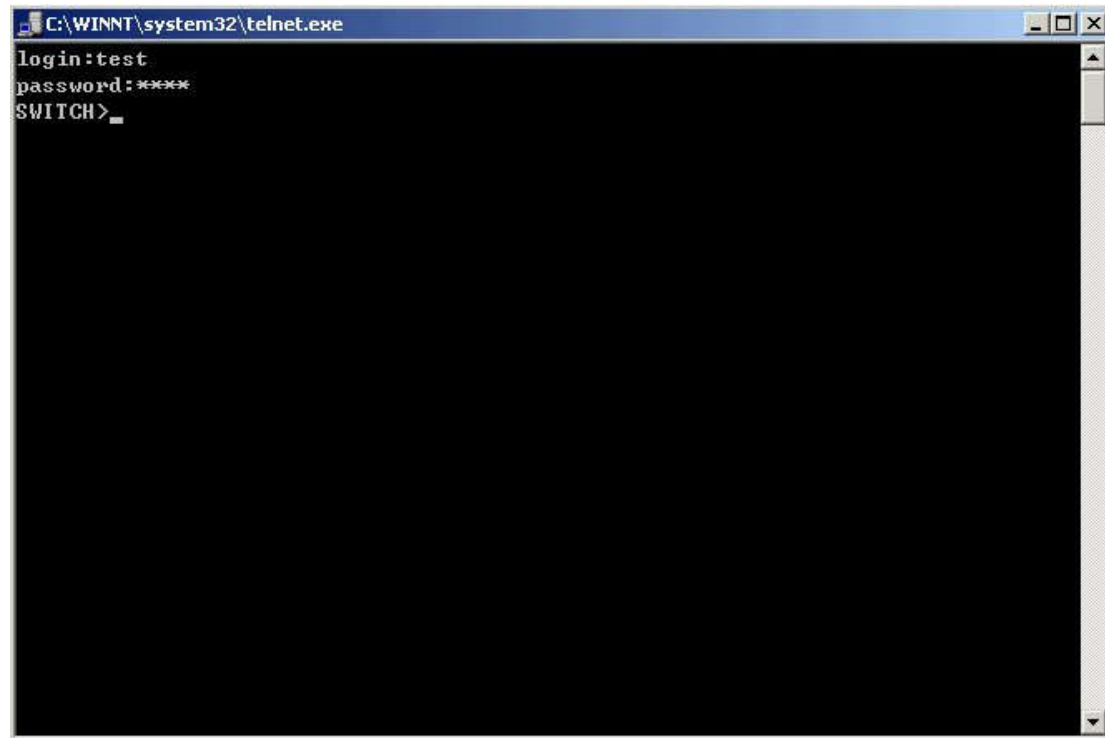


图 1-9 Telnet 配置界面

1.1.2.2 通过 HTTP 管理交换机

通过 HTTP 管理交换机要具备的条件：

- 1) 交换机配置 IPv4/IPv6 地址；
- 2) 作为客户端的主机 IPv4/IPv6 地址与其所属交换机的 VLAN 接口的 IPv4/IPv6 地址在相同网段；
- 3) 若不满足 2)，则客户端可以通过路由器等设备到达交换机某个 IPv4/IPv6 地址。

与 Telnet 用户登录交换机类似，只要主机能够 ping/ping6 通交换机的 IPv4/IPv6 地址，并且输入正确的登录口令，该主机就可通过 HTTP 访问交换机。步骤如下：

第一：配置交换机的 IP 地址，并且启动交换机的 HTTP Server 功能。

通过带外管理配置交换机 IP 地址，参见通过 telnet 管理交换机一节。

在 Console 的全局配置模式下使用命令 **ip http server** 启动 HTTP Server 功能，使能 Web 配置。配置如下：

```
Switch>enable  
Switch#config  
Switch(config)#ip http server
```

第二：在配置主机上运行 HTTP 协议。

在主机上运行 Web 浏览器，在地址栏处输入交换机的 IP 地址，或直接运行 Windows 的 HTTP 协议，比如交换机的 IP 地址为“10.1.128.251”；



图 1-10 执行 HTTP 协议

在使用 IPv6 地址访问交换机时，推荐使用浏览器 Firefox，版本在 1.5 以上，比如交换机的 IPv6 地址为 3ffe:506:1:2::3，在地址处输入交换机的 IPv6 地址 http://[3ffe:506:1:2::3]，地址需要用方括号括起来。

第三：Web 访问交换机。

登录到 Web 的配置界面，需要输入正确的用户名和口令，否则交换机将拒绝该 HTTP 访问。该项措施是为了保护交换机免受非授权用户的非法操作。若交换机没有设置授权 Web 用户，则任何用户都无法进入交换机的 Web 配置界面。因此在允许 Web 方式管理交换机时，必须在 Console 方式下的全局配置模式下使用命令 **username <username> privilege <privilege> [password (0 | 7) <password>]** 为交换机设置 Web 授权用户和口令并使用命令 **authentication line web login local** 打开本地验证方式，其中 privilege 选项必须存在且为 15。如交换机的授权用户名为 admin，口令为明文的 admin，设置方式如下：

```
Switch>enable
```

```
Switch#config
```

```
Switch(config)#username admin privilege 15 password 0 admin
```

```
Switch(config)#authentication line web login local
```

下面是 CS6200-28X-P-EI 的 Web 配置的登录界面：



图 1-11 Web 登录界面

输入正确的用户名和密码，进入交换机的 Web 配置主界面。

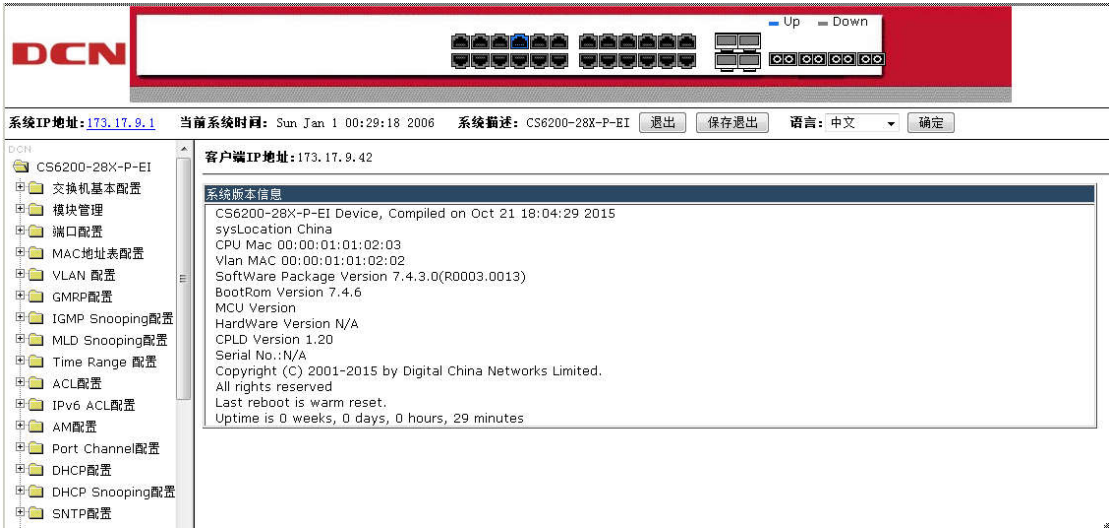


图 1-12 Web 配置界面

注意：通过 Web 配置交换机名称时，交换机名称由英文字母构成。

1.1.2.3 通过 snmp 网管软件管理交换机

通过 snmp 网管软件管理交换机要具备的条件：

- 1) 交换机配置 IP 地址；

- 2) 作为客户端的主机 IP 地址与其所属交换机的 VLAN 接口的 IP 地址在相同网段;
- 3) 若不满足 2), 则客户端可以通过路由器等设备到达交换机某个 IP 地址;
- 4) 开启了 snmp 功能。

安装 snmp 网管软件的主机必须能 ping 通交换机的 IP 地址, 这样在运行 Snmp 网管软件时, Snmp 网管软件就能找到交换机设备, 并且对其进行可读写的操作。具体如何通过 Snmp 网管软件管理交换机在本手册中不做介绍, 请参看《Snmp 网管软件用户手册》。

1.2 CLI 界面

交换机为用户提供了三种管理界面: CLI (Command Line Interface 命令行) 界面、Web 界面和 Snmp 网管软件。我们将对 CLI 界面做详细的介绍, Web 界面与 CLI 界面功能相似, 就略去不介绍了, Snmp 网管软件请参看《Snmp 网管软件用户手册》。

用户对 CLI 界面并不陌生, 前面我们提到的 Console 管理方式、Telnet 登录到交换机都是通过 CLI 界面对交换机进行配置管理的。

CLI 界面由 Shell 程序提供, 它是由一系列的配置命令组成的, 根据这些命令在配置管理交换机时所起的作用不同, Shell 将这些命令分类, 不同类别的命令对应着不同的配置模式。下面将介绍交换机的 Shell 的特点:

