S6550 系列 三层以太网交换机
配置指南
(Rel_08)

浪潮思科网络科技有限公司（以下简称“浪潮思科”）为客户提供全方位的技术支持和服务。直接向浪潮思科购买产品的用户，如果在使用过程中有任何问题，可与浪潮思科各地办事处或用户服务中心联系，也可直接与公司总部联系。

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

公司网址：　　http://www.inspur.com/

技术支持热线：　400-691-1766

技术支持邮箱：　inspur_network@inspur.com

技术文档邮箱：　inspur_network@inspur.com

客户投诉热线：　400-691-1766

公司总部地址：　北京市海淀区西北旺东路 10 号院（中关村软件园）东区 20 号

邮政编码：　　100094

声　　明

前 言

概述

本文档系统介绍了 S6550 系列三层以太网交换机，设备支持的特性及其相关配置。主要内容包括基础配置、以太网、环网保护、IP 业务、IP 路由、可靠性、安全性、QoS 等基本原理和配置过程，并提供相关的配置案例。在本文档的附录中，提供了该文档所涉及的术语和缩略语。

阅读本文档有助于读者系统掌握设备的原理和各种配置信息，以及如何应用该设备进行组网。

产品版本

与本文档相对应的产品版本如下所示。

产品名称	软件版本	硬件版本
S6550 系列 三层以太网交换机	V3.60	B

约定

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
 警告	以本标志开始的文本表示有潜在危险，如果不能避免，可能导致人员伤害。
 注意	以本标志开始的文本表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
 说明	以本标志开始的文本是正文的附加信息，是对正文的强调和补充。

符号	说明
	以本标志开始的文本能帮助您解决某个问题或节省您的时间。

通用格式约定

格式	说明
宋体	正文采用宋体表示。
黑体	一级标题、二级标题、三级标题、Block 采用**黑体**表示。
楷体	警告、提示等内容用楷体表示。
“Lucida Console”格式	“Lucida Console”格式表示屏幕输出信息。此外，屏幕输出信息中夹杂的用户从终端输入的信息采用加粗字体表示。

命令行格式约定

格式	说明
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**粗体**表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从两个或多个选项中选取一个。
[x | y | ...]	表示从两个或多个选项中选取一个或者不选。
{ x | y | ... } *	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | ...] *	表示从两个或多个选项中选取多个或者不选。

修订记录

修订记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

目 录

图目录

表格目录

1 基础配置

本章介绍交换机设备的基础配置信息及配置过程，并提供相关的配置案例。

- 命令行
- 登录设备
- 管理文件
- 加载与升级
- 时间管理
- 接口管理
- 配置设备基本信息
- 任务调度功能
- 看门狗
- 配置 Banner

1.1 命令行

1.1.1 简介

命令行是用户与交换机进行对话的通道。用户可以通过相应的命令行来实现对设备的配置、监控和管理。

用户通过终端设备或运行终端仿真程序的 PC 登录到设备，出现命令行提示符后，即进入命令行接口。

命令行接口有如下特性：

- 允许通过 Console 口进行本地配置。
- 允许通过 Telnet、SSH（Secure Shell，安全外壳协议）进行本地或远程配置。
- 命令行分级保护，不同级别的用户只能执行相应级别的命令。
- 不同类型的命令行分属于不同的命令行模式，用户只有在对应的命令行模式下才能进行某一类型的配置。
- 用户可以使用快捷键来操作命令。

- 用户可以通过调用历史记录来查看或执行某条历史命令，设备支持保存最近输入的 20 条历史命令。
- 用户可以随时键入“?”以获得在线帮助。
- 提供命令行不完全匹配和上下文关联等多种智能解析方法，方便用户输入。

1.1.2 命令行级别

交换机设备对命令行采用分级保护的方式，将命令行从低到高划分为 4 个级别。

- 0～4：参观级，用户可以执行网络诊断工具命令（**ping**）、清除统计信息命令（**clear**）、显示历史记录命令（**history**）等。
- 5～10：监控级，用户可以执行用于系统维护命令（**show**）等。
- 11～14：配置级，用户可以执行用于配置包括 VLAN（Virtual Local Area Network，虚拟局域网）、IP（Internet Protocol，网络互联协议）路由等各类业务的命令。
- 15：管理级，用于系统基本运行的命令。

1.1.3 命令行模式

命令行模式就是执行命令行的界面环境。系统的所有命令都注册在某个（或某些）命令行模式下，只有在相应的模式下才能执行该模式下的命令。

如果此设备是缺省配置，则会显示“Login:”提示符，输入用户名 Inspur 和密码 Inspur 后，进入特权用户模式，在屏幕上显示：

```
Inspur#
```

设备支持超级密码功能，即可以通过 Ctrl+P 按键输入默认密码 switch0501，然后输入 Inspur/Inspur，即可登陆，但是不会创建 Inspur 用户，如果需要创建用户还需要使用 **user name** 命令。

说明

权限低于 11 的用户，进入特权用户模式不需要输入密码。

在特权用户模式下，输入 **config terminal** 命令，则可进入全局配置模式。

```
Inspur#config
Inspur(config)#
```

说明

- 命令行提示符“Inspur”是设备缺省的主机名。用户可以在特权用户模式下通过 **hostname** *string* 命令修改主机名。
- 有些在全局配置模式下实现的命令，在其它模式下也可以实现，但实现的功能与命令行模式密切相关。
- 在某一命令行模式下通过 **quit** 命令或 **exit** 命令均可以回到上一级命令行模式。
- 用户可以通过 **end** 命令从特权用户模式以外的任一命令行模式回退到特权用户模式。

交换机设备支持以下命令行模式。

模式	进入方式	标识说明
特权用户模式	登录设备后“Login:”提示符显示状态下，输入用户名和密码后进入。	Inspur#
全局配置模式	在特权用户模式下，输入 **config terminal** 命令。	Inspur(config)#
物理接口配置模式	在全局配置模式下，使用 **interface** { **gigaethernet | tengigabitethernet** }*unit/slot/interface* 命令。	Inspur(config-gigaethernet1/1/*interface*)# Inspur(config-tengigabitethernet1/1/*interface*)#
物理接口批量配置模式	在全局配置模式下，使用 **interface range** { **gigaethernet | tengigabitethernet** }*unit/slot/interface* 命令。	Inspur(config-range)#
三层物理接口配置模式	在全局配置模式下，使用 **interface** { **gigaethernet | tengigabitethernet** }*unit/slot/interface* 命令。 使用 **no portswitch** 命令将接口配置为三层接口模式	Inspur(config-gigaethernet1/1/*interface*)# Inspur(config-tengigabitethernet1/1/*interface*)#
SNMP 接口配置模式	在全局配置模式下，使用 **interface fastethernet 1/0/1** 命令。	Inspur(config-fastethernet1/0/1)#
LOOPBACK 接口配置模式	在全局配置模式下，输入 **interface loopback** *lb-number* 命令。	Inspur(config-loopback*)#

模式	进入方式	标识说明
隧道接口配置模式	在全局配置模式下，使用 **interface tunnel** *tunnel-id* 命令。	`Inspur(config-tunnel)#`
VLAN 配置模式	在全局配置模式下，输入 **vlan** *vlan-id* 命令。	`Inspur(config-vlan)#`
聚合组配置模式	在全局配置模式下，使用 **interface port-channel** *channel-number* 命令。	`Inspur(config-port-channel*)#`
流分类配置模式	在全局配置模式下，输入 **class-map** *class-map-name* 命令。	`Inspur(config-cmap)#`
流策略配置模式	在全局配置模式下，输入 **policy-map** *policy-map-name* 命令。	`Inspur(config-pmap)#`
绑定流分类的流策略配置模式	在流策略配置模式下，输入 **class-map** *class-map-name* 命令。	`Inspur(config-pmap-c)#`
基本 IP ACL 配置模式	在全局配置模式下，使用 **access-list** *acl-number* 命令，其中 *acl-number* 取值范围是 1000～1999。	`Inspur(config-acl-ip-std)#`
扩展 IP ACL 配置模式	在全局配置模式下，使用 **access-list** *acl-number* 命令，其中 *acl-number* 取值范围是 2000～2999。	`Inspur(config-acl-ip-ext)#`
MAC ACL 配置模式	在全局配置模式下，使用 **access-list** *acl-number* 命令，其中 *acl-number* 取值范围是 3000～3999。	`Inspur(config-acl-mac)#`
User ACL 配置模式	在全局配置模式下，使用 **access-list** *acl-number* 命令，其中 *acl-number* 取值范围是 5000～5999。	`Inspur(config-acl-udf)#`
MST 域配置模式	在全局配置模式下，输入 **spanning-tree region-configuration** 命令。	`Inspur(config-region)#`
Profile 配置模式	在全局配置模式下，输入 **igmp filter profile** *profile-number* 命令。	`Inspur(config-igmp-profile)#`

模式	进入方式	标识说明
cos-remark 配置模式	在全局配置模式下，使用 **mls qos mapping cos-remark** *profile-id* 命令。	`Inspur(cos-remark)#`
cos-to-pri 配置模式	在全局配置模式下，使用 **mls qos mapping cos-to-local-priority** *profile-id* 命令。	`Inspur(cos-to-pri)#`
dscp-mutation 配置模式	在全局配置模式下，使用 **mls qos mapping dscp-mutation** *profile-id* 命令。	`Inspur(dscp-mutation)#`
dscp-to-pri 配置模式	在全局配置模式下，使用 **mls qos mapping dscp-to-local-priority** *profile-id* 命令。	`Inspur(dscp-to-pri)#`
WRED 模板配置模式	在全局配置模式下，使用 **mls qos wred profile** *profile-id* 命令。	`Inspur(wred)#`
流量监管模板配置模式	在全局配置模式下，使用 **mls qos policer-profile** *policer-name* [**single**]命令。	`Inspur(traffic-policer)#`
堆叠接口配置模式	在全局配置模式下，使用 **interface isf-port** *interface-number*	`Inspur(config-isf-port3/1/1)`
中文提示模式	在任意配置模式下，输入 **language chinese** 命令。	`Inspur#`
英文提示模式	在任意配置模式下，输入 **language english** 命令。	`Inspur#`

1.1.4 命令行快捷键

交换机设备支持以下命令行快捷键。

快捷键	说明
上光标键（↑）	如果还有更早的历史命令，则显示上一条输入的命令，若此命令属于历史记录中的最早的一条，则按下此键不会令屏幕发生任何变化。
下光标键（↓）	如果还有更新的历史命令，则显示下一条输入的命令，若此命令属于历史记录中的最新的一条，则按下此键不会令屏幕发生任何变化。
左光标键（←）	光标向左移动一个字符位置，若光标位于命令首，则按下此键不会令屏幕发生任何变化。

快捷键	说明
右光标键（→）	光标向右移动一个字符位置，若光标位于命令尾，则按下此键不会令屏幕发生任何变化。
Backspace	删除光标所在位置的前一个字符。若光标位于命令首，则按下此键不会令屏幕发生任何变化。
Tab	输入完整的关键字后按下 Tab 键，光标自动距词尾空一格，再次按下 Tab 键，会显示出后续可以输入的关键字。 输入不完整的关键字后按下 Tab 键，系统自动执行部分帮助： • 如果与之匹配的关键字唯一，则系统用此完整的关键字替代原输入，且光标距词尾空一格； • 对于不匹配或者匹配的关键字不唯一的情况，首先显示前缀，继续按下 Tab 键则循环翻词，此时光标距词尾不空格，按空格键输入下一个单词； • 如果输入错误关键字，按下 Tab 键后，换行并提示错误信息，已输入的关键字不变。
“Ctrl+A”	将光标移动到行首。
“Ctrl+B”	作用同左光标键（←）。
“Ctrl+C”	中断某些正在运行的操作，如 **ping**、**traceroute** 等。仅在分屏显示功能使能的情况下生效。
“Ctrl+D”或“Delete”	删除光标所在位置的字符。
“Ctrl+E”	将光标移动到行尾。
“Ctrl+F”	作用同右光标键（→）。
“Ctrl+K”	将光标所在位置之后的字符（含光标所在位置）全部删除。
“Ctrl+L”	清除屏幕信息。
“Ctrl+S”	作用同下光标键（↓）。
“Ctrl+W”	作用同上光标键（↑）。
“Ctrl+X”	将光标所在位置之前的字符（不含光标所在位置）全部删除。
“Ctrl+Y”	查看历史命令。
“Ctrl+Z”	从其它模式退到特权用户模式。
“Space”或“y”	当终端列打印的命令行信息超过屏幕时，继续显示下一屏的信息。

快捷键	说明
“Enter”	当终端列打印的命令行信息超过屏幕时，继续显示下一行的信息。

1.1.5 命令行帮助信息

完整帮助

在以下三种情况中，用户可以获取完整帮助：

- 在任一命令行模式下，按下“?”键获取该命令视图下所有的命令行及其简单描述。

```
Inspur#?
```

显示信息如下：

```
clear     Clear screen
enable    Turn on privileged mode command
exit      Exit current mode and down to previous mode
help      Message about help
history   Most recent history command
language  Language of help message
list      List command
quit      Exit current mode and down to previous mode
terminal  Configure terminal
```

- 输入某一命令，后接以空格分隔的“?”，如果该位置为关键字，则列出全部关键字及其简单描述。

```
Inspur(config)#ntp ?
```

显示信息如下：

```
peer             Configure NTP peer
refclock-master  Set local clock as reference clock
server           Configure NTP server
```

- 键入某一命令，后接以空格分隔的“?”，如果该位置为参数，则列出参数的取值范围和参数作用的描述。

```
Inspur(config)#interface vlan ?
```

显示信息如下：

```
  <1-4094>  vlan interface number
```

部分帮助

在以下三种情况中，用户可以获取部分帮助：

- 输入一字符串，其后紧接“?”，设备将列出在当前模式下，以该字符串开头的所有关键字。

```
Inspur(config)#c?
```

显示信息如下：

```
class-map    Set class map
clear        Clear buffer content
command-log  Log the command to the file
console      console
cpu          Configure cpu parameters
cpu-protect  Config cpu protect information
create       Create static VLAN
```

- 键入一命令行，后接一字符串紧接“?”，设备将列出在当前模式下，该命令行中以该字符串开头的所有关键字。

```
Inspur(config)#show li?
```

显示信息如下：

```
link-state-tracking  Fault tracking
link-trace           Link trace
```

- 输入命令行的某个关键字的前几个字母，如果这几个字母可以唯一标示出该关键字，按下<Tab>键，可以显示出完整的关键字；否则，连续按下<Tab>键，将会循环出现不同的关键字，用户可以从中选择所需要的关键字。

错误提示信息说明

当命令行输入错误时，设备会依据错误的类型，打印以下错误提示信息。

错误提示信息	说明
% Incomplete command..	% 未完成命令。
Error input in the position market by '^'.	用‘^’标记的位置输入不合法。
Ambiguous input in the position market by '^'	用‘^’标记的位置输入存在歧义。

说明

出现上述错误提示信息时，请采用命令行帮助信息获取帮助解决。

1.1.6 命令行显示信息

显示特性

命令行接口提供如下显示特性：

- 命令行接口的帮助信息和提示信息提供中、英文两种语言显示。
- 在一次显示信息超过一屏时，提供暂停功能，在暂停显示时用户可以有以下选择，如表 1-1 所示。

表1-1 命令行信息显示特性功能键说明

功能键	说明
键入“Space”或“y”	继续显示下一屏信息。
键入“Enter”	继续显示下一行信息。
键入任意字母键（除“y”外）	停止显示和命令执行。

显示信息过滤

交换机设备支持一系列以“**show**”作为开头的命令行，用于查看设备的配置信息、运行状态或诊断信息。通常情况下此类命令行的输出信息比较多，为了帮助用户提取需要查看的信息，过滤掉不需要的内容，可以在命令行中添加信息的过滤规则。

交换机设备的 **show** 命令支持三种过滤方式：

- | **begin** *string*：查看从匹配指定字符串开始的所有行，是否区分大小写是可选择的。
- | **exclude** *string*：查看与指定字符串不匹配的所有行，是否区分大小写是可选择的。
- | **include** *string*：查看只与指定字符串匹配的所有行，是否区分大小写是可选择的。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**show** *command-string* | { **begin** | **include** | **exclude** } *expression* [**igncase**]	查看设备的配置信息、运行状态或诊断信息时用户可进行是否对大小写进行区分的选择。

显示信息分页

显示信息分页功能，是指在一次显示信息超过一屏时，提供暂停功能，可利用表 1-1 中的显示特性功能键控制信息显示。如果禁止显示信息分页功能，当显示信息超过一屏时，将不提供暂停功能，一次滚动显示全部信息。

缺省情况下，系统显示信息分页功能使能。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**terminal page-break enable**	使能显示信息分页功能。

1.1.7 命令行历史信息

命令行接口能够自动保存用户键入的历史命令，用户可以随时采用上光标键（↑）或下光标键（↓）调用命令行保存的历史命令，重复执行。

缺省情况下，系统在缓存中保存最近的 20 条历史命令。用户可以设置系统保存的历史命令条数。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**terminal history** *number*	（可选）配置系统保存的历史命令条数。
2	Inspur#**terminal time-out** *period*	（可选）配置控制台终端超时退出时间。
3	Inspur#**history**	查看用户键入的历史命令。
4	Inspur#**show terminal**	查看终端用户配置信息。

1.1.8 恢复命令行缺省值

恢复命令行的缺省值，通常使用 **no** 选项或 **enable | disable** 选项。

- **no** 选项，在命令行前部提供，用来恢复缺省值、禁止某个功能、删除某项设置等，执行与命令本身相反的操作。带 **no** 选项的命令也叫反向命令。
- **enable | disable** 选项，在命令行后部或中部提供，**enable** 是使能某个特性或功能，**disable** 是禁止某个特性或功能。

举例如下：

- 在物理层接口模式下执行 **description** *text* 命令是修改接口描述信息，执行 **no description** 命令是删除接口描述信息，恢复缺省值。
- 在物理层接口模式下执行 **shutdown** 命令是关闭某接口，执行 **no shutdown** 命令是使能某接口。
- 在特权用户模式下执行 terminal page-break enable 命令使能终端分页显示信息功能，执行 terminal page-break disable 命令禁止终端分页显示信息功能。

说明

配置命令大多都有缺省值，通常使用 **no** 选项恢复配置命令的缺省值。

1.1.9 命令行记录

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**command-log enable** Inspur(config)#**exit**	使能命令行记录功能。

1.2 登录设备

1.2.1 简介

登录交换机设备进行配置和管理，可以采用 CLI（Command-Line Interface，命令行界面）方式，也可以采用 NView NNM 网管方式。

交换机命令行方式下有多种配置方式：

- Console 方式：第一次配置时必须采用 Console 方式，设备支持 RJ45 类型的 Console 口。
- Telnet 方式：需要先通过 Console 方式登录，在交换机上配置 VLAN 接口 IP 地址，以及设置用户名和密码，然后才可以进行远程 Telnet 配置。
- SSH 方式：在通过 SSH 登录设备之前，需要先通过 Console 接口登录设备并启动 SSH 服务。

当需要在 NView NNM 网管方式下配置时，也必须先通过命令行方式，配置 VLAN 接口 IP 地址，然后才可以通过 NView NNM 网管平台对设备进行配置。

1.2.2 通过 Console 口登录设备

Console 口简介

Console 口是网络设备用来与运行终端仿真程序的 PC 进行连接的常用接口，用户可以借助此接口对本地设备进行配置和管理。这种管理方式不需借助网络进行通信，所以被称为带外（out-of-band）管理方式，在网络运行异常的情况下，用户也可以通过 Console 口对设备进行配置和管理。

在以下两种情况中，只能通过 Console 口登录设备进行配置：

- 设备第一次加电启动
- 无法通过 Telnet 方式登录设备

通过 RJ45 Console 口登录

当用户希望通过 PC 连接 RJ45 Console 口登录设备时，首先需要通过配置线缆将设备的 Console 口和 PC 的 RS-232 串口相连，如图 1-1 所示，然后在 PC 上运行终端仿真程序，如微软公司的 Windows XP 操作系统自带的“超级终端”程序，将通信参数如图 1-2 配置，完成后即可登录设备。

图1-1 通过 PC 连接 RJ45 Console 口登录设备的组网示意图

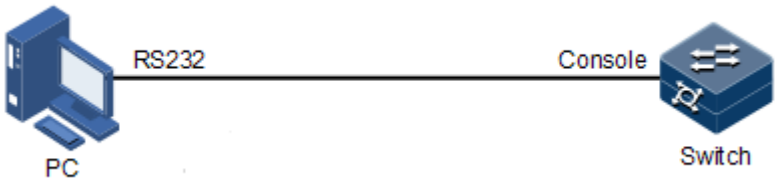


图1-2 “超级终端”中的通信参数配置示意图

说明

初始情况下，串口波特率为 115200。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config** Inspur(config)#**console baud-rate { 115200 | 19200 | 38400 | 9600 }**	修改串口登录波特率。

1.2.3 通过 Telnet 登录设备

说明

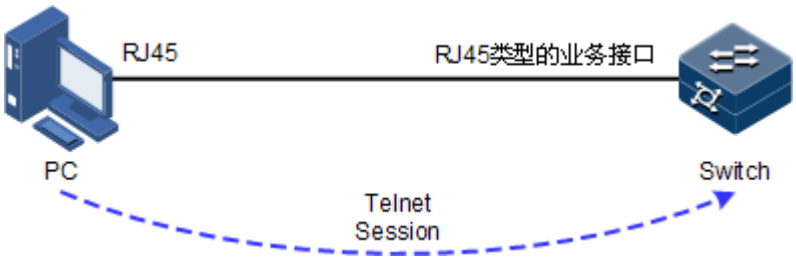
初始情况下，设备带外管理口（SNMP 口：**fastethernet 1/0/1**）缺省管理 IP 地址为 192.168.0.1，子网掩码为 255.255.255.0。如需修改设备 IP 地址，用户可以通过 Console 口登录设备，并对设备进行配置。设备的缺省用户名为 admin，密码为 inspur123。Telnet 连接状态下输错 3 次密码自动断开连接。

Telnet 提供了一种通过 PC 远程登录设备的方式。用户可以先通过 PC 登录到一台网络设备，然后再通过 Telnet 方式远程登录到联网的其他网络设备，而不需要为每一台网络设备都连接一台 PC。

交换机设备提供的 Telnet 服务包括：

- Telnet Server：用户在 PC 上运行 Telnet 客户端程序登录到设备，对设备进行配置管理。如图 1-3 所示，交换机此时提供的是 Telnet Server 服务。

图1-3 交换机作为 Telnet Server 设备的组网示意图



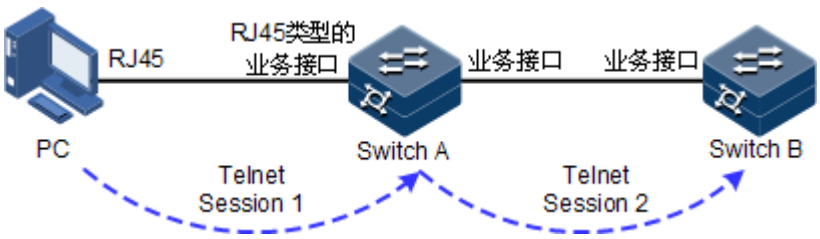
在通过 Telnet 登录设备之前，用户需要通过 Console 接口登录设备并启动 Telnet 服务，请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#interface fastethernet 1/0/1`	进入带外网管接口配置模式。
3	`Inspur(config-fastethernet1/0/1)#ip address` *ip-address* [*ip-mask*]	配置设备带外网管接口的 IP 地址。缺省为 192.168.0.1/24，缺省登录用户名密码均为 Inspur
4	`Inspur(config-fastethernet1/0/1)#shutdown`	（可选）关闭设备带外管理接口。
5	`Inspur(config)#telnet-server accept` *interface-type interface-list*	（可选）配置设备支持 Telnet 功能的接口。
6	`Inspur(config)#telnet-server close terminal-telnet` *session-number*	（可选）断开指定的 Telnet 连接。

步骤	配置	说明
7	Inspur(config)#**telnet-server max-session** *session-number*	（可选）配置设备支持的最大 Telnet 连接数。缺省情况下，最大连接数为 10。
8	Inspur(config)#**telnet-server access-list** { *ip-access-list-number* | *ipv6-access-list-number* }	（可选）配置 Telnet 的访问控制列表号。
9	Inspur(config)#**telnet-server disable**	(可选)关闭 Telnet server 功能，对应端口号同时也会关闭。
10	Inspur(config)#**telnet-server port** *port-id*	（可选）配置设备的 TELNET 侦听端口号。

- Telnet Client：用户在 PC 上通过终端仿真程序或 Telnet 客户端程序建立与设备的连接后，再通过 telnet 命令登录到其它设备，对其进行配置管理。如图 1-4 所示，Switch A 此时既作为 Telnet Server，也同时提供 Telnet Client 服务。

图1-4 交换机设备作为 Telnet Client 设备的组网示意图



请在作为 Telnet Client 的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**telnet** { *ipv4-address* | *ipv6-address* } [**port** *port-id*] Inspur#**telnet** *ipv4-address* [**port** *port-id*] [**sourceip** *source-ip-address*]	以 Telnet 方式登录其他设备。

1.2.4 通过 SSH 登录设备

Telnet 缺少安全的认证方式，而且传输过程采用 TCP（Transmission Control Protocol，传输控制协议）进行明文传输，存在很大的安全隐患。单纯提供 Telnet 服务容易招致 DoS（Deny of Service，拒绝服务）、主机 IP 地址欺骗、路由欺骗等恶意攻击。

传统的 Telnet 和 FTP（File Transfer Protocol，文件传输协议）通过明文传送密码和数据的方式，已经慢慢不被用户所接受。SSH 是一个网络安全协议，通过对网络数据的加密，可以有效防止远程管理过程中的信息泄露问题，在网络环境中为远程登录和其他网络服务提供了更高的安全性。

SSH 通过 TCP 进行数据交互，它在 TCP 之上构建了一个安全的通道。另外，SSH 服务除了支持标准端口 22 以外，还支持其他服务端口，以防止设备受到来自网络的非法攻击。

在通过 SSH 登录设备之前，用户需要通过 Console 接口登录设备并启动 SSH 服务。

设备上 SSH 登录设备的缺省配置如下。

功能	缺省值
SSH 服务器功能状态	禁止
本地 SSH 密钥对长度	512bit
密钥重协商周期	0h
SSH 采用的认证方式	password
SSH 认证超时时间	600s
SSH 认证允许失败次数	20
SSH 侦听端口号	22
SSH 会话功能状态	禁用
SSH 协议版本	v2

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**generate ssh-key** *length*	生成本地 SSHv2 密钥对并指定其长度。缺省情况下，设备的本地 SSHv2 密钥对长度为 512bit。
3	Inspur(config)#**ssh2 server**	启动 SSHv2 服务器。缺省情况下，设备没有启动 SSHv2 服务器。 启动 SSHv2 服务器后可以通过 **no ssh2 server** 关闭 SSHv2 服务器。
4	Inspur(config)#**ssh2 server authentication** { **password** | **rsa-key** }	（可选）配置设备的 SSHv2 认证方式。缺省情况下，设备采用 password 认证方式。
5	Inspur(config)#**ssh2 server authentication** *public-key-name* **public-key** [*public-key*]	（可选）采用 rsa-key 认证方式时，将客户端的公钥录入设备。
6	Inspur(config)#**ssh2 server authentication-timeout** *period*	（可选）配置设备的 SSHv2 认证超时时间。当客户端认证时间超过此上限时，设备将拒绝其继续认证并断开连接。缺省情况下，设备的 SSHv2 认证超时时间是 600 秒。

步骤	配置	说明
7	Inspur(config)#**ssh2 server authentication-retries** *times*	（可选）配置设备的 SSHv2 认证允许失败次数。当客户端认证失败的次数超过此上限时，设备将拒绝其继续认证并断开连接。缺省情况下，设备的 SSHv2 认证允许失败次数是 20 次。
8	Inspur(config)#**ssh2 server port** *port-number*	（可选）配置设备的 SSHv2 侦听端口号。缺省情况下，设备的 SSHv2 侦听端口号是 22。 **说明** 配置设备的 SSHv2 侦听端口号时，输入的参数并不能立刻生效，而是要等 SSHv2 服务重新启动之后才会生效。
9	Inspur(config)#**ssh2 server max-session** *session-number*	（可选）配置设备支持的最大 SSH2 会话数。
10	Inspur(config)#**ssh2 access-list** { *ip-access-list-number* | *ipv6-access-list-number* }	（可选）配置 SSH 的访问控制列表号。
11	Inspur(config)#**ssh2 server rekey-interval** *value*	（可选）配置 SSH 的重协商时间。
12	Inspur(config)#**ssh2 server close session** *session-number*	（可选）关闭指定的 SSH2 会话。

1.2.5 管理登录用户

第一次启动交换机设备时，用户只要将 PC 通过 Console 接口与设备连接，在超级终端中输入初始的用户名和密码，即可以登录设备并对其进行配置。

说明

初始情况下，设备的用户名为 admin 和密码为 inspur123。

如果为设备的业务接口配置了 IP 地址，在没有任何权限控制的情况下，任意远端用户都可以通过 Telnet 方式登录设备，或者通过与设备建立 PPP（Point to Point Protocol，点对点协议）连接来访问网络，这显然对设备和网络都是不安全的。为此需要为设备创建用户并设置密码和权限，对登录用户进行管理。

设备上用户管理的缺省配置如下。

功能	缺省值
本地用户信息	• 用户名：admin • 密码：inspur123 • 用户权限：15

功能	缺省值
新建用户权限	15
新建用户激活状态	**active**
新建用户服务类型	无
Enable 密码	无
用户登录认证方式	**local-user**
Enable 登录认证方式	**local-user**

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**user name** *user-name* **password** [**cipher** | **simple**] *password* [**confirm**] Inspur#**no username** *user-name*	（可选）创建或修改登录用户的用户名和密码。 使用 no 格式删除用户。
2	Inspur#**user name** *user-name* **privilege** *privilege-level*	（可选）配置登录用户的权限。
3	Inspur#**user name** *user-name* **state** { **active** | **inactive** }	（可选）配置登录用户的状态。
4	Inspur#**user** *user-name* { **allow-exec** | **disallow-exec** } *first-keyword* [*second-keyword*] [**confirm**]	（可选）配置登录用户执行命令行的优先级规则。
5	Inspur#**user** *user-name* **service-type** { **lan-access** | **ssh** | **telnet** | **web** | **console** | **all** }	（可选）配置用户支持的服务类型。
6	Inspur#**user login** { **console** | **telnet** | **ssh** | **web** } { **local-radius** | **local-user** | **radius-local** [**server-no-response**] | **radius-user** | **local-tacacs** | **tacacs-local** [**server-no-response**] | **tacacs-user** }	（可选）配置不同方式用户登录的认证方式。
7	Inspur#**enable password** [**cipher** *password*]	（可选）修改进入特权用户模式的密码。权限低于 11 的用户，进入特权用户模式不需要密码。
8	Inspur#**password check** { **complex** | **none** | **simple** }	（可选）配置密码的的检验强度。
9	Inspur#**logout**	退出当前登录状态。
10	Inspur#**enable** [*privilege*]	（可选）配置用户权限。
11	Inspur#**line password** *password*	（可选）配置串口线性密码。
12	Inspur#**line encrypt-password** *password*	（可选）配置串口线性密文密码。

- 除缺省用户 Inspur 外，设备最多可再创建 9 个本地用户。
- 用户的登录密码长度与密码检查方式相关：complex 方式下密码需要不小于 8 个字节，不大于 16 个字节，还需要保证密码必须包含大写、小写和数字三种类型的字符；simple 方式下密码需要不小于 8 个字节，不大于 16 个字节；none 模式下密码需要不小于 1 个字节，不大于 16 个字节。
- 对于权限低于 15 级的本地用户，除非允许执行修改登录密码的命令，否则不允许修改登录密码。

1.2.6 配置 HTTP Server 功能

使能 HTTP Server 功能，用户可以通过登录 Web 界面对设备进行配置。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ip http server { enable | disable }**	使能 HTTP Server 功能，使用 disable 格式禁用此功能。

1.2.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show user table [detail]**	查看设备的用户信息。
2	Inspur#**show user active**	查看登录到设备的用户信息。
3	Inspur#**show telnet-server**	查看 Telnet Server 的配置情况。
4	Inspur#**show ssh2 public-key [authentication | rsa]**	查看设备和客户端上用于进行 SSH 认证的公钥。
5	Inspur#**show ssh2 { server | session }**	查看 SSHv2 服务器或会话端的信息。
6	Inspur#**show privilege**	查看设备优先级信息。

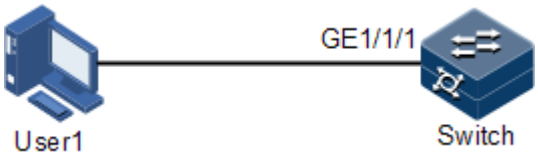
1.2.8 配置用户管理示例

组网需求

如图 1-5 所示，为了防止登录用户对 Switch 设备进行非法操作，给设备带来不安全隐患，需要对登录设备的用户进行有效管理。具体要求如下：

- 配置用户登录方式为 local-user。
- 创建本地用户 user1，明文密码为 aaAA123@。
- 配置用户 user1 的权限为 10 级。
- 配置用户 user1 的服务类型为 Telnet。

图1-5 用户管理组网示意图



配置步骤

步骤 1 配置用户登录认证方式。

```
Inspur#user login local-user
```

步骤 2 创建本地用户 user1。

```
Inspur#user name user1 password simple aaAA123@
```

步骤 3 配置用户权限。

```
Inspur#user name user1 privilege 10
```

步骤 4 配置用户服务类型。

```
Inspur#user user1 service-type telnet
```

检查结果

通过 **show user table detail** 命令查看本地用户的配置信息。

```
Inspur#show user table detail
Default Login:local-user

Username:Inspur
Priority:15
Server:Local
Login   :console
Status  :online
Service type:console telnet ssh web lan-access
User State  :active
```

```
Username:user1
Priority:10
Server:Local
Login   :--
Status  :offline
Service type:console telnet ssh web lan-access
User State  :active
```

使用新创建的用户名 user1、密码 aaAA123@登录设备，检查用户权限配置是否正确。

```
Login:user1
Password:
Inspur#config
Inspur(config)#arp 192.168.0.2 000E.5E12.3456
Set successfully.
```

如需删除默认的 Inspur 账号，可使用如下命令：

```
Inspur#no username Inspur
```

1.2.9 配置 Telnet 登录示例

组网需求

如图 1-6 所示，用户希望通过 PC 远程登录到交换机设备，并对设备进行远程配置和管理。为保证网络安全，配置 GE 1/1/1 接口可以通过 Telnet 登录设备，同一时间最多允许 3 个用户远程登录设备。

图1-6 通过 Telnet 方式远程登录设备组网示意图

配置步骤

步骤 1 使能 Telnet 功能。

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

步骤 2 配置 GE 1/1/1 接口支持 Telnet 功能，最多允许 3 个用户同时远程登录设备。

```
Inspur(config)#telnet-server accept gigaethernet 1/1/1
Inspur(config)#telnet-server max-session 3
```

检查结果

查看 Telnet 服务器配置信息。

```
Inspur#show telnet-server
Telnet server state         : enable
Listen port on (default 23)  : 23
Max session: 3
Accept port-list: gigaethernet1/1/1
Using session-list: --
Access list ipv4: --
Access list ipv6: --
```

用户可以通过终端仿真程序登录设备，并远程配置和管理设备。

1.2.10 配置 SSH 登录示例

组网需求

如图 1-7 所示，当 PC 通过一个不能保证安全的网络远程登录到交换机设备时，为了更大限度的保证数据信息交换的安全性，需要在交换机设备上配置 SSH 服务器功能，并采用 RSA 认证。具体要求如下：

- 配置 SSH 认证超时时间为 400s，允许认证失败次数为 3 次
- 配置 SSH 认证公钥名称为 Inspur，SSH 认证方式为 rsa-key
- 用来进行 SSH 登录的用户使用缺省用户名 Inspur

图1-7 SSH 登录设备组网示意图

配置步骤

步骤 1 配置设备的 IP 地址，使设备和 PC 之间路由可达。

```
Inspur#config
Inspur(config)#interface vlan 1
Inspur(config-vlan1)#ip address 172.16.70.134
```

步骤 2 生成本地 SSH 密钥对，并使能 SSH 服务器功能。

```
Inspur#config
Inspur(config)#generate ssh-key
Inspur(config)#ssh2 server
```

步骤 3 配置 SSH 认证超时时间为 400s，允许认证失败次数为 3 次。

```
Inspur(config)#ssh2 server authentication-timeout 400
Inspur(config)#ssh2 server authentication-retries 3
```

步骤 4 生成用于登录认证的密钥对，包括主机私钥和主机公钥，将主机私钥保存在 SSH 客户端，该步骤需要终端仿真软件进行，例如 SecureCRT。

步骤 5 将客户端的主机公钥录入设备。将步骤 4 生成的公钥拷贝到终端仿真程序进行粘贴，并按下“Ctrl+S”保存公钥。

```
Inspur(config)#ssh2 server authentication Inspur public-key
(Ctrl+s) for save input and return
(Ctrl+z) for discard input and return.
------------------------------------------------------------.
AAAAB3NzaC1yc2EAAAADAQABAAAAgQCwMf+rJOF3cccsbU9NnVSVKqlvvFDOJqYX
kwvMIzCmz1qKhhbguUxHTPnuuOyLbA9Yz+AFeaCdWxxdKvNCFXBJvu2pHjTZcJxm
cThqD3kvvRKnR3BjV9HioBjGHPO1gni2Bqc1z91/RoZ6oaNoQfN885SgwigbGt6K
eei/I8pJgQ==
```

步骤 6 配置设备的 SSH 认证方式为 rsa-key。

```
Inspur(config)#ssh2 server authentication rsa-key
```

步骤 7 建立 SSH 连接，使用 SSH 方式登录设备。

检查结果

- 查看 SSH 服务器配置信息。

```
Inspur#show ssh2 server
SSH server information:
-----------------------
State:    Enable
Version:  sshv2
Authentication method(default:local user-password ):  rsa-key
Authentication timeout(default 600):                  400s
Authentication retries(default 20):                   3
Rekey interval time(default 0):                       0h
Max client count(default 10):                         10
Current client count:                                 0
Current channel count:                                0
Listen port on (default 22):                          22
```

- 查看 SSH 认证公钥。

```
Inspur#show ssh2 public-key
RSA public key :
---- BEGIN SSH PUBLIC KEY ----
Comment: "rsa-key"
AAAAB3NzaC1yc2EAAAADAQABAAAAQwDGOmZvhPtWd5zo6naC6Vrz4cK4QEoj
O1+WlD94RmPyF/atwjzHOjQOB63J3tg/vcazH2nNVG3jwu912u1cuYTsZWE=
Fingerprint: md5 b6:1b:e8:88:73:1b:11:a9:af:9f:7b:e6:08:b8:b8:9c
---- END SSH PUBLIC KEY ----


Authentication public key :
---- BEGIN SSH PUBLIC KEY ----
Comment: "rsa-key"

Public-key name: Inspur
Public-key:
AAAAB3NzaC1yc2EAAAADAQABAAAAgQCwMf+rJOF3cccsbU9NnVSVKqlvvFDO
```

```
JqYXkwvMIzCmz1qKhhbguUxHTPnuuOyLbA9Yz+AFeaCdWxxdKvNCFXBJvu2p
HjTZcJxmcThqD3kvvRKnR3BjV9HioBjGHPO1gni2Bqc1z91/RoZ6oaNoQfN8
85SgwigbGt6Keei/I8pJgQ==

---- END SSH PUBLIC KEY ----
```

- 查看 SSH 会话信息。可以看出已经建立会话 1 的 SSH 连接。

```
Inspur#show ssh2 session
ID  Ver  Cipher(IN/OUT)      Auth-Type        Con-Time    State
UserId           Ip
-------------------------------------------------------------------------
--------------------------
 1  2.0  aes/aes            rsa             0h:0m:23s   OK(1channels)
Inspur         172.16.70.110
 2  --   --/--              --              --         Closed         --
--
 3  --   --/--              --              --         Closed         --
--
 4  --   --/--              --              --         Closed         --
--
 5  --   --/--              --              --         Closed         --
--
 6  --   --/--              --              --         Closed         --
--
 7  --   --/--              --              --         Closed         --
--
 8  --   --/--              --              --         Closed         --
--
 9  --   --/--              --              --         Closed         --
--
 10 --   --/--              --              --         Closed         --
--
```

1.3 管理文件

1.3.1 管理 BootROM 文件

设备在通电之后，首先运行 BootROM 文件，当出现“Press Ctrl+b or Ctrl+B to enter boot menu:”时，键入“Ctrl+B”，即可进入 Bootrom 命令模式。

在 Boot 模式下，用户可进行如下操作。

操作	说明
t	升级系统软件到设备中。
m	升级 Boot 软件到设备中。
b	从设备读取系统软件，并加载。
s	选择设备启动时加载的系统软件的顺序。

操作	说明
e	清除环境变量。
r	重新启动设备。
p	设置 BootROM 密码。
k	配置 Console 接口速率

请在设备上进行以下配置。

以下配置步骤均为可选，各步骤之间没有先后顺序。

步骤	配置	说明
1	Inspur#**upload bootstrap** { **ftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* | **tftp** { *ipv4-address* | *ipv6-address* } *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* } [*dir*]	（可选）通过 FTP 方式、SFTP 方式或 TFTP 方式上传 BootROM 文件到本地。
2	Inspur#**download bootstrap** { **ftp** { *ipv4-address* | *ipv6-address* } *user-name password* [**unit** *unit-id*] *file-name* | **tftp** { *ipv4-address* | *ipv6-address* } [**unit** *unit-id*] *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password* [**unit** *unit-id*] *file-name* } [*dir*]	（可选）通过 FTP 方式、SFTP 方式或 TFTP 方式下载 BootROM 文件。
3	Inspur#**erase** [*file-name*]	（可选）删除存储器中的文件。
4	Inspur#**bootrom password** *word*	（可选）配置 Bootrom 密码。

1.3.2 管理系统文件

系统文件是指设备运行过程中所需要的文件（如系统启动软件、配置文件等），此类文件一般被保存在设备的存储器中，为了方便用户对存储器进行有效的管理，设备以文件系统的方式对这些文件进行管理。文件系统功能主要包括对文件和目录的创建、删除、修改等。

此外，设备支持双系统，即在设备的存储器中可同时存储两个版本的系统软件，两个系统软件相对独立。当用户升级失败导致设备无法使用时，可使用另一个系统软件启动设备。

请在设备上进行以下配置。

以下配置步骤均为可选，各步骤之间没有先后顺序。

步骤	配置	说明
1	Inspur#**download system-boot** { **ftp** { *ipv4-address* | *ipv6-address* } *user-name password* [**unit** *unit-id*] *file-name* | **tftp** { *ipv4-address* | *ipv6-address* } [**unit** *unit-id*] *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password* [**unit** *unit-id*] *file-name* } [**system1.z** | **system2.z**]	（可选）通过 FTP 方式、SFTP 方式或 TFTP 方式下载系统启动软件。
2	Inspur#**erase** [*file-name*]	（可选）删除存储器中的文件。
3	Inspur#**upload system-boot** { **ftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* | **tftp** { *ipv4-address* | *ipv6-address* } *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* } [**system1.z** | **system2.z**]	（可选）通过 FTP 方式、SFTP 方式或 TFTP 方式上传系统启动软件。

1.3.3 管理配置文件

配置文件在系统启动后被加载，不同的配置文件用于不同的应用场景，以实现不同的业务功能。系统启动后，可以对设备进行配置，保存配置文件，下次启动设备时新配置生效。

配置文件为一个以“.conf”为后缀名的文件，在微软公司的 Windows 系列操作系统中可以通过记事本功能打开，其内容格式如下：

- 以模式＋命令行的格式保存。
- 为了节省空间，只保留非缺省参数（各配置参数的缺省值请详见命令参考）。
- 命令行的组织以其模式为基本框架，同一模式的命令行组织在一起，形成一节，节与节之间通常用“!”隔开。

设备在通电之后，从存储器中读取配置文件进行设备的初始化工作，因此该配置文件中的配置称为初始配置。如果存储器中没有配置文件，则设备将采用缺省参数进行初始化。

与初始配置相对应，设备在运行过程中正在生效的配置称为当前配置。

用户通过命令行可以修改设备的当前配置。为了使当前配置能够作为设备下次通电时的起始配置，需要用 **write** 命令保存当前配置到存储器中，形成配置文件。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**download startup-config** { **ftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* | **tftp** { *ipv4-address* | *ipv6-address* } *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* } } [*dir*]	（可选）通过 FTP 方式、SFTP 方式或 TFTP 方式下载系统启动主配置文件。

步骤	配置	说明
2	Inspur#**download backup-config** { **ftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* | **tftp** { *ipv4-address* | *ipv6-address* } *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* } [*dir*]	（可选）通过 FTP 方式、SFTP 方式或 TFTP 方式下载系统启动备份配置文件。
3	Inspur#**download dhcplease** { **ftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* | **tftp** { *ipv4-address* | *ipv6-address* } *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* } [*dir*]	（可选）通过 FTP 方式、SFTP 方式或 TFTP 方式下载 DHCP 租约文件。
4	Inspur#**download dhcpsnooping-binding** { **ftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* | **tftp** { *ipv4-address* | *ipv6-address* } *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* } [*dir*]	（可选）通过 FTP 方式、SFTP 方式或 TFTP 方式下载 DHCP Snooping 绑定表文件。
5	Inspur#**download poe tftp** { *ipv4-address* | *ipv6-address* } *file-name* [*dir*]	（可选）通过 TFTP 方式下载 POE Firmware 文件。
6	Inspur#**erase** [*file-name*]	（可选）删除存储器中的文件。
7	Inspur#**upload startup-config** { **ftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* | **tftp** { *ipv4-address* | *ipv6-address* } *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* } } [*dir*]	（可选）通过 FTP 方式、SFTP 方式或 TFTP 方式上传系统启动主配置文件。
8	Inspur#**upload backup-config** { **ftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* | **tftp** { *ipv4-address* | *ipv6-address* } *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* } [*dir*]	（可选）通过 FTP 方式、SFTP 方式或 TFTP 方式上传系统启动备份配置文件。
9	Inspur#**upload command-log** { **ftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* | **tftp** { *ipv4-address* | *ipv6-address* } *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* } [*dir*]	（可选）通过 FTP 方式、SFTP 方式或 TFTP 方式上传命令行记录信息文件。
10	Inspur#**upload logging-file** { **ftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* | **tftp** { *ipv4-address* | *ipv6-address* } *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* } [*dir*]	（可选）通过 FTP 方式、SFTP 方式或 TFTP 方式上传系统日志文件。

步骤	配置	说明
11	Inspur#**upload running-config** { **ftp** { *ipv4-address* |*ipv6-address* } *user-name password file-name* | **tftp** { *ipv4-address* |*ipv6-address* } *file-name* | **sftp** { *ipv4-address* |*ipv6-address* } *user-name password file-name* } [*dir*]	（可选）通过 FTP 方式、SFTP 方式或 TFTP 方式上传运行系统配置信息的文件。
12	Inspur#**upload license** { **ftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* | **tftp** { *ipv4-address* | *ipv6-address* } *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* } [*dir*]	（可选）通过 FTP 方式、SFTP 方式或 TFTP 方式上传 License 文件。
13	Inspur#**upload dhcpLease** { **ftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* | **tftp** { *ipv4-address* | *ipv6-address* } *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* } [*dir*]	（可选）通过 FTP 方式、SFTP 方式或 TFTP 方式上传 DHCP 租约文件。
14	Inspur#**upload dhcpsnooping-binding** { **ftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* | **tftp** { *ipv4-address* | *ipv6-address* } *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* } [*dir*]	（可选）通过 FTP 方式、SFTP 方式或 TFTP 方式上传 DHCP Snooping 绑定表文件。
15	Inspur#**write**	（可选）将配置好的文件写入存储器。

1.3.4 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show startup-config**	查看设备启动时加载的配置信息。
2	Inspur#**show running-config**	查看设备的当前配置信息。
3	Inspur#**show backup-config**	查看系统启动时的备用配置信息。

1.3.5 维护

用户可以通过以下命令维护文件管理特性。

命令	说明
Inspur#**write [backup-config]**	将运行配置文件写入 Flash，保存为启动配置文件，使当前配置在下次启动时仍然有效。 **注意** 将运行配置文件保存到 Flash 中时，设备会自动覆盖原启动配置文件。因此，需要先对 Flash 中的启动配置文件进行备份。
Inspur#**dir**	查看 Flash 中的系统文件名称，支持查看 Flash 剩余容量。
Inspur#**erase [** *file-name* | **backup-config]**	删除指定系统文件。不选择 *file-name* 参数时默认删除启动配置文件。 **注意** 执行删除命令后，删除的文件将不能恢复，请谨慎使用。
Inspur(config)#**syslog save**	保存日志文件
Inspur#**startup-config write**	保存配置信息。

1.4 加载与升级

1.4.1 简介

加载

传统的配置文件加载方式为串口加载，该方式加载速度慢、耗时长、不具备远程加载功能，导致操作很不方便。为了解决这些问题，引入了 FTP 加载方式、TFTP 加载方式等。

设备支持 TFTP 自动加载方式。

TFTP 自动加载方式是指用户通过 TFTP 协议获取存储在服务器中的配置文件到设备，对设备进行配置的一种方式。自动配置加载功能允许 TFTP 服务器上的配置文件中包含自动配置加载功能的相关命令，以形成多次配置加载，从而满足复杂网络环境下自动配置加载的需求。

设备提供多种方法用于确定设备在 TFTP 服务器上的配置文件名称，比如手动输入、使用 DHCP 客户端获取、使用默认的配置文件名。除此之外，用户还可以指定某种配置文件命名规则，根据规则使用设备自身的属性（例如设备型号、MAC 地址、软件版本号）确定与指定设备对应的配置文件名称。

升级

当需要为设备增加新特性、优化原有功能或解决当前软件版本的 BUG 时，可以对设备进行升级。

设备支持以下升级方式：

- BootROM 升级方式
- 命令行升级方式

说明

建议用户在专业的技术人员指导下进行 BootROM 升级方式。

1.4.2 通过 BootROM 升级方式升级系统软件

当出现以下情况时，需要通过 BootROM 升级方式升级系统软件。

- 系统文件损坏
- 板卡不能正常启动

在通过 BootROM 升级方式升级系统软件前，需要首先搭建 TFTP 境，PC 作为 TFTP 服务器，交换机设备作为客户端，基本要求如下：

- 配置 TFTP 服务器端，确保服务器处于可用状态。
- 配置 TFTP 服务器的 IP 地址，使之与设备的 IP 地址处于同一网段。
- 将 TFTP 服务器网口和交换机 SNMP 的接口用网线连接，SNMP 接口默认 IP 地址为 192.168.0.1。

通过 BootROM 升级方式升级系统软件的步骤如下：

步骤	操作
1	以具有管理员权限的用户身份通过串口登录设备并进入特权用户模式，通过 **reboot** 命令重新启动设备。 `Inspur#reboot`

步骤	操作
2	当出现“Press Ctrl+b or Ctrl+B to enter boot menu: 0”时，键入“Ctrl+B”，即可进入 Bootrom 命令模式。并显示命令列表。 BOOT ********** t: Update system from tftp. m: Update boot from tftp. b: Boot system from flash. e: Erase bootline para. s: Select system image to boot. p: Password setting. r: Reboot. k: Console baudrate Config. ********** [Boot]:
3	输入“t”，升级系统软件到设备中。 [Boot]:**t** ipaddr: 192.168.0.1 serverip: 192.168.0.2 filename: S6550_B_SYSTEM_3.60.124_20190315 press y to confirm: y Current system partiton info: Partition number Name Size ---------- 1 SYSTEM_3.60.262 22798289 2 SYSTEM_3.50.208 21969706 Please input system partition number for upgrading(1-2): 1 Loading...
4	输入“r”，快速执行引导文件，设备将重新启动，并加载刚刚下载的系统启动文件。

1.4.3 通过命令行升级方式升级系统软件

在通过命令行升级方式升级系统软件前，需要首先搭建 FTP/TFTP 环境，PC 作为 FTP/TFTP 服务器，交换机设备作为客户端，基本要求如下：

- 将 TFTP 服务器网口和交换机 SNMP 的接口用网线连接，SNMP 接口默认 IP 地址为 192.168.0.1。

- 配置 FTP/TFTP 服务器端，确保服务器处于可用状态。
- 配置 TFTP 服务器的 IP 地址，使之与设备的 IP 地址处于同一网段，使设备可以访问服务器。

通过命令行升级方式升级系统软件的步骤如下：

步骤	配置	说明
1	Inspur#**download system-boot** { **ftp** { *ipv4-address* | *ipv6-address* } *user-name password* [**unit** *unit-id*] *file-name* | **tftp** { *ipv4-address* | *ipv6-address* } [**unit** *unit-id*] *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password* [**unit** *unit-id*] *file-name* } [**system1.z** | **system2.z**]	通过 FTP 协议、SFTP、TFTP 协议下载系统启动软件。支持 IPv6 地址。
2	Inspur#**boot sequence**	（可选）配置系统文件启动顺序。
3	Inspur#**reboot** [**now** | **in** *time*]	重新启动设备，设备将自动加载刚下载的系统启动文件。
4	Inspur#**switch startup-config backup-config**	（可选）交替加载配置文件。

1.4.4 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show startup-config**	查看设备启动时加载的配置信息。
2	Inspur#**show running-config**	查看设备的当前配置信息。
3	Inspur#**show version**	查看系统的版本信息。

1.5 时间管理

1.5.1 简介

随着互联网在社会各个方面的发展和延伸，网络上多种涉及时间的应用，如网上实时交易、分布性的网络计算和处理、交通航班航路管理、数据库管理等，都需要精确、可靠的时间。

为了保证设备系统时间的精准，设备提供了完善的时间管理功能，包括手动配置系统时间和时区、手动配置夏令时、NTP 功能以及 SNTP 功能。

时间和时区

通常情况下设备时间配置为设备所在地的实时时间，将时区配置为以格林尼治标准时间为基础的所在地时区（如中国北京在格林尼治为基准的东八区，即配置为+08:00）。

设备支持“年月日时分秒”的时间显示和时区偏移显示，可手动配置设备的时间和时区。

夏令时

夏令时（DST，Daylight Saving Time）是一种为节约资源而人为规定地方时间的制度。一般在夏季人为将时间调整提前一小时，可以使人早起早睡以减少照明量。但各个国家对夏令时的具体规定不同，所以在配置夏令时前需要考虑当地的具体情况。

设备支持配置夏令时开始的时间和结束的时间，以及调整时间的偏移量。

NTP

NTP（Network Time Protocol，网络时间协议）是用于互联网中时间同步的标准互联网协议，用于快速使网络内所有具有时钟的设备进行时钟同步。NTP 基于 UDP 进行传输，使用的端口号是 123，保证较高的精度（误差在 10ms 左右）。

NTP 基本原理如图 1-8 所示，时钟同步的工作过程如下：

步骤 1 Switch A 发送一个 NTP 消息包给 Switch B，该消息包带有离开 Switch A 时的时间戳，该时间戳为 10:00:00am，记为 t1。

步骤 2 当此 NTP 消息包到达 Switch B 时，Switch B 加上自己的时间戳，该时间戳为 11:00:01am，记为 t2。

步骤 3 当此 NTP 消息包离开 Switch B 时，Switch B 再加上自己的时间戳，该时间戳为 11:00:02am，记为 t3。

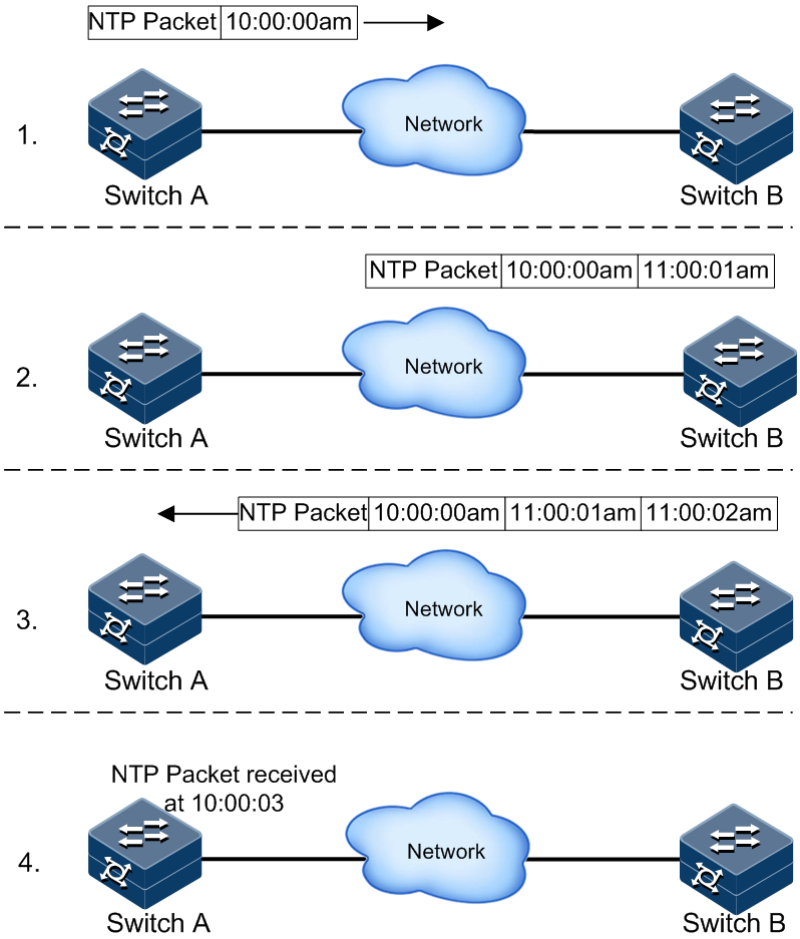
步骤 4 当 Switch A 接收到该响应消息包时，加上一个新的时间戳，该时间戳为 10:00:03am，记为 t4。

至此，Switch A 已经拥有足够的信息来计算两个重要的参数：

- NTP 消息来回一个周期的时延：Delay=(t4-t1)-(t3-t2)。
- Switch A 和 Switch B 之间的时间差：Offset=((t2-t1)+(t3-t4))/2。

Switch A 根据这些信息来设定自己的时钟，实现与 Switch B 的时钟同步。

图1-8 NTP 基本原理



NTP 支持多种工作模式进行时间同步：

- 服务器/客户端模式

在服务器/客户端模式中，客户端向不同的服务器发送时钟同步报文。服务器收到报文后会自动工作在服务器模式，并发送应答报文。客户端收到应答报文后，进行时钟过滤和选择，并同步到优选的服务器。

在该模式下，客户端能同步到服务器，而服务器无法同步到客户端。设备既支持作为客户端，也支持作为服务器。

- 对等体模式

在对等体模式中，在主动对等体上配置被动对等体，主动对等体先向被动对等体发送时钟同步报文，被动对等体收到报文后自动工作在被动对等体模式，并发送应答报文。经过报文的交互，建立起对等体模式，层数小的对等体同步层数大的对等体。

在该模式下，主动对等体和被动对等体可以互相同步。设备既支持作为主动对等体，指定被动对等体进行互相同步；也支持作为被动对等体。

SNTP

SNTP（Simple Network Time Protocol，简单网络时间协议）将设备系统时间同步为格林尼治时间，然后根据系统时区的设置来转化成本地时间。当 SNTP 客户端与服务器不在同一地区时，SNTP 客户端同步的时间为格林威治时间，然后根据系统时区的设置来转化成本地时间。

SNTP 客户端获取时间有两种方式，即主动发送请求报文和被动监听报文，通过不同模式实现：

- 单播模式：SNTP 客户端主动发送请求报文。指定设备的 SNTP 单播服务器地址后，设备将每隔 10s 尝试一次从 SNTP 服务器获取时钟信息，并且每次从 SNTP 服务器获取时钟信息的最大超时时间为 60 秒。
- 组播或广播模式：SNTP 客户端被动监听报文。
- 配置 SNTP 客户端为组播模式后，设备将时刻监听组播地址 224.0.1.1，从 SNTP 组播服务器获取时钟信息，并且每次从 SNTP 获取时钟信息的最大超时时间为 60s。
- 配置 SNTP 客户端为广播模式后，设备将时刻监听广播地址 255.255.255.255，从 SNTP 广播服务器获取时钟信息，并且每次从 SNTP 获取时钟信息的最大超时时间为 60s。

1.5.2 配置准备

场景

配置设备的系统时间，保证系统时间的精准。

- 无论何时，手动配置时间和时区立即生效。
- 开启 NTP 或 SNTP 功能，经过同步周期后，设备同步到的时间会实时刷新，覆盖当前系统时间。
- NTP 功能与 SNTP 功能互斥，不能同时配置。

前提

无

1.5.3 缺省配置

时间和时区

设备上时间和时区的缺省配置如下。

功能	缺省值
时区偏移	+08:00-CCT
系统时钟显示模式	**default**

说明

CCT 是一种标准时间代码。以格林威治时间 GMT 作为零时区的地方，其他地区在此基础上根据自己所处经度或时区进行加或者减计算即可得该地的标准时间，为了方便，规定了一系列标准时间代码，常见的有：

- CCT +8:00 中国沿海时间(北京时间)
- EDT -4:00 美国东部夏令时
- EST -5:00 美国东部标准时间
- CDT -5:00 美国中部夏令时
- CST -6:00 美国中部标准时间
- MDT -6:00 美国山地夏令时
- MST -7:00 美国山地标准时间
- PDT -7:00 美国太平洋夏令时
- PST -8:00 美国太平洋标准时间

夏令时

设备上夏令时的缺省配置如下。

功能	缺省值
夏令时功能状态	禁止

NTP

设备上 NTP 的缺省配置如下。

功能	缺省值
设备是否作为 NTP 主时钟	否
全局 NTP 服务器	无
全局 NTP 对等体	无
参考时钟源	0.0.0.0
身份验证功能	关闭
身份验证密钥 ID	无
可信密钥	无

SNTP

设备上 SNTP 的缺省配置如下。

功能	缺省值
SNTP 服务器地址	无

1.5.4 配置时间与时区

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**clock set** *hour minute second year month day*	配置系统时间。
2	Inspur#**clock timezone** { **+** | **-** } *hour minute timezone-name*	配置系统所属时区。
3	Inspur#**clock display** { **default** | **utc** }	配置系统时钟显示模式。

1.5.5 配置夏令时

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**clock summer-time enable**	启动设备的夏令时功能。
2	Inspur#**clock summer-time recurring** { *week* | **last** } { **fri** | **mon** | **sat** | **sun** | **thu** | **tue** | **wed** } *month hour minute* { *week* | **last** } { **fri** | **mon** | **sat** |**sun** | **thu** | **tue** | **wed** } *month hour minute offset-mm*	配置系统夏令时计算周期。 **说明** 命令格式中带下划线的参数表示夏令时的终止时间。

说明

手动设置系统时间时，如果系统使用夏令时，例如夏令时为每年的四月第二个星期天早上 2 点钟，到九月的第二个星期天早上 2 点钟，在这个时间区域内时钟拨快一个小时，即时间偏移为 60 分钟，那么每年的四月第二个星期天早上 2 点钟到 3 点钟为不存在时间。手动设置时间在该时间段内的结果是设置失败。

南半球的夏季与北半球相反，其夏令时间一般是从 9 月到次年的 4 月。假如配置的开始时间比结束时间晚，系统就假定你在南半球，也就是说夏令时是从当年的开始时间到下一年的结束时间。

1.5.6 配置 NTP

配置 NTP 基本功能

请在设备上进行以下配置。

注意

NTP 功能和 SNTP 功能互斥，二者不能同时使用。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ntp server** { *ipv4-address* | *ipv6-address* } [**version** *version-number*] [**keyid** *key-id*]	（可选）为工作在服务器/客户端模式下的客户端设备配置 NTP 服务器地址。
3	Inspur(config)#**ntp peer** { *ipv4-address* / *ipv6-address* } [**version** *version-number*] [**keyid** *key-id*]	（可选）为工作在对等体模式下的交换机设备配置 NTP 对等体地址。
4	Inspur(config)#**ntp refclock-master** [*ip-address*] [*stratum*]	为需要作为时钟源的交换机设备配置本设备时钟作为 NTP 参考时钟源。

说明

如果设备被配置为 NTP 参考时钟源，则无法配置 NTP 服务器或 NTP 对等体；反之亦然，如果配置了 NTP 服务器或对等体，则无法将设备配置为 NTP 参考时钟源。

配置 NTP 身份验证功能

在对安全性要求较高的网络中，使用 NTP 协议时需要进行身份验证。NTP 客户端使能身份验证功能后只与通过验证的服务器进行同步，保证了网络的安全性。NTP 客户端只有使能了身份验证功能才会对服务器进行验证，若未使能身份验证功能，即使服务器携带密钥信息，客户端也不会进行验证，直接与服务器进行时间同步。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ntp authenticate enable**	使能 NTP 服务器/客户端的身份验证功能。
3	Inspur(config)#**ntp authentication-keyid** *key-id* **md5** *password*	配置 NTP 服务器/客户端的身份验证密钥 ID 和密钥值。

步骤	配置	说明
4	Inspur(config)#**ntp trust-keyid** *key-id*	配置 NTP 服务器/客户端的身份验证密钥 ID 为可信 ID。 **说明** NTP 客户端只有使能了身份验证功能才会对服务器进行验证，并且客户端只会向提供可信密钥的服务器进行同步。

1.5.7 配置 SNTP

配置 SNTP 客户端单播功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**sntp server** { *ipv4-address* | *ipv6-address* } [**version** *version-number*]	配置 SNTP 单播服务器地址。 配置 SNTP 服务器地址后，设备将每隔 10 秒钟尝试一次从 SNTP 服务器获取时钟信息，并且每次从 SNTP 获取时钟信息的最大超时时间为 60s。

1.5.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show clock** [**summer-time-recurring**]	查看设备的系统时间、时区以及夏令时的配置信息。
2	Inspur#**show sntp**	查看 SNTP 的配置信息。
3	Inspur#**show ntp status**	查看 NTP 的配置信息。
4	Inspur#**show ntp associations** [**detail**]	查看 NTP 的连接信息。
5	Inspur#**show ntp authentication**	查看 NTP 安全认证信息。

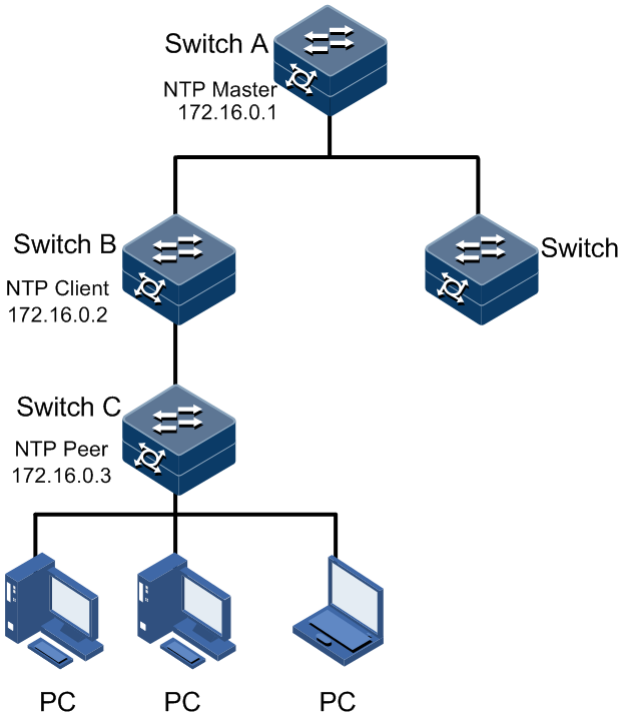
1.5.9 配置 NTP 功能示例

组网需求

某公司搭建稳定的时钟同步系统，使公司内部设备保持系统时间的一致和精准。基本规划为：

- Switch A 作为时钟同步系统的主时钟。
- Switch B 作为时钟同步系统的客户端，需设置上层的 Switch A 为 NTP 服务器。
- 设置 Switch C 为 Switch B 的 NTP 对等体，接收 Switch B 发出的下行同步数据流。

图1-9 NTP 组网示意图



配置步骤

步骤 1 配置 Switch A。

```
Inspur#hostname SwitchA
SwitchA#config
SwitchA(config)#ntp refclock-master
```

步骤 2 配置 Switch B。

```
Inspur#hostname SwitchB
SwitchB#config
SwitchB(config)#ntp server 172.16.0.1
SwitchB(config)#ntp peer 172.16.0.3
```

检查结果

- 查看 Switch A。

通过 **show ntp status** 查看 Switch A 配置是否正确。

```
SwitchA#show ntp status
Clock status   :synchronized
NTP peer       :0.0.0.0
NTP version    :3
NTP mode       :ntpMaster
Leap           :0
Poll           :6
Stratum        :8
Precision      :2**-16
Reference clock :127.127.1.0
Reference time  :00000000.00000000(Thu 1970-01-01,08:00:00)
Current time   :5333d6de.33428f00(Thu 2014-03-27,15:45:44.070)
Root delay     :0.000000
Root dispersion :0.000000
```

- 查看 Switch B。

通过 **show ntp status** 查看 Switch B 配置是否正确。

```
SwitchB#show ntp status
Clock status   :synchronized
NTP peer       :172.16.0.1
NTP version    :3
NTP mode       :ntpSlave
Leap           :0
Poll           :6
Stratum        :9
Precision      :2**-16
Reference clock :172.16.0.1
Reference time  :5333d671.383980f6(Thu 2014-03-27,15:44:58.466)
Current time   :5333d697.0a917f54(Thu 2014-03-27,15:45:58.765)
Root delay     :0.000000
Root dispersion :0.010004
```

通过 **show ntp associations** 查看 Switch B 的 NTP 会话信息。

```
SwitchB#show ntp associations
Server(ip)       refid         stratum  poll  when       delay
offset      dispersion   mode reach
------------------------------------------------------------------------------
----------------------------------------
(s)172.16.0.1  127.127.1.0    8       6    55        0.000000     -
1.965874    14.875517    4   255
Peer(ip)         refid         stratum  poll  when       delay
offset      dispersion   mode reach
------------------------------------------------------------------------------
----------------------------------------
(u)172.16.0.3  0.0.0.0        16      6    125       0.000000
0.000000     16.000000    0   0
```

- 查看 Switch C。

通过 **show ntp status** 查看 Switch C 配置是否正确。

```
Inspur#show ntp status
Clock status :     synchronized
NTP peer :         172.16.0.2
NTP version :      3
NTP mode :         ntpSlave
Leap :             0
Poll :             6
Stratum :          10
Precision :        2**-22
Reference clock :   172.16.0.2
Reference time :    4d62a905.00000000(Mon 2011-02-22,02:03:49)
Current time :      5333dd97.00000000(Thu 2014-03-27,16:13:11)
Root delay :       4.154726
Root dispersion :   14.034068
```

通过 **show ntp associations** 查看 Switch C 的 NTP 会话信息。

```
Inspur#show ntp associations
Active(IP)       refid      stratum poll  when      delay       offset
dispersion    mode reach
-------------------------------------------------------------------------
----------------------------------------
(s)172.16.0.2   172.16.0.1         9         6     97596571    4.154726
13447.112484  0.000930     1    6
```

1.6 接口管理

1.6.1 简介

以太网以其高度灵活、相对简单、易于实现的特点，成为重要的局域网组网技术。以太网接口分为：以太网电接口和以太网光接口。

交换机设备支持以太网电接口和以太网光接口。

自协商功能

自动协商的主要功能就是使物理链路两端的设备通过交互信息自动选择同样的工作参数。自动协商的内容主要包括双工模式、运行速率等参数。一旦协商通过，链路两端的设备就锁定在同样的双工模式和运行速率。

连接线缆

一般以太网标准网线分为直通线 MDI（Medium Dependent Interface）和交叉线 MDI-X（Medium Dependent Interface cross-over）两种。MDI 提供终端到网络中继设备的物理和电路连接。MDI-X 提供同种设备（终端到终端）的连接。主机和路由器的接口类型为 MDI，集线器和交换机的端口类型为 MDI-X。一般情况下，异类设备互连用直通线，同类设备互连用交叉线。自适应连接则无需考虑直通线或交叉线。

设备以太网线连接支持自适应 MDI/MDI-X。

1.6.2 接口的缺省配置

设备上物理层接口的缺省配置如下。

功能	缺省值
接口的最大转发帧长	12Kb
接口的双工模式	自协商
接口的速率	自协商
接口速率监控时间间隔	5s
接口速率统计功能状态	禁止
接口动态统计时间间隔	2s
接口的流控功能状态	禁止
接口状态	打开

1.6.3 配置接口基本属性

当互连的两个设备的接口属性，如 MTU（Maximum Transfered Unit，最大传输单元）、双工模式、速率等参数不一致时，会造成设备间无法正常通信，此时需要调整接口的属性使两端设备互相匹配。

以太网物理层分为半双工、全双工和自协商三种工作模式。

- 半双工在任意时刻只能接收或发送报文。
- 全双工在任意时刻可以同时接收和发送报文。
- 自协商是指链路两端的设备通过交互信息自动选择双工模式，一旦协商通过，两端的设备就使用同样的双工模式进行报文传输。

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#interface` *vlan-id*	进入 VLAN 接口配置模式。
3	`Inspur(config-vlan*)#mtu` *max-frame-length* `Inspur(config-vlan*)#exit`	配置接口的最大传输单元，当接收的 IP 报文长度超过该值，则对 IP 报文进行分片。
4	`Inspur(config)#interface` *interface-type interface-number*	进入物理接口配置模式。
5	`Inspur(config-gigaethernet1/1/*)#duplex { full | half | auto }`	（可选）配置接口的双工模式。

步骤	配置	说明
6	Inspur(config-gigaethernet1/1/*)**#speed** { **auto** | **10** | **100** | **1000** }	（可选）配置接口的速率。 对于光接口而言，接口的速率还取决于光模块的规格。
7	Inspur(config-gigaethernet1/1/*)**#tpid** { **8100** | **9100** | **88a8** }	（可选）配置接口的 TPID。 缺省情况下，接口的 TPID 为 0x8100。
8	Inspur(config-gigaethernet1/1/*)**#description** *string*	（可选）配置接口的描述信息，字符串形式，取值范围 1～225，支持“空格，\，’，<，>，&”等特殊字符
9	Inspur(config-gigaethernet1/1/*)**#jumboframe** *frame-size*	（可选）配置接口允许通过的最大帧长。
10	Inspur(config-gigaethernet1/1/*)**#mdi** { **xover** | **auto** | **normal** }	（可选）配置电口的 MDI/MDIX 模式。
11	Inspur(config-gigaethernet1/1/*)**#mac** *mac-address*	（可选）配置接口的 MAC 地址。
12	Inspur(config-gigaethernet1/1/*)**#portswitch**	（可选）配置接口由路由模式转为交换模式，使用 **no** 格式恢复为路由模式。
13	Inspur(config-gigaethernet1/1/*)**#vibration-suppress period** *value*	（可选）配置接口震荡抑制周期。
14	Inspur(config-tengigabitethernet1/1/*)**port-type** { **1000base_t1** | **1000base_t2** | **1000base_x** | **10Gbase_r** } Inspur(config-tengigabitethernet1/1/*)**exit**	（可选）配置 SFP 接口连接模式。
15	Inspur(config)**#interface tunnel** *interface-number*	创建 Tunnel 接口。
16	Inspur(config-tunnel1/1/*)**#tunnel source** *ip-address*	配置 Tunnel 接口的源 IP 地址。
17	Inspur(config-tunnel1/1/*)**#tunnel destination** *ip-address*	配置 Tunnel 接口的目的 IP 地址。
18	Inspur(config-tunnel1/1/*)**#tunnel mode ipv6ip**	配置 Tunnel 的封装类型。

1.6.4 配置接口信息统计功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur**#config**	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**dynamic statistics time** *time*	（可选）配置接口动态统计周期
3	Inspur(config)#**interface statistic period** *value*	（可选）配置端口信息统计周期。
4	Inspur(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式。
5	Inspur(config-vlan*)#**statistics enable**	使能接口统计功能。
6	Inspur(config-vlan*)#**clear interface statistics**	（可选）清除接口的统计信息。

1.6.5 配置接口流控功能

IEEE802.3x 是全双工以太网数据链路层的流量控制方法。当客户端向服务器发出请求后，自身系统或网络产生拥塞时，客户端会向服务器发出 PAUSE 帧，以延缓服务器向客户端的数据传输。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**flowcontrol** { **receive** | **send** } { **off** | **on** }	使能或禁止接口对 802.3x 报文的流量控制功能。

1.6.6 配置接口打开或关闭

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**shutdown**	关闭当前接口。 可以使用 **no shutdown** 命令再次打开接口。

1.6.7 配置 Console 接口

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**console open**	（可选）使能 Console 接口。 只能在非 Console 命令行会话中使用该命令。 **注意** 使用 **console close** 命令禁用 Console 接口，可能会导致设备无法控制，请谨慎使用。
3	Inspur(config)#**login-trap enable**	（可选）使能用户退出或登录中发送 Trap。

1.6.8 配置 Combo 接口

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**medium-priority** { **copper** | **fiber** }	（可选）配置 Combo 接口优先级信息，选择光口或者电口为优先使用。缺省情况下，优先使用光接口。
4	Inspur(config-gigaethernet1/1/*)#**medium-type** { **auto** | **fiber** | **copper** }	（可选）配置 Combo 接口的光/电选择模式。

说明

只有在支持 Combo 接口的设备上才能配置。

1.6.9 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show interface** [**range**] [*interface-type interface-number*]	查看接口状态，支持显示 Block VLAN。
2	Inspur#**show interface brief**	查看接口概要信息。

序号	检查项	说明
3	Inspur#**show interface** [*interface-type interface-number*] **description**	查看接口描述信息。
4	Inspur#**show interface** *interface-type interface-number* **statistics** [**dynamic** [**detail**]] Inspur#**show interface statistics dynamic** [**detail**]	查看接口的统计信息。
5	Inspur#**show interface** [*interface-type interface-number*] **configuration**	查看接口概要信息。
6	Inspur#**show port split**	查看接口拆分状态。

1.7 配置设备基本信息

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**hostname** *name*	（可选）配置设备名称。 缺省情况下，设备名称是 Inspur。 系统支持更改设备名称，方便用户区分网络中的不同设备，支持“空格、\、’、<、>、&”等特殊字符。设备名称更改后立即生效，可以在终端提示符看到设备名称。
2	Inspur#**language** { **chinese** | **english** }	（可选）配置切换语言模式。 缺省情况下，设备提供的语言模式是英文。
3	Inspur#**write**	保存配置信息。 设备配置完成后，需要将配置信息保存到设备中，新保存的配置信息将覆盖原有的配置信息。 配置完成后，如果不进行保存操作，设备重启后会丢失新的配置，继续执行原有的配置。 **注意** 删除设备配置文件用 **erase** *file-name* 命令，执行删除命令后，删除的文件将不能恢复，请谨慎使用。
4	Inspur#**reboot** [**now** | **in** *time*]	（可选）配置设备重启。 设备出现故障时，可根据实际情况，通过重启设备来尝试解决故障。

步骤	配置	说明
5	Inspur#**show** { **assert** | **bootlog** | **exception** | **memory_errors** | **ros_errors** } [**last** [*count*]]	查看设备中的显示信息或日志信息。
6	Inspur#**clear** [**all** | **assert** | **bootlog** | **exception** | **memory_errors** | **ros_errors**]	（可选）清除设备中的显示信息或日志信息。
7	Inspur#**show loadcfg**	查看缓存配置信息。
8	Inspur#**show tech-support**	查看常规的系统信息，包括 CPU、内存、终端连接状态、DDM 等
9	Inspur#**show semaphore** [*semaphore-id*]	查看平台的信号量信息。
10	Inspur#**show timer** [*timer-id*]	查看定时器信息。
11	Inspur#**show twltimer** [*timer-level*]	查看平台定时器信息。

注意

- 重启设备会中断业务，请谨慎操作。
- 重启前请根据需要保存配置，以免配置丢失。

1.8 任务调度功能

1.8.1 简介

当用户需要周期性或指定时间执行某些命令行时，可以考虑配置任务调度功能。设备支持通过计划列表结合命令行的方式来实现任务调度，用户只需要在计划列表中指定任务的开始时间、周期和结束时间，再将计划列表和命令行绑定，就可以实现对这部分命令行的周期性操作。

1.8.2 配置任务调度

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**schedule-list** *list-number* **start date-time** { *mm-dd-yyyy hh:mm:ss* [**every** { **day** | **week** } **stop** *mm-dd-yyyy hh*:*mm*:*ss*] | **every** *days-interval time-interval* [**stop** *mm-dd-yyyy hh*:*mm*:*ss*] }	创建并配置计划列表。

步骤	配置	说明
	Inspur(config)#**schedule-list** *list-number* **start date-time** *mm-dd-yyyy hh:mm:ss* **every weekday-list** { **fri** | **mon** | **off-day** | **sta** | **sun** | **thu** | **tue** | **wed** | **working-day** | *weekday-list* }	
	Inspur(config)#**schedule-list** *list-number* **start up-time** *days-after-startup hh*:*mm*:*ss* [**every** *days-interval time-interval* [**stop** *days-after-startup hh*:*mm*:*ss*]]	
3	Inspur(config)#*command-string* **schedule-list** *list-number*	将需要周期性执行且支持计划列表的命令行与计划列表绑定。

1.8.3 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show schedule-list** [*list-number*]	查看计划列表的配置信息。

1.9 看门狗

1.9.1 简介

由于单片机的工作会受到外界电磁场的干扰，造成程序的跑飞，而陷入死循环，使系统无法正常工作。出于对单片机运行状态进行实时监测的考虑，产生了一种专门用于监测交换机硬件设备运行状态的程序，俗称“看门狗”（Watchdog）。

当任务挂起或陷入死循环而导致交换机无法继续工作时，并且在一定周期之内没有发出信号对看门狗计数器清零，系统会自动重启。

看门狗功能可以防止系统程序由于不确定的故障造成的死循环，提高系统的稳定性。

1.9.2 配置准备

场景

通过配置看门狗功能，可以防止系统程序由于不确定的故障造成的死循环，从而提高系统的稳定性。

前提

无

1.9.3 看门狗的缺省配置

设备上看门狗的缺省配置如下。

功能	缺省值
看门狗功能状态	使能

1.9.4 配置看门狗功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**watchdog enable**	使能看门狗功能。

1.9.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show watchdog**	查看看门狗功能状态。

1.10 配置 Banner

1.10.1 配置准备

场景

Banner 公告信息是用户登录设备或退出登录时，系统界面显示的一段提示语，比如注意事项、免责声明等。

用户可根据需要自行设置设备的公告信息内容。同时提供 Banner 开关功能，使能 Banner 显示功能，则配置的公告内容会在登录或退出设备时在系统界面显示。

用户配置完上述功能后应使用 **write** 命令保存配置，否则设备重启导致 Banner 信息丢失。

前提

无

1.10.2 配置 Banner 公告

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**banner login** *word*单击回车 Enter text message followed by the character '*word*' to finish.User can stop configuration by inputing' Ctrl+c' *message word*	配置 Banner 公告信息内容。用户输入 **banner login** 及开始标志符 *word* 后单击回车，在提示信息后输入公告信息的内容，最后以与开始标志符相同的字符 *word* 结束。 **说明** • 参数 *word* 是长度为 1 的字符，是公告信息的开始标志和结束标志，这两个标志必须是相同的字符。建议选择不会在 *message* 中出现的特殊字符。 • 参数 *message* 是公告信息的内容，最大长度为 2560 个字符。
3	Inspur(config)#**clear banner login**	（可选）清除 Banner 公告信息内容。

1.10.3 使能 Banner 显示功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**banner enable**	使能 Banner 公告显示功能。 缺省情况下，禁用公告显示功能。使能该功能后，可使用 **banner disable** 命令禁用。

1.10.4 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show banner login**	查看 Banner 使能状态及配置的公告信息内容。

2 ISF

本章介绍 ISF 的原理和配置过程，并提供相关的配置案例。

- 简介
- ISF 基本概念
- 搭建 ISF 环境
- ISF 配置
- 独立运行模式下预配置 ISF
- ISF 模式下配置 ISF
- 检查配置
- ISF 典型配置举例

2.1 简介

ISF（Intelligent Stacking Framework，智能堆叠框架）协议是一种典型的堆叠协议。ISF 是浪潮思科自主研发的软件虚拟化技术，它的核心思想是将多台设备连接在一起，进行必要的配置后，虚拟化成一台设备。使用这种虚拟化技术可以集合多台设备的硬件资源和软件处理能力，实现多台设备的协同工作、统一管理和不间断维护。

说明

ISF 接口需要选择万兆接口，并且需要相同型号的设备才可以组成 ISF。ISF 中的成员设备最多为 9 台。

S6550-48 口设备交换机的接口 1/1/49～1/1/52 可以分别加入不同的堆叠逻辑口中，接口 1/1/49 只能和接口 1/1/50 加到同一个堆叠逻辑口中，接口 1/1/51 也只能和接口 1/1/52 加到同一个堆叠逻辑口中（比如 1/1/49 加入了 isf 1/1/1 里面，那么 1/1/50 也只能加入 isf 1/1/1 中，而接口 1/1/51 和 1/1/52 加入 isf 1/1/2 中）。

2.1.1 ISF 的优点

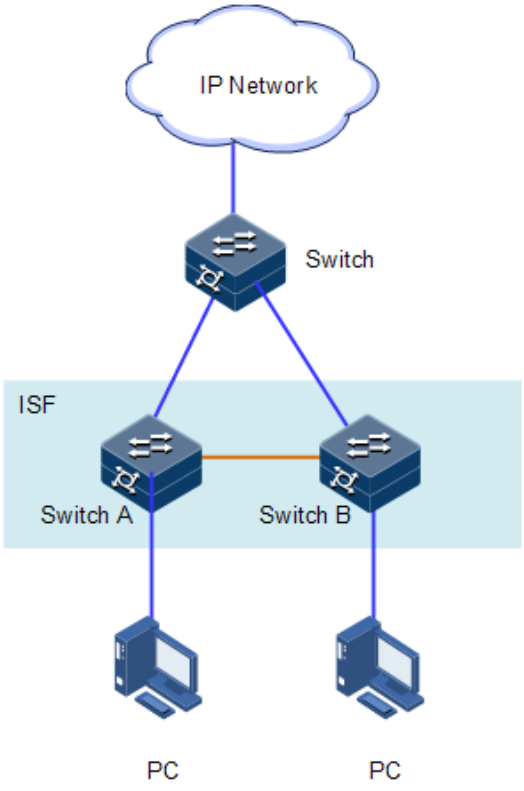
ISF 主要具有以下优点：

- 简化管理。堆叠形成之后，ISF 用户连接到任何一台成员设备的任何一个端口都可以登录 ISF，对 ISF 内所有成员设备进行统一管理。
- 强大的网络扩展能力。通过增加成员设备，可以轻松自如的扩展 ISF 系统的端口数、带宽和处理能力。
- 高可靠性。ISF 的高可靠性体现在多个方面，例如：ISF 由多台成员设备组成，Master 设备负责 ISF 的运行、管理和维护，Backup 与 Slave 设备在作为备份的同时也可以处理业务。一旦 Master 设备故障，系统会迅速自动选举新的 Master，以保证业务不中断，从而实现了设备的 1:N 备份功能；成员设备之间 ISF 链路支持聚合功能，ISF 和上、下层设备之间的物理连接也支持聚合功能，多条链路之间可以互为备份也可以进行负载分担，从而进一步提高了 ISF 系统的可靠性。

2.1.2 ISF 的应用

如图 2-1 所示，Master 和 Backup 组成 ISF，对上、下层设备来说，它们就是一台设备。

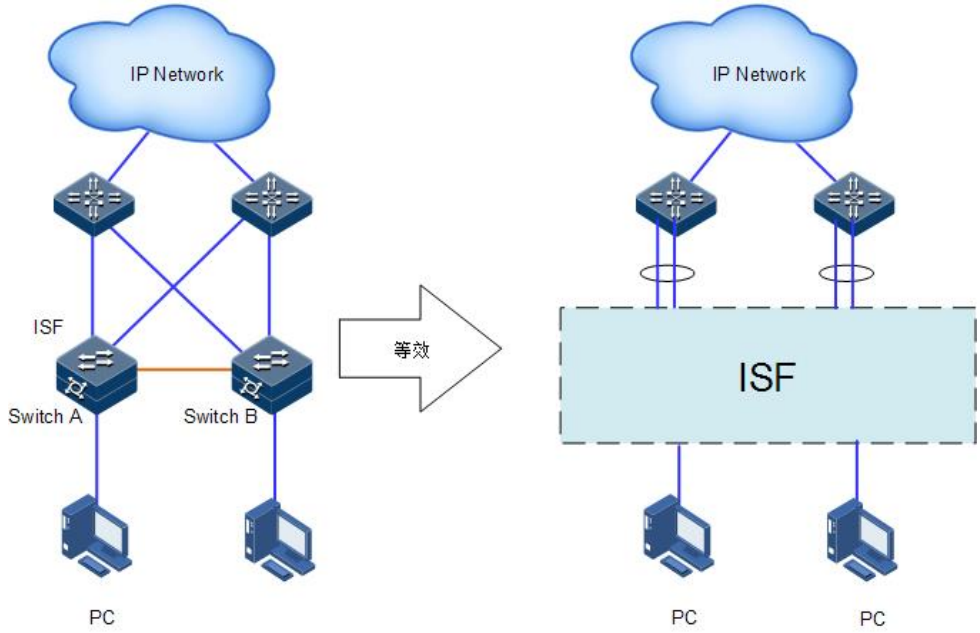
图2-1 ISF 组网应用示意图



2.2 ISF 基本概念

如图 2-2 所示，将 Device A 和 Device B 物理连线，进行必要的配置后，就能形成虚拟化的 ISF。ISF 统一管理 Device A 和 DeviceB 的物理资源和软件资源。

图2-2 ISF 虚拟化示意图



ISF 虚拟化技术涉及如下基本概念：

运行模式

设备支持两种运行模式：

- 独立运行模式：处于该模式下的设备只能单机运行，不能与别的设备形成 ISF。
- ISF 模式：处于该模式下的设备可以与其它设备互连形成 ISF。

两种模式之间通过命令行进行切换。

角色

ISF 中每台设备都称为成员设备。成员设备按照功能不同，分为 3 种角色：

- Master：负责管理整个 ISF。
- Backup：负责所谓 Master 的备份，优先成为主。
- Slave：同样作为 Master 的备份设备运行。当 Master 与 Backup 故障时，系统会自动从 Slave 中选举一个新的 Master 接替原 Master 工作。

Master 和 backup，Slave 均由角色选举产生。一个 ISF 中同时只能存在一台 Master，一台 Backup，其它成员设备都是 Slave。

成员编号

ISF 中使用成员编号（Member ID）来标识和管理成员设备，ISF 中所有设备的成员编号都是唯一的。比如，ISF 中接口的编号会加入成员编号信息：设备在独立运行模式下，某个接口的编号为 tengigabitethernet1/1/1；当该设备加入 ISF 后，如果成员编号为 2，则该接口的编号将变为 tengigabitethernet2/1/1。

设备处于独立运行模式时，缺省配置成员编号为 1。如果新设备加入 ISF，但是该设备与已有成员设备的编号冲突，则该设备不能加入 ISF。所以用户在将设备加入 ISF 前，需要统一规划、配置设备的成员编号，以保证 ISF 中成员编号的唯一性。

说明

成员编号的取值为 1～9。

ISF 接口

专用于 ISF 的逻辑接口，如果成员编号为 N，那么分为 ISF-PortN/1/1 和 ISF-PortN/1/2。它需要和物理端口绑定之后才能生效。ISF 逻辑端口可以与一个或多个物理口绑定，以提高 ISF 链路的带宽以及可靠性。目前，设备支持一个 ISF 接口最多可以与 8 个物理端口绑定。双芯片设备配置时需注意，不同芯片堆叠物理口不能放到相同堆叠口中。相同芯片堆叠物理口，不能放到不同堆叠口中。

说明

在独立运行模式下，ISF 接口分为 ISF-Port1/1/1 和 ISF-Port1/1/2；在 ISF 模式下，ISF 接口分为 ISF-PortN/1/1 和 ISF-PortN/1/2，其中 N 为设备的成员编号。为简洁起见，本文描述时统一使用 ISF-Port1 和 ISF-Port2。

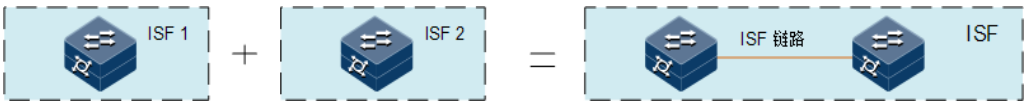
ISF 物理接口

设备上用于 ISF 连接的物理接口，当它们与 ISF 接口绑定后，则成为 ISF 物理端口，用于成员设备间转发报文。可转发的报文包括 ISF 相关协商报文以及需要跨成员设备转发的业务报文。

ISF 合并

如图 2-3 所示，两个 ISF 各自已经稳定运行，通过物理连接和必要的配置，形成一个 ISF，这个过程称为 ISF 合并（Merge）。

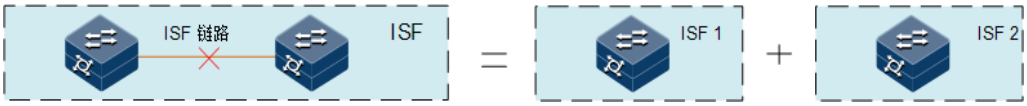
图2-3 ISF 合并示意图



ISF 分裂

如图 2-4 所示，一个 ISF 形成后，由于 ISF 链路故障，导致 ISF 中两相邻成员设备物理上不连通，一个 ISF 变成两个 ISF，这个过程称为 ISF 分裂（Split）。

图2-4 分裂示意图



ISF 域

域是一个逻辑概念。为了适应各种组网应用，同一个网络里可以部署多个 ISF，ISF 之间使用域编号（Domain ID）来以示区别。ISF 域之间互不干扰。ISF 协议主要描述设备之间的发现过程，探究设备的连通性。说明主设备、备设备的选举过程。根据收集到的信息生成拓扑，监听成员设备的连通状况，保证整个虚拟化系统正常运行。

成员优先级

成员优先级是成员设备的一个属性，主要用于角色选举过程中确定成员设备的角色。优先级值越大表示优先级越高，优先级越高当选为 Master 的可能性越大。设备的缺省优先级均为 0，如果想让某台设备当选为 Master，则在组建 ISF 前，可以通过命令行手工提高该设备的成员优先级。当主设备优先级相同时，会根据堆叠系统运行时间较长的一个设备选为主设备，堆叠模式下，在主设备上可以设置其他设备的优先级。

2.2.2 ISF 工作原理

ISF 系统将经历物理连接、拓扑收集、角色选举、管理与维护四个阶段。成员设备之间需要先建立 ISF 物理连接，然后会自动进行拓扑收集和角色选举，完成 ISF 的建立，此后进入 ISF 管理和维护阶段。

物理连接

- 连接介质

要形成一个 ISF，需要先连接成员设备的 ISF 物理端口。设备支持的 ISF 物理端口的类型不同使用的连接介质不同：使用光口作为 ISF 物理端口，则使用光纤连接。这种连接方式可以将距离很远的物理设备连接组成 ISF，使得应用更加灵活。

- 连接拓扑

ISF 的连接拓扑有两种：链形连接和环形连接，如图 2-5 和图 2-6 所示。

图2-5 链型结构拓扑示意图

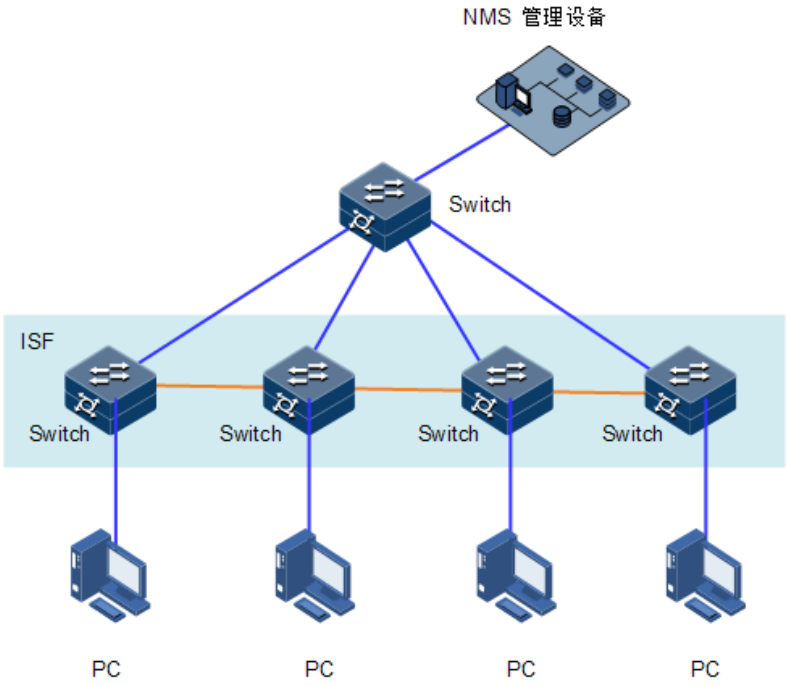
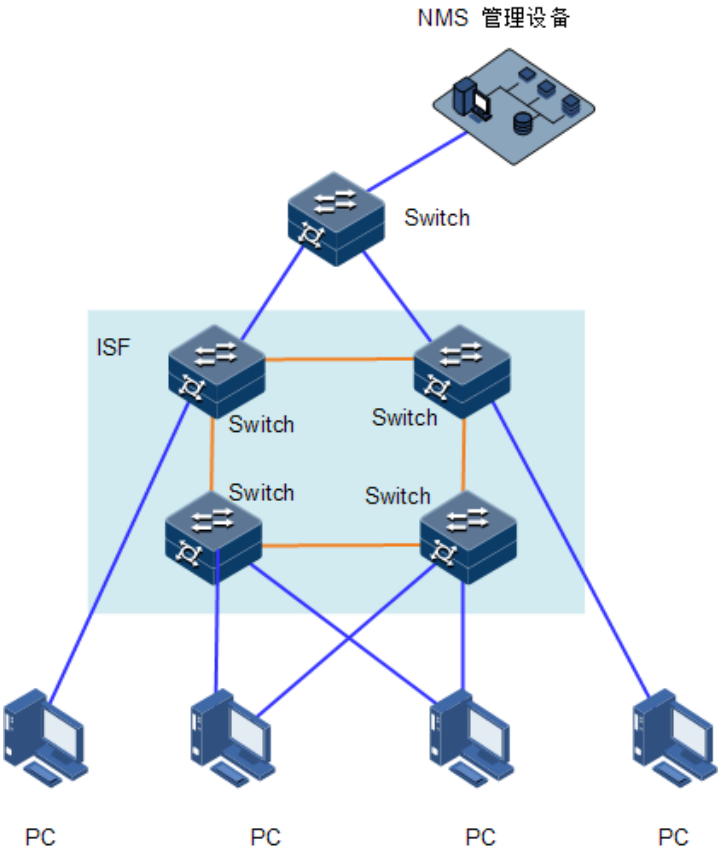


图2-6 环型结构拓扑示意图



相比环形连接，链形连接对成员设备的物理位置要求更低，主要用于成员设备物理位置分散的组网。环形连接比链形连接更可靠。因为当链形连接中出现链路故障时，会引起 ISF 分裂；而环形连接中某条链路故障时，会形成链形连接，ISF 的业务不会受到影响。

拓扑收集

每个成员设备和邻居成员设备通过交互 ISF Probe 报文来收集整个 ISF 的拓扑。ISF Route 报文会携带拓扑信息，具体包括 ISF 端口连接关系、成员设备编号、成员设备优先级、成员设备的桥 MAC 等内容。

设备刚启动时，当 ISF 端口状态变为 Up 后，本地主用主控板会进行以下操作：

- 将已知的拓扑信息周期性地从 Up 状态的 ISF 端口发送出去。
- 在收到直接邻居的拓扑信息后，更新本地记录的拓扑信息。

经过一段时间的收集，所有成员设备都会收集到完整的拓扑信息（称为拓扑收敛）。此时会进入角色选举阶段。

角色选举

确定成员设备角色为 Master 或 Slave 的过程称为角色选举。

角色选举会在拓扑变更的情况下产生，比如 ISF、新设备加入、Master 设备离开或者故障、两个 ISF 合并等。角色选举规则如下：

当前 Master 优先（ISF 系统形成时，没有 Master 设备，所有加入的设备都认为自己是 Master，会跳转到第二条规则继续比较）；

- 成员优先级大的优先；
- 系统运行时间长的优先（各设备的系统运行时间信息也是通过 ISF Hello 报文来传递的）；
- 成员桥 MAC 地址小的优先；

从第一条开始判断，如果判断的结果是多个最优，则继续判断下一条，直到找到唯一最优的成员设备才停止比较。此最优成员设备即为 Master，其它成员设备则均为 Slave。

通过以上规则选出的最优成员设备即为主设备，次优成员设备为备设备，其它成员设备则均为从设备。在角色选举完成后，ISF 主设备发 Config 报文确认通讯正常，ISF 形成，进入 ISF 管理与维护阶段。

说明

ISF 合并的情况下，也会进行 ISF 竞选，竞选仍然遵循角色选举的规则，竞选失败方的成员设备重启后以 Backup 和 Slave 的角色加入获胜方，最终合并为一个 ISF 。合并过程中的重启需要用户手工完成。

不管设备与其它设备一起形成 ISF，还是加入已有 ISF，如果该设备被当选为 Slave，则该设备会使用 Master 的配置重新初始化和启动，以保证和 Master 上的配置一致，而不管该设备在重新初始化之前有哪些配置、是否保存了当前配置。

2.2.3 ISF 聚合与分裂

ISF 聚合

ISF 成员聚合分两种情况：

- 设备上电重启加入，则该设备选为备或者从（由堆叠域中是否已经有备设备来决定，堆叠域中只能存在一台备设备）。例如：A 设备已经由堆叠协议选为主设备（上电后开启堆叠协议，如果未有新成员加入，则将自己选为主设备），此时 B 设备重启加入，将选为备（堆叠选举规则决定，详见堆叠选举规则第一条）。对外使用的 MAC 地址为 A 设备的 MAC 地址。
- 新加入的设备已经是主设备(堆叠协议已经运行完毕，再用堆叠线连接起来)，这时两台设备将发生竞争，竞争失败的一方将重启（设备默认开启分裂和合并自动重启功能，否则需要手工重启），然后作为备或从加入堆叠域中（原因是优先级低或运行时间短等），对外使用的 MAC 地址为主设备的 MAC 地址。堆叠设备之间可以设置 MAC 同步，缺省情况下，MAC 同步处于关闭状态。

ISF 聚合后，对外呈现为主设备的 MAC 地址，备设备、从设备只负责转发工作并将管理报文与协议报文转发给主设备。

形成稳定的堆叠系统后，主设备将进行批量备份，此时主设备会将自己的配置下发到备从设备上，保证主备从有相同环境。

批量备份后，将进行实时备份。主设备负责业务处理，备设备与从设备负责主设备的备份。在堆叠系统运行过程中进行严格的配置与数据的同步，实时将配置和数据可靠的传给备设备与从设备，这样当主设备出现问题时，备设备将经过约 15 秒后替代为主设备，这样当提高系统的稳定性。

ISF 分裂

ISF 成员分裂也分两种情况：

- 相邻设备间会定期发送心跳报文，如果持续多个周期没有收到邻居的心跳报文时（10 个周期），会认为邻居离开堆叠域中，将会重新生成拓扑。
- 如果发现堆叠口 Down 时，会进行重新选举，生成新的拓扑：如果是主设备离开，备设备将会优先选为主设备；如果是备设备离开，将会由从设备中重新选举出一个备设备；如果是从设备离开，将不会影响其他设备的角色。

分裂后，相连的两台设备，将删除对方有关的物理接口。两台设备将会独立开来，独立设备不需重启，配置不需要重新配置。

ISF 分裂后，对外呈现为各个设备的 MAC 地址，原来的备设备、从设备不在负责将管理报文与协议报文转发给原主设备。

2.2.4 ISF 的管理与维护

角色选举完成之后，ISF 形成，所有的成员设备组成一台虚拟的设备存在于网络中，所有成员设备上的资源归该虚拟设备拥有并由 Master 统一管理。

成员编号

在运行过程中，ISF 使用成员编号（Member ID）来标志和管理成员设备。例如 ISF 中接口的编号会加入成员编号信息：当设备处于独立运行模式时，接口编号格式（如 tengigabitethernet1/1/1）加入 ISF 后 ，接口编号会变（如 tengigabitethernet2/1/1）。所以，在 ISF 中必须保证所有设备成员编号的唯一性，否则不能建立 ISF。

ISF 拓扑维护

如果某成员设备 A Down 或者 ISF 链路 Down，其邻居设备会立即将“成员设备 A 离开”的信息广播通知给 ISF 中的其它设备。获取到离开消息的成员设备会根据本地维护的 ISF 拓扑信息表来判断离开的是 Master 还是 Slave，如果离开的是 Master，则触发新的角色选举，再更新本地的 ISF 拓扑；如果离开的是 Slave，则直接更新本地的 ISF 拓扑，以保证 ISF 拓扑能迅速收敛。

说明

ISF 端口的状态由与它绑定的 ISF 物理端口的状态决定。与 ISF 端口绑定的所有 ISF 物理端口状态均为 Down 时，ISF 端口的状态才会变成 Down。

MAD

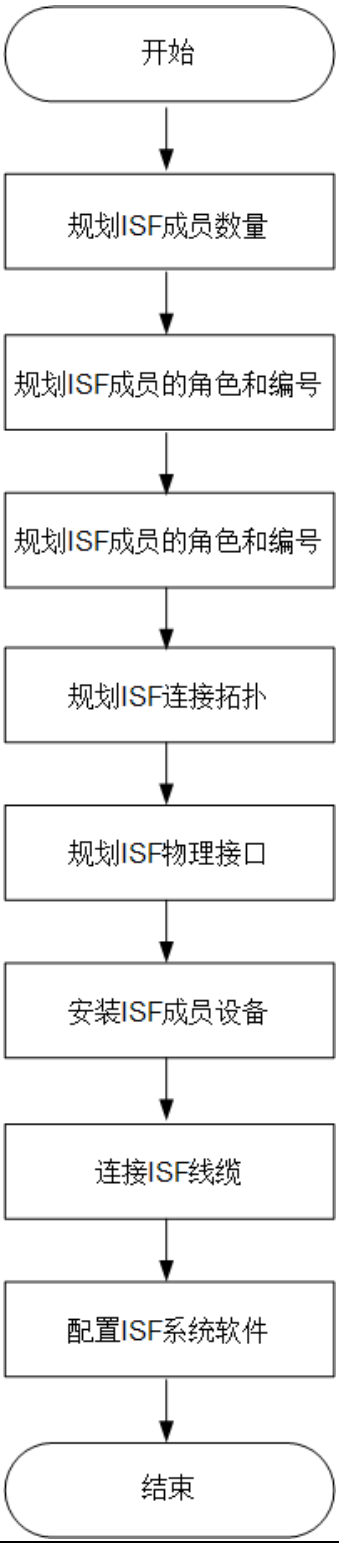
MAD（Multi-Active Detection，多 Active 检测）是一种检测和处理机制。当 ISF 链路故障时，会导致一个 ISF 变成两个新的 ISF。这两个 ISF 拥有相同的 IP 地址，会引起地址冲突，导致故障在网络中扩大。为了提高系统的可用性，当 ISF 分裂时我们就需要一种机制，能够检测出网络中同时存在多个 ISF，并进行相应的处理尽量降低 ISF 分裂对业务的影响，让分裂前的主设备一侧的堆叠系统正常工作。它主要提供以下功能：

- 分裂检测：通过 BFD（Bidirectional Forwarding Detection，双向转发检测）来检测网络中是否存在多个 ISF。
- 冲突处理：ISF 分裂后，通过分裂检测机制 ISF 会检测到网络中存在其它处于 Active 状态（表示 ISF 处于正常工作状态）的 ISF。冲突处理会让主设备 Unit 编号最小的 ISF 继续正常工作，其它 ISF 会迁移到 Recovery 状态（表示 ISF 处于禁用状态），并关闭 Recovery 状态 ISF 中所有成员设备上除保留端口以外的其它所有物理端口，以保证该 ISF 不能再转发业务报文。
- MAD 故障恢复：ISF 链路故障导致 ISF 分裂，从而引起冲突。因此修复故障的 ISF 链路，让冲突的 ISF 重新合并为一个 ISF，就能恢复 MAD 故障。如果在 MAD 故障恢复前，处于 Recovery 状态的 ISF 也出现了故障，则需要将故障 ISF 和故障链路都修复后，才能让冲突的 ISF 重新合并为一个 ISF，恢复 MAD 故障；如果在 MAD 故障恢复前，故障的是 Active 状态的 ISF，则可以通过命令行先启用 Recovery 状态的 ISF，让它接替原 ISF 工作，以便保证业务尽量少受影响，再恢复 MAD 故障。

2.3 搭建 ISF 环境

搭建 ISF 环境的具体流程如图 2-7，建议您提前规划好 ISF 配置方案，再进行设备的安装，以使设备安装位置便于 ISF 线缆的物理连接。

图2-7 搭建 ISF 环境流程图



2.3.2 规划 ISF 成员设备数量

将多台设备组成 ISF 后，ISF 能提供的交换容量为各成员设备的交换容量之和，请根据网络的接入和上行需求确定需要组成 ISF 的设备数量和型号，一个 ISF 系统中最多允许拥有 9 台成员设备。

2.3.3 规划 ISF 成员设备的角色和编号

确定 Master 设备

用户可以根据实际需要，将自己期望的设备的成员优先级配置为较大值，当多台设备初次形成 ISF 时，该设备就能在角色选举中获胜，成为 Master。

确定成员设备的编号

ISF 系统在运行过程中，使用成员编号（Member ID）来标识和管理成员设备。请您在将设备加入 ISF 前，统一规划、配置设备的成员编号，以保证 ISF 中成员编号的唯一性。

2.3.4 规划 ISF 连接拓扑

ISF 支持链形连接和环形连接两种拓扑，环形连接比链形连接更可靠。因此建议用户使用环形连接方式。

2.3.5 规划 ISF 物理端口

每个 ISF 接口最多可以绑定 8 个物理接口，建议将每个 ISF 端口至少绑定 2 个物理端口，以提高 ISF 端口的带宽以及可靠性。连接相邻两台成员设备的 ISF 端口下，绑定的 ISF 物理端口数目应保持一致，以使两台设备之间的 ISF 物理端口能一一互连，如 Device A 的 ISF-Port2 绑定的 ISF 物理端口数量应和 Device B 的 ISF-Port1 上绑定的 ISF 物理端口数量保持一致。

在独立运行模式下，将设备的某个物理端口作为 ISF 物理端口，当设备切换到 ISF 模式后，该物理端口原先配置的业务都将失效。用户需提前规划，确保原先业务不受影响。

2.3.6 安装 ISF 成员设备

在规划好 ISF 方案之后，请根据具体规划安装 ISF 成员设备。

2.3.7 连接 ISF 线缆

使用以太网光口作为 ISF 物理端口，则需要在光口上安装适用的可插拔接口模块、再通过光纤连接。

2.3.8 配置 ISF 系统软件

完成 ISF 成员设备的安装后，启动交换机。请分别登录各 ISF 成员设备进行 ISF 系统软件配置。请根据 ISF 的网络规划，进行 ISF 系统软件配置。

2.4 ISF 配置

ISF 有两种配置方式：预配置方式和非预配置方式。采用预配置方式，整个 ISF 配置过程设备只需要重启一次，所以推荐采用预配置的方式配置 ISF。

2.4.1 配置准备

场景

建立 ISF 前，确保多台设备的系统工作模式必须相同，否则不能形成 ISF。

确保每台设备编号不一致。

前提

要形成一个 ISF，需要将成员设备的物理接口先进行连接。

2.4.2 ISF 的缺省配置

设备上 ISF 的缺省配置如下。

功能	缺省值
堆叠模式	单机模式
Unit 编号	1
域编号	0
优先级	0
自动升级功能	禁用
自动合并功能	使能

2.4.3 预配置方式

该方式是在独立运行模式的设备上配置 ISF 端口、成员编号、成员优先级，这些配置不会影响本设备的运行，只有设备切换到 ISF 模式下才会生效。在组建 ISF 前，通常使用该方式配置。将成员优先级配置为较大值，当多台设备初次形成 ISF 时，该设备就能在角色选举中获胜，成为 Master；配置 ISF 端口，以便将运行模式切换到 ISF 模式后，就能直接和别的设备形成 ISF（最终组成 ISF 只需要一次重启）。

配置任务		说明
配置 ISF 端口	配置 ISF 端口	必选
	配置成员编号	必选
	配置成员优先级	可选
配置 ISF 模式		必选
ISF 模式下配置 ISF	配置 ISF 的桥 MAC 保留时间	可选
	使能 ISF 合并自动重启功能	可选
	使能 ISF 系统启动文件的自动加载功能	可选
	MAD 配置	可选

2.4.4 非预配置方式

该方式是在独立运行模式的设备上配置成员编号，然后切换到 ISF 模式，再配置 ISF 端口、成员优先级等相关参数（整个过程设备需要多次重启）。该配置方式通常用于修改当前配置。比如，将某个成员设备的编号修改为指定值（请注意修改后的编号需要重启该成员设备才能生效，而且重启后会导致原编号相关配置失效）；修改成员设备的优先级，让该设备在下次 ISF 竞选时成为 Master；修改 ISF 端口的已有绑定关系（删除某个绑定或者添加新的绑定），ISF 端口的配置可能会影响本设备的运行（比如引起 ISF 分裂、ISF 合并）。

配置任务		说明
独立运行模式下配置 ISF 成员编号		必选
配置 ISF 模式		必选
ISF 模式下配置 ISF	配置 ISF 的桥 MAC 保留时间	可选
	使能 ISF 合并自动重启功能	可选
	使能 ISF 系统启动文件的自动加载功能	可选
	MAD 配置	可选

2.5 独立运行模式下预配置 ISF

为了在运行模式切换后能直接与其它设备形成 ISF，可以在独立运行模式下预配置 Unit 编号、成员优先级、成员域 ID 以及 ISF 接口。这些参数配置在独立运行模式下并不生效，需要设备重启切换到 ISF 模式后才会生效。

2.5.1 配置 ISF 接口

ISF 端口是一个逻辑概念，创建 ISF 接口并与物理接口绑定后，此物理接口就是 ISF 物理接口，可以与另一台设备建立 ISF 连接。一个 ISF 接口最多可以与 8 个物理接口绑定，可以通过多次执绑定命令实现。这种聚合而成的 ISF 接口称为聚合 ISF 接口。这样两台设备间最多可以通过 16 条以太网线或者光纤来连接，从而提高 ISF 端口的带宽以及 ISF 接口的可靠性。

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#interface isf-port` *interface-number*	创建堆叠接口，并进入堆叠接口配置模式。
3	`Inspur(config-isf-port1/1/*)#isf port-group` *interface-type interface-number* `Inspur(config-isf-port1/1/*)#exit`	将物理接口与堆叠接口绑定。

说明

请将该配置保存到下次启动配置文件，以便设备切换到 ISF 模式时选择转换下次配置文件，该配置能够生效。

在独立运行模式下将 ISF 接口和 ISF 物理接口绑定，并不会影响 ISF 物理接口的当前业务。当设备切换到 ISF 模式后，物理接口的配置将恢复到缺省状态 ISF（即原有的业务配置会被删除）。

出厂时，设备处于独立运行模式，没有成员编号。必须配置成员编号后，才能将设备从独立运行模式切换到 ISF 模式。用户可以使用 **show isf configuration** 命令查看成员编号，同时为了避免加入 ISF 时与别的成员设备编号冲突，需预先规划 ISF 的编号方案。

2.5.2 配置成员编号

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**isf renumber** *number*	（可选）修改 Unit 编号，将原有的 Unit 编号修改为新的 Unit 编号。

在 ISF 中以成员编号标识设备，ISF 接口和成员优先级的配置也和成员编号紧密相关。所以，修改设备成员编号可能导致配置发生变化或者丢失，请慎重使用。

该命令的配置结果可以通过 **show isf configuration** 回显信息中的 next unit 查看，而不在 **show running** 的回显信息中查看。

2.5.3 配置成员优先级

成员优先级用于角色选举，优先级高的设备竞选时成为 Master 的可能性越大。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**isf priority** *priority-number*	配置设备优先级。

2.5.4 配置 ISF 模式

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**isf-mode single** Set successfully. The device will switch to single mode , take effect after reboot	配置堆叠模式。

当配置命令行完成时，系统会提示“Set successfully. The device will switch to single mode ，take effect after reboot”，如果不需要重启，可以输入“**no**”，系统将不会重启，可以继续进行其他配置。

2.6 ISF 模式下配置 ISF

2.6.1 配置 ISF 模式

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#isf mode isf`	配置堆叠模式。

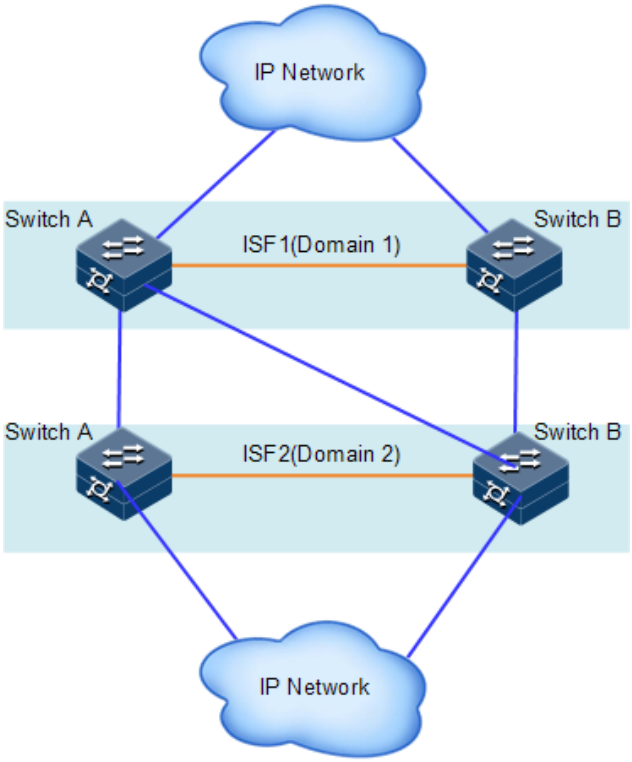
说明

当配置命令行完成时，系统会提示“Set successfully. The device will switch to isf mode ，take effect after reboot”，如果不需要重启，可以输入“**no**”，系统将不会重启，可以继续进行其他配置。

2.6.2 配置 ISF 域编号

域是一个逻辑概念，设备通过 ISF 链路连接在一起就组成一个 ISF，这些成员设备的集合就是一个 ISF 域。为了适应各种组网应用，同一个网络里可以部署多个 ISF，ISF 之间使用域编号（DomainID）来以 Device A 和 Device B 组成 ISF1，Switch A 和 Switch B 组成 ISF2。如图 2-8 所示，如果 ISF1 和 ISF2 之间有 MAD 检测链路，则 ISF1 和 ISF2 会通过检测链路互相发送 MAD 检测报文，从而彼此影响 ISF 系统的状态和运行。这种情况下，可以给两个 ISF 配置不同的域编号，以保证两个 ISF 互不干扰。

