锐捷 S3550　配置手册

第一部分：交换机概述

一：交换机的几种配置方法

本部分包括以下内容：

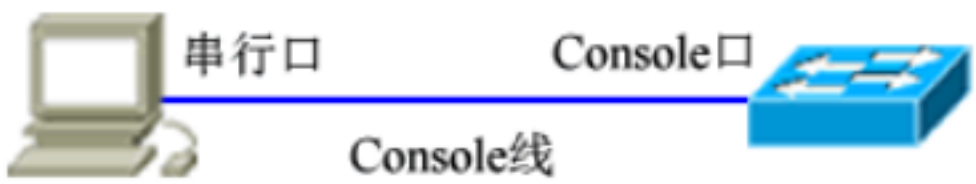
控制台

远程登录

其它配置方法

本部分内容适用于交换机、路由器等网络设备。

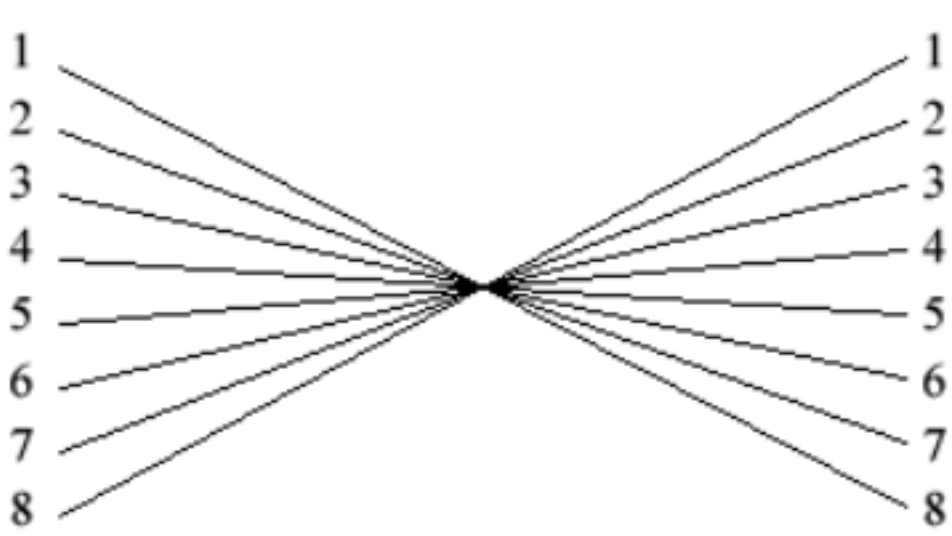
控制台



1、硬件连接：

把 Console　线一端连接在计算机的串行口上，另一端连接在网络设备的　　Console　口上。

Console　线在购置网络设备时会提供，它是一条反转线，你也可以自己用双绞线进行制作。



按照上面的线序制作一根双绞线，一端通过一个转接头连接在计算机的串行口上，另一端连接在网络设备的 Console 口上。

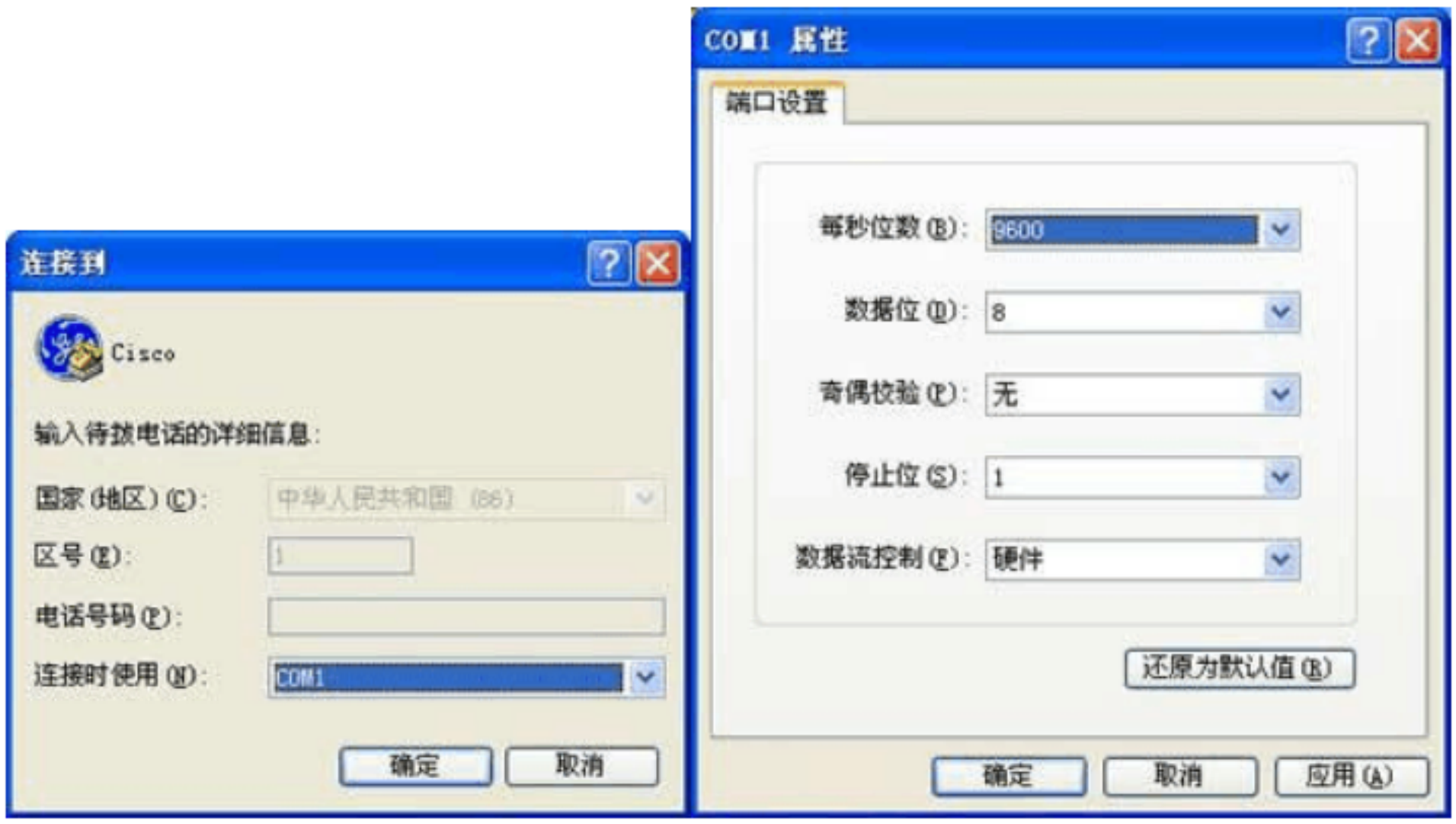
注意：不要把反转线连接在网络设备的其他接口上，这有可能导致设备损坏。

2、软件安装：

在计算机上需要安装一个终端仿真软件来登录网络设备。 通常我们使用 Windows 自带的“超级终端”。超级终端的安装方法：

开始 | 程序 | 附件 | 通信 | 超级终端。

按照提示的步骤进行安装，其中连接的接口应选择 “COM1”，端口的速率应选择 “9600”，数据流控制应选择 “无”，其它都使用默认值。



登录后，就可以对网络设备进行配置了。

说明：超级终端只需安装一次， 下次再使用时可从 “开始 | 程序 | 附件 | 通信 | 超级终端”中找到上次安装的超级终端，直接使用即可。

远程登录

通过一台连接在网络中的计算机，用　Telnet　命令登录网络设备进行配置。

远程登录条件：

1、网络设备已经配置了　IP 地址、远程登录密码和特权密码。

2、网络设备已经连入网络工作。

3、计算机也连入网络，并且可以和网络设备通信。

说明：远程登录的计算机不是连接在网络设备　Console　口上的计算机，而是网络中任一台计算机。

远程登录方法：

在计算机的命令行中，输入命令　‘telnet　网络设备 IP 地址 ”，输入登录密码就可以进入网络设备的命令配置模式。

说明：远程登录方式不能用来配置新设备，新设备应该用控制台配置　IP 地址等参数，以后才能使用远程登录进行配置。

其它配置方法

除了控制台和远程登录之外，还有其它一些配置方法配置网络设备。

1、TFTP　服务器：

TFTP 服务器是网络中的一台计算机，　你可以把网络设备的配置文件等信息备份到　TFTP 服务器之中，也可以把备份的文件传回到网络设备中。

由于设备的配置文件是文本文件，所以，你可以用文本编辑软件打开进行修改，再把修改后的配置文件传回网络设备，这样就可以实现配置功能。你也可以用　TFTP 服务器把一个已经做好的配置文件上传到一台同型号的设备中实现对它的配置。

2、SSH ：

SSH 是一种安全的配置手段，其功能类似于远程登录。与　Telnet　不同的是，SSH 传输中所

有信息都是加密的，所以如果需要在一个不能保证安全的环境中配置网络设备，最好使用SSH。

3、Web ：

有些种类的设备支持 Web 配置方式，你可以在计算机上用浏览器访问网络设备并配置。

Web 配置方式具有较好的直观性，用它可观察到设备的连接情况。

二：命令行 (CLI) 操作

本部分包括以下内容：

命令模式

交换机和路由器的命令是按模式分组的，每种模式中定义了一组命令集，所以想要使用某个命令，必须先进入相应的模式。各种模式可通过命令提示符进行区分，命令提示符的格式是：

提示符名 模式

提示符名一般是设备的名字，交换机的默认名字 “ Switch ”，路由器的默认名字是 “ Router ”（锐捷设备的默认名字是 “ Ruijie ）”，提示符模式表明了当前所处的模式。如： “ > ”代表用户模式， “ # ”代表特权模式。

以下是常见的几种命令模式：

模式	提示符	说明

User EXEC 用户模式	>	可用于查看系统基本信息和进行基本测试
Privileged EXEC 特权模式	#	查看、保存系统信息，该模式可使用密码保护
Global configuration 全局配置模式	(config)#	配置设备的全局参数
Interface configuration 接口配置模式	(config-if)#	配置设备的各种接口
Line configuration 线路配置模式	(config-line)#	配置控制台、远程登录等线路
Router configuration 路由配置模式	(config-router)#	配置路由协议
Config-vlan VLAN 配置模式	(config-vlan)#	配置 VLAN 参数

命令模式的切换

交换机和路由器的模式大体可分为四层：用户模式→特权模式→全局配置模式→其它配置模式。

进入某模式时，需要逐层进入。

要求	命令举例	说明
进入用户模式		登录后就进入

进入特权模式	Ruijie> enable Ruijie#	在用户模式中输入 enable 命令
进入全局配置模式	Ruijie# configure terminal Ruijie(config)#	在特权模式中输入 conf t 命令
进入接口配置模式	Ruijie(config)# interface f0/1 Ruij e(config-if)#	在全局配置模式中输入 interface 命令，该命令可带不同参数
进入线路配置模式	Ruijie(config)# line console 0 Ruijie(config-line)#	在全局配置模式中输入 line 命令，该命令可带不同参数
进入路由配置模式	Ruijie(config)# router rip Ruijie(config-router)#	在全局配置模式中输入 router 命令，该命令可带不同参数
进入 VLAN 配置模式	Ruijie(config)# vlan 3 Ruijie(config-vlan)#	在全局配置模式中输入 vlan 命令，该命令可带不同参数
退回到上一层模式	Ruijie(config-if)# exit Ruijie(config)#	用 exit 命令可退回到上一层模式
退回到特权模式	Ruijie(config-if)# end Ruijie#	用 end 命令或 Ctrl+Z 可从各种配置模式中直接退回到特权模式
退回到用户模式	Ruijie# disable Ruijie>	从特权模式退回到用户模式

说明： interface 等命令都是带参数的命令，应根据情况使用不同参数。

特例： 当在特权模式下输入 Exit 命令时，会直接退出登录，不是回到用户模式。从特权模式返回用户模式的命令是 disable 。

CLI 命令的编辑技巧

CLI （命令行）有以下特点。

1、命令不区分大小写。

2、可以使用简写。

命令中的每个单词只需要输入前几个字母。 要求输入的字母个数足够与其它命令相区分即可。
如：configure terminal 命令可简写为 conf t 。

3、用 Tab 键可简化命令的输入。

如果你不喜欢简写的命令，可以用 Tab 键输入单词的剩余部分。每个单词只需要输入前几个字母，当它足够与其它命令相区分时， 用 Teb 键可得到完整单词。 如：输入 conf(Tab) t(Tab) 命令可得到 configure terminal 。

4、可以调出历史来简化命令的输入。

历史是指你曾经输入过的命令， 可以用“↑”键和“↓”键翻出历史命令再回车就可执行此命令。（注：只能翻出当前提示符下的输入历史。）

系统默认记录的历史条数是 10 条，你可以用 history size 命令修改这个值。

5、编辑快捷键：

Ctrl+A ——光标移到行首， Ctrl+E ——光标移到行尾。

6、用“ ?可帮助输入命令和参数。

在提示符下输入 “ ?可查看该提示符下的命令集，在命令后加 “ ?,” 可查看它第一个参数，在参数后再加“ ?,” 可查看下一个参数，如果遇到提示 “ <cr> ”表示命令结束，可以回车了。

常见 CLI 错误提示

% Ambiguous command: "show c"

用户没有输入足够的字符，设备无法识别唯一的命令。

% Invomplete command.

命令缺少必需的关键字或参数。

% Invalid input detected at '^' marker.

输入的命令错误，符号　^　指明了产生错误的单词的位置

使用　no　和　default　　选项

很多命令都有　no　选项和　default　　选项。

no　选项可用来禁止某个功能，或者删除某项配置。

default　选项用来将设置恢复为缺省值。

由于大多数命令的缺省值是禁止此项功能，这时　　default　选项的作用和　no　选项是相同的。但部分命令的缺省值是允许，这时　default　选项的作用和　no　选项的作用是相反的。

no　选项和　default　选项的用法是在命令前加　no　或　defaule　前缀。如：

no shutdown

no ip address

default hostname

相比之下，我们多使用　no　选项来删除有问题的配置信息。

三：交换机的初始化配置

本部分包括以下内容：

交换机的初始化配置

setup　命令

交换机的初始化配置

新出厂的交换机没有配置文件，或者你删除了交换机的配置文件，在用控制台登录时，可以进行一些基础配置， 你可以在此处配置一些基本参数。 （注：有些设备没有 setup 配置模式，它在没有配置文件时会自动按照缺省值启动。）

把控制台连接到交换机上，打开超级终端，如果交换机中没有配置文件，就会进入 setup 配置模式：

```
--- System Configuration Dialog ---
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Continue with configuration dialog? [yes/no]:                    y
Enter IP address:        192.168.1.5
Enter IP netmask:        255.255.255.0
Enter host name [Switch]:
The enable secret is a one-way cryptographic secret use
instead of the enable password when it exists.
Enter enable secret:        123
Would you like to configure a Telnet password? [yes/no]:                    y
Enter Telnet password:        456
Would you like to disable web service? [yes/no]:                    y
The following configuration command script was created:

interface VLAN 1
ip address 192.168.1.5 255.255.255.0
!
enable secret 5 $xH.Y*T7xC,tz[V/xD+S(\W&xG1X)sv'
!
end
Use this configuration? [yes/no]:                y

Building configuration...
OK
```

在上面的配置中，依次配置了管理 IP、子网掩码、交换机名、特权密码、远程登录密码等，并且关闭了 Web 服务。最后一步选择 “ yes ”则交换机把生成的配置文件应用于交换机。

setup 命令

如果交换机已经有配置文件，你可以用　setup　命令初始化它。

模式： 特权模式。

配置命令：

Switch#　setup

此时就会重复上面的步骤，配置交换机的初始参数。

注意： setup　命令生成的配置文件会覆盖原有配置文件，所以这种方法可用于删除原来的配置文件，使交换机恢复到比较初始的状态。

说明： 有些设备没有　setup　配置模式，你可以用删除命令删除它的配置文件，在启用时它会自动按照缺省值启动。

四：配置文件的保存、查看与备份

本部分包括以下内容：

查看配置文件

保存配置文件

删除配置文件

备份配置文件

交换机和路由器都有两个配置文件：

1、运行配置文件：

这个文件位于　RAM 中，名为　running-config　　。它是设备在工作时使用的配置文件。

2、启动配置文件：

这个文件位于　NVRAM　中，名为　startup-config　　。当设备启动时，它被装入　RAM，成为运行配置文件。

新出厂的交换机或路由器是没有配置文件的，当我们第一次配置它时会进入　　setup　方式配

置一些基本信息，这些信息就生成了 running-config ，我们以后所做的配置信息都会添加到 running-config 中。（注：有些设备没有 setup 配置模式，它在没有配置文件时会自动按照缺省值启动。）

由于 RAM 中的运行配置文件在断电或重启时就会消失，所以我们在配置好设备后，应该把配置文件保存到 NVRAM 中，这样配置文件就可以长期使用了。

从效果上讲， RAM 相当于设备的内存， NVRAM 相当于设备的硬盘， 把 running-config 保存为 startup-config 相当于一个存盘过程。