- ☞ 配置模式
- ☞ 配置语法
- ☞ 快捷键
- ☞ 帮助功能
- ☞ 对输入的检查
- ☞ 支持不完全匹配

1.2.1 配置模式介绍

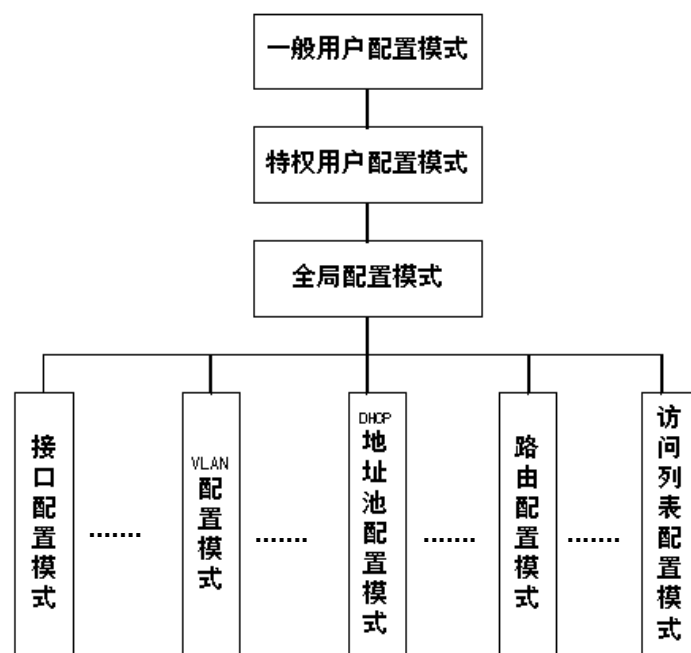


图 1-13 交换机的 Shell 配置模式

1.2.1.1 一般用户模式

用户进入 CLI 界面，首先进入的就是一般用户模式，提示符为“**Switch>**”，符号“>”为一般用户模式的提示符。当用户从特权用户模式使用命令 **exit** 退出时，可以回到一般用户模式。

1.2.1.2 特权用户模式

在一般用户模式使用 **enable** 命令，如果已经配置了进入特权用户的口令，则输入相应的特权用户口令，即可进入特权用户模式“**Switch#**”。当用户从全局配置模式使用 **exit** 退出时，也可以回到特权用户模式。另外交换机提供“**Ctrl+z**”的快捷键，使得交换机在任何配置模式（一般用户模式除外），都可以退回到特权用户模式。

在特权用户模式下，用户可以查询交换机配置信息、各个端口的连接情况、收发数据统计等。而且进入特权用户模式后，可以进入到全局模式对交换机的各项配置进行修改，因此进入特权用户模式后必须要设置特权用户口令，防止非特权用户的非法使用，对交换机配置进行恶意修改，造成不必要的损失。

1.2.1.3 全局配置模式

进入特权用户模式后，只需使用命令 **config**，即可进入全局配置模式“**Switch(config)#**”。当用户在其他配置模式，如接口配置模式、VLAN 配置模式时，可以使用命令 **exit** 退回到全局配置模式。

在全局配置模式，用户可以对交换机进行全局性的配置，如对 MAC 地址表、端口镜像、创建 VLAN、启动 IGMP Snooping、STP 等。用户在全局配置模式还可通过命令进入到接口配置模式对各个接口进行配置。

接口配置模式

在全局配置模式，使用命令 **interface** 就可以进入到相应的接口配置模式。交换机操作系统提供了三种端口类型：1.VLAN 接口；2.以太网端口；3.port-channel，因此就有三种接口的配置模式。

接口类型	进入方式	可执行操作	退出方式
VLAN 接口	在全局配置模式下，输入命令 interface vlan <Vlan-id> 。	配置交换机的 IP 等。	使用 exit 命令即可退回全局配置模式。
以太网端口	在全局配置模式下，输入命令 interface ethernet <interface-list> 。	配置交换机提供的以太网接口的双工模式、速率等。	使用 exit 命令即可退回全局配置模式。
port-channel	在全局配置模式下，输入命令 interface port-channel <port-channel-number> 。	配置 port-channel 有关的双工模式、速率等。	使用 exit 命令即可退回全局配置模式。

VLAN 配置模式

在全局配置模式，使用命令 **vlan <vlan-id>** 就可以进入到相应的 VLAN 配置模式。在 VLAN 配置模式，用户可以配置属于本 VLAN 的成员端口。执行 **exit** 命令即可从 VLAN 配置模式退回到全局配置模式。

DHCP 地址池配置模式

在全局配置模式下用 **ip dhcp pool <name>** 命令进入到 DHCP 地址池配置模式 “Switch(Config-<name>-dhcp)#”。在 DHCP 地址池配置模式下可以配置 DHCP 地址池的属性。执行 **exit** 命令即可从 DHCP 地址池配置模式退回到全局配置模式。

路由配置模式

路由协议类型	进入方式	可执行操作	退出方式
RIP 路由协议	在全局配置模式下输入 router rip 命令。	配置 RIP 协议参数。	执行 exit 命令即可退回全局配置模式。
OSPF 路由协议	在全局配置模式下输入 router ospf 命令。	配置 OSPF 协议参数。	执行 exit 命令即可退回全局配置模式。
BGP 路由协议	在全局配置模式下输入 router bgp <AS number> 命令。	配置 BGP 协议参数。	执行 exit 命令即可退回全局配置模式。

访问列表配置模式

访问列表类型	进入方式	可执行操作	退出方式
命名标准 IP 访问列表配置模式	在全局配置模式下输入 ip access-list standard 命令。	配置标准访问列表配置模式。	执行 exit 命令即可退回全局配置模式。
命名扩展 IP 访问列表配置模式	在全局配置模式下输入 ip access-list extended 命令。	配置扩展访问列表的参数。	执行 exit 命令即可退回全局配置模式。

置模式			式。
-----	--	--	----

1.2.2 配置语法

交换机为用户提供的配置命令形式不完全一样，但它们都遵循交换机配置命令的语法。以下是交换机提供的通用命令格式：

cmdtxt <variable> {enum1 | ... | enumN} [option1 | ... | optionN]

语法说明：黑体字 **cmdtxt** 表示命令关键字；**<variable>**表示参数为变量；**{enum1 | ... | enumN}**表示在参数集 **enum1~enumN** 中必须选一个参数；**[option1 | ... | optionN]**表示该参数可选择一个或者不选。在各种命令中还会出现“<>”，“{ }”，“[]”符号的组合使用，如：**[<variable>]**，**{enum1 <variable> | enum2}**，**[option1 [option2]]**等等。

下面是几种配置命令语法的具体分析：

- ☞ **show version**，没有任何参数，属于只有关键字没有参数的命令，直接输入命令即可；
- ☞ **vlan <vlan-id>**，输入关键字后，还需要输入相应的参数值；
- ☞ **firewall {enable | disable}**，此类命令用户可以输入 **firewall enable** 或者 **firewall disable**；
- ☞ **snmp-server community {ro | rw} <string>**，出现以下几种输入情况：
 snmp-server community ro <string>
 snmp-server community rw <string>

1.2.3 支持快捷键

交换机为方便用户的配置，特别提供了多个快捷键，如上、下、左、右键及删除键 **BackSpace** 等。如果超级终端不支持上下光标键的识别，可以使用 **ctrl+p** 和 **ctrl+n** 来替代。

按键	功能	
删除键 BackSpace	删除光标所在位置的前一个字符，光标前移	
上光标键“↑”	显示上一个输入命令。最多可显示最近输入的二十个命令	
下光标键“↓”	显示下一个输入命令。当使用上光标键回溯到以前输入的命令时，也可以使用下光标键退回到相对于前一个命令的下一个命令	
左光标键“←”	光标向左移动一个位置	左右键的配合使用， 可对已输入的命令做覆盖修改
右光标键“→”	光标向右移动一个位置	
Ctrl+p	相当于上光标键“↑”的作用	
Ctrl+n	相当于下光标键“↓”的作用	
Ctrl+b	相当于左光标键“←”的作用	
Ctrl+f	相当于右光标键“→”的作用	
Ctrl+z	从其他配置模式（一般用户配置模式除外）直接退回到特权用户模式	
Ctrl+c	打断交换机 ping 或其它正在执行的命令进程	
Tab 键	当输入的字符串可以无冲突的表示命令或关键字时，可以使用 Tab 键将其补充成完整的命令或关键字	

1.2.4 帮助功能

交换机为用户提供了两种方式获取帮助信息，其中一种方式为使用“**help**”命令，另一种

为“?”方式。

帮助	使用方法及功能
Help	在任一命令模式下，输入“help”命令均可获取有关帮助系统的简单描述。
“?”	1. 在任一命令模式下，输入“?”获取该命令模式下的所有命令及其简单描述； 2. 在命令的关键字后，输入以空格分隔的“?”，若该位置是参数，会输出该参数类型、范围等描述；若该位置是关键字，则列出关键字的集合及其简单描述；若输出“<cr>”，则此命令已输入完整，在该处键入回车即可； 3. 在字符串后紧接着输入“?”，会列出以该字符串开头的命令。

1.2.5 对输入的检查

1.2.5.1 成功返回信息

通过键盘输入的所有命令都要经过 Shell 的语法检查。当用户正确输入相应模式下的命令后，且命令执行成功，不会显示信息。

1.2.5.2 错误返回信息

当用户输入的命令错误，或者参数范围，类型，格式有错误，交换机会提示错误。

1.2.6 支持不完全匹配

交换机的 Shell 支持不完全匹配的搜索命令和关键字，当输入无冲突的命令或关键字时，Shell 就会正确解析。

例如：

- 1. 对特权用户配置命令“show interface ethernet 1/0/1”，只要输入“sh in e 1/0/1”即可。
- 2. 对特权用户配置命令 “show running-config”，如果仅输入“sh r”，系统会报“> Ambiguous command!”，因为 Shell 无法区分“show r”是“show radius”命令还是“show running-config”命令，因此必须输入“sh ru”，Shell 才会正确的解析。