图2-8 多 ISF 域示意图



请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur_1#config`	进入全局配置模式。
2	`Inspur_1(config)#isf unit` *number* `domain` *domain-number*	配置域编号。

2.6.3 配置 ISF 端口

多台设备切换到 ISF 模式后，创建各自的 ISF 接口，并将 ISF 接口与各自的物理接口绑定，形成 ISF 物理接口。最后，用 ISF 线缆分别连接到多台设备的 ISF 物理接口，设备的 ISF 功能才能生效。一台成员设备上的 ISF-Port1（ISF 模式下表示为：ISF-Port2/1/1）端口只能和另一台成员设备 ISF-Port2（ISF 模式下表示为：ISF-Port2/1/2）端口相连。

一个 ISF 端口最多可以与 8 个物理接口绑定，可以通过多次执行 **isf port-group** 命令实现。这种聚合而成的 ISF 端口称为聚合 ISF 端口。这样两台设备间最多可以通过 16 根以太网线或者光纤来连接，从而提高 ISF 端口的带宽以及 ISF 端口的可靠性。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur_1#**config**	进入全局配置模式。
2	Inspur_1(config)#**interface isf-port** *interface-number*	进入堆叠接口配置模式，并创建堆叠接口。
3	Inspur_1(config-isf-port1/1/*)#**isf port-group** *interface-type interface-number*	将物理接口与堆叠接口绑定。

说明

在将物理接口加入 ISF 端口后，该物理端口原先配置的业务都将失效。用户需提前规划，确保原先业务不受影响。

多次执行 **isf port-group**，可以将 ISF 端口与多个 ISF 物理端口绑定，以实现 ISF 链路的备份/负载分担，从而提高 ISF 链路的带宽和可靠性。一个 ISF 端口最多可以与 8 个物理端口绑定。当绑定的物理端口数达到上限时，该命令将执行失败。

将设备上的物理端口和 ISF 端口进行绑定或取消绑定后，必须用 **write** 命令保存配置到下次启动配置文件，否则下次启动时此配置无效。

2.6.4 配置成员编号

ISF 通过成员编号唯一的识别各成员设备，设备上的许多信息、配置与成员编号相关，比如接口（包括物理接口和逻辑接口）的编号以及接口下的配置、成员优先级的配置等。

- 修改成员编号后，但是没有重启本设备，则原编号继续生效，各物理资源仍然使用原编号来标识；配置文件中，只有 ISF 端口的编号以及 ISF 端口下的配置、成员优先级的配置会跟着改变，其它配置均不会跟着改变。
- 修改成员编号后，如果保存当前配置，重启本设备，则新的成员编号生效，需要用新编号来标识物理资源；配置文件中，只有 ISF 端口的编号以及 ISF 端口下的配置、成员优先级会继续生效，其它与成员编号相关的配置（比如普通物理接口的配置、chassis 参数值等于原成员编号的配置等）不再生效，需要重新配置。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur_1#**config**	进入全局配置模式。
2	Inspur_1(config)#**isf unit** *old-number* **renumber** *new-number*	修改 Unit 编号，将原有的 Unit 编号修改为新的 Unit 编号。

说明

需要重启设备，新成员编号 *new-member-id* 才能生效。

在 ISF 中以成员编号标识设备，ISF 接口和成员优先级的配置也和成员编号紧密相关。所以，修改设备成员编号可能导致配置发生变化或者丢失，请慎重使用。

该命令的配置结果可以通过 **show isf configuration** 回显信息中的 next unit 查看，而不在 **show running** 的回显信息中查看。

2.6.5 配置成员优先级

成员优先级用于角色选举，优先级高的设备竞选时成为 Master 的可能性越大。

步骤	配置	说明
1	`Inspur_1#config`	进入全局配置模式。
2	`Inspur_1(config)#isf unit` *number* `priority` *priority-number*	配置成员设备优先级。

2.6.6 配置 ISF 的桥 MAC 保留时间

桥 MAC 是设备作为网桥与外界通信时使用的 MAC 地址。一些二层协议（例如 LACP）会使用桥 MAC 标识不同设备，所以网络上的桥设备必须具有唯一的桥 MAC。如果网络中存在多台桥 MAC 相同的设备，则会引起桥 MAC 冲突，从而导致通信故障。

ISF 作为一台虚拟设备与外界通信，也具有唯一的桥 MAC，称为 ISF 桥 MAC。通常情况下使用 Master 设备的桥 MAC 作为 ISF 桥 MAC。

因为桥 MAC 冲突会引起通信故障，桥 MAC 的切换又会导致流量中断。因此，用户需要根据网络实际情况配置 ISF 桥 MAC 的保留时间：

- 如果配置 ISF 桥 MAC 地址保留时间为 10 分钟。即当 Master 离开 ISF 时，ISF 桥 MAC 地址 10 分钟内保持不变化；如果 10 分钟后 Master 没有回到 ISF，则使用新选举的 Master 的桥 MAC 作为 ISF 桥 MAC。该配置适用于 Master 设备短时间内离开又回到 ISF 的情况（比如 Master 重启或者链路临时故障等），可以减少不必要的桥 MAC 导致的流量中断。
- 如果配置了 ISF 桥 MAC 地址保留时间为永久，则不管 Master 设备是否离开 ISF，桥 MAC 始终保持不变。
- 如果配置了 ISF 桥 MAC 地址不保留，则当 Master 设备离开 ISF 时，系统立即会使用新选举的 Master 设备的桥 MAC 做 ISF 桥 MAC。

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur_1#config`	进入全局配置模式。

步骤	配置	说明
2	Inspur_1(config)#**isf mac-address persistent always**	配置当 Master 设备离开 ISF 时，ISF 的桥 MAC 地址会永久保留。
3	Inspur_1(config)#**isf mac-address persistent timer**	配置当 Master 设备离开 ISF 时，ISF 的桥 MAC 地址的保留时间为 10 分钟。
4	Inspur_1(config)#**no isf mac-address persistent**	配置当 Master 设备离开 ISF 时，ISF 的桥 MAC 地址不保留，会立即变化。

说明

桥 MAC 变化可能会导致流量短时间中断。

如果两个 ISF 的桥 MAC 相同，则它们不能合并为一个 ISF。

在 ISF 模式下使用 VRRP 负载均衡功能时，须配置 ISF 的桥 MAC 地址为永久保留（缺省情况下，ISF 的桥 MAC 地址为永久保留）。

2.6.7 配置 MAC 地址同步

在堆叠情况下，交换机端口退出 VLAN 后，会删除端口下该 VLAN 对应的 MAC 地址；端口所在成员交换机在删除 MAC 过程中，如果接收到其他成员交换机同步过来的 MAC 是不作处理的，直到 MAC 删除结束，在配置的同步时间周期后，如果再接收到同步过来的 MAC，才接收处理，插入到本交换机 MAC 表项中。

步骤	配置	说明
1	Inspur_1#**config**	进入全局配置模式。
2	Inspur_1(config)#**mac-address synchronizing enable**	堆叠模式下或双芯片设备中，使能 MAC 地址同步功能。
3	Inspur_1(config)#**mac-address synchronizing long-interval** *time*	堆叠模式下或双芯片设备中，配置 MAC 地址同步周期。

2.6.8 配置堆叠设备重启

在堆叠模式下，配置堆叠设备重启功能。如果配置的重启设备为 Master 设备，那么 Backup 设备将成为新的 Master 设备。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur_1#**isf reboot** *number*	重新启动堆叠状态中的某一台设备。

2.6.9 配置远程连接设备

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur_1#isf connect` *number*	通过串口方式可以远程连接到其它设备。

说明

该命令应用在 Master 设备对应的串口上，并且只能连接到堆叠系统中非 Master 设备的成员串口上。

2.6.10 配置平滑升级

平滑升级是指在堆叠系统上行及下行链路形成备份的组网中，将堆叠系统中主设备和备设备分为两个相互备份的流量区域。使能升级功能后，主设备和备设备依次进行升级，以保证其中一个设备的流量不会中断，从而减少升级对业务造成的影响。平滑升级方式适用于对业务中断时间要求较高的场景。

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur_1#isf upgrade start`	使能堆叠平滑升级功能。

说明

在进行堆叠平滑升级功能时要注意以下几点：

采集并备份设备信息。

升级堆叠系统中 Master 设备和非 Master 设备的系统镜像文件，建议在 Master 设备上进行操作。

检查升级后的业务恢复情况。

对配置文件进行备份，以避免升级失败所导致的后果。

2.6.11 使能 ISF 自动合并功能

堆叠合并功能通常应用在堆叠链路故障或设备故障导致堆叠分裂的情况下。在堆叠链路或设备故障恢复后，分裂的堆叠系统成员会进行合并操作。如果此时自动合并功能使能，则堆叠系统能正常合并并形成新的堆叠系统，如果此时自动合并功能禁止，则无法形成新的堆叠系统。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur_1#**config**	进入全局配置模式。
2	Inspur_1(config)#**isf auto-merge { enable | disable }**	使能自动合并功能，使用 **disable** 命令禁用自动合并功能。

说明

堆叠系统正常运行的情况下不能修改自动合并功能的状态，要使其处于缺省状态，即使能状态。

目前默认方式是使能。

2.6.12 配置 MAD

MAD（Multi-Active Detection，多 Active 检测）是一种检测和处理机制。当 ISF 链路故障时，会导致一个 ISF 变成两个新的 ISF。这两个 ISF 拥有相同的 IP 地址，会引起地址冲突，导致故障在网络中扩大。为了提高系统的可用性，当 ISF 分裂时我们就需要一种机制，能够检测出网络中同时存在多个 ISF，并进行相应的处理尽量降低 ISF 分裂对业务的影响。

ISF 支持的 MAD 检测方式为 BFD MAD 检测和 ARP MAD 检测。

ARP MAD 检测简介

- ARP MAD 检测原理

ARP MAD 检测是通过扩展 ARP 协议报文来实现的，也就是说使用 ARP 协议报文中未使用的字段来交互 ISF 的 Active ID 和 Domain ID。ARP MAD 检测功能使能后，成员设备之间可以通过 ARP 协议报文交互 Active ID 和 Domain ID 信息。

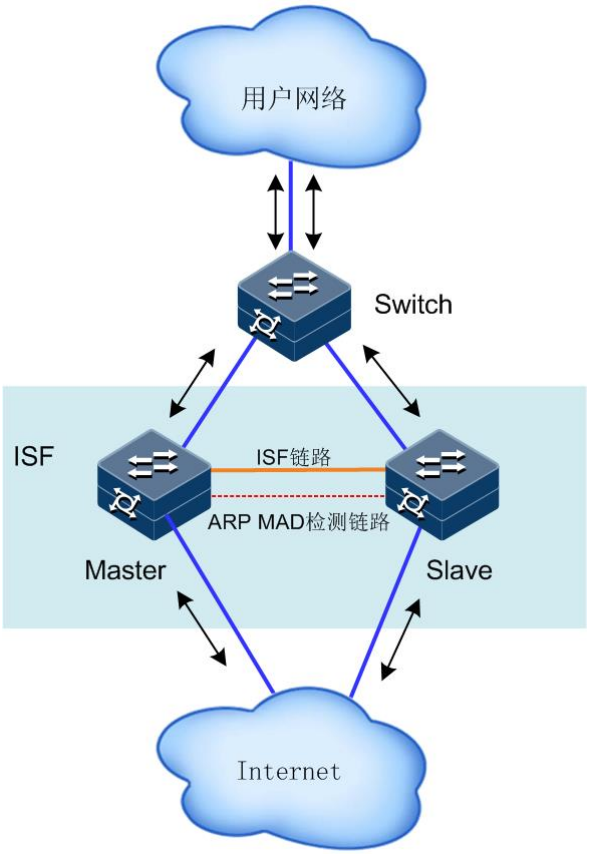
当成员设备收到 ARP 协议报文后，先比较 Domain ID。如果 Domain ID 相同，再比较 Active ID；如果 Domain ID 不同，则认为报文来自不同的 ISF，不再进行 MAD 处理。

如果 Active ID 相同，则表示 ISF 正常运行，没有发生多 Active 冲突；如果 Active ID 值不同，则表示 ISF 分裂，检测到多 Active 冲突。

- ARP MAD 检测组网要求

ARP MAD 检测方式可以通过中间设备进行连接，也可以不通过中间设备进行连接。通常采用如图 2-9 所示的组网：成员设备之间通过 Switch 交互 ARP 报文，Switch、Master 和 Slave 上都要配置生成树功能，以防止形成环路。

图2-9 ARP MAD 检测组网示意图



配置 ARP MAD 检测

ARP MAD 检测功能的配置顺序为：

步骤 1 创建一个新 VLAN，专用于 ARP MAD 检测（如果用到中间设备组网，中间设备上也需要进行该项配置）。

步骤 2 确定使用哪些物理接口用作 ARP MAD 检测，并将这些端口都添加到 ARP MAD 检测专用 VLAN 中（如果用到中间设备组网，中间设备上也需要进行该项配置）。

步骤 3 为 ARP MAD 检测专用 VLAN 创建 VLAN 接口，在接口下使能 ARP MAD 检测功能，并配置 MAD IP 地址。

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur_1#config`	进入全局配置模式。
2	`Inspur_1(config)#interface vlan` *`vlan-id`*	进入 VLAN 接口配置模式。
3	`Inspur_1(config-vlan*)#mad arp enable`	（可选）使能 MAD ARP 检测功能。

步骤	配置	说明
4	Inspur_1(config-vlan*)#**mad ip address** *ip-address* [*ip-mask*] **unit** *number*	（可选）配置堆叠中指定 Unit 的 MAD IP 地址。
5	Inspur_1(config)#**mad restore**	（可选）将 MAD 冲突检测后禁用的设备恢复到正常状态。

说明

当 ARP MAD 检测组网中使用中间设备进行连接时，可以使用普通的数据链路作为 ARP MAD 检测链路；当不使用中间设备时，需要在所有的成员设备之间建立两两互联的 ARP MAD 检测链路。

如果使用中间设备组网，在 ISF 和中间设备上均需配置 STP 功能。

使能 ARP MAD 检测功能后，所在 VLAN 需保留，不再用作其它用途。

BFD MAD 检测简介

- BFD MAD 检测原理

BFD MAD 检测是通过 BFD 协议来实现的。要使 BFD MAD 检测功能正常运行，除在 VLAN 接口下使能 BFD MAD 检测功能外，还需要在该接口上配置 MAD IP 地址。MAD IP 地址与普通 IP 地址不同的地方在 MAD IP 地址与成员设备是绑定的，ISF 中的每个成员设备上都需要配置，且必须属于同一网段。

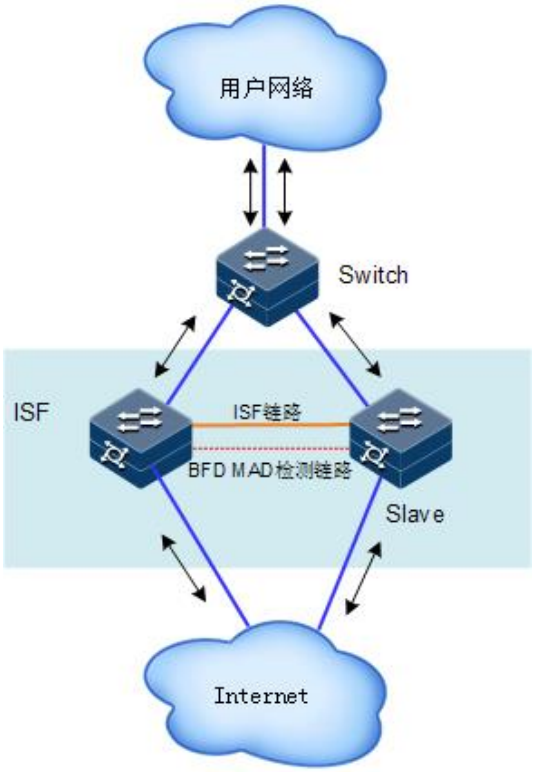
当 ISF 正常运行时，只有 Master 设备上配置的 MAD IP 地址生效，Slave 设备上配置的 MAD IP 地址不生效，BFD 会话处于 Down 状态；（使用 **show bfd state** 命令查看 BFD 会话的状态。如果 Session State 显示为 Up，则表示激活状态；如果显示为 Down，则表示处于 Down 状态）。

当 ISF 分裂后会形成多个 ISF，不同 ISF 中 Master 上配置的 MAD IP 地址均会生效，BFD 会话被激活，此时会检测到多 Active 冲突。

- BFD MAD 检测组网要求

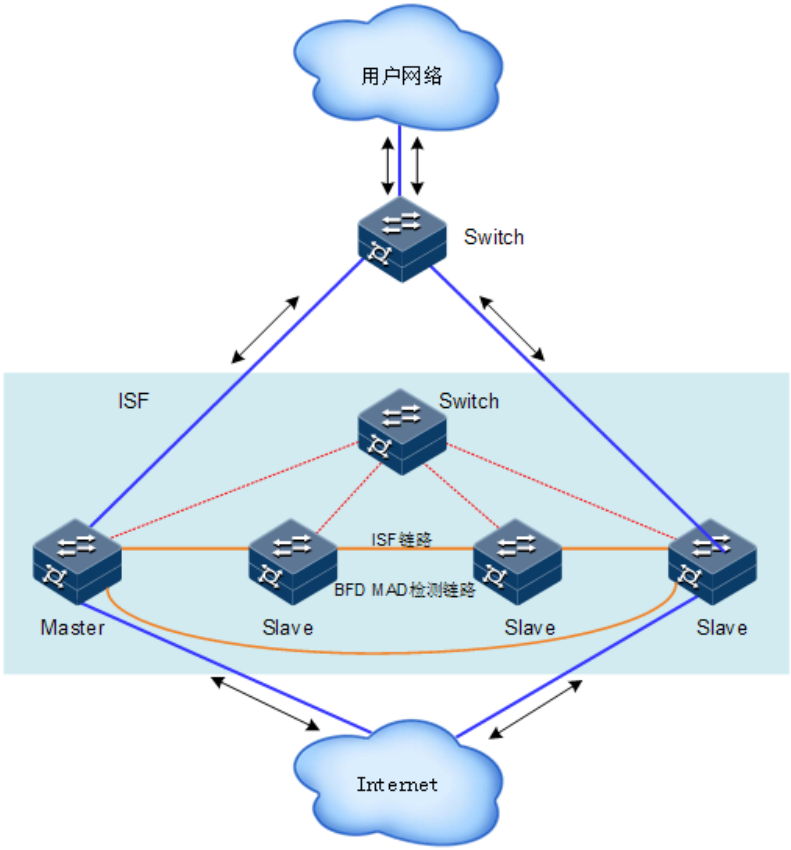
如果当前 ISF 系统中成员设备仅有两台，那么 BFD MAD 检测方式可以使用中间设备来进行连接，也可以不使用中间设备。通常采用如图 2-10 所示的组网方式：所有成员设备之间必须有一条 BFD MAD 检测链路，这些链路连接的接口必须属于同一 VLAN，在该 VLAN 接口配置模式下给不同成员设备配置同一网段下的不同 IP 地址。

图2-10 BFD MAD 检测组网示意图（不使用中间设备）



如果当前 ISF 系统中成员设备有 3 台或者 4 台，那么 BFD MAD 检测方式必须使用中间设备来进行连接，通常采用如图 2-11 所示的组网方式：所有成员设备之间必须有一条 BFD MAD 检测链路与中间设备 Swich 相连，这些链路连接的接口必须属于同一 VLAN，在该 VLAN 接口视图下给不同成员设备配置同一网段下的不同 IP 地址。

图2-11 BFD MAD 检测组网示意图（使用中间设备）



配置 BFD MAD 检测

BFD MAD 检测功能的配置顺序为：

步骤 1 创建一个新 VLAN，专用于 BFD MAD 检测（如果用到中间设备组网，中间设备上也需要进行该项配置）。

步骤 2 确定使用哪些物理接口用作 BFD MAD 检测（每台成员设备上至少一个），并将这些端口都添加到 BFD MAD 检测专用 VLAN 中（如果用到中间设备组网，中间设备上也需要进行该项配置）。

步骤 3 为 BFD MAD 检测专用 VLAN 创建 VLAN 接口，在接口下使能 BFD MAD 检测功能，并配置 MAD IP 地址。

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur_1#config`	进入全局配置模式。
2	`Inspur_1(config)#interface vlan` *`vlan-id`*	进入 VLAN 接口配置模式。
3	`Inspur_1(config-vlan*)#mad bfd enable`	使能 MAD BFD 检测功能。

步骤	配置	说明
4	Inspur_1(config-vlan*)#**mad ip address** *ip-address* [*ip-mask*] **unit** *number*	配置堆叠中指定 Unit 的 MAD IP 地址。
5	Inspur_1(config)#**mad restore**	（可选）将 MAD 冲突检测后禁用的设备恢复到正常状态。

说明

使能 BFD MAD 检测功能后，所在 VLAN 需保留，不再用作其它用途。

如果 BFD MAD 检测专用 VLAN 中包含 Trunk 端口，且此 Trunk 端口允许多个 VLAN 的报文通过，请确保 Trunk 端口的缺省 VLAN 与 BFD MAD 检测专用 VLAN 不相同，否则 Trunk 端口上配置的其他业务可能会受影响。

不能在 VLAN 1 接口上使能 BFD MAD 检测功能。

在用于 BFD MAD 检测的接口下必须使用 **mad ip address** 命令配置 MAD IP 地址，不能配置其它 IP 地址（包括使用 **ip address** 命令配置的普通 IP 地址、VRRP 虚拟 IP 地址等），以免影响 MAD 检测功能。

BFD MAD 检测功能与生成树功能互斥，在使能了 BFD MAD 检测功能的 VLAN 接口所对应 VLAN 内的物理接口上，请不要使能生成树协议。为了防止环路的产生，请用户确保在物理连接上不存在环路。

Mad IP 地址需要进行规划，避免与外部学习路由相互冲突。

配置保留接口

ISF 系统在进行多 Active 处理的时候，缺省情况下，会关闭 Recovery 状态 ISF 中的所有业务接口。如果接口有特殊用途需要保持 Up 状态（比如 Telnet 登录接口、用于 MAD 检测的接口等），则用户可以通过命令行将这些接口配置为保留接口。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur_1#**config**	进入全局配置模式。
2	Inspur_1(config)#**mad exclude interface** *interface-type interface-number*	配置保留接口，当设备进入 Recovery 状态时，该接口不会被关闭。

说明

ISF 物理端口和 Console 接口自动作为保留接口，不需要配置。

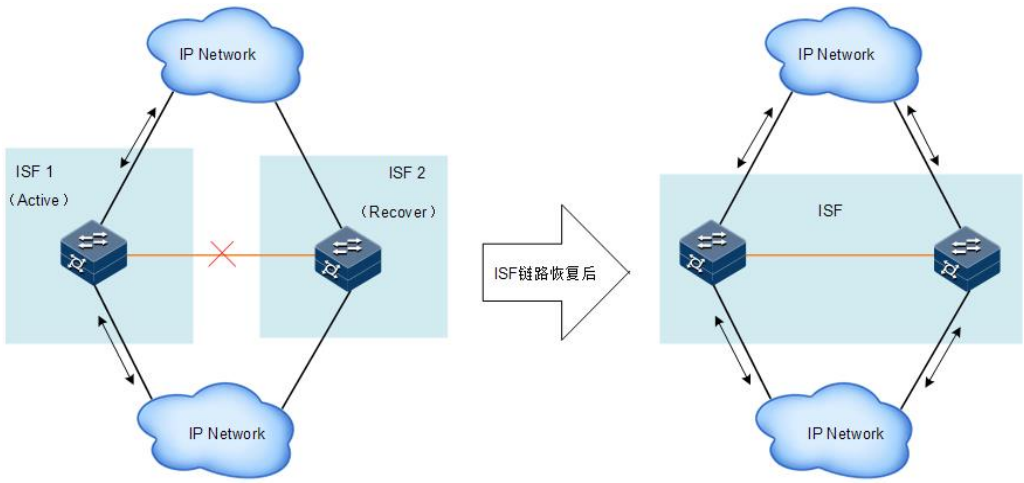
如果要求处于 Recovery 状态的 ISF 中的某个 VLAN 接口能够继续收发报文（比如使用该 VLAN 接口进行远程登录），则需要将该 VLAN 接口以及该 VLAN 接口对应的二层以太网接口都配置为保留接口。

MAD 故障恢复

ISF 链路故障将一个 ISF 分裂为两个 ISF，从而导致多 Active 冲突。当系统检测到多 Active 冲突后，两个冲突的 ISF 会进行竞选：首先比较两个 ISF 中的成员数量，成员数量多的获胜，继续正常运行，失败的 ISF 会转入 Recovery 状态，暂时不能转发业务报文；如果成员数量相同，则比较 Master 成员的编号，Master 优先级高的获胜，继续正常运行，失败的 ISF 转入 Recovery 状态，暂时不能转发业务报文。此时通过修复 ISF 链路可以恢复 ISF 系统（设备会尝试自动修复 ISF 链路，如果修复失败的话，则需要用户手工修复）。

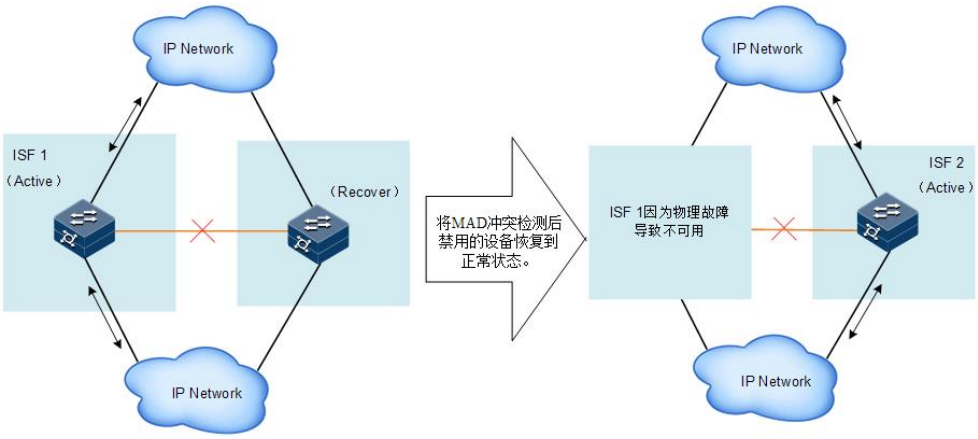
ISF 链路修复后，处于 Active 的 ISF 和处于 Recovery 状态的 ISF 将合并为一个 ISF：系统将提示需要重启指定 Recovery 状态的 ISF，完成重启后，Recovery 状态的 ISF 中被强制关闭的业务接口会自动恢复到真实的物理状态，整个 ISF 系统恢复。如图 2-12 所示。但如果用户重启的是处于 Active 状态的 ISF，则重启后两个 ISF 合二为一，需要手工执行 mad restore 命令使原 Recovery 状态的 ISF 中被强制关闭的业务接口恢复到真实的物理状态，整个 ISF 系统恢复。

图2-12 MAD 故障恢复（ISF 链路故障）



如果 MAD 故障还没来得及修复而处于 Active 的 ISF 也故障了（原因可能是设备故障或者上下行线路故障），如图 2-13 所示。此时可以在 ISF2（处于 Recovery 状态的 ISF）上执行 mad restore 命令，让 ISF2 恢复到正常状态，先接替 ISF 1 工作。然后再修复 ISF 1 和 ISF 链路，修复后，两个 ISF 发生合并，整个 ISF 系统恢复。

图2-13 MAD 故障恢复（ISF 链路故障和 Active 状态的 ISF 故障）



请在设备上进行以下配置。

步骤	配置	说明
1	Inspur_1#**config**	进入全局配置模式。
2	Inspur_1(config)#**mad restore**	将 MAD 冲突检测后禁用的设备恢复到正常状态。

2.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur_1#**show isf**	查看所有收集到的堆叠信息。
2	Inspur_1#**show isf topology**	查看堆叠拓扑结构信息。
3	Inspur_1#**show isf packet**	查看堆叠报文统计信息。
4	Inspur_1#**show isf configuration**	查看 ISF 预配置信息。
5	Inspur_1#**show isf mac-address persistent**	查看堆叠的桥 MAC 保留时间信息。
6	Inspur_1#**show isf state [unit** *number*]	查看堆叠状态信息。
7	Inspur_1#**show mad info**	查看 MAD 配置信息和运行状态。
8	Inspur_1#**show mac-address synchronizing config**	查看 MAC 地址同步配置信息。

2.8 ISF 典型配置举例

说明

以下配置举例以 S6550-24 口设备进行举例说明。

2.8.1 ISF 典型配置举例（采用预配置方式配置 ISF，检测方式为 BFD MAD）

组网需求

由于网络规模迅速扩大，当前中心交换机（Device A）转发能力已经不能满足需求，现需要在保护现有投资的基础上将网络转发能力提高一倍，并要求网络易管理、易维护。

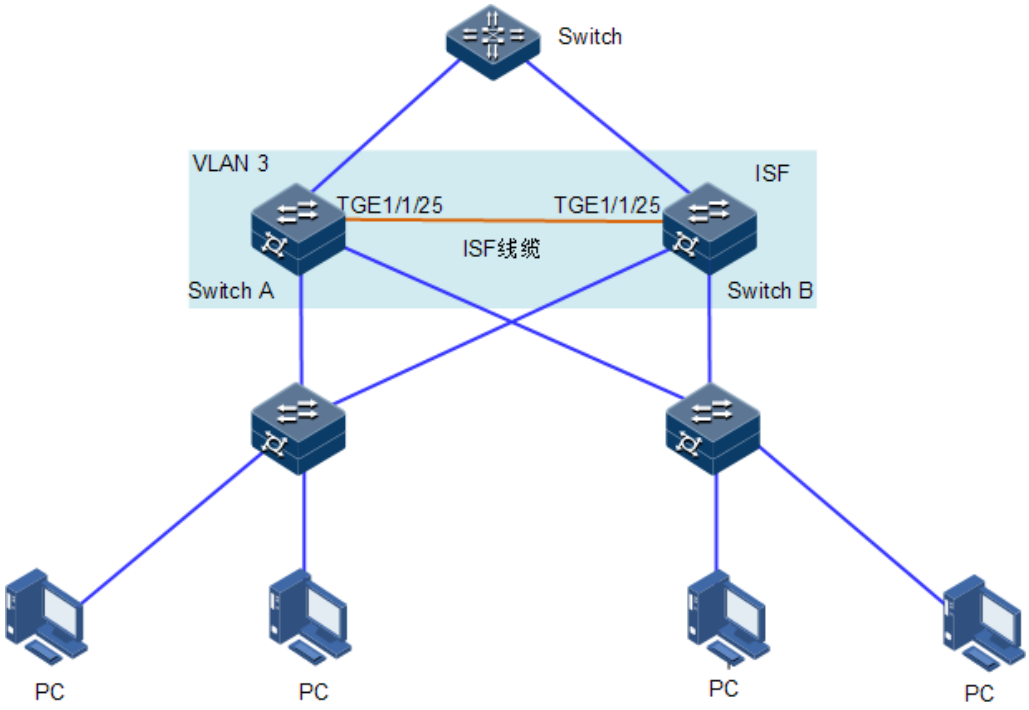
配置思路

为了将 Device A 的转发能力提高一倍，需要另外增加一台设备 Device B。即在 Device A 和 Device B 上配置 ISF 功能。

为了防止万一 ISF 链路故障导致 ISF 分裂、网络中存在两个配置冲突的 ISF，需要启用 MAD 检测功能。采用 BFD MAD 检测方式来监测 ISF 的状态。

组网图

图2-14 ISF 典型配置组网图（BFD MAD 检测方式）



配置步骤

步骤 1 单机模式下配置。

- 配置 Device A。

设置 Device A 的成员编号为 1，成员优先级为 12，创建 ISF 接口 1，并将它与物理端接口 Tengigabitethernet1/1/25 绑定。

```
Inspur#config
Inspur(config)#isf renumber 1
Inspur(config)#isf priority 12
Inspur(config)#interface tengigabitethernet 1/1/25
Inspur(config-tengigabitethernet1/1/25)#portswitch
Inspur(config-tengigabitethernet1/1/25)#exit
Inspur(config)#interface isf-port 1/1/1
Inspur(config-isf-port1/1/1)#isf port-group tengigabitethernet 1/1/25
Inspur(config-isf-port1/1/1)#exit
Inspur(config)#exit
```

将当前配置保存到下次启动配置文件。

```
Inspur#write
```

将设备的运行模式切换到 ISF 模式。

```
Inspur#config
Inspur(config)#isf mode isf
next unit is: 9, please input 'yes':yes
```

```
This configuration will go into effect after reboot, Please input 'yes'
to reboot:yes
Will you change start-config ? please input 'yes' to change:yes

1970-01-01,08:06:46 System-4-SYSTEM_REBOOT:unit1: Change work Mode
reboot !
Operation successfully
Inspur(config)#
BOOTROM starting ..
```

设备重启后 Device A 组成了只有一台成员设备的 ISF。

- 配置 Device B。

配置 Device B 的成员编号为 2，成员优先级为 26，创建 ISF 端口 1，并将它与物理接口 Tengigabitethernet1/1/25 绑定。

```
Inspur#config
Inspur(config)#isf renumber 2
Member ID change will take effect after the switch reboots and work in
ISF mode
Will you change start-config ? please input 'yes' to change:no
Inspur(config)#isf priority 26
Inspur(config)#interface  tengigabitethernet 1/1/25
Inspur(config-tengigabitethernet1/1/25)#portswitch
Inspur(config)#interface isf-port 1/1/1
Inspur(config-isf-port1/1/1)#isf port-group tengigabitethernet 1/1/25
Inspur(config)#exit
```

将当前配置保存到下次启动配置文件。

```
Inspur#write
```

将设备的运行模式切换到 ISF 模式。

```
Inspur#config
Inspur(config)#isf mode isf
next unit is: 2, are you sure ? please input 'yes':yes
This config reboot go into effect, Please input 'yes' to reboot:yes
Will you change start-config ? please input 'yes' to change:yes
1970-01-01,08:10:05 System-4-SYSTEM_REBOOT:unit1: Change work Mode
reboot !
Operation successfully
Inspur(config)#
BOOTROM starting ..
```

步骤 2 ISF 模式下配置：

配置 BFD MAD 检测。

- 配置 Device A。

创建 VLAN 3，并配置 MAD IP 地址，将 Device A（成员编号为 1）使能 BFD MAD 检测。

```
Inspur_1#config
Inspur_1(config)#create vlan 3 active
Inspur_1(config)#interface vlan 3
```

```
Inspur_1(config-vlan3)#mad ip address 192.168.2.1 unit 1
Inspur_1(config-vlan3)#mad bfd enable
1970-01-01,08:17:21 BFD-5-BFD_SESSIONID_DOWN:unit1: Bfd session 65 is
down.#
```

- 配置 Device B。

创建 VLAN 3，并配置 MAD IP 地址，将 Device B（成员编号为 2）使能 BFD MAD 检测。

```
Inspur_2#config
Inspur_2(config)#create vlan 3 active
Inspur_2(config)#interface vlan 3
Inspur_2(config-vlan3)#mad ip address 192.168.2.2 unit 2
Inspur_2(config-vlan3)#mad bfd enable
1970-01-01,08:17:21 BFD-5-BFD_SESSIONID_DOWN:unit1: Bfd session 65 is
down.#
```

2.8.2 ISF 典型配置举例（采用非预配置方式配置 ISF，检测方式为 BFD MAD）

组网需求

由于网络规模迅速扩大，当前中心交换机（Device A）转发能力已经不能满足需求，现需要在保护现有投资的基础上将网络转发能力提高一倍，并要求网络易管理、易维护。

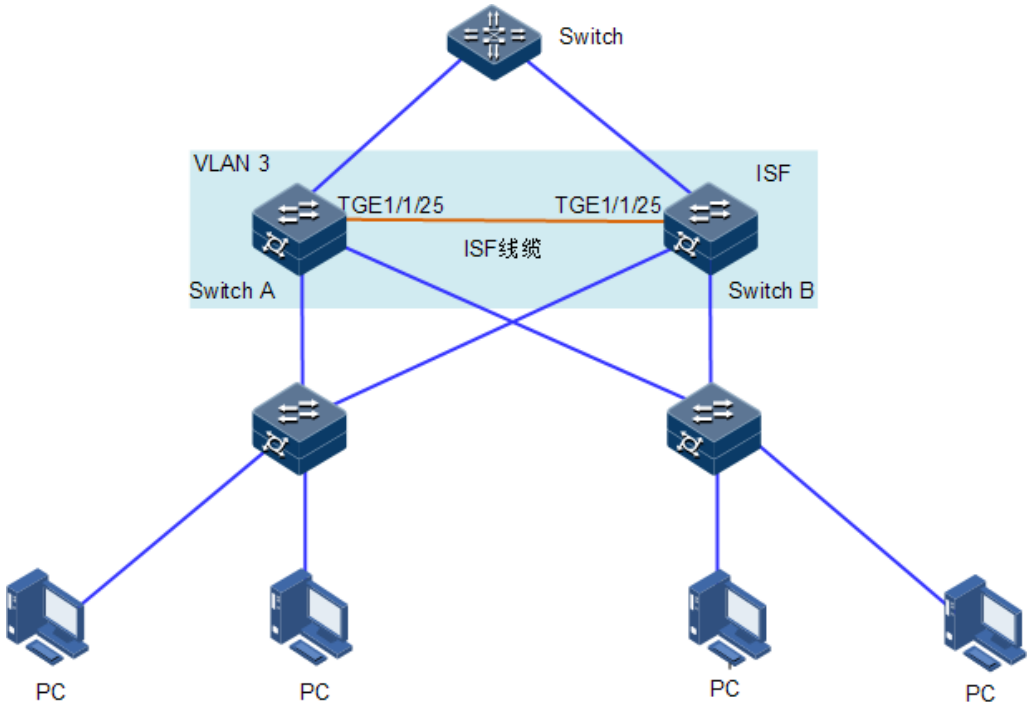
配置思路

断开 ISF 连接。可以直接将 ISF 物理连接线缆拔出也可以使用命令行关闭 Master 设备上所有的 ISF 物理端口。本举例采用命令行关闭的方式。

ISF 分裂后，分别将两台成员设备从 ISF 模式切换到独立运行模式。

组网图

图2-15 成员设备从 ISF 模式恢复到独立运行模式组网图



配置步骤

- 确定 Master 设备。

```
Inspur_1#show isf
Inspur_1(config)#isf renumber 1
Inspur_1(config)#isf mode isf
next unit is: 1, are you sure ? please input 'yes':yes
This config reboot go into effect, Please input 'yes' to reboot:yes
1970-01-01,08:07:17 System-4-SYSTEM_REBOOT:unit1: Change work Mode
reboot !
BOOTROM starting ..
```

配置 ISF 端口 1/1/1，并将它与物理端口 Tengigabitethernet 1/1/25 绑定。

```
Inspur_1(config)#interface tengigabitethernet 1/1/25
Inspur_1(config-tengigabitethernet1/1/25)#portswitch
Inspur_1(config-tengigabitethernet1/1/25)#exit
Inspur_1(config)#interface isf-port 1/1/1
Inspur_1(config-isf-port1/1/1)#isf port-group tengigabitethernet 1/1/25
Inspur_1(config-isf-port1/1/1)#exit
Inspur_1(config)#isf unit 1 priority 64
Inspur_1(config)#exit
```

将当前配置保存到下次启动配置文件。

```
Inspur_1#write
```

- 配置 Device B。

将 Device B 的运行模式切换到 ISF 模式。

```
Inspur_1#config
Inspur_1(config)#isf renumber 2
Inspur_1(config)#isf-mode isf
next unit is: 2, are you sure ? please input 'yes':yes
This config reboot go into effect, Please input 'yes' to reboot:yes
1970-01-01,08:07:17 System-4-SYSTEM_REBOOT:unit1: Change work Mode
reboot !
BOOTROM starting ..
```

配置 ISF 端口 1/1/1，并将它与物理端口 Tengigabitethernet 1/1/25 绑定。

```
Inspur_2(config)#interface tengigabitethernet 1/1/25
Inspur_2(config-tengigabitethernet1/1/25)#portswitch
Inspur_2(config-tengigabitethernet1/1/25)#exit
Inspur_2(config)#interface isf-port 1/1/1
Inspur_2(config-isf-port1/1/1)#isf port-group tengigabitethernet 1/1/25
Inspur_2(config-isf-port1/1/1)#exit
Inspur_2(config)#isf unit 1 priority 255
Inspur_2(config)#exit
```

将当前配置保存到下次启动配置文件。

```
Inspur_1#write
```

步骤 1 ISF 模式下配置：

配置 BFD MAD 检测。

- 配置 Device A。

创建 VLAN 3，并配置 MAD IP 地址，将 Device A（成员编号为 1）使能 BFD MAD 检测。

```
Inspur_1#config
Inspur_1(config)#create vlan 3 active
Inspur_1(config)#interface vlan 3
Inspur_1(config-vlan3)#mad ip address 192.168.2.1 unit 1
Inspur_1(config-vlan3)#mad bfd enable
1970-01-01,08:17:21 BFD-5-BFD_SESSIONID_DOWN:unit1: Bfd session 65 is
down.#
```

- 配置 Device B。

创建 VLAN 3，并配置 MAD IP 地址，将 Device B（成员编号为 2）使能 BFD MAD 检测。

```
Inspur_2#config
Inspur_2(config)#create vlan 3 active
Inspur_2(config)#interface vlan 3
Inspur_2(config-vlan3)#mad ip address 192.168.2.2 unit 2
Inspur_2(config-vlan3)#mad bfd enable
1970-01-01,08:17:21 BFD-5-BFD_SESSIONID_DOWN:unit1: Bfd session 65 is
down.#
```

说明

如果中间设备是一个 ISF 系统，则必须通过配置确保其 ISF 域编号与被检测的 ISF 系统不同。

2.8.3 将成员设备从 ISF 模式恢复到独立运行模式配置举例

组网需求

ISF 已经稳定运行，Device A 和 Device B 是 ISF 的成员设备。现因网络调整，需要将 Device A 和 Device B 从 ISF 模式下恢复到独立运行模式待用。

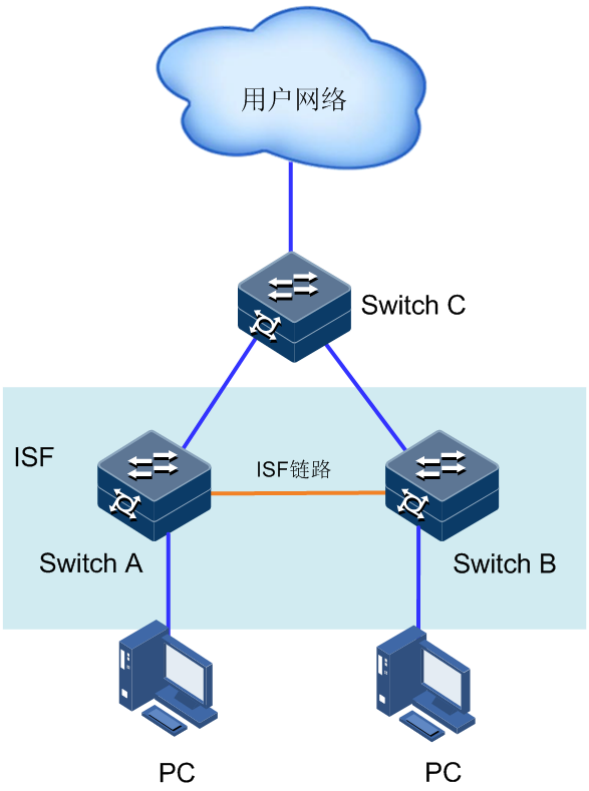
配置思路

断开 ISF 连接。可以直接将 ISF 物理连接线缆拔出也可以使用命令行关闭 Master 设备上所有的 ISF 物理端口。本举例采用命令行关闭的方式。

ISF 分裂后，分别将两台成员设备从 ISF 模式切换到独立运行模式。

组网图

图2-16 将成员设备从 ISF 模式恢复到独立运行模式配置组网图



配置步骤

- 确定 Master 设备，在设备 A 上进行如下操作。

```
Inspur_1#show isf
MODE：ISF mode
ISF MAC：00:01:22:44:76:78
-----------------------------------------------
Isf-port1/1/1
Tengigabitethernet1/1/25
Number    MAC Address       Domain       Unit    Priority    Role
Stk Time   Version   Minversion
1       00:01:22:44:76:78       0          2       255         master
18            2         9
2       00:0e:5e:61:91:cf       0          1       64          backup
30            2         9
```

通过以上显示信息可以看出，设备 B 是 Master 设备。

- 断开 ISF 连接：手工关闭 Master 设备 ISF 物理接口 Tengigabitethernet1/1/25。
- 将 Device A 的运行模式切换到独立运行模式。

在设备 A 上进行如下操作：

```
Inspur_1#config
Inspur_1#(config)#isf mode single
This config reboot go into effect, Please input 'yes' to reboot:yes
Will you change start-config ? please input 'yes' to change:yes
1970-01-01,08:36:35 System-4-SYSTEM_REBOOT:unit2: Change work Mode
reboot !
Operation successfully
BOOTROM starting ..
```

- 登录 Device B 后，将 Device B 的运行模式切换到独立运行模式。

```
Inspur_2#config
Inspur_2(config)#isf mode single
This config reboot go into effect, Please input 'yes' to reboot:yes
Will you change start-config ? please input 'yes' to change:yes
1970-01-01,08:36:35 System-4-SYSTEM_REBOOT:unit2: Change work Mode
reboot !
Operation successfully
BOOTROM starting ..
```

2.8.4 四台设备形成 ISF 典型配置举例

组网需求

由于网络规模迅速扩大，当前中心交换机（Device A）转发能力已经不能满足需求，如图 2-17 所示。使网络易管理、易维护。现在需要另增三台设备，将这四台设备组成一个 ISF，如图 2-18 所示。

组网图

图2-17 配置 ISF 之前的组网图

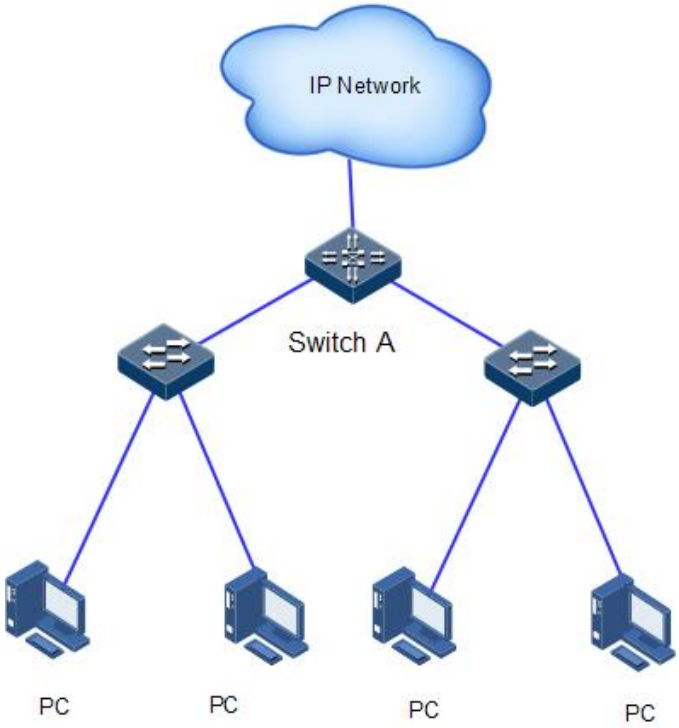
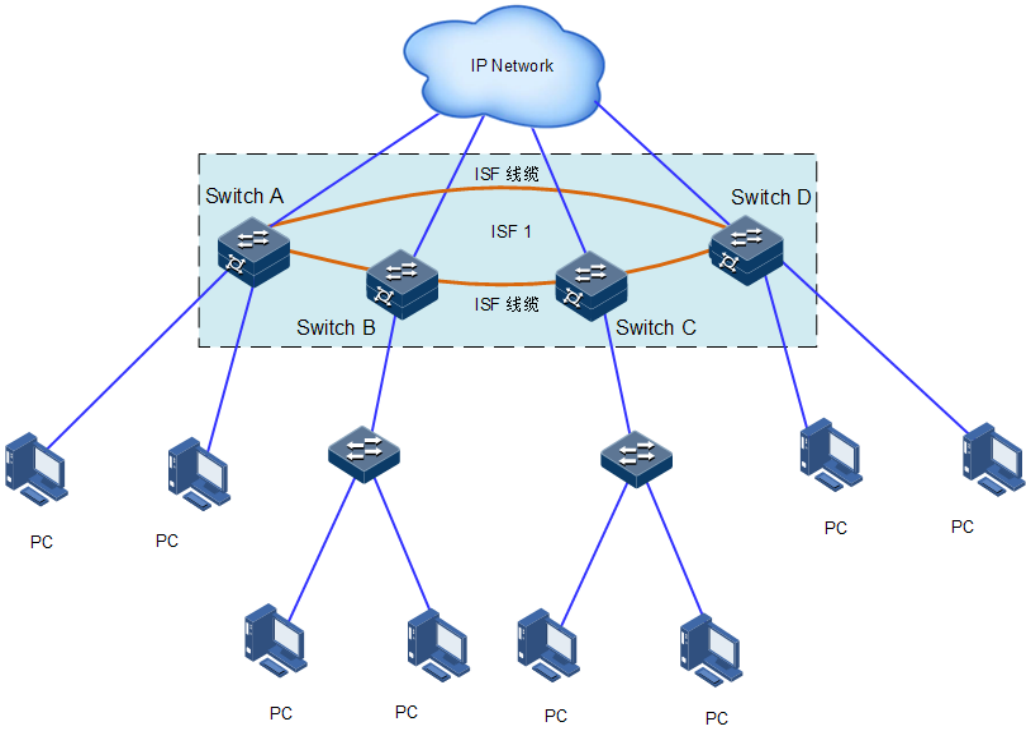


图2-18 将 Device A 改为 ISF 后的组网图



配置思路

- 分别配置四台成员设备的成员编号、优先级、ISF 端口；
- 分别在四台成员设备上配置 ISF 增强功能，按照拓扑进行物理连接；
- 将四台设备切换到 ISF 模式。

配置步骤

- 配置 Device A

Device A 的成员编号为 1，成员优先级为 12。

```
Inspur#config
Inspur(config)#isf renumber 1
Inspur(config)#isf priority 12
Inspur(config)#interface tengigabitethernet 1/1/25
Inspur(config-tengigabitethernet1/1/25)#portswitch
Inspur(config-tengigabitethernet1/1/25)#exit
Inspur(config)#interface tengigabitethernet 1/1/27
Inspur(config-tengigabitethernet1/1/27)#portswitch
Inspur(config-tengigabitethernet1/1/27)#exit
Inspur(config)#interface isf-port 1/1/1
Inspur(config-isf-port1/1/1)#isf port-group tengigabitethernet 1/1/25
Inspur(config-isf-port1/1/1)#exit
Inspur(config)#interface isf-port 1/1/2
Inspur(config-isf-port1/1/2)#isf port-group tengigabitethernet 1/1/27
Inspur(config-isf-port1/1/2)#exit
```

将当前配置保存到下次启动配置文件：

```
Inspur#write
```

将设备的运行模式切换到 ISF 模式：

```
Inspur#config
Inspur(config)#isf mode isf
next unit is: 1, are you sure ? please input 'yes':yes
This config reboot go into effect, Please input 'yes' to reboot:yes
1970-01-01,08:07:17 System-4-SYSTEM_REBOOT:unit1: Change work Mode
reboot !
Operation successfully
BOOTROM starting ..
```

设备重启后 Device A 组成了只有一台成员设备的 ISF。

- 配置 Device B

配置 Device B 的成员编号为 2，成员优先级为 26。

```
Inspur#config
Inspur(config)#isf renumber 2
Inspur(config)#isf priority 26
Inspur(config)#interface tengigabitethernet 1/1/25
Inspur(config-tengigabitethernet1/1/25)#portswitch
Inspur(config-tengigabitethernet1/1/25)#exit
Inspur(config)#interface tengigabitethernet 1/1/27
Inspur(config-tengigabitethernet1/1/27)#portswitch
```

```
Inspur(config-tengigabitethernet1/1/27)#exit
Inspur(config)#interface isf-port 1/1/1
Inspur(config-isf-port1/1/1)#isf port-group tengigabitethernet 1/1/25
Inspur(config-isf-port1/1/1)#exit
Inspur(config)#interface isf-port 1/1/2
Inspur(config-isf-port1/1/2)#isf port-group  tengigabitethernet  1/1/27
Inspur(config-isf-port1/1/2)#exit
```

将当前配置保存到下次启动配置文件。

```
Inspur#write
```

将设备的运行模式切换到 ISF 模式。

```
Inspur#config
Inspur(config)#isf mode isf
next unit is: 9, please input 'yes':yes
This configuration will go into effect after reboot, Please input 'yes'
to reboot:yes
Will you change start-config ? please input 'yes' to change:yes

1970-01-01,08:06:46 System-4-SYSTEM_REBOOT:unit1: Change work Mode
reboot !
Operation successfully
Inspur(config)#
BOOTROM starting ..
```

设备 B 重启后与设备 A 形成 ISF。

- 配置 Device C

配置 Device C 的成员编号为 3，成员优先级为 6。

```
Inspur#config
Inspur(config)#isf renumber 3
Inspur(config)#isf priority 6
Inspur(config)#interface  tengigabitethernet 1/1/25
Inspur(config-tengigabitethernet1/1/25)#portswitch
Inspur(config-tengigabitethernet1/1/25)#exit
Inspur(config)#interface tengigabitethernet 1/1/27
Inspur(config-tengigabitethernet1/1/27)#portswitch
Inspur(config-tengigabitethernet1/1/27)#exit
Inspur(config)#interface isf-port 1/1/1
Inspur(config-isf-port1/1/1)#isf port-group tengigabitethernet 1/1/25
Inspur(config-isf-port1/1/1)#exit
Inspur(config)#interface isf-port 1/1/2
Inspur(config-isf-port1/1/2)#isf port-group tengigabitethernet 1/1/27
Inspur(config-isf-port1/1/2)#exit
```

将当前配置保存到下次启动配置文件：

```
Inspur#write
```

设备的运行模式切换到 ISF 模式：

```
Inspur#config
Inspur(config)#isf mode isf
next unit is: 3, are you sure ? please input 'yes':yes
This config reboot go into effect, Please input 'yes' to reboot:yes
```

```
1970-01-01,08:07:17 System-4-SYSTEM_REBOOT:unit1: Change work Mode
reboot !
Operation successfully
BOOTROM starting ..
```

设备 C 重启后与设备 A、设备 B 形成 ISF。

- 配置 Device D

配置 Device B 的成员编号为 4，成员优先级为 2。

```
Inspur#config
Inspur(config)#isf renumber 4
Inspur(config)#isf priority 2
Inspur(config)#interface tengigabitethernet 1/1/25
Inspur(config-tengigabitethernet1/1/25)#portswitch
Inspur(config-tengigabitethernet1/1/25)#exit
Inspur(config)#interface tengigabitethernet 1/1/27
Inspur(config-tengigabitethernet1/1/27)#portswitch
Inspur(config-tengigabitethernet1/1/27)#exit
Inspur(config)#interface isf-port 1/1/1
Inspur(config-isf-port1/1/1)#isf port-group tengigabitethernet 1/1/25
Inspur(config-isf-port1/1/1)#exit
Inspur(config)#interface isf-port 1/1/2
Inspur(config-isf-port1/1/2)#isf port-group tengigabitethernet 1/1/27
Inspur(config-isf-port1/1/2)#exit
```

将当前配置保存到下次启动配置文件。

```
Inspur#write
```

将设备的运行模式切换到 ISF 模式：

```
Inspur#config
Inspur(config)#isf mode isf
next unit is: 4, are you sure ? please input 'yes':yes
This config reboot go into effect, Please input 'yes' to reboot:yes
1970-01-01,08:07:17 System-4-SYSTEM_REBOOT:unit1: Change work Mode
reboot !
BOOTROM starting ..
```

设备 D 重启后与设备 A、设备 B 和设备 C 形成 ISF。

3 以太网

本章介绍以太网特性的原理和配置过程，并提供相关的配置案例。

- MAC 地址转发表
- VLAN
- PVLAN
- Super VLAN
- QinQ
- VLAN 转换
- STP/RSTP
- MSTP
- 环路检测
- 接口保护
- 接口镜像
- L2CP
- GARP/GVRP
- Voice VLAN

3.1 MAC 地址转发表

3.1.1 简介

以太网设备转发以太网报文是通过 MAC 地址转发规则实现的快速转发，每台设备都有一个 MAC 地址与每个接口的转发对应表，这就是 MAC 地址转发表。所有入接口报文都会依据 MAC 地址转发表进行转发，是以太网设备实现二层报文快速转发的基础。MAC 地址转发表存储在设备的缓存中，缓存容量决定设备能存储多少 MAC 地址。

MAC 地址转发表的表项中包含如下信息：

- 目的 MAC 地址
- 目的 MAC 地址所对应的接口号

- 接口所属的 VLAN ID
- 标志位 Flag

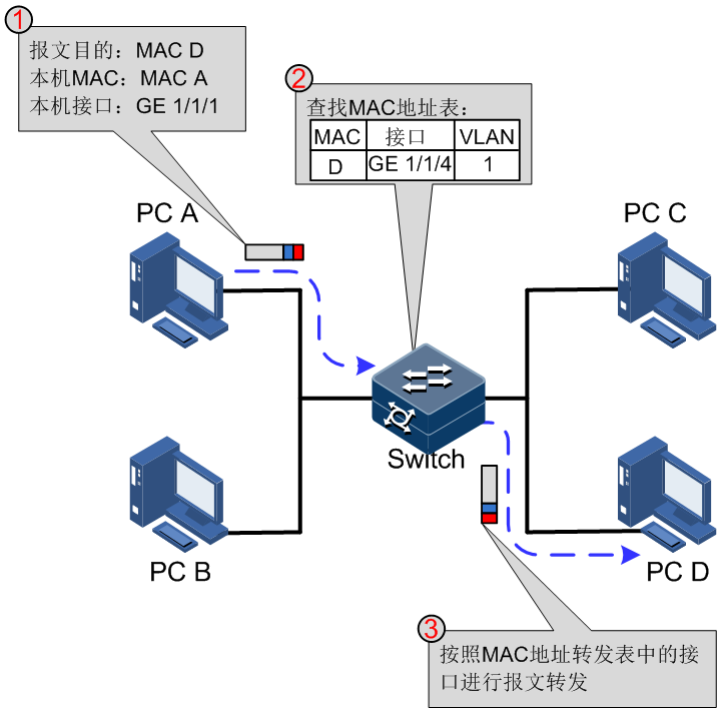
设备可基于设备、接口和 VLAN 来查看 MAC 地址表信息。

MAC 地址转发方式

以太网设备在转发报文时，根据 MAC 地址表项信息，会采取以下转发方式：

- 单播方式：当 MAC 地址转发表中包含与报文目的 MAC 地址对应的表项时，设备直接将报文从该表项中的转发接口发送；如不包含对应表项，则以广播方式向除接收接口外的所有接口转发。如图 3-1 所示。

图3-1 MAC 地址表转发示意图



- 组播方式：当设备收到目的地址为组播 MAC 地址的报文时，组播以广播形式发送，如果开启了组播功能并设置了未知组播过滤，则发送到指定 Report 接口。如无指定 Report 接口，则报文丢弃不转发。
- 广播方式：当设备收到目的地址为全 F 的报文，或 MAC 地址转发表中没有包含对应报文目的 MAC 地址的表项时，设备将采取广播方式将报文向除接收接口外的所有接口转发。

MAC 地址表项的分类

MAC 地址转发表分为静态地址表和动态地址表两项。

- 静态 MAC 地址表项：也称为“永久地址”，由用户手工添加和删除，不会随着时间老化。对于一个设备变动较小的网络，手工添加静态地址表项可以减少网络中的广播流量，能够提高接口的安全性，且系统复位后，表项不丢失。
- 动态 MAC 地址表项：交换机可以通过 MAC 地址学习机制学习动态 MAC 地址表项，该表项会按照用户配置的老化时间而老化掉。系统复位后，表项会清空。

MAC 地址老化时间

以太网交换机的 MAC 地址转发表是有容量限制的。为了最大限度利用地址转发表资源，以太网交换机利用老化机制更新 MAC 地址转发表，即：系统在动态创建某条表项的同时，开启老化定时器，如果在老化时间内没有再次收到来自该表项中的 MAC 地址的报文，交换机就会把该 MAC 地址表项删除。

设备支持 MAC 地址自动老化，老化时间设置范围为 0 或 10s～1 000 000s，其中 0 表示永不老化。

说明

MAC 地址的老化机制只对动态 MAC 地址表项生效。

MAC 地址转发策略

MAC 地址转发表有 2 种转发策略：

- 当报文进入设备接口时，会在 MAC 地址表查找报文中的目的 MAC 地址所关联的接口，如果在 MAC 地址表中有目的 MAC，并且目的 MAC 对应的接口与报文进入设备的接口不同，则从目的 MAC 对应的接口转发报文，并会将报文中的源 MAC 地址记录下来，与入报文的接口号、VLAN ID 相关联记录到 MAC 地址表中。当其它接口有去往该 MAC 地址时，可以通过 MAC 对应表将报文直接转发到对应的接口。
- 如果在 MAC 地址表中没有这个报文的目的 MAC，就会向除源接口外所有相同广播域的接口转发数据包，并记录该数据包中的源 MAC 地址到设备 MAC 地址表中。

MAC 地址学习数目限制

MAC 地址学习数目限制功能主要是为了限制 MAC 地址条目数，避免了因 MAC 地址表过于庞大，可能延长查找转发表项的时间，导致以太网交换机的转发性能下降的情况，是一种管理 MAC 地址表的有效方法。

MAC 地址学习数目限制主要用于限制 MAC 地址转发表的大小，提高交换机芯片的转发速度。

3.1.2 配置准备

场景

在以下情况，需要配置静态 MAC 地址转发表：

- 在公司内固定服务器、以及特定人员（经理、财务等）位置相对固定且较重要的主机上配置固定的静态 MAC 地址。以保证所有去往该 MAC 地址的数据流优先从静态 MAC 地址对应的接口进行转发。
- 对于固定静态 MAC 地址的接口，可以设置禁止 MAC 地址学习，防止其他主机通过该接口访问局域网数据。

同时，为避免 MAC 地址转发表中保存过多的 MAC 地址表项，而耗尽 MAC 地址表资源，需要配置 MAC 地址转发表的老化时间，以实现动态 MAC 地址的老化功能。

前提

无

3.1.3 MAC 地址转发表的缺省配置

设备上 MAC 地址转发表的缺省配置如下。

功能	缺省值
MAC 地址学习功能状态	使能
MAC 地址老化时间	300s
MAC 地址学习数目限制	无限制

3.1.4 配置静态 MAC 地址

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**mac-address static unicast** *mac-address* **vlan** *vlan-id interface-type interface-number*	配置静态单播 MAC 地址。

说明

- 源设备的 MAC 地址、组播地址、FFFF.FFFF.FFFF 及 0000.0000.0000 不能被配置为静态单播 MAC 地址。

3.1.5 配置黑洞 MAC 地址

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**mac-address blackhole** *mac-address* **vlan** *vlan-id*	配置黑洞 MAC 地址。

3.1.6 配置未知组播报文过滤

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**mac-address multicast drop-unknown** { **reserved-address** | **vlan** *vlan-list* }	（可选）配置 MAC 地址表的组播过滤模式。

3.1.7 配置 MAC 地址学习

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**vlan** *vlan-id*	进入 VLAN 接口配置模式。
3	Inspur(config-vlan)#**mac-address learning enable**	使能 MAC 地址学习功能。

3.1.8 配置 MAC 地址学习数目限制

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或 VLAN 配置模式。以下步骤以物理接口配置模式为例。
3	Inspur(config-gigaethernet1/1/*)#**mac-address threshold** *threshold-value*	配置接口下 MAC 地址学习数目限制阈值。

3.1.9 配置 MAC 老化时间

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**mac-address aging-time** { **0** | *period* }	配置 MAC 地址老化时间。

3.1.10 配置 MAC 地址漂移抑制

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**mac-address move-restrain enable**	使能全局 MAC 地址漂移抑制功能。
3	Inspur(config)#**mac-address mac-move trap enable**	（可选）使能 MAC 地址漂移告警功能。

3.1.11 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show mac-address** { **all** | **static** | **dynamic** | **blackhole** | *mac-address* } [**vlan** *vlan-id*] [*interface-type interface-number*]	查看 MAC 地址表项信息。
2	Inspur#**show mac-address multicast** [**vlan** *vlan-id*] [**count**]	查看二层组播地址或当前已存在的组播 MAC 地址数目。
3	Inspur#**show mac-address blackhole**	查看黑洞 MAC 地址。
4	Inspur#**show mac-address threshold** [*interface-type interface-number* | **vlan** [*vlan-list*]]	查看 MAC 地址学习数目限制值。
5	Inspur#**show mac-address aging-time**	查看 MAC 地址老化时间。
6	Inspur#**show mac-address learning** [**vlan** | *interface-type interface-number*]	查看 MAC 地址学习功能状态。
7	Inspur#**show mac-address count** [**vlan** *vlan-id*] [*interface-type interface-number*]	查看 MAC 地址表条目的数量。
8	Inspur#**show mac-address mac-move**	查看 MAC 地址表自漂移信息。

3.1.12 维护

用户可以通过以下命令维护 MAC 地址转发表特性。

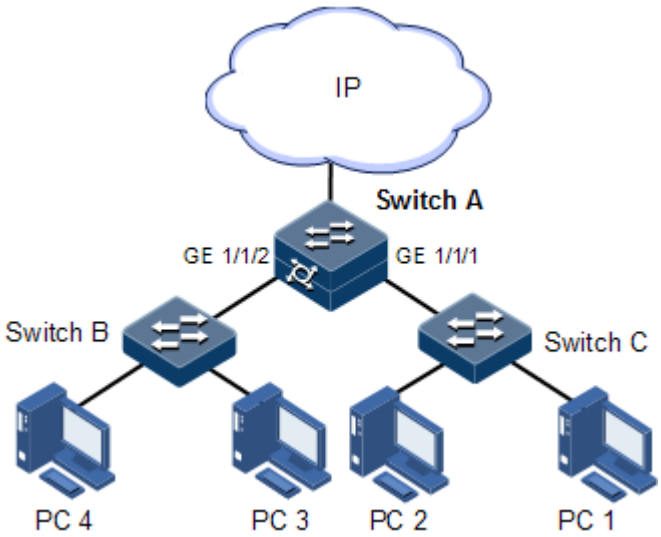
命令	描述
Inspur(config)#**clear mac-address** { **all** | *mac-address* | **blackhole** | **static** } [**vlan** *vlan-id*] [*interface-type interface-number*]	清除 MAC 地址。
Inspur(config)#**clear mac-address dynamic** [*mac-address*] [**vlan** *vlan-id*] [*interface-type interface-number*]	清除动态 MAC 地址表项。
Inspur(config)#**search mac-address** *mac-address* { **all** | **dynamic** | **static** } [*interface-type interface-number*] [**vlan** *vlan-id*]	查找 MAC 地址。

3.1.13 配置 MAC 地址转发表示例

组网需求

如图 3-2 所示，在 Switch A 上进行操作，在 GE 1/1/2 配置一条静态单播 MAC 地址 0001.0203.0405，所属 VLAN 为 VLAN 10；配置 MAC 地址老化时间为 500s。

图3-2 MAC 应用组网示意图



配置步骤

步骤 1 创建 VLAN 10 并激活，将 GE 1/1/2 加入 VLAN 10。

```
Inspur#config
Inspur(config)#create vlan 10 active
```

```
Inspur(config)#interface gigaethernet 1/1/2
Inspur(config-gigaethernet1/1/2)#switchport mode access
Inspur(config-gigaethernet1/1/2)#switchport access vlan 10
Inspur(config-gigaethernet1/1/2)#exit
```

步骤 2 在 GE 1/1/2 配置一条静态单播 MAC 地址 0001.0203.0405，所属 VLAN 10。

```
Inspur(config)#mac-address static unicast 0001.0203.0405 vlan 10
gigaethernet 1/1/2
```

步骤 3 配置 MAC 地址老化时间为 500s。

```
Inspur(config)#mac-address aging-time 500
```

检查结果

通过 **show mac-address** 命令查看 MAC 地址配置。

```
Inspur#show mac-address all gigaethernet 1/1/2

Aging time: 300 seconds

Mac Address       Port                        Vlan/Vxlan     Flag

--------------------------------------------------------------------

0001.0203.0405    gigaethernet1/1/2             2             static
```

3.2 VLAN

3.2.1 简介

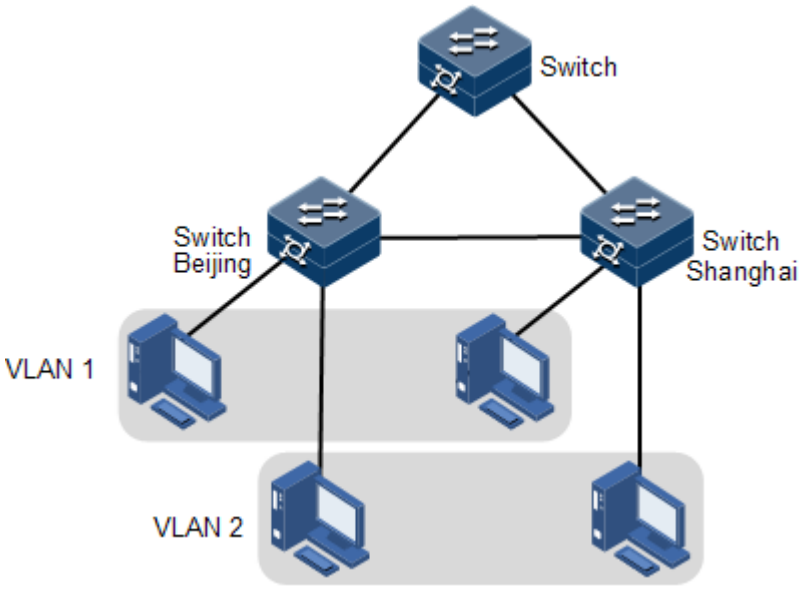
VLAN 概述

VLAN 是为解决以太网的广播问题和安全性而提出的一种协议。它是一种通过将局域网内的设备逻辑地而不是物理地划分成不同的广播域，从而实现多个互不影响的虚拟工作组的二层隔离技术。从功能上看，VLAN 和 LAN 有着相同的特性，但两者的主要区别在于同一 VLAN 内的成员可以不受物理位置的限制进行相互访问。

VLAN 划分

VLAN 划分有多种方式，例如基于接口、基于 MAC 地址和基于 IP 子网等，如图 3-3 所示。

图3-3 VLAN 划分示意图



VLAN 技术允许将一个物理的 LAN 逻辑地划分成不同的广播域。通过划分 VLAN，将没有互通需求的主机进行隔离，在增强网络安全性、减少广播流量的同时也减少了广播风暴的发生。

设备符合 IEEE 802.1Q 标准的 VLAN，支持 4094 个并发 VLAN。

- 基于接口划分 VLAN

设备支持基于接口划分 VLAN。交换机设备的接口模式分为 Access 和 Trunk 两种，接口模式与报文转发处理方式比较请参考表 3-1。

表3-1 接口模式与报文转发

接口类型	入报文处理		出报文处理
	Untag 报文	带 Tag 报文	
Access	为报文打上 Access VLAN 的 Tag	• 报文 VLAN ID＝Access VLAN ID，接收该报文 • 报文 VLAN ID≠Access VLAN ID，丢弃该报文	• 报文 VLAN ID＝Access VLAN ID，去掉 Tag 发送该报文 • 接口允许通过的 VLAN ID 列表中不包含报文 VLAN ID，丢弃该报文
Trunk	为报文打上 Native VLAN 的 Tag	• 接口允许通过的 VLAN ID 列表中包含报文 VLAN ID，接收该报文 • 接口允许通过的 VLAN ID 列表中不包含报文 VLAN ID，丢弃该报文	• 报文 VLAN ID＝Native VLAN ID，去掉 Tag 发送该报文 • 报文 VLAN ID≠Native VLAN ID，且接口允许通过时，保持原有 Tag 发送该报文

- 基于 MAC 地址划分 VLAN

  基于 MAC 地址划分 VLAN 是指根据报文源 MAC 地址对 VLAN 进行划分。

  - 当接口收到的报文为 Untag 报文时，根据报文的源 MAC 地址匹配 MAC VLAN 表项。如果报文中的源 MAC 地址与 MAC VLAN 表项中的 MAC 地址完全相同，则匹配成功，给报文添加表项中指定的 VLAN ID 并转发该报文。如果没有找到匹配 MAC VLAN 表项，则继续按照基于 IP 子网 VLAN、基于接口 VLAN 的先后顺序进行匹配。
  - 当接口收到的报文为 Tag 报文时，如果 VLAN ID 在接口允许通过的 VLAN ID 列表里时，则接收该报文；如 VLAN ID 不在接口允许通过的 VLAN ID 列表里时，则丢弃该报文。

- 基于 IP 子网划分 VLAN

  基于 IP 子网划分 VLAN 是指根据报文源 IP 地址及子网掩码对 VLAN 进行划分。

  - 设备从接口接收到 Untag 报文后，会根据报文的源 IP 地址及子网掩码确定报文所属的 VLAN，然后将报文自动划分到指定 VLAN 中传输。
  - 当接口收到的报文为 Tag 报文时，如果 VLAN ID 在接口允许通过的 VLAN ID 列表里时，则接收该报文；如 VLAN ID 不在接口允许通过的 VLAN ID 列表里时，则丢弃该报文。

3.2.2 配置准备

场景

VLAN 最主要功能是划分逻辑网段，通常有 2 种典型应用模式。

- 一种是在小型局域网中，一台设备下划分多个 VLAN，用 VLAN 将所有连接到设备的主机逻辑的划分开，同一个 VLAN 内的主机之间可以相互通信，不同 VLAN 间的主机之间无法通信。例如财务部门与其他部门需要划分开，互相不能访问，通常连接主机的接口设置为 Access 模式。
- 另一种是在稍大型局域网或企业网中，有多台设备连接较多的主机，并且设备之间级联，转发数据报文时都携带 VLAN Tag，多台设备的相同 VLAN 的接口可以相互通信，不同 VLAN 的主机之间无法通信。主要用在公司人员及主机数量较多，并且同一个部门所在位置不同，但是要求部门内的主机可以互相访问，需要在多台设备上划分 VLAN。如果不同 VLAN 之间需要通信，则要通过路由器等 3 层设备。设备之间级联的接口设置为 Trunk 模式。

当需要为 VLAN 配置 IP 地址时，可以为其关联一个三层接口，每一个三层接口将对应一个 IP 地址并关联一个 VLAN。

前提

无

3.2.3 VLAN 的缺省配置

设备上 VLAN 的缺省配置如下。

功能	缺省值
创建 VLAN	存在 VLAN 1
静态 VLAN 的活动状态	suspend
接口模式	Access
Access VLAN	VLAN 1
Trunk 接口的 Native VLAN	VLAN 1
接口 Trunk 模式时所允许通过的 VLAN	所有 VLAN
接口 Trunk 模式时所允许通过的 Untag VLAN	VLAN 1
VLAN 映射表号	VLAN ID 值

3.2.4 配置 VLAN 属性

请在需要配置 VLAN 属性信息的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**create vlan** *vlan-list* **active**	创建 VLAN。 该命令也可用于批量创建 VLAN。
3	Inspur(config)#**vlan** v*lan-id*	进入 VLAN 配置模式。

说明

- 用 **vlan** *vlan-id* 命令新创建的 VLAN 为活动状态。
- VLAN 的所有配置仅在该 VLAN 被激活后才会在系统中生效。

3.2.5 配置接口模式

请在需要配置接口模式的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。

步骤	配置	说明
3	Inspur(config-gigaethernet1/1/*)#**switchport mode** { **access** | **trunk** }	配置接口模式为 Access 或 Trunk。

3.2.6 配置基于 Access 接口的 VLAN

请在需要配置基于 Access 接口 VLAN 的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**switchport mode access** Inspur(config-gigaethernet1/1/*)#**switchport access vlan** *vlan-id*	配置接口模式为 Access，并将 Access 接口加入 VLAN。
4	Inspur(config-gigaethernet1/1/*)#**switchport access egress-allowed vlan** { **all** | [**add** | **remove**] *vlan-list* }	（可选）配置 Access 接口允许通过的 VLAN。

说明

- 无论 Access 接口允许通过的 VLAN 列表如何配置，该接口都允许 Access VLAN 的数据包通过，且转发出去的数据包不携带相应 VLAN TAG 标记。
- 设置 Access VLAN 时，如果该 VLAN 没有创建并激活，系统将自动创建并激活该 VLAN。
- 如果 Access VLAN 被用户手动删除或挂起，系统将自动设置该接口 Access VLAN 为缺省 VLAN。
- 当配置接口 Access VLAN 为非缺省的 Access VLAN 时，缺省 Access VLAN 1 为 Access 出接口允许通过的 VLAN，通过配置删除 Access 出接口允许通过的 VLAN，可以将缺省 Access VLAN 1 从 Access 出接口允许通过 VLAN 列表中删除。
- 如果配置 Access VLAN 不是缺省 VLAN，且 Access 接口允许通过的 VLAN 列表中没有缺省 VLAN，该接口将不允许缺省 VLAN 的数据包通过。
- Access 接口允许通过的 VLAN 列表只对静态 VLAN 生效，对 GVRP 动态 VLAN 等不生效。

3.2.7 配置基于 Trunk 接口的 VLAN

请在需要配置基于 Trunk 接口 VLAN 的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**switchport mode trunk**	配置接口模式为 Trunk。
4	Inspur(config-gigaethernet1/1/*)#**switchport trunk native vlan** *vlan-id*	配置接口 Native VLAN。
5	Inspur(config-gigaethernet1/1/*)#**switchport trunk allowed vlan** { **all** | [**add** | **remove**] *vlan-list* }	（可选）配置 Trunk 接口允许通过的 VLAN。
6	Inspur(config-gigaethernet1/1/*)#**switchport trunk untagged vlan** { **all** | [**add** | **remove**] *vlan-list* } [**confirm**]	（可选）配置 Trunk 接口可以去掉 Tag 的 VLAN。
7	Inspur(config-gigaethernet1/1/*)#**switchport trunk native vlan** { **tagged** | **untagged** }	（可选）配置 Trunk 接口的 Native VLAN 出端口的 TAG 属性。

说明

- 无论 Trunk 接口允许通过的 VLAN 列表和 Untagged VLAN 列表如何配置，该接口都允许 NATIVE VLAN 的数据包通过，且转发出去的数据包不携带相应 VLAN TAG 标记。
- 设置 Native VLAN 时，如果该 VLAN 没有创建并激活，系统将自动创建并激活该 VLAN。
- 如果 Native VLAN 被用户手动删除或阻塞，系统将自动设置该接口 Trunk Native VLAN 为缺省 VLAN。
- 接口允许 Trunk Allowed VLAN 报文出入，且如果该 VLAN 为 Trunk Untagged VLAN，则报文出接口时去掉该 VLAN TAG，否则不修改报文。
- 如果配置 Native VLAN 不是缺省 VLAN，且 Trunk 接口允许通过的 VLAN 列表中没有缺省 VLAN，该接口将不允许缺省 VLAN 的数据包通过。
- 设置 Trunk Untagged VLAN 列表时，系统自动将全部 Untagged VLAN 添加为 Trunk 允许 VLAN。
- Trunk 允许 VLAN 列表和 Trunk Untagged VLAN 列表都只对静态 VLAN 生效，对 GVRP 动态 VLAN 等不生效。

3.2.8 配置基于 MAC 地址的 VLAN

请在需要配置基于 MAC 地址的 VLAN 的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**mac-vlan** *mac-address* **vlan** *vlan-id* [**priority** *value*]	配置 MAC 地址与 VLAN 的关联
3	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
4	Inspur(config-gigaethernet1/1/*)#**mac-vlan enable**	使能 MAC-VLAN 功能。
5	Inspur(config-gigaethernet1/1/*)#**vlan precedence** { **mac-vlan** | **ip-subnet-vlan** }	（可选）MAC-VLAN 和 IP 子网 VLAN 优先级。

注意

- MAC 地址为组播 MAC 地址、全 0 或全 F 时，配置失败。
- 创建的 MAC 地址与 VLAN 关联与已经存在的关联冲突（例如同一 MAC 地址关联到不同的 VLAN），则配置失败。

3.2.9 配置基于 IP 子网的 VLAN

请在需要配置基于 IP 子网的 VLAN 的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ip-subnet-vlan** *ip-address* [*ip-mask*] **vlan** *vlan-id* [**priority** *value*]	配置 VLAN 与 IP 子网地址的关联。
3	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
4	Inspur(config-gigaethernet1/1/*)#**ip-subnet-vlan enable**	使能基于 IP 子网划分 VLAN 功能。
5	Inspur(config-gigaethernet1/1/*)#**vlan precedence** { **mac-vlan** | **ip-subnet-vlan** }	（可选）MAC-VLAN 和 IP 子网 VLAN 优先级。

注意

- IP 地址或掩码无效时，配置失败。
- 创建的 IP 子网与 VLAN 关联与已经存在的关联冲突（例如同一子网关联到不同的 VLAN 时），配置失败。

3.2.10 配置基于协议的 VLAN

请在需要配置基于协议划分 VLAN 的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**protocol-vlan** *protocol-index* { **ipv4** | **ipv6** | **ethertype** *protocol-id* }	配置协议 VLAN 与以太报文关联规则
3	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
4	Inspur(config-gigaethernet1/1/*)#**switchport protocol-vlan** *protocol-index* **vlan** *vlan-id*	配置接口和协议 VLAN 的关联规则

3.2.11 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

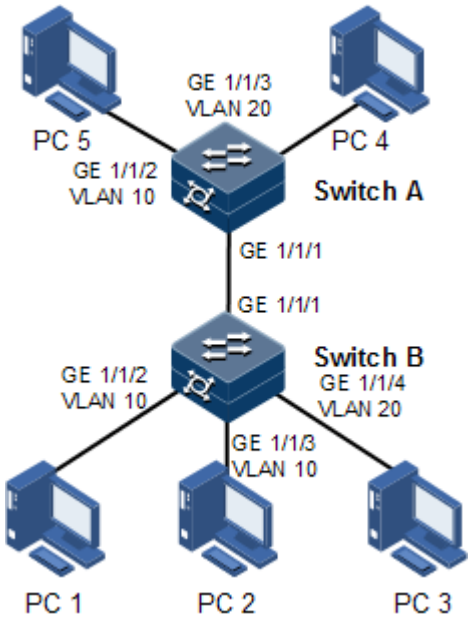
序号	检查项	说明
1	Inspur#**show vlan** [*vlan-list* | **static** | **dynamic**] [**detail**]	查看 VLAN 配置。
2	Inspur#**show vlan precedence**	查看 MAC-VLAN 和 IP 子网 VLAN 优先级信息。
3	Inspur#**show switchport interface** *interface-type interface-number*	查看接口 VLAN 配置信息。
4	Inspur#**show mac-vlan** { **all** | **vlan** *vlan-id* }	查看 MAC VLAN 配置信息
5	Inspur#**show ip-subnet-vlan** { **all** | **vlan** *vlan-id* }	查看 IP 子网 VLAN 的配置信息。
6	Inspur#**show protocol-vlan all**	查看全部协议 VLAN 配置信息。
7	Inspur#**show protocol-vlan interface** *interface-type interface-number*	查看接口的协议 VLAN 配置信息。

3.2.12 配置 VLAN 示例

组网需求

如图 3-4 所示，PC 1、PC 2、PC 5 属于 VLAN 10，PC3、PC4 属于 VLAN 20；两台设备相连的接口为 Trunk 模式，但不允许 VLAN 20 的报文通过，使 PC 3 和 PC 4 无法通信；在同一 Switch B 设备下的 PC 1 和 PC 2 的接口开启接口保护功能，使 PC 1 和 PC 2 无法通信，但 PC 1 和 PC 2 分别可以和 PC 5 通信。

图3-4 VLAN 和接口保护组网示意图



配置步骤

步骤 1 在两台设备上分别创建 VLAN 10 和 VLAN 20 并激活。

配置 Switch A。

```
Inspur#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 10,20 active
```

配置 Switch B。

```
Inspur#hostname SwitchB
SwitchB#config
SwitchB(config)#create vlan 10,20 active
```

步骤 2 将 Switch B 的接口 GE1/1/2 和 GE 1/1/3 以 Access 模式加入 VLAN 10，接口 GE 1/1/4 以 Access 模式加入 VLAN 20，接口 GE 1/1/1 为 Trunk 模式允许 VLAN 10 通过。

```
SwitchB(config)#interface gigaethernet 1/1/2
SwitchB(config-gigaethernet1/1/2)#switchport mode access
SwitchB(config-gigaethernet1/1/2)#switchport access vlan 10
SwitchB(config-gigaethernet1/1/2)#exit
SwitchB(config)#interface gigaethernet 1/1/3
SwitchB(config-gigaethernet1/1/3)#switchport mode access
SwitchB(config-gigaethernet1/1/3)#switchport access vlan 10
SwitchB(config-gigaethernet1/1/3)#exit
SwitchB(config)#interface gigaethernet 1/1/4
SwitchB(config-gigaethernet1/1/4)#switchport mode access
SwitchB(config-gigaethernet1/1/4)#switchport access vlan 20
SwitchB(config-gigaethernet1/1/4)#exit
SwitchB(config)#interface gigaethernet 1/1/1
SwitchB(config-gigaethernet1/1/1)#switchport mode trunk
```

```
SwitchB(config-gigaethernet1/1/1)#switchport trunk allowed vlan 10
confirm
SwitchB(config-gigaethernet1/1/1)#exit
```

步骤 3 将 Switch A 的接口 GE 1/1/2 以 Access 模式加入 VLAN 10，接口 GE 1/1/3 以 Trunk 模式加入 VLAN 20，接口 GE 1/1/1 为 Trunk 模式允许 VLAN 10 通过。

```
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#switchport mode access
SwitchA(config-gigaethernet1/1/2)#switchport access vlan 10
SwitchA(config-gigaethernet1/1/2)#exit
SwitchA(config)#interface gigaethernet 1/1/3
SwitchA(config-gigaethernet1/1/3)#switchport mode trunk
SwitchA(config-gigaethernet1/1/3)#switchport trunk native vlan 20
SwitchA(config-gigaethernet1/1/3)#exit
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport mode trunk
SwitchA(config-gigaethernet1/1/1)#switchport trunk allowed vlan 10
confirm
```

检查结果

通过 **show vlan** 命令查看 VLAN 的配置信息是否正确。

以 Switch B 为例。

```
SwitchB#show vlan
Switch Mode: --
VLAN Name          State   Status  Priority Member-Ports
-------------------------------------------------------------------------
1   Default        active  static  --       gigaethernet1/1/1
10  VLAN0010       active  static  --      gigaethernet1/1/2
gigaethernet1/1/3
20  VLAN0020       active  static  --       gigaethernet1/1/4
```

通过 **show switchport interface** *interface-type interface-number* 查看接口 VLAN 配置是否正确。

以 Switch B 为例。

```
SwitchB#show switchport interface gigaethernet 1/1/2
Interface: gigaethernet1/1/2
Switch Mode: switch
Reject frame type: none
Administrative Mode: access
Operational Mode: access
Access Mode VLAN: 10
Administrative Access Egress VLANs:
Operational Access Egress VLANs: 10
Trunk Native Mode VLAN: 1
Trunk Native VLAN: untagged
Administrative Trunk Allowed VLANs:
Operational Trunk Allowed VLANs: 1
Administrative Trunk Untagged VLANs:
Operational Trunk Untagged VLANs: 1
Administrative private-vlan host-association:  1
Administrative private-vlan mapping: 1
```

```
Operational private-vlan: --
```

通过 PC 1 ping PC 5、PC 2 ping PC 5、PC 3 ping PC 4 是否能够 ping 通，查看 Trunk 接口允许通过 VLAN 是否正确。

- PC 1 ping PC 5，可以 ping 通，VLAN 10 通信正常
- PC 2 ping PC 5，可以 ping 通，VLAN 10 通信正常
- PC 3 ping PC 4，不能 ping 通，VLAN 20 无法通信

3.3 PVLAN

3.3.1 简介

PVLAN（Private VLAN，私有 VLAN）提供在同一个 VLAN 内，接口之间的二层隔离功能，是网络中一种用于解决 VLAN 资源有效分配的技术。

PVLAN 类型

PVLAN 将 VLAN 划分为两种不同的属性：Primary VLAN（主 VLAN）和 Secondary VLAN（辅助 VLAN）。Primary VLAN 和 Secondary VLAN 组成一个 PVLAN 域，Primary VLAN 可在 PVLAN 内部和外部网络进行通信，Secondary VLAN 只能在 PVLAN 内部进行通信。Secondary VLAN 根据转发隔离规则不同，分为 Isolated VLAN 和 Community VLAN。

- Primary VLAN：主 VLAN，每个 PVLAN 中有且只能有一个主 VLAN，PVLAN 中各种类型的接口都是 Primary VLAN 的成员。
- Isolated VLAN：隔离 VLAN，每个 PVLAN 中只能有一个隔离 VLAN。
- Community VLAN：团体 VLAN，每个 PVLAN 中可以配置多个团体 VLAN。

PVLAN 接口模式

Primary VLAN 中可与外部网络进行通信的接口为 Promiscuous 接口（混杂接口），Secondary VLAN 中的接口为 Host 接口（主机接口）。根据 Secondary VLAN 的两种类型，主机接口又分为 Isolated 接口和 Community 接口。

- Promiscuous 接口：混杂接口，属于 PVLAN 域所对应的所有 PVLAN。处于该模式下的接口可与所有的接口进行通信。
- Isolated 接口：隔离接口。处于该模式下的接口是被隔离的，互相之间不能访问，只能与 Promiscuous 接口和 Trunk 接口通信。
- Community 接口：团体接口。团体接口可以互相通信，但不同团体之间的接口不能通信，所有团体接口都可以与 Promiscuous 接口和 Trunk 接口通信。

3.3.2 配置准备

场景

PVLAN 通常用于企业内部网，只允许 PVLAN 内的设备与默认网关通信，防止内部设备与外部网络通信。

前提

配置 PVLAN 之前，需要完成静态 VLAN 的创建并激活。

3.3.3 PVLAN 的缺省配置

设备上 PVLAN 的缺省配置如下。

功能	缺省值
接口 PVLAN 模式	Access 模式

3.3.4 配置 PVLAN 类型

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**private-vlan** { **primary vlan** *vlan-id* | **isolated vlan** *vlan-id* | **community vlan** *vlan-list* }	配置 PVLAN 类型。

注意

- 最多允许配置 32 个主 VLAN，2048 个辅助 VLAN。
- 若 VLAN 已经配置了关联，则不能改变或者删除 PVLAN 类型。

3.3.5 配置 PVLAN 关联

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**private-vlan** { **primary vlan** *vlan-id* | **isolated vlan** *vlan-id* | **community vlan** *vlan-list* }	配置 PVLAN 类型。
3	Inspur(config)#**private-vlan association** *primary-vlan-id* [**add** | **remove**] *secondary-vlan-list*	配置主 VLAN 和辅助 VLAN 的关联。 可使用 **no private-vlan association** *primary-vlan-id* 命令删除指定主 VLAN 下的主 VLAN 和辅助 VLAN 的关联。

注意

- 在配置 VLAN 关联时，要求完成 VLAN 的创建并激活，完成主 VLAN 和辅助 VLAN 配置 PVLAN 类型，并且关联的类型正确，否则不能配置关联。
- 主 VLAN 和辅助 VLAN 不能配置为默认 VLAN。
- 辅助 VLAN 只能加入到最多一个 PVLAN 中。
- 主 VLAN 只能关联一个隔离 VLAN，最多可以关联 64 个辅助 VLAN。

3.3.6 配置接口 PVLAN 模式

设备的 VLAN 功能中支持 Access 和 Trunk 两种接口模式，PVLAN 功能中增加了混杂接口模式和主机接口模式。

注意

- 主机接口模式和混杂接口模式允许在任意模式下配置关联或者映射，但要求 PVLAN 关联或者映射已经存在，否则配置失败。
- 当接口转换为主机接口模式或者混杂接口模式，但是没有正确配置主 VLAN 和辅助 VLAN 关联或映射时，该接口仅允许不带 VLAN Tag 的报文进入。
- IGMP 协议只能运行在主 VLAN 上，由于 PVLAN 中数据流上、下行通过的 VLAN 不同，不能配置 IGMP Snooping 功能实现组播功能，必须使用 IGMP MVR 功能实现。

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。

步骤	配置	说明
3	Inspur(config-gigaethernet1/1/*)#**switchport mode private-vlan** { **host**| **promiscuous** }	配置接口的 PVLAN 模式。
4	Inspur(config-gigaethernet1/1/*)#**exit**	返回全局配置模式。
5	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
6	Inspur(config-gigaethernet1/1/*)#s**witchport private-vlan host-association** *primary-vlan-id secondary-vlan-id*	配置主机接口上的主 VLAN 和辅助 VLAN 关联。 可使用 **no switchport private-vlan host-association** 命令删除主机接口上的主 VLAN 和辅助 VLAN 关联。
7	Inspur(config-gigaethernet1/1/*)#**switchport private-vlan trunk host-association** *secondary-vlan-id*	配置辅 VLAN 关联的主机接口可以转发 Tag 报文。 可使用 **no switchport private-vlan trunk host-association** 删除该配置。
8	Inspur(config-gigaethernet1/1/*)#**switchport private-vlan mapping** *primary-vlan-id* [**add** | **remove**] *secondary-vlan-list*	配置混杂接口上的主 VLAN 和辅助 VLAN 映射。 可使用 **no switchport private-vlan mapping** 命令删除混杂接口上的主 VLAN 和辅助 VLAN 映射。
9	Inspur(config-gigaethernet1/1/*)#**switchport private-vlan trunk mapping** *primary-vlan-id*	配置与主 VLAN 映射的接口可以转发 Tag 报文。 可使用 **no switchport private-vlan trunk mapping** 删除该配置。

3.3.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show vlan private-vlan**	查看 PVLAN 配置信息。
2	Inspur#**show switchport interface** *interface-type interface-number*	查看接口的交换功能配置信息。
3	Inspur#**show vlan** [*vlan-list* | **static** | **dynamic**] [**detail**]	查看 VLAN 配置信息。

3.3.8 配置 PVLAN 示例

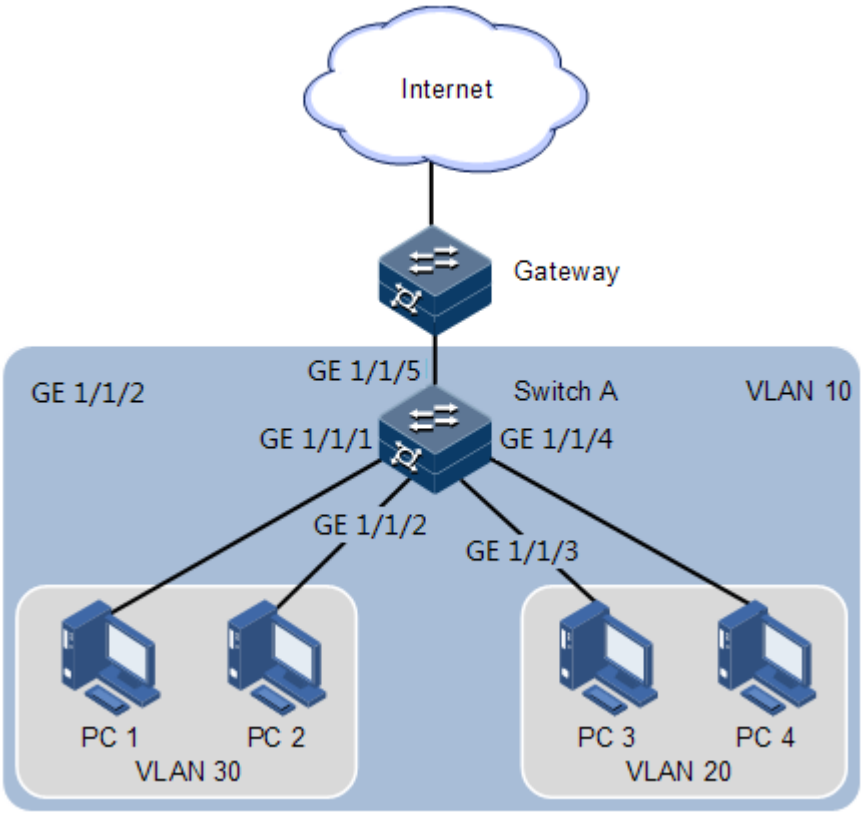
组网需求

为了解决 VLAN 资源有效分配，对 VLAN 进行合理的划分和配置。如图 3-5 所示为辅助 VLAN 与混杂接口的通信。在 Switch A 上配置 VLAN 10 为主 VLAN，VLAN 20 为隔离 VLAN，VLAN 30 为团体 VLAN。

- 配置 Gigaethernet 1/1/1 与 Gigaethernet 1/1/2 为设备团体接口，配置 PVLAN 关联 VLAN 10 和 VLAN 30。
- 配置 Gigaethernet 1/1/3 与 Gigaethernet 1/1/4 为设备隔离接口，配置 PVLAN 关联 VLAN 10 和 VLAN 20。
- 配置 Gigaethernet 1/1/5 为混杂接口，配置 PVLAN 映射为 VLAN 10、VLAN 20 和 VLAN 30。

PC 1 和 PC 2 分别连接设备团体接口（Gigaethernet 1/1/1 与 Gigaethernet 1/1/2），可与团体接口（Gigaethernet 1/1/1 与 Gigaethernet 1/1/2）和混杂接口（Gigaethernet 1/1/5）通信；PC 3 和 PC 4 分别连接设备隔离接口（Gigaethernet 1/1/3 与 Gigaethernet 1/1/4），只能与混杂接口（Gigaethernet 1/1/5）通信。

图3-5 PVLAN 应用组网示意图



配置步骤

步骤 1 配置 PVLAN 类型。

```
Inspur#config
Inspur(config)#create vlan 10,20,30 active
Inspur(config)#private-vlan primary vlan 10
Inspur(config)#private-vlan community vlan 30
Inspur(config)#private-vlan isolated vlan 20
Inspur(config)#private-vlan association 10 20,30
```

步骤 2 配置混杂接口模式及混杂接口上的主 VLAN 和辅助 VLAN 映射。

```
Inspur(config)#interface gigaethernet 1/1/5
Inspur(config-gigaethernet1/1/5)#switchport mode private-vlan promiscuous
Inspur(config-gigaethernet1/1/5)#switchport private-vlan mapping 10 20,30
Inspur(config-gigaethernet1/1/5)#exit
```

步骤 3 配置主机接口模式及主机接口上的主 VLAN 和辅助 VLAN 关联。

接口 Gigaethernet 1/1/1 与 Gigaethernet 1/1/2，Gigaethernet 1/1/3 与 Gigaethernet 1/1/4 配置相同，在此仅介绍 Gigaethernet 1/1/1 与 Gigaethernet 1/1/3 的配置。

```
Inspur(config)#interface gigaethernet 1/1/1
Inspur(config-gigaethernet1/1/1)#switchport mode private-vlan host
Inspur(config-gigaethernet1/1/1)#switchport private-vlan host-association
10 30
Inspur(config-gigaethernet1/1/1)#exit
Inspur(config)#interface gigaethernet 1/1/3
Inspur(config-gigaethernet1/1/3)#switchport mode private-vlan host
Inspur(config-gigaethernet1/1/3)#switchport private-vlan host-association
10 20
```

检查结果

在设备上通过 **show vlan private-vlan** 命令查看 PVLAN 配置信息。

```
Inspur#show vlan private-vlan
VLAN ID: 10
Pvlan type: primary
Associated-isolated vlan: 20
Associated-community vlan: 30
Member Port-list:
         gigaethernet1/1/1         gigaethernet1/1/3
         gigaethernet1/1/5
Untag Port-list:
         gigaethernet1/1/1         gigaethernet1/1/3
         gigaethernet1/1/5

VLAN ID: 20
Pvlan type: isolated
Associated-primary vlan: 10
Member Port-list:
         gigaethernet1/1/3         gigaethernet1/1/5
Untag Port-list:
         gigaethernet1/1/3         gigaethernet1/1/5
```

```
VLAN ID: 30
Pvlan type: community
Associated-primary vlan: 10
Member Port-list:
         gigaethernet1/1/1          gigaethernet1/1/5
Untag Port-list:
         gigaethernet1/1/1          gigaethernet1/1/5
```

3.4 Super VLAN

3.4.1 简介

传统的 ISP 网络给每个用户被分配一个 IP 子网，每分配一个子网，就有三个 IP 地址被占用，分别作为子网的网络号、广播地址和缺省网关。如果一些用户的子网中有大量未分配的 IP 地址，也无法给其他用户使用，因此这种方法会造成 IP 地址的浪费。

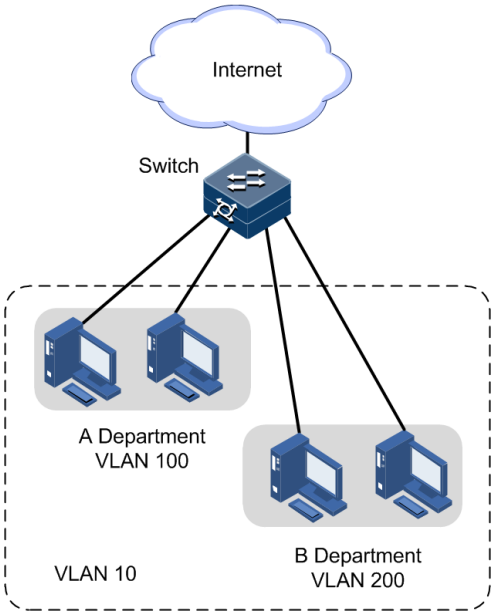
Super VLAN 引入了 Super VLAN 和 Sub VLAN 的概念，Super VLAN 可以逻辑上可以认为是 SubVLAN 的集合，具有如下特点：

- Super VLAN：只建立逻辑三层接口，而不包含物理端口，可以看作是若干 Sub VLAN 的集合。
- Sub VLAN：不能建立逻辑三层接口，只包含物理接口，与外部的三层交换依靠 Super VLAN 的逻辑三层接口 IP 作为默认网关，通过 ARP 代理功能完成互访。Sub VLAN 之间仍像普通 VLAN 一样二层相互隔离。

ARP 代理功能是指一个物理网络子网中的源主机向另一个物理网络的子网中的目的主机发 ARP 请求，与源主机直连的网关利用自己接口的 MAC 地址代替目的主机进行 ARP Reply。

如图 1-1 所示，Sub VLAN 100 内的主机与 Sub VLAN 200 内的主机进行通信，当 Super VLAN 10 开启 ARP 代理功能时，ARP 学习、ARP 收发包处理、代理 ARP 的流程，都利用 Super VLAN 10 的三层接口完成。

图3-6 Sub VLAN 与 Super VLAN 划分示意图



3.4.2 配置准备

场景

通过配置 Super VLAN 功能，使接入到同一个交换机相同网段但归属不同 VLAN 的主机可以使用其所属 Super VLAN 的三层接口 IP 地址作为默认网关进行三层通信。

前提

- 配置 Super VLAN 后，Super VLAN 下不能有任何成员端口，若该 VLAN 下已经有成员端口，也不能使能 Super VLAN 属性。
- 待加入 Super VLAN 的相关 VLAN 已创建并激活。若物理接口默认为三层接口需将其配置为二层接口。

3.4.3 配置 Super VLAN 功能

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#create vlan` *`vlan-id`* `active`	创建 VLAN 并进入 VLAN 配置模式。
3	`Inspur(config-vlan)#supervlan`	更改 VLAN 属性为 Supervlan。
4	`Inspur(config-vlan)#subvlan [ add | remove ]` *`subvlan-id`*	配置该 Super VLAN 下的 Sub VLAN。

步骤	配置	说明
5	Inspur(config-vlan)#**exit**	退出 VLAN 配置模式。
6	Inspur(config)#**interface vlan** *vlan-id*	进入 VLAN 接口模式。
7	Inspur(config-vlan)#**arp local-proxy enable**	启用 Super VLAN 的本地 ARP 代理功能。

说明

配置完成 Super VLAN 接口后，必须配置 IP 地址；属于 Super VLAN 的 VLAN 称为 Sub VLAN，VLAN 配置为 Sub VLAN 后，不再支持作为 VLAN 接口及配置 IP 地址。

3.4.4 检查配置

请在需要的设备上进行以下配置。

序号	检查项	说明
1	Inspur#**show supervlan** [*vlan-id*]	查看 Super VLAN 及其 Sub VLAN 配置信息。
2	Inspur#**show ip interface brief**	查看 Super VLAN 的 IP 配置信息。

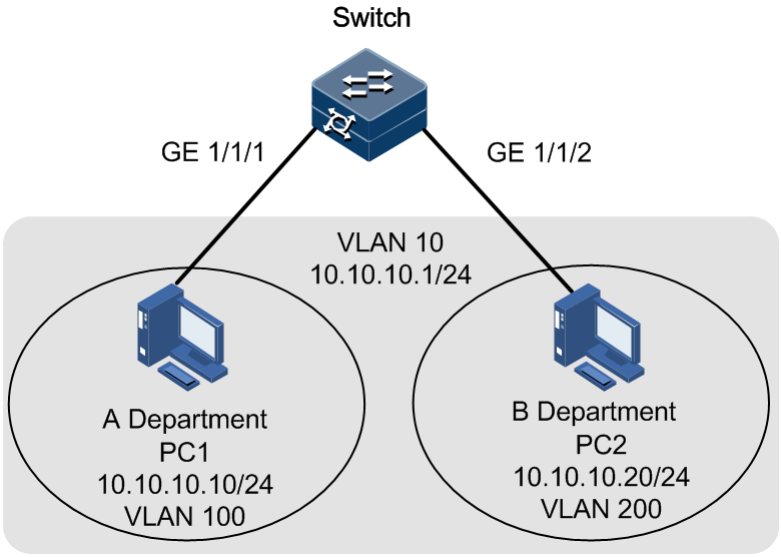
3.4.5 配置 Super VLAN 示例

组网需求

某企业 A 部门有 PC1，B 部门有 PC2，两台 PC 在不同的 VLAN 里，但有互通需求。如果单独为两个 VLAN 配置子网，会浪费大量 IP 地址。通过配置 Super VLAN 功能，进行三层通信，比使用普通 VLAN 方式少占用 IP 地址。

如图 3-7 所示，PC 1 属于 VLAN100、PC 2 属于 VLAN 200，将 VLAN 100 和 VLAN 200 划入 Super VLAN 10，实现 Sub VLAN 100 的主机 PC1 和 Sub VLAN 200 的主机 PC2 可以共用 Super VLAN 的网关 10.10.10.1 实现互通。

图3-7 Super VLAN 组网示意图



配置步骤

步骤 1 在交换机设备上创建 VLAN 10，100，200，并将接口加入 VLAN。

```
Inspur#config
Inspur(config)#create vlan 10,100,200 active
Inspur(config)#interface gigaethernet 1/1/1
Inspur(config-gigaethernet1/1/1)#switchport access vlan 100
Inspur(config-gigaethernet1/1/1)#interface gigaethernet 1/1/2
Inspur(config-gigaethernet1/1/2)#switchport access vlan 200
Inspur(config-gigaethernet1/1/2)#exit
```

步骤 2 配置 VLAN 10 为 Super VLAN。

```
Inspur(config)#vlan 10
Inspur(config-vlan)#supervlan
```

步骤 3 为该 Super VLAN 10 增加 Sub VLAN 100、Sub VLAN 200。

```
Inspur(config-vlan)#subvlan add 100,200
Inspur(config-vlan)#exit
```

步骤 4 为 Super VLAN 配置 IP 地址。

```
Inspur(config)#interface vlan 10
Inspur(config-vlan10)#ip address 10.10.10.1 255.255.255.0
```

步骤 5 使能 Super VLAN 的 ARP 本地代理功能。

```
Inspur(config-vlan10)#arp local-proxy enable
```

检查结果

通过 **show supervlan** 命令查看 Super VLAN 和 Sub VLAN 配置是否正确。

```
Inspur#show supervlan
Supervlan ID     Subvlanlist
------------------------------------
10               100，200
```

通过 **show ip interface brief** 命令查看 Super VLAN 接口配置是否正确。

```
Inspur#show ip interface brief
VRF                    IF            Address        NetMask     Catagory
------------------------------------------------------------------------------
-------------------------
Default-IP-Routing-Table    vlan10           10.10.10.1     255.255.255.0
primary
```

为 PC1 配置 10.10.10.1 为默认网关，并通过 **ping** 命令查看和 PC2 之间是否能够互通。

```
Inspur#ping 10.10.10.20

正在 Ping 10.10.10.20 具有 32 字节的数据:
来自 10.10.10.20 的回复: 字节=32 时间=1ms TTL=62
来自 10.10.10.20 的回复: 字节=32 时间=2ms TTL=62
来自 10.10.10.20 的回复: 字节=32 时间=2ms TTL=62
来自 10.10.10.20 的回复: 字节=32 时间=1ms TTL=62

10.10.10.20 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms，最长 = 2ms，平均 = 1ms
```

3.5 QinQ

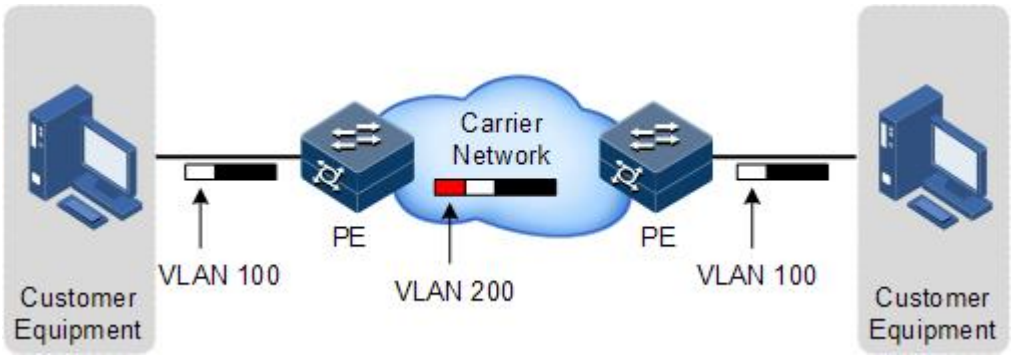
3.5.1 简介

QinQ（也称 Stacked VLAN 或 Double VLAN）技术是对 802.1Q 的扩展，是 IEEE 在 802.1ad 标准中定义的。

基本 QinQ

基本 QinQ 是一种简单的二层 VPN 隧道技术，它通过在运营商接入端为用户的私网报文封装外层 VLAN Tag，使报文携带两层 VLAN Tag 穿越运营商的骨干网络（公网）。在公网中，报文只根据外层 VLAN Tag（即公网 VLAN Tag）进行传输，用户的私网 VLAN Tag 则当作报文中的数据部分来进行传输。

图3-8 基本 QinQ 典型组网示意图



基本 QinQ 典型组网应用如图 3-8 所示，设备作为运营商 PE（Provider Edge）。

报文从用户设备中传送到达 PE 设备，此时报文携带标签的 VLAN ID 为 100。经过 PE 设备用户侧接口时打上外层标签 VLAN 200，经由 PE 设备的网络侧接口进入运营商网络。

带外层标签 VLAN 200 的报文经过运营商传送到达另一端 PE 设备，另一端的 PE 把外层签 VLAN 200 剥去，然后发送到用户设备。报文此时又恢复到只携带一层标签 VLAN 100。

通过该技术可以缓解日益紧缺的公网 VLAN ID 资源，使得用户可以规划自己的私网 VLAN ID，不会导致和公网 VLAN ID 冲突。

灵活 QinQ

灵活 QinQ 是基本 QinQ 的一种增强应用，可以根据一些特性对用户数据进行流分类，然后对不同的类别封装不同的外层 VLAN 标签，它基于接口与 VLAN 结合的方式来实现。除了能实现所有基本 QinQ 的功能外，灵活 QinQ 还能够对同一个接口收到的报文根据不同的 VLAN Tag 做不同的动作，为报文的不同内层 VLAN ID 添加不同的外层 VLAN ID。通过配置内外层 Tag 映射规则，还可以为具有不同内层 Tag 的报文按映射规则封装不同的外层 Tag。

灵活 QinQ 功能可以使运营商的网络构架更为灵活，在连接接入层设备的接口上可以根据 VLAN Tag 对不同的终端用户进行分类，为各类用户封装不同的外层 Tag，并可以在公网中按外层 Tag 配置 QoS 策略，灵活配置数据的传输优先级，使各类用户获得相应的服务。

3.5.2 配置准备

场景

对设备进行基本 QinQ 配置还是灵活 QinQ 配置，需要根据不同的业务需求进行选择。

- 基本 QinQ

通过基本 QinQ 技术应用，用户可以添加外层 VLAN Tag 自由规划自己的私网 VLAN ID，使得运营商网络两端的用户设备之间的数据可以通过运营商网络进行透明输，而不会导致和服务提供商网络中 VLAN ID 冲突。

- 灵活 QinQ

与基本 QinQ 不同，外层 VLAN Tag 是可以根据业务不同进行选择的。用户网络中有多种业务，并设定不同的私网 VLAN ID，针对语音、视频、或数据业务等在运营商网络中通过加不同的外层 VLAN Tag 区分出来，针对不同业务转发的同时实现不同的分流，实现内外层的 VLAN 映射。

前提

在配置 QinQ 之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。
- 创建 VLAN。

说明

同一接口下，双层 VLAN 转换不能与基本 QinQ、单层 CVLAN/Priority-Tagged 的 VLAN 转换同时配置。

3.5.3 QinQ 的缺省配置

设备上 QinQ 的缺省配置如下。

功能	缺省值
外层 VLAN Tag 的 TPID 值	0x8100
基本 QinQ 功能状态	禁用
灵活 QinQ 功能状态	禁用

3.5.4 配置基本 QinQ

请在需要的设备的用户侧接口上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**dot1q-tunnel**	使能接口基本 QinQ 功能，支持聚合组接口配置，支持堆叠模式配置。
4	Inspur(config-gigaethernet1/1/*)#**switchport qinq default-cvlan** *vlan-id*	配置使能接口的基本 QinQ 功能，添加双层 TAG，指定 CVLAN，SVLAN 使用 PVID。

步骤	配置	说明
5	Inspur(config-gigaethernet1/1/*)#**switchport reject-frame** { **tagged** | **untagged** }	配置接口禁止转发的报文类型。

说明

- 采用接口的基本 QinQ 功能时，必须配置接口的接口属性，即指定接口类型为 Access 或 Trunk，并配置接口的缺省 VLAN。
- 当接口开启基本 QINQ 时，所有报文均当做 Untagged 报文处理，若同时配置 Untagged 报文丢弃，那么 Tagged 的报文也会同时丢弃。
- 匹配条件为 VLAN+CoS 与匹配条件只有 VLAN 的 VLAN 转换在同一端口下不能同时配置。

3.5.5 配置灵活 QinQ

请在需要的设备用户侧接口上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**switchport vlan-mapping-miss discard**	配置接口丢弃不能与灵活 QINQ 或 VLAN 转换规则匹配的 Tagged 报文。
4	Inspur(config-gigaethernet1/1/*)#**switchport vlan-mapping ethertype** { **arp** | **eapol** | **flowcontrol** | **ip** | **ipv6** | **loopback** | **mpls** | **mpls-mcast** | **pppoe** | **pppoedisc** | **user-define** *protocol-id* | **x25** | **x75** } **add-outer** *outer-vlan-id*	配置基于 EtherType 的灵活 QinQ 添加 TAG VLAN 的映射规则。
5	Inspur(config-gigaethernet1/1/*)#**switchport vlan-mapping both priority-tagged** [**cos** *cos-value*] **add-outer** *outer-vlan-id* [**cos** *cos-value*] [**remove** | **translate** *vlan-id*] Inspur(config-gigaethernet1/1/*)#**switchport vlan-mapping both cvlan** *custom-vlan-list* [**cos** *cos-value*] **add-outer** *outer-vlan-id* [**cos** *cos-value*] { **remove** | **translate** *vlan-id* } Inspur(config-gigaethernet1/1/*)#**switchport vlan-mapping both** { **untag** | **inner** *inner-vlan-id* } [**cos** *cos-value*] **add-outer** *outer-vlan-id* [**cos** *cos-value*]	配置基于双方向的灵活 QinQ 添加外层 VLAN 规则，支持聚合组配置，支持堆叠模式配置。

同一接口下，双层 VLAN 转换不能与基本 QinQ、单层 CVLAN/Priority-Tagged 的 VLAN 转换同时配置；但配置灵活 QinQ，需要指定外层 VLAN 的 Cos 值时，必须先开启基本 QinQ 功能。

3.5.6 配置网络侧接口为 Trunk 模式

请在需要配置基本 QinQ 或灵活 QinQ 的设备网络侧接口上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**switchport mode trunk**	配置接口 Trunk 模式，可允许双 Tag 报文通过。

3.5.7 配置 TPID

请在需要设备的网络侧接口进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	Inspur(config-gigaethernet1/1/*)#**tpid** *tpid*	配置接口的外层 VLAN Tag 的 TPID。

3.5.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show dot1q-tunnel**	查看接口基本 QinQ 配置信息。
2	Inspur#**show vlan-mapping both interface** interface-type *interface-number*	查看接口的双方向 QinQ 配置信息。
3	Inspur#**show vlan-mapping interface** interface-type *interface-number*	查看接口的 EtherType 的灵活 QinQ 配置。

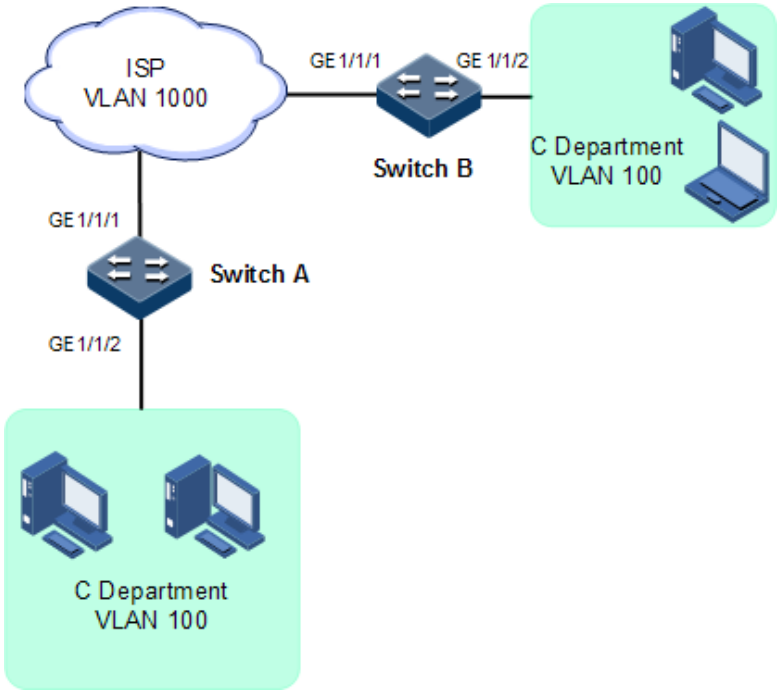
3.5.9 配置基本 QinQ 示例

组网需求

如图 3-9 所示，Switch A 和 Switch B 分别连接了 C 部门的 2 个不同地点的网络。C 部门为 VLAN100，要通过运营商 VLAN1000 网络进行通信。运营商的 TPID 为 9100。