查看配置文件

模式： 特权配置模式。

查看运行配置文件：

```
Ruijie# show running-config
```

或者：

```
Ruijie# write terminal
```

查看启动配置文件：

```
Ruijie# show startup-config
```

show running-config 命令和 write terminal 命令的效果是完全相同的。

保存配置文件

保存配置文件就是把 running-config 保存为 startup-config 。

模式： 特权配置模式。

命令 1：

Ruijie# copy running-config startup-config

命令 2：

Ruijie# write

write 命令与 copy running-config startup-config 命令的功能相同，它是人们习惯使用的一种简化写法。

删除配置文件

删除配置文件就是把 NVRAM 中的 startup-config 删除。

模式： 特权配置模式。

命令：

Ruijie# delete flash:config.text

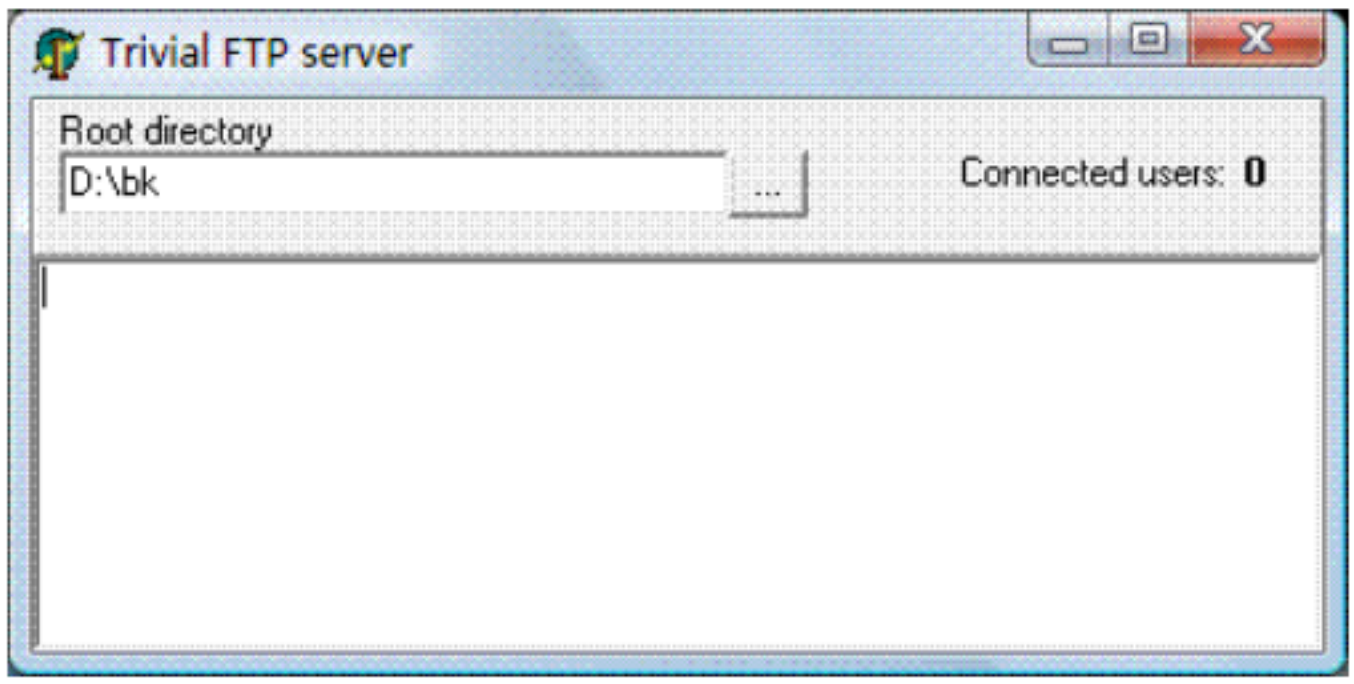
说明： config.text 是配置文件在 NVRAM 中的文件名，它被删除后，再重启设备时会自动进入 setup 配置模式。

注： 有些设备没有 setup 配置模式，它在没有配置文件时会自动按照缺省值启动。

备份配置文件

通常我们把配置文件备份到 TFTP 服务器上，在需要时可以再从 TFTP 服务器上把配置文件回传到设备中。

准备： 在作为 TFTP 服务器的计算机上打开 TFTP 服务器软件，并设置存放文件的路径（如下图）。然后在交换机或路由器上进行以下操作。



模式： 特权配置模式。

命令：

```
Ruijie#  copy running-config tftp
Address or name of remote host [ ]?          192.168.0.2
Destination filename [ ]?       S1-config.txt
```

说明： 输入 copy 命令后还需要回答两个问题，一是 TFTP 服务器的地址，本例中假设为 192.168.0.2 ，二是备份的配置文件名， 本例中假设为 S1-config.txt 。备份成功后， 在 TFTP 服务器指定的目录中可看到此文件。

从 TFTP 服务器回传配置文件：

```
Ruijie#  copy tftp running-config
Address or name of remote host [ ]?          192.168.0.2
Source filename [ ]?       S1-config.txt
```

说明： 有些设备不支持备份 running-config 文件，但支持备份 startup-config 文件。

五：文件系统

本部分包括以下内容：

文件系统概述

交换机和路由器用一个并行 Flash 作为辅助存储器存储文件， Flash 是一个可读可写的存储器，设备断电后， Flash 的内容不会丢失，所以在交换机和路由器中 Flash 可被当作硬盘使用，用于存放需要长期保存的信息。

Flash 中的文件主要包括：

1、主体文件

这个文件相当于交换机或路由器的操作系统，它的扩展名一般为 bin 或 upd，bin 文件是一个单独的文件，而 upd 文件是由多个文件打包而成，包含了 bin 文件和 Web 配置等文件。

主体文件很大，一般存放在 Flash 的根目录中。它是管理软件运行的主程序，如果该文件被删除或被破坏，设备将不能启动，开机后会进入 ROM 模式。

2、启动配置文件

这个文件由 CLI 命令组成，文件名一般为 config.text ，它是一个文本文件。该文件就是我们在命令行中使用的 startup-config ，在设备启动时，该文件被装入 RAM 成为 running-config ，设备执行其中的 CLI 命令完成初始化。

新设备是没有 config.text 文件的，此时，设备所有参数都采用缺省配置，有些种类的设备在启动时会进入 setup 模式，用户配置一些基本参数后，就生成了 config.text 文件。

你也可以在特权模式下用 setup 命令来初始化配置文件，它可以清除原来的配置文件，生成一个只有几项基本参数的配置文件。

几点说明：

1、文件名对大小写不敏感，文件名长度不能超过 23 个字符。

2、不要删除主程序文件，它会导致设备不能启动。

3、可以删除启动配置文件，用这种方法可以把设备恢复到缺省状态。

4、Flash 中的文件有两种状态：激活状态和删除状态。当删除一个文件时，该文件只是被标记为删除，但仍然在 Flash 中，我们可以使用碎片整理功能把处于删除状态的文件彻底删除，腾出空间保存新文件。

文件操作

所有文件操作都是在特权模式下进行。

1、查看 Flash 中文件目录：

Ruijie# dir

```
Ruijie#    dir
Directory of flash:/
<DIR>                       Dec 11 2002        09:41:34          temp
-rw-              511       Dec 11 2002        10:11:08          conf_bak.text
-rw-             1002       Jan 15 2003        09:20:19          config.text
-rw-          2833568        Jan 14 2003        19:21:37          cs3550b.bin
-rw-               80       Jan 14 2002        08:50:24          vlan.dat
```

列表中列出的是处于激活状态的文件信息。

Ruijie# dir delete

该命令用于查看处于删除状态的文件信息。

2、删除文件：

Ruijie# delete flash: filename

filename 是删除的文件名。例如：

```
Ruijie#    delete flash:conf_bak.text
```

删除的文件名被标记为删除状态，用 dir delete 命令可以看到。

3、查看文件内容：

Ruijie# more flash: filename

filename 是文件名。例如：

```
Ruijie# more flash:config.text
```

本命令只能查看文本文件。

4、重命名文件：

Ruijieh# rename flash: filename flash: newname

filename 是原文件名， newname 是新文件名。例如：

```
Ruijie# rename flash:config.text flash:config.old
```

对主体文件的重命名要谨慎，它会导致设备复位后不能启动。

5、碎片整理：

Ruijieh# squeeze flash:

碎片整理可以把处于删除状态的文件彻底清除，腾出空间保存新文件。

6、格式化：

Ruijieh# format flash:

格式化会清除 Flash 中所有文件，它会导致设备复位后不能启动，要慎重使用。

目录操作

Flash 中的文件可以使用树形的目录结构，文件可以存放在不同的子目录中，也可以在目录之间移动、复制文件。

所有目录操作都是在特权模式下进行。

1、创建目录：

Ruijie# mkdir directory

directory 是要创建的目录名称。例如：

```
Ruijie# mkdir txt
```

表示在当前目录中创建一个名为 txt 的子目录。

2、切换目录：

Ruijie# cd directory

directory 是要进入的目录名称。 其中当前目录用 “ 表示，上级目录用 “ ..表示，根目录用 “ / ” 表示。例如：

①进入 txt 目录：

```
Ruijie# cd txt
```

②返回上一级目录：

```
Ruijie# cd ..
```

③返回根目录：

```
Ruijie# cd /
```

注意：在 cd 后要有空格，用 cd/ 是错误的。

3、删除目录：

Ruijieh# rmdir directory

directory 是要删除的目录名称。

注意：本命令只能删除空目录。例如：

```
Ruijie# rmdir txt
```

4、查看目录下的文件：

Ruijie# ls pathname

pathname 是路径名，如果省略路径，则显示当前目录下的文件。例如：

```
Ruijie# ls
```

显示当前目录下的文件列表。

5、复制文件：

把文件从一个目录复制到另一个目录中。

Ruijieh# cp sour pathname dest pathname

sour pathname 是源文件， dest pathname 是目的文件。例如：

```
Ruijie# cp sour c1.txt dest ./txt/c1.txt
```

表示把当前目录中的 c1.txt 复制到 txt 子目录中。

注意： cp 命令不支持通配符，也不支持目录的复制。

6、移动文件：

把文件从一个目录移动到另一个目录中。

Ruijieh# mv sour pathname dest pathname

sour pathname 是源文件， dest pathname 是目的文件。例如：

```
Ruijie# mv sour c1.txt dest ./txt/c1.txt
```

表示把当前目录中的 c1.txt 移动到 txt 子目录中。

7、删除文件：

Ruijieh# rm filename

filename 是要删除的文件名。例如：

```
Ruijie# rm c1.txt
```

表示删除当前目录中的 c1.txt 文件。

六：系统文件的备份与升级

本部分包括以下内容：

搭建环境

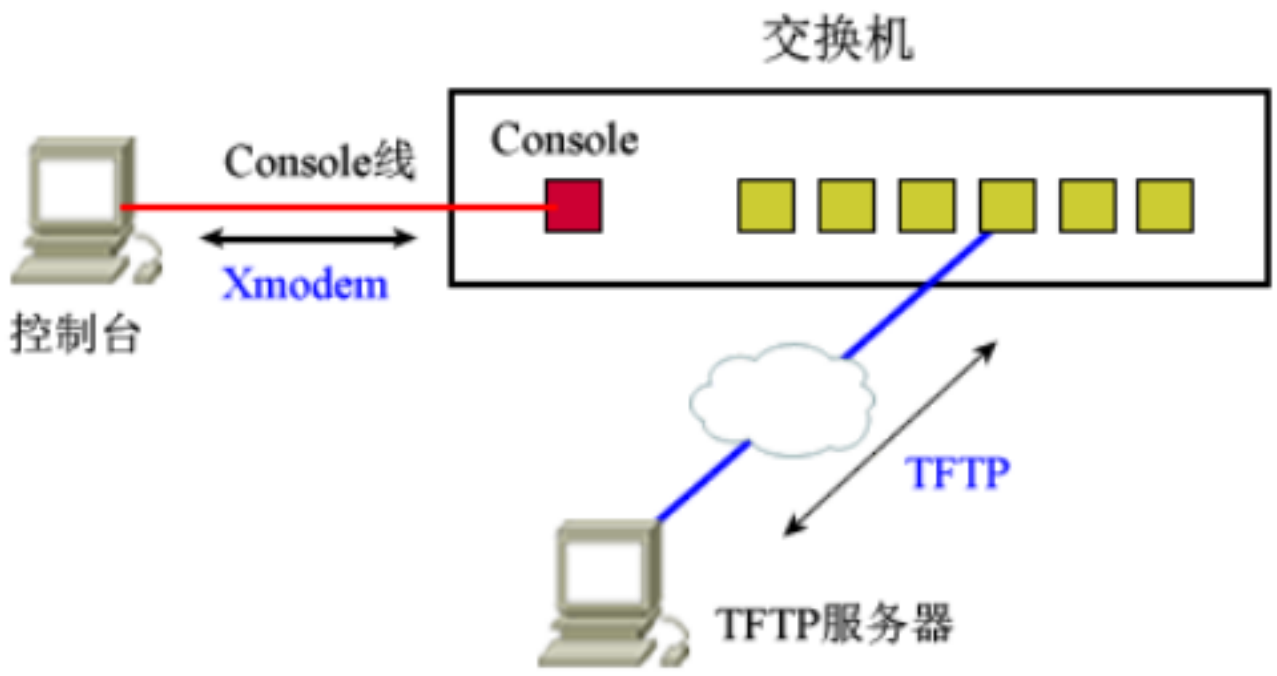
用 TFTP 传输文件

用 Xmodem 传输文件

ROM 监控模式

搭建环境

在备份和升级时需要搭建通信环境，让设备和计算机间可以传输文件。有三个方案：



方案一： TFTP

计算机是通过网络访问设备的。要求设备已经配置了 IP 地址，且可以与计算机正常通信。 计算机上应该运行 TFTP 服务器软件。

方案二： Xmodem

计算机是通过 Console 线连接在设备上。要求在计算机上运行终端仿真软件 （如：超级终端），设备可以没有 IP 地址。

利用 TFTP 和 Xmodem 都可以实现在设备和计算机间传输文件， 两者的区别在于， TFTP 是

通过网络传输数据的， Xmodem 是通过 Console 线传输数据的。

相比之下， Xmodem 的传输速度较慢，而且不能进行远程传输，所以在传输较大的文件时建议使用 TFTP。

方案三： ROM 监控模式

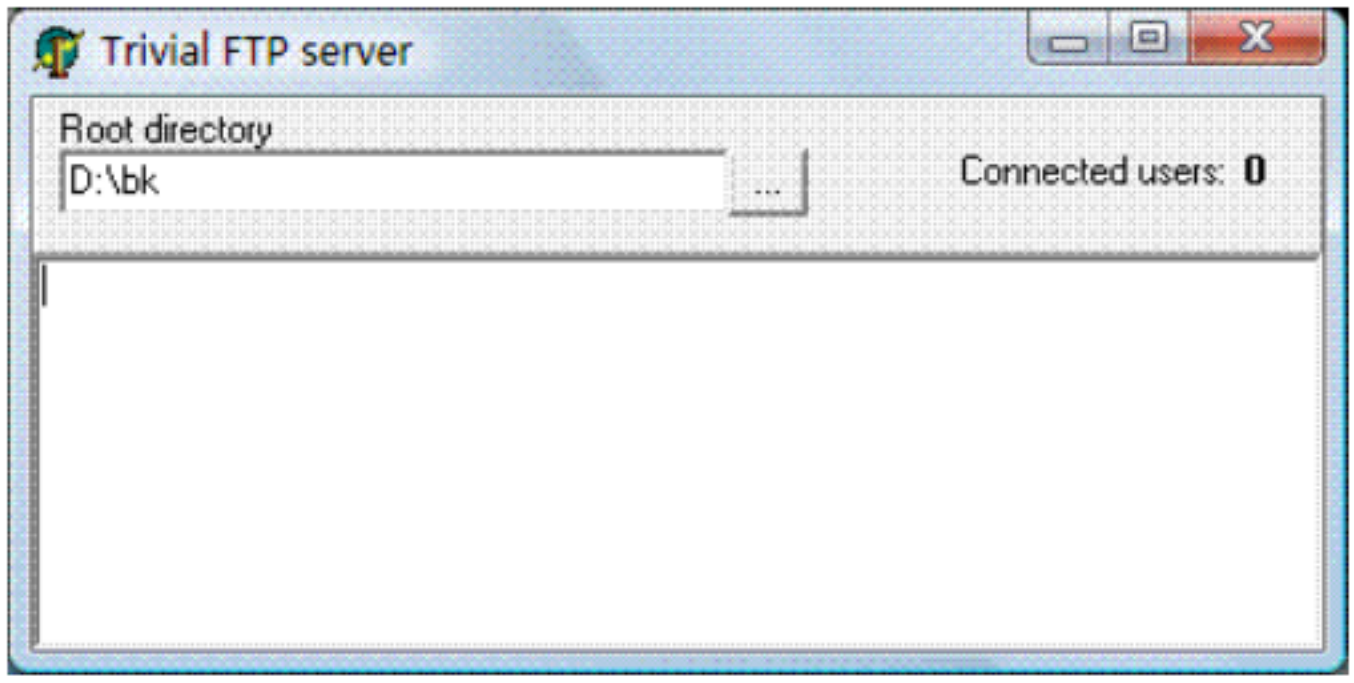
如果交换机或路由器的主体文件损坏了，在设备启动时会进入 ROM 监控模式，在此模式下可以用 TFTP 或 Xmodem 向设备传输文件

用 TFTP 传输文件

准备工作：

1、设备已经配置了 IP 地址，且可以与计算机正常通信（可以用 ping 命令检查）。

2、在计算机上运行 TFTP 服务器软件，并设置好文件保存的路径。如下图：



把设备中的文件传输到计算机中：

用控制台或 Telnet 登录设备，然后在特权模式下执行以下命令：

Ruijie# copy filename tftp

filename 是交换机或路由器上的文件。例如：

① 把 running-config 传输到计算机中

```
Ruijie#  copy running-config tftp
Address or name of remote host [ ]?          192.168.1.2
Destination filename [ ]?        S1-config.txt
```

192.168.1.2 是目的计算机的 IP 地址，应根据实际情况设置。 S1-config.txt 是在计算机上保存的文件名，可自行命名。

以上操作也可以直接写作：

```
Ruijie#  copy running-config tftp://192.168.1.2/S1-config.txt
```

② 把主体文件传输到计算机中

```
Ruijie#  copy flash:cs3550b.bin tftp
Address or name of remote host [ ]?          192.168.1.2
Destination filename [ ]?        cs3550b.bin
```

