NETGEAR 7000 系列网管交换机
管理手册 6.0

美国网件公司

2008 年 5 月

目录

关于这本手册

这个参考手册描述了如何安装、配置和故障排除 7000 系列全网管交换机。在这本手册黎的信息是提供给具有中等计算机和网络技能的读者使用的。

惯例、格式和范围

关于这本手册的惯例、格式和范围在下面的段落进行描述：

- **印刷上的习惯。**这本手册使用以下印刷上的习惯：

斜体	强调，书籍，光碟，URL 地址
粗体	使用者输入
固定	筛选文本，文件和服务器名称，扩展名，命令，IP 地址

- **格式。**这本手册使用以下格式来突出特别信息：

	注意：这个格式用来突出重要的或需要特别关注的信息。

	提示：这个格式用来突出一个将节省时间或资源的程序。

	警告：忽略这种类型的注解将导致设备的故障或损害。

	危险：这个是安全警告。疏忽留意这个通知将导致人身损害或

- **范围。**这本手册根据这些规范来撰写 7000 系列全网管交换机：

产品版本	7000 系列全网管交换机
手册发布时间	2007 年 1 月

	注意：产品的更新可查阅 NETGEAR 公司的网站 *http://kbserver.netgear.com/products/7xxx.asp*

如何使用这本手册

这本手册的 HTML 版本，如果提供，将包括以下：

- 按钮，  和  ，让用户每次一页地向前或向后浏览这本手册
- 按钮  和  显示了目录。双击在目录或索引中的这个链接以直接到达这本手册中描述这个主题的地方。
- 按钮  能访问 NETGEAR 公司对于这个产品型号的在线知识库。
- 链接到全手册和个别章节的 PDF 版本。

如何打印这本手册

你可以根据你的需要选择下面任何一种方法来打印这本手册：

- 从 HTML 打印一页。这本手册 HTML 版本的每一页都专注于一个主要的题目。选择文件>从浏览器菜单打印来打印该页的内容。
- 从 PDF 打印。你的电脑必须安装免费的 Adobe Acrobat 来阅读和打印 PDF 文件。

— 打印 PDF 版本的一个章节。使用在任何一个页面左边的链接*这个章节*。
你要阅读的 PDF 版本的这个章节在视窗浏览器中打开。
点击你的视窗浏览器左上部的打印图标。

— 打印 PDF 版本的完整手册。使用在任何一个页面左边的*完整 PDF 手册*链接。
PDF 版本的完整手册在视窗浏览器中打开。
点击你的视窗浏览器左上部的打印图标。

提示：如果你的打印机支持在一张纸上打印两面，你可以通过选择这个功能来节省纸张和打印墨水。

修订资料

部件号	版本号	描述
202-10238-01	1.0	产品更新：新的固件和新的用户接口

第一章 介绍

这个文档提供了对 6.0 版本软件特性的命令行界面和 Web 配置选项的理解。

文档组织结构

这个文档提供了在一个典型网络中使用交换机软件的示例。它描述了 7000 系列全网管交换机特定功能的使用和优势，包括使用命令行界面和 Web 接口配置的功能和信息。
交换机软件可运作在二层的交换、三层的路由或者交换/路由的结合。交换机同样包括对网络管理和服务质量功能的支持，例如访问控制列表和区分服务（Differentiated Service）。你选择启用哪项功能取决于你的网络的大小和复杂程度：这个文档描述一些常用功能的配置。
这个文档包含以下的配置信息：

- 二层
  — VLANs
- 三层
  — 端口路由
  — VLAN 路由
  — 虚拟路由冗余协议（VRRP）
  — RIP
  — OSPF
  — Proxy ARP
- 服务质量（QoS）
  — 访问控制列表（ACLs）
  — 服务类型（CoS）
  — 区分服务
- 多播
  — IGMP 侦听
- 安全
  — 服务拒绝
  — 端口安全
- 操作系统
  — 双配置
- 工具
  — 告警管理
  — 路由跟踪
  — 配置脚本
  — Advance Keying
  — 登录公告
  — 端口镜像

— 简单网络时间协议
— 系统日志
— 数据迁移

读者

使用这本指导：

- 负责使用交换机软件配置和运作网络的有经验的系统管理员
- 一级和二级的技术支持提供者

为了从这本指导中获取最多的东西，你需要对交换机软件基础有一定的理解，并且已阅读你的网络设备平台的说明。同时你需要有以太网和网络的相关基础知识。

命令行界面文档

命令行参考提供了用于配置交换机和堆叠的命令行信息。文档提供了 CLI 描述、语法和默认值。

相关的文档

先阅读本交换机产品的发行注释。发行注释给出了交换、路由、SNMP、配置、管理和其它插件的特定功能平台的详细描述。另外，参阅以下的出版物：

- Netgear 7000 系列全网管交换机快速安装指南
- Netgear Prosafe 7X00 系列全网管交换机 CLI 参考手册。这个系列有三个文档，选择适合你产品的那个。
- Netgear 硬件安装指南

这些文档可以在http://www.NETGEAR.com上找到。

第二章 开启交换机

开始配置前连接一个终端到交换机。

In-band 和 Out-of-band 连接

咨询系统管理员以决定你将配置交换机用于 in-band 或 out-of-band 连接。

配置 In-band 连接

In-band 连接允许你从一个远端的工作站使用以太网络访问交换机。你需要配置交换机的 IP 信息（IP 地址、子网掩码和默认网关）来使用 in-band 连接。
使用下面的方法来配置 In-band 连接：

- BootP 或者 DHCP
- EIA-232 端口

使用 BootP 或者 DHCP

你可以通过网络或 BootP 或 DHCP 以太网服务端口来指派 IP 信息。与你的系统管理员确定是否已经启用了 BootP 或 DHCP。
你需要配置 BootP 或 DHCP 服务器用于交换机的 IP 信息——通过连接串行端口，使用 show network 命令来获取信息。通过以下的值来设置 BootP 或 DHCP 服务器：

IP 地址 交换机唯一的 IP 地址。每个 IP 参量由四个从 0 到 255 的十进制的数字构成。默认所有 IP 参量是 0（0.0.0.0）。
子网掩码 局域网的子网掩码
网关 默认路由的 IP 地址，如果交换机是在局域网 IP 网段外的一个节点
MAC 地址 交换机的 MAC 地址

在设备了 BootP 和 DHCP 服务器后，当你第一次连接交换机到你的网络，将会对交换机配置上面提供的信息。交换机已经准备好通过网络进行 in-band 连接。
如果你不使用 BootP 或者 DHCP，用以下描述的方法通过 EIA-232 端口访问交换机，并配置网络信息。

使用 EIA-232 端口

你可以使用本地或远程的连接终端来通过 EIA-232 端口配置 in-band 管理。

1. 使用本地的连接终端。连接一个串口线到交换机的 EIA-232 端口，另外一端连接到终端或工作站的 COM 口。

对于远程的连接。连接串口线的一端到交换机的 EIA-232 端口，另一端到调制解调器。

2. 设置 VT100 终端仿真程序：
   a.开启终端
   b.启动 VT100 程序
3. 配置 COM 口：
   a.设置波特率 9600。
   b.设置数据格式 8bits，
   c.设置流控为无。
   d.在**属性**里选择正确的模式。
   e.选择终端功能键。
4. 输入许可的用户名和密码。默认用户名是 admin，密码是空。
   交换机安装和加载默认的配置。
5. 关闭网络配置协议以减少网络流量。输入以下命令：
   config network protocol none
6. 通过以下命令设置 IP 地址、子网掩码和网关地址：
   confige network parms *ipaddress netmask gateway*

IP 地址 交换机唯一的 IP 地址。每个 IP 参量由四个从 0 到 255 的十进制的数字构成。默认所有 IP 参量是 0（0.0.0.0）。

子网掩码 局域网的子网掩码

网关 默认路由的 IP 地址，如果交换机是在局域网 IP 网段外的一个节点

7. 为了让这些设置在交换机重启后人能保留，输入 **Ctrl-Z** 返回到主提示，在主菜单提示输入 **save config**，并键入 y 确认。
8. 查看更改和确认 in-band 信息，输入命令：**show network**。
9. 交换机配置了 in-band 连接，并准备好基于 Web 的管理。

配置 Out-of-Band 连接

为了使用 out-of-band 连接来监控和配置交换机，可以使用 console 接口来连接交换机到一个运行终端仿真软件的终端桌面系统。Console 接口连接器是一个公型 DB-9 连接器，被用作一个数据终端设备（DTE）连接器。

使用 console 接口需要以下的硬件设备：

- 具有串行接口运行 VT100 终端仿真软件的 VT-100 兼容的终端，或一个桌面，或一个便携式系统。
- 一个具有用于 console 接口的母型 DB-9 转接器的 RS-232 交叉线，和用于终端的适当转接器。

执行以下的任务来连接一个终端到交换机 console 接口使用 out-of-band 连通性：

1. 连接 RS-232 交叉线到运行 VT100 终端仿真软件的终端
2. 按以下的配置终端仿真软件：
   a. 选择合适的串口
   b. 设置波特率
   c. 设置数据格式为 8 数据比特，1 个停止比特，并无校验。
   d. 设置流控为 none。
   e. 在**属性**里选择正确的模式。

f. 选择终端 keys。

注意：当使用微软 Windows2000 的超级终端时，确认你已经安装了 Windows 2000 Service Pack 2 或更新的 Service Pack。只有这样，方向按键才能在超级终端 VT100 仿真软件上正常工作。

3. 连接 RS-232 交叉线的母型连接器到交换机的 console 接口，并扭紧外加螺丝。

开启交换机

1. 确认交换机的 console 接口是连接到 VT100 终端或通过 RS-232 交叉线连接到 VT100 终端模拟器。
2. 连接交换机到交流电源插座。

当本地的终端已经连接上，打开电源交换机会加电自检（POST）。POST 在每次初始化交换机时运行，并检查硬件设备以决定交换机在引导前是否完全运作的。如果 POST 侦测到致命性的问题，开始程序将终止。如果能成功地经过 POST，一个有效的可运行镜像将载入 RAM。POST 信息在终端上显示，并指示检测成功与否。引导过程运行大概 60 秒。

初始化配置

初始化简单配置程序是基于下面的假定：

- 交换机在之前没有配置并和你接收时的状态一致。
- 交换机成功引导。
- console 连接已经建立并且在 VT100 终端或终端模拟器的屏幕上显示 console 提示。

初始交换机配置是通过 console 接口执行的。在初始配置之后，你可以通过已经连接的 console 接口来管理交换机或通过在初始配置中定义的接口来远程管理。

交换机没有配置默认的用户名和密码。

要允许 Telnet 或 HTTP 远程管理交换机，所有下面的设置是必需的。

在设置交换机初始配置之前，从你的网络管理员处获取以下信息：

- 分配给管理接口的 IP 地址
- 网络的 IP 子网掩码
- 默认网关的 IP 地址

初始配置程序

你可以使用简易设置向导或命令行界面来运行初始配置。当交换机配置文件是空的，设置向导将自动启动。你可以在任何时刻输入[ctrl+z]来推出向导。要想获取 CLI 初始配置的更多信息，查阅*用户配置指南*。指南展示如何使用设置向导来初始化交换机配置。向导在交换机设置下面的配置：

- 建立初始特权用户账号和有效的密码。向导在设置过程中配置一个特权用户账号。
- 启用 CLI 登陆和 HTTP 访问使用本地认证设置。
- 设置管理接口的 IP 地址。

- 设置让特定 IP 地址使用 SNMP 管理的 SNMP 字段。如果 SNMP 管理不在这台交换机上使用，你可以忽略这一步。
- 允许你指定管理服务器的 IP 或允许从所有 IP 地址对交换机 SNMP 访问。
- 配置默认网关 IP 地址。

软件安装

这部分包含帮助你快速熟悉交换机软件的程序。在安装交换机软件之前，你应该确认交换机运行在最新的固件。

快速启动网络设备

1. 配置交换机用于 In-band 或 Out-of-band 的连通性。In-band 连接允许本地或从远端工作站访问软件。你必须配置设备的 IP 信息（IP 地址、子网掩码和默认网关）。
2. 打开电源。
3. 允许设备装载软件直到出现登陆提示。设备的初始状态被称为默认模式。
4. 当提示操作者登陆，进行以下的步骤：

— 在登陆提示里输入 admin。因为一连串的快速设置命令需要管理员帐户权限，登录到管理员帐户。
— 不用输入密码因为默认模式下不使用密码。
— 检查在命令行界面显示用户（User EXEC）提示。
— 输入 enable 从用户（User EXEC）模式转换到特权（Privileged EXEC）模式。
— 输入 configure 从特权（Privileged EXEC）模式切换到全局配置（Global Config）模式。
— 输入 exit 返回到之前的模式。
— 输入？显示在现行模式下可用的命令列表。

系统信息和系统设置

这部分描述你查看系统信息和设置网络设备所使用的命令。表 2-1 包含允许你查看或配置下面信息的快速启动命令：

- 软件版本
- 物理端口数据
- 用户账号管理
- IP 地址配置
- 从网络设备上传到 Out-of-Band 计算机（仅 XModem）
- 从 Out-of-Band 计算机下载到网络设备（仅 XModem）
- 从 TFTP 服务器下载
- 恢复出厂默认值

如果你配置任何网络参数，你需要执行下面的命令：

copy system:running-config nvram:startup-config

这条命令保存改变的设置到配置文件。你必须在正确的模式下运行命令。如果你不保存配置，所有配置上的改变将会在关闭电源或重启网络设备后丢失。在一个堆叠的环境，运行的配置被保存在堆叠中的所有单元。

表 2-1 描述了命令语法，执行命令所需要的模式、命令的目的和输出。

命令	模式	描述
show hardware	特权执行	显示硬件版本、MAC 地址和软件版本等信息
show users	特权执行	显示所有允许访问网络设备的用户 Access Mode 显示在网络设备上你是否可以改变参数（Read/Write）或者只是可以查看它们（Read Only）。出厂默认 admin 用户具有读/写的访问权限，而 guest 用户只有读的权限。最多可以有 5 个只读的用户。
show loginsession	用户执行	显示所有登录的会话信息。
users passwd <username>	全局配置	允许用户为登录设置密码或改变密码。 输入命令后提示要求旧的用户密码。没有旧密码则留空该相。 用户密码的长度不应超过 8 个字符。
copy system:running -config nvram:startup -config	特权执行	保存密码或所有其他的修改。 如果你没有保存配置，所有的改变将在网络设备断电或重启后丢失。在堆叠的环境，运行的配置被保存到堆叠中的所有单元。
logout	用户执行 特权执行	用户注销退出网络设备。
show network	用户执行	显示下面的网络配置信息： •IP Address-接口的 IP 地址（默认：0.0.0.0） •Subnet Mask-接口的 IP 子网掩码（默认：0.0.0.0） •Default Gateway-接口的默认网关（默认：0.0.0.0） •Burned in MAC Address-用于 in-band 连接的 MAC 地址 •Locally Administered MAC Address-可以配置来允许一个本地管理的 MAC 地址 •MAC Address Type-指定哪些 MAC 地址该被用于 in-band 连接 •Network Configurations Protocol Current-指示哪些网络协议正在被使用中（默认：无） •Management VLAN ID-指示管理 VLAN •Web Mode-显示是否启用 HTTP/Web •Java Mode-显示是否启用 java 模式
network parms <ipaddr> <netmask> [gateway]	特权执行	设置 IP 地址、子网掩码和网关地址。IP 地址和网关必须在同一个子网。IP 地址范围从 0.0.0.0 到 255.255.255.255。
copy nvram:startup -config <tftp://<ipadd	特权执行	开始上传配置文件、显示模式和上传的类型并确认上传正在进行中。

-ress>/<filepath>/ <filename>>		URL 必须按以下指定： xmodem:<filepath>/<filename> 例如：如果用户使用超级终端，则用户必须指示哪个文件将被计算机所接收。
copy nvram:errorlog <tftp://<ipaddress>/ <filepath>/<filename>	特权执行	开始错误日志的上传、显示模式和上传的类型并确认上传正在进行中。 URL 必须按以下指定： xmodem:<filepath>/<filename>
copy nvram:traplog <tftp://<ipaddress>/ <filepath>/<filename>	特权执行	开始上传陷进日志，显示模式和上传类型并确认上传正在进行中。 URL 必须按以下指定： xmodem:<filepath>/<filename>
copy <tftp:// <ipaddress>/<filepath> /<filename>> nvram:startup-config	特权执行	设置目标（下载）数据类型为一个镜像（system:image）或一个配置文件（nvram:startup-config）。 URL 必须按以下指定： xmodem:<filepath>/<filename> 例如：如果用户使用超级终端，用户必须指示哪个文件将被发送到网络设备。 一旦下载完代码，网络设备将自动重新启动。
copy <tftp:// <ipaddress>/<filepath> /<filename>> system:image	特权执行	设置目标(下载)数据类型为一个镜像(system:image)或一个配置文件（nvram:startup-config）。 URL 必须按以下指定： xmodem:<filepath>/<filename>
copy <tftp:// <ipaddress>/<filepath> <fielname>> nvram:startup-config	特权执行	设置目标（下载）数据类型为一个配置文件。 URL 必须按以下指定： tftp://<ipaddress>/<filepath>/<filename> 在开始 TFTP 服务器下载之前，你必须配置 IP 地址。
copy <tftp:// <ipaddress>/<filepath> /<filepath>> system:image	特权执行	设置目标（下载）数据类型为一个镜像。 URL 必须按以下指定： tftp://<ipaddress>/<filepath>/<filename> system:image 选项为下载的代码文件。
clear config	特权执行	当提示输入，键入 Yes 如果你想要清除所有在网络设备上的配置信息。
copy system:running -config nvram:startup -config	特权执行	当提示输入，键入 Yes 如果你想要保存配置信息到网络设备。
reload（或冷启动网络设备）	特权执行	当提示输入，键入 Yes 如果你想要重启系统。 你可以重启网络设备或冷启动网络设备。两者皆有效。

第三章 使用 Ezconfig 设置交换机

Ezconfig 是一个交互式的应用，它为设置以下交换机参数提供了一个简化的程序。

- 交换机管理 IP 地址
- 交换机管理用户密码
- 交换机的名称和位置

Ezconfig 可在全局配置模式（#）或显示模式（>）下输入。

当你输入 ezconfig 命令，应用会显示以下的文本：

```
(FSM7352S) >ezconfig

NETGEAR EZ Configuration Utility
--------------------------------
Hello and Welcome!
This utility will walk you thru assigning the IP address for the switch
management CPU. It will allow you to save the changes at the end. After the
session, simply use the newly assigned IP address to access the Web GUI using
any public domain Web browser.

Admin password not defined. Do you want to change the password? (Y/N/Q)
```