第2章 交换机基本配置

2.1 基本配置

交换机的基本配置包括进入和退出特权用户模式的命令、进入和退出接口配置模式的命令、设置及显示交换机的时钟、显示交换机的系统版本信息等。

命令	解释
一般用户配置模式/特权用户配置模式	
enable [<1-15>] disable	用户使用 enable 命令，从一般用户配置模式进入特权用户配置模式或修改当前用户权限级别， disable 为退出特权用户模式命令。
特权用户配置模式	
config [terminal]	从特权用户配置模式进入到全局配置模式。
各种配置模式	
exit	从当前模式退出，进入上一个模式，如在全局配置模式使用本命令退回到特权用户配置模式，在特权用户配置模式使用本命令退回到一般用户配置模式等。
show privilege	显示当前用户权限。
一般用户配置模式和特权用户配置模式之外的其它模式	
end	当前处于非一般用户配置模式或特权用户配置模式时，使用该命令可以直接退回到特权用户配置模式。
特权用户配置模式	
clock set <HH:MM:SS> [YYYY.MM.DD]	设置系统日期和时钟。
show version	显示交换机版本信息。
set default	恢复交换机的出厂设置。
write	将当前运行时配置参数保存到 Flash Memory。
reload	热启动交换机。
show cpu usage	显示 CPU 使用率。
show cpu utilization	显示当前 CPU 的使用率。
force sync software-version	强制将软件版本从 Active Master 同步到 Standby

enable	Master，重启后生效
show memory usage	显示内存使用率。
全局配置模式	
banner motd <LINE> no banner motd	配置使用 telnet 或通过 console 等方式登陆交换机认证成功时显示的欢迎信息。
web-auth privilege <1-15> no web-auth privilege	设置 web 登录交换机的级别。

2.2 远程管理

2.2.1 Telnet

2.2.1.1 Telnet 简介

Telnet 远程登录是一个简单的远程终端协议。用户用 Telnet 就可在其所在地通告 TCP 连接注册（即登录）到远程的另一个主机上（使用 IP 地址或主机名）。Telnet 能把用户的击键传到远程的主机，同时也能把远程主机的输出通过 TCP 连接返回到用户屏幕。这种服务是透明的，因为用户的感觉是键盘和显示器是直接连接在远程主机上。

Telnet 使用客户—服务器模式，在本地的系统为 Telnet 客户端，远程主机为 Telnet 服务器。交换机既可以作为 Telnet 服务器也可以作为 Telnet 客户端。

当交换机作为 Telnet 服务器时，用户可以通过 Windows 或其他操作系统自带的 Telnet 客户端软件，Telnet 登录到交换机，就如前面介绍带内管理章节中介绍的一样。交换机作为 Telnet 服务器时最多可以同时与 5 个 Telnet 客户端建立 TCP 连接。

当作为 Telnet 客户端时，在交换机的特权用户配置模式下使用 telnet 命令即可登录到其他远端主机。交换机作为 Telnet 客户端时只能与一个远程主机建立 TCP 连接，如果想与另一个远程主机建立连接，则必须先断开与上一个远程主机的 TCP 连接。

2.2.1.2 Telnet 任务序列

1. 配置 Telnet 服务器
2. 交换机 Telnet 登录到远程主机

1. 配置 Telnet 服务器

命令	解释
全局配置模式	

telnet-server enable no telnet-server enable	打开交换机的 Telnet 服务器功能；本命令的 no 操作为关闭 Telnet 服务器功能。
username <username> [privilege <privilege>] [password [0 7] <password>] no username <username>	配置 Telnet 登录到交换机的本地用户名和口令；本命令的 no 操作为删除本地授权 Telnet 用户。本地 Telnet 用户的执行命令权限必须设为 15。
authentication securityip <ip-addr> no authentication securityip <ip-addr>	配置 Telnet 登录到交换机的安全 IP 地址；本命令的 no 操作为删除授权 Telnet 安全地址。
authentication securityipv6 <ipv6-addr> no authentication securityipv6 <ipv6-addr>	配置 Telnet 登录到交换机的安全 IPv6 地址；本命令的 no 操作为删除授权 Telnet 安全地址。
authentication ip access-class {<num-std> <name>} no authentication ip access-class	为 Telnet/SSH/Web 登录方式绑定标准的 IP ACL 规则；本命令的 no 操作为取消绑定 ACL。
authentication ipv6 access-class {<num-std> <name>} in no authentication ipv6 access-class	为 Telnet/SSH/Web 登录方式绑定标准的 IPv6 ACL 规则；本命令的 no 操作为取消绑定 ACL。
authentication line {console vty web} login method1 [method2 ...] no authentication line {console vty web} login	配置远程登录认证方法列表。
authentication enable method1 [method2 ...] no authentication enable	配置 enable 认证方法列表
authorization line {console vty web} exec method1 [method2 ...] no authorization line {console vty web} exec	配置远程登录授权方法列表。
authorization line vty command <1-15> {local radius tacacs} (none) no authorization line vty command <1-15>	配置 VTY（即指 Telnet 和 ssh 登录方式）登录用户的命令授权方式和授权选择优先级。
accounting line {console vty} command <1-15> {start-stop stop-only none} method1 [method2...] no accounting line {console vty} command <1-15>	配置登录记账方法列表
特权模式	

terminal monitor terminal no monitor	使登录到交换机的 Telnet 客户端显示调试信息；本命令的 no 操作为关闭 Telnet 客户端显示调试信息的功能。
show users	显示通过 telnet 和 ssh 登陆的用户信息，包括线路号，登陆的用户名及用户的 IP。
clear line vty <0-31>	删除指定线路上登陆的用户，强制 telnet 或 ssh 登陆的用户下线。

2. 交换机 Telnet 登录到远程主机

命令	解释
特权模式	
telnet [vrf <vrf-name>] {<ip-addr> <ipv6-addr> host <hostname>} [<port>]	使用交换机提供的 Telnet 客户端登录到远程主机。

2.2.2 SSH

2.2.2.1 SSH 简介

SSH 是 Secure Shell 安全外壳的简写，它建立在可靠的 TCP/IP 等通信协议之上，通过 SSH 服务器和 SSH 客户端软件之间的密钥交换，身份认证，加密等算法的协商，在它们之间建立一条安全的传输信息的通道，保证双方交互的信息不能被任何第三方截取和破译，从而最大限度的保证了对实现 SSH 服务器功能的交换机的配置和管理。目前交换机上实现的是符合 SSH2.0 协议规定的 SSH 服务器。支持 SSH2.0 标准的终端软件如 SSH Secure Client、putty 等可以利用 SSH2.0 协议，远程登陆交换机上的 SSH 服务器，实现对该交换机的安全的配置和管理。

目前 SSH 服务器支持客户端软件对主机的 RSA 公钥认证，支持协议规定的 3DES 加密算法，以及 SSH 服务器对 SSH 用户的密码认证等。

2.2.2.2 SSH 服务器配置任务序列

命令	解释
全局配置模式	
ssh-server enable no ssh-server enable	打开交换机的 SSH 服务器功能；本命令的 no 操作为关闭 SSH 服务器功能。

username <username> [privilege <privilege>] [password [0 7] <password>] no username <username>	配置 SSH 客户端软件登录到交换机的用户名和口令；本命令的 no 操作为删除授权 SSH 用户。
ssh-server timeout <timeout> no ssh-server timeout	设置 SSH 认证超时时间；本命令的 no 操作恢复缺省的 SSH 认证超时时间。
ssh-server authentication-retries <authentication-retries> no ssh-server authentication-retries	设置 SSH 认证重试次数；本命令的 no 操作恢复缺省的 SSH 认证重试次数。
ssh-server host-key create rsa modulus <modulus>	生成新的 SSH 服务器的 RSA 主机密钥对。
特权模式	
terminal monitor terminal no monitor	使登录到交换机的 SSH 客户端显示调试信息；本命令的 no 操作为关闭 SSH 客户端显示调试信息的功能。
show crypto key	显示 ssh 加密密钥。
crypto key clear rsa	清除 ssh 加密密钥。

2.2.2.3 SSH 服务器配置举例

案例 1:

组网需求：交换机端运行 SSH 服务器，终端运行支持 SSH2.0 标准的客户端软件如 Secure shell client 或 putty 等。客户端使用用户名和密码方式登录交换机。

交换机首先配置本地的地址，然后增加 SSH 用户，启动 SSH 服务，这样 SSH2.0 客户端软件就可以利用交换机配置的用户名和密码远程登录配置 SSH 服务的交换机了。

```
Switch(config)#ssh-server enable
```

```
Switch(config)#interface vlan 1
```

```
Switch(Config-if-Vlan1)#ip address 100.100.100.200 255.255.255.0
```

```
Switch(Config-if-Vlan1)#exit
```

```
Switch(config)#username test privilege 15 password 0 test
```

如果是 IPv6 网络，终端需要运行支持 IPv6 功能的 SSH 客户端软件，例如 putty6，交换机上除配置本地的地址为 IPv6 地址外，其它配置不变。

2.3 配置交换机的 IP 地址

交换机所有以太网接口都默认为二层（DataLink Layer）端口，进行二层转发。VLAN 接口（Interface VLAN）代表了某一个 VLAN 的三层接口功能，可以配置 IP 地址，该 IP 地址也是交换机的 IP 地址。VLAN 接口相关的配置命令都可以在 VLAN 接口模式下配置。交换机为用户提供了三种配置 IP 地址的方式：