主体文件的扩展名一般是 bin，不同型号的设备文件名有所不同，应先用 dir 命令查看后再备份。

以上操作也可以直接写作：

```
Ruijie#  copy flash:cs3550b.bin tftp://192.168.1.2/cs3550b.bin
```

注意：由于在设备中，主体文件有固定的名字，为了方便以后的回传，最好使用相同的名字备份，且要做好记录。

其它文件的传输方法和以上实例类似。

把计算机中的文件回传到设备中：

① 把计算机中备份的配置文件回传到设备中

```
Ruijie#  copy tftp running-config
Address or name of remote host [ ]?          192.168.1.2
Source filename [ ]?        S1-config.txt
```

本例把计算机中的 S1-config.txt 文件回传到设备中，使它成为 running-config 。

② 把计算机中备份的主体文件回传到设备中

```
Ruijie#  copy tftp flash:cs3550b.bin
Address or name of remote host [ ]?          192.168.1.2
```

```
Source filename [ ]?        cs3550b.bin
```

注意：各个设备的主体文件有固定的文件名和版本，回传时一定要保证版本正确，文件名正确，不然会导致设备复位后不能启动。

③ 把计算机中打包的主体文件回传到设备中

有些型号的设备主体文件的扩展名为 udp，该文件实际上是一个软件包， 里面包含了 bin 文件和 Web 配置软件。

udp 文件不能用 copy tftp flash 命令传输，应该使用 copy tftp update 命令传输。

```
Ruijie#  copy tftp update
Address or name of remote host [ ]?              192.168.1.2
Source filename [ ]?        rgnos.upd
```

用 Xmodem 传输文件

准备工作：

1、用 Console 线把设备和计算机连接起来，一端连接在设备的 Consloe 口上，另一端连接在计算机的串行口上。

2、在计算机上运行终端仿真软件（如：超级终端），登录设备。

把文件从设备传输到计算机中

在设备的特权模式下输入命令：

```
Ruijie#  copy flash:config.text xmodem
```

在计算机的超级终端中，选择 “传送”菜单中的“接收文件”功能，在弹出的对话框中设置文件的存放位置，接收协议选择 “Xmodem”，点击“接收”，系统会提示存储于本地的文件名称，设置好后，单击 “确定”按钮开始接收文件。

②把文件从计算机回传到设备中

在设备的特权模式下输入命令：

```
Ruijie#  copy xmode flash:config.text
```

在计算机的超级终端中，选择 “传送”菜单中的“发送文件”功能，在弹出对话框的文件名中设置文件在本机中的位置，协议选择 “Xmodem”，点击“发送”。

本例给出的是 Flash 中的 config.text 文件的传输，其它文件的操作方法与此相同。

ROM 监控模式

进入 ROM 监控模式有两种方法：

1、如果设备在启动时，无法在 Flash 中找到设备的主体文件，便直接进入 ROM 监控模式。

2、用手工进入，先用 Console 线连接设备和计算机，并在计算机上运行终端仿真软件（如：超级终端），然后开启设备，在开机后的 3 秒内按下 Ctrl+C ，便进入 ROM 监控模式了。

进入监控模式后，先显示一些版本信息，然后是主菜单： () 中的蓝字为注解

```
Main Menu:
  1. TFTP Download & Run          (用 TFTP 传入文件并运行 )
  2. TFTP Download & Write Into File          (用 TFTP 传入文件并写入 Flash)
  3. X-Modem Download & Run          (用 Xmodem 传入文件并运行 )
  4. X-Modem Download & Write Into File          (用 Xmodem 传入文件并写入 Flash)
  5. List Active Files          (列出 Flash 中文件信息 )
  6. List Deleted Files          (列出 Flash 中删除文件的信息 )
  7. Run A File          (运行一个文件 )
  8. Delete A File          (删除一个文件 )
  9. Rename A File          (重命名一个文件 )
```

```
a. Squeeze File System          (碎片整理 )
b. Format File System           (格式化  Flash)
c. Other Utilities        (其它 )
d. hardware test
e. TFTP Download & Update          (用 TFTP 传入打包的主体文件   )
f. X-Modem Download & Update              ( 用 Xmodem    传入打包的主体文件   )
Please select an item:
```

选项 1 和选项 2 的区别在于：选项 1 把文件传入到内存中，不写入 Flash ，所以在重启设备后，仍会使用原来的文件；选项 2 是把文件传入内存并写入 Flash ，使它永久有效。

通常，如果我们想要传入一个文件进行测试，应该使用选项 1，如果想要传入一个永久有效的文件，应该使用选项 2。

实例：假设某路由器的主体文件被损坏， 现把 TFTP 服务器上备份的文件传入路由器的 Flash 中，使路由器恢复正常。

启动路由器，由于主体文件损坏，进入 ROM 监控模式，选择项目 2 进行传输。

```
Please select an item:          2
File name[]:       85_1_b10_r36.bin
Local IP[]:       192.168.1.1
Remote IP[]:       192.168.1.2
```

85_1_b10_r36.bin 是主体文件名， Local IP 是路由器 IP 地址，Remote IP 是 TFTP 服务器的 IP 地址，这两个地址必须在同一网络中。然后就开始传输了。其中 TFTP 服务器可按前面的方法设置。

传输完成后，重新开启路由器，就可以使用新的主体文件了。

七：密码丢失的解决方法

如果忘记了路由器或交换机的登录密码，可以用以下方法解决：

用一台计算机作为控制台，用 Console 线连接在设备上，在计算机上运行终端仿真程序（如：超级终端）。

① 重启设备，在超级终端上按下 Ctrl+C ，使设备进入 ROM 监控模式。

```
Main Menu:
  1. TFTP Download & Run
  2. TFTP Download & Write Into File
  3. X-Modem Download & Run
  4. X-Modem Download & Write Into File
```

```
5. List Active Files
6. List Deleted Files
7. Run A File
8. Delete A File
9. Rename A File
a. SqueezeFile System
b. Format File System
c. Other Utilities
d. hardware test
e. TFTP Download & Update
f. X-Modem Download & Update
Please select an item:          5
```

使用项目 5，列出 Flash 中的文件目录，找到其中的配置文件（通常是名为 config.text 的文件）。

② 用项目 9 更改配置文件的文件名。

```
Please select an item:          9
Old file name input.
Enter File Name (Input ESC to quit:             config.text
New file name input.
Enter File Name (Input ESC to quit:             config.bak
```

③ 重启设备，由于找不到配置文件，设备以默认参数启动，此时原有的配置也没有了。

④ 进入特权模式，把原来的配置文件再装入设备。

```
Ruijie>   enable
Ruijie#   copy flash:config.bak running-config
Ruijie#
```

这样就恢复了原来的配置。由于此时已经进入特权模式，可以用命令删除原来的密码，
也可以重新配置新密码。

⑤ 各部分密码都重新配置后，保存配置文件，以后就可以用新密码登录了。

```
Ruijie#   copy running-config startup-config
```

第二部分：交换机的基本配置

一：配置主机名

配置主机名

主机名用于标识交换机和路由器，通常它会作为提示符的一部分显示在命令提示符的前面。

交换机的默认名字一般是 “ Switch ”，路由器的默认名字一般是 “ Router ”。锐捷设备一般把名字默认为“ Ruijie ,”你可以用命令重新设置设备的名字。

1、配置主机名

模式： 全局配置模式。

命令： hostname name

参数： name 是要设置的主机名，必须由可打印字符组成，长度不能超过 255 个字符。

主机名一般会显示在提示符前面，显示时最多只显示 22 个字符。

2、删除配置的主机名

在全局配置模式下，用 no hostname 命令可删除配置的主机名，恢复默认值。

配置举例： 配置交换机的名字为 S3550-1 。

```
Switch>  enable
Switch#  configure terminal
Switch(config)#  hostname S3550-1
S3550-1(config)#
```

二：配置口令

本部分包括以下内容：

配置控制台口令

配置远程登录口令

配置特权口令

口令（密码）可用于防范非法人员登录到交换机或路由器上修改设备的配置。

我们可以在几个不同位置设置口令，以达到多重保护的目的。

控制台口令： 当我们从连接在 Console 口的控制台登录设备时，需要输入控制台口令。由于控制台是一种本地配置方式，所以不设置这个口令影响也不大。

远程登录口令： 当我们从网络中的计算机通过 Telnet 命令登录设备时，需要输入远程登录口令。远程登录是一种远程配置方式，这个口令应该设置。在锐捷设备中，没有设置远程登录口令的设备是不能用 Telnet 命令登录的。

特权口令： 当我们登录设备后，从用户模式进入特权模式，需要输入特权口令。由于特权模式是进入各种配置模式的必经之路， 在这里设置口令可有效防范非法人员对设备配置的修改。在锐捷设备中，特权模式可设置多个级别，每个级别可设置不同的口令和操作权限，你可以根据情况让不同人员使用不同的级别。在锐捷设备中，没有设置特权口令的设备也不能用 Telnet 命令登录。

在实际应用中，一般特权口令和远程登录口令是必需的，设置的口令不应该太简单，不同位置的口令也不应该相同。

配置控制台口令

控制台口令是通过控制台登录交换机或路由器时设置的口令。

1、设置控制台口令

模式： 线路配置模式。

配置命令：

```
Ruijie(config)#      line console 0
Ruijie(config-line)#        login
Ruijie(config-line)#        password    password
```

line console 0　　命令表示配置控制台线路，　　0 是控制台的线路编号。

login　命令用于打开登录认证功能。

password　 password　 为控制台线路设置口令。

说明： 设置的口令长度最大长度为　 25 个字符。口令中不能有问号和其他不可显示的字符。

如果口令中有空格，则空格不能位于最前面，只有中间和末尾的空格可作为口令的一部分。

在 running-config　　中可以查看口令设置，但锐捷设备的口令都是以密文存放的，所以看到的是乱码。

注意： 如果没有设置 login ， 即使配置了口令，登录时口令认证会被忽略。

2、删除配置的控制台口令：

```
Ruijie(config)#      line console 0
Ruijie(config-line)#        no password
```

配置举例：

```
Ruijie>   enable
Ruijie#   configure terminal
Ruijie(config)#       line console 0
Ruijie(config-line)#        login
Ruijie(config-line)#        password 123
Ruijie(config-line)#        end
Ruijie#
```

本例设置控制台口令为　123 。

- 配置远程登录口令

远程登录口令是通过 Telnet 登录交换机或路由器时设置的口令。

1、设置远程登录口令

模式： 线路配置模式。

配置命令：

```
Ruijie(config)#      line vty 0 4
Ruijie(config-line)#        login
Ruijie(config-line)#        password    password
```

line vty 0 4 命令表示配置远程登录线路, 0~4 是远程登录的线路编号。

login 命令用于打开登录认证功能。

password password 为远程登录线路设置口令。

说明： 设置的口令长度最大长度为 25 个字符。口令中不能有问号和其他不可显示的字符。

如果口令中有空格，则空格不能位于最前面，只有中间和末尾的空格可作为口令的一部分。

在 running-config 中可以查看口令设置，但锐捷设备的口令都是以密文存放的，所以看到的是乱码。

注意： 远程登录口令是用 Telnet 登录的必备条件。

2、删除配置的远程登录口令：

```
Ruijie(config)#      line vty 0 4
Ruijie(config-line)#        no password
```

配置举例： 为交换机设置远程登录密码为 123 。

```
Ruijie>   enable
Ruijie#   configure terminal
Ruijie(config)#       line vty 0 4
```

```
Ruijie(config-line)#        login
Ruijie(config-line)#        password 123
Ruijie(config-line)#        end
Ruijie#
```

本例设置远程登录口令为　123 。

配置特权口令

 特权口令是从用户模式进入特权模式时设置的口令。

1、设置特权口令

模式： 全局配置模式。

配置命令：

```
Ruijie(config)#      enable password      password
Ruijie(config)#      enable secret      password
```

enable password　　password　　命令配置的口令在配置文件中是用简单加密方式存放的。　　（有些种类的设备是用明文存放的）

enable secret　　password　　命令配置的口令在配置文件中是用安全加密方式存放的。

说明： 以上两种口令只需要配置一种，如果两种都配置了，则两个口令不应该相同，且用 secret　定义的口令优先。

2、删除配置的特权口令：

```
Ruijie(config)#      no enable password
Ruijie(config)#      no enable secret
```

配置举例：

```
Ruijie>   enable
```

```
Ruijie#  configure terminal
Ruijie(config)#      enable secret 123
```

本例设置特权口令为 123 。使用安全加密的密文存放。

说明： 本部分配置的特权口令是为最高的 15 级设置的口令，如果想要使用多级别的特权模式，需要先用 privilege 命令为相应级别授权，再用 enable secret 命令配置该级别的口令。

三：配置管理 IP 和默认网关

本部分包括以下内容：

配置交换机的管理 IP

配置交换机的默认网关

配置交换机的管理 IP

3 层交换机在每个 3 层口上都可以设置 IP 地址，这里所说的管理 IP 是指为一台新交换机设置一个 IP 地址，使它可以正常访问并管理，将来再根据实际应用配置各 3 层口的 IP 地址。

新出厂的交换机在用控制台登录时，可以进行一些基础配置，其中就包括管理 IP，你应该在此处配置 IP 地址等参数。

如果需要修改管理 IP，可以在登录后用命令行进行修改。

修改管理 IP ：

```
Ruijie(config)#      interface vlan 1
Ruijie(config-if)#      ip address    IP-address Subnet-mask
```

interface 命令用于把管理 IP 指定给 VLAN 1 。

ip address 命令用于设置 IP 地址和子网掩码。

说明： 通常我们把管理 IP 指定给 VLAN1 ， 因为在初始时，所有接口都属于 VLAN1 ， 这样

你就可以通过任意一个接口管理交换机了。

删除管理 IP ：

Ruijie(config)# interface vlan 1
Ruijie(config-if)# no ip address

配置举例： 配置交换机的管理 IP 为 192.168.1.5/24 。

```
Ruijie> enable
Ruijie# configure terminal
Ruijie(config)# interface vlan 1
Ruijie(config-if)# ip address 192.168.1.5 255.255.255.0
Ruijie(config-if)# end
Ruijie#
```

说明：在命令中，子网掩码必须采用完整写法，不能简写为 /24 。

配置交换机的默认网关

当交换机接收到一个不知该发往何处的数据报时，就把该数据报发往默认网关。

只有 2 层设备才需要配置默认网关， 3 层设备是通过配置路由把数据报发送出去的。

模式： 在全局配置模式中配置。

配置命令：

Ruijie(config)# ip default-gateway IP-address

IP-address 是默认网关的 IP 地址。

删除配置的默认网关：

Ruijie(config)# no ip default-gateway

配置举例： 配置交换机的默认网关为 192.168.1.1 。

```
Ruijie>  enable
Ruijie#  configure terminal
Ruijie(config)#      ip default-gateway 192.168.1.1
Ruijie(config)#      end
Ruijie#
```

配置的默认网关可以在配置文件中看到。

四：远程登录（Telnet） 的配置

本部分包括以下内容：

远程登录条件

一台交换机能够通过 Telnet 登录的条件是：

1. 交换机已经配置了 IP 地址；
2. 交换机已经配置了远程登录密码；
3. 交换机已经配置了特权密码；
4. 交换机已经接入网络并开始工作。

这时，我们可以通过网络中的一台计算机，在命令行下输入 “ telnet 交换机 IP 地址 ”登录到交换机上对交换机进行配置。

如果登录的交换机没有配置远程登录密码，会显示 “ Password required, but none set ”的错误提示信息；如果没有设置特权密码，在进入特权模式时会显示 “ %No password set ” 的

错误提示信息。

所以，对于一台新购置的交换机，　必须先用控制台为交换机配置　IP 地址和远程登录密码，　以后就可以用远程登录管理这台交换机了。

配置举例：　用控制台为交换机配置　IP 地址、远程登录密码和特权密码。

```
Switch>    enable
Switch#    configure terminal
Switch(config)#        interface vlan 1
Switch(config-if)#         ip address 192.168.1.5 255.255.255.0
Switch(config-if)#         exit
Switch(config)#        line vty 0 4
Switch(config-line)#           login
Switch(config-line)#           password 123
Switch(config-line)#           exit
Switch(config)#        enable secret 456
Switch(config)#        end
Switch#
```

完成以上配置后，我们可以通过网络中的一台计算机，用　　telnet 192.168.1.5　　登录交换机，登录密码为　123 。登录后，进入特权模式的密码为　456 。

开启和禁止远程登录

默认情况下，　Telnet Server　　是打开的，　任何人都可以用　Telnet　访问交换机，　我们可以用命令禁止使用　Telnet　访问交换机。

模式：　在全局配置模式中配置。

关闭　Telnet Server　　：

```
        Switch(config)#     no enable service telnet-server
```

开启　Telnet Server　　：

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

说明： 关闭 Telnet 访问不影响使用控制台、 Web 和 SNMP 访问交换机。

配置举例： 关闭交换机的远程登录访问。

```
Switch>    enable
Switch#    configure terminal
Switch(config)#        no enable service telnet-server
```

限制远程登录访问

当 Telnet Server 开启时，我们可以配置允许远程登录的 IP 地址，这样，可以限制用户只能从指定计算机远程登录交换机。

模式： 在全局配置模式中配置。

配置命令：

Switch(config)# service telnet host host-ip

参数 host-ip 为允许远程登录的用户的 IP 地址。

说明：你可以多次使用此命令设置多个允许远程登录的合法用户 IP。如果不配置此项，默认是不限制使用者的 IP 地址。

删除配置的 Telnet 限制：

Switch(config)# no service telnet host host-ip

此命令只删除指定的 IP。

Switch(config)# no service telnet host

此命令删除所有的 IP。

配置举例： 只允许 IP 地址为 192.168.1.10 和 192.168.1.30 的用户用 Telnet 登录交换机。

```
Switch>  enable
Switch#  configure terminal
Switch(config)#      service telnet host 192.168.1.10
Switch(config)#      service telnet host 192.168.1.30
```