注意：在设置中，你可以键入 Q 中断程序。此时，Ezconfig 会检查是否有任何更改，并提示你是否保存更新设置。

更改密码

Ezconfig 询问的第一个问题是你是否想要更改管理密码。为了安全理由，你应键入 Y 更改密码。如果你已经设置好密码并不希望再一次改变，输入 N。

```
Enter new password:********
Confirm new password:********
Password Changed!

The 'enable' password required for switch configuration via the command line
interface is currently not configured. Do you wish to change it (Y/N/Q)?  y


Enter new password:********
Confirm new password:********
Password Changed!
```

设置交换机的 IP 地址

更改了管理和特权模式的密码后，将提示你设置交换机的 IP 地址。

```
Assigning an IP address to your switch management

Current IP Address Configuration
--------------------------------
IP address: 0.0.0.0
Subnet mask: 0.0.0.0

Would you like to assign an IP address now (Y/N/Q)?  y

IP Address:
```

Ezconfig 会显示现在的 IP 地址和子网掩码。默认情况下，管理 IP 地址使用 DHCP 协议，从 DHCP 服务器动态获取 IP 地址。然而，你可以在这里通过指派固定的 IP 地址来改写 DHCP 客户端的模式。一旦分配了固定 IP 地址，Ezconfig 将动态地禁用 DHCP 客户端模式并指派静态 IP 地址给管理 VLAN。
如果已经给交换机分配了 IP 地址并且不想再次修改 IP 地址，直接输入 N。

设置交换机名称和位置信息

Ezconfig 在设置中将继续下一步：

```
Do you want to assign switch name and location information (Y/N/Q)?

System Name: Alpha1-1
System Location: Bld1
System Contact: James

There are changes detected, do you wish to save the changes permanently (Y/N)?
```

	注意：系统名称、系统位置和系统联络信息只接受文字和数字的字符。不支持类似于“#$...”的字符。

	注意：最大长度不能大于 31 个字节。

保存配置

输入名称和位置信息后，Ezconfig 将询问是否将更改保存到闪存中。输入 Y 保存配置。

```
There are changes detected, do you wish to save the changes permanently (Y/N)?
y

The configuration changes have been saved successfully.
Please enter 'show running-config' to see the final configuration.

Thanks for using EzConfig!
```

如果在这个过程中交换机断电，那么在 Ezconfig 还没有在断电前保存更新，设置信息将会丢失。

第四章 使用 Web 图形用户界面

这个章节主要介绍 Web 图形用户界面，例如解释如何访问基于 web 的管理界面来配置和管理系统。

提示：使用 Web 图形用户接口替代 CLI 命令行界面。Web 的配置比起要求输入多条 CLI 命令更简单和快捷。无论 Web 接口和终端接口都具有相同的功能，应用程序使用相同的菜单去完成一个任务。例如：当你登陆，都有一个相同功能的主菜单。

你可以通过 Web 浏览器和因特网连接管理你的交换机。这个被认为是基于 Web 的管理。为了使用基于 Web 的管理，系统需要设备 in-band 连接。

为了访问交换机，Web 浏览器必须支持：

- HTML 4.0 或更新的版本
- HTTP 1.1 或更新的版本
- JavaScript™ 1.2 或更新的版本

Web 接口和终端接口有许多不同的地方。例如：在 Web 接口可以显示整个转发 数据库，然而在终端接口只能显示从特定地址开始的 10 个条目。

结束 Web 登陆会话，直接关闭 web 浏览器。

配置 Web 接口访问

为了能从 Web 接口访问到交换机：

1. 配置交换机 in-band 连接。在交换机*开始*章节提供了说明。
2. 启用 Web 模式：
   a. 在 CLI 提示，输入 show network 命令。
   b. 设置 **Web Mode** 为启用。

开始 Web 接口访问

下面的步骤开始交换机 Web 接口的访问：

1. 在 Web 浏览器的地址栏里输入交换机的 IP 地址。
2. 当显示登陆面板，点击 **Login**。
3. 输入正确的用户名和密码。用户名和关联的密码与在终端接口使用的是一致的。点击 Login 按钮。
4. 显示系统描述菜单，在屏幕的左边显示导航树菜单。
5. 在导航树菜单中选择正确的项目并点击进入该页面。

网页的版面

交换机管理页面的接口面板有三个区块构成。
交换机的图形横幅显示在面板的最上方。
第二个区块是在面板左部显示的分层次导航树。导航树由目录、子目录和配置状态 HTML 页面组成。只有选择配置状态页面（非目录或子目录）才会显示一个新的 HTML 页面。目录和子目录没有对应的 HTML 页面。
第三个区块是在面板的右下部，显示的是设备的配置状态或用户的配置信息。

配置 SNMPv3 用户模版

配置 SNMP v3 用户模版是用户配置的一部分。任何用户都可以通过 SNMP v3 协议连接到交换机，但是为了认证和加密需要额外的步骤。使用以下的步骤来配置一个 SNMP v3 新的用户模版。

1. 在 Web 图形用户接口左边的层次导航树菜单中选择 System>Configuration>User Accounts。
2. 使用 User 下拉菜单，选择 Create 去创建新的用户。
3. 输入新的用户名。
4. 输入新的用户密码并重输一遍确认密码。

	注意：如果 SNMPv3 认证用于该用户，密码必须是多于 8 位的文字或数字字符

5. 如果不需要认证，直接到第 9 步。
6. 为了启用认证，使用 Authentication Protocol 下拉菜单选择 MD5 或 SHA 作为认证协议。
7. 如果不需要加密，直接到第 9 步。
8. 为了启用加密，使用 Encryption Protocol 下拉菜单选择 DES 作为加密。然后输入不少于 8 位数字或字母形式的字符作为加密密钥。
9. 点击 Submit。

命令按钮

下面的命令按钮遍及在交换机 Web 图形用户接口面板使用：

Save	点击 Save 按钮保存你刚刚所做的修改。有些设置会要求你重启系统以便这些设置能生效。
Refresh	点击 Refresh 按钮更新在 Web 图形用户接口面板上显示的数据。
Submit	点击 Submit 按钮发送更新的配置到交换机。配置更新马上生效，但是这些更新在重启后并没有保存，必须直到执行保存才不会丢失。

第五章 虚拟局域网（Virtual LANs）

一方面，一台支持 Vlan 功能的交换机像网桥一样，根据二层的数据帧头信息高速的转发数据流量。另一方面，它又类似一台路由器，将网络分割网络成不同的逻辑部分，这样能提供更好的管理、安全和对多播流量的控制。VLAN 分割网络成不同的逻辑 部分，这样能提供更好的管理、安全和对多播流量的管理。

一个 VLAN 是一组终端节点和连接它们的交换机端口。你可能会有许多对于逻辑上区隔开来的原因，例如部门或项目成员。在物理上的要求只是终端节点和连接它们的端口都是属于同一个 VLAN。

在网络中的每一个 VLAN 有一个关联的 VLAN ID。当数据帧在一个 VLAN 上传输时，VLAN ID 出现在二层数据帧的头部的 IEEE 802.1Q 标记（tag）。终端节点会忽略这个标记或这个标记中的 VLAN 部分。在这种情况下，第一个接收数据帧的交换端口不是拒绝这个数据帧就是使用默认的 VLAN ID 在数据帧中插入标记。一个端口会处理多于一个 VLAN 的数据流量，但是一个端口只能支持一个默认 VLAN ID。

私有边缘 VLAN（Private Edge VLAN）特性让你在交换机的端口间设置保护。这意味着在同一个交换机上，一个所保护端口不能转发流量到另外一个受保护端口。

这个特性并不提供对在不同交换机上端口之间的保护。

VLAN 配置示例

在这个部分的图表显示了一个交换机的四个端口被配置去处理两个 VLAN 的流量。端口 1/0/2 同时处理两个 VLANs 的流量，然而端口 1/0/1 只是 VLAN 2 的成员，端口 1/0/3 和 1/0/4 只是 VLAN 3 的成员。在图表后的文本显示了你将要使用去配置交换机成如图所示所需要的命令。

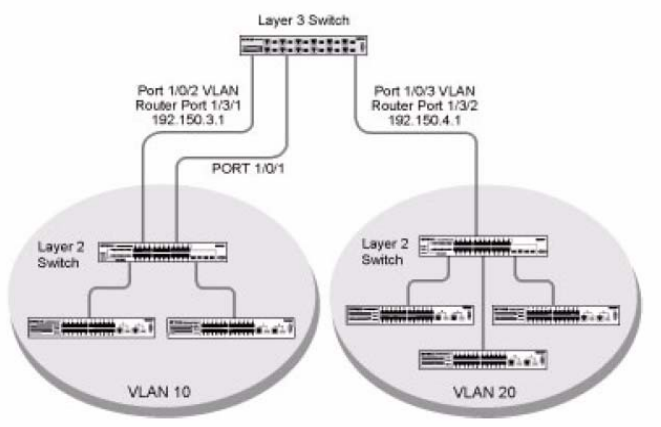


Figure 5-1

命令行界面示例

以下的例子展示了如何创建 VLANs、分配相应的端口到 VLANs 中和给一个端口指派 VLAN 作为它的默认 VLAN。

示例#1：创建两个 VLANs

使用以下的命令去创建两个 VLANs 并分配 VLAN IDs，同时不需要配置 VLAN 的名称。

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 2
(Netgear Switch) (Vlan)#vlan 3
(Netgear Switch) (Vlan)#exit
```

示例#2：分配端口到 VLAN 2

接下来展示如何分配端口到 VLAN 2，指示数据帧从所有成员端口上将总是被打上标记（tagged）传输，同时那些没有被打上标记的（untagged）数据帧将被拒绝接收。

```
(Netgear Switch) # config
(Netgear Switch) (Config)#interface range 1/0/1-1/0/2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan participation include 2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan acceptframe vlanonly
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan pvid 2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#exit
(Netgear Switch) (Config)#vlan port tagging all 2
(Netgear Switch) (Config)#
```

示例#3：分配端口到 VLAN 3

这个例子展示如何分配端口使它们属于 VLAN 3，并指示未打标记的数据帧将在端口 1/0/4 上被接收。
注意:端口 1/0/2 属于两个 VLANs，端口 1/0/1 不属于 VLAN 3。

```
(Netgear Switch) (Config)#interface range 1/0/2-1/0/4
(Netgear Switch) (conf-if-range-1/0/2-1/0/4)#vlan participation include 3
(Netgear Switch) (conf-if-range-1/0/2-1/0/4)#exit
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#vlan acceptframe all
(Netgear Switch) (Interface 1/0/4)#exit
(Netgear Switch) (Config)#exit
```

示例#4：指派 VLAN 3 作为默认 VLAN

这个例子展示如何指派 VLAN 3 作为端口 1/0/2 的默认 VLAN。

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#vlan pvid 3
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```

图形用户接口

使用以下的在图形用户接口上完成相同的配置：

- **Switch-->VLAN-->Configuration**. 创建 VLAN 并指派端口。
- **Switch-->VLAN-->Port Configuration**. 指示对不打标记的数据帧的接收处理和数据帧是否打上标记或不打标记传输。

第六章 链路聚合（Link Aggregation）

这个部分包括使用命令行界面和图形用户接口配置链路聚合的用法说明。
链路聚合（LAG）使交换机视在两个终端之间的多个物理链路作为一个逻辑上的单一链接。在一个给定的 LAG 中的所有物理链接必须运作在相同速率的全双工模式下。
当在交换机之间的数据流量需要高带宽和稳定性，或者连接到一个公共网络提供更高的带宽时，链路聚合可以被用来连接两台交换机。LAG 贡献了以下的好处：

- 增加了稳定性和实用性——如果在 LAG 里的其中一条物理链接断开了，流量将自动和透明地重新分配到另外的物理链接。
- 更好地使用物理资源——流量能通过物理链接负载均衡。
- 增加带宽——聚合的物理链接比单一链接传递更高的带宽。
- 在带宽上的增量增加——一个物理上的升级能产生 10 倍带宽的增加；LAG 产生两倍或五倍的带宽增加，如果只是需要小量的增加将会相当有效。

管理功能视一个 LAG 好像一个单独的物理接口。
你可以将一个 LAG 包含在一个 VLAN 里。你也可以为给定的交换机配置多于一个 LAG。

命令行界面示例

这个部分提供一个配置软件以支持在服务器和三层交换机之间链路聚合的示例。
Figure 6-1 shows the example network.

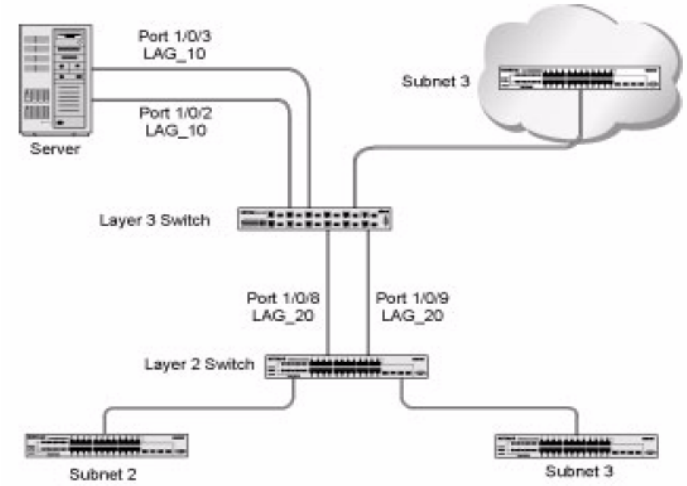


Figure 6-1

示例#1：创建两个 LAGs：

```
(Netgear Switch) #config
(Netgear Switch) (Config)#port-channel lag_10
(Netgear Switch) (Config)#port-channel lag_20
(Netgear Switch) (Config)#exit
```

使用命令 show port-channel all 显示逻辑接口标识（logical interface ids），并且在接下的命令中你将使用逻辑接口标识去确定 LAGs。假定 lag_10 被指派的标识是 1/1/1，lag_20 被指派的标识是 1/1/2。

```
(Console) #show port-channel all

            Port-                   Link
Log.       Channel             Adm. Trap  STP           Mbr      Port     Port
Intf        Name        Link   Mode Mode  Mode   Type   Ports    Speed    Active
------ ---------------- ------ ---- ---- ------- -------- ------ ---------- ------
1/1/1    lag_10          Down   En.  En.  Dis.    Dynamic
1/1/2    lag_20          Down   En.  En.  Dis.    Dynamic
```

示例#2：添加端口到 LAGs：

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 0/2
(Netgear Switch) (Interface 0/2)#addport 1/1
(Netgear Switch) (Interface 0/2)#exit
(Netgear Switch) (Config)#interface 0/3
(Netgear Switch) (Interface 0/3)#addport 1/1
(Netgear Switch) (Interface 0/3)#exit
(Netgear Switch) (Config)#interface 0/8
(Netgear Switch) (Interface 0/8)#addport 1/2
(Netgear Switch) (Interface 0/8)#exit
(Netgear Switch) (Config)#interface 0/9
(Netgear Switch) (Interface 0/9)#addport 1/2
(Netgear Switch) (Interface 0/9)#exit
(Netgear Switch) (Config)#exit
```

示例#3：启用两边的 LAGs：

默认，系统会启用链路陷阱通知。

```
(Console) #config
(Console) (Config)#port-channel adminmode all
(Console) (Config)#exit
```

这样地话，LAGs 能被添加到 VLANs 里。

第七章 IP 路由服务

IP 路由服务分成五类：

- 端口路由
- VLAN 路由
- 路由信息协议（RIP）
- 开放最短路径优先协议（OSPF）
- 代理地址解析协议（ARP）

端口路由

最开始的网络是足够小来应付终端之间的直接通信。当网络不断扩展，二层的桥接被使用来隔离流量。这个技术对单播的流量有效，但是在应对大量的多播数据包的时候出现了问题。下一个主要的发展是路由，数据包在第三层被检查和重定向。终端需要知道如何到达离它们最近的路由器，同时路由器需要了解整个网络拓扑以便它们可以转发流量。尽管网桥趋向于比路由器要快，但是使用路由器能将网络划分成逻辑子网，从而限制了多播的流量并方便了安全机制的发展。

终端在数据包的 IP 包头里指定了目的地站点的三层地址，但是却发送数据包到路由器的 MAC 地址。当三层路由器接收到数据包，它最低限度会：

- 在它的路由表里检查三层地址从而决定向外发送的端口
- 更新三层数据包头
- 从新产生新的二层数据帧头

路由器的 IP 地址常常是在终端站点被静态配置的，尽管 7000 系列全网管交换机支持像 DHCP 动态分配地址的协议。同样地，你可以在路由表里配置某些被路由器静态使用的条目，但是像 RIP 和 OSPF 协议允许路由表在网络配置发生改变时动态地生成和更新。

端口路由配置

7000 系列全网管交换机总是支持二层桥接，但是三层路由必须显示地被启用。首先作为一个整体启用 7000 系列全网管交换机的路由功能，然后是每个参与到路由网络的端口。

在这部分示例中的配置命令在端口 1/0/2、1/0/3 和 1/0/5 上启用 IP 路由。路由器标识将会被设置成 7000 系列全网管交换机的管理 IP 地址，或者在管理地址没有配置的情况下设置成任何活动的路由接口。

在配置了路由命令后，以下的功能将会被激活：

- IP 转发，负责转发收到的 IP 数据包。
- ARP 映射，负责维护用于关联 IP 和 MAC 地址的 ARP 表。改表包括静态配置的条目和基于接收到的 ARP 数据帧动态更新的条目。
- 路由表对象，负责维护被所有已记录的路由协议使用的公共路由表。

然后你会在 IP 路由的基础上激活路由器之间用于交换路由信息的 RIP 或 OSPF 协议。RIP

较常用于小型的网络，而 OSPF 则是为较大型和较复杂的拓扑设计的。

命令行界面示例

这个图表展示了三层交换机被配置成端口路由。它链接三个不同的子网，每个子网链接到一个不同的端口。文本展示了你配置 7000 系列管理交换机提供端口路由所使用的命令。

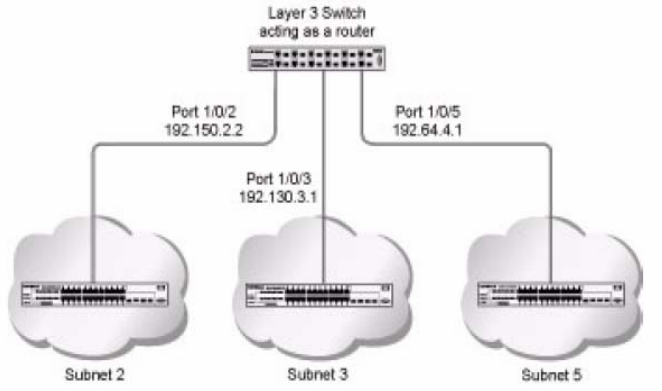


Figure 7-1

示例#1：为交换机启用路由功能

使用以下的命令为交换机启用路由功能。执行这个命令默认启用 IP 转发。

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#exit
```

示例#2：在交换机上为端口启用路由功能

使用以下的命令在交换机上为端口启用路由功能。默认的链接封装格式是以太网。为端口配置 IP 地址和子网掩码。网络定向的广播帧将会被丢弃，同时最大传输单元（MTU）的大小是 1500 字节。

