目 录

1 登录交换机典型配置举例 ····· 1-1
1.1 简介 ····· 1-1
1.2 通过Console口登录交换机典型配置举例 ····· 1-1
1.2.1 适用产品和版本 ····· 1-1
1.2.2 组网需求 ····· 1-1
1.2.3 配置思路 ····· 1-1
1.2.4 配置步骤 ····· 1-2
1.2.5 验证配置 ····· 1-4
1.2.6 配置文件 ····· 1-4
1.3 通过Telnet方式登录交换机典型配置举例 ····· 1-5
1.3.1 适用产品和版本 ····· 1-5
1.3.2 组网需求 ····· 1-5
1.3.3 配置思路 ····· 1-5
1.3.4 配置步骤 ····· 1-6
1.3.5 验证配置 ····· 1-6
1.3.6 配置文件 ····· 1-6
1.4 通过Web网管登录交换机典型配置举例 ····· 1-7
1.4.1 适用产品和版本 ····· 1-7
1.4.2 组网需求 ····· 1-7
1.4.3 配置思路 ····· 1-7
1.4.4 配置步骤 ····· 1-7
1.4.5 验证配置 ····· 1-8
1.4.6 配置文件 ····· 1-8

1 登录交换机典型配置举例

1.1 简介

本章介绍登录交换机的几种方法，其中包括通过 console 口登录、通过 Telnet 登录、通过 Web 网管登录。

1.2 通过Console口登录交换机典型配置举例

1.2.1 适用产品和版本

表1 配置适用的产品与软件版本关系

产品	软件版本
S10500系列以太网交换机	Release 1120系列，Release 1130系列，Release 1200系列
S5800&S5820X系列以太网交换机	Release 1808
S5830系列以太网交换机	Release 1115，Release 1118
S5500-EI&S5500-SI系列以太网交换机	Release 2220

1.2.2 组网需求

如 图 1所示，PC机的串口通过配置电缆与设备的Console口连接。现要求用户能通过设备的Console口登录到交换机，并且下次通过Console口登录时需要本地认证，以提高设备的安全性。

图1 通过 Console 口登录交换机的组网图

1.2.3 配置思路

- 缺省情况下，用户通过 Console 口登录，认证方式为 none（即不需要进行认证）。因此，只要用户终端的通信参数配置和交换机 Console 口的缺省配置保持一致，就能通过 Console 口登录到以太网交换机上。交换机 Console 口的缺省配置如下：

表2 交换机 Console 口缺省配置

属性	缺省配置
传输速率	9600bit/s
流控方式	不进行流控
校验方式	不进行校验

属性	缺省配置
停止位	1
数据位	8

- 要对下次 Console 口登录的用户进行本地认证，需配置 Console 口登录的认证方式为 **scheme**，并且需要创建本地用户和设置用户密码。
- 缺省情况下，本地用户无服务类型，能够访问的命令级别为 0。因此，需要设置本地用户的服务类型为 terminal，能够访问的命令级别为 3，才能使用户成功登录并在登录后对设备进行管理和配置。

1.2.4 配置步骤

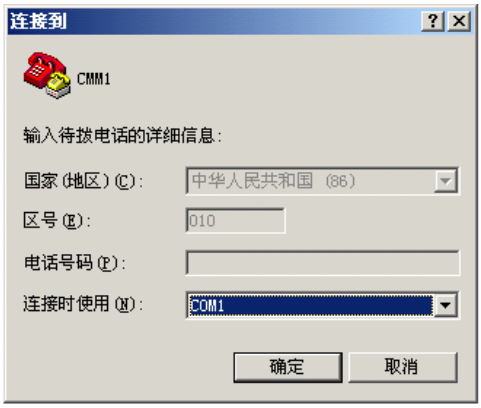
在PC机上运行终端仿真程序（如Windows XP/Windows 2000 的超级终端等，以下配置以Windows XP为例），选择与交换机相连的串口，如 图 2 至 图 3 所示。

说明

如果您的 PC 使用的是 Windows Server 2003 操作系统，请在 Windows 组件中添加超级终端程序后，再按照本文介绍的方式登录和管理交换机；如果您的 PC 使用的是 Windows Server 2008、Windows 7 、Windows Vista 或其它操作系统，请您准备第三方的终端控制软件，使用方法请参照软件的使用指导或联机帮助。