- ☞ 手工配置方式
- ☞ BootP 方式
- ☞ DHCP 方式

手工配置 IP 地址，即用户为交换机指定一个 IP 地址。

BootP/DHCP 方式是交换机作为 BootP/DHCP Client，向 BootP/DHCP Server 发出 BootPRequest（申请获取地址的请求包）广播包，BootP/DHCP Server 接收到请求后将地址分配给交换机。另外交换机还具有了 DHCP Server 的功能，能够动态的为 DHCP Client 分配 IP 地址、网关地址及 DNS 服务器地址等网络参数。具体 DHCP Server 的配置参见网络协议操作部分。

2.3.1 配置交换机的 IP 地址任务序列

1. 进入 VLAN 接口配置模式
2. 手工配置方式
3. BootP 方式
4. DHCP 方式

1. 进入 VLAN 接口配置模式

命令	解释
全局配置模式	
interface vlan <vlan-id> no interface vlan <vlan-id>	创建一个 VLAN 接口（VLAN 接口属于三层接口）；本命令的 no 操作为删除交换机创建的 VLAN 接口（三层接口）。

2.手工配置方式

命令	解释
VLAN 接口配置模式	
ip address <ip_address> <mask> [secondary] no ip address <ip_address> <mask> [secondary]	配置交换机的 VLAN 接口的 IP 地址；本命令的 no 操作为删除交换机的 VLAN 接口的 IP 地址。
ipv6 address <ipv6-address / prefix-length> [eui-64] no ipv6 address <ipv6-address / prefix-length>	配置 IPv6 地址，包括可聚合全球单播地址，本地站点地址，本地链路地址。本命令的 no 操作为删除 IPv6 地址。

3.BootP 方式

命令	解释
----	----

VLAN 接口配置模式	
ip bootp-client enable no ip bootp-client enable	使能交换机为 BootP Client，通过 BootP 协商方式获取 IP 地址及网关地址；本命令的 no 操作为关闭 BootP Client 功能。

4.DHCP

命令	解释
VLAN 接口配置模式	
ip dhcp-client enable no ip dhcp-client enable	使能交换机为 DHCP Client，通过 DHCP 协商方式获取 IP 地址及网关地址；本命令的 no 操作为关闭 DHCP Client 功能。

2.4 SNMP 配置

2.4.1 SNMP 介绍

SNMP（Simple Network Management Protocol，简单网络管理协议）是目前使用最广泛的网络管理协议，大量应用于以 TCP/IP 为基础的计算机网络。SNMP 是一个不断发展着的协议：SNMP v1 简单、易实现，被众多厂家支持；SNMPv2c 对 v1 的功能进行了部分修正和丰富，开始支持分层式的网管；SNMPv3 在安全性上做了极大的扩充，添加了 USM（基于用户的安全模型）和 VACM（基于视图的访问控制模型）子系统。

SNMP 协议提供了一个在网络中两点之间交换管理信息的直接的、基本的方法。SNMP 采用轮询的消息查询机制，采用被广泛使用的面向无连接的传输层协议 UDP 来传输消息，因此能够很好的被现有的计算机网络支持。

SNMP 协议采用管理站/代理模式，因此 SNMP 结构包括两个部分：NMS 网络管理站（Network Management Station），是运行支持 SNMP 协议的网管软件客户端程序的工作站，在 SNMP 的网络管理中起核心作用。Agent 代理，是运行在被管理网络设备上的服务器端软件，直接管理被管对象。NMS 利用通信手段，通过 Agent 代理来管理各被管对象。（本款及后续系列交换机都具有 Agent 代理功能）。

SNMP 的 NMS 和 Agent 之间通过标准消息进行通信，采取客户/服务器模式，由 NMS 发出请求，Agent 做出应答。SNMP 共有 7 种消息类型：

- ☞ Get-Request
- ☞ Get-Response
- ☞ Get-Next-Request
- ☞ Get-Bulk-Request
- ☞ Set-Request
- ☞ Trap

Inform-Request

NMS 通过 Get-Request、Get-Next-Request、Get-Bulk-Request 和 Set-Request 消息来对 Agent 发出查询和设置管理变量的请求，Agent 在收到请求后，用 Get-Response 消息来对请求进行回复。在某些特殊情况下，如网络设备端口 UP/DOWN、网络拓扑变化时候，Agent 会主动的向 NMS 发送 Trap 消息来通知 NMS 发生了异常事件。（当然，NMS 还可以通过设置 RMON 功能，自行对一些情况设置警报，当设定的警报事件触发后，Agent 将根据设置发送 Trap 或记录 Log，关于 RMON，下面有具体介绍）。Inform-Request 主要用于 NMS 之间进行通信，一般应用于分层式的网络管理。

USM 提供了完善的加密和鉴别服务，保证了传输的安全性。根据用户输入的密码，USM 对报文进行加密，保证报文在传输过程中不被察看，对报文进行鉴别，保证报文在传输过程中不被修改。USM 的标准加密算法为 DES-CBC 算法，鉴别算法为 HMAC-MD5 和 HMAC-SHA 算法。同时 USM 提供了时间窗的检查，防止网络延迟和重播的干扰。

VACM 提供了优秀的用户鉴权服务，保证了访问的安全性。VACM 将访问权限相同的用户放入同一组中，并为组划分了读写和通告操作的安全范围，有效地防止了用户的越权行为。

2.4.2 MIB 介绍

NMS 可以访问的网管信息是经过精确的定义的，被完备的组织在一个管理信息数据库中，即 MIB。所谓 **MIB 管理信息库**（Management Information Base），是对于通过网络管理协议可以访问信息的精确定义。它使用一个层次化、结构化的形式，定义了可以从被监测网络设备上获得的管理信息。ISO ASN.1 为 MIB 定义了一个树型结构，每个 MIB 都用这种树型结构来组织所有的可用信息，树的每个节点都包含一个 OID 对象标识符(Object Identifier)和一个关于该节点的简短文本描述。OID 是有句点隔开的一组整数，它命名节点并且可以由它指示该节点在 MIB 树型结构中的位置，如下图所示：

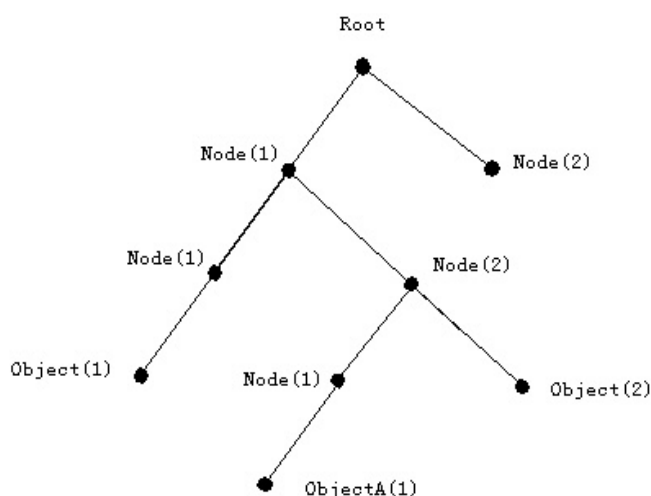


图 2-1 ASN.1 树实例

在该图中，对象 A 的 OID 为 1.2.1.1，NMS 通过这个独一无二的 OID，可以没有歧义的访问到这个对象，从而获取这个对象包含的标准变量。MIB 就按照这个结构定义了一个所监控网络设备的标准变量的集合。

如果您需要浏览 Agent 的 MIB 中的变量信息，需要在 NMS 上运行 MIB 浏览软件。Agent 上的 MIB 一般包括公有 MIB 和私有 MIB 两部分，公有 MIB 内定义的是公开的，所有 NMS 都可以访问的网络管理信息，私有 MIB 内定义的是各设备特有的属性信息，需要设备厂商的支持才可以浏览和控制。

MIB-I [RFC1156]是 SNMP 公有 MIB 库的第一个版本，后来经过扩充，被 MIB-II [RFC1213]所取代，MIB-II 保留了 MIB-I 在原来的 MIB 树中的对象标识符。MIB-II 下面包含很多子树，我们将之称为组，这些组里的对象覆盖了网络管理的各个功能域，NMS 通过访问 SNMP Agent 的 MIB 库，就可以得到相应的网络管理信息。

本交换机可以做为 SNMP Agent，支持 SNMPv1/v2c 和 SNMPv3。本交换机支持基本的 MIB-II、RMON 公有 MIB，还支持 BRIDGE MIB 等相关公有 MIB，同时支持自定义的私有 MIB，基本涵盖了本款交换机所涉及的各个相关参数，为网管软件管理提供全面的支持。

2.4.3 RMON 介绍

RMON 是对 SNMP 标准基本体系的最重要的扩充。RMON 是一套 MIB 定义，其作用是定义标准的网络监视功能和接口，使基于 SNMP 的管理终端和远程监视器之间能够通信。RMON 提供了一种有效并且高效的方法来监视子网范围内的行为。

RMON 的 MIB 分为 10 组，该交换机支持其中最常用的 1、2、3、9 组，即：

统计组(statistics): 维护代理监视的每一个子网的基本使用和错误统计。

历史组(history): 记录从统计组可得到的信息的周期性统计样本。

警报组(alarm): 允许管理控制台人员为 RMON 代理记录的任何计数或整数设置采样间隔和报警阈值。

事件组(event): 一个关于由 RMON 代理产生的所有事件的表。

其中，警报组需要事件组的实现。统计组和历史组是显示现在或以前的一些子网统计数据。警报组和事件组则提供了一种可以监视网络上任意整数型数据变化的方法，并在数据异常时提供一些警告动作（发送 Trap 或者记录 Log）。

2.4.4 SNMP 配置

2.4.4.1 SNMP 配置任务序列

- 1.打开或关闭 SNMP 代理服务器功能
- 2.配置 SNMP 团体字符串及代理设备的属性
- 3.配置 SNMP 管理站地址
- 4.配置引擎号
- 5.配置用户