```
(Netgear Switch) #config
(Netgear Switch) (Config)# interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#routing
(Netgear Switch) (Interface 1/0/2)#ip address 192.150.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/2)#exit

(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#routing
(Netgear Switch) (Interface 1/0/3)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface 1/0/3)#exit

(Netgear Switch) (Config)#interface 1/0/5
(Netgear Switch) (Interface 1/0/5)# routing
(Netgear Switch) (Interface 1/0/5)#ip address 192.150.5.1 255.255.255.0
(Netgear Switch) (Interface 1/0/5)#exit
(Netgear Switch) (Config)#exit
```

VLAN 路由

你可以配置 7000 系列全网管交换机某些端口支持 VLAN 和支持路由。你可以配置交换机以允许一个 VLAN 里的流量，而这个 VLAN 好像被视作是一个路由端口。
当一个端口被启用作为桥接（默认模式）而不是路由功能，将对转发进来的数据包实施所有标准的桥接处理，而那个转发进来的数据包稍候将被关联到一个 VLAN。它的 MAC 目标地址和 VLAN ID 被用来搜索 MAC 地址表。如果路由功能在 VLAN 上被启用并且目标 MAC 地址是一个交换机内部的桥接－路由接口地址，那么这个转发进来的单播数据包将会被路由。如果一个进来的多播数据包在一个可路由的 VLAN 上被接收，那个这个数据包将会被转发到这个 VLAN 中的所有端口和内部的桥接－路由接口。
由于一个端口可以配置成属于多个 VLAN，那么 VLAN 路由会在这个端口上的所有 VLAN 或一个子网被启用。VLAN 路由可被用于允许多于一个物理接口在一个相同的子网内。它也可以用于一个 VLAN 跨越多个物理网路，或者需要额外隔离的或安全的情况。
下部分将展示如何配置 7000 系列全网管交换机支持 VLAN 路由和如何使用 RIP 和 OSPF。一个端口要么是一个 VLAN 接口或一个路由接口，不能同时是 VLAN 和路由接口。然而一个 VLAN 接口是一个 VLAN 的一部分，而这个 VLAN 它自己本身也是一个路由接口。

VLAN 路由配置

这部分提供如何配置 7000 系列全网管交换机支持 VLAN 路由的示例。配置 VLAN 路由接口和配置普通的物理接口类似。主要的区别是在 VLAN 被创建之后，你需要使用命令 show ip vlan 去查看 VLAN 的接口 ID，那么你将可以在路由配置命令中使用这个接口 ID。

命令行界面示例

这部分的图表显示一个三层交换机配置支持 VLAN 路由。三层交换机连接两个 VLAN，其中两个端口在一个 VLAN 里，另一个端口在另外一个 VLAN。文本显示你配置 7000 系列全网

管交换机支持如图中 VLAN 路由所需要使用的命令。

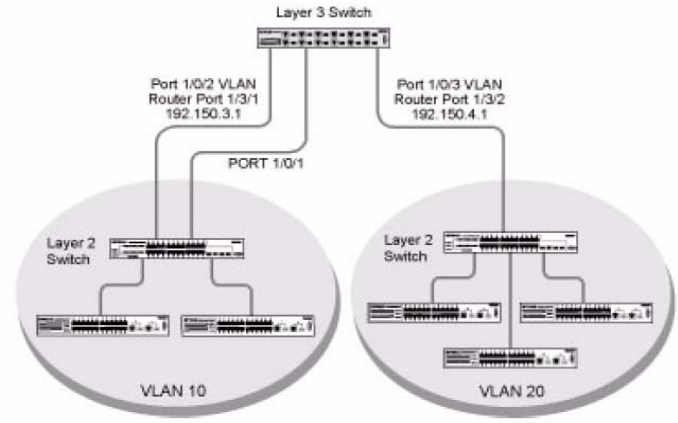


Figure 7-2

示例#1：创建两个 VLANs

接下来的代码序列展示创建两个 VLANs，并且在发送出去的数据帧上打上标记。

```
(Netgear Switch) #vlan data
(Netgear Switch) (Vlan)#vlan 10
(Netgear Switch) (Vlan)#vlan 20
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #conf
(Netgear Switch) (Config)#interface range 1/0/1-1/0/2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan participation include 10
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan pvid 10
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#vlan participation include 20
(Netgear Switch) (Interface 1/0/3)#vlan pvid 20
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#vlan port tagging all 10
(Netgear Switch) (Config)#vlan port tagging all 20
(Netgear Switch) (Config)#exit
```

示例#2：为交换机和 VLAN 配置 VLAN 路由

接下来的代码序列展示如何为 VLAN 启用路由。

```
(Netgear Switch) #vlan data
(Netgear Switch) (Vlan)#vlan routing 10
(Netgear Switch) (Vlan)#vlan routing 20
(Netgear Switch) (Vlan)#exit
```

返回的逻辑接口 ID 将用于后续的路由命令。假定 VLAN 10 被指派的 ID 是 3/1，而 VLAN 20 被指派的 ID 是 3/2。

为交换机启用全局路由：

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#exit
```

接下来的代码序列显示为虚拟路由接口配置 IP 地址和子网掩码的示例。

```
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface-vlan 10)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface-vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface-vlan 20)#ip address 192.150.4.1 255.255.255.0
(Netgear Switch) (Interface-vlan 20)#exit
(Netgear Switch) (Config)#exit
```

VLAN 路由 RIP 配置

路由信息协议（RIP）是被路由器用于交换网络拓扑信息的其中一个协议。它被描述成一个内部网关协议，通常用于小到中型的网络。

运行 RIP 的路由器将每隔 30 秒发送它的路由表内容到它毗邻的路由器。当一条路由信息从路由表上被移除，这条路由信息将会在 180 秒后被接受路由信息的其它路由器标记为不可用，并且在 120 秒之后从它们的路由表中移除。

有两种版本的 RIP 协议：

- 在 RFC 1058 中定义的 RIPv1
  - 路由信息通过目标网络的 IP 和跳数来详细说明
  - 路由表被广播到连接网络上的所有站点
- 在 RFC1723 中定义的 RIPv2
  - 路由信息扩展到包含子网掩码和网关
  - 路由表被发送到一个多播地址，减少网络流量
  - 增加用于安全的认证方法

7000 系列全网管交换机支持两种版本的 RIP。你可以配置一个给定的端口：

- 用单一或两种接收数据包
- 用 RIPv1、RIPv2 或发送 RIPv2 的数据包到 RIPv1 的广播地址的形式发送数据包
- 阻止任何 RIP 的数据包被接收
- 阻止任何 RIP 的数据包被发送

命令行界面示例

这个示例在 VLAN 路由配置的基础上增加了配置以支持 RIPv2。第二个路由器被添加到网络中，这个路由器使用端口路由而非 VLAN 路由。

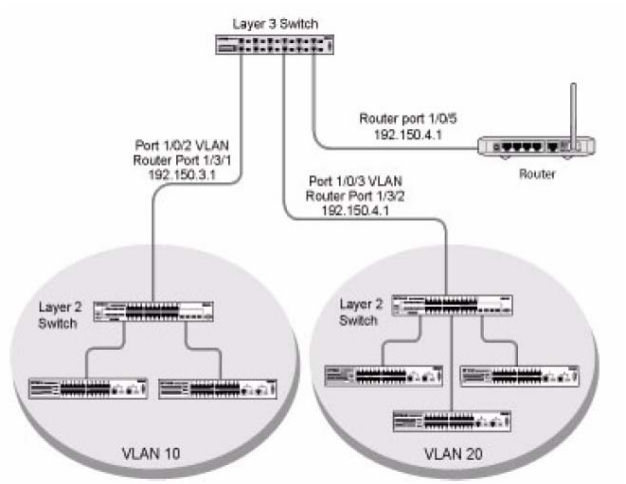


Figure 7-3

在 7000 系列全网管交换机上配置支持 RIP 的 VLAN 路由示例。

```
(Netgear Switch) #vlan data
(Netgear Switch) (Vlan)#vlan 10
(Netgear Switch) (Vlan)#vlan 20
(Netgear Switch) (Vlan)#vlan routing 10
(Netgear Switch) (Vlan)#vlan routing 20
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #conf
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#vlan port tagging all 10
(Netgear Switch) (Config)#vlan port tagging all 20
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#vlan participation include 10
(Netgear Switch) (Interface 1/0/2)#vlan pvid 10
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#vlan participation include 20
(Netgear Switch) (Interface 1/0/3)#vlan pvid 20
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface vlan 10)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface vlan 20)#ip address 192.150.4.1 255.255.255.0
(Netgear Switch) (Interface vlan 20)#exit
```

```
Enable RIP for the switch. The route preference will default to 15.
(Netgear Switch) (Config)#router rip
(Netgear Switch) (Config router)#enable
(Netgear Switch) (Config router)#exit

Configure the IP address and subnet mask for a non-virtual router port.
(Netgear Switch) (Config)#interface 1/0/5
(Netgear Switch) (Interface 1/0/5)#ip address 192.150.5.1 255.255.255.0
(Netgear Switch) (Interface 1/0/5)#exit

Enable RIP for the VLAN router ports. Authentication will default to none, and
no default route entry will be created.
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface vlan 10)#ip rip
(Netgear Switch) (Interface vlan 10)#exit
(Netgear Switch) (Config)# interface vlan 20
(Netgear Switch) (Interface vlan 20)#ip rip
(Netgear Switch) (Interface vlan 20)#exit
(Netgear Switch) (Config)#exit
```

VLAN 路由 OSPF 配置

通常在大型的网络中优先使用最短路由优先（OSPF）协议。OSPF 提供了很多在管理大型的和/或复杂的网络下的优势：

- 更少的网络流量
  - 路由表的更新只是在发生改变的情况下被发送
  - 只是发送路由表中改变的部分
  - 更新被发送到多播地址而非广播地址
- 层次的管理允许对网络进行细分

OSPF 网络最高层是一个自治系统或路由区域，这是一个有共同管理和路由策略的网络集合。自治系统被划分成不同区域：内部区域路由（intra-area routing）使用在当源和目的地址在同一个区域，区域间路由(inter-area routing)在跨越一个 OSPF 骨干网络时被用。跨区域路由器与每个区域中提供连接的边界路由器通信。

7000 系列全网管交换机可配置成如同一个路由器并运行 OSPF，并通过使用消耗（cost）和 OSPF 路由条目来决定最佳的路由。如有多于一种类型的路由条目存在将按以下顺序选取路由：

- Intra-area
- Inter-area
- External Type 1：在自治系统外的路由
- External Type 2：通过其它路由协议学习到的路由，如 RIP

命令行界面示例

这个示例在 VLAN 路由的基础上增加了支持 OSPF 的配置。文本展示你配置 7000 系列全网管交换机作为一个区域间路由器所使用的命令。图表参考 Figure 7-2。

在 7000 系列全网管交换机上配置 OSPF 作为一个区域路由器：

```
(Netgear Switch) #vlan data
(Netgear Switch) (Vlan)#vlan 10
(Netgear Switch) (Vlan)#vlan 20
(Netgear Switch) (Vlan)#vlan routing 10
(Netgear Switch) (Vlan)#vlan routing 20
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #conf
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#vlan port tagging all 10
(Netgear Switch) (Config)#vlan port tagging all 20
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#vlan participation include 10
(Netgear Switch) (Interface 1/0/2)#vlan pvid 10
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#vlan participation include 20
(Netgear Switch) (Interface 1/0/3)#vlan pvid 20
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface vlan 10)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface vlan 20)#ip address 192.150.4.1 255.255.255.0
(Netgear Switch) (Interface vlan 20)#exit
```

```
Specify the router ID and enable OSPF for the switch.
(Netgear Switch) (Config)#router ospf
(Netgear Switch) (Config router)#router-id 192.150.9.9
(Netgear Switch) (Config router)#enable
(Netgear Switch) (Config router)#exit

Enable OSPF for the VLAN and physical router ports.
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface vlan 10)#ip ospf areaid 0.0.0.2
(Netgear Switch) (Interface vlan 10)#ip ospf
(Netgear Switch) (Interface vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface vlan 20)# ip ospf areaid 0.0.0.3
(Netgear Switch) (Interface vlan 20)#ip ospf
(Netgear Switch) (Interface vlan 20)#exit
```

```
Set the OSPF priority and cost for the VLAN and physical router ports.
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface vlan 10)#ip ospf priority 128
(Netgear Switch) (Interface vlan 10)#ip ospf cost 32
(Netgear Switch) (Interface vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface vlan 20)#ip ospf priority 255
(Netgear Switch) (Interface vlan 20)#ip ospf cost 64
(Netgear Switch) (Interface vlan 20)#exit
(Netgear Switch) (Config)#exit
```

路由信息协议

路由信息协议（RIP）是路由器用于交换网络拓扑信息的协议。它被认为是一种“内部”网关协议，常用于小型到的网络。

RIP 配置

一个运行 RIP 的路由器会每隔 30 秒就发送它的路由表信息到与它毗邻的路由器。当一条路由从路由表中被移除，它会在 180 秒后被接受的路由器标记为不可用的路由信息，并在 120 秒后从它们的路由表中移除。

有两个版本的 RIP：

- 在 RFC 1058 中定义的 RIPv1
  - 路由信息通过目标网络的 IP 和跳数来详细说明
  - 路由表被广播到连接网络上的所有站点
- 在 RFC1723 中定义的 RIPv2
  - 路由信息扩展到包含子网掩码和网关
  - 路由表被发送到一个多播地址，减少网络流量
  - 增加用于安全的认证方法

7000 系列全网管交换机支持两种版本的 RIP。你可以配置一个给定的端口：

- 用单一或两种接收数据包
- 用 RIPv1、RIPv2 或发送 RIPv2 的数据包到 RIPv1 的广播地址的形式发送数据包
- 阻止任何 RIP 的数据包被接收
- 阻止任何 RIP 的数据包被发送

命令行界面示例

在下面示例中使用的配置命令在端口 1/0/2 和 1/0/3 上启用了 RIP。如 Figure 7-4 中的网络所示：

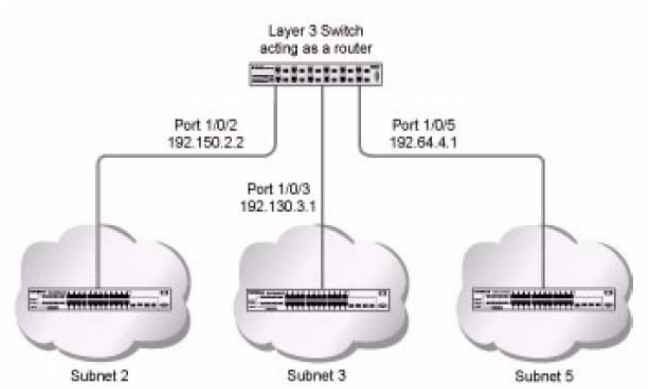


Figure 7-4

示例#1：为交换机启用路由功能

以下的命令序列为交换机启用路由功能：

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#exit
```

示例#2：为端口启用路由功能

以下的命令序列为端口 1/0/2 和 1/0/3 启用路由并分配 IP 地址。

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#routing
(Netgear Switch) (Interface 1/0/2)#ip address 192.150.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#routing
(Netgear Switch) (Interface 1/0/3)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#exit
```

示例#3：为交换机启用 RIP

接下来的序列为交换机启用 RIP。这条路由的优先级默认为 15。

```
(Netgear Switch) #config
(Netgear Switch) (Config)#router rip
(Netgear Switch) (Config router)#enable
(Netgear Switch) (Config router)#exit
(Netgear Switch) (Config)#exit
```

示例#4：为端口 1/0/2 和 1/0/3 启用 RIP

以下的命令行序列为端口 1/0/2 和 1/0/3 启用 RIP。默认没有认证，并且没有创建默认路由。命令指定两个端口都接收 RIPv1 和 RIPv2 的数据帧，但只发送 RIPv2 格式的数据帧。

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#ip rip
(Netgear Switch) (Interface 1/0/2)#ip rip receive version both
(Netgear Switch) (Interface 1/0/2)#ip rip send version rip2
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#ip rip
(Netgear Switch) (Interface 1/0/3)#ip rip receive version both
(Netgear Switch) (Interface 1/0/3)#ip rip send version rip2
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#exit
```

OSPF

通常在大型的网络中优先使用最短路由优先（OSPF）协议。OSPF 提供了很多在管理大型的和/或复杂的网络下的优势：

- 更少的网络流量
  - 路由表的更新只是在发生改变的情况下被发送
  - 只是发送路由表中改变的部分

— 更新被发送到多播地址而非广播地址

- 层次的管理允许对网络进行细分

OSPF 网络最高层是一个自治系统或路由区域，这是一个有共同管理和路由策略的网络集合。自治系统被划分成不同区域：内部区域路由（intra-area routing）使用在当源和目的地址在同一个区域，区域间路由(inter-area routing)在跨越一个 OSPF 骨干网络时被用。跨区域路由器与每个区域中提供连接的边界路由器通信。

7000 系列全网管交换机可配置成如同一个路由器并运行 OSPF，并通过使用消耗（cost）和 OSPF 路由条目来决定最佳的路由。如有多于一种类型的路由条目存在将按以下顺序选取路由：

— Intra-area
— Inter-area
— External Type 1：在自治系统外的路由
— External Type 2：通过其它路由协议学习到的路由，如 RIP

命令行界面示例

在这个章节的示例中将展示如何配置 7000 系列全网管交换机首先作为一个区域间路由器，然后作为一个边界路由器。有两个区域，每个区域都有连接到一个区域间路由器的边界路由器。

第一个图表展示一个区域间路由器连接 0.0.0.2 和 0.0.0.3 区域的网络部分。示例文本显示了通过在区域 0.0.0.2 中的端口 1/0/2 和区域 0.0.0.3 中的端口 1/0/3 启用 OSPF 配置 7000 系列全网管交换机作为一个区域间路由器所使用的配置命令。

示例#1：配置一个区域间路由器

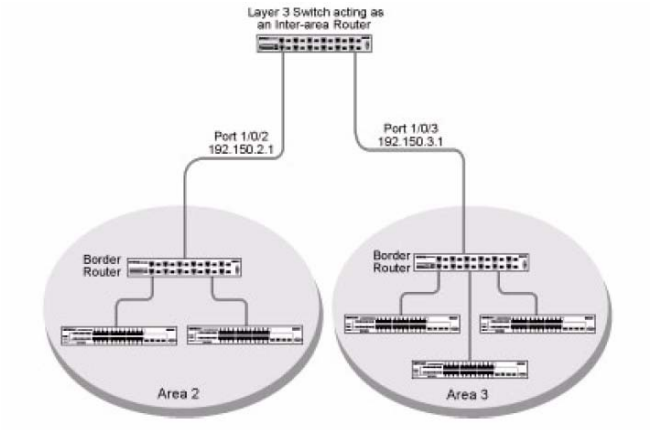


Figure 7-5

为交换机启用路由功能。下面的命令行序列为交换机启用 IP 路由功能。

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#exit
```