通过在 Switch A 和 Switch B 配置基本 QinQ 功能来实现部门内部通过运营商网络的正常通信。

图3-9 基本 QinQ 应用组网示意图



配置步骤

配置 Switch A 和 Switch B。

Switch A 和 Switch B 配置步骤完全相同，仅以配置 Switch A 为例。

步骤 1 创建 VLAN 100 和 VLAN 1000 并激活。

```
Inspur#config
Inspur(config)#create vlan 100,1000 active
Inspur(config)#interface gigaethernet 1/1/1
Inspur(config-gigaethernet1/1/1)#switchport mode trunk
Inspur(config-gigaethernet1/1/1)#switchport trunk allowed vlan 1000
Inspur(config-gigaethernet1/1/1)#tpid 9100
Inspur(config-gigaethernet1/1/1)#exit
```

步骤 2 使能接口的基本 QinQ 功能。

```
Inspur(config)#interface gigaethernet 1/1/2
Inspur(config-gigaethernet1/1/2)#switchport mode trunk
Inspur(config-gigaethernet1/1/2)#switchport trunk native vlan 1000
Inspur(config-gigaethernet1/1/2)#dot1q-tunnel
Inspur(config-gigaethernet1/1/2)#exit
```

检查结果

通过 **show dot1q-tunnel** 命令查看 QinQ 配置信息。

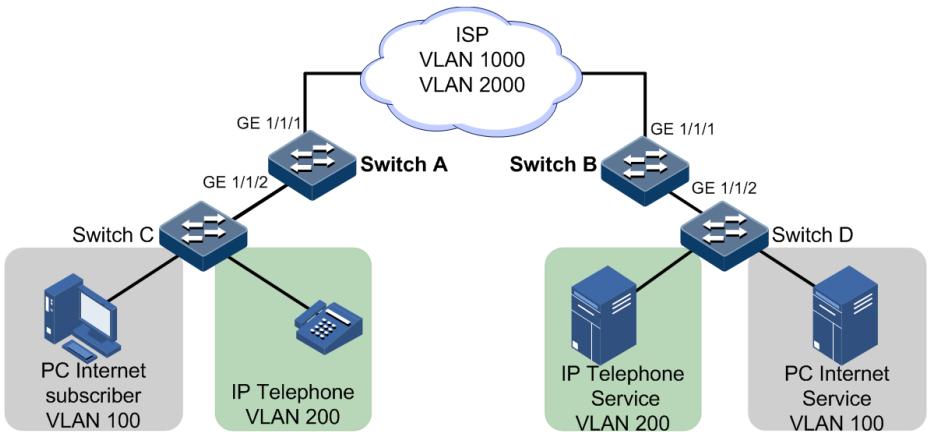
```
Inspur#show dot1q-tunnel
Interface          QinQ Status  Outer TPID on port  Cos override Vlan-
map-miss
-------------------------------------------------------
gigaethernet1/1/1     -              0x9100          -       disable
gigaethernet1/1/2  Dot1q-tunnel       0x8100          -       disable
```

3.5.10 配置灵活 QinQ 示例

组网需求

如图 3-10 所示，运营商网络区分普通 PC 上网业务和 IP 电话业务，故将 PC 上网业务分配 VLAN 1000，IP 电话业务分配的 VLAN 是 2000。在 Switch A 和 Switch B 上设置灵活 QinQ，将分配给 PC 上网业务的 VLAN 100 添加外层 Tag VLAN 1000，将分配给 IP 电话业务的 VLAN 200 添加外层 Tag VLAN 2000，使用户和服务器间通过运营商的网络能够正常通信。运营商的 TPID 为 9100。

图3-10 灵活 QinQ 应用组网示意图



配置步骤

配置 Switch A 和 Switch B。

Switch A 和 Switch B 配置步骤完全相同，仅以配置 Switch A 为例。

步骤 1 创建 VLAN 100，200，1000，2000 并激活，TPID 为 9100。

```
Inspur#name SwitchA
```

```
SwitchA#config
SwitchA(config)#create vlan 100,200,1000,2000 active
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport mode trunk
SwitchA(config-gigaethernet1/1/1)#switchport trunk allowed vlan 1000,2000
SwitchA(config-gigaethernet1/1/1)#tpid 9100
SwitchA(config-gigaethernet1/1/1)#exit
```

步骤 2 使能接口 1/1/2 的灵活 QinQ 功能。

```
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#switchport mode trunk
Inspur(config-gigaethernet1/1/2)#switchport trunk allowed vlan
100,200,1000,2000
SwitchA(config-gigaethernet1/1/2)#switchport vlan-mapping both inner 100
add-outer 1000
SwitchA(config-gigaethernet1/1/2)#switchport vlan-mapping both inner 200
add-outer 2000
SwitchA(config-gigaethernet1/1/2)#exit
```

检查结果

通过 **show switchport inteface** *interface-type interface-number* **vlan-mapping add-outer** 命令查看灵活 QinQ 配置信息。

以 Switch A 为例。

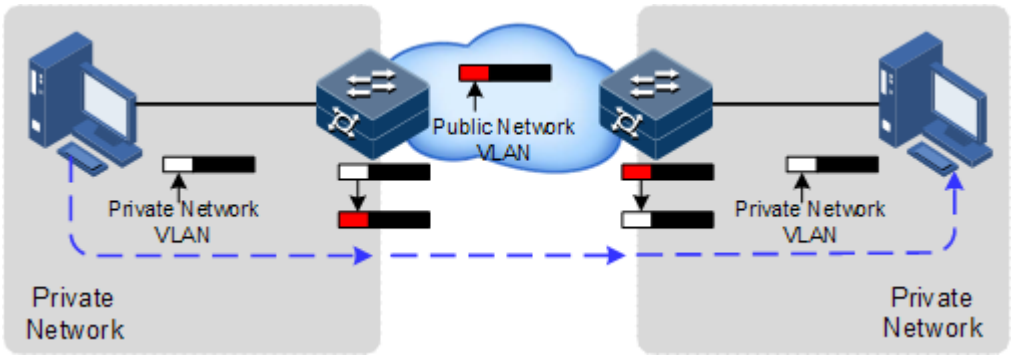
```
SwitchA#show vlan-mapping both interface gigaethernet 1/1/1
Based inner VLAN flexible QinQ mapping rule:
Interface          CVLAN   Add-SVlan   Cos   CVlan-Action Translate-
CVlan Hardware
-------------------------------------------------------------------------
gigaethernet1/1/1    100     1000       0     Reserve     -
Yes
gigaethernet1/1/2    200     2000       0     Reserve     -
Yes
```

3.6 VLAN 转换

3.6.1 简介

VLAN 转换主要功能是将以太网业务报文中的私网 VLAN Tag 替换为运营商的 VLAN Tag，使其按照运营商的 VLAN 转发规则进行传输。在报文从运营商网络转发到对端用户私网时，再按照同样的规则将 VLAN Tag 恢复为原有的用户私网 VLAN Tag，使报文正确到达目的地。VLAN 转换原理如图 3-11 所示。

图3-11 VLAN 转换原理组网示意图



交换机收到带有用户私网报文的 VLAN Tag 后，根据配置的 VLAN 转换规则对用户私网报文的 VLAN Tag 进行匹配，如果匹配成功，则按照 VLAN 转换规则将私网 VLAN Tag 进行替换。设备支持 1:1 的 VLAN 转换，即将来自某一特定 VLAN 的报文所携带的 VLAN Tag 替换为新的 VLAN Tag。

与 QinQ 功能不同的是，VLAN 转换功能不需要对报文进行多层 VLAN Tag 的封装，只需要更改 VLAN Tag 标记即可，使其按照运营商的 VLAN 转发规则进行传输。

3.6.2 配置准备

场景

与 QinQ 区别的是，VLAN 转换只是变更 VLAN 标签，不额外进行多层 VLAN Tag 的封装，只需要更改 VLAN Tag 标记即可，使其按照运营商的 VLAN 转发规则进行传输，不会增加原报文的帧长度。VLAN 转换可以用在如下场景：

- 用户业务转换为一个运营商的 VLAN ID。
- 多种用户业务转换为一个运营商的 VLAN ID。

前提

在配置 VLAN 转换之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。
- 创建 VLAN。

3.6.3 VLAN 转换的缺省配置

设备上 VLAN 转换的缺省配置如下。

功能	缺省值
VLAN 转换功能状态	禁止

3.6.4 配置 VLAN 转换

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**switchport vlan-mapping both outer** *vlan-id* **translate** *vlan-id* Inspur(config-gigaethernet1/1/*)#**switchport vlan-mapping both outer** *vlan-id* **inner** *inner -vlan-id* **translate outer** *vlan-id* **inner** *inner -vlan-id*	配置双方向基于内外层 VLAN 的 VLAN 转换规则。
4	Inspur(config-gigaethernet1/1/*)#**switchport vlan-mapping both** *vlan-list* **translate** *vlan-id*	配置双方向的 N:1 VLAN 转换规则。

说明

- 同一接口下，双层 VLAN 转换不能与基本 QinQ、单层 CVLAN/Priority-Tagged 的 VLAN 转换同时配置。
- 当同时配置 N:1 VLAN 转换和 VLAN COPY 功能时，需要先配置 VLAN COPY，后配置 N:1 VLAN 转换；
- 当同时配置 N:1 VLAN 转换和 PIM 功能时，需要先配置 PIM，后配置 N:1 VLAN 转换；

3.6.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show vlan-mapping both interface** *interface-type interface-number*	查看 VLAN 配置信息。
2	Inspur#**show vlan-mapping interface** *interface-type interface-number* **both translate**	查看接口的 N:1 转换配置信息。

3.6.6 配置 VLAN 转换示例

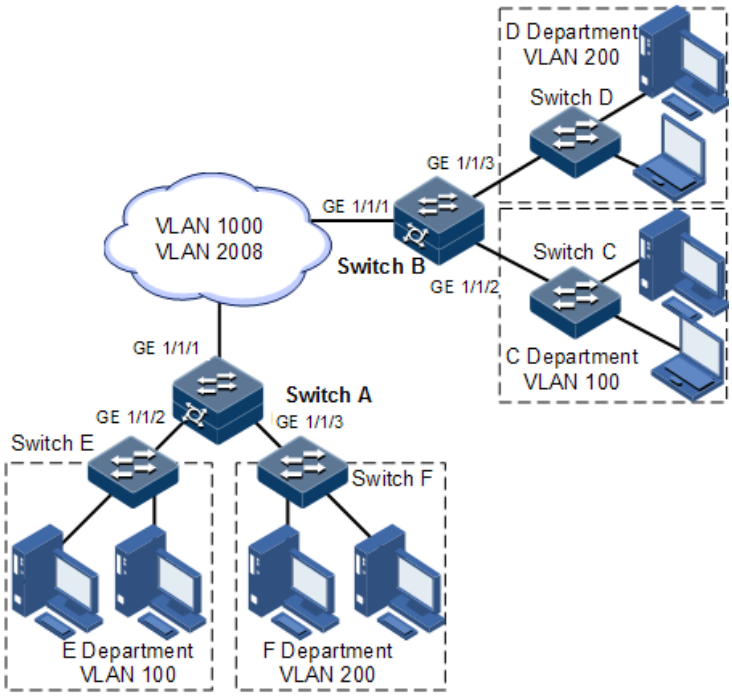
组网需求

如图 3-12 所示，Switch A 的 GE1/1/2 和 GE1/1/3 分别连接使用 VLAN 100 的 E 部门和使用 VLAN 200 的 F 部门，Switch B 的 GE 1/1/2 和 GE 1/1/3 分别连接使用 VLAN 100

的 C 部门和使用 VLAN 200 的 D 部门。在运营商网络中为 E 部门和 C 部门分配 VLAN 1000 来传输，为 F 部门和 D 部门分配使用 VLAN 2008 来传输。

通过在 Switch A 和 Switch B 配置 1:1 的 VLAN 转换功能来实现 PC 用户和终端用户与其服务器之间的正常通信。

图3-12 VLAN 转换应用组网示意图



配置步骤

Switch A 和 Switch B 配置相同，在这里只描述 Switch A 的配置信息。

步骤 1 创建 VLAN 并激活。

```
Inspur#name SwitchA
SwitchA#config
SwitchA(config)#create vlan 100,200,1000,2008 active
```

步骤 2 配置接口 GE 1/1/1 为 Trunk 模式，允许 VLAN 1000 和 VLAN 2008 通过。

```
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport mode trunk
SwitchA(config-gigaethernet1/1/1)#switchport trunk allowed vlan 1000,2008
confirm
SwitchA(config-gigaethernet1/1/1)#exit
```

步骤 3 配置接口 GE 1/1/2 为 Trunk 模式，允许 VLAN 100 通过，配置 VLAN 转换规则。

```
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#switchport mode trunk
SwitchA(config-gigaethernet1/1/2)#switchport trunk allowed vlan 100
confirm
```

```
SwitchA(config-gigaethernet1/1/2)#switchport vlan-mapping both outer 100
translate 1000
SwitchA(config-gigaethernet1/1/2)#exit
```

步骤 4 配置接口 GE 1/1/3 为 Trunk 模式，允许 VLAN 200 通过，配置 VLAN 转换规则。

```
SwitchA(config)#interface gigaethernet 1/1/3
SwitchA(config-gigaethernet1/1/3)#switchport mode trunk
SwitchA(config-gigaethernet1/1/3)#switchport trunk allowed vlan 200
confirm
SwitchA(config-gigaethernet1/1/3)#switchport vlan-mapping both outer 200
translate 2008
```

检查结果

通过 **show vlan-mapping both interface** 命令查看 1:1 VLAN 转换配置。

```
SwitchA#show vlan-mapping both interface gigaethernet 1/1/2
Both Direction VLAN QinQ mapping rule:
Interface  : GE 1/1/2
Default cvlan: --
---------------------------
Original Outer VLANs: 100
Original Outer COS:   --
Original Inner VLANs: --
Original Inner COS:   --
Vlan mapping Mode:    S-TRANS
New Outer-VID:       1000
New Outer-COS:       --
New Inner-VID:       --
New Inner-COS:       --

-------------------------

SwitchA#show vlan-mapping both interface gigaethernet 1/1/3
Both Direction VLAN QinQ mapping rule:
Interface  : GE 1/1/3
Default cvlan: --
---------------------------
Original Outer VLANs: 200
Original Outer COS:   --
Original Inner VLANs: --
Original Inner COS:   --
Vlan mapping Mode:    S-TRANS
New Outer-VID:       2008
New Outer-COS:       --
New Inner-VID:       --
New Inner-COS:       --
```

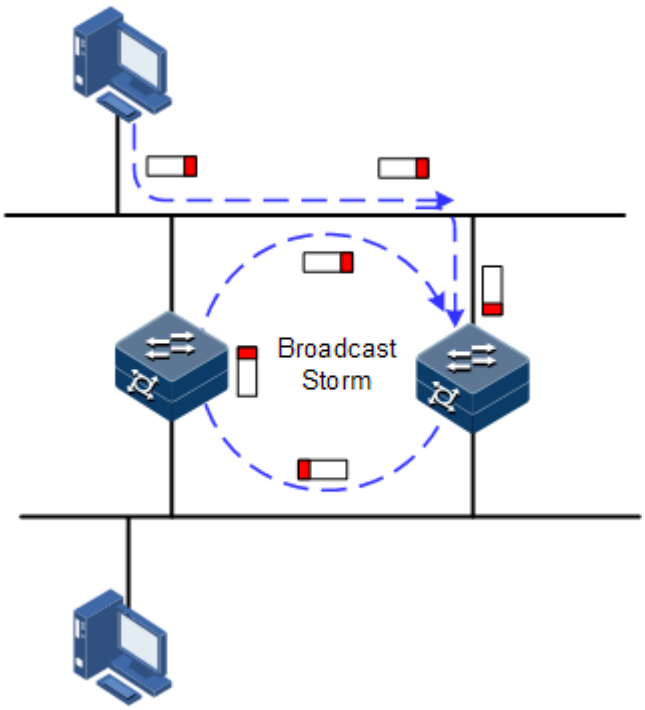
3.7 STP/RSTP

3.7.1 简介

STP

随着网络结构的日益复杂和网络中交换机数量的增多，网络环路成为以太网中最突出的问题。由于交换机对报文的广播机制，网络环路会使得网络中产生网络风暴，耗尽网络资源，对正常的数据转发产生严重的影响。由于网络环路产生的网络风暴示意图如图 3-13 所示。

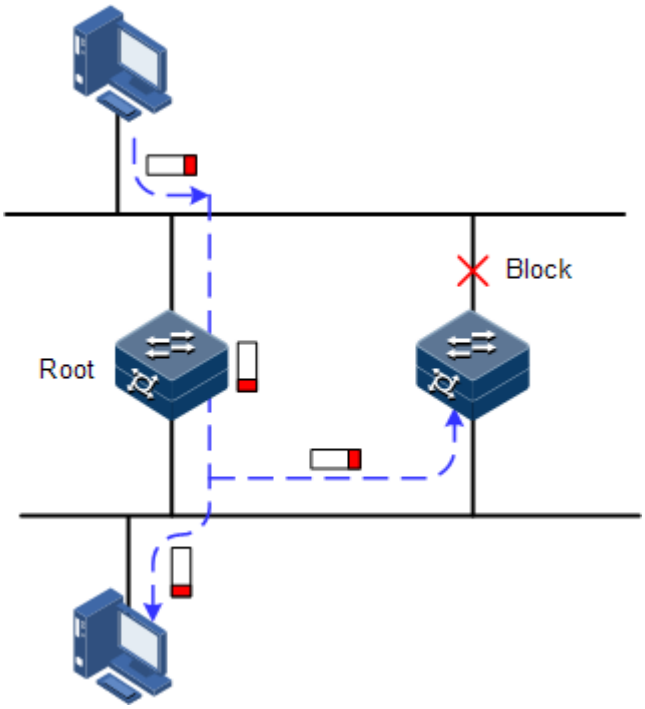
图3-13 网络环路造成网络风暴示意图



STP（Spanning Tree Protocol，生成树协议）是根据 IEEE 802.1d 标准建立的，用于在局域网中消除数据链路层物理环路的协议。

运行 STP 的设备可以通过彼此交互 BPDU（Bridge Protocol Data Unit，桥协议数据单元）报文进行根交换机的选举、根端口和指定端口的选择，并根据选择结果对设备中存在环路的接口进行逻辑上的阻塞，最终将环路网络结构修剪成以某一台设备为根（Root）的无环路的树型网络结构，从而防止报文在环路网络中不断增生和无限循环而导致广播风暴，并避免主机由于重复接收相同的报文造成的报文处理能力下降的问题发生。运行了 STP 协议的环网示意图如图 3-14 所示。

图3-14 运行 STP 协议的环网示意图



虽然 STP 协议能够很好的消除环网，防止广播风暴的产生，但是随着应用的深入和网络技术的发展，STP 协议的缺点也逐渐暴露了出来。

STP 协议的主要缺点表现在收敛速度较慢。

RSTP

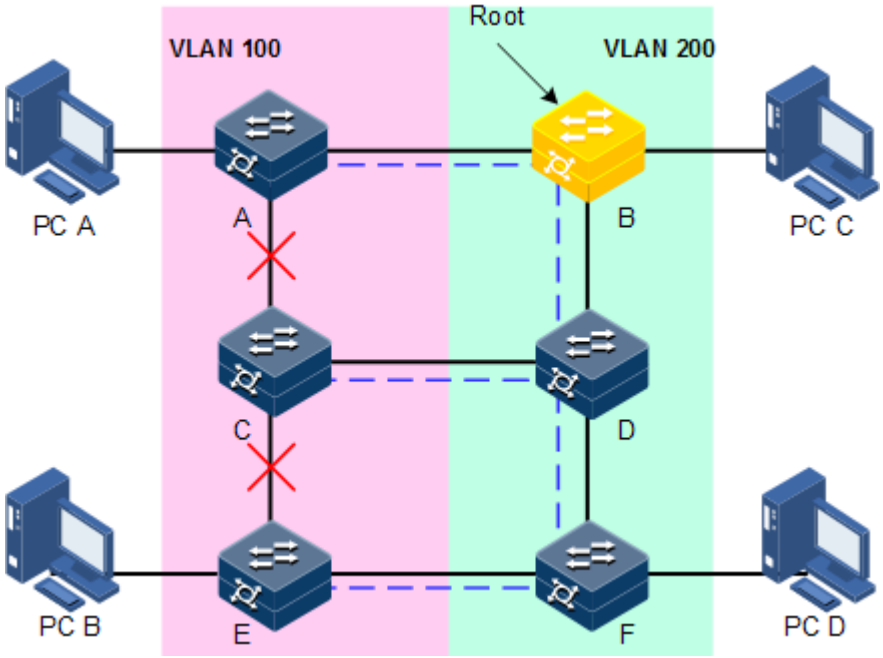
为了弥补 STP 协议收敛速度较慢的不足，IEEE 802.1w 制定了 RSTP（Rapid Spanning Tree Protocol，快速生成树协议）。在普通 STP 协议的基础上，增加了接口可以快速由阻塞状态转变为转发状态的机制，加快了拓扑的收敛速度。

STP/RSTP 协议的目的都是将一个桥接的局域网，修剪成为逻辑拓扑上的一棵单一的生成树，从而避免广播风暴的产生。

由于 VLAN 技术快速发展，STP/RSTP 的局限性逐渐暴露出来。STP/RSTP 协议将网络拓扑修剪为单一生成树，会导致以下问题：

- 整个交换网络只有一个生成树，在网络规模比较大的时候会导致较长的收敛时间。
- 链路被阻塞后将不承载任何流量，造成带宽的浪费。
- 在网络结构不对称时，可能造成部分 VLAN 的报文无法转发。如图 3-15 所示，由于 RSTP 协议，选举 Switch B 为根交换机，且逻辑上阻断了 Switch A 和 Switch C 之间的链路，造成 VLAN 100 中的 VLAN 报文无法转发，Switch A 和 Switch C 无法通信。

图3-15 RSTP 协议造成 VLAN 报文无法转发示意图



3.7.2 配置准备

场景

在较大型的局域网中，有多台设备进行级连满足多主机相互访问的需求，为防止设备之间组成环路造成 MAC 地址学习错误，并导致数据帧快速在环路中进行复制转发造成广播风暴、网络瘫痪，需要在这些设备上开启 STP。通过 STP 协议计算，阻塞掉环路当中的其中一个接口，保证每一个数据流去往目的主机的路径只有一条，并且被 STP 协议计算为最优路径。

前提

无

3.7.3 STP 的缺省配置

设备上 STP 的缺省配置如下。

功能	缺省值
全局 STP 功能状态	禁止
接口 STP 功能状态	使能
设备的 STP 优先级	32768
接口的 STP 优先级	128

功能	缺省值
接口的路径开销	0
Max Age 定时器	20s
Hello Time 定时器	2s
Forward Delay 定时器	15s

3.7.4 使能 STP 功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**spanning-tree enable**	使能全局生成树协议。
3	Inspur(config)#**spanning-tree mode** { **stp** | **rstp** }	配置生成树的运行模式。
4	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
5	Inspur(config-gigaethernet1/1/*)#**spanning-tree enable**	使能接口生成树协议。

3.7.5 配置 STP 参数

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**spanning-tree** [**instance** *instance-id*] **priority** *priority-value*	（可选）配置设备优先级。
3	Inspur(config)#**spanning-tree** [**instance** *instance-id*] **root** { **primary** | **secondary** }	（可选）配置设备为根设备或备份根设备。
4	Inspur(config)#**interface** *interface-type interface-number* Inspur(config-gigaethernet1/1/*)#**spanning-tree** [**instance** *instance-id*] **priority** *priority-value*	（可选）配置设备接口优先级。
5	Inspur(config-gigaethernet1/1/*)#**spanning-tree extern-path-cost** *cost-value* Inspur(config-gigaethernet1/1/*)#**exit**	（可选）配置设备接口路径开销。

步骤	配置	说明
6	Inspur(config)#**spanning-tree hello-time** *value*	（可选）配置 Hello Time 的值。
7	Inspur(config)#**spanning-tree transmit-limit** *value*	（可选）配置接口最大发送速率。
8	Inspur(config)#**spanning-tree forward-delay** *value*	（可选）配置 Forward Delay 的值。
9	Inspur(config)#**spanning-tree max-age** *value*	（可选）配置 Max Age 的值。
10	Inspur(config)#**spanning-tree pathcost-standard** { **dot1d-1998** | **dot1t** }	（可选）配置生成树路径开销计算标准。

3.7.6（可选）配置 RSTP 边缘接口

边缘接口是指不直接与任何设备连接，也不通过接口所连接的网络间接与任何设备相连的接口。

设置为边缘接口能够使该接口的状态迅速转变为转发状态，而不需要时间等待，对于直接与用户终端相连的以太网接口，为能使其快速迁移到转发状态，应将其设置为边缘接口。

当某个接口设置为边缘接口自动检测（auto）则边缘接口的属性是由实际情况决定的。当某个接口设置为边缘接口（force-true）时，当接口收到 BPDU 后实际运行值会变为非边缘接口。当某个接口设置为非边缘接口（force-false）时，同样，无论其实际情况下为边缘或非边缘接口，此接口会保持为非边缘接口，直到配置改变。

缺省情况下，以太网设备中所有接口的均设置为自动检测属性。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**spanning-tree edged-port** { **auto** | **force-true** | **force-false** }	配置 RSTP 边缘接口属性。

3.7.7（可选）配置 RSTP 链路类型

点对点链路相连的两个接口可以通过传送同步报文快速迁移到转发状态，减少了不必要的转发延迟时间。缺省情况下，MSTP 根据双工状态设定接口的链路类型。全双工接口被认为是点到点链路，半双工被认作共享链路。

用户可以手工强行配置当前以太网接口与点对点链路相连，但是如果该链路不是点到点链路会使系统出现问题，一般情况下建议用户将此配置项设为自动状态，由系统自动发现接口是否与点到点链路相连。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**spanning-tree link-type** { **auto** | **point-to-point** | **shared** }	配置接口的链路类型。

3.7.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

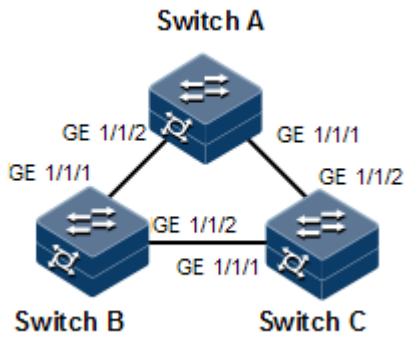
序号	检查项	说明
1	Inspur#**show spanning-tree**	查看 STP 基本配置信息。
2	Inspur#**show spanning-tree** *interface-type interface-list* [**detail**]	查看接口下生成树配置信息。

3.7.9 配置 STP 示例

组网需求

如图 3-16 所示，三台设备 Switch A、Switch B 和 Switch C 组网成一个环，需在物理链路成环情况下解决环路问题，三台设备上需开启 STP，并设置 Switch A 的优先级为 0，Switch B 到 Switch A 的开销改为 10。

图3-16 STP 应用组网示意图



配置步骤

步骤 1 在三台设备上均开启 STP 功能。

配置 Switch A。

```
Inspur#hostname SwitchA
SwitchA#config
SwitchA(config)#spanning-tree enable
SwitchA(config)#spanning-tree mode stp
```

配置 Switch B。

```
Inspur#hostname SwitchB
SwitchB#config
SwitchB(config)#spanning-tree enable
SwitchB(config)#spanning-tree mode stp
```

配置 Switch C。

```
Inspur#hostname SwitchC
SwitchC#config
SwitchC(config)#spanning-tree enable
SwitchC(config)#spanning-tree mode stp
```

步骤 2 配置三台设备的接口模式。

配置 Switch A。

```
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport mode trunk
SwitchA(config-gigaethernet1/1/1)#exit
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#switchport mode trunk
SwitchA(config-gigaethernet1/1/2)#exit
```

配置 Switch B。

```
SwitchB(config)#interface gigaethernet 1/1/1
SwitchB(config-gigaethernet1/1/1)#switchport mode trunk
SwitchB(config-gigaethernet1/1/1)#exit
SwitchB(config)#interface gigaethernet 1/1/2
SwitchB(config-gigaethernet1/1/2)#switchport mode trunk
SwitchB(config-gigaethernet1/1/2)#exit
```

配置 Switch C。

```
SwitchC(config)#interface gigaethernet 1/1/1
SwitchC(config-gigaethernet1/1/1)#switchport mode trunk
SwitchC(config-gigaethernet1/1/1)#exit
SwitchC(config)#interface gigaethernet 1/1/2
SwitchC(config-gigaethernet1/1/2)#switchport mode trunk
SwitchC(config-gigaethernet1/1/2)#exit
```

步骤 3 配置生成树优先级及接口路径开销。

配置 Switch A。

```
SwitchA(config)#spanning-tree priority 0
```

```
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#spanning-tree extern-path-cost 10
```

配置 Switch B。

```
SwitchB(config)#interface gigaethernet 1/1/1
SwitchB(config-gigaethernet1/1/1)#spanning-tree extern-path-cost 10
```

检查结果

通过 **show spanning-tree** 命令查看桥状态，以 Switch A 为例。

```
SwitchA#show spanning-tree
Spanning-tree admin state: enable
Spanning-tree protocol mode: STP
Spanning-tree pathcost-standard: Dot1t
BridgeId:    Mac 5051.5051.5053  Priority 0
Root:       Mac 5051.5051.5053  Priority 0     RootCost 0
Operational:  HelloTime 2   ForwardDelay 15  MaxAge 20
Configured:   HelloTime 2   ForwardDelay 15  MaxAge 20  TransmitLimit 3
           MaxHops   20  Diameter 7
```

通过 **show spanning-tree** *interface-type interface-number* 查看接口状态，以 Switch A 为例。

```
SwitchA#show spanning-tree gigaethernet 1/1/1
GE1/1/1
PortProtocolEnable: admin: enable oper: enable
Rootguard:  disable
Loopguard:  disable
Bpduguard:  disable
TcRejection:disable
ExternPathCost:20000
Partner STP Mode: stp
Bpdus send:   48    (TCN<0>  Config<48>  RST<0>  MST<0>)
Bpdus received:0     (TCN<0>  Config<0>  RST<0>  MST<0>)
State:forwarding  Role:designated  Priority:128    Cost: 20000
Root:           Mac 5051.5051.5053  Priority 0      RootCost       0
DesignatedBridge: Mac 5051.5051.5053  Priority 0      DesignatedPort
33041
```

3.8 MSTP

3.8.1 简介

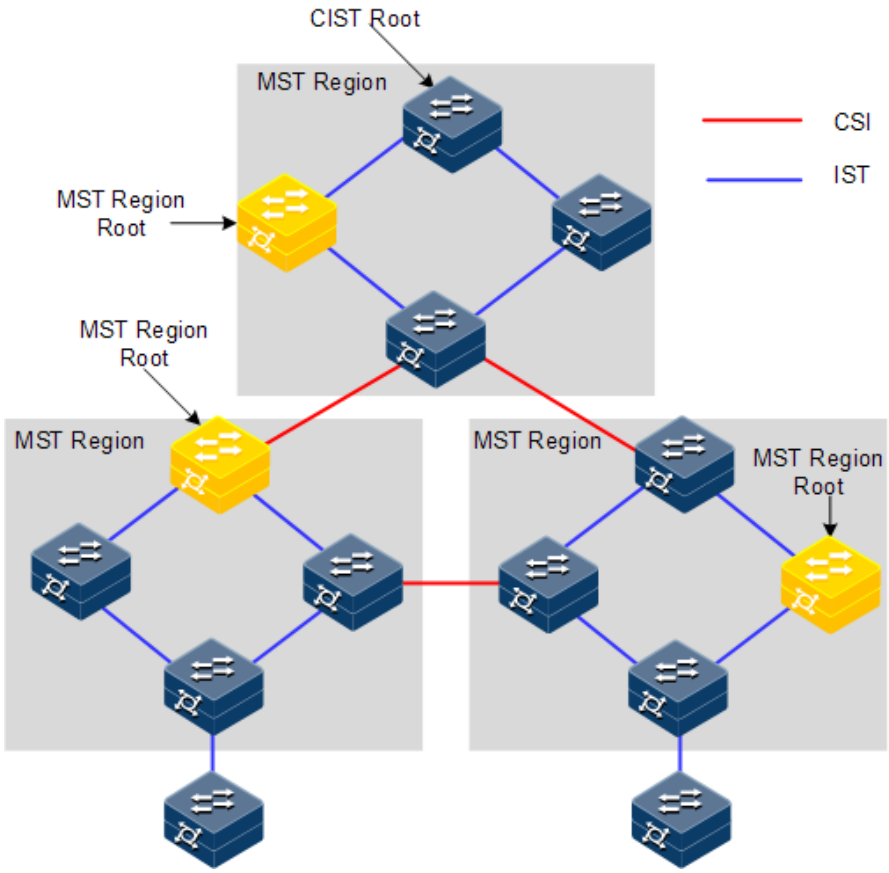
IEEE 802.1s 标准定义了 MSTP（Multiple Spanning Tree Protocol，多生成树协议）。MSTP 可以弥补 STP 和 RSTP 的缺陷，既可以快速收敛，也能使不同 VLAN 的流量沿各自的路径分发，从而提供了很好的负荷分担机制。

MSTP 把一个交换网络划分成多个域，每个域叫做一个 MST 域。每个域内形成多棵生成树，生成树之间彼此独立。每棵生成树叫做一个 MSTI（Multiple Spanning Tree Instance，多生成树实例）。

MSTP 协议引入了 CST（Common Spanning Tree，公共生成树）和 IST（Internal Spanning Tree，内部生成树）的概念。其中 CST 是指把 MST 域当成一个整体时，计算生成的一棵生成树。而 IST 是指在 MST 域内部生成的生成树。

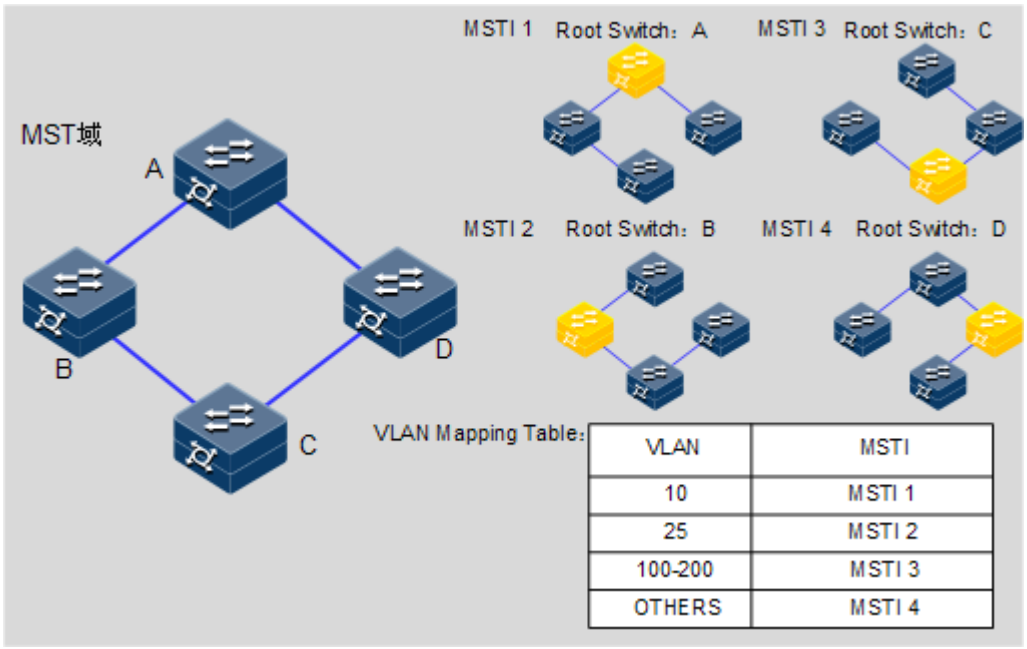
与 STP 和 RSTP 相比，MSTP 中还引入了总根（CIST Root）和域根（MST Region Root）的概念。总根是一个全局概念，对于所有运行的 STP/RSTP/MSTP 的交换机只能有 1 个总根，也即是 CIST 的根。而域根是一个局部概念，是相对于某个域的某个实例而言。如图 3-17 所示，所有相连的设备，总根只有 1 个，而每个域包含的域根数目与实例个数相关。

图3-17 MSTP 网络基本概念示意图



在每个 MST 域中，可以有不同的 MST 实例，通过设置 VLAN 映射表（即 VLAN 和 MSTI 的对应关系表），把 VLAN 和 MSTI 联系起来。MSTI 概念示意图如图 3-18 所示。

图3-18 MSTI 概念示意图

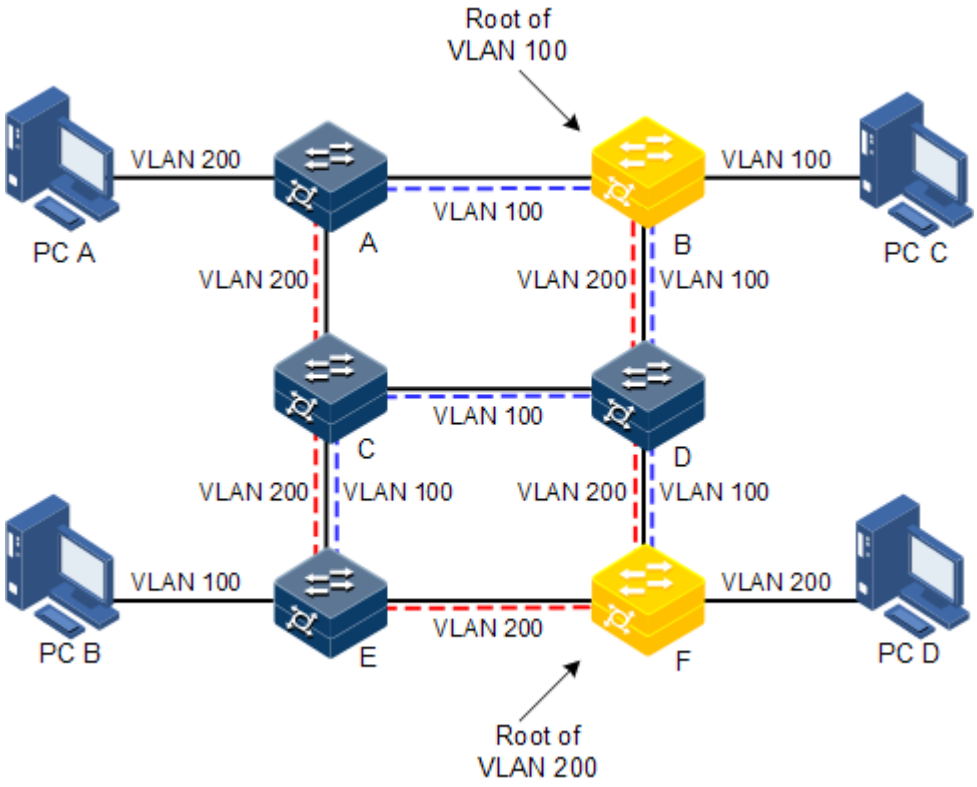


说明

每个 VLAN 只能对应一个 MSTI，即同一 VLAN 的数据只能在一个 MSTI 中传输；而一个 MSTI 可能对应多个 VLAN。

MSTP 协议相对于之前的 STP 协议和 RSTP 协议，优势非常明显。MSTP 具有 VLAN 认知能力，可以实现负载均衡分担，可以实现类似 RSTP 的端口状态快速切换，可以捆绑多个 VLAN 到一个 MST 实例中，以降低资源占用率。此外，网络中运行 MSTP 协议的设备可以很好的与运行 STP 协议和 RSTP 协议的设备兼容。

图3-19 MST 域内多生成树实例组网示意图



将 MSTP 应用于如图 3-19 所示的网络，经计算最终生成两棵生成树（也即 2 个 MST 实例）：

- MSTI1 以 B 为根交换设备，转发 VLAN100 的报文；
- MSTI2 以 F 为根交换设备，转发 VLAN200 的报文。

这样所有 VLAN 内部可以互通，同时不同 VLAN 的报文沿不同的路径转发，实现了负荷分担。

3.8.2 配置准备

场景

大型局域网或小区汇聚时，汇聚设备之间组成一个环作为线路的备份，在实现线路备份的同时，需要防止环路以及实现业务的负载分担，MSTP 协议可以为每一个或一组 VLAN 选择不同且唯一的转发路径。

前提

无

3.8.3 MSTP 的缺省配置

设备上 MSTP 的缺省配置如下。

功能	缺省值
全局 MSTP 功能状态	禁止
接口 MSTP 功能状态	使能
MST 域的最大跳数	20
设备的 MSTP 优先级	32768
接口的 MSTP 优先级	128
接口的路径开销	0
每个 Hello time 内的最大发送报文数量	3
Max Age 定时器	20s
Hello Time 定时器	2s
Forward Delay 定时器	15s
MST 域的修订级别	0

3.8.4 使能 MSTP 功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**spanning-tree mode mstp**	配置生成树模式为 MSTP。
3	Inspur(config)#**spanning-tree enable**	使能全局生成树协议。
4	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式或聚合组接口配置模式。
5	Inspur(config-gigaethernet1/1/*)#**spanning-tree enable**	使能接口生成树协议，支持聚合组接口。

3.8.5 配置 MST 域和 MST 域最大跳数

当设备的运行模式为 MSTP 时，可为设备设置其归属的域信息。设备属于哪个 MST 域，是由域名，VLAN 映射表，MSTP 修订级别配置决定的。用户可以通过下面的配置过程将当前设备划分在一个特定的 MST 域内。

MST 域的最大跳数限制了 MST 域的规模。从域内的生成树的根桥开始，域内的配置消息（BPDU）每经过一台设备的转发跳数就被减 1，设备将丢弃收到的跳数为 0 的配置消息。使处于最大跳数外的设备无法参与生成树的计算，从而限制了 MST 域的规模。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**spanning-tree region-configuration**	进入 MST 域配置模式。
3	Inspur(config-region)#**name** *name*	配置 MST 域名。
4	Inspur(config-region)#**revision-level** *level-value*	配置 MST 域的修订级别。
5	Inspur(config-region)#**instance** *instance-id* **vlan** *vlan-list* Inspur(config-region)#**exit**	配置 MST 域的 VLAN 到实例映射关系。
6	Inspur(config)#**spanning-tree max-hops** *hops-value*	配置设备 MST 域最大跳数。

说明

当且仅当配置的设备为域根时，配置的最大跳数才作为 MST 域的最大跳数，其他非域根桥配置此项无效。

3.8.6 配置根桥/备份根桥

MSTP 根桥的选举，一方面可以通过配置设备的优先级，然后经过生成树计算，来确定生成树的根桥或备份根桥；另一方面，用户也可以通过此命令来直接指定。当根桥出现故障或被关机时，备份根桥可以取代根桥成为相应实例的根桥。此时如果用户设置了新的根桥，则备份根桥将不会成为根桥。如果用户为一棵生成树实例配置了多个备份根桥，当根桥失效时，MSTP 将选择 MAC 地址最小的那个备份根桥作为根桥。

注意

如果采用这种直接指定根桥的方式，建议用户不要再修改网络中任何设备的优先级，否则，可能会造成指定根桥或备份根桥无效。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**spanning-tree** [**instance** *instance-id*] **root** { **primary** | **secondary** }	为某个生成树实例，设置设备为根桥或备份根桥。

说明

- 用户可以通过参数 **instance** *instance-id* 确定根桥或备份根桥生效的实例。如果 *instance-id* 取值为 0，或者省去参数 **instance** *instance-id* 时，当前设备将被指定为 CIST 的根桥或备份根桥。
- 设备在各实例中的根类型是互相独立的，即它既可以作为一个实例的根桥或备份根桥，同时又可以作为其他生成树实例的根桥或备份根桥。但在同一棵生成树实例中，同一台设备不能既作为根桥，又作为备份根桥。
- 用户不能同时为一棵生成树实例指定两个或两个以上的根桥。相反，用户可以给同一棵生成树指定多个备份树根。一般情况下，建议用户给一棵生成树指定一个树根和多个备份树根。

3.8.7 配置设备接口和系统的优先级

接口是否被选为根接口需要根据接口优先级进行判断。同等条件下，接口优先级值越小，接口越优先被选为根接口。接口可在不同的实例中具有不同的接口优先级，也可以在不同实例中充当不同的角色。

设备 Bridge ID 的大小决定了这台设备是否能够被选作生成树的根。通过配置较小的优先级，可以得到较小的设备 Bridge ID，达到指定某台设备成为生成树树根的目的。优先级相同的情况下，MAC 地址小的为树根。

与配置根与备份根相同，优先级在不同实例中的配置相互独立。用户可以通过参数 **instance** *instance-id* 确定的配置优先级的实例。如果 *instance-id* 取值为 0，或者省去参数 **instance** *instance-id* 时，则是为 CIST 配置的桥优先级。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式或聚合组接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**spanning-tree** [**instance** *instance-id*] **priority** *priority-value* Inspur(config-gigaethernet1/1/*)#**exit**	配置某个生成树实例的接口优先级。
4	Inspur(config)#**spanning-tree** [**instance** *instance-id*] **priority** *priority-value*	配置某个生成树实例的系统优先级。

说明

优先级取值必须为 4096 的倍数，如 0、4096、8192 等，缺省值为 32768。

3.8.8 配置交换网络的网络直径

网络直径指的是交换网络中设备个数最多的那条路径上节点的个数。在 MSTP 中，设置网络直径只对 CIST 有效，对 MST 实例无效。并且在相同域内，无论路径经过多少节点，只当作一个节点计算。实际上，网络直径应定义为跨越域最多的那条路径上，域的个数。如果整个网络只有一个域，那么运行网络直径就为 1。

对比 MST 域的最大跳数是用来表征域的规模，网络直径则是表征整个网络规模的一个参数。网络直径越大说明一个网络的规模越大。

与 MST 域的最大跳数类似，当且仅当配置的设备为 CIST 根设备时，配置生效。当用户配置设备的网络直径参数时，MSTP 通过计算自动将设备的 Hello Time，Forward Delay 以及 Max Age 三个时间参数设置为一个较优的值。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**spanning-tree bridge-diameter** *bridge-diameter-value*	配置交换网络直径。

3.8.9 配置接口的内部路径开销

在选举根接口（root port）和指定接口（designated port）时，路径开销越小的接口越容易被选举为根接口或者指定接口。接口的内部路径开销在不同实例中的配置相互独立。用户可以通过参数 **instance** *instance-id* 确定的配置接口的内部路径开销的实例。如果 *instance-id* 取值为 0，或者省去参数 **instance** *instance-id* 时，则是为 CIST 配置的接口内部路径开销。

接口的开销一般依据其物理特性，缺省情况如下：

- 10Mbit/s 为 2000000
- 100Mbit/s 为 200000
- 1000Mbit/s 为 20000
- 10Gbit/s 为 2000

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式或聚合组接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**spanning-tree** [**instance** *instance-id*] **inter-path-cost** *cost-value*	配置接口的内部路径开销。

3.8.10 配置接口的外部路径开销

外部路径开销是设备到 CIST 总根的路径开销，同一个域内外部路径开销是相同。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式或聚合组接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**spanning-tree extern-path-cost** *cost-value*	配置接口的外部路径开销。

3.8.11 配置接口最大发送速率

MSTP 每 Hello Time 时间内允许发送的最大 BPDU 数量。此参数是一个相对值，没有单位，该参数被配置得越大，则每个 Hello Time 内允许发送的报文个数就越多，同时也会占用会更多的设备资源。与时间参数相同，只有根设备的此项配置生效。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**spanning-tree transit-limit** *value*	配置接口最大发送速率。

3.8.12 配置 MSTP 定时器

- Hello Time：设备定期发送桥配置信息（BPDU）的时间间隔，用于设备检测链路是否存在故障。设备每隔 Hello Time 时间，会向周围的设备发送 Hello 报文，以确认链路是否存在故障。缺省值为 2s，用户可以根据网络情况对此值进行调整。当网络中链路出现频繁变化时，可以适当缩短该值，来增强生成树协议的健壮性。相反，增大此值则可以降低生成树协议对系统 CPU 资源的占用率。
- Forward Delay：保证设备状态安全迁移的时间参数。链路故障会引发网络重新进行生成树的计算，不过重新计算得到的新配置消息无法立刻传遍整个网络。如果新选出的根接口和指定接口立刻开始数据转发，可能会造成暂时性的路径回环。为此协议采用了一种状态迁移的机制：根接口和指定接口重新开始数据转发之前，要经历一个中间状态（学习状态），中间状态经过 Forward Delay 时间的延时后，才能进入转发状态。这个延时保证了新的配置消息已经传遍整个网络。用户可以根据实际情况调整该值，当网络拓扑不频繁变化时可以将该值减小，反之增大。

- Max Age：生成树协议所使用的桥配置信息有生存周期，用来判断配置消息是否过时。设备会将过时的配置消息丢弃。当桥配置信息过期后，生成树协议将重新计算生成树。缺省值为 20s，该值过小会导致生成树重计算过于频繁，过大则会导致生成树协议不能及时适应网络拓扑结构的变化。

整个交换网络中所有的设备采用 CIST 根设备上的三个时间参数，因此只有在根设备上的配置生效。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**spanning-tree hello-time** *value*	配置 Hello Time 的值。
3	Inspur(config)#**spanning-tree forward-delay** *value*	配置 Forward Delay 的值。
4	Inspur(config)#**spanning-tree max-age** *value*	配置 Max Age 的值。

3.8.13 配置边缘接口

边缘接口是指不直接与任何设备连接，也不通过接口所连接的网络间接与任何设备相连的接口。

设置为边缘接口能够使该接口的状态迅速转变为转发状态，而不需要时间等待，对于直接与用户终端相连的以太网接口，为能使其快速迁移到转发状态，应将其设置为边缘接口。

当某个接口设置为边缘接口自动检测（auto）则边缘接口的属性是由实际情况决定的。当某个接口设置为边缘接口（force-true）时，当接口收到 BPDU 后实际运行值会变为非边缘接口。当某个接口设置为非边缘接口（force-false）时，同样，无论其实际情况下为边缘或非边缘接口，此接口会保持为非边缘接口，直到配置改变。

缺省情况下，以太网设备中所有接口的均设置为自动检测属性。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式或聚合组接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**spanning-tree edged-port** { **auto** | **force-true** | **force-false** }	配置接口边缘接口属性。

3.8.14 配置 BPDU 过滤

用户使能边缘接口的 BPDU 过滤功能后，边缘接口不会发送 BPDU 报文，也不会处理收到的 BPDU 报文。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**spanning-tree edged-port bpdu-filter enable** *interface-type interface-number*	使能边缘接口的 BPDU 过滤功能。

3.8.15 配置 BPDU 保护

在交换机上，通常将直接与用户终端（如 PC 机）或文件服务器等非交换机设备相连的接口配置为边缘接口，以实现这些接口的快速迁移。

正常情况下，这些边缘接口不会收到 BPDU。如果有人伪造 BPDU 恶意攻击交换机，当这些接口接收到 BPDU 时，会自动将这些接口设置为非边缘接口，并重新进行生成树计算，从而引起网络震荡。

MSTP 提供 BPDU 保护功能来防止这种攻击。启动 BPDU 保护功能后，可以防止伪造 BPDU 恶意攻击。

如果使能 BPDU 保护功能，则边缘接口收到了 BPDU，设备将关闭这些接口，同时通知网管系统。被关闭的接口只能由网络管理人员通过命令手动恢复。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**spanning-tree bpduguard enable**	使能 BPDU 保护功能。
3	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式或聚合组接口配置模式。
4	Inspur(config-gigaethernet1/1/*)#**no spanning-tree bpduguard shutdown port**	手动恢复由于 BPDU 保护生效 Down 掉的接口。

说明

当边缘接口使能了 BPDU 过滤功能，同时设备使能了 BPDU 保护功能，则 BPDU 保护功能优先生效，即边缘接口接收到 BPDU 报文时，接口被关闭。

3.8.16 配置 STP/RSTP/MSTP 模式切换

当生成树协议开启时，支持三种生成树运行模式，分别为 STP 兼容模式、RSTP 模式和 MSTP 模式。

- STP 兼容模式：不执行替换接口到根接口的快速转换和指定接口快速 Forwarding。只发送 STP 配置报文（STP Configuration BPDU）和拓扑变化通知（STP TCN BPDU）。收到 MST BPDU 将丢弃不识别部分。
- RSTP 模式：执行替换接口到根接口的快速转换和指定接口快速 Forwarding。只发送 RST BPDU。收到 MST BPDU 将丢弃不识别部分；如果本交换机接口的对端运行 STP 协议，接口将转移到 STP 兼容模式下。如果本交换机接口的对端运行 MSTP 协议，本接口依旧保持 RSTP 协议。
- MSTP 模式：发送 MST BPDU。如果本交换机接口的对端运行 STP 协议，接口将转移到 STP 兼容模式下。如果本交换机接口的对端运行 RSTP 协议，本接口依旧保持 MSTP 协议，仅将其作为域外信息处理。

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#spanning-tree mode { stp | rstp | mstp }`	配置生成树的运行模式。

3.8.17 配置链路类型

点对点链路相连的两个接口可以通过传送同步报文快速迁移到转发状态，减少了不必要的转发延迟时间。缺省情况下，MSTP 根据双工状态设定接口的链路类型。全双工接口被认为是点到点链路，半双工被认作共享链路。

用户可以手工强行配置当前以太网接口与点对点链路相连，但是如果该链路不是点到点链路会使系统出现问题，一般情况下建议用户将此配置项设为自动状态，由系统自动发现接口是否与点到点链路相连。

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#interface` *interface-type interface-number*	进入物理层接口配置模式或聚合组接口配置模式。
3	`Inspur(config-gigaethernet1/1/*)#spanning-tree link-type { auto | point-to-point | shared }`	配置接口的链路类型。

3.8.18 配置根接口保护

当桥收到更高优先级的报文的时候就需要重新选举，重新选举一个是会影响网络的连通性，二来会消耗 CPU 资源。对于开启了 MSTP 功能的网络，如果有人发送高优先级的 BPDU 报文进行攻击，网络就会由于不断的选举而导致不稳定。而一般而言，各个桥的优先级是在网络规划阶段就已经配置好，越是靠近边缘的桥优先级越低，因此下行接口一般不会收到比桥优先级高的报文，除非有人恶意攻击。对于这些接口，可以通过开启根接口保护功能，拒绝处理比桥优先级高的报文，并在收到高优先级报文的时候阻塞接口一段时间，防止攻击源的其他攻击损害更上层的链路。

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式或聚合组接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**spanning-tree rootguard enable**	使能接口的根接口保护功能。

3.8.19 配置接口环路保护

生成树主要作用有两个：防止环路和链路备份。防止环路就要求必须将拓扑裁剪成树状结构，而如果需要进行链路备份，拓扑中必须有冗余的链路。生成树就是通过阻塞冗余链路来达到防止环路的功能，而在链路发生故障的时候放开冗余链路从而达到链路备份的功能。

生成树模块会周期性交换报文，如果一定时间内没有收到报文即认为发生了链路故障。然后选举，放开备份接口。而在实际应用中，导致收不到报文的原因可能并不是链路故障，如果在这种情况下放开备份接口就有可能导致环路。

环路保护的目的是当接口在一定时间内收不到报文的时候，不进行重新选举，保持接口原来的状态不变。注意：环路保护的功能和链路备份的功能是对立的，也即环路保护是以失去链路备份功能的代价来实现环路避免。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式或聚合组接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**spanning-tree loopguard enable**	使能接口环路保护功能。

3.8.20 配置端口 TC 报文抑制功能

用户接入网络的拓扑改变会引起核心网络的转发地址更新，当用户接入网络的拓扑因某种原因而不稳定时，就会对核心网络形成冲击。为了避免这种情况，可以在端口上使能 TC 报文抑制功能，此后当该端口收到 TC 报文时，不会再向其他端口传播。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式或聚合组接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**spanning-tree tc-rejection** { **enable** | **disable** }	（可选）配置端口 TC 抑制功能

3.8.21 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show spanning-tree**	查看 STP 基本配置信息。
2	Inspur#**show spanning-tree** [**instance** *instance-id*] *interface-type interface-list* [**detail**]	查看接口下生成树配置信息。
3	Inspur#**show spanning-tree region-operation**	查看 MST 域操作信息。
4	Inspur(config-region)#**show spanning-tree region-configuration**	查看 MST 域配置信息。
5	Inspur(config-gigaethernet1/1/*)#**spanning-tree mcheck**	强制端口变为 MSTP 模式，以检查对端是否支持 MSTP。

3.8.22 维护

用户可以通过以下命令维护 MSTP 特性。

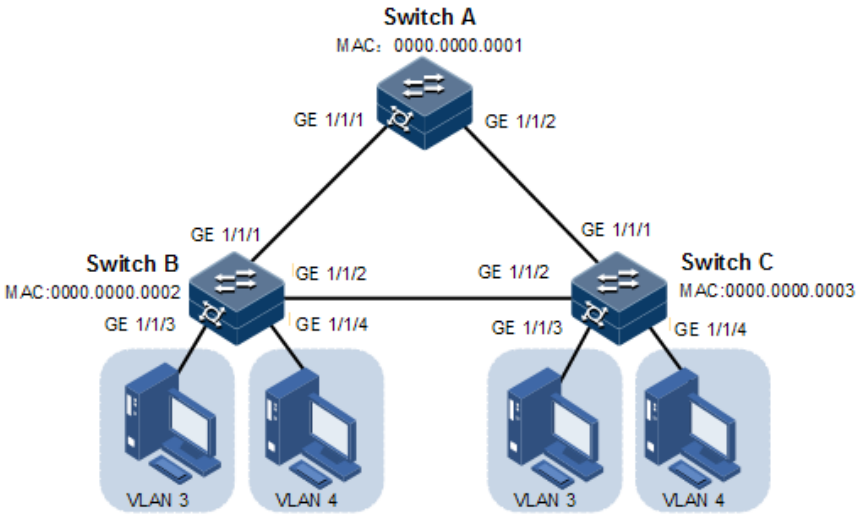
命令	描述
Inspur(config-gigaethernet1/1/*)#**spanning-tree clear statistics**	清除接口生成树统计信息。

3.8.23 配置 MSTP 示例

组网需求

如图 3-20 所示，三台交换机设备组成环形网络运行 MSTP 协议，域名 aaa。Switch B 和 Switch C 上分别各连接两台 PC，分别属于 VLAN 3 和 VLAN 4。实例 3 关联 VLAN 3，实例 4 关联 VLAN 4。配置 Switch B 实例 3 的路径开销，使两个 VLAN 的报文分别在两条路径进行转发，消除了环路的同时实现了负载分担。

图3-20 MSTP 应用组网示意图



配置步骤

步骤 1 在三台交换机上分别创建 VLAN 3 和 VLAN 4 并激活。

配置 Switch A。

```
Inspur#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 3,4 active
```

配置 Switch B。

```
Inspur#hostname SwitchB
SwitchB#config
SwitchB(config)#create vlan 3,4 active
```

配置 Switch C。

```
Inspur#hostname SwitchC
SwitchC#config
SwitchC(config)#create vlan 3,4 active
```

步骤 2 Switch A 的接口 GE 1/1/1、GE 1/1/2 以 Trunk 模式允许所有 VLAN 通过，Switch B 的接口 GE 1/1/1、GE 1/1/2 以 Trunk 模式允许所有 VLAN 通过，Switch C 的接口 GE 1/1/1、GE 1/1/2 以 Trunk 模式允许所有 VLAN 通过。Switch B、Switch C 的接口 GE 1/1/3、GE 1/1/4 以 Access 模式分别允许 VLAN 3、VLAN 4 通过。

配置 Switch A。

```
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport mode trunk
SwitchA(config-gigaethernet1/1/1)#exit
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#switchport mode trunk
SwitchA(config-gigaethernet1/1/2)#exit
```

配置 Switch B。

```
SwitchB(config)#interface gigaethernet 1/1/1
SwitchB(config-gigaethernet1/1/1)#switchport mode trunk
SwitchB(config-gigaethernet1/1/1)#exit
SwitchB(config)#interface gigaethernet 1/1/2
SwitchB(config-gigaethernet1/1/2)#switchport mode trunk
SwitchB(config-gigaethernet1/1/2)#exit
SwitchB(config)#interface gigaethernet 1/1/3
SwitchB(config-gigaethernet1/1/3)#switchport access vlan 3
SwitchB(config-gigaethernet1/1/3)#exit
SwitchB(config)#interface gigaethernet 1/1/4
SwitchB(config-gigaethernet1/1/4)#switchport access vlan 4
SwitchB(config-gigaethernet1/1/4)#exit
```

配置 Switch C。

```
SwitchC(config)#interface gigaethernet 1/1/1
SwitchC(config-gigaethernet1/1/1)#switchport mode trunk
SwitchC(config-gigaethernet1/1/1)#exit
SwitchC(config)#interface gigaethernet 1/1/2
SwitchC(config-gigaethernet1/1/2)#switchport mode trunk
SwitchC(config-gigaethernet1/1/2)#exit
SwitchC(config)#interface gigaethernet 1/1/3
SwitchC(config-gigaethernet1/1/3)#switchport access vlan 3
SwitchC(config-gigaethernet1/1/3)#exit
SwitchC(config)#interface gigaethernet 1/1/4
SwitchC(config-gigaethernet1/1/4)#switchport access vlan 4
SwitchC(config-gigaethernet1/1/4)#exit
```

步骤 3 Switch A、Switch B、Switch C 设置生成树模式为 MSTP，并开启生成树协议。进入 MSTP 配置模式设置域名为 aaa，修正版本为 0，instance 3 映射 VLAN 3、instance 4 映射 VLAN 4，退出 mst 配置模式。

配置 Switch A。

```
SwitchA(config)#spanning-tree mode mstp
SwitchA(config)#spanning-tree enable
SwitchA(config)#spanning-tree region-configuration
SwitchA(config-region)#name aaa
SwitchA(config-region)#revision-level 0
SwitchA(config-region)#instance 3 vlan 3
SwitchA(config-region)#instance 4 vlan 4
```

配置 Switch B。

```
SwitchB(config)#spanning-tree mode mstp
SwitchB(config)#spanning-tree enable
SwitchB(config)#spanning-tree region-configuration
SwitchB(config-region)#name aaa
SwitchB(config-region)#revision-level 0
SwitchB(config-region)#instance 3 vlan 3
SwitchB(config-region)#instance 4 vlan 4
SwitchB(config-region)#exit
```

配置 Switch C。

```
SwitchC(config)#spanning-tree mode mstp
SwitchC(config)#spanning-tree enable
SwitchC(config)#spanning-tree region-configuration
SwitchC(config-region)#name aaa
SwitchC(config-region)#revision-level 0
SwitchC(config-region)#instance 3 vlan 3
SwitchC(config-region)#instance 4 vlan 4
```

步骤 4 Switch B 修改生成树实例 3 接口 GE 1/1/1 的内部路径开销为 500000。

```
SwitchB(config)#interface gigaethernet 1/1/1
SwitchB(config-gigaethernet1/1/1)#spanning-tree instance 3 inter-path-
cost 500000
```

检查结果

通过 **show spanning-tree region-operation** 命令查看 MST 域的配置信息，以 Switch A 为例。

```
SwitchA#show spanning-tree region-operation
Operational Information:
---------------------------------------------
Name: aaa
Revision level: 0
Instances running: 3
Digest: 0X024E1CF7E14D5DBBD9F8E059D2C683AA
Instance   Vlans Mapped
--------   ------------------------------
0          1-2,5-4094
3          3
4          4
```

通过 **show spanning-tree instance 3** 查看多生成树实例 3 的基本信息是否正确，以 Switch A 为例。

```
SwitchA#show spanning-tree instance 3
Spanning-tree admin state: enable
Spanning-tree protocol mode: MSTP
Spanning-tree pathcost-standard: Dot1t

MST ID: 3
------------------------------------------------------------
BridgeId:    Mac 5051.5051.5053  Priority 32768
RegionalRoot: Mac 5051.5051.5053  Priority 32768  InternalRootCost 0
```

```
Port     PortState   PortRole   PathCost  PortPriority  LinkType
----------------------------------------------------------------
```

通过 **show spanning-tree instance 4** 查看多生成树实例 4 的基本信息是否正确，以 Switch A 为例。

```
SwitchA#show spanning-tree instance 4
Spanning-tree admin state: enable
Spanning-tree protocol mode: MSTP
Spanning-tree pathcost-standard: Dot1t

MST ID: 4
------------------------------------------------------------
BridgeId:    Mac 5051.5051.5053  Priority 32768
RegionalRoot: Mac 5051.5051.5053  Priority 32768  InternalRootCost 0
Port     PortState   PortRole   PathCost  PortPriority  LinkType
----------------------------------------------------------------
```

3.9 环路检测

3.9.1 简介

环路检测功能可以消除因环路对网络造成的影响，提高网络的自检错性、容错性和健壮性。

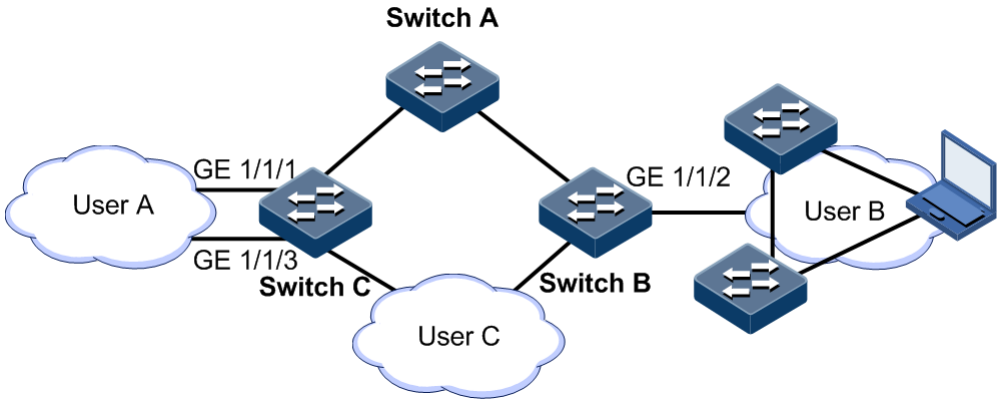
环路检测过程中每个开启环路检测功能的接口周期性地发送环路检测报文（Hello 报文），由于环路检测功能主要应用于网络边缘接口，因此，正常情况下边缘接口是不应该收到任何环路检测报文的。如果边缘设备接收到了环路检测报文，则认为网络出现了环路。接收环路检测报文分为两种情况：接收到了自身发送的报文和接收到了其他设备发送的报文，主要依据设备 MAC 地址和报文携带的 MAC 地址进行比较区分。

环路类型

常见的环路类型有自环、内环和外环三种。如图 3-21 所示，Switch B 和 Switch C 是连接用户网络的边缘交换机。

- 自环：同一设备上同一以太网接口下存在的用户环路，例如用户网络 B 自身存在环路使 Switch B 的 Gigaethernet 1/1/2 接口形成自环。
- 内环：同一设备上不同以太网接口之间形成的环路，例如 Switch C 的接口 Gigaethernet 1/1/1 和接口 Gigaethernet 1/1/3 与用户网络 A 形成内环。

图3-21 环路类型示意图



环路处理机制

设备遵循如下原则进行环路处理：

- 如果接收和发送环路检测报文的设备是同一设备，但不是同一接口，则处理接口号小的接口消除环路（内环）。
- 如果接收和发送环路检测报文的设备是同一设备且是同一接口，则处理该接口消除环路（自环）。

在图 3-21 中，假设 Switch B 和 Switch C 连接用户网络的接口都使能了环路检测功能。环路检测针对不同环路类型的处理机制如下：

- 对于自环，Switch B 收发报文接口号相同，将在 Gigaethernet 1/1/2 接口采取配置的环路检测动作来消除自环。
- 对于内环，Switch C 会收到自身发出的环路检测报文，而且收发报文接口号不同，因此会在接口号小的 Gigaethernet 1/1/1 采取配置的环路检测动作来消除内环。

环路处理动作

环路处理动作即设备检测到接口出现环路时的处理方式，用户可以根据实际情况在指定接口上配置不同的环路处理动作。包括以下几种：

- Block：阻塞指定接口并发送 Trap 信息。
- Trap-only：只发送 Trap 信息。
- Shutdown：关闭指定接口并发送 Trap 信息。

环路检测模式

环路检测模式为 Port 模式：

Port 模式：出现环路时，若环路处理方式为 Block，则阻塞接口并发送 Trap；若环路处理方式为 Shutdown 方式，则关闭物理接口并发送 Trap。

若环路处理方式为 Trap-only，则只发送 Trap 信息。

环路恢复

接口由于环路被阻塞或者关闭之后，可以根据用户配置进行自动恢复，如配置为不自动恢复或者指定时间后自动恢复。

- 如果配置为指定时间后自动恢复，达到恢复时间后应该进行一次环路探测，如果环路已经消除再放开接口，否则接口继续保持阻塞或者关闭状态。
- 如果配置为不自动恢复，即自动恢复时间为 infinite，则不会自动恢复接口状态。

3.9.2 配置准备

场景

在网络中，所有接入设备下连的主机或二层设备都可能存在有意、无意的连接而引起的环路，在每台接入设备上开启环路检测功能，可以避免网络环路造成数据流无限制复制而形成的网络拥塞状况。

前提

设备上环路检测、接口备份、STP、G.8032 和 RRPS 功能之间可能会相互影响，建议不要同一接口上同时开启这些功能。

3.9.3 环路检测的缺省配置

设备上环路检测的缺省配置如下。

功能	缺省值
环路检测功能状态	禁止
接口阻塞后的自动恢复时间	**infinite**，即不自动恢复
环路检测处理方式	**trap-only**
环路检测报文发送周期	4s
环路检测模式	接口模式

3.9.4 配置环路检测功能

请在设备上进行以下配置。

说明

环路检测与生成树协议冲突，二者不能同时开启。

直连设备两端不能同时开启环路检测。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入接口配置模式或批量端口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**loopback-detection** [**pkt-vlan** { **untag** | *vlan-id*}] [**hello-time** *second*] [**restore-time** *second*] [**action** {**block** | **trap-only** | **shutdown** | **shutdown-restore** }] [**log-interval** *log-interval time*]	在需要的接口上开启环路检测功能。 （可选）同时配置发包 vlan，（可选）hello 周期，（可选）恢复时间和环路动作
4	Inspur(config-gigaethernet1/1/*)#**loopback-detection manual restore**	手动恢复因检测到环路而被阻塞的接口。

3.9.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show loopback-detection** [*interface-type interface-number*] [**detail**]	查看接口环路检测配置。

3.9.6 维护

用户可以通过以下命令维护环路检测特性。

命令	描述
Inspur(config)#**clear loopback-detection statistic** [*interface-type interface-number*]	清除环路检测统计信息。

3.9.7 配置环路检测内环应用示例

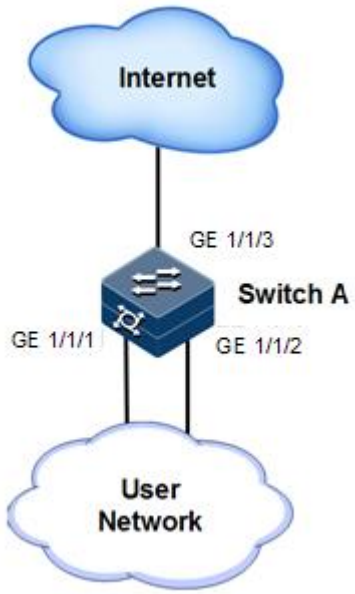
组网需求

如图 3-22 所示，Switch A 通过 GE 1/1/1 和 GE 1/1/2 接口连接 VLAN 3 用户网络，为了避免用户网络中存在环路，需要在 Switch A 上开启环路检测功能，及时检测用户网络中的环路并进行处理。具体要求如下：

- 使能 GE 1/1/1 和 GE 1/1/2 接口的环路检测功能。
- 配置环路检测报文发送间隔为 3s。
- 配置环路检测 VLAN 为 VLAN3。

- 配置接口的环路检测处理动作为 Block，发送告警信息并阻塞接口。

图3-22 环路检测内环应用组网示意图



配置步骤

步骤 1 创建 VLAN，并将接口加入 VLAN。

```
Inspur#config
Inspur(config)#create vlan 3 active
Inspur(config)#interface gigaethernet 1/1/1
Inspur(config-gigaethernet1/1/1)#switchport access vlan 3
Inspur(config-gigaethernet1/1/1)#exit
Inspur(config)#interface gigaethernet 1/1/2
Inspur(config-gigaethernet1/1/2)#switchport access vlan 3
Inspur(config-gigaethernet1/1/2)#exit
```

步骤 2 配置环路检测 VLAN、环路检测处理动作和环路检测报文发送周期。

```
Inspur(config)#interface gigaethernet 1/1/1
Inspur(config-gigaethernet1/1/1)#loopback-detection pkt-vlan 3 hello-time
3 action block
Inspur(config-gigaethernet1/1/1)#exit
Inspur(config)#interface gigaethernet 1/1/2
Inspur(config-gigaethernet1/1/2)#loopback-detection pkt-vlan 3 hello-time
3 action block
```

检查结果

通过 **show loopback-detection** 命令查看接口环路检测状态，GE 1/1/1 接口号小被阻塞，环路消除。

```
Inspur#show loopback-detection

Interface  pktVlan  detect-vlanlist    hellotime  restoretime  loop-act
log-interval  Status  loop-srcMAC     loop-srcPort  loop-Duration  loop-
vlanlist

-------------------------------------------------------------------------
-------------------------------------------------------------------------
-----------------

GE1/1/1   3      --              3        15         block          0
yes     000E.5E55.0001   GE1/1/2       121          --


GE1/1/2   3      --              3        15         block          0
no      --             --           --          --
```

3.10 接口保护

3.10.1 简介

通过接口保护特性，用户可以将需要进行控制的接口使能保护特性，实现接口之间二层数据的隔离，达到类似于接口之间物理隔离效果，既增强了网络的安全性，也为用户提供了灵活的组网方案。

配置接口保护后，在使能接口保护的接口之间报文不能互通，使能接口保护的接口和未使能接口保护的接口之间的通信不会受影响。

3.10.2 配置准备

场景

通过配置接口保护功能，可以实现接口之间互相隔离，能增强网络的安全性，也为用户提供了灵活的组网方案。

前提

无

3.10.3 接口保护的缺省配置

设备上接口保护的缺省配置如下。

功能	缺省值
各接口的接口保护功能状态	禁止

3.10.4 配置接口保护

注意

接口保护与接口所属 VLAN 无关。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**switchport protect**	使能接口保护，支持堆叠设备跨设备端口隔离。端口隔离支持基于聚合口隔离，支持聚合口与聚合口隔离，聚合口与普通口隔离。

3.10.5 配置接口隔离

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**protect-group** *group-id* **vlan** *vlan-id interface-type interface-number*	创建隔离组，配置隔离组关联的隔离 VLAN 及隔离端口列表。

3.10.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

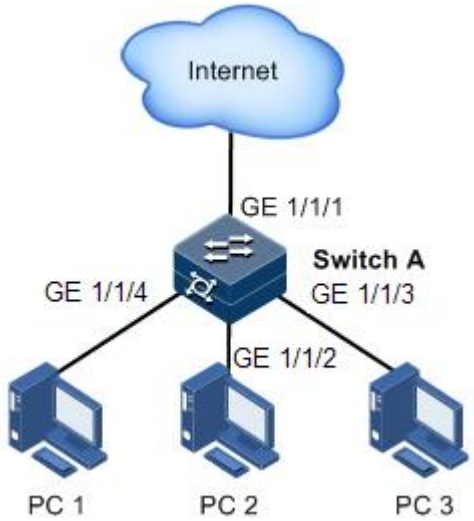
序号	检查项	说明
1	Inspur#**show switchport protect**	查看接口保护配置。
2	Inspur#**show protect-group** { **all** | *group-id* }	查看接口隔离配置信息。

3.10.7 配置接口保护示例

组网需求

如图 3-23 所示，为了使 PC1 和 PC2 之间不能互通，但 PC 1 和 PC 2 可以分别与 PC 3 通信，可以在 Switch A 的 GE 1/1/1 和 GE 1/1/2 接口上开启接口保护功能。

图3-23 接口保护组网示意图



配置步骤

步骤 1 使能 GE 1/1/1 的接口保护功能。

```
Inspur#config
Inspur(config)#interface gigaethernet 1/1/1
Inspur(config-gigaethernet1/1/1)#switchport protect
Inspur(config-gigaethernet1/1/1)#exit
```

步骤 2 使能 GE 1/1/2 的接口保护功能。

```
Inspur(config)#interface gigaethernet 1/1/2
Inspur(config-gigaethernet1/1/2)#switchport protect
```

检查结果

通过 **show switchport protect** 查看接口保护配置是否正确。

```
Inspur#show switchport protect
Port              Protected State
--------------------------
gigaethernet1/1/1    enable
gigaethernet1/1/2    enable
gigaethernet1/1/3    disable
gigaethernet1/1/4    disable
```

```
gigaethernet1/1/5    disable
gigaethernet1/1/6    disable
……
```

通过 PC 1 ping PC 3、PC 2 ping PC 3 是否能够 ping 通。

- PC 1 ping PC 3，可以 ping 通。
- PC 2 ping PC 3，可以 ping 通。

通过 PC 1 ping PC 2 是否能够 ping 通，查看接口保护功能是否正确。

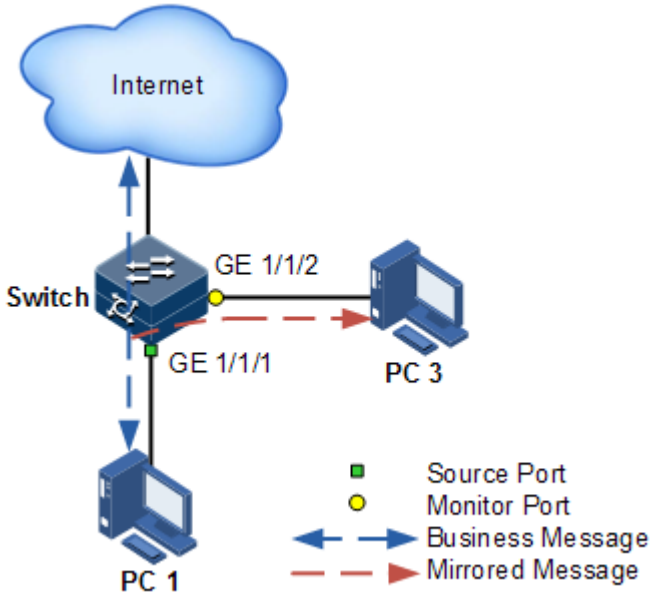
PC 1 ping PC 2，不能 ping 通，接口保护功能生效。

3.11 接口镜像

3.11.1 简介

接口镜像功能是指将指定源接口的某些报文镜像到目的接口，即监视接口，而不影响正常报文转发的功能。交换机设备用户使用该功能可以监控某个接口的报文接收和发送情况，并分析相关网络状况。

图3-24 接口镜像功能原理示意图



接口镜像功能基本原理如图 3-24 所示。PC 1 通过交换机的 Gigaethernet 1/1/1 与外网连接，PC 3 为监测 PC，通过交换机的 Gigaethernet 1/1/2 与外网连接。

当要监测从 PC 1 发出的报文时，需要将 PC 1 所连接设备的 Gigaethernet 1/1/1 指定为镜像源接口，并使能对入接口报文的镜像功能，而将 Gigaethernet 1/1/2 指定为监视接口，即镜像目的接口。

当 Gigaethernet 1/1/1 发出的业务报文进入交换机时，交换机将对入报文进行转发，并复制一份到监视接口（Gigaethernet 1/1/2）。连接在监视接口的监控设备可以接收这些被镜像的报文，并进行相关的分析工作。

设备支持基于入接口和出接口的数据流镜像。镜像功能生效后，出/入镜像接口的报文会被复制一份到监视接口。监视接口与镜像接口不能为同一个接口。

3.11.2 配置准备

场景

接口镜像功能主要用在网络管理人员定期监控网络内数据类型及流量。

接口镜像功能是将需要被监控接口的流量复制到一个监视接口或者 CPU，从而抓取入/出接口出现故障或异常时的数据流，用来分析、发现问题根源并及时解决。

前提

无

3.11.3 接口镜像的缺省配置

设备上接口镜像的缺省配置如下。

功能	缺省值
接口镜像功能状态	禁止
镜像源接口	无
镜像监视接口	gigaethernet1/1/1

3.11.4 配置接口镜像功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**mirror-group** *group-id*	创建接口镜像组。
3	Inspur(config)#**mirror-group** *group-id* **remote-vlan** *vlan-id*	配置镜像组的远程镜像 VLAN
4	Inspur(config)#**mirror-group** *group-id* **reflector-port** *interface-type interface-number*	配置镜像组反射接口
5	Inspur(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。

步骤	配置	说明
6	Inspur(config-gigaethernet1/1/*)#**mirror-group** *group-id* **monitor-port**	配置镜像功能的监视接口。
7	Inspur(config-gigaethernet1/1/*)#**mirror-group** *group-id* **source-port** { **ingress** | **egress** }	配置镜像功能的镜像接口及镜像规则。可以对接口入方向、出方向进行镜像。
8	Inspur(config-gigaethernet1/1/*)#**exit** Inspur(config)#**mirror-group** *group-id* **source-cpu** [**ingress** | **egress**]	添加镜像组源 CPU 接口。

3.11.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show mirror-group** [*group-id*]	查看镜像功能基本信息。

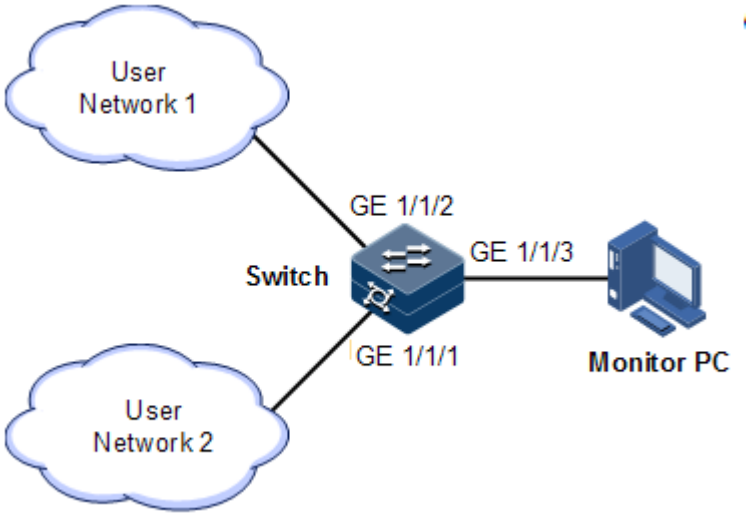
3.11.6 配置接口镜像应用示例

组网需求

如图 3-25 所示，网络管理员希望通过数据监测设备仅对用户网络 1 的报文进行监控，从而抓取出现故障或异常时的数据流，来分析、发现问题根源并及时解决。

交换机禁止所有自发包功能和风暴抑制功能。用户网络 1 通过 GE 1/1/2 接入交换机；用户网络 2 通过 GE 1/1/1 接入交换机；数据监测设备连接在交换机的 GE 1/1/3 上。

图3-25 接口镜像应用组网示意图



配置步骤

在 Switch 上使能接口镜像功能。

```
Inspur#config
Inspur(config)#mirror-group 1
Inspur(config)interface gigaethernet 1/1/3
Inspur(config-gigaethernet1/1/3)#mirror-group 1 monitor-port
Inspur(config-gigaethernet1/1/3)#exit
Inspur(config)interface gigaethernet 1/1/2
Inspur(config-gigaethernet1/1/2)#mirror-group source-port ingress
```

检查结果

通过 **show mirror** 查看接口镜像信息配置是否正确。

```
Inspur#show mirror-group
Mirror Group 1 :
Monitor Port :
   gigaethernet1/1/3
Source Port :
   gigaethernet1/1/1       : ingress
   gigaethernet1/1/2       : ingress
Remote Vlan: --
```

3.12 L2CP

3.12.1 简介

MEF（Metro Ethernet Forum，城域以太网论坛）引入了服务的概念，如 EPL、EVPL、EP-LAN 和 EVP-LAN 等六种服务类型，每种服务对 L2CP（Layer 2 Control Protocol，二层控制协议）报文的处理方式不同。

在 MEF6.1 中定义了 L2CP 报文的处理方式，分别为：

- discard：丢弃报文，将配置的 L2CP 模版应用到设备的入接口。
- peer：上交到 cpu，处理方式与 discard 相同。
- tunnel：传递到城域网，处理方式配置相比 discard 和 peer 较为复杂。需通过将用户网络侧接口的模板应用和运营商侧接口 tunnel 终端的配合使用，才能使报文穿过运营商网络。

3.12.2 配置准备

场景

在城域网的接入型设备上，根据运营商提供的服务，对用户网络的二层控制报文处理方式进行不同的配置，可在用户网络侧端口上通过配置模板完成。

准备

无

3.12.3 L2CP 的缺省配置

设备上 L2CP 的缺省配置如下。

功能	缺省值
L2CP 全局功能状态	禁用
接口应用模板	未应用模板
指定组播目的 MAC 地址	0x0100-0ccd-cdd0
L2CP 模板的描述信息	空

3.12.4 配置 L2CP

请在需要的设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**l2cp-process tunnel destination-address** *mac-address*	（可选）配置透传报文的目的 MAC 地址。

3.12.5 配置 L2CP 模板

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**l2cp-process profile** *profile-number*	创建并进入 L2CP 模板。
3	Inspur(config-l2cp-profile)#**name** *string*	（可选）添加模板描述信息。
4	Inspur(config-l2cp-profile)#**l2cp-process protocol** { **oam** | **stp** | **dot1x** | **elmi** | **garp** | **pagp** | **udld** | **lacp** | **lldp** | **cdp** | **vtp** | **pvst** |**all** } **action** { **tunnel** | **drop** | **peer** }	（可选）配置 L2CP 协议报文的处理动作。
5	Inspur(config-l2cp-profile)#**tunnel vlan** *vlan-id*	（可选）配置透传的指定 VLAN。
6	Inspur(config-l2cp-profile)#**tunnel** *interface-type interface-number*	（可选）配置透传的指定出接口。
7	Inspur(config-l2cp-profile)#**tunnel tunnel-type mac**	（可选）配置透传的通道类型。

3.12.6 配置接口应用 L2CP 模板

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**l2cp profile** *profile-number*	在接口应用 L2CP 模板。

说明

在使能全局 L2CP 状态下，接口应用模板才会生效。在禁用全局 L2CP 状态下，配置成功但不生效，当使能全局 L2CP 时配置再生效。

3.12.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show l2cp-process profile** [*profile-number*]	查看已创建的 L2CP 模板信息。
2	Inspur#**show l2cp-process** [*interface-type interface-number*]	查看接口 L2CP 相关配置信息。
3	Inspur#**show l2cp-process** [**tunnel statistics**] [*interface-type interface-number*]	查看接口 L2CP 报文统计信息。

3.12.8 维护

可以通过以下命令进行维护。

命令	说明
Inspur(config)#**clear l2cp-process tunnel statistic** [*interface-type interface-number*]	清除接口 L2CP 报文统计信息

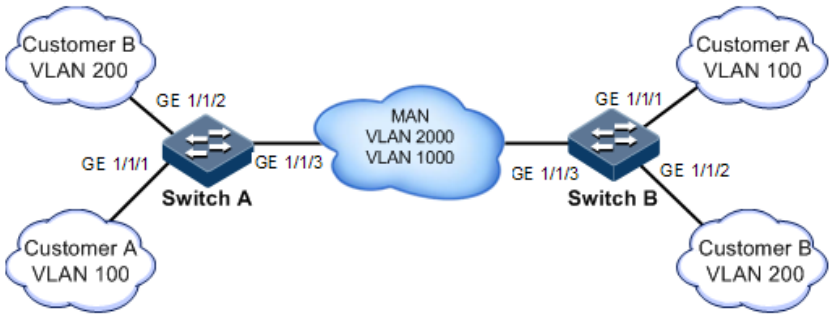
3.12.9 配置 L2CP 应用示例

组网需求

如图 3-26 所示，在 Switch A～Switch B 上，配置 L2CP 功能如下，Switch A 和 Switch B 指定组播目的 MAC 地址为 0100.1234.1234：

- Custemer A 的 stp 报文可以穿过城域网，其它报文全部丢弃。
- Custemer B 的 stp 和 vtp 报文可以穿过城域网，elmi 报文上交到 cpu，其它报文丢弃。

图3-26 配置 L2CP 功能组网示意图



配置步骤

配置 Switch A 和 Switch B。

Switch A 和 Switch B 配置步骤项完全相同，仅以配置 Switch A 为例。

步骤 1 配置交换机名称。

```
Inspur#hostname SwitchA
```

步骤 2 配置指定组播目的 MAC 地址。

```
Inspur(config)#l2cp-process tunnel destination-address 0100.1234.1234
```

步骤 3 配置 L2CP 模板 1，应用模板到接口 GE 1/1/1，适用于 Custemer A。

```
Inspur(config)#l2cp-process profile 1
Inspur(config-l2cp-profile)#name CustomerA
Inspur(config-l2cp-profile)#l2cp-process protocol all action drop
Inspur(config-l2cp-profile)#l2cp-process protocol stp action tunnel
Inspur(config-l2cp-profile)#exit
Inspur(config)#interface gigaethernet 1/1/1
Inspur(config-gigaethernet1/1/1)#l2cp-process profile 1
Inspur(config-gigaethernet1/1/1)#exit
```

步骤 4 配置 L2CP 模板 2，应用模板到接口 GE 1/1/2，适用于 Custemer B。

```
Inspur(config)#l2cp-process profile 2
Inspur(config-l2cp-proflie)#name CustomerB
Inspur(config-l2cp-proflie)#l2cp-process protocol all action drop
Inspur(config-l2cp-proflie)#l2cp-process protocol stp action tunnel
Inspur(config-l2cp-proflie)#l2cp-process protocol vtp action tunnel
Inspur(config-l2cp-proflie)#l2cp-process protocol elmi action peer
Inspur(config-l2cp-proflie)#exit
Inspur(config)#interface gigaethernet 1/1/2
Inspur(config-gigaethernet1/1/2)#l2cp-process profile 2
Inspur(config-gigaethernet1/1/2)#exit
```

检查结果

在设备上通过 **show l2cp-process profile** 查看 L2CP 配置是否正确。

```
Inspur#show l2cp-process profile

Destination MAC Address for Encapsulated Packets: 010E.5E00.0003

ProfileId: 1

Name:

BpduType    Mac-address     l2cp-process  Mac-vlan  EgressPort  tunneltype
------------------------------------------------------------------------
-------------
stp         0180.C200.0000   tunnel       --                 none
dot1x       0180.C200.0003   peer         --                 none
lacp        0180.C200.0002   peer         --                 none
gmrp(garp)  0180.C200.0020   tunnel       --                 none
gvrp(garp)  0180.C200.0021   tunnel       --                 none
cdp         0100.0CCC.CCCC   drop         --                 none
vtp         0100.0CCC.CCCC   drop         --                 none
pvst        0100.0CCC.CCCD   drop         --                 none
lldp        0180.C200.000E   peer         --                 none
oam         0180.C200.0002   peer         --                 none
elmi        0180.C200.0007   peer         --                 none
udld        0100.0CCC.CCCC   drop         --                 none
pagp        0100.0CCC.CCCC   drop         --                 none
```

在设备上通过 **show l2cp** 查看端口相关配置信息。

```
Inspur#show l2cp-process
L2CP running informatiom
Port     ProfileID    BpduType    mac-address     l2cp-process
------------------------------------------------------------------------
-----
PC1      --          --          --              --
PC8      --          --          --              --
GE1/1/1   --          --          --              --
GE1/1/2   --          --          --              --
GE1/1/3   --          --          --              --
…
```

3.13 GARP/GVRP

3.13.1 简介

GARP（Generic Attribute Registration Protocol，通用属性注册协议）提供了一种机制，用于协助同一个局域网内的 GARP 成员之间分发、传播和注册某种信息（如 VLAN 和组播信息等）。

GARP 本身不作为一个实体存在于设备中，遵循 GARP 协议的应用称为 GARP 应用。GVRP（GARP VLAN Registration Protocol，基于 GARP 的 VLAN 注册协议）就是

GARP 的一种应用。当 GARP 应用实体存在于设备的某个接口上时，该接口就对应于一个 GARP 应用实体。

GARP 应用实体的协议数据报文以特定的组播 MAC 地址为目的 MAC 地址。设备在接收到 GARP 应用实体的报文后，会根据其目的 MAC 地址加以区分并交给不同的 GARP 应用（如 GVRP）去处理。

GARP 消息

GARP 成员之间借助消息的传递来实现信息交互。涉及的消息主要有以下三种：

- Join 消息：当某个 GARP 应用实体希望其它设备注册自己的属性信息时（例如某个 VLAN 信息），该应用实体将对外发送 Join 消息；当收到其它实体的 Join 消息或本设备静态配置了某些属性，需要其它 GARP 应用实体进行注册时，也会向外发送 Join 消息。
- Leave 消息：当某个 GARP 应用实体希望其它设备注销自己的某个属性信息时，该应用实体将对外发送 Leave 消息；当收到其它实体的 Leave 消息注销某些属性或静态注销了某些属性时，也会向外发送 Leave 消息。
- LeaveAll 消息：GARP 应用实体启动后，将会同时启动 LeaveAll 定时器。当该定时器超时后，GARP 应用实体将对外发送 LeaveAll 消息。LeaveAll 消息用来注销所有属性，以使其它 GARP 应用实体重新注册本实体上所有的属性信息。当一个实体接收到对端发来的 LeaveAll 消息时，该实体的 LeaveAll 定时器刷新，重新计时。

Leave 消息、LeaveAll 消息通过与 Join 消息配合，确保属性的注销或重新注册。通过消息交互，所有待注册的属性信息可以传播到同一局域网内使能 GARP 功能的所有设备上。

GARP 定时器

GARP 消息发送的时间间隔通过定时器来实现，GARP 定义了三种定时器，用于控制 GARP 消息的发送周期。

- Join 定时器：如果第一次发送的 Join 消息没有得到回复时，GARP 应用实体会第二次发送 Join 消息，以保证 Join 消息的可靠传输。两次 Join 消息发送之间的时间间隔用 Join 定时器来控制。如果该定时器超时之前收到了其他成员的回复，则不再重发 Join 消息。
- Leave 定时器：当一个 GARP 应用实体希望注销某属性信息时，将对外发送 Leave 消息。接收到该消息的 GARP 应用实体启动 Leave 定时器，如果在该定时器超时之前没有收到要注销属性的 Join 消息，则注销该属性信息。
- LeaveAll 定时器：每个 GARP 应用实体启动后，将同时启动 LeaveAll 定时器。当该定时器超时后，GARP 应用实体将对外发送 LeaveAll 消息，以使其它 GARP 应用实体重新注册本实体上所有的属性信息。随后再启动 LeaveAll 定时器，开始新一轮循环。

GVRP

GVRP（GARP VLAN Registration Protocol，基于 GARP 的 VLAN 注册协议）是 GARP 的一种应用，它基于 GARP 的工作机制，维护交换机中的 VLAN 动态注册信息，并传播该信息到其它交换机。

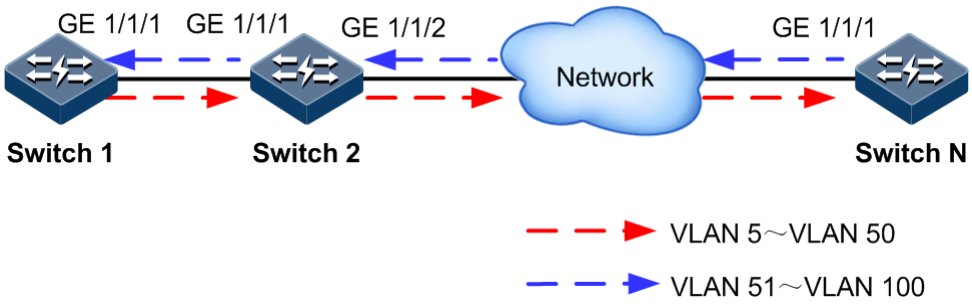
所有支持 GVRP 特性的交换机能够接收来自其它交换机的 VLAN 注册信息，并动态更新本地的 VLAN 注册信息。而且所有支持 GVRP 特性的交换机能够将本地的 VLAN 注册信息向其它交换机传播，以便使同一交换网内所有支持 GVRP 特性的设备 VLAN 信息达成一致。GVRP 传播的 VLAN 注册信息既包括本地手工配置的静态注册信息，也包括来自其它交换机的动态注册信息。

GVRP 有三种注册模式：

- 正常模式（Normal）：允许动态注册、注销 VLAN，传播动态、静态 VLAN 信息。
- 固定模式（Fixed）：禁止动态注册、注销 VLAN，只传播静态 VLAN 信息，不传播动态 VLAN 信息，只允许静态 VLAN 通过，即只对其他 GVRP 成员传播静态 VLAN 信息。
- 禁止模式（Forbidden）：禁止动态注册、注销 VLAN，禁止静态 VLAN 在接口上的创建，同时删除接口上除 VLAN 1 外的所有 VLAN，只允许缺省 VLAN（即 VLAN 1）通过，只对其他 GARP 成员传播缺省 VLAN 的信息。

存在多台设备的网络中，如图 3-27 所示，如果想在每台设备上配置 VLAN 信息，并允许指定 VLAN 的报文通过是比较繁琐的。采用 GVRP 来动态注册和传播指定 VLAN，可以帮助网管人员提高工作效率，提高准确性。

图3-27 GVRP 原理示意图



在图 3-27 中，Switch 1 的 GE 1/1/1，Switch 2 的 GE 1/1/1 和 GE 1/1/2，Switch N 的 GE 1/1/1 均为 Trunk 接口。在 Switch 1 中创建 VLAN 5～VLAN 50，则会按照红色连接线方向在接收接口上动态注册该 VLAN，直到传播到 Switch N 交换机。在 Switch N 上创建 VLAN 51～VLAN 100，则沿蓝色连接线注册该 VLAN 信息，使每个交换机可以完全处理 VLAN 5～VLAN 100 的报文。

3.13.2 配置准备

场景

利用 GARP 机制，一个 GARP 成员上的配置信息会迅速传播到整个局域网中所有使能 GARP 功能的设备上。

通过 GARP 功能配置的 Join 定时器、Leave 定时器和 LeaveAll 定时器的值，将应用于所有在同一网络内运行的 GARP 应用，包括 GVRP 特性和 GMRP 特性。

前提

无

3.13.3 GARP 的缺省配置

设备上 GARP 的缺省配置如下。

功能	缺省值
GARP Join 定时器	20（单位是 10ms）
GARP Leave 定时器	60（单位是 10ms）
GARP LeaveAll 定时器	1000（单位是 10ms）
全局 GVRP 功能状态	使能
接口 GVRP 功能状态	禁止
GVRP 注册模式	Normal

3.13.4 配置 GARP 基本功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-num*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**garp timer** { **join** | **leave** | **leaveall** } *time-value*	配置 GARP 定时器。

注意

- Join 定时器值必须小于 Leave 定时器值的一半；
- Leave 定时器值必须大于 2 倍的 Join 定时器值并且小于 LeaveAll 定时器值；
- LeaveAll 定时器值必须大于 Leave 定时器值；
- 实际组网时，建议 Join 定时器、Leave 定时器和 LeaveAll 定时器的值分别配置为 3000、15000 和 20000（单位是 10ms）。

3.13.5 配置 GVRP

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**gvrp enable**	使能全局 GVRP 功能。
3	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
4	Inspur(config-gigaethernet1/1/*)#**switchport mode trunk**	配置接口为 Trunk 模式。
5	Inspur(config-gigaethernet1/1/*)#**gvrp registration** { **fixed** | **forbidden** | **normal** }	（可选）配置 GVRP 注册模式。
6	Inspur(config-gigaethernet1/1/*)#**gvrp enable**	使能接口 GVRP 功能。

注意

- 接口必须先配置为 Trunk 模式才能使能接口 GVRP 功能。
- 不建议用户在聚合组成员接口上使能 GVRP 功能。

3.13.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show garp** [*interface-type interface-number*]	查看 GARP 定时器的配置信息。
2	Inspur# **show garp** [*interface-type interface-number*] **statistics**	查看 GARP 的统计信息。
3	Inspur#**show gvrp** [*interface-type interface-number*]	查看 GVRP 的配置信息。
4	Inspur#**show gvrp** [*interface-type interface-number*] **statistics**	查看 GVRP 的统计信息。
5	Inspur#**show gvrp local-vlan** *interface-type interface-number*	查看 GVRP 的本地 VLAN 信息。

3.13.7 维护

可以通过以下命令进行维护。

命令	说明
Inspur(config)#**clear gvrp** [*interface-type interface-number*] **statistics**	清除 GVRP 的统计信息。

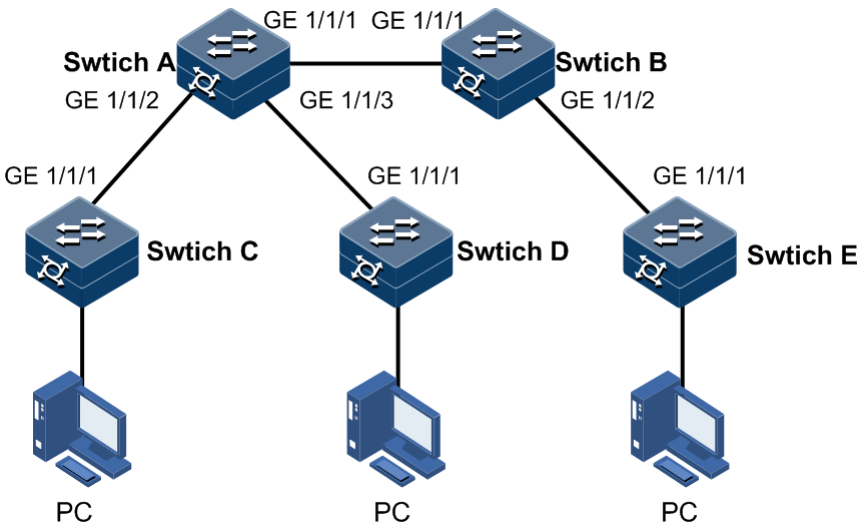
3.13.8 配置 GVRP 应用示例

组网需求

为了在交换机之间动态注册和更新 VLAN 信息，如图 3-28 所示，需要在各交换机上配置 GVRP 功能，来实现各交换机设备之间 VLAN 信息的动态注册和注销。具体要求如下：

- 在 Switch A 和 Switch C 中配置静态 VLAN 5～VLAN 10。
- Switch D 中配置静态 VLAN 15～VLAN 20。
- Switch E 中配置静态 VLAN 25～VLAN 30。
- 将所有与其他交换机相连的接口设置为 Trunk 模式，然后使能接口的 GVRP 功能。
- 配置各接口 GARP 的 Join 定时器、Leave 定时器和 LeaveAll 定时器分别为 3000、15000 和 20000。

图3-28 GVRP 应用组网示意图



配置步骤

步骤 1 创建 VLAN 并使能全局 GVRP 功能。

配置 Switch A。

```
Inspur#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 5-10 active
SwitchA(config)#gvrp enable
```

配置 Switch B。

```
Inspur#hostname SwitchB
SwitchB#config
```

```
SwitchB(config)#gvrp enable
```

配置 Switch C。

```
Inspur#hostname SwitchC
SwitchC#config
SwitchC(config)#create vlan 5-10 active
SwitchC(config)#gvrp enable
```

配置 Switch D。

```
Inspur#hostname SwitchD
SwitchD#config
SwitchD(config)#create vlan 15-20 active
SwitchD(config)#gvrp enable
```

配置 Switch E。

```
Inspur#hostname SwitchE
SwitchE#config
SwitchE(config)#create vlan 25-30 active
SwitchE(config)#gvrp enable
```

步骤 2 分别配置 Switch A 的 GE 1/1/1、GE 1/1/2、GE 1/1/3 接口，Switch B 的 GE 1/1/1、GE 1/1/2，Switch C 的 GE 1/1/1，Switch D 的 GE 1/1/1 接口为 Trunk 模式，并使能接口的 GVRP 功能。以配置 Switch A 的 GE 1/1/1 接口为例，其余接口配置步骤相同。

```
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport mode trunk
SwitchA(config-gigaethernet1/1/1)#gvrp enable
SwitchA(config-gigaethernet1/1/1)#exit
```

步骤 3 分别配置 Switch A 的 GE 1/1/1、GE 1/1/2、GE 1/1/3 接口、Switch B 的 GE 1/1/1、GE 1/1/2，Switch C 的 GE 1/1/1，Switch D 的 GE 1/1/1 接口的 GARP 定时器时间。以配置 Switch A 为例，其余接口配置步骤相同。

配置 Switch A。

```
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#garp timer leaveall 20000
SwitchA(config-gigaethernet1/1/1)#garp timer leave 15000
SwitchA(config-gigaethernet1/1/1)#garp timer join 3000
```

检查结果

通过 **show gvrp** 命令查看设备上接口的 GVRP 配置信息，以 Switch A 为例。

```
SwitchA#show gvrp gigaethernet 1/1/1
Gvrp Globle Status: Enable
Port     PortStatus     RegMode
-------------------------------------------------
GE1/1/1   Enable       Normal
GE1/1/2   Enable       Normal
GE1/1/3   Enable       Normal
GE1/1/4   Disable       Normal
GE1/1/5   Disable       Normal
GE1/1/6   Disable       Normal
GE1/1/7   Disable       Normal
```

```
GE1/1/8   Disable        Normal
GE1/1/9   Disable        Normal
GE1/1/10  Disable        Normal
```

通过 **show vlan** 命令查看设备上的 VLAN 信息，以 Switch A 为例。

```
SwitchA#show vlan
VLAN Name                          State   Status        Priority Member-
Ports
------------------------------------------------------------------------------
------------------------------------------------
1    Default                       active  static        --
gigaethernet1/1/1         gigaethernet1/1/2
5    VLAN0005                      active  static        --
6    VLAN0006                      active  static        --
7    VLAN0007                      active  static        --
8    VLAN0008                      active  static        --
9    VLAN0009                      active  static        --
10   VLAN0010                      active  static        --
15   VLAN0015                      active  dynamic-gvrp   --
gigaethernet1/1/3

16   VLAN0016                      active  dynamic-gvrp   --
gigaethernet1/1/3

17   VLAN0017                      active  dynamic-gvrp   --
gigaethernet1/1/3

18   VLAN0018                      active  dynamic-gvrp   --
gigaethernet1/1/3

19   VLAN0019                      active  dynamic-gvrp   --
gigaethernet1/1/3

20   VLAN0020                      active  dynamic-gvrp   --
gigaethernet1/1/3
--More--
```

3.14 Voice VLAN

3.14.1 简介

随着语音技术的日益发展，语音设备应用越来越广泛，尤其在宽带小区，网络中经常同时存在语音、数据和业务数据两种流量。语音数据在传输时需要具有比业务数据更高的优先级，以减少传输过程中可能产生的时延和丢包现象。

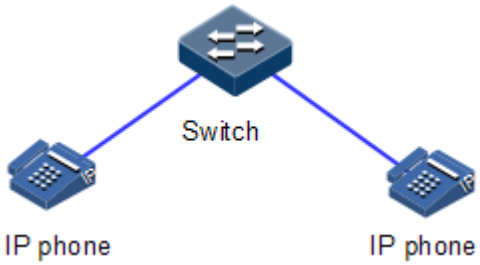
Voice VLAN 指为用户的语音数据流而专门划分的 VLAN。通过划分 Voice VLAN 并将连接语音设备的端口加入 Voice VLAN，可以为语音数据配置 QoS（Quality of Service，服务质量），提高语音流量的传输优先级，保证通话质量。

相对于使用其他语音流的方法，Voice VLAN 对语音流的管理具有以下一些优势：

- 配置简单：用户只需要在全局和端口下进行简单的配置，开启 Voice VLAN 功能，即可对语音数据进行分类处理。
- 便于维护：用户可以在全局配置对语音数据的匹配规则（Voice VLAN OUI 地址）进行修改，在新增 IP 语音设备的情况下，各端口能够迅速根据更新的匹配规则识别语音流。
- 实现灵活：Voice VLAN 功能在全局提供了安全/普通两种模式，端口上又可以分为自动/手动模式，实现更为灵活，用户可以根据自己需要进行组合，最大限度满足用户的需求。

适用于 IP 电话单独接入交换机（端口仅传输语音报文）的组网方式（如图 2 所示），这种静态加入的方式可以使该端口专用于传输语音数据，最大限度避免业务数据对语音数据传输的影响。

图3-29 IP 电话单独接入交换机组网示意图



3.14.2 配置准备

场景

语音流量可通过专属 VLAN（Voice VLAN）传输，在一段时间内，如果语音设备发生故障或语音设备退出网络，连接语音设备的端口会自动从 Voice VLAN 中退出。

前提

已经创建 VLAN，并且正确设备 VLAN 属性。

3.14.3 Voice VLAN 的缺省配置

设备上 Voice VLAN 的 OUI（Organizationally Unique Identifier，全球统一标识符地址）缺省配置如下。

OUI-Address	Mask address	Description
0001.E300.0000	FFFF.FF00.0000	Siemens-phone
0003.6B00.0000	FFFF.FF00.0000	Cisco-phone
0004.0D00.0000	FFFF.FF00.0000	Avaya-phone
00D0.1E00.0000	FFFF.FF00.0000	Pingtel-phone
0060.B900.0000	FFFF.FF00.0000	Philips/NEC-phone

00E0.7500.0000	FFFF.FF00.0000	Verilink-phone
00E0.BB00.0000	FFFF.FF00.0000	NBX-phone

设备上 Voice VLAN 的其他缺省配置如下。

功能	缺省值
Voice VLAN 功能	禁止
Voice Vlan 工作模式为安全模式	使能
Voice Vlan 报文的 Cos 和 DSCP 值	Voice VLAN 报文 COS 为 6，DSCP 为 46
Voice Vlan QoS 优先级信任	无

3.14.4 配置 OUI 地址

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**voice-vlan mac-address** *mac-address* [*mask address*] [**description** *word*]	配置 Voice VLAN 的 OUI。

3.14.5 使能 Voice VLAN 功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**voice-vlan** *vlan-id* **enable**	配置 Voice VLAN 功能使能。

3.14.6 配置 Voice VLAN 的 QoS

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**voice-vlan qos cos** *cos value* **dscp** *dscp value*	配置 Voice Vlan 报文的 Cos 和 DSCP 值。
4	Inspur(config-gigaethernet1/1/*)**voice-vlan qos trust**	配置 Voice Vlan QoS 优先级信任，配置完成后，接口就不会修改 Voice VLAN 报文的优先级。

3.14.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show voice-vlan mac-address**	查看当前设备上的 OUI 地址、OUI 地址掩码和描述信息。
2	Inspur#**show voice-vlan status**	查看当前设备上 Voice VLAN 的状态。

4 环网保护

本章介绍环网保护特性的原理和配置过程，并提供相关的配置案例。

- ERPS（G.8032）
- ELPS（G.8031）

4.1 ERPS（G.8032）

4.1.1 简介

G.8032 以太网环网保护倒换（Ethernet Ring Protection Switching，ERPS）是基于 ITU-T G.8032 标准的 APS 协议，是一种专门应用于以太网环的链路层协议。正常情况下，它在以太网环中能够防止数据环路引起的广播风暴。当以太网环上链路或设备故障时，能迅速切换到备份链路，保证业务快速恢复。

G.8032 利用环网内专用的控制 VLAN 传递环网控制信息，同时结合环网本身的拓扑特点，在网络发生故障时快速发现，并启用备份链路从而做到快速恢复。

4.1.2 配置准备

场景

随着以太网向电信级网络的发展，语音、视频组播业务对以太网的冗余保护和故障恢复时间提出了更高的要求。现有的 STP 机制对故障恢复的收敛时间都在秒级，远远达不到要求。G.8032 技术通过定义环上节点的不同角色，在正常情况下阻断环路防止产生广播风暴，在环上链路或节点故障的情况下迅速切换到备份链路，从而实现消除环路、故障保护倒换和自动故障恢复等功能，并且故障保护倒换时间低于 50ms，支持单环、相交环和相切环三种组网方式。

G.8032 提供基于物理接口状态来检测故障，能够快速获知链路故障达到快速倒换的目的，适用于相邻设备之间。

前提

在配置 G.8032 之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up；
- 创建 VLAN；
- 将接口加入 VLAN。

4.1.3 G.8032 的缺省配置

设备上 G.8032 的缺省配置如下。

功能	缺省值
协议 VLAN	1
保护环模式	返回模式
环 WTR 定时器	6min
环协议版本	2
Guard 定时器	500ms
环 HOLDOFF 定时器	0
ERPS 故障信息上报到网管系统	禁止
相交节点上子环虚通路模式	with 模式
相交节点上环 Propagate 开关	禁止

4.1.4 创建 G.8032 保护环

注意

环上只允许一台设备配置为 RPL（Ring Protection Link，环保护链路）Owner，一台设备配置为 RPL Neighbour，其他设备只能配置为环转发节点。

相切环实际为两个独立的单环，配置与普通单环相同；相交环分为主环和子环，主环与单环配置相同，子环配置请参见“4.1.6 （可选）创建 G.8032 保护子环”。

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**ethernet ring-protection** *ring-id* **east** { *interface-type interface-number* | **port-channel** *port-channel-number* } **west** { *interface-type interface-number* | **port-channel** *port-channel-number* } [**node-type rpl-owner rpl** { **east** | **west** }] [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	创建环并配置节点为 RPLOwner。 **说明** 东向和西向接口不能相同。
	Inspur(config)#**ethernet ring-protection** *ring-id* **east** { *interface-type interface-number* | **port-channel** *port-channel-number* } **west** { *interface-type interface-number* | **port-channel** *port-channel-number* } **node-type rpl-neighbour rpl** { **east**| **west** } [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	创建环并配置节点为 RPL Neighbour。
	Inspur(config)#**ethernet ring-protection** *ring-id* **east** { *interface-type interface-number* | **port-channel** *port-channel-number* } **west** { *interface-type interface-number* | **port-channel** *port-channel-number* } [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	创建环并配置节点为环转发节点。
3	Inspur(config)#**ethernet ring-protection** *ring-id* **name** *string*	（可选）配置环名称。名称长度不能超过 32 字节。
4	Inspur(config)#**ethernet ring-protection** *ring-id* **version** { **1** | **2** }	（可选）配置协议版本。同一个环上所有节点协议版本应一致，版本 1 通过协议 VLAN 区分不同环，因此不同环需配置不同的协议 VLAN，即使使用协议版本 2 也建议不同环配置不同的协议 VLAN。
5	Inspur(config)#**ethernet ring-protection** *ring-id* **guard-time** *guard-time*	（可选）配置环 Guard 定时器后，故障节点恢复时一段时间内不处理 APS 协议报文。在较大的环网络中，节点故障后如果立即恢复，可能会收到从环上传来的邻居节点发送的故障通知，从而再次陷于 Down 状态，而这个通知却是由本节点引起的。配置环 Guard 定时器可以解决这个问题。
6	Inspur(config)#**ethernet ring-protection** *ring-id* **wtr-time** *wtr-time*	（可选）配置环 WTR 定时器。在返回模式下当工作链路故障恢复时，等待 WTR 定时器超时之后，才会恢复到工作链路上工作。

步骤	配置	说明
7	Inspur(config)#**ethernet ring-protection** *ring-id* **holdoff-time** *holdoff-time*	（可选）配置环 HOLDOFF 定时器后，当工作链路故障时，系统会延时上报故障，即延时一段时间后再倒换到保护链路，可以防止工作链路震荡引起的频繁倒换。 **说明** HOLDOFF 定时器配置值较大时会影响 50ms 倒换性能，所以推荐使用缺省值 0。

4.1.5 配置 ERPS 故障检测方式

请在需要启动 ERPS 的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ethernet ring-protection** *ring-id* { **east** | **west** } **failure-detect physical-link**	配置故障检测方式为物理链路方式。
3	Inspur(config)#**ethernet ring-protection** *ring-id* { **east** | **west** } **failure-detect cc** [**md** *md-name*] **ma** *ma-name* **level** *level* **mep** *local-mep-id remote-mep-id*	配置故障检测方式为 cc 方式。
4	Inspur(config)#**ethernet ring-protection** *ring-id* { **east** | **west** } **failure-detect physical-link-or-cc** [**md** *md-name*] **ma** *ma-name* **level** *level* **mep** *local-mep-id remote-mep-id*	配置故障检测方式为 **physical-link-or-cc** 方式。

4.1.6（可选）创建 G.8032 保护子环

注意

- 只有相交环存在主环和子环之分。
- 相交环主环的配置与单环或相切环相同，具体配置请参见“创建 G.8032 保护环”。
- 配置相交环时应先配置主环，再配置子环，否则子环找不到主环接口，将无法建立子环虚通路。
- 子环的环号必须大于主环的环号。
- 相交环子环上的非相交节点配置与单环或相切环相同，具体配置请参见“4.1.4 创建 G.8032 保护环”。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ethernet ring-protection** *ring-id* { **east** | **west** } { *interface-type interface-number* | **port-channel** *port-channel-number* } **node-type rpl-owner** [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	在相交节点上创建子环并配置节点为 RPLOwner。如果配置了 **not-revertive** 参数，则保护环变为非返回模式。非返回模式与返回模式的区别在于，返回模式下工作链路故障恢复时，流量由环保护链路切换回工作链路，非返回模式下不切换。缺省情况下，保护环处于返回模式。 **说明** 相交环两个相交节点之间的链路属于主环，所以在相交节点上配置子环时只能配置东向或西向其中一个方向的接口。
	Inspur(config)#**ethernet ring-protection** *ring-id* { **east** | **west** } { *interface-type interface-number* | **port-channel** *port-channel-number* } **node-type rpl-neighbour** [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	在相交节点上创建子环并配置节点为 RPL Neighbour。
	Inspur(config)#**ethernet ring-protection** *ring-id* { **east** | **west** } { *interface-type interface-number* | **port-channel** *port-channel-number* } [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	在相交节点上创建子环并配置节点为环转发节点。