- 6.配置组
- 7.配置视图
- 8.配置 TRAP
- 9.启动/关闭 RMON

1.打开或关闭 SNMP 代理服务器功能

命令	解释
全局配置模式	
snmp-server enable no snmp-server enable	打开交换机作为 SNMP 代理服务器功能；本命令的 no 操作为关闭 SNMP 代理服务器功能。

2.配置 SNMP 团体字符串

命令	解释
全局配置模式	
snmp-server community {ro rw} {0 7} <string> [access {<num-std> <name>}] [ipv6-access {<ipv6-num-std> <ipv6-name>}] [read <read-view-name>] [write <write-view-name>] no snmp-server community <string> [access {<num-std> <name>}] [ipv6-access {<ipv6-num-std> <ipv6-name>}]	设置交换机的团体字符串；本命令 no 操作为删除配置的团体字符串。

3.配置 SNMP 管理站地址

命令	解释
全局配置模式	
snmp-server securityip {<ipv4-address> <ipv6-address> } no snmp-server securityip {<ipv4-address> <ipv6-address> }	设置允许访问本交换机的NMS管理站的安全IPv4或者IPv6地址；本命令的no操作为删除配置的安全IPv4或者IPv6地址。
snmp-server securityip enable snmp-server securityip disable	打开/关闭 NMS 管理站的安全 IP 地址检查功能。

4.配置引擎号

命令	解释
----	----

全局配置模式	
snmp-server engineid <engine-string> no snmp-server engineid	设置交换机的本地引擎号，用于 v3。

5.配置用户

命令	解释
全局配置模式	
snmp-server user <use-string> <group-string> [{authPriv authNoPriv} auth {md5 sha} <word>] [access {<num-std> <name>}] [ipv6-access {<ipv6-num-std> <ipv6-name>}] no snmp-server user <user-string> [access {<num-std> <name>}] [ipv6-access {<ipv6-num-std> <ipv6-name>}]	为一个 SNMP 的组添加一个新用户，完成 USM 配置，用于 v3。

6.配置组

命令	解释
全局配置模式	
snmp-server group <group-string> {noauthnopriv authnopriv authpriv} [[read <read-string>] [write <write-string>] [notify <notify-string>]] [access {<num-std> <name>}] [ipv6-access {<ipv6-num-std> <ipv6-name>}] no snmp-server group <group-string> {noauthnopriv authnopriv authpriv} [access {<num-std> <name>}] [ipv6-access {<ipv6-num-std> <ipv6-name>}]	设置交换机的组信息，完成 VACM 配置，用于 v3。

7.配置视图

命令	解释
全局配置模式	
snmp-server view <view-string> <oid-string> {include exclude}	设置交换机的视图信息，用于 v3。

no snmp-server view <view-string> [<oid-string>]	
---	--

8.配置 TRAP

命令	解释
全局配置模式	
snmp-server enable traps no snmp-server enable traps	设置允许设备发送 Trap 消息，用于 v1/v2c/v3。
snmp-server host {<host-ipv4-address> <host-ipv6-address>} {v1 v2c {v3 {Noauthnopriv Authnopriv Authpriv}}} <user-string> no snmp-server host {<host-ipv4-address> <host-ipv6-address>} {v1 v2c {v3 {Noauthnopriv Authnopriv Authpriv}}} <user-string>	设置接收 SNMP 的 Trap 消息的网络管理站 IPv4 或者 IPv6 地址，v1/v2c 中的 Trap 团体字符串，v3 中的用户名和安全级别。本命令的 no 操作为删除指定的接收 Trap 消息的网络管理站的 IPv4 或者 IPv6 地址。
snmp-server trap-source {<ipv4-address> <ipv6-address>} no snmp-server trap-source {<ipv4-address> <ipv6-address>}	设置本交换机发送 trap 时所使用源 IPv4 或 IPv6 地址；本命令的 no 操作为删除配置的发送 trap 使用的源 IPv4 或 IPv6 地址。
端口配置模式	
[no] switchport updown notification enable	开启或者关闭端口 UP/DOWN 事件发送 trap 信息的功能。

9.启动/关闭 RMON

命令	解释
全局配置模式	
rmon enable no rmon enable	打开/关闭 RMON。

2.4.5 SNMP 典型配置举例

管理站（NMS）的 IP 地址是 1.1.1.5；交换机（Agent）的 IP 地址是 1.1.1.9。

案例 1：管理站的网管软件使用 SNMP 协议从交换机获取数据。

配置步骤如下：

Switch(config)#snmp-server enable

Switch(config)#snmp-server community rw private

```
Switch(config)#snmp-server community ro public
```

```
Switch(config)#snmp-server securityip 1.1.1.5
```

这样，管理站就可以使用 **private** 作为团体字符串对交换机进行可读写的访问，也可以使用 **public** 作为团体字符串对交换机进行只读的访问。

案例 2：管理站要接收来自交换机的 v1 Trap 消息（注：管理站可能设置了对 Trap 的团体字符串的验证，那么此例假设管理站的 Trap 验证团体字符串为 **usertrap**）。

配置步骤如下：

```
Switch(config)#snmp-server enable
```

```
Switch(config)#snmp-server host 1.1.1.5 v1 usertrap
```

```
Switch(config)#snmp-server enable traps
```

案例 3：管理站的网管软件使用 SNMP v3 协议从交换机获取数据。

配置步骤如下：

```
Switch(config)#snmp-server enable
```

```
Switch(config)#snmp-server user tester UserGroup authPriv auth md5 hellotst
```

```
Switch(config)#snmp-server group UserGroup AuthPriv read max write max notify max
```

```
Switch(config)#snmp-server view max 1 include
```

案例 4：管理站要接收来自交换机的 v3Trap 消息。

配置步骤如下：

```
Switch(config)#snmp-server enable
```

```
Switch(config)#snmp-server host 10.1.1.2 v3 authpriv tester
```

```
Switch(config)#snmp-server enable traps
```

案例 5：管理站（NMS）的 IPv6 地址是 2004:1:2:3::2，交换机（Agent）的 IPv6 地址是 2004:1:2:3::1。管理站的网管软件使用 SNMP 协议从交换机获取数据。

交换机端的配置如下：

```
Switch(config)#snmp-server enable
```

```
Switch(config)#snmp-server community rw private
```

```
Switch(config)#snmp-server community ro public
```

```
Switch(config)#snmp-server securityip 2004:1:2:3::2
```

这样，管理站就可以使用 **private** 作为团体字符串对交换机进行可读写的访问，也可以使用 **public** 作为团体字符串对交换机进行只读的访问。

案例 6：管理站要接收来自交换机的 Trap 消息（注：管理站可能设置了对 Trap 的团体字

字符串的验证，那么此例假设管理站的 Trap 验证团体字符串为 usertrap）。

交换机端的配置如下：

```
Switch(config)#snmp-server host 2004:1:2:3::2 v1 usertrap
```

```
Switch(config)#snmp-server enable traps
```

2.4.6 SNMP 排错帮助

在配置、使用 SNMP 时，可能会由于物理连接、配置错误等原因导致 SNMP 未能正常运行。因此，用户应注意以下要点：

- ☞ 首先应该保证物理连接的正确无误；
- ☞ 其次，保证接口和链路协议是 UP（使用 show interface 命令），保证交换机和主机能互相 ping 通（使用 ping 命令）；
- ☞ 然后，务必确认交换机打开了 SNMP Agent 服务器功能（使用 snmp-server enable 命令）；
- ☞ 接着，保证为 NMS 配置安全 IP（使用 snmp-server securityip 命令）和团体字符串（使用 snmp-server community 命令）正确，因为只要有一个错误 SNMP 将不能正确和 NMS 通信；
- ☞ 如果需要使用 Trap 功能，务必打开 Trap 功能（使用 snmp-server enable traps 命令），为了保证 Trap 能发送到指定的主机，请记住正确配置 Trap 的目标主机的 IP 和团体字符串（使用 snmp-server host 命令）；
- ☞ 如果需要使用 RMON 功能，必须首先打开 RMON（使用 rmon enable 命令）；
- ☞ 在 SNMP 运行过程中，如果用户还有疑惑，可以使用 show snmp 命令查看 SNMP 收发包的统计信息；可以使用 show snmp status 命令查看 SNMP 的配置信息；可以使用 debug snmp packet 命令打开 SNMP 的调试开关，查看调试信息。

如果上述查看方式的尝试仍无法解决 SNMP 的问题，那么请与技术服务中心联系。

2.5 交换机升级

2.5.1 交换机系统文件

系统文件包括系统映像文件和引导文件。交换机的升级就是对这两个文件更新，方法就是用新的文件覆盖旧的文件。

系统映像文件是指交换机硬件驱动和软件支持程序等的压缩文件，即我们通常说的 IMG 升级文件。交换机系统映像文件只允许保存在 FLASH 中，文件名固定为 nos.img。

引导文件是指引导交换机初始化等的文件，即我们通常说的 ROM 升级文件（如果文件较大，可以压缩为 IMG 文件）。引导文件只允许保存在 ROM 中。交换机规定引导文件的文件名固定为 boot.rom。