为端口分配 IP 地址。下面的序列启用路由功能并为端口 1/0/2 和 1/0/3 分配 IP 地址。

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#routing
(Netgear Switch) (Interface 1/0/2)#ip address 192.150.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#routing
(Netgear Switch) (Interface 1/0/3)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#exit
```

指定路由器 ID 和为交换机启用 OSPF。下面的序列指定路由器 ID 并为交换机启用 OSPF。设置 disable 1583 compatibility 以阻止环路。

```
(Netgear Switch) #config
(Netgear Switch) (Config)#router ospf
(Netgear Switch) (Config router)#enable
(Netgear Switch) (Config router)#router-id 192.150.9.9
(Netgear Switch) (Config router)#no 1583compatibility
(Netgear Switch) (Config router)#exit
(Netgear Switch) (Config)#exit
```

为端口启用和配置 OSPF。下面的序列启用 OSPF 和为端口设置 OSPF 的优先级和开销。

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#ip ospf
(Netgear Switch) (Interface 1/0/2)#ip ospf areaid 0.0.0.2
(Netgear Switch) (Interface 1/0/2)#ip ospf priority 128
(Netgear Switch) (Interface 1/0/2)#ip ospf cost 32
(Netgear Switch) (Interface 1/0/2)#exit

(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#ip ospf
(Netgear Switch) (Interface 1/0/3)#ip ospf areaid 0.0.0.3
(Netgear Switch) (Interface 1/0/3)#ip ospf priority 255
(Netgear Switch) (Interface 1/0/3)#ip ospf cost 64
(Netgear Switch) (Interface 1/0/3)#exit(Netgear Switch) (Config)#exit
```

示例#2：在一个边界路由器上配置 OSPF

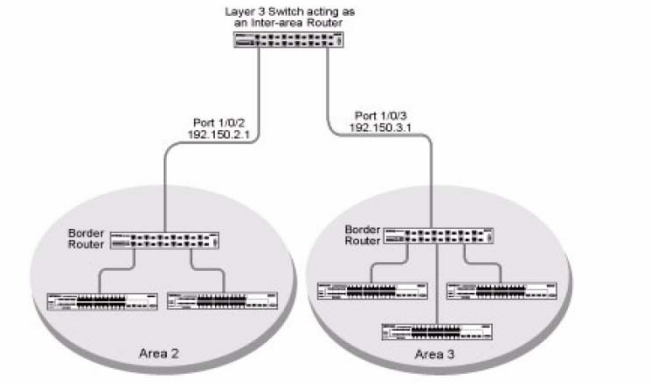


Figure 7-6

下面的示例在一个 7000 系列全网管交换机上配置 OSPF 作为一个边界路由器。

```
Enable routing for the switch.

(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing

Enable routing & assign IP for ports 1/0/2, 1/0/3 and 1/0/4.

(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#routing
(Netgear Switch) (Interface 1/0/2)#ip address 192.150.2.2 255.255.255.0
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#routing
(Netgear Switch) (Interface 1/0/3)#ip address 192.130.3.1 255.255.255.0
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#routing
(Netgear Switch) (Interface 1/0/4)#ip address 192.64.4.1 255.255.255.0
(Netgear Switch) (Interface 1/0/4)#exit

Specify the router ID and enable OSPF for the switch. Set disable
1583compatibility to prevent a routing loop.

(Netgear Switch) (Config)#router ospf
(Netgear Switch) (Config router)#enable
(Netgear Switch) (Config router)#router-id 192.130.1.1
(Netgear Switch) (Config router)#no 1583compatibility
(Netgear Switch) (Config router)#exit
(Netgear Switch) (Config)#exit
```

代理地址解析协议（Proxy ARP）

这部分描述代理地址解析协议（Proxy ARP）的特性。

概述

- 代理 ARP 允许路由器响应目标 IP 地址不是路由器本身但是路由器可达的 ARP 请求
- 如果一台主机不知道默认的网关，代理 ARP 可以学习到第一条地址
- 在一个物理网络里的机器看似另外一个逻辑网络的一部分
- 没有代理 ARP，路由器只响应目标 IP 地址是配置在路由器接口上的地址的 ARP 请求，这些接口 ARP 请求可以到达

命令行界面示例

下面是用于配置代理 ARP 特性的命令行界面示例。

示例#1：show ip interface

```
(Netgear Switch) #show ip interface ?

<slot/port>              Enter an interface in slot/port format.
brief                    Display summary information about IP configuration
                         settings for all ports.

(Netgear Switch) #show ip interface 0/24

Routing Mode..................................... Disable
Administrative Mode.............................. Enable
Forward Net Directed Broadcasts.................. Disable
Proxy ARP........................................ Disable
Active State..................................... Inactive
Link Speed Data Rate............................. Inactive
MAC Address...................................... 08:00:17:05:05:02
Encapsulation Type............................... Ethernet
IP MTU........................................... 1500
```

示例#2：ip proxy-arp

```
(Netgear Switch) (Interface 0/24)#ip proxy-arp ?

<cr>                     Press Enter to execute the command.

(Netgear Switch) (Interface 0/24)#ip proxy-arp
```

第八章 虚拟路由器冗余协议（VRRP）

当一个终端站点被静态地配置了路由器地址，并由改路由器来处理它的数据流量，从而在网络中引入了单点的故障。如果路由器不能工作，那么终端站点也无法通信。由于静态配置是一个指派路由器地址的方便方法，虚拟路由器冗余协议（VRRP）被开发来提供备份的机制。VRRP 通过启用后备路由器来接管主路由器，同时不影响终端站点发送数据包来消除静态默认路由导致的单点故障。终端站点将使用一个在主路由器出现故障时能被后备路由器识别的虚拟 IP 地址。路由器使用一个选举协议来决定在特定的时间哪个路由器是主路由器。一个特定的端口看似在网络中多于一个虚拟路由器，同样地在 7000 系列全网管交换机多于一个端口可被配置作为一个虚拟路由器。一个实际的物理接口或一个路由的 VLAN 接口都可参与实现该项功能。

命令行界面示例

这个例子展示如何配置 7000 系列全网管交换机支持 VRRP。路由器 1 是默认的主路由器，路由器 2 则是后备路由器。

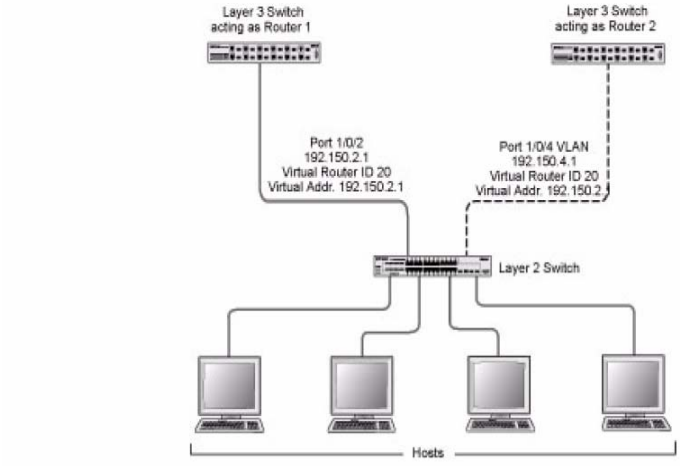


Figure 8-1

以下是在 7000 系列全网管交换机上配置 VRRP 作为主路由器的示例。

```
             Enable routing for the switch. IP forwarding will then be enabled
             by default.
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing

             Configure the IP addresses and subnet masks for the port that will
             particpate in the protocol.
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#routing
(Netgear Switch) (Interface 1/0/2)#ip address 192.150.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/2)#exit

             Enable VRRP for the switch.
(Netgear Switch) (Config)#ip vrrp

             Assign virtual router IDs to the port that will particpate in the
             protocol.
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#ip vrrp 20

             Specify the IP address that the virtual router function will rec-
             ognize. Note that the virtual IP address on port 1/0/2 is the same
             as the port's actual IP address, therefore this router will always
             be the VRRP master when it is active. And the priority default is
             255.
(Netgear Switch) (Interface 1/0/2)#ip vrrp 20 ip 192.150.2.1

             Enable VRRP on the port.
(Netgear Switch) (Interface 1/0/2)#ip vrrp 20 mode
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```

下面是在 7000 系列全网管交换机上配置 VRRP 作为后备路由器的示例。

```
             Enable routing for the switch. IP forwarding will then be enabled
             by default.
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing

             Configure the IP addresses and subnet masks for the port that will
             particpate in the protocol.
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#routing
(Netgear Switch) (Interface 1/0/4)#ip address 192.150.4.1 255.255.255.0
(Netgear Switch) (Interface 1/0/4)#exit

             Enable VRRP for the switch.
(Netgear Switch) (Config)#ip vrrp 20

             Assign virtual router IDs to the port that will particpate in the
             protocol.
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#ip vrrp 20

             Specify the IP address that the virtual router function will rec-
             ognize. Since the virtual IP address on port 1/0/4 is the same as
             Router 1's port 1/0/2 actual IP address, this router will always
             be the VRRP backup when Router 1 is active.
(Netgear Switch) (Interface 1/0/4)#ip vrrp 20 ip 192.150.2.1

             Set the priority for the port. The default priority is 100.
(Netgear Switch) (Interface 1/0/4)#ip vrrp 20 priority 254

             Enable VRRP on the port.
(Netgear Switch) (Interface 1/0/4)#ip vrrp 20 mode
(Netgear Switch) (Interface 1/0/4)#exit
(Netgear Switch) (Config)#exit
```

第九章 访问控制列表（ACLs）

这个部分描述访问控制列表（ACLs）的特性。

概述

访问控制列表可以控制进入网络的流量。通常 ACLs 设置在一个防火墙路由器或连接两个内部网络的路由器。当你配置 ACLs，你可以选择地允许或拒绝进来的流量，从而控制对你的网络或在网络上特定资源的访问。
你可以设置 ACLs 来控制在第二或第三层的流量。MAC ACLs 用于第二层，IP ACLs 用于第三层。
每个 ACL 包含一套应用于进来流量的规则。每条规则用于指定特定域的内容是否允许或拒绝访问网络，并且应用到数据包的一个或多个域中。

限制

ACLs 的应用存在以下的限制。这些限制由不同的平台来决定。

- 最多 100 条 ACLs
- 每条 ACL 最多 9－23 条规则
- 堆叠系统不支持重定向

系统在相同的端口上不支持 MAC ACLs 和 IP ACLs。
系统只支持为进来的数据流量设定 ACLs。

	注意：GSM73xxS,FSM73xxS 系列才支持 23 个 ACL 规则。FSM7326P，GSM7248，GSM7312，GSM7324 只支持 9 个 ACL 规则。

MAC ACLs

MAC ACLs 是第二层的 ACLs。你可以配置规则来检查一个数据包的以下域（平台限制）：

- 源 MAC 地址和掩码
- 目标 MAC 地址和掩码
- VLAN ID（或 IDs 范围）
- 服务类型（CoS）（802.1p）
- Ethertype
- L2 ACLs 可应用到一个或多个接口
- 多个访问列表可应用到单一个接口——序号决定执行的顺序
- 不能在同一个接口上配置 MAC ACL 和 IP ACL
- 使数据包根据指定的队列选项来排队
- 使用重定向选项来重定向数据包

配置 IP ACLs

IP ACL 归类为第三层。
每个 ACL 是一套应用于进来数据流量的规则。每条规则用于指定给定域的数据内容是否允许或拒绝访问网络，并且在一个数据包上应用于一个或多个域：

- 源 IP 地址
- 目标 IP 地址
- 源四层端口
- 目标四层端口
- ToS 字节
- 协议号

注意规则的顺序是很重要的：当一个数据包与多条规则匹配，第一条规则优先处理。同样地，一旦定义对于给定端口的 ACL，所有没有由 ACL 指定允许的数据流量将会被拒绝访问。

步骤

配置 ACL 遵循以下步骤：

- 通过指定一个名称（MAC ACL）或一个号码（IP ACL）来创建 ACL
- 增加新的规则到 ACL
- 为规则制定匹配的标准
- 应用 ACL 到一个或多个接口

IP ACL 命令行界面示例

在这个部分的文本展示了如何设置具有两条规则的 IP ACL，一个应用到 TCP 流量，另外一个应用到 UDP 流量。这两条规则的内容是一样的。如果源和目的站点和定义的规则中的 IP 地址一样，则 TCP 和 UDP 的数据包将允许通过 7000 系列全网管交换机。

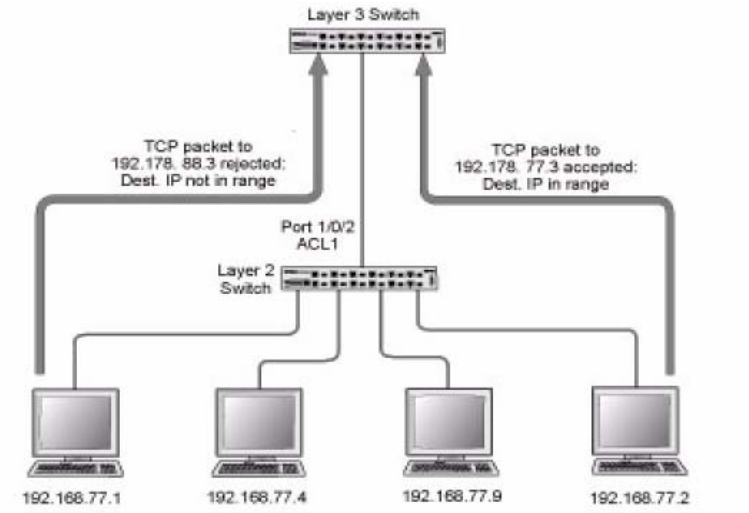


Figure 9-1

下面是在 7000 系列交换机上配置 ACL 的示例：

```
              Create ACL 101.
              Define the first rule: it will permit packets with a match on the
              specified Source IP address, after the mask has been applied, that
              are carrying TCP traffic, and are sent to the specified
              Destination IP address.
(Netgear Switch) #config
(Netgear Switch) (Config)#access-list 101 permit tcp 192.168.77.0 0.0.0.255
192.178.77.0 0.0.0.255

              Define the second rule for ACL 101.
              Define the rule to set similar conditions for UDP traffic as for
              TCP traffic.
(Netgear Switch) (Config)#access-list 101 permit udp 192.168.77.0 0.0.0.255
192.178.77.0 0.0.0.255

              Apply the rule to inbound traffic on port 1/0/2. Only traffic
              matching the criteria will be accepted.
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#ip access-group 101 in
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```

MAC ACL 命令行界面示例

下面是用于配置 MAC ACL 的命令行界面示例。

示例#1：mac access list

```
(Netgear Switch)(Config)#mac access-list ?

extended     Configure extended MAC Access List parameters.

Netgear Switch)(Config)#mac access-list extended ?

<name>    Enter access-list name up to 31 characters in length.
rename    Rename MAC Access Control List.

(Netgear Switch) (Config)#mac access-list extended b1 ?

<cr>      Press Enter to execute the command.

(Netgear Switch) (Config)#mac access-list extended b1
```

示例#2：permit any

```
(Netgear Switch) (Config-mac access-list)#permit ?

<srcmac>    Enter a MAC address.
any         Configure a match condition for all the destination MAC
            addresses in the Destination MAC Address field.

(Netgear Switch) (Config-mac access-list)#permit any ?

<dstmac>    Enter a MAC address.
any         Configure a match condition for all the destination MAC
            addresses in the Destination MAC Address field.


(Netgear Switch) (Config-mac access-list)#permit any any ?

assign-queue     Configure the Queue Id assignment attribute.
cos              Configure a match condition based on a CoS value.
<ethertypekey>   Enter one of the following keywords to specify an Ethertype
                (appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast, mplsucast,
                 netbios, novell, pppo,rarp).
<0x0600-0xffff)  Enter a four-digit hexadecimal number in the range of 0x0600 to
                 0xffff to specify a custom Ethertype value.
vlan             Configure a match condition based on a VLAN ID.
<cr>             Press Enter to execute the command.

(Netgear Switch) (Config-mac access-list)#permit any any
```

示例#3：配置 mac access-group

```
(Netgear Switch) (Config)#interface 1/0/5

(Netgear Switch) (Interface 1/0/5)#mac ?

access-group    Attach MAC Access List to Interface.

(Netgear Switch) (Interface 1/0/5)#mac access-group ?

<name>    Enter name of MAC Access Control List.

(Netgear Switch) (Interface 1/0/5)#mac access-group b1 ?

in    Enter the direction <in>.

(Netgear Switch) (Interface 1/0/5)#mac access-group b1 in ?

<cr>              Press Enter to execute the command.

<1-4294967295>    Enter the sequence number (greater than 0) to rank precedence
                  for this interface and direction. A lower sequence number has
                  higher precedence.

(Netgear Switch) (Interface 1/0/5)#mac access-group b1 in
```

示例#4：permit

```
(Netgear Switch) (Config)#mac access-list extended b2

(Netgear Switch) (Config-mac-access-list)#permit 00:00:00:00:00:00 ?

<dstmac>        Enter a MAC Address.
any             Configure a a match condition for all the destination MAC
                addresses in the Destination MAC Address field.

(Netgear Switch) (Config-mac-access-list)#permit 00:00:00:00:00:00 any

access-queue    Configure the Queue Id assignment attribute.
cos             Configure a match condition based on a CoS value.
<ethertypekey>  Enter one of the following keywords to specify an Ethertype
               (appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast, mplsucast,
                netbios, novell, pppo,rarp).
<0x0600-0xffff) Enter a four-digit hexadecimal number in the range of 0x0600 to
                0xffff to specify a custom Ethertype value.
vlan            Configure a match condition based on a VLAN ID.
<cr>            Press Enter to execute the command.
```

示例#5：show mac access-lists

```
(Netgear Switch) #show mac access-lists
Current number of all ACLs: 2    Maximum number of all ACLs: 100

MAC ACL Name    Rules     Interface(s)     Direction
------------    -----    ------------    ---------
b1              1        1/0/5           inbound
b2              1

(Netgear Switch)     #show mac access-lists ?

<name>    Enter access-list name up to 31 characters in length.
<cr>      Press Enter to execute the command.

(Netgear Switch)     #show mac access-lists b1 ?

<cr>      Press Enter to execute the command.

(Netgear Switch)     #show mac access-lists b1

Rule Number: 1
Action.................................    permit
Match All..............................    TRUE
```