步骤	配置	说明
3	Inspur(config)#**ethernet ring-protection** *ring-id* **raps-vc** { **with** | **without** }	（可选）在相交节点上配置子环虚通路模式。因为相交节点间的链路属于主环，所以子环中协议报文的传输方式与主环不同，可分为 with 和 without 模式： • with：主环为子环 APS 报文提供通路，子环相交节点收到子环 APS 报文会传送到主环，利用主环完成子环相交节点间的通信。 • without：相交节点上子环 APS 报文要求终结，不会传送到主环。这种方式要求子环不能阻塞子环协议 VLAN（以保证子环报文可以通过 Owner）。 缺省情况下，子环虚通路采用 with 模式。两个相交节点模式必须配置一致。
4	Inspur(config)#**ethernet ring-protection** *ring-id* **propagate enable**	在相交节点上使能环 Propagate 开关。 因为子环的数据需要通过主环转发，所以主环设备上会存在子环的 MAC 地址列表，在子环出现故障时需要通过 Propagate 开关及时通知主环刷新 MAC 地址列表，避免流量丢失。

4.1.7（可选）配置 G.8032 倒换控制

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ethernet ring-protection** *ring-id* **force-switch** { **east** | **west** }	配置环上的流量强制倒换到西向或东向。 强制倒换可配置在多个环节点的多个接口上。
3	Inspur(config)#**ethernet ring-protection** *ring-id* **manual-switch** { **east** | **west** }	配置环上的流量手工倒换到西向或东向，优先级低于强制倒换和工作链路故障时产生的自动倒换。 手工倒换只能配置在同一个环节点的一个接口上。
4	Inspur(config)#**clear ethernet ring-protection** *ring-id* { **command** | **statistics** }	清除倒换控制命令作用，包括 **force-switch**、**manual-switch**、WTR 定时器和 WTB 定时器。

说明

缺省情况下，工作链路故障时流量会自动倒换到保护链路。所以只在某些特殊情况下才需要配置 ERPS 倒换控制。

4.1.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show ethernet ring-protection** [*ring-id*]	查看 G.8032 环配置信息。
2	Inspur#**show ethernet ring-protection** [*ring-id*] **status**	查看 G.8032 环状态信息。
3	Inspur#**show ethernet ring-protection** [*ring-id*] **statistics**	查看 G.8032 环统计信息。

4.1.9 维护

用户可以通过以下命令，维护设备 ERPS 特性的运行情况和配置情况。

命令	描述
Inspur(config)#**clear ethernet ring-protection** *ring-id* **statistics**	清除保护环统计信息。

4.2 ELPS（G.8031）

4.2.1 简介

ELPS（Ethernet Linear Protection Switching，以太网线性保护倒换）是基于 ITU-T G.8031 标准的 APS（Automatic Protection Switching，自动保护倒换）协议，用于保护一条以太网连接，它是一种端到端的保护技术。

在 ELPS 的保护切换机制中，对工作资源都分配相应的保护资源，如路径和带宽等。ELPS 技术简单快速，以一种可预测的方式实现网络资源切换，更易于运营商有效地规划网络和了解网络的活动状态，实现电信级的运营。

4.2.2 配置准备

场景

为了使以太网可靠性达到电信级（网络自愈时间小于 50ms），可以在以太网中部署 ELPS 特性。ELPS 用于保护一条以太网连接，它是一种端到端的保护技术。

ELPS 支持 1+1 和 1:1 两种保护方式：

- 1+1 保护倒换：每个工作路径分配一个保护路径。在保护域内，源端在工作和保护路径都传输流量，而在宿端选择其中一个路径接收流量。
- 1:1 保护倒换：每个工作路径分配一个保护路径。与 1+1 保护不同的是，流量只在工作路径或保护路径中的一个路径进行传输。正常情况下，流量在工作路径上传输，保护路径做备份。当工作路径故障时，需要通过 APS 协议进行协商，以便源端和宿端同时切换到备份路径。

按照链路发生故障时，两端是否同时切换，ELPS 可以分为单向倒换和双向倒换。

- 单向倒换是指一条链路的一个方向发生故障时，导致一端能够接收流量，一端不能接收，此时不能接收的一端检测到故障发生切换，能够接收的一端未检测到故障则不进行切换，切换的结果是 ELPS 连接的两端可能选择不同的链路接收流量。
- 双向倒换是指链路发生故障时，即使仅有一个方向故障，两端也需要 APS 协议协商同时切换到备份链路，切换的结果是 ELPS 连接的两端需要选择同一条链路进行发送和接收。

本设备只有配置为 1+1 方式时才区分单向和双向倒换，1:1 方式仅支持双向倒换。

ELPS 提供了两种方式来检测故障：

- 基于物理接口状态来检测故障：能够快速获知链路故障达到快速倒换的目的，适用于相邻设备之间。
- 基于 CC 来检测故障：适用于单向检测或跨越多个设备检测的情况。

前提

在配置 ELPS 之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up；
- 创建 VLAN；
- 将接口加入 VLAN；
- 设备之间配置 CFM 检测，并形成邻居关系（当选用 CFM 为检测方式时准备）。

4.2.3 ELPS 的缺省配置

设备上 ELPS 的缺省配置如下。

功能	缺省值
保护组模式	返回模式

功能	缺省值
WTR 定时器	5min
HOLDOFF 定时器	0ms
ELPS 故障信息上报到网管系统状态	使能
故障检测方式	物理链路

4.2.4 创建保护线路

请在需要启动 ELPS 的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ethernet line-protection** *line-id* **working** *interface-type interface-number vlan-list* **protection** *interface-type interface-number vlan-list* **one-to-one** [**non-revertive**] **protocol-vlan** *vlan-id*	创建 ELPS 保护线路，并配置保护方式。如果配置了 **non-revertive** 参数，则保护组变为非返回模式。非返回模式与返回模式的区别在于，返回模式下工作链路故障恢复时，流量由保护链路切换回工作链路，非返回模式下不切换。缺省情况下，保护组处于返回模式。
3	Inspur(config)#**ethernet line-protection** *line-id* **name** *string*	（可选）配置 ELPS 保护线路名称。
4	Inspur(config)#**ethernet line-protection** *line-id* **wtr-timer** *wtr-timer*	（可选）配置 WTR 定时器。在返回模式下当工作链路故障恢复时，等待 WTR 定时器超时之后，才会恢复到工作链路上工作。缺省情况下，WTR 定时器取值为 5min。 **说明** 建议两端 WTR 定时器值配置保持一致，否则无法保证 50ms 快速倒换。
5	Inspur(config)#**ethernet line-protection** *line-id* **hold-off-timer** *hold-off-timer*	（可选）配置 HOLDOFF 定时器。配置 HOLDOFF 定时器后，当工作链路故障时，系统会延时处理故障，即延时一段时间后再倒换到保护链路，可以防止工作链路震荡引起的频繁倒换。缺省情况下，HOLDOFF 定时器为 0。 **说明** HOLDOFF 定时器配置值较大时会影响 50ms 倒换性能，所以推荐使用缺省值 0。

步骤	配置	说明
6	Inspur(config)#**ethernet line-protection trap enable**	（可选）配置使能 ELPS 故障信息上报到网管系统。缺省情况下未使能。可以使用命令 **ethernet port-protection trap disable** 禁用此功能。

4.2.5 配置 ELPS 故障检测方式

请在需要启动 ELPS 的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ethernet line-protection** *line-id* { **working** | **protection** } **failure-detect physical-link**	配置工作路径或保护路径故障检测方式为检查物理链路。缺省情况下，故障检测方式为物理链路。
	Inspur(config)#**ethernet line-protection** *line-id* { **working** | **protection** } **failure-detect cc** [**md** *md-name*] **ma** *ma-name* **level** *level* **mep** *local-mep-id remote-mep-id*	配置工作路径或保护路径故障检测方式为 CC。需要先完成 CFM 相关配置，故障检测方式才能生效。
	Inspur(config)#**ethernet line-protection** *line-id* { **working** | **protection** } **failure-detect physical-link-or-cc** [**md** *md-name*] **ma** *ma-name* **level** *level* **mep** *local-mep-id remote-mep-id*	配置工作路径或保护路径故障检测方式为物理链路或 CC，即，物理链路或 CC 任何一种检测到故障都上报。需要先完成 CFM 相关配置，故障检测方式才能生效。

说明

工作路径和保护路径配置的故障检测方式可以不同，但是建议工作路径或者保护路径的两端故障检测方式配置保持一致。

4.2.6（可选）配置 ELPS 倒换控制

请在需要配置 ELPS 倒换控制的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ethernet line-protection** *line-id* **lockout**	锁定保护倒换。配置此命令后即使工作链路故障流量也不会倒换到保护链路。
3	Inspur(config)#**ethernet line-protection** *line-id* **force-switch**	配置流量由工作链路强制倒换到保护链路。

步骤	配置	说明
4	Inspur(config)#**ethernet line-protection** *line-id* **manual-switch**	配置流量由工作链路手工倒换到保护链路，优先级低于强制倒换和工作链路故障时产生的自动倒换。
5	Inspur(config)#**ethernet line-protection** *line-id* **manual-switch-to-work**	非返回模式下，配置流量由保护链路切换回工作链路。
6	Inspur(config)#**clear ethernet line-protection** *line-id* **end-to-end command**	清除端到端的倒换控制命令，包括 **lockout**、**force-switch**、**manual-switch**、**manual-switch-to-work** 和 WTR 定时器。

说明

缺省情况下，工作链路故障时流量会自动倒换到保护链路。所以只在某些特殊情况下才需要配置 ELPS 倒换控制。

4.2.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show ethernet line-protection** [*line-id*]	查看保护线路配置是否正确。
2	Inspur#**show ethernet line-protection** [*line-id*] **statistics**	查看保护线路统计信息。
3	Inspur#**show ethernet line-protection** [*line-id*] **aps**	查看 APS 协议相关信息。

4.2.8 维护

用户可以通过以下命令进行维护。

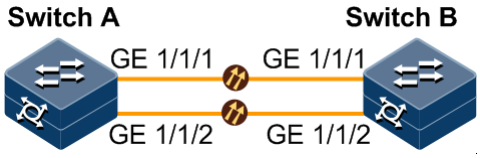
命令	说明
Inspur(config)#**clear ethernet line-protection** [*line-id*] **statistics**	清除保护线路统计信息，包括发送 APS 报文数，接收 APS 报文数，最近倒换时间，最近状态切换时间等。

4.2.9 配置 1:1 方式 ELPS 保护示例

组网需求

如图 4-1 所示，为提高 Switch A 与 Switch B 之间链路的可靠性，在两台设备上配置 1:1 方式的 ELPS，并基于物理接口状态来检测故障。GE 1/1/1 和 GE 1/1/2 所属的 VLAN 范围为 100～200。

图4-1 1:1 方式 ELPS 应用组网示意图



配置步骤

步骤 1 创建 VLAN 100～VLAN 200 并将接口加入到 VLAN 100～VLAN 200 中。

配置 Switch A。

```
Inspur#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 100-200 active
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport mode trunk
SwitchA(config-gigaethernet1/1/1)#switchport trunk allowed vlan 100-200
confirm
SwitchA(config-gigaethernet1/1/1)#exit
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#switchport mode trunk
SwitchA(config-gigaethernet1/1/2)#switchport trunk allowed vlan 100-200
confirm
SwitchA(config-gigaethernet1/1/2#exit
```

配置 Switch B。

```
Inspur#hostname SwitchB
SwitchB#config
SwitchB(config)#create vlan 100-200 active
SwitchB(config)#interface gigaethernet 1/1/1
SwitchB(config-gigaethernet1/1/1)#switchport mode trunk
SwitchB(config-gigaethernet1/1/1)#switchport trunk allowed vlan 100-200
confirm
SwitchB(config-gigaethernet1/1/1)#exit
SwitchB(config)#interface gigaethernet 1/1/2
SwitchB(config-gigaethernet1/1/2)#switchport mode trunk
SwitchB(config-gigaethernet1/1/2)#switchport trunk allowed vlan 100-200
confirm
SwitchB(config-gigaethernet1/1/2)#exit
```

步骤 2 创建 1:1 方式 ELPS 保护线路。

配置 Switch A。

```
SwitchA(config)#ethernet line-protection 1 working gigaethernet 1/1/1
100-200 protection gigaethernet 1/1/2 100-200 one-to-one
```

配置 Switch B。

```
SwitchB(config)#ethernet line-protection 1 working gigaethernet 1/1/1
100-200 protection gigaethernet 1/1/2 100-200 one-to-one
```

步骤 3 配置故障检测方式。

配置 Switch A。

```
SwitchA(config)#ethernet line-protection 1 working failure-detect
physical-link
SwitchA(config)#ethernet line-protection 1 protection failure-detect
physical-link
```

配置 Switch B。

```
SwitchB(config)#ethernet line-protection 1 working failure-detect
physical-link
SwitchB(config)#ethernet line-protection 1 protection failure-detect
physical-link
```

检查结果

在设备上通过 **show ethernet line-protection** 查看 1:1 方式 ELPS 配置是否正确。

以 Switch A 为例：

```
SwitchA#show ethernet line-protection 1
Trap State:Enable

Id:1
Name:--
ProtocolVlan:1
Working Entity Information:
Port:    gigaethernet1/1/1
Vlanlist: 100-200
FaiureDetect:physical
MAID:    --
MdLevel:  0
LocalMep: 0
RemoteMep:0
State/LCK/M:Active/N/N
Link State:failure
Protection Entity Information:
Port:    gigaethernet1/1/2
Vlanlist: 100-200
FaiureDetect:physical
MAID:    --
MdLevel:  0
LocalMep: 0
RemoteMep:0
State/F/M:Standby/N/N
Link State:failure
```

```
Wtr(m):5
Holdoff(100ms):0
```

在设备上通过 **show ethernet line-protection aps** 查看 1:1 方式 ELPS 的 APS 协议信息。

以 Switch A 为例：

```
SwitchA#show ethernet line-protection 1 aps
C-Direction: Configuration Direction
N-Direction: Negotiated Direction
R-Signal: Requested Signal
B-Signal: Bridged Signal
Id       Type C-Direction N-Direction Revert Aps State R-Signal B-Signal
------------------------------------------------------------------------
1-Local   1:1  bi        bi        yes    yes SF-P  null    null
```

5 IP 业务

本章介绍 IP 业务特性的基本原理和配置过程，并提供相关的配置案例。

- IP 基础配置
- LOOPBACK 接口
- 接口环回
- ARP
- NDP
- 路由管理
- 静态路由
- 路由策略
- OSPFv2
- OSPFv3
- ISIS
- BGP
- RIP
- RIPng
- ND Snooping

5.1 IP 基础配置

5.1.1 简介

IP 接口是基于 VLAN 的虚拟接口。一般应用于需要对设备进行网管或多台设备之间需要进行路由连通的场合。

5.1.2 配置准备

场景

为每一个 VLAN 接口或 LOOPBACK 接口配置 IP 地址。

前提

需创建 VLAN 并激活。

5.1.3 VLAN 接口的缺省配置

设备上三层接口的缺省配置如下。

功能	缺省值
管理 VLAN 内层 TPID	0x8100
管理 VLAN 内层 VLAN	1
管理 VLAN CoS 值	0

5.1.4 配置 VLAN 接口 IPv4 地址

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#interface vlan` *vlan-id*	进入 VLAN 接口配置模式。
3	`Inspur(config-vlan*)#ip address` *ip-address* [*ip-mask*] [`sub`]	配置 VLAN 接口的 IP 地址。 可以使用 **no ip address** *ip-address* 命令删除 IP 地址配置。

说明

设备可配置 255 个 IP 接口，取值范围是 0～254。

5.1.5 配置 VLAN 接口 IPv6 地址

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#interface vlan` *vlan-id*	进入 VLAN 接口配置模式。

步骤	配置	说明
3	Inspur(config-vlan*)#**ipv6 address** *ipv6-address* **link-local** Inspur(config-vlan*)#**ipv6 address** *ipv6-address/prefix-length* [**eui-64**]	配置 VLAN 接口的 IPv6 地址。

5.1.6 配置基本属性

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式。
3	Inspur(config-vlan*)#**ip management-traffic cos** *cos-value*	配置管理 VLAN CoS 值，缺省值为 6。
4	Inspur(config-vlan*)#**ip management-traffic mode double-tagging** [**inner-vlan** *vlan-id*] [**inner-cos** *cos-id*]	配置管理报文双 Tag 模式。
5	Inspur(config-vlan*)#**exit**	返回全局配置模式。
6	Inspur(config)#**ip dest-address illegal syslog** { **enable** | **disable** }	使能或禁止 IP 包中目的地址包含非法地址的处理功能。
7	Inspur(config)#**ip packet unknown forward**	未知类型报文转发，对于含有未知类型选项的 IP 报文，设备转发此 IP 报文。
8	Inspur(config)#**icmp unreach send**	使能发送 ICMP 不可达报文功能。
9	Inspur(config)#**exit**	返回特权用户模式。
10	Inspur#**ip soft-forward** { **enable** | **disable** }	使能设备产生的控制报文的转发功能，使用 disable 格式禁用该功能。

5.1.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show ip interface brief**	查看三层接口的 IP 地址配置信息。
2	Inspur#**show ipv6 interface brief**	查看三层接口的 IPv6 地址配置信息。

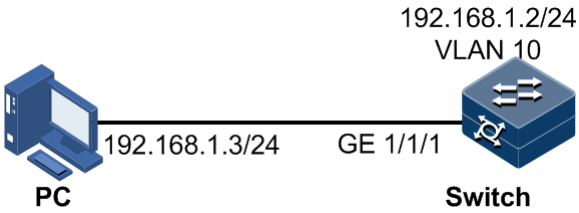
序号	检查项	说明
3	Inspur#**show ip management-traffic**	查看 VLAN 接口下管理报文信息。

5.1.8 配置 VLAN 接口 IP 地址实现和主机互通示例

组网需求

配置交换机设备 VLAN 接口 10，使图 5-1 中的主机和设备之间能够相互 Ping 通。

图5-1 配置 VLAN 接口组网示意图



配置步骤

步骤 1 创建 VLAN 10，并将接口 GE 1/1/1 加入 VLAN 10。

```
Inspur#config
Inspur(config)#create vlan 10 active
Inspur(config)#interface gigaethernet 1/1/1
Inspur(config-gigaethernet1/1/1)#switchport access vlan 10
```

步骤 2 在交换机设备上创建三层 VLAN 10 接口，配置 VLAN 10 接口的 IP 地址。

```
Inspur(config)#interface vlan 10
Inspur(config-vlan10)#ip address 192.168.1.2 255.255.255.0
```

检查结果

通过 **show vlan** 命令查看 VLAN 和物理接口的绑定关系是否正确。

```
Inspur#show vlan 10
VLAN Name                          State   Status  Priority Member-Ports
------------------------------------------------------------------------------
--------------------------------------
10   VLAN0010                      active  static  --
```

通过 **show ip interface brief** 命令查看三层接口配置是否正确。

```
Inspur#show ip interface brief
VRF                  IF                          Address        NetMask
Catagory
------------------------------------------------------------------------------
-----------------------------
```

```
Default-IP-Routing-Table  fastethernet1/0/1            192.168.0.1
255.255.255.0   primary
Default-IP-Routing-Table  vlan10                      192.168.1.2
255.255.255.0   primary
```

通过 **ping** 命令查看设备和 PC 之间是否能够互通。

```
Inspur#ping 192.168.1.3
Type CTRL+C to abort
Sending 5, 8-byte ICMP Echos to 192.168.1.3, timeout is 3 seconds:
Reply from 192.168.1.3: time<1ms
Reply from 192.168.1.3: time<1ms
Reply from 192.168.1.3: time<1ms
Reply from 192.168.1.3: time<1ms
Reply from 192.168.1.3: time<1ms

---- PING Statistics----
5 packets transmitted, 5 packets received,
Success rate is 100 percent(5/5),
round-trip (ms)  min/avg/max = 0/0/0.
```

5.2 LOOPBACK 接口

5.2.1 简介

LOOPBACK 接口是一种虚拟接口，可以分为两类：

- 由系统自动创建的 LOOPBACK 接口。IP 地址固定为 127.0.0.1，用来接收所有发送给本机的数据包。不通过路由协议对外发布。
- 由用户创建的 LOOPBACK 接口。在不影响物理接口配置的情况下，配置一个带有指定 IP 地址的本地接口，并且接口状态永远是 up 状态，能够被路由协议发布出去。

LOOPBACK 接口状态不受物理接口 Up/Down 的影响，只要保证设备运行正常，该 LOOPBACK 接口就不会 Down 掉。因此，LOOPBACK 接口地址常被用来标示物理设备本身，作为设备的管理地址。

5.2.2 配置准备

场景

使用 LOOPBACK 接口 IP 地址对设备进行 Telnet 登录，可以保证 Telnet 操作不会因接口的物理状态改变为 Down 掉，如果 PC 需要 ping 通 LOOPBACK 接口地址，需要 PC 端设置相对应的静态路由表项。LOOPBACK 接口还常被用来作为动态路由协议如 OSPF 等协议的 Router ID，作为设备的唯一标识。

前提

无

5.2.3 LOOPBACK 接口的缺省配置

无

5.2.4 配置 LOOPBACK 接口 IP 地址

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface loopback** *lb-number*	进入 LOOPBACK 接口配置模式。
3	Inspur(config-loopback)#**ip address** *ip-address* [*ip-mask*]	配置 LOOPBACK 接口的 IP 地址。
4	Inspur(config-loopback)#**ipv6 address** *ipv6-address/prefix-length* [**sub**]	配置 LOOPBACK 接口的 IPV6 地址。

5.2.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show interface loopback** [*loopback-number*]	查看 LOOPBACK 接口配置信息。

5.3 接口环回

5.3.1 简介

接口环回功能即接口 Loopback（本地环回）功能通过将符合用户设定的环回规则以及对应规则参数要求的报文，由接收接口返回，发送给对端发送设备，以实现对网络的通信情况进行检查。

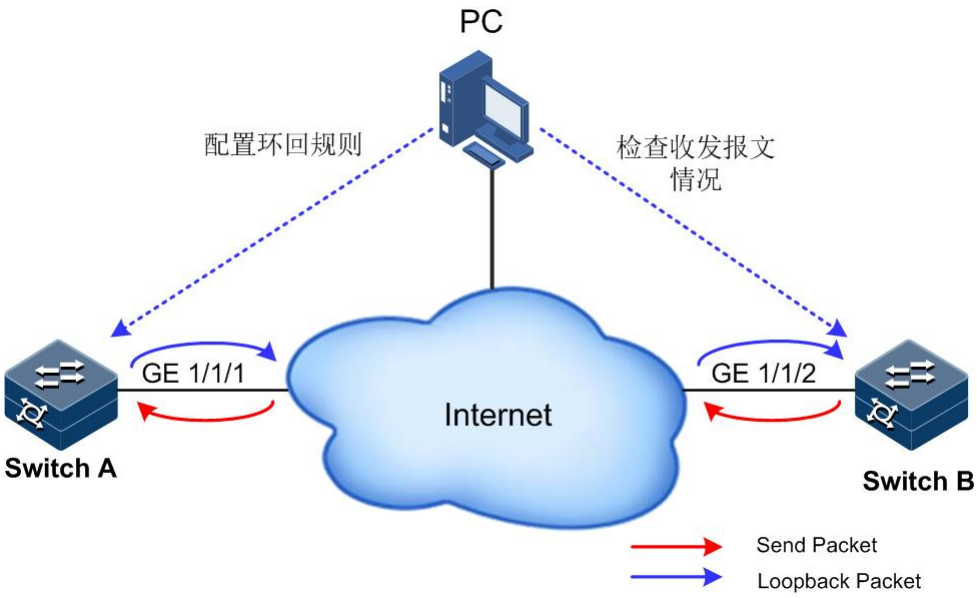
接口 Loopback 功能是在不影响业务的情况下执行环回，即符合条件的报文在进行环回的同时，也可以正常转发或上送到 CPU。

如图 5-2 所示，用户在 Switch A 的 Gigaethernet 1/1/1 接口上设置环回规则。由 Switch B 的 Gigaethernet 1/1/2 接口发出的报文到达 Switch A 的 Gigaethernet 1/1/1 接口，设备检查报文是否符合当前环回规则。

- 如果符合环回规则，将报文进行环回，通过 Gigaethernet 1/1/1 接口返回给 Switch B 的 Gigaethernet 1/1/2 接口。
- 如果不符合环回规则，报文正常转发或上送到 CPU。

用户可以通过对比 Switch B 发送和接收的报文来检查网络的通信情况。

图5-2 接口环回示意图



5.3.2 配置准备

场景

接口环回功能通过设置接口环回规则以及规则参数，将符合条件的报文由接收接口环回到对端报文发送接口，以实现对网络通讯情况进行检查。

前提

无

5.3.3 接口环回的缺省配置

无

5.3.4 配置接口环回功能

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#interface` *interface-type interface-number*	进入物理接口配置模式。

步骤	配置	说明
3	Inspur(config-gigaethernet1/1/*)#**loopback external** [**cvlan** *vlan-id* [**cos** *cos-value*]] [**svlan** *vlan-id* [**cos** *cos-value*]] [**dmac** *mac-address*] [**smac** *mac-address*][**swap smac** *mac-address*] [**swap dmac-disable**]	配置端口环回功能。

5.3.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show loopback** [*interface-type interface-number*]	查看端口环回的配置信息。
2	Inspur#**show loopback-statistics** [*interface-type interface-number*]	查看环回报文的统计信息。

5.3.6 维护

用户可以通过以下命令，维护设备接口环回特性的运行情况和配置情况。

命令	描述
Inspur(config)#**clear loopback-statistics** [*interface-type interface-number*]	清除环回报文的统计信息。

5.4 ARP

5.4.1 简介

在 TCP/IP 网络环境中，每台主机都被分配了一个 32 位的 IP 地址，这种互联网地址是在网际范围内标识主机的一种逻辑地址。为了让报文在物理链路中传送，必须知道目的主机的物理地址。这就需要把 IP 地址通过映射关系转换成物理地址。在以太网环境中采用的物理地址是 48 位 MAC 地址，为了正确地向目的主机传送报文，必须把目的主机的 32 位 IP 地址转换成为 48 位以太网的地址。为此产生了 ARP（Address Resolution Protocol，地址解析协议），该协议主要用于 IP 地址到 MAC 地址的解析，建立 IP 地址和 MAC 地址的映射关系。

ARP 地址映射表项包括以下两种类型：

- 静态表项：静态表项是将 IP 地址和 MAC 地址进行静态绑定，用于防止 ARP 动态学习欺骗。

  - 静态 ARP 地址表项需要手动添加，手动删除。
  - 静态 ARP 地址不老化。
- 动态表项：设备通过 ARP 协议自动学习到的 MAC 地址。
  - 动态表项生成由交换机自动完成，不需要手动配置，可以调整动态 ARP 的一些参数。
  - 如果不使用，到达老化时间会老化。

设备支持两种 ARP 地址映射表项动态学习模式：**learn-all** 和 **learn-reply-only**。

- 当设备处于 **learn-all** 模式时，对 ARP 请求报文和应答报文都进行学习。当 A 设备在发送其 ARP 请求分组时，会将自己 IP 地址和物理地址的映射关系写入 ARP 请求报文。当 B 设备收到 A 设备的 ARP 请求报文时，会将 A 设备的地址映射关系学习到自己的地址映射表中。这样 B 设备后续向 A 设备发送报文时就不用再进行 ARP 请求了。
- 当设备处于 **learn-reply-only** 模式时，只对自己发出的 ARP 请求报文对应的 ARP 应答报文进行学习。对于来自其他设备的 ARP 请求报文，只回应 ARP 应答报文，但不进行 ARP 地址映射表项的学习。这种情况下加重了网络的负担，但可以避免某些基于 ARP 请求报文的网络攻击。

5.4.2 配置准备

场景

IP 地址和 MAC 地址的映射关系保存在 ARP 地址映射表中。

一般情况下，ARP 地址映射表项由设备动态维护，设备按照 ARP 协议自动寻找 IP 地址和 MAC 地址之间的映射关系，无需用户关注。只有在防止 ARP 动态学习欺骗，需要添加静态 ARP 地址映射表项时，才需要对设备进行手动配置。

前提

无

5.4.3 ARP 的缺省配置

设备上 ARP 的缺省配置如下。

功能	缺省值
静态 ARP 表项	无
动态 ARP 学习模式	**learn-all**
动态 ARP 老化时间	1200 秒
接口动态学习 ARP 功能	使能
本地代理 ARP 功能	禁止
接口动态学习 ARP 的最大数目	8192

功能	缺省值
接口学习免费 ARP 功能	使能

5.4.4 配置静态 ARP 表项

注意

- 静态添加的 ARP 表项的 IP 地址必须属于交换机三层接口所属的 IP 网段。
- 静态 ARP 表项，需要手动添加和手动删除。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**arp** *ip-address mac-address*	配置静态 ARP 表项。

5.4.5 配置动态 ARP 表项

请在需要配置的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**arp mode** { **learn-all** | **learn-reply-only** }	（可选）配置动态 ARP 表项的学习模式。
3	Inspur(config)#**arp aging-time** *time*	配置动态 ARP 老化时间。
4	Inspur(config)#**interface vlan** *vlan-id* Inspur(config-vlan*)#**arp max-learning-num** *number*	（可选）配置三层接口下允许学习的最大动态 ARP 表项数目。
5	Inspur(config-vlan*)#**arp learning** [**strict**] { **enable** | **disable** }	配置动态学习 ARP 功能。

5.4.6 配置本地代理 ARP 功能

请在需要配置的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式。
3	Inspur(config-vlan*)#**arp local-proxy enable**	使能本地 ARP 代理功能。

5.4.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show arp** [*ip-address* | **interface** [*interface-type interface-number* | **vlan** *vlan-id*] [**valid**] | **static** | **valid**]	查看 ARP 地址映射表中的表项信息。
2	Inspur#**show arp local-proxy** [**interface vlan** *vlan-id*]	查看本地代理 ARP 信息。

5.4.8 维护

用户可以通过以下命令，维护设备 ARP 特性的运行情况和配置情况。

命令	描述
Inspur(config)#**clear arp** [*ip-address* | **interface** { *interface-type interface-number* | **vlan** *vlan-id* }]	清空 ARP 地址映射表中所有表项。

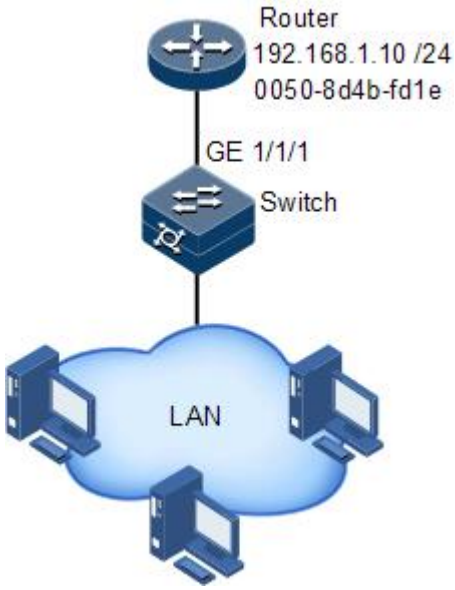
5.4.9 配置 ARP 示例

组网需求

如图 5-3 所示，交换机设备连接主机，通过接口 GE 1/1/1 连接上游的 Router。Router 的 IP 地址为 192.168.1.10/24，MAC 地址为 0050.8d4b.fd1e。

为了增加交换机和 Router 通信的安全性，需要在交换机上配置相应的静态 ARP 表项。

图5-3 配置 ARP 组网示意图



配置步骤

配置增加一条 ARP 静态表项。

```
Inspur#config
Inspur(config)#arp 192.168.1.10 0050.8d4b.fd1e
```

检查结果

通过 **show arp** 命令查看 ARP 地址映射表中的所有表项信息是否正确。

```
Inspur#show arp
ARP aging-time: 1200 seconds(default: 1200s)
ARP mode: Learn all
ARP table:
Total: 1    Static: 1    Dynamic: 0
IP Address      Mac Address     Interface                    Type
Age(s)    status
------------------------------------------------------------------------------
---------------------------
192.168.1.10     0050.8D4B.FD1E    0                      static    --
PERMANENT
```

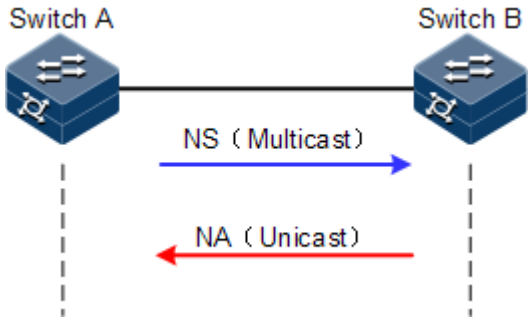
5.5 NDP

5.5.1 简介

NDP（Neighbor Discovery Protocol，邻居发现协议）通过在同一链路上的 IPv6 设备上使用邻居发现机制，来发现彼此的存在、确定彼此的 MAC 地址并维护邻居设备信息。

NDP 通过邻居请求消息 NS（Neighbor Solicitation）和邻居通告消息 NA（Neighbor Advertisement）获取同一链路上邻居设备的链路层地址，即 MAC 地址。

图5-4 NDP 地址解析原理示意图



如图 5-4 所示，以 Switch A 为例，Switch A 要获取 Switch B 的链路层地址。具体报文处理过程如下：

1. Switch A 通过组播方式发送 NS 消息。其中 NS 消息的源地址是 Switch A 三层接口的 IPv6 地址，目的地址是 Switch B 的被请求节点组播地址，消息内容中还包含了 Switch A 的链路层 MAC 地址。
2. Switch B 收到 NS 消息后，判断报文的目的地址是否为自己的 IPv6 地址对应的被请求设备组播地址。如果是，则 Switch B 可以学习到 Switch A 的链路层地址，并以单播方式发送 NA 消息，其中包含了自身的链路层地址。
3. Switch A 收到 Switch B 发送的 NA 消息，就可以获得 Switch B 的链路层地址。

IPv6 邻居发现协议通过使用 ICMPv6 消息，还可以实现验证邻居是否可达、重复地址检测、路由设备发现/前缀发现、地址自动配置和重定向等功能。

5.5.2 配置准备

场景

IPv6 邻居发现协议不但实现了 IPv4 中的 ARP 协议、ICMP 重定向和 ICMP 设备发现等功能，还提供了邻居可达性检测功能。

前提

在配置 NDP 功能之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。

- 配置三层接口的 IPv6 地址。

5.5.3 NDP 的缺省配置

设备上 NDP 的缺省配置如下。

功能	缺省值
重复地址检测发送 NS 次数	1
允许学习的最大 NDP 数量	4096
动态 NDP 老化时间	1200 秒

5.5.4 配置静态邻居表项

将邻居节点的 IPv6 地址解析为链路层地址，可以通过邻居请求消息 NS 及邻居通告消息 NA 来动态实现，也可以通过手工配置静态邻居表项来实现。

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#ipv6 neighbor` *ipv6-address mac-address*	配置静态邻居表项信息。

5.5.5 配置动态 NDP 老化时间

邻居信息表项中的表项并非永远有效，每一条记录都有一个生存周期，到达生存周期仍得不到刷新的记录将从邻居信息表项中删除，这个生存周期被称作老化时间。

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#ipv6 neighbor aging-time` *time*	配置动态 NDP 老化时间。

5.5.6 配置重复地址检测发送 NS 次数

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ipv6 nd dad attempts** *value*	配置重复地址检测时发送 NS 的次数。

说明

当设备获得一个 IPv6 地址后，需要使用重复地址检测功能确定该 IPv6 地址是否已被其他设备使用。发送指定的 NS 次数之后，如果没有收到任何回应，则认为该 IPv6 地址没有重复，可以使用。

5.5.7 配置允许学习的最大 NDP 数量

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ipv6 neighbors max-learning-num** *number*	配置允许学习的最大 NDP 数量。

5.5.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show ipv6 neighbors**	查看所有 NDP 邻居信息。
2	Inspur#**show ipv6 neighbors** *ipv6-address*	查看指定 IPv6 地址的邻居信息。
3	Inspur#**show ipv6 neighbors** *interface-type interface-number*	查看指定三层接口上的邻居信息。
4	Inspur#**show ipv6 neighbors vlan** *vlan-id*	查看指定 VLAN 接口上的邻居信息。
5	Inspur#**show ipv6 neighbors static** [**count**]	查看 IPv6 静态邻居信息。
6	Inspur#**show ipv6 neighbors dynamic count**	查看 IPv6 动态邻居数目信息。
7	Inspur#**show ipv6 neighbors all count**	查看 IPv6 所有邻居数目信息。
8	Inspur#**show ipv6 interface nd** [*interface-type interface-number*]	查看接口下配置的 ND 信息。

5.5.9 维护

用户可以通过以下命令维护 NDP 特性。

命令	描述
Inspur(config)#**clear ipv6 neighbors**	清除所有 IPv6 邻居信息。

5.6 路由管理

5.6.1 配置准备

场景

动态路由协议要求使用 Router ID，如果在启动这些路由协议时没有指定 Router ID，则缺省使用路由管理的 Router ID。

设备有建立、刷新路由表的能力，并根据路由表转发数据包，通过查看路由表信息，也有助于了解网络拓扑结构和定位问题。

前提

无

5.6.2 配置路由管理

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router id** *router-id*	配置路由设备 ID。 缺省情况下，路由设备 ID 为 192.168.1.1。
3	Inspur(config)#**route recursive-lookup tunnel** [**ip-prefix** *listname*]	配置非标签公网路由迭代到 LSP 隧道。

5.6.3 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show router id**	查看设备的路由设备 ID。

序号	检查项	说明
2	Inspur#**show ip route protocol** { **static** | **connected** | **bgp** | **ospf** | **isis** | **rip** } [**detail**] Inspur#**show ipv6 route protocol** { **static** | **connected** | **bgp** | **ospf** | **isis** | **rip** } [**detail**]	查看路由表路由协议信息。
3	Inspur#**show ip route** *ip-address* [*mask-address*] [**longer-prefixes**] [**detail**]	查看去往某一目的地址的路由信息。
4	Inspur#**show ip route** *ip-address1* [*mask-address1*] *ip-address2* [*mask-address2*] [**detail**]	查看两个 IP 地址范围内的路由信息。
5	Inspur#**show**{ **ip** | **ipv6** } **route summary**	查看路由摘要信息。
6	Inspur#**show ip fib** [*ip-address* | **nexthop** *ip-address*]	查看 IP 路由转发表信息。
7	Inspur#**show ipv6 fib** [*ipv6-address* | **nexthop** *ipv6-address*]	查看 IPv6 FIB 表项信息。
8	Inspur#**show ip fib summary**	查看路由转发表统计信息。
9	Inspur#**show ipv6 fib summary**	查看 IPv6 路由转发表统计信息。

5.7 静态路由

5.7.1 简介

路由是将报文穿过网络传递到目的地的行为，在传递过程中采用路由表进行转发。不同 VLAN 间的设备进行通讯，或同一 VLAN 跨越不同网络进行通信，需要使用路由功能。

路由功能执行有以下三种方式：

缺省路由

缺省路由是一种特殊的静态路由，只有在路由表中没有找到匹配的路由表项时才会被使用。在路由表中，缺省路由以到达网络 IP 地址 0.0.0.0、掩码为 0.0.0.0 的路由形式出现。可通过命令 **show ip route** 查看当前是否配置了缺省路由。如果设备没有配置缺省路由且报文的目的 IP 地址不在路由表中，那么设备在丢弃该报文的同时，会向报文发送端返回一个 ICMP 报文，报告该目的地址或网络不可达。

静态路由

静态路由是需要用户手动配置的路由，对系统要求低，适用于拓扑结构简单并且稳定的小型网络。缺点是不能自动适应网络拓扑的变化，需要人工干预，当网络拓扑结构发生变化时，必须经过人工介入。

动态路由

动态路由，通过路由协议动态学习路由，可以为报文转发动态计算出最优的路径，计算过程中需要占用较多的带宽和网络资源。目前有两类动态路由协议：

- 距离矢量协议，每台设备维护一个矢量表，表中列出了当前已知的到其他目标设备的最佳距离，以及所通过的路径。通过在邻居设备之间相互交换信息，设备不断地更新它们内部的矢量表。
- 链路状态协议，设备之间通过通告网络接口的状态来建立链路状态数据库，该数据库中包含与所有设备直连的每条链路的状态。所有设备将会有共同的网络拓扑，但是每一台设备都会独立判断到达网络拓扑内每一个节点的最佳路径。链路状态协议能够快速响应拓扑变化的情况，但是相对于距离矢量协议需要占用更多的带宽和资源。

5.7.2 配置准备

场景

对于拓扑结构比较简单的网络，可以配置静态路由。静态路需要由用户手动配置，通过配置静态路由可以建立一个互通的网络。

前提

正确配置 VLAN 接口的 IP 地址。

5.7.3 配置静态路由

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ip route** *ip-address ip-mask* { **tunnel** *tunnel-number* | *next-hop-ip-address* [*interface-type interface-num* | **vlan** *vlan-id*] | **NULL 0** } [**distance** *distance-num*] [**description** *description-text*] [**tag** *tag-id*] [**track bfd-session** *session-id*] Inspur(config)#**ip route** *ip-address/mask-length* { *next-hop-ip-address* | **NULL 0** } [**distance** *distance-num*] [**description** *description-text*] [**tag** *tag-id*] [**track bfd-session** *session-id*]	配置 IPv4 静态路由。支持 BFD 检测。接口断开，BFD 为 down，静态路由删除；接口 up，BFD 为 up，静态路由添加到列表中。

步骤	配置	说明
	Inspur(config)#**ipv6 route** *ipv6-address/prefix-length* { *next-hop-ipv6-address* | **tunnel** *tunnel-number* | **NULL 0** } [**distance** *distance-num*] [**description** *text*] [**tag** *tag-id*]	配置 IPv6 静态路由。
3	Inspur(config)#**ip route static distance** *distance*	（可选）配置 IPv4 静态路由的缺省管理距离。缺省情况下，管理距离为 1。
	Inspur(config)#**ipv6 route static distance** *distance*	（可选）配置 IPv6 静态路由的缺省管理距离。缺省情况下，管理距离为 1。

5.7.4 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

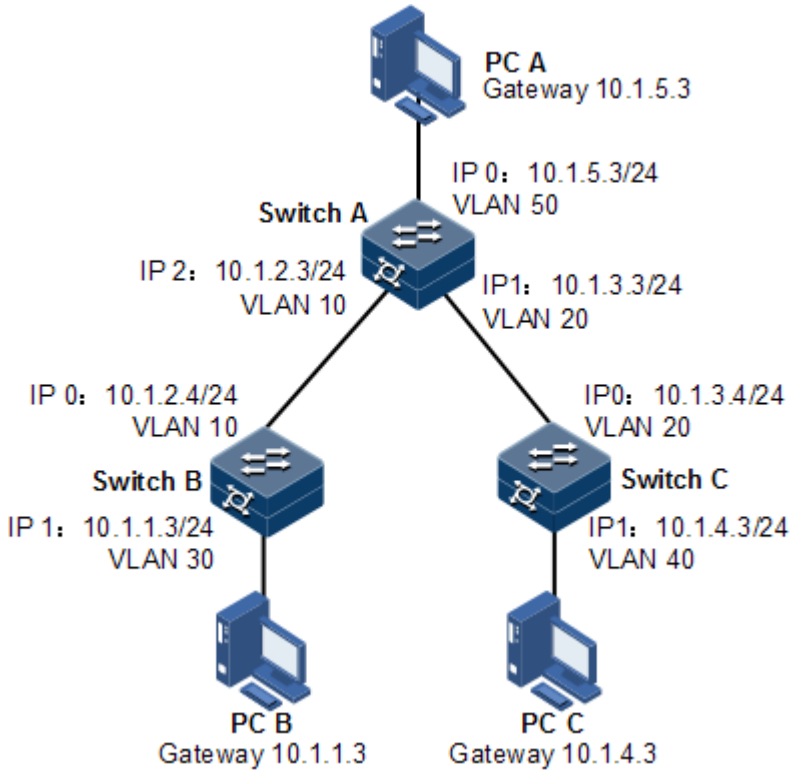
序号	检查项	说明
1	Inspur#**show ip route** [**detail**]	查看 IPv4 路由信息。
2	Inspur#**show ipv6 route** [**all**]	查看 IPv6 路由信息。
3	Inspur#**show ip route protocol** { **static** | **connected** | **bgp** | **ospf** | **isis** | **rip** } [**detail**] Inspur#**show ipv6 route** [**all**] **protocol** { **static** | **connected** | **bgp** | **ospf** | **isis** | **rip** }	查看路由表路由协议信息。
4	Inspur#**show ip route** *ip-address* [*mask-address*] [**longer-prefixes**] [**detail**]	查看去往某一目的地址的路由信息。
5	Inspur#**show ip route** *ip-address1* [*mask-address1*] *ip-address2* [*mask-address2*] [**detail**]	查看两个 IP 地址范围内的路由信息。
6	Inspur#**show** { **ip** | **ipv6** } **route summary**	查看路由摘要信息。

5.7.5 配置静态路由示例

组网需求

配置静态路由，使图 5-5 中的任意两台主机或交换机设备之间能够相互 Ping 通。

图5-5 配置静态路由组网示意图



配置步骤

步骤 1 配置各设备的 IP 地址。具体配置略。

步骤 2 在 Switch A 上配置静态路由。

```
Inspur#hostname SwitchA
SwitchA#config
SwitchA(config)#ip route 10.1.1.0 255.255.255.0 10.1.2.4
SwitchA(config)#ip route 10.1.4.0 255.255.255.0 10.1.3.4
```

步骤 3 在 Switch B 上配置缺省网关。

```
Inspur#hostname SwitchB
SwitchB#config
SwitchB(config)#ip route 0.0.0.0 0.0.0.0 10.1.2.3
```

步骤 4 在 Switch C 上配置缺省网关。

```
Inspur#hostname SwitchC
SwitchC#config
SwitchC(config)#ip route 0.0.0.0 0.0.0.0 10.1.3.3
```

步骤 5 在主机 A 上配置默认网关为 10.1.5.3，具体配置略。

在主机 B 上配置默认网关为 10.1.1.3，具体配置略。

在主机 C 上配置默认网关为 10.1.4.3，具体配置略。

检查结果

通过 **ping** 命令查看所有设备之间是否均能两两互通。

```
SwitchA#ping 10.1.1.3
Type CTRL+C to abort
Sending 5, 8-byte ICMP Echos to 10.1.1.3, timeout is 3 seconds:
Reply from 10.1.1.3: time<1ms
Reply from 10.1.1.3: time<1ms
Reply from 10.1.1.3: time<1ms
Reply from 10.1.1.3: time<1ms
Reply from 10.1.1.3: time<1ms

---- PING Statistics----
5 packets transmitted, 5 packets received,
Success rate is 100 percent(5/5),

round-trip (ms)  min/avg/max = 0/0/0.
```

5.8 路由策略

5.8.1 配置 IP 前缀列表

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ip prefix-list** *prefix-name* **seq** *seq-number* { **deny** | **permit** } **any**	创建 IP 前缀列表，或向其中添加一项结点。 若不配置前缀列表序号 *seq-number*，则由系统自动生成，生成的序号步长为 5。
	Inspur(config)#**ip prefix-list** *prefix-name* **seq** *seq-number* { **deny** | **permit** } *ip-address/mask* [**ge** *min-length*] [**le** *max-length*]	
3	Inspur(config)#**ip prefix-list** *prefix-name* **description** *string*	配置 IP 前缀列表的描述信息。 若输入的描述信息超过 80 字符，则不会生效。
4	Inspur(config)#**ipv6 prefix-list** *prefix-name* **seq** *seq-number* { **deny** | **permit** } **any** Inspur(config)#**ipv6 prefix-list** *prefix-name* **seq** *seq-number* { **deny** | **permit** } *ipv6-address/mask* [**ge** *min-length*] [**le** *max-length*]	创建 IPv6 前缀列表，或向其中添加一项节点。
5	Inspur(config)#**ipv6 prefix-list** *prefix-name* **description** *string*	配置 IPv6 前缀列表的描述信息。

说明

- 若一条记录为 **permit** 类型，所有不匹配的路由均默认为 **deny** 类型，则只有匹配的路由可以通过该列表的过滤。
- 若一条记录为 **deny** 类型，所有不匹配的路由均默认为 **deny** 类型，则即使有匹配的路由也不能通过。故需要在多条 **deny** 类型的记录后添加一条 **permit** 类型的记录，允许其它所有路由通过。
- 故若 IP 前缀列表中有多条记录，则至少有一条是 **permit** 类型。

5.8.2 配置路由映射表

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**route-map** *map-name* { **permit** | **deny** } *number*	创建路由映射表，并进入路由映射配置模式。
3	Inspur(config-route-map)#**description** *string*	（可选）配置路由映射表的描述信息。 若描述信息中携带空格，请用引号将描述信息括起来。
4	Inspur(config-route-map)#**on-match next**	（可选）配置 on-match 子句为，匹配后去下一个结点继续匹配。 缺省情况下，匹配后结束匹配过程。
5	Inspur(config-route-map)#**on-match goto** *number*	（可选）配置 on-match 子句为，匹配后去某一个结点继续匹配。 缺省情况下，匹配后结束匹配过程。
6	Inspur(config-route-map)#**call** *map-name*	（可选）配置路由匹配后调用其它路由映射表继续匹配。 缺省情况下，匹配后结束匹配过程。
7	Inspur(config-route-map)#**match ip next-hop** *acl-number*	（可选）配置 match 子句，基于扩展 IP ACL 匹配下一跳。
8	Inspur(config-route-map)#**match ip next-hop prefix-list** *prefix-name*	（可选）配置 match 子句，基于 IP 前缀列表匹配下一跳。
9	Inspur(config-route-map)#**match ip address** *acl-number*	（可选）配置 match 子句，基于扩展 IP ACL 匹配 IP 地址。
10	Inspur(config-route-map)#**match ip address prefix-list** *prefix-name*	（可选）配置 match 子句，基于 IP 前缀列表匹配 IP 地址。
11	Inspur(config-route-map)#**match interface** *name*	（可选）配置 match 子句，匹配接口名称。

步骤	配置	说明
12	Inspur(config-route-map)#**match metric** *metric*	（可选）配置 match 子句，基于路由度量值的匹配规则。
13	Inspur(config-route-map)#**match tag** *tag*	（可选）配置 match 子句，基于路由标记 Tag 字段的匹配规则。
14	Inspur(config-route-map)#**set metric** [**+** | **-**] *metric*	（可选）配置 set 子句，匹配后修改路由度量值。
15	Inspur(config-route-map)#**set metric-type** { **type-1** | **type-2** }	（可选）配置 set 子句，匹配后修改路由的度量值类型。
16	Inspur(config-route-map)#**set src** *ip-address*	（可选）配置 set 子句，匹配后修改源 IP 地址。
17	Inspur(config-route-map)#**set ip next-hop** *ip-address*	（可选）配置 set 子句，匹配后修改路由下一跳 IP 地址。
18	Inspur(config-route-map)#**set tag** *tag*	（可选）配置 set 子句，匹配后修改路由信息标记。

5.8.3 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show ip prefix-list** [*prefix-name*] [**seq** *seq-number*] Inspur#**show ip prefix-list** *prefix-name ip-address/mask* { **longer** | **first-match** }	查看 IP 前缀列表信息。
2	Inspur#**show ip prefix-list summary** [*prefix-name*]	查看 IP 前缀列表概要信息。
3	Inspur#**show ip prefix-list detail** [*prefix-name*]	查看 IP 前缀列表统计信息。
4	Inspur#**show ipv6 prefix-list** [*prefix-name*] [**seq** *seq-number*] Inspur#**show ipv6 prefix-list** *prefix-name ipv6-address/mask* { **longer** | **first-match** }	查看 IPv6 前缀列表信息。
5	Inspur#**show ipv6 prefix-list summary** [*prefix-name*]	查看 IPv6 前缀列表概要信息。
6	Inspur#**show ipv6 prefix-list detail** [*prefix-name*]	查看 IPv6 前缀列表统计信息。
7	Inspur#**show route-map** [*map-name*]	查看路由映射表配置信息。

5.8.4 维护

用户可以通过以下命令，维护设备路由策略特性的运行情况和配置情况。

命令	描述
Rasiecom#**clear ip prefix-list** [*prefix-name* [*ip-address/mask*]]	清空 IP 前缀列表的统计信息。
Rasiecom#**clear ipv6 prefix-list** [*prefix-name* [*ipv6-address/mask*]]	清空 IPv6 前缀列表的统计信息。

5.9 OSPFv2

5.9.1 简介

OSPF（Open Shortest Path First，开放最短路径优先）是一种基于链路状态的动态路由选择协议。本文的 OSPF 均指对 IPv4 协议使用的 OSPFv2。

由于 RIP 协议存在收敛慢、路由环路及扩展性差等问题，不适合大规模网络。与 RIP 等路由协议相比，OSPF 具有如下特点：

- 适应范围广：支持各种规模的网络，特别是大型网络。
- 收敛速度快：在网络拓扑结构发生变化后立即发送更新报文，并将变化在 AS（Autonomous System，自治系统即由一组使用相同路由协议来交换路由信息的路由设备组成的网络）中同步。
- 无路由自环：OSPF 根据收集到的链路状态利用最短路径树算法计算路由，从算法本身保证了不会形成路由自环。
- 支持区域划分：允许将网络划分成不同区域来分层管理，区域间传送的路由信息被进一步抽象，从而减少了占用的网络带宽。
- 支持等价路由：支持到同一目的地址的多条等价路由。
- 支持组播：在某些类型的链路上以组播地址发送协议报文，减少对其它设备的干扰。
- 支持动态学习和发布公网路由。
- 支持支持 BFD for OSPF。

OSPF 的网络类型

根据链路层协议类型，OSPF 将网络分为以下几种类型：

- 广播（Broadcast）类型：当链路层协议是 Ethernet 或 FDDI 时，OSPF 缺省认为网络类型是 Broadcast。在该类型的网络中，通常以组播形式（组播地址为 224.0.0.5 和 224.0.0.6）发送协议报文。
- P2MP（Point-to-MultiPoint，点到多点）类型：没有一种链路层协议会被缺省的认为是 P2MP 类型，必须是由其他的网络类型强制更改的。常用做法是将 NBMA 改

为 P2MP。在该类型的网络中，缺省情况下，以组播形式（组播地址为 224.0.0.5）发送协议报文。可以根据用户需要，以单播形式发送协议报文。

- P2P（Point-to-Point，点到点）类型：当链路层协议是 PPP 或 HDLC（High-Level Data Link Control，高级数据链路控制）时，OSPF 缺省认为网络类型是 P2P。在该类型的网络中，以组播形式（组播地址为 224.0.0.5）发送协议报文。

路由设备 ID 号

一台路由设备如果要运行 OSPF 协议，则必须存在 Router ID（路由设备 ID）。Router ID 是一个 32 比特无符号整数，可以在一个自治系统中唯一的标识一台路由设备。

说明

Router ID 可以由系统选举产生，也可以手动进行配置。Router ID 选举规则如下：

- 若存在配置 IP 地址的 Loopback 接口，则选择 Loopback 接口地址中最大的作为 Router ID；
- 若没有配置 IP 地址的 Loopback 接口，则从 IP 接口中选择 IP 地址最大的作为 Router ID；
- 若 IP 地址已经被其它 OSPF 进程选用，则不能被该进程选用；
- 若没有配置任何 IP 地址，则无法选举 Router ID，无法创建进程，只能手动配置 Router ID。

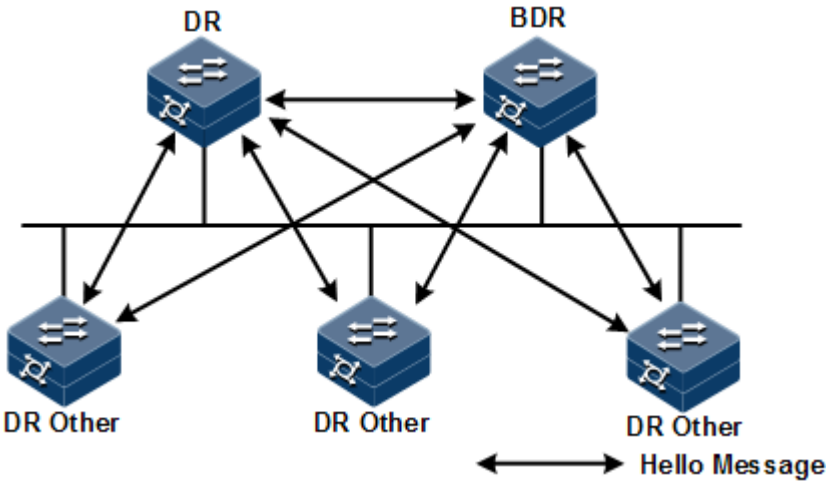
DR/BDR

在广播网络中，任意两台路由设备之间都要交换路由信息。这使得任何一台路由设备的路由变化都会导致多次传递，浪费了带宽资源。为解决这一问题，OSPF 协议定义了 DR（Designated Router，指定路由设备），所有路由设备都只将信息发送给 DR，由 DR 将网络链路状态发送出去。

当 DR 由于某种故障而失效，为了避免 DR 重新选举时间内路由计算的不正确性，OSPF 提出了 BDR（Backup Designated Router，备份指定路由设备）的概念。在选举 DR 的同时也选举出 BDR，BDR 也和本网段内的所有路由设备建立邻接关系并交换路由信息。当 DR 失效后，BDR 会立即成为 DR。这时还需要重新选举一个新的 BDR，但不会影响路由的计算。

运行 OSPF 进程的网络中，既不是 DR 也不是 BDR 的路由设备为 DR Other（其他路由设备）。DR Other 仅与 DR 和 BDR 之间建立邻接关系，DR Other 之间不交换任何路由信息，如图 5-6 所示，减少了广播网络和 NBMA 网络上各路由设备之间邻接关系的数量，同时减少网络流量，节约了带宽资源。

图5-6 广播类型接口角色示意图



说明

- 只有在广播类型接口才会选举 DR，在 P2MP 或 P2P 类型的接口上不需要选举 DR。
- DR 是某个网段中的概念，针对路由设备的接口。某台路由设备在一个接口上可能是 DR，在另一个接口上可能是 BDR 或者 DR Other。
- DR 和 BDR 是由同一网段中所有的路由设备根据路由设备优先级、Router ID 通过 Hello 报文选举出来的，只有优先级大于 0 的设备才具有选举资格。如果优先级相等，则 Router ID 大者胜出。优先级为 0 路由设备不会被选举为 DR 或 BDR。
- 路由设备的优先级可以影响 DR/BDR 的选举，但当选举结束，再有更高优先级的路由设备变为有效，也不会替换原 DR/BDR，直到重新进行 DR/BDR 选举。

OSPF 的协议报文

OSPF 协议报文主要包括以下几种：

- Hello 报文：周期性发送，用来发现和维持 OSPF 邻居关系。内容包括一些定时器的时间值、DR、BDR、优先级以及已知的邻居信息。
- DD（Database Description，数据库描述）报文：描述了本地 LSDB 中每一条 LSA（Link State Advertisement，链路状态通告）的摘要信息，即 LSA 报文头部，用于两台路由设备进行数据库同步。
- LSR（Link State Request，链路状态请求）报文：向对方请求所需的 LSA。两台路由设备互相交换 DD 报文之后，得知对端路由设备有哪些 LSA 是本地 LSDB 所缺少的，就需要发送 LSR 报文向对方请求所需的 LSA。内容包括所需要的 LSA 摘要。
- LSU（Link State Update，链路状态更新）报文：向对方发送其所需要的 LSA。内容是多条 LSA 的集合。

- LSAck（Link State Acknowledgment，链路状态确认）报文：用来对收到的 LSA 进行确认。内容是需要确认的 LSA 头部（一个报文可对多个 LSA 进行确认）。

LSA 的类型

OSPF 对链路状态信息的描述被封装在 LSA 中发布出去，常用的 LSA 有以下几种类型：

- Router LSA（Type1）：由每个路由设备产生，描述该路由设备的链路状态和开销，在其始发的区域内传播。
- Network LSA（Type2）：由 DR 产生，描述本网段所有路由设备的链路状态，在其始发的区域内传播。
- Network Summary LSA（Type3）：由 ABR（Area Border Router，区域边界路由设备）产生，描述区域内某个网段的路由，并通告给其他区域。
- ASBR Summary LSA（Type4）：由 ABR 产生，描述到 ASBR（Autonomous System BoundaryRouter，自治系统边界路由设备）的路由，通告给相关区域。
- AS External LSA（Type5）：由 ASBR 产生，描述到 AS 外部的路由，通告到所有的区域，除了 Stub 区域。

邻居和邻接

OSPF 路由设备启动后，通过 OSPF 接口向外发送 Hello 报文。收到 Hello 报文的设备会检查报文中所定义的参数（包括 Hello 报文发送间隔、失效时间以及区域掩码信息等），如果双方一致就会形成邻居（Neighbor）关系。

形成邻居关系的双方不一定都能形成邻接关系，要根据网络类型而定。只有当双方成功交换 DD 报文，交换 LSA 并达到 LSDB 的同步之后，才形成真正意义上的邻接（Adjacency）关系。

OSPF 路由的计算过程

OSPF 协议中，路由的计算过程如下：

1. 每台 OSPF 路由设备根据网络拓扑结构生成 LSA，并通过更新报文将 LSA 发送给网络中的其它 OSPF 路由设备。
2. 每台 OSPF 路由设备都会收集其它路由设备通告的 LSA，所有的 LSA 组成了 LSDB。LSA 是对路由设备周围网络拓扑结构的描述，LSDB 则是对整个自治系统的网络拓扑结构的描述。
3. OSPF 路由设备将 LSDB 转换成一张带权值的有向图，这张图便是对整个网络拓扑结构的真实反映。各个路由设备得到的有向图是完全相同的。
4. 每台路由设备根据有向图，使用 SPF（Shortest Path First，最短路径优先）算法计算出一棵以自己为根的最短路径树，这棵树给出了到自治系统中各节点的路由。

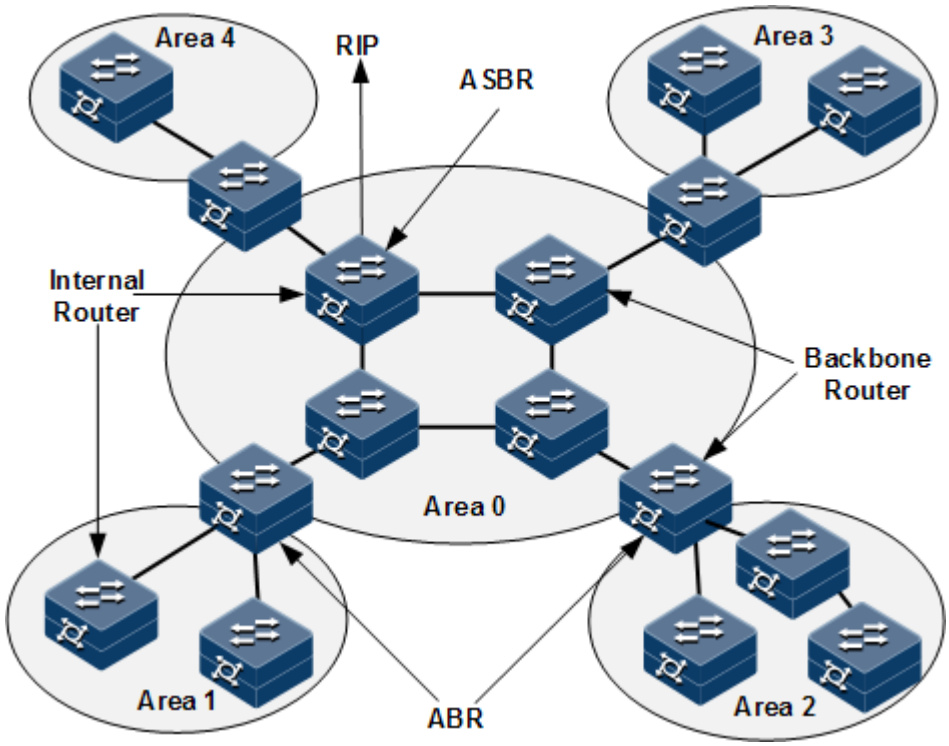
区域划分

当大型网络中的路由设备都运行 OSPF 协议时，路由设备数量的增多会导致 LSDB 非常庞大，占用大量存储空间，导致 CPU 负担很重。网络规模增大，拓扑结构发生变化的概率也会增大，网络会经常处于“振荡”之中，造成网络中会有大量的 OSPF 协议

报文在传递，降低网络带宽的利用率，并且每一次变化都会导致网络中所有路由设备重新进行路由计算。

OSPF 协议通过将自治系统划分成不同的区域（Area）来解决上述问题。区域是指从逻辑上将路由设备划分为不同的组，每个组用区域号（Area ID）来标识。如图 5-7 所示，每个区域内的路由设备只维护本区域内的路由信息，而不是整个网络的路由信息。

图5-7 OSPF 区域及路由设备类型



每个区域的边界是路由设备，而不是链路。一个路由设备可以属于不同的区域，但是一个网段（链路）只能属于一个区域，或者说每个运行 OSPF 的接口必须指明属于哪一个区域。划分区域后，可以在区域边界路由设备上进行路由聚合，以减少通告到其他区域的 LSA 数量，还可以将网络拓扑变化带来的影响最小化。

路由设备的类型

如图 5-7 所示，OSPF 路由设备根据在 AS 中的不同位置，可以分为以下四类：

- 区域内路由设备（Internal Router）：该类路由设备所有接口都属于同一 OSPF 区域。
- 区域边界路由设备（Area Border Router，ABR）：该类路由设备可以同时属于两个以上的区域，但其中一个必须是骨干区域。ABR 用来连接骨干区域和非骨干区域，它与骨干区域之间既可以是物理连接，也可以是逻辑上的连接。
- 骨干路由设备（Backbone Router）：该类路由设备至少有一个接口属于骨干区域。因此，所有的 ABR 和位于 Area 0 的内部路由设备都是骨干路由设备。

- 自治系统边界路由设备（Autonomous System Border Router，ASBR）：与其他 AS 交换路由信息的路由设备称为 ASBR。ASBR 并不一定位于 AS 的边界，可能是区域内路由设备或者 ABR。只要 OSPF 路由设备引入了外部路由信息，就会成为 ASBR。

骨干区域

OSPF 划分区域之后，并非所有区域都是平等关系，有一个特殊的区域，区域号（Area ID）是 0，被称为骨干区域。骨干区域负责区域之间的路由，非骨干区域之间的路由信息必须通过骨干区域来转发。要求如下：

- 所有非骨干区域必须与骨干区域保持连通。
- 骨干区域自身也必须保持连通。

Stub 区域

由于边缘路由设备性能较低，需要对路由表进行一定的限制。配置 Stub 区域就是为了让外部 LSA 尽可能少的进入到区域内部。

在 Stub 区域内，只通告 Type1、Type2 和 Type3 类 LSA，ABR 不允许注入 Type5 LSA，大大减少了路由表规模以及路由信息传递的数量。还可以将该区域配置为 Totally Stub（完全 Stub）区域，只通告 Type1、Type2 和一条默认的 Typr3 类 LSA，以进一步减少 Stub 区域中路由设备的路由表规模以及路由信息传递的数量。完全 Stub 区域的 ABR 不会将区域间路由信息和外部路由信息传递到本区域。

并不是每个区域都符合配置（Totally）Stub 区域的条件。通常来说，（Totally）Stub 区域位于自治系统的边界。为保证到本自治系统的其他区域或者自治系统外的路由依旧可达，该区域的 ABR 将生成一条缺省路由，并发布给本区域中的其他非 ABR 路由设备。

路由类型

OSPF 将路由分为四类，按照优先级从高到低的顺序依次为：区域内路由（Intra Area）、区域间路由（Inter Area）、第一类外部路由（Type1 External）和第二类外部路由（Type2 External）。

区域内路由和区域间路由描述的是 AS 内部的网络结构；外部路由则描述了应该如何选择到 AS 以外目的地址的路由，根据是否计算 AS 内部路径开销分为第一类外部路由和第二类外部路由。

- 第一类外部路由的开销=本地路由设备到相应 ASBR 的开销+ASBR 到该路由目的地址的开销。
- 第二类外部路由的开销=ASBR 到该路由目的地址的开销。

OSPF 协议认为第一类外部路由可信度高一些，在对于同一个目的地址同时存在第一类外部路由和第二类外部路由时，不管这两条外部路由的花费是多少，均优选第一类外部路由。

5.9.2 配置 OSPF 基本功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router ospf** *process-id* [**router-id** *router-id*]	启动一个 OSPF 进程，并进入 OSPF 配置模式。
3	Inspur(config-router-ospf)#**network** *ip-address wild-card-mask* **area** *area-id*	配置 OSPF 区域包含的网段。

- 若通过 **router ospf** *process-id* [**router-id** *router-id*]命令中的可选参数，手动配置了 *router-id*，则 OSPF 进程首选该 *router-id*，否则自动选举出 *router-id*。
- 若进程已经配置或选举出 *router-id*，如果再次修改 *router-id*，则在设备进程重启后生效。

5.9.3 配置 OSPF 路由属性

配置接口的开销值

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**ip ospf cost** *cost*	配置 IP 接口的路由开销。 缺省情况下，未配置接口路由开销。

配置带宽参考值

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router ospf** *process-id* [**router-id** *router-id*]	启动一个 OSPF 进程，并进入 OSPF 配置模式。
3	Inspur(config-router-ospf)#**reference-bandwidth** *bandwidth*	配置链路的带宽参考值。 缺省情况下，带宽参考值为 100Mbit/s。

- 已使用 **ip ospf cost** 命令手动配置接口路由开销时，路由开销按手动配置为准。
- 未手动配置接口路由开销时，配置链路的带宽参考值，则根据链路的带宽参考值自动计算接口路由开销，公式为：开销=带宽参考值（bit/s）/链路带宽，如计算出的开销值大于 65535，取最大值 65535。未配置链路的带宽参考值，则使用缺省值 100Mbit/s。

配置 OSPF 管理距离

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router ospf** *process-id* [**router-id** *router-id*]	启动一个 OSPF 进程，并进入 OSPF 配置模式。
3	Inspur(config-router-ospf)#**distance** *administrative-distance*	配置 OSPF 路由协议的管理距离。 缺省情况下，OSPF 路由协议的管理距离为 110。
4	Inspur(config-router-ospf)#**distance ospf** { **intra-area** | **inter-area** | **external** } *distance*	配置 OSPF 指定类型路由的管理距离。 缺省情况下，OSPF 指定类型路由的管理距离取值为 0。但 OSPF 路由的管理距离仍以 RM 提供的 110 为准。

配置兼容 RFC 1583

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router ospf** *process-id* [**router-id** *router-id*]	启动一个 OSPF 进程，并进入 OSPF 配置模式。
3	Inspur(config-router-ospf)#**compatible rfc1583**	配置 OSPF 兼容 RFC1583。 缺省情况下，OSPF 兼容 RFC1583。

5.9.4 配置负载分担

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router ospf** *process-id* [**router-id** *router-id*]	启动一个 OSPF 进程，并进入 OSPF 配置模式。
3	Inspur(config-router-ospf)#**maximum load-balancing** *number*	配置 IP 等价多路径负载分担的最大路径数。

5.9.5 配置 OSPF 网络

配置 OSPF 网络类型

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**ip ospf network** { **broadcast** | **non-broadcast** | **ptmp** | **ptp** }	配置三层接口网络类型。 缺省情况下，IP 接口的网络类型为广播网络。

配置 DR 选举优先级

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**ip ospf priority** *priority*	在 IP 接口下配置路由器的 DR 选举优先级。 缺省情况下，路由器的 DR 选举优先级为 1。

配置 OSPF NBMA 网络邻居

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**ip ospf network non-broadcast** Inspur(config-gigaethernet1/1/*)#**exit**	配置三层接口网络类型为 NBMA，并退出三层接口配置模式。
4	Inspur(config)#**router ospf** *process-id* [**router-id** *router-id*]	启动一个 OSPF 进程，并进入 OSPF 配置模式。
5	Inspur(config-router-ospf)#**neighbor** *ip-address* [**priority** *priority*]	配置 NBMA 邻居及其优先级。 缺省情况下，未配置 NBMA 邻居，配置邻居时缺省优先级为 0。

注意

使用 **neighbor** 命令和使用 **ip ospf priority** *priority* 命令配置的优先级具有不同的作用：

- **neighbor** 命令配置的优先级用于表示邻居是否具有选举权。如果在配置邻居时将优先级指定为 0，则本地路由设备认为该邻居不具备选举权，不向该邻居发送 Hello 报文，这种配置可以减少在 DR 和 BDR 选举过程中网络上的 Hello 报文数量。但如果本地路由设备是 DR 或 BDR，它也会向优先级为 0 的邻居发送 Hello 报文，以建立邻接关系。
- **ip ospf priority** *priority* 命令配置的优先级用于实际的 DR 选举。

5.9.6 优化 OSPF 网络

配置 OSPF 报文定时器

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**ip ospf dead-interval** *seconds*	配置 OSPF 邻居失效时间。 缺省情况下，失效时间为 4 倍 Hello 报文发送间隔。若没有配置 Hello 发送间隔，P2P、Broadcast 类型接口的缺省值为 40 秒；P2MP、NBMA 类型接口的缺省值为 120 秒。

步骤	配置	说明
4	Inspur(config-gigaethernet1/1/*)#**ip ospf hello-interval** *seconds*	配置 OSPF Hello 报文发送间隔。 缺省情况下，P2P 和 Broadcast 类型接口的 Hello 报文发送间隔为 10 秒；P2MP 和 NBMA 类型接口的 Hello 报文发送间隔为 30 秒。
5	Inspur(config-gigaethernet1/1/*)#**ip ospf poll-interval** *seconds*	配置 OSPF Poll 定时器间隔。 缺省情况下，Poll 定时器间隔为 120 秒。
6	Inspur(config-gigaethernet1/1/*)#**ip ospf retransmit-interval** *seconds*	配置 IP 接口上 LSA 的重传间隔。 缺省情况下，LSA 重传间隔为 5 秒。
7	Inspur(config-gigaethernet1/1/*)#**ip ospf transmit-delay** *seconds*	配置 IP 接口上 LSA 的传输延迟时间。 缺省情况下，IP 接口上 LSA 的传输延迟时间为 1 秒。

注意

未手动配置 dead-interval 时：

- 配置 hello-interval 后 dead-interval 和 poll-interval 自动变为 4 倍 hello-interval。

手动配置了 dead-interval 时：

- 配置 hello-interval 对 dead-interval 和 poll-interval 无影响。
- 不论是否配置 poll-interval，poll-interval 的值会随 dead-interval 的值改变。

因此建议先配置 hello-interval，再配置 dead-interval，最后配置 poll-interval。

配置 SPF 计算时间间隔

当 OSPF 的链路状态数据库（LSDB）发生改变时，需要重新计算最短路径。如果网络频繁变化，且每次变化都立即计算最短路径，将会占用大量系统资源，并影响路由设备的效率。通过调节 SPF 计算时间间隔，可以抑制由于网络频繁变化带来的影响。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router ospf** *process-id* [**router-id** *router-id*]	启动一个 OSPF 进程，并进入 OSPF 配置模式。

步骤	配置	说明
3	Inspur(config-router-ospf)#**timers spf** *delay-time hold-time*	配置 OSPF 路由计算的延时时间和间隔时间。 缺省情况下，延时时间为 2 秒，间隔时间为 3 秒。

配置 OSPF 被动接口

若要使 OSPF 路由信息不被某一网络中的路由设备获得，可以通过配置接口为 OSPF 被动接口来禁止该接口发送 OSPF 报文。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**ip ospf passive-interface enable**	使能 OSPF 接口的被动接口功能。 缺省情况下，禁用接口的被动接口功能。

配置忽略 MTU 功能

缺省情况下，DD 报文中 MTU 域的值为发送该报文接口的 MTU 值。不同设备间 MTU 值的缺省配置可能不同，且如果 DD 报文中的 MTU 值大于接口的 MTU 值，则丢弃该报文。为了保证报文能被正确接收，使能 MTU 检查忽略功能，将报文的 MTU 值配置为 0，使其能被所有设备接收。

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**ip ospf mtu-ignore enable**	使能 IP 接口的 MTU 检查忽略功能。 缺省情况下，设备禁用 IP 接口的 MTU 检查忽略功能，对 OSPF Hello 报文的 MTU 进行检查。

5.9.7 配置 OSPF 认证模式

配置 OSPF 区域认证模式

同一个区域的所有路由设备上都需要配置相同的区域认证模式（不认证、简单认证、MD5 认证）。OSPF 区域没有认证密码，采用接口认证密码。若没有配置接口认证密码，则采则用空密码进行认证。

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)# **router ospf** *process-id* [**router-id** *router-id*]	启动一个 OSPF 进程，并进入 OSPF 配置模式。
3	Inspur(config-router-ospf)#**area** *area-id* **authentication** { **md5** | **simple** }	配置区域认证模式。 缺省情况下，区域认证模式为不认证。

配置 OSPF 接口认证模式

报文认证优先选择接口认证模式，如果接口认证模式为不认证，则选择区域认证模式。只有认证模式和认证密码相同，OSPF 接口才能建立邻居关系。

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**ip ospf authentication** { **md5** | **simple** }	配置 IP 接口认证模式。 缺省情况下，接口认证模式为不认证，以区域认证模式为准。
4	Inspur(config-gigaethernet1/1/*)#**ip ospf authentication-key** { **simple** { **0** | **7** } *password* | **md5** { *key-id* { **0** | **7** } *password* | **keychain** *keychain-name* } }	配置 IP 接口认证密码。

5.9.8 配置 Stub 区域

对于位于 AS 边缘的非骨干区域，可以在该区域的所有路由设备上配置 **stub** 命令，把该区域配置为 Stub 区域。这样，描述自治系统外部路由的 Type5 LSA 不会在 Stub 区域里泛洪，减小路由表的规模。

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router ospf** *process-id* [**router-id** *router-id*]	启动一个 OSPF 进程，并进入 OSPF 配置模式。
3	Inspur(config-router-ospf)#**area** *area-id* **stub** [**no-summary**]	配置区域为 Stub 区域。 **no-summary** 参数用于禁止 ABR 向 Stub 区域内发送 Summary LSA，即 Totally Stub 区域，只用于 Stub 区域的 ABR。 缺省情况下，没有区域被配置为 Stub 区域。
4	Inspur(config-router-ospf)#**area** *area-id* **default-cost** *cost*	配置 Stub 区域缺省路由开销。 该命令只有在 Stub 区域的 ABR 上配置才能生效。 缺省情况下，Stub 区域缺省路由开销值为 1。
5	Inspur(config-router-ospf)#**area** *area-id* **nssa** [**no-summary**]	（可选）配置区域为 NSSA（Not So Stubby Area，次末节区域）

注意

- Stub 区域内的所有路由设备必须使用 **area** *area-id* **stub** 命令配置成 Stub 属性。
- 如果要将一个区域配置成 Totally Stub 区域，该区域中的所有路由器设备必须配置 **area** *area-id* **stub** 命令，且该区域的 ABR 路由设备需要配置 **area** *area-id* **stub no-summary** 命令。
- 骨干区域不能配置为 Stub 区域。
- Stub 区域内不能存在 ASBR，即自治系统外部的路由不能在本区域内传播。

5.9.9 控制 OSPF 路由信息

配置 OSPF 引入路由

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router ospf** *process-id* [**router-id** *router-id*]	启动一个 OSPF 进程，并进入 OSPF 配置模式。

步骤	配置	说明
3	Inspur(config-router-ospf)#**redistribute** { **static** | **connected** | **isis** | **bgp** } [**metric** *metric-value*] [**metric-type** { **1** | **2** }] [**tag** *tag-value*] [**route-map** *map-name*]	配置 OSPF 路由引入策略。 缺省情况下，不引入外部路由。引入外部路由时： • 当引入直连和静态时 metric 缺省为 1，其他类型的路由引入时以外部路由的原始 metric 值作为 LSA 的 metric 值； • 若不指定 Metric-type，则 Metric-type 缺省类为 Type2； • 若不指定 Tag，则以外部路由的原始 Tag 作为 LSA 的 Tag。
	Inspur(config-router-ospf)#**redistribute ospf** [*process-id*] [**metric** *metric*] [**metric-type** { **1** | **2** } [**tag** *tag-value*] [**route-map** *map-name*]	
4	Inspur(config-router-ospf)#**redistribute limit** *limit-number*	配置 OSPF 外部路由引入的数目限制。 缺省情况下，不限制外部路由引入的数目。

配置域间路由聚合

如果区域里存在一些连续的网段，则可以在 ABR 上配置路由聚合，将这些连续的网段聚合成一个网段，ABR 向其它区域发送路由信息时，以网段为单位生成 Type3 LSA。

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router ospf** *process-id* [**router-id** *router-id*]	启动一个 OSPF 进程，并进入 OSPF 配置模式。
3	Inspur(config-router-ospf)#**area** *area-id* **range** *ip-address ip-mask* [**not-advertise**]	配置区域间路由聚合。 缺省情况下，无聚合路由。配置聚合路由时开销缺省为明细 LSA 中最大的 Metric，且发布聚合路由。

配置对引入的外部路由聚合

ASBR 引入外部路由后，配置路由聚合，设备只把聚合后的路由放在 ASE LSA 中向外宣告，减少了 LSDB 中 LSA 的数量。

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router ospf** *process-id* [**router-id** *router-id*]	启动一个 OSPF 进程，并进入 OSPF 配置模式。
3	Inspur(config-router-ospf)#**summary-address** *ip-address ip-mask* [**not-advertise**] [**metric** *metric*]	配置外部路由汇聚。 缺省情况下，不汇聚外部路由。汇聚外部路由时，Metric 缺省为明细 LSA 的最大 Metric。

配置引入缺省路由

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router ospf** *process-id* [**router-id** *router-id*]	启动一个 OSPF 进程，并进入 OSPF 配置模式。
3	Inspur(config-router-ospf)#**default-information originate** [**always**] [**metric** *metric*] [**type** { **1** | **2** }]	引入缺省路由。 缺省情况下，不产生缺省路由。产生缺省 LSA 时，若指定 **always** 关键字，则缺省 Metric 为 1，若不指定 **always** 产生缺省 LSA，则 Metric 为 10。

5.9.10 配置 OSPF 路由策略

配置 OSPF 接收策略

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ip prefix-list** *list-name* { **permit** | **deny** } *ip-address mask-length* [**ge** *ge-length*] [**le** *le-length*]	配置地址前缀列表。
3	Inspur(config)#**access-list** *acl-number*	创建 ACL 并进入 ACL 配置模式。当 *acl-number* 取值为取值在 1000～1999 之间时，进入基本 IP ACL 配置模式。

步骤	配置	说明
	Inspur(config-acl-ip-std)#**rule** [*rule-id*] { **deny** | **permit** } { *source-ip-address source-ip-mask* | **any** }	配置基本 IP ACL 的规则。
4	Inspur(config)#**router ospf** *process-id* [**router-id** *router-id*]	启动一个 OSPF 进程，并进入 OSPF 配置模式。
5	Inspur(config-router-ospf)#**distribute-list** { **ip-access-list** *acl-number* | **prefix-list** *list-name* } **in**	配置 OSPF 接收 OSPF 区域内、区域间和 AS 外部路由的过滤策略。

说明

- 配置 OSPF 接收过滤策略前，需要保证策略引用的 IP ACL 已经创建。
- 基于 IP ACL 进行过滤时，若 ACL 模式为 permit，则匹配该 ACL 的路由通过，否则均不通过。
- 当且仅当 IP ACL 未被任何路由策略引用时，才允许修改 IP ACL。
- 与 IP ACL 不同，地址前缀列表被引用时也可以修改。
- 若配置的前缀列表不存在，不对接收的路由进行过滤。

配置 OSPF 发布策略

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ip prefix-list** *list-name* { **permit** | **deny** } *ip-address mask-length* [**ge** *ge-length*] [**le** *le-length*]	配置地址前缀列表。 可以使用 **no ip prefix-list** *list-name* 命令删除该配置。
3	Inspur(config)#**access-list** *acl-number*	创建 ACL 并进入 AC;配置模式。当 *acl-number* 取值为取值在 1000～1999 之间时，进入基本 IP ACL 配置模式。
	Inspur(config-acl-ip-std)#**rule** [*rule-id*] { **deny** | **permit** } { *source-ip-address source-ip-mask* | **any** }	配置基本 IP ACL 的规则。
4	Inspur(config)#**router ospf** *process-id* [**router-id** *router-id*]	启动一个 OSPF 进程，并进入 OSPF 配置模式。
5	Inspur(config-router-ospf)#**distribute-list** { **ip-access-list** *acl-number* | **prefix-list** *list-name* } **out**	配置 OSPF 向自治系统内发布 5 类 LSA 的过滤策略。

步骤	配置	说明
6	Inspur(config-router-ospf)#**distribute-list** { **ip-access-list** *acl-number* | **prefix-list** *list-name* } **out** [**static** | **connected** | **bgp**]	配置 OSPF 协议发布策略。
	Inspur(config-router-ospf)#**distribute-list** { **ip-access-list** *acl-number* | **prefix-list** *list-name* } **out ospf** *process-id*	

说明

- 配置 OSPF 全局发布策略前，需要保证策略引用的 IP ACL 已经创建。
- 当且仅当 IP ACL 未被任何路由策略引用时，才允许修改 IP ACL。
- 与 IP ACL 不同，地址前缀列表被引用时也可以修改。
- 配置全局发布策略后，只有引入路由通过全局发布策略后，才能够被引入到本地 LSDB 中。配置协议发布策略后，还需要通过协议发布策略才能被引入。
- 配置协议发布策略后，引入的该协议路由只有通过协议发布策略才能够被引入到本地 LSDB 中。若同时配置了全局发布策略，还需要通过全局发布策略才能被引入。

配置 Type3 LSA 过滤策略

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ip prefix-list** *list-name* { **permit** | **deny** } *ip-address mask-length* [**ge** *ge-length*] [**le** *le-length*]	配置地址前缀列表。 可以使用 **no ip prefix-list** *list-name* 命令删除该配置。
3	Inspur(config)#**router ospf** *process-id* [**router-id** *router-id*]	启动一个 OSPF 进程，并进入 OSPF 配置模式。
4	Inspur(config-router-ospf)#**area** *area-id* **filter prefix-list** *list-name* { **in** | **out** }	配置区域中对 3 类 LSA 的过滤策略。

说明

若配置的过滤策略不存在，则认为该命令没有配置，不对接收的路由进行过滤。

5.9.11 配置 OSPF GR 功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router ospf** *process-id* [**router-id** *router-id*]	启动一个 OSPF 进程，并进入 OSPF 配置模式。
3	Inspur(config-router-ospf)#**capability opaque**	使能 OSPF 的 Opaque LSA 功能。 缺省情况下，禁用该功能。
4	Inspur(config-router-ospf)#**capability restart** { **graceful** | **signaling** }	配置 OSPF 的 GR 功能。
5	Inspur(config-router-ospf)#**ospf restart grace-period** *seconds*	（可选）配置 OSPF 的标准 GR 周期。 缺省情况下，OSPF 的标准 GR 周期为 120 秒。
6	Inspur(config-router-ospf)#**ospf restart helper** { **never** | **planned-only** } Inspur(config-router-ospf)#**ospf restart helper** [**planned-only**] **max-grace-period** *second*	（可选）配置 OSPF 的标准 GR 模式下启用 GR helper 的规则。
7	Inspur(config-router-ospf)#**exit** Inspur(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式。
8	Inspur(config-vlan*)#**ip ospf resync-timeout** *seconds*	（可选）配置 OSPF 的 GR 重启到重新同步之间的间隔。 缺省情况下，间隔与 OSPF 邻居失效时间相同。

5.9.12 配置 BFD for OSPF

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入接口配置模式，以下步骤以聚合组接口配置模式为例。
3	Inspur(config-port-channel*)#**ip ospf bfd**	使能接口的 BFD 功能。
4	Inspur(config-port-channel*)#**exit** Inspur(config)#**router ospf** *process-id* [**router-id** *router-id*]	启动一个 OSPF 进程，并进入 OSPF 配置模式。

步骤	配置	说明
5	Inspur(config-router-ospf)#**bfd all-interfaces**	使能全局 BFD 功能。

5.9.13 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show ip ospf** [*process-id*]	查看 OSPF 基本信息。
2	Inspur#**show ip ospf** [*process-id*] **interface** [*interface-type interface-number*]	查看 OSPF 接口信息。
3	Inspur#**show ip ospf** [*process-id*] **neighbor** [*interface-type interface-number*] [*neighbor-id*]	查看 OSPF 邻居信息。
4	Inspur#**show ip ospf** [*process-id*] **route**	查看 OSPF 路由信息。
5	Inspur#**show ip ospf** [*process-id*] **database** [**max-age** | **self-originate**]	查看 OSPF 链路状态数据库信息及统计信息。
	Inspur#**show ip ospf** [*process-id*] **database** [**router** | **network** | **summary** | **asbr-summary** | **external**] [*linkstate-id*] [**adv-router** *ip-address* | **self-originate**]	
	Inspur#**show ip ospf** [*process-id*] **database statistics**	
6	Inspur#**show ip ospf** [*process-id*] **border-routers**	查看区域边界路由器和 AS 边界路由器的信息。
7	Inspur#**show ip ospf** [*process-id*] **neighbor statistics**	查看 OSPF 统计信息或邻居统计信息。
8	Inspur#**show ip ospf** [*process-id*] **summary-address**	查看 OSPF ASBR 的外部路由汇聚信息。

5.9.14 维护

用户可以通过以下命令，维护设备 OSPF 特性的运行情况和配置情况。

命令	描述
Rasiecom#**clear ip ospf** [*process-id*] **process** [**graceful**]	重启 OSPF 进程。

5.10 OSPFv3

5.10.1 配置 OSPFv3 基本功能

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ipv6 router ospf** *process-id* [**router-id** *router-id*]	启动一个 OSPFv3 进程，并进入 OSPFv3 配置模式。 **说明** 设备最多支持 1 个 OSPFv3 进程，1 个进程可包含多个 OSPFv3 实例。
3	Inspur(config-ospf6)#**interface** *interface-type interface-number* **area** *area-id*	使能 OSPFv3 区域的接口。

5.10.2 配置 OSPFv3 实例

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入三层接口配置模式。
3	Inspur(config-tengigabitethernet1/1/*)#**ipv6 ospf6 instance-id** *instance-id*	配置 OSPFv3 区域接口所属的实例号。 缺省情况下，OSPFv3 区域接口所属的实例号为 0。

5.10.3 配置 OSPFv3 网络类型

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入三层接口配置模式。

步骤	配置	说明
3	Inspur(config-tengigabitethernet1/1/*)#**ipv6 ospf6 network** { **broadcast** | **ptp** }	配置 OSPFv3 区域接口网络类型。 缺省情况下，OSPFv3 区域接口的网络类型为广播网络。

5.10.4 配置 OSPFv3 接口

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入三层接口配置模式。
3	Inspur(config-tengigabitethernet1/1/*)#**ipv6 ospf6 mtu-ignore**	配置 OSPFv3 区域接口对报文进行检查时忽略 MTU 检查。 缺省情况下，OSPFv3 区域接口进行 MTU 的检查。
4	Inspur(config-tengigabitethernet1/1/*)#**ipv6 ospf6 passive**	配置接口为被动接口。 缺省情况下，接口为非被动接口。

5.10.5 配置 OSPFv3 报文定时器

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入三层接口配置模式。
3	Inspur(config-tengigabitethernet1/1/*)#**ipv6 ospf6 hello-interval** *seconds*	配置 OSPFv3 区域接口 Hello 报文发送间隔。 缺省情况下，OSPFv3 区域接口 Hello 报文发送间隔为 10s。
4	Inspur(config-tengigabitethernet1/1/*)#**ipv6 ospf6 dead-interval** *seconds*	配置 OSPFv3 区域接口的邻居失效时间。 缺省情况下，邻居失效时间为 4 倍 Hello 报文发送间隔；若未配置 Hello 报文发送间隔，则缺省为 40s。

步骤	配置	说明
5	Inspur(config-tengigabitethernet1/1/*)#**ipv6 ospf6 transmit-delay** *seconds*	配置 OSPFv3 区域接口上 LSA 的传输延迟时间。 缺省情况下，OSPFv3 区域接口上 LSA 的传输延迟时间为 1s。
6	Inspur(config-tengigabitethernet1/1/*)#**ipv6 ospf6 retransmit-interval** *seconds*	配置 OSPFv3 区域接口重传丢失的 LSA 报文的间隔。 缺省情况下，OSPFv3 区域接口重传丢失的 LSA 报文的间隔为 5s。

5.10.6 配置 OSPFv3 路由属性

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入三层接口配置模式。
3	Inspur(config-tengigabitethernet1/1/*)#**ipv6 ospf6 cost** *value*	配置 OSPFv3 区域接口路由开销。 缺省情况下，OSPFv3 接口的路由开销值=10^8（bit/s）/接口带宽（bit/s），如计算出的开销值大于 65535，取最大值 65535。
4	Inspur(config-tengigabitethernet1/1/*)#**ipv6 ospf6 priority** *value*	配置 OSPFv3 区域接口路由优先级。 缺省情况下，OSPFv3 区域接口的路由优先级均为 1。

5.10.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show ipv6 ospf**	查看 OSPFv3 基本信息。
2	Inspur#**show ipv6 ospf interface** [*interface-type interface-number*]	查看 OSPFv3 接口信息。
3	Inspur#**show ipv6 ospf neighbor**	查看 OSPFv3 邻居信息。
4	Inspur#**show ipv6 ospf route**	查看 OSPFv3 路由信息。
5	Inspur#**show ipv6 ospf database [detail]**	查看 OSPFv3 链路状态数据库信息。

5.11 ISIS

5.11.1 配置 ISIS 基本功能

ISIS 协议正常运行需要启动 ISIS 进程并配置网络实体名称两个步骤。

- 使用 router isis 命令启动 ISIS 进程；
- 在接口下使用 ip router isis 或者 ipv6 router isis 命令启动 ISIS 进程。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router isis** [*area-tag*]	启动一个 ISIS 进程，并进入 ISIS 配置模式。
3	Inspur(config)#**interface** *interface-type interface-number*	（可选）进入接口配置模式。
4	Inspur(config-tengigabitethernet1/1/*)#**ip router isis** [*area tag*] Inspur(config-tengigabitethernet1/1/*)#**ipv6 router isis** [*area tag*] Inspur(config-tengigabitethernet1/1/*)#**exit**	（可选）接口下启动一个 ISIS 进程。
	Inspur(config-tengigabitethernet1/1/*)#**exit**	
5	Inspur(config)#**router isis** [*area-tag*]	进入 ISIS 配置模式。
6	Inspur(config-router-isis)#**net** *network-entity*	配置 ISIS 路由进程的网络标识实体。

5.11.2 配置 ISIS 路由属性

配置路由器类型

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router isis** [*area-tag*]	启动一个 ISIS 进程，并进入 ISIS 配置模式。

步骤	配置	说明
3	Inspur(config-router-isis)#**is-type** { **level-1** | **level-1-2** | **level-2-only** }	配置 ISIS 路由器的类型。 缺省情况下，IS-IS 路由器的类型为 level-1-2。
4	Inspur(config-router-isis)#**hostname dynamic**	（可选）使能动态主机名交换机制功能。 缺省情况下，动态主机名交换机制功能未使能。

配置开销值

ISIS 开销值可以自动计算或手动配置。使能接口开销自动计算后，将按照以下规则自动计算接口开销。

- 开销值类型为 wide 时，ISIS 会根据该接口的带宽自动计算其开销值，公式：接口开销＝带宽参考值/接口带宽*10，计算出来的开销最大值为 16777214。
- 开销值类型为 narrow 时，
  - 接口带宽为 1Mbit/s～10Mbit/s 时，接口开销值为 60；
  - 接口带宽为 11Mbit/s～100Mbit/s 时，接口开销值为 50；
  - 接口带宽为 101Mbit/s～155Mbit/s 时，接口开销值为 40；
  - 接口带宽为 156Mbit/s～622Mbit/s 时，接口开销值为 30；
  - 接口带宽为 623Mbit/s～2500Mbit/s 时，接口开销值为 20；
  - 其它情况接口开销值为 10。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router isis** [*area-tag*]	启动一个 ISIS 进程，并进入 ISIS 配置模式。
3	Inspur(config-router-isis)#**metric-style** { **narrow** | **transition** | **wide** } Inspur(config-router-isis)#**exit**	配置 ISIS 开销值的类型。 缺省情况下，开销值类型为 narrow。
4	Inspur(config-router-isis)#**auto-metric** { **enable** | **disable** }	使能接口开销值自动计算功能。 缺省情况下，接口开销值自动计算功能未使能。
5	Inspur(config)#**interface** *interface-type interface-number*	进入接口配置模式。
6	Inspur(config-tengigabitethernet1/1/*)#**isis metric** *metric* [**level-1** | **level-2**]	配置接口的开销值。 缺省情况下，ISIS 接口的开销值为 10。

配置带宽参考值

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router isis** [*area-tag*]	启动一个 ISIS 进程，并进入 ISIS 配置模式。
3	Inspur(config-router-isis)#**reference-bandwidth** *bandwidth*	配置技术链路开销时所依据的带宽参考值。 缺省情况下，带宽参考值为 100Mbit/s。

配置 ISIS 管理距离

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router isis** [*area-tag*]	启动一个 ISIS 进程，并进入 ISIS 配置模式。
3	Inspur(config-router-isis)#**distance** *distance* [*ip-address mask-address*]	配置 ISIS 协议路由的管理距离。 缺省情况下，ISIS 协议路由的管理距离为 115。

5.11.3 配置 ISIS 网络

配置 ISIS 网络类型

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入接口配置模式。
3	Inspur(config-tengigabitethernet1/1/*)#**isis network point-to-point**	配置接口网络类型为 P2P。 缺省情况下，路由器接口网络类型是广播网。

配置邻接关系

该配置仅适用于 Level-1-2 路由器。

- 如本机是 Level-1-2 路由器，需要和对端路由器建立某区域（Level-1 或 Level-2）的关联关系，配置邻接关系建立区域可以限制本接口只发送和接收该区域的 Hello 报文。
- 在点到点链路上，接口只能发送和接收一种类型的 Hello 报文，配置邻接关系建立区域可以减少路由器处理时间，节省带宽。

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#interface` *interface-type interface-number*	进入接口配置模式。
3	`Inspur(config-tengigabitethernet1/1/*)#isis circuit-type { level-1 | level-1-2 | level-2-only }`	配置接口邻接关系的建立区域。 缺省情况下，接口可以建立 Level-1-2 的邻接关系。

配置 DIS 优先级

ISIS 的 DIS（Designated Intermedia System，被指定的中间系统）选举是抢占式、可预见的，ISIS 中不存在备份 DIS，当一个 DIS 不能工作时，直接选举另一个。DIS 选举规则如下：

- DIS 选举优先级最高的路由器会当选。如果所有路由器优先级相同，则 MAC 地址最高者当选。
- Level-1 和 Level-2 的 DIS 分别选举，选举结果可能不是同一个 IS。
- DIS 发送 Hello 包的间隔是普通路由器的 1/3，以保证如果 DIS 失效可以被快速检测到。

请在需要的设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#interface` *interface-type interface-number*	进入接口配置模式。
3	`Inspur(config-tengigabitethernet1/1/*)#isis priority` *priority* `[ level-1 | level-2 ]`	配置接口在不同区域的 DIS 优先级。 缺省情况下，接口的 DIS 优先级为 64。

5.11.4 优化 ISIS 网络

配置 ISIS 报文定时器

Hello 报文的失效数目设置的是 Holddown 时间（保持时间）。如果路由器在 Holddown 时间内没有收到对端路由器发送的 Hello 报文，就认为对端路由器已经失效。Holddown 时间基于接口配置，同一区域中的不同路由器可以设置不同的值。

改变 ISIS 的 Hello 报文发送间隔或改变 Hello 报文的失效数目，都可以达到调整 Holddown 时间的目的。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入接口配置模式。
3	Inspur(config-tengigabitethernet1/1/*)#**isis hello-interval** *seconds* [**level-1** | **level-2**]	配置接口不同区域的 Hello 报文发送间隔。 缺省情况下，Hello 报文发送间隔为 10 秒。
4	Inspur(config-tengigabitethernet1/1/*)#**isis hello-multiplier** *number* [**level-1** | **level-2**]	配置接口不同区域的 ISIS 邻居 Hello 报文失效数目。 缺省情况下，Hello 报文失效数目为 3。
5	Inspur(config-tengigabitethernet1/1/*)#**isis csnp-interval** *seconds* [**level-1** | **level-2**]	配置广播网上接口不同区域的 CSNP 报文发送间隔。 缺省情况下，CSNP 报文在广播网络中发送的时间间隔为 10 秒。

配置 LSP

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入接口配置模式。
3	Inspur(config-tengigabitethernet1/1/*)#**isis lsp-interval** *milliseconds*	配置接口发送 LSP 报文的时间间隔。 缺省情况下，发送 LSP 报文的间隔为 33 毫秒。

步骤	配置	说明
4	Inspur(config-tengigabitethernet1/1/*)#**isis retransmit-interval** *seconds* Inspur(config-tengigabitethernet1/1/*)#**exit**	配置点到点链路上 LSP 报文的重传间隔。 缺省情况下，LSP 报文的重传间隔为 5 秒。
5	Inspur(config)#**router isis** [*area-tag*] Inspur(config-router-isis)#**lsp-gen-interval** *seconds* [**level-1** | **level-2**]	配置 LSP 的生成间隔。 缺省情况下，LSP 生成间隔为 5 秒。
6	Inspur(config-router-isis)#**max-lsp-lifetime** *seconds* [**level-1** | **level-2**]	配置生成的 LSP 的最大生存时间。 缺省情况下，LSP 的最大生存时间为 1200 秒。
7	Inspur(config-router-isis)#**lsp-refresh-interval** *seconds* [**level-1** | **level-2**]	配置 LSP 的刷新间隔。 缺省情况下，LSP 刷新间隔为 900 秒。
8	Inspur(config-router-isis)#**ignore-lsp-errors**	使能忽略 LSP 的校验和检验错误功能。 缺省情况下，禁用忽略 LSP 的校验和检验错误功能，即丢弃校验和错误的 LSP。

配置 SPF 计算时间间隔

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router isis** [*area-tag*]	启动一个 ISIS 进程，并进入 ISIS 配置模式。
3	Inspur(config-router-isis)#**spf-interval** *seconds* [**level-1** | **level-2**]	配置 ISIS 中 SPF 计算间隔。 缺省情况下，ISIS 中 SPF 计算间隔为 10 秒。
4	Inspur(config-router-isis)#**set-overload-bit**	（可选）使能过载标志位功能。 缺省情况下，过载标识位功能未使能。

配置 ISIS 被动接口

若要使 ISIS 路由信息不被某一网络中的路由设备获得，可以通过配置接口为 ISIS 协议被动接口来禁止该接口发送 ISIS 报文。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入接口配置模式。
3	Inspur(config-tengigabitethernet1/1/*)#**isis passive**	使能 ISIS 协议接口被动功能。 缺省情况下，接口被动功能未使能。

配置 Hello 报文填充功能

Hello 报文填充功能是将 MTU 字段填充进 Hello 报文中，通告对端本端接口的 MTU 值。

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router isis** [*area-tag*]	启动一个 ISIS 进程，并进入 ISIS 配置模式。
3	Inspur(config-router-isis)#**hello padding**	使能 Hello 报文填充功能。 缺省情况下，所有类型接口填充标准 Hello 报文。

5.11.5 配置 ISIS 认证

配置 ISIS 区域认证

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router isis** [*area-tag*]	启动一个 ISIS 进程，并进入 ISIS 配置模式。
3	Inspur(config-router-isis)#**area-password** { **clear** *password* | **md5** *password* } [**authenticate snp** { **send-only** | **validate** }]	配置 Level-1 区域认证。
4	Inspur(config-router-isis)#**domain-password** { **clear** *password* | **md5** *password* } [**authenticate snp** { **send-only** | **validate** }]	配置 Level-2 区域认证。

配置 ISIS 接口认证

报文认证优先选择接口认证模式，如果接口认证方式为不认证，则选择区域认证模式。只有认证模式和密码相同，OSPF 接口才能建立邻居关系。

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入接口配置模式。
3	Inspur(config-tengigabitethernet1/1/*)#**isis password** { **clear** *password* | **md5** *password* } [**level-1** | **level-2**]	配置接口的 ISIS 认证模式和密码。

5.11.6 控制 ISIS 路由信息

配置 ISIS 引入路由

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router isis** [*area-tag*]	启动一个 ISIS 进程，并进入 ISIS 配置模式。
3	Inspur(config-router-isis)#**redistribute** { **connected** | **static** | **rip** | **ospf** *process-id* | **isis** *area-tag* | **bgp** } [**route-map** *map-name*] [**level-1** | **level-2** | **level-1-2**] [**metric** *metric*] [**metric-type** { **external** | **internal** }]	配置协议路由引入策略。 缺省情况下，ISIS 不引入其它协议路由，引入时如不指定区域，缺省引入到 Level-2。
4	Inspur(config-router-isis)#**redistribute isis ip level-2 into level-1**	配置 ISIS 各区域间的路由引入策略。 缺省情况下，Level-2 区域的路由信息不向 Level-1 区域发布。

配置引入缺省路由

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**router isis** [*area-tag*]	启动一个 ISIS 进程，并进入 ISIS 配置模式。
3	Inspur(config-router-isis)#**default-information originate**	配置引入 Level-2 级别的缺省路由。

配置 ISIS 路由聚合

路由汇聚不仅可以减小路由表规模，还可以减少本路由器生成的 LSP 报文大小和 LSDB 的规模。

- 被汇聚的路由可以是 ISIS 协议发现的路由，也可以是引入的外部路由。
- 聚合路由的开销值取所有被汇聚路由开销值的最小值。
- 路由器只对本地生成的 LSP 中的路由进行汇聚。

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router isis** [*area-tag*]	启动一个 ISIS 进程，并进入 ISIS 配置模式。
3	Inspur(config-router-isis)#**summary-address** *ip-address mask-address* [**level-1** | **level-2** | **level-2-only**]	配置区域间路由聚合。 缺省情况下，无聚合路由。配置聚合路由时开销缺省为明细 LSA 中最大的 Metric，且发布聚合路由。

配置 ISIS 等价多路径负载分担

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router isis** [*area-tag*]	启动一个 ISIS 进程，并进入 ISIS 配置模式。
3	Inspur(config-router-isis)#**maximum load-balancing** *number*	配置 ISIS 等价多路径负载分担的最大路径数。

5.11.7 配置 ISIS BFD

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router isis** [*area-tag*]	启动一个 ISIS 进程，并进入 ISIS 配置模式。
3	Inspur(config-router-isis)#**isis bfd enable**	使能全局 ISIS BFD 功能。 缺省情况下，禁用该功能。
4	Inspur(config-router-isis)#**bfd all-interfaces**	使能所有接口 ISIS BFD 功能。 缺省情况下，禁用该功能。

5.11.8 配置 ISIS GR

配置 ISIS 的平滑重启功能，重启时主备倒换不断业务。请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router isis** [*area-tag*]	启动一个 ISIS 进程，并进入 ISIS 配置模式。
3	Inspur(config-router-isis)#**graceful-restart**	使能 ISIS 的平滑重启功能。 缺省情况下，禁用该功能。
4	Inspur(config-router-isis)#**graceful-restart interval** *seconds*	配置 ISIS 平滑重启的时间间隔。 缺省情况下，ISIS 平滑重启的时间间隔为 300s。
5	Inspur(config-router-isis)#**graceful-restart sa enable**	使能 ISIS 的平滑重启抑制邻居设备发布功能。 缺省情况下，使能该功能。

5.11.9 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show isis interface** [**detail**]	查看 ISIS 的接口信息。
2	Inspur#**show isis neighbor** [*system-id* | **detail**]	查看 ISIS 的邻居信息。

序号	检查项	说明
3	Inspur#**show isis hostname**	查看主机名称与系统 ID 的映射关系表。
4	Inspur#**show isis route**	查看 ISIS 的 IPv4 路由信息。
5	Inspur#**show isis topology** [**level-1** | **level-2**]	查看 ISIS 的拓扑信息。
6	Inspur#**show isis database** [*lsp-id* | **detail**] [**level-1** | **level-2**][**local**]	查看 ISIS 的链路状态数据库。
7	Inspur#**show isis summary**	查看 ISIS 基本配置信息。

5.11.10 维护

用户可以通过以下命令，维护设备特性的运行情况和配置情况。

命令	描述
Rasiecom#**clear isis process** *area-tag* [**graceful-restart**]	清除 ISIS 信息。
Rasiecom#**clear isis neighbor** [*system-id*]	清除 ISIS 邻居信息。

5.12 BGP

5.12.1 配置 BGP 基本功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router bgp** *as-id*	使能 BGP 功能并创建 BGP 实例，进入 BGP 配置模式。
3	Inspur(config-router)#**bgp router-id** *router-id*	配置 BGP 协议的 Router ID。

5.12.2 配置 BGP 引入路由

配置对等体

由于 BGP 使用 TCP 连接，所以配置 BGP 时要指定对等体的 IP 地址。BGP 对等体不一定是相邻的路由器，利用逻辑链路也可以建立 BGP 对等体关系。为了增强 BGP 连接的稳定性，推荐使用 LOOPBACK 接口地址建立连接。

指定的对等体的 IP 地址可以有两种：

- 直连对等体的接口 IP 地址。
- 路由可达的对等体的 LOOPBACK 接口地址，这种方式需要再配置路由更新源，以保证对等体正确建立。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router bgp** *as-id*	进入 BGP 配置模式。
3	Inspur(config-router)#**neighbor** { *ip-address* | *ipv6-address* } **remote-as** *as-id*	创建 BGP 对等体，并指定对等体的 AS 号。 缺省情况下，无 BGP 对等体。
4	Inspur(config-router)#**neighbor** *ip-address1* **update-source** *ip-address2* Inspur(config-router)#**neighbor** *ip-address1* **update-source** *interface-type interface-number*	配置建立 BGP 连接时使用指定的本地源接口。 建立连接的两端中有一端配置正确的更新源，BGP 连接就可以成功建立，但可能出现连接建立时间过长的问题。为保证两端连接建立的稳定性，建议对等体两端同时配置更新源地址。
5	Inspur(config-router)#**neighbor** *ip-address* **weight** *weight*	配置从 BGP 对等体学到的路由的权重值。 缺省情况下，从 BGP 对等体学到的路由的权重值为 0。
6	Inspur(config-router)#**neighbor** *ip-address* **activate**	使能 BGP 对等体交换指定地址族路由的功能。 缺省情况下，使能与 BGP 对等体交换 IPv4 单播地址族路由信息，禁止交换其它地址族路由信息。
7	Inspur(config-router)#**neighbor** *ip-address* **default-originate**	使能向对等体发送默认路由功能。 缺省情况下，不向对等体发送默认路由。
8	Inspur(config-router)#**neighbor** *ip-address* **description** *string*	配置 BGP 对等体的描述信息。 缺省情况下，BGP 对等体无描述信息。

步骤	配置	说明
9	Inspur(config-router)#**neighbor** *ip-address* **next-hop-self**	配置路由器向对等体发布路由时修改路由下一跳地址为发送端自身 IP 地址。 缺省情况下，向 IBGP 对等体发布路由时，路由的下一跳 IP 地址与本地 BGP 路由表中路由的下一跳 IP 地址相同。
10	Inspur(config-router)#**bgp log-neighbor-changes**	使能提示 BGP 对等体状态变化的日志信息的功能。 缺省情况下，已使能提示 BGP 对等体状态变化的日志信息的功能。
11	Inspur(config-router)#**neighbor** *ip-address* **shutdown**	（可选）禁止与指定对等体建立 BGP 连接。 缺省情况下，允许与 BGP 对等体建立 BGP 连接。
12	Inspur(config-router)#**neighbor** *ip-address* **ebgp-multihop** [*ttl*]	（可选）配置允许非直连网络上的对等体建立 EBGP 连接，同时可指定 EBGP 连接允许的最大跳数。 缺省情况下，仅允许物理直连的对等体建立 EBGP 连接。
13	Inspur(config-router)#**bgp redistribute-internal**	配置将从 IBGP 对等体学习的路由信息重发布到 IGP 中。 缺省情况下，禁止重发布 IBGP 路由到 IGP 中。

配置 BGP 引入路由

BGP 协议自身不能发现路由，所以需要引入其他协议的路由（如 IGP 或静态路由等）注入到 BGP 路由表中，从而将这些路由在 AS 之内和 AS 之间传播。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router bgp** *as-id*	进入 BGP 配置模式。
3	Inspur(config-router)#**redistribute** { **connected** | **static** | **ospf** | **isis** } [**metric** *metric*] [**route-map** *map*]	配置 BGP 通过重发布方式引入其它协议的路由到 BGP 路由表中。

配置 BGP 引入静态路由

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router bgp** *as-id*	进入 BGP 配置模式。
3	Inspur(config-router)#**network** *ip-address* [*mask-address*] [**route-map** *route-map-name*]	配置向 BGP 路由表静态引入路由。

配置引入缺省路由

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router bgp** *as-id*	进入 BGP 配置模式。
3	Inspur(config-router)#**default-information originate**	配置 BGP 引入缺省路由。

5.12.3 配置 BGP 路由属性

配置 BGP 管理距离

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router bgp** *as-id*	进入 BGP 配置模式。
3	Inspur(config-router)#**distance bgp ebgp** *distance1* **ibgp** *distance2* **local** *distance3*	配置 BGP 路由的管理距离。 缺省情况下： • 外部路由（通过 EBGP 学到的路由）的管理距离为 20； • 内部路由（通过 IBGP 学到的路由）的管理距离是 200； • 本地路由（通过聚合命令引入 BGP 的路由）的管理距离是 200。

配置 BGP 路径选择策略

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router bgp** *as-id*	进入 BGP 配置模式。
3	Inspur(config-router)#**bgp deterministic-med**	（可选）配置 BGP 路由优选不考虑路由接收顺序。 缺省情况下，BGP 路由优选考虑路由接收顺序。
4	Inspur(config-router)#**bgp always-compare-med**	配置 BGP 对所有路径都比较 MED。
5	Inspur(config-router)#**bgp bestpath compare-routerid**	配置 BGP 最优路径选择策略为优选 Router-ID 小的路由。 缺省情况下，BGP 优选最早收到的 BGP 路由。
6	Inspur(config-router)#**bgp bestpath as-path ignore**	配置 BGP 选择最优路径时忽略 AS-PATH 属性。

配置 BGP 与 IGP 路由同步功能

使能 BGP 同步功能后：

- 通过 IBGP 学习的路由（下一跳可达）如果在 RM 中精确匹配到通过 IGP 协议学习的路由，且 IGP 路由的管理距离小于 BGP 路由的管理距离，则 BGP 路由可以参加优选，如果优选则下发 RM 至路由表；
- 通过 IBGP 学习的路由（下一跳可达）如果精确匹配到通过 IGP 协议学习的路由，但 IGP 路由的管理距离大于 BGP 路由的管理距离，则 BGP 路由状态会发生震荡，时而具有优选资格，时而不具有优选资格。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router bgp** *as-id*	进入 BGP 配置模式。
3	Inspur(config-router)#**synchronization**	使能 BGP 与 IGP 路由的同步功能。 缺省情况下，禁用 BGP 与 IGP 路由的同步功能。

配置路由抑制功能

路由不稳定的主要表现形式是路由震荡（Route Flapping），即路由表中的某条路由反复消失、重现。使用路由衰减（Route Dampening）可解决路由震荡问题。

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#router bgp` *as-id*	进入 BGP 配置模式。
3	`Inspur(config-router)#bgp dampening` *half-life reuse suppress max-suppress-time*	使能 BGP 路由抑制功能，或修改 BGP 路由抑制参数。 缺省情况下，未使能 BGP 路由抑制功能。 使能 BGP 路由抑制功能后，各参数的缺省值为：衰减半周期 15 分钟，解除抑制阈值 750，抑制阈值 2000，最大抑制时间 60 分钟。

5.12.4 配置 BGP 网络

配置路由反射器

路由反射器的前缀通告规则如下：

- Rule 1：RR 只通告或反射它所回到的最佳路径。
- Rule2：RR 总向 EBGP 对等体通告。
- Rule3：RR 客户在通告前缀的时候遵循常规的 IBGP 环路防止规则。
- Rule4：如果向 IBGP 对等体、客户，或者非客户通告，则需遵循规则 Rule 5 6 7。
- Rule5：如果 RR 从外部对等体学到前缀，就向它所有的客户和非客户通告。
- Rule6：如果前缀通过一个非客户 IBGP 对等体到达 RR，RR 向它所有的客户反射。
- Rule7：如果前缀通过客户到达 RR，RR 就向所有其他的客户和非客户反射这条路由。

说明

在某些网络中，路由反射器的客户机之间已经建立了全连接，可以直接交换路由信息，不需要路由反射，此时可使用 **no bgp client-to-client reflection** 命令禁用客户机之间的路由反射。

为增加网络的可靠性，防止单点故障，需要在一个集群中配置一个以上的路由反射器时，可以为同一集群内所有的路由反射器配置相同的集群 ID，以标识该集群，避免路由环路。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router bgp** *as-id*	进入 BGP 配置模式。
3	Inspur(config-router)#**neighbor** *ip-address* **route-reflector-client**	配置本机为路由反射器，并将指定的对等体作为路由反射器的客户。 缺省情况下，禁用路由反射器功能。
4	Inspur(config-router)#**bgp client-to-client reflection**	使能路由反射器客户机之间的路由反射。 缺省情况下，路由反射器客户机之间的路由反射使能。
5	Inspur(config-router)#**bgp cluster-id** *cluster-id*	配置路由反射器的集群 ID。 缺省情况下，路由反射器的集群 ID 为其 Router ID。

配置 BGP 缺省本地优先级

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router bgp** *as-id*	进入 BGP 配置模式。
3	Inspur(config-router)#**bgp default local-preference** *priority*	配置 BGP 缺省本地优先级。 缺省情况下，BGP 缺省本地优先级为 100。

配置 BGP 定时器

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router bgp** *as-id*	进入 BGP 配置模式。
3	Inspur(config-router)#**bgp scan-time** *time*	配置扫描 BGP 路由表的时间间隔。 缺省情况下，BGP 路由扫描间隔为 60 秒。

步骤	配置	说明
4	Inspur(config-router)#**timers bgp** *keep-alive-time hold-time*	配置全局 BGP 连接的存活时间和维持时间。 缺省情况下全局 BGP 连接的存活时间为 60 秒，维持时间为 180 秒。
5	Inspur(config-router)#**neighbor** *ip-address* **timers** *keep-alive-time hold-time*	配置对等体的存活时间和维持时间。 缺省情况下，对等体的存活时间和维持时间以 BGP 全局存活时间和维持时间为准。

配置 BGP 路由聚合

- 设备目前只支持 BGP 手动聚合，手动聚合对 BGP 本地路由表中已经存在的路由表项有效，如 BGP 路由表中没有掩码长度大于 16 的路由，即使使用命令 aggregate 10.1.1.1 255.255.0.0 对其进行聚合，BGP 也不会将这条聚合路由发布出去。
- 聚合路由不能配置为默认路由 0.0.0.0/0。

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router bgp** *as-id*	进入 BGP 配置模式。
3	Inspur(config-router)#**aggregate-address** *ip-address mask-address*	配置 BGP 路由聚合，且发布聚合路由和明细路由。
4	Inspur(config-router)#**aggregate-address** *ip-address mask-address* **summary-only**	配置 BGP 路由聚合，且只发布聚合路由，抑制明细路由。
5	Inspur(config-router)#**aggregate-address** *ip-address mask-address* **as-set**	配置 BGP 路由聚合，且设置 AS_SET 选项，生成的聚合路由包括 AS_PATH 中所有的 AS 号并将其作为一个 AS_SET，有效防止路由环路。