系统映像文件和引导文件的升级方法是一样的。交换机为用户提供了两种模式下的交换

机升级：一、BootROM 模式；二、Shell 模式下的 TFTP 升级、FTP 升级。下面两节详细介绍这两种模式的升级方法。

2.5.2 BootROM 模式升级

在 BootROM 模式下升级交换机有一种升级方式：TFTP，可通过 BootROM 下的命令设置。

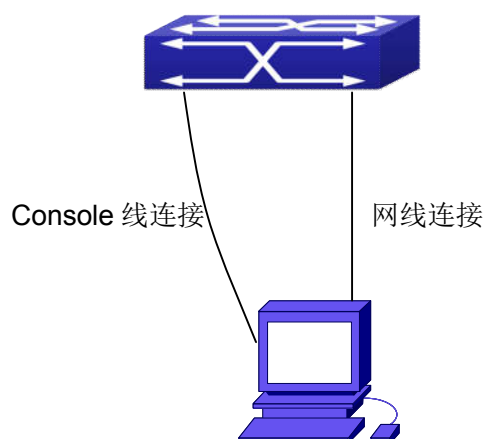


图 2-2 在 BootROM 模式下交换机升级的典型拓扑

升级步骤如下：

第一步：

如图将一台 PC 作为交换机的控制台，并且该控制台的以太网口与交换机的网管端口相连，在 PC 上安装有 TFTP 的服务器软件，及需要升级的 boot 文件。

第二步：

在交换机启动的过程中，按住“ctrl+b”键，直到交换机进入 BootROM 监控模式。显示如下：

[Boot]:

第三步：

在 BootROM 模式下，执行命令 `setconfig`，设置本机在 BootROM 模式下的 IP 地址、服务器的 IP 地址。如设置本机地址为 192.168.1.2，PC 地址为 192.168.1.66，配置如下：

[Boot]: `setconfig`

Host IP Address: [10.1.1.1] 192.168.1.2

Server IP Address: [10.1.1.2] 192.168.1.66

[Boot]:

第四步：

打开 PC 中 TFTP 服务器，运行 TFTP Server 程序。在往交换机下传升级版本时，请先检

查服务器与被升级交换机之间的连接状态，在交换机端使用 ping 命令，ping 通后，在交换机的 BootROM 模式下执行 load 命令；若 ping 不通，则检查原因。

以下是更新引导文件 boot.rom。

```
[Boot]: load boot.rom
```

```
TFTP from server 192.168.1.66; our IP address is 192.168.1.2
```

```
Filename 'boot.rom'.
```

```
Load address: 0x300000
```

```
Loading:
```

```
#####
```

```
#####
```

```
done
```

```
Bytes transferred = 496240 (79270 hex)
```

```
[Boot]:
```

第五步：

在 BootROM 模式下，执行命令 write boot.rom。以下是对更新引导文件的保存：

```
[Boot]: write boot.rom
```

```
File exists, overwrite? (Y/N)[N] y
```

```
Writing flash:/boot.rom.....
```

```
Write flash:/boot.rom OK.
```

```
[Boot]:
```

第六步：

升级交换机成功，在 BootROM 模式下，执行命令 run 或 reboot，回到 CLI 配置界面。

```
[Boot]:run（或者 reboot）
```

BootROM 模式下的其他命令

1. DIR 命令

用于显示 FLASH 中现存的文件。

```
[Boot]: dir
```

```
5399893 nos.img
```

```
1 file(s), 0 dir(s)
```

```
Total size:6995456 bytes , used size:5422080 bytes, free size:1573376 bytes
```

```
[Boot]:
```

2.5.3 FTP/TFTP 升级

2.5.3.1 FTP/TFTP 简介

FTP（File Transfer Protocol）/TFTP（Trivial File Transfer Protocol）都是文件传输协议，在TCP/IP协议族中处于第四层，即属于应用层协议，主要用于主机之间、主机与交换机之间传输文件。它们都采用客户机—服务器模式进行文件传输。下面是它们的不同之处。

FTP承载于TCP之上，提供可靠的面向连接数据流的传输服务，但它不提供文件存取授权，以及简单的认证机制（通过明文传输用户名和密码来实现认证）。FTP在进行文件传输时，客户机和服务器之间要建立两个连接：控制连接和数据连接。首先由FTP客户机发出传送请求，与服务器的21号端口建立控制连接，通过控制连接来协商数据连接。

数据连接有两种方式：

一种为主动连接。客户端是主动告诉服务器自己用于数据传输的地址和端口号，控制连接将一直保留到数据传输完成。接着服务器在20号端口没有被使用的条件下采用20号端口与客户机提供的地址和端口号建立数据连接，并传输数据；如果20号端口正在被使用，通过设置20号端口可以重用，服务器通过系统自动生成另外的端口号建立数据连接。

另外一种方式是被动连接。客户端通过控制连接告诉服务器端建立被动连接，服务器端就建立自己的数据监听端口，将这个端口通过控制连接告诉客户端，由客户端主动与指定地址的端口建立数据连接。

由于数据连接是通过指定的地址和端口号，还存在通过第三方来提供数据连接服务。

TFTP 承载在 UDP 之上，提供不可靠的数据流传输服务，同时也不提供用户认证机制以及根据用户权限提供对文件操作授权；它是通过发送报文，应答方式，加上超时重传方式来保证数据的正确传输。TFTP 相对于 FTP 的优点是提供简单的、开销不大的文件传输服务。

交换机实现 FTP/TFTP 客户机和服务器的功能。当交换机作为 FTP/TFTP 客户机时，在不影响交换机正常工作的情况下，能从远端 FTP/TFTP 服务器（可以是主机和其它交换机）下载配置文件或系统文件，（FTP 客户端可以查看服务器上的文件列表），也可以将交换机当前配置文件或系统文件上载到远端 FTP/TFTP 服务器上（可以是主机和其它交换机）的功能；当交换机作为 FTP/TFTP 服务器时，同样它能为它授权的 FTP/TFTP 客户机提供上传和下载文件的服务，（FTP 服务器还提供传输服务器上文件列表功能）。

下面介绍 FTP/TFTP 中经常用到的术语：

ROM: EPROM 的简称，可擦写只读寄存器。交换机采用 FLASH 闪存代替 EPROM。

SDRAM: 交换机内存，用于系统软件的运行和配置序列的存放。

FLASH: 闪存，用于保存系统文件和配置文件。

系统文件: 包括系统映像文件和引导文件。

系统映像文件: 是指交换机硬件驱动和软件支持程序等的压缩文件，即我们通常说的 IMG 升级文件。交换机系统映像文件只允许保存在 FLASH 中。交换机规定，在全局配置模式下通过 FTP 上载系统映像文件的文件名固定为 nos.img，拒绝其它系统 IMG 文件的上载。

引导文件: 是指引导交换机初始化等的文件，即我们通常说的 ROM 升级文件（如果文件较大，可以压缩为 IMG 文件）。引导文件只允许保存在 ROM 中。交换机规定引导文件的文

件名固定为 **boot.rom**。

配置文件：包括启动配置文件和运行配置文件。区分启动配置文件和运行配置文件便于实现配置的备份和更新。

启动配置文件：是指交换机启动时采用的配置序列。启动配置文件存放在非易失存储介质中，即对应着所谓的配置保留。对于不支持 **CF** 卡的设备，交换机启动配置文件只存放在 **FLASH** 中。对于支持 **CF** 卡的设备，启动配置文件可以存放在 **FLASH** 中或者 **CF** 卡中。对于支持配置多启动配置文件的设备，启动配置文件名为扩展名为 **.cfg** 的文件，默认情况下为 **startup.cfg**。对于不支持多配置文件的设备，启动配置文件名固定为 **startup-config**。

运行配置文件：是指交换机当前运行的配置序列。交换机运行配置文件存放在内存中。目前，使用命令 **write** 或命令 **copy running-config startup-config**，可将运行配置序列 **running-config** 从内存中保存到 **FLASH** 中，即实现运行配置序列到启动配置文件的转变，形成配置保留。为了禁止非法文件的上载和方便配置，交换机规定，运行配置文件名固定为 **running-config**。

出厂配置文件：即 **factory-config** 文件，是交换机出厂时的配置文件，使用命令 **set default** 和命令 **write**，重启后可将配置文件恢复成出厂配置文件。

2.5.3.2 FTP/TFTP 配置

交换机作为 **FTP** 或者 **TFTP** 客户机时，在配置上极其相似，因此本手册把 **FTP** 和 **TFTP** 作为客户机时的配置结合在一起说明。

2.5.3.2.1 FTP/TFTP 配置任务序列

1. FTP/TFTP 客户机配置

- (1) 上载/下载配置文件或系统文件
- (2) **FTP** 客户机查看服务器上文件列表

2. FTP 服务器配置

- (1) 启动 **FTP Server**
- (2) 配置 **FTP** 登录用户名和口令
- (3) 修改 **FTP Server** 连接空闲时限
- (4) 关闭 **FTP Server**

3. TFTP 服务器配置

- (1) 启动 **TFTP Server**
- (2) 配置 **TFTP Server** 连接空闲时限
- (3) 配置超时范围内没有收到应答报文的重传次数
- (4) 关闭 **TFTP Server**

1. FTP/TFTP 客户机配置

(1) FTP/TFTP 客户机端上下载文件

命令	解释
特权用户配置模式	
copy <source-url> <destination-url> [ascii binary]	FTP/TFTP 客户机上下载文件。

(2) FTP 客户机查看服务器上文件列表

特权用户配置模式	
ftp-dir <ftpServerUrl>	FTP 客户机查看服务器上文件列表 FtpServerUrl 为 ftp://user:password@IPv4 IPv6 Address 格式。

2.FTP 服务器配置

(1) 启动 FTP 服务器

命令	解释
全局配置模式	
ftp-server enable no ftp-server enable	启动 FTP Server; 本命令的 no 操作为关闭 FTP Server 服务, 禁止 FTP 用户登录。