第十章 服务类别（CoS）队列

这部分描述服务类别（CoS）队列映射和流量整形特性。

概述

每个端口有一个或多个数据包传送的队列。在配置的过程中，你可以决定这些队列的映射和配置。
基于服务等级和其他设置的标准，队列为特定数据包提供优先。如果时延是必需的，系统会保存数据包直到调度程序认准数据包的传输。当队列已经排满了，数据包将会被丢弃。数据包丢弃的优先级别显示出在队列拥塞的时候数据包丢弃的灵敏度。
CoS 映射、队列参数和队列管理可基于每个接口进行配置。
某些硬件的应用允许使用尾部丢弃或加权随机早期丢弃（WRED）等队列深度管理。
CoS 队列操作包括队列映射和队列配置。

CoS 队列映射

CoS 队列映射使用信任和不信任端口。

信任端口

- 系统根据表面的估值为到达的数据包采取特定的优先权
- 信任只应用到那些具有信任信息的数据包
- 每个端口一次只能有一个信任域
  - 802.1p 用户优先权（默认信任模式—通过交换配置管理）
  - IP 优先权
  - IP 区分服务代码点（DSCP）

系统可以基于在二层的数据帧帧头的 802.1p 优先级域来指派服务级别。可通过映射 802.1p 优先级到以下三个流量类别队列中的其中一个来配置服务级别。这些队列包括：

- 队列 2—最少 50％的可用带宽
- 队列 1—最少 33％的可用带宽
- 队列 0—最低的优先级，最少 17％的可用带宽

对于没打标记的流量，你可以在每个端口的基础上指定默认的 802.1p 优先级。

不信任的端口

- 对进来的数据包优先级指定是不信任的，因此使用端口默认的优先级。
- 数据包在不信任的端口通过 ACL 或区分服务的策略进行分类，所有从不信任端口进来

的数据包都定向到适当的外出端口上的特定队列。特定的 CoS 队列由端口默认的优先级或区分服务策略或 ACL 来指派队列的属性。

- 当信任端口镜像不可用时使用。例如：当一个非 IP DSCP 数据包达到一个配置为信任 IP DSCP 的端口。

CoS 队列配置

CoS 队列配置包括端口外出队列配置和丢弃优先权配置（每个队列。）在每个队列、每个丢弃优先权基础上的设计允许用户为不同的流量类型创建想要的服务特性。

端口外出队列配置

- 调度程序类型
  - 精确 vs.加权
- 最小的保证带宽
- 最小的允许带宽
  - 每个队列整形
- 队列管理类型
- 尾部丢弃 vs. 加权随机早期丢弃（WRED）

丢弃优先权配置（每个队列）

- WRED 参数
  - 最小门槛
  - 最大门槛
  - 丢弃概率
  - 比例因素
- 尾部丢弃参数
  - 门槛

基于每个端口

- 队列管理类型
  - 尾部丢弃 vs. WRED

  不支持每个队列配置
- WRED 衰减指数
- 流量整形
  - 对于整个接口

命令行界面示例

下面是用于配置 CoS 队列特性的命令示例。

示例#1：show classofservice trust

```
(Netgear Switch) #show classofservice trust ?

<cr>                    Press Enter to execute the command.

(Netgear Switch) #show classofservice trust

Class of Service Trust Mode: Dot1P
```

示例#2：set classofservice trust mode

```
(Netgear Switch) (Config)#classofservice ?

dot1p-mapping            Configure dot1p priority mapping.
ip-dscp-mapping          Maps an IP DSCP value to an internal traffic class.
trust                    Sets the Class of Service Trust Mode of an Interface.

(Netgear Switch) (Config)#classofservice trust ?

dot1p                    Sets the Class of Service Trust Mode of an Interface
                         to 802.1p.
ip-dscp                  Sets the Class of Service Trust Mode of an Interface
                         to IP DSCP.

(Netgear Switch) (Config)#classofservice trust dot1p ?

<cr>                     Press Enter to execute the command.

(Netgear Switch) (Config)#classofservice trust dot1p
```

示例#3：show classofservice ip-precedence-mapping

```
(Netgear Switch) #show classofservice ip-precedence-mapping

IP Precedence    Traffic Class
-------------    -------------
    0                1
    1                0
    2                0
    3                1
    4                2
    5                2
    6                3
    7                3
```

示例#4：配置 Cos-queue Min-bandwidth 和 Strict Priority Scheduler Mode

```
(Netgear Switch) (Config)#cos-queue min-bandwidth ?

<bw-0>                   Enter the minimum bandwidth percentage for Queue 0.

(Netgear Switch) (Config)#cos-queue min-bandwidth 15

Incorrect input! Use 'cos-queue min-bandwidth <bw-0>..<bw-7>.

(Netgear Switch) (Config)#cos-queue min-bandwidth 15 25 10 5 5 20 10 10


(Netgear Switch) (Config)#cos-queue strict ?

<queue-id>               Enter a Queue Id from 0 to 7.

(Netgear Switch) (Config)#cos-queue strict 1 ?

<cr>                     Press Enter to execute the command.
<queue-id>               Enter an additional Queue Id from 0 to 7.

(Netgear Switch) (Config)#cos-queue strict 1
```

示例#5：配置接口 CoS Trust Mode

```
(Netgear Switch) (Config)#classofservice trust ?

dot1p                     Sets the Class of Service Trust Mode of an Interface
                          to 802.1p.
ip-dscp                   Sets the Class of Service Trust Mode of an Interface
                          to IP DSCP.

(Netgear Switch) (Config)#classofservice trust dot1p ?

<cr>                      Press Enter to execute the command.

(Netgear Switch) (Config)#classofservice trust dot1p
```

流量整形

这部分描述流量整形的特性。
流量整形控制通过网路传输的流量。流量整形具有平滑临时突发的数据流量的作用。

命令行界面示例

使用 traffic-shape 命令来启用流量整形，为所有接口（全局配置模式）或单一个接口（接口配置模式）指定最大的传输带宽限制。
<bw>值是从 0 到 100 递增 5 的百分比。默认的带宽值是 0，意味着没有上限，允许接口以最大的线速来传输。
<bw>值不受每队列最大带宽值约束并被认为是一个二层传输速率控制机制，用来调节整个接口的输出不管外出的流量源于哪个队列。

示例#1：traffic-shape

```
(Netgear Switch) (Config)#traffic-shape ?

<bw>                      Enter the shaping bandwidth percentage from 0 to 100
                          in increments of 5.

(Netgear Switch) (Config)#traffic-shape 70 ?

<cr>                      Press Enter to execute the command.

(Netgear Switch) (Config)#traffic-shape 70

(Netgear Switch) (Config)#
```

第十一章 差异化服务(Differentiated Services)

差异化服务(DiffServ) 是实现服务质量(QoS)的一种技巧。在您的网络中使用 DiffServ 让您在交换机和路由器上直接配置相应参数比使用特定协议更方便。这一章介绍如何配置 7000 系列网管交换机来定义一个数据包属于何种流量类型及这类数据包应如何设置让它得到相应的 QoS。作为 7000 系列网管交换机的一个功能，DiffServ 允许您控制哪种流量该接收转发、哪种流量该丢弃。

如何在 7000 系列交换机上设置 DiffServ 支持将根据您的交换机在网络中的扮演的角色而变化:

- **边缘设备：**边缘设备处理输入的流量，将流量转发到网络核心以及将核心输出的流量转发出来。边缘设备将进站的流量隔离成小的流量类型集,负责决定一个数据包分级。 分级主要根据第三层和第四层的数据包报头内容以及记录在数据包 IP 报文头的差异化服务编码点（DSCP）。
- **内部节点：**网络核心交换机负责数据包转发多过为它们分级。它对进来的数据包的 DSCP 编码点进行解码并提供适当的队列管理算法进行存储转发服务。

在您对 7000 系列网管交换机进行详细的 DiffServ 配置之前，您必须确定这个网络的 QoS 需求。这些需求以在特定接口上定义的进站流量的分类规则来表示，交换机软件暂时不支持出站方向的 DiffServ。

DiffServ 规则是根据分类（Class）、策略（Policy）和服务（Service）来定义的:

- **Class：** 一个分类是由一组定义数据包归属分类的规则组成的。进站流量根据第三层和第四层数据报头、VLAN 号和已定义的相应 DSCP 值来划分成流量分类的。支持一种分类：**All**，它指定所有分类的匹配标准都必须匹配才生效。
- **Policy：** 为一个或多个分类定义 QoS 特征，例如可以为进入的数据包做标记。7000 系列网管交换机支持流量情况的策略。这类策略结合进站流量分类来指定数据包遇到匹配的分类时的动作：
  – 给数据包打上 DSCP 编码点、IP 优先级或者 CoS 标记。
  – 制定数据包转发策略如丢弃或者重新标记超过分类指定带宽的数据包
  – 在分类里面统计流量
- **Service：**为一个接口的进站流量指定策略。

命令行界面示例：

该示例介绍网络管理员如何为一个公司的不同部门提供平等的上网(或外部其他网络)带宽。四个部门均有自己的 B 类地址段并允许使用上网端口的 25% 的带宽。

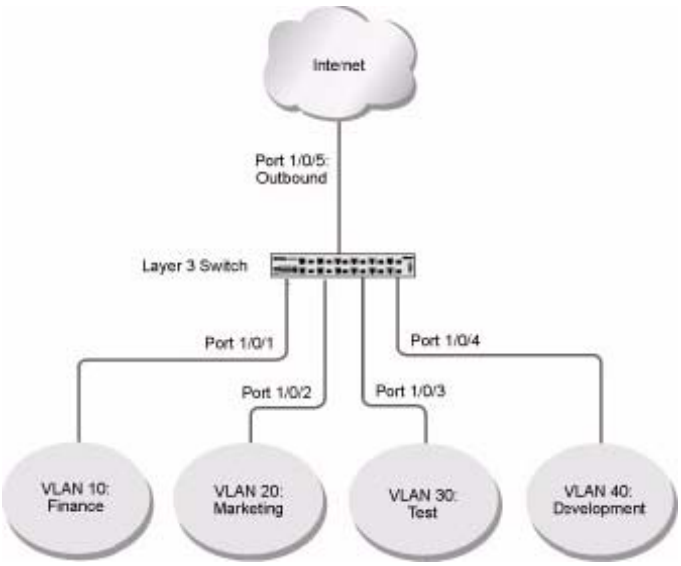


图 11-1

以下是配置 7000 系列网管交换机的示例：

在交换机上启用DiffServ功能。

(Netgear Switch) #config(Netgear Switch) (Config)#**diffserv**

为各部门创建DiffServ匹配分类为all的Class并为它们命名。为新的Class定义匹配标准——源IP地址。

(Netgear Switch) (Config)#**class-map match-all finance_dept**

(Netgear Switch) (Config class-map)#**match srcip 172.16.10.0 255.255.255.0**

(Netgear Switch) (Config class-map)#**exit**

(Netgear Switch) (Config)#**class-map match-all marketing_dept**

(Netgear Switch) (Config class-map)#**match srcip 172.16.20.0 255.255.255.0**

(Netgear Switch) (Config class-map)#**exit**

(Netgear Switch) (Config)#**class-map match-all test_dept**

(Netgear Switch) (Config class-map)#**match srcip 172.16.30.0 255.255.255.0**

(Netgear Switch) (Config class-map)#e**xit**

(Netgear Switch) (Config)#**class-map match-all development_dept**

(Netgear Switch) (Config class-map)#**match srcip 172.16.40.0 255.255.255.0**

(Netgear Switch) (Config class-map)#**exit**

为进站流量创建名为"internet_access"的Diffserv策略，在这个策略里增加示例里先前创建的Class。这个策略为各部门传出的流量定义不同的队列属性。下面是如何建立DiffServ的进站策略与CoS队列设置的关联：

(Netgear Switch) (Config)#**policy-map internet_access in**
(Netgear Switch) (Config policy-map)#**class finance_dept**
(Netgear Switch) (Config policy-class-map)#**assign-queue 1**
(Netgear Switch) (Config policy-class-map)#**exit**
(Netgear Switch) (Config policy-map)#**class marketing_dept**
(Netgear Switch) (Config policy-class-map)#**assign-queue 2**
(Netgear Switch) (Config policy-class-map)#**exit**
(Netgear Switch) (Config policy-map)#**class test_dept**
(Netgear Switch) (Config policy-class-map)#**assign-queue 3**
(Netgear Switch) (Config policy-class-map)#**exit**
(Netgear Switch) (Config policy-map)#**class development_dept**
(Netgear Switch) (Config policy-class-map)#**assign-queue 4**
(Netgear Switch) (Config policy-class-map)#**exit**
(Netgear Switch) (Config policy-map)#**exit**

将定义的策略应用到接口1/0/1到1/0/4上的进站方向。

(Netgear Switch) (Config)#**interface 1/0/1**

(Netgear Switch) (Interface 1/0/1)#**service-policy in internet_access**

(Netgear Switch) (Interface 1/0/1)#**exit**

(Netgear Switch) (Config)#**interface 1/0/2**

(Netgear Switch) (Interface 1/0/2)#**service-policy in internet_access**

(Netgear Switch) (Interface 1/0/2)#**exit**

(Netgear Switch) (Config)#**interface 1/0/3**

(Netgear Switch) (Interface 1/0/3)#**service-policy in internet_access**

(Netgear Switch) (Interface 1/0/3)#**exit**

(Netgear Switch) (Config)#**interface 1/0/4**

(Netgear Switch) (Interface 1/0/4)#**service-policy in internet_access**

(Netgear Switch) (Interface 1/0/4)#**exit**

在(假设的)出口的接口1/0/5上为CoS队列如1，2，3和4设置最少保证带宽为25%。这个接口上的全部队列使用照默认一系列的最有利时序安排。DiffServ进站策略指定这些为各

部门流量的等待队列的属性，它假设交换机将普通的目标地址为因特网流量到1/0/5接口。

(Netgear Switch) (Config)#**interface 1/0/5**

(Netgear Switch) (Interface 1/0/5)#**cos-queue min-bandwidth 0 25 25 25 25 0 0 0**

(Netgear Switch) (Interface 1/0/5)#**exit**

(Netgear Switch) (Config)#**exit**

DiffServ 设置 VoIP 的示例

一个很有价值的 DiffServ 用途就是支持基于 IP 的语音（VOIP）。VoIP 流量是固定的时间感应：在一个提供接受服务的网络里，保证传输率是很重要的。这个示例说明了如何设置单向提供必要的服务质量。

一类UDP流量，在进站方向已经做了流量标记，然后在出站方向保证这些流量的畅通。如这个图11-2里的Router 1的配置脚本，同样Router 2也应做相应的配置脚本。

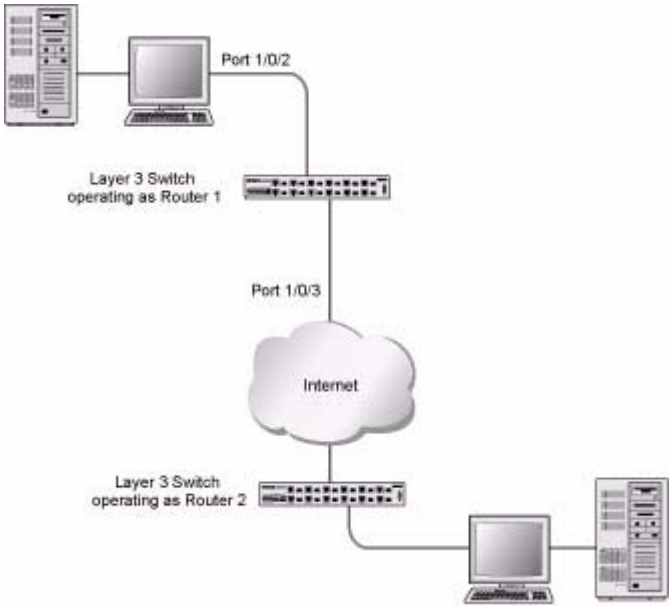


图 11-2

以下示例配置了 DiffServ 支持 VoIP:

进入全局配置模式。设置所有端口上的队列5使用精确优先级模式，这个队列为所有VoIP包使用。并在交换机上激活DiffServ功能。

(Netgear Switch) #**config**

(Netgear Switch) (Config)#**cos-queue strict 5**

(Netgear Switch) (Config)#**diffserv**

创建DiffServ分类名字为"Class_voip"并为要检测的UDP包定义单个匹配标准。这个分类的类型为"全部匹配"指出所有的匹配标准都必须匹配以使每个数据包被正确匹配处理.

(Netgear Switch) (Config)#**class-map match-all class_voip**

(Netgear Switch) (Config class-map)#**match protocol udp**

(Netgear Switch) (Config class-map)#**exit**

创建第二个DiffServ分类名字为"class_ef"并为检测DiffServ的差异化服务编码点(DSCP)为"EF"（expedited forward）的数据包定义单个匹配标准。它处理进来的在网络其他地方预先标记为"EF"的流量。

(Netgear Switch) (Config)#**class-map match-all class_ef**

(Netgear Switch) (Config class-map)#**match ip dscp ef**

(Netgear Switch) (Config class-map)#**exit**

为进站流量创建一个DiffServ策略名为"pol_voip"，然后将先前定义的分类"class_ef"和"class_voip"增加这个策略内。
这个策略处理进来的已经标记DSCP值为"EF"数据包(由'class_ef'定义)，或者由'class_voip'标记了的UDP数据包，给它们标记DSCP值为'EF'。匹配的数据包在数据转发的出端口使用队列5内部标记。

(Netgear Switch) (Config)#**policy-map pol_voip in**

(Netgear Switch) (Config policy-map)#**class class_ef**

(Netgear Switch) (Config policy-class-map)#**assign-queue 5**

(Netgear Switch) (Config policy-class-map)#**exit**

(Netgear Switch) (Config policy-map)#**class class_voip**

(Netgear Switch) (Config policy-class-map)#**mark ip-dscp ef**

(Netgear Switch) (Config policy-class-map)#**assign-queue 5**

(Netgear Switch) (Config policy-class-map)#**exit**

(Netgear Switch) (Config policy-map)#**exit**

在端口进站方向应用已经定义的策略。

(Netgear Switch) (Config)#**interface 1/0/2**

(Netgear Switch) (Interface 1/0/2)#**service-policy in pol_voip**

(Netgear Switch) (Interface 1/0/2)#**exit**

(Netgear Switch) (Config)#**exit**

第十二章 IGMP 侦听(IGMP Snooping)

这一部分讲述因特网组管理协议（IGMP）的特性：IGMPv3和IGMP侦听。

概述

IGMP:

- 使用IGMPv3版本
- 包括IGMP侦听
- IGMP侦听可以根据每个VLAN来启用

命令行界面示例

以下是使用IGMP侦听特性的命令示例。

示例#1: Enable IGMP Snooping

这个示例显示了如何启用IGMP侦听。

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip igmpsnooping
(Netgear Switch) (Config)#ip igmpsnooping interfacemode
(Netgear Switch) (Config)#exit
```

示例#2: show igmpsnooping

```
(Netgear Switch)#show igmpsnooping ?