设置远程登录的超时时间

当你用 Telnet 登录交换机后， 如果在设定的超时时间内没有任何输入， 交换机会自动断开该连接，所以设置超时时间有一定的保护作用。

Telnet 的超时时间默认为 5 分钟，你可以用命令修改它。

模式： 线路配置模式

配置命令：

Switch(config-line)# exec-timeout time

参数 time 为设置的超时时间，单位为秒，取值为 0~3600 ，如果设置为 0，表示不限定超时时间。

说明： 你必须先用 line vty 命令进入远程登录的线路模式再配置超时时间。

删除配置的 Telnet 超时时间：

Switch(config-line)# no exec-timeout

删除后，超时时间恢复为默认的 5 分钟。

配置举例： 设置远程登录的超时时间为 10 分钟（600 秒）。

```
Switch>  enable
Switch#  configure terminal
```

```
Switch(config)#       line vty
Switch(config-line)#          exec-timeout 600
```

查看 Telnet Server 的状态

在特权模式下，用 show service 命令可以查看 Telnet Server 是否已被禁用。

举例： 查看交换机 Telnet Server 的状态。

```
Switch>    enable
Switch#    show service
SSH-server : Enabled
Snmp-agent : Disabled
Telnet-server : Enabled
Web-server : Enabled
```

show service 命令显示了 SSH Server 、SNMP Agent 、Telnet Server 和 Web Server 四种管理方式的使能状态, “ Enabled ”为开启, “ Disabled ”为关闭。

五：配置接口的基本参数

本部分包括以下内容：

交换机接口的类型

交换机接口的默认配置

交换机接口配置的一般方法

配置接口描述

配置接口速率

配置接口的双工模式

禁用 / 启用交换机接口

查看交换机接口信息

交换机接口的类型

交换机的每个物理接口可处于以下模式中的一种：

类型	模式	描述
Access Port	2 层口	实现 2 层交换功能，且只转发来自同一个 VLAN 的帧
Trunk Port	2 层口	实现 2 层交换功能，可转发来自多个 VLAN 的帧
L2 Aggregate Port	2 层口	由多个物理接口组成的一个高速传输通道
Routed Port	3 层口	用单个物理接口构成的三层网关接口
SVI	3 层口	用多个物理接口构成的三层网关接口
L3 Aggregate Port	3 层口	由多个物理接口组成的一个高速三层网关接口

默认情况下，交换机所有接口都是 2 层的 Access Port 接口，所以如果一台没有经过配置的 3 层交换机可作为一台 2 层交换机直接使用。

交换机接口的默认配置

参数	默认设置
工作模式	2 层交换模式

接口类型	Access Port
缺省 VLANL	VLAN 1
接口状态	UP（激活）
接口描述	无
工作速度	自协商
双工模式	自协商
流控	关闭
风暴控制	关闭
接口保护	关闭
接口安全	关闭

默认情况下，交换机所有接口都是 2 层的 Access Port 接口，所有接口都属于 VLAN 1，所有接口默认都是激活的。

交换机接口配置的一般方法

配置接口时，可以配置单个接口，也可以成组配置多个接口。

配置单个接口：

```
Switch(config)#      interface    port-ID
Switch(config-if)#       配置接口参数
```

interface 命令用于指定一个接口，之后的命令都是针对此接口的。

说明： interface 命令可以在全局配置模式下执行， 此时会进入接口配置模式， 它也可以在接口配置模式下执行， 所以配置完一个接口后， 可直接用 interface 命令指定下一个接口。

参数： port-ID 是接口的标识，它可以是一个物理接口，也可以是一个 VLAN（此时应该把 VLAN 理解为一个接口），或者是一个 Aggregate Port 。

配置举例： 配置交换机的 IP 地址为 192.168.1.5 ，并把接口 fastethernet0/1 和 fastethernet0/2 设置为全双工模式。

```
Switch>  enable
Switch#  configure terminal
Switch(config)#     interface vlan 1
Switch(config-if)#      ip address 192.168.1.5 255.255.255.0
Switch(config-if)#      interface f0/1
Switch(config-if)#      duplex full
Switch(config-if)#      interface f0/2
Switch(config-if)#      duplex full
Switch(config-if)#      end
Switch#
```

说明：当交换机没有 3 层口时，所有接口都属于 VLAN1 ，所以 VLAN1 的 IP 地址就是交换机的 IP 地址。

成组配置接口：

如果有多个接口需要配置相同的参数时，可以成组配置这些接口。

Switch(config)# interface range port-range
Switch(config-if)# 配置接口参数

参数：port-range 是接口的范围， 它可以指定多个范围段， 各范围段之间用逗号隔开。

说明： port-range 指定接口范围可以是物理接口范围，也可以是一个 VLAN 范围。如： f0/1-6 、vlan 2-4 等。

注意： 在 interface range 中的接口必须是相同类型的接口。

配置举例： 配置交换机的接口 fastethernet0/1~fastethernet0/12 的速度为 100Mbps ，并把 fastethernet0/1~fastethernet0/3 和 fastethernet0/7~fastethernet0/10 分配给 VLAN2 。

```
Switch>  enable
Switch#  configure terminal
Switch(config)#  interface range f0/1-12
Switch(config-if)#  speed 100
Switch(config-if)#  interface range f0/1-3,0/7-10
Switch(config-if)#  switchport access vlan 2
Switch(config-if)#  end
Switch#
```

配置接口描述

接口描述常用于标注一个接口的功能、用途等，有利于记录和了解网络拓扑。

模式： 在接口配置模式中配置。

配置命令：

```
Ruijie(config)#  interface  interface-ID
Ruijie(config-if)#  description  string
```

interface 命令用于指定要配置的接口。参数 interface-ID 是接口的类型和编号。

description 命令用于设置此接口的描述文字。

说明： 接口描述的文字最多不得超过 32 个字符。

删除配置的描述：

```
Ruijie(config)#  interface  interface-ID
Ruijie(config-if)#  no description
```

配置举例：

```
Ruijie>   enable
Ruijie#   configure terminal
Ruijie(config)#      interface f0/1
Ruijie(config-if)#       description to-PC1
Ruijie(config-if)#       interface f0/2
Ruijie(config-if)#       description to-Switch1
Ruijie(config-if)#       end
Ruijie#
```

本例为 fastethernet0/1 和 fastethernet0/2 配置了接口描述， 这样可方便了解它们所连接的设备。

配置的接口描述可以在配置文件中看到。

配置接口速率

S3550 的接口都是具有多种速率的自适应接口， FastEthernet 接口有 10/100M 两种速率， GigabitEthernet 接口有 10/100/1000M 三种速率，默认情况下，他们用自协商方式确定他的工作速率。用配置可指定他们只使用某一个固定速率。

模式： 在接口配置模式中配置。

配置命令：

```
Switch(config)#      interface    port-ID
Switch(config-if)#       speed   10 | 100 | 1000 | auto
```

interface 命令用于指定要配置的接口。指定的接口可以是物理接口或 Aggregate Port 接口。

speed 命令用于设置此接口的速率。

参数： 10 —— 10Mbps ， 100 —— 100Mbps ， 1000 —— 1000Mbps （只能用于

GigabitEthernet　　接口）， auto ——使用自协商模式（默认值）。

说明： 当接口速率不是 auto 时，自协商过程被关闭，此时要求与该接口相连的设备必须支持此速率。

删除配置的速率：

Switch(config)#　　interface　port-ID
Switch(config-if)#　　no speed

删除配置的速率后，此接口的速率默认为　　auto 。

配置举例： 配置交换机的 fastethernet0/1　　口速率为 100Mbps 。

```
Switch>  enable
Switch#  configure terminal
Switch(config)#      interface f0/1
Switch(config-if)#       speed 100
Switch(config-if)#       end
Switch#
```

配置的接口速率可以在配置文件中看到。

配置接口的双工模式

S3550　的接口可工作于半双工模式或全双工模式，默认情况下，他们用自协商方式确定他的双工模式。用配置可指定他们只使用某一种双工模式。

模式： 在接口配置模式中配置。

配置命令：

Switch(config)#　　interface　port-ID
Switch(config-if)#　　duplex　auto | half | full

interface　命令用于指定要配置的接口。指定的接口可以是物理接口或　　Aggregate

Port 接口。

duplex 命令用于设置此接口的双工模式。

参数： auto ——使用自协商模式（默认值）， half ——半双工模式， full ——全双工模式。

说明： 当双工模式不是 auto 时，自协商过程被关闭，此时要求与该接口相连的设备必须支持此双工模式。

删除配置的双工模式：

Switch(config)# interface port-ID
Switch(config-if)# no duplex

删除配置的双工模式后，此接口的双工模式默认为 auto 。

配置举例： 配置交换机的 fastethernet0/1 口双工模式为全双工模式。

```
Switch>  enable
Switch#  configure terminal
Switch(config)#  interface f0/1
Switch(config-if)#  duplex full
Switch(config-if)#  end
Switch#
```

配置的接口双工模式可以在配置文件中看到。

禁用 / 启用交换机接口

交换机的所有接口默认是启用的，此时接口的状态为 Up。如果禁用了一个接口，则该接口不能收发任何帧，此时接口的状态为 Down 。

模式： 在接口配置模式中配置。

禁用指定接口：

Switch(config)# interface port-ID
Switch(config-if)# shutdown

启用指定接口：

Switch(config)# interface port-ID
Switch(config-if)# no shutdown

说明： interface 指定的接口可以是物理接口、 VLAN 或 Aggregate Port 接口。

配置举例： 禁用交换机的 fastethernet0/1 口。

```
Switch> enable
Switch# configure terminal
Switch(config)# interface f0/1
Switch(config-if)# shutdown
Switch(config-if)# end
Switch#
```

查看交换机接口信息

在特权模式下，用 show interfaces 命令可查看交换机指定接口的设置和统计信息。

模式： 特权模式。

命令：

Switch# show interfaces [port-ID] [counters | description | status | switchport | trunk]

参数：

port-ID ：可选，指定要查看的接口，可以是物理接口、 VLAN 或 Aggregate Port 接口。

counters ：可选，只查看接口的统计信息。

description ：可选，只查看接口的描述信息。

status ：可选，查看接口的各种状态信息，包括速率、双工等。

switchport ：可选，查看 2 层接口信息，只对 2 层口有效。

trunk ：可选，查看接口的 Trunk 信息。

说明： 如果未指定参数，则显示所有接口信息。

配置举例： 查看交换机的 fastethernet0/1 口的信息。

```
Switch>  enable
Switch#  show interfaces f0/1
Interface : FastEthernet0/1
Description : to-PC1
AdminStatus : up
OperStatus : down
Medium-type : fiber
Hardware : GBIC
Mtu : 1500
LastChange : 0d:0h:0m:0s
AdminDuplex : Auto
OperDuplex : Unknown
AdminSpeed : Auto
OperSpeed : Unknown
FlowControlAdminStatus : Auto
FlowControlOperStatus : Off
Priority : Auto
```

六：单个接口的配置

本部分包括以下内容：

2 层 Access Port （普通口）的配置

2 层 Trunk Port （Trunk 口）的配置

3 层 Routed Port （路由口）的配置

2 层 Access Port （普通口）的配置

3 层交换机的所有物理接口默认都是 2 层 Access Port ，所以不需要进行配置。

Access 接口具有以下特性：

1. Access 接口是 2 层口，不能为它配置 IP 地址，没有路由功能。
2. 每个 Access 接口只能属于一个 VLAN （默认是 VLAN1 ），它只能转发属于同一个 VLAN 的帧。

2 层 Trunk Port （Trunk 口）的配置

交换机的接口默认是 Access 接口，此时它只能转发来自同一个 VLAN 的帧，如果需要让它能够转发不同 VLAN 的帧，需要设置为 Trunk 接口。

通常我们需要把交换机和交换机、交换机和路由器连接的接口设置为 Trunk 接口。

1、把接口配置为 Trunk 接口：

Switch(config)# interface port-id
Switch(config-if)# switchport mode trunk

interface 命令用于指定要修改的接口，这个接口只能是物理接口。

switchport mode trunk 命令用于把该接口设置为 Trunk Port 。

2、恢复 Trunk 接口为 Access 接口：

Switch(config)# interface port-id
Switch(config-if)# switchport mode access

说明：也可以使用 no switchport mode 命令把接口模式恢复为默认值, 而默认值就是 Access Port 。

配置举例： 配置交换机的 FastEthernet0/1 为 Trunk 接口。

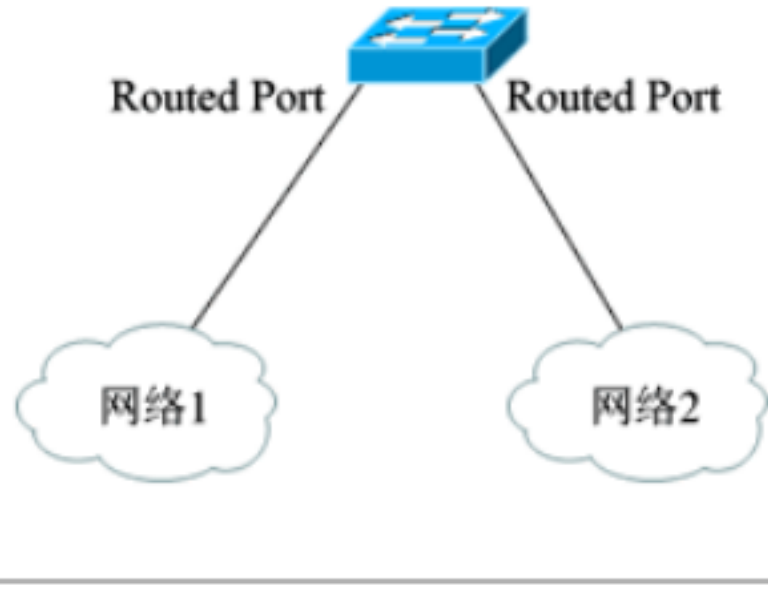
```
Switch>  enable
Switch#  configure terminal
Switch(config)#  interface f0/1
Switch(config-if)#  switchport mode trunk
Switch(config-if)#  end
Switch#
```

3 层 Routed Port （路由口）的配置

3 层交换机的所有接口默认都是 2 层 Access Port ，需要经过配置，才能使某个接口成为 3 层路由口。

Routed 接口具有以下特性：

1. Routed 接口是 3 层口，我们可以为它配置一个 IP 地址。
2. 每个 Routed 接口可用于连接一个子网， Routed 接口的 IP 地址就是该子网的网关。
3. 如果一台交换机配置了多个 3 层口，各个 3 层口的 IP 地址应属于不同的网络。



1、把一个 Access 接口配置为 Routed 接口：

```
Switch(config)#      interface    port-id
Switch(config-if)#       no switchport
Switch(config-if)#       ip address    IP-address Subnet-Mask
```

interface 命令用于指定要修改的接口，这个接口只能是物理接口。

no switchport 命令用于把 2 层 Access Port 设置为 3 层 Routed Port 。

ip address 命令用于给 3 层 Routed Port 设置 IP 地址和子网掩码。

说明：每个 3 层路由口只能对应一个物理接口。 只有 3 层口才能配置 IP 地址，2 层口不能配置 IP 地址。

2、把一个 Routed 接口还原为 Access 接口：

```
Switch(config)#      interface    port-id
Switch(config-if)#       switchport
```

配置举例： 把 FastEthernet0/1 配置为 3 层 Routed Port ，并设置 IP 地址。

```
Switch>   enable
Switch#   configure terminal
Switch(config)#       interface f0/1
Switch(config-if)#        no switchport
Switch(config-if)#        ip address 192.168.2.1 255.255.255.0
Switch(config-if)#        end
Switch#
```

七：VLAN 和 SVI 的配置

本部分包括以下内容：

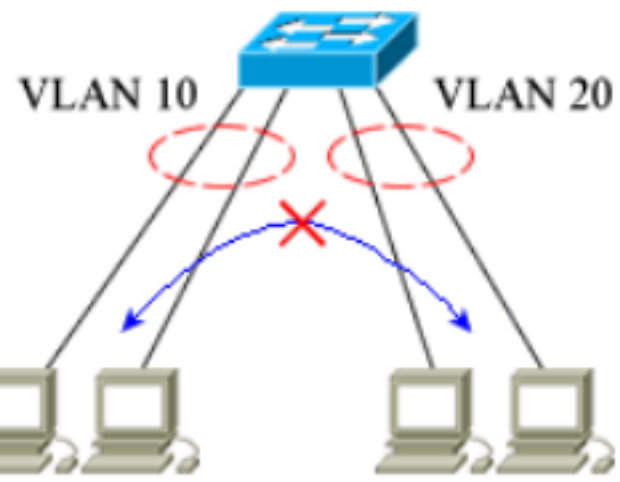
VLAN 的配置

SVI 的配置

VLAN 的配置

VLAN 是一个 2 层接口组成的集合，它具有以下特性：

1. 每个 VLAN 可包含多个 2 层口，其中可以有 Access 接口，也可以有 Trunk 接口。
2. 每个 Access 接口只能属于一个 VLAN（默认是 VLAN1），它只能转发属于同一个 VLAN 的帧。
3. Trunk 接口可同时属于多个 VLAN（默认是所有 VLAN），它可以转发属于不同 VLAN 的帧。
4. 每个 VLAN 用一个整数标识，称为 VLAN ID，取值范围为 1~1007（有些交换机的取值范围可以更大）。
5. 初始时，交换机已经定义了一个 ID 为 1 的 VLAN，所有物理接口默认属于这个 VLAN。



属于同一个 VLAN 的接口可以相互通信，属于不同 VLAN 的接口间不能通信。

1、创建 VLAN：

```
Switch(config)#      vlan   vlan-id
Switch(config-vlan)#        name   vlan-name
```

vlan 命令用于指定一个 VLAN，如果指定的 VLAN 不存在，则创建这个 VLAN。

name 命令用于给 VLAN 定义一个名字。如果没有这一步，系统会自动命名为 VLAN xxxx，其中 xxxx 是以 0 开头的 4 位 VLAN ID 号。