(2) 配置 FTP 登录用户名和口令

命令	解释
全局配置模式	
ip ftp username <username> password [0 7] <password> no ip ftp username <username>	配置 FTP 登录用户名和登录口令; 本命令的 no 操作为删除配置的用户名, 同时也删除密码。

(3) 修改 FTP Server 连接空闲时限

命令	解释
全局配置模式	
ftp-server timeout <seconds>	设置连接空闲时限。

3.TFTP 服务器配置

(1) 启动 TFTP 服务器

命令	解释
全局配置模式	
tftp-server enable no tftp-server enable	启动 TFTP Server; 本命令的 no 操作为关闭 TFTP Server 服务, 禁止 TFTP 用户登录。

(2) 修改 TFTP Server 连接空闲时限

命令	解释
全局配置模式	

tftp-server transmission-timeout <seconds>	设置超时的时间间隔。
---	------------

(3) 修改 TFTP Server 连接重传次数

命令	解释
全局配置模式	
tftp-server retransmission-number <number>	设置超时时间内的最大重传次数。

2.5.3.3 FTP/TFTP 配置举例

无论地址为 IPv4 还是 IPv6，命令设置方式相同，下面的举例中仅以 IPv4 地址为例。

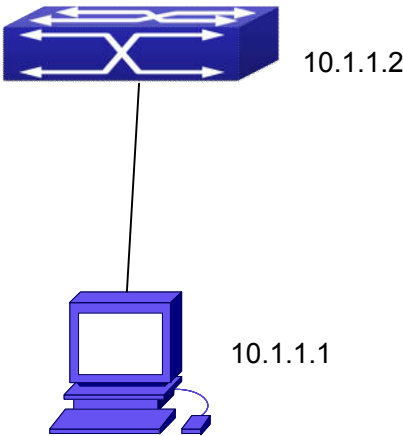


图 2-3 作为 FTP/TFTP client 下载 nos.img 文件

实例 1：交换机作为 FTP/TFTP 客户端来使用。交换机通过某个端口与计算机相连接，计算机为 FTP/TFTP 服务器，IP 地址为 10.1.1.1，交换机作为 FTP/TFTP 客户端，交换机管理 VLAN 的 IP 地址为 10.1.1.2。从计算机上下载交换机的“nos.img”文件。

✎ FTP 配置：

计算机端配置：

在计算机上启动 FTP Server 软件，并且设置用户名为“Switch”，密码为“superuser”。并将“12_30_nos.img”文件放到计算机上对应的 FTP Server 目录下。

交换机的配置步骤如下：

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip address 10.1.1.2 255.255.255.0

```
Switch(Config-if-Vlan1)#no shut
Switch(Config-if-Vlan1)#exit
Switch(config)#exit
Switch#copy ftp://Switch:superuser@10.1.1.1/12_30_nos.img nos.img
```

执行完上述命令，交换机就可将计算机上的“nos.img”文件下载到 FLASH 中了。

☞ TFTP 配置：

计算机端配置：

在计算机机上启动 TFTP Server 软件，并将“12_30_nos.img”文件放到计算机上对应的 TFTP Server 目录下。

交换机的配置步骤如下：

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-Vlan1)#no shut
Switch(Config-if-Vlan1)#exit
Switch(config)#exit
Switch#copy tftp://10.1.1.1/12_30_nos.img nos.img
```

实例 2：交换机作为 FTP 服务器来使用。交换机通过某个端口与计算机相连接，交换机作为 FTP 服务器，计算机作为 FTP 客户端，将交换机上的“nos.img”文件传送到计算机上，保存为 12_25_nos.img。

交换机的配置步骤如下：

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-Vlan1)#no shut
Switch(Config-if-Vlan1)#exit
Switch(config)#ftp-server enable
Switch(config)#ip ftp username Switch password 0 superuser
```

计算机端配置：

通过 FTP 客户端软件，登录到交换机，用户名为“Switch”，密码为“superuser”，通过“get nos.img 12_25_nos.img”命令将交换机上的“nos.img”文件下载到计算机上。

实例 3：交换机作为 TFTP 服务器来使用。交换机通过某个端口与计算机相连接，交换机作为 TFTP 服务器，计算机作为 TFTP 客户端，将交换机上的“nos.img”文件传送到计算机上。交换机的配置步骤如下：

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.1.2 255.255.255.0
```

```
Switch(Config-if-Vlan1)#no shut
```

```
Switch(Config-if-Vlan1)#exit
```

```
Switch(config)#ftp-server enable
```

计算机端配置：

通过 TFTP 客户端软件，登录到交换机，通过“tftp”命令将交换机上的“nos.img”文件下载到计算机上。

实例 4： 交换机作为 FTP 客户机查看 FTP 服务器上文件列表。同步情况：交换机通过以太口和计算机相连，计算机为 FTP 服务器，IP 地址为 10.1.1.1，交换机作为 FTP 客户端，交换机 VLAN1 接口 IP 地址为 10.1.1.2。

FTP 配置：

计算机端：

在计算机上启动 FTP Server 软件，并且设置用户 Switch，密码为 superuser。

交换机：

```
Switch(config)#interface vlan 1
```

```
Switch(Config-if-Vlan1)#ip address 10.1.1.2 255.255.255.0
```

```
Switch(Config-if-Vlan1)#no shut
```

```
Switch(Config-if-Vlan1)#exit
```

```
Switch(config)#exit
```

```
Switch#ftp-dir ftp://Switch:superuser@10.1.1.1
```

```
220 Serv-U FTP-Server v2.5 build 6 for WinSock ready...
```

```
331 User name okay, need password.
```

```
230 User logged in, proceed.
```

```
200 PORT Command successful.
```

```
150 Opening ASCII mode data connection for /bin/ls.
```

```
recv total = 480
```

```
nos.img
```

```
nos.rom
```

```
parsecommandline.cpp
```

```
position.doc
```

```
qmdict.zip
```

```
...(省略部分显示)
```

```
show.txt
```

```
snmp.TXT
```

```
226 Transfer complete.
```

2.5.3.4 FTP/TFTP 排错帮助

2.5.3.4.1 FTP 排错帮助

在使用 FTP 协议上下载系统文件时，务必保证链路的可达，即在使用 FTP 之前，使用 Ping 命令检验 FTP 客户机和服务器的是否可达。如 Ping 不通，则需查看相应排错信息，恢复链路的可达性。

- ☞ 下面是发送文件时的正确信息，如果不正确，请检查链路的可达性并重新执行 copy 命令。

```
220 Serv-U FTP-Server v2.5 build 6 for WinSock ready...
```

```
331 User name okay, need password.
```

```
230 User logged in, proceed.
```

```
200 PORT Command successful.
```

```
nos.img file length = 1526021
```

```
read file ok
```

```
send file
```

```
150 Opening ASCII mode data connection for nos.img.
```

```
226 Transfer complete.
```

```
close ftp client.
```

- ☞ 下面是接收文件时的正确信息，如果不正确，请检查链路的可达性并重新执行 copy 命令。

```
220 Serv-U FTP-Server v2.5 build 6 for WinSock ready...
```

```
331 User name okay, need password.
```

```
230 User logged in, proceed.
```

```
200 PORT Command successful.
```

```
recv total = 1526037
```

```
*****
```

```
write ok
```

```
150 Opening ASCII mode data connection for nos.img (1526037 bytes).
```

```
226 Transfer complete.
```

- ☞ 如果交换机通过 FTP 升级系统文件或系统启动文件时，必须等待系统提示出现表示升级成功的“close ftp client.”或“226 Transfer complete.”的字样，此时交换机可以进行重启的操作，否则将会导致交换机无法启动。若出现通过 FTP 升级系统文件及系统启动文件失败时，请重新升级或进入到 BootROM 模式升级。

2.5.3.4.2 TFTP 排错帮助

在使用 TFTP 协议上下载系统文件时，务必保证链路的可达，即在使用 TFTP 之前，使用 Ping 命令检验 TFTP 客户机和服务器的是否可达。如 Ping 不通，则需查看相应排错信息，恢复链路的可达性。

- ☞ 下面是发送文件时的正确信息，如果不正确，请检查链路的可达性并重新执行 copy 命

令。

```
nos.img file length = 1526021
read file ok
begin to send file,wait...
file transfers complete.
close tftp client.
```

☞ 下面是接收文件时的正确信息，如果不正确，请检查链路的可达性并重新执行 `copy` 命令。