<cr>                    Press Enter to execute the command.
<slot/port>         Enter interface in slot/port format.
mrouter                 Display IGMP Snooping Multicast Router information.
<1-4093>                Display IGMP Snooping valid VLAN ID information.
(Netgear Switch)#show igmpsnooping


Admin Mode.....................     Enable
Multicast Control Frame Count.....     0
```

```
Interfaces Enabled for IGMP Snooping.....    1/0/10
Vlans enabled for IGMP snooping.....    20
```

示例#3: show mac-address-table igmpsnooping

```
(Netgear Switch) #show mac-address-table igmpsnooping ?

<cr>                    Press Enter to execute the command.

(Netgear Switch) #show mac-address-table igmpsnooping

                                        Type            Description                 Interfaces
----------------------          -------         --------------          -----------
00:01:01:00:5E:00:01:16         Dynamic     Network Assist          Fwd: 1/0/47
00:01:01:00:5E:00:01:18         Dynamic     Network Assist          Fwd: 1/0/47
00:01:01:00:5E:37:96:D0         Dynamic     Network Assist          Fwd: 1/0/47
00:01:01:00:5E:7F:FF:FA         Dynamic     Network Assist          Fwd: 1/0/47
00:01:01:00:5E:7F:FF:FE         Dynamic     Network Assist          Fwd: 1/0/47
```

第十三章 端口安全（Port Security）

这一部分描述端口安全的特性。

概述

端口安全（Port Security）：

- 允许在一个端口上限制MAC地址的数量。
- 匹配了MAC地址的数据包（安全数据包）就转发，其他数据包（不安全数据包）就限制。
- 基于端口启用。
- 锁定后，只有允许的MAC地址的数据包才会被转发。
- 同时支持动态和静态
- 两种流量过滤的实现方法
  - 动态锁定 – 用户指定一个端口的最多 MAC 地址学习数量。最大 MAC 数要参照软件版本的发布说明。当达到上限时，增加的 MAC 地址将不再学习，只有允许的源 MAC 地址的数据帧才会被转发。
  - 静态锁定 – 用户手工指定一个端口上的静态 MAC 地址列表，动态锁定的地址可以更改成静态锁定。

这些方法可以同时使用。

作用

端口安全：

- 从转发的数据包中预防未知设备来保护网络
- 当连接失效，端口上所有动态锁定的地址将“释放自由”
- 如果一个特定的MAC地址被设置在端口上,设置动态条目为0，那么将仅允许匹配静态列表里的MAC地址的数据包通过。
- 如果其他数据包在老化时间内没有看这个东态锁定的MAC地址，这个地址将老化掉。用户可以设置老化时间。
- 动态锁定的MAC地址可以被其他端口学习。
- 静态锁定的MAC地址将不会老化。
- 动态锁定的地址可以更改成静态锁定。

命令行界面示例

以下是端口安全特性的命令示例。

示例#1: show port security

```
(Netgear Switch) #show port-security ?

<cr>                          Press Enter to execute the command.
All                           Display port-security information for all interfaces.
<unit/slot/port>      Enter interface in unit/slot/port format.
dynamic                   Display dynamically locked MAC addresses.
static                      Display statically locked MAC addresses.
violation                  Display the source MAC address of the last packet that was discarded on a locked
                                port.

(Netgear Switch) #show port-security

Port Security Administration Mode: Enabled
```

示例#2: show port security on a specific interface

```
(Netgear Switch) #show port-security 1/0/10
              Admin            Dynamic       Static       Violation
Intf       Mode               Limit           Limit       Trap Mode
----      --------       -------       ------        ----------
1/0/10   Disabled          600             20               Disabled
```

示例#3: (Config) port security

```
(Netgear Switch) (Config) #port-security ?
<cr>        Press Enter to execute the command.
(Netgear Switch) (Config) #port-security
```

示例#4: (Interface) port security 0

```
(Netgear Switch Routing)(Interface 0/7)#port-security ?
<cr>   Press Enter to execute the command.
mac-address       Add Static MAC address to the interface.
max-dynamic       Set Dynamic Limit for the interface.
max-static       Set Static Limit for the interface.
(Netgear Switch Routing)(Interface 0/7)#port-security max-static ?
<0-20>   Set Static Limit for the interface.
(Netgear Switch Routing)(Interface 0/7)#port-security max-static 5
(Netgear Switch Routing)(Interface 0/7)#port-security max-dynamic 10
```

第十四章 路由跟踪 (Traceroute)

这一部分描述路由跟踪(Traceroute)的特性。

使用Traceroute命令来发现数据包通过一跳接一跳的方式到达目标所经过的网络路由器。 用小的Time-to-Live(TTL)值及观察ICMP超时公告来记录网络路由器。

命令显示所有三层设备Command displays all L3 devices
可以用来检测网络问题Can be used to detect issues on the network
最多跟踪20跳
默认使用UPD33343端口除非用traceroute命令更改

	注意：您只能使用命令行界面的命令执行 TraceRoute 命令——在 WEB 页面没有这个功能。

命令行界面示例

以下是一个用traceroute命令去确定达到目标所需跳数的示例。这个命令输出显示每个经过的路由地址及到达所需的时间。在这个示例里，数据包到达目标一共经过了16跳路由。

```
(Netgear Switch) #traceroute ?
<ipaddr> Enter IP address.
(Netgear Switch) #traceroute 216.109.118.74 ?
<cr>   Press Enter to execute the command.
<port>          Enter port no.
(Netgear Switch) #traceroute 216.109.118.74
Tracing route over a maximum of 20 hops
 1                10.254.24.1      40 ms       9 ms      10 ms
 2                10.254.253.1     30 ms      49 ms      21 ms
 3                63.237.23.33     29 ms      10 ms      10 ms
 4                63.144.4.1          39 ms      63 ms      67 ms
 5                63.144.1.141     70 ms      50 ms      50 ms
 6                205.171.21.89    39 ms      70 ms      50 ms
 7                205.171.8.154    70 ms      50 ms      70 ms
 8                205.171.8.222    70 ms      50 ms      80 ms
 9                205.171.251.34   60 ms      90 ms      50 ms
10                209.244.219.181  60 ms      70 ms      70 ms
11                209.244.11.9     60 ms      60 ms      50 ms
12                4.68.121.146     50 ms      70 ms      60 ms
13                4.79.228.2          60 ms      60 ms      60 ms
14                216.115.96.185  110 ms      59 ms      70 ms
15                216.109.120.203  70 ms      66 ms      95 ms
```

16	216.109.118.74	78 ms	121 ms	69 ms

第十五章 配置脚本(Configuration Scripting)

这一部分描述配置脚本（Configuration Scripting）的特性。

概述

配置脚本:

- 允许您生成文本格式的文件
- 提供可以上传和下载到系统的脚本
- 可以方便地创建命令配置脚本
- 可以应用在好几款交换机上
- 可以保存10份或者500K大小的脚本
- 允许查看，删除，应用，上传，下载
- 提供每一个命令行界面命令的脚本格式

要点

- 存储在交换机的脚本数量由存储器大小决定。
- 如果脚本损坏，脚本是分部分执行的。例如，脚本执行了十个命令中的五句，然后损坏了，那么脚本就会挺在第五个。
- 脚本正在应用的时候是不可以修改或者删除的。
- 脚本只检查语法错误，如果脚本检查不通过则不会运行。

命令行界面示例

以下是使用脚本配置这项特性的命令参考

示例#1: script

(Netgear Switch) #**script ?**	
apply	Applies configuration script to the switch.
delete	Deletes a configuration script file from the switch.
list	Lists all configuration script files present on the switch.
show	Displays the contents of configuration script.
validate	Validate the commands of configuration script.

示例#2: script list and script delete

```
(Netgear Switch) #script list
Configuration Script Name                Size(Bytes)
-------------------------            ----------
basic.scr                                    93
running-config.scr                           3201

2 configuration script(s) found.
1020706 bytes free.
(Netgear Switch) #script delete basic.scr
Are you sure you want to delete the configuration script(s)? (y/n) y
1 configuration script(s) deleted.
```

示例#3: script apply running-config.scr

```
(Netgear Switch) #script apply running-config.scr
Are you sure you want to apply the configuration script? (y/n) y
The systems has unsaved changes.
Would you like to save them now? (y/n) y
Configuration Saved!
```

示例#4: Creating a Configuration Script

```
(Netgear Switch) #show running-config running-config.scr
Config script created successfully.
(Netgear Switch) #script list
Configuration Script Name            Size(Bytes)
-------------------------          ------------
running-config.scr                       32011

configuration script(s) found.
1020799 bytes free.
```

示例#5: Upload a Configuration Script

```
(Netgear Switch) #copy nvram: script running-config.scr
  tftp://192.168.77.52/running-config.scr
Mode.....................       TFTP
Set TFTP Server IP.....              192.168.77.52
TFTP Path.....................          ./
```

```
TFTP Filename.....              running-config.scr
Data Type.....                  Config Script
Source Filename.....            running-config.scr
Are you sure you want to start? (y/n) y
File transfer operation completed successfully.
```

第十六章 出站 TELNET（Outbound Telnet）

这一部分介绍出站TELNET(Outbound Telnet)的特性。

概述

出站Telnet(Outbound Telnet):

- 在设备和远程主机之间建立一个出站telnet连接。
- 一个telnet连接开始之后，每一端的连接都被假定在网络虚拟终端(Network Virtual Terminal" (NVT))开始和结束。
- 服务器和用户主机不维护对方的终端及处理机制的特有信息。
- 必须使用有效的IP地址。

命令行界面示例

以下是使用出站Telnet特性的命令示例。

示例#1: show network

```
(Netgear Switch Routing) >telnet 192.168.77.151
Trying 192.168.77.151...
(Netgear Switch Routing)
User:admin
Password:
(Netgear Switch Routing)>en
Password:
(Netgear Switch Routing)#show network
IP Address..... 192.168.77.151
Subnet Mask..... 255.255.255.0
Default Gateway..... 192.168.77.127
Burned In MAC Address..... 00:10:18.82.04:E9
Locally Administered MAC Address..... 00:00:00:00:00:00
MAC Address Type..... Burned In
Network Configuration Protocol Current... DHCP
Management VLAN ID..... 1
Web Mode..... Enable
Java Mode ..... Disable
```

示例#2: show telnet

```
(Netgear Switch Routing)#show telnet
Outbound Telnet Login Timeout (minutes)..... 5
Maximum Number of Outbound Telnet Sessions..... 5
Allow New Outbound Telnet Sessions..... Yes
```

示例#3: transport output telnet

```
(Netgear Switch Routing) (Config)#lineconfig ?
<cr>                    Press Enter to execute the command.
(Netgear Switch Routing) (Config)#lineconfig
(Netgear Switch Routing) (Line)#transport ?
input                   Displays the protocols to use to connect to a
                        specific line of the router.
output                  Displays the protocols to use for outgoing
                        connections from a line.
(Netgear Switch Routing) (Line)#transport output ?
telnet                  Allow or disallow new telnet sessions.
(Netgear Switch Routing) (Line)#transport output telnet ?
<cr>                    Press Enter to execute the command.
(Netgear Switch Routing) (Line)#transport output telnet
(Netgear Switch Routing) (Line)#
```

示例#4: session-limit and session-timeout

```
(Netgear Switch Routing) (Line)#session-limit ?
<0-5>       Configure the maximum number of outbound telnet sessions allowed.
(Netgear Switch Routing) (Line)#session-limit 5
(Netgear Switch Routing) (Line)#session-timeout ?
<1-160>                 Enter time in minutes.
(Netgear Switch Routing) (Line)#session-timeout 15
```

第十七章 端口镜像（Port Mirroring）

这一部分描述端口镜像（Port Mirroring）特性。

概述

端口镜像：

- 使您可以使用一个外部的网络分析仪器监控网络流量。
- 为进出的数据包转发一份拷贝到指定的端口
- 作为一个诊断工具，常用于网络排错或者防止攻击
- 指定一个特定的端口来复制全部数据包
- 允许进站到交换机或者出站到它们目标的数据包复制到镜像端口

命令行界面示例

以下是使用端口镜像特性的命令示例。

示例#1: show monitor session

```
(Netgear Switch Routing) #show monitor session 1
Session ID      Admin Mode      Probe Port   Mirrored Port
----------      ----------      ----------   -------------
1                  Enable           1/0/8          1/0/7
```

注意：镜像会话号“1”-这个“1”是硬件限制。

示例#2: show port all

```
(Netgear Switch Routing) #show port all
                        Admin     Physical    Physical     Link      Link      LACP
Intf      Type          Mode      Mode          Status       Status    Trap      Mode
----      ----      ------  -------    --------    ------    ----    ----
1/0/1                   Enable    Auto                      Down      Enable    Enable
1/0/2                   Enable    Auto                       Down     Enable    Enable
1/0/3                   Enable    Auto                       Down     Enable    Enable
1/0/4                   Enable    Auto                       Down     Enable    Enable
1/0/5                   Enable    Auto                       Down     Enable    Enable
```

```
1/0/6                Enable   Auto                    Down    Enable   Enable
1/0/7     Mirror     Enable   Auto                    Down    Enable   Enable
1/0/8     Probe      Enable   Auto                    Down    Enable   Enable
1/0/10               Enable   Auto                    Down    Enable   Enable
```

示例#3: show port interface

为特定的端口使用这个命令，输出显示这个端口是否被设置成镜像或者被镜像端口以及端口其他功能的启用或停用功能。

```
(Netgear Switch Routing) #show port 0/7
                     Admin    Physical   Physical   Link     Link     LACP
Intf      Type       Mode     Mode       Status     Status   Trap     Mode
--------  ---------- -------- ---------- ---------- -------- -------- --------
1/0/7     Mirror     Enable   Auto                  Down     Enable   Enable
(Netgear Switch Routing) #show port 0/8
                     Admin    Physical   Physical   Link     Link     LACP
Intf      Type       Mode     Mode       Status     Status   Trap     Mode
--------  ---------- -------- ---------- ---------- -------- -------- --------
1/0/8     Probe      Enable   Auto                  Down     Enable   Enable
```

示例#4: (Config) monitor session 1 mode

设置端口镜像，指定监控会话及模式

```
(Netgear Switch Routing)(Config)#monitor ?
session      Configure port mirroring.

(Netgear Switch Routing)(Config)#monitor session ?
<1-1>        Session number.

(Netgear Switch Routing)(Config)#monitor session 1 ?
destination  Configure the probe interface.
mode         Enable/Disable port mirroring session.
source       Configure the source interface.

(Netgear Switch Routing)(Config)#monitor session 1 mode ?
<cr>         Press Enter to execute the command.

(Netgear Switch Routing)(Config)#monitor session 1 mode
```

示例#5: (Config) monitor session 1 source interface

指定镜像会话的源（被监控）端口和目标（监控）端口。

```
(Netgear Switch Routing)(Config)#monitor session 1 source ?
interface       Configure interface.

(Netgear Switch Routing)(Config)#monitor session 1 source interface ?
<slot/port>     Enter the interface.

(Netgear Switch Routing)(Config)#monitor session 1 source interface 0/7

(Netgear Switch Routing)(Config)#monitor session 1 destination ?
interface       Configure interface.

(Netgear Switch Routing)(Config)#monitor session 1 destination interface ?
<slot/port>     Enter the interface.

(Netgear Switch Routing)(Config)#monitor session 1 destination interface 0/8
```

第十八章 简单网络时间协议 (SNTP)

这一部分描述简单网络时间协议 (SNTP)的特性。

概述

SNTP:

- 用来同步网络资源
- 由网络时间协议（NTP）改编
- 提供同步的网络时间戳
- 可以用于广播和单播模式
- SNTP客户端使用UDP 123端口进行侦听

命令行界面示例

以下是使用SNTP特性的命令行示例。

示例#1: show sntp

```
(Netgear Switch Routing) #show sntp ?