配置 BGP 路由过滤

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**ip as-path access-list** *access-list-number* { **permint** | **deny** } *regexp*	配置 AS 路径列表的过滤器。
3	Inspur(config)#**router bgp** [*as-id*]	进入 BGP 配置模式。
4	Inspur(config-router)#**neighbor** *ip-address* **filter-list** *access-list-number* { **in** | **out** }	配置基于 AS 路径列表的 BGP 路由过滤策略。
5	Inspur(config-router)#**neighbor** *ip-address* **route-map** *map-name* { **in** | **out** }	配置对指定对等体使用路由策略，过滤接收或发布的路由。
6	Inspur(config-router)#**distribute-list prefix** *list-name*{ **in** | **out** }	配置基于前缀列表过滤 BGP 路由信息。
7	Inspur(config-router)#**distribute-list prefix** *list-name* **out** [**connected** | **static** | **rip** | **ospf** | **isis**]	配置基于前缀列表过滤重发布到 BGP 路由表中的路由。
8	Inspur(config-router)#**neighbor** *ip-address* **prefix-list** *prefix-list-name* { **in** | **out** }	配置指定对等体基于 IP 前缀列表过滤接收或发布的路由。

5.12.5 配置 BGP GR

通过使能 BGP 协议的 GR（Graceful Restart，平滑重启）功能，避免协议重启带来的转发中断。请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router bgp** *as-id*	进入 BGP 配置模式。
3	Inspur(config-router)#**bgp graceful-restart all**	开启 BGP GR 功能。
4	Inspur(config-router)#**bgp graceful-restart restart-time** *seconds*	设置 GR 过程中邻居关系重建需要的时间上限，缺省值为 120 秒。
5	Inspur(config-router)#**bgp graceful-restart stalepath-time** *seconds*	设置 GR 过程中 Helper 保持 Stale 路由的时间上限，缺省值为 360 秒。

5.12.6 配置 BFD for BGP

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**router bgp** *as-id*	进入 BGP 配置模式。
3	Inspur(config-router)#**neighbor** *ip-address* **fall-over bfd**	开启使用 BFD 会话检测对等体 BGP 连接的功能。 缺省情况下，BFD 会话检测对等体 BGP 连接的功能为关闭。

5.12.7 配置 BGP 认证

配置 BGP 认证

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router bgp** *as-id*	进入 BGP 配置模式。
3	Inspur(config-router)#**neighbor** *ip-address* **password** *password*	使能 BGP 对等体建立 TCP 连接时以及对 BGP 消息进行 MD5 认证。 缺省情况下，禁用该功能。

5.12.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show ip bgp**	查看本地 BGP 路由表的内容。
2	Inspur#**show ip bgp** *ip-address* [*ip-mask*]	查看本地 BGP 路由表中指定网络的信息。
3	Inspur#**show ip bgp dampening dampened-paths**	查看被抑制的路由信息。
4	Inspur#**show ip bgp dampening parameters**	查看路由抑制参数。
5	Inspur#**show ip bgp dampening flap-statistics**	查看路由震荡统计信息。
6	Inspur#**show ip bgp summary**	查看 BGP 对等体的摘要信息。
7	Inspur#**show ip bgp neighbors** [*ip-address*]	查看 BGP 对等体的详细状态信息。
8	Inspur#**show ip bgp ipv6 unicast summary**	查看 IPv6 BGP 对等体的摘要信息。
9	Inspur#**show ip bgp ipv6 unicast neighbors**	查看 IPv6 BGP 对等体的状态信息。

5.12.9 维护

用户可以通过以下命令，维护设备特性的运行情况和配置情况。

命令	描述
Rasiecom#**clear ip bgp dampening** [*network-address* [*network-mask*]]	清除路由衰减信息。
Rasiecom#**clear ip bgp** { **all** | *ip-address* | **external** | **internal** } [**ipv4 unicast**]	重置公网所有或指定的 BGP 连接。
Rasiecom#**clear ip bgp** [**ipv4 unicast**]*as-id*	
Rasiecom#**clear ip bgp** { **all** | *ip-address* | **external** | **internal** } [**ipv4 unicast**] { **in** | **out** | **soft** }	更新公网所有或指定的 BGP 路由，不断开 BGP 连接，即软重置。
Rasiecom#**clear ip bgp** [**ipv4 unicast**] *as-id* { **in** | **out** | **soft** }	

5.13 RIP

5.13.1 配置 RIP 基本功能

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router rip**	启动 RIP 进程，并进入 RIP 配置模式。
3	Inspur(config-rip)#**network** *ip-address*	配置 RIP 直连生效的网络。
4	Inspur(config-rip)#**offset-list** *access-list-name* { **in** | **out** } *offset-value* [*interface-type interface-number*]	配置接口接收或者发送 RIP 路由时的附加度量值。 缺省情况下，接口接收或者发送 RIP 路由时的附加度量值均为 0。
5	Inspur(config-rip)#**passive-interface** { *interface-type interface-number* | **default** }	（可选）配置接口为被动接口。 缺省情况下，接口均为非被动接口。

5.13.2 配置 RIP 版本

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router rip**	启动 RIP 进程，并进入 RIP 配置模式。
3	Inspur(config-rip)#**version** *version-id*	配置全局 RIP 版本号。 缺省情况下，没有配置全局 RIP 版本，此时所有使能了 RIP 功能但没有配置发送方向 RIP 版本的接口发送 V1 报文，使能了 RIP 功能但没有配置接收方向 RIP 版本的接口可以接收所有版本报文。
4	Inspur(config-rip)#**exit** Inspur(config)#**interface** *interface-type interface-number*	进入接口配置模式。
5	Inspur(config-vlan*)#**ip rip receive version** { **1** | **2** }*	配置接口接收方向 RIP 版本。 缺省情况下，接口接收方向 RIP 版本以全局 RIP 版本的配置为准。
6	Inspur(config-vlan*)#**ip rip send version** { **1** | **2** } *	配置接口发送方向 RIP 版本。 缺省情况下，接口发送方向 RIP 版本以全局 RIP 版本的配置为准。
7	Inspur(config-vlan*)#**ip rip v2-broadcast**	在运行 RIPv2 接口上，配置接口发送的广播更新。 缺省情况下，运行 RIPv2 的接口发送组播更新。

说明

设备既支持配置全局 RIP 版本，也支持在接口上配置 RIP 版本。如果接口上配置了 RIP 版本，则以接口的配置为准。

5.13.3 配置引入外部路由

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router rip**	启动 RIP 进程，并进入 RIP 配置模式。
3	Inspur(config-rip)#**host-route**	使能接收主机路由的功能。 缺省情况下，已开启接收主机路由的功能。

步骤	配置	说明
4	Inspur(config-rip)#**default-information originate**	使能广播缺省路由功能。 缺省情况下，关闭广播缺省路由功能。
5	Inspur(config-rip)#**redistribute** { **static** | **connected** | **isis** | **bgp** | **ospf** *process-id* } [**metric** *metric-value*] [**route-map** *map-name*] [**tag** *tag-value*]	配置 RIP 路由引入策略。
6	Inspur(config-rip)#**default-metric** *metric*	配置引入外部路由的缺省度量值。 缺省情况下，引入外部路由的缺省度量值为 1。
7	Inspur(config-rip)#**auto-summary**	使能自动聚合功能（该功能仅 RIPv2 版本支持）。 缺省情况下，已使能路由自动聚合功能。
8	Inspur(config-rip)#**validate-update-source**	使能对收到的 RIP 报文的源 IP 地址进行检查的功能。 缺省情况下，已使能 RIP 报文的源 IP 地址检查功能。

5.13.4 配置定时器

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router rip**	启动 RIP 进程，并进入 RIP 配置模式。
3	Inspur(config-rip)#**timers basic** *update-time invalid-time holddown-time flush-time*	配置 RIP 定时器。 缺省情况下，更新时间间隔为 30s，失效时间间隔为 180s，抑制时间间隔为 120s，刷新时间间隔为 120s。

5.13.5 配置环路抑制

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入接口配置模式。

步骤	配置	说明
3	Inspur(config-vlan*)#**ip rip split-horizon**	使能接口水平分割功能，即从一个接口学习到的路由不会再广播回该接口。 缺省情况下，接口已使能水平分割功能。
4	Inspur(config-vlan*)#**ip rip poisoned-reverse**	使能接口毒性逆转功能，从一个接口学到的路由还可以从这个接口向外发布，但这些路由的度量值已设置为 16，即不可达。 缺省情况下，禁用毒性逆转功能。

说明

如果同时使能毒性逆转、水平分割功能，则水平分割功能无效。

5.13.6 配置认证

请在需要的设备上进行以下配置，仅 RIP V2 报文。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入接口配置模式。
3	Inspur(config-vlan*)#**ip rip authentication mode** { **text** | **md5** }	配置接口下报文的认证方式。 缺省情况下，接口下 RIPv2 报文认证方式为不认证。
4	Inspur(config-vlan*)#**ip rip authentication string** *password-string*	配置接口关联的密码字。
5	Inspur(config-vlan*)#**ip rip authentication key-chain** *key-chain-name*	配置接口关联的认证密钥链。

5.13.7 配置路由策略

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router rip**	启动 RIP 进程，并进入 RIP 配置模式。

步骤	配置	说明
3	Inspur(config-rip)#**distribute-list** { **ip-access-list** *acl-number* | **prefix-list** *list-name* | **route-map** *rmap-name* } **in** [*interface-type interface-number*]	配置 RIP 协议入方向路由策略。
4	Inspur(config-rip)#**distribute-list** { **ip-access-list** *acl-number* | **prefix-list** *list-name* | **route-map** *rmap-name* } **out** [*interface-type interface-number*]	配置 RIP 协议出方向路由策略。
5	Inspur(config-rip)#**distribute-list gateway** *list-name* **in** [*interface-type interface-number*]	配置 RIP 协议对接收报文的源地址实施路由策略。

5.13.8 配置路由计算

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router rip**	启动 RIP 进程，并进入 RIP 配置模式。
3	Inspur(config-rip)#**distance** *administrative-distance* [*ip-address wild-card-mask*]	配置 RIP 协议管理距离，即路由协议的优先级。管理距离值越小，优先级越高。 缺省情况下，RIP 管理距离为 120。
4	Inspur(config-rip)#**maximum load-balancing** *number*	配置 IP 等价多路径负载分担的最大路径数。

5.13.9 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show ip rip**	查看 RIP 基本信息。
2	Inspur#**show ip rip database**	查看 RIP 路由数据库信息。
3	Inspur#**show ip rip interface**	查看运行 RIP 协议的接口配置与状态信息。

5.13.10 维护

用户可以通过以下命令，维护设备特性的运行情况和配置情况。

命令	描述
Rasiecom#**clear rip database**	清除 RIP 路由数据库信息。
Rasiecom#**clear rip statistics**	清除 RIP 接口统计信息。

5.14 RIPng

5.14.1 简介

RIPng（RIP next generation，下一代 RIP）是一种单播路由协议，是对原来 IPv4 网络的 RIPv2 协议的扩展，使其可以应用于 IPv6 网络，RIP 的概念同样适用于 RIPng。RIPng 仍然属于 IGP (Interior Gateway Protocol，内部网关协议)，适用于规模较小的网络。

RIPng 对原有的 RIPv2 协议扩展修改，组播方式发送 RIPng 报文，使用 IPv6 组播地址 FF02::9，源地址 FE80::/10，UDP 的 521 端口（RIP 使用 520 端口）发送和接收路由信息。

5.14.2 配置 RIP 基本功能

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router ripng**	启动 RIPng 进程，并进入 RIPng 配置模式。
3	Inspur(config-ripng)#**network** *interface-type interface-number*	配置 RIPng 直连生效的网络。
4	Inspur(config-ripng)#**offset-list** *access-list-name* { **in** | **out** } *offset-value* [*interface-type interface-number*]	配置接口接收或者发送 RIPng 路由时的附加度量值。 缺省情况下，接口接收或者发送 RIPng 路由时的附加度量值均为 0。
5	Inspur(config-rip)#**passive-interface** *interface-type interface-number*	（可选）配置接口为被动接口。 缺省情况下，接口均为非被动接口。

5.14.3 配置引入外部路由

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router ripng**	启动 RIPng 进程，并进入 RIPng 配置模式。
3	Inspur(config-ripng)#**default-information originate**	使能广播缺省路由功能。 缺省情况下，关闭广播缺省路由功能。
4	Inspur(config-ripng)#**redistribute** { **static** | **connected** | **bgp** | **ospfv3** } [**metric** *metric*] [**route-map** *map-name*] [**tag** *tag-value*]	配置 RIPng 路由引入策略。
5	Inspur(config-ripng)#**default-metric** *metric*	配置引入外部路由的缺省度量值。 缺省情况下，引入外部路由的缺省度量值为 1。
6	Inspur(config-ripng)#**validate-update-source**	使能对收到的 RIPng 报文的源 IPv6 地址进行检查的功能。 缺省情况下，已使能 RIPng 报文的源 IPv6 地址检查功能。

5.14.4 配置定时器

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router ripng**	启动 RIPng 进程，并进入 RIPng 配置模式。
3	Inspur(config-ripng)#**timers basic** *update-time invalid-time holddown-time flush-time*	配置 RIPng 定时器。 缺省情况下，更新时间间隔为 30s，失效时间间隔为 180s，抑制时间间隔为 120s，刷新时间间隔为 120s。

5.14.5 配置环路抑制

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入接口配置模式。

步骤	配置	说明
3	Inspur(config-vlan*)#**ipv6 ripng split-horizon**	使能接口水平分割功能，即从一个接口学习到的路由不会再广播回该接口。 缺省情况下，接口已使能水平分割功能。
4	Inspur(config-vlan*)#**ipv6 ripng poisoned-reverse**	使能接口毒性逆转功能，从一个接口学到的路由还可以从这个接口向外发布，但这些路由的度量值已设置为 16，即不可达。 缺省情况下，禁用毒性逆转功能。

说明

如果同时使能毒性逆转、水平分割功能，则水平分割功能无效。

5.14.6 配置路由计算

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router ripng**	启动 RIPng 进程，并进入 RIP 配置模式。
3	Inspur(config-ripng)#**distance** *administrative-distance*	配置 RIPng 协议管理距离，即路由协议的优先级。管理距离值越小，优先级越高。 缺省情况下，RIPng 管理距离为 120。

5.14.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show ipv6 ripng protocol**	查看 RIPng 基本信息。
2	Inspur#**show ipv6 ripng database**	查看 RIPng 路由数据库信息。
3	Inspur#**show ipv6 ripng interface**	查看运行 RIPng 协议的接口配置与状态信息。

5.15 ND Snooping

5.15.1 简介

ND（Neighbor Discovery，邻居发现）是确定邻居节点之间关系的一组消息和进程。邻居发现协议替代了 IPv4 的 ARP（Address Resolution Protocol）、ICMP 路由器发现（Router Discovery）和 ICMP 重定向（Redirect）消息，并提供了地址冲突检测、邻居地址解析、确定邻居可达性以及进行主机地址配置等功能。

ND Snooping 功能主要应用于接入设备上，检查用户的合法性。对于合法用户的 ND 报文进行正常转发，否则直接丢弃，从而防止仿冒用户、仿冒网关的攻击。

用户合法性检查是根据 ND 报文中源 IPv6 地址和源 MAC 地址，检查用户是否是报文收到端口所属 VLAN 上的合法用户。

ND Snooping 功能将接入设备上的端口分为两种：ND 信任端口、ND 非信任端口。

- 对于 ND 信任端口，不进行用户合法性检查
- 对于 ND 非信任端口，如果收到消息，则认为是非法报文直接丢弃。

5.15.2 配置准备

场景

ND Snooping 用来防止网络中常见的 ND 欺骗攻击，实现了对不安全来源的 ND 报文进行隔离。是否对 ND 报文信任通过配置接口的信任状态实现，而是否符合要求则通过配置绑定表实现。

前提

无

5.15.3 ND Snooping 的缺省配置

设备上 ND Snooping 的缺省配置如下。

功能	缺省值
ND Snooping 接口信任状态	不信任

5.15.4 配置 ND Snooping

请在需要的设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#ipv6 nd snooping`	开启全局 ND Snooping 功能。

步骤	配置	说明
3	Inspur(config)#**vlan** *vlan-id*	(可选)配置 VLAN 下开启 ND Snooping 功能。
4	Inspur(config)#**interface** *interface-type interface-number*	(可选)进入物理层接口配置模式。
5	Inspur(config-gigaethernet1/1/*)#**ipv6 nd snooping**	(可选)配置连接网关的接口开启 ND Snooping 功能。
6	Inspur(config-gigaethernet1/1/*)#**ipv6 nd snooping trust**	配置连接网关的接口为信任接口。

5.15.5 配置 RA snooping

说明

RA（router advertisement，路由通告消息）能够携带很多网络配置信息，包括默认路由器，网络前缀列表，是否使用 DHCP 服务器进行有状态地址分配等网络配置的关键信息。如果受害者接收了虚假的 RA 信息，会造成网络配置错误，从而引发欺骗攻击。

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ipv6 ra snooping**	全局启动 RA Snooping 功能。
3	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
4	Inspur(config-gigaethernet1/1/*)#**ipv6 ra snooping trust**	设置端口为信任端口。

5.15.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show ipv6 nd snooping** [**interface** *interface-type interface-number*]	查看 ND Snooping 功能配置信息。
2	Inspur#**show ipv6 nd snooping binding** [**interface** *interface-type interface-number*]	查看所有或指定端口的静态绑定关系。

序号	检查项	说明
3	Inspur#**show ipv6 nd-snooping statistics** [**interface** *interface-type interface-number*]	查看 ND Snooping 用户报文统计信息。
4	Inspur#**show ipv6 ra snooping** [*interface-type interface-number*]	查看 RA Snooping 的相关配置信息。

5.15.7 维护

用户可以通过以下命令，维护设备 ND Snooping 功能的配置信息。

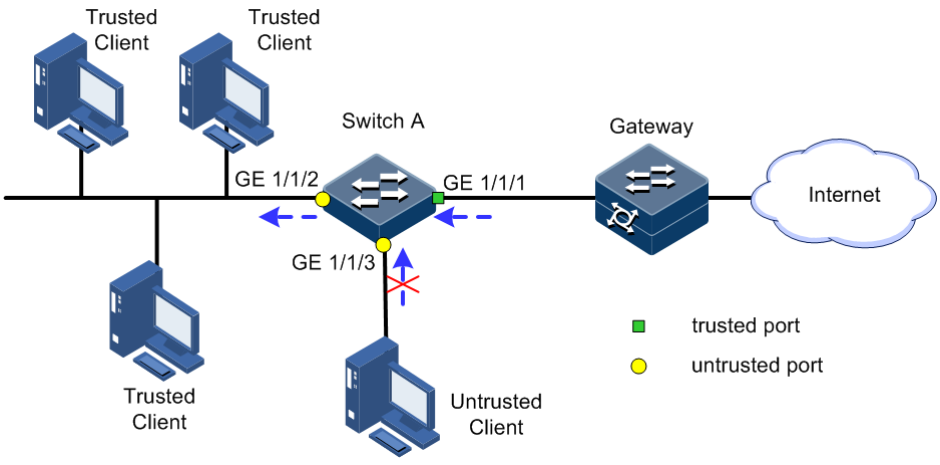
序号	检查项	说明
1	Inspur(config)#**clear ipv6 nd snooping statistics** [**interface** *interface-type interface-number*]	清除设备接收到的 ND Snooping 用户报文统计信息。
2	Inspur(config)#**clear ipv6 nd snooping ip-address** *ipv6-address* **vlan** *vlan-id*	删除指定 VLAN 下 ND Snooping 的动态学习的表项。

5.15.8 配置 ND Snooping 示例

组网需求

如图 5-8 所示，某局域网络用户主机通过 Switch A 连接网关设备，由于网络中未部署 DHCPv6 服务器，这些主机需要根据网关分配给用户网络前缀信息，通过无状态地自动配置方式获取 IPv6 地址。为防止非法用户发送 NA/NS/RS/RA 报文，导致合法主机无法获取 IPv6 地址，需要在 Switch 上开启 ND Snooping 功能，对非法的报文进行拦截。

图5-8 配置 ND Snooping 组网示意图



配置步骤

步骤 1 在 Switch 上创建 VLAN 10 并激活。

配置 Switch。

```
Inspur#name SwitchA
SwitchA#config
SwitchA(config)#create vlan 10 active
```

步骤 2 将 Switch A 的接口 GE1/1/2 以 Access 模式加入 VLAN 10，设置接口 GE 1/1/1 为 Trunk 模式并允许 VLAN 10 通过。

```
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#switchport mode access
SwitchA(config-gigaethernet1/1/2)#switchport access vlan 10
SwitchA(config-gigaethernet1/1/2)#exit
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport mode trunk
SwitchA(config-gigaethernet1/1/1)#switchport trunk allowed vlan 10
confirm
SwitchB(config-gigaethernet1/1/1)#exit
```

步骤 3 全局和 VLAN 10 分别使能 ND Snooping 功能，配置 GE 1/1/1 为信任接口。

```
SwitchA(config)#ipv6 nd snooping
SwitchA(config)#vlan 10
SwitchA(config-vlan10)#ipv6 nd snooping
SwitchA(config-vlan10)#exit
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#ipv6 nd snooping trust
SwitchA(config-gigaethernet1/1/1)#exit
```

步骤 4 配置 GE1/1/3 为非信任端口，使能 ND 协议报文合法性检查功能。

```
SwitchA(config)#interface gigaethernet 1/1/3
SwitchA(config-gigaethernet1/1/3)#ipv6 nd snooping
SwitchA(config-gigaethernet1/1/3)#ipv6 nd snooping check ns
SwitchA(config-gigaethernet1/1/3)#ipv6 nd snooping check na
SwitchA(config-gigaethernet1/1/3)#ipv6 nd snooping check rs
SwitchA(config-gigaethernet1/1/3)#exit
```

检查结果

通过 **show ipv6 nd snooping** 命令查看配置是否正确。

```
Inspur#show ipv6 nd snooping
Global ND Snooping: Enable
Vlan Port                          Trust   RRRAEnable  NSEnable NAEnable
RSEnable
------------------------------------------------------------------------
-----------
--
1    --                            --    Disable   Disable  Disable
Disable
```

```
10   gigaethernet1/1/1                              yes     Enable     Enable
Enable   Enable
```

通过 **show ipv6 nd snooping binding** 命令查看绑定表信息。

```
Inspur# show ipv6 nd snooping binding
History Max Entry Num: 4
Current Entry Num: 2
IP Address                          VLAN     MAC Address        Port      sec
Type    Inhw
------------------------------------------------------------------------------
-------------------------------------------
FE80::C49:FE9:1CFE:437F                10      484d.7eaa.1a15
gigaethernet1/1/2             1385  nd     yes
FE80::415A:E214:F155:6163              10      509a.4c13.2020
gigaethernet1/1/2             1455  nd     yes
```

6 PoE

说明

本章内容只有 PoE 机型支持，非 PoE 机型不支持。PoE 机型支持热重启过程中，POE 供电不间断；注意重启前需要保存当前配置，否则配置丢失后，PoE 相关配置参数会恢复到缺省状态，导致供电功能不满足实际需求。

本章介绍 PoE 的基本原理和配置过程，并提供相关的配置案例。

- 简介
- 配置 PoE
- 配置 Smart PoE
- 配置 PoE 交换机供电示例

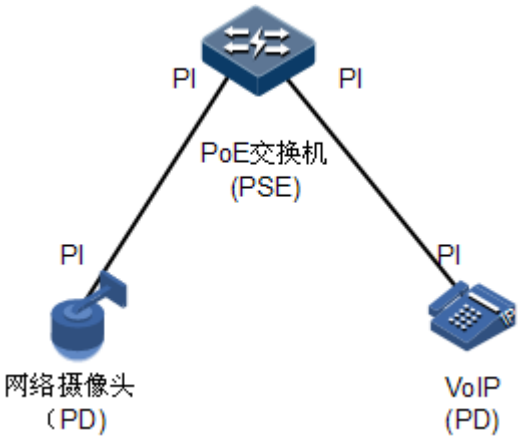
6.1 简介

6.1.1 PoE 原理

PoE（Power over Ethernet，以太网供电，又称远程供电）是指 PSE（Power Sourcing Equipment，供电设备）设备通过以太网电口，利用以太网线对网络远端下挂的 PD（Power Device，受电设备）进行远程供电，实现供电与数据传输并行的机制。

PoE 功能应用组网示意图如图 6-1 所示。

图6-1 PoE 功能应用示意图



6.1.2 PoE 的系统组成

PoE 的系统组成：

- PSE：由电源和 PSE 功能模块构成。可实现 PD 检测、PD 功率信息获取、远程供电、供电监控、设备断电等功能。
- PD：接受 PSE 供电的设备。分为标准 PD 和非标准 PD，标准 PD 是指符合 IEEE 802.3af 或者 IEEE 802.3at 标准的 PD 设备。常见的 PD 有 IP 电话、网络摄像头。
- PI（Power Interface，电源接口）：PSE/PD 与网线的接口，也就是 RJ45 接口。

6.1.3 PoE 供电的优点

PoE 供电的优点：

- 可靠：集中式电源供电，备份方便，电源统一管理，安全性高；
- 连接简捷：网络终端不需要外接电源，只需一根与 PoE 接口相连的网线供电；
- 标准：符合 IEEE 802.3at 标准，使用全球统一的电源接口；
- 应用前景广泛：可以用于 IP 电话、无线 AP（Access Point，接入点）、便携设备充电器、刷卡机、网络摄像头、数据采集系统。

6.1.4 PoE 相关概念

PoE 供电相关概念：

- 接口供电最大输出功率

配置接口供电最大功率后，配置值即为该接口为下挂的 PD 所能提供的最大输出功率。

- 接口供电优先级

接口供电优先级有三个等级 **critical**，**high**，**low**。优先对优先级为 **critical** 的接口下挂的 PD 供电，次之对优先级为 **high** 的接口下挂 PD 供电，最后对优先级 **low** 的接口下挂 PD 供电。

- 交换机过温保护功能

当设备当前温度高于高温阈值时产生高温告警，向网管发送 Trap 信息。

- 全局 Trap 功能

当设备出现过温情况，或当前 PSE 功率利用率超过阈值百分比，PoE 接口供电状态发生变化时，都会向网管发送 Trap 消息。

- PSE 供电功率使用阈值百分比

当 PSE 在当前功率利用率首次超过或低于设置的供电功率使用阈值时，系统会发送 Trap 告警信息。

6.1.5 Smart PoE

在普通 PoE 功能基础上，Smart PoE 提供了更加智能化的设备管理功能，支持如下特性：

- 支持 PD 设备 Active 检查探测，检测供电设备是否处于活动状态；
- 支持 PoE 调度，定期重启供电设备功能；
- 支持 PoE 调度，指定时间供电；
- 支持状态监控：PoE 功能状态、功率、电流、电压、Trap 上报等。

PD 设备 Active 检查探测通过连接跟踪实时监测 PD 是否还在活动，如果 PD 没有响应，会根据检测动作的配置，产生告警或者重启 PoE 供电接口。

PoE 调度可以控制每一个 PoE 接口在指定的时间间隔内进行供电，以帮助企业节省电力及资金；还可以控制每一个 PoE 接口在指定周期内进行重启，以降低 PD 设备损坏或者缓存溢出的可能。

PoE 调度模板是一组配置的集合，将 PoE 调度模板应用到多个 PoE 接口，则这些接口就具有相同的 PoE 特性；如果 PD 的接入接口变更，则把原接口上应用的 PoE 调度模板应用到新的接入接口即可，不再需要重新逐条配置，从而方便了网管人员对 PoE 特性的配置。

设备支持创建多个 PoE 调度模板，针对不同 PD 定义不同的 PoE 配置存放在不同的 PoE 调度模板中，并在 PD 的接入接口应用相应的 PoE 调度模板即可。用户可以通过配置 PoE 调度，为接口预设 PoE 功能的起始时间、重启时间等参数，使设备可以智能的进行 PoE 供电，控制何时需要关闭 PoE 供电接口。

6.2 配置 PoE

6.2.1 配置准备

场景

网络远端下挂的 PD 设备取电不方便，需要通过与之相连的以太网电口进行远程供电，实现供电和数据传输并行的机制。

前提

无

6.2.2 PoE 的缺省配置

设备上 PoE 的缺省配置如下。

功能	缺省值
供电接口 PoE 功能状态	使能
识别非标准 PD 功能	使能
供电接口供电的最大输出功率	30000mW
交换机供电管理模式	auto
交换机供电优先级	low
交换机过温保护功能状态	使能
交换机供电全局 Trap 开关状态	使能
交换机 PSE 供电功率使用阈值百分比	99%

6.2.3 使能接口 PoE 功能

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**poe enable**	使能接口 PoE 功能。

6.2.4 配置接口供电的最大输出功率

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**poe max-power** *max-power-value*	配置接口供电的最大输出功率。

6.2.5 配置接口供电优先级

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**poe priority** { **critical** | **high** | **low** }	配置接口供电优先级。

6.2.6 配置 PSE 供电功率使用阈值百分比

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**poe pse power-thredshold** *percent*	配置 PSE 供电功率使用阈值百分比。

6.2.7 使能识别非标准 PD 功能

说明

使用非标准 PD 时，建议先确认非标准 PD 的供电功率、电压和电流值等，以方便在 PSE 设备上设置合适的最大输出功率，以免 PSE 输出功率过大损坏 PD。

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**poe legacy enable**	使能设备对非标准 PD 识别功能。

6.2.8 使能接口强制供电功能

注意

在使用 PoE 交换机对远端 PD 进行供电时，建议使用标准 PD、预标准 PD 或思科私有标准 PD。若使用其他非标准 PD，需要采用交换机的强制供电功能，请务必先确认非标准 PD 的供电功率、电压和电流值等，以方便在 PSE 设备上设置合适的最大输出功率，以免 PSE 输出功率过大损坏 PD。

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**poe force-power**	使能接口强制 PoE 供电功能。

6.2.9 使能交换机过温保护功能

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**poe temperature-protection enable**	使能交换机过温保护功能。

6.2.10 使能全局 Trap 功能

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**poe pse trap enable**	使能全局 Trap 功能。

6.2.11 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show poe** *interface-type interface-number* [**detail**]	查看指定接口的供电状态。
2	Inspur#**show poe pse** [**detail**]	查看 PSE 的配置、实时运行信息。

6.3 配置 Smart PoE

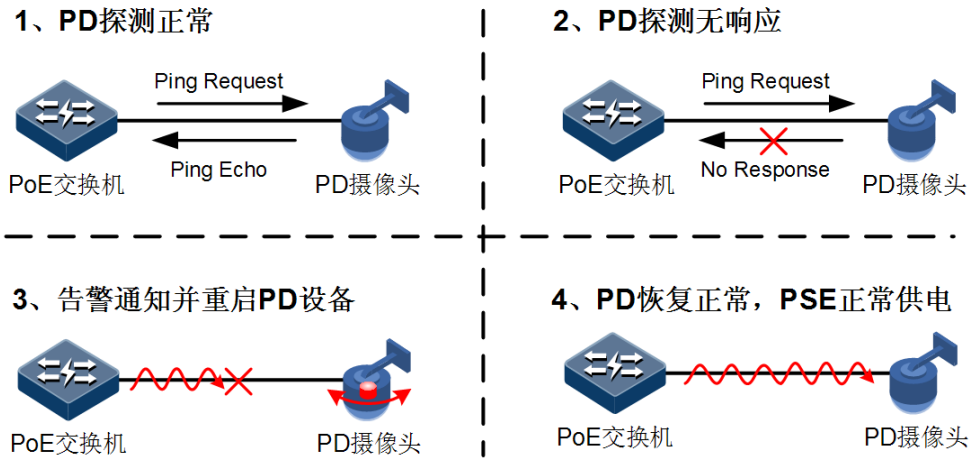
6.3.1 配置准备

场景

PD 设备 Active 检查探测通过连接跟踪实时监测 PD 是否还在活动，如果 PD 没有响应，会根据检测动作的配置，产生告警或者重启 PoE 供电接口。使用该界面可以配置 PoE 接口和 PD 连接跟踪，

如图 6-2 所示，配置 PD 连接检测功能 PoE 交换机设备，通过实时的 Ping 操作来监控连接的 PD 设备活动状态。一旦 PD 设备无响应并停止了活动，PoE 交换机设备将重启 PoE 接口，使 PD 设备重新恢复工作状态。通过 PD 连接检测可以提高 PoE 供电的可靠性并降低设备管理成本。

图6-2 PD 设备 Active 检查探测示意图



PoE 调度可以控制每一个 PoE 接口在指定的时间间隔内进行供电，以帮助企业节省电力及资金；还可以控制每一个 PoE 接口在指定周期内进行重启，以降低 PD 设备损坏或者缓存溢出的可能。

通过 PoE Profile（调度模板）配置，并将 PoE Profile 应用到指定的 PoE 接口。该方式通常用于批量配置 PoE 接口，可以简化用户的操作。

用户可以通过配置调度模板，为接口预设 PoE 功能的起始时间、重启时间等参数，使设备可以智能的进行 PoE 供电，控制何时需要关闭 PoE 供电接口。

前提

无

6.3.2 PoE 的缺省配置

设备上 PoE 的缺省配置如下。

功能	缺省值
使能 PD 检测功能	使能
PD 检测行为	无行为
重启时间间隔	无

6.3.3 配置接口预定义模板

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**poe schedule profile** *profile* Inspur(config-profile1)#**rule** *rule-id* { **reboot-time** | **start-time** | **end-time** } *week hour minute*	配置预定义模板规则。
3	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
4	Inspur(config-gigaethernet1/1/*)#**poe schedule profile** *profile*	配置端口预定义模板。

6.3.4 配置连接跟踪检测功能

连接跟踪主要用来检测目标主机是否可达，判断网络连接情况。

通过配置连接跟踪，以检测到达目的主机的链路是否可达，例如可以应用在 PoE 模块中对 PD 设备 Active 活动状态的检查探测。

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**linktrace track** *track-id*	配置连接跟踪 ID。
3	Inspur(config-linktrace)#**icmp** *ip-address* { *interface-type interface-number* | **source ip** *source-ip-address* }	配置连接跟踪目的 IP 地址并指定连接跟踪类型。
4	Inspur(config-linktrace)#**icmp interval** *period*	配置连接跟踪的发包间隔。
5	Inspur(config-linktrace)#**icmp retry count** *count*	配置连接跟踪的最大重试次数。

6.3.5 配置 PD 检测功能

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**poe alive check enable**	使能 PD 检测功能。
4	Inspur(config-gigaethernet1/1/*)#**poe alive action** { **reboot** | **reboot-alarm** | **alarm** }	配置 PD 检测行为。
5	Inspur(config-gigaethernet1/1/*)#**poe reboot interval** *period*	配置重启时间间隔。
6	Inspur(config-gigaethernet1/1/*)#**poe linktrace track** *track-id*	配置 PoE 接口绑定指定的连接跟踪 ID。

说明

当需要配置 PD 设备 Active 跟踪检测时，需要先创建相应 PD 设备 IP 的连接跟踪，然后再与指定的 PoE 接口进行连接跟踪 ID 绑定。

6.3.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show poe profile** { **all** | *profile* }	查看预定义模板的规则。
2	Inspur#**show poe interface** *interface-type interface-number* [**detail**]	查看指定接口的供电状态。

序号	检查项	说明
3	Inspur#show link-trace	查看连接跟踪检测配置信息。

6.4 配置 PoE 交换机供电示例

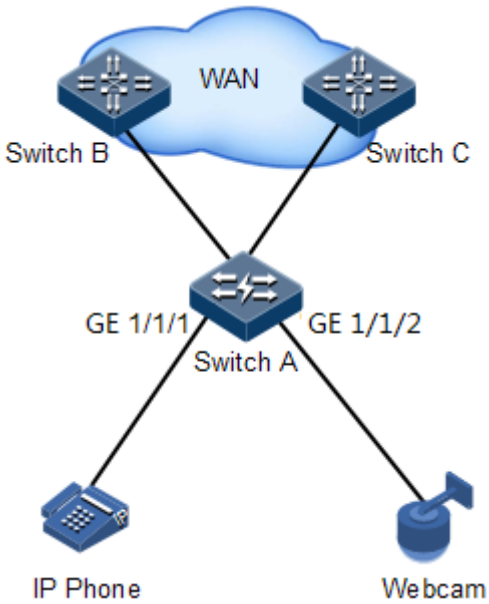
组网需求

如图 6-3 所示，Switch B 和 Switch C 为 Switch A 在上层网络所连接的设备。使用 PoE 交换机 Switch A 为 IP 电话和网络摄像头供电，要求在交换机设备满负荷的情况下，要优先对摄像头供电。

根据用户需求对设备参数设置如下：

- 接口 1、接口 2 的最大输出功率均为 30000mW；
- 使能交换机供电过温保护功能；
- 使能交换机供电 Trap 功能；
- 接口 2 的优先级为 high，接口 1 的优先级为 low。

图6-3 PoE 交换机供电组网示意图



配置步骤

步骤 1 使能接口 GE1/1/1 和接口 GE1/1/2 的 PoE 功能。

```
Inspur#config
Inspur(config)#interface gigaethernet1/1/1
```

```
Inspur(config-gigaethernet1/1/1)#poe enable
Inspur(config-gigaethernet1/1/1)#exit
Inspur(config)#interface gigaethernet1/1/2
Inspur(config-gigaethernet1/1/2)#poe enable
Inspur(config-gigaethernet1/1/2)#exit
```

步骤 2 配置接口 1 和接口 2 的 PoE 供电最大功率 30000mW。

```
Inspur(config)#interface gigaethernet1/1/1
Inspur(config-gigaethernet1/1/1)#poe max-power 30000
Inspur(config-gigaethernet1/1/1)#exit
Inspur(config)#interface gigaethernet1/1/2
Inspur(config-gigaethernet1/1/2)#poe max-power 30000
Inspur(config-gigaethernet1/1/2)#exit
```

步骤 3 使能供电过温保护功能。

```
Inspur(config)#poe temperature-protection enable
```

步骤 4 使能全局 Trap 功能。

```
Inspur(config)#poe pse trap enable
```

步骤 5 配置接口 GE1/1/2 的优先级为 **high**，接口 GE1/1/1 的优先级为 **low**。

```
Inspur(config)#interface gigaethernet1/1/2
Inspur(config-gigaethernet1/1/2)#poe priority high
Inspur(config-gigaethernet1/1/2)#exit
Inspur(config)#interface gigaethernet1/1/1
Inspur(config-gigaethernet1/1/1)#poe priority low
```

检查结果

通过 **show poe gigaethernet 1/1/1 detail**、**show poe gigaethernet 1/1/2 detail** 命令查看接口 1，2 的 PoE 功能配置情况。

```
Inspur#show poe gigaethernet 1/1/1 detail
Port: gigaethernet 1/1/1
POE administrator status: Enable
POE operation status: Enable
Power detection status:Searching
POE Power Pairs mode:Signal
PD power classification:Class0
POE power Priority:Low
POE power max:30000 (mW)
POE power output:0 (mW)
POE power average:0 (mW)
POE power peak:0 (mW)
POE current output:0 (mA)
POE voltage output:0 (V)

Inspur#show poe gigaethernet 1/1/2 detail
Port: gigaethernet 1/1/1
POE administrator status: Enable
POE operation status: Enable
Power detection status:Searching
POE Power Pairs mode:Signal
```

```
PD power classification:Class0
POE power Priority:High
POE power max:30000 (mW)
POE power output:0 (mW)
POE power average:0 (mW)
POE power peak:0 (mW)
POE current output:0 (mA)
POE voltage output:0 (mV)
```

7 DHCP

本章介绍 DHCP 的基本原理和配置过程，并提供相关的配置案例。

- DHCP Client
- 零配置
- DHCP Snooping
- DHCP Option
- DHCP Server
- DHCP Relay

7.1 DHCP Client

7.1.1 简介

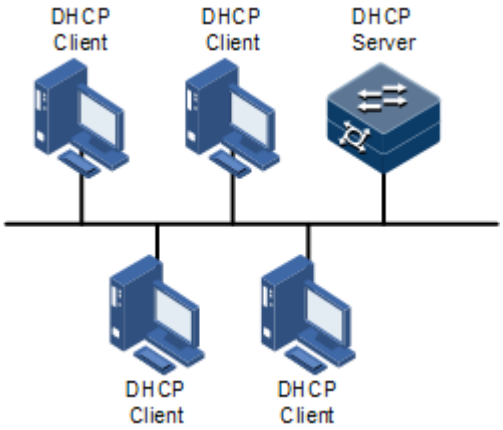
DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）在 TCP/IP 网络上给用户动态分配 IP 地址等配置信息的协议。它是基于 BOOTP（Bootstrap Protocol）协议，并在 BOOTP 协议的基础上添加了自动分配可用网络地址、网络地址重复使用以及其他扩展配置选项等功能。

随着网络规模的不断扩大和网络复杂度的提高，计算机的数量经常超过可供分配的 IP 地址数量。同时随着便携机及无线网络的广泛使用，计算机的位置也经常变化，相应的 IP 地址也必须经常更新，从而导致网络配置越来越复杂。DHCP 就是为解决这些问题而发展起来的。

DHCP 采用客户端/服务器通信模式，由客户端向服务器提出配置申请（包括 IP 地址、子网掩码、缺省网关等参数），服务器返回为客户端分配的 IP 地址等相应的配置信息，以实现 IP 地址等信息的动态配置。

在 DHCP 的典型应用中，一般包含一台 DHCP 服务器和多台客户端（如 PC 和便携机），如图 7-1 所示。

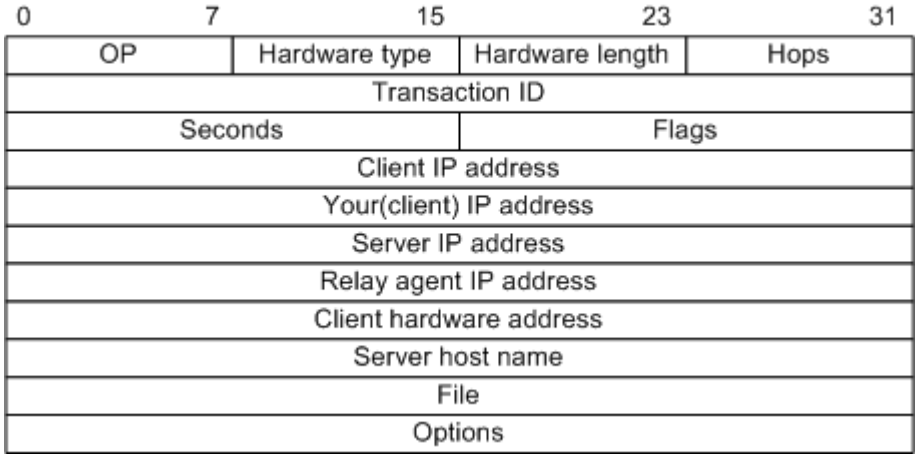
图7-1 DHCP 典型应用组网示意图



DHCP 技术保证了 IP 地址的合理分配问题，从而避免了 IP 地址的浪费，提高了整网的 IP 地址使用率。

DHCP 报文格式如图 7-2 所示。DHCP 报文被封装在 UDP 数据报中。

图7-2 DHCP 报文结构示意图



DHCP 报文中的各个字段含义如表 7-1 所示。

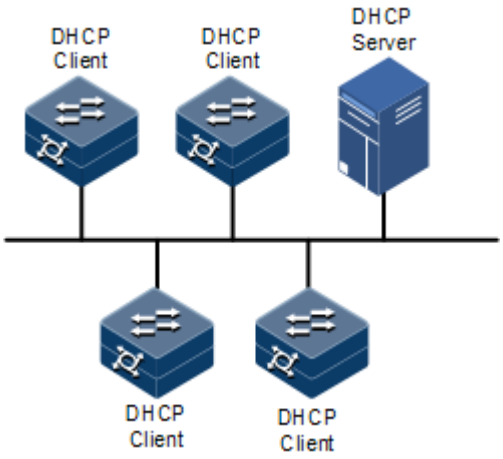
表7-1 DHCP 报文字段含义列表

字段名	字段长度（Byte）	描述
OP	1	报文类型。 • 取值为 1 时，表示该报文为客户端请求报文； • 取值为 2 时，表示该报文为服务器端回应报文。
Hardware type	1	DHCP 客户端的硬件地址类型。

字段名	字段长度（Byte）	描述
Hardware length	1	DHCP 客户端的硬件地址长度。
Hops	1	DHCP 报文经过的 DHCP 中继的数目。 DHCP 请求报文每经过一个 DHCP 中继，该字段就会加 1。
Transaction ID	4	客户端发起一次请求时选择的随机数，用来标识一次地址请求过程。
Seconds	2	DHCP 客户端开始 DHCP 请求后所经过的时间。目前没有使用，固定为 0。
Flags	2	第 1 个比特为广播回应标识位，用来标识 DHCP 服务器回应报文是采用单播还是广播方式发送。 • 0 表示采用单播方式； • 1 表示采用广播方式。 其它比特保留不用。
Client IP address	4	DHCP 客户端的 IP 地址，只有当客户端在绑定，更新或重新绑定状态时进行填充，且可以用于回应 ARP 请求。
Your(client) IP address	4	DHCP 服务器分配给客户端的 IP 地址。
Server IP address	4	DHCP 服务器的 IP 地址。
Relay agent IP address	4	DHCP 客户端发出请求报文后经过的第一个 DHCP 中继的 IP 地址。
Client hardware address	16	DHCP 客户端的硬件地址。
Server host name	64	DHCP 服务器的名称。
File	128	DHCP 服务器为 DHCP 客户端指定的启动配置文件名称及路径信息。
Options	可变	可选变长选项字段，包含报文的类型、有效租期、DNS（Domain Name System，域名系统）服务器的 IP 地址、WINS（Windows Internet Name Server ，Windows 网际命名服务）服务器的 IP 地址等配置信息。

设备支持作为 DHCP 客户端，从 DHCP 服务器获取 IP 地址，以便后续对该设备进行管理，如图 7-3 所示。

图7-3 DHCP 客户端组网示意图



7.1.2 配置准备

场景

设备作为 DHCP 客户端时，从指定的 DHCP 服务器获取 IP 地址，可以用于后续对该设备的管理。

当采用动态地址分配方式时，DHCP 客户端所分配到的 IP 地址有一定的租借期限。租借期满后，DHCP 服务器会收回该 IP 地址。如果 DHCP 客户端希望继续使用该地址，需要续租 IP 地址。如果租借期未满，DHCP 客户端不需要继续使用该地址，可以释放 IP 地址。

若 DHCP 客户端需要通过多台 DHCP 中继向 DHCP 服务器获取 IP 地址，建议 DHCP 中继的台数不超过 4 台。

前提

在配置 DHCP 客户端之前，需完成以下任务：

- 创建 VLAN 并将三层接口加入 VLAN；
- 设备未启动 DHCP Snooping 功能。
- SNMP 接口支持通过 DHCP 方式、零配置方式获取 IP 地址。

7.1.3 DHCP 客户端的缺省配置

设备上 DHCP 客户端的缺省配置如下。

功能	缺省值
hostname	Inspur
class-id	Inspur-ROS
client-id	Inspur-SYSMAC-IF0

7.1.4 配置 DHCP 客户端

DHCP 客户端申请 IP 地址，需先创建 VLAN，并且把 IP 接口所在接口加入 VLAN，同时配置好 DHCP 服务器，否则接口通过 DHCP 获取 IP 地址会失败。

对于接口 IP 0，通过 DHCP 获取的 IP 地址与手动配置的 IP 地址之间允许相互覆盖。

说明

- 设备缺省情况下使能 DHCP 客户端功能，执行 **no ip address dhcp** 命令关闭 DHCP 客户端。
- 若设备之前曾通过 DHCP 方式从某一 DHCP 服务器获取了 IP 地址，用户通过 **ip address dhcp** 命令修改了 DHCP 服务器的地址后，设备将会重新启动 IP 地址的申请流程。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface vlan** *vlan-id*	进入三层接口配置模式。
3	Inspur(config-vlan*)#**ip dhcp client** { **class-id** *class-id* | **client-id** *client-id* | **hostname** *hostname* }	（可选）配置 DHCP 客户端信息，可以配置的信息有类型标识符、客户端标识符和主机名称。 **注意** DHCP 客户端获取到 IP 地址后，不允许修改客户端信息。
4	Inspur(config-vlan*)#**ip address dhcp** [**server-ip** *ip-address*]	配置通过 DHCP 方式申请 IP 地址。
5	Inspur(config-vlan*)#**ip dhcp client renew**	（可选）续租 IP 地址。 若此前设备的三层接口通过 DHCP 方式获取了 IP 地址，在 IP 地址租约到期时将会自动续租。
6	Inspur(config-vlan*)#**no ip address dhcp**	（可选）释放 IP 地址。

7.1.5 配置 DHCPv6 Client

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式。
3	Inspur(config-vlan*)#**ipv6 address dhcp** [**server-ip** *ipv6-address*]	配置通过 DHCPv6 方式申请 IPv6 地址。 若设备之前曾通过 DHCP 方式从某一 DHCP 服务器获取了 IP 地址，用户通过该配置修改了 DHCP 服务器的地址后，设备将会重新启动 IP 地址的申请流程。
4	Inspur(config-vlan*)#**ipv6 dhcp client renew**	（可选）续租 IP 地址。 若此前设备的 IP 接口通过 DHCP 方式获取了 IP 地址，在 IP 地址租约到期时将会自动续租。
5	Inspur(config-vlan*)#**ipv6 dhcp client rapid-commit**	（可选）使能 DHCPv6 Client 申请快速交互方式。

7.1.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

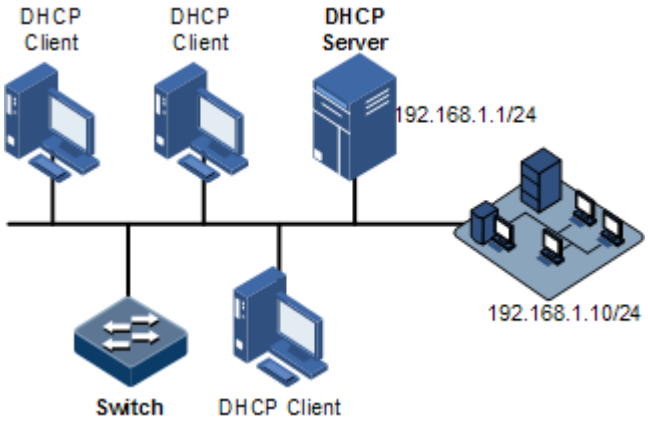
序号	检查项	说明
1	Inspur#**show ip dhcp client** [*interface-type interface-number* | **vlan** *vlan-id*]	查看 DHCP 客户端配置信息。
2	Inspur#**show ipv6 dhcp client** [**interface** { *interface-type interface-number* | **vlan** *vlan-id* }]	查看 DHCPv6 Client 的配置信息。

7.1.7 配置 DHCP 客户端示例

组网需求

如图 7-4 所示，Switch 作为 DHCP 客户端，主机名为 Inspur，接入 DHCP 服务器和网管平台。需要由 DHCP 服务器分配 IP 地址给 Switch，从而使网管平台能够管理 Switch。

图7-4 配置 DHCP 客户端组网示意图



配置步骤

步骤 1 配置 DHCP 客户端信息。

```
Inspur#config
Inspur(config)#interface vlan 1
Inspur(config-vlan1)#ip dhcp client hostname Inspur
```

步骤 2 配置通过 DHCP 方式申请 IP 地址。

```
Inspur(config-vlan1)#ip address dhcp server-ip 192.168.1.1
```

检查结果

通过 **show ip dhcp client** 命令查看 DHCP 客户端配置是否正确。

```
Inspur#show ip dhcp client
DHCP Client Mode:              Normal Mode
  Interface :                   vlan1
  Hostname:                    Inspur
  Class-ID:                    Inspur-ROS_5.2.1
  Client-ID:                   Inspur-000e5e112233-IF0
  DHCP Client Is Requesting For A Lease.
  Assigned IP Addr:             0.0.0.0
  Subnet Mask:                 0.0.0.0
  Default Gateway:              --
  Client Lease Starts:          Jan-01-1970 08:00:00
  Client Lease Ends:           Jan-01-1970 08:00:00
  Client Lease Duration:        0(sec)
  DHCP Server:                 0.0.0.0
  TFTP Server Name:             --
  TFTP Server IP Addr:          --
  Bootfile Filename:           --
  NTP Server IP Addr:           --
  Root Path:                   --

  DHCP Client Mode:             Normal Mode
  Interface :                  vlan10
```

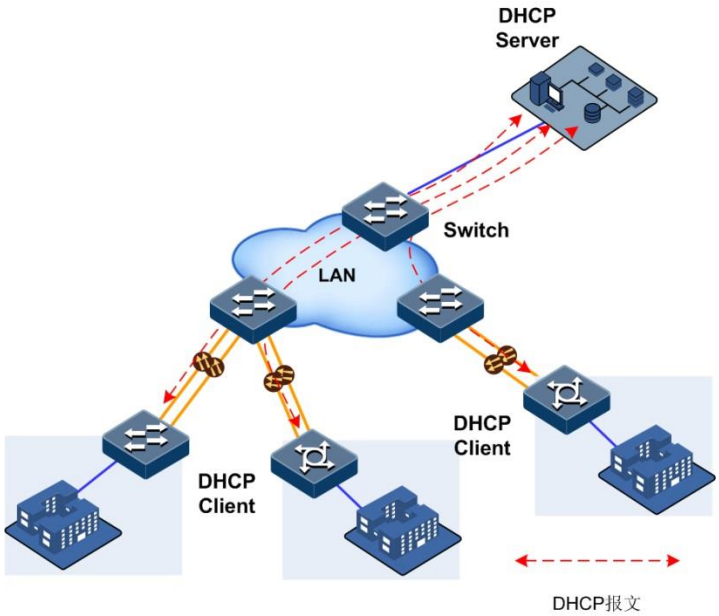
```
Hostname:                    Inspur
Class-ID:                    Inspur-ROS_5.2.1
Client-ID:                   Inspur-000e5e112233-IF0
DHCP Client Is Disabled.
Assigned IP Addr:             0.0.0.0
Subnet Mask:                 0.0.0.0
Default Gateway:              --
Client Lease Starts:          Jan-01-1970 08:00:00
Client Lease Ends:            Jan-01-1970 08:00:00
Client Lease Duration:        0(sec)
DHCP Server:                 0.0.0.0
TFTP Server Name:             --
TFTP Server IP Addr:          --
Bootfile Filename:            --
NTP Server IP Addr:           --
Root Path:                   --
```

7.2 零配置

7.2.1 简介

零配置功能是指设备无需进行任何手动配置，加电后，向零配置服务器自动发送申请 IP 地址的 DHCP 报文；当设备从零配置服务器获取 IP 后，自动下载服务器中的配置文件，自动更新自身配置。设备通过零配置服务器实现远端零配置的组网如图 7-5 所示。

图7-5 零配置服务器组网示意图



注意

缺省情况下，设备零配置模式打开。当用户不需要使用零配置功能时，建议切换为普通客户端模式，即关闭零配置功能。

7.2.2 零配置缺省配置

设备缺省配置如下。

功能	缺省值
零配置远端轮询周期	2 小时
零配置模式	使能

7.2.3 配置准备

场景

远端设备加电即可自动申请 IP 地址，无需手工配置。当用户需要更改零配置功能参数时，可根据本节内容进行配置。

前提

- 设备与 DHCP 服务器连接正确，且 DHCP 服务器已经正确配置。
- 连接零配置服务器的物理层接口状态为 UP。
- 上联交换机需要允许零配置远端设备中的某一 VLAN 通过。
- SNMP 接口支持通过 DHCP 方式、零配置方式获取 IP 地址。

7.2.4 配置 DHCP 客户端功能

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#ip dhcp client mode { zeroconfig | normal }` `Inspur(config)#ipv6 dhcp client mode { zeroconfig | normal }`	配置 DHCP 客户端工作模式为零配置模式或普通客户端模式。 缺省情况下，DHCP 客户端为零配置模式。 **注意** 当用户不需要使用零配置功能时，可通过命令切换为普通客户端模式。

7.2.5（可选）配置零配置轮询功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ip dhcp client zeroconfig polling period** *hour* Inspur(config)#**ipv6 dhcp client zeroconfig polling period** *hour*	配置零配置轮询周期时间，单位是小时，轮询周期可配置时间范围是 1～24。 缺省情况下，零配置远端轮询周期时间为 2 小时。

7.2.6 检查配置

设备获取到 IP 地址后，可通过以下命令检查结果。

步骤	检查项	说明
1	Inspur#**show ipv6 dhcp client** Inspur#**show ip dhcp client**	查看 DHCP 客户端配置信息和自动获取的信息。

7.2.7 IPv6 零配置应用举例

组网需求

如图 7-6 所示，DHCP Server 软件安装在虚拟机中，与 TFTP Server 所在 PC 的网卡桥接。Switch A 分别通过 GE 1/1/2 端口上联 TFTP Server、GE 1/1/1 端口下联 Switch B 的 GE1/1/1。Switch B 设备在空配置启动，没有 IPv6 地址时能通过零配置功能，从 DHCP Server 获取 IPv6 全球单播地址，获取地址后，自动从同一网段的 TFTP Server 下载配置文件、系统文件并加载。具体数据规划如表 7-2 所示。

图7-6 零配置应用示意图

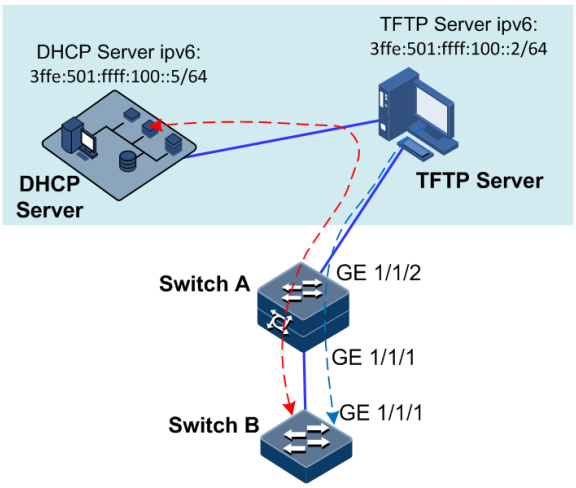


表7-2 数据规划

设备	参数
DHCP Server	• IPv6 address：3ffe:501:ffff:100::5/64 • IPv4 address：172.16.125.201/24 • DHCPv6 Server Pool: • 3ffe:501:ffff:100::5/64～3ffe:501:ffff:100::102
TFTP Server	• IPv6 address：3ffe:501:ffff:100::2/64 • IPv4 address：172.16.125.135/24
Switch A	端口配置： • GE1/1/2 端口模式：Access，接入 VLAN 10 • GE1/1/1 端口模式：Trunk，允许通过 VLAN10
Switch B	空配置

配置思路

- 搭建 DHCPv6 Server，配置 DHCPv6 地址池，定义 Option59、Option60 字段。
- 搭建 TFTP Server 环境，并存储需要下发给 SwicthB 的配置文件和系统文件。
- 配置 Switch A，与 TFTP Server 可以互通。

配置步骤

搭建 DHCPv6 Server，配置 DHCPv6 地址池，定义 Option59、Option60 字段。

步骤 1 安装虚拟机软件，具体请参考实际使用的虚拟机软件操作手册。

步骤 2 设置虚拟机所在 PC 的 IPv4 地址 172.16.125.135/24、IPv6 地址 3ffe:501:ffff:100::2。

步骤 3 将 DHCPv6 Server 系统安装到虚拟机中，安装步骤参考实际使用的系统软件操作手册。

步骤 4 设置该 DHCPv6 Server 系统的 IPv4 地址和 IPv6 地址。

- 设置 DHCPv6 Server 的 IPv4 地址 172.16.125.201/24、IPv6 地址 3ffe:501:ffff:100::5/64。
- 设置虚拟机的网卡与所在 PC 的网卡为桥接模式。

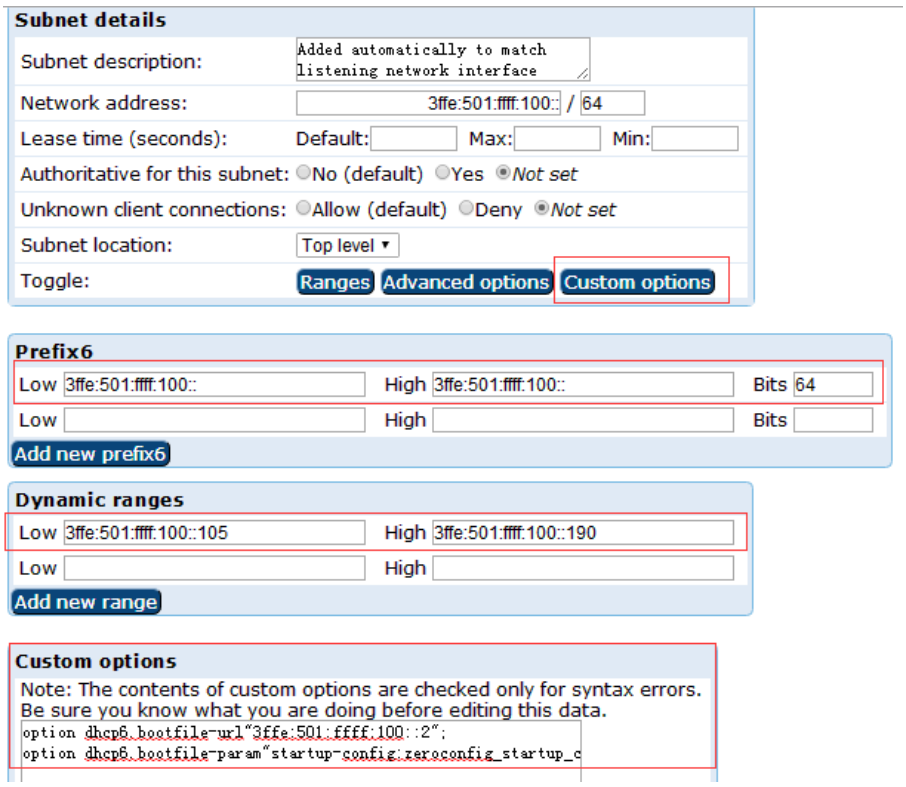
步骤 5 配置 DHCPv6 地址池及前缀长度，以下内容以某 DHCPv6 Server 软件为例进行介绍。

- 通过管理地址 https://172.16.125.201 登录到 DHCPv6 Server 管理控制台。
- 配置 DHCPv6 地址池 3ffe:501:ffff:100::105～3ffe:501:ffff:100::190 及前缀长度 64，如图 7-7 所示。

步骤 6 配置 Option59、Option60 字段，如图 7-7 所示。

- 设置 Option59 字段格式：option dhcp6.bootfile-url"3ffe:501:ffff:100::2";
- 设置 Option60 字段格式：option dhcp6.bootfile-param"startup-config:zeroconfig_startup_config,system-boot:S6550_SYSTEM_3.11.142_20170315";

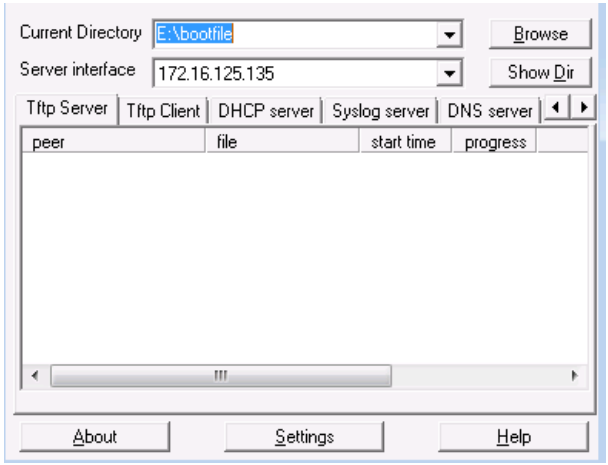
图7-7 配置 DHCPv6 地址池及前缀

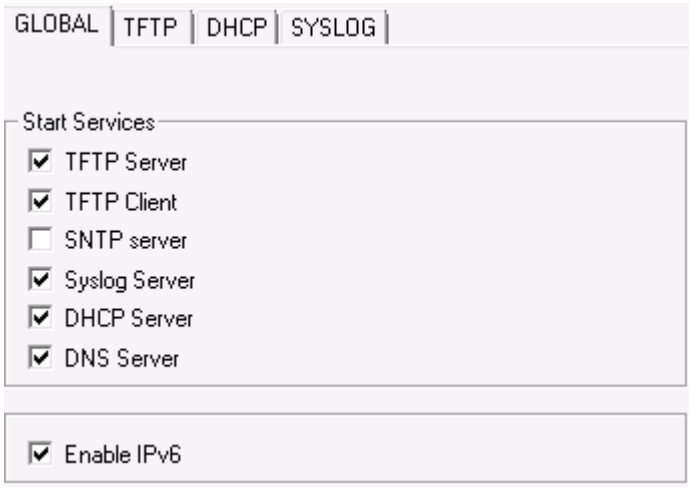


使用 TFTP 软件搭建需要下发给 SwicthB 的配置文件和系统文件的 TFTP Server 环境。

步骤 7 在虚拟机所在 PC 中，设置 TFTP Server 读取存储文件的目录和 TFTP Server 地址，如所示，并全局启用 IPv6，如所示。

- 设置 TFTP Server 软件服务目录为 bootfile，并在该目录下放置配置文件和系统文件。
- 设置 TFTP Server 软件服务地址为 PC 的网卡 IPv4 地址 172.16.125.135。
- 设置全局启用 IPv6 地址。





配置 Switch A。

步骤 8 单机模式下配置。

- 配置 Switch A。

配置 Switch A 的 GE 1/1/1 接口模式为 Trunk，并允许 VLAN10 通过，GE 1/1/2 口模式为 Access，接入 VLAN10。

```
Inspur#config
Inspur(config)#create vlan 10 active
Inspur(config)#interface  gigaethernet 1/1/1
Inspur(config-gigaethernet1/1/1)#switchport mode trunk
```

```
Inspur(config-gigaethernet1/1/1)#switchport trunk allowed vlan 10
Inspur(config-gigaethernet1/1/1)#interface  gigaethernet 1/1/2
Inspur(config-gigaethernet1/1/2)#switchport access vlan 10
```

- Switch B 上电启动。

Switch B 上电启动，将自动获取到 IPv6 地址，并下载文件。

检查配置

SwitchB 上电后，可以查看设备自动下载配置文件和系统文件，如图 7-8 所示。

图7-8 零配置自动获取文件

```
1970-01-01,08:01:06 DHCPC6-5-ACQUIRING_IPV6_ADDR:unit1: Acquiring IP address via DHCPv6.

1970-01-01,08:01:08 DHCPC6-5-ACQUIRING_IPV6_ADDR:unit1: Acquiring IP address via DHCPv6.

1970-01-01,08:01:10 DHCPC6-5-GET_IPADDR_SUCCESSFULLY:unit1: Acquire configuration information successfully.
ISCOM2600G_SYSTEM_3.    7% |**                              |  1733k  0:06:42 ETA
```

7.3 DHCP Snooping

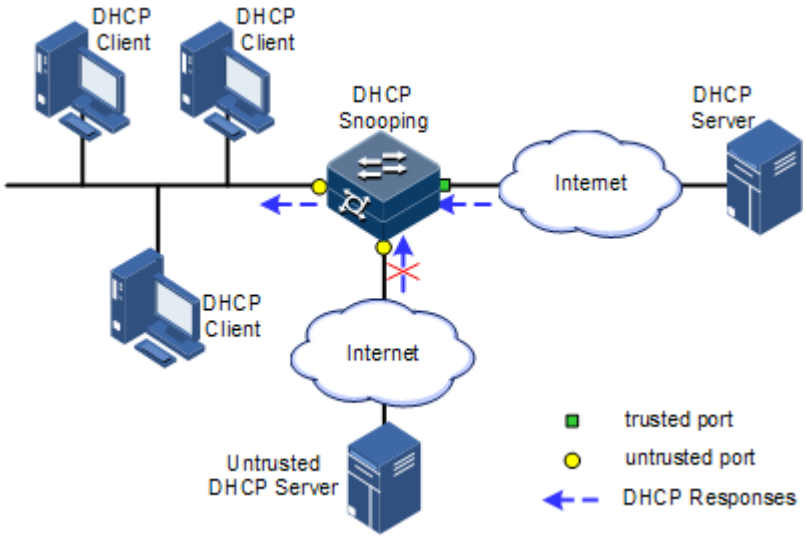
7.3.1 简介

DHCP Snooping 是 DHCP 的一种安全特性，具有如下功能：

- 保证 DHCP 客户端从合法的 DHCP 服务器获取 IP 地址；

网络中如果存在私自架设的伪 DHCP 服务器，则可能导致 DHCP 客户端获取错误的 IP 地址和网络配置参数，无法正常通信。如图 7-9 所示，为了使 DHCP 客户端能通过合法的 DHCP 服务器获取 IP 地址，DHCP Snooping 安全机制允许将接口设置为信任接口和不信任接口：信任接口正常转发接收到的 DHCP 报文；不信任接口接收到来自 DHCP 服务器的回应报文后将其丢弃。

图7-9 DHCP Snooping 组网示意图



- 记录 DHCP 客户端 IP 地址与 MAC 地址的对应关系。

DHCP Snooping 通过监听请求和信任接口收到的回应报文，记录 DHCP Snooping 表项，其中包括客户端的 MAC 地址、获取到的 IP 地址、与 DHCP 客户端连接的接口及该接口所属的 VLAN 等信息。利用这些信息可以实现：

- ARP Detection：根据 DHCP Snooping 表项来判断发送 ARP 报文的用户是否合法，从而防止非法用户的 ARP 攻击。
- IP Source Guard：通过动态获取 DHCP Snooping 表项对接口转发的报文进行过滤，防止非法报文通过该接口。
- VLAN 映射：发送给用户的报文通过查找映射 VLAN 对应的 DHCP Snooping 表项中的 DHCP 客户端 IP 地址、MAC 地址和原始 VLAN 的信息，将报文的映射 VLAN 修改为原始 VLAN。

DHCP 报文中的 Option 字段记录了 DHCP 客户端的位置信息。管理员可以利用该选项定位 DHCP 客户端，实现对客户端的安全和计费等控制。

如果设备配置了 DHCP Snooping 支持 Option 功能：

- 当设备接收到 DHCP 请求报文时，将根据报文中是否包含 Option 字段以及用户配置的处理策略及填充模式等对报文进行相应的处理，并将处理后的报文转发给 DHCP 服务器；
- 当设备接收到 DHCP 回应报文时，如果报文中含有 Option 字段，则删除该字段，并转发给 DHCP 客户端；如果报文中不含有 Option 字段，则直接转发。

7.3.2 配置准备

场景

DHCP Snooping 作为 DHCP 的一种安全特性，用于保证 DHCP 客户端从合法的 DHCP 服务器获取 IP 地址，并记录 DHCP 客户端 IP 地址与 MAC 地址的对应关系。

DHCP 报文中的 Option 字段记录了 DHCP 客户端的位置信息。管理员可以利用该选项定位 DHCP 客户端，实现对客户端的安全和计费等控制。配置了 DHCP Snooping 支持 Option 功能的交换机设备可以根据报文中是否包含 Option 字段，对其进行相应的处理。

前提

无

7.3.3 DHCP Snooping 的缺省配置

设备上 DHCP Snooping 的缺省配置如下。

功能	缺省值
全局 DHCP Snooping 状态	禁止
接口 DHCP Snooping 状态	使能
接口信任状态	不信任
DHCP Snooping 支持 Option 82	禁止

7.3.4 配置 DHCP Snooping

通常情况下，需要确保设备连接 DHCP 服务器侧的接口为信任状态，连接用户侧的接口为不信任状态。

对于启动了 DHCP Snooping 的设备，如果没有配置 DHCP Snooping 支持 Option 功能，则设备将不会对报文的 Option 字段进行任何处理。对于没有携带 Option 字段的报文，设备也不会进行插入处理。

缺省情况下设备所有接口的 DHCP Snooping 功能均已使能，但只有在使能全局 DHCP Snooping 功能后，接口的 DHCP Snooping 功能才会生效。

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#ip dhcp snooping`	使能全局 DHCP Snooping 功能。
3	`Inspur(config)#interface` *`interface-type interface-number`*	进入物理层接口或聚合组接口配置模式。
4	`Inspur(config-gigaethernet1/1/*)#ip dhcp snooping`	使能接口的 DHCP Snooping 功能，支持 QinQ 接口。
5	`Inspur(config-gigaethernet1/1/*)#ip dhcp snooping trust`	配置 DHCP Snooping 信任接口。

步骤	配置	说明
6	Inspur(config-gigaethernet1/1/*)#**ip dhcp snooping binding max** *number*	配置 DHCP Snooping 绑定表最大数量。
7	Inspur(config-gigaethernet1/1/*)# **ip dhcp snooping outer** *vlan-id* **inner** *vlan-list*	（可选）使能基于端口和双层 VLAN 开启 DHCP Snooping 功能
8	Inspur(config)#**ip dhcp snooping option client-id**	（可选）配置 DHCP Snooping 支持 Option61 功能。
9	Inspur(config)#**ip dhcp snooping autosave enable**	（可选）使能 DHCP Snooping 绑定表自动保存。
10	Inspur(config)#**ip dhcp snooping autosave write-interval** *time*	（可选）配置 DHCP Snooping 绑定表自动保存时间间隔。

7.3.5（可选）配置 DHCP Snooping 支持 Option 82 功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ip dhcp snooping information option**	配置全局开启 DHCP Snooping 支持 Option 82 功能。
3	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
4	Inspur(config-gigaethernet1/1/*)#**ip dhcp snooping information option vlan-list** *vlan-list*	配置接口 DHCP Snooping 支持 Option 82 的 VLAN 列表。

7.3.6 配置 DHCPv6 Snooping

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ipv6 dhcp snooping**	使能全局 DHCPv6 Snooping 功能。
3	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
4	Inspur(config-gigaethernet1/1/*)#**ipv6 dhcp snooping**	使能接口的 DHCPv6 Snooping 功能。

步骤	配置	说明
5	Inspur(config-gigaethernet1/1/*)#**ipv6 dhcp snooping trust** [**access-list** *acl-number*]	配置 DHCPv6 Snooping 信任接口。
6	Inspur(config-gigaethernet1/1/*)#**ipv6 dhcp snooping binding max** *number*	配置 DHCPv6 Snooping 绑定表最大数量。
7	Inspur(config-gigaethernet1/1/*)#**ipv6 dhcp snooping vlan** *vlan-id*	使能指定接口和指定 VLAN 的 IPv6 DHCP Snooping 功能。
8	Inspur(config-gigaethernet1/1/*)#**exit** Inspur(config)#**ipv6 dhcp snooping option** *number*	（可选）配置 DHCPv6 Snooping 支持自定义的 Option 功能。
9	Inspur(config)#**ipv6 dhcp snooping option interface-id**	（可选）配置 DHCPv6 Snooping 支持 Option18 功能。
10	Inspur(config)#**ipv6 dhcp snooping option remote-id**	（可选）配置 DHCPv6 Snooping 支持 Option37 功能。

7.3.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show ip dhcp snooping**	查看 DHCP Snooping 功能配置信息。
2	Inspur#**show ip dhcp snooping binding**	查看 DHCP Snooping 绑定表信息。
3	Inspur#**show ipv6 dhcp snooping**	查看基于 IPv6 的 DHCP Snooping 的配置信息。
4	Inspur#**show ipv6 dhcp snooping binding** [**prefix**]	查看基于 IPv6 的 DHCP Snooping 的绑定表信息。
5	Inspur#**show ip dhcp snooping autosave**	查看 DHCP Snooping 绑定表自动保存状态信息。

7.3.8 维护

用户可以通过以下命令，维护设备 DHCP Snooping 特性的运行情况和配置情况。

命令	描述
Rasiecom(config)#**clear ip dhcp snooping binding** [*interface-type interface-number* | **vlan** *vlan-id* | **ip-address** *ip-address*]	清除 IPv4 绑定表信息。

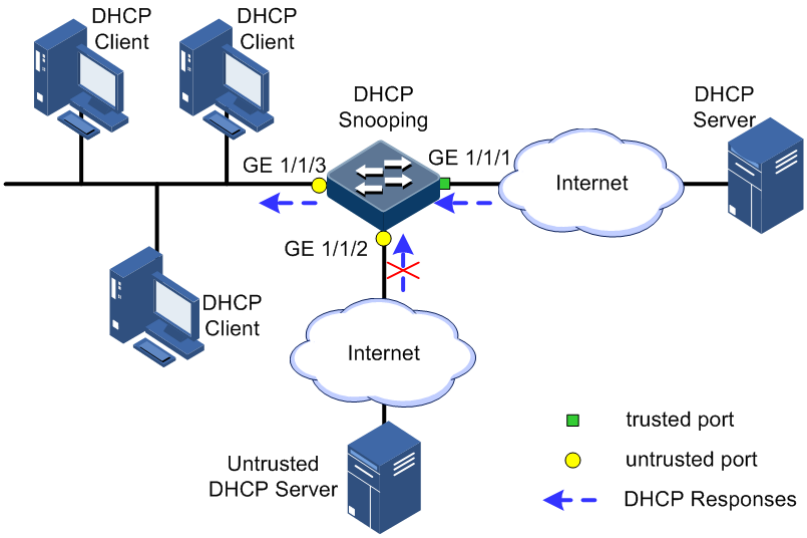
命令	描述
Rasiecom(config)#**clear ipv6 dhcp snooping binding** [*interface-type interface-number* | **vlan** *vlan-id* | **ipv6-address** *ipv6-address* | **ipv6-prefix** *ipv6-address/prefix-length*]	清除 IPv6 绑定表信息。

7.3.9 配置 DHCP Snooping 示例

组网需求

如图 7-10 所示，Switch 作为 DHCP Snooping 设备，需要保证 DHCP 客户端从合法的 DHCP 服务器获取 IP 地址，此外为了便于对客户端的管理，还需要设备支持 Option82 功能，在接口 GE 1/1/3 上配置电路 ID 子选项信息填充内容为 Inspur，远程 ID 子选项信息填充内容为 user01。

图7-10 配置 DHCP Snooping 组网示意图



配置步骤

步骤 1 配置全局 DHCP Snooping 功能。

```
Inspur#config
Inspur(config)#ip dhcp snooping
```

步骤 2 配置信任接口。

```
Inspur(config)#interface gigaethernet 1/1/1
Inspur(config-gigaethernet1/1/1)#ip dhcp snooping
Inspur(config-gigaethernet1/1/1)#ip dhcp snooping trust
Inspur(config-gigaethernet1/1/1)#quit
```

步骤 3 配置 DHCP Snooping 支持 Option82 功能并配置 Option82 字段。

```
Inspur(config)#ip dhcp snooping information option
```

```
Inspur(config)#ip dhcp information option remote-id string user01
Inspur(config)#interface gigaethernet 1/1/3
Inspur(config-gigaethernet1/1/3)#ip dhcp information option circuit-id
Inspur
```

检查结果

通过 **show ip dhcp snooping** 命令查看 DHCP 服务器配置是否正确。

```
Inspur#show ip dhcp snooping
DHCP Snooping: Enabled
DHCP Option 82: Enabled
Port                        vlan         Enabled Status  Trusted Status
Option82 Vlanlist
-------------------------------------------------------------------------
------------------------
gigaethernet1/1/1             --           enabled       yes           1-
4094
gigaethernet1/1/2             --           enabled       no            1-
4094
gigaethernet1/1/3             --           enabled       no            1-
4094
gigaethernet1/1/4             --           enabled       no            1-
4094
gigaethernet1/1/5             --           enabled       no            1-
4094
gigaethernet1/1/6             --           enabled       no            1-
4094
……
```

7.4 DHCP Option

7.4.1 简介

DHCP 利用报文中的 Option 字段传递控制信息和网络配置参数，实现地址的动态分配，为客户端提供更加丰富的网络配置信息。DHCP 协议规范定义的选项有 255 种，其中结束选项为 255。常用的 DHCP 选项如下表所示：

options	描述
3	路由器选项，用来指定 DHCP 客户端的网关地址。
6	DNS 服务器选项，用来指定为 DHCP 客户端分配的 DNS 服务器地址。
18	基于 IPv6 的 DHCP 客户端标识选项，用来指定 DHCP 客户端的接口信息。
37	基于 IPv6 的 DHCP 客户端标识选项，用来指定 DHCP 客户端的设备信息。
51	IP 地址租约选项。

options	描述
53	DHCP 报文类型选项，标识 DHCP 报文的类型。
55	请求参数列表选项。客户端利用该选项指明需要从服务器获取哪些网络配置参数。该选项内容为客户端请求的参数对应的选项值。
61	DHCP 客户端标识选项，用来指定 DHCP 客户端的设备信息。
66	TFTP 服务器名选项，用来指定为 DHCP 客户端分配的 TFTP 服务器的域名。
67	启动文件名选项，用来指定为 DHCP 客户端分配的启动文件名。
82	DHCP 客户端标识选项，可由用户自定义，主要用于标识 DHCP 客户端的位置信息，包含 Circuit ID 和 Remote ID 两个子选项。
150	TFTP 服务器地址选项，用来指定为 DHCP 客户端分配的 TFTP 服务器的地址。
184	DHCP 保留选项，目前 Option184 的使用主要是用来携带语音呼叫所需的信息。通过 Option184，可以实现在为具有语音功能的 DHCP 客户端分配 IP 地址的同时，为其提供语音呼叫相关信息。
255	结束选项。

DHCP Option 中的 18、37、61、82 字段均是 DHCP 报文中的中继代理信息选项。DHCP 客户端发送请求报文到 DHCP 服务器时，若需要经过 DHCP 中继或 DHCP Snooping，则由 DHCP 中继或 DHCP Snooping 将 Option 字段添加到请求报文中。

Option18、37、61、82 字段实现了 DHCP 客户端信息在 DHCP 服务器上的记录，与其他软件配合使用可以实现 IP 地址分配的限制和计费等功能。比如与 IP Source Guard 结合起来，可以有效抵御 IP 地址+MAC 地址的欺骗。

Option82 字段最多可以包含 255 个子选项。若定义了 Option82 字段，则至少要定义一个子选项。目前设备支持两类子选项：Sub-Option 1（Circuit ID，电路 ID 子选项）和 Sub-Option 2（Remote ID，远程 ID 子选项）。

- Sub-Option 1 的内容是接收到 DHCP 客户端请求报文的接口号，接口所属的 VLAN，及附加信息。
- Sub-Option 2 的内容是接收到 DHCP 客户端请求报文的接口 MAC 地址（DHCP 中继）或设备的桥 MAC 地址（DHCP Snooping 设备）或用户自定义的字符串。

7.4.2 配置准备

场景

DHCP Option 中的 18、37、61、82 字段是 DHCP 报文中的中继代理信息选项，DHCP 客户端发送请求报文到 DHCP Server 时，若需要经过 DHCP Snooping 或 DHCP 中继，则由 DHCP Snooping 或 DHCP 中继将 Option 字段添加到请求报文中。

DHCP Option18、37 字段用于记录基于 IPv6 的 DHCP 客户端信息，DHCP Option61、82 字段用于记录基于 IPv4 的 DHCP 客户端信息。DHCP 服务器基于此类信息，与其他软件配合使用可以实现 IP 地址分配的限制和计费等功能。

前提

无

7.4.3 DHCP Option 的缺省配置

设备上 DHCP Option 的缺省配置如下。

功能	缺省值
全局配置 attach-string	空
全局配置 remote-id	switch-mac
接口模式下 circuit-id	空

7.4.4 配置 DHCP Option 字段

请在设备上进行以下配置。

以下配置步骤均为可选，各步骤之间没有先后顺序。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ip dhcp information option attach-string** *attach-string*	（可选）配置 Option82 字段的附加信息。
	Inspur(config)#**interface** *interface-type interface-number* Inspur(config-gigaethernet1/1/*)#**ip dhcp information option circuit-id** *circuit-id* [**prefix-mode**]	（可选）在接口下配置 Option82 字段的电路 ID 子选项信息。
	Inspur(config-gigaethernet1/1/*)#**ip dhcp option vlan** *vlan-id* **description** *string* Inspur(config-gigaethernet1/1/*)#**exit**	（可选）配置 Option 82 字段中填入端口和 VLAN 的描述信息
	Inspur(config)#**ip dhcp information option** { **attach-string** | **circuit-id format** | **circuit-id hex** } *string*	（可选）配置 DHCP 报文的 Option82 中的附加字符串信息
	Inspur(config)#**ip dhcp information option circuit-id mac-format** *string*	（可选）配置 DHCP 报文的 Option82 中的 Circuit ID 可变参数 MAC 地址的格式

步骤	配置	说明
	Inspur(config)#**ip dhcp information option remote-id** { **client-mac** | **client-mac-string** | **hostname** | **string** *string* | **switch-mac** | **switch-mac-string** } Inspur(config)#**ip dhcp information option remote-id extend** { **client-mac** | **client-mac-string** | **switch-mac** | **switch-mac-string** }	（可选）配置 Option82 字段的远程 ID 子选项信息。DHCP Relay 支持 option82 的 remoteID 字段兼容华为 Default 模式。
3	Inspur(config)#**ipv4 dhcp option** *option-id* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* }	（可选）配置基于 IPv4 的自定义 Option。
	Inspur(config)#**interface** *interface-type interface-number* Inspur(config-gigaethernet1/1/*)#**ipv4 dhcp option** *option-id* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* }	（可选）在接口下创建自定义的 Option 字段信息。
4	Inspur(config-gigaethernet1/1/*)#**exit** Inspur(config)#**ipv4 dhcp option client-id** { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* }	（可选）配置 Option61 字段的信息。
	Inspur(config-gigaethernet1/1/*)#**ipv4 dhcp option client-id** { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* }	（可选）在接口下配置 Option61 字段的信息。

7.4.5 配置 IPv6 DHCP Option 18 字段

请在需要配置的设备上进行以下配置。

基于 IPv6 的 Option18 功能，需要在开启 DHCP Snooping 功能的设备上使用。

以下配置步骤均为可选，各步骤之间没有先后顺序。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ipv6 dhcp option interface-id** { **ascii** *ascii-string* | **hex** *hex-string* | **ipv6-address** *ipv6-address* }	（可选）配置 Option 18 字段的信息。
3	Inspur(config)#**interface** *interface-type interface-number* Inspur(config-gigaethernet1/1/*)#**ipv6 dhcp option interface-id** { **ascii** *ascii-string* | **hex** *hex-string* | **ipv6-address** *ipv6-address* }	（可选）在接口下配置 Option18 字段的信息。

7.4.6 配置 IPv6 DHCP Option 37 字段

请在需要配置的设备上进行以下配置。

基于 IPv6 的 Option37 功能，需要在开启 DHCP Snooping 功能的设备上使用。

以下配置步骤均为可选，各步骤之间没有先后顺序。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ipv6 dhcp option remote-id** { **ascii** | **hex** } *string*	（可选）配置 Option 37 字段的信息。
3	Inspur(config)#**interface** *interface-type interface-number* Inspur(config-gigaethernet1/1/*)#**ipv6 dhcp option remote-id mac-format** *string*	（可选）配置 DHCPv6 报文的 Option37 中的 Remote ID 可变参数 MAC 地址的格式。

7.4.7 配置 IPv6 的自定义 DHCP Option 字段

请在需要的设备上进行以下配置。

基于 IPv6 的自定义 Option，需要在开启 DHCP Snooping 功能的设备上使用。

以下配置步骤均为可选，各步骤之间没有先后顺序。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ipv6 dhcp option** *number* { **ascii** *ascii-string* | **hex** *hex-string* | **ipv6-address** *ipv6-address* }	（可选）创建基于 IPv6 自定义的 Option 字段信息。
3	Inspur(config)#**interface** *interface-type interface-number* Inspur(config-gigaethernet1/1/*)#**ipv6 dhcp option** *number* { **ascii** *ascii-string* | **hex** *hex-string* | **ipv6-address** *ipv6-address* }	（可选）在接口下创建基于 IPv6 自定义的 Option 字段信息。

7.4.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show ip dhcp information option**	查看 DHCP Option 字段配置信息。

序号	检查项	说明
2	`Inspur#show ip dhcp option port vlan description`	查看 DHCP Option 字段配置的端口和 VLAN 信息。

7.5 DHCP Server

7.5.1 简介

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）是在 TCP/IP 网络上给用户动态分配 IP 地址等配置信息的协议。它是基于 BOOTP（Bootstrap Protocol）协议，并在 BOOTP 协议的基础上添加了自动分配可用网络地址、网络地址重复使用以及其他扩展配置选项等功能。

随着网络规模的不断扩大和网络复杂度的提高，计算机的数量经常超过可供分配的 IP 地址数量。同时随着便携机及无线网络的广泛使用，计算机的位置也经常变化，相应的 IP 地址也必须经常更新，从而导致网络配置越来越复杂。DHCP 就是为解决这些问题而发展起来的。

DHCP 采用客户端/服务器通信模式，由客户端向服务器提出配置申请（包括 IP 地址、子网掩码、缺省网关等参数）服务器端返回为客户端分配的 IP 地址等相应的配置信息，以实现 IP 地址等信息的动态配置。

在 DHCP 的客户端/服务器通信模式中指定专门的主机分配网络地址，传送网络配置参数给需要的网络主机，被指定的主机称为 DHCP Server。

DHCP 应用

一般情况下，在以下场合会利用 DHCP Server 来完成 IP 地址分配：

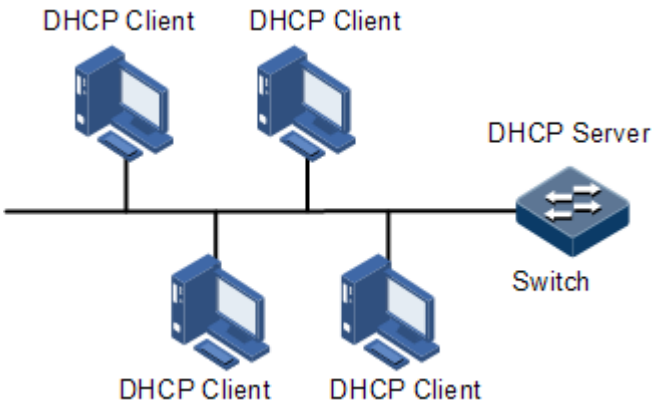
- 网络规模较大，手工配置需要很大的工作量，并难以对整个网络进行集中管理。
- 网络中主机数目大于该网络支持的 IP 地址数量，无法给每个主机分配一个固定的 IP 地址，且对同时接入网络的用户数目也有限制。
- 网络中只有少数主机需要固定的 IP 地址，大多数主机没有固定 IP 地址需求。

DHCP Client 从 DHCP Server 获得 IP 地址后，并不能永久使用其获得的 IP 地址，而是有一个固定的使用期限，称为租约时间。

DHCP 技术解决了 IP 地址的合理分配问题，从而避免了 IP 地址的浪费，提高了整网的 IP 地址使用率。

设备支持作为 DHCP Server，向客户端提供动态 IP 地址，如图 7-11 所示。

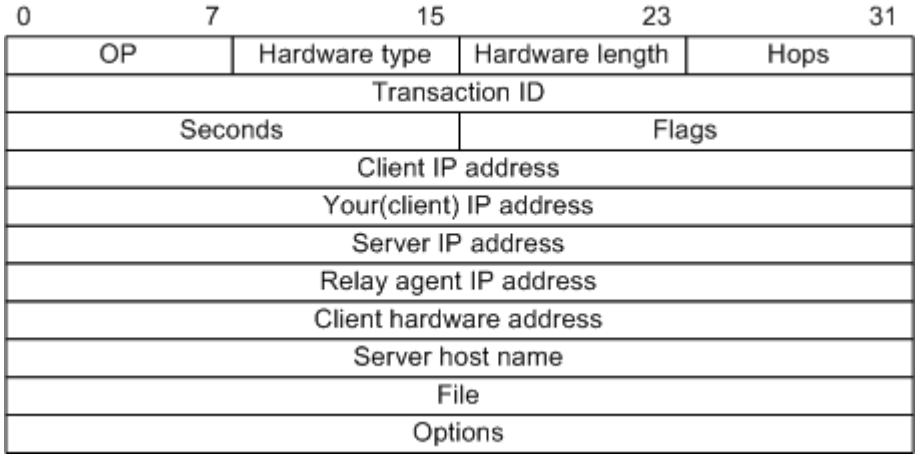
图7-11 DHCP Server 和 DHCP Client 应用组网示意图



DHCP 报文

DHCP 报文格式如图 7-12 所示。DHCP 报文被封装在 UDP 数据报中。

图7-12 DHCP 报文结构示意图



DHCP 报文中的各个字段含义如表 7-3 所示。

表7-3 DHCP 报文字段含义列表

字段名	字段长度（Byte）	描述
OP	1	报文类型。 • 取值为 1 时，表示该报文为客户端请求报文； • 取值为 2 时，表示该报文为服务器端回应报文。
Hardware type	1	DHCP 客户端的硬件地址类型。

字段名	字段长度（Byte）	描述
Hardware length	1	DHCP 客户端的硬件地址长度。
Hops	1	DHCP 报文经过的 DHCP 中继的数目。 DHCP 请求报文每经过一个 DHCP 中继，该字段就会加 1。
Transaction ID	4	客户端发起一次请求时选择的随机数，用来标识一次地址请求过程。
Seconds	2	DHCP 客户端开始 DHCP 请求后所经过的时间。目前没有使用，固定为 0。
Flags	2	第 1 个比特为广播回应标识位，用来标识 DHCP 服务器回应报文是采用单播还是广播方式发送。 • 0 表示采用单播方式； • 1 表示采用广播方式。 其它比特保留不用。
Client IP address	4	DHCP 客户端的 IP 地址，只有当客户端在绑定，更新或重新绑定状态时进行填充，且可以用于回应 ARP 请求。
Your(client) IP address	4	DHCP 服务器分配给客户端的 IP 地址。
Server IP address	4	DHCP 服务器的 IP 地址。
Relay agent IP address	4	DHCP 客户端发出请求报文后经过的第一个 DHCP 中继的 IP 地址。
Client hardware address	16	DHCP 客户端的硬件地址。
Server host name	64	DHCP 服务器的名称。
File	128	DHCP 服务器为 DHCP 客户端指定的启动配置文件名称及路径信息。
Options	可变	可选变长选项字段，包含报文的类型、有效租期、DNS（Domain Name System，域名系统）服务器的 IP 地址、WINS（Windows Internet Name Server ，Windows 网际命名服务）服务器的 IP 地址等配置信息。

7.5.2 配置准备

场景

设备作为 DHCPv4 服务器时，DHCPv4 客户端可以向设备获取 IP 地址。

前提

设备未启动 DHCPv4 客户端功能，且 DHCP 服务器的工作模式为普通 DHCP 服务器。

7.5.3 创建并配置 IPv4 地址池

请在需要创建并配置 IPv4 地址池的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ip dhcp server pool** *pool-name*	创建 IPv4 地址池并进入地址池配置模式。
3	Inspur(config-pool)#**address** *start-ip-address end-ip-address* **mask** { *mask* | *mask-length* }	配置 IPv4 地址池的地址范围。
4	Inspur(config-pool)#**excluded-ip-address** *start-ip-address* [*end-ip-address*]	配置 IPv4 地址池排除的地址范围。
5	Inspur(config-pool)#**lease expired** { *minute* | **infinite** }	配置 IPv4 地址池的地址租期。
6	Inspur(config-pool)#**dns-server** *ip-address* [**secondary**]	配置 IPv4 地址池的 DNS 服务器。
7	Inspur(config-pool)#**gateway** *ip-address*	配置 IPv4 地址池的缺省网关。
8	Inspur(config-pool)#**option 60** *vendor-string*	配置 Option60 携带信息。
9	Inspur(config-pool)#**option 43** [**sub-option** *option-code*] { **ascii** *ascii-string* | **hex** *hex-string* }	配置 Option43 携带信息。
10	Inspur(config-pool)#**tftp-server** *ip-address*	配置 IPv4 地址池的 TFTP 服务器。
11	Inspur(config-pool)#**trap server-ip** *ip-address*	配置 IPv4 地址池的 Trap 服务器。

7.5.4 配置 VLAN 接口的 DHCP Server 功能

只有在全局和三层接口均使能 DHCP Server 功能，该三层接口才会接收并处理客户端的 DHCP 请求报文。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式。
3	Inspur(config-vlan*)#**ip dhcp server**	使能 VLAN 接口的 DHCP Server 功能。

7.5.5（可选）配置 DHCP Server 支持 Option 82 功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ip dhcp server information option**	配置 DHCP Server 支持 Option 82。

7.5.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show ip dhcp server**	查看 DHCP 服务器的配置信息。
2	Inspur#**show ip dhcp server lease**	查看已分配的 IPv4 地址及其客户端信息。
3	Inspur#**show ip dhcp server statistics**	查看 DHCPv4 服务器的报文统计信息。
4	Inspur#**show ip dhcp static-bind**	查看 DHCPv4 静态租约信息。
5	Inspur#**show ip server pool** [**excluded-ip-address**] [**statistics**] [*pool-name*]	查看 DHCPv4 服务器的地址池配置信息。

7.5.7 维护

用户可以通过以下命令，维护设备 DHCP Server 特性的运行情况和配置情况。

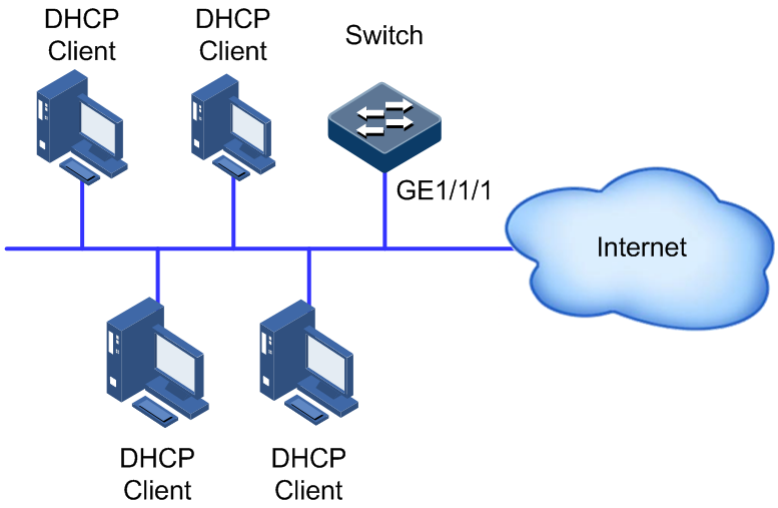
命令	描述
Rasiecom(config)#**clear ip dhcp server statistics**	清空 DHCP Server 统计信息。

7.5.8 配置 DHCPv4 服务器示例

组网需求

如图 7-13 所示，Switch 设备作为 DHCP 服务器分配 IP 地址给 DHCP 客户端，租期为 8 小时，IP 地址池名称为 pool，IP 地址范围是 172.31.1.2～172.31.1.100，DNS 服务器的 IP 地址为 172.31.100.1。

图7-13 配置 DHCP 服务器组网示意图



配置步骤

步骤 1 创建并配置 IP 地址池。

```
Inspur#config
Inspur(config)#ip dhcp server pool pool
Inspur(config-pool)#address 172.31.1.2 172.31.1.100 mask 24
Inspur(config-pool)#lease expired 480
Inspur(config-pool)#dns-server 172.31.100.1
Inspur(config-pool)#exit
```

步骤 2 配置接口的 DHCP 服务器功能。

```
Inspur(config)#interface vlan 1
Inspur(config-vlan1)#ip address 172.31.1.1 255.255.255.0
Inspur(config-vlan1)#ip dhcp server
```

检查结果

通过 **show ip dhcp server** 命令查看 DHCP 服务器配置是否正确。

```
Inspur#show ip dhcp server
Option 82: Enabled
Interface                  Status
-------------------------------------
vlan 1                     Enable
```

通过 **show ip server pool** 命令查看 DHCP 服务器的地址池配置是否正确。

```
Inspur#show ip server pool
Pool Name           :       pool
pool type           :       DHCP
Address Range        :       172.31.1.2~172.31.1.100
Address Mask         :       255.255.255.0
Gateway             :       0.0.0.0
DNS Server           :       172.31.100.1
Secondary DNS        :       0.0.0.0
Tftp Server          :       0.0.0.0
Lease time           :       480  minutes
Trap Server          :       0.0.0.0
interface            :       vlan1
option60             :
```

7.6 DHCP Relay

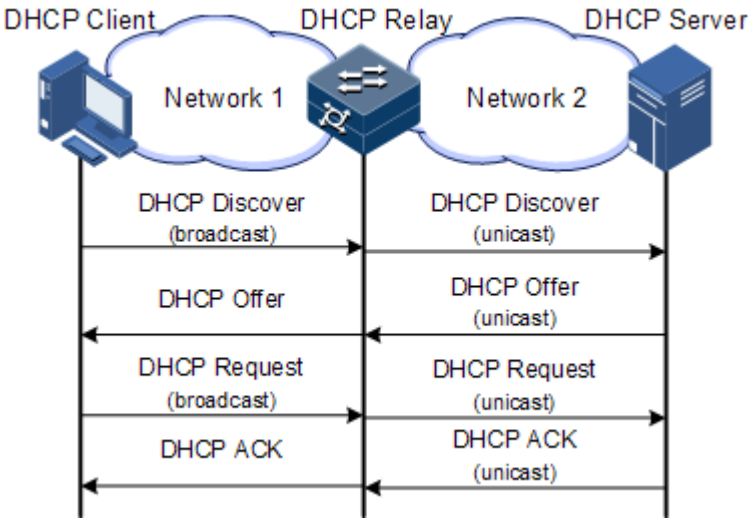
7.6.1 简介

最初的 DHCP 协议要求客户端和 DHCP 服务器只能在一个网段内，不可以跨网段工作。因此，为进行动态主机配置，需要在所有网段上都设置一个 DHCP 服务器，这显然是不经济的。

DHCP Relay（DHCP 中继）的引入解决了这个问题，它可使处于不同网段间的 DHCP 客户端和 DHCP 服务器之间承担中继服务，将 DHCP 协议报文跨网段中继到目的 DHCP 服务器，于是处在不同网段的 DHCP 客户端可以共同使用同一个 DHCP 服务器。

DHCP Relay 工作原理如图 7-14 所示。

图7-14 DHCP Relay 工作原理示意图



DHCP 客户端发送请求报文给 DHCP 服务器，DHCP 中继在收到该报文并适当处理后，发送给指定网段上的 DHCP 服务器。服务器根据请求报文中提供的必要信息，通过 DHCP 中继返回给客户端，完成对客户端的动态配置。

7.6.2 配置准备

场景

当 DHCP 客户端和 DHCP 服务器不在同一网段时，可以使用 DHCP Relay 功能解决这一问题。它可使处于不同网段间的 DHCP 客户端和 DHCP 服务器之间承担中继服务，将 DHCP 协议报文跨网段中继到目的 DHCP 服务器，于是处在不同网段的 DHCP 客户端可以共同使用同一个 DHCP 服务器。

前提

无

7.6.3 DHCP Relay 的缺省配置

设备上 DHCP Relay 的缺省配置如下。

功能	缺省值
全局 DHCP Relay 功能状态	禁止
接口 DHCP Relay 功能状态	禁止
全局 DHCPv6 Relay 功能状态	禁止
接口 DHCPv6 Relay 功能状态	禁止

7.6.4 配置全局 DHCP Relay

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#ip dhcp relay`	使能全局 DHCP Relay 功能。

7.6.5 配置 VLAN 接口 DHCP Relay 功能

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式。
3	Inspur(config-vlan*)#**ip dhcp realy target-ip** *ip-address*	配置报文转发的目的 IP 地址。

7.6.6 配置物理接口 DHCP Relay 功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface gigaethernet** *1/1/*.sub*	进入物理接口配置模式。
3	Inspur(config-gigaethernet1/1/*.sub)#**ip dhcp relay**	使能接口下 DHCP Relay 功能。
4	Inspur(config-gigaethernet1/1/*.sub)#**ip dhcp realy target-ip** *ip-address*	配置报文转发的目的 IP 地址。
5	Inspur(config-gigaethernet1/1/*)#**ip dhcp realy relay-ip** *ip-address*	配置中继 IP 地址，实现二层 Relay 功能。

7.6.7 配置全局 DHCPv6 Relay

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ipv6 dhcp relay**	使能全局 DHCPv6 Relay 功能。
3	Inspur(config)#**ipv6 dhcp relay option interface-id**	使能 DHCPv6 Relay 支持 Option18 的功能。
4	Inspur(config)#**ipv6 dhcp relay option remote-id**	使能 DHCPv6 Relay 支持 Option37 的功能。

7.6.8 配置 VLAN 接口 DHCPv6 Relay 功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式。
3	Inspur(config-vlan*)#**ipv6 dhcp relay**	使能 VLAN 接口下 DHCPv6 Relay 功能。
4	Inspur(config-vlan*)#**ipv6 dhcp relay target-ip** *ipv6-address*[**vlan** *vlan-id*]	配置报文转发的目的 IPv6 地址。

7.6.9（可选）配置 DHCP Relay 支持 Option 82 功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ip dhcp relay information option**	配置 DHCP Relay 支持 Option 82。DHCP Relay 支持 option82 的 remoteID 字段，兼容华为 Default 模式。
3	Inspur(config)#**ip dhcp relay information policy** { **drop** | **keep** | **replace** }	配置 DHCP Relay 对含 Option 82 的 DHCP 请求报文处理策略。
4	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
5	Inspur(config-gigaethernet1/1/*)#**ip dhcp relay information trusted**	配置 DHCP Relay 信任接口。

7.6.10 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show ip dhcp relay**	查看 DHCP Relay 功能配置信息。
2	Inspur#**show ip dhcp relay information**	查看 DHCP Relay 功能支持的 Option 82 信息选项。
3	Inspur#**show ipv6 dhcp relay**	查看 DHCPv6 Relay 功能配置信息。

7.6.11 维护

用户可以通过以下命令，维护设备 DHCP RELAY 特性的运行情况和配置情况。

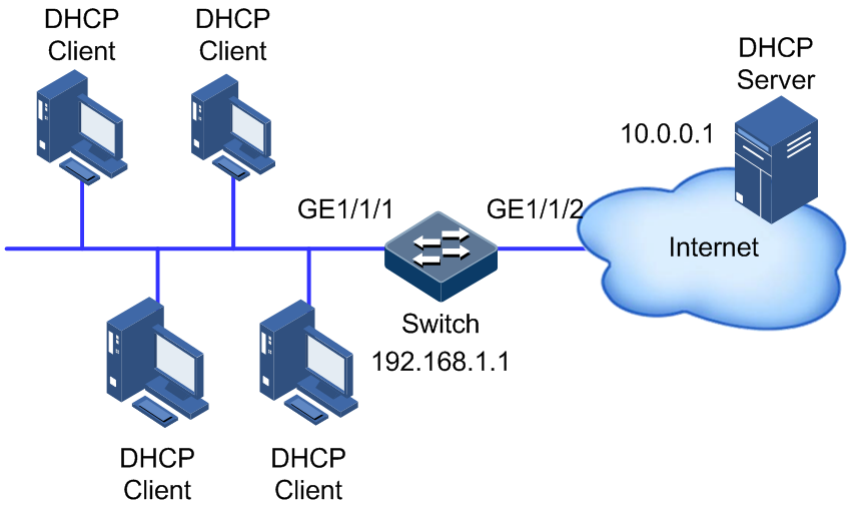
命令	描述
Rasiecom#**clear ip dhcp relay statistics**	清空 DHCP RELAY 统计信息。

7.6.12 配置 DHCPv4 中继示例

组网需求

如图 7-15 所示，Switch 设备作为 DHCP 中继，主机名为 Inspur，通过业务接口接入 DHCP 服务器。需要由 DHCP 服务器分配 IP 地址给客户端设备，从而使网管平台能够发现并管理该设备。

图7-15 配置 DHCP 中继组网示意图



配置步骤

步骤 1 使能全局的 DHCP 中继功能。

```
Inspur#config
Inspur(config)#ip dhcp relay
Inspur(config)#create vlan 2,3 active
Inspur(config)#interface vlan 2
Inspur(config-vlan2)#ip dhcp relay relay-ip 192.168.1.1
Inspur(config-vlan2)#exit
Inspur(config)#interface vlan 3
Inspur(config-vlan3)#ip dhcp relay relay-ip 192.168.1.1
Inspur(config-vlan3)#exit
```

步骤 2 配置 DHCP 中继的目的 IP。

```
Inspur(config)#interface vlan 2
Inspur(config-vlan2)#ip dhcp relay target-ip 10.0.0.1
```

检查结果

通过 **show ip dhcp relay** 命令查看 DHCP 中继配置是否正确。

```
Inspur#show ip dhcp relay
DHCP Relay Global Status: Enable
Interface                Status       Relay Address      Target Address
```

```
-------------------------------------------------------------------------------
-------
vlan2                     Enable       192.168.1.1       10.0.0.1
vlan3                     Enable       192.168.1.1       --
```

8 QoS

本章介绍 QoS 的基本原理和配置过程，并提供相关的配置案例。

- 简介
- 配置优先级
- 配置拥塞管理
- 配置拥塞避免
- 配置流分类和流策略
- 配置流量限速
- 带宽限速
- 配置举例

8.1 简介

随着网络应用种类的日益丰富，用户对不同的网络应用提出了不同的服务质量需求，这就需要网络能够根据用户的需求为不同的网络应用分配和调度资源。QoS（Quality of Service，服务质量）技术的产生，使网络在发生过载或拥塞时，能够确保重要业务的实时性和完整性，同时保证整个网络的高效运行。

QoS 由一组流量管理技术组成：

- 服务模型
- 优先级信任
- 流分类
- 流策略
- 优先级映射
- 拥塞管理
- 拥塞避免

8.1.1 服务模型

QoS 技术服务模型：

- Best-effort Service（尽力而为服务模型）
- Differentiated Service（区分服务模型，简称 DiffServ）

Best-effort

Best-effort 服务模型是基于储存转发机制的 Internet（IPv4 标准）最基本、最简单的服务模型。在 Best-effort 服务模型中，应用程序在任何时刻，发送任意数量的报文，而且事先不需要经过批准，也不需要通知网络。对 Best-effort 服务来说，网络尽最大可能来发送报文，但对时延、可靠性等不做任何保证。

Best-effort 模型是现在 Internet 缺省的服务模型，适用于大多数网络应用，如 FTP，E-mail 等，它通过先入先出（FIFO）队列来实现。

DiffServ

DiffServ 模型是一个多服务模型，它可以满足不同的 QoS 需求。

对于 DiffServ 模型来说，它不需要为每个流维护状态。它根据每个报文的 QoS 分类来提供差异化的服务。可以使用不同的方法进行报文的 QoS 分类，如 IP 报文的优先级（IP Precedence）、报文的源地址或目的地址等。

DiffServ 一般用来为一些重要的应用提供端到端的 QoS 服务。主要通过以下技术来实现：

- CAR（Committed Access Rate，承诺访问速率）：根据预先设定的报文匹配规则。如 IP 报文的优先级、报文的源地址或目的地址等，进行报文的分类。如果是符合令牌桶流量规则的报文，就继续发送。如果是超出流量规定的报文，则被丢弃或者重新标记 IP Precedence、DSCP、EXP 等。CAR 不仅可以进行流量控制，还可以对报文进行标记和重标记。
- 队列技术：SP、WRR、DRR、SP+WRR、SP+DRR 等队列技术对拥塞的报文进行缓存和调度，实现拥塞管理。

8.1.2 优先级信任

优先级信任是指设备采用报文自身携带的优先级作为分类依据，对报文进行后续的 QoS 管理操作。

信任的优先级种类有：

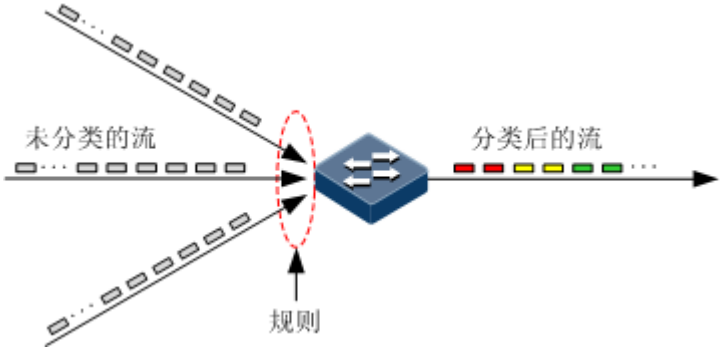
- 基于 DSCP（Differentiated Services Code Point，差分服务代码点）优先级
- 基于 CoS（Class of Service，服务等级）优先级
- 基于 ToS（Type of Service，服务类型）优先级

8.1.3 流分类

流分类是指采用一定的规则识别符合某类特征的报文，对匹配不同规则的报文实施不同的 QoS 策略。它是有区别的进行服务的前提和基础。

包括基于 IP 报文的 IP 优先级、DSCP 优先级和基于 CoS 优先级进行分类，基于 ACL（Access Control List，访问控制列表）规则、VLAN ID 进行分类。流量分类过程如图 8-1 所示。

图8-1 流分类过程示意图



IP 优先级和 DSCP 优先级

IP 报文头部结构如图 8-2 所示，该报文中含有 8bit 的 ToS 字段。根据 RFC1122 的定义，IP 优先级（IP Precedence）使用最高 3 位（第 0～3 位），取值范围为 0～7。在 RFC2474 中，重新定义了 ToS 字段，将该部分的前 6 位（0～5 位）用于表示 DSCP 优先级，取值范围是 0～63，后 2 位（6、7 位）是保留位。两类优先级的结构如图 8-3 所示。

图8-2 IP 报文头部结构示意图

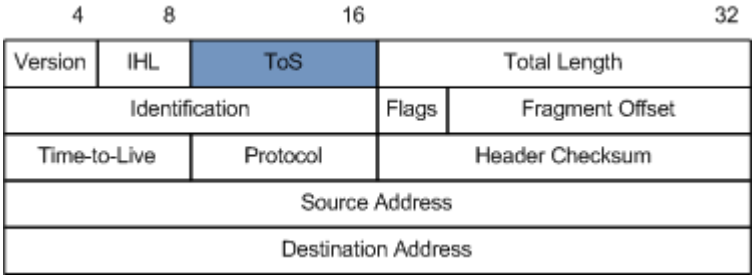
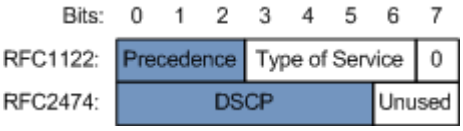


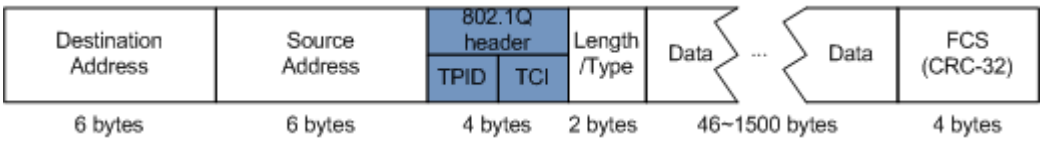
图8-3 IP 优先级和 DSCP 优先级报文结构示意图



CoS 优先级

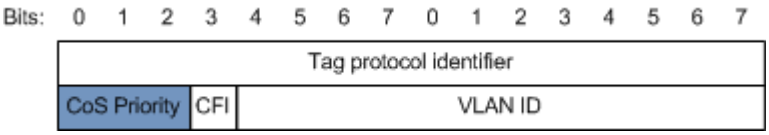
基于 IEEE 802.1Q 标准的 VLAN 报文对 Ethernet 报文的格式进行了修改，在源 MAC 地址字段和协议类型字段之间加入 4 字节的 802.1Q 标签，如图 8-4 所示，该标签包含了 2 个字节的 TPID（Tag Protocol Identifier，标签协议标识，取值是 0x8100）字段和 2 个字节的 TCI（Tag Control Information，标签控制信息）字段。

图8-4 VLAN 报文结构示意图



CoS 优先级位于 TCI 字段的前 3 位，取值范围是 0～7，如图 8-5 所示。适用于只需要在二层网络中保证服务质量的场合。

图8-5 CoS 优先级报文结构示意图



8.1.4 流策略

当对报文进行流分类后，需要对不同类别的报文执行不同的操作，流分类和操作的绑定即形成了流策略。

流量限速

流量限速就是指对网络流量进行控制，通过监督进入网络的流量速率，对超出部分流量采取丢弃措施，使进入的流量被限制在一个合理的范围之内，从而保护网络资源和运营商的利益。

S6550 设备支持在接口的入方向进行基于流策略的流量限速。

S6550 设备支持使用令牌桶进行限速，支持两种令牌桶方式，即单令牌桶和双令牌桶。

重定向

重定向是指不按报文原始的目的地址与接口的对应关系进行转发，而是将报文重定向到指定的接口进行转发，以实现策略路由。

S6550 设备支持在接口的入方向上将其重定向到指定的接口进行转发。

重标记

重标记是指设备对报文中的某些优先级字段进行重新设置，从而能够根据自己的标准对报文重新分类。此外，网络中的下游节点也可以根据重标记信息提供有差别的 QoS 服务。

S6550 设备支持对报文的以下优先级字段进行重标记：

- IP 报文的 IP 优先级
- DSCP 优先级

- CoS 优先级

流量统计

流量统计用于统计指定业务流的数据报文，它统计的是匹配流分类的报文中通过和丢弃的报文数量和字节数。

流量统计本身不是 QoS 控制措施，但是可以和其他 QoS 动作组合使用，以提高网络的可监管性。

8.1.5 优先级映射

优先级映射是指当报文进入设备时，将其按照预先设定的外部优先级到本地优先级的映射关系，分别送入不同本地优先级的报文队列，以便在报文的出方向对不同的队列进行调度处理。

S6550 设备支持基于 DSCP 优先级或 CoS 优先级进行优先级映射。对于 IPv6 报文，Traffic-Class 字段对应于 IPv4 报文的 DSCP 域，现有的 DSCP 域到本地优先级映射的功能也适用于 IPv6 报文，使用时取 Traffic-Class 字段的前 6 位即可。

缺省情况下，S6550 设备的本地优先级和 DSCP 优先级，本地优先级和 CoS 优先级的映射关系如表 8-1 所示。

表8-1 DSCP 优先级、CoS 优先级和本地优先级的映射关系表

local	0	1	2	3	4	5	6	7
DSCP	0～7	8～15	16～23	24～31	32～39	40～47	48～55	56～63
CoS	0	1	2	3	4	5	6	7

本地优先级是指设备为报文分配的一种具有内部意义的优先级，QoS 队列调度过程中与队列相对应的优先级。

本地优先级的范围为 0～7，S6550 设备每个接口支持 8 个队列，本地优先级与接口队列的对应关系是一对一关系，依据本地优先级和队列之间的映射关系将报文送入指定队列。映射关系如表 8-2 所示。