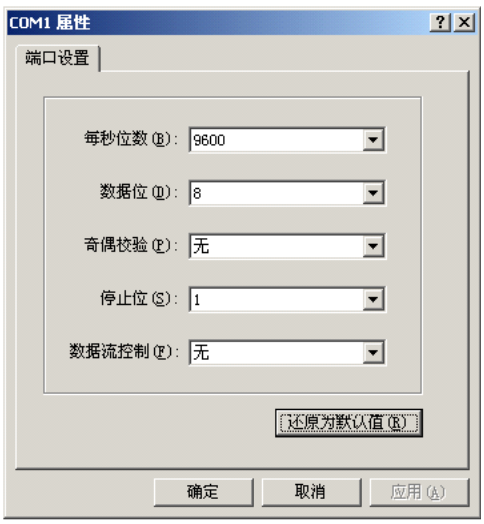
图2 新建连接

图3 连接端口设置



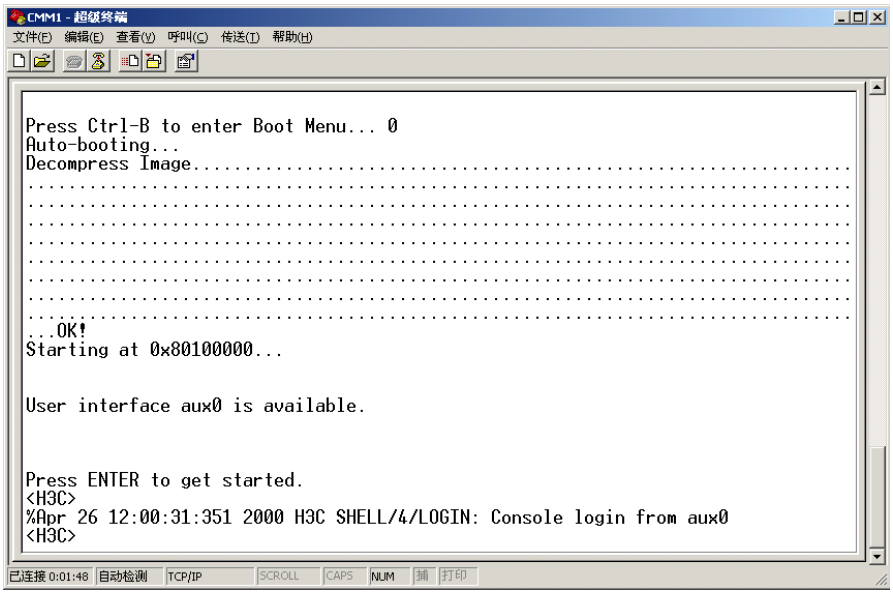
设置终端通信参数：传输速率为 9600bit/s、8 位数据位、1 位停止位、无校验和无流控，如 图 4 所示。

图4 端口通信参数设置



以太网交换机上电，终端上显示设备自检信息，自检结束后提示用户键入回车，之后将出现命令行提示符（如<H3C>），如 图 5 所示。输入命令，配置交换机或查看交换机运行状态。需要帮助可以随时键入“?”。

图5 以太网交换机配置界面



进入 AUX 用户界面视图

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
```

设置通过 Console 口登录交换机的用户进行 Scheme 认证

```
[Sysname-ui-aux0] authentication-mode scheme
[Sysname-ui-aux0] quit
```

进入系统视图，创建本地用户 admin，并进入本地用户视图

```
[Sysname] local-user guest
New local user added.
```

设置本地用户的认证口令为明文方式，口令为 Admin1234)

```
[Sysname-luser-guest] password simple Admin1234)
```

设置本地用户的服务类型为 Terminal 且用户级别为 3

```
[Sysname-luser-guest] service-type terminal
[Sysname-luser-guest] authorization-attribute level 3
[Sysname-luser-guest] quit
```

1.2.5 验证配置

配置完成后，当用户再次通过 Console 口登录设备时，键入回车后，设备将要求用户输入登录用户名和密码，正确输入用户名和密码并回车，登录界面中将出现命令行提示符（如<H3C>）。

1.2.6 配置文件

```
#
local-user guest
 password cipher $c$3$wI+ls++f5LrYDLV7fR5DTEvRniz/+tHtbnYLbio=
 authorization-attribute level 3
```