说明：创建 VLAN 的过程可以没有，你可以在添加接口时创建 VLAN。

2、向 VLAN 中添加 Access 接口：

Switch(config)# interface port-id
Switch(config-if)# switchport access vlan vlan-id

interface 命令用于指定一个接口，这个接口只能是物理接口。

switchport 命令用于把该接口分配给指定的 VLAN。如果指定的 VLAN 不存在，则创建这个 VLAN。

说明： 添加多个接口时，可反复使用上面的过程。

3、删除 VLAN ：

Switch(config)# no vlan vlan-id

说明： VLAN 1 不能删除。

4、查看 VLAN ：

Switch# show vlan

配置举例：定义一个 ID 为 20 的 VLAN，并把 FastEthernet0/1 和 FastEthernet0/2 指派给这个 VLAN。

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# name VLAN20
Switch(config-vlan)# exit
Switch(config)# interface f0/1
Switch(config-if)# switchport access vlan 20
Switch(config-if)# interface f0/2
Switch(config-if)# switchport access vlan 20
Switch(config-if)# end
Switch#
```

SVI 的配置

如果给一个 VLAN 配置上 IP 地址，它就成为一个 SVI 接口，它具有以下特性：

1. SVI 接口由多个物理接口组成，但在逻辑上，可把它理解为一个 3 层口。
2. 每个 SVI 接口可用于连接一个子网， SVI 接口的 IP 地址就是该子网的网关。
3. 组成 SVI 的物理接口都必须是 Access 接口，不能是 3 层口。

1、配置 SVI 接口：

Switch(config)# interface vlan vlan-id
Switch(config-if)# ip address IP-address Subnet-Mask

interface 命令用于指定一个 VLAN。

ip address 命令用于给这个 VLAN 设置 IP 地址和子网掩码，使它成为 SVI 接口。

2、恢复 SVI 为 VLAN ：

Switch(config)# interface vlan vlan-id
Switch(config-if)# no ip address

配置举例： 配置一个 SVI，其中包含了 FastEthernet0/1 和 FastEthernet0/2 两个接口。

```
Switch>  enable
Switch#  configure terminal
Switch(config)#      interface f0/1
Switch(config-if)#       switchport access vlan 20
Switch(config-if)#       interface f0/2
Switch(config-if)#       switchport access vlan 20
Switch(config-if)#       interface vlan 20
Switch(config-if)#       ip address 192.168.10.1 255.255.255.0
Switch(config-if)#       end
Switch#
```

八： Aggregate Port 的配置

本部分包括以下内容：

2 层 Aggregate Port （通道口）的配置

当两台交换机互联时，为了提高连接的带宽，可以使用多个接口进行互联，这时需要把这些接口设置为 Aggregate 接口。

Aggregate Port 具有以下特性：

1. 从物理上看， Aggregate 接口是由多个物理接口组成的，但在逻辑上，我们可把它理解为一个高速接口，它的带宽是组成它的各接口带宽之和。
2. 组成 Aggregate 口的物理接口必须是同类接口，接口参数也必须相同，同属于一个 VLAN 。
3. 一个 Aggregate 口包含的物理接口数量一般不能超过 8 个。
4. Aggregate 口具有流量平衡功能，当其中一条成员链路断开时，系统会自动把它的流量分配到其它有效链路上，不影响该接口的使用。
5. 每个 Aggregate 接口用一个整数标识，称为 AP ID ，取值范围为 1~12 。

1 、创建 Aggregate 口：

Switch(config)# interface port-id
Switch(config-if)# port-group AP-id

interface 命令用于指定要加入 Aggregate 的接口，这个接口只能是物理接口。

port-group 命令用于把该接口加入到指定的 Aggregate 中。 AP-id 是 Aggregate 接口的编号，取值为 1~12 。如果指定的 Aggregate 接口还不存在，则创建该接口。

说明： 重复上面的操作，可以向 Aggregate 口添加多个接口。

2 、从 Aggregate 中删除接口：

Switch(config)# interface port-ID
Switch(config-if)# no port-group

3、查看 Aggregate 接口：

Switch# show aggregateport AP-id

配置举例：把交换机的 FastEthernet0/4 和 FastEthernet0/5 组成一个 Aggregate 接口。

```
Switch>  enable
Switch#  configure terminal
Switch(config)#      interface f0/4
Switch(config-if)#       port-group 1
Switch(config-if)#       interface f0/5
Switch(config-if)#       port-group 1
Switch(config-if)#       end
Switch#
```

3 层 Aggregate Port （通道口）的配置

3 层 Aggregate Port 和 2 层 Aggregate Port 的区别在于 3 层 Aggregate Port 具有 IP 地址，可作为网关连接一个子网。

配置 3 层 Aggregate Port 时，可以先创建一个 3 层 Aggregate Port ，再向其中加入成员接口，也可以先配置一个 2 层 Aggregate Port ，再把它定义为 3 层口。

定义 3 层 Aggregate Port ：

Switch(config)# interface aggregateport AP-id
Switch(config-if)# no switchport
Switch(config-if)# ip address IP-address Subnet-Mask

interface aggregateport 命令用于指定一个 Aggregate 接口，如果指定的 Aggregate 接口还不存在，则创建该接口。

no switchport 命令用于把该接口转换为 3 层口。

ip address 命令用于给这个 3 层 Aggregate Port 设置 IP 地址和子网掩码。

配置举例： 把交换机的 FastEthernet0/4 和 FastEthernet0/5 组成一个 3 层 Aggregate 接口。

```
Switch>  enable
Switch#  configure terminal
Switch(config)#      interface aggregateport 1
Switch(config-if)#       no switchport
Switch(config-if)#       ip address 192.168.8.1 255.255.255.0
Switch(config-if)#       interface f0/4
Switch(config-if)#       port-group 1
Switch(config-if)#       interface f0/5
Switch(config-if)#       port-group 1
Switch(config-if)#       end
Switch#
```

九：路由的配置与查看

本部分包括以下内容：

启用和关闭 IP 路由

要使用交换机的三层功能，必须打开 IP 路由功能。在 S3550 系列交换机中， IP 路由功能默认是打开的。如果没有打开，需要用命令打开它。

1、启用 IP 路由功能：

```
Ruijie(config)#      ip routing
```

说明：启用 IP 路由后，连接在三层交换机上的各个子网间就可以互相访问了。你可以使用 show ip route 命令查看路由表。

2、关闭 IP 路由功能：

Ruijie(config)# no ip routing

配置举例： 交换机的 fastethernet0/1 连接了一个子网 192.168.1.0/24 ，

fastethernet0/2 连接了一个子网 192.168.2.0/24 。利用交换机的 3 层功能使它们能够通信。

```
Ruijie>  enable
Ruijie#  configure terminal
Ruijie(config)#      interface f0/1
Ruijie(config-if)#       no switchport
Ruijie(config-if)#       ip address 192.168.1.1 255.255.255.0
Ruijie(config-if)#       interface f0/2
Ruijie(config-if)#       no switchport
Ruijie(config-if)#       ip address 192.168.2.1 255.255.255.0
Ruijie(config-if)#       exit
Ruijie(config)#      ip routing
Ruijie(config)#      exit
Ruijie#  show ip route
```

本例中，首先把 f0/1 和 f0/2 都配置为 3 层路由口，并配置了 IP 地址。之后用 ip routing 命令启用 IP 路由。在路由表中应该可以看到网络 192.168.1.0/24 和 192.168.2.0/24 的路由表项。

配置静态路由

静态是手工添加的路由项目。

模式： 全局配置模式。

1、配置静态路由：

Ruijie(config)# ip route network-number network-mask ip-address

参数：

network-number　　是目的地址，一般是一个网络地址。

network-mask　　是目的地址的子网掩码。

ip-address　　是下一跳地址。

说明： ip route　命令定义的是一条传输路径，可以告知设备把某个地址的数据报送往何处。

配置完成后可以使用　show ip route　　命令查看路由表。

2、删除静态路由：

Ruijie(config)#　　no ip route　　network-number network-mask

配置举例　1 ：

```
Ruijie>　enable
Ruijie#　configure terminal
Ruijie(config)#　　ip route 172.16.0.0 255.255.0.0 192.168.3.2
```

ip route 172.16.0.0 255.255.0.0 192.168.3.2　　命令表示把所有目的地址在 172.16.0.0/16　　网络中的数据报发往地址　192.168.3.2　　处。

配置举例　2 ：

```
Ruijie>　enable
Ruijie#　configure terminal
Ruijie(config)#　　no ip route 172.16.0.0 255.255.0.0
```

本例删除了路由表中目的地址为　172.16.0.0/16　　网络的静态路由。

配置默认路由

默认路由又称为缺省静态路由，是静态路由的特例，它表示把所有本机不能处理的数据报发往指定的设备。

模式： 全局配置模式。

1、配置默认路由：

Ruijie(config)#　ip route 0.0.0.0 0.0.0.0　ip-address

参数：

0.0.0.0 0.0.0.0　表示任意地址。

ip-address　是下一跳地址。

说明：默认路由的优先级是最低的，设备首先会匹配静态路由和由路由协议生成的路由，只有当没有相匹配的项目时，才按照默认路由指定的地址发送。

2、删除默认路由：

Ruijie(config)#　no ip route 0.0.0.0 0.0.0.0

配置举例：

```
Ruijie>  enable
Ruijie#  configure terminal
Ruijie(config)#  ip route 0.0.0.0 0.0.0.0 192.168.10.2
```

ip route 0.0.0.0 0.0.0.0 192.168.10.2　命令表示把所有没有匹配成功的目的地址发往地址 192.168.10.2　处。

查看路由表

在特权模式下使用 show ip route 命令可以查看交换机的路由表。

示例：

```
Switch>  enable
Switch#  show ip route

Type: C - connected, S - static, R - RIP, O - OSPF, IA - OSPF inter area
```

配置的接口描述可以在配置文件中看到。

十：RIP　协议的配置

本部分包括以下内容：

RIP 协议的一般配置

RIP 协议参数的配置

RIP 是一种距离矢量协议，属于内部网关协议。

RIP 协议的特点：

1. RIP 协议用跳数来评估路由，跳数最大为　15，所以 RIP 协议不适合大规模的网络。
2. RIP 协议每隔 30 秒（更新时间）发送路由更新报文。如果一个设备在　180 秒（失效时间）内没有发送更新报文，则该设备提供的路由被设置为不可用；如果再过　120 秒（清除时间）后仍未发送更新报文，则删除到此设备的路由。
3. RIP 协议使用 UDP 报文发送路由更新，端口号为　520 。
4. RIP 协议的管理距离是　120 。
5. RIP 协议有 RIPv1　和 RIPv2　两个版本。

说明：在路由器和　3 层交换机上都可以配置　RIP 协议。

RIP　协议的一般配置

1、配置　RIP　协议：

```
Ruijie(config)#　　router rip
Ruijie(config-router)#　　network　network-number
```

router rip　　命令用于启用　RIP，并进入 RIP 的配置模式。

network　　命令用于指定参与　RIP 路由的网络，它的参数是网络号。如果设备连接了多个网络，你可以用多条　network　　命令指定它们；如果要指定设备连接的所有网络，可以用 network 0.0.0.0　　来表示所有网络。

说明：对于运行　RIP 协议的设备，只有用　　network　　命令指定的网络会参与到　RIP 发布的

路由更新中，可以被其它运行 RIP 协议的设备学习到；而那些没有用 network 命令指定的网络，不会参与 RIP 路由，其它设备也不能学习到。

路由配置好后，可以在特权模式下用 show ip route 命令查看学习到的路由项目。

2、删除 RIP 关联的网络：

Ruijie(config)# router rip
Ruijie(config-router)# no network network-number

3、关闭 RIP 协议：

Ruijie(config)# no router rip

关闭后，本设备的 RIP 协议将不再工作。

配置举例 1：

```
Ruijie> enable
Ruijie# configure terminal
Ruijie(config)# router rip
Ruijie(config-router)# network 192.168.1.0
Ruijie(config-router)# network 192.168.5.0
Ruijie(config-router)# end
```

本例在设备上启用了 RIP 协议，关联的网络是 192.168.1.0/24 和 192.168.5.0/24 。

注意：192.168.1.0/24 和 192.168.5.0/24 都只能是和本设备直连的网络。

配置举例 2：

```
Ruijie> enable
Ruijie# configure terminal
Ruijie(config)# router rip
Ruijie(config-router)# network 0.0.0.0
Ruijie(config-router)# end
```

本例用 network 0.0.0.0 来指定关联所有直连的网络，这样就无需再逐个指定各个接口上的网络了。

RIP 协议参数的配置

通常情况下，我们让 RIP 协议的各项参数取默认值就行了，无需进行配置，如果需要的话可以用命令修改它们的值，修改时应该先用 router rip 命令进入 RIP 的配置模式。

1、配置默认跳数：

Ruijie(config-router)# default-metric number

默认跳数是指访问本地网络的花费（跳数）。它的取值范围为 1~15 ，缺省值为 1。

2、配置计时器：

Ruijie(config-router)# timers basic update invalid holddown

update ：更新时间。是发送更新报文的时间间隔。默认为 30 秒，有效取值范围是 0~2147483647 。

invalid ：失效时间。是宣布无效的时间间隔。默认为 180 秒，有效取值范围是 1~2147483647 。

holddown ：清除时间。是对失效项目保持的时间。默认为 120 秒，有效取值范围是 0~2147483647 。

3、配置邻居：

Ruijie(config-router)# neighbor ip-address

RIP 协议是用广播发布路由更新的，设置邻居可以使 RIP 和非广播网络的路由器交换路由信息。命令中的 ip-address 是邻居路由器的地址。

4、设置 RIP 版本：

Ruijie(config-router)# version version-number

version-number 的取值为 1 或 2。默认情况下， RIP 协议可接收 RIPv1 和 RIPv2 的报文，发送 RIPv1 的报文。用 version 1 命令可设置为仅发送和接收 RIPv1 的报文，用 version 2 命令可设置为仅发送和接收 RIPv2 的报文。另外，你也可以用 ip rip send|receive version 命令设置各个接口发送和接收的版本。

十一： OSPF 协议的配置

本部分包括以下内容：

OSPF 协议的一般配置

OSPF 是一种基于链路状态的内部网关路由协议。

OSPF 协议的特点：

1. OSPF 协议用链路状态来评估路由，可用于规模很大的网络。
2. OSPF 可通过区域划分网络，对于规模较小的网络一般只设置一个区域 0，对于规模较大的网络，可划分多个区域，其中区域 0 是必不可少的，它用于连接其它各区域。
3. OSPF 协议采用组播方式进行 OSPF 包交换，组播地址为 224.0.0.5 （全部 OSPF 路由器）和 224.0.06 （指定路由器）。
4. OSPF 协议的管理距离是 110，低于 RIP 协议的 120，所以如果设备同时运行 OSPF 协议和 RIP 协议，则 OSPF 协议产生的路由优先级高。

说明：在路由器和 3 层交换机上都可以配置 OSPF 协议。

OSPF 协议的一般配置

1、配置 OSPF 协议：

Ruijie(config)# router ospf process-id
Ruijie(config-router)# network network-number wildcard-mask area area-id

router ospf 命令用于启用 OSPF，并进入 OSPF 的配置模式。 process-id 是进程号，用于路由器内部。

network 命令用于指定参与 OSPF 路由的网络，参数 network-number 是网络号，wildcard-mask 是通配符掩码， area-id 是区域号。

说明：

通配符掩码用于指定网络号中有效的位，取 “ 0代表匹配该位，取 “ 1代表忽略该位。很多情况下，通配符掩码是子网掩码的反码。

路由配置好后，可以在特权模式下用　show ip route　命令查看学习到的路由项目。

2、删除 OSPF 中配置的项目：

Ruijie(config)# router ospf
Ruijie(config-router)# no network network-number wildcard-mask area area-id

3、关闭 OSPF 协议：

Ruijie(config)# no router ospf process-id

关闭后，本设备的 OSPF 协议将不再工作。

配置举例 1：

```
Ruijie> enable
Ruijie# configure terminal
Ruijie(config)# router ospf 1
Ruijie(config-router)# network 192.168.1.0 0.0.0.255 area 0
Ruijie(config-router)# network 192.168.5.0 0.0.0.255 area 0
Ruijie(config-router)# end
```

本例在设备上启用了 OSPF 协议，关联的网络是 192.168.1.0/24 和 192.168.5.0/24 。

配置举例 2：

```
Switch> enable
Switch# configure terminal
Switch(config)# router ospf 1
Switch(config-router)# network 192.168.0.0 0.0.255.255 area 0
Switch(config-router)# end
```

本例在设备上启用了 OSPF 协议，关联的网络是所有形如 192.168.0.0 的网络。

第三部分：交换机的高级配置

一：配置系统时间

本部分包括以下内容：

设置系统时间

交换机的系统时钟主要用于系统日志等需要记录事件发生时间的地方。你可以用手工配置交换机时间为当前时间，之后，交换机的时间会自动走下去，即使交换机下电也不影响时钟的走动，所以一般只需要设置一次交换机时钟。

注：有些低档交换机（如　S2126S　）没有系统时钟，对时钟的设置命令无效。

设置系统时间：

模式： 特权模式。

命令：

Switch#　clock set　hh:mm:ss day month year

hh:mm:ss　　是 24 小时制的时、分、秒；

day month year　　是日、月、年。

配置举例： 设置系统时间为 2009 年 5 月 1 日下午 3 点 30 分。

```
Switch>　enable
Switch#　clock set 15:30:00 1 5 2009
```

设置时区

锐捷交换机的缺省时区是东　8 区（北京时间）。

模式： 特权模式。

命令：

Switch#　clock time-zone　　time-zone

参数 time-zone　是设置的时区，取值范围为　-23~23　，如 8 表示东 8 区， -8 表示西 8 区，0 表示格林威治标准时间。

配置举例： 设置时区为东 6 区。