表8-2 本地优先级和队列的映射关系

local	0	1	2	3	4	5	6	7
队列	1	2	3	4	5	6	7	8

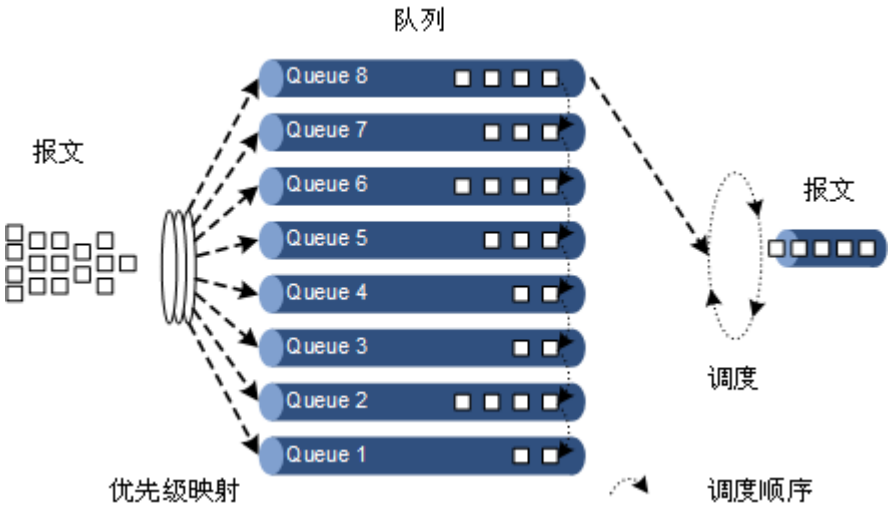
8.1.6 拥塞管理

当时延敏感业务要求得到比非时延敏感业务更高质量的 QoS 服务，或网络间歇性的出现拥塞时，需要进行队列调度。

队列调度是指使用不同的调度算法来发送队列中的报文流。S6550 设备支持的队列调度算法有 SP（Strict-Priority，严格优先级调度）、WRR（Weight Round Robin，加权循环调度）、DRR（Deficit Round Robin，差额循环调度）、SP+WRR、SP+DRR。每种调度算法都是为了解决特定网络流量的问题，并对带宽资源的分配、延迟、抖动等有不同的影响。

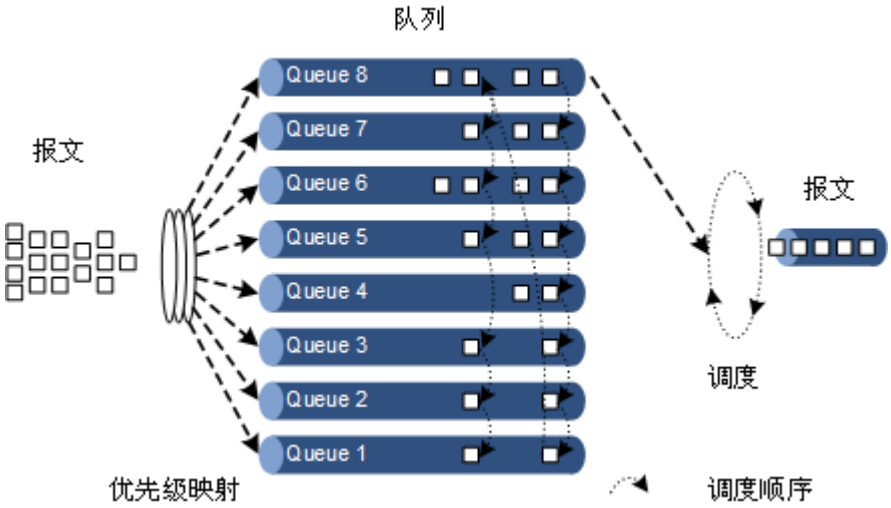
- SP：设备严格按照队列优先级的高低顺序进行调度。只有高优先级队列中的报文全部调度完毕后，低优先级队列才有调度的机会。如图 8-6 所示。

图8-6 SP 调度示意图



- WRR：在按照队列的优先级次序以循环方式调度每个队列报文的基础上，根据每个队列的权重来调度各队列中的报文。如图 8-7 所示。

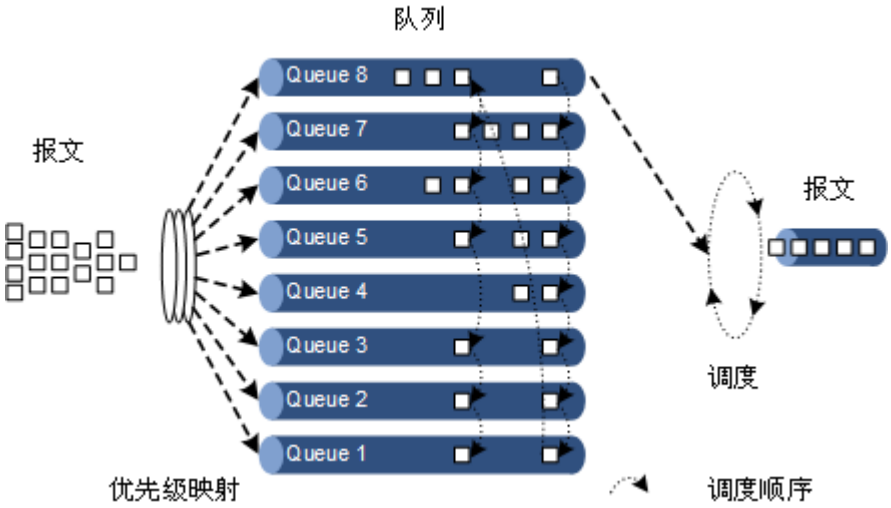
图8-7 WRR 调度示意图



- DRR：在按照队列的优先级次序以循环方式调度每个队列报文的基础上，根据每个队列的权重来调度各队列中的报文。此外，当其中某一队列在一轮调度中有多

余的带宽，设备会临时将该带宽借给其他队列使用，在稍后的某轮调度中，借入带宽的队列会将这部分带宽归还给原先借出带宽的队列，如图 8-8 所示。

图8-8 DRR 调度示意图



- SP+WRR：SP 调度和 WRR 调度相结合的调度方式，将设备接口上的队列分为两组，用户可以指定其中的某几组队列进行 SP 调度，其他队列进行 WRR 调度。
- SP+DRR：SP 调度和 DRR 调度相结合的调度方式，将设备接口上的队列分为两组，用户可以指定其中的某几组队列进行 SP 调度，其他队列进行 DRR 调度。

8.1.7 拥塞避免

拥塞避免（Congestion Avoidance）是指通过监视网络资源（如队列或内存缓冲区）的使用情况，在拥塞发生或有加剧的趋势时主动丢弃报文，通过调整网络的流量来解除网络过载的一种流量控制机制。

传统的丢包策略采用尾部丢弃（Tail-Drop）的方法，同等的对待所有的报文，不对服务等级进行区分。在拥塞发生期间，队列尾部的数据包将被丢弃，直到拥塞解决。

这种丢弃策略会引发 TCP 全局同步现象，使网络流量忽大忽小，影响链路利用率。

RED

RED（Random Early Detection，随机早期检测）技术通过随机地丢弃报文，让多个 TCP 连接不同时降低发送速度，从而避免了 TCP 的全局同步现象。

在 RED 技术的算法中，为每个队列的长度都设定了阈值上下限，并规定：

- 当队列的长度小于阈值下限时，不丢弃报文。
- 当队列的长度大于阈值上限时，丢弃所有收到的报文。
- 当队列的长度在阈值上限和阈值下限之间时，随机丢弃到来的报文。队列越长，报文被丢弃的概率越高。

8.1.8 基于接口和 VLAN 的流量限速

S6550 除了支持基于流策略对报文流量进行限速外，还支持基于接口、基于 VLAN、基于接口+VLAN 对报文流量进行限速。与基于流策略的流量限速类似，设备对超出部分流量采取丢弃措施。

8.1.9 带宽限速

带宽限速是 QoS 的一个子功能，它比基本 QoS 更加灵活，在交换机设备上应用广泛。

带宽限速的主要功能如下：

- 入端口
  - 带宽保证：实现基于端口或基于流的带宽服务，同时支持分层带宽保证，细化不同业务流的带宽。
  - 识别：当流从带宽保证端口进入时，决定是否对报文进行颜色识别。
- 出端口
  - 带宽保证：实现基于端口或基于流的带宽服务，不支持分层带宽保证。
  - 标记：当流从带宽保证端口转出时，决定是否对报文进行颜色标记。

带宽保证

带宽保证功能能够保证接入网络的业务流量保持在规定的范围内，对于超出的流量进行“惩罚”，如丢弃或选择调度。带宽保证既能满足用户对业务带宽的要求，也能保护网络资源和运营商的利益。

用户通过配置带宽保证模板并在端口上应用模板，可以实现对端口的流量进行颜色（绿色、黄色和红色）标记。设备会根据流量的颜色作出不同处理，绿色流量保证转发，黄色流量选择调度，红色流量直接丢弃。

分层带宽保证

分层带宽保证是一种更灵活的带宽保证，用户不仅可以为每个流量单独配置带宽保证，还可以通过分层带宽对多个流量的总和进行带宽保证。

颜色识别与标记

使能颜色识别功能，设备会处于 Color-aware 状态，可以识别从上游设备流入端口的流量是否带有颜色。如果禁用颜色识别功能，设备处于 Color-blind 状态，将忽略进入端口的流量是否带有颜色，设备会重新判断该流量的颜色。

颜色标记是设备根据用户在带宽保证模板中设定的 CIR、CBS、EIR、EBS 参数来判断业务流量属于哪一种颜色，并根据 802.1ad 标准定义的报文格式，修改流量报文中相关标志位，使之带有颜色。

8.2 配置优先级

8.2.1 配置准备

场景

对于来自上游设备的报文，用户可以选择信任报文携带的优先级，对于不信任其优先级的报文可以交由流分类和流策略处理。配置优先级信任模式后，设备可以依据不同优先级对报文进行相应的操作，提供相应的服务。

为报文指定本地优先级是进行队列调度的前提条件，对于来自上游设备的报文，用户可以将报文携带的外部优先级映射到不同的本地优先级，也可以基于接口直接配置报文的本地优先级，之后设备将依据本地优先级对报文进行队列调度。通常来说，对于 IP 报文，需要配置 IP 优先级或 DSCP 优先级与本地优先级的映射关系；对于 VLAN 报文，需要配置 CoS 优先级与本地优先级的映射关系。

前提

无

8.2.2 基本 QoS 的缺省配置

设备上基本 QoS 的缺省配置如下。

功能	缺省值
全局 QoS 功能状态	使能
接口信任的优先级类型	信任 CoS 优先级
Cos 到本地优先级及颜色映射	请参见表 8-3
DSCP 到本地优先级及颜色映射	请参见表 8-4
本地优先级到 CoS 优先级的映射关系	请参见表 8-5
接口优先级	0

表8-3 缺省情况下 CoS 和本地优先级及颜色的映射关系

CoS	0	1	2	3	4	5	6	7
local	0(green)	1(green)	2(green)	3(green)	4(green)	5(green)	6(green)	7(green)

表8-4 缺省情况下 DSCP 和本地优先级及颜色的映射关系

DSCP	0～7	8～15	16～23	24～31	32～39	40～47	48～55	56～63
local	0(green)	1(green)	2(green)	3(green)	4(green)	5(green)	6(green)	7(green)

表8-5 缺省情况下本地优先级到 CoS 优先级的映射关系

Local	0	1	2	3	4	5	6	7
CoS	0	1	2	3	4	5	6	7

8.2.3 配置接口信任的优先级类型

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**mls qos trust** { **cos** | **dscp** | **dscp-or-cos** | **port-priority** }	配置接口信任的优先级类型。
4	Inspur(config-gigaethernet1/1/*)#**mls qos priority** *portpri-value*	配置接口优先级。

8.2.4 配置 CoS 到本地优先级及颜色映射

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**mls qos mapping cos-to-local-priority** *profile-id*	创建 CoS 到本地优先级及颜色映射模板，并进入 cos-to-pri 配置模式。
3	Inspur(cos-to-pri)#**cos** *cos-value* **to local-priority** *localpri-value* [**color** { **green** | **red** | **yellow** }]	（可选）修改 CoS 到本地优先级及颜色模板信息。
4	Inspur(cos-to-pri)#**exit** Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。

步骤	配置	说明
5	Inspur(config-gigaethernet1/1/*)#**mls qos cos-to-local-priority** *profile-id* [**dei** { **enable** | **disable** }]	配置接口应用 CoS 到本地优先级及颜色模板。

8.2.5 配置 DSCP 到本地优先级及颜色映射

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**mls qos mapping dscp-to-local-priority** *profile-id*	创建 DSCP 到本地优先级及颜色映射模板，并进入 dscp-to-pri 配置模式。
3	Inspur(dscp-to-pri)#**dscp** *dscp-value* **to local-priority** *localpri-value* [**color** { **green** | **red** | **yellow** }]	（可选）修改 DSCP 到本地优先级及颜色模板信息。
4	Inspur(dscp-to-pri)#**exit** Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
5	Inspur(config-gigaethernet1/1/*)#**mls qos dscp-to-local-priority** *profile-id*	配置接口应用 DSCP 到本地优先级及颜色模板，与 DSCP 转换共用一个模板。

8.2.6 配置 DSCP 转换

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**mls qos mapping dscp-mutation** *profile-id*	创建 DSCP 转换映射模板，并进入 dscp-mutation 配置模式。
3	Inspur(dscp-mutation)#**dscp** *dscp-value* **to new-dscp** *newdscp-value*	（可选）修改 DSCP 转换模板信息，与 DSCP 到本地优先级共用一个模板。
4	Inspur(dscp-mutation)#**exit** Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
5	Inspur(config-gigaethernet1/1/*)#**mls qos dscp-mutation** *profile-id*	配置接口应用 DSCP 转换模板。

8.2.7 配置 CoS 重标记

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**mls qos mapping cos-remark** *profile-id*	创建 CoS 重标记模板，并进入 cos-remark 配置模式。
3	Inspur(cos-remark)#**local-priority** *localpri-value* **to cos** *newcos-value*	修改 CoS 重标记模板信息。
4	Inspur(cos-remark)#**exit** Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
5	Inspur(config-gigaethernet1/1/*)#**mls qos cos-remark** *profile-id*	配置接口应用 CoS 重标记模板。
6	Inspur(config-gigaethernet1/1/*)#**mls qos cos-remark-mapping** { **enable** [**dei** { **enable** | **disable** }] | **disable** } Inspur(config-gigaethernet1/1/*)#**exit**	使能本地优先级到 CoS 的映射，使用 disable 格式禁用该功能

8.2.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show mls qos interface** [*interface-type interface-number*]	查看接口的 QoS 优先级、信任模式和调度模式信息。
2	Inspur#**show mls qos mapping cos-to-local-priority** [**default** | *profile-id*]	查看 CoS 到本地优先级及颜色模板映射信息。
3	Inspur#**show mls qos mapping dscp-to-local-priority** [**default** | *profile-id*]	查看 DSCP 到本地优先级及颜色模板映射信息。
4	Inspur#**show mls qos mapping dscp-mutation** [**default** | *profile-id*]	查看 DSCP 转换模板映射信息。
5	Inspur#**show mls qos mapping cos-remark** [**default** | *profile-id*]	查看 CoS 重标记模板信息。

8.3 配置拥塞管理

8.3.1 配置准备

场景

当网络发生拥塞时，若用户希望能均衡各类报文的延迟和延迟抖动，关键业务（如视频业务、语音业务）的报文能够得到优先处理；同时对于非关键业务（如 E-Mail）的报文，保证相同优先级业务得到公平处理，不同优先级业务按照各自权值处理。可以通过配置队列调度来实现。具体选择何种调度算法，需要依据当时的业务情况与客户需求。

前提

全局 QoS 功能使能。

8.3.2 拥塞管理的缺省配置

设备上拥塞管理的缺省配置如下。

功能	缺省值
队列调度模式	SP
队列权重	• WRR 调度 8 个队列的权重均为 1 • DRR 调度 8 个队列的权重均为 1

8.3.3 配置 SP 队列调度

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**mls qos queue scheduler sp**	配置接口队列调度方式为 SP。

8.3.4 配置 WRR 或 SP+WRR 队列调度

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**mls qos queue scheduler wrr** *weigh1 weight2 weight3…weight8*	配置接口队列调度方式为 WRR 并且配置各队列的权重。 当配置某个队列的优先级值为 0 时，则对该队列进行 SP 调度。

8.3.5 配置 DRR 或 SP+DRR 队列调度

请在需要配置 DRR 或 SP+DRR 队列调度的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**mls qos queue scheduler drr** *weigh1 weight2 weight3…weight8*	配置接口队列调度方式为 DRR 并配置各队列的权重。 当配置某个队列的优先级值为 0 时，则对该队列进行 SP 调度。

8.3.6 配置队列带宽保证

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**mls qos queue** *queue-id* **shaping cir** *cir* **pir** *pir*	（可选）配置基于接口队列的带宽保证，同时设置突发尺寸。

8.3.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show mls qos queue interface** *interface-type interface-number*	查看接口的队列权重信息。
2	Inspur#**show mls qos queue statistics interface** *interface-type interface-number*	查看接口下队列的统计信息。
3	Inspur#**show mls qos queue shaping interface** *interface-type interface-list*	查看接口的队列整形信息。

8.4 配置拥塞避免

8.4.1 配置准备

场景

为避免网络拥塞的发生，解决 TCP 全局同步的问题，可以通过配置拥塞避免，调整网络流量，解除网络过载。

设备基于 WRED 进行拥塞避免。

前提

全局 QoS 功能使能。

8.4.2 拥塞避免的缺省配置

设备上拥塞避免的缺省配置如下。

功能	缺省值
全局 WRED 功能状态	使能

8.4.3 配置 WRED

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**mls qos wred profile** *profile-id*	创建 WRED 模板，并进入 WRED 配置模式。

步骤	配置	说明
3	Inspur(wred)#**wred** [**color** { **green** | **red** | **yellow** }] **start-drop-threshold** *start-drop* **end-drop-threshold** *end-drop* **max-drop-probability** *max-drop*	修改 WRED 模板信息。
4	Inspur(wred)#**exit** Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式或聚合组接口配置模式。以下步骤以物理接口配置模式为例。
5	Inspur(config-gigaethernet1/1/*)#**mls qos queue** *queue-id* **wred** *profile-id*	配置接口上应用 WRED 模板

8.4.4 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show mls qos wred profile** [*profile-list*]	查看 WRED 模板信息。
2	Inspur#**show mls qos queue wred interface** *interface-type interface-number*	查看接口 WRED 信息。

8.5 配置流分类和流策略

8.5.1 配置准备

场景

流分类是 QoS 的基础，对于来自上游设备的报文，用户可以根据报文携带的优先级进行分类，也可以根据 ACL 规则对报文进行分类，分类完成后，设备可以依据不同类别对报文执行相应的操作，提供相应的服务。

完成流分类的配置后，还需要绑定到流策略中才能生效，具体采取何种流策略，与所处的阶段以及网络当前的负载状况有关。通常，当报文进入网络时依据承诺速率对它进行流量限速，依据报文的业务特性对它进行优先级重标记等。

前提

全局 QoS 功能使能。

8.5.2 流分类和流策略的缺省配置

设备上流分类和流策略的缺省配置如下。

功能	缺省值
流策略功能状态	禁用
流策略统计功能状态	禁用

8.5.3 创建流分类

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**class-map** *class-map-name* [**match-all** | **match-any**]	创建流分类，并进入流分类 cmap 配置模式。
3	Inspur(config-cmap)#**description** *string*	（可选）描述流分类信息。

8.5.4 配置流分类规则

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**class-map** *class-map-name* [**match-all** | **match-any**]	创建流分类，并进入流分类 cmap 配置模式。
3	Inspur(config-cmap)#**match access-list** { *acl-number* | **name** *word* } Inspur(config-cmap)#**exit**	（可选）配置基于 ACL 规则进行的流分类。 采用的 ACL 规则必须首先定义，且其类型必须为 permit。
4	Inspur(config)#**policy-map** *policy-map-name* Inspur(config-pmap)#**class-map** *class-map-name*	（可选）配置基于流分类规则进行的流分类。 所依据的流分类必须已经创建，并且其匹配类型必须与该流分类的匹配类型一致。
5	Inspur(config-cmap)#**match cos** *cos-value*	（可选）配置基于报文的 CoS 优先级进行流分类。
6	Inspur(config-cmap)#**match inner-vlan** *inner-vlan-value*	（可选）配置基于报文的内层 VLAN 进行流分类。
7	Inspur(config-cmap)#**match vlan** *vlan-value* [*vlan-mask*]	（可选）配置基于报文的 VLAN 进行流分类。

步骤	配置	说明
8	Inspur(config-cmap)#**match dscp** *dscp-value*	（可选）配置基于 DSCP 优先级规则进行的流分类。

说明

- 一个流分类必须为其配置流分类规则，即进行 **match** 配置。
- 已经被流策略引用的流分类，不允许修改流分类规则，即修改流分类的 **match**。

8.5.5 创建流量限速和整形规则

当用户需要对报文进行基于流策略的流量限速时，需要创建令牌桶，对令牌桶设置流量限速和整形规则，并在绑定到流策略的流分类下引用此规则。

请在需要创建流量限速规则的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**mls qos policer-profile** *policer-name* [**single** | **hierarchy** | **aggregate**]	创建流量监管模板，并进入流量监管模板配置模式。
3	Inspur(traffic-policer)#**cir** *cir* **cbs** *cbs*	（可选）配置 Flow 模式令牌桶的参数。 **说明** Flow 模式令牌桶是单令牌桶，只支持配置红色和绿色报文动作。
4	Inspur(traffic-policer)#**cir** *cir* **cbs** *cbs* **ebs** *ebs*	（可选）配置 RFC2697 模式令牌桶的参数。
5	Inspur(traffic-policer)#**cir** *cir* **cbs** *cbs* **pir** *pir* **pbs** *pbs*	（可选）配置 RFC2698 模式令牌桶的参数。
6	Inspur(traffic-policer)#**cir** *cir* **cbs** *cbs* **eir** *eir* **ebs** *ebs* [**coupling**]	（可选）配置 RFC4115 模式或 MEF 令牌桶的参数。
7	Inspur(traffic-policer)#**color-mode** { **aware** | **blind** }	（可选）配置令牌桶的感色模式。
8	Inspur(traffic-policer)#**drop-color** { **red** [**yellow**] | **yellow** }	（可选）配置令牌桶丢弃带颜色的报文。

步骤	配置	说明
9	Inspur(traffic-policer)#**recolor green-recolor** { **yellow** | **red** } [**yellow-recolor** { **green** | **red** }] [**red-recolor** { **green** | **yellow** }] Inspur(traffic-policer)#**recolor red-recolor** { **green** | **yellow** } Inspur(traffic-policer)#**recolor yellow-recolor** { **green** | **red** } [**red-recolor** { **green** | **yellow** }]	（可选）配置报文重着色。
10	Inspur(traffic-policer)#**set-cos** { **green** *cos* [**yellow** *cos*] [**red** *cos*] | **red** *cos* | **yellow** *cos* [**red** *cos*] }	（可选）配置报文颜色到 CoS 值的映射。
11	Inspur(traffic-policer)#**set-dscp** { **green** *green-value* [**yellow** *yellow-value*] [**red** *red-value*] | **red** *red-value* | **yellow** *yellow-value* [**red** *red-value*] }	（可选）配置报文颜色到 DSCP 值的映射。
12	Inspur(traffic-policer)#**set-pri** { **green** *green-value* [**yellow** *yellow-value*] [**red** *red-value*] | **red** *red-value* | **yellow** *yellow-value* [**red** *red-value*] }	（可选）配置报文颜色到本地优先级的映射。

8.5.6 创建流策略

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**policy-map** *policy-map-name*	创建流策略，并进入 pmap 配置模式。
3	Inspur(config-pmap)#**description** *string*	（可选）描述流策略信息。

8.5.7 定义流策略映射

说明

可以将一个或多个已经定义的流分类定义成一个流策略。

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**policy-map** *policy-map-name*	创建流策略，并进入 pmap 配置模式。
3	Inspur(config-pmap)#**class-map** *class-map-name*	将流分类绑定到流策略中，只对匹配流分类的报文采用该流策略。 **说明** 绑定流策略的流分类需要基于至少一类规则，否则无法成功绑定。

8.5.8 定义流策略动作

说明

对策略中不同流定义不同的动作。

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**policy-map** *policy-map-name*	创建流策略并进入 pmap 配置模式。
3	Inspur(config-pmap)#**class-map** *class-map-name*	将流分类绑定到流策略中，只对匹配流分类的报文采用该流策略。 **说明** 绑定流策略的流分类需要基于至少一类规则，否则无法成功绑定。
4	Inspur(config-pmap-c)#**police** *policer-name* [**hierarchy-police** *hierarchy-police-name* **mode** { **and** | **or** }]	（可选）在流策略上应用令牌桶，进行流量限速和整形。 **说明** 应用的令牌桶需要事先进行创建，并配置限速和整形规则，否则无法应用成功。
5	Inspur(config-pmap-c)#**redirect-to** { *interface-type interface-number* | **next-hop** *next-hop-ipaddress* }	（可选）在流分类下配置重定向规则，将匹配流分类的报文从指定接口转发。
6	Inspur(config-pmap-c)#**set** { **cos** *cos-value* | **dscp** *dscp-value* | **local-priority** *value* | **vlan** *vlan-id* | **inner-vlan** *inner-vlan-id* }	（可选）在流分类下配置重标记规则，修改匹配该流分类的报文 CoS 优先级、本地优先级、内层 VLAN、DSCP 优先级、IP 优先级或 VLAN ID。

步骤	配置	说明
7	Inspur(config-pmap-c)#**copy-to-mirror** *mirror-id*	（可选）配置流镜像到监控接口。
8	Inspur(config-pmap-c)#**statistics enable**	（可选）在流分类下配置流量统计规则，对匹配流分类的报文流量进行统计。
9	Inspur(config-pmap-c)#**forward-to-cpu**	（可选）配置流转发至 CPU。

8.5.9 将流策略应用到接口上

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或 VLAN 接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**service-policy** { **ingress** | **egress** } *policy-map-name*	将配置好的流策略应用到接口上。
4	Inspur(config-gigaethernet1/1/*)#**exit**	返回到全局配置模式。
5	Inspur(config)#**interface port-channel** *channel-number*	进入聚合组接口配置模式。
6	Inspur(config-port-channel*)#**service-policy ingress** *policy-map-name*	将配置好的流策略应用到接口上。
7	Inspur(config-port-channel*)#**exit**	返回到全局配置模式。
8	Inspur(config)#**service-policy** { **ingress** | **egress** } *policy-map-name* **vlanlist** *vlan-list*	在 VLAN 下应用流策略。

8.5.10 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show service-policy statistics interface** { *interface-type interface-number* | **vlan** *vlan-id* } { **ingress** | **egress** } [**class-map** *class-map-name*]	查看已应用的流策略统计信息。

序号	检查项	说明
2	Inspur#**show service-policy interface** [{ *interface-type interface-number* | **vlan** *vlan-id* } [**ingress** | **egress**]]	查看已应用的流策略信息。
3	Inspur#**show class-map** [*class-map-name*]	查看流分类信息。
4	Inspur#**show policy-map** [*policy-map-name*]	查看流策略信息。
5	Inspur#**show policy-map** [*policy-map-name*] [**class** *class-map-name*]	查看流策略中的流分类信息。
6	Inspur#**show mls qos policer** [*policer-name*]	查看指定的令牌桶（流量限速和整形）信息。

8.5.11 维护

用户可以通过以下命令，维护二层组播特性的运行情况和配置情况。

命令	描述
Inspur(config)#**clear service-policy statistics interface** *interface-type interface-number* { **ingress** | **egress** }	清除流策略的统计信息。

8.6 配置流量限速

8.6.1 配置准备

场景

为避免网络发生拥塞或缓解网络拥塞状况，用户可以配置基于接口的流量限速。通过限制某一接口的突发流量，使之以比较均匀的速率发送。

前提

无

8.6.2 配置基于接口的流量限速

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**interface** *interface-type interface-number*	进入接口配置模式。以下步骤以物理接口配置模式为例。
3	Inspur(config-gigaethernet1/1/*)#**rate-limit** { **egress** | **ingress** } **cir** *cir-value* **cbs** *cbs-value*	配置基于接口的流量限速。
4	Inspur(config)#**rate-limit mode** { **l1** | **l2** }	配置流量限速的工作模式。

说明

- 缺省情况下，未配置接口的带宽限制。
- 入接口限速资源超过设定的限速值后的处理方式 drop 丢弃。
- 接口配置限速值和突发值时，在配置的限速值小于 256kbit/s 时，突发值设置不能太大，否则会出现不连续的情况。
- 限速值很小时，建议限速值和突发值在数字上成 4 倍的关系，如果出现了报文不连续的情况，此时请减小突发值，或者增大限速值。
- 出接口的限速丢包会统计到入接口的丢包统计上。
- 聚合组接口模式下不支持出方向的流量限速。

8.6.3 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show rate-limit interface** [{ *interface-type interface-number* | **vlan** *vlan-id* } [**ingress** | **egress**]]	查看基于接口的流量限速。
2	Inspur#**show rate-limit mode**	查看接口的带宽限速模式。

8.7 带宽限速

8.7.1 配置准备

场景

带宽限速功能主要用来保证用户对业务带宽的要求，并保护网络资源和运营商的利益。

前提

无

8.7.2 带宽限速功能的缺省配置

设备上带宽限速功能的缺省配置如下。

功能	缺省值
颜色识别	禁用

8.7.3 配置带宽保证功能

创建带宽保证模板

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**bandwidth-profile** *bwp-profile-id* **cir** *cir* **cbs** *cbs* [**color-aware**] Inspur(config)#**bandwidth-profile** *bwp-profile-id* **cir** *cir* **cbs** *cbs* [**eir** *eir* **ebs** *ebs*] [**color-aware** [**coupling**]]	创建带宽保证模板。
3	Inspur(config)#**bandwidth-profile** *bwp-profile-id* **description** *word*	配置带宽保证模板的描述信息。
4	Inspur(config)#**interface** *interface-type interface-number* Inspur(config-gigaethernet1/1/*)#**bandwidth** { **egress** | **ingress** } *bwp-profile-id*	在端口上应用带宽保证模板。
5	Inspur(config-gigaethernet1/1/*)#**bandwidth color-aware** { **enable** | **disable** }	使能带宽保证端口入方向报文的颜色识别功能，使用 **disable** 格式禁止该功能。

配置端口+VLAN 带宽保证

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**bandwidth-profile** *bwp-profile-id* **cir** *cir* **cbs** *cbs* [**eir** *eir* **ebs** *ebs*] [**color-aware**]	创建带宽保证模板。
3	Inspur(config)#**interface** *interface-type interface-number* Inspur(config-gigaethernet1/1/*)#**bandwidth** { **egress** | **ingress** } **vlan** *vlan-id bwp-profile-id*	在端口+VLAN 上应用带宽保证模板。

配置端口+VLAN+CoS 带宽保证

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**bandwidth-profile** *bwp profile-id* **cir** *cir* **cbs** *cbs* [**eir** *eir* **ebs** *ebs*] [**color-aware**]	创建带宽保证模板。
3	Inspur(config)#**interface** *interface-type interface-number* Inspur(config-gigaethernet1/1/*)#**bandwidth** { **egress** | **ingress** } [**vlan** *vlan-id*] **coslist** *cos-value-list bwp-profile-id*	在端口+VLAN+CoS 上应用带宽保证模板。

说明

当删除带宽保证模板时，如果该模板被其它分层模板引用或该模板已被应用，则不能删除。

配置 VLAN 接口下的带宽保证

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**bandwidth-profile** *bwp-profile-id* **cir** *cir* **cbs** *cbs* [**eir** *eir* **ebs** *ebs*] [**color-aware** [**coupling**]]	创建带宽保证模板。
3	Inspur(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式。

步骤	配置	说明
4	Inspur(config-vlan*)#**bandwidth** { **ingress** | **egress** } *bwp-profile-id*	在 VLAN 接口上应用带宽保证模板。
5	Inspur(config-vlan*)#**bandwidth** { **ingress** | **egress** } **coslist** *cos-value-list bwp-profile-id*	在端口+VLAN 上应用带宽保证模板。

8.7.4 配置分层带宽保证功能

配置分层 CoS 带宽保证

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**bandwidth-profile** *profile-id* **cir** *cir* **cbs** *cbs* [**eir** *eir* **ebs** *ebs*] [**color-aware**]	创建带宽保证模板。
3	Inspur(config)#**hierarchy-cos bandwidth-profile** *hc-profile-id*	创建分层 CoS 模板并进入 HCoS 配置模式。
4	Inspur(config-hcos)#**bandwidth coslist** *cos-list bwp-profile-id* Inspur(config-hcos)#**exit**	配置分层 CoS 模板信息。
5	Inspur(config)#**interface** *interface-type interface-number* Inspur(config-gigaethernet1/1/*)#**bandwidth ingress vlan** *vlan-id bwp-profile-id* **hierarchy-cos** *hc-profile-id*	在入接口+VLAN 上应用分层 CoS 模板。

配置分层 VLAN 带宽保证

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**bandwidth-profile** *profile-id* **cir** *cir* **cbs** *cbs* [**eir** *eir* **ebs** *ebs*] [**color-aware**]	创建带宽保证模板。
3	Inspur(config)#**hierarchy-vlan bandwidth-profile** *hv-profile-id*	创建分层 VLAN 模板并进入 HVLAN 配置模式。
4	Inspur(config-hvlan)#**bandwidth vlanlist** *vlan-list profile-id* Inspur(config-hvlan)#**exit**	配置分层 VLAN 模板信息。

步骤	配置	说明
5	Inspur(config)#**interface** *interface-type interface-number* Inspur(config-gigaethernet1/1/*)#**bandwidth ingress** *bwp-profile-id* **hierarchy-vlan** *hv-profile-id*	在入接口上应用分层 VLAN 模板。

说明

如果分层带宽保证模板已被应用，则不能删除或修改。

8.7.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show bandwidth-profile** [*bwp-profile-id*]	查看带宽保证模板信息。
2	Inspur#**show bandwidth interface** *interface-type interface-number*	查看端口的带宽保证配置信息。
3	Inspur#**show hierarchy-cos-bandwidth profile** [*hc-profile-id*]	查看分层 CoS 带宽保证模板信息。
4	Inspur#**show hierarchy-vlan-bandwidth profile** [*hv-profile-id*]	查看分层 VLAN 带宽保证模板信息。

8.8 配置举例

8.8.1 配置拥塞管理示例

组网需求

如图 8-9 所示，来自 User 的业务类型有语音、视频和数据。

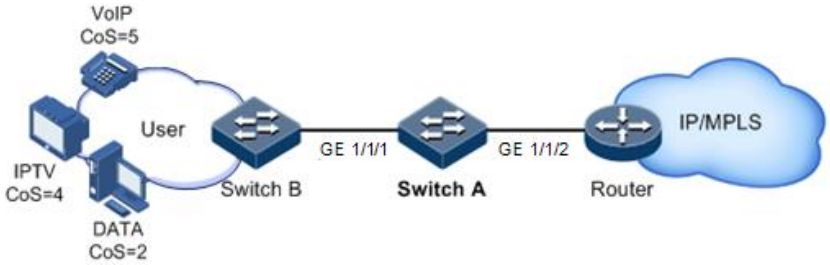
语音业务的 CoS 优先级为 5，视频业务的 CoS 优先级为 4，数据业务的 CoS 优先级为 2。这三类业务的本地优先级分别映射为 6、5、2。

在 Switch A 处容易发生拥塞，为了减轻网络拥塞造成的影响，根据不同的业务类型，需要制定如下规则：

- 对于语音业务，需要对其进行 SP 调度，优先保证这部分流量通过；
- 对于视频业务，需要对其进行 WRR 调度，权重值为 50；

- 对于数据业务，需要对其进行 WRR 调度，权重值为 20。

图8-9 配置队列调度组网示意图



配置步骤

步骤 1 配置接口优先级信任模式。

```
Inspur#hostname SwitchA
SwitchA#config
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#mls qos trust cos
SwitchA(config-gigaethernet1/1/2)#quit
```

步骤 2 配置 CoS 优先级和本地优先级的映射模板。

```
SwitchA(config)#mls qos mapping cos-to-local-priority 1
SwitchA(cos-to-pri)#cos 5 to local-priority 6
SwitchA(cos-to-pri)#cos 4 to local-priority 5
SwitchA(cos-to-pri)#cos 2 to local-priority 2
SwitchA(cos-to-pri)#quit
```

步骤 3 配置在 GE 1/1/2 应用 CoS 到本地优先级映射模板。

```
SwitchA(config)#interface gigaethernet1/1/2
SwitchA(config-gigaethernet1/1/2)#mls qos cos-to-local-priority 1
SwitchA(config-gigaethernet1/1/2)#quit
```

步骤 4 配置在 GE 1/1/1 出方向进行 SP+WRR 队列调度。

```
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#mls qos queue scheduler wrr 1 1 20 1 1
50 0 0
SwitchA(config-gigaethernet1/1/1)#quit
```

检查结果

查看接口优先级信任模式。

```
Inspur#show mls qos interface
Interface                TrustMode  Priority    Cos-PriProfile Dscp-
PriProfile Dscp-Mutation Cos-Remark DEI-Status
-------------------------------------------------------------------------
-----------------------------------------
```

```
gigaethernet1/1/1           cos       untagged 0   0           0
0           0        --
gigaethernet1/1/2           cos       untagged 0   1           0
0           0        --
```

查看 CoS 优先级和本地优先级的映射关系配置是否正确。

```
Inspur#show mls qos mapping cos-to-local-priority
G:GREEN
Y:YELLOW
R:RED
cos-to-localpriority(color)
Index Description    Ref   CoS:           0      1      2      3      4
5      6      7
--------------------------------------------------------------------------------
--------------------------------
1                  1    localpri(color) :0(G)   1(G)   2(G)   3(G)
5(G)   6(G)   6(G)   7(G)
```

查看接口上队列调度方式配置是否正确。

```
Inspur#show mls qos queue interface gigaethernet 1/1/1
gigaethernet1/1/1
Queue    Weight(WRR)
-------------------------
  1       1
  2       1
  3       20
  4       1
  5       1
  6       50
  7       0
  8       0
```

8.8.2 配置基于流策略的流量限速示例

组网需求

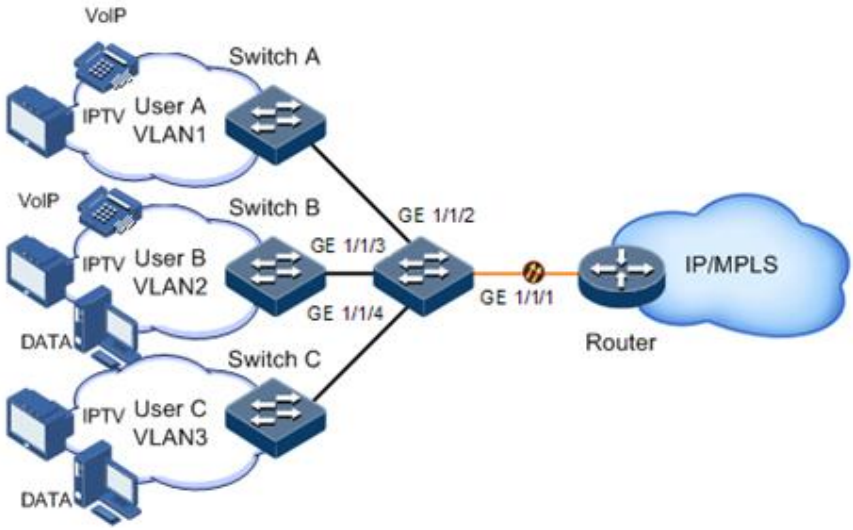
如图 8-10 所示，User A、User B、User C 分别属于 VLAN1、VLAN2、VLAN3，且分别通过 Switch A、Switch B、Switch C 和交换机相连。

来自 User A 的业务类型有语音和视频，来自 User B 的业务类型有语音、视频和数据，来自 User C 的业务类型有视频和数据。

根据各用户的业务需求，需要制定如下规则：

- 对于 User A，须为其提供保证带宽 25Mbit/s，突发流量允许 100kB，丢弃多余的流量；
- 对于 User B，须为其提供保证带宽 35Mbit/s，突发流量允许 100kB，丢弃多余的流量；
- 对于 User C，须为其提供保证带宽 30Mbit/s，突发流量允许 100kB，丢弃多余的流量。

图8-10 配置基于流策略的流量限速组网示意图



配置步骤

步骤 1 创建并配置流分类，对不同的用户依据 VLAN ID 进行分类。

```
Inspur#config
Inspur(config)#class-map usera match-any
Inspur(config-cmap)#match vlan 1
Inspur(config-cmap)#quit
Inspur(config)#class-map userb match-any
Inspur(config-cmap)#match vlan 2
Inspur(config-cmap)#quit
Inspur(config)#class-map userc match-any
Inspur(config-cmap)#match vlan 3
Inspur(config-cmap)#quit
```

步骤 2 创建流量限速规则。

```
Inspur(config)#mls qos policer-profile usera single
Inspur(traffic-policer)#cir 25000 cbs 100
Inspur(traffic-policer)##quit
Inspur(config)#mls qos policer-profile userb single
Inspur(traffic-policer)#cir 35000 cbs 100
Inspur(traffic-policer)##quit
Inspur(config)#mls qos policer-profile userc single
Inspur(traffic-policer)#cir 30000 cbs 100
Inspur(traffic-policer)##quit
```

步骤 3 创建并配置流策略。

```
Inspur(config)#policy-map usera
Inspur(config-pmap)#class-map usera
Inspur(config-pmap-c)#police usera
Inspur(config-pmap-c)#quit
Inspur(config-pmap)#quit
Inspur(config)#interface gigaethernet 1/1/1
```

```
Inspur(config-gigaethernet1/1/1)#service-policy ingress usera
Inspur(config-gigaethernet1/1/1)#exit
Inspur(config)#policy-map userb
Inspur(config-pmap)#class-map userb
Inspur(config-pmap-c)#police userb
Inspur(config-pmap-c)#quit
Inspur(config-pmap)#quit
Inspur(config)#interface gigaethernet 1/1/2
Inspur(config-gigaethernet1/1/2)#service-policy ingress userb
Inspur(config-gigaethernet1/1/1)#exit
Inspur(config)#policy-map userc
Inspur(config-pmap)#class-map userc
Inspur(config-pmap-c)#police userc
Inspur(config-pmap-c)#quit
Inspur(config-pmap)#quit
Inspur(config)#interface gigaethernet 1/1/3
Inspur(config-gigaethernet1/1/3)#service-policy userc ingress 4
Inspur(config-gigaethernet1/1/1)#exit
```

检查结果

通过 **show class-map** 命令查看流分类配置是否正确。

```
Inspur#show class-map usera
Class Map match-any usera (id 0)(ref 1)
    Match vlan 1
Inspur#show class-map userb
 Class Map match-any userb (id 1)(ref 1)
    Match vlan 2
Inspur#show class-map userc
 Class Map match-any userb (id 2)(ref 1)
    Match vlan 3
```

通过 **show mls qos policer** 查看流量限速规则配置是否正确。

```
Inspur(config)#show mls qos policer
single-policer: USERC        mode:flow   color:blind
cir: 30000 kbps  cbs: 100 kB

single-policer: usera        mode:flow   color:blind
cir: 25000 kbps  cbs: 100 kB

single-policer: userb        mode:flow   color:blind
cir: 35000 kbps  cbs: 100 kB
```

通过 **show policy-map** 查看流策略配置是否正确。

```
Inspur(config)#show policy-map
  Policy Map usera
    Class usera
        police usera

  Policy Map userb
    Class userb
        police userb
```

```
Policy Map userc
  Class userc
      police userc
```

8.8.3 配置基于接口的流量限速示例

组网需求

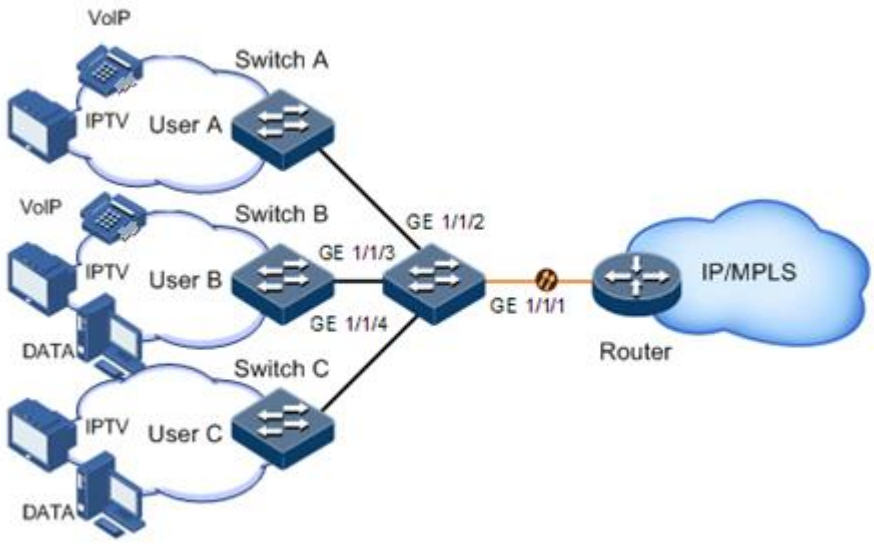
如图 8-11 所示，User A、User B、User C 分别通过 Switch A、Switch B、Switch C 和交换机相连。

来自 User A 的业务类型有语音和视频，来自 User B 的业务类型有语音、视频和数据，来自 User C 的业务类型有视频和数据。

根据各用户的业务需求，需要制定如下规则：

- 对于 User A，须为其提供保证带宽 25M，突发流量允许 100kB，丢弃多余的流量；
- 对于 User B，须为其提供保证带宽 35M，突发流量允许 100kB，丢弃多余的流量；
- 对于 User C，须为其提供保证带宽 30M，突发流量允许 100kB，丢弃多余的流量。

图8-11 配置基于接口的流量限速组网示意图



配置步骤

步骤 1 配置基于接口的流量限速。

```
Inspur#config
```

```
Inspur(config)#interface gigaethernet 1/1/1
Inspur(config-gigaethernet1/1/1)#rate-limit ingress cir 25000 cbs 100
Inspur(config-gigaethernet1/1/1)#exit
Inspur(config)#interface gigaethernet 1/1/2
Inspur(config-gigaethernet1/1/2)#rate-limit ingress cir 35000 cbs 100
Inspur(config-gigaethernet1/1/2)#exit
Inspur(config)#interface gigaethernet 1/1/3
Inspur(config-gigaethernet1/1/3)#rate-limit ingress cir 30000 cbs 100
Inspur(config-gigaethernet1/1/3)#exit
```

检查结果

通过 **show rate-limit interface** 命令查看基于接口的流量限速配置是否正确。

```
Inspur(config)#show rate-limit interface
Interface            Direction Cir(kbps)        Cbs(kb)
CirOper(kbps)         CbsOper(kb)
------------------------------------------------------------------------------
---------------------------------------
gigaethernet1/1/1     ingress   25000            100            25024
101
gigaethernet1/1/2     ingress   35000            100            30016
101
gigaethernet1/1/3     ingress   30000            100            30016
101
```

9 组播

本章介绍了组播特性的原理和配置过程，并提供相关的配置案例。

- 组播概述
- IGMP
- 二层组播基础
- IGMP Snooping
- IGMP MVR
- 配置 IGMP 过滤
- 组播 VLAN 复制
- MLD
- PIM-SM

9.1 组播概述

随着 Internet 网络的不断发展，一方面网络中交互的各种数据、语音和视频信息越来越多；另一方面新兴的电子商务、网上会议、网上拍卖、视频点播、远程教学等服务逐渐兴起，这些服务对网络带宽、信息安全性和有偿性提出了更高的要求。传统的单播和广播方式无法很好的满足这些要求，组播及时满足了这些需求。

组播（Multicast）是一种点到多点的数据传输方式。组播技术能够有效地解决单点发送，多点接收的问题，在网络数据传输时，能够节约网络资源，提高信息安全性。

三种通信方式的比较

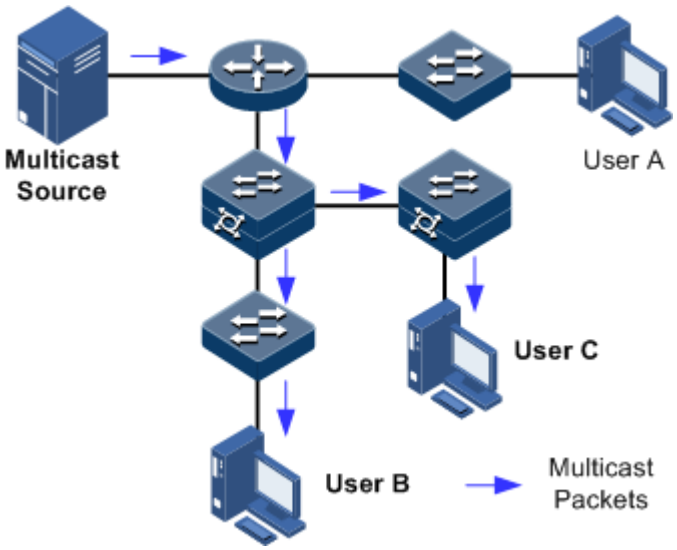
组播是与单播、广播并列的通信方式：

- 单播方式：系统为每个需要信息的用户单独建立一条数据传送通路，并为该用户发送一份独立的拷贝信息。利用单播方式，网络中传输的信息量和需要该信息的用户量成正比，因此当需要该信息的用户量庞大时，网络中将出现多份相同信息。此时，带宽将成为重要瓶颈，单播方式不利于信息规模化发送。
- 广播方式：系统把信息传送给网络中的所有用户，不管他们是否需要，任何用户都会接收到广播来的信息。利用广播方式，信息源将把信息传递给网段中所有用户，用户信息安全性和有偿服务得不到保障。另外，当同一网络中需要该信息的用户量很小时，网络资源利用率将非常低，带宽浪费严重。

- 组播方式：当网络中的某些用户需求特定信息时，组播信息发送者仅发送一份信息，被传递的信息在尽可能远的分叉路口才开始复制和分发。

组播方式传输如图 9-1 所示。假设用户 B、C 需要信息，采用组播方式传输，将用户 B、C 组成一个接收者集合，信息源只需发送一份信息，由网络中各交换机根据 IGMP 报文建立自己的组播转发表，信息只传输给实际需要的接收者 B、C。

图9-1 组播方式传输信息示意图



综上所述，单播方式适合用户稀少的网络，广播方式适合用户稠密的网络，当网络中需要某信息的用户量不确定时，单播和广播方式效率很低。组播方式传输，用户数量成倍增长时，主干带宽不需要随之增加，而且只将信息传递给需要的用户，这些优点使它成为当前网络技术中的研究热点之一。

组播优势与应用

与单播和广播通信方式相比，组播的优势主要在于：

- 提高效率：降低网络流量，减轻了服务器和 CPU 负荷。
- 优化性能：减少冗余量，保障了信息的安全性。
- 分布式应用：解决了点到多点数据传输问题。

组播技术主要应用在以下几个方面：

- 多媒体、流媒体的应用，如：网络电视、网络电台、实时视/音频会议。
- 培训、联合作业场合的通信，如：远程教育、远程医疗。
- 数据仓库、金融应用（股票）。
- 其它任何“点到多点”的应用。

组播中的基本概念

介绍组播中的基本概念：

- 组播组

组播组是指使用一个 IP 组播地址标识的接收者集合。任何用户主机（或其他接收设备）加入一个组播组，就成为了该组成员，可以识别并接收以该 IP 组播地址为目的地址的组播数据。

- 组播组成员

所有加入某组播组的主机便成为该组播组的成员。组播组中的成员是动态的，主机可以在任何时刻加入或离开组播组。组成员可能广泛分布在网络中的任何地方。

- 组播源

以组播组地址为目的地址，发送 IP 报文的信源称为组播源。一个组播源可以同时向多个组播组发送数据，多个组播源可以同时向一个组播组发送数据。

- 组播路由器

在组播传输中提供三层组播功能的路由器。组播路由器能够实现组播路由，指导组播报文转发，也能够在与用户连接的末梢网段上提供组播组成员管理功能。

- 路由器接口

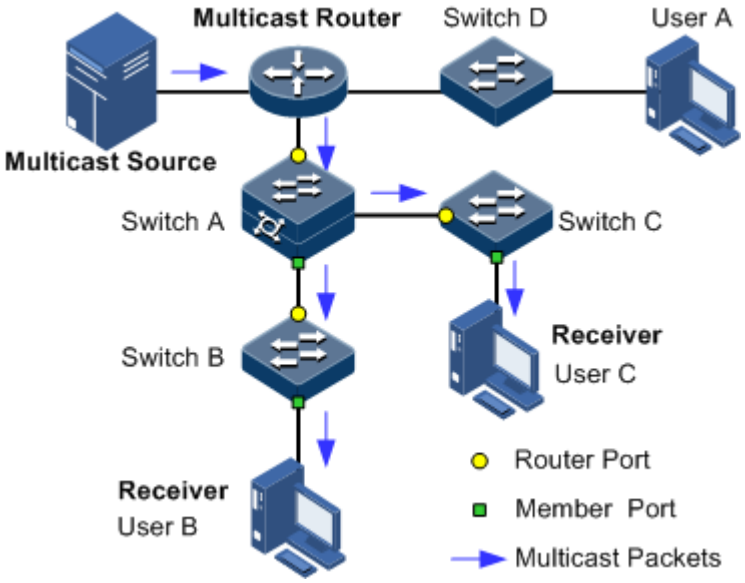
是指组播路由器和主机之间的设备上，朝向组播路由器的接口，设备从该接口接收组播报文。

- 成员接口

也称接收接口，是指组播路由器和主机之间的设备上，朝向主机的接口，设备从该接口发出组播报文。

组播基本概念中路由器接口，成员接口位置标示如图 9-2 所示。

图9-2 组播基本概念在网络中相应位置标示示意图



组播地址

为了让组播源和组播组成员进行通信，需要提供网络层组播地址和链路层组播地址，即 IP 组播地址和组播 MAC 地址。需要注意的是组播地址都只能作为目的地址，而不能作为源地址来使用。

- IP 组播地址

IANA（Internet Assigned Numbers Authority，互联网编号分配委员会）将 D 类地址空间分配给 IPv4 组播使用，IPv4 组播地址范围 224.0.0.0～239.255.255.255。

- 组播 MAC 地址

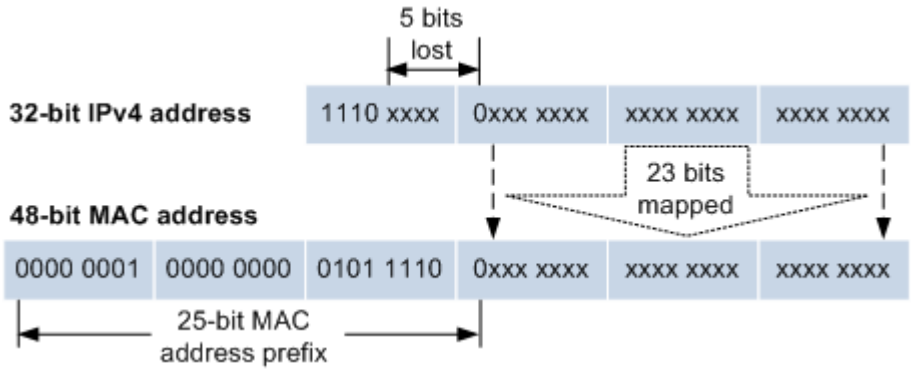
以太网传输单播 IP 报文时，目的 MAC 地址使用的是接收者的 MAC 地址。但是在传输组播数据包时，其目的地不再是一个具体的接收者，而是一个成员不确定的组，所以要使用组播 MAC 地址。

组播 MAC 地址用于在链路层上标识属于同一组播组的接收者。

IANA 规定，组播 MAC 地址的高 24 位为 0x01005E，第 25 位为 0，低 23 位为 IPv4 组播地址的低 23 位。

IP 组播地址和 MAC 地址以一种映射关系相关联，映射关系如图 9-3 所示。

图9-3 IPv4 组播地址和组播 MAC 地址的映射关系



由于 IP 组播地址的前 4 位是 1110，代表组播标识，而后 28 位中只有 23 位被映射到 MAC 地址，这样 IP 地址中就有 5 位信息丢失，可能导致 32 个 IP 组播地址映射到同一 MAC 地址上。因此在二层处理过程中，设备可能要接收一些本 IPv4 组播组以外的组播数据，而这些多余的组播数据就需要设备的上层进行过滤了。

组播协议基础

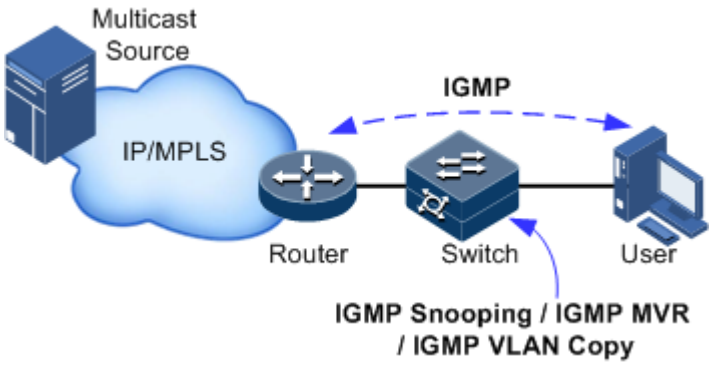
实现一套完整的组播服务，需要在网络各个位置部署多种组播协议相互配合，共同运作。

通常，把工作在网络层的 IP 组播称为“三层组播”，相应的组播协议称为“三层组播协议”，包括 IGMP（Internet Group Management Protocol，因特网组管理协议）等；把工作在数据链路层的 IP 组播称为“二层组播”，相应的组播协议称为“二层组播协

议”，包括 IGMP Snooping（Internet Group Management Protocol Snooping，因特网组管理协议监听）等。

IGMP 和二层组播特性运行位置如图 9-4 所示。

图9-4 IGMP 和二层组播特性运行位置示意图



IGMP 是 TCP/IP 协议族中负责 IPv4 组播成员管理的协议。IGMP 运行在组播路由器和主机之间，该协议定义了主机与组播路由器之间建立、维护组播组成员关系的机制。IGMP 不包括组播路由器之间的组成员关系信息的传播与维护，这部分工作由组播路由协议完成。

IGMP 通过在主机和组播路由器之间交互 IGMP 报文实现组成员管理功能。IGMP 报文封装在 IP 报文中，IGMP 报文类型有 Query 查询报文、Report 报告报文和 Leave 离开报文。IGMP 基本功能：

- 主机发送 Report 报文加入组播组，发送 Leave 报文离开组播组，自主决定接收哪些组播组的报文。
- 组播路由器周期发送 Query 报文，并接收主机反馈的 Report 报文和 Leave 报文，了解连接的网段上有哪些组播组成员。如果有组播组成员，应将组播数据转发到这个网段；如果没有组播组成员则不转发。

到目前为止，IGMP 有三个版本：IGMPv1 版本、IGMPv2 版本和 IGMPv3 版本，新版本完全兼容旧版本。目前应用最广泛的是 IGMPv2，其中 Leave 报文 IGMPv1 版本不支持。

二层组播运行在主机和组播路由器之间的二层设备上。

二层组播通过监听和分析主机和组播路由器之间交互的 IGMP 报文来管理和控制组播组，实现组播数据在二层的转发，抑制组播数据在二层网络中的扩散。

设备支持的组播特性

目前设备支持的组播特性：

- IGMP 基础功能
- IGMP Snooping
- IGMP MVR（Multicast VLAN Registration，组播 VLAN 注册）

- IGMP 过滤

说明

设备上 IGMP Snooping 和 IGMP MVR 或组播 VLAN 复制功能不能在同一组播 vlan 下使能；组播 VLAN 复制和 IGMP MVR 不能在同一组播 vlan 的同组播组下同时使能。

设备同时支持 IGMPv1，IGMPv2，IGMPv3。

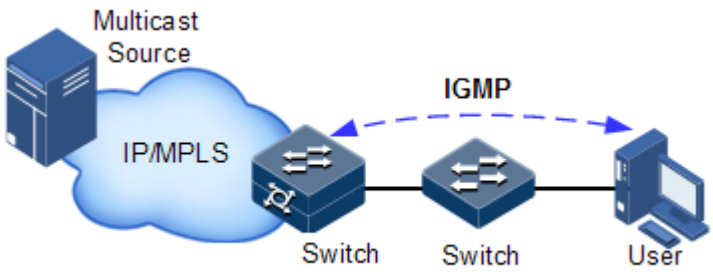
9.2 IGMP

9.2.1 简介

IGMP 是 TCP/IP 协议族中负责 IPv4 组播成员管理的协议。IGMP 运行在组播路由器和主机之间，该协议定义了主机与组播路由器之间建立、维护组播组成员关系的机制。IGMP 不包括组播路由设备之间的组成员关系信息的传播与维护，这部分工作由组播路由协议完成。

IGMP 通过在主机和组播路由设备之间交互 IGMP 报文实现组成员管理功能，IGMP 在网络中的运行位置如图 9-5 所示。

图9-5 IGMP 运行位置示意图



IGMP 报文封装在 IP 报文中，IGMP 报文类型有 Query 查询报文、Report 报告报文和 Leave 离开报文。IGMP 基本功能：

- 主机发送 Report 报文加入组播组，发送 Leave 报文离开组播组，自主决定接收哪些组播组的报文。
- 组播路由器周期发送 Query 报文，并接收主机反馈的 Report 报文和 Leave 报文，了解连接的网段上有哪些组播组成员。如果有组播组成员，应将组播数据转发到这个网段；如果没有组播组成员则不转发。

到目前为止，IGMP 有三个版本：IGMPv1 版本、IGMPv2 版本和 IGMPv3 版本，新版本完全兼容旧版本。目前应用最广泛的是 IGMPv2，其中 Leave 报文 IGMPv1 版本不支持。设备同时支持 IGMPv1，IGMPv2。

与 IGMP 有关的概念介绍如下。

报文查询间隔

查询器周期性地发送 IGMP 普通组查询报文，以判断网络上是否有组播组成员。可以根据网络的实际情况来配置发送 IGMP 普通组查询报文的时间间隔。

查询报文最大响应时间

查询报文最大响应时间用于控制主机反馈组成员关系报告的最后期限。主机收到查询报文后，会为其加入的每个组播组都启动一个定时器，其值在 0～“最大响应时间”中随机选定，当定时器超时，主机会发出针对该组播组的 Report 报文。

最后成员查询间隔

也称特定组查询时间间隔。交换机在收到主机发送的针对某个组的 IGMP Leave 报文时，周期性地发送针对特定组的查询报文。

特定组查询报文询问该组播组是否存在成员，如果接口下存在该组的成员，则成员必须在最大响应时间内发送 Report 报文，交换机在指定时间内收到主机发送的 Report 报文，就继续维护该组的组播转发表项，否则认为该接口下该组的最后一个成员已经离开，删除该组的组播转发表项。

健壮系数

健壮系数是指查询器发送 IGMP 特定组查询报文的次数，即为了防止可能发生的网络丢包而设置的报文重传次数。健壮系数越大，IGMP 查询器就越“健壮”，但是组播组超时所需的时间也就越长。

查询者超时时间

查询者超时时间是指当一个组播路由设备停止发送查询报文后，另一路由设备取代其成为新的查询报文发送者的等待时间。

当一个网段上存在多个组播路由设备时，由查询路由设备（简称查询器）负责在接口上定期发送查询消息，如果在“查询者超时时间”内，其他非查询器收不到查询器的查询消息，就认为原查询器失效，自己可以充当查询器。

9.2.2 配置准备

场景

IGMP 应用在路由设备与用户主机相连的网段，通过在与用户网段相连的组播设备接口上配置 IGMP 功能，用户主机可以接入组播网络，组播报文才能够到达接收者。

主机通过 IGMP 协议通知本地路由设备希望加入并接收某个特定组播组的信息，同时路由设备通过 IGMP 协议周期性地查询网络内某个已知组的成员是否处于活动状态，实现所连网络组成员关系的收集与维护。

前提

在配置 IGMP 功能之前，需完成以下任务：

- 配置接口的网络层属性，使网络连通。
- 使能组播路由功能。

9.2.3 IGMP 的缺省配置

设备上 IGMP 的缺省配置如下。

功能	缺省值
IGMP 功能状态	禁止
健壮系数	2
其他查询者超时时间	255s
最大查询响应时间	10s
IGMP 报文查询间隔	125s
最后成员查询间隔	1s

9.2.4 使能 IGMP 功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式。
3	Inspur(config-vlan*)#**ip igmp version** { **2** | **3** }	配置支持的 IGMP 协议版本。
4	Inspur(config-vlan*)#**ip igmp enable**	使能 VLAN 接口的 IGMP 功能。

9.2.5 配置静态组成员

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式。
3	Inspur(config-vlan*)#**ip igmp static group** *group-address*	在 VLAN 接口上配置静态组成员。

9.2.6 配置 IGMP 报文查询间隔

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式。
3	Inspur(config-vlan*)#**ip igmp query-interval** *period*	配置 IGMP 报文查询间隔。

9.2.7 配置健壮系数

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式。
3	Inspur(config-vlan*)#**ip igmp robustness-variable** *value*	配置健壮系数，即网络丢包产生的报文重传次数。

9.2.8 配置最后成员查询时间

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式。
3	Inspur(config-vlan*)#**ip igmp last-member-query-interval** *interval*	配置最后成员查询间隔，即特定组查询消息之间的时间间隔。该值可以用来调整网络的“离开延时”。

9.2.9 配置最大查询响应时间

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式。
3	Inspur(config-vlan*)#**ip igmp query-max-response-time** *period*	配置最大查询响应时间，该值要比 IGMP 报文查询间隔小。

9.2.10 配置组播成员快速离开功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式。
3	Inspur(config-vlan*)# **ip igmp immediate-leave**	配置组播成员快速离开功能。

9.2.11 配置组播组和组播源的访问控制

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ip igmp ssm-mapping** { *group-ip-address group-ip-mask* | *group-ip-addresss/mask* } *source-ip-address*	配置组播组和组播源的映射规则
3	Inspur(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式。
4	Inspur(config-vlan*)#**ip igmp group-policy** *acl-number*	（可选）配置接口加入的组播组范围
5	Inspur(config-vlan*)#**ip igmp ssm-mapping** { **enable** | **disable** }	（可选）使能指定组播组和组播源的映射功能

9.2.12 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show ip igmp group** [*group-address* | **interface ip** *if-number*]	查看组播组成员关系信息。

序号	检查项	说明
2	Inspur#**show ip igmp interface** [**ip** *if-number*]	查看三层接口的 IGMP 配置信息。
3	Inspur#**show ip igmp statistics** [**interface ip** *if-number*]	查看 IGMP 报文统计信息。
4	Inspur#**show ip igmp ssm-mapping group**	查看用户配置的组播组和源的映射关系。

9.2.13 维护

用户可以通过以下命令维护 IGMP 特性。

命令	说明
Inspur(config)#**clear ip igmp statistcs** [**interface ip** *if-number*]	清除 IGMP 报文统计信息。
Inspur(config)#**clear ip igmp group** [*group-address* | *interface-type interface-number*]	清除组播转发表。

9.3 二层组播基础

9.3.1 简介

二层组播基础功能包含：

- 指定组播路由器接口；
- 使能立即离开功能；
- 设置组播转发表项和路由器接口的老化时间；
- 使能接口的 IGMP 环网转发功能。

二层组播基础功能提供二层组播的公共特性，需要在设备开启 IGMP Snooping 或 IGMP MVR 功能基础上使用。

说明

基础功能相关内容的配置对 IGMP Snooping 或 IGMP MVR 同时生效。

与二层组播基础功能有关的概念说明。

- 组播路由器接口

在运行组播功能的二层交换机上，可以动态学习（需要在组播路由器上开启组播路由协议，通过 IGMP 查询报文学习）到路由器接口，也可以手工设置，以使下游的组播报告、离开等报文可以转发到该路由器接口。

动态学习到的路由器接口有老化时间，手工配置的路由器接口不会老化。

- 老化时间

设置的老化时间同时作用于组播转发表项的老化时间和路由器接口的老化时间。

在运行组播功能的二层交换机上，每个动态学习到的路由器接口会启动一个定时器，定时器的超时时间为“IGMP Snooping 老化时间”。到达老化时间时未收到 IGMP Query 报文，该路由器接口将被删除；收到 IGMP Query 报文时，更新路由器接口的超时时间。

每条组播转发表项会启动一个定时器，也就是组播成员的老化时间，定时器的超时时间为“IGMP Snooping 老化时间”，到达老化时间时未收到 IGMP Report 报文，该组播成员将会被删除；收到 IGMP Report 报文时，更新组播转发表项的超时时间。

- 立即离开功能

在运行组播功能的二层交换机上，当用户发送 Leave 报文时，并不立即删除对应的组播转发表项，而是等待表项老化时才删除。当下游用户数量较多，并且加入离开比较频繁时，可以打开此功能，这样对应的组播转发表项被快速删除。

说明

立即离开功能只适用于 IGMP v2/v3 版本。

- IGMP 环网转发功能

在运行组播功能的二层交换机上，可以在任何类型的环网接口使能 IGMP 环网转发功能。

使能 IGMP 环网转发功能后，可以实现组播在环网上的备份保护功能，使组播服务更具有稳定性。防止某些链路的故障，引起组播服务的故障。

IGMP 环网转发功能适用的环网类型，包含 RRPS 环、STP/RSTP/MSTP 环和 G.8032 环等。

9.3.2 配置准备

场景

二层组播基础功能提供二层组播的公共特性，需要在设备开启 IGMP Snooping 或 IGMP MVR 功能基础上使用。

前提

在配置二层组播基础之前，需完成以下任务：

- 禁用 snooping 组播 vlan 下的 IGMP MVR 和组播 VLAN 复制功能

- 将相应接口加入 VLAN。

9.3.3 二层组播基础的缺省配置

设备上二层组播基础的缺省配置如下。

功能	缺省值
IGMP 的立即离开功能状态	禁止
组播转发表项老化时间	260s
接口的 IGMP 环网转发功能状态	禁止

9.3.4 配置二层组播基础功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**igmp mrouter vlan** *vlan-id interface-type interface-number*	（可选）配置组播路由接口。
3	Inspur(config)#**igmp member-timeout** { *seconds* | **infinite** }	（可选）配置 IGMP 成员的老化时间。
4	Inspur(config)#**igmp ring** *interface-type interface-number*	（可选）使能接口的 IGMP 环网转发功能。
5	Inspur(config)#**igmp report-suppression**	（可选）使能 Report 抑制功能，报文抑制与 Proxy 配置互斥。
6	Inspur(config)#**igmp version** { **2** | **3** }	（可选）配置 IGMP 的版本
7	Inspur(config)#**igmp snooping mrouter vlan** *vlan-list* **priority** *priority-number*	（可选）配置 IGMP 路由 VLAN 的 CoS 优先级
8	Inspur(config)#**igmp unknown forward-router**	（可选）使能 IGMP 未知组播报文转发到路由端口功能，使用 **no** 格式禁止该功能。
9	Inspur(config)#**igmp forward-router**	（可选）使能 IGMP 已知组播报文转发到路由端口功能，使用 **no** 格式禁止该功能。
10	Inspur(config)#**interface** *interface-type interface-number*	（可选）进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
11	Inspur(config-gigaethernet1/1/*)#**igmp immediate-leave** [**vlan** *vlan-list* | **user-mac**]	（可选）配置立即离开功能。如下游口没有开启立即离开功能，路由口收到 leave 报文，会生依照鲁棒系数计算老化时间离开组超时定时器设置为 GMI(Group Membership Interval)，GMI = (robust-value*lastmember-queryinterval)

9.3.5 检查配置

配置完成后，请在设备上进行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show igmp configuration**	查看 IGMP 基础配置信息
2	Inspur#**show igmp mrouter**	查看组播路由接口配置信息。
3	Inspur#**show igmp immediate-leave** [*interface-type interface-number*]	查看二层组播的立即离开配置信息。
4	Inspur#**show igmp statistics** [*interface-type interface-number*]	查看二层组播统计信息。
5	Inspur#**show igmp snooping mrouter vlan-priority**	查看 IGMP 路由 VLAN 的 CoS 优先级
6	Inspur#**show igmp ring**	查看 IGMP 环网接口信息
7	Inspur#**show igmp user-mac** [*interface-type interface-number* | **user-vlan** *vlan-id*]	查看 IGMP 的用户 MAC 信息。
8	Inspur#**show igmp user-mac count** [*interface-type interface-number* | **vlan** *vlan-id*]	查看 IGMP 的用户 MAC 数目信息。

9.3.6 维护

用户可以通过以下命令，维护二层组播特性的运行情况和配置情况。

命令	描述
Inspur(config)#**clear igmp statistics** [*interface-type interface-number*]	清除二层组播 IGMP 的统计信息。
Inspur(config)#**no igmp member** *interface-type interface-number*	删除指定组播转发表项。

9.4 IGMP Snooping

9.4.1 简介

IGMP Snooping 是运行在二层设备上的组播约束机制，用于管理和控制组播组，实现二层组播。

IGMP Snooping 允许交换机监听主机和组播路由器之间的 IGMP 会话。当交换机监听到主机发往某个组的 IGMP Report，交换机将主机所在的接口加入到这个组的转发列表中，同样，当转发表项达到老化时间时，就将主机所在的接口从转发表中删除。

IGMP Snooping 利用二层组播转发表进行组播数据转发，当交换机收到组播数据时，会直接根据组播转发表项的相应的接收接口进行转发，并不向所有接口洪泛，因此有效地节省了交换机的带宽。

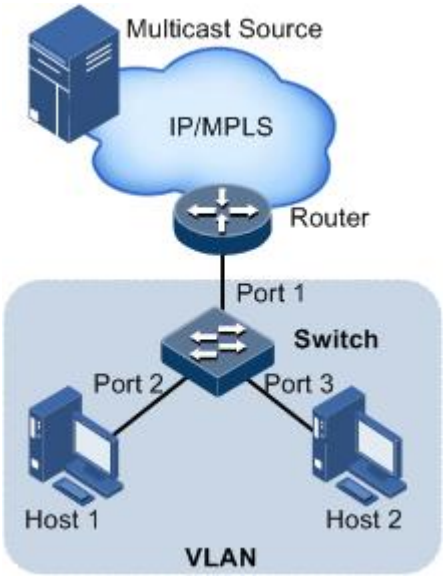
IGMP Snooping 建立二层组播转发表，可以通过 IGMP Snooping 动态学习，也可以进行手工配置。

9.4.2 配置准备

场景

如图 9-6 所示，多个主机接收组播源的数据，多个主机属于同一个 VLAN。可以在组播路由器和主机相连的交换机上运行 IGMP Snooping，通过监听组播路由器和主机之间的 IGMP 报文，建立和维护组播转发表，实现二层组播。

图9-6 IGMP Snooping 应用场景



前提

在配置 IGMP Snooping 之前，需完成以下任务：

- 设备上组播 VLAN 复制功能禁用；
- 创建 VLAN，并将相应接口加入 VLAN。

9.4.3 IGMP Snooping 的缺省配置

设备上 IGMP Snooping 的缺省配置如下。

功能	缺省值
全局 IGMP Snooping 状态	禁用
VLAN 的 IGMP Snooping 状态	禁用
IGMP 的健壮系数	2

9.4.4 配置 IGMP Snooping 功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**igmp snooping**	使能全局 IGMP Snooping。
3	Inspur(config)#**igmp member-timeout** { *seconds* | **infinite** }	（可选）设置 IGMP 成员的老化时间。
4	Inspur(config)#**igmp snooping vlan** *vlan-list*	（可选）配置全局 VLAN 使能 IGMP Snooping 功能。
5	Inspur(config)#**vlan** *vlan-id* Inspur(config-vlan)#**igmp snooping static** *ip-address interface-type interface-number*	（可选）VLAN 模式下配置 IGMP Snooping 的静态成员。
6	Inspur(config)#**interface** *interface-type interface-number* Inspur(config-gigaethernet1/1/*)#**igmp snooping host-join** *group-address* **vlan** *vlan-id*	（可选）配置模拟主机加入功能。

说明

IGMP snooping 和 IGMP MVR 不能在同一组播 vlan 下同时开启，否则配置失败。

IGMP Snooping 和组播 VLAN 复制不能在同一组播 vlan 下同时开启，否则配置失败。

9.4.5 检查配置

配置完成后，请在设备上进行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show igmp snooping** [**vlan** *vlan-id* | **member vlan** *vlan-list* | **mrouter vlan-priority**]	查看 IGMP Snooping 配置信息。
2	Inspur#**show igmp snooping member** [*interface-type interface-number* | **vlan** *vlan-id*]	查看 IGMP Snooping 的组播组成员信息。
3	Inspur#**show igmp snooping member count** [*interface-type interface-number* | **vlan** *vlan-id*]	查看 IGMP Snooping 的组播组成员数目信息。
4	Inspur#**show igmp snooping vlan** *vlan-id*	查看指定 VLAN 下的 IGMP Snooping 的相关配置信息。

9.4.6 配置环网上组播应用示例

组网需求

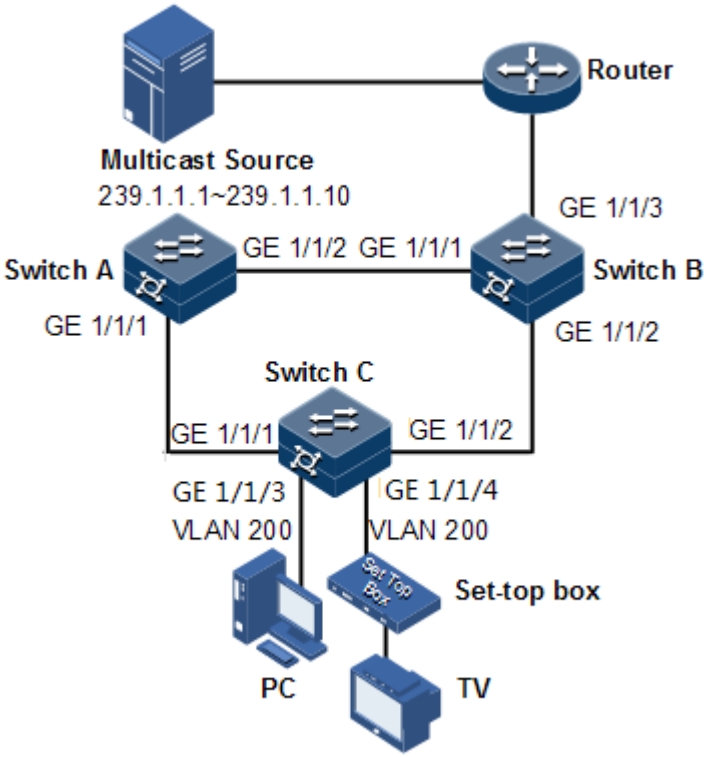
以太网环单环上配置 IGMP 环转发功能，使组播服务更具有稳定性，防止某些链路的故障，引起组播服务的故障。

如图 9-7 所示，Switch A 的 GE 1/1/1 和 GE1/1/2，Switch B 的 GE 1/1/1 和 GE1/1/2，Switch C 的 GE 1/1/1 和 GE 1/1/2 一起构成了物理环网，组播流量从 Switch B 的 Gigaethernet 1/1/1 口引入，客户在 Switch C 的 GE1/1/3 和 GE 1/1/4 点播组播流，这样任意两个交换机之间的链路出现故障，都不会影响客户点播的组播流。

使用以太网单环提供组播服务，可以采用 IGMP MVR 或 IGMP Snooping 功能进行组播流接收。

下面以 STP 提供环网检测、IGMP Snooping 提供组播功能为例进行配置。

图9-7 环网上组播应用组网图



配置步骤

步骤 1 开启 STP 功能，创建 VLAN，并将接口加入 VLAN。

配置 Switch A。

```
SwitchA#config
SwitchA(config)#spanning-tree enable
SwitchA(config)#spanning-tree mode stp
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport mode trunk
SwitchA(config-gigaethernet1/1/1)#switchport trunk native vlan 200
SwitchA(config-gigaethernet1/1/1)#exit
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#switchport mode trunk
SwitchA(config-gigaethernet1/1/2)#switchport trunk native vlan 200
```

配置 Switch B。

```
SwitchB#config
SwitchB(config)#spanning-tree enable
SwitchB(config)#spanning-tree mode stp
SwitchB(config)#interface gigaethernet 1/1/1
SwitchB(config-gigaethernet1/1/1)switchport mode trunk
SwitchB(config-gigaethernet1/1/1)#switchport trunk native vlan 200
SwitchB(config-gigaethernet1/1/1)#exit
```

```
SwitchB(config)#interface gigaethernet 1/1/2
SwitchB(config-gigaethernet1/1/2)#switchport mode trunk
SwitchB(config-gigaethernet1/1/2)#switchport trunk native vlan 200
```

配置 Switch C。

```
SwitchC#config
SwitchC(config)#spanning-tree enable
SwitchC(config)#spanning-tree mode stp
SwitchC(config)#interface gigaethernet 1/1/1
SwitchC(config-gigaethernet1/1/1)#switchport mode trunk
SwitchC(config-gigaethernet1/1/1)#switchport trunk native vlan 200
SwitchC(config-gigaethernet1/1/1)#exit
SwitchC(config)#interface gigaethernet 1/1/2
SwitchC(config-gigaethernet1/1/2)#switchport mode trunk
SwitchC(config-gigaethernet1/1/2)#switchport trunk native vlan 200
```

步骤 2 使能 IGMP Snooping 和接口的 IGMP 环网转发功能。

配置 Switch A。

```
SwitchA(config)#igmp ring gigaethernet 1/1/1
SwitchA(config)#igmp ring gigaethernet 1/1/2
SwitchA(config)#igmp snooping
SwitchA(config)#igmp snooping vlan 200
```

配置 Switch B。

```
SwitchB(config)#igmp ring gigaethernet 1/1/1
SwitchB(config)#igmp ring gigaethernet 1/1/2
SwitchB(config)#igmp snooping
SwitchA(config)#igmp snooping vlan 200
```

配置 Switch C。

```
SwitchC(config)#igmp ring gigaethernet 1/1/1
SwitchB(config)#igmp ring gigaethernet 1/1/2
SwitchC(config)#igmp snooping
```

检查结果

可断开环链路上任意一条链路，查看是否能正常接收组播流。

9.5 IGMP Querier

9.5.1 简介

IGMP Querier 是 IGMP 协议代理机制，运行在二层以太网交换机上辅助管理和控制组播组。IGMP Querier 会对 IGMP 报文进行终结，对上代理主机功能，对下代理组播路由器功能。

开启 IGMP Querier 功能的二层网络设备，有两种身份：

- 对用户侧，它是一个查询器，承担 Server 的角色，发送 Query 报文定期查询用户信息，并处理用户发来的 Report 和 Leave 报文。

- 对于网络路由侧，它是一个主机，承担 Client 的角色，响应组播路由器的 Query 报文；发送 Report 和 Leave 报文，在需要时将当前的用户信息发送给网络。

这种代理机制能有效地获取和控制用户信息，同时在减少网络侧协议报文以降低网络负荷方面起到一定作用。

IGMPQuerier 是靠拦截用户和组播路由器之间的 IGMP 报文建立组播转发表。

说明

IGMP Querier 功能一般是配合 IGMP Snooping / IGMP MVR 使用。

与 IGMP Querier 有关的概念介绍。

- IGMP 报文抑制

IGMP 报文抑制是指交换机过滤掉相同的 Report 报文。交换机收到来自某组播组成员的 Report 报文时，在一个查询间隔内只将某组播组的第一个 Report 报文转发给组播路由器，而不转发来自同一组播组的其他相同 Report 报文，减少网络中的报文数量。

说明

IGMP 报文抑制功能在开启 IGMP Snooping / IGMP MVR / 组播 VLAN 复制时可以单独使能或禁止。

- IGMP 查询者

IGMP 查询者功能是指在交换机设备上启动查询者功能后，交换机可以主动发送 IGMP 查询报文，查询接口下组播成员信息。未启动查询者功能的交换机只转发组播路由器的 IGMP 查询报文，不主动发起查询。

说明

查询者功能在开启 IGMP Snooping / IGMP MVR/ 组播 VLAN 复制时都可以单独使能或禁止。

- IGMP 查询者发送查询报文的源 IP 地址

IGMP 查询者发送查询报文的源 IP 地址。缺省情况下使用 IP 接口 0 的 IP 地址，如果 IP 接口 0 没有配置，使用 0.0.0.0。在使用 0.0.0.0 的时候，部分主机所在的平台收到此种 IGMP 报文可能认为是一个非法 IGMP 报文而不做反应，因此建议指定发送查询报文的源 IP 地址。

- 查询时间间隔

即普通组查询时间间隔。普遍组查询消息是交换机定期向共享网段内所有主机以组播方式发送的查询消息，用于查询哪些组播组存在成员。

- 查询报文最大响应时间

最大响应时间用于控制主机反馈组成员关系报告的最后期限。主机收到查询报文后，会为其加入的每个组播组都启动一个定时器，其值在 0～“最大响应时间”中随机选定，当定时器超时，主机会发出针对该组播组的 Report 报文。

- 最后成员发送 Query 间隔

也称特定组查询时间间隔。交换机在收到主机发送的针对某个组的 IGMP Leave 报文时，连续发送针对特定组的查询报文时间间隔。

特定组查询报文询问该组播组是否存在成员，如果接口下存在该组的成员，则成员必须在最大响应时间内发送 Report 报文，交换机在指定时间内收到主机发送的 Report 报文，就继续维护该组的组播转发表项，否则认为该接口下该组的最后一个成员已经离开，删除该组的组播转发表项。

9.5.2 配置准备

场景

在一个大规模应用组播路由协议的网络中，存在多个主机或接收组播信息的客户端子网。在组播路由器和主机相连的交换机上设置 IGMP Querier，拦截主机和路由器之间的 IGMP 报文，减少网络负担。

配置 IGMP Querier 可以减少组播路由器对客户子网络的配置和管理工作，同时又可实现客户子网络的组播连接。

IGMP Querier 功能一般用来配合 IGMP Snooping 或 IGMP MVR 功能使用。

前提

在配置 IGMP Querier 之前，需完成以下任务：

- 创建 VLAN；
- 将相应接口加入 VLAN。

9.5.3 IGMP Querier 的缺省配置

设备上 IGMP Querier 的缺省配置如下。

功能	缺省值
IGMP Querier 状态	禁止
IGMP 报文抑制功能	禁止
IGMP 查询者功能	禁止
IGMP 查询者和 Igmp querier 发送报文的源 IP 地址	使用 IP 接口 0 的 IP 地址，如果 IP 接口 0 没有配置，使用 0.0.0.0
IGMP 查询时间间隔	125 秒
发送 Query 报文的最大响应时间	10 秒

功能	缺省值
最后成员发送 Query 间隔	1 秒

9.5.4 配置 IGMP Querier 功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**igmp querier**	使能 IGMP 查询者功能。
3	Inspur(config)#**igmp source-ip** *ip-address*	（可选）配置 IGMP 查询者发送 Query 报文的源 IP 地址。
4	Inspur(config)#**igmp query-interval** *period*	（可选）配置 IGMP 查询时间间隔。
5	Inspur(config)#**igmp query-max-response-time** *period*	（可选）配置 Query 报文的最大响应时间。
6	Inspur(config)#**igmp last-member-query-interval** *period*	（可选）配置最后组成员发送 Query 报文时间间隔。
7	Inspur(config)#**igmp proxy**	配置 IGMP 代理功能。

说明

- 如果 IGMP Querier 没有使能，允许对 IGMP Querier 进行配置：设置源 IP 地址、查询时间间隔、发送 Query 报文的最大响应时间、最后成员发送 Query 间隔。当使能 IGMP Querier 功能后，这些配置立即生效。
- IGMP Querier 功能在开启 IGMP Snooping 或 IGMP MVR 时都可以启动。
- IGMP Proxy 与 IGMP Querier 功能互斥；IGMP proxy 与 IGMP Report-Suppression 功能互斥。

9.5.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show igmp querier**	查看 IGMP querier 配置信息。

9.5.6 配置 IGMP Snooping 和 IGMP Querier 应用示例

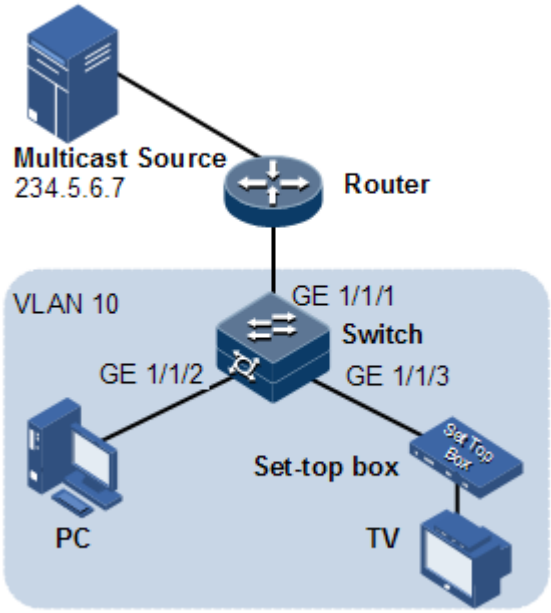
组网需求

如图 9-8 所示，交换机接口 Gigaethernet 1/1/1 连接组播路由器，接口 Gigaethernet 1/1/2，Gigaethernet 1/1/3 连接用户，用户在同一个 VLAN 10 中，配置 IGMP Snooping 功能，实现用户接收组播地址是 234.5.6.7 的组播数据功能。

在交换机上开启 IGMP Querier 功能，减少主机和组播路由器之间的通信，同时又不影响组播功能实现。

图中 PC 和机顶盒加入同一个组播组时，交换机收到两份 IGMP Report 报文，只向组播路由器发送一份 IGMP Report 报文。组播路由器发送的 IGMP Query 报文不再向下游转发，而是由交换机定时发送 IGMP Query 报文。

图9-8 IGMP Snooping 应用组网图



配置步骤

步骤 1 创建 VLAN，并将接口加入 VLAN。

```
Inspur#config
Inspur(config)#create vlan 10 active
Inspur(config)#interface gigaethernet 1/1/2
Inspur(config-gigaethernet1/1/2)#switchport mode trunk
Inspur(config-gigaethernet1/1/2)#switchport trunk native vlan 10
Inspur(config-gigaethernet1/1/2)#exit
Inspur(config)#interface gigaethernet 1/1/3
Inspur(config-gigaethernet1/1/3)#switchport access vlan 10
Inspur(config-gigaethernet1/1/3)#exit
Inspur(config)#interface gigaethernet 1/1/1
```

```
Inspur(config-gigaethernet1/1/1)#switchport access vlan 10
Inspur(config-gigaethernet1/1/1)#exit
```

步骤 2 配置使能 IGMP Snooping。

```
Inspur(config)#igmp snooping
Inspur(config)#igmp snooping vlan 10
```

步骤 3 配置 IGMP Querier 功能。

```
Inspur(config)#igmp querier
Inspur(config)#igmp source-ip 192.168.1.2
```

检查结果

查看 IGMP Snooping 配置信息是否正确。

```
Inspur#show igmp snooping
  IGMP snooping              :Enable
  IGMP report-suppression     :Disable
  IGMP version               :v2
  IGMP snooping active vlan    :10
  IGMP aging-time(s)          :260
  IGMP ring                  :--
```

查看 IGMP Snooping 组播组成员信息是否正确。

```
Inspur#show igmp snooping member vlan 10
R- ring port   D - Dynamic   S - Static
Vlan   Group                                Port       Live-time(s)  Flag
-------------------------------------------------------------------------

10     234.5.6.7                            GE1/1/1          --          S
```

查看 IGMP Querier 配置信息是否正确。

```
Inspur#show igmp querier
Global IGMP querier configuration:
----------------------------------
Querier Status               : Enable
Querier Source Ip             : 192.168.1.2
Query Interval(s)             :125
Query Max Response Interval(s)  :10
Last Member Query Interval(s)   :1
Robust Count                 :2
Next General Query(s)         :--
```

9.6 IGMP MVR

9.6.1 简介

IGMP MVR（Multicast VLAN Registration，组播 VLAN 注册）是运行在二层设备上的组播约束机制，用于管理和控制组播组，实现二层组播。

IGMP MVR 是通过配置组播 VLAN，将交换机中属于不同用户 VLAN 的成员接口加入组播 VLAN 内，使不同 VLAN 内的用户共用一个组播 VLAN，这样组播数据只在一个组播 VLAN 内传输，不必再为每个用户 VLAN 复制一份，从而节省了带宽。同时组播 VLAN 和用户 VLAN 完全隔离，也增加了安全性。

IGMP MVR 与 IGMP Snooping 都可以实现二层组播，两者的区别是：IGMP Snooping 中的组播 VLAN 和用户 VLAN 相同，而 IGMP MVR 的组播 VLAN 和用户 VLAN 可以不同。

说明

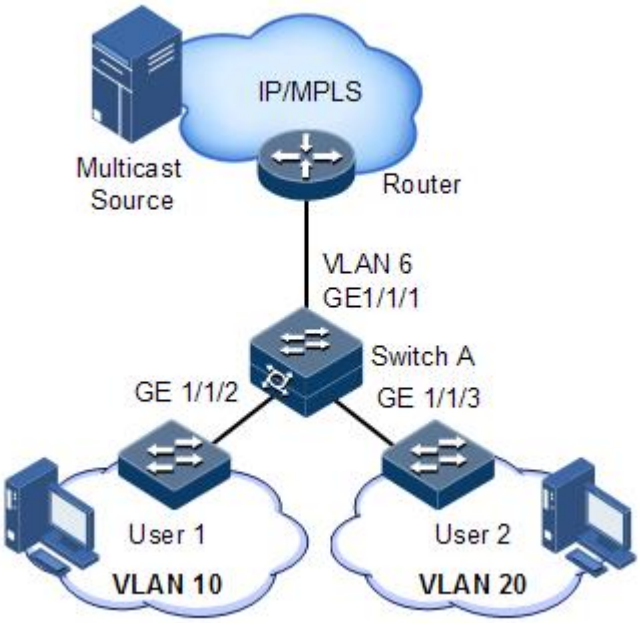
一个交换机最多能配置 10 个组播 VLAN，最少配置 1 个组播 VLAN 及其组地址集。支持的最大组播组数是 1024 个组。

9.6.2 配置准备

场景

如图 9-9 所示，多个用户接收组播源的数据，多个用户之间和组播路由器之间均属于不同 VLAN。可以在 Switch A 上运行 IGMP MVR，配置组播 VLAN，实现不同 VLAN 内的用户共用一个组播 VLAN 接收相同的组播数据，同时也可以减少带宽浪费。

图9-9 IGMP MVR 应用场景



前提

在配置 IGMP MVR 之前，需完成以下任务：

- 设备上组播 VLAN 复制功能禁止；
- 创建 VLAN，并将相应接口加入 VLAN。

9.6.3 IGMP MVR 的缺省配置

设备上 IGMP MVR 的缺省配置如下。

功能	缺省值
全局 IGMP MVR 状态	禁止
接口 IGMP MVR 状态	禁止
组播 VLAN 和组地址集	无

9.6.4 配置 IGMP MVR 功能

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**igmp mvr**	使能全局 IGMP MVR。
3	Inspur(config)#**igmp mvr mcast-vlan** *vlan-id* **group** { *start-ip-address* [*end-ip-address*] | **any** }	配置组播 VLAN 的组地址集。 **说明** 设备使能 IGMP MVR 后，需要配置组播 VLAN 和绑定的组地址集，如果接收的 IGMP Report 报文不属于任何 VLAN 的组地址集则不处理该 Report 报文，用户无法点播到组播流。
4	Inspur(config)#**interface** *interface-type interface-number*	（可选）进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
5	Inspur(config-gigaethernet1/1/*)#**igmp mvr mcast-vlan** *vlan-id* **static** *ip-address* [**user-vlan** *vlan-id*]	（可选）配置 MVR 的静态组播成员。
6	Inspur(config-gigaethernet1/1/*)#**igmp mvr user-vlan** *vlan-id*	（可选）配置组播跨 VLAN 复制的生效范围。
7	Inspur(config-gigaethernet1/1/*)#**igmp mvr mcast-vlan** *vlan-id* **host-join** *ip-address* [**user-vlan** *vlan-id*]	（可选）配置 MVR 的模拟主机加入功能。

说明

IGMP MVR 和 IGMP snooping 不能在同一组播 vlan 下同时开启，否则配置失败。

IGMP MVR 和组播 VLAN 复制不能在同一组播 vlan 同组播组下同时开启，否则配置失败。

9.6.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur# **show igmp mvr** [**interface** | *interface-type interface-number*]	查看指定接口的 IGMP MVR 的相关配置信息。
2	Inspur#**show igmp mvr member** [*interface-type interface-number* | **user-vlan** *vlan-id*]	查看 IGMP MVR 的组播组成员信息。
3	Inspur#**show igmp mvr member count** [*interface-type interface-number* | **user-vlan** *vlan-id*]	查看 IGMP MVR 的组播组成员数目信息。

序号	检查项	说明
4	Inspur#**show igmp mvr vlan-group** [**mcast-vlan** *vlan-id*]	查看组播 VLAN 及其组地址集。

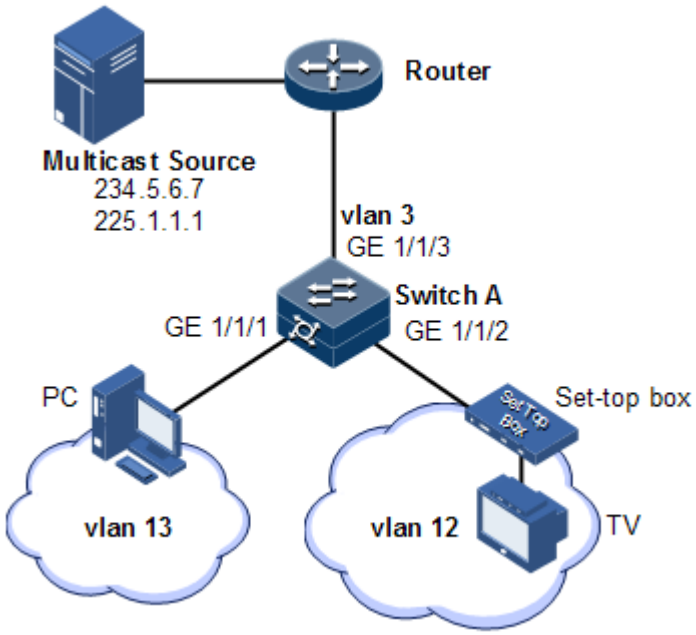
9.6.6 配置 IGMP MVR 应用示例

组网需求

如图 9-10 所示，Switch A 的接口 GE 1/1/3 连接组播路由器，接口 GE 1/1/1，GE1/1/2 连接位于不同 VLAN 的用户，实现用户接收组播 234.5.6.7 和 225.1.1.1 的组播数据功能。

在 Switch A 上配置 IGMP MVR 功能，指定 VLAN 3 为组播 VLAN，这样组播数据不需在每个用户 VLAN 复制一份，只需要在组播 VLAN 内复制一份，节省了带宽。

图9-10 IGMP MVR 应用组网图



配置步骤

步骤 1 在 Switch A 上创建 VLAN，并将接口加入 VLAN。

```
Inspur(config)#config
Inspur(config)#creat vlan 3,12,13 active
Inspur(config)#interface gigaethernet 1/1/1
Inspur(config-gigaethernet1/1/1)#switchport mode trunk
Inspur(config-gigaethernet1/1/1)#switchport trunk native vlan 13
Inspur(config-gigaethernet1/1/1)#switchport trunk untagged vlan 12
```

```
Inspur(config-gigaethernet1/1/1)#exit
Inspur(config)#interface gigaethernet 1/1/2
Inspur(config-gigaethernet1/1/2)#switchport mode trunk
Inspur(config-gigaethernet1/1/2)#switchport trunk native vlan 12
Inspur(config-gigaethernet1/1/2)#switchport trunk untagged vlan 13
Inspur(config-gigaethernet1/1/2)#exit
Inspur(config)#interface gigaethernet 1/1/3
Inspur(config-gigaethernet1/1/3)#switchport mode trunk
Inspur(config-gigaethernet1/1/3)#switchport trunk native vlan 3
Inspur(config-gigaethernet1/1/3)#switchport trunk untagged vlan 12,13
Inspur(config-gigaethernet1/1/3)#exit
```

步骤 2 配置 Switch A 上的 IGMP MVR 功能。

```
Inspur(config)#igmp mvr
Inspur(config)#interface gigaethernet 1/1/1
Inspur(config-gigaethernet1/1/1)#igmp mvr
Inspur(config-tengigabitethernet1/1/1)#igmp mvr user-vlan 13
Inspur(config-gigaethernet1/1/1)#exit
Inspur(config)#interface gigaethernet 1/1/2
Inspur(config-gigaethernet1/1/2)#igmp mvr
Inspur(config-tengigabitethernet1/1/2)#igmp mvr user-vlan 12
Inspur(config-gigaethernet1/1/2)#exit
Inspur(config)#igmp mvr mcast-vlan 3 group 234.5.6.7
Inspur(config)#igmp mvr mcast-vlan 3 group 225.1.1.1
```

检查结果

查看 Switch A 上的 IGMP MVR 的配置信息是否正确。

```
Inspur#show igmp mvr
igmp mvr running             :Enable
igmp mvr port                :GE1/1/1 GE1/1/2
igmp mvr multicast vlan(ref)   :3(2)
igmp aging time(s)           :260
igmp ring                    :--
```

查看 Switch A 上的组播 VLAN 和组地址信息是否正确。

```
Inspur#show igmp mvr vlan-group
Inspur(config)#show igmp mvr vlan-group
Mcast-vlan     Start-group    End-group
-----------------------------------------
3            225.1.1.1      225.1.1.1
3            234.5.6.7      234.5.6.7
```

9.7 配置 IGMP 过滤

9.7.1 简介

为了控制用户的访问权限，可以设置 IGMP 过滤。IGMP 过滤包含通过滤模板限制可访问组播组范围和最大组数限制：

- IGMP 过滤模板

为了保证信息的安全性，管理员需要对组播用户进行限制，如允许用户可以接收哪些组播数据，不能接收哪些组播数据。

通过配置 IGMP Profile 过滤模板，可以在接口上进行这种控制。一个 IGMP Profile 可以设置对一个或多个组播组的访问控制限制，通过设置（**permit** 和 **deny**）规则限制对组播组的访问。如果一个拒绝类型的 IGMP Profile 过滤模板被应用到接口上，当接口收到这个组的 IGMP 报告报文时，直接丢弃，不允许这个接口接收这个组的组播数据。

IGMP 过滤模板可以在接口上或“接口+VLAN”上进行设置。

IGMP Profile 只应用于动态的组播组，对静态的不适用。

- 最大组播组数限制

可以在接口上或“接口+VLAN”上设置允许加入的最大组播组数和最大组限制规则。

最大组限制规则设置用户加入的组数达到最大组数时采取的动作，是不允许用户再加入组，还是覆盖原来加入的组。

说明

IGMP 过滤功能一般是配合 IGMP Snooping / IGMP MVR / 组播 VLAN 复制使用。

9.7.2 配置准备

场景

同一组播中的不同用户，接收组播需求或权限不同，允许在组播路由器和主机相连的交换机上设置过滤规则，对组播用户进行限制。

还可以设置允许用户加入的最大组播组组数。

IGMP 过滤功能一般用来配合 IGMP Snooping 或 IGMP MVR 功能使用。

前提

在配置 IGMP 过滤之前，需完成以下任务：

- 创建 VLAN；
- 将相应接口加入 VLAN。

9.7.3 IGMP 过滤的缺省配置

设备上 IGMP 过滤的缺省配置如下。

功能	缺省值
全局 IGMP 过滤	禁止

功能	缺省值
IGMP 过滤模板 Profile	无
IGMP 过滤模板动作	拒绝
接口下 IGMP 过滤	无最大组限制，最大组动作为 drop，无应用过滤模板
“接口+VLAN”下 IGMP 过滤	无最大组限制，最大组动作为 drop，无应用过滤模板

9.7.4 配置全局使能 IGMP 过滤

请在设备上执行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**igmp filter**	全局使能 IGMP 过滤。

说明

配置应用 IGMP 过滤模板或最大组数限制时，均需要先执行 **igmp filter** 命令全局使能 IGMP 过滤。

9.7.5 配置 IGMP 过滤模板

IGMP 过滤模板可以在接口下使用，也可以在“接口+VLAN”上应用。

请在设备上执行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**igmp filter profile** *profile-number*	创建 IGMP Profile 并进入 Profile 配置模式。
3	Inspur(config-igmp-profile)#{ **permit** | **deny** }	配置 IGMP Profile 的动作。
4	Inspur(config-igmp-profile)#**range** *range-id start-ip-address* [*end-ip-address*]	配置控制访问的 IP 组播地址或范围。
5	Inspur(config-igmp-profile)#**exit** Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式或聚合组配置模式。

步骤	配置	说明
6	Inspur(config-gigaethernet1/1/*)#**igmp filter profile** *profile-number* [**vlan** *vlan-list*]	配置在物理层接口或“接口+VLAN”上应用IGMP Profile 过滤模板。
	Inspur(config-port-channel*)#**igmp filter profile** *profile-number* [**vlan** *vlan-list*] Inspur(config-port-channel*)#exit	配置在聚合组接口或“接口+VLAN”上应用IGMP Profile 过滤模板。
7	Inspur(config)#**igmp drop** [**query** | **report**]	（可选）使能 IGMP 过滤来自用户端口的查询报文功能或过滤来自上游端口的加入离开报文功能

说明

通过在接口配置模式下执行 **igmp filter profile** *profile-number* 命令，可以将已经创建的 IGMP Profile 应用到指定接口。一个 IGMP Profile 可以应用到多个接口，但是每个接口只能有一个 IGMP Profile。

9.7.6 配置最大组数限制

用户可加入的最大组数限制，可以应用在接口下，也可以应用在“接口+VLAN”下。

请在设备上执行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式或聚合组配置模式。
3	Inspur(config-gigaethernet1/1/*)#**igmp filter max-groups** *group-number* [**vlan** *vlan-list*]	配置在物理层接口或“接口+VLAN”上允许加入的最大组数限制。
	Inspur(config-port-channel*)#**igmp filter max-groups** *group-number* [**vlan** *vlan-list*]	配置在聚合组接口或“接口+VLAN”上允许加入的最大组数限制。
4	Inspur(config-gigaethernet1/1/*)#**igmp filter max-groups action** { **drop** | **replace** } [**vlan** *vlan-list*]	（可选）配置当物理层接口或“接口+VLAN”加入的组数超过最大组数时采取的动作。
	Inspur(config-port-channel*)#**igmp filter max-groups action** { **drop** | **replace** } [**vlan** *vlan-list*]	（可选）配置当聚合组接口或“接口+VLAN”加入的组数超过最大组数时采取的动作。

9.7.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show igmp filter** [{ **interface** | *interface-type interface-number* } [**vlan** [*vlan-id*]]]	查看 IGMP 过滤的配置信息。
2	Inspur#**show igmp filter profile** [*profile-number*]	查看 IGMP Profile 信息。

9.7.8 配置接口下应用 IGMP 过滤示例

组网需求

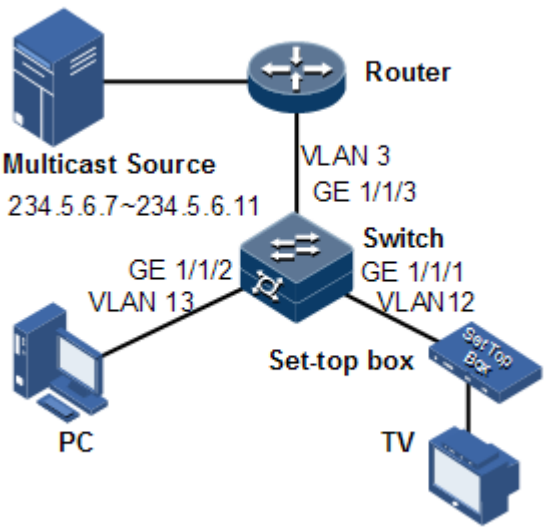
在交换机上开启 IGMP 过滤，通过添加接口下的过滤规则，对组播用户进行限制。

如图 9-11 所示，创建 IGMP 过滤规则 Profile 1，设置地址范围为 234.5.6.7 到 234.5.6.10 的组播组，动作为放行。在接口 GE 1/1/1 下应用过滤规则，机顶盒可以加入 234.5.6.7 的组播组，不能加入 234.5.6.11 的组播组；GE 1/1/2 未采用过滤规则，PC 可以加入 234.5.6.11 的组播组。

对 GE 1/1/1 接口设置最大组限制，在机顶盒加入 234.5.6.7 之后，再加入 234.5.6.8，则退出之前的 234.5.6.7 的组播组。

如图 9-11 所示场景，可以采用 IGMP MVR 功能提供组播服务。

图9-11 接口下应用 IGMP 过滤组网图



配置步骤

步骤 1 创建 VLAN，并将接口加入 VLAN。

```
Inspur#config
Inspur(config)#creat vlan 3,12,13 active
Inspur(config)#interface gigaethernet 1/1/1
Inspur(config-gigaethernet1/1/1)#switchport mode trunk
Inspur(config-gigaethernet1/1/1)#switchport trunk native vlan 12
Inspur(config-gigaethernet1/1/1)#switchport trunk untagged vlan 3
Inspur(config-gigaethernet1/1/1)#exit
Inspur(config)#interface gigaethernet 1/1/2
Inspur(config-gigaethernet1/1/2)#switchport mode trunk
Inspur(config-gigaethernet1/1/2)#switchport trunk native vlan 13
Inspur(config-gigaethernet1/1/2)#switchport trunk untagged vlan 3
Inspur(config-gigaethernet1/1/2)#exit
Inspur(config)#interface gigaethernet 1/1/3
Inspur(config-gigaethernet1/1/3)#switchport mode trunk
Inspur(config-gigaethernet1/1/3)#switchport trunk native vlan 3
Inspur(config-gigaethernet1/1/3)#switchport trunk untagged vlan 12,13
Inspur(config-gigaethernet1/1/3)#exit
```

步骤 2 配置 IGMP MVR 功能。

```
Inspur(config)#igmp mvr
Inspur(config)#interface gigaethernet 1/1/1
Inspur(config-gigaethernet1/1/1)#igmp mvr
Inspur(config-tengigabitethernet1/1/1)#igmp mvr user-vlan 12
Inspur(config-gigaethernet1/1/1)#exit
Inspur(config)#interface gigaethernet 1/1/2
Inspur(config-gigaethernet1/1/2)#igmp mvr
Inspur(config-tengigabitethernet1/1/2)#igmp mvr user-vlan 13
Inspur(config-gigaethernet1/1/2)#exit
Inspur(config)#igmp mvr mcast-vlan 3 group any
```

步骤 3 配置 IGMP 过滤模板。

```
Inspur(config)#igmp filter profile 1
Inspur(config-igmp-profile)#permit
Inspur(config-igmp-profile)#range 1 234.5.6.7 234.5.6.10
Inspur(config-igmp-profile)#exit
```

步骤 4 配置在机顶盒接口应用 IGMP 过滤模板。

```
Inspur(config)#igmp filter
Inspur(config)#interface gigaethernet 1/1/1
Inspur(config-gigaethernet1/1/1)#igmp filter profile 1
```

步骤 5 配置机顶盒接口的最大组数限制。

```
Inspur(config-gigaethernet1/1/1)#igmp filter max-groups 1
Inspur(config-gigaethernet1/1/1)#igmp filter max-groups action replace
```

检查结果

检查接口下应用过滤信息配置是否正确。

```
Inspur#show igmp filter gigaethernet 1/1/1
```

```
igmp profile:   1
max group:       1
current group:   0
action:        replace
```

9.8 组播 VLAN 复制

9.8.1 简介

组播 VLAN 复制是在交换机上当不同的用户 VLAN 点播同一组播源时，指定这些不同的 VLAN 为一个组播 VLAN 的用户 VLAN。使能组播 VLAN 复制功能后，上层设备只需将组播数据在组播 VLAN 中复制一份，不必再为每个用户复制一份，从而节省了带宽。在交换机上根据组播 VLAN 和组播组地址查找相应的出接口，在出接口为每个用户 VLAN 复制一份。

组播 VLAN 复制与 IGMP MVR 都可以实现用户 VLAN 和组播 VLAN 不在同一个 VLAN 的组播功能，两者的区别是：IGMP MVR 中的组播数据只能在一个组播 VLAN 内转发，而组播 VLAN 复制是在出接口将组播数据复制到用户 VLAN。

IGMP MVR 数据传输方式如图 9-12 所示，组播 VLAN 复制数据传输方式如图 9-13 所示。

图9-12 IGMP MVR 数据传输示意图

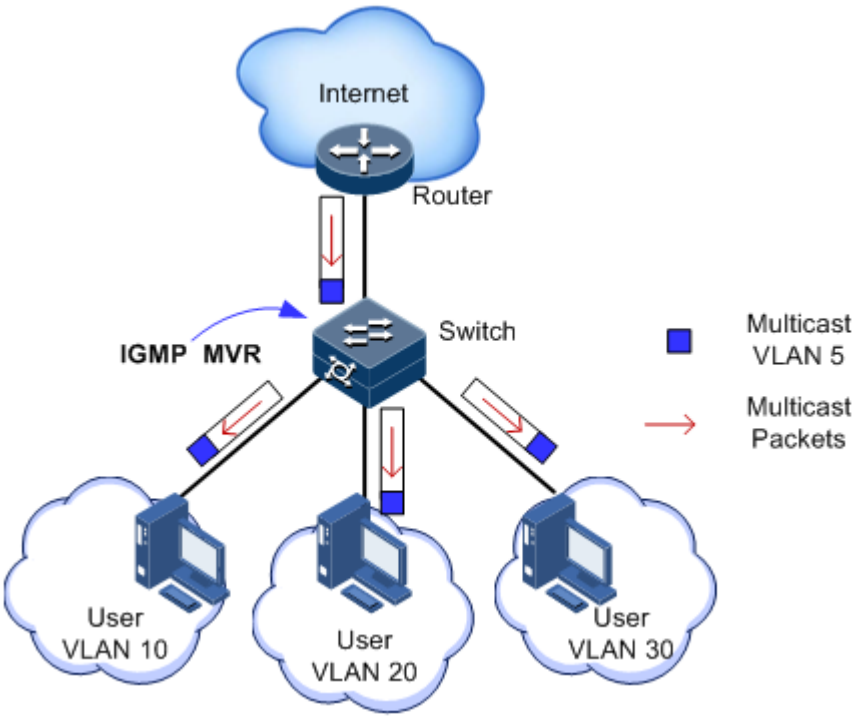
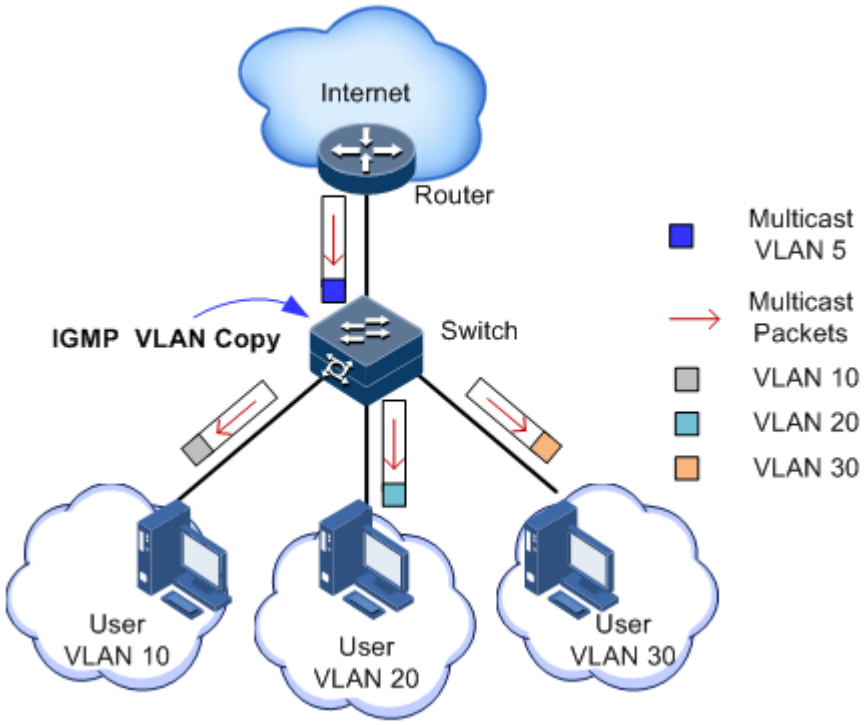


图9-13 组播 VLAN 复制数据传输示意图



说明

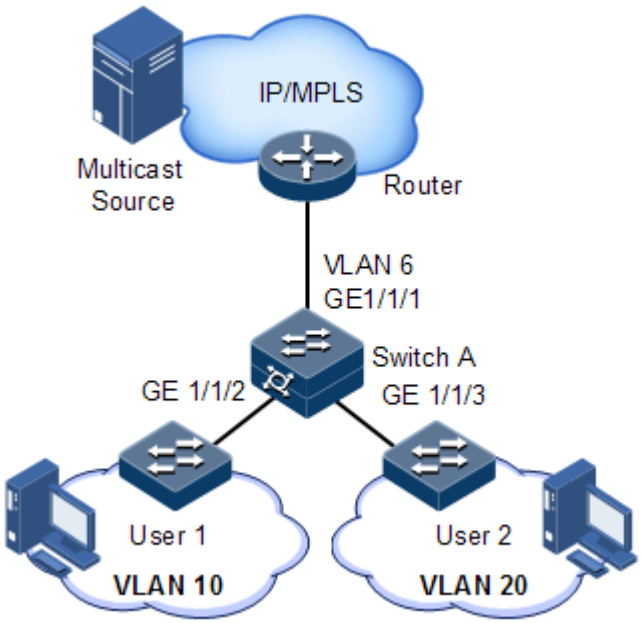
一个交换机最多能配置 10 个组播 VLAN，最少配置 1 个组播 VLAN 及其组地址集。支持的最大组播组数是 1024 个组。

9.8.2 配置准备

场景

如图 9-14 所示，多个主机接收组播源的数据，多个主机之间属于不同 VLAN。可以在 Switch A 上运行组播 VLAN 复制，配置组播 VLAN，在接收接口将组播数据复制到用户 VLAN，实现不同 VLAN 内的用户共用一个组播 VLAN 接收相同的组播数据，同时也可以减少带宽浪费。

图9-14 组播 VLAN 复制应用场景



前提

在配置组播 VLAN 复制之前，需完成以下任务：

- 创建 VLAN，并将相应接口加入 VLAN。

9.8.3 组播 VLAN 复制的缺省配置

设备上组播 VLAN 复制的缺省配置如下。

功能	缺省值
全局组播 VLAN 复制状态	禁止
接口组播 VLAN 复制状态	禁止
组播 VLAN 和组地址集	无

说明

- 当同时配置 N:1 VLAN 转换和 VLAN COPY 功能时，需要先配置 VLAN COPY，后配置 N:1 VLAN 转换；
- 当同时配置 N:1 VLAN 转换和 PIM 功能时，需要先配置 PIM，后配置 N:1 VLAN 转换；