```
 service-type terminal
#
user-interface aux 0
 authentication-mode scheme
```

1.3 通过Telnet方式登录交换机典型配置举例

1.3.1 适用产品和版本

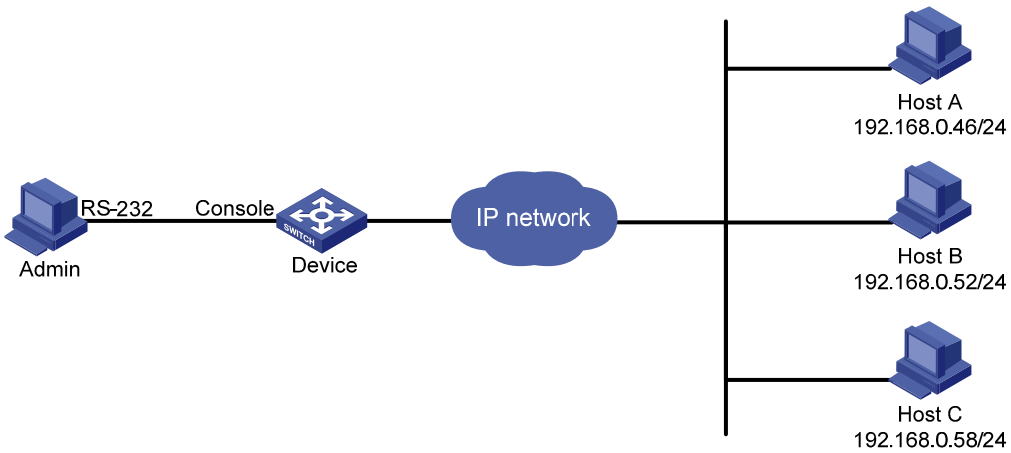
表3 配置适用的产品与软件版本关系

产品	软件版本
S10500系列以太网交换机	Release 1120系列，Release 1130系列，Release 1200系列
S5800&S5820X系列以太网交换机	Release 1808
S5830系列以太网交换机	Release 1115，Release 1118
S5500-EI&S5500-SI系列以太网交换机	Release 2220

1.3.2 组网需求

如 图 6 所示，Host A、Host B、Host C到Device均路由可达。现要求仅允许来自源IP为 192.168.0.46 和 192.168.0.52 的Telnet用户无需认证就能登录设备，并且在登录后对设备进行管理和配置。

图6 通过 Telnet 登录交换机配置



1.3.3 配置思路

- 缺省情况下，设备的 Telnet 服务处于关闭状态，因此需要通过 Console 登录后开启设备的 telnet 服务功能。
- 缺省情况下，通过 VTY 用户界面登录系统所能访问的命令级别是 0。因此，需要设置 VTY 用户的命令级别为 3，才能使用户对设备进行管理和配置。

1.3.4 配置步骤

进入系统视图，开启 Telnet 服务

```
<Sysname> system-view
[Sysname] telnet server enable
```

设置通过 VTY 用户界面登录交换机的 Telnet 用户不需要进行认证

```
[Sysname] user-interface vty 0 15
[Sysname-ui-vty0-15] authentication-mode none
```

配置从 VTY 用户界面登录后可以访问的命令级别为 3 级

```
[Sysname-ui-vty0-15] user privilege level 3
```

创建并进入基本 ACL 视图 2000

```
[Sysname] acl number 2000
[Sysname-acl-basic-2000]
```

定义规则，仅允许来自 192.168.0.52 和 192.168.0.46 的 Telnet 用户访问交换机。

```
[Sysname-acl-basic-2000] rule 1 permit source 192.168.0.52 0
[Sysname-acl-basic-2000] rule 2 permit source 192.168.0.46 0
[Sysname-acl-basic-2000] rule 3 deny source any
[Sysname-acl-basic-2000] quit
```

引用访问控制列表 2000，通过源 IP 对 Telnet 用户进行控制

```
[Sysname] user-interface vty 0 15
[Sysname-ui-vty0-15] acl 2000 inbound
```

1.3.5 验证配置

配置完成后，Host A 与 Host B 能通过 Telnet 登录设备，但 Host C 无法通过 Telnet 登录设备。

1.3.6 配置文件