<cr>        Press Enter to execute the command.
client      Display SNTP Client Information.
server      Display SNTP Server Information.
```

示例#2: show sntp client

```
(Netgear Switch Routing) #show sntp client

Client Supported Modes:         unicast broadcast
SNTP Version:                   4
Port:                           123
Client Mode:                    unicast
Unicast Poll Interval:      6
Poll Timeout (seconds):         5
Poll Retry:                     1
```

示例#3: show sntp server

```
(Netgear Switch Routing) #show sntp server

Server IP Address:              81.169.155.234
Server Type:                    ipv4
Server Stratum:                 3
Server Reference Id:            NTP Srv: 212.186.110.32
Server Mode:                    Server
Server Maximum Entries:         3
Server Current Entries:         1
SNTP Servers
------------
IP Address:                     81.169.155.234
Address Type:                   IPV4
Priority:                       1
Version:                        4
Port:                           123
Last Update Time:               MAY 18 04:59:13 2005
Last Attempt Time:              MAY 18 11:59:33 2005
Last Update Status:             Other
Total Unicast Requests:         1111
Failed Unicast Requests:        361
```

示例#4: Configure SNTP

NETGEAR交换机没有内置的实时时钟。然而，他可以使用SNTP去互联网上的开放的SNTP/NTP服务器获得时间。您需要从这些时间服务器获得许可。以下步骤是设置交换机的SNTP。

1. 配置SNTP服务器的IP地址。这个IP地址可以是开放的NTP服务器或者是您自己的。您可以搜索互联网来定位开放的服务器。这些可用的服务器可能是用域名格式代替IP地址格式列出来。在本案例中，在PC上使用ping命令来找出服务器的IP地址。示例中配置的SNTP服务器地址为208.14.208.19。

```
(Netgear Switch) (Config)#sntp server 208.14.208.19
```

2. 设置IP地址以后，启用SNTP客户端模式。客户端模式可以是广播模式也可以是单播模式。如果NTP服务器不是您自己的，您必须使用单播模式。

```
(Netgear Switch) (Config)#sntp client mode unicast
```

3. 一旦启用，客户端就会等待刷新间隔去发送请求到服务器。这个默认值大约是1分钟。这个时期过后，使用show命令来确认是否接收到时间。这个时间将被用以所有的日志记录。

```
(Netgear Switch) #show sntp server
Server IP Address:                208.14.208.19
Server Type:                      ipv4
Server Stratum:                   4
Server Reference Id:              NTP Srv: 208.14.208.3
Server Mode:                      Server
Server Maximum Entries:           3
Server Current Entries:           1
SNTP Servers
-------------
IP Address: 208.14.208.19
Address Type: IPV4
Priority: 1Version: 4
Port: 123
Last Update Time: Mar 26 03:36:09 2006
Last Attempt Time: Mar 26 03:36:09 2006
Last Update Status: Success
Total Unicast Requests: 2
Failed Unicast Requests: 0
```

示例#5: Setting Time Zone

SNTP/NTP服务器默认情况下是国际标准时间(UTC) 。以下示例说明如何设置时区为北京时间(Beijing)，北京时间比GMT/UTC早8个小时。

```
(Netgear switch)(config)#clock timezone Beijing 8
```

示例#6: Setting Named SNTP Server

NETGEAR提供可以被访问的SNTP服务器，因为NETGEAR可能会改变对这些时间服务器指定的IP地址，最好用域名代替IP地址来访问SNTP服务器。这些公开的时间服务器分别是time-a、time-b和time-c。要使用这项功能，请参考以下步骤：用以下命令来启用DNS及访问时间服务器。

```
(Netgear switch) (config)#ip domain-lookup
(Netgear switch) (config)#ip name-server 192.168.1.1
(Netgear switch) (config)#sntp server time-a.netgear.com
```

这里的 “192.168.1.1” 是您设备的网关地址。用这个方法来设置DNS域名解释可以同时用作其他要解释IP地址的程序，例如RADIUS服务器。

第十九章 交换机堆叠管理（Managing Switch Stacks）

这一部分描述NETGEAR可堆叠网管交换机4.x.x.x以上版本的概念和操作步骤。NETGEAR可以堆叠网管交换机包括以下型号：

- FSM7328S
- FSM7328PS
- FSM7352S
- FSM7352PS
- GSM7328S
- GSM7328FS
- GSM7352S

	注意：目前 FSM 系列和 GSM 系列不可以混合堆叠。

这一章包括以下话题：

- 初始化安装及打开交换机堆叠的电源
- 从交换机堆叠移除一台设备
- 增加一台设备到正在运行的交换机堆叠
- 用新的设备替代交换机堆叠里的主交换机
- 重新设置堆叠成员号
- 转移主交换机到交换机堆叠里的另一个设备
- 从运行中的交换机堆叠里移除主交换机
- 合并两个正在运行的交换机堆叠
- 预配置
- 软件升级
- 软件升级后的配置移植

理解交换机堆叠

一个*交换机堆叠*可以通过他们堆叠口连接最多8台以太网交换机。堆叠中的其中一台操作和控制整个堆叠交换机叫做主交换机。主交换机和其他堆叠里的交换机都是堆叠成员。堆叠成员通过堆叠拓扑当成一个系统来运作。交换机堆叠的二层和三层协议在网络中都可以看作单一台设备。

主交换机是整个堆叠的单一管理点，通过主交换机，您设置：

- 系统等级（全局）的特性将应用到整个交换机堆叠
- 任意堆叠成员的所有接口的接口等级的特性

交换机堆叠式通过它的IP地址被网络识别的。IP地址则关联堆叠的主交换机MAC地址。每一个堆叠成员是根据它们的堆叠号来识别的。

所有堆叠成员都可以作为主交换机。如果主交换机变得不可用，剩下的堆叠成员将从他们自己中间选出一台作为主交换机。一系列因素决定哪一台将交换机被选为主交换机，它们是：

1. 主交换机一直保持作为主交换机的优先权.
2. 指定的优先级
3. MAC地址

如果主交换机不能根据(1)来选择，则根据(2),如果(2)也不能决定哪台堆叠成员成为主交换机，那么就根据(3)决定。

主交换机为交换机堆叠存储已保存的和正在运行的配置文件。这些配置文件包括整个交换机堆叠的系统级别的设置，以及所有堆叠成员端口级别的设置。每一个堆叠成员拥有一份已保存的配置文件的副本作为备份用。

如果主交换机被移除，其他成员将选出新的主交换机，然后使用保存的配置文件运行。

您可以使用这些方法来管理交换机堆叠：

- 堆叠WEB。
- 通过连接主交换机Console口的命令行界面(CLI) 。
- 通过一个简单网络管理协议(SNMP)的软件程序。

交换机堆叠成员

一个交换机堆叠可以通过他们的堆叠端口拥有最多八个堆叠成员。一个交换机堆叠只有一台主交换机。

一台独立的交换机是一个只有一台堆叠成员的交换机堆叠，它同时作为主交换机。您可以连接一台独立的交换机到另一台来创建一个包含两个堆叠成员的交换机堆叠，其中一台将成为主交换机。您可以连接一台独立的交换机到已有的交换机堆叠上来增加堆叠成员的数量。

如果用同样型号的交换机更换一个堆叠成员，新的交换机将使用原交换机的配置正常运行。更多预配置的好处请看“预配置”。

堆叠成员改变期间，交换机运行是不会中断的。除非移除了主交换机或者添加一台已经开了机的单独交换机/交换机堆叠。

- 增加已经开机的交换机会导致并入的交换机重新选举主交换机。重新选举的主交换机将使用它原有的配置来担任主交换机角色。所有保留的交换机包括以前的主交换机将以堆叠成员的身份重新启动并加入堆叠，它们的堆叠号被改变为最小的可用号码并使用重新选出的主交换机的配置信息。因此，当您合并两个已经开了机的交换机堆叠,你无法控制哪台交换机将成为新的主交换机及使用哪个配置。基于这些愿意，建议增加交换机到现有的堆叠时先关掉电源。
- 移除已开机的堆叠成员会导致原交换机堆叠分成两个以上的交换机堆叠。每个都使用相同的配置，但如果线缆全部接好，交换机堆叠就不会被分隔。
    - 如果交换机堆叠分隔了，并且您希望保留分隔出来的部分，请更改新的交换机堆叠的IP地址。
    - 如果您不希望交换机堆叠被分隔：

- 关闭新分隔出来的交换机堆叠的电源。
- 通过堆叠端口重新连接它们到之前的交换机堆叠。
- 打开交换机的电源。

堆叠电缆(FSM73xxS)

图19-1和图19-2阐明了单独的交换机如何连接成为一个交换机堆叠，您可以使用标准的8芯五类线。

Switch Stack Cabling (FSM73xxS)

Figure 19-1 and Figure 19-2 illustrate how individual switches are interconnected to form a stack. You can use the regular Category 5 Ethernet 8 wire cable.

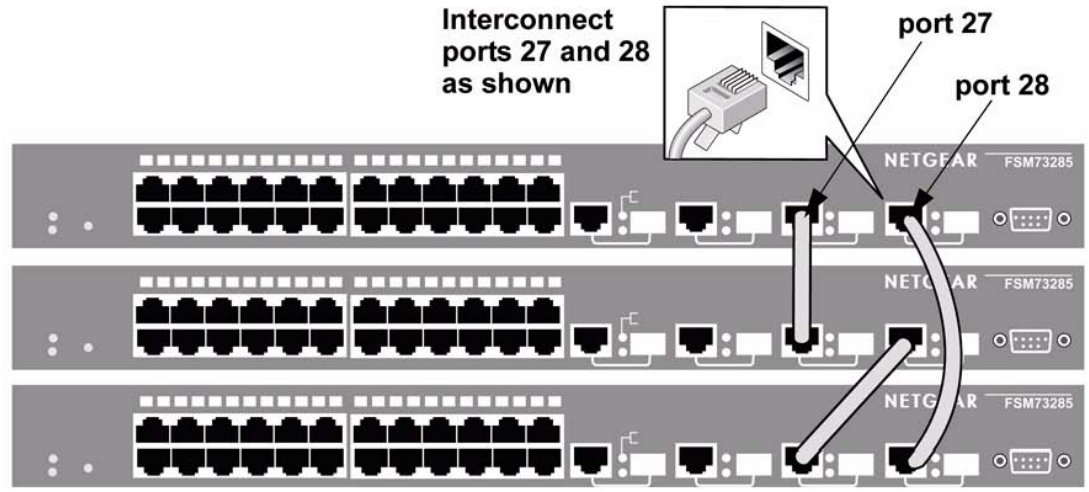


Figure 19-1

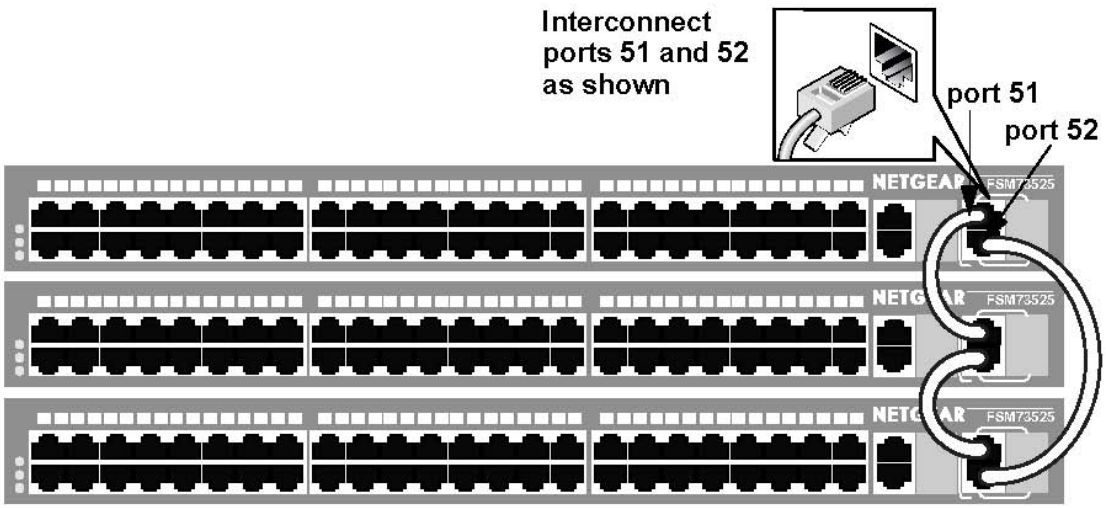
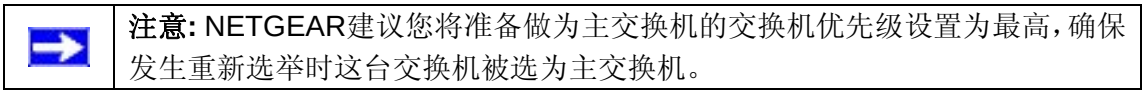


Figure 19-2

主交换机选举和重新选举

主交换机是根据以下规则顺序选举和重新选举的：

1 交换机目前是主交换机
2 拥有的最高优先值的交换机堆叠成员



3 拥有最高MAC地址的交换机

主交换机将保留它的角色，除非发生以下事件之一：

- 主交换机从交换机堆叠中移除
- 主交换机重启或者电源关闭
- 主交换机坏了。
- 交换机堆叠成员增加了已经开机的交换机或交换机堆叠。

当主交换机重新选举，一台新的主交换机会在几秒钟后生效。同时，交换机堆叠使用内存里的转发表来工作以使网络中断减少到最少。当新的主交换机选出来后，其他可用的堆叠成员的物理接口将不受影响。

如果一台新的主交换机选出来后，之前的主交换机恢复工作，那么之前的主交换机将不恢复它的主交换机角色。

堆叠成员号

堆叠成员号（1到8）识别交换机堆叠里的各个成员。成员号同时决定堆叠成员的接口等级配置。您可以使用**show switch**命令来查看堆叠成员号。

一个新的，刚拆箱的（未加入过交换机堆叠或者未被手动指定堆叠成员号的）交换机默认的堆叠成员号是1。当它加入到一个交换机堆叠，他的默认堆叠成员号将被改成堆叠里最小的可用堆叠成员号。

交换机堆叠里的堆叠成员不能使用相同的堆叠成员号。每个堆叠成员，包括独立的交换机，将保留它的堆叠成员号，除非您手动更改或者是这个号码已经被堆叠里的其他成员使用。

请查看 “重新设置堆叠成员号” 和 “合并两个正在运行的交换机堆叠”。

堆叠成员优先值

如果用户希望改变哪个交换机去管理堆叠，可以改变堆叠成员优先值。使用以下命令来改变堆叠成员的优先值（这个命令在全局配置模式下）：

switch unit **priority** value

交换机堆叠脱机配置

您可以使用脱机配置的特性在一个新交换机加入交换机堆叠之前对它进行预配置（应

用到新交换机的配置）。您可以预先对还没成为堆叠成员的交换机配置堆叠成员号，交换机类型，接口等信息。(请参阅 “预配置”)

增加一个做了预配置的交换机到交换机堆叠的结果

当您增加一个做了预配置的交换机到交换机堆叠，堆叠将使用预先做好的配置或者默认配置。表19-1罗列了当交换机堆叠比较新增的交换机的预配置时的结果：

表 19-1. 比较新交换机的预设置时的结果

情形	结果
堆叠成员号和交换机类型匹配。 • 如果预配置交换机的堆叠成员号匹配交换机堆叠里配置的堆叠成员号，并且 • 预配置的交换机类型匹配交换机堆叠里配置的交换机类型	交换机堆叠将应用它的配置到预配置的交换机，并将它加入堆叠。
堆叠成员号匹配但交换机类型不匹配。 •如果预配置交换机的堆叠成员号匹配交换机堆叠里配置的堆叠成员号，但是 • 预配置的交换机类型与交换机堆叠里配置的交换机类型不匹配	• 交换机堆叠将应用默认配置到预配置的交换机，并将它加入堆叠 • 预配置交换机里的配置将改成新的信息。
配置里找不到堆叠成员号。	• 交换机堆叠将应用默认配置到预配置的交换机，并将它加入堆叠 • 预配置交换机里的配置将改成新的信息。
配置里没有预配置交换机设置的堆叠成员号。	交换机堆叠将应用默认配置到预配置的交换机，并将它加入堆叠

在交换机堆叠里更换预配置的交换机的结果

当交换机堆叠里的一台预配置的交换机坏了，从堆叠里移除，并用另一台交换机替代后，交换机将使用预先做好的配置或者默认配置。当交换机比较预配置交换机的配置是，它的结果和“增加一个做了预配置的交换机到交换机堆叠的结果”描述的一样。

从交换机移除一台预配置的交换机的结果

如果从交换机堆叠里移除一台预配置的交换机，移除的堆叠成员的配置仍然保留在交换机堆叠的运行配置里面。要完全移除它配置，使用**no member** *unit_number* *命令*。 (在堆叠模式下).

交换机堆叠软件兼容建议

所有堆叠成员必须运行在相同的软件版本来确保交换机堆叠成员之间的兼容性。包括主交换机，必须一致。这有利于确保堆叠成员间的堆叠协议版本完全兼容。

如果堆叠成员运行在不同的软件版本，堆叠成员将不允许加入堆叠，使用**show switch**命令可以列出堆叠成员及其软件版本。详见“软件不匹配”。

不兼容软件及堆叠成员固件升级

您可以使用命**archive download-sw** xmodem | ymodem | zmodem | tftp://*ip/filepath/filename*令来升级不兼容交换机的固件 (在堆叠配置模式下). 它将复制现有堆叠成员的软件到那台不兼容版本的交换机。交换机将自动重启并当以完整功能的成员身份加入交换机堆叠。

交换机堆叠配置文件

交换机配置文件记录所有全局设置及堆叠成员和独立交换机接口设置下的配置信息。执行**save config**命令，所有堆叠成员均存储一份配置文件。如果主交换机不可用，任意堆叠成员担任主交换机后将使用原配置文件。

当一个新的，刚拆包装的交换机加入交换机堆叠，它将使用交换机堆叠设置的系统等级的配置信息。然而您要存储系统等级的配置，您需要运行**save config**命令。

你可以像使用单台交换机那样用copy命令来备份或恢复堆叠配置。

连接交换机堆叠的管理

您可以通过主交换机管理交换机堆叠和交换机堆叠成员的接口配置。您可以通过WEB页面、命令行界面和SNMP。您不可以对单独地对一个堆叠成员进行管理。

通过 Console 口连接交换机堆叠

您只可以通过主交换机的console口连接到主交换机。

通过 Telnet 连接交换机堆叠

您可以通过telnet到交换机堆叠的IP地址来连接主交换机。

交换机堆叠配置情形

表19-2提供了交换机堆叠的配置情形。大多数情形都假设有至少两台交换机通过堆叠端

口进行连接。

表 19-2 交换机堆叠配置情形

情形	结果
主交换机是原有的主交换机 **注意**: 不推荐： • 通过堆叠口连接两台已经开机的交换机。	两台主交换机中只有一台成为新堆叠的主交换机。其他堆叠成员不会成为主交换机。
主交换机由堆叠成员的优先值选出来 • 通过堆叠口连接两台交换机。 • 使用**switch** *stack-member-number* **priority** *new-priority-number* 全局配置命令设置一台堆叠成员为更高的优先值。 • 同时重启两台堆叠成员。	拥有较高优先值的堆叠成员将被选为主交换机。
主交换机根据MAC地址选出来 • 两台堆叠成员有用相同的优先值及软件版本，同时重启两台堆叠成员。	拥有较高MAC地址的堆叠成员将被选为主交换机。
增加一个新的堆叠成员 • 关闭新交换机电源。 • 通过堆叠端口连接新交换机到已经开机的交换机堆叠。 • 开启新交换机电源.	主交换机保持不变。新增加的交换机加入交换机堆叠。
主交换机失效 • 移除 (或者关闭) 主交换机。	根据“主交换机选举和重新选举”, 其中一台堆叠成员将成为新的主交换机。所有剩下的其他堆叠成员仍然保持原有角色，不行要重启。

堆叠建议

这一章节主要是收集堆叠网管交换机的一般流程和实现预期目标时的注意事项。以下列出的是最初的各种步骤。

- 初始化安装及打开交换机堆叠的电源
- 从交换机堆叠移除一台设备
- 增加一台设备到正在运行的交换机堆叠
- 用新的设备替代交换机堆叠里的主交换机
- 重新设置堆叠成员号
- 转移主交换机到交换机堆叠里的另一个设备
- 从运行中的交换机堆叠里移除主交换机
- 合并两个正在运行的交换机堆叠
- 预配置
- 软件升级
- 软件升级后的配置移植

常规操作

- 当执行一个命令时 (例如move management,renumber等),建议在执行下一个命令前先让这个命令完全处理完毕。举例说,如果其中一个堆叠成员刚重启，那么使用show port”命令确认它是否重新加入到堆叠，等所有端口都加进来以后再执行下一个命令。
- 当物理移除或者重新放置一台设备，在断开堆叠线前通常先关闭设备的电源。
- 当重新连接堆叠线缆，应该在开机前连接。如果可以的话，上紧所有（适当的）接口螺丝能确保稳定的连接。

初始化安装及打开交换机堆叠的电源

1 安装设备到机架上。
2 安装所有堆叠电缆。完全安装，包括冗余堆叠链路。强烈建议连接冗余链路。
3 识别哪个设备将作为主交换机。先打开这台的电源。
4 观察console口。让这台机开到登录提示。如果它使用默认配置，它将作为unit#1启用，并自动成为主交换机。否则，需要重新编号。
5 如果可以的话，对其他要加入堆叠的设备做预配置。预配置在“预配置”这一节描述。
6 打开第二台设备的电源，确定它是与已经开机那台临近（堆叠里的下一个设备）。这样能确保第二台设备启动成为堆叠成员而不是另一个堆叠的主交换机。
7 观察主交换机看第二台设备加入堆叠的情况。当第二台设备加入堆叠，使用“show switch”命令来确定。它将分配到一个堆叠号 (unit #2,如果它使用的是默认配置)。
8 给设备重新定义堆叠号，如果需要，建议参阅“重新设置堆叠成员号” 来重新设置堆叠成员号。
9 重复第6-8步增加其他成员到堆叠。同样先打开临近已加入堆叠的设备的电源。

从交换机堆叠移除一台设备

1 确定冗余堆叠连接已经连接并工作。所有堆叠成员应当做成一个环状连接。
2 关掉要移除的设备的电源。
3 断开堆叠电缆。
4 如果设备没有被替换，用堆叠线重新连接被移除的设备的上下级堆叠成员。
5 从机架上移除这台设备。
6 需要的话，可以执行命令: **no member** <unit-id>将设备从配置里移除。

增加一台设备到正在运行的交换机堆叠

1 确定冗余堆叠连接已经连接并工作。所有堆叠成员应当做成一个环状连接。
2 如果可以的话，对新设备做预配置。

3 安装新的设备到机架上。（如安装在原堆叠的最上面或者最下面。）
4 在加入新设备的位置，断开交换机堆叠第一台和最后地台堆叠成员间的冗余堆叠电缆。
5 连接堆叠电缆到新设备，按照“上联”接“下联”的次序建立连接。
6 打开新设备的电源,观察主交换机的console口信息，可以执行**show switch**命令来确定新设备完全加入堆叠。新设备通常以堆叠成员身份加入(不会以主交换机身份；现有的主交换机将不会改变)。
7 如果最新增加的成员的软件与现有堆叠的不同，参考“软件升级”章节进行软件升级。

用新的设备替代交换机堆叠里的主交换机

这里有两种可能出现的情况。

首先，如果您使用相同型号的设备更换主交换机，按照下列步骤操作：

- 参考“从交换机堆叠移除一台设备”章节移除主交换机
- 参考“增加一台设备到正在运行的交换机堆叠”章节及以下特殊情况增加一台新成员到交换机堆叠：
  - 增加的新成员的位置是被移除的设备的位置。
  - “如果可以的话，对新设备做预配置。”这个步骤不需要。

其次，如果您用不同的型号更换主交换机，请按照下列步骤操作：

- 参考“从交换机堆叠移除一台设备”章节移除主交换机。
- 使用**no member**命令来删除刚移除的堆叠成员的配置。
- 参考“增加一台设备到正在运行的交换机堆叠”章节增加一台新成员到交换机堆叠。该设备可以放到刚移除的堆叠成员的位置或者放在堆叠的最后面。任一种情况，都要确保所有堆叠线缆是连接好的，除了新设备将要放入的地方,这样可以使交换机堆叠不会被分成两个堆叠而选出新的主交换机。

重新设置堆叠成员号

1 如果需要明确的编号方法，建议在第一次安装配置堆叠时给交换机堆叠成员指定特定的堆叠成员号。
2 如果堆叠成员号不合适，它可以被重新设置，使用简单的**switch** <oldunit-id> **renumber** <newunit-id>命令行界面命令。这个命令可以在全局配置模式找到。
3 如果新的成员号已经做了预配置。在您重新设置堆叠成员号之前，您需要删除这个成员号的配置。
4 如果必须为现有的多个堆叠成员号重新定义，可能关系到配置信息不匹配。这种情况下，建议除主交换机外的所有堆叠成员都关闭电源，并参考“增加一台设备到正在运行的交换机堆叠”一次增加一个成员回去。

转移主交换机到交换机堆叠里的另一个设备

1 使用 “move management”命令,转移主交换机到您希望指定的堆叠成员号。根据堆叠的大小及配置文件情况，这个操作约需要30秒到3分钟。
2 确保您可以登录到新的主交换机控制台。使用**show switch**命令来检查是否所有设备已经重新加入堆叠。
3 建议更换主交换机后，使用**reload**命令重启交换机堆叠。

从运行中的交换机堆叠里移除主交换机

1 首先,参考“转移主交换机到交换机堆叠里的另一个设备”将主交换机转移到堆叠里的另一个设备。
2 然后，参考“从交换机堆叠移除一台设备”,从堆叠中移除这个设备。

合并两个正在运行的交换机堆叠

强烈建议不要单单使用堆叠电缆将两个正在运行的交换机堆叠（每个都有主交换机）连接起来。如果那样做的话可能因堆叠成员号重复导致不可用。

1 在将一个交换机堆叠加入另一个堆叠前，关闭堆叠里所有设备的电源。
2 物理连接那组关闭电源的堆叠设备到那组运行中的堆叠。
3 完全连接好堆叠电缆，确定冗余链路也已经连接上。
4 然后，打开设备的电源，一次一台，参考“增加一台设备到正在运行的交换机堆叠”的方法。

预配置

除设备号外，堆叠的所有配置都存在管理设备。也就是说，用相同型号的设备更换一台堆叠成员是不需要重新配置的。设备号单独存在每一台交换机，那样重启交换机堆叠后也能用回原先的设备号。连接的设备或者管理员预配置好的设备类型与每个设备自动从管理设备学习到的设备号有关。

1 执行**member** <unit-id> <switchindex>命令来对一个设备进行预配置。支持的设备类型可以用**show supported switchtype**命令显示。
2 然后，用相关的配置命令对刚定义的设备进行配置，就像已经连接的设备一样。
3 预配置的设备的端口会以“分离”状态启用并可以用**show port all**命令查看。这些分离的端口现在可以进行VLAN成员和其他端口细节配置。
4 对一个特定的设备预配置设备类型后，增加一个不同类型的设备会导致交换机报告错误。**show switch** 命令显示新设备“配置不匹配”并且这个设备的端口不会启用。用户可以更改它的堆叠号或者用no member <unit-id>命令删除这个预配置的设备来解决这种情况。

软件升级

新软件可以在主交换机下用copy命令通过TFTP或者xmodem下载管理设备。当软件成功加载到管理设备，将会自动传到堆叠里的其他设备。如果软件传送到堆叠里其他设备的过程中产生错误，运行**archive**命令（在堆叠配置模式）来尝试复制软件到那些没有升级的设备。软件传送到堆叠里其他设备的过程中产生的错误可能由堆叠电缆移除或者设备在传输阶段被重新配置。错误还有可能由目前网络流量（例如广播事件）过大造成。

堆叠里的所有设备必须使用同一个软件版本。不同版本的堆叠设备的端口有可能不能启用，可以用show switch命令来查看“软件不匹配”错误。可以运行archive命令来解决这个问题。这个命令将管理设备的软件复制到堆叠里版本不匹配的其他设备。运行这个命令前，确定管理设备上的软件是您希望使用的版本。当所有堆叠成员的版本均已加载，设备需要重新启动以使用新的软件版本来运行。

软件升级后的配置移植

某些情况，配置不可以和软件升级一起转移。应该参考下列步骤来更新：

1 保存当前配置并将它从交换机堆叠上传，在命令行界面使用copy命令。
2 加载新的软件到堆叠的主交换机，重启堆叠。
3 重启完成前,进去启动菜单并删除配置文件(“restore to factory defaults”)
4 继续启动操作软件。
5 当堆叠启动完，下载保存的配置到主交换机。配置将自动传到堆叠里的所有堆叠成员。

软件不匹配

如果增加到堆叠的设备与主交换机的软件版本不相同，可能产生下列情况：

- “新”设备启动成为堆叠里的“成员”。
- 增加设备的端口将保留“分离”状态。
- 新增的设备的命令行界面将显示一个软件版本不匹配的标记信息。
- 要让这个新增设备正常并入堆叠，应该用copy命令将主交换机的软件加载这台设备上。这台新增的设备应该重启，将正常重启加入堆叠。

第二十章 登录公告（Pre-Login Banner）

这一部分描述登录公告（Pre-Login Banner）的特性。

概述

登录公告（Pre-Login Banner）：

允许您创建命令行登录时的信息屏幕

- 默认情况下，没有公告文件
- 可以上传和下载
- 文件大小不可以大于2K
- 登录公告特性仅在命令行界面界面使用

命令行界面示例

创建登录公告，按以下步骤：

1 在您的PC，用记事本创建一个banner.txt文件，包含将被显示的公告内容。