9.8.4 配置组播 VLAN 复制功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**igmp vlan-copy**	使能全局组播 VLAN 复制。
3	Inspur(config)#**igmp vlan-copy mcast-vlan** *vlan-id* **group** { *start-ip* [*end-ip*] | **any** }	配置组播 VLAN 的组地址集。 **说明** 设备使能组播 VLAN 复制后，需要配置组播 VLAN 和绑定的组地址集，如果接收的 IGMP Report 报文不属于任何 VLAN 的组地址集则不处理该 Report 报文，用户无法点播到组播流。
4	Inspur(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
5	Inspur(config-gigaethernet1/1/*)#**igmp vlan-copy**	使能接口模式下的组播 VLAN 复制功能。

9.8.5 配置 VLAN-Copy 的静态组播成员

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**igmp vlan-copy mcast-vlan** *vlan-id* **static** *ip-address* [**user-vlan** *vlan-id*]	配置 VLAN-Copy 的静态组播成员。

说明

组播 VLAN 复制和 IGMP MVR 不能在同一组播 vlan 下的同组播组同时开启，否则配置失败。

组播 VLAN 复制和 IGMP Snooping 不能在同一组播 vlan 下同时开启，否则配置失败。

9.8.6 配置 VLAN-Copy 的用户 VLAN

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**igmp vlan-copy user-vlan** *vlan-id*	配置组播 VLAN 复制的用户 VLAN。

9.8.7 配置 VLAN-Copy 的模拟主机加入功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**igmp vlan-copy mcast-vlan** *vlan-id* **host-join** *ip-address* [**user-vlan** *vlan-id*]	配置 VLAN-Copy 的模拟主机加入功能。

9.8.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show igmp vlan-copy**	查看组播 VLAN 复制的相关配置信息。
2	Inspur#**show igmp vlan-copy** *interface-type interface-number*	查看指定接口的组播 VLAN 复制的相关配置信息。
3	Inspur#**show igmp vlan-copy member**	查看组播 VLAN 复制的组播组成员信息。
4	Inspur#**show igmp vlan-copy member** *interface-type interface-number*	查看指定接口的组播 VLAN 复制的组播组成员信息。
5	Inspur#**show igmp vlan-copy member user-vlan** *vlan-id*	查看指定用户 VLAN 的组播 VLAN 复制的组播组成员信息。
6	Inspur#**show igmp vlan-copy vlan-group** [**mcast-vlan** *vlan-id*]	查看组播 VLAN 复制的组播 VLAN 及绑定的组地址集。

9.9 MLD

9.9.1 简介

MLD 是组播技术中使用的一种网络协议。路由器通过 MLD 协议，可以侦听自己的直连网段上是否有 IPv6 组播组的侦听者，并在数据库里做相应记录。同时，路由器还维护与这些 IPv6 组播地址相关的定时器信息。通过 MLD 协议，用户主机和预期直接相连的组播路由器之间建立、维护组播成员关系。

MLD 路由器使用 IPv6 单播链路本地地址作为源地址发送 MLD 报文，使用 ICMPv6（Internet Control Message Protocol for IPv6，针对 IPv6 的互联网控制报文协议）报文类型。所有的 MLD 报文被限制在本地链路上，跳数为 1。

设备支持两个 MLD 版本：

- MLDv1：由 RFC2710 定义，源自 IGMPv2。
- MLDv2：由 RFC3810 定义，源自 IGMPv3。

MLDv1 主要基于查询和响应机制完成对 IPv6 组播组成员的管理。MLDv2 在 MLDv1 基础上，

- 增加对 IPv6 组播源的过滤，主机在加入某 IPv6 组播组时，能够明确要求接收或拒绝来自某特定 IPv6 组播源的信息。
- 增加了最大响应时间配置，适合于较大的网络。
- 取消了响应抑制功能，主机不必处理来自其他主机的报文，简化了主机的实现。
- 在查询报文中，增加了 S 标志位，可以提高系统的健壮性。
- 查询和响应报文均增加了重传机制。

9.9.2 配置准备

场景

出现于 IPv4 时代的组播技术，有效解决了单点发送、多点接收的问题，实现了网络中点到多点的高效数据传送，能够大量节约网络带宽、降低网络负载。在 IPv6 网络中，组播技术的应用得到了进一步的丰富和加强。设备通过侦听 MLD 消息建立组播数据报文的转发表，从而管理和控制组播数据报文的转发，把组播数据报文转发给需要接收该数据的主机。

前提

接口上已配置 IPv6 地址。

9.9.3 MLD 的缺省配置

设备上 MLD Snooping 的缺省配置如下。

功能	缺省值
接口的 MLD 环网转发功能	未使能

功能	缺省值
MLD Snooping 功能	未使能
MLD 的版本	1
MLD 成员的老化时间	260s
MLD 健壮系数	2

9.9.4 配置 MLD 基本功能

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**mld mrouter vlan** *vlan-id interface-type interface-number*	创建指定 VLAN 上的组播路由器接口。
3	Inspur(config)#**mld ring** *interface-type interface-number*	使能接口的 MLD 环网转发功能。
4	Inspur(config)#**mld report-suppression**	（可选）开启 Report 抑制功能。设备在一定的时间内收到多个相同组的 Report 报文，只向路由端口转发一个 Report 报文，其他报文将被抑制。
5	Inspur(config)#**mld member-timeout** { *second* | **infinite** }	（可选）配置 MLD 成员的老化时间。
6	Inspur(config)#**mld version** { **1** | **2** }	配置 MLD 的版本。
7	Inspur(config)#**interface** i*nterface-type interface-number*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
8	Inspur(config-gigaethernet1/1/*)#**mld immediate-leave** [**vlan** *vlan-list* | **user-mac**]	（可选）使能基于接口、基于“接口+VLAN”或基于用户的 MLD 的立即离开功能。如果下游口没有开启立即离开功能，路由口收到 leave 报文，会生依照鲁棒系数计算老化时间离开组超时定时器设置为 GMI(Group Membership Interval)，GMI = (robust-value*lastmember-queryinterval)。

9.9.5 配置 MLD Snooping 功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**mld snooping**	使能全局 MLD Snooping。
3	Inspur(config)#**mld snooping vlan** *vlan-list*	（可选）配置全局 VLAN 使能 MLD Snooping 功能。
4	Inspur(config)#**vlan** *vlan-id* Inspur(config-vlan)#**mld snooping static** *ip-address* [*interface-type interface-number*]	（可选）VLAN 模式下配置 MLD Snooping 的静态成员。
5	Inspur(config)#**interface** *interface-type interface number* Inspur(config-gigaethernet1/1/*)#**mld snooping host-join** *group-address* **vlan** *vlan-id*	（可选）端口下配置 MLD Snooping 模拟主机加入功能

9.9.6 配置 MLD Querier 功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**mld querier**	使能 MLD 查询者功能。
3	Inspur(config)#**mld source-ip** *ip-address*	（可选）配置 MLD 查询者发送 Query 报文的源 IP 地址。
4	Inspur(config)#**mld query-interval** *period*	（可选）配置 MLD 查询时间间隔。
5	Inspur(config)#**mld query-max-response-time** *period*	（可选）配置 Query 报文的最大响应时间。
6	Inspur(config)#**mld last-member-query-interval** *period*	（可选）配置最后组成员发送 Query 报文时间间隔。
7	Inspur(config)#**mld robust-count** *value*	配置 MLD 的健壮系数。
8	Inspur(config)#**mld proxy**	开启 MLD Proxy 功能。

- 如果 MLD Querier 没有使能，允许对 MLD Querier 进行配置：设置源 IP 地址、查询时间间隔、发送 Query 报文的最大响应时间、最后成员发送 Query 间隔。当使能 MLD Querier 功能后，这些配置立即生效。
- MLD proxy 与 mld querier 互斥;MLD proxy 与 mld report-suppression 互斥。

9.9.7 配置 MLD 过滤

配置全局使能 MLD 过滤

请在设备上执行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**mld filter**	全局使能 MLD 过滤。
3	Inspur(config-gigaethernet1/1/*)# **mld drop** { **query** | **report** }	（可选）使能 IGMP 过滤来自用户端口的查询报文功能或过滤来自上游端口的加入离开报文功能

配置应用 MLD 过滤模板或最大组数限制时，均需要先执行 **mld filter** 命令全局使能 MLD 过滤。

配置 MLD 过滤模板

MLD 过滤模板可以在接口下使用，也可以在“接口+VLAN”上应用。

请在设备上执行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**mld filter profile** *profile-number*	创建 MLD Profile 并进入 Profile 配置模式。
3	Inspur(config-mld-profile)#{ **permit** | **deny** }	配置 MLD Profile 的动作。
4	Inspur(config-mld-profile)#**range** *range-id start-ip-address* [*end-ip-address*]	配置控制访问的 IPv6 组播地址或范围。

步骤	配置	说明
5	Inspur(config-mld-profile)#**exit** Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式或聚合组配置模式。
6	Inspur(config-gigaethernet1/1/*)#**mld filter profile** *profile-number* [**vlan** *vlan-list*]	配置在物理层接口或“接口+VLAN”上应用 MLD Profile 过滤模板。
	Inspur(config-port-channel*)#**mld filter profile** *profile-number* [**vlan** *vlan-list*] Inspur(config-port-channel*)#exit	配置在聚合组接口或“接口+VLAN”上应用 MLD Profile 过滤模板。

说明

通过在接口配置模式下执行 **mld filter profile** *profile-number* 命令，可以将已经创建的 MLD Profile 应用到指定接口。一个 MLD Profile 可以应用到多个接口，但是每个接口只能有一个 MLD Profile。

配置最大组数限制

用户可加入的最大组数限制，可以应用在接口下，也可以应用在“接口+VLAN”下。

请在设备上执行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式或聚合组配置模式。
3	Inspur(config-gigaethernet1/1/*)#**mld filter max-groups** *group-number* [**vlan** *vlan-list*]	配置在物理层接口或“接口+VLAN”上允许加入的最大组数限制。
	Inspur(config-port-channel*)#**mld filter max-groups** *group-number* [**vlan** *vlan-list*]	配置在聚合组接口或“接口+VLAN”上允许加入的最大组数限制。
4	Inspur(config-gigaethernet1/1/*)#**mld filter max-groups action** { **drop** | **replace** } [**vlan** *vlan-list*]	（可选）配置当物理层接口或“接口+VLAN”加入的组数超过最大组数时采取的动作。
	Inspur(config-port-channel*)#**mld filter max-groups action** { **drop** | **replace** } [**vlan** *vlan-list*]	（可选）配置当聚合组接口或“接口+VLAN”加入的组数超过最大组数时采取的动作。

9.9.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show mld immediate-leave** [*interface-type interface-number* | **port-channel** *port-channel-id*]	查看 MLD 的立即离开配置信息。。
2	Inspur#**show mld mrouter**	查看 MLD 的组播路由器接口信息。
3	Inspur#**show mld snooping** [**vlan** *vlan-id*]	查看 MLD Snooping 的相关配置信息。
4	Inspur#**show mld snooping member** [*interface-type interface-number* | **vlan** *vlan-id*]	查看 MLD Snooping 的组播组成员信息。
5	Inspur#**show mld snooping member count** [*interface-type interface-number* | **vlan** *vlan-id*]	查看 MLD Snooping 的组播组成员数目信息。
6	Inspur#**show mld statistics** [*interface-type interface-number*]	查看 MLD 报文统计信息。
7	Inspur#**show mld filter** [{ **interface** | *interface-type interface-number* } [**vlan** [*vlan-id*]]]	查看 MLD 过滤的配置信息。
8	Inspur#**show mld filter profile** [*profile-number*]	查看 MLD 过滤模板的配置信息。
9	Inspur#**show mld configuration**	查看 MLD 基础配置信息。
10	Inspur#**show mld ring**	查看 MLD 环网接口信息。
11	Inspur#**show mld querier**	查看 MLD Querier 的相关信息。
12	Inspur#**show mld user-mac** [*interface-type interface-number* | **user-vlan** *vlan-id*]	查看 MLD 的用户 MAC 信息。
13	Inspur#**show mld user-mac count** [*interface-type interface-number* | **vlan** *vlan-id*]	查看 MLD 的用户 MAC 数目信息。

9.9.9 维护

用户可以通过以下命令，维护设备特性的运行情况和配置情况。

命令	描述
Inspur(config)#**clear mld statistics** [*interface-type interface-number*]	清除 MLD 的统计信息。

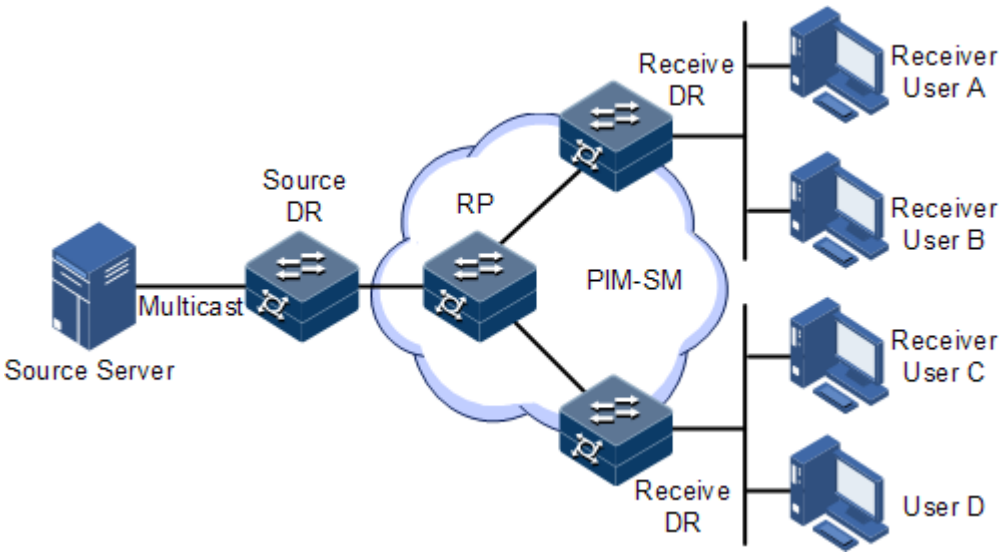
命令	描述
Inspur(config)#**no mld member** *interface-type interface-number*	删除指定接口组播转发表项。

9.10 PIM-SM

9.10.1 简介

PIM-SM（Protocol Independent Multicast-Sparse Mode）是一种稀疏模式的组播路由协议，适用于组成员分布相对分散、范围较广、大规模的网络。因为 PIM-SM 不依赖于任何特定的单播路由协议，所以被称作是协议无关的（Protocol Independent）组播路由协议。PIM-SM 在组播网络中的作用和位置如图 9-15 所示。

图9-15 PIM-SM 应用场景示意图



PIM-SM 设备之间通过 Hello 报文来发现邻居。一旦 PIM-SM 设备启动，它就周期性地在每个配置了 PIM-SM 的接口上发送 Hello 报文。Hello 报文有一个保持时间（Hello Hold Time）字段，这个时间参数定义了邻居等待下一个 Hello 报文的最长时间。如果邻居在这个时间内没有收到另一个 Hello 报文，就会将这个设备从邻居关系表中删除。

PIM-SM 使用加入/剪枝建立组播分发树。接收者发送 Report 到接收端 DR，DR 向 RP 方向发送（*，G）加入报文来建立共享树；组播源发送数据，组播源 DR 向 RP 发起注册，若 RP 上有接收者，则 RP 向组播源方向发送（S,G）加入报文来建立源树。PIM-SM 网络中的组播源数据通过 RP 沿共享树到达接收者。当接收者离开，发送 Leave 报文到接收端 DR，DR 向 RP 方向发送(*,G)剪枝报文来剪枝共享树；当 RP 上无 G 接收者时，RP 向组播源端方向发送(S,G)剪枝报文来剪枝源树。

PIM-SM 使用 SPT 切换来减小共享树的负担。接收端 DR 可选择合适的切换策略来将(S,G)的数据切换到 SPT 树上以减小 RPT 树负载。当接收端 DR 的切换策略满足时，接收端 DR 向组播源方向发送(S,G)加入报文来建立组播源到接收端 DR 的 SPT 树，向 RP

方向发送(S,G,rpt)剪枝报文来剪掉 RPT 树上(S,G)的组播流，从而达到减小共享树负担的目的。

9.10.2 配置准备

场景

通过配置 PIM-SM，可以实现组播路由与数据转发。

前提

无

9.10.3 PIM-SM 的缺省配置

设备上 PIM-SM 的缺省配置如下。

功能	缺省值
接口 PIM-SM 功能状态	禁止
DR 优先级	1
配置组播源生存时间	210s
RPT 切换到 SPT 前检查组播数据速率是否达到阈值的时间间隔	15s

说明

- 当同时配置 N:1 VLAN 转换和 VLAN COPY 功能时，需要先配置 VLAN COPY，后配置 N:1 VLAN 转换；
- 当同时配置 N:1 VLAN 转换和 PIM 功能时，需要先配置 PIM，后配置 N:1 VLAN 转换；

9.10.4 配置动态 RP 功能

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#router [ ipv6 ] pim`	进入 PIM 模式。

步骤	配置	说明
3	Inspur(config-router-pim)#**bsr-candidate** { *interface-type interface-number* | **vlan** *vlan-id* | **loopback** *interface-number* } [**hash-mask-length** *mask-length*] [**priority** *priority*] Inspur(config-router-pim6)#**bsr-candidate** *ipv6-address* [**hash-mask-length** *mask-length2*] [**priority** *priority*]	配置候选 BSR。
4	Inspur(config-router-pim)#**rp-candidate** { *interface-type interface-number* | **vlan** *vlan-id* | **loopback** *interface-number* } [**group** *ip-addresss/mask*] Inspur(config-router-pim6)#**rp-candidate** *ipv6-address* [**group** *ipv6-addresss/prefix-length*] Inspur(config-router-pim)#**rp-candidate** Inspur(config-router-pim6)#**rp-candidate** **priority** priority **priority** priority	配置候选 RP 及候选 RP 优先级。
5	Inspur(config-router-pim)#**spt-threshold** { *rate* | **infinity** } [**group-policy** *acl-number*]	配置 SPT 切换控制参数。
6	Inspur(config-router-pim)#**source-lifetime** *interval*	配置组播路由表项的老化时间。
7	Inspur(config-router-pim)#**timer spt-switch** *interval*	配置 RPT 切换到 SPT 前检查组播数据速率是否达到阈值的时间间隔。

9.10.5 配置静态 RP 功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**router pim**	进入 PIM 模式。
3	Inspur(config-router-pim)#**rp-address** *ip-address* [**group** *ip-addresss/mask*]	配置静态 RP 的 IP 地址。

9.10.6 配置 PIM BFD

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入三层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**ip pim bfd enable**	配置 PIM-SM BFD 功能。 缺省情况下，组播源的生存时间为 210s。

9.10.7 配置接口下 PIM-SM 功能

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入三层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#{ **ip** | **ipv6** } **pim dr-priority** *priority-value*	配置接口参与 DR 竞选的优先级。
4	Inspur(config-gigaethernet1/1/*)#{ **ip** | **ipv6** } **pim sparse-mode**	使能接口 PIM-SM 功能。

9.10.8 配置三层组播转发功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ip multicast routing**	使能三层组播转发功能。

9.10.9 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show** { **ip** | **ipv6** } **pim neighbor**	查看 PIM 邻居信息。
2	Inspur#**show** { **ip** | **ipv6** } **pim interface**	查看 PIM 邻居信息。
3	Inspur#**show** { **ip** | **ipv6** } **pim bsr-router**	查看 BSR 信息。

序号	检查项	说明
4	Inspur#**show { ip | ipv6 } pim rp-candidate**	查看候选 RP 信息。
5	Inspur#**show { ip | ipv6 } pim rp**	查看 RP 信息。
6	Inspur#**show { ip | ipv6 } pim route**	查看 PIM 组播路由表信息。

10 OAM

本章介绍 OAM 特性的基本原理和配置过程，并提供相关的配置案例。

- EFM
- BFD
- CFM（IEEE802.1ag/ITU-Y.1731）

10.1 EFM

10.1.1 简介

以太网最初为局域网设计，由于规模较小，所以 OAM（Operation，Administration and Maintenance，运行、管理和维护）能力较弱，且只有网元级的管理系统。随着以太网技术的不断发展，以太网在电信级网络中的应用也越来越广泛，但电信级网络在链路长度和网络规模上都较局域网大很多，有效管理维护机制的缺乏，已成为以太网技术在电信级网络中应用的严重障碍。

为了在以太网层能确定以太网虚链接的连通性，有效地检测、确认并定位以太网层网络内部的故障，并且可以衡量网络的利用率以及度量网络的性能，从而能根据与用户签订的 SLA（Service Level Agreement，服务等级协议）提供业务，在以太网上实现 OAM 机制已经成为必然的发展趋势。

遵循 IEEE 802.3ah 协议的 EFM（Ethernet in the First Mile，第一公里以太网）是一种链路级以太网 OAM 技术，针对两台直连设备之间的链路，提供链路连通性检测功能、链路故障监控功能、远端故障通知功能等。EFM 主要用于用户接入的网络边缘的以太网链路。

OAM 模式与 OAM 发现

以太网 OAM 连接过程也称作 Discovery 阶段，本阶段是 OAM 实体发现远端设备的 OAM 实体，并与之建立稳定对话的过程。

在这个阶段中，相连的以太网 OAM 实体（使能 OAM 功能的端口）通过交互 Information OAM PDU 向对端通报各自的以太网 OAM 配置信息及本地节点支持的以太网 OAM 能力信息，OAM 实体收到对端配置参数后，决定是否同意建立 OAM 连接。如果两端都同意建立 OAM 连接时，以太网 OAM 协议将在链路层开始正常工作。

设备可以选择两种模式来进行以太网 OAM 的连接。

- 主动模式
- 被动模式

以太网 OAM 连接过程只能由主动模式的 OAM 实体发起，而被动模式的 OAM 实体只能等待对端 OAM 实体的连接请求。

以太网 OAM 连接建立后，两端的 OAM 实体通过发送 Information OAM PDU 保持连接。若在 5 秒钟内没有收到对端 OAM 实体的 Information OAM PDU，则认为连接超时，需要重新建立 OAM 连接。

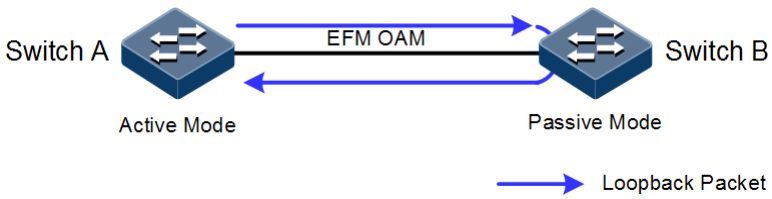
远端环回

远端环回功能可用于定位故障发生的区域，同时借助仪器仪表还可以对链路质量进行测试。定期地进行环回检测可以及时发现网络故障，并通过分段环回检测来定位故障发生的具体区域，有助于用户排除故障。

OAM 环回只有在以太网 OAM 连接建立完成后才能实现。在连接建立的情况下，主动模式的 OAM 实体发起 OAM 环回命令，对端实体对该命令进行响应。当对端处于环回模式时，除 OAM PDU 报文以外的所有报文都将按原路返回。

如图 10-1 所示，本地处于主动模式的 Switch A 设备将通过返回报文的情况，确定链路状况。

图10-1 OAM 环回示意图



OAM 事件

以太网的故障检测是非常困难的，特别是网络物理通信没有中断而网络性能缓慢下降的情况。OAM PDU 定义了一个标志（Flag 域）允许以太网 OAM 实体把该故障信息传送给对端。该标志可以表示下列故障：

- 链路故障（Link Fault）：对端链路信号丢失；
- 致命故障（Dying Gasp）：不可预知的状态发生，比如电源中断；
- 紧急事件（Critical Event）：不能确定的紧急事件发生。

设备不支持致命故障和紧急事件故障检测。

以太网 OAM 连接是在过程中不断发送 Information OAM PDU，本端 OAM 实体可以将本端发生的有门限事件信息通过 Information OAM PDU 告诉远端 OAM 实体。这样，管理员可以动态地了解链路的状态，对相应的错误及时进行处理。

以太网 OAM 利用 Event Notification OAM PDU 的交互来进行链路监控。当链路故障发生时，本地链路监控到故障后，将向对端以太网 OAM 实体发送 Event Notification OAM PDU，通报下列有门限事件。管理员可以通过链路监控过程动态地掌握网络的状况。

- 误帧事件：单位时间内的错误帧数量超过定义的阈值；
- 误帧周期事件：指定帧数 N 为周期，在收到 N 个帧的周期内错误帧数超过定义的阈值；
- 误帧秒事件：指定 M 秒数下有错误帧的秒数超过了定义的阈值；
- 误符号周期事件：是指设备对链路的误符号周期进行统计，当在一段事件内（监控窗口）内接收到的误符号周期数量统计超过阈值。

说明

在某一秒内产生了错误帧，则该秒为误帧秒。

OAM MIB 获取

设备可以通过 OAM 获取对端设备链路配置/统计值，从而获悉链路的状态和参数。

10.1.2 配置准备

场景

在直连设备之间部署 EFM 特性可以有效提高对以太网链路的管理和维护能力，保障网络的稳定运行。

前提

需要连接接口并配置接口的物理参数，使接口的物理层状态为 Up。

10.1.3 配置 EFM 基础功能

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#interface` *interface-type interface-number*	进入二层或三层物理接口配置模式。
3	`Inspur(config-gigaethernet1/1/*)#oam { active | passive }`	配置 EFM 的工作模式。 缺省情况下，设备是被动模式。

步骤	配置	说明
4	Inspur(config-gigaethernet1/1/*)#**oam send-period** *period-number* **timeout** *time*	（可选）配置 OAM PDU 的发送周期及超时时间。 缺省情况下，OAM PDU 的发送周期为 1s（即 *period-number* 取 10，10×100ms=1s），链路超时时间为 5s
5	Inspur(config-gigaethernet1/1/*)#**oam enable**	使能链路的 EFM OAM 功能。 缺省情况下，未使能。

10.1.4 配置 EFM 主动功能

说明

EFM 主动功能必须在设备处于主动模式时配置。

（可选）配置设备发起 EFM 远端环回功能

说明

- 定期地进行环回检测可以及时发现网络故障，通过分段环回检测可以定位故障发生的具体区域，帮助用户排除故障。
- 当处于链路环回状态时，设备将该链路收到的除了 OAM 报文外所有报文环回到对端设备，此时用户数据报文不能正常转发，所以不需要检测时请及时关闭该功能。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**oam remote-loopback**	使能物理接口发起远端环回。
4	Inspur(config-gigaethernet1/1/*)#**oam loopback timeout** *time*	（可选）配置物理接口远端环回超时时间。 缺省情况下，物理接口环回超时时间是 3s。
5	Inspur(config-gigaethernet1/1/*)#**oam loopback retry** *times*	（可选）配置物理接口远端环回超时重试次数。 缺省情况下，物理接口环回超时重试次数是 2 次。

（可选）查看对端设备当前的变量取值情况

说明

通过获取对端设备当前的变量取值情况，可以获取当前链路的状态。IEEE802.3 Clause30 详细定义和说明了支持 OAM 获取的变量及其表示方式。变量以对象（Object）作为最大的划分，每个对象下包含组件（Package）和属性（Attribute），组件又包含若干个属性，属性为变量表示的最小单元。OAM 变量获取时以 Clause30 定义对象、组件、属性的枝和叶描述请求对象，并以枝和叶后跟变量取值的方式表示对象响应变量请求。设备支持 OAM 信息和接口统计两种对象变量获取。

对端变量获取只有在 EFM 连接建立完成后才能实现。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**show oam peer oam-info** [*interface-type interface-number*]	查看对端 OAM 基本信息。
	Inspur#**show oam peer** [*interface-type interface-number*]	

10.1.5 配置 EFM 被动功能

说明

EFM 被动功能在设备处于主动模式或被动模式时均能配置。

（可选）配置设备响应 EFM 远端环回

说明

只有配置本端的远端环回响应功能，对端的 EFM 远端环回功能才能生效。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式。

步骤	配置	说明
3	Inspur(config-gigaethernet1/1/*)#oam loopback { ignore | process }	配置二层物理接口收到远端环回命令后是否响应。 缺省情况下，不响应对端发送的远端环回命令。

10.1.6 配置链路监控和故障指示功能

（可选）配置 OAM 链路监控功能

说明

OAM 链路监控用于检测和报告不同情况的链路错误。当检测链路发生错误时，设备通过 OAM 事件通知报文通知对端错误产生时间、窗口以及门限配置等信息，对端在收到事件通知后即通过 SNMP Trap 通知网管中心。此外，本端设备还可以指定端口通过 SNMP Trap 直接将事件上报到网管中心。

缺省情况下，系统对错误产生时间、窗口以及门限配置等均配置有默认值。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#config	进入全局配置模式。
2	Inspur(config)#interface *interface-type interface-number*	进入二层物理接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#oam errored-frame window *framewindow* threshold *framethreshold*	配置误帧事件监控窗口和阈值。 缺省情况下，监控窗口为 1s，阈值为 1 个错误帧。
4	Inspur(config-gigaethernet1/1/*)#oam errored-frame-period window *frameperiodwindow* threshold *frameperiodthreshold*	配置误帧周期事件监控窗口和阈值。缺省情况下，监控窗口为 1000ms，阈值为 1 个错误帧。
5	Inspur(config-gigaethernet1/1/*)#oam errored-frame-seconds window *framesecswindow* threshold *framesecsthreshold*	配置误帧秒统计事件的监控窗口和阈值。缺省情况下，监控窗口为 60s，阈值为 1s。
6	Inspur(config-gigaethernet1/1/*)#oam errored-symbol-period window *symperiodwindow* threshold *symperiodthreshold*	配置误符号周期事件监控窗口和阈值。缺省情况下，监控窗口为 1s，阈值为 1 个错误帧。

（可选）配置 OAM 故障指示功能

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**oam notify** { **critical-event** | **dying-gasp** | **errored-frame** | **errored-frame-period** | **errored-frame-seconds** | **errored-symbol-period** } **enable**	使能故障信息和 OAM 链路事件通知功能。 缺省情况下，使能所有链路的 OAM 事件通知。
4	Inspur(config-gigaethernet1/1/*)#**oam event trap enable**	使能本端 OAM 链路事件的 Trap 功能。 缺省情况下，未使能 OAM 链路事件的 Trap 功能。
5	Inspur(config-gigaethernet1/1/*)#**oam peer event trap** { **enable** | **disable** }	使能对端 OAM 链路事件的 Trap 功能。 缺省情况下，未使能对端 OAM 链路事件的 Trap 功能。

10.1.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show oam** [*interface-type interface-number*]	查看 OAM 基本功能配置。
2	Inspur#**show oam event** [*interface-type interface-number*] [**critical**]	查看本端 OAM 链路事件。
3	Inspur#**show oam loopback** [*interface-type interface-number*]	查看 OAM 远端环回配置信息。
4	Inspur#**show oam notify** [*interface-type interface-number*]	查看 OAM 事件通知配置信息。
5	Inspur#**show oam peer event** [*interface-type interface-number*] [**critical**]	查看 OAM 对端事件信息。
6	Inspur#**show oam peer link-statistic** [*interface-type interface-number*]	查看对端 OAM 链路统计信息。
7	Inspur#**show oam statistics** [*interface-type interface-number*]	查看 OAM 统计信息。
8	Inspur#**show oam trap** [*interface-type interface-number*]	查看 OAM Trap 信息。

10.1.8 维护

用户可以通过以下命令，维护设备 EFM OAM 特性的运行情况和配置情况。

命令	描述
Inspur(config-gigaethernet1/1/*)#clear oam statistics	清除 EFM OAM 接口链路统计信息。
Inspur(config-gigaethernet1/1/*)#clear oam event	清除 EFM OAM 链路事件信息。
Inspur(config)#clear oam config	清除 EFM OAM 配置信息。

10.2 BFD

10.2.1 简介

BFD（Bidirectional Forwarding Detection，双向转发检测）可以对系统之间、同一路径上的一种数据协议的连通性进行检测。路径可以是物理链路或逻辑链路，也包括隧道，当 BFD 发现系统之间的通信故障时，通知上层应用。

BFD 检测机制

在通信系统的两端建立 BFD 会话，并在检测路径上周期性的发送 BFD 控制报文，如果一端在规定时间内没有收到 BFD 控制报文，则认为路径上发生故障。

BFD 控制报文封装在 UDP 报文中传送。会话开始阶段，双方系统通过控制报文中携带的参数（系统两端的会话标识符、收发报文最小时间间隔、本端 BFD 会话状态等）进行协商。协商成功后，按照协商的报文收发时间在路径上定时发送 BFD 控制报文。

BFD 会话建立方式

BFD 会话有两种建立方式，静态建立 BFD 会话和动态建立 BFD 会话。BFD 通过控制报文中的本端标识符和远端标识符区分不同的会话。

- 静态建立 BFD 会话：通过手工配置 BFD 会话参数，包括本地标识符和远端标识符。
- 动态建立 BFD 会话：系统自动分配动态会话标识符区域的值作为 BFD 会话的本地标识符，然后与对方进行协商。对端收到协商报文判断是否与本地 BFD 会话匹配，如匹配则自动学习远端会话标识符。

设备支持静态建立 BFD 会话。

BFD 应用类型

设备支持以下 BFD 应用：

- 基于 IP 链路的 BFD：在 IP 链路上建立 BFD 会话，利用 BFD 检测机制快速检测故障。设备支持对 IP 链路进行单跳 IP 检测或多跳 IP 检测。
  - 单跳 IP 检测：BFD 用于快速检测系统之间的通信故障，支持在直连设备之间进行 IP 连通性检测。
  - 多跳 IP 检测：BFD 用于快速检测系统之间的通信故障，支持在非直连设备之间进行 IP 连通性检测。
- 基于 ISIS 的 BFD：
- 基于 OSPF 的 BFD：

10.2.2 配置准备

场景

为了减小设备故障对业务的影响，提高网络的可用性，网络设备需要能够尽快检测到与相邻设备间的通信故障，以便及时采取措施，保证业务继续进行。

前提

无

10.2.3 配置 BFD 会话绑定

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#bfd` *session-id* `bind peer-ip` *ip-address* `[ source-ip ]`	创建 BFD 会话检测多跳 IP 路径并进入 BFD 会话配置模式。
	`Inspur(config)#bfd` *session-id* `bind { peer-ip` *ip-address* `} interface` *interface-type interface-number*	创建静态 BFD 会话检测单跳 IP 路径并进入 BFD 会话模式。
3	`Inspur(config)#bfd trap enable`	（可选）使能 BFD Trap 功能。 缺省情况下，禁用 BFD Trap 功能。

10.2.4 配置 BFD 会话参数

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**bfd** *session-id*	进入 BFD 会话模式。 **说明** 需要创建 BFD 并绑定相应的路径后，才能使用该命令进入 BFD 会话模式。
3	Inspur(config-bfd-session)#**description** *description*	配置 BFD 会话描述信息。
4	Inspur(config-bfd-session)#**local discriminator** *value*	配置 BFD 会话本端标识符。 缺省情况下，标识符显示为 0 表示没有配置。 **说明** 如果不配置 BFD 本端标识符，则该标识符由系统自动生成。
5	Inspur(config-bfd-session)#**min send-interval** *interval*	配置 BFD 会话最小发送间隔。 缺省情况下，BFD 会话最小发送间隔是 1000ms。
6	Inspur(config-bfd-session)#**min receive-interval** *interval*	配置 BFD 会话最小接收间隔。 缺省情况下，BFD 会话最小接收间隔是 1000ms。
7	Inspur(config-bfd-session)#**detect-multiplier** *multiplier*	配置 BFD 会话本地检测倍数。 缺省情况下，BFD 会话本地检测倍数是 3。
8	Inspur(config-bfd-session)#**remote discriminator** *value*	配置 BFD 会话远端标识符。 缺省情况下，标识符显示为 0 表示没有配置。 **说明** 如果不配置 BFD 远端标识符，则该标识符由系统自动生成。
9	Inspur(config-bfd-session)#**session enable**	使能 BFD 会话功能。 缺省情况下，禁用 BFD 会话功能。
10	Inspur(config-bfd-session)#**exit**	返回全局配置模式。

步骤	配置	说明
11	Inspur(config)#**bfd** { **detect-multiplier** *multiplier* | **receive-interval** *interval* | **send-interval** *interval* } *	配置全局下动态 BFD 会话本地检测倍数、最小发送间隔、最小接收间隔。 **说明** 全局模式下配置适用于多跳 IP，接口模式适用于单跳 IP 或者缺省 IP。
12	Inspur(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
13	Inspur(config-gigaethernet1/1/*)#**bfd** { **detect-multiplier** *multiplier* | **receive-interval** *interval* | **send-interval** *interval* } *	配置接口模式下动态 BFD 会话本地检测倍数、最小发送间隔、最小接收间隔。

10.2.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show bfd**	查看 BFD 全局配置信息。
2	Inspur#**show bfd** [*session-id*] **config**	查看指定 BFD 会话的配置信息。
3	Inspur#**show bfd** [*session-id*] **state**	查看指定 BFD 会话状态信息。
4	Inspur#**show bfd** [*session-id*] **statistics**	查看指定 BFD 会话统计信息。
5	Inspur#**show bfd** [*session-id*] **diagnostic-code**	查看诊断码。

10.3 CFM（IEEE802.1ag/ITU-Y.1731）

10.3.1 简介

CFM 是一种网络级以太网 OAM 技术，针对网络实现端到端的连通性故障检测、故障通告、故障判定和故障定位功能。用于对 EVC（Ethernet Virtual Connection，以太网虚连接）进行主动的故障诊断，并通过使用故障管理功能有效降低网络维护成本，提高以太网的可维护性。

交换机设备提供兼容 IEEE 802.1ag 和 ITU-T Y.1731 标准的 CFM 功能。

CFM 的相关概念

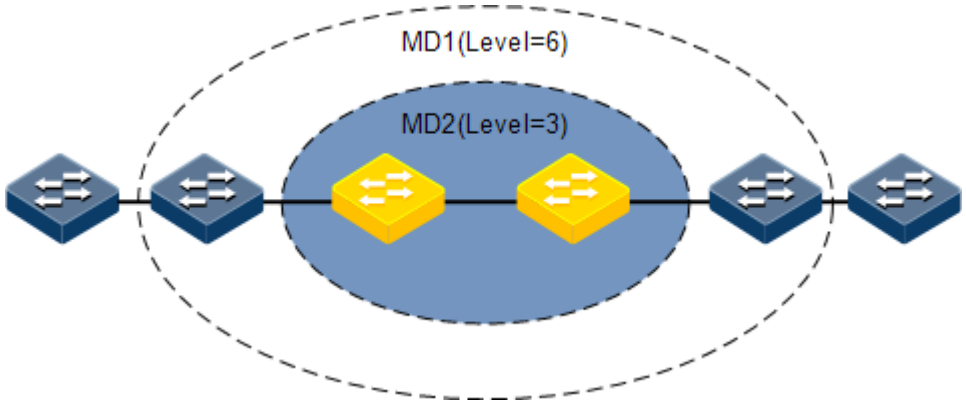
CFM 由如下组件组成：

- MD

维护域 MD（Maintenance Domain，又称 MEG，Maintenance Entity Group，维护实体组）是一个运行 CFM 功能的网络，它确定了进行 OAM 管理的网络范围。维护域具有级别属性，共分为 8 级（0～7），数字越大表示维护域级别越高，对应维护域的范围越大。低级别 MD 的协议报文进入高级别的 MD 后被丢弃，（如果高级别 MD 中不存在 MEP，而只有 MIP，则报文能够通过。）高级别 MD 的协议报文可以穿越低级别的 MD。在同一 VLAN 范围内，不同的维护域之间可以相邻、嵌套，但不能交叉。

如图 10-2 所示，MD2 包含在 MD1 中，MD1 的协议报文需要穿越 MD2。因此，将 MD1 的级别配置为 6，MD2 的级别配置为 3，这样 MD1 内的协议报文就可以穿越 MD2 实现整个 MD1 的连通性故障管理，而 MD2 的协议报文不会扩散到 MD1 中。MD2 为服务器层，MD1 为客户层。

图10-2 不同级别 MD 网络示意图



- 服务实例

服务实例（Service Instance）又称作 MA（Maintenance Association，维护联盟），是 MD 的一部分，一个 MD 可以划分成一个或多个服务实例。服务实例对应一个业务，可以映射到一组 VLAN，不同服务实例映射的 VLAN 不能交叉。虽然服务实例可以映射到多个 VLAN，但一个服务实例只能使用一个 VLAN 用于收发 OAM 报文，这个 VLAN 称为服务实例的主 VLAN。

- MEP

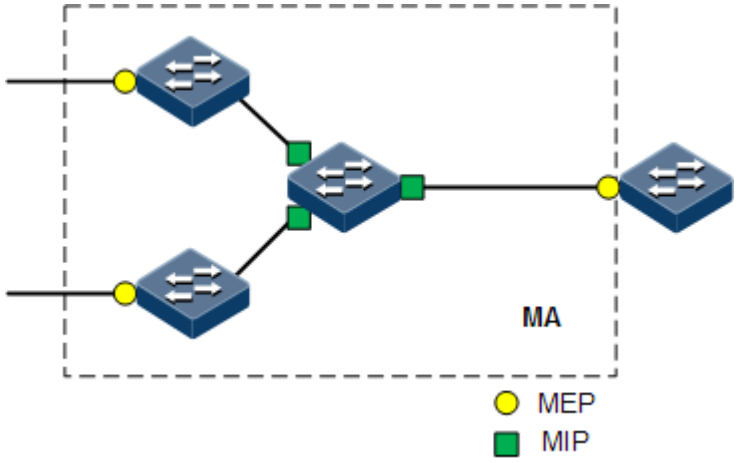
如图 10-3 所示，MEP（Maintenance associations End Point，维护联盟边缘节点）是服务实例的边缘节点。MEP 可以发送和处理 CFM 报文，MEP 所在服务实例和 MD 决定了 MEP 收发报文的 VLAN 和级别。

对于运行 CFM 的网络中的任意一台设备，该设备上的 MEP 称为本地 MEP，同一服务实例内其它设备上的 MEP 对本设备而言称为 RMEP（Remote Maintenance association End Point，远端维护联盟边缘节点）。

一个服务实例内可以配置多个 MEP，同一服务实例中的 MEP 发送的报文带有相同的 S-VLAN TAG，相同的优先级和相同的 C-VLAN TAG，MEP 可以接收同一服务实例中

其它 MEP 发送的 OAM 报文，并截止与自身同级或比自身级别低的报文，转发比自身级别高的报文。

图10-3 MEP 和 MIP 网络示意图



- MIP

如图 10-3 所示，MIP（Maintenance association Intermediate Point，维护联盟内部节点）是服务实例的内部节点，是设备按照规则自动创建的。MIP 不能主动发送 CFM 报文，但是可以处理和回应 LTM（LinkTrace Message，链路追踪消息）和 LBM（LoopBack Message，环回消息）报文。

- MP

MEP 和 MIP 统称为维护节点 MP（Maintenance Point）。

CFM 的功能

CFM 能够提供以下 OAM 功能：

- 故障检测功能

  故障检测功能是指使用 CC（Continuity Check，连续性检测）协议来检测一个以太网虚连接的连通性，确定 MP 之间的连接状态。该功能通过 MEP 周期性地发送 CCM（Continuity Check Message，连续性检测报文）实现，同一服务实例内其他 MEP 接收该报文，由此确定 RMEP 的状态。如果设备故障或者链路中间配置错误，会导致 MEP 无法正常接收和处理 RMEP 发送的 CCM。如果 MEP 在 3.5 个 CCM 间隔周期内未收到远端的 CCM 报文，则认为链路存在故障，会根据告警优先级配置发送故障告警。

- 故障确认功能

  故障确认功能利用 LB（LoopBack，环回功能），通过源 MEP 发送 LBM 和目的 MP 回应 LBR 以确定两个 MP 之间的连通性。源 MEP 发送 LBM 给要进行故障确认的 MP，当该 MP 收到 LBM 报文后，发送一个 LBR 给源 MEP，如果源 MEP 接收到 LBR，则确认路径是连通的，如果源 MEP 没有接收到 LBR，则确认存在连通性故障。

- 故障定位功能

故障定位功能利用 LT（LinkTrace，链路跟踪），通过源 MEP 发送 LTM 给目的 MP，LTM 传输路径上的每个 MP 设备都会回应 LTR 给源 MEP，通过记录有效的 LTR 和 LTM 定位故障点。

- 告警指示信号功能（AIS，Alarm Indication Signal）

  用于在服务器层（子层）检测到故障情况后终止告警。AIS 信息的帧可以由 MEP（包括服务器 MEP）在检测到故障情况时向客户层 MD 等级上发出。带有 ETH-AIS 信息的帧的传输在 MEP 上（或服务器 MEP 上）可以进行或终止。由于接收到带有 AIS 信息的帧时，该 AIS 帧不包含遇到故障的对等 MEP 信息，所以该 MEP 必须抑制所有对等 MEP 的告警，不管是否仍有连通性。通过告警指示信号功能，可以在服务器层（子层）发生故障的情况下，抑制在客户层的告警信息，使网络更易于进行维护和管理。

- 以太网锁定信号功能（LCK，Lock）

  用于通告服务器层（子层）MEP 的管理性锁定以及随后的数据业务流中断，该业务流是送往期待接收这业务流的 MEP 的。它使得接收带有 ETH-LCK 信息的帧的 MEP 能区分是故障情况，还是服务器层（子层）MEP 的管理性锁定动作。锁定是按需的 OAM 管理功能，需要对一个 MEP 进行管理锁定的典型应用场景是服务中断情况下的诊断测试。

- 以太网客户端信号故障功能（CSF）

  以太网客户端信号故障功能（ETH-CSF）用于向服务器层通告客户层的信号故障。

  当一个 UP 方向的 MEP 所在的客户侧产生故障时，会向对端 MEP 周期性地发送带有 LOS 标识的 CSF 报文。当对端 MEP 收到带有 LOS 标识的 CSF 报文时，会上报 CSF 告警。当客户侧故障恢复时，本地 MEP 会连续发送 3 个带有 DCI 标识的 CSF 报文，当对端 MEP 收到带有 DCI 标识的 CSF 报文时，退出 CSF 状态，并上报 CSF 清除告警。应用于抑制告警。

总之，CFM 实现了在端到端服务层面的 OAM 技术，降低了服务提供商的运行维护成本，在一定程度上可以提高服务提供商的竞争优势。

10.3.2 配置准备

场景

为拓展以太网技术在电信级网络中的应用，以太网需要达到与电信级传送网相同的服务水平。CFM 通过为电信级以太网提供全面的 OAM 工具解决了此问题。

前提

在配置 CFM 之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。
- 创建 VLAN。
- 将接口加入 VLAN。

10.3.3 使能 CFM

请在设备上进行以下配置。

只有在设备上使能了 CFM 功能后，CFM 的故障检测、定位等功能才能生效。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ethernet cfm enable**	全局使能 CFM 功能。 缺省情况下，使能全局 CFM 功能。
3	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
	Inspur(config)#**interface port-channel** *port-channel*	进入聚合组配置模式。
4	Inspur(config-gigaethernet1/1/*)#**ethernet cfm enable**	（可选）在接口上使能 CFM 功能。 缺省情况下，接口未使能 CFM 功能。
	Inspur(config-port-channel*)#**ethernet cfm enable**	在聚合组上使能 CFM 功能。 缺省情况下，聚合组未使能 CFM 功能。

10.3.4 配置 CFM 基本功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ethernet cfm domain** [**md-name** *domain-name*] **level** *level*	创建维护域。使用 md-name 参数指定维护域名称表示维护域为 802.1ag 风格，维护域下的 MA 和 CCM 报文均为 802.1ag 风格；不指定名称表示维护域为 Y.1731 风格，维护域下的 MA 和 CCM 报文均为 Y.1731 风格。如果指定了维护域的名称，维护域名称必须全局唯一，否则将导致维护域配置失败。  不同的维护域的级别不能相同，否则将导致维护域配置失败。
3	Inspur(config)#**service** *cis-id* **level** *level*	创建服务实例并进入服务实例配置模式。（维护域名称，服务实例名称）组成的字符串在全局范围内唯一。如果服务实例已经存在，使用此命令将直接进入服务实例配置模式。

步骤	配置	说明
4	Inspur(config-service)#**service vlan-list** *vlan-list* [**primary-vlan** *vlan-id*]	配置服务实例 VLAN 映射。 VLAN 列表中最多允许出现 32 个 VLAN，如不使用 primary-vlan 参数指定主 VLAN 则最小的 VLAN 作为服务实例的主 VLAN。服务实例中的所有 MEP 通过主 VLAN 进行收发包。 **说明** 由于使用主 VLAN 用作收发包，即在逻辑上将列表中所有非主 VLAN 映射到了主 VLAN。这种逻辑上的 VLAN 映射关系是全局性的，不同级别的服务实例的 VLAN 映射关系可以相同，但不能出现交叉。例如：服务实例 1 映射到 VLAN 12～VLAN 20，服务实例 2 映射到 VLAN 15～VLAN 30，其中 VLAN 15～VLAN 20 为交叉部分，配置非法。
5	Inspur(config-service)#**service mep [up |down]mpid** *mep-id* [*interface-type interface-number* | **port-channel** *port-channel*] [**priority** *priority*]	配置基于服务实例的 MEP。 配置此种 MEP 时，服务实例必须映射 VLAN。 缺省情况下，MEP 是 Up 方向，即向接口的上行方向检测故障。
6	Inspur(config-service)#**service sdp** { *interface-type backup-interface-number*|**port-channel** *port-channel-list* } { *interface-type backup-interface-number*|**port-channel** *port-channel-list* } **secondary**	配置基于服务实例的分发接口。 设备的上行接口才可配置为分发接口。

10.3.5 配置故障检测

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ethernet cfm errors archive-hold-time** *minute*	（可选）配置错误 CCM 报文的保存时间。设备上保存了所有 MEP 报告的故障信息。 缺省情况下，错误 CCM 报文的保存时间是 100 分钟。当系统配置了新的保存时间会立即检查数据库中的数据，如果有数据超出时间将立即清除数据。
3	Inspur(config)#**service** *cis-id* **level** *level*	进入服务实例配置模式。

步骤	配置	说明
4	Inspur(config-service)#**service cc interval** { **3ms** | **10ms** | **100ms** | **1** | **10** | **60** | **600** }	（可选）配置服务实例 CCM 报文发送时间间隔。 缺省情况下，服务实例的 CCM 报文发送时间间隔是 1 秒。CCM 报文发送功能使能的情况下，不能修改 CCM 报文发送间隔。 **说明** 当设备在 Down 方向或 802.1ag 风格的 Up 方向发送硬件 CC 报文时，参数 **3ms** | **10ms** | **100ms** 才支持，Y.1731 风格的 UP 方向发送软件 CC 报文，不支持参数 **3ms** | **10ms** | **100ms**。
5	Inspur(config-service)#**service cc enable mep** { *mep-id-list* | **all** }	使能 MEP 发送 CCM 报文。 缺省情况下，MEP 不发送 CCM 报文。
6	Inspur(config-service)#**service remote-mep** *mep-list* [**remote-mac** *mac-address*] [*interface-type interface-number*]	（可选）配置静态远端 MEP。配合 CCM 报文检测功能使用。 通过选择参数 remote-mac *mac-address* 指定远端 MEP 的 MAC 地址。
7	Inspur(config-service)#**service cvlan** *vlan-id*	（可选）配置 CFM OAM 报文的客户 VLAN，在 QinQ 组网环境中才需要配置。 缺省情况下，CFM OAM 报文不携带 C-TAG，当配置服务实例的客户 VLAN 后，服务实例下的所有 MEP 发送的 CCM、LTM、LBM、DMM 将携带双层 TAG，其中 C-TAG 是用此命令配置的客户 VLAN。
8	Inspur(config-service)#**service priority** *priority*	（可选）配置 CFM OAM 报文优先级。 配置报文优先级后，服务实例下所有 MEP 发送的 CCM、LBM、LTM、DMM 报文均使用指定的优先级。 缺省情况下，报文的优先级为 7。
9	Inspur(config-service)#**snmp-server trap cfm** { **all** | **macremerr** | **remerr** | **ccmerr** | **xcon** | **none** } **mep** { **all** | *mep-list* }	（可选）配置 CFM OAM 告警级别。

10.3.6 配置故障确认

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**service** *cis-id* **level** *level*	进入服务实例配置模式。
3	Inspur(config-service)#**ping** { *mac-address* | **mep** *mep-id*} [**ttl** *ttl-value*] [**count** *count-number*] [**size** *size-value*] [**source** *mep-id*] [**interval** *interval-value*] [**timeout** *time*] [**padding** { **prbs** | **pbrs-crc** | **null** | **null-crc** }] [**cos** *cos-value*] [**non-drop**] Inspur(config-service)#**ping ethernet multicast** [**size** *size-number*] [**timeout** *time-out*] [**padding** { **prbs** | **pbrs-crc** | **null** | **null-crc** }] [**cos** *cos-value*] [**non-drop**]	执行二层 ping 功能，用于故障确认。 缺省情况下，发送 LBM 报文个数为 5，报文 TLV 长度为 64，并自动寻找一个可用的源 MEP。 如果通过指定目的 mepid 的方式进行二层 ping 操作，CFM 需要先通过 mepid 找到目的 MEP 的 MAC 地址才能完成 ping 操作。源 MEP 发现远端 MEP 并且稳定后，会将远端 MEP 的数据信息保存在 MEP 下的远端 MEP 数据库中，从远端 MEP 数据库中根据 mepid 可以查找到远端 MEP 的 MAC 地址。

说明

- 在执行该命令之前，必须保证全局 CFM 功能使能，否则会执行失败；
- 如果服务实例中没有配置 MEP，会因为找不到源 MEP 导致 ping 操作失败；
- 如果指定的源 MEP 无效将导致 ping 操作失败，例如指定的源 MEP 不存在或者指定的源 MEP 所在接口 CFM 功能被禁用等情况；
- 如果指定目的 MEPID 进行 ping 操作，根据 MEPID 无法找到目的 MEP 的 MAC 地址将导致 ping 操作失败；
- 如果有其他用户正使用指定的源 MEP 发起 ping 操作将导致操作失败。

10.3.7 配置故障定位

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ethernet cfm traceroute cache enable**	（可选）使能故障定位数据库开关。开关处于关闭状态时，traceroute 的结果会在 traceroute 执行完毕后被自动清除。 缺省情况下，未使能故障定位数据库开关。
3	Inspur(config)#**ethernet cfm traceroute cache hold-time** *minute*	（可选）配置故障定位数据库数据保存时间。当故障定位数据库开关处于开启状态时，可对数据保存时间进行设置。 缺省情况下，保存时间为 100 分钟。

步骤	配置	说明
4	Inspur(config)#**ethernet cfm traceroute cache size** *size*	（可选）配置故障定位数据库可保存数据的条目数。当故障定位数据库开关处于使能状态时，可对数据库可保存数据的条目数进行设置。开关处于使能状态时，缺省可保存条数为 100；开关关闭时，不保存数据。
5	Inspur(config)#**service** *cis-id* **level** *level*	进入服务实例配置模式。
6	Inspur(config-service)#**traceroute** { *mac-address* [**ttl** *ttl*] [**source** *mep-id*] [**size** *size*] | **mep** *mep-id* [**ttl** *ttl*] [**source** *mep-id*] [**interface-mode**] [**timeout** *time*] [**size** *size*] }	执行二层 Traceroute 功能，用于故障定位。 缺省情况下，报文 TLV 长度为 64，并自动寻找一个可用的源 MEP。

说明

- 在执行该命令之前，必须保证全局 CFM 功能使能，否则会执行失败；
- 如果服务实例中没有配置 MEP，会因为找不到源 MEP 导致 Traceroute 操作失败；
- 如果指定的源 MEP 无效将导致 Traceroute 操作失败，例如指定的源 MEP 不存在或者指定的源 MEP 所在接口 CFM 功能被禁用等情况；
- 如果指定目的 MEPID 进行 Traceroute 操作，根据 MEPID 无法找到目的 MEP 的 MAC 地址将导致 Traceroute 操作失败；
- 如果 CC 功能未生效，通过配置静态远端 MEP 并且指定 MAC 地址，可以保证 2 层 traceroute 操作正常使用；
- 如果有其他用户正使用指定的源 MEP 发起 Traceroute 操作将导致操作失败。

10.3.8 配置告警指示信号功能

请在设备上进行以下配置。

- 在服务器层设备上进行如下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**service** *cis-id* **level** *level*	进入服务实例配置模式。
3	Inspur(config-service)#**service ais enable**	使能 AIS 发送功能。 缺省情况下，系统未使能 AIS 发送功能。

步骤	配置	说明
4	Inspur(config-service)#**service ais period** { **1** | **60** }	配置 AIS 发送周期。 缺省情况下，发送周期为 1 秒。
5	Inspur(config-service)#**service ais level** *level*	配置 AIS 被发送到的客户层 MD 的级别。

- 在客户层设备上进行如下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**service** *cis-id* **level** *level*	进入服务实例配置模式。
3	Inspur(config-service)#**service suppress-alarms enable mep** { *mep-id* | **all** }	使能告警抑制功能。 缺省情况下，告警抑制功能使能。

10.3.9 配置以太网锁定信号功能

请在设备上进行以下配置。

- 在服务器层设备上进行如下配置：

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**service** *cis-id* **level** *level*	进入服务实例配置模式。
3	Inspur(config-service)#**service lck start mep** { *mep-id* | **all** }	使能 LCK 报文发送功能。 缺省情况下，系统未使能 LCK 发送功能。
4	Inspur(config-service)#**service lck period** { **1** | **60** }	配置 LCK 报文发送周期。 缺省情况下，发送周期为 1 秒。
5	Inspur(config-service)#**service lck level** *level* [**vlan** v*lan-id*]	配置 LCK 被发送到的客户层 MD 的级别。

- 在客户层设备上进行如下配置：

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**service** *cis-id* **level** *level*	进入服务实例配置模式。

步骤	配置	说明
3	Inspur(config-service)#**service suppress-alarms enable mep** { *mep-id* |**all** }	使能告警抑制功能。 缺省情况下，告警抑制功能使能。

10.3.10 配置以太网客户信号失效功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**service** *csi-id* **level** *ma-level*	进入 MA 配置模式。
3	Inspur(config-service)#**service csf enable mpid** *mep-id*	使能 CSF（Client Signal Fail，客户信号失效）报文发送功能。 缺省情况下，设备没有使能 CSF 报文的发送功能。
4	Inspur(config-service)#**service csf period** { **1**|**60** }	配置 CSF 报文的发送周期。仅适用于 PW OAM。 缺省情况下，设备发送 CFM 报文的周期为 1s。
5	Inspur(config-service)#**service csf trap enable**	使能 CSF 模块的 Trap 上送功能。仅适用于 PW OAM。 缺省情况下，设备没有使能 CSF 模块的 Trap 上送功能。

10.3.11 配置性能监控

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**service** *csi-id* **level** *ma-level*	进入 MA 配置模式。
3	Inspur(config-service)#**service pm enable mep** { **all** | *mep-id* }	使能 MEP 的性能监控功能。

10.3.12 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

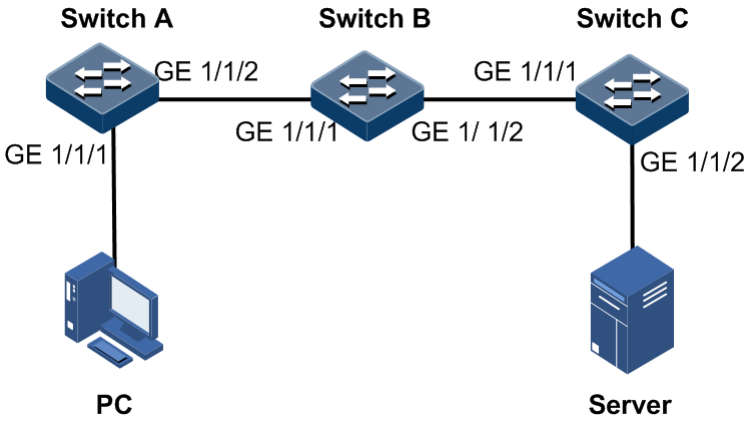
序号	检查项	说明
1	Inspur#**show ethernet cfm**	查看 CFM 全局配置信息。
2	Inspur#**show ethernet cfm domain** [**level** *level*]	查看维护域及服务实例配置信息。
3	Inspur#**show ethernet cfm errors** [**level** *level*]	查看错误 CCM 数据库信息。
4	Inspur#**show ethernet cfm lck** [**level** *level*] [**source**]	查看以太网锁定信号。
5	Inspur#**show ethernet cfm local-mp** [interface *interface-type interface-number*| **level** *level*]	查看本地的 MEP 配置信息。
6	Inspur#**show ethernet cfm remote-mep** [**level** *level*]**static**	查看静态远端 MEP 信息。
7	Inspur#**show ethernet cfm remote-mep**[**level** *level*[**service** *service-instance*[**mpid** *mep-id*]]]	查看远端 MEP 发现信息。
8	Inspur#**show ethernet cfm suppress-alarms** [**level** *level*]	查看 CFM 告警抑制功能的配置信息。
9	Inspur#**show ethernet cfm traceroute-cache**	查看故障定位数据库路径发现信息。

10.3.13 配置 CFM 应用示例

组网需求

如图 10-4 所示，用户通过 Switch A、Switch B 和 Switch C 组成的网络与服务器通信，为使服务器与用户之间的以太链路达到电信级的服务水平，需要在 Switch 设备上部署 CFM 特性，实现主动的故障检测、确认和定位。Switch A 和 Switch C 为 MEP，Switch B 为 MIP，检测由 Switch A 的 Port 1 到 Switch C 的 Port 2 之间的以太网故障，维护域级别为 3 级。

图10-4 CFM 应用组网示意图



配置步骤

步骤 1 配置接口加入 VLAN。

配置 Switch A。

```
Inspur#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 100 active
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport access vlan 100
SwitchA(config-gigaethernet1/1/1)#exit
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#switchport mode trunk
SwitchA(config-gigaethernet1/1/2)#exit
```

配置 Switch B。

```
Inspur#hostname SwitchB
SwitchB#config
SwitchB(config)#interface gigaethernet 1/1/1
SwitchB(config-gigaethernet1/1/1)#switchport mode trunk
SwitchB(config-gigaethernet1/1/1)#exit
SwitchB(config)#interface gigaethernet 1/1/2
SwitchB(config-gigaethernet1/1/2)#switchport mode trunk
SwitchB(config-gigaethernet1/1/2)#exit
```

配置 Switch C。

```
Inspur#hostname SwitchC
SwitchC#config
SwitchC(config)#create vlan 100 active
SwitchC(config)#interface gigaethernet 1/1/2
SwitchC(config-gigaethernet1/1/2)#switch access vlan 100
SwitchC(config-gigaethernet1/1/2)#exit
SwitchC(config)#interface gigaethernet 1/1/1
SwitchC(config-gigaethernet1/1/1)#switchport mode trunk
SwitchC(config-gigaethernet1/1/1)#exit
```

步骤 2 配置 CFM 故障检测功能。

配置 Switch A。

```
SwitchA(config)#ethernet cfm domain level 3
SwitchA(config)#service ma1 level 3
SwitchA(config-service)#service vlan-list 100
SwitchA(config-service)#service mep up mpid 301 gigaethernet 1/1/1
SwitchA(config-service)#service remote-mep 302
SwitchA(config-service)#service cc enable mep all
SwitchA(config-service)#exit
SwitchA(config)#ethernet cfm enable
```

配置 Switch B。

```
SwitchB(config)#ethernet cfm domain level 3
SwitchB(config)#service ma1 level 3
SwitchB(config-service)#service vlan-list 100
SwitchB(config-service)#exit
SwitchB(config)#ethernet cfm enable
```

配置 Switch C。

```
SwitchC(config)#ethernet cfm domain level 3
SwitchC(config)#service ma1 level 3
SwitchC(config-service)#service vlan-list 100
SwitchC(config-service)#service mep up mpid 302 gigaethernet 1/1/2
SwitchC(config-service)#service remote mep 301
SwitchC(config-service)#service cc enable mep all
SwitchC(config-service)#exit
SwitchC(config)#ethernet cfm enable
```

步骤 3 执行 CFM 故障确认。

以 Switch A 为例。

```
Switch(config)#service ma1 level 3
Switch(config-service)#ping mep 302 source 301
Sending 5 ethernet cfm loopback messages to 000e.5e03.688d, timeout is
2.5 seconds:
!!!!!
Success rate is 100 percent (5/5).
Ping statistics from 000e.5e03.688d:
Received loopback replys：< 5/0/0 > (Total/Out of order/Error)
Ping successfully.
```

步骤 4 执行 CFM 故障定位。

以 Switch A 为例。

```
SwitchA(config)#service ma1 level 3
SwitchA(config-service)#traceroute mep 302 source 301
TTL: <64>
Tracing the route to 000E.5E00.0002 on level 3, service ma1.
Traceroute send via port1.
------------------------------------------------------------------------
---------
Hops  HostMac       Ingress/EgressPort  IsForwarded  RelayAction  NextHop
```

```
------------------------------------------------------------------------
---------
 1    000E.5E00.0003      2/1         Yes         rlyFdb      000E.5E00.0003
 2    000E.5E00.0003      1/2         Yes         rlyFdb      000E.5E00.0001
 3    000E.5E00.0001      1/-          No          rlyHit      000E.5E00.0002
```

检查结果

在交换机设备上通过 **show ethernet cfm** 查看 CFM 配置是否正确。

以 Switch A 为例：

```
SwitchA#show ethernet cfm
Global CFM Admin Status: enable
Port CFM Enabled Portlist: P:1-28  PC:1-3
Archive hold time of error CCMs: 100(Min)
Remote mep aging time: 100(Min)
Device mode: Slave
```

11 可靠性

本章介绍了网络可靠性的基本原理和配置过程，并提供相关的配置案例。

- 链路聚合
- 故障转移
- VRRP
- 接口备份
- KEY-CHAIN
- UDLD

11.1 链路聚合

11.1.1 简介

链路聚合通过将多个物理以太网接口聚合在一起形成一个逻辑上的聚合组，并把同一聚合组内的多条物理链路视为一条逻辑链路。链路聚合可以实现流量在聚合组各成员接口之间负载分担，在有效提高设备之间链路可靠性的同时，还在不进行硬件升级的条件下增大了带宽。

按照聚合方式的不同，设备支持以下 2 种链路聚合方式：

- 手工聚合方式

手工聚合方式将多个物理接口加入链路聚合组，形成一个逻辑接口，同一逻辑接口下的链路实现负荷分担。

- 静态 LACP 聚合方式

LACP（Link Aggregation Control Protocol，链路聚合控制协议）是一种基于 IEEE802.3ad 标准的协议。LACP 协议通过 LACPDU（Link Aggregation Control Protocol Data Unit，链路聚合控制协议数据单元）与对端交互信息，也需要用户手工配置聚合组。使能某接口的 LACP 协议后，该接口将通过发送 LACPDU 向对端通告自己的系统 LACP 协议优先级、系统 MAC、接口的 LACP 协议优先级、接口号和操作 Key。

对端接收到 LACPDU 后，将其中的信息与其它接口所收到的信息进行比较，以选择能够处于 Selected 状态的接口，从而双方可以对接口处于 Selected 状态达成一致。操作

Key 是在链路聚合时，聚合控制根据接口的配置（即速率、双工模式、Up/Down 状态、基本配置等信息）自动生成的一个配置组合。在聚合组中，处于 Selected 状态的接口有相同的操作 Key。

11.1.2 配置准备

场景

当需要为 2 台设备之间的链路提供更高的通讯带宽和更高的可靠性时，可以配置选择手工模式或者静态 LACP 链路聚合功能。

前提

- 在配置链路聚合之前，需配置接口的物理参数，使接口的物理层状态为 Up。
- 在同一个链路聚合组中，参与负载分担的成员接口必须有一致的配置，否则数据转发存在问题。这些配置主要包括 QoS、QinQ、VLAN、接口属性、MAC 地址学习几个方面：
  - QoS 配置一致：流量监管、流量整形、拥塞避免、接口限速、SP 队列、WRR 队列调度、WFQ 队列、接口优先级、接口信任模式。
  - QinQ 配置一致：接口的 QinQ 功能使能/禁用状态、添加的外层 VLAN Tag、不同内层 VLAN ID 添加外层 VLAN Tag 的策略。
  - VLAN 配置一致：接口上允许通过的 VLAN、接口缺省 VLAN ID、接口的链路类型（即 Trunk、Hybrid、Access 类型）、子网 VLAN 配置、协议 VLAN 配置、VLAN 报文是否带 Tag 配置。
  - 接口属性配置一致：接口是否加入隔离组、接口速率、双工模式、链路 up/down 状态。
  - MAC 地址学习配置一致：是否使能 MAC 地址学习功能、接口是否具有最大学习 MAC 地址个数的限制。

11.1.3 配置手工链路聚合

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#interface port-channel` *`channel-number`*	进入聚合组配置模式。
3	`Inspur(config-port-channel*)#mode manual`	配置链路聚合组的工作模式为手工链路聚。
4	`Inspur(config-port-channel*)#{ max-active | min-active } links` *`value threshold`*	（可选）配置 LACP 链路聚合组最大或最小的活跃链路数量。 缺省情况下，最大活跃链路数为 8，最小活跃链路数为 1。

步骤	配置	说明
5	Inspur(config-port-channel*)#**load-sharing mode** { **dst-ip** | **dst-mac** | **src-dst-ip** | **src-dst-mac** | **src-ip** | **src-mac** }	（可选）配置链路聚合组的负载均衡模式。 缺省情况下，系统采用 **sxordmac** 模式，即依据源和目的 MAC 地址逻辑或的结果选择转发接口。
6	Inspur(config-port-channel*)#**exit**	返回全局配置模式。

11.1.4 配置静态 LACP 链路聚合

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**lacp system-priority** *system-priority*	（可选）配置 LACP 协议优先级，优先级高的一端为主动端，LACP 按主动端的配置情况选择活动接口和备份接口。数值越小优先级越高，系统 LACP 优先级相同时，选择系统 MAC 地址小的作为主动端。 缺省情况下，系统的 LACP 优先级为 32768。
3	Inspur(config)#**lacp timeout** { **fast** | **slow** }	（可选）配置 LACP 超时模式。 缺省情况下，LACP 超时模式为慢速模式。
4	Inspur(config)#**interface port-channel** *channel-number*	进入聚合组配置模式。
5	Inspur(config-port-channel*)#**mode lacp**	配置链路聚合组的工作模式为静态 LACP 链路聚合。
6	Inspur(config-port-channel*)#{ **max-active** | **min-active** } **links** *value threshold*	（可选）配置 LACP 链路聚合组最大或最小的活跃链路数量。 缺省情况下，最大活跃链路数为 8，最小活跃链路数为 1。
7	Inspur(config-port-channel*)#**lacp priority preempt enable**	使能链路聚合组的优先级抢占功能。
8	Inspur(config-port-channel*)#**lacp wait-timer** *time*	配置端口恢复延时。
9	Inspur(config-port-channel*)#**exit**	退回全局配置模式。
10	Inspur(config)#**interface** *interface-type interface-number*	进入二层或三层物理接口配置模式。
11	Inspur(config-gigaethernet1/1/*)#**port-channel** *channel-number*	将二层物理接口加入链路聚合组。

步骤	配置	说明
12	Inspur(config-gigaethernet1/1/*)#**lacp mode** { **active** | **passive** }	（可选）配置成员接口的 LACP 协议模式，同一链路两端均为被动模式时，LACP 连接无法建立。 缺省情况下，LACP 协议模式是主动模式。
13	Inspur(config-gigaethernet1/1/*)#**lacp port-priority** *port-priority*	（可选）配置接口的 LACP 协议优先级，接口协议优先级影响 LACP 协议的缺省接口的选举，数值越小优先级越高。 缺省情况下，系统的 LACP 优先级为 32768。

说明

- 在静态 LACP 链路聚合组中，成员接口可以处于 Active 或 Standby 两种状态。Active 接口和 Standby 接口都能收发 LACP 协议报文，但 Standby 接口不能转发用户报文。
- 系统按照是否发现邻居、接口速率最大、接口 LACP 协议优先级最高、接口号最小的顺序选择缺省接口，缺省接口处于 Active 状态，与缺省接口具有相同速率、相同对端设备和对端设备操作 key 的接口也处于 Active 状态，其他接口则处于 Standby 状态。

11.1.5 配置手工主备方式链路聚合

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface port-channel** *channel-number*	进入聚合组配置模式。
3	Inspur(config-port-channel*)#**mode manual backup**	配置链路聚合组的工作模式为手工备份方式链路聚合。
4	Inspur(config-port-channel*)#**master-port** *interface-type interface-number*	配置链路聚合的主接口。
5	Inspur(config-port-channel*)#**restore-mode** { **non-revertive** | **revertive** [**restore-delay** *second*] }	配置链路聚合组恢复模式及延迟恢复时间。 缺省情况下，聚合组恢复模式为非返回模式。
6	Inspur(config-port-channel*)#**exit**	返回全局配置模式。
7	Inspur(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。

步骤	配置	说明
8	Inspur(config-gigaethernet1/1/*)#**port-channel** *channel-number*	将成员接口加入链路聚合组中。
9	Inspur(config-gigaethernet1/1/*)#**exit**	退回全局配置模式。

说明

在配置链路聚合组故障返回模式为非返回模式时，必须先通过 **master-port** 命令进行主接口的配置。

11.1.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

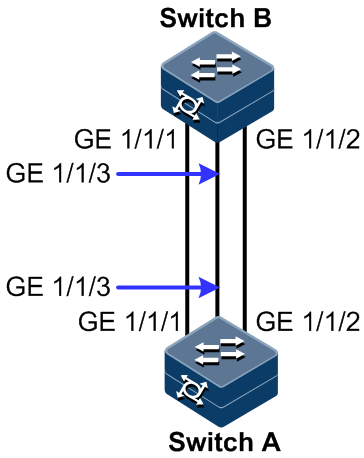
序号	检查项	说明
1	Inspur#**show lacp internal**	查看本端系统 LACP 协议接口状态、标志、接口优先级、管理 key、操作 key 和接口状态机状态。
2	Inspur#**show lacp neighbor**	查看邻居 LACP 协议信息，包括标志、接口优先级、设备 ID、Age、操作键值、接口号、接口状态机状态。
3	Inspur#**show lacp statistics**	查看接口 LACP 协议统计信息，包括 LACP 报文的总收发数、Marker 报文的收发数、Marker Response 报文的收发数和错误报文数。
4	Inspur#**show lacp sys-id**	查看本端系统 LACP 协议全局使能情况，设备 ID，包括系统的 LACP 协议优先级与系统 MAC 地址。
5	Inspur#**show port-channel** [*channel-number*]	查看当前系统是否使能聚合链路、链路聚合负载均衡模式、当前所有聚合组设置的组成员接口列表和当前生效的成员接口列表等信息。 **说明** 当前生效的成员接口是指组成员接口中接口状态为 Up 的接口列表。

11.1.7 配置静态 LACP 方式的链路聚合示例

组网需求

如图 11-1 所示，为提高 Switch A 与 Switch B 之间链路的可靠性，在 Switch A 与 Switch B 之间配置静态 LACP 方式的链路聚合，将 GE 1/1/1、GE 1/1/2 和 GE 1/1/3 加入链路聚合组，其中 GE 1/1/1 和 GE 1/1/2 作为活动接口，GE 1/1/3 作为备份接口。

图11-1 静态 LACP 方式链路聚合应用组网示意图



配置步骤

步骤 1 在 Switch A 上配置静态 LACP 链路聚合组，并将 Switch A 配置成主动端。

```
Inspur#hostname SwitchA
SwitchA#config
SwitchA(config)#lacp system-priority 1000
SwitchA(config)#interface port-channel 1
SwitchA(config-port-channel1)#mode lacp
SwitchA(config-port-channel1)#max-active links 2
SwitchA(config-port-channel1)#exit
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#portswitch
SwitchA(config-gigaethernet1/1/1)#port-channel 1
SwitchA(config-gigaethernet1/1/1)#lacp port-priority 1000
SwitchA(config-gigaethernet1/1/1)#exit
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#portswitch
SwitchA(config-gigaethernet1/1/2)#port-channel 1
SwitchA(config-gigaethernet1/1/2)#lacp port-priority 1000
SwitchA(config-gigaethernet1/1/2)#exit
SwitchA(config)#interface gigaethernet 1/1/3
SwitchA(config-gigaethernet1/1/3)#portswitch
SwitchA(config-gigaethernet1/1/3)#port-channel 1
SwitchA(config-gigaethernet1/1/3)#exit
```

步骤 2 在 Switch B 上配置静态 LACP 链路聚合组。

```
Inspur#hostname SwitchB
SwitchB#config
SwitchB(config)#interface gigaethernet 1/1/1
SwitchB(config-gigaethernet1/1/1)#portswitch
SwitchB(config-gigaethernet1/1/1)#port-channel 1
SwitchB(config-gigaethernet1/1/1)#exit
SwitchB(config)#interface gigaethernet 1/1/2
SwitchB(config-gigaethernet1/1/2)#portswitch
SwitchB(config-gigaethernet1/1/2)#port-channel 1
```

```
SwitchB(config-gigaethernet1/1/2)#exit
SwitchB(config)#interface gigaethernet 1/1/3
SwitchB(config-gigaethernet1/1/3)#portswitch
SwitchB(config-gigaethernet1/1/3)#port-channel 1
SwitchB(config-gigaethernet1/1/3)#exit
```

检查结果

在 Switch A 上通过 **show port-channel** 查看静态 LACP 方式链路聚合全局配置是否正确。

```
SwitchA#show port-channel
Group 1 information:
Mode   :  Lacp          Load-sharing mode  : src-dst-mac
MinLinks:  1                  Max-links        : 2
UpLinks :  3                  Priority-Preemptive: Disable
Member Port  :  gigaethernet1/1/1 gigaethernet1/1/2 gigaethernet1/1/3
Efficient Port: gigaethernet1/1/1 gigaethernet1/1/2
```

在 Switch A 上通过 **show lacp internal** 查看本端系统 LACP 协议接口状态、标志、接口优先级、管理 Key、操作 Key 和接口状态机状态配置是否正确。

```
SwitchA#show lacp internal
Flags:
  S - Device is requesting Slow LACPDUs  F - Device is requesting Fast
LACPDUs
  A - Device in Active mode  P - Device in Passive mode   MP - MLACP Peer
Port
Interface               State      Flag    Port-Priority   Admin-key  Oper-
key   Port-State
------------------------------------------------------------------------
----------------------
gigaethernet1/1/1       Active     SA      1000          1        2
0x3D
gigaethernet1/1/2       Active     SA      1000          1        2
0x3D
gigaethernet1/1/3       Standby    SA      32768         1        2
0x5
```

在 Switch A 上通过 **show lacp neighbor** 查看对端系统 LACP 协议接口状态、标志、接口优先级、管理 Key、操作 Key 和接口状态机状态配置是否正确。

```
SwitchA#show lacp neighbor
Flags:
  S - Device is requesting Slow LACPDUs  F - Device is requesting Fast
LACPDUs
  A - Device in Active mode  P - Device in Passive mode  MP - MLACP Peer
Port
Interface               Flag Port-Priority Age   Device-ID      Oper-key
Partner-Port Port-State
------------------------------------------------------------------------
---------------------------
gigaethernet1/1/1       SA    32768      23s   000E.5EAB.CDEF  1       17
0x3D
gigaethernet1/1/2       SA    32768      14s   000E.5EAB.CDEF  1       18
0xD
```

```
gigaethernet1/1/3       SA    32768      10s   000E.5EAB.CDEF  1       19
0xD
```

11.2 故障转移

11.2.1 简介

故障转移功能提供了一种接口联动方案，可以扩展链路备份的范围，即通过监控上行链路并对下行链路进行同步设置，将上、下行接口加入到一个故障转移组中，使上层设备的故障迅速传达给下层，从而触发主备切换。故障转移功能可避免因上行链路故障无法被下层设备感知而出现的流量丢失。

一旦上行接口全部故障，则下行接口就会被置为 Down 状态，并且只要有一个上行接口恢复后，下行接口就将恢复 Up 状态，从而及时的将上行链路的故障情况通知到下层设备。下行接口故障时不影响上行接口。

11.2.2 配置准备

场景

中间设备上行链路故障时，如无法及时通知下层设备，会导致流量不能切换到备份路径，从而产生流量中断。

故障转移特性将中间设备的上行接口和下行接口加入同一故障转移组，并实时监控上行接口，当上行接口全部故障时，使上层设备的故障迅速传达给下层，保证主链路向备份链路的快速切换，以尽可能减少流量丢失。

前提

无

11.2.3 故障转移功能的缺省配置

设备上故障转移功能的缺省配置如下。

功能	缺省值
故障转移组	无
接口故障处理动作	无
故障转移组 Trap 告警功能	禁止

11.2.4 配置故障转移

说明

故障转移支持物理接口及聚合组接口配置。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**link-state-tracking group** *group-number*	创建转移组并使能故障转移功能。
3	Inspur(config)#**link-state-tracking group** *group-number* **trap** { **enable** | **disable** }	配置故障转移上报 Trap 功能。
4	Inspur(config)#**link-state-tracking group** *group-number* **upstream ma-name** *ma-name* **cfm-mepid** *cfm-mepid* **level** *level*	配置基于远端 MEP 的故障转移组。
5	Inspur(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
6	Inspur(config-gigaethernet1/1/*)#**link-state-tracking group** *group-number* { **downstream** | **upstream** }	配置接口所属转移组和接口类型。一个接口只能属于一个故障转移组，并且只能配置成上行接口或者下行接口。
7	Inspur(config-gigaethernet1/1/*)#**link-state-tracking group** *group-number* **action modify-pvid** *vlan-id*	配置故障转移组的故障处理动作为修改 PVID。

说明

一个故障转移组中可以有多个上行接口，只要有一个上行接口为 Up 状态就不会发生故障转移；只有当全部上行接口都为 Down 的状态时才发生故障转移。

在全局模式下，使用 **no link-state-tracking group** *group-number* { **downstream** | **upstream** }命令禁止故障转移功能时，如果此转移组下无接口，则会删除此转移组。

在物理层接口模式下，使用 **no link-state-tracking group** *group-number* { **downstream** | **upstream** }命令从故障转移组中删除一个接口。

11.2.5 配置故障转移组的故障处理动作

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**link-state-tracking group** *group-number* **action** { **block-vlan** *vlan-id interface-type interface-number* | **delete-vlan** *vlan-id* | **flush-erps** *rind-id* | **suspend-vlan** *vlan-id* }	配置故障转移组故障处理模式。

11.2.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show link-state-tracking group** [*group-number*]	查看故障转移组配置和状态信息。

11.2.7 配置故障转移示例

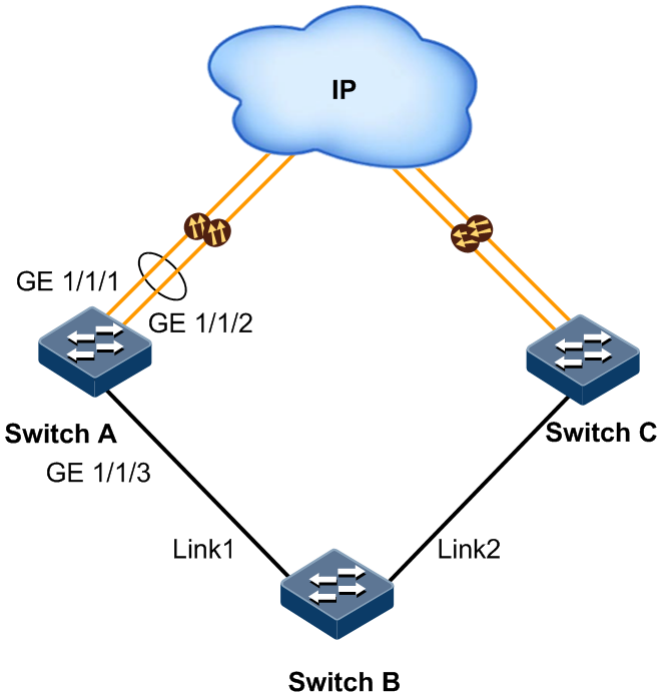
组网需求

如图 11-2 所示，为提高网络可靠性，Switch B 通过 Link1 和 Link2 两条链路分别连接到 Switch A 和 Switch C，Link1 为主链路，Link2 为备份链路，只有在 Link1 故障时，才启用 Link2 转发数据。

Switch A 和 Switch C 上行通过链路聚合的方式与上级网络相连，在 Switch A 或 Switch C 上行链路全部故障时，需要及时让 Switch B 感知，从而及时将流量切换到备份链路。

所以需要在 Switch A 和 Switch C 上部署故障转移特性。

图11-2 故障转移应用组网示意图



配置步骤

步骤 1 配置 Switch A 的故障转移功能。

创建链路聚合组 1，并将上行口 GE 1/1/1 和 GE 1/1/2 加入到链路聚合组中。

```
Inspur#config
Inspur(config)#interface gigaethernet 1/1/1
Inspur(config-gigaethernet1/1/1)#port-channel 1
Inspur(config-gigaethernet1/1/1)#exit
Inspur(config)#interface gigaethernet 1/1/2
Inspur(config-gigaethernet1/1/2)#port-channel 1
Inspur(config-gigaethernet1/1/2)#exit
```

创建故障转移组 1，将链路聚合组接口加入到故障转移组中。

```
Inspur(config)#link-state-tracking group 1
Inspur(config)#interface port-channel 1
Inspur(config-port-channel1)#link-state-tracking group 1 upstream
Inspur(config-port-channel1)#exit
```

将下行接口 GE 1/1/3 加入到故障转移组中。

```
Inspur(config)#interface gigaethernet 1/1/3
Inspur(config-gigaethernet1/1/3)#link-state-tracking group 1 downstream
```

步骤 2 在 Switch C 上配置故障转移功能。

配置同 Switch A，略。

检查结果

以 Switch A 为例，通过 **show link-state-tracking group** 查看故障转移组配置是否正确。

```
SwitchA#show link-state-tracking group 1
Link-state-tracking Group: 1
Trap State: disable
UpStream Type: port
UpStream PortList: portchannel 1
Action Mode: Shutdown-port
Action PortList: gigaethernet 1/1/3
Link-state-tracking State: normal
Fault-type: none
```

Switch A 上行链路均故障后，再次通过 **show link-state-tracking group** 查看故障转移组配置可以看到已经发生故障转移。

```
SwitchA#show link-state-tracking group 1
Link-state-tracking Group: 1
Trap State: enable
UpStream Type: port
UpStream PortList: portchannel 1
Action Mode: Shutdown-port
Action PortList: gigaethernet 1/1/3
Link-state-tracking State: failover
Fault-type: port-shutdown
```

11.3 VRRP

11.3.1 配置准备

场景

在网络环境中，通常会为同局域网内的所有主机配置一条指向出口网关的缺省路由，实现局域网内主机与外部网络之间的通信。如果该网关发生故障，则局域网内主机与外部网络的通信就会中断。

VRRP 技术将多台路由器组合到一起形成备份组，用户通过为备份组配置虚拟 IP 地址，使用时只需要将局域网主机的缺省网关配置为备份组的虚拟 IP 地址，即可实现局域网内主机与外部网络之间的通信。

VRRP 功能的部署可以提高网络的可靠性，有效避免因为单一链路中断而造成的网络中断的问题，也无需因为链路中断而更改路由配置。

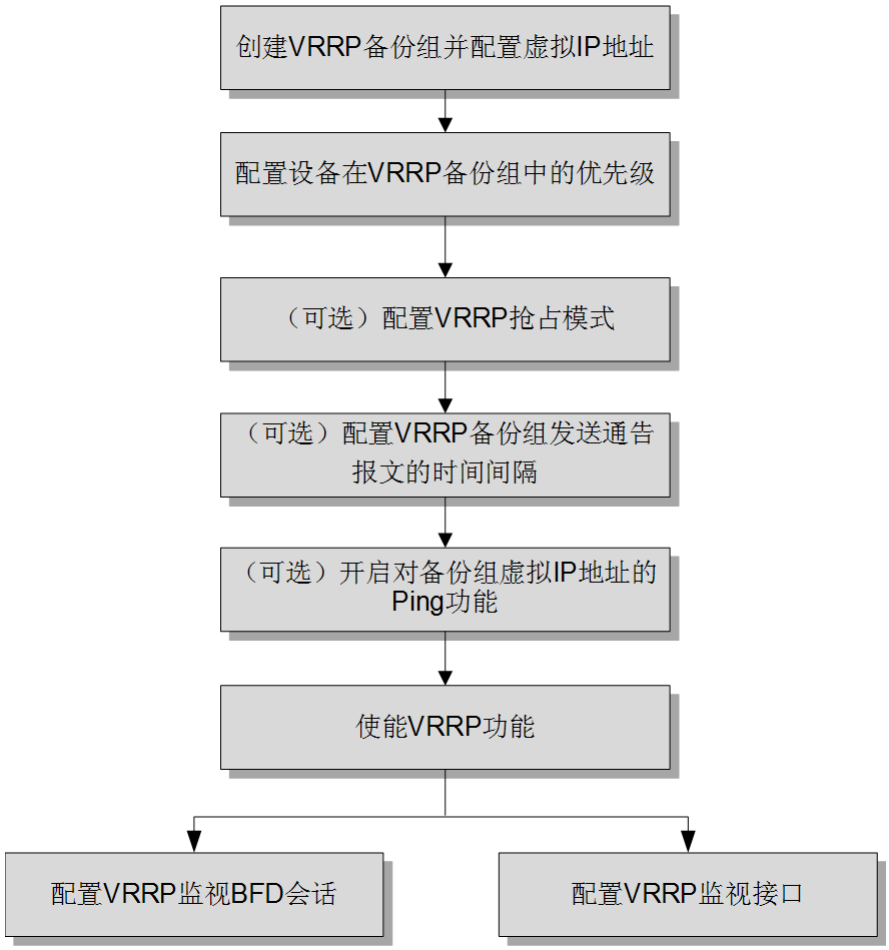
前提

无

11.3.2 配置流程

VRRP 配置流程如图 11-3 所示。

图11-3 VRRP 配置流程



11.3.3 配置 VRRP 备份组

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#interface` *interface-type interface-number*	进入三层物理接口接口配置模式。
3	`Inspur(config-gigaethernet1/1/*)#vrrp` *group-id* `ip` *ip-address*	创建 VRRP 备份组并为备份组配置虚拟 IP 地址。虚拟 IP 地址必须与接口 IP 地址在同一网段。

步骤	配置	说明
4	Inspur(config-gigaethernet1/1/*)#**vrrp** *group-id* **description** *description*	（可选）配置 VRRP 备份组描述信息。
5	Inspur(config-gigaethernet1/1/*)#**vrrp** *group-id* **preempt** [**delay-time** *second*]	（可选）开启 VRRP 备份组抢占模式。 缺省情况下，新创建的 VRRP 备份组处于抢占模式，抢占延迟时间是 0 秒。
6	Inspur(config-gigaethernet1/1/*)#**vrrp** *group-id* **priority** *priority*	配置设备在 VRRP 备份组中的优先级。 缺省情况下，新创建的 VRRP 备份组，其优先级是 100。
7	Inspur(config-gigaethernet1/1/*)#**vrrp** *group-id* **timers advertise-interval** *seconds*	（可选）配置 VRRP 备份组发送通告报文的时间间隔。 缺省情况下，发送通告报文的时间间隔是 1 秒。
8	Inspur(config-gigaethernet1/1/*)#**vrrp** *group-id* **enable**	使能 VRRP 功能。 缺省情况下，新创建的备份组 VRRP 功能已使能。

11.3.4 配置 VRRP 虚拟地址 Ping 开关

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**vrrp ping**	开启对备份组虚拟 IP 地址的 Ping 功能。 缺省情况下，开启对新创建的 VRRP 备份组的虚拟 IP 地址的 Ping 功能。

11.3.5 配置 VRRP 监视接口

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入三层物理接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**vrrp** *group-id* **track** *interface-type interface-number* [**reduced** *priority*]	配置 VRRP 监视接口功能。

reduced *priority*：当被监视接口从 UP 状态变为 DOWN 状态时，优先级减少的数值，整数形式，取值范围是 1～255，不配置该参数，设备在备份组中的优先级在原有基础上降低 10，减少后的优先级范围是 1～254

当被监视接口从 DOWN 状态变为 UP 状态时，优先级恢复原来的数值，建议在 Master 设备进行配置。

11.3.6 配置 BFD for VRRP

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入三层物理接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**vrrp** *group-id* **track bfd-session** *session-id* [**increased** *priority* | **reduced** *priority*]	配置 VRRP 备份组对 BFD 会话进行监测，以达到快速切换的目的。

increased *priority*：配置当被监视的 BFD 会话状态变为 DOWN 时，优先级增加的数值，整数形式，取值范围是 1～255，增加后的优先级范围是 1～254。如果从 DOWN 状态变为 UP 状态，则优先级恢复原来的数值。建议在 Backup 设备上进行配置。

reduced *priority*：配置当被监视的 BFD 会话状态变为 DOWN 时，优先级降低的数值，整数形式，取值范围是 1～255，减少后的优先级范围是 1～254。如果从 DOWN 状态变为 UP 状态，则优先级恢复原来的数值。建议在 Master 设备上进行配置。

11.3.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show vrrp** *group-id*	查看 VRRP 备份组的配置信息。
2	Inspur#**show vrrp interface** *interface-type interface-number* [*group-id*]	查看接口下 VRRP 备份组的配置信息。

序号	检查项	说明
3	Inspur#**show vrrp interface** *interface-type interface-number* [*group-id*] **statistics**	查看接口下 VRRP 备份组的统计信息。
4	Inspur#**show vrrp** [*group-id*] **track**	查看 VRRP 备份组监视信息。

11.4 接口备份

11.4.1 简介

双上行组网是目前常用的应用组网之一，该组网下常通过生成树协议（STP，Spanning Tree Protocol）阻塞冗余链路，起备份作用。虽然这种方案从功能上可以实现客户冗余备份的需求，但是在性能上却不能达到很多用户的要求，即使采用快速生成树协议的快速迁移，也只能是秒级的收敛速度。这对于应用于电信级网络核心的高端以太网交换机，是非常不利的一个性能参数。

接口备份解决方案针对双上行组网，实现主备链路冗余备份及快速迁移。该方案为双上行组网量身定做，既保证了性能，又简化了配置。

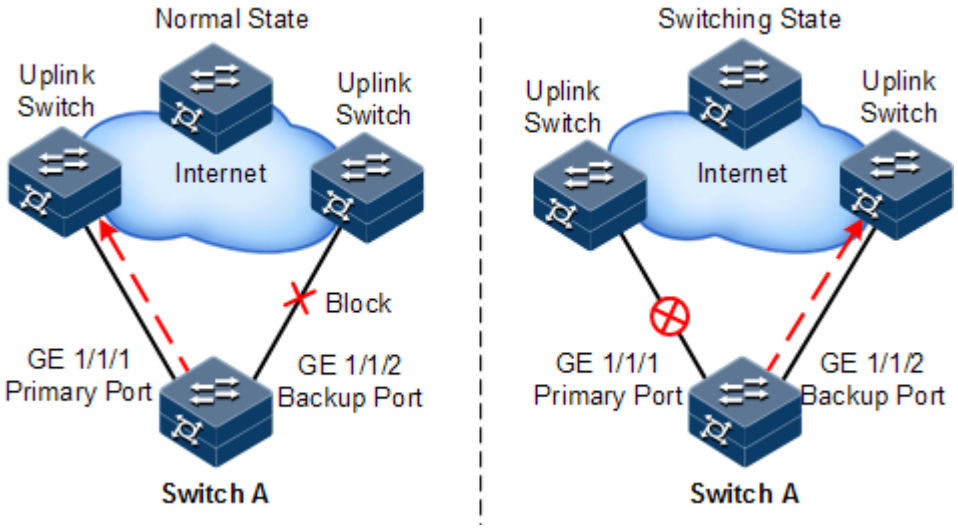
接口备份功能是 STP 协议的另一个解决方案，用户可以在关闭 STP 功能的情况下，通过手动设置接口实现基本的链路冗余。如果交换机已经开启 STP，就需要禁止接口备份功能，因为 STP 已经提供了类似的功能。

接口备份原理

接口备份功能需要设置接口备份组来实现。接口备份组包括一对接口，其中一个接口是主接口，另一个接口是备份接口。主接口所在的链路称为主链路，备份接口所在的链路称为备份链路。接口备份组的成员接口支持物理接口和链路聚合组，不支持三层接口。

在接口备份组中，当一个接口处于转发（Forward）状态时，另一个接口则处于阻塞状态（Block）。任何时刻，两个接口中只有一个接口处于转发状态。当处于转发状态的接口发生链路故障时，处于待命状态的接口才会切换到转发状态，以保持链路正常。

图11-4 接口备份原理示意图



接口备份原理如图 11-4 所示。Switch A 上的 Gigaethernet 1/1/1、Gigaethernet 1/1/2 分别与上行交换机相连，接口转发状态如下：

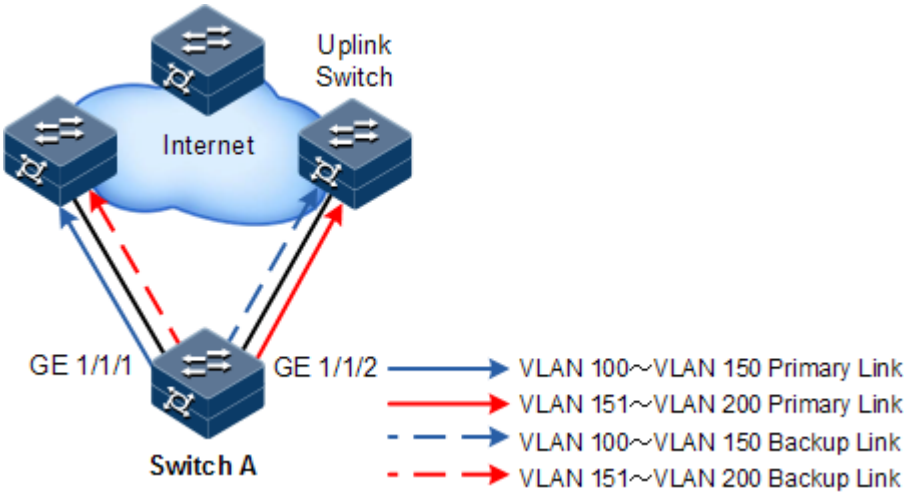
- 正常状态下，Switch A 的 Gigaethernet 1/1/1 为主接口，Gigaethernet 1/1/2 为备份接口，Gigaethernet 1/1/1 和上行交换机之间转发报文，Gigaethernet 1/1/2 和上行交换机之间不转发报文。
- 当 Gigaethernet 1/1/1 与上行交换机之间出现链路故障时，备份接口 Gigaethernet 1/1/2 和上行交换机之间转发报文。
- 当 Gigaethernet 1/1/1 链路故障恢复并保持一段时间（恢复延时）后，Gigaethernet 1/1/1 变为转发状态，Gigaethernet 1/1/2 变为待命状态。

如果主接口和备份接口之间发生切换，交换机会发送一个 Trap 上报网管系统。

接口备份在不同 VLAN 上的应用

接口备份通过在 VLAN 上进行应用，还可以实现两个接口在不同 VLAN 上同时进行转发，如图 11-5 所示。

图11-5 接口备份在不同 VLAN 上的应用原理示意图



在不同的 VLAN 上，接口的转发状态如下：

- 正常情况下，配置 Switch A 在 VLAN 100～VLAN 150 上，Gigaethernet 1/1/1 为主接口，Gigaethernet 1/1/2 为备份接口；在 VLAN 151～VLAN 200 上，Gigaethernet 1/1/2 为主接口，Gigaethernet 1/1/1 为备份接口。那么，Gigaethernet 1/1/1 在 VLAN 100～VLAN 150 转发流量，Gigaethernet 1/1/2 在 VLAN 151～VLAN 200 上转发流量。
- 当 Gigaethernet 1/1/1 发生链路故障时，Gigaethernet 1/1/2 负责转发 VLAN 100～VLAN 200 上的流量。
- 当 Gigaethernet 1/1/1 恢复正常并保持一段时间（恢复延时）后，Gigaethernet 1/1/1 在 VLAN 100～VLAN 150 上转发流量，Gigaethernet 1/1/2 在 VLAN 151～VLAN 200 上转发流量。

利用这种方法，接口备份可以用于负载均衡。同时，这种应用不依赖于上联交换机的配置，便于用户操作。

11.4.2 配置准备

场景

在双上行网络中，通过配置端口备份功能，可以实现主备链路的冗余备份及其快速倒换。通过在不同 VLAN 中应用端口备份，还可以实现各端口之间的负载分担。

与 STP 功能相比，端口备份功能既保证了毫秒级的倒换性能，又简化了配置。

前提

无

11.4.3 接口备份的缺省配置

设备上接口备份的缺省配置如下。

功能	缺省值
接口备份组	无
故障恢复延时时间	15s
恢复模式	返回模式

11.4.4 配置接口备份基本功能

注意

设备上接口备份与 STP、环路检测、以太网环和 ERPS 功能之间可能会相互影响，建议不要在同一接口上同时开启这些功能。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type primary-interface-number*	进入物理层接口配置模式或者聚合组配置模式。
3	Inspur(config-tengigabitethernet1/1/*)#**port backup** *interface-type backup-interface-number* **vlanlist** *vlan-list*	配置接口备份组。 在 VLAN 列表上配置接口 *backup-interface-number* 为备份接口，而 *primary-interface-number* 为主接口。 如果配置接口备份组不指定 VLAN 列表，则缺省 VLAN 范围是 1～4094。
	Inspur(config-tengigabitethernet1/1/*)#**port backup** *interface-type backup-interface-number* [**vlanlist** *vlan-list*]	
4	Inspur(config-tengigabitethernet1/1/*)#**port backup fault-detect lldp**	（可选）配置 LLDP 故障探测。
5	Inspur(config-tengigabitethernet1/1/*)#**port backup restore-mode** { **non-revertive** | **revertive** [**restore-delay** *second*] }	（可选）配置恢复模式。

说明

- 在一个接口备份组中，一个接口不能既是主接口，又是备份接口。
- 在同一 VLAN 上，一个接口/链路聚合组不能同时充当两个接口备份组的成员。

11.4.5 配置接口强制倒换

注意

- 配置强制倒换成功后，主备链路将进行倒换，工作链路被强制倒换到备份链路上（不考虑主备端口的 Up/Down 状态）。
- 在配置端口强制倒换命令中端口关键字为备份端口号，可选参数。如果主端口在不同 VLAN 上配置了多个端口备份组，要求必须输入备份端口号。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式或者聚合组配置模式。
3	Inspur(config-tengigabitethernet1/1/*)#**port backup** *interface-type backup-interface-number* **force-switch** Inspur(config-port-channel*)#**port backup** [*interface-type backup-interface-number*] **force-switch**	配置接口强制倒换。 可以通过 **no port backup** [*interface-type backup-interface-number*] **force-switch** 取消强制倒换。工作链路将根据链路 Link 状态重新进行选择，选取的原则是： • Up 接口优先； • 两个接口都是 Up 的情况下主接口优先。

11.4.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show port backup**	查看接口备份相关的状态信息。
2	Inspur#**show port backup group**	查看接口备份组相关的配置信息。

11.4.7 配置接口备份示例

组网需求

如图 11-6 所示，为实现远程 PC 到服务器的可靠访问，需要在 Switch A 上配置接口备份组，并指定 VLAN 列表，实现接口链路保护和负载分担。其要求如下：

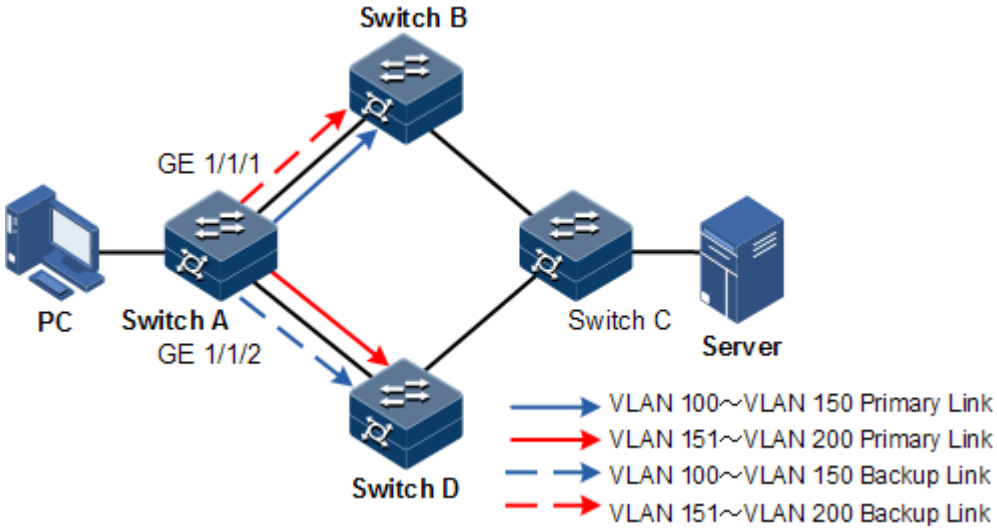
- 配置 Switch A 在 VLAN 100～VLAN 150 上，GE 1/1/1 为主接口，GE 1/1/2 为备份接口；

- 配置 Switch A 在 VLAN 151～VLAN 200 上，GE 1/1/2 为主接口，GE 1/1/1 为备份接口。

当 GE 1/1/1 发生链路故障时，切换到备份接口 GE 1/1/2，以保持链路正常。

Switch A 需要支持接口备份功能，Switch B、Switch C、Switch D 无需支持接口备份功能。

图11-6 接口备份应用组网示意图



配置步骤

步骤 1 创建 VLAN 100～VLAN 200，并将 GE 1/1/1 和 GE 1/1/2 加入到 VLAN 100～VLAN 200 中。

```
Inspur#config
Inspur(config)#create vlan 100-200 active
Inspur(config)#interface gigaethernet 1/1/1
Inspur(config-gigabitethernet1/1/1)#portswitch
Inspur(config-gigabitethernet1/1/1)#switchport mode trunk
Inspur(config-gigabitethernet1/1/1)#switchport trunk allowed vlan 100-200
confirm
Inspur(config-gigabitethernet1/1/1)#exit
Inspur(config)#interface gigaethernet 1/1/2
Inspur(config-gigabitethernet1/1/2)#portswitch
Inspur(config-gigaethernet1/1/2)#switchport mode trunk
Inspur(config-gigaethernet1/1/2)#switchport trunk allowed vlan 100-200
confirm
Inspur(config-gigaethernet1/1/2)#exit
```

步骤 2 在 VLAN 100～VLAN 150 上配置 GE 1/1/1 为主接口，GE 1/1/2 为备份接口。

```
Inspur(config)#interface gigaethernet 1/1/1
Inspur(config-gigabitethernet1/1/1)#port backup gigaethernet 1/1/2
vlanlist 100-150
Inspur(config-gigabitethernet1/1/1)#exit
```

步骤 3 在 VLAN 151～VLAN 200 上配置 Gigaethernet 1/1/2 为主接口，Gigaethernet 1/1/1 为备份接口。

```
Inspur(config)#interface gigaethernet 1/1/2
Inspur(config-gigaethernet1/1/2)#port backup gigaethernet 1/1/1 vlanlist
151-200
```

检查结果

通过 **show port backup group** 命令，分别在正常状态和链路故障情况下查看接口备份相关的状态信息。

当 Gigaethernet 1/1/1 和 Gigaethernet 1/1/2 链路均为 Forward 时，Gigaethernet 1/1/1 在 VLAN 100～VLAN 150 上转发流量，Gigaethernet 1/1/2 在 VLAN 151～VLAN 200 上转发流量。

```
Inspur#show port backup group
Active Port(State)        Backup Port(State)      ForceSwitch   Vlanlist
-------------------------------------------------------------------------
-------------------------------------
GE1/1/1(Forward)         GE1/1/2(Block)            NO          100-150
GE1/1/2(Forward)         GE1/1/1(Block)            NO          151-200
```

手动断开 Switch A 和 Switch B 之间的链路来模拟故障，此时 Gigaethernet 1/1/1 变为 Down，则 Gigaethernet 1/1/2 负责转发 VLAN 100～VLAN 200 上的流量。

```
Inspur#show port backup group
Active Port(State)        Backup Port(State)      ForceSwitch   Vlanlist
-------------------------------------------------------------------------
-------------------------------------
GE1/1/1(Down)            GE1/1/2(Forward)       NO          100-150
GE1/1/2(Forward)         GE1/1/1(Down)          NO          151-200
```

当 Gigaethernet 1/1/1 恢复正常 Up 状态并保持 15s 后（恢复延时），Gigaethernet 1/1/1 在 VLAN 100～VALN 150 上转发流量，Gigaethernet 1/1/2 在 VLAN 151～VALN 200 上转发流量。

```
Inspur#show port backup group
Active Port(State)        Backup Port(State)      ForceSwitch   Vlanlist
-------------------------------------------------------------------------
-------------------------------------
GE1/1/1(Forward)         GE1/1/2(Block)         NO          100-150
GE1/1/2(Forward)         GE1/1/1(Block)         NO          151-200
```

11.5 KEY-CHAIN

11.5.1 简介

为了安全，在网络上需要不断对应用层的认证信息进行更改。通过认证算法和共享安全密钥来共同决定信息在不安全的网络上进行传输时是否被篡改。使用这种认证方式

对数据进行认证时，需要数据发送者和接收者之间共享安全密钥和认证算法。并且密钥不能在网络上进行传输。

如果每个应用层协议维护一套认证规则（包括认证算法和密钥），将会有大量的应用程序采用相同的认证方式。这将导致认证信息被复制和更改。同样，如果每个应用程序都采用一个固定的认证密钥，每次更改需要网络管理员手工修改。而手工更改密钥或认证算法是非常复杂和繁琐的，要想更改所有路由器的密码而不丢包也是非常困难的。

因此，需要系统能够集中管理所有的认证处理和更改认证算法和密钥，而无需过多的人工干预。Key-chain 就实现了这个功能。Key-chain 提供了对所有应用层协议的认证，并且 Key-chain 能够在不丢包的情况下，动态更改密码链。

11.5.2 配置准备

场景

系统能够集中管理所有的认证处理和更改认证算法和密钥，而无需过多的人工干预。Key-chain 就实现了这个功能。Key-chain 提供了对所有应用层协议的认证，并且 Key-chain 能够在不丢包的情况下，动态更改密码链。

前提

无

11.5.3 key-chain 功能的缺省配置

无

11.5.4 配置 key-chain

请在需要配置 key-chain 功能的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**key-chain** *keychain-name*	创建密钥链，并进入 KEY-CHAIN 配置模式。使用 **no key-chain** *keychain-name* 命令删除该配置。
3	Inspur(config-keychain)#**key** *key-id* **key-string** [**0** | **7**] *string*	配置密钥和密码字。
4	Inspur(config-keychain)#**key** *key-id* **accept-lifetime** *start-time* { **infinite** | *end-time* | **duration** *duration-time* }	（可选）配置密钥的接收时间。使用 **no key** *key-id* **accept-lifetime** 命令恢复到缺省情况。
5	Inspur(config-keychain)#**key** *key-id* **send-lifetime** *start-time* { **infinite** | *end-time* | **duration** *duration-time* }	（可选）配置密钥的发送时间。使用命令 **no key** *key-id* **send-lifetime** 恢复缺省配置。

步骤	配置	说明
6	Inspur(config-keychain)#**accept-tolerance** { *time* | **infinite** }	（可选）配置密钥链接收容忍时间。使用命令 **no accept-tolerance** 恢复缺省配置。

11.5.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show key-chain** [*keychain-name* [**key** *key-id*]]	查看密钥链信息。

11.6 UDLD

11.6.1 简介

UDLD（UniDirectional Link Detection，单向链路检测）用于监听利用光纤或以太网线连接的物理配置，当出现单向链路（只能向一个方向传输）时，UDLD 可以检测出这一状况，关闭相应接口并发送警告信息。单向链路可能引起很多问题，尤其是生成树，可能会造成回环。

11.6.2 配置准备

场景

当出现单向链路（只能向一个方向传输）时，UDLD 可以检测出这一状况，关闭相应接口并发送警告信息。

前提

UDLD 需要链路两端设备都支持才能正常运行。

11.6.3 故障转移功能的缺省配置

设备上故障转移功能的缺省配置如下。

功能	缺省值
UDLD 功能	禁用

11.6.4 配置 UDLD

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config** Inspur(config)#**interface** *interface-type primary-interface-number*	进入全局或端口配置模式。
2	Inspur(config)#**uldp enable** Inspur(config-gigaethernet1/1/*)#**uldp enable**	使能全局或者端口下 UDLD 功能。
3	Inspur(config)#**uldp recovery-time** *time*	（可选）配置单向链路恢复时间。

11.6.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show uldp**	查看 UDLD 配置信息。

12 安全性

本章介绍安全特性的基本原理和配置过程，并提供相关的配置案例。

- ACL
- 安全 MAC
- 动态 ARP 检测
- RADIUS
- TACACS+
- 风暴抑制
- 802.1x
- IP Source Guard
- PPPoE+
- 配置 URPF
- 配置 CPU 保护
- ARP 防攻击

12.1 ACL

12.1.1 简介

ACL（Access Control List，访问控制列表）是一系列有序规则的集合，通过应用这些规则控制设备接收或拒绝某些数据报文。

在网络中为了控制非法报文对网络的影响，需要在设备上配置一系列的规则，以决定什么样的数据包能够通过，这些规则就是通过 ACL 定义的。

访问控制列表是由 permit | deny 语句组成的一系列有顺序的规则，这些规则根据数据包的源 MAC 地址、目的 MAC 地址、源 IP 地址、目的 IP 地址、端口号等来描述。设备根据这些规则判断哪些数据包可以接收，哪些数据包需要拒绝。

12.1.2 配置准备

场景

网络设备为了过滤数据包，需要配置 ACL，以识别需要过滤的对象。在识别出特定的对象之后，才能根据预先设定的策略允许或禁止相应的数据包通过，丢弃动作支持报文上送 CPU。当 ACL 否定目的 MAC 地址后，相应报文的源 MAC 地址不进行学习且不显示。

访问控制列表可以分为以下几种类型：

- 基本 IPv4 ACL：根据数据包 IP 头所携带的源 IP、目的 IP 地址制定分类规则。
- 扩展 IPv4 ACL：根据数据包 IP 头所携带的源 IP、目的 IP、承载的协议类型、使用的 TCP 或 UDP 端口号（默认为 0）等数据包的属性信息制定分类规则，支持限制 Telnet/SSH 登录。
- MAC ACL：根据数据包二层帧头携带的源 MAC 地址、目的 MAC 地址、二层协议类型等二层信息制定分类规则，ACL 拒绝的目的 MAC 地址报文，源 MAC 地址也不再学习、不显示。
- User ACL：可以以报文的报文头、IP 头等为基准，指定从第几个字节开始与掩码进行“与”操作，将从报文提取出来的字符串与用户定义的字符串进行比较，从而找到相匹配的报文，支持匹配以太网帧前 64 字节任意字段的信息。
- IPv6 ACL：根据数据包 IP 头所携带源 IPv6 地址信息、目的 IPv6 地址信息、IPv6 承载的协议类型、使用的 TCP 或 UDP 端口号（默认为 0）等数据包的属性信息制定分类规则，支持 IPv6 ACL 限制 Telnet/SSH 登录。
- 高级 ACL：根据数据包二层帧头携带的源 MAC 地址、目的 MAC 地址、IP 头所携带的源 IP、目的 IP 等数据包的属性信息制定分类规则。

根据实际场景的差异，应用 ACL 的方式有四种：基于整个设备、基于接口、基于从入接口到出接口的流和基于 VLAN。

前提

无

12.1.3 配置 ACL

请在设备上进行以下配置。步骤 3～步骤 7 请根据需要选择配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**access-list** *acl-number* [**name** *acl-name*]	创建 ACL，进入 ACL 配置模式。 • 取值在 1000～1999 之间时，进入基本 IP ACL 配置模式 • 取值在 2000～2999 之间时，进入扩展 IP ACL 配置模式 • 取值在 3000～3999 之间时，进入 MAC ACL 配置模式 • 取值在 5000～5999 之间时，进入 User ACL 配置模式 • 取值在 6000～6999 之间时，进入 IPv6 ACL 配置模式 • 取值在 7000～7999 之间时，进入高级 ACL 配置模式
3	Inspur(config-acl-ip-std)#**rule** [*rule-id*] { **deny** | **permit** } { *source-ip-address source-ip-mask* | **any** } [**time-range** *time-range-name*]	（可选）配置基本 IP ACL 的规则。
4	Inspur(config-acl-ip-ext)#**rule** [*rule-id*] { **deny** | **permit** } { *protocol-id* | **icmp** | **igmp** | **ip** } { *source-ip-address source-ip-mask* | **any** } { *destination-ip-address destination-ip-mask* | **any** } [**icmp-type** *icmp-type-value* [*icmp-message-code*]] [**igmp-type** *igmp-type-value*] [**igmp-group** *igmp-ip-address igmp-ip-mask*] [**dscp** *dscp-value* | **precedence** *precedence-value* | **tos** *tos-value*] [**ttl** *ttl-value*] [**fragment**] [**time-range** *time-range-name*]	（可选）配置扩展 IP ACL 的规则。
	Inspur(config-acl-ip-ext)#**rule** [*rule-id*] { **deny** | **permit** } { **tcp** | **udp** } { *source-ip-address source-ip-mask* | **any** } [*source-port*] [**range** *minimum-source-port maximum-source-port*] { *destination-ip-address destination-ip-mask* | **any** } [*destination-port*] [**range** *minimum-source-port maximum-source-port*] [**ack** *ack-value*] [**fin** *fin-value*] [**psh** *psh-value*] [**rst** *rst-value*] [**syn** *syn-value*] [**urg** *urg-value*] [**tos** *tos-value*] [**dscp** *dscp-value* | **precedence** *precedence-value* | **ttl** *ttl-value*] [**fragment**] [**time-range** *time-range-name*]	
5	Inspur(config-acl-mac)#**rule** [*rule-id*] { **deny** | **permit** } { *source-mac-address source-mac-mask* | **any** } { *destination-mac-address destination-mac-mask* | **any** } [**ethertype** { *ethertype* [*ethertype-mask*] | **ip** | **arp** }] [**svlan** *svlanid*] [**cvlan** *cvlanid*] [**cos** *cos-value*] [**inner-cos** *inner-cos*] [**time-range** *time-range-name*]	（可选）配置 MAC ACL 的规则。