```
#
 telnet server enable
#
acl number 2000
 rule 1 permit source 192.168.0.52 0
 rule 2 permit source 192.168.0.46 0
 rule 3 deny
#
user-interface vty 0 15
 acl 2000 inbound
 authentication-mode none
 user privilege level 3
#
```

1.4 通过Web网管登录交换机典型配置举例

1.4.1 适用产品和版本

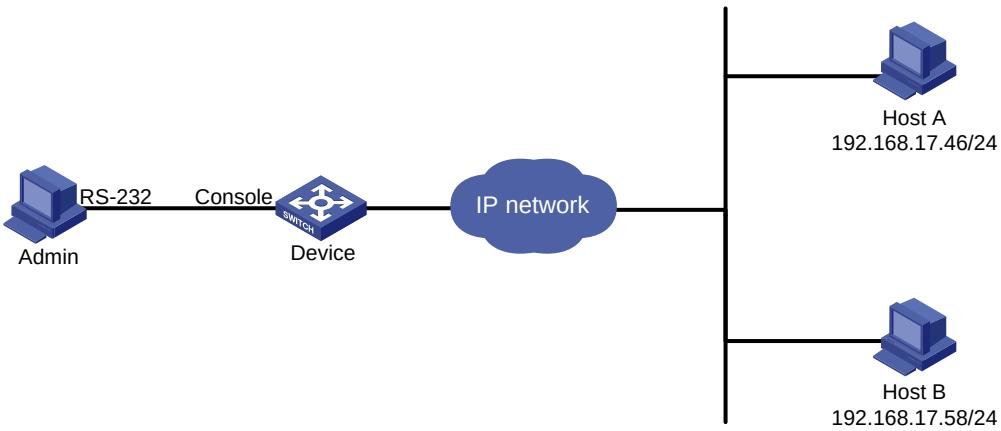
表4 配置适用的产品与软件版本关系

产品	软件版本
S5800&S5820X系列以太网交换机	Release 1808
S5830系列以太网交换机	Release 1115，Release 1118
S5500-EI&S5500-SI系列以太网交换机	Release 2220

1.4.2 组网需求

如 图 7 所示，Host A、Host B到Device均路由可达。某管理员想使用Web网管登录交换机，以实现对交换机的远程管理。出于安全考虑，需要对通过Web网管登录的用户进行控制，仅允许来自源IP为 192.168.17.0 网段的Web用户登录交换机。

图7 通过 Web 网管登录交换机配置示意图



1.4.3 配置思路

- 缺省情况下，用户不能通过 Web 登录到设备上，需要通过 Console 口登录到设备上，开启设备的 Web 登录功能（开启 http 或 https 协议）。本例以 http 协议为例。
- 要使用户能通过 Web 登录设备需创建本地用户和本地认证密码，并且配置用户的服务类型和 Web 登录的用户级别，

1.4.4 配置步骤

开启交换机的 Web Server 功能。

```
<Sysname> system-view
[Sysname] ip http enable
```

配置 Web 网管用户名为 admin，认证口令为 admin。

```
[Sysname] local-user admin
[Sysname-luser-admin] password simple admin
```

配置用户的服务类型为 Web，用户级别为 3 级。

```
[Sysname-luser-admin] service-type web
[Sysname-luser-admin] authorization-attribute level 3
[Sysname-luser-admin] quit
```

定义基本访问控制列表。

```
[Sysname] acl number 2030
[Sysname-acl-basic-2030] rule 1 permit source 192.168.17.0 0.0.0.255
```

引用访问控制列表，仅允许来自 192.168.17.0 网段的 Web 用户访问交换机。

```
[Sysname] ip http acl 2030
```

1.4.5 验证配置

通过浏览器登录交换机，在 Web 网管终端(PC)的浏览器地址栏内输入 http://192.168.17.52（Web 网管终端和以太网交换机之间要路由可达），浏览器会显示 Web 网管的登录页面。

输入在设备上添加的用户名 admin 和密码 admin、以及提示的验证码，点击<登录>按钮后即可登录，显示 Web 网管初始页面。

1.4.6 配置文件

```
#
 ip http acl 2030
 ip http enable
#
acl number 2030
 rule 1 permit source 192.168.17.0 0.0.0.255
#
local-user admin
 password cipher $c$3$jHCLjGzr9htQVvu616OmnfD+s73he3iO
 authorization-attribute level 3
 service-type web
#
```