```
Login Banner - Unauthorized access is punishable by law.
```

2 通过TFTP将文件从PC传送到交换机TFTP

```
(Netgear Switch Routing) #copy tftp://192.168.77.52/banner.txt nvram:clibanner
Mode..................................... TFTP
Set TFTP Server IP..... 192.168.77.52
TFTP Path..... ./
TFTP Filename..... banner.txt
Data Type..... Cli Banner
Are you sure you want to start? (y/n) y
CLI Banner file transfer operation completed successfully!
(Netgear Switch Routing) #exit
(Netgear Switch Routing) >logout

Login Banner - Unauthorized access is punishable by law.
User:
```

	注意：使用“no clibanner”删除交换机公告。

第二十一章 系统日志(Syslog)

这一部分描述系统日志(Syslog)的特性。

概述

系统日志（Syslog）

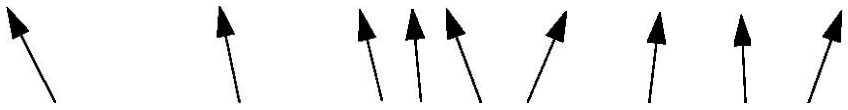
- 允许您存储系统信息和(或)错误
- 可以存储在交换机本地文件或者运行了syslog程序的远程服务器
- 是从多个系统收集信息日志的方法

稳定的日志文件

目前三个-每个的最后三个会话
每个日志包含两部分
系统启动后的头32个启动日志信息
当启动日志满了以后，最后收到的32个操作日志
文件以ASCII格式保存
slog0.txt – slog2.txt
oog0.txt – olog2.txt
0为启动，1为最后启动，2为上次启动;第三个将在下次启动覆盖。
可以保存在本地以及时显示最新的信息

日志文件说明

<130> JAN 01 00:00:06 0.0.0.0-1 UNKN [0x800023]: bootos.c(386) 4 %% Event (0xaaaaaaaa)



A. 优先级
B. 时间戳
C. 堆叠号
D. 类型名称
E. 类型标识
F. 文件名
G. 行号

命令行界面示例

以下是使用系统日志特性的示例。

示例#1: show logging

```
(Netgear Switch Routing) #show logging
Logging Client Local Port              :514
CLI Command Logging                          :      disabled
Console Logging                              :      disabled
Console Logging Severity Filter       :      alert
Buffered Logging                             :      enabled
Syslog Logging                               :      enabled
Log Messages Received                        :66
Log Messages Dropped                         :0
Log Messages Relayed                         :0
Log Messages Ignored                         :0
```

示例#2: show logging buffered

```
(Netgear Switch Routing) #show logging buffered ?
<cr>    Press Enter to execute the command.
(Netgear Switch Routing) #show logging buffered
Buffered (In-Memory) Logging          :      enabled
Buffered Logging Wrapping Behavior    :      On
Buffered Log Count                           :      66

<1>JAN 01 00:00:02 0.0.0.0-0 UNKN[268434944]: usmdb_sim.c(1205) 1 %% Error 0(0x0)
<2>JAN 01 00:00:09 0.0.0.0-1 UNKN[268434944]: bootos.c(487) 2 %% Event (0xaaaaaaaa)
<6> JAN 01 00:00:09 0.0.0.0-1 UNKN[268434944]: bootos.c(531) 3 %% Starting code...
<6>JAN 01 00:00:16 0.0.0.0-3 UNKN[251627904]: cda_cnfgr.c(383) 4 %% CDA: Creating new STK file.
<6>JAN 01 00:00:39 0.0.0.0-3 UNKN[233025712]: edb.c(360) 5 %% EDB Callback: Unit Join: 3.
<6>JAN 01 00:00:40 0.0.0.0-3 UNKN[251627904]: sysapi.c(1864) 6 %% File user_mgr_cfg: same
version (6) but the sizes (2312->7988) differ
```

示例#3: show logging traplogs

```
(Netgear Switch Routing)      #show logging traplogs ?
<cr>    Press Enter to execute the command.
(Netgear Switch Routing)      #show logging traplogs
```

```
Number of Traps Since Last Reset.....           6
Trap Log Capacity.....                          256
Number of Traps Since Log Last Viewed.....      6
Log  System Up Time          Trap
---  --------------      ----------------------------------------------
0    0 days 00:00:46         Link Up: Unit: 3 Slot: 0 Port: 2
1    0 days 00:01:01     Cold Start: Unit: 0
2    0 days 00:21:33     Failed User Login: Unit: 1 User ID: admin
3    0 days 18:33:31     Failed User Login: Unit: 1 User ID: \
4    0 days 19:27:05     Multiple Users: Unit: 0      Slot: 3 Port: 1
5    0 days 19:29:57     Multiple Users: Unit: 0      Slot: 3 Port: 1
```

示例#4: show logging hosts

```
(Netgear Switch Routing) #show logging hosts ?
  <cr>                  Press Enter to execute the command.
(Netgear Switch Routing) #show logging hosts
Index       IP Address              Severity   Port  Status
-----  -----------          ---------      ----   -------
1         192.168.21.253     critical      514          Active
```

示例#5: logging port configuration

```
(Netgear Switch Routing)     #config
(Netgear Switch Routing) (Config)#logging ?

buffered              Buffered (In-Memory) Logging Configuration.
cli-command           CLI Command Logging Configuration.
console               Console Logging Configuration.
host                  Enter IP Address for Logging Host
syslog                Syslog Configuration.
(Netgear Switch Routing) (Config)#logging host ?
<hostaddress>       Enter Logging Host IP Address
reconfigure         Logging Host Reconfiguration
remove              Logging Host Removal
(Netgear Switch Routing) (Config)#logging host 192.168.21.253 ?
<cr>                  Press Enter to execute the command.
<port>                Enter Port Id
(Netgear Switch Routing) (Config)#logging host 192.168.21.253 4 ?
<cr>                  Press Enter to execute the command.
<severitylevel> Enter Logging Severity Level (emergency|0, alert|1,critical|2, error|3, warning|4, notice|5,
info|6, debug|7).
(Netgear Switch Routing) (Config)#logging host 192.168.21.253 4 1 ?
```

```
<cr>                    Press Enter to execute the command.
(Netgear Switch Routing) (Config)#logging host 192.168.21.253 4 1
(Netgear Switch Routing) #show logging hosts
Index       IP Address              Severity   Port  Status
-----     ---------------     --------      ----   ------
1           192.168.21.253 alert        4             Active
```

第二十二章 IGMP 查询器（IGMP Querier）

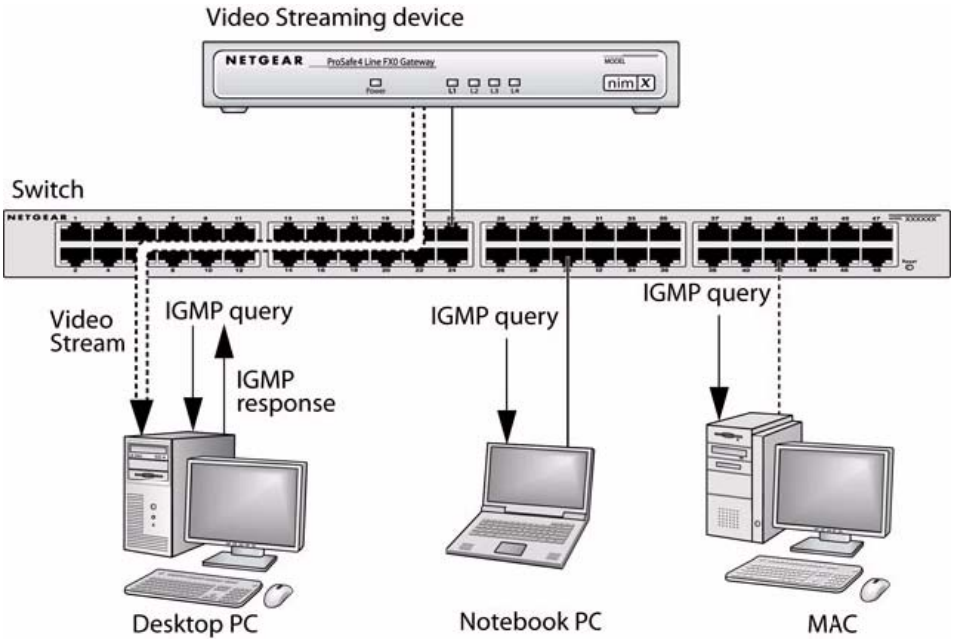
当交换机在使用一些视频服务的网络程序如IPTV、视频流及游戏的时候，视频流量可以分发到所有连接的端口，因为这类流量通常有一个组播以太网地址。IGMP侦听可以启用来创建一个组播群用来定位那些流量到有需要的用户。

然而，IGMP侦听操作通常需要一个额外的网络设备—通常是一个路由器—来发起IGMP成员查询并让有需要的节点做出回应。交换机具备内置IGMP查询器的特性后，就不再需要那样的外部设备了。

由于IGMP查询器是设计来为IGMP侦听工作的，要使用它必须先启用IGMP侦听功能。

这一章的例子说明如何设置交换机来发起IGMP查询

图22-1 显示一个视频流服务的网络程序使用IGMP查询器的特性。



命令行界面示例

示例#1: Enable IGMP Querier

使用以下命令行界面的命令来设置交换机为制定的VLAN发出IGMP查询包。IGMP包浆传送到这个VLAN的所有端口。以下示例在VLAN 1启用了查询器功能。更多IGMP查询器命令选项的详细信息，请参考命令行手册。

```
(Netgear switch) # vlan database
(Netgear switch) (vlan) #ip igmp 1
```

```
(Netgear switch) (vlan) #ip igmpsnooping querier 1
(Netgear switch) (vlan) #exit
(Netgear switch) # config
(Netgear switch) (config) #ip igmpsnooping
(Netgear switch) (config) #exit
(Netgear switch) #
```

示例#2 Show IGMP Querier Status

要查看IGMP查询器的状态，可以使用以下命令。

```
(Netgear switch) #show ip igmpsnooping querier 1

Vlan ID..... 1

Admin Mode..... Active

Query IP Address..... 10.10.10.1

Querier Interval..... 60

Query Packets Sent Count..... 242
```

这个命令显示IGMP的工作模式是激活的，这个模式使用“ip igmpsnooping”命令来控制，如果模式没有激活，就不会发送查询包。