```
Switch>　enable
Switch#　clock time-zone 6
```

查看系统时间

模式： 特权模式。

命令：

Switch#　show clock

举例： 查看系统时间。

```
Switch>　enable
Switch#　show clock
System clock : 19:46:15.0 2009-05-04 Monday.
```

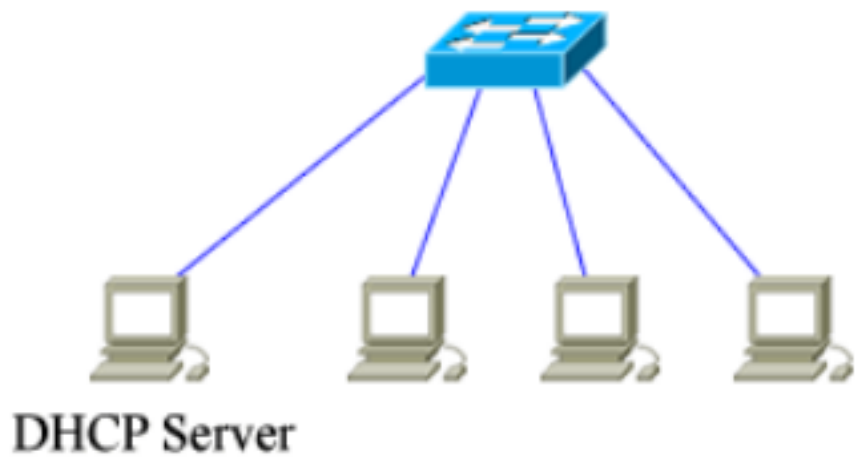
表示 2009 年 5 月 4 日，下午 7 点 46 分 15 秒，星期一

二：配置 DHCP 代理

本部分包括以下内容：

多网段的 DHCP 构建

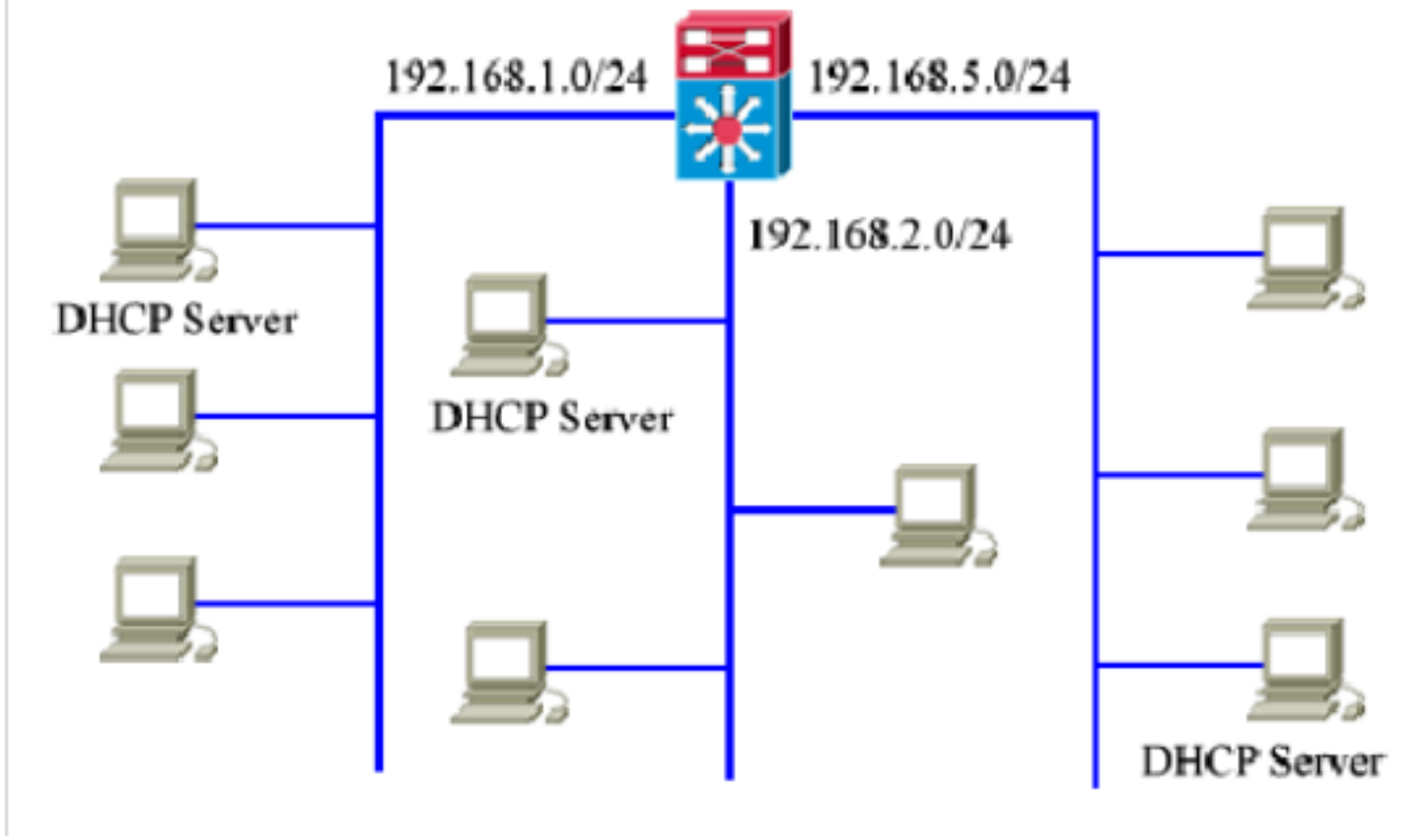
DHCP 协议用于在局域网环境中动态分配 IP 地址。



网络中的客户机 (DHCP Client) 通过广播向 DHCP 服务器 (DHCP Server) 发出请求，DHCP 服务器为客户机分配 IP 地址，再以广播的方式回传给客户机，客户机绑定获得的 IP 地址就可以开始正常的网络通信了。

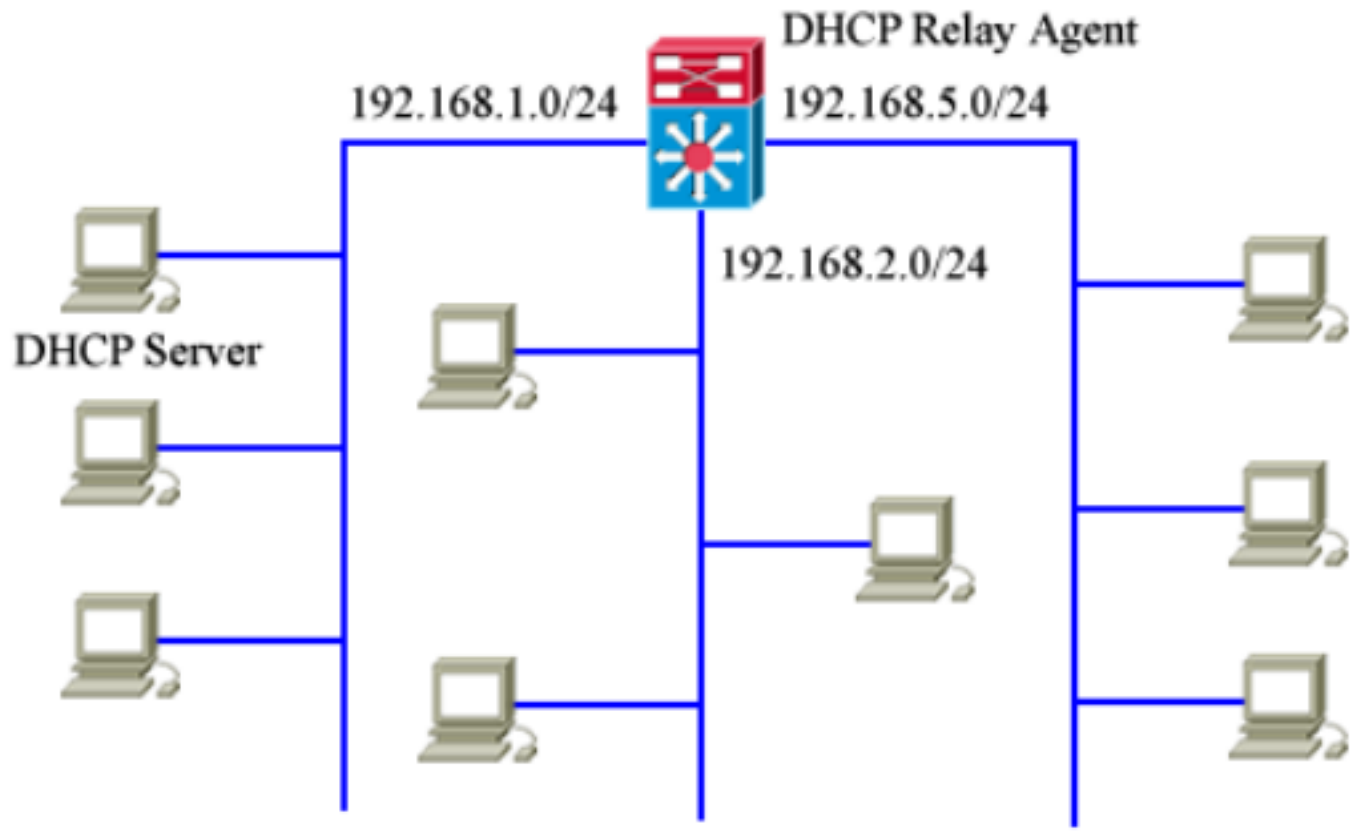
由于 DHCP 服务是以广播方式进行的，这使得这种应用只能限定在一个网段之中，对于多网段的局域网环境常用的解决方案有：

1、每个网段设立一个 DHCP Server ：



这种方法可由各个网段自行设立　DHCP 服务器，为本网段的客户机提供　IP 地址。

2、使用 DHCP　代理：



在这种方法中，只需在一个网段中设立　DHCP 服务器，把 3 层交换机配置为 DHCP 代理(DHCP Relay Agent)　，它可以把收到的 DHCP 请求转发给 DHCP 服务器，再把 DHCP 响应报文转发给客户机，这样就可以实现　DHCP 的跨网段服务。

DHCP　代理的配置

在缺省情况下， 3 层交换机的 DHCP 代理服务是关闭的，配置时，需要打开该服务。

1、打开 DHCP Relay Agent ：

模式： 全局配置模式。

命令：

Switch(config)# service dhcp

service dhcp 命令用于打开 DHCP Relay Agent ，这时，交换机就可以进行代理工作了。

2、配置 DHCP Server 的 IP 地址：

如果没有指定 DHCP 服务器的 IP 地址，交换机会以 255.255.255.255 为地址转发 DHCP 请求，这种转发是向所有接口转发， 我们不推荐这种做法。解决方法就是把 DHCP 服务器的 IP 地址告知交换机。

模式： 全局配置模式。

命令：

Switch(config)# ip helper-address IP-address

这条命令用于指定 DHCP 服务器的 IP 地址。

3、关闭 DHCP 代理：

在全局配置模式下，可以用 no ip helper-address 命令把 DHCP Server 的 IP 地址恢复为默认值，用 no service dhcp 命令可以关闭交换机的 DHCP Relay Agent 功能。

4、查看 DHCP Relay Agent 状态：

在特权模式下， 可以用 show ip management 命令查看 DHCP Relay Agent 状态。

配置举例： 已知 DHCP 服务器的 IP 地址为 192.168.1.15 ，把交换机配置成 DHCP Relay Agent 。

```
Switch>  enable
Switch#  configure terminal
Switch(config)#      service dhcp
Switch(config)#      ip helper-address 192.168.1.15
Switch(config)#      end
Switch#
```

说明：想要实现多网段的 DHCP 服务功能， 除了把交换机配置为 DHCP Relay Agent 外，还需要把 DHCP 服务器配置成可为多网段提供 IP 地址的工作方式， 相关内容请参考 DHCP 服务器的配置。

三：接口风暴控制的配置

本部分包括以下内容：

风暴控制

回到顶部

如果网络中出现过量的广播、组播和未知名单播包时，就可能发生了风暴，它会导致网络变慢，正常的网络活动难以进行。

风暴控制采用流控制机制解决风暴。当某一类数据包过量时，交换机会暂时禁止该类数据包的转发，直至数据流恢复正常。

S35 系列交换机的接口支持风暴控制设置，它把百兆接口每 8 个组成一个单位，共享风暴控制的设置。

S3550-24 交换机包含 3 个单位：1-8 ， 9-16 ， 17-24 ；S3550-48 交换机包含 6 个单位：1-8 ， 9-16 ， 17-24 ， 25-32 ， 33-40 ， 41-48 。

当一个接口配置了风暴控制时，其它 7 个接口也会自动配置上。如果 8 个接口中的一个变为

Aggregate Port　成员时，需要对其它接口重新配置，以免配置失效。

1、配置风暴控制功能：

命令：

```
Switch(config)#　interface　interface-id
Switch(config-if)#　storm-control level　level
Switch(config-if)#　storm-control broadcase
Switch(config-if)#　storm-control multicast
Switch(config-if)#　storm-control unicast
```

interface　命令用于指定要配置的接口。

storm-control level　命令用于指定风暴控制级别。它的参数　level　是一个百分数，取值范围是 1~100　。它表示接口允许某类数据包的最大流量占接口最大带宽的百分比，　当流量超过这个百分比时说明风暴发生，接口将丢弃超出部分的此类数据包。缺省值是　100　。

storm-control broadcase　命令用于开启广播风暴的控制功能。

storm-control multicast　命令用于开启组播风暴的控制功能。

storm-control unicast　命令用于开启对未知名单播风暴的控制功能。

说明：风暴控制级别的值不应该设置太小。　3 种风暴控制功能不一定全部开启，应根据网络环境适当开启。

2、关闭风暴控制功能：

命令：

```
Switch(config)#　interface　interface-id
Switch(config-if)#　no storm-control broadcase
Switch(config-if)#　no storm-control multicast
Switch(config-if)#　no storm-control unicast
```

配置举例：

```
Switch>　enable
Switch#　configure terminal
```

```
Switch(config)#       interface f0/1
Switch(config-if)#        storm-control level 20
Switch(config-if)#        storm-control broadcase
Switch(config-if)#        storm-control multicast
Switch(config-if)#        end
Switch#
```

本例在 f0/1 口上启用了广播和组播的风暴控制功能， 限制广播或组播的流量不能超过最大带宽的 20% 。同时 f0/2~f0/8 也都启用了该风暴控制功能。

- 查看风暴控制信息

模式： 特权模式。

命令：

Switch# show storm-control interface-id

interface-id 是可选的，用于查看指定接口的风暴控制信息。如：

```
Switch#    show storm-control
interface              Broadcase         Multicast         Unicast             Level
---------              ---------         ---------         -------          --------
Fa0/1                    Enable              Enable           Disable            20%
Fa0/2                    Enable              Enable           Disable            20%
Fa0/3                    Enable              Enable           Disable            20%
Fa0/4                    Enable              Enable           Disable            20%
Fa0/5                    Enable              Enable           Disable            20%
Fa0/6                    Enable              Enable           Disable            20%
Fa0/7                    Enable              Enable           Disable            20%
Fa0/8                    Enable              Enable           Disable            20%
Fa0/9                   Disable             Disable          Disable            100%
Fa0/10                  Disable             Disable          Disable            100%
Fa0/11                  Disable             Disable          Disable            100%
Fa0/12                  Disable             Disable          Disable            100%
.....
```

各个栏目依次为：接口、 Broadcase(广播风暴)、Multicast(组播风暴)、Unicast(未知名单播风暴)、控制级别。

“ Enable 表示开启， “ Disable 表示关闭。

四：配置预防 DoS 攻击的入口过滤

本部分包括以下内容：

DoS 攻击概述

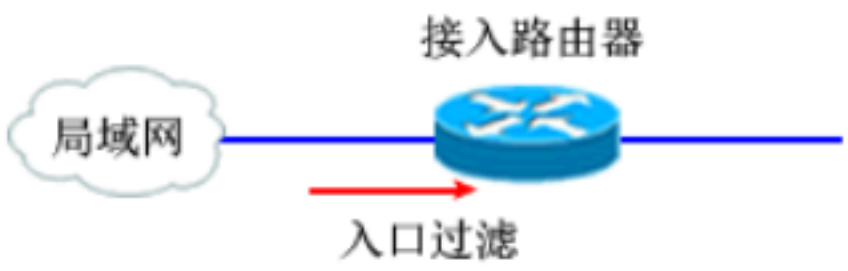
拒绝服务攻击（ DoS ）是目前互联网上常见的攻击手段。 DoS 攻击方式有很多种，最基本的 DoS 攻击是利用大量的合理服务请求来占用服务资源，使合法用户无法得到服务的响应。而攻击报文多采用伪装源 IP 地址以防暴露其踪迹。

预防 DoS 攻击的方法之一就是在网络的接入设备上设置入口过滤，来限制伪装源 IP 的报文进入网络，这样可以在攻击的早期防止 DoS 的发生，因而具有较好的效果。 ISP 可通过此项措施防止攻击进入 Internet ，局域网的网管也有义务确保局域网不会成为此类攻击的发源地。

锐捷交换机采用基于 RFC2827 的入口过滤规则来预防 DoS 攻击，该过滤采用硬件实现， 不会给网络转发增加负担。

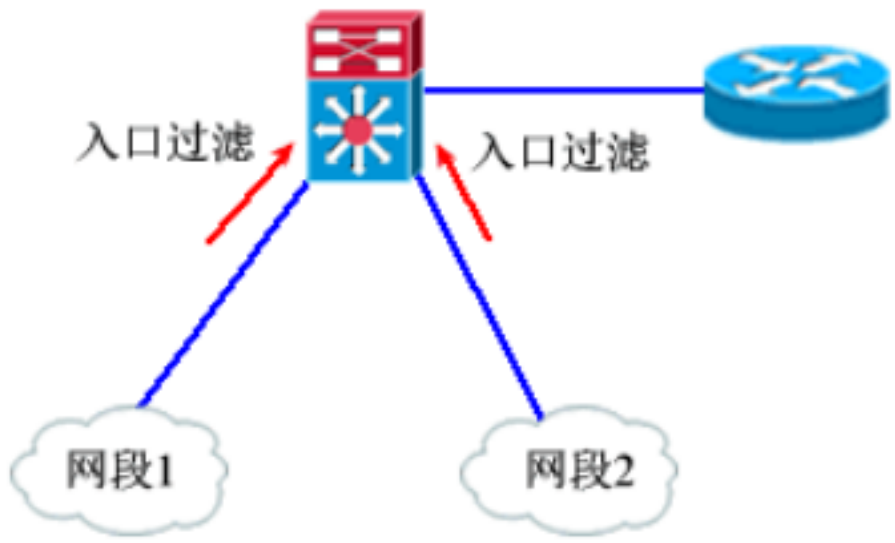
入口过滤的设置位置通常有两种：

1、ISP 在接入路由器上设置：



这种设置可防范攻击从局域网进入 Internet 。

2、局域网在三层交换机上设置：



这种设置可防范局域网内部发起的攻击。

在三层交换机上配置　DoS　过滤

在缺省情况下，　3 层交换机的预防　DoS 攻击的入口过滤功能是关闭的，配置时，需要打开该服务。

1、打开预防　DoS　攻击入口过滤的开关：

模式：接口配置模式。

命令：

Switch(config-if)#　　ip deny spoofing-source

这条命令用于打开指定接口的入口过滤开关。

说明：

1、这条命令只能用于　3 层口。

2、过滤开关打开后，系统会自动为该接口生成一个　　ACL，ACL 的名称为 auto_defeat_dos_　　interfaceID　，其中 interfaceID　　是接口名。假设这个　3 层口的 IP 地址

是 192.168.5.1/24 ，则生成的 ACL 的内容为：