```
begin to receive file,wait...
recv 1526037
*****

write ok
transfer complete
close tftp client.
```

如果交换机通过 TFTP 升级系统文件或系统启动文件时，必须等待系统提示出现表示升级成功的“close tftp client.”的字样，此时交换机可以进行重启的操作，否则将会导致交换机无法启动。若出现通过 TFTP 升级系统文件及系统启动文件失败时，请重新升级或进入到 BootROM 模式升级。

第3章 文件系统操作

3.1 文件存储设备介绍

交换机的文件存储设备主要是 FLASH。FLASH 是交换机上最常用的存储设备，可以用来存放系统映像文件（IMG 文件）、系统引导文件（ROM 文件）和系统配置文件（CFG 文件）。

FLASH 可以在 Shell 模式下或 Bootrom 模式下进行文件的复制、删除、重命名操作。

3.2 文件系统操作任务配置序列

- 1.存储设备格式化操作
- 2.子目录的创建操作
- 3.子目录的删除操作
- 4.修改当前存储设备的工作路径
- 5.显示当前工作路径
- 6.显示存储设备中的指定文件或目录信息
- 7.删除文件系统上的指定文件
- 8.文件重命名操作
- 9.文件复制操作

1.存储设备格式化操作

命令	解释
特权用户配置模式	
format <device>	格式化存储设备。

2.子目录的创建操作

命令	解释
特权用户配置模式	
mkdir <directory>	在指定设备的指定目录下创建子目录。

3.子目录的删除操作

命令	解释
特权用户配置模式	
rmdir <directory>	在指定设备的指定目录下删除子目录。

4.修改当前存储设备的工作路径

命令	解释
特权用户配置模式	
cd <directory>	修改当前存储设备的工作路径。

5.显示当前工作路径

命令	解释
特权用户配置模式	
pwd	显示当前工作路径。

6.显示存储设备中的指定文件或目录信息

命令	解释
特权用户配置模式	
dir [WORD]	显示存储设备中的指定文件或目录信息。

7.删除文件系统上的指定文件

命令	解释
特权用户配置模式	
delete <file-url>	删除文件系统上的指定文件。

8.文件重命名

命令	解释
特权用户配置模式	
rename <source-file-url> <dest-file >	把交换机上的某个指定的文件重命名为新的文件名。

9.文件复制

命令	解释
特权用户配置模式	
copy <source-file-url > <dest-file-url>	把交换机上的某个指定文件复制为新的文件。

3.3 典型应用

将当前系统上 FLASH 中的 IMG 文件 flash:/nos.img 复制一份为 flash:/nos-6.1.11.0.img 文件。

交换机配置如下：

```
Switch#copy flash:/nos.img flash:/nos-6.1.11.0.img  
Copy flash:/nos.img to flash:/nos-6.1.11.0.img? [Y:N] y  
Copied file flash:/nos.img to flash:/nos-6.1.11.0.img.
```

3.4 排错帮助

当用户进行文件系统操作出现错误时，请检查是否是以下原因所引起的：

- ☞ 文件名或文件路径输入是否正确；
- ☞ 重命名文件时，该文件是否正在被使用，或目标文件名是否与已有的文件或目录相同。

第4章 集群网管配置

4.1 集群网管介绍

集群网管是一种带内配置管理手段，与常规的 CLI、SNMP、Web Config 不同的是，它借助某台中间交换机（命令交换机）对目标交换机（成员交换机）进行间接配置管理，而不是在管理工作站上对目标交换机进行直接配置管理。命令交换机和成员交换机之间是一对多的关系，在一台命令交换机上可以配置和管理多台成员交换机。只要在命令交换机上配置公网 IP，集群中所有成员交换机均可不配置公网 IP 也可以被远程配置管理，在 IP 资源日益紧张的今天，集群网管的配置手段节省了 IP 地址资源。而且集群网管做到了动态地发现具有集群功能的交换机（候选交换机），管理员可以根据需要手动或自动把发现的候选交换机加入已建立的集群，成为集群的成员交换机，从而可以通过命令交换机对成员交换机进行所有的配置和管理操作。当多台成员交换机分布在不同的地理位置（典型情况如不同的楼层）时，集群网管的方便性是很明显的。集群网管还有一个优点就是带内管理，即不需要为配置管理成员交换机而建立专门的通信联接，而是直接利用命令和成员之间的中继连线，因而是非常节省网络资源的。

基于集群网管以上特征，集群网管主要有以下优点：

- ☞ 节省 IP 地址
- ☞ 简化配置管理任务
- ☞ 不受网络拓扑结构和距离的限制
- ☞ 自动发现和自动建立功能
- ☞ 在出厂默认配置下就可以通过集群网管管理多台交换机
- ☞ 支持对集群内任意一台交换机的升级和配置管理

4.2 集群网管基本配置

集群网管配置任务序列如下：

1. 启动或停止集群功能
2. 建立集群
 - 1) 配置集群中成员设备使用的私有 IP 地址池
 - 2) 创建或删除集群
 - 3) 在集群中加入或删除一个成员
3. 在命令交换机上配置集群相关属性
 - 1) 使能或禁止集群自动加入功能
 - 2) 设置自动加入的 member 成为手动加入的 member
 - 3) 设置或修改集群中的交换机发送保活报文的时间间隔
 - 4) 设置或修改集群内部的保活报文最大允许丢失的个数
 - 5) 清除命令交换机维护的候选交换机列表

4. 在候选交换机上配置集群相关参数
 - 1) 设置集群发送保活报文的时间间隔
 - 2) 设置集群内部保活报文最大允许丢失的个数
5. 利用集群网管进行远程管理
 - 1) 远程配置管理
 - 2) 对成员交换机进行远程升级
 - 3) 重启成员交换机
6. 利用 web 管理集群网管
 - 1) 启动 http
7. 利用 snmp 管理集群网管
 - 1) 启动 snmp server

1. 启动或停止集群功能

命令	解释
全局配置模式	
cluster run [key <WORD>] [vid <VID>] no cluster run	启动或停止交换机本设备的集群功能。

2. 建立集群

命令	解释
全局配置模式	
cluster ip-pool <commander-ip> no cluster ip-pool	配置集群中成员设备使用的私有 IP 地址池。
cluster commander [<cluster_name>] no cluster commander	创建或者删除集群。
cluster member {candidate-sn <candidate-sn> mac-address <mac-addr> [id <member-id>]} no cluster member {id <member-id> mac-address <mac-addr>}	添加或删除集群成员。

3. 在命令交换机上配置集群相关属性

命令	解释
全局配置模式	
cluster auto-add no cluster auto-add	使能或禁止把新发现的候选交换机自动加入集群。

cluster member auto-to-user	把自动加入的成员变成手动加入的成员。
cluster keepalive interval <second> no cluster keepalive interval	设置集群的保活时间。
cluster keepalive loss-count <int> no cluster keepalive loss-count	设置集群中保活报文最大允许丢失个数。
特权模式	
clear cluster nodes [nodes-sn <candidate-sn-list> mac-address <mac-addr>]	清除命令交换机维护的候选交换机列表中的节点。

4. 在候选交换机上配置集群相关参数

命令	解释
全局配置模式	
cluster keepalive interval <second> no cluster keepalive interval	设置集群的保活时间。
cluster keepalive loss-count <int> no cluster keepalive loss-count	设置集群中保活报文最大允许丢失个数。

5. 利用集群网管进行远程管理

命令	解释
特权模式	
rcommand member <member-id>	在命令交换机上使用该命令对集群的成员交换机进行配置管理。
rcommand commander	在成员交换机上使用该命令对命令交换机进行配置管理。
cluster reset member [id <member-id> mac-address <mac-addr>]	在命令交换机上使用该命令重启成员交换机。
cluster update member <member-id> <src-url> <dst-filename> [ascii binary]	在命令交换机上对成员交换机进行远程升级。

6. 利用 web 管理集群网管

命令	解释
全局配置模式	

ip http server	在命令交换机和成员交换机上启动 http 功能。 注：通过 web 从 commander 访问 member 时必须确保 member 上面开启了 http 功能。commander 通过点击其集群拓扑图上 member 节点来访问 member。
-----------------------	--

7. 利用 snmp 管理集群网管

命令	解释
全局配置模式	
snmp-server enable	在命令交换机和成员交换机上启动 snmp server 功能。 注：通过 snmp 从 commander 访问 member 时必须确保 member 上面开启了 snmp server 功能。commander 通过设置团体字符串 <commander-community>@sw<member id> 的方式访问指定的 member。

4.3 集群网管举例

案例：
四台交换机 SW1-SW4，其中指定 SW1 为命令交换机，其余交换机为成员交换机，其中 SW2 和 SW4 和命令交换机直接相连，交换机 SW3 通过交换机 SW2 连接到命令交换机。

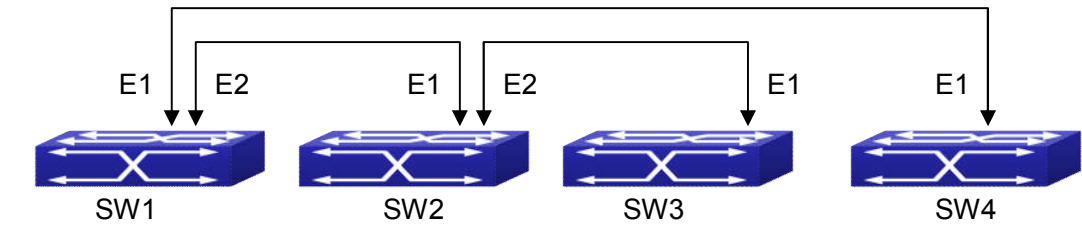


图 4-1 集群网管配置

配置步骤：

1. 配置命令交换机

SW1 的配置：

```
Switch(config)#cluster run
Switch(config)#cluster ip-pool 10.2.3.4
```

```
Switch(config)#cluster commander 5526
```

```
Switch(config)#cluster auto-add
```

2. 配置成员交换机

SW2-SW4 的配置:

```
Switch(config)#cluster run
```

4.4 集群网管排错帮助

当在使用集群网管过程中遇到问题，请检查是否是如下原因：

- ☞ 是否正确配置了命令交换机，并启动了自动加入功能(cluster auto-add)，并且是否命令交换机和成员交换机相连的端口属于配置的 cluster vlan。
- ☞ 在命令交换机的 VLAN1 启动 cluster commander 后，请不要在该 Vlan 下启动路由协议(rip,ospf,bgp)等，以避免该路由协议将该 Vlan 的私有集群网管地址广播到其它交换机，造成路由环路。
- ☞ 命令交换机和成员交换机之间的连接是否正常，可通过相关的 debug 命令观察交换机能否正确接收和处理相关的集群网管报文。