```
permit 192.168.5.0 0.0.0.255
permit host 0.0.0.0
deny any
```

这个 ACL 会作用在接口的传入检查中， 它只允许源地址和 192.168.5.0 匹配的数据报传入，以及源地址为 0.0.0.0 的数据报传入（这种数据报是 DHCP 请求报文），如果源地址是其它值，说明是伪造的，交换机会直接把它丢弃。

3、你只能在和下层网段直连的接口上配置过滤功能，不要在和上层网络相连的接口（如 Uplink 口）上配置过滤功能，这会导致源自 Internet 的各种源 IP 报文无法进入该网段。

4、如果在接口上有一个自定义的 ACL，则它不能和过滤生成的 ACL 同时应用。解决方法是不开启过滤功能，但在自定义的 ACL 中加入过滤用的语句。

5、在设置了过滤功能后，如果修改了接口的 IP 地址，必须先关闭过滤功能然后再打开，这样才能使入口过滤对新的地址生效。

2 、 关闭入口过滤功能：

模式： 接口配置模式。

命令：

Switch(config-if)# no ip deny spoofing-source

3 、查看入口过滤配置：

模式： 特权模式。

命令：

Switch# show access-group

本命令用于查看 ACL。

配置举例 1 ：在一个 3 层路由口上启用入口过滤功能。

```
Switch>    enable
Switch#    configure terminal
Switch(config)#        interface f0/3
Switch(config-if)#         no switchport
Switch(config-if)#         ip address 192.168.30.1 255.255.255.0
Switch(config-if)#         ip deny spoofing-source
Switch(config-if)#         end
Switch#
```

配置后会生成一个名为 auto_defeat_dos_fastethernet_3 的 ACL，并且被关联在 f0/3 的传入端，它会禁止源 IP 为 192.168.30.0 以外的数据报从此接口进入交换机。（ DHCP 请求报文除外）

配置举例 2 ：在一个 3 层 SVI 接口上启用入口过滤功能。

```
Switch>    enable
Switch#    configure terminal
Switch(config)#        interface vlan 2
Switch(config-if)#         ip address 192.168.120.1 255.255.255.0
Switch(config-if)#         ip deny spoofing-source
Switch(config-if)#         end
Switch#
```

配置后会生成一个名为 auto_defeat_dos_vlan_2 的 ACL，并且被关联在 vlan 2 的传入端，它会禁止源 IP 为 192.168.120.0 以外的数据报从此接口进入交换机。 （DHCP 请求报文除外）

五：配置防范扫描攻击的系统保护

本部分包括以下内容：

扫描攻击概述

许多黑客和网络病毒的入侵都是从扫描网络内活动的主机开始的，大量的扫描报文也会占用网络带宽，影响网络通信性能。

扫描攻击主要有两种：

1、对某一 IP 地址段进行不断扫描。这种扫描攻击危害最大，会消耗大量网络带宽，增加交换机的负担。

2、向不存在的 IP 地址发送大量报文。这种攻击会消耗交换机的 CPU 资源，也有一定危害。

锐捷交换机可以在接口上启用防扫描的系统保护功能，当发现可能的扫描攻击时，会把发动攻击的 IP 地址进行隔离，在一段时间后再解除隔离。管理员也可以通过查看日志获取攻击的信息，从而采取进一步手段。

在三层交换机上配置系统保护

在缺省情况下， 3 层交换机上防扫描的系统保护功能是关闭的， 配置时， 需要打开该服务。

1、打开系统保护功能：

模式： 接口配置模式。

命令：

Switch(config-if)# system-guard enable

这条命令用于打开指定接口的系统保护功能。

说明： 这条命令只能用于 3 层口。你可以使用 interface range 命令在一批接口上进行设置。

2、关闭系统保护功能：

模式： 接口配置模式。

命令：

Switch(config-if)# no system-guard

3、配置系统保护参数：

模式： 接口配置模式。

①配置攻击阀值：

攻击阀值是判断是否发生扫描攻击的条件，当系统检测到连续的扫描次数超过设定的阀值时就认为发生了扫描攻击。

攻击阀值有两个：一是 scan dest ip attack packets ，它用于判断是否发生对一批网段进行扫描的攻击，每个端口的默认值都是每秒 10 个；另一是 same dest ip attack packets ，它用于判断是否发生不存在的 IP 发送报文的攻击，每个端口的默认值都是每秒 20 个。你可以用命令修改它们。

命令：

Switch(config-if)# system-guard scan-dest-ip-attack-packets number
Switch(config-if)# system-guard same-dest-ip-attack-packets number

scan dest ip attack packets 的取值范围是 0~1000 ，单位是每秒报文数，默认值为 10 。如果设置为 0 表示不对这种攻击进行监控。

same dest ip attack packets 的取值范围是 0~2000 ，单位是每秒报文数，默认值为 20 。如果设置为 0 表示不对这种攻击进行监控。

说明： 如果把攻击阀值设置太小，会导致判断攻击的准确度变差，容易误隔离正常上网的主机。

②配置隔离时间：

当保护系统发现攻击时，会自动隔离发动攻击的 IP 地址，隔离一段时间该 IP 地址会自动恢复通信。

命令：

Switch(config-if)# system-guard isolate-time time

隔离时间的取值范围是 30~3600 ，单位是秒，默认值为 120 秒。

说明：当用户被隔离时， 会发一个 LOG 记录到日志系统， 解除隔离时也会发一个 LOG 通知，管理员可以在日志中进行查询。

③配置监控主机的最大数目：

这个数目是同时被隔离的和监控的 IP 地址的最大数量。

命令：

Switch(config-if)# system-guard detect-maxnum number

number 的取值范围是 1~500 ，默认值为 100 个。

说明： 一般来说， 这个数目保持在 “实际运行的主机数 /20 ”左右即可， 当发现实际隔离的主机数已接近最大数值时，应适当扩大此数值。但如果你把它改小，会引起当前隔离的主机数据清空。

4 、手工解除隔离的主机：

被隔离的 IP 在隔离时间到后会自动解除隔离，你也可以用命令提前解除某些主机的隔离。

模式： 特权模式。

命令：

Switch# clear system-guard interface interface-id ip-address ip-address

用 clear system-guard 命令可清除所有隔离的 IP ；

用 clear system-guard interface interface-id 命令可清除指定接口下所有隔离的 IP ；

用 clear system-guard interface interface-id ip-address ip-address 命令可清除指定接口下指定的 IP。

配置举例：

```
Switch>  enable
Switch#  configure terminal
Switch(config)#      interface range f0/1-5
Switch(config-if)#       system-guard enable
Switch(config-if)#       system-guard scan-dest-ip-attack-packets 20
Switch(config-if)#       system-guard same-dest-ip-attack-packets 30
Switch(config-if)#       end
Switch#
```

本例假设 f0/1~f0/5 都已经配置为 3 层路由口，然后在它们上面启用系统保护功能。

系统保护信息的查看

模式： 特权模式。

1、查看系统保护信息：

Switch# show system-guard interface interface-id

interface interface-id 是可选的，用于查看指定接口的 IP 系统保护信息。如：

```
Switch#  show system-guard
detect-maxnum number : 100              监控主机的最大数目
isolated host number : 11           已隔离的主机数
interface       state       isolate time       same-attack-pkts          scan-attack-pkts
---------       -------      ------------       ----------------          ----------------
Fa0/1           ENABLE      120                      20                        10
```

```
Fa0/2          DISABLE      110                21                 11
.....
```

2、查看被隔离的主机：

Switch# show system-guard isolated-ip interface interface-id

interface interface-id 是可选的，用于查看指定接口的被隔离主机。如：

```
Switch#  show system-guard isolated-ip
interface        ip-address          isolate reason        remain-time(second)
---------      --------------      -----------------      -------------------
Fa0/1          192.168.5.119        scan ip attack              110
Fa0/1          192.168.5.131        same ip attack               62
```

各个栏目依次为：隔离 IP 出现的端口、隔离的 IP 地址、隔离原因、隔离的剩余时间。

一般交换机的硬件只支持每端口隔离 100~120 个 IP 地址，如果一些用户的 isolate reason 中显示“ chip resource full ，表明这些用户实际上没有被隔离，管理员应采取其它措施来处理这些攻击者。

3、查看被监控的主机：

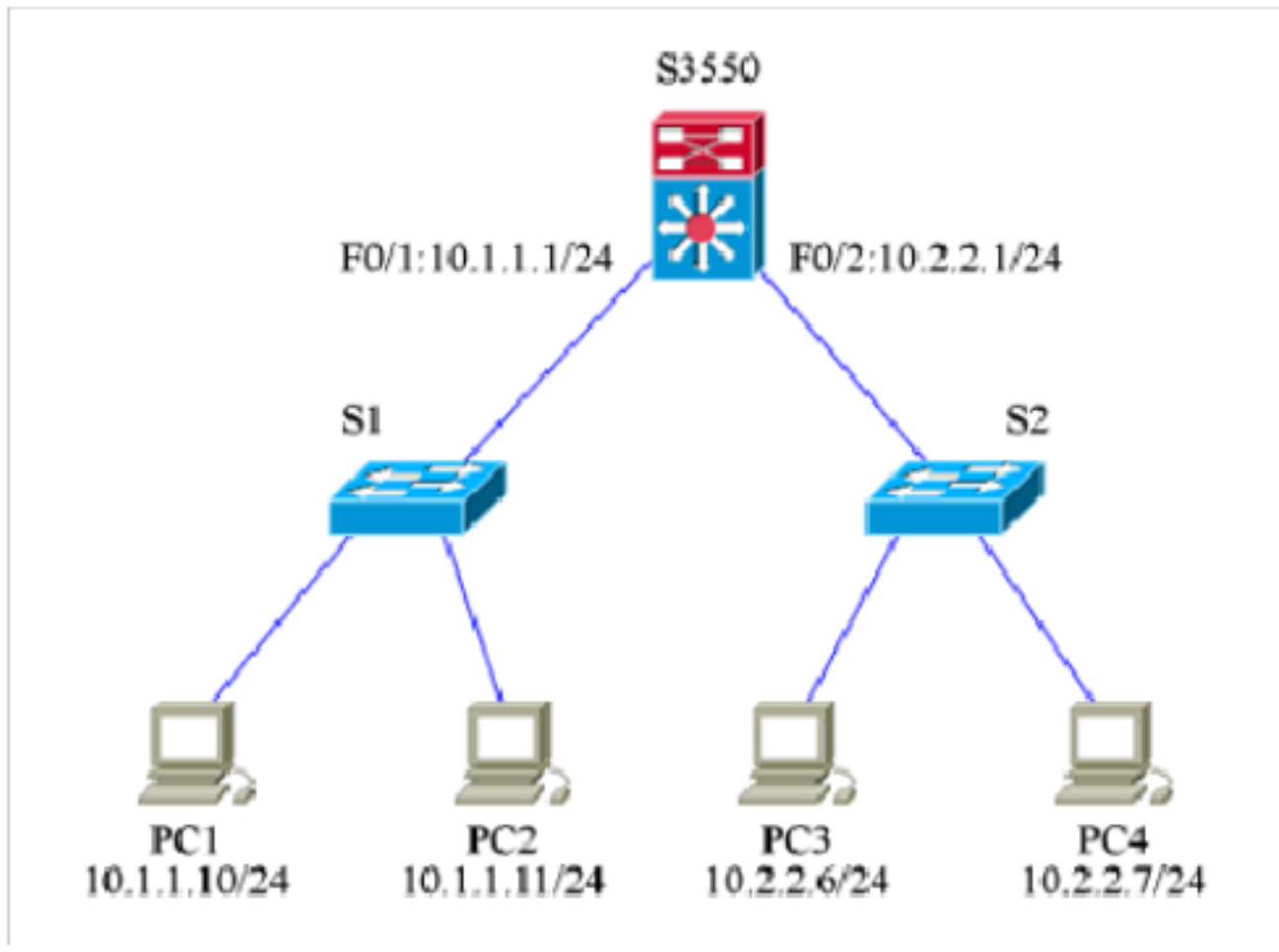
Switch# show system-guard detect-ip interface interface-id

被监控的主机是指被怀疑正在进行攻击。 interface interface-id 是可选的，用于查看指定接口的被监控主机。如：

```
Switch#  show system-guard detect-ip
interface        ip-address        same ip attack packets        scan ip attack packets
---------      --------------      ----------------------      --------------------
Fa0/1          192.168.5.110                0                           8
Fa0/1          192.168.5.121                12                          2
```

第四部分：交换机配置举例 **********

一：实例 ---- 用 3 层交换机划分子网



3 层交换机 S3550 把局域网分割成两个子网：

子网 1：10.1.1.0/24 ，连接在 FastEthernet0/1 接口，网关地址为 10.1.1.1/24 。

子网 2：10.2.2.0/24 ，连接在 FastEthernet0/2 接口，网关地址为 10.2.2.1/24 。

配置 S3550 ：

```
Switch>  enable
Switch#  configure terminal
!  配置交换机名字
Switch(config)#  hostname S3550
!  配置 F0/1 为 3 层路由口
S3550(config)#  interface f0/1
S3550(config-if)#  no switchport
S3550(config-if)#  ip address 10.1.1.1 255.255.255.0
!  配置 F0/2 为 3 层路由口
S3550(config-if)#  interface f0/2
S3550(config-if)#  no switchport
S3550(config-if)#  ip address 10.2.2.1 255.255.255.0
S3550(config-if)#  exit
!  启用 IP 路由
S3550(config)#  ip routing
S3550(config)#  end
!  查看配置结果
S3550#  show running-config
!  保存配置
S3550#  copy running-config startup-config
```

说明：

no switchport　　命令用于把 2 层口转换为 3 层路由口。只有 3 层口才能配置 IP 地址，2 层口不能配置。

ip routing　　命令用于启用 IP 路由。如果不启用 IP 路由功能，两个子网间将不能通信。（有些种类交换机的 IP 路由默认是启用的，此时可以没有此命令）。

在本网络中，两个 2 层交换机 S1 和 S2 不需要进行配置。

配置计算机时， PC1 和 PC2 的默认网关应该设置为 10.1.1.1 ，PC3 和 PC4 的默认网关应该设置为 10.2.2.1 。

效果验证：

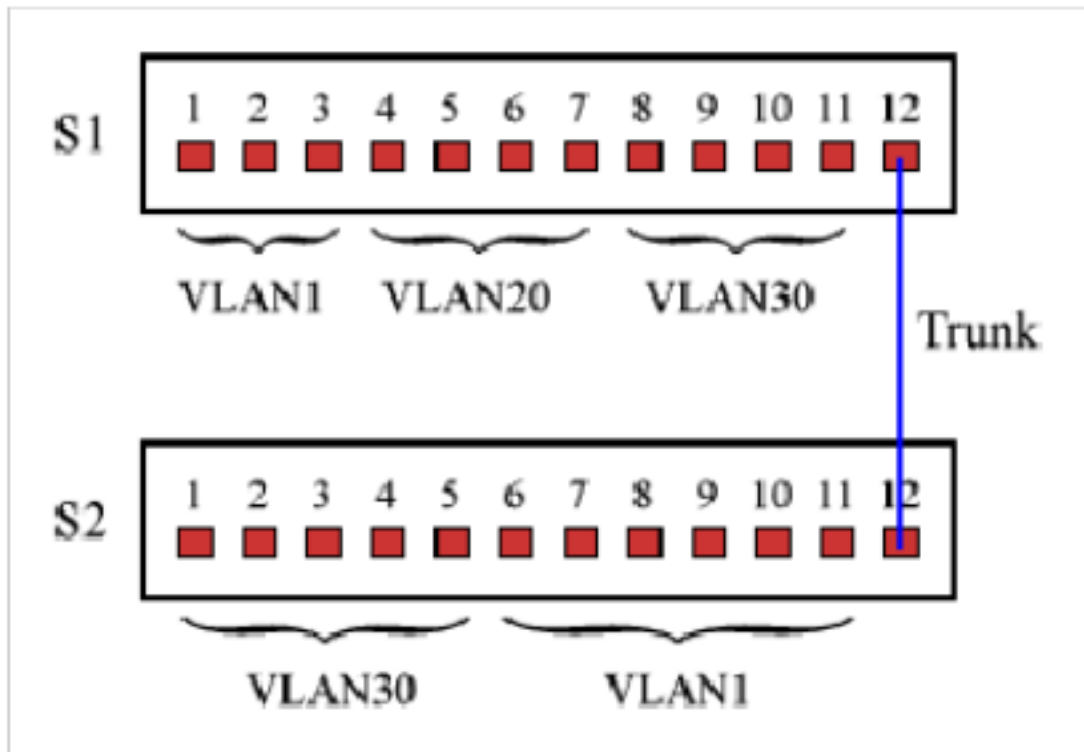
PC1 和 PC2 属于同一个子网，彼此间可以通信，也能通过 “网上邻居”共享文件。 PC3 和 PC4 也是如此。

两个子网间也可以通信，但不能通过 “网上邻居”共享彼此的文件。

二：实例 ---- 交换机 VLAN 的划分

作者：风林

来源：风林的家



两台 S3550-12 交换机利用 VLAN 分割了几个虚拟局域网，使用时属于同一个 VLAN

的计算机之间可以通信，属于不同 VLAN 的计算机之间不能通信。

配置 S1 ：

```
S1> enable
S1# configure terminal
! 创建 VLAN20
S1(config)# vlan 20
S1(config-vlan)# name VLAN20
! 创建 VLAN30
S1(config-vlan)# vlan 30
S1(config-vlan)# name VLAN30
S1(config-vlan)# exit
! 把 F0/4~F0/7 指派给 VLAN20
S1(config)# interface f0/4
S1(config-if)# switchport access vlan 20
S1(config-if)# interface f0/5
S1(config-if)# switchport access vlan 20
S1(config-if)# interface f0/6
S1(config-if)# switchport access vlan 20
S1(config-if)# interface f0/7
S1(config-if)# switchport access vlan 20
! 把 F0/8~F0/11 指派给 VLAN30
S1(config-if)# interface f0/8
S1(config-if)# switchport access vlan 30
S1(config-if)# interface f0/9
S1(config-if)# switchport access vlan 30
S1(config-if)# interface f0/10
S1(config-if)# switchport access vlan 30
S1(config-if)# interface f0/11
S1(config-if)# switchport access vlan 30
! 把 F0/12 配置为 Trunk 模式
S1(config-if)# interface f0/12
S1(config-if)# switchport mode trunk
S1(config-if)# end
! 查看配置结果
S1# show vlan
! 保存配置
S1# copy running-config startup-config
```

配置 S2 ：

```
S2> enable
```

```
S2#  configure terminal
!  创建  VLAN30
S2(config)#      vlan 30
S2(config-vlan)#        name VLAN30
S2(config-vlan)#        exit
!  把 F0/1~F0/5      指派给  VLAN30
S2(config)#      interface range f0/1-5
S2(config-if)#       switchport access vlan 30
!  把 F0/12   配置为  Trunk   模式
S2(config-if)#       interface f0/12
S2(config-if)#       switchport mode trunk
S2(config-if)#       end
!  查看配置结果
S2#  show vlan
!  保存配置
S2#  copy running-config startup-config
```

说明：

为了简化配置过程，在配置　S2 时采用了接口组的配置方式，你也可以在　S1 中使用此方法。

加入 VLAN 的接口必须是 Access 口，你可以添加　switchport mode access　　命令来保证这一点。

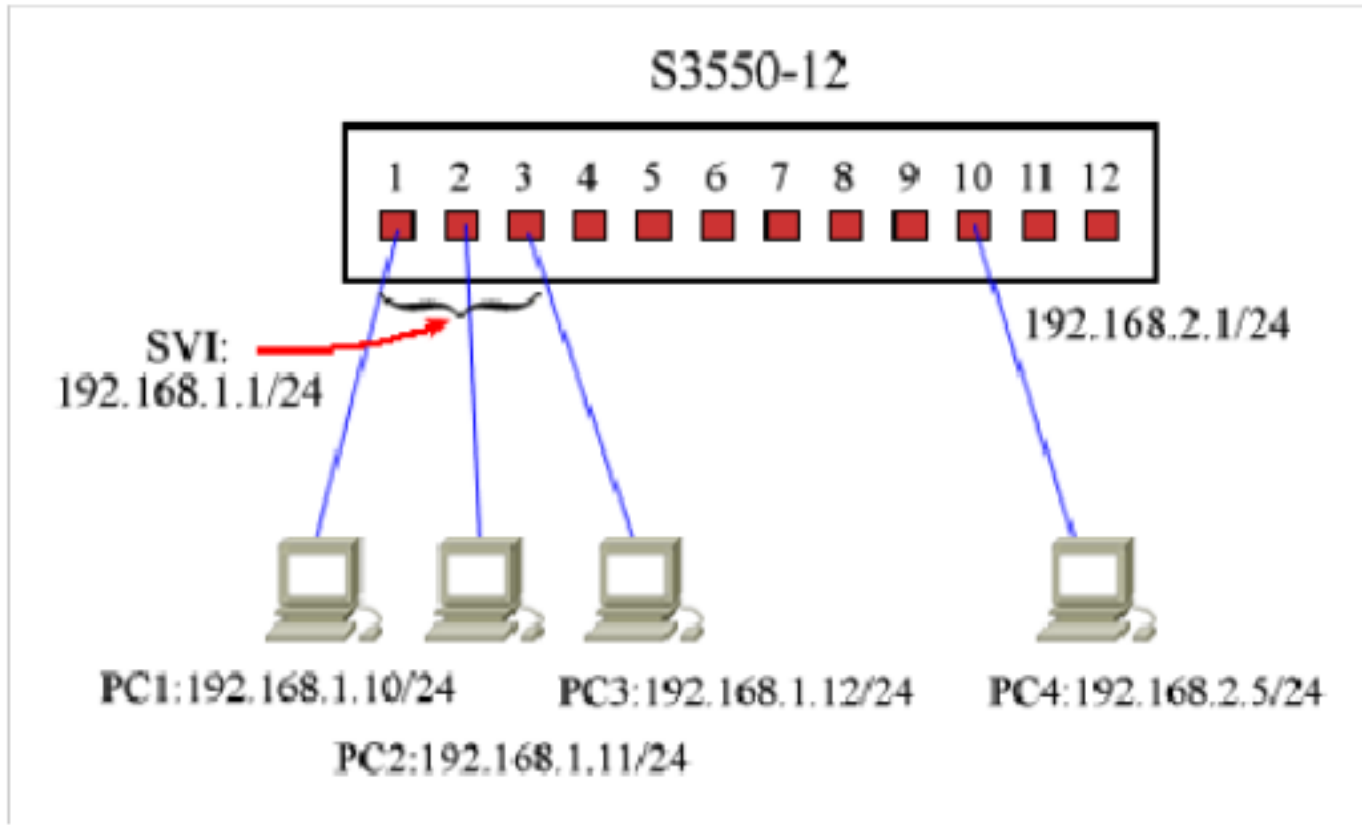
创建 VLAN 的过程可以没有，　当你把一个接口加入一个不存在的　VLAN 时，交换机会自动创建此 VLAN。

所有未指派的接口默认属于　VLAN1。

效果验证：

在交换机上连接计算机，连接在同一个　VLAN 上的计算机间可以通信，而连接在不同 VLAN 上的计算机间不能通信。

三：实例 ----　交换机 SVI　接口的定义



把交换机的 F0/1~F0/3 定义为一个 3 层 SVI 接口， IP 地址为 192.168.1.1/24 。把 F0/10 定义为一个 3 层路由口， IP 地址为 192.168.2.1/24 。

配置交换机：

```
Switch>  enable
Switch#  configure terminal
! 创建一个和 SVI 对应的 VLAN
Switch(config)#     vlan 2
Switch(config-vlan)#       name VLAN2
Switch(config-vlan)#       exit
! 把 F0/1~F0/3   指派给 VLAN2
Switch(config)#     interface f0/1
Switch(config-if)#       switchport access vlan 2
Switch(config-if)#       interface f0/2
Switch(config-if)#       switchport access vlan 2
Switch(config-if)#       interface f0/3
Switch(config-if)#       switchport access vlan 2
! 为 VLAN2 配置 IP 地址，使它成为一个 3 层 SVI 接口
Switch(config-if)#       interface vlan 2
Switch(config-if)#       ip address 192.168.1.1 255.255.255.0
Switch(config-if)#       no shutdown
! 把 F0/10 配置为 3 层路由口
Switch(config-if)#       interface f0/10
Switch(config-if)#       no switchport
Switch(config-if)#       ip address 192.168.2.1 255.255.255.0
Switch(config-if)#       exit
! 启用 IP 路由
Switch(config)#     ip routing
```

```
Switch(config)#       exit
!  查看配置结果
Switch#    show vlan
Switch#    show running-config
Switch#    show ip route
!  保存配置
Switch#    copy running-config startup-config
```

说明：

SVI 是一种和 VLAN 相对应的 3 层口，你只需要给 VLAN 配置一个 IP 地址就成了 SVI 接口。

SVI 是一种由多个物理接口组成的 3 层口，用它们连接的计算机构成一个网段，比如图中的 PC1、PC2、PC3 与 SVI 在同一个网段中，彼此可以共享资源。

在实际应用中， SVI 多用做交换机的管理接口，你也可以通过 SVI 使处于不同网段的 VLAN 可以通信。

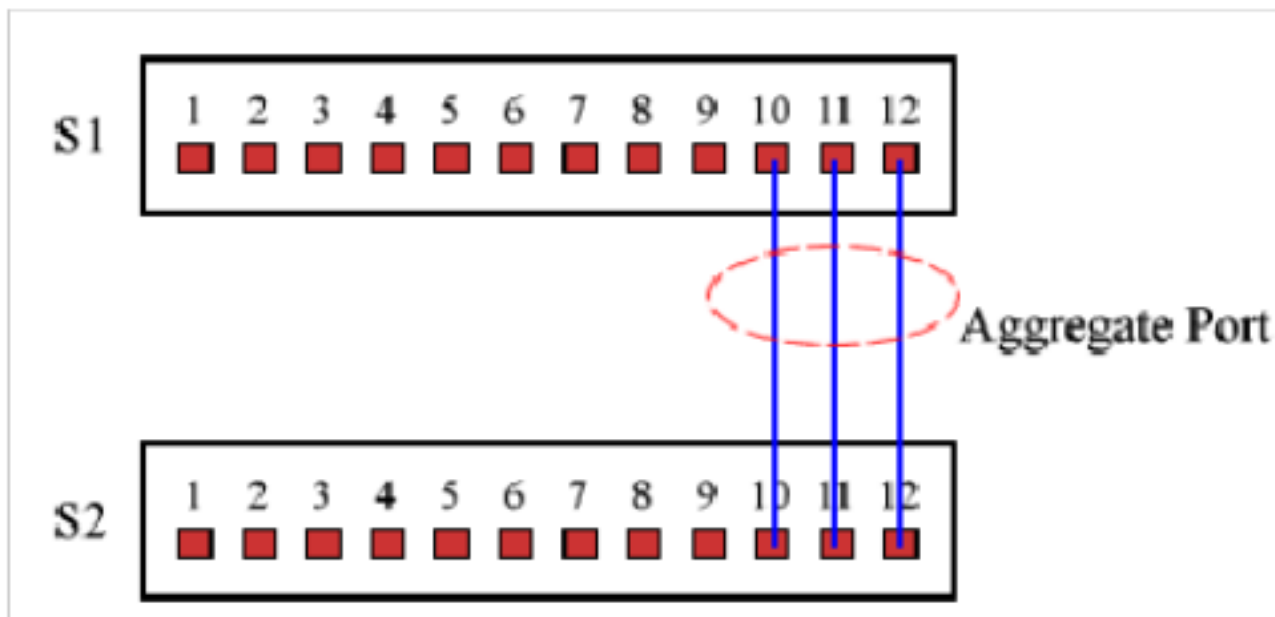
效果验证：

PC1、PC2、PC3 彼此间可以通信，也能通过 “网上邻居”共享文件。它们和 PC4 可以通信，但不能通过 “网上邻居”共享文件。

四：实例 ---- 交换机通道口的配置

作者：风林

来源：风林的家



两台交换机之间通过 F0/10~F0/12 互联，把它们定义为 Aggregate Port 接口，使之成为两个交换机间的高速通道。

配置交换机 S1 ：

```
S1> enable
S1# configure terminal
! 把 F0/10~F0/12 加入到同一个 Aggregate Port 接口组中
S1(config)# interface f0/10
S1(config-if)# port-group 2
S1(config-if)# interface f0/11
S1(config-if)# port-group 2
S1(config-if)# interface f0/12
S1(config-if)# port-group 2
S1(config-if)# end
! 查看配置结果
S1# show aggregateport 2
S1# show running-config
! 保存配置
S1# copy running-config startup-config
```

配置交换机 S2 ：

```
S2> enable
S2# configure terminal
! 把 F0/10~F0/12 加入到同一个 Aggregate Port 接口组中
S2(config)# interface f0/10
S2(config-if)# port-group 2
S2(config-if)# interface f0/11
S2(config-if)# port-group 2
S2(config-if)# interface f0/12
S2(config-if)# port-group 2
S2(config-if)# end
! 查看配置结果
S2# show aggregateport 2
S2# show running-config
! 保存配置
S2# copy running-config startup-config
```

说明：

Aggregate Port 接口用于构建交换机之间的高速通道，它的速率是组成它的各个接口速率之和。

Aggregate Port 接口由多个物理接口组成，接口用一个 ID 号标识（本例为 2），使用 port-group 命令可以向其中添加接口。

不同型号的交换机对 Aggregate Port 接口的支持不同，在锐捷的 3550 系列交换机中：

S3550-24 交换机最大支持 6 个 AP，每个 AP 最多包含 8 个接口，其中 6 号 AP 只为模块 1 和模块 2 保留；

S3550-48 交换机不支持 AP；

S3550-12G 、S3550-24G 交换机最大支持 12 个 AP，每个 AP 最多包含 8 个接口；

S3550-12SFP/GT 交换机最大支持 12 个 AP，每个 AP 最多包含 8 个接口。

如果需要配置 3 层 Aggregate Port ，可以在配置中增加以下内容：

```
S1(config)#     interface aggregateport 2
S1(config-if)#      no switchport
S1(config-if)#      ip address 192.168.1.1 255.255.255.0
```

这样交换机 S1 的 AP2 就成为一个 3 层口，它连接了一个地址为 192.168.1.0/24 的网段。

锐捷 S3550 配置手册目录：

作者：风林

来源：风林的家

锐捷设备的配置命令与思科 (Cisco) 设备的配置命令基本相同，只是部分功能有所区别。

目录：

交换机概述：

- 交换机的几种配置方法
  - 控制台
  - 远程登录
  - 其它配置方法
- 命令行 (CLI) 操作
  - 命令模式
  - 命令模式的切换
  - CLI 命令的编辑技巧
  - 常见 CLI 错误提示
  - 使用 no 和 default 选项
- 交换机的初始化配置
  - 交换机的初始化配置
  - setup 命令
- 配置文件的保存、查看与备份
  - 查看配置文件
  - 保存配置文件
  - 删除配置文件
  - 备份配置文件
- 文件系统
  - 文件系统概述
  - 文件操作
  - 目录操作
- 系统文件的备份与升级
  - 搭建环境
  - 用 TFTP 传输文件
  - 用 Xmodem 传输文件
  - ROM 监控模式
- 密码丢失的解决方法

交换机的基本配置：

- 配置主机名
- 配置口令
  - 配置控制台口令
  - 配置远程登录口令
  - 配置特权口令

- 配置管理 IP 和默认网关
  - 配置交换机的管理 IP
  - 配置交换机的默认网关
- 远程登录 (Telnet) 的配置
  - 远程登录条件
  - 开启和禁止远程登录
  - 限制远程登录访问
  - 设置远程登录的超时时间
  - 查看 Telnet Server 的状态
- 配置接口的基本参数
  - 交换机接口的类型
  - 交换机接口的默认配置
  - 交换机接口配置的一般方法
  - 配置接口描述
  - 配置接口速率
  - 配置接口的双工模式
  - 禁用 / 启用交换机接口
  - 查看交换机接口信息
- 单个接口的配置
  - 2 层 Access Port （普通口）的配置
  - 2 层 Trunk Port （Trunk 口）的配置
  - 3 层 Routed Port （路由口）的配置
- VLAN 和 SVI 的配置
  - VLAN 的配置
  - SVI 的配置
- Aggregate Port 的配置
  - 2 层 Aggregate Port （通道口）的配置
  - 3 层 Aggregate Port （通道口）的配置
- 路由的配置与查看
  - 启用和关闭 IP 路由
  - 配置静态路由
  - 配置默认路由
  - 查看路由表
- RIP 协议的配置
  - RIP 协议的一般配置
  - RIP 协议参数的配置
- OSPF 协议的配置
  - OSPF 协议的一般配置

交换机的高级配置：

- 配置系统时间
  - 设置系统时间
  - 设置时区
  - 查看系统时间
- 配置 DHCP 代理
  - 多网段的 DHCP 构建
  - DHCP 代理的配置
- 接口风暴控制的配置
  - 风暴控制
  - 查看风暴控制信息
- 配置预防 DoS 攻击的入口过滤
  - DoS 攻击概述
  - 在三层交换机上配置 DoS 过滤
- 配置防范扫描攻击的系统保护
  - 扫描攻击概述
  - 在三层交换机上配置系统保护
  - 系统保护信息的查看

交换机配置举例：

- 用 3 层交换机划分子网
- 交换机 VLAN 的划分
- 交换机 SVI 接口的定义
- 交换机通道口的配置