步骤	配置	说明
6	Inspur(config-acl-udf)#**rule** [*rule-id*] { **deny** | **permit** } { **layer2** | **l2-head** } *rule-string rule-mask offset* [**second** *rule-string rule-mask offset* [**third** *rule-string rule-mask offset* [**fourth** *rule-string rule-mask offset* [**fifth** *rule-string rule-mask offset* [**sixth** *rule-string rule-mask offset* [**seventh** *rule-string rule-mask offset*]]]]]] [**time-range** *time-range-name*] Inspur(config-acl-udf)#**rule** [*rule-id*] { **deny** | **permit** } **ipv4** *rule-string rule-mask offsets* [**second** *rule-string rule-mask offsets* [**third** *rule-string rule-mask offsets* [**fourth** *rule-string rule-mask offsets* [**fifth** *rule-string rule-mask offsets* [**sixth** *rule-string rule-mask offsets* [**seventh** *rule-string rule-mask offsets*]]]]]] [**time-range** *time-range-name*]	（可选）配置 User ACL 的规则。
7	Inspur(config-acl-ipv6)#**rule** [*rule-id*] { **deny** | **permit** } { *protocol-id* | **ipv6** | **icmpv6** } { *source-ipv6-address/prefix* | **any** } { *destination-ipv6-address/prefix* | **any** } [**icmpv6-type** *icmp-type-value* [*icmp-message-code*]] [**dscp** *dscp-value*] [**flow-label** *flow-label-value*] [**fragment**] [**time-range** *time-range-name*] Inspur(config-acl-ipv6)#**rule** [*rule-id*] { **deny** | **permit** } { **tcp** | **udp** } { *source-ipv6-address/prefix* | **any** } [*source-port*] { *destination-ipv6-address/prefix* | **any** } [*destination-port*] [**ack** *ack-value*] [**dscp** *dscp-value*] [**fin** *fin-value*] [**psh** *psh-value*] [**rst** *rst-value*] [**syn** *syn-value*] [**urg** *urg-value*] [**dscp** *dscp-value*] [**flow-label** *flow-label-value*] [**fragment**] [**time-range** *time-range-name*]	（可选）配置 MAP ACL 的规则。
8	Inspur(config-acl-advanced)#**rule** [*rule-id*] { **deny** | **permit** } { *source-mac-address source-mac-mask* | **any** } { *destination-mac-address destination-mac-mask* | **any** } [**svlan** *svlanid*] [**cvlan** *cvlanid*] [**cos** *cos-value*] [**inner-cos** *inner-cos*] { *source-ip-address source-ip-mask* | **any** } { *destination-ip-address destination-ip-mask* | **any** } [**dscp** *dscp-value* | **precedence** *precedence-value* | **tos** *tos-value*] [**ttl** *ttl-value*] [**fragment**] [**time-range** *time-range-name*]	（可选）配置 Advanced ACL 的规则

12.1.4 配置过滤器

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入接口配置模式，支持 VLAN 接口上配置。
3	Inspur(config-gigaethernet1/1/*)#**filter** { **egress** | **ingress** } **access-list** { *acl-number* | **name** *acl-name* } [**statistics**]	在接口上应用 ACL。
4	Inspur(config-gigaethernet1/1/*)#**exit**	返回全局配置模式。
5	Inspur(config)#**filter ingress access-list** { *acl-number* | **name** *acl-name* } **vlanlist** *vlan-list* [**statistics**]	在 VLAN 上应用 ACL 规则。

12.1.5 配置时间段

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**time-range** *time-range-name* { *hour minute seconds* **to** *hour minute seconds* { *weekday-list* | **sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sta** | **off-day** | **working-day** | **daily** } [**from** *hour minute seconds month-day-year*] [**to** *hour minute seconds month-day-year*] | **from** *hour minute seconds month-day-year* [**to** *hour minute seconds month-day-year*] | **to** *hour minute seconds month-day-year* }	创建时间段，可被 ACL 规则应用。

12.1.6 配置 SNMP 访问控制 IP 列表

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式。
3	Inspur(config-vlan*)#**local-access access-list** *acl-number*	配置 SNMP 访问控制 IP 列表。

12.1.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show access-list** [*acl-number*]	查看 ACL 信息。
2	Inspur#**show acl resource** { **egress** | **ingress** }	查看 ACL 资源利用信息。
3	Inspur#**show filter interface**	查看过滤器信息。
	Inspur#**show filter interface** *interface-type interface-number* [**ingress** | **egress**]	
	Inspur#**show filter statistics interface** *interface-type interface-number* { **ingress** | **egress** } [**access-list** { *acl-number* | **name** *acl-name* }]	
	Inspur#**show filter vlanlist** [*vlan-list*]	
4	Inspur#**show local-access access-list**	查看 SNMP 的服务器认证信息。

12.1.8 维护

用户可以通过以下命令，维护设备 ACL 特性的运行情况和配置情况。

命令	描述
Inspur(config)#**clear filter statistics interface** { *interface-type interface-number* | **vlan** *vlan-id* } { **egress** | **ingress** } [**access-list** { *acl-number* | **name** *acl-name* }]	清除 ACL 过滤器配置统计信息。

12.2 安全 MAC

12.2.1 简介

接口安全 MAC 主要应用于网络边缘用户侧的交换设备上，用于保证某个接口接入数据的安全性，根据源 MAC 地址对输入的报文加以控制。用户可以启动接口安全功能来限制和区分哪些用户可以通过安全接口来访问网络，只有接口安全 MAC 地址才能够访问网络，非安全 MAC 地址均按照用户配置的接口访问违例模式处理。

安全 MAC 地址分类

设备支持的安全 MAC 地址分为以下三类：

- 静态安全 MAC 地址

静态安全 MAC 地址由用户在安全接口手动配置生成，该 MAC 地址在接口安全 MAC 功能使能后生效。该类安全 MAC 地址不会被老化且支持配置加载。

- 动态安全 MAC 地址

动态安全 MAC 地址是由设备自己学习得到的。用户可以在允许学习的 MAC 地址最大数目范围内，将学习到的 MAC 地址都设置为安全 MAC 地址。该类安全 MAC 地址会被老化，不支持配置加载。

动态安全 MAC 地址可以通过转换为 Sticky 安全 MAC 地址，以实现不老化，支持配置加载。

- Sticky 安全 MAC 地址

Sticky 安全 MAC 地址由用户在安全接口手动配置生成或者由动态安全 MAC 地址转化而来。与静态安全 MAC 地址不同，Sticky 安全 MAC 地址需要配合 Sticky 学习功能一起使用，支持配置加载：

- 当 Sticky 学习功能使能时，Sticky 安全 MAC 地址生效，该地址不会被老化。
- 当 Sticky 学习功能禁止时，Sticky 安全 MAC 地址失效，仅保存在系统中。

说明

- 当 Sticky 学习功能使能时，接口下学习到的所有动态安全 MAC 地址均转换为 Sticky 安全 MAC 地址。
- 当 Sticky 学习功能禁止时，接口下所有 Sticky 安全 MAC 地址均转换为动态安全 MAC 地址。

安全 MAC 违例处理方式

当接口安全 MAC 的数目已经达到最大数目时，再有陌生源 MAC 报文输入则视为违规操作。对于非法的用户接入，根据安全 MAC 的违规策略配置交换机的不同处理方式如下：

- Protect 模式：对于非法接入的用户，安全接口直接丢弃该用户的报文。
- Restrict 模式：对于非法接入的用户，安全接口丢弃该用户的报文，同时在控制台打印 Syslog 信息，并发送告警信息至网管系统。
- Shutdown 模式：对于非法接入的用户，安全接口丢弃该用户的报文，同时在控制台打印 Syslog 信息、发送告警信息至网管系统并将该安全接口关闭。

注意

当发生 MAC 地址飘移，即安全接口 A 收到一个已经存在于安全接口 B 中的安全 MAC 所对应用户的访问时，安全接口 A 将其作为违例处理。

12.2.2 配置准备

场景

为了保证交换机接口接入数据的安全性，可以根据源 MAC 地址对输入的报文加以控制。通过安全 MAC 可以将接入接口配置成只允许特定的几个用户接入，也可以配置成允许特定数量的用户从该接口接入。但接入的用户超过限制时，接入的报文将按照安全 MAC 的违规策略进行处理。

前提

无

12.2.3 安全 MAC 功能的缺省配置

设备上安全 MAC 功能的缺省配置如下。

功能	缺省值
接口安全 MAC 功能状态	禁止
动态安全 MAC 老化时间	30min
动态安全 MAC 老化类型	**absolute**
接口安全 MAC 恢复时间	**disable**，即不恢复
动态安全 MAC Sticky 学习功能状态	禁止
接口安全 MAC Trap 功能状态	禁止
接口安全 MAC 违规处理方式	保护模式
接口安全 MAC 的最大数量	1024

12.2.4 配置安全 MAC 基本功能

注意

- 不建议用户在聚合组的单个成员接口上使能接口安全 MAC 功能。
- 不建议用户在同一接口上使能接口安全 MAC 功能的同时，使用 MAC 地址管理功能来配置静态 MAC 地址，会导致接口安全 MAC 功能失效。
- 当 802.1x 接口认证方式为基于 MAC 地址进行认证时，安全 MAC 功能与 802.1x 功能互斥，不建议用户在同一接口上同时进行配置。
- 安全 MAC 功能与基于接口和基于接口 VLAN 的 MAC 地址数目限制互斥，不能同时配置。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**switchport port-security**	使能接口安全 MAC 功能。
4	Inspur(config-gigaethernet1/1/*)#**switchport port-security maximum** *maximum*	（可选）配置接口安全 MAC 最大数目。
5	Inspur(config-gigaethernet1/1/*)#**switchport port-security violation** { **protect** | **restrict** | **shutdown** }	（可选）配置安全 MAC 违例模式。
6	Inspur(config-gigaethernet1/1/*)#**no port-security shutdown** Inspur(config-gigaethernet1/1/*)#**exit**	（可选）将因违反接口安全 MAC 而被关闭的接口重新开启。
7	Inspur(config)#**port-security recovery-time** *second*	(可选)配置接口安全 MAC 恢复时间。

说明

当安全 MAC 违规策略为 Shutdown 模式时，可以使用该命令将因违反接口安全 MAC 而被关闭的接口重新开启。

当接口 Up 以后，配置的安全 MAC 违例模式继续保持。

12.2.5 配置接口静态安全 MAC 地址

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**switchport port-security**	使能接口安全 MAC 功能。
4	Inspur(config-gigaethernet1/1/*)#**switchport port-security mac-address** *mac-address* **vlan** *vlan-id*	配置接口静态安全 MAC 地址。

12.2.6 配置接口动态安全 MAC 地址

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**port-security aging-time** *period*	（可选）配置接口安全 MAC 地址老化时间。
3	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
4	Inspur(config-gigaethernet1/1/*)#**switchport port-security aging-type** { **absolute** | **inactivity** }	（可选）配置动态安全 MAC 地址老化类型。
5	Inspur(config-gigaethernet1/1/*)#**switchport port-security**	使能接口动态安全 MAC 学习功能。
6	Inspur(config-gigaethernet1/1/*)#**switchport port-security trap enable**	（可选）使能接口安全 MAC Trap 功能。
7	Inspur(config-gigaethernet1/1/*)#**switchport port-security trap period** *value*	（可选）配置接口 Trap 发送周期

说明

使用 **switchport port-security** 命令使能接口安全 MAC 功能的同时，也就使能了动态安全 MAC 的学习功能。

12.2.7 配置接口 Sticky 安全 MAC 地址

注意

建议用户不要在 Sticky 安全 MAC 功能禁止的情况下配置 Sticky 安全 MAC 地址，否则可能导致功能异常。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**switchport port-security**	使能接口安全 MAC 功能。
4	Inspur(config-gigaethernet1/1/*)#**switchport port-security mac-address sticky**	使能 Sticky 安全 MAC 学习功能。
5	Inspur(config-gigaethernet1/1/*)#**switchport port-security mac-address sticky** *mac-address* **vlan** *vlan-id*	（可选）手动配置接口 Sticky 安全 MAC 地址。

说明

Sticky 安全 MAC 学习功能使能后，动态安全 MAC 地址转换为 Sticky 安全 MAC 地址；手动设置的 Sticky 安全 MAC 地址生效。

12.2.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show port-security** [*interface-type interface-list*]	查看安全 MAC 的接口配置信息。
2	Inspur#**show port-security mac-address** [*interface-type interface-list*]	查看安全 MAC 地址配置及学习情况。

12.2.9 维护

用户可以通过以下命令，维护设备安全 MAC 特性的运行情况和配置情况。

命令	描述
Inspur(config-gigaethernet1/1/*)#**clear port-security** { **all** | **configured** | **dynamic** | **sticky** }	清除指定接口下指定类型的安全 MAC。

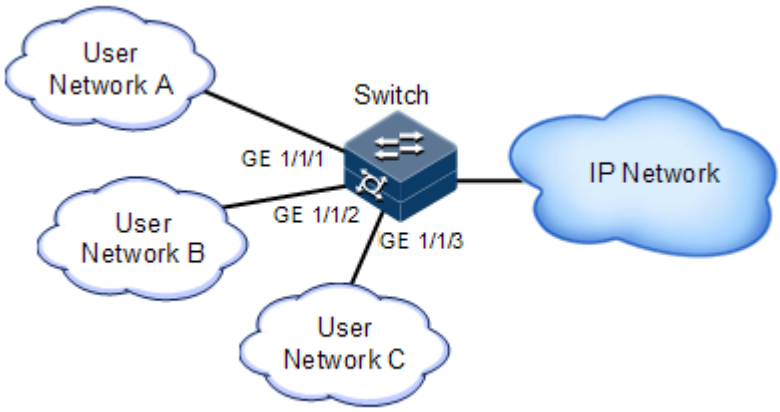
12.2.10 配置安全 MAC 示例

组网需求

如图 12-1 所示，交换机下联 3 个用户网络，为了保证交换机接口接入数据的安全性，要求配置如下：

- 接口 GE 1/1/1 最大允许 3 个用户接入网络。其中一个指定用户的 MAC 地址为 0000.0000.0001。其他 2 个用户为动态学习，每学习到一条 MAC 地址，网管系统均能收到 Trap 信息。违例模式采用 Protect 模式，且这 2 个学习用户 MAC 地址的老化时间为 10min。
- 接口 GE 1/1/2 要求最大允许 2 个用户接入网络。这 2 个用户的 MAC 地址通过学习确定，一旦确定后，不能被老化。违例模式采用 Restrict 模式。
- 接口 GE 1/1/3 要求最大允许 1 个用户接入网络。该指定用户的 MAC 地址为 0000.0000.0002，该用户的 MAC 地址可以控制是否老化。违例模式采用 Shutdown 模式。

图12-1 安全 MAC 应用组网示意图



配置步骤

步骤 1 配置 GE 1/1/1 接口安全 MAC。

```
Inspur#config
Inspur(config)#interface gigaethernet 1/1/1
Inspur(config-gigaethernet1/1/1)#switchport port-security
Inspur(config-gigaethernet1/1/1)#switchport port-security maximum 3
Inspur(config-gigaethernet1/1/1)#switchport port-security mac-address
0000.0000.0001 vlan 1
Inspur(config-gigaethernet1/1/1)#switchport port-security violation
protect
Inspur(config-gigaethernet1/1/1)#switchport port-security trap enable
Inspur(config-gigaethernet1/1/1)#exit
Inspur(config)#port-security aging-time 10
```

步骤 2 配置 GE 1/1/2 的接口安全 MAC。

```
Inspur(config)#interface gigaethernet 1/1/2
Inspur(config-gigaethernet1/1/2)#switchport port-security
Inspur(config-gigaethernet1/1/2)#switchport port-security maximum 2
Inspur(config-gigaethernet1/1/2)#switchport port-security mac-address
sticky
Inspur(config-gigaethernet1/1/2)#switchport port-security violation
restrict
Inspur(config-gigaethernet1/1/2)#exit
```

步骤 3 配置 GE 1/1/3 的接口安全 MAC。

```
Inspur(config)#interface gigaethernet 1/1/3
Inspur(config-gigaethernet1/1/3)#switchport port-security
Inspur(config-gigaethernet1/1/3)#switchport port-security maximum 1
Inspur(config-gigaethernet1/1/3)#switchport port-security mac-address
sticky 0000.0000.0002 vlan 1
Inspur(config-gigaethernet1/1/3)#switchport port-security mac-address
sticky
Inspur(config-gigaethernet1/1/3)#switchport port-security violation
shutdown
```

检查结果

通过 **show port-security** 查看安全 MAC 的接口配置是否正确。

```
Inspur#show port-security
Port security aging time:10 (mins)
Port security recovery time:Disable (s)
port                  status    Max-Num   Cur-Num  His-MaxNum   vio-Count
vio-action Dynamic-Trap Aging-Type
--------------------------------------------------------------------------
----------------------------------------
gigaethernet1/1/1       Enable    3        1      1          0
protect   Enable     Absolute
gigaethernet1/1/2       Enable    2        0      0          0
restrict  Disable    Absolute
gigaethernet1/1/3       Enable    1        1      1          0
shutdown  Disable    Absolute
gigaethernet1/1/4       Disable   1024     0      0          0
protect   Disable    Absolute
gigaethernet1/1/5       Disable   1024     0      0          0
…
```

通过 **show port-security mac-address** 查看设备上接口安全 MAC 地址配置及学习情况。

```
Inspur#show port-security mac-address
VLAN  Security-MAC-Address  Flag            Port                   Age(min)
------------------------------------------------------------------------------
1    0000.0000.0001      Security-static  gigaethernet1/1/1       --
1    0000.0000.0002      sticky           gigaethernet1/1/3       --
```

12.3 动态 ARP 检测

12.3.1 简介

动态 ARP 检测（Dynamic ARP Inspection）用于对不安全接口进行 ARP 保护，阻止对不符合要求的 ARP 报文进行响应，以防止网络中常见的 ARP 欺骗攻击。

动态 ARP 检测有两种方式：

- 静态绑定方式：手工设置绑定关系。
- 动态绑定方式：与 DHCP Snooping 合作产生动态绑定关系。DHCP Snooping 表项变化时，动态 ARP 检测也将同步更新动态绑定表项。

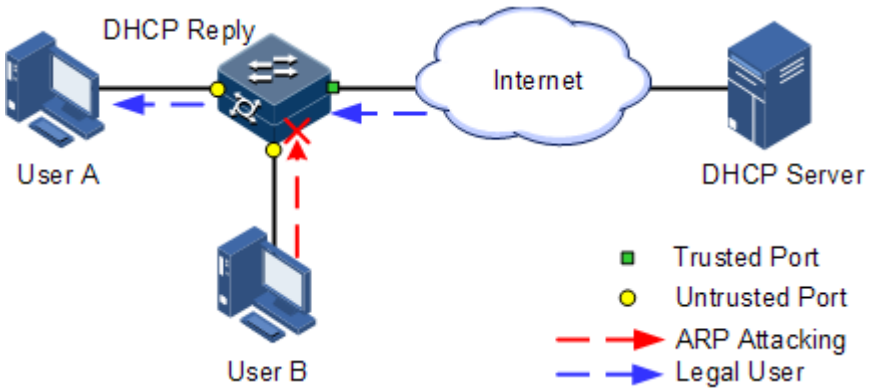
防御 ARP 攻击的 ARP 检测表是由 DHCP Snooping 表项和静态配置 ARP 检测规则构成的，包括 IP 地址、MAC 地址和 VLAN 绑定信息，并将这些信息与特定的接口相关联。动态 ARP 检测绑定表支持以下表项的组合：

- 接口＋IP
- 接口＋IP＋MAC
- 接口＋IP＋VLAN
- 接口＋IP＋MAC＋VLAN

动态 ARP 检测中接口的根据信任状态分为以下两种：

- 信任接口：接口将停止 ARP 检测，即不对该接口进行 ARP 保护，所有 ARP 报文均允许通过。
- 非信任接口：接口将进行 ARP 保护，只有匹配绑定表规则的 ARP 报文才允许通过，否则丢弃。

图12-2 动态 ARP 检测原理示意图



动态 ARP 检测原理如图 12-2 所示。当设备收到 ARP 报文时，将此 ARP 报文中的源 IP 地址、源 MAC 地址、接口号、VLAN 信息和 DHCP Snooping 表项的信息进行比较。如果信息匹配，说明是合法用户，则允许此用户的 ARP 报文通过；否则认为是 ARP 攻击，丢弃该 ARP 报文。

动态 ARP 检测同时还提供 ARP 报文限速功能，用于防止非法用户通过发送大量的 ARP 报文对设备进行攻击。

- 当接口上每秒收到的 ARP 报文数目超过报文限速阈值，系统认为该接口收到 ARP 攻击。此后系统将丢弃该接口收到的所有 ARP 报文，从而避免攻击。
- 系统提供接口的自动恢复功能并支持配置恢复时间，对于收到的 ARP 报文数目已经超过设定阈值的接口，在恢复时间后将自动恢复为正常收发状态。

动态 ARP 检测还可以实现对指定的 VLAN 进行保护。配置保护 VLAN 以后，将对非信任接口指定 VLAN 内的 ARP 报文进行保护，只有符合绑定表规则的 ARP 报文才允许通过，其余丢弃。

12.3.2 配置准备

场景

动态 ARP 检测用来防止网络中常见的 ARP 欺骗攻击，实现了对不安全来源的 ARP 报文进行隔离。是否对 ARP 报文信任通过接口的信任状态实现，而是否符合要求则通过绑定表实现。

前提

配置动态 ARP 检测之前，需要完成以下任务：

- 如果存在 DHCP 用户，则需要使能 DHCP Snooping 功能。

12.3.3 动态 ARP 检测的缺省配置

设备上动态 ARP 检测的缺省配置如下。

功能	缺省值
动态 ARP 检测接口信任状态	不信任
动态 ARP 检测静态绑定功能状态	禁止
动态 ARP 检测动态绑定功能状态	禁止
动态 ARP 检测静态绑定表	无
动态 ARP 检测保护 VLAN	所有 VLAN
接口 ARP 报文限速速率	60pps
接口下的绑定表个数限制	无限制

12.3.4 配置动态 ARP 检测信任接口

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**ip arp-inspection trust**	配置接口为信任接口。可用 **no ip arp-inspection trust** 命令配置接口为非信任接口，即接口不信任 ARP 报文。

12.3.5 配置 ARP 报文限制速率

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**ip arp-rate-limit rate** *rate-value*	配置接口 ARP 报文限制速率阈值。

12.3.6 配置动态 ARP 检测静态绑定功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ip arp-inspection static-config**	使能全局静态绑定功能。
3	Inspur(config)#**ip arp-inspection binding** *ip-address* [*mask*] [*mac-address*] [**vlan** *vlan-id*] *interface-type interface-number*	配置静态绑定关系。

12.3.7 配置动态 ARP 检测动态绑定功能

注意

使能动态 ARP 检测动态绑定功能，需要先使用 **ip dhcp snooping** 命令使能 DHCP Snooping 功能。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ip arp-inspection dhcp-snooping**	使能全局动态绑定功能。

12.3.8 配置动态 ARP 检测保护 VLAN

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ip arp-inspection binding dhcp-snooping** { **auto-update** | **static** }	配置 ARP 表项转换。
3	Inspur(config)#**ip arp-inspection vlan** *vlan-list*	配置动态 ARP 检测保护 VLAN。

12.3.9 配置接口的绑定表个数

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**ip arp-inspection binding-number** *number*	配置端口下允许的绑定表的个数，包括静态绑定表和 DHCP Snooping 绑定表。

12.3.10 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show ip arp-inspection**	查看动态 ARP 检测配置信息。
2	Inspur#**show ip arp-inspection binding** [*interface-type interface-number*]	查看设备动态 ARP 检测绑定表信息。
3	Inspur#**show ip arp-rate-limit**	查看 ARP 限速信息。

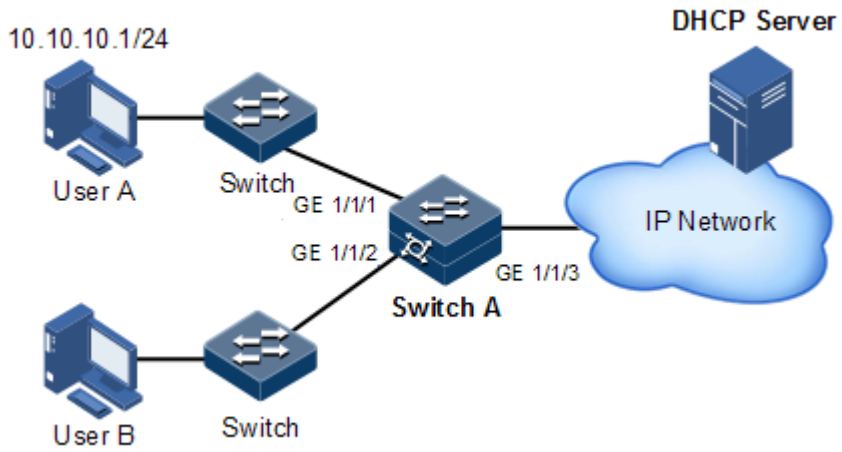
12.3.11 配置动态 ARP 检测示例

组网需求

为了防止 ARP 攻击，如图 12-3 所示，需要在 Switch A 设备上配置动态 ARP 检测功能。要求如下：

- 上联接口 GE 1/1/3 允许所有 ARP 报文通过。
- 下联接口 GE 1/1/1 允许指定 10.10.10.1 的 ARP 报文通过。
- 其他接口允许符合 DHCP Snooping 学习到的动态绑定关系的 ARP 报文通过。
- 下联接口 GE 1/1/2 配置 ARP 报文限速，限速速率为 20pps。

图12-3 动态 ARP 检测应用组网示意图



配置步骤

步骤 1 配置 GE 1/1/3 为信任接口。

```
Inspur#config
Inspur(config)#interface gigaethernet 1/1/3
Inspur(config-gigaethernet1/1/3)#ip arp-inspection trust
Inspur(config-gigaethernet1/1/3)#exit
```

步骤 2 配置静态绑定关系。

```
Inspur(config)#ip arp-inspection static-config
Inspur(config)#ip arp-inspection binding 10.10.10.1 gigaethernet 1/1/1
```

步骤 3 使能动态 ARP 绑定功能。

```
Inspur(config)#ip dhcp snooping
Inspur(config)#ip arp-inspection dhcp-snooping
```

步骤 4 配置接口 ARP 报文限速。

```
Inspur(config)#interface gigaethernet 1/1/2
Inspur(config-gigaethernet1/1/2)#ip arp-rate-limit rate 20
```

```
Inspur(config-gigaethernet1/1/2)#exit
```

检查结果

通过 **show ip arp-inspection** 命令查看设备上接口信任配置和静态/动态绑定功能配置结果。

```
Inspur#show ip arp-inspection
Static Config ARP Inspection: Enable
DHCP Snooping ARP Inspection: Enable
ARP Inspection Protect Vlan : 1-4094
Bind Rule Num            : 1
Vlan Rule Num            : 0
Bind Acl Num             : 1
Vlan Acl Num             : 0

Remained Rule Num         : 1023
Remained Acl Num          : 1023

Port                        Trust
----------------------------------------
gigaethernet1/1/1             no
gigaethernet1/1/2             no
gigaethernet1/1/3             yes
gigaethernet1/1/4             no
gigaethernet1/1/5             no
……
```

通过 **show ip arp-inspection binding** 命令查看动态 ARP 检测绑定表信息。

```
Inspur#show ip arp-inspection binding
History Max Rules Num : 0
Ip Address        Mask             Mac Address     VLAN   Port
Type          Inhw
------------------------------------------------------------------------------
------------------------------------------
10.10.10.1        255.255.255.255       --          --
gigaethernet1/1/1         static         yes
```

通过 **show ip arp-rate-limit** 命令查看接口限速配置和限速恢复时间配置结果。

```
Inspur#show ip arp-rate-limit
Port                       Rate(Num/Sec)
-----------------------------------------------
gigaethernet1/1/1             --
gigaethernet1/1/2             20
gigaethernet1/1/3             --
gigaethernet1/1/4             --
gigaethernet1/1/5             --
gigaethernet1/1/6             --
gigaethernet1/1/7             --
gigaethernet1/1/8             --
gigaethernet1/1/9             --
gigaethernet1/1/10            --
```

12.4 RADIUS

12.4.1 简介

RADIUS（Remote Authentication Dial In User Service，远程用户拨号认证系统）是一种用于对远程访问用户进行集中鉴别的标准化通信协议。RADIUS 使用 UDP 作为传输协议（端口 1812、1813），具有良好的实时性；同时也支持重传机制和备用服务器机制，从而具有较好的可靠性。

RADIUS 认证功能

RADIUS 使用客户端/服务器模式，网络访问设备作为 RADIUS 服务器的客户端。RADIUS 服务器负责接收用户的连接请求、对用户进行鉴别，然后将所有客户端所需的配置信息传回，以便为用户提供服务。通过这种方式可以控制用户对设备和网络的访问，提高网络的安全性。

客户端与 RADIUS 服务器之间的通信是通过共享密钥的使用来鉴别的，这个共享密钥不会通过网络传送。此外，任何用户口令在客户机和 RADIUS 服务器间发送时都需要进行加密过程，以避免有人通过嗅探非安全网络得到用户密码。

RADIUS 计费功能

RADIUS 计费功能主要针对通过 RADIUS 认证的用户进行。在用户登录时给 RADIUS 计费服务器发送一个开始计费的报文，在登录期间根据计费策略给 RADIUS 计费服务器发送计费更新报文，退出登录时，给 RADIUS 计费服务器发送停止计费报文，报文里面包含用户的登录时间。通过这些报文，RADIUS 计费服务器可以记录每个用户的访问时间和操作。

12.4.2 配置准备

场景

为了控制用户对设备和网络的访问，可以在网络中部署 RADIUS 服务器对用户进行认证和计费。本设备可以作为 RADIUS 服务器的代理设备，根据 RADIUS 服务器反馈的结果对用户访问进行授权。

前提

无

12.4.3 RADIUS 的缺省配置

设备上 RADIUS 的缺省配置如下。

功能	缺省值
RADIUS 计费功能	禁止
RADIUS 服务器 IP 地址	0.0.0.0

功能	缺省值
RADIUS 服务器超时时间	3s
RADIUS 计费服务器的 IP 地址	0.0.0.0
RADIUS 认证服务器端口号	1812
RADIUS 计费服务器端口号	1813
与 RADIUS 计费服务器通信的共享密钥	无
计费失败处理策略	**online**
更新报文发送周期	0

12.4.4 配置 RADIUS 认证

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**radius** [**backup**] { *ipv4-address* | *ipv6-address* } [**auth-port** *port-id*]	指定 RADIUS 认证服务器 IP 地址。配置 **backup** 参数用以指定备份的 RADIUS 认证服务器。
2	Inspur#**radius-key** *string*	配置 RADIUS 认证的共享密钥。
3	Inspur#**radius-encrypt-key** *word*	配置 RADIUS 共享服务器以密文密钥信息。
4	Inspur#**radius backup key** *word*	配置 RADIUS 备份认证服务共享密钥。
5	Inspur#**radius backup encrypt-key** *word*	以密文的形式配置备份 RADIUS 共享服务器密钥信息。
6	Inspur#**user login** { **local-radius** | **radius-local** [**server-no-response**] | **radius-user** }	配置用户通过 RADIUS 进行登录认证。
7	Inspur#**radius nas-ip-address** *ip-address*	配置 Radius 认证 NAS IP 地址。
8	Inspur#**radius response-timeout** *time*	配置 Radius 认证服务器响应超时时间。
9	Inspur#**radius authorization no-privilege** { **default** |**offline** | *priority* }	配置 RADIUS 授权失败的处理策略。
10	Inspur#**radius** [**backup**] **sourceip** { *ipv4-address* | *ipv6-address* }	配置 RADIUS 认证服务器的源 IP 地址。

12.4.5 配置 RADIUS 计费

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**aaa accounting login enable**	使能 RADIUS 计费功能。
2	Inspur# **radius** [**backup**] **accounting-server** { *ipv4-address* | *ipv6-address* } [**acct-port** *port-id*]	指定 RADIUS 计费服务器 IP 地址和 UDP 端口号。配置 **backup** 参数用以指定备份的 RADIUS 计费服务器。
3	Inspur#**radius accounting-server key** *string* Inspur#**radius accounting-server encrypt-key** *string*	配置与 RADIUS 计费服务器通信的共享明文密钥或者密文密钥。密钥必须与 RADIUS 计费服务器上设置的共享密钥一致，否则将计费失败。
4	Inspur#**radius accounting nas-ip-address** *ip-address*	配置 Radius 计费服务器 NAS IP 地址。
5	Inspur#**aaa accounting fail** { **offline** | **online** }	配置计费失败处理策略。
6	Inspur#**aaa accounting update** *minute*	配置计费更新报文发送周期。如果配置为 0，则不发送计费更新报文。 **说明** 通过计费开始报文、计费更新报文和计费结束报文，RADIUS 计费服务器可以记录每个用户的访问时间和操作。
7	Inspur#**radius** [**backup**] **accounting-server sourceip** { *ipv4-address* | *ipv6-address* }	配置 RADIUS 计费服务器的源 IP 地址。

12.4.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

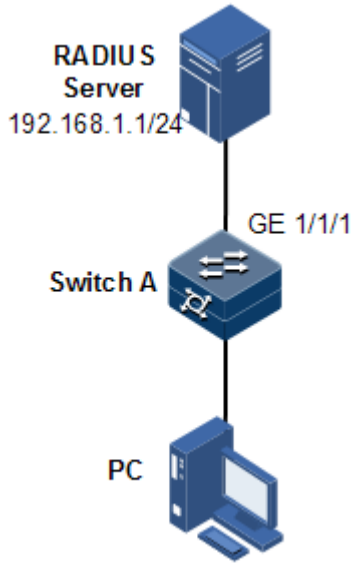
序号	检查项	说明
1	Inspur#**show radius-server**	查看 RADIUS 服务器配置信息。
2	Inspur#**show aaa**	查看 RADIUS 计费信息。

12.4.7 配置 RADIUS 应用示例

组网需求

如图 12-4 所示，为了控制用户对设备的访问，需要在 Switch A 上部署 RADIUS 认证和计费特性对登录 Switch A 的用户进行认证并记录其操作。要求更新报文发送间隔为 2min，并且计费失败时，使用户下线。

图12-4 RADIUS 应用组网示意图



配置步骤

步骤 1 配置通过 RADIUS 对登录用户认证。

```
Inspur#radius 192.168.1.1
Inspur#radius-key Inspur
Inspur#user login radius-user
```

步骤 2 配置通过 RADIUS 对登录用户计费。

```
Inspur#aaa accounting login enable
Inspur#radius accounting-server 192.168.1.1
Inspur#radius accounting-server key Inspur
Inspur#aaa accounting fail offline
Inspur#aaa accounting update 2
```

检查结果

通过 **show radius-server** 查看 RADIUS 配置是否正确。

```
Inspur#show radius-server
Server Response Timeout        :3s
Authentication server IP       :192.168.1.1
```

```
port                        :1812
Backup authentication server IP :
port                        :1812
Authentication server key      :o7MCKszV2X38
Backup authentication server Key:--
Accounting server IP          :192.168.1.1
port                        :1813
Backup accounting server IP    :
port                        :1813
Accounting server key         :gWOIjAJxkJKy
Backup Accounting server Key   :--
authorization fail policy      :15
NAS IP Address               :--
Accounting NAS IP Address      :--
Authentation source ip        :--
Authentation backup source ip  :--
Accounting source ip          :--
Accounting backup source ip    :--
```

通过 **show aaa** 查看 RADIUS 计费配置是否正确。

```
Inspur#show aaa
Accounting login:            enable
Update interval(minute):      2
Accounting fail policy:       offline
```

12.5 TACACS+

12.5.1 简介

TACACS+（Terminal Access Controller Access Control System，终端访问控制器访问控制系统）是一种与 RADIUS 类似的网络接入认证协议。其区别如下：

- TACACS+使用 TCP 端口 49，相对于 RADIUS 使用的 UDP 端口，具有更高的传输可靠性。
- TACACS+加密数据包除标准的 TACACS+头部外的整体，而包头中有一个区域会指示数据包是否加密。相对于 RADIUS 的只加密用户密码，安全性更高。
- TACACS+的认证功能与授权、计费功能相分离，部署更灵活。

综上所述，TACACS+较 RADIUS 更加安全、可靠，但是 RADIUS 作为一种开放性的协议，在网络中的应用更加广泛。

12.5.2 配置准备

场景

为了控制用户对设备和网络的访问，可以在网络中部署 TACACS+服务器对用户进行认证和计费。TACACS+较 RADIUS 更加安全、可靠。本设备可以作为 TACACS+服务器的代理设备，根据 TACACS+服务器反馈的结果对用户访问进行控制。

前提

无

12.5.3 TACACS+的缺省配置

设备上 TACACS+的缺省配置如下。

功能	缺省值
TACACS+功能状态	禁止
登录模式	local-user
TACACS+服务器 IP 地址	0.0.0.0，显示为“--”
TACACS+计费服务器 IP 地址	0.0.0.0，显示为“--”
与 TACACS+服务器通信的共享密钥	空
计费失败处理策略	online
更新报文发送周期	0

12.5.4 配置 TACACS+认证

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**tacacs-server [backup] {** *ipv4-address* | *ipv6-address* **}[auth-port** *port-id* **]**	指定 TACACS+认证服务器 IP 地址。配置 **backup** 参数用以指定备份的 TACACS+认证服务器。
2	Inspur#**tacacs-server [backup] key** *string* Inspur#**tacacs-server [backup] encrypt-key** *string*	配置 TACACS+认证的共享明文密钥或者密文密钥。配置 **backup** 参数用以指定备份的 TACACS+认证服务器。
3	Inspur#**user login { local-tacacs | tacacs-local [server-no-response] | tacacs-user }**	配置用户通过 TACACS+进行登录认证。
4	Inspur#**tacacs-server response-timeout** *time*	配置 TACACS+认证服务器响应超时时间。

12.5.5 配置 TACACS+计费

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**aaa accounting login enable**	使能 TACACS+计费功能。
2	Inspur#**tacacs** [**backup**] **accounting-server** { *ipv4-address* | *ipv6-address* }[**acct-port** *port-id*]	指定 TACACS+计费服务器 IP 地址。配置 **backup** 参数用以指定备份的 TACACS+计费服务器。
3	Inspur#**tacacs** [**backup**] **accounting-server key** *string* Inspur#**tacacs** [**backup**] **accounting-server encrypt-key** *string*	配置与 TACACS+计费服务器通信的共享明文密钥或者密文密钥。
4	Inspur#**aaa accounting fail** { **offline** | **online** }	配置计费失败处理策略。
5	Inspur#**aaa accounting update** *period*	配置计费更新报文发送周期。如果配置为 0，则不发送计费更新报文。

12.5.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show tacacs-server**	查看 TACACS+服务器配置信息。
2	Inspur#**show aaa**	查看 TACACS+计费的配置信息。

12.5.7 维护

用户可以通过以下命令，维护设备 TACACS+特性的运行情况和配置情况。

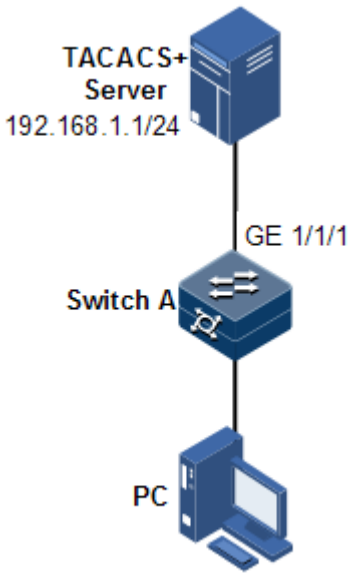
命令	描述
Inspur#**clear tacacs statistics**	清除 TACACS+统计信息。

12.5.8 配置 TACACS+应用示例

组网需求

如图 12-5 所示，为了控制用户对设备的访问，需要在 Switch A 上部署 TACACS+认证特性对登录 Switch A 的用户进行认证。

图12-5 TACACS+应用组网示意图



配置步骤

配置通过 TACACS+对登录用户认证。

```
Inspur#tacacs-server 192.168.1.1
Inspur#tacacs-server key Inspur
Inspur#user login tacacs-user
```

检查结果

通过 **show tacacs-server** 查看 TACACS+配置是否正确。

```
Inspur#show tacacs-server
Server Address               : 192.168.1.1
Port:  49
Server Status               : Active
Backup Server Address         : --
Port:  49
Backup Server Status         : --
Server Shared Key             : QHkoBSbi4CrD
Backup Authentication server Shared Key:       --
Accounting server Address      : --
Port:  49
Accounting server Status      : --
Backup Accounting server Address: --
Port:  49
Backup Accounting server Status: --
Accounting server Shared Key:                --
Backup Accounting server Shared Key:          --
Total Packet Sent               : 0
Total Packet Recv               : 0
Num of Error Packets             : 0
```

```
Server Response Timeout(s):  5
Server Quiet Time(m):  30
```

12.6 风暴抑制

12.6.1 简介

二层网络是一个广播域，当接口接收到大量的广播、未知组播和未知单播报文时，就会产生广播风暴。如果不对广播风暴进行限制，就会耗费大量的网络带宽，造成网络速率下降，甚至造成通信中断，影响正常报文的转发。

对网络中的广播流量进行限制，能在广播流量激增时抑制广播风暴的产生，从而保证正常报文的转发。

广播风暴产生

下面几种情况可能会产生广播风暴：

- 未知单播报文：目的 MAC 地址不在 MAC 地址表中的单播报文，即 DLF（Destination Lookup Failure，寻找目标失败）报文，如果某段时间内此种报文流量过多，进行大量的广播发送，可能会形成广播风暴。
- 未知组播报文：目的 MAC 地址不在 MAC 地址表中的组播报文，如果某段时间内此种报文流量过多，进行大量的广播发送，可能会形成广播风暴。
- 广播报文：目的 MAC 地址为广播的报文，如果某段时间内此种报文流量过多，可能会形成广播风暴。

风暴抑制原理

风暴抑制是对网络上可能形成广播风暴的广播、未知组播或未知单播报文进行过滤。当设备接收到的广播报文超过一定阈值时，将自动丢弃收到的广播报文。当未启用该功能或广播报文未达到一定阈值时，广播报文将被正常广播到设备的其它接口。

风暴抑制方式

风暴抑制方式有以下几种：

- Ratio（带宽比）：即允许广播、未知组播和未知单播流量占接口总带宽的百分比。
- BPS（Bits Per Second，每秒位数）：每秒允许通过的位数。
- PPS（Packets Per Second，每秒包数）：每秒允许通过的包数。

设备只支持 BPS 和 PPS 风暴抑制方式。

12.6.2 配置准备

场景

在二层网络中配置风暴抑制功能，当网络中未知组播、未知单播和广播报文增多时可以抑制广播风暴的产生，从而保证正常报文的转发。

前提

无

12.6.3 风暴抑制的缺省配置

设备上风暴抑制的缺省配置如下。

功能	缺省值
广播流量风暴抑制状态	使能
风暴抑制增强功能	禁用
组播流量和未知单播流量的风暴抑制状态	禁用
帧间隙和前导码的字节数	20B
风暴抑制方式	pps
每秒允许通过的包数，即 PPS 值	1024pps
DLF 报文转发功能状态	使能
接口的风暴抑制动作	丢弃报文
接口的恢复周期	300s
接口风暴抑制 Trap 功能	禁用

12.6.4 配置风暴抑制功能

注意

风暴抑制和基于 VLAN 的流量限速功能会相互影响，不建议用户在同一接口上同时开启这两个功能。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**storm-control detection enable**	使能风暴抑制增强功能。
3	Inspur(config)#**interface** *interface-type interface-number* Inspur(config)#**interface port-channel** *port-channel-number*	进入物理层接口配置模式或聚合组接口配置模式。

步骤	配置	说明
4	Inspur(config-gigaethernet1/1/*)#**storm-control** { **broadcast** | **unknown-multicast** | **dlf** | **all** } { **bps** *value* [**burst** *value*] | **pps** *value* } Inspur(config-port-channel*)#**storm-control** { **broadcast** | **unknown-multicast** | **dlf** | **all** } { **bps** *value* [**burst** *value*] | **pps** *value* }	使能物理接口或聚合组下的风暴抑制功能，配置风暴抑制的限速阈值。
5	Inspur(config-gigaethernet1/1/*)#**storm-control action** { **shutdown** | **drop** }	配置接口的风暴抑制动作。
6	Inspur(config-gigaethernet1/1/*)#**storm-control interval second** *interval*	配置风暴抑制关闭接口后接口的恢复周期。
7	Inspur(config-gigaethernet1/1/*)#**storm-control trap enable**	使能接口风暴抑制 Trap 功能。

注意

- 风暴限速同一时间只能用一种控制方式，当某一个报文类型切换控制限速方式时，会有提示信息告诉这样的切换会引起其他两类报文切换到相同的模式。
- 配置聚合组下的风暴抑制，端口下无法配置风暴抑制，否则配置不生效。

12.6.5 配置 DLF 报文转发

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**dlf-forwarding enable**	使能 DLF 报文转发功能。

12.6.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show storm-control interface** [*interface-type interface-number*]	查看风暴抑制配置信息。
2	Inspur#**show dlf-forwarding**	查看 DLF 报文转发状态。

序号	检查项	说明
3	Inspur#**show storm-control status interface** [*interface-type interface-number*]	查看风暴抑制状态。

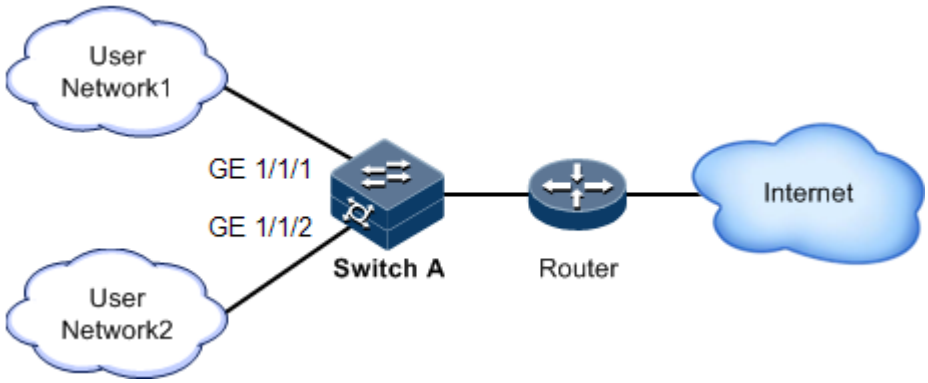
12.6.7 配置风暴抑制应用示例

组网需求

如图 12-6 所示，当 Switch A 的 GE 1/1/1 和 GE 1/1/2 接口接收到大量的未知单播或广播报文，Switch A 就会向 VLAN 内除了接收接口之外的所有接口转发这些报文，就可能会导致广播风暴，降低 Switch A 的转发性能。

为限制广播风暴对 Switch A 的影响，需要在 Switch A 的 GE 1/1/1 和 GE 1/1/2 接口上部署风暴抑制功能，分别限制来自用户网络 1 和用户网络 2 的广播报文，抑制阈值为 640kbit/s。

图12-6 风暴抑制应用组网示意图



配置步骤

步骤 1 配置风暴抑制阈值。

```
Inspur(config)#interface gigaethernet 1/1/1
Inspur(config-gigaethernet1/1/1)#storm-control broadcast bps 640
Inspur(config-gigaethernet1/1/1)#exit
Inspur(config)#interface gigaethernet 1/1/2
Inspur(config-gigaethernet1/1/2)#storm-control broadcast bps 640
```

检查结果

通过 **show storm-control** 查看风暴抑制配置是否正确。

```
Inspur#show storm-control interface
Interface      Packet-Type      Pps(pps)         Bps(Kbps)
-------------------------------------------------------------------------
```

```
GE1/1/1       Broadcast        --              640
              Multicast        --              0
              Dlf              --              0
GE1/1/2       Broadcast        --              640
              Multicast        --              0
              Dlf              --              0
```

12.7 802.1x

12.7.1 简介

802.1x 是基于 IEEE 802.1x 协议即基于接口的网络接入控制技术。802.1x 功能的主要目的是解决局域网用户的接入认证和安全问题。

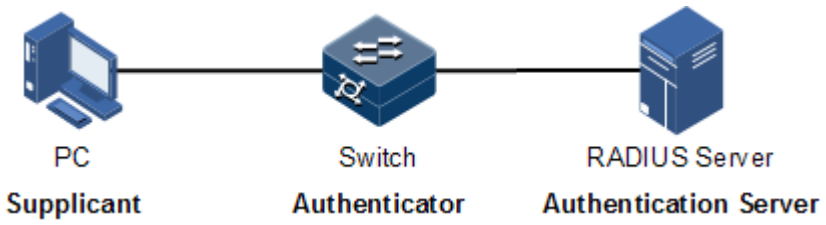
在网络设备的物理接入层对接入设备进行认证和控制，仅定义了设备接口和用户设备之间的点到点连接方式。连接在接口上的用户设备如果能够通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法通过交换机访问网络中的资源。

802.1x 体系结构

802.1x 认证采用客户端/服务器模式，如图 12-7 所示，包括以下 3 个部分：

- 申请者（Supplicant）：需要安装 802.1x 客户端软件（例如 Windows XP 自带的 802.1x 客户端）的用户侧设备，如计算机等。
- 认证者（Authenticator）：提供 802.1x 认证功能的接入控制设备，如交换机等。
- 认证服务器（Authentication Server）：用于对用户进行认证、授权和计费，通常使用 RADIUS 服务器作为 802.1x 认证服务器。

图12-7 802.1x 认证体系结构



接口接入控制模式

认证者利用认证服务器对需要接入局域网的客户端进行认证，并根据认证结果对接入接口授权或者非授权状态进行控制。用户可以通过配置接口的接入控制模式来控制接口的接入状态。802.1x 认证支持三种接口接入控制模式：

- 协议授权模式（auto）：由协议状态机决定认证授权结果，在认证成功之前，仅允许收发 EAPoL 报文，不允许用户访问网络资源和交换机提供的服务。如果认证通过，则接口切换到授权状态，允许用户访问网络资源和交换机提供的服务。

- 强制接口授权模式（authorized-force）：接口始终处于授权状态，允许用户不经认证授权即可访问网络资源和交换机提供的服务。
- 强制接口非授权模式（unauthorized-force）：接口始终处于非授权状态，不允许用户访问网络资源和交换机提供的服务，即不允许用户进行认证。

802.1x 认证过程

802.1x 系统支持 EAP 中继和 EAP 终结两种方式完成与 RADIUS 服务器之间的认证过程。

- EAP 中继方式

申请者与认证服务器之间通过 EAP（Extensible Authentication Protocol，可扩展认证协议）报文交换信息。申请者与认证者之间则以 IEEE802.1x 协议所定义的 EAPoL（EAP over LAN，基于局域网的 EAP）报文交换信息。EAP 报文中封装了认证数据，该认证数据将被封装在 RADIUS 协议的报文中，以穿越复杂的网络到达认证服务器，这一过程称为 EAP 中继。

认证者或申请者均能发起 802.1x 认证过程。以申请者发起认证过程为例，EAP 中继认证过程如下：

1. 用户输入用户名和密码，申请者向认证者发送一个 EAPoL-Start 报文，开始一次 802.1x 认证；
2. 认证者向申请者发送 EAP-Request/Identity 报文，询问请求者的用户名；
3. 申请者响应一个 EAP-Response/Identity 给认证者，其中包括用户名信息；
4. 认证者将 EAP-Response/Identity 报文封装到 RADIUS 协议报文中，发送给认证服务器；
5. 认证服务器将接收到的用户名信息与数据库中的用户名表进行比对，找到该用户的口令信息，利用随机生成的加密字对口令信息进行加密处理。同时，认证服务器将此加密字发送给认证者，认证者再将此加密字发送给申请者；
6. 申请者利用接收到的加密字对口令进行加密，并通过认证者发送给认证服务器；
7. 认证服务器对比收到的加密口令与自身生成的加密口令否一致。如果认证成功，认证者将接口改为授权状态，允许用户通过接口访问网络，并发送 EAP-Success 报文给申请者；如果认证失败，则接口为非授权状态，并发送 EAP-Failure 报文给通知申请者。

- EAP 终结方式

将 EAP 报文在设备端终结并映射到 RADIUS 报文中，利用标准 RADIUS 协议完成认证、授权和计费过程。设备端支持与 RADIUS 服务器之间采用 PAP 或者 CHAP 认证方法。

在 EAP 终结方式中，用来对用户密码信息进行加密处理的随机加密字由设备端生成，之后设备端会把用户名、随机加密字和客户端加密后的密码信息共同发送给 RADIUS 服务器，进行相关的认证处理。

802.1x 定时器

802.1x 认证过程中，认证设备上涉及到 5 个定时器：

- Reauth-period：重认证定时器。在该定时器超时后，会重新发起 802.1x 认证。
- Quiet-period：静默定时器。用户认证失败以后，认证设备需要静默一段时间，静默定时器超时后再重新发起认证。在静默期间，交换机不处理认证报文。

- Tx-period：请求报文发送超时定时器。当交换机向用户请求端发送 Request/Identity 请求报文后，会启动该定时器，在该定时器超时后，用户端软件未成功发送认证应答报文，则设备重发认证请求报文，此报文共重发 3 次。
- Supp-timeout：申请者认证超时定时器。当交换机向用户请求端发送了用于请求用户端 MD5 加密密文的 Request/Challenge 请求报文后，交换机启动该定时器。若在该定时器设置的时长内用户请求端未成功响应，交换机将重发该报文，此报文共重发两次。
- Server-timeout：认证服务器超时定时器。该定时器定义认证者和认证服务器会话超时的总时长，此定时器超时后认证者结束同认证服务器会话，重新开始一次新的认证过程。

12.7.2 配置准备

场景

为了实现对局域网用户的接入认证，并解决接入用户的安全问题，需要在设备上配置 802.1x 认证。

对于认证通过的用户，允许其访问网络中的资源；如果认证未通过，则该用户无法访问网络资源。通过对用户接入接口的认证控制，达到对用户管理的目的。

前提

配置 802.1x 认证之前，如果使用 RADIUS 认证服务器，需要完成以下任务：

- 配置 RADIUS 服务器 IP 地址和 RADIUS 公有密钥。
- 交换机能够与 RADIUS 服务器 Ping 通。

12.7.3 802.1x 功能的缺省配置

设备上 802.1x 功能的缺省配置如下。

功能	缺省值
全局 802.1x 功能状态	禁止
接口 802.1x 功能状态	禁止
全局认证方式	**chap**
接口接入控制模式	**auto**
接口认证方式	**portbased**
RADIUS 服务器超时定时器时间	100s
802.1x 重认证功能状态	禁止
802.1x 重认证定时器时间	3600s
802.1x 静默定时器时间	60s

功能	缺省值
请求报文重传定时器时间	30s
请求者超时定时器时间	30s

12.7.4 配置 802.1x 基本功能

注意

- 802.1x 和 STP 在接口上互斥，不能同时使用。
- 一个接口同一时刻只能处理一个用户认证请求。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**dot1x enable**	使能全局 802.1x 功能。
3	Inspur(config)#**dot1x authentication-method** { **chap** | **pap** | **eap** }	配置全局认证方式。
4	Inspur(config)#**dot1x auth-mode** { **radius** | **local** | **tacacs+** }	配置 802.1x 认证的认证模式。
5	Inspur(config)#**dot1x free-ip** *ip-address* [*ip-mask* | *mask-lenth*]	配置认证失败或退出授权的 802.1x 终端用户可以访问的 IP 地址段。
6	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
7	Inspur(config-gigaethernet1/1/*)#**dot1x enable**	使能接口 802.1x 功能。
8	Inspur(config-gigaethernet1/1/*)#**dot1x auth-control** { **auto** | **authorized-force** | **unauthorized-force** }	配置接口接入控制模式。
9	Inspur(config-gigaethernet1/1/*)#**dot1x auth-method** { **portbased** | **macbased** }	配置接口认证方式。
10	Inspur(config-gigaethernet1/1/*)#**dot1x keepalive** { **enable** | **disable** }	配置端口 802.1x 握手使能或者关闭
11	Inspur(config-gigaethernet1/1/*)#**dot1x max-user** *user-number*	配置 802.1x 端口允许认证的最大用户数。
12	Inspur(config-gigaethernet1/1/*)#**dot1x guest-vlan** *vlan-id*	配置指定端口的 802.1x Guest VLAN。

说明

如果全局或接口模式下未使能 802.1x 功能，则 802.1x 功能的接口控制模式为强制接口授权模式。

12.7.5 配置 802.1x 重认证

注意

重认证功能是针对已授权的用户发起的，所以在使能重认证功能之前，应该保证使能全局和接口 802.1x 功能。处于授权状态的接口在重认证过程中仍保持授权状态，如果重认证失败，才进入非授权状态。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**dot1x reauthentication enable**	使能 802.1x 重认证功能。

12.7.6 配置 802.1x 定时器

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**dot1x timer reauth-period** *reauth-period*	配置重认证定时器时间。
4	Inspur(config-gigaethernet1/1/*)#**dot1x timer quiet-period** *second*	配置静默定时器时间。
5	Inspur(config-gigaethernet1/1/*)#**dot1x timer supp-timeout** *supp-timeout*	配置申请者认证超时定时器时间。
6	Inspur(config-gigaethernet1/1/*)#**dot1x timer server-timeout** *server-timeout*	配置认证服务器超时定时器时间。

步骤	配置	说明
7	Inspur(config-gigaethernet1/1/*)#**dot1x timer keepalive-period** *second*	配置端口 802.1x 重传 Keepalive 报文时间间隔。
8	Inspur(config-gigaethernet1/1/*)#**dot1x timer tx-period** *second*	配置 Request/Identity 请求报文超时定时器。

12.7.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show dot1x** *interface-type interface-list*	查看接口 802.1x 配置信息
2	Inspur#**show dot1x** *interface-type interface-list* **statistics**	查看接口 802.1x 统计信息。
3	Inspur#**show dot1x** *interface-type interface-list* **user**	查看接口 802.1x 认证的用户信息。
4	Inspur#**show dot1x free-ip**	查看认证失败或退出授权的 802.1x 终端用户可以访问的 IP 地址段信息。

12.7.8 维护

用户可以通过以下命令，维护 802.1x 特性的运行情况和配置情况。

命令	描述
Inspur(config)#**clear dot1x** *interface-type interface-list* **statistics**	清除接口 802.1x 统计信息。

12.7.9 配置 802.1x 示例

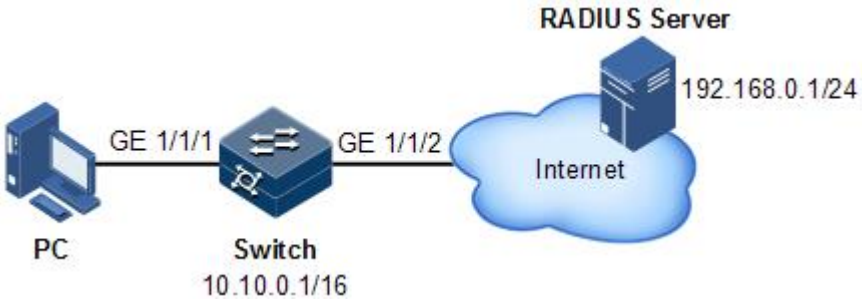
组网需求

为了使用户访问外部网络，如图 12-8 所示，在交换机上配置 802.1x 认证，具体要求如下：

- 交换机的 IP 地址是 10.10.0.1，掩码是 255.255.0.0，缺省网关地址为 10.10.0.2。
- 通过 RADIUS 服务器进行认证和授权，RADIUS 服务器的 IP 地址是 192.168.0.1，密码是 Inspur。
- 接口控制模式为协议授权模式。

- 在认证通过后，可以在 600s 后自动发起重认证过程。

图12-8 802.1x 应用组网示意图



配置步骤

步骤 1 配置交换机 IP 地址及 RADIUS 服务器地址。

```
Inspur#config
Inspur(config)#interface vlan 1
Inspur(config-vlan1)#ip address 10.10.0.1 255.255.0.0
Inspur(config-vlan1)#exit
Inspur(config)#ip route 0.0.0.0 0.0.0.0 10.10.0.2
Inspur(config)#exit
Inspur#radius 192.168.0.1
Inspur#radius-key Inspur
```

步骤 2 使能全局及接口 802.1x 认证功能。

```
Inspur#config
Inspur(config)#dot1x enable
Inspur(config)#interface gigaethernet 1/1/1
Inspur(config-gigaethernet1/1/1)#dot1x enable
```

步骤 3 （可选）配置授权模式为协议授权，缺省状态下为需要认证，无需配置。

```
Inspur(config-gigaethernet1/1/1)#dot1x auth-control auto
```

步骤 4 使能重认证功能，并设置重认证时间为 600s。

```
Inspur(config-gigaethernet1/1/1)#dot1x reauthentication enable
Inspur(config-gigaethernet1/1/1)#dot1x timer reauth-period 600
```

检查结果

通过 **show dot1x** 命令查看设备上 802.1x 功能的配置结果。

```
Inspur#show dot1x gigaethernet 1/1/1
802.1x Global Admin State: enable
802.1x Authentication Method: chap
802.1x Authentication Mode: radius
802.1x allowed max user number: 512
-------------------------------------------------------
Port gigaethernet1/1/1
```

```
------------------------------------------------------
802.1X Port Admin State: Enable
PAE: Authenticator
PortMethod: Portbased
PortControl: Auto
ReAuthentication: Enable
KeepAlive: Enable
QuietPeriod: 60(s)
ServerTimeout: 100(s)
SuppTimeout: 30(s)
ReAuthPeriod: 600(s)
TxPeriod: 30(s)
KeepalivePeriod: 60(s)
MaxUserNum: 512
GuestVlanID: 0
```

12.8 IP Source Guard

12.8.1 简介

IP Source Guard 利用绑定表来防御 IP 源欺骗，在不进行身份认证的情况下解决 IP 地址盗用的问题。IP Source Guard 可以和 DHCP Snooping 合作生成动态的绑定关系，也可以手工配置静态的绑定关系。DHCP Snooping 通过建立和维护一个 DHCP 绑定数据库来过滤不可信的 DHCP 消息。

IP Source Guard 绑定表项

IP Source Guard 用于匹配报文的特征项包括源 IP 地址、源 MAC 地址和 VLAN 标签，并且可支持接口与以下特征项的组合（以下简称绑定表项）：

- 接口＋IP
- 接口＋IP＋MAC
- 接口＋IP＋VLAN
- 接口＋IP＋MAC＋VLAN

按照绑定表项的产生方式，IP Source Guard 分为以下两种：

- 静态绑定：通过手工配置绑定信息，产生绑定表项来完成接口的控制功能，适用于主机数较少或者需要对某台主机进行单独绑定的情况。
- 动态绑定：通过 DHCP Snooping 自动获取绑定信息来完成接口的控制功能，适用于主机数较多并且采用 DHCP 进行动态主机配置的情况，可有效防止 IP 地址冲突和盗用等问题。

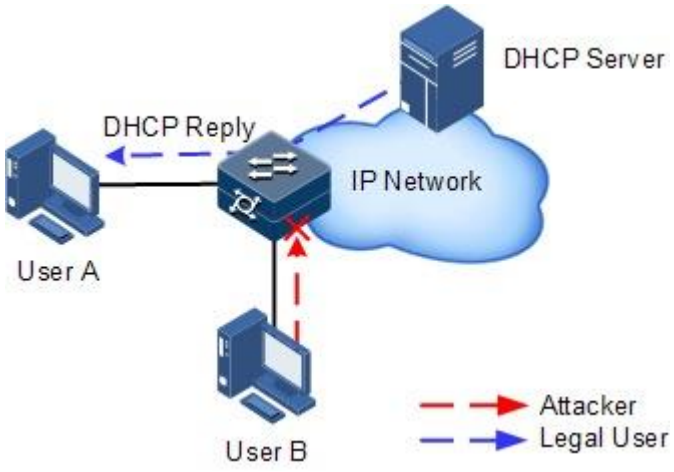
IP Source Guard 原理

IP Source Guard 的基本原理是在设备内部构建一个 IP 源绑定表，作为每个接口对接收数据包的检验依据。IP Source Guard 原理如图 12-9 所示，其转发原则如下：

- 所接收到的 IP 报文满足 IP 源绑定表中 Port/IP/MAC/VLAN 绑定表项的对应关系，则转发；

- 所接收到的 IP 报文为 DHCP 数据包，则转发；
- 所接收到的 IP 报文为其他情况，则丢弃。

图12-9 IP Source Guard 功能示意图



当设备在转发 IP 报文时，将此 IP 报文中的源 IP、源 MAC、接口、VLAN 信息和绑定表的信息进行比较，如果信息匹配，说明是合法用户，则允许此报文正常转发；否则认为是攻击者，丢弃该用户发送的 IP 报文。

12.8.2 配置准备

场景

网络中常常存在针对 IP 源进行欺骗的攻击行为，如攻击者仿冒合法用户发送 IP 报文给服务器，或者伪造其他用户的源 IP 地址进行通信，从而导致合法用户不能正常获得网络服务。

通过 IP Source Guard 绑定功能，可以对接口转发的报文进行过滤控制，防止非法报文通过接口，从而限制了对网络资源的非法使用，如非法主机仿冒合法用户 IP 接入网络等，提高了接口的安全性。

前提

配置 IP Source Guard 之前，需要完成以下任务：

- 如果存在 DHCP 用户，则需要使能 DHCP Snooping 功能。

12.8.3 IP Source Guard 功能的缺省配置

设备上 IP Source Guard 功能的缺省配置如下。

功能	缺省值
静态绑定功能状态	禁止

功能	缺省值
动态绑定功能状态	禁止
接口信任状态	不信任

12.8.4 配置 IP Source Guard 接口信任状态

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**ip verify source trust**	（可选）配置接口为信任状态。 使用 **no ip verify source trust** 配置接口为不信任状态。此时，除了 DHCP 报文以及符合绑定关系之外的所有 IP 报文都不被转发。接口处于信任状态时，所有报文均被正常转发。
4	Inspur(config-gigaethernet1/1/*)#**ipv6 verify source trust**	（可选）配置 IPv6 接口为信任状态。

12.8.5 配置 IP Source Guard 绑定功能

配置静态绑定功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ip verify source**	使能静态绑定功能。
3	Inspur(config)#**ip source binding** *ip-address* [*ip-mask-address*] [*mac-address*] [**vlan** *vlan-id*] *interface-type interface-number*	配置静态绑定关系。
4	Inspur(config)#**ipv6 source binding** *ipv6-address* [*mac-address*] [**vlan** *vlan-id*] *interface-type interface-number* Inspur(config)#**ipv6 source binding prefix** *ipv6-address/prefix-length* [*mac-address*] [**vlan** *vlan-id*] *interface-type interface-number*	配置 IPv6 静态绑定关系。

说明

在全局静态绑定功能禁止的情况下，配置的静态绑定关系不生效。只有当全局静态绑定功能使能时，静态绑定关系才生效。

手工配置的静态绑定关系会覆盖相同 IP 地址的动态绑定关系，但不能覆盖已有的静态绑定关系。当静态绑定关系删除后，系统会自动恢复被覆盖的动态绑定关系。

配置动态绑定功能

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#ip verify source dhcp`	使能动态绑定功能。
3	`Inspur(config)#ipv6 verify source dhcp-snooping`	使能 IPv6 动态绑定功能。

说明

在全局动态绑定功能禁止的情况下，通过 DHCP Snooping 学习到的动态绑定关系是不生效的；只有当全局动态绑定功能使能时，动态绑定关系才生效。

如果相同 IP 地址已经存在于静态绑定表中，则动态绑定关系不生效，不能覆盖已有的静态绑定关系。

配置绑定关系转换

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#ip verify source dhcp`	使能动态绑定功能。
3	`Inspur(config)#ip source binding dhcp static`	配置动态绑定关系转换为静态绑定关系。
4	`Inspur(config)#ip source binding auto-update`	（可选）使能自动转换为静态表项功能。由 DHCP Snooping 学到的动态绑定表项将直接转换成静态绑定表项。

12.8.6 配置 IP 报文的优先级和限速

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**ip verify source** [*ip-address ip-mask*] **set-cos** *cos-value*	配置 IP 报文的优先级和限速。

12.8.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show ip verify source**	查看全局绑定功能状态及接口信任状态。
2	Inspur#**show ip source binding** [*interface-type interface-number*]	查看绑定功能配置情况、接口信任状态以及绑定关系表。
3	Inspur#**show ip verify source set-cos**	查看优先级配置情况。
4	Inspur#**show ipv6 source binding** [*interface-type interface-number*]	查看 IPv6 Source Guard 的绑定关系信息。
5	Inspur#**show ipv6 verify source**	查看 IPv6 全局绑定功能状态及接口信任状态。

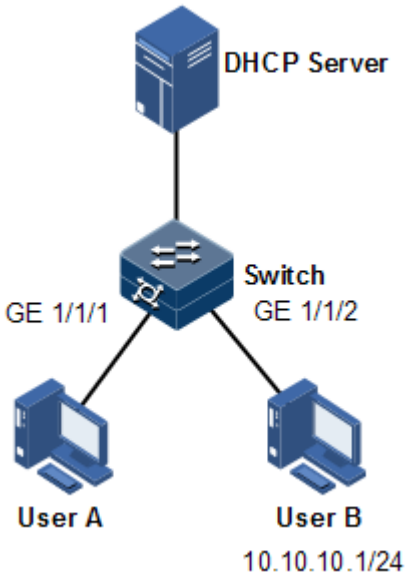
12.8.8 配置 IP Source Guard 示例

组网需求

如图 12-10 所示，为了防止 IP 地址盗用，需要在交换机上配置 IP Source Guard 功能，要求如下：

- 交换机允许接口 GE 1/1/1 上的所有 IP 报文通过；
- 接口 GE 1/1/2 允许指定 IP 地址为 10.10.10.1，子网掩码为 255.255.255.0 的 IP 报文以及符合 DHCP Snooping 学习到的动态绑定关系的报文通过；
- 其它接口仅允许通过 DHCP Snooping 学习的动态绑定关系的报文通过。

图12-10 IP Source Guard 应用组网示意图



配置步骤

步骤 1 配置 GE 1/1/1 为信任接口。

```
Inspur#config
Inspur(config)#interface gigaethernet 1/1/1
Inspur(config-gigaethernet1/1/1)#ip verify source trust
Inspur(config-gigaethernet1/1/1)#exit
```

步骤 2 配置静态绑定关系。

```
Inspur(config)#ip verify source
Inspur(config)#ip source binding 10.10.10.1 gigaethernet 1/1/2
```

步骤 3 使能全局动态绑定关系。

```
Inspur(config)#ip verify source dhcp
```

检查结果

通过 **show ip source binding** 命令查看静态绑定表配置结果。

```
Inspur#show ip source binding
History Max Entry Num: 1
Current Entry Num: 1
Ip Address        Mask                Mac Address     VLAN   Port
Type          Inhw
------------------------------------------------------------------------
------------------------------------------
10.10.10.1        255.255.255.255       --            --
gigaethernet1/1/2         static         yes
```

通过 **show ip verify source** 命令查看设备上接口信任状态和静态/动态绑定功能状态。

```
Inspur#show ip verify source
Static Bind: Enable
Dhcp Bind: Enable
Port                          Trust
----------------------------------------
gigaethernet1/1/1              yes
gigaethernet1/1/2              no
gigaethernet1/1/3              no
gigaethernet1/1/4              no
gigaethernet1/1/5              no
gigaethernet1/1/6              no
gigaethernet1/1/7              no
gigaethernet1/1/8              no
gigaethernet1/1/9              no
gigaethernet1/1/10             no
……
```

12.9 PPPoE+

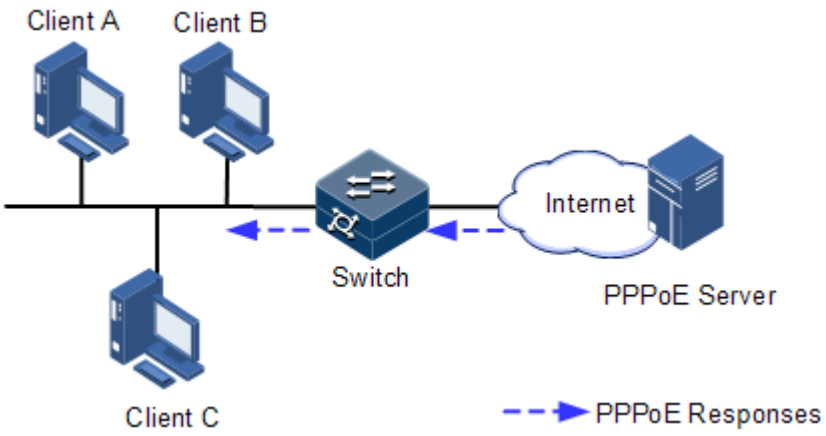
12.9.1 简介

PPPoE+（PPPoE Intermediate Agent，PPPoE 中继代理）协议用于对 PPPoE（Point to Point Protocol Over Ethernet，基于以太网承载点到点协议）认证报文进行处理，即对 PPPoE 报文附加更多接入设备信息，使服务器能获得足够的信息辨别用户。PPPoE+协议可以有效防止在 PPPoE 认证过程中的账号共享或者账号盗用问题，保证了网络的安全性。

使用 PPPoE 拨号方式连接网络，用户通过设备的不同接口，只要通过同一个认证服务器认证成功，就可以使用这个账号访问网络。但是服务器仅根据包含用户名和密码的认证信息，很难对用户进行区分。增加 PPPoE+特性以后，认证时除了需要用户名和密码信息外，在认证报文中还将携带设备接口等信息。如果认证服务器识别的接口号等信息与配置不一致，则认证不通过，这样就可以防止非法用户盗用其他合法用户的账号进行上网。

PPPoE 协议采用客户端/服务器模式，如图 12-11 所示，Switch 起到中继代理的作用，用户通过 PPPoE 认证连接网络。如果服务器需要定位用户，在认证报文中则需要更多的客户信息。

图12-11 用户通过 PPPoE 认证连接网络示意图



用户通过 PPPoE 访问网络需要经过两个阶段：第一个阶段是发现阶段，即认证阶段，第二个阶段是会话阶段。PPPoE+功能需要处理的就是发现阶段的报文。

- 客户端通过 PPPoE 访问网络，首先会发送一个广播报文 PADI（PPPoE Active Discovery Initiation，PPPoE 活动发现发起报文），该报文的作用是查找认证服务器；
- 收到 PADI 报文的认证服务器会发送一个单播 PADO（PPPoE Active Discovery Offer，PPPoE 活动发现提供报文）报文响应；
- 如果有多个认证服务器发送了 PADO 报文，客户端会从中选择一个，发送单播 PADR（PPPoE Active Discovery Request，PPPoE 活动发现请求报文）报文请求认证；
- 认证服务器收到 PADR 报文后，如果判定用户合法，则发送一个单播报文 PADS（PPPoE Active Discovery Session-confirmation，PPPoE 活动发现会话确认报文）作为 PADR 的响应。至此，发现阶段完毕。

PPPoE+的主要功能是在 PADI 和 PADR 报文中添加用户标识信息，服务器可以判定标识信息是否和用户账号匹配，决定是否分配资源。

12.9.2 配置准备

场景

为了防止在 PPPoE 认证过程中有非法用户接入，需要配置 PPPoE+功能，在 PPPoE 协议报文中加入附加的用户标识信息。

由于添加的用户标识信息和具体的交换机及接口相关，因此认证服务器可以将用户和交换机以及接口等信息绑定。从而有效防止账号共享和账号盗用问题，还可以更好的定位用户，以保证网络的安全性。

前提

无

12.9.3 PPPoE+功能的缺省配置

设备上 PPPoE+功能的缺省配置如下。

功能	缺省值
全局 PPPoE+功能状态	禁止
接口 PPPoE+功能状态	禁止
Circuit ID 的填充模式	Switch 模式
Circuit ID 信息	接口号/VLAN 号/附加字符串
Circuit ID 的附加字符串	交换机的主机名（hostname）
Remote ID 填充的 MAC 地址	交换机的 MAC 地址
Remote ID 填充形式	二进制形式
接口信任状态	非信任接口
信息字段 Tag 覆盖功能状态	禁止

说明

缺省情况下，PPPoE 报文可以通过接口并且不会被附加任何信息。

12.9.4 配置 PPPoE+基本功能

注意

PPPoE+功能用于处理 PADI 和 PADR 报文，只针对 PPPoE 的客户端。一般只有连接客户端的接口使能 PPPoE+功能，而信任接口是指交换机与 PPPoE 服务器连接的接口，这两种接口角色是互斥的，即一个接口不能既使能 PPPoE+功能又是信任接口。

使能 PPPoE+功能

使能设备全局和接口的 PPPoE+功能后，发送到该接口的 PPPoE 认证报文会附加上用户信息，再发往信任接口。

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#pppoeagent enable`	使能全局 PPPoE+功能。

步骤	配置	说明
3	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
4	Inspur(config-gigaethernet1/1/*)#**pppoeagent enable**	使能接口 PPPoE+功能。

配置 PPPoE+信任接口

配置 PPPoE+信任接口主要是为了防止 PPPoE 服务器欺骗和因 PPPoE 报文转发至其他非业务接口而造成的安全隐患，一般将与 PPPoE 服务器相连的接口设置为信任接口。从 PPPoE 客户端到服务器方向的 PPPoE 协议报文将只会由信任接口转发，同时也只有从信任接口收到的 PPPoE 协议报文才会被转发至 PPPoE 客户端。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**pppoeagent trust**	配置 PPPoE+的信任接口。

说明

由于 PPPoE+功能针对 PPPoE 的客户端而不是服务器，设备的下联接口不可能收到 PADO 和 PADS 报文，即使能 PPPoE+功能的接口不应该收到 PADO 和 PADS 报文。若收到这些报文说明有错误报文，应该丢弃，但可以转发来自信任接口的 PADO 和 PADS 报文。同时，PADI 和 PADR 报文应该只向信任接口转发。

12.9.5 配置 PPPoE+报文信息

PPPoE+功能主要是对 PPPoE 报文中的一个特定 Tag 进行处理，这个 Tag 包含 Circuit ID 和 Remote ID 两个字段。其中：

- Circuit ID 填充的是接收客户端请求报文接口属于的 VLAN ID、接口号以及主机名信息；
- Remote ID 填充的是客户端的 MAC 地址或者交换机的 MAC 地址。

配置 Circuit ID

Circuit ID 有两种填充模式：Switch 模式和 ONU 模式，缺省为 Switch 模式。在 ONU 模式下，Circuit ID 的格式是固定的，不存在自定义格式。这些命令用于在 Switch 模式下配置 Circuit ID 的填充内容。

在 Switch 模式下，Circuit ID 有两种填充格式：

- 默认格式：即未配置自定义 Circuit ID 时，填充为 VLAN 号/接口号/附加字符串（如果没有定义附加字符串，默认是主机名 hostname）。
- 自定义格式：即配置了自定义 Circuit ID 时，填充为配置的 Circuit ID 字符串。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**pppoeagent circuit-id** { **attach-string** | **format** | **hex** } *string*	配置交换机 Circuit ID 的附加字符串。
3	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
4	Inspur(config-gigaethernet1/1/*)#**pppoeagent circuit-id** *string*	（可选）配置 Circuit ID 为自定义的字符串。

Circuit ID 在默认格式下包含了一个附加字符串，附加字符串默认是交换机的 hostname，用户可以将其配置为自定义的字符串。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**pppoeagent circuit-id attach-string** *string*	（可选）配置 Circuit ID 的附加字符串。 如果 Circuit ID 是默认格式，该命令配置的内容会被添加到 Circuit ID 中。

配置 Remote ID

Remote ID 填充的是一个 MAC 地址，可以选择填充交换机的 MAC 地址或者客户端的 MAC 地址，并且可以选择二进制形式或者 ASCII 形式填充 Remote ID。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**pppoeagent remote-id** { **client-mac** | **switch-mac** | **user-define** *string* }	（可选）配置接口 PPPoE+的 Remote ID 填充的 MAC 地址。

步骤	配置	说明
4	Inspur(config-gigaethernet1/1/*)#**pppoeagent remote-id format** { **ascii** | **binary** }	（可选）配置接口 PPPoE+的 Remote ID 填充形式。

配置信息字段 Tag 覆盖功能

由于某些原因，如某些信息字段的 Tag 可能是客户端伪造的，需要将报文原有的 Tag 覆盖掉。使能 Tag 覆盖功能后，如果 PPPoE 报文已经携带信息字段 Tag，会将其覆盖，如果没有则添加。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**pppoeagent vendor-specific-tag overwrite enable**	使能信息字段 Tag 覆盖功能。

12.9.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show pppoeagent** [*interface-type interface-number*]	查看 PPPoE+的配置信息。
2	Inspur#**show pppoeagent statistic** [*interface-type interface-number*]	查看 PPPoE+的统计信息。

12.9.7 维护

用户可以通过以下命令，维护 PPPoE+特性的运行情况和配置情况。

命令	描述
Inspur(config)#**clear pppoeagent statistic** [*interface-type interface-number*]	清除 PPPoE+的统计信息，支持指定端口清除统计信息。

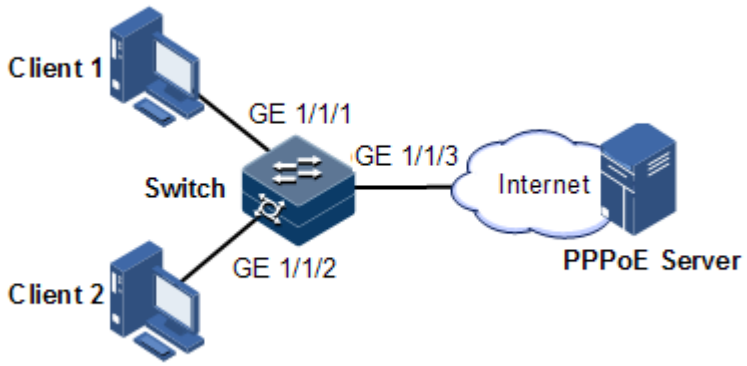
12.9.8 配置 PPPoE+示例

组网需求

如图 12-12 所示，为了防止在 PPPoE 认证过程中非法用户的接入，对用户上网进行控制和监管，可以在交换机上配置 PPPoE+功能，具体要求如下：

- 接口 GE 1/1/1 和 GE 1/1/2 分别连接 Client 1 和 Client 2，GE 1/1/3 连接 PPPoE 服务器；
- 使能全局 PPPoE+功能和 GE 1/1/1、GE 1/1/2 的 PPPoE+功能，配置 GE 1/1/3 为信任接口；
- 配置 Circuit ID 的附加字符串信息为 Inspur，GE 1/1/1 的 Circuit ID 的填充内容为 user01，GE 1/1/2 的 Remote ID 为客户端 MAC 地址，填充形式为 ASCII 码形式；
- 使能接口 GE 1/1/1 和 GE 1/1/2 的 Tag 覆盖功能。

图12-12 PPPoE+应用组网示意图



配置步骤

步骤 1 配置 GE 1/1/3 为信任接口。

```
Inspur#config
Inspur(config)#interface gigaethernet 1/1/3
Inspur(config-gigaethernet1/1/1)#pppoeagent trust
Inspur(config-gigaethernet1/1/1)#exit
```

步骤 2 配置 GE 1/1/1 和 GE 1/1/2 的报文信息。

```
Inspur(config)#pppoeagent circuit-id attach-string Inspur
Inspur(config)#interface gigaethernet 1/1/1
Inspur(config-gigaethernet1/1/1)#pppoeagent circuit-id user01
Inspur(config-gigaethernet1/1/1)#exit
Inspur(config)#interface gigaethernet 1/1/2
Inspur(config-gigaethernet1/1/2)#pppoeagent remote-id client-mac
Inspur(config-gigaethernet1/1/2)#pppoeagent remote-id format ascii
Inspur(config-gigaethernet1/1/2)#exit
```

步骤 3 使能 GE 1/1/1 和 GE 1/1/2 的 Tag 覆盖功能。

```
Inspur(config)#interface gigaethernet 1/1/1
Inspur(config-gigaethernet1/1/1)#pppoeagent vendor-specific-tag overwrite
enable
Inspur(config-gigaethernet1/1/1)#exit
Inspur(config)#interface gigaethernet 1/1/2
Inspur(config-gigaethernet1/1/2)#pppoeagent vendor-specific-tag overwrite
enable
Inspur(config-gigaethernet1/1/2)#exit
```

步骤 4 使能全局 PPPoE+功能，并使能 GE 1/1/1 和 GE 1/1/2 的 PPPoE+功能。

```
Inspur(config)#pppoeagent enable
Inspur(config)#interface gigaethernet 1/1/1
Inspur(config-gigaethernet1/1/1)#pppoeagent enable
Inspur(config-gigaethernet1/1/1)#exit
Inspur(config)#interface gigaethernet 1/1/2
Inspur(config-gigaethernet1/1/2)#pppoeagent enable
```

检查结果

通过 **show pppoeagent** 命令查看设备上 PPPoE+功能的配置结果。

```
Inspur#show pppoeagent
Global PPPoE+ status: disable
Attach-string: %default%
Circuit ID padding mode: switch

Port        :gigaethernet1/1/1
State       :disable
Overwrite    :disable
Format-rules :binary
Remote-ID    :switch-mac
Circuit-ID   :%default%

Port        :gigaethernet1/1/2
State       :disable
Overwrite    :disable
Format-rules :binary
Remote-ID    :switch-mac
Circuit-ID   :%default%

Port        :gigaethernet1/1/3
State       :disable
Overwrite    :disable
Format-rules :binary
 --More--
```

12.10 配置 URPF

12.10.1 配置准备

场景

为防止基于源地址欺骗的网络攻击行为，可使能路由器接口 URPF（Unicast Reverse Path Forwarding，单播逆向路径转发）功能。使能该功能后，当接口收到报文时，首先会对报文的源地址进行合法性检查，通过源地址合法性检查的报文，才会查找去往目的地址的转发表项，进入报文转发流程；否则，将丢弃报文。

前提

无

12.10.2 配置 URPF

请在需要的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**ip urpf** { **loose** | **strict** } [**allow-default-route**]	使能接口的 URPF 功能。 缺省情况下，设备禁用接口的 URPF 功能。

12.11 配置 CPU 保护

12.11.1 配置准备

场景

当设备短时间内接收到大量的攻击报文，导致 CPU 满负荷运转，利用率达到 100%，会导致设备的正常功能无法运行。使用 CPU CAR 功能可以有效限制进入 CPU 的报文的速率。

前提

无

12.11.2 配置全局 CPU CAR 功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**cpu-protect car** { **arp** | **bpdu** | **dhcp** | **icmp** | **global** | **igmp** | **lldp** | **mld** | **stp** } { **pps** *pps-value* | **kbps cir** *cir* **cbs** *cbs* }	配置全局 CPU 报文保护的协议类型、CIR 及 CBS。
3	Inspur(config)#**cpu-protect car period** *time*	配置全局 CPU 报文保护的恢复时间间隔，使用 no 格式删除该配置。
4	Inspur(config)#**cpu-protect car trap** { **enable** | **disable** }	使能或禁止全局 CPU 报文保护告警功能

说明

CPU 保护的配置对各协议模块的功能有重要的影响，建议不要轻易修改 CPU 保护的参数配置，只有专家才能修改相关配置。

12.11.3 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show cpu-protect car statistics** [*interface-type interface-number* | **dynamic**]	查看 CPU CAR 统计信息。

12.11.4 维护

命令	说明
Inspur(config)#**clear cpu-protect car** { **arp** | **bpdu** | **dhcp** | **global** | **icmp** | **igmp** | **lldp** | **mld** | **stp** } **statistics**	清除全局的 CPU CAR 统计信息。

12.12 ARP 防攻击

12.12.1 配置准备

场景

ARP 协议有简单、易用的优点，但是也因为其没有任何安全机制而容易被攻击发起者利用。

攻击者可以仿冒用户、仿冒网关发送伪造的 ARP 报文，使网关或主机的 ARP 表如果网络中有主机通过向设备发送大量目标 IP 地址不能解析的 IP 报文来攻击设备，则会造成下面的危害：

- 设备向目的网段发送大量 ARP 请求报文，加重目的网段的负载。
- 设备会试图反复地对目标 IP 地址进行解析，增加了 CPU 的负担。

为避免这种 IP 报文攻击所带来的危害，设备提供了下 ARP 防攻击功能。

前提

无

12.12.2 配置 ARP 功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface vlan** *vlan-id*	进入 VLAN 接口配置模式。
3	Inspur(config-vlan*)#**arp learning strict enable**	使能设备只学习自己请求的 ARP 表项功能。
4	Inspur(config-vlan*)#**arp check-destination-ip enable**	使能 ARP 目的地址检查功能。
5	Inspur(config-vlan*)#**arp filter** { **gratuitous** | **mac-illegal** | **tha-filled-request** }	配置 ARP 过滤功能。
6	Inspur(config-vlan*)#**arp anti-attack entry-check** { **fixed-all** | **fixed-mac** | **send-ack** }	配置 ARP 表项固化功能。

12.12.3 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show arp**	查看 ARP 信息。
2	Inspur#**show ip arp filter**	查看 ARP 过滤信息。

13 系统管理

本章介绍系统管理与维护特性的基本原理和配置过程，并提供相关的配置案例。

- SNMP
- RMON
- LLDP
- 光模块数字诊断
- 系统日志
- 配置告警管理
- 硬件环境监控
- 风扇监控
- 性能统计
- Ping
- Traceroute

13.1 SNMP

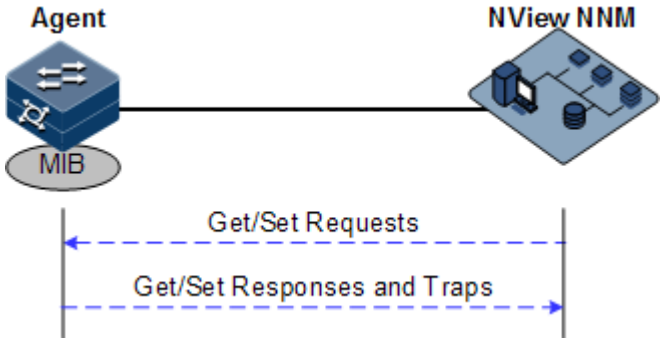
13.1.1 简介

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

工作机制

SNMP 的结构分为代理 Agent 和网管系统两部分。代理和网管系统之间是通过 UDP 传送 SNMP 报文进行通信。SNMP 工作机制如图 13-1。

图13-1 SNMP 工作机制示意图



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

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

代理是驻留在被管设备上的一个进程，主要实现以下功能：

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

说明

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

协议版本

目前，SNMP 协议共有 v1、v2c 和 v3 三个版本。

- SNMPv1 采用共同体名（Community Name）认证机制。共同体名用来定义 SNMP 网管系统和 SNMP 代理之间的关系，起到了类似于密码的作用，用来限制 SNMP 网管系统对 SNMP 代理的访问。如果 SNMP 报文携带的共同体名在设备上没有认证通过，该报文将被丢弃。
- SNMPv2c 也采用共同体名认证机制。它在兼容 SNMP v1 的同时又扩充了 SNMP v1 的功能：支持更多的操作类型、数据类型和错误代码、能够更细致地区分错误。
- SNMPv3 采用了 USM（User-Based Security Model，基于用户的安全模型）和 VACM（View-based Access Control Model，基于视图的访问控制模型）安全机制。用户可以设置认证和加密功能，通过有无认证和有无加密等功能组合，可以

为 SNMP 网管系统和 SNMP 代理之间的通信提供更高的安全性。认证用于验证报文发送方的合法性，避免非法用户的访问；加密则是对网管系统和代理之间的传输报文进行加密，以免被窃听。

设备同时支持 SNMP 的 v1、v2c、v3 三个版本。

MIB

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

- 名字
- 访问权限
- 数据类型

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

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

设备支持标准的 MIB 库和浪潮思科自定义的 MIB 库。

13.1.2 配置准备

场景

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

前提

在配置 SNMP 之前，需完成以下任务：

- 配置路由协议，使设备和网管系统之间路由可达。

13.1.3 SNMP 的缺省配置

设备上 SNMP 的缺省配置如下。

功能	缺省值
SNMP 视图	缺省存在：system、internet 视图
SNMP 共同体	缺省存在：public、private 共同体 Index CommunityName ViewName Permission 1 public internet ro 2 private internet rw

功能	缺省值
SNMP 访问组	缺省存在：initialnone、initial 组
SNMP 用户	缺省存在： none、md5nopriv、shapriv、md5priv、shanopriv 用户
SNMP 用户和访问组的映射关系	Index GroupName UserName SecModel ---------- 0 initialnone none usm 1 initial md5priv usm 2 initial shapriv usm 3 initial md5nopriv usm 4 initial shanopriv usm
网管人员的标识和联系方法	support@Inspur.com
设备放置的物理位置	world china Inspur
Trap 状态	使能
SNMP 目标主机地址	无
SNMP 引擎 ID	800022B603000E5E000016

13.1.4 配置 SNMP v1/v2c 基本功能

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

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

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

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#snmp-server view` *view-name oid-tree* [*mask*] { `excluded` | `included` }	（可选）创建 SNMP 视图，并配置访问的 MIB 变量范围。 缺省视图是 internet，范围包括 MIB 树中“1.3.6”节点以下的所有 MIB 变量。

步骤	配置	说明
3	Inspur(config)#**snmp-server community** [**encryption**] *string* [**view** *view-name*] { **ro** | **rw** }	创建共同体名并配置对应的视图和访问权限。 如果没有填写 **view** *view-name* 选项，则采用缺省视图 internet。

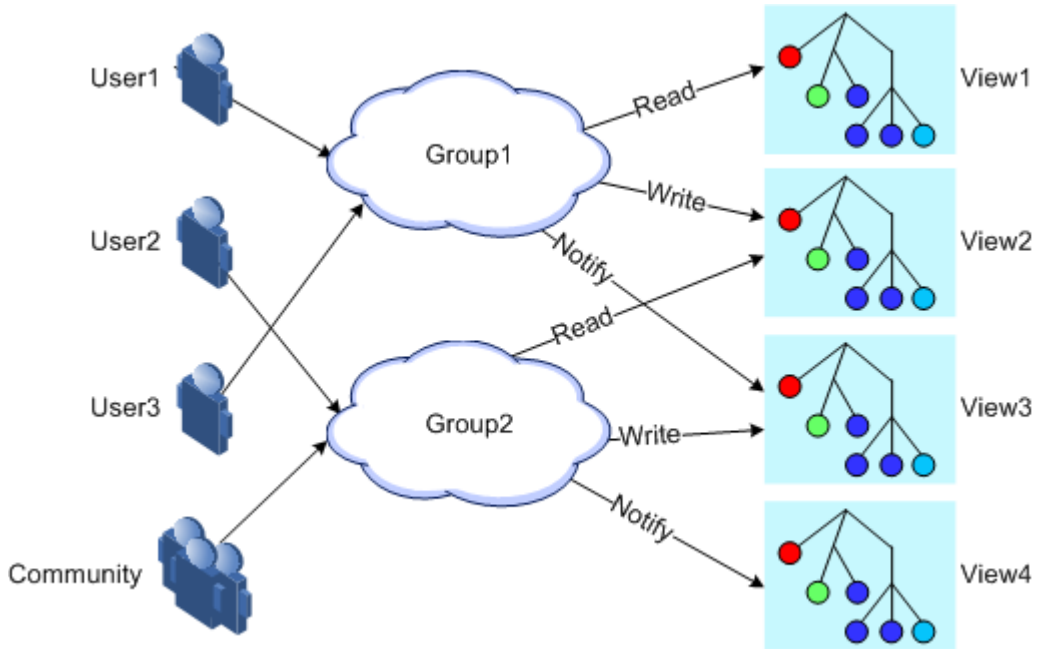
13.1.5 配置 SNMP v3 基本功能

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

如图 13-2 所示，网管站采用 SNMP v3 对交换机正常的访问，需要进行的配置如下：

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

图13-2 SNMP v3 认证机制示意图



请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**snmp-server view** *view-name oid-tree* [*mask*] { **excluded** | **included** }	创建 SNMP 视图，并配置访问的 MIB 变量范围。
3	Inspur(config)#**snmp-server user** *user-name* [**remote** *engine-id*] **authentication** { **md5** | **sha** } *authpassword* [**privacy** *privacypassword*]	创建用户并配置认证方式。
4	Inspur(config)#**snmp-server user** *user-name* [**remote** *engine-id*] **authkey** { **md5** | **sha** } *authpassword* [**privkey** *privkeypassword*]	（可选）修改用户认证密钥及加密密钥。
5	Inspur(config)#**snmp-server access** *group-name* [**read** *view-name*] [**write** *view-name*] [**notify** *view-name*] [**context** *context-name* { **exact** | **prefix** }] **usm** { **authnopriv** | **authpriv** | **noauthnopriv** }	创建并配置 SNMP v3 访问组。
6	Inspur(config)#**snmp-server group** *group-name* **user** *user-name* **usm**	配置用户和访问组的映射关系。

13.1.6 配置 SNMP 服务器 IP 认证

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**snmp-server server-auth** { **enable** | **disable** }	使能或关闭 SNMP 服务器 IP 认证功能。
3	Inspur(config)#**snmp-server server-auth** *ip-address*	配置 SNMP 服务器 IP 认证地址。

13.1.7 配置 SNMP 其他信息

配置 SNMP 的其他信息包括：

- 网管人员的标识和联系方法：用来设置管理人员的标识及联系方法。
- 设备存放的物理位置：描述交换机存放的物理位置。

SNMP v1、v2c、v3 均支持以上信息的配置。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**snmp-server contact** *contact*	（可选）配置网管人员的标识与联系方法。 **说明** 例如采用 E-mail 作为人员的标识与联系方法。
3	Inspur(config)#**snmp-server location** *location*	（可选）指定设备放置的物理位置。
4	Inspur(config)#**snmp-agent source** *ip-address*	（可选）配置读取（walk）设备 mib 时回应报文的源 IP 地址。

13.1.8 配置 Trap

说明

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

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

在配置 Trap 功能之前，需完成以下任务：

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

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**snmp-server host** { *ip-address* | *ipv6-address* } **version 3** { **authnopriv** | **authpriv** | **noauthnopriv** } *user-name* [**udpport** *udpport*]	（可选）配置基于 SNMP v3 的 Trap 目标主机。
3	Inspur(config)#**snmp-server host** { *ip-address* | *ipv6-address* } **version** { **1** | **2c** } *com-name* [**udpport** *udpport*]	（可选）配置基于 SNMP v1 和 SNMP v2c 的 Trap 目标主机。
4	Inspur(config)#**snmp-server enable traps**	使能交换机发送 Trap 的功能。
5	Inspur(config)#**snmp-server trap-source** *interface-type interface-number*	指定交换机发送 Trap 的源接口。
6	Inspur(config)#**snmp-server trap-source** *ip-address*	配置 SNMP TRAP 报文的源 IP 地址。

步骤	配置	说明
7	Inspur(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
8	Inspur(config-gigaethernet1/1/*)#**snmp trap link-status** { **enable** | **disable** }	使能 SNMP 产生 LINK TRAPS 功能，使用 **disable** 格式禁止该功能。

13.1.9 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show snmp access**	查看 SNMP 访问组的配置信息。
2	Inspur#**show snmp community**	查看 SNMP 共同体的配置信息。
3	Inspur#**show snmp config**	查看 SNMP 的基本配置信息。 包含本地 SNMP 引擎 ID，网管人员的标识及联系方法，设备所在位置，Trap 开关状态信息。
4	Inspur#**show snmp group**	查看 SNMP 用户和访问组的映射关系。
5	Inspur#**show snmp host**	查看 Trap 目标主机信息。
6	Inspur#**show snmp statistics**	查看 SNMP 的统计信息。
7	Inspur#**show snmp user**	查看 SNMP 用户信息。
8	Inspur#**show snmp view**	查看 SNMP 的视图信息。
9	Inspur#**show snmp server-auth**	查看 SNMP 服务器认证配置信息。

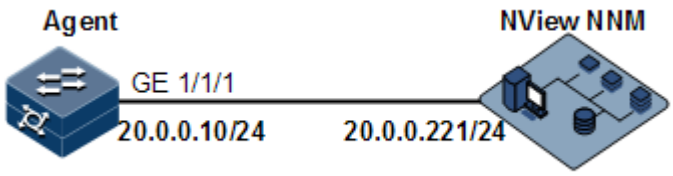
13.1.10 配置 SNMP v1/v2c 和 Trap 示例

组网需求

如图 13-3 所示，NView NNM 网管系统与交换机设备之间路由可达，NView NNM 通过 SNMP v1/v2c 可以查看远程交换机的对应视图下的 MIB，交换机出现紧急情况时可以主动向 NView NNM 发送 Trap。

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

图13-3 SNMP v1/v2c 组网示意图



配置步骤

步骤 1 配置交换机设备的 IP 地址。

```
Inspur#config
Inspur(config)#interface vlan 1
Inspur(config-vlan1)#ip address 20.0.0.10 255.255.255.0
Inspur(config-vlan1)#exit
```

步骤 2 配置 SNMP v1/v2c 的视图。

```
Inspur(config)#snmp-server view mib2 1.3.6.1.2.1 included
```

步骤 3 配置 SNMP v1/v2c 的共同体。

```
Inspur(config)#snmp-server community Inspur view mib2 ro
```

步骤 4 配置 Trap 告警。

```
Inspur(config)#snmp-server enable traps
Inspur(config)#snmp-server host 20.0.0.221 version 2c Inspur
```

检查结果

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

```
Inspur#show ip interface brief
VRF                  IF                          Address        NetMask
Catagory
-------------------------------------------------------------------------
------------------------------
Default-IP-Routing-Table  fastethernet1/0/1            192.168.0.1
255.255.255.0   primary
Default-IP-Routing-Table  vlan1                      20.0.0.10
255.255.255.0   primary
```

通过 **show snmp view** 查看视图配置是否正确。

```
Inspur#show snmp view
Index:    0
View Name: mib2
OID Tree:  1.3.6.1.2.1
Mask:     1.1.1.1.1.1.1.1
Type:     included

Index:    1
```

```
View Name: system
OID Tree:  1.2.840.10006.300.43
Mask:      --
Type:      included

Index:     2
View Name: system
OID Tree:  1.3.6.1.2.1.1
Mask:      --
Type:      included

Index:     3
View Name: internet
OID Tree:  1.3.6
Mask:      --
Type:      included

Index:     4
View Name: internet
OID Tree:  1.2.840.10006.300.43
Mask:      --
Type:      included
```

通过 **show snmp community** 查看共同体配置是否正确。

```
Inspur#show snmp community
Index   Community Name      View Name          Permission
-------------------------------------------------------------
1       private             internet           rw
2       public              internet           ro
3       Inspur            mib2               ro
```

通过 **show snmp host** 查看目标主机配置是否正确。

```
Inspur#show snmp host
Index:         0
IP family:      IPv4
IP address:     20.0.0.221
Port:          162
User Name:      Inspur
SNMP Version:   v2c
Security Level: noauthnopriv
TagList:       bridge config interface rmon snmp ospf
```

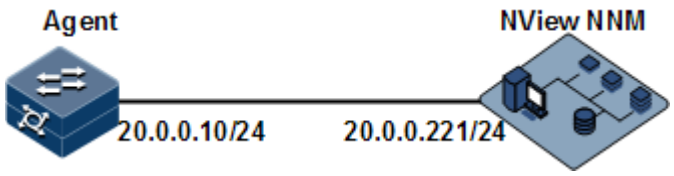
13.1.11 配置 SNMP v3 和 Trap 示例

组网需求

如图 13-4 所示，NView NNM 网管系统与 Agent 之间有可达路由，NView NNM 通过 SNMP v3 对 Agent 进行监控，Agent 出现紧急情况时可以主动向 NView NNM 发送 Trap。

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

图13-4 SNMP v3 和 Trap 组网示意图



配置步骤

步骤 1 配置交换机设备的 IP 地址。

```
Inspur#config
Inspur(config)#interface vlan 1
Inspur(config-vlan1)#ip address 20.0.0.10 255.255.255.0
Inspur(config-vlan1)#exit
```

步骤 2 配置 SNMP v3 访问。

创建访问视图 mib2，包括 1.3.6.1.2.1 下的所有 MIB 变量。

```
Inspur(config)#snmp-server view mib2 1.3.6.1.2.1 1.1.1.1.0.1 included
```

创建用户 guestuser1，采用 md5 鉴别算法，口令为 Inspur。

```
Inspur(config)#snmp-server user guestuser1 authentication md5 Inspur
```

创建 guestgroup 的访问组，安全模式安全模型为 usm，安全等级为鉴别但不加密，可读视图名为 mib2。

```
Inspur(config)#snmp-server access guestgroup read mib2 usm authnopriv
```

配置 guestuser1 用户映射到访问组 guestgroup。

```
Inspur(config)#snmp-server group guestgroup user guestuser1 usm
```

步骤 3 配置 Trap 告警。

```
Inspur(config)#snmp-server enable traps
Inspur(config)#snmp-server host 20.0.0.221 version 3 authnopriv
guestuser1
```

检查结果

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

```
Inspur#show snmp access
Index:          0
Group:          initial
Security Model: usm
Security Level: authnopriv
Context Prefix: --
Context Match:  exact
Read View:      internet
Write View:     internet
Notify View:    internet
```

```
Index:        1
Group:        guestgroup
Security Model: usm
Security Level: authnopriv
Context Prefix: --
Context Match:  exact
Read View:     mib2
Write View:    --
Notify View:   internet

Index:        2
Group:        initialnone
Security Model: usm
Security Level: noauthnopriv
Context Prefix: --
Context Match:  exact
Read View:     system
Write View:    --
Notify View:   internet
…
```

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

```
Inspur#show snmp group
Index    GroupName          UserName           SecModel
------------------------------------------------------------
0       initialnone        none              usm
1       initial            md5priv            usm
2       initial            shapriv            usm
3       initial            md5nopriv          usm
4       initial            shanopriv          usm
5       guestgroup         guestuser1         usm
```

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

```
Inspur#show snmp host
Index:        0
IP family:     IPv4
IP address:    20.0.0.221
Port:          162
User Name:     guestuser1
SNMP Version:   v3
Security Level: authnopriv
TagList:       bridge config interface rmon snmp ospf
```

13.2 RMON

13.2.1 简介

RMON（Remote Network Monitoring，远端网络监控）是 IETF 制定的一种可以通过不同的网络代理 Agent 和网管中心进行网络数据监控的标准。

RMON 基于 SNMP 体系结构实现，包括网管中心和运行在各网络设备上的代理 Agent 两部分。在 SNMP 基础上增加了子网流量、统计、分析能力，可以实现对一个网段乃至整个网络的监控，而 SNMP 只能监控单个设备局部信息，对一个网段的监控非常困难。

RMON 中代理 Agent 一般称为探测程序，RMON Probe（RMON 探测器）能够统计和分析子网的通信性能指标，无论何时发现网络故障，RMON Probe 都能够上报网管中心，并描述不正常情况的捕获信息，网管中心无需对设备进行不停的轮询。RMON 可以比 SNMP 更主动、有效地监测远程设备，网络管理员可以更快地跟踪网络、网段或设备出现的故障。该方法减少了网管中心同代理 Agent 间的数据流量，使简单而有力地管理大型网络成为可能，弥补了 SNMP 在日益扩大的分布式互联中所面临的局限性。

RMON Probe 收集数据的方式：

- 分布式 RMON：利用专用的 RMON Probe 收集数据，网管中心直接从 RMON Probe 获取管理信息并控制网络资源。
- 嵌入式 RMON：将 RMON Agent 直接嵌入网络设备（如交换机）中，使它们成为带 RMON Probe 功能的网络设备。网管中心使用 SNMP 的基本操作与 RMON Agent 交换数据信息，收集网络管理信息。

设备采用嵌入式 RMON。如图 13-5 所示，在设备上实现了 RMON Agent 功能。通过该功能，管理站可以获得与被管网络设备接口相连的网段上的整体流量、错误统计和性能统计等信息，从而实现对一个网段的监控。

图13-5 RMON 应用示意图

RMON MIB 中按照功能分成 9 个组，目前实现了 RMON 的四个功能组：即统计组、历史组、告警组和事件组。

- 统计组：负责收集在一个接口上的统计信息，包括接收到的报文计数和大小分布统计。
- 历史统计组：类似于统计组，但它是在一个指定的检测周期内收集统计信息。
- 告警组：在指定的时间间隔内，监视一个指定的管理信息库（MIB）对象，并且设定上升阈值和下降阈值，若监视对象达到阈值则触发一个事件。
- 事件组：配合告警组使用，当告警触发一个事件时，用来记录相应的事件信息，如发送 Trap 信息，写入日志等操作。

13.2.2 配置准备

场景

当用户需要对某一网段进行监控或流量统计时，可以配置 RMON。

RMON 是一种比 SNMP 更高效的监控手段。用户只需要指定告警阈值，超出该阈值时设备将会主动发送告警信息，而不用去获取变量信息。减少管理设备和被管理设备的通信量，对网络进行简单有效的管理。

前提

设备和网管系统之间链路可达。

13.2.3 RMON 的缺省配置

设备上 RMON 的缺省配置如下。

功能	缺省值
统计组	所有接口统计功能使能
历史统计组	禁止
告警组	无
事件组	无

13.2.4 配置 RMON 统计功能

RMON 统计功能可以设置对接口的统计，包括接口收发报文、过小或过大包、冲突、循环冗余校验和错误数、丢弃报文，接收报文长度、碎片、广播、多播、单播消息等。

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#rmon statistics` *`interface-type interface-list`* `[ owner` *`owner-name`* `]`	使能接口的 RMON 统计功能并配置相关参数。

说明

当使用 **no rmon statistics** *interface-type interface-list* 命令关闭某接口的统计功能时，是指用户不能继续获取该接口的统计数据了，而不是接口不再进行数据统计了。

13.2.5 配置 RMON 历史统计功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**rmon history** *interface-type interface-list* [**shortinterval** *short-period*] [**longinterval** *long-period*] [**buckets** *buckets-number*] [**owner** *owner-name*]	使能接口的 RMON 历史统计功能并配置相关参数。

说明

当使用 **no rmon history** *interface-type interface-list* 命令禁止某接口的历史组统计功能时，不再进行数据收集统计，并且将以前收集的所有历史数据清除。

13.2.6 配置 RMON 告警组

可通过设置 RMON 一个告警组实例（*alarm-id*），监控一个 MIB 变量（*mibvar*）。当被监控数据的值越过定义的阈值时会产生告警事件，再按照告警事件的定义进行记录日志或向网管站发送 Trap 信息。

所监控的 MIB 变量必须是真实存在的，并且数据值类型设置正确。

- 如果在设置时，变量不存在或值类型不正确，则返回错误。
- 在已经设置成功的告警中，如果后期该变量无法被采集，则该告警就被关掉，若想重新监控该变量，必须重新设置。

缺省情况下，触发事件的事件号是 0，表示不会触发事件。如果配置事件号不为 0，但在事件组中没有相应地设置该事件，则当监控变量异常时，不会成功触发事件，一直到该事件建立后才可以成功地触发该事件。

只要事件表中配置了上限或下限其中一个事件，符合条件便会触发相应的告警。如果告警上限和下限所对应事件（*rising-event-id*、*falling-event-id*）在事件表中均没有配置，即使达到了告警条件也不会产生告警。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**rmon alarm** *alarm-id mibvar* [**interval** *period*] { **absolute** | **delta** } **rising-threshold** *rising-value* [*rising-event-id*] **falling-threshold** *falling-value* [*falling-event-id*] [**owner** *owner-name*]	在 RMON 告警组中添加告警实例，并配置相关参数。

13.2.7 配置 RMON 事件组

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**rmon event** *event-id* [**log**] [**trap**] [**description** *string*] [**owner** *owner-name*]	在 RMON 事件组中添加事件，并配置事件的处理方式。

13.2.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show rmon**	查看 RMON 配置信息。
2	Inspur#**show rmon alarms**	查看 RMON 告警组信息。
3	Inspur#**show rmon events**	查看 RMON 事件组信息。
4	Inspur#**show rmon statistics** [*interface-type interface-list*]	查看 RMON 统计组信息。
5	Inspur#**show rmon history** *interface-type interface-list*	查看 RMON 历史统计组信息。
6	Inspur#**show rmon latest statistics** [**long** | **short**] **portlist** *interface-type interface-number*	查看 RMON 最新统计组信息。

13.2.9 维护

用户可以通过以下命令维护 RMON 特性的运行情况和配置情况。

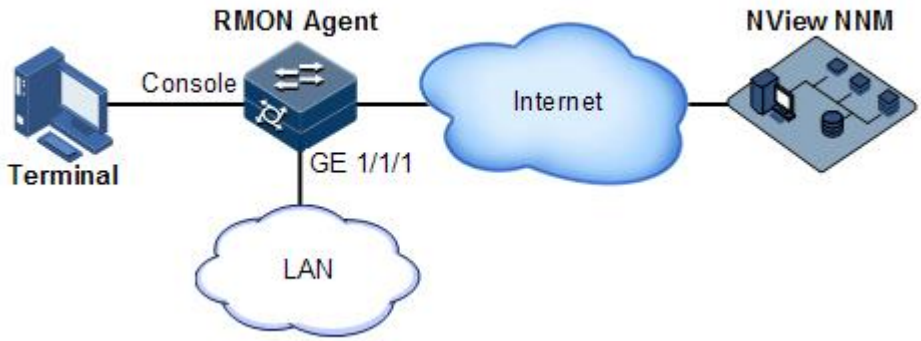
命令	描述
Inspur(config)#**clear rmon**	清除 RMON 的所有配置信息。

13.2.10 配置 RMON 告警组应用示例

组网需求

如图 13-6 所示，交换机设备作为 Agent，通过 Console 口连接配置终端，通过 Internet 连接远端 NNM 系统。使能 RMON 统计功能并对 GE 1/1/1 接口进行性能统计，当接口在一段时间内收到的报文数量超过设置的阈值后，记录日志并发送 Trap 告警。

图13-6 RMON 典型应用组网示意图



配置步骤

步骤 1 创建索引号为 1 的事件，该事件用于记录并发送描述字符串为 High-ifOutErrors 的日志信息，该日志信息的所有者为 **system**。

```
Inspur#config
Inspur(config)#rmon statistics gigaethernet 1/1/1
Inspur(config)#rmon event 1 log description High-ifOutErrors owner system
```

步骤 2 创建索引号为 10 的告警项，该告警项用于监控 MIB 变量 1.3.6.1.2.1.2.2.1.20.1，每 20 秒检查一次，如果该变量的取值增加了 15 以上，便触发 Trap 告警，该告警信息的所有者也为 **system**。

```
Inspur(config)#rmon alarm 10 1.3.6.1.2.1.2.2.1.20.1 interval 20 delta
rising-threshold 15 1 falling-threshold 0 owner system
```

检查结果

通过 **show rmon alarms** 命令查看设备上是否有告警组信息。

```
Inspur#show rmon alarms
Alarm group information:
Alarm 10 is active, owned by system
Monitors 1.3.6.1.2.1.2.2.1.20.1 every 20 seconds
Taking delta samples, last value was 0
Rising threshold is 15, assigned to event 1
Falling threshold is 0, assigned to event 0
```

```
On startup enable rising and falling alarm
```

通过 **show rmon events** 命令查看设备上是否有事件组信息。

```
Inspur#show rmon events
Event group information:
Event 1 is active, owned by system
Event description:  High-ifOutErrors
Event generated at 0:0:0
Register log information when event is fired.
```

当告警事件被触发时，在 NNM 系统的告警管理部分也可以查看相应的记录。

13.3 LLDP

13.3.1 简介

随着网络规模的扩大，网络设备的增多，网络拓扑日趋复杂，对网络的管理变得尤为重要。为了跟踪网络拓扑信息的变化，许多网络管理软件都采用“自动发现”功能来跟踪网络拓扑的变化，但大多数网络管理软件只能分析到网络层拓扑结构，无法确定设备通过哪些接口与其他设备相连。

LLDP（Link Layer Discovery Protocol，链路层发现协议）是由 IEEE 802.1AB 定义的一种链路层发现协议。网络管理系统可以通过该协议快速掌握二层网络的拓扑及其变化情况。

LLDP 将本地设备的信息组织成不同的 TLV（Type Length Value，类型/长度/值单元），并封装在 LLDPDU（Link Layer Discovery Protocol Data Unit，链路层发现协议数据单元）中发送给直连的邻居，同时将邻居发来的信息以标准 MIB（Management Information Base，管理信息库）的形式保存起来，以供网管系统查询及判断链路的通信状况。

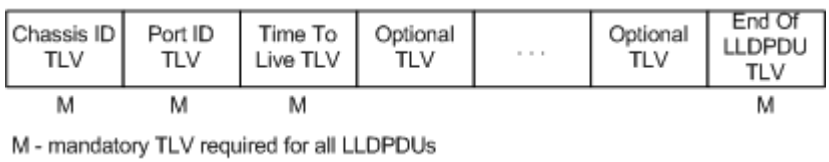
基本概念

LLDP 报文是指在数据单元封装了 LLDPDU 的以太网报文。

LLDPDU 是 LLDP 报文的数据单元。在组成 LLDPDU 之前，设备先将本地信息封装成 TLV，再由若干 TLV 组合成一个 LLDPDU，封装在以太网数据部分进行传送。

如图 13-7 所示，LLDPDU 由若干个 TLV 组合而成，其中包含四个必选的 TLV 和若干个可选的 TLV。

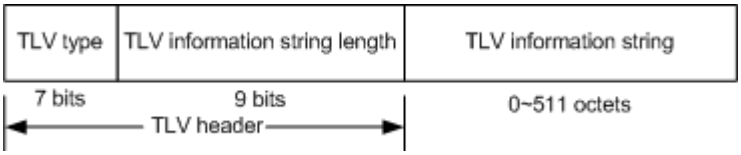
图13-7 LLDPDU 结构图



TLV 是组成 LLDPDU 的单元，表示一个对象的类型、长度和信息的单元。

TLV 的结构如图 13-8 所示，每个 TLV 代表一个本端信息。例如设备 ID，接口 ID 等各自对应 Chassis ID TLV，Port ID TLV 固定的 TLV。

图13-8 基本 TLV 结构图



TLV 类型值对应如表 13-1 所示，目前只用到其中的 0～8 种类型。

表13-1 TLV 类型

TLV 类型	说明	是否必选
0	End Of LLDPDU，表示 LLDP 报文结束	必选
1	Chassis Id，发送设备的 MAC 地址	必选
2	Port Id，LLDP 报文发送端的接口	必选
3	Time To Live，本设备信息在邻居设备上的老化时间	必选
4	Port Description，以太网接口的描述信息	可选
5	System Name，设备名称	可选
6	System Description，系统描述	可选
7	System Capabilities，系统的主要功能以及已使用的功能项	可选
8	Management Address，管理地址	可选

组织定义 TLV 属于可选的 TLV 集合，根据用户的实际需要在 LLDPDU 中发布。目前比较常见的组织定义 TLV 如下。

表13-2 IEEE 802.1 组织定义的 TLV

TLV 类型	TLV 说明
Port VLAN ID TLV	端口的 VLAN 标识符
Port And Protocol VLAN ID TLV	端口的协议 VLAN 标识符
VLAN Name TLV	端口的 VLAN 名称
Protocol Identity TLV	端口支持的协议类型

表13-3 IEEE 802.3 组织定义的 TLV

TLV 类型	TLV 说明
MAC/PHY Configuration//Status TLV	端口的速率双工状态、是否支持并使能自动协商功能
Power Via MDI TLV	端口的供电能力
Link Aggregation TLV	端口的链路聚合能力及当前的聚合状态
Maximum Frame Size TLV	端口所能传输的最大的帧的大小

LLDP 工作原理

LLDP 是一种点对点单向发布协议，通过本机向对端周期性的发送 LLDP 报文（或者本端信息有变化时发送 LLDP 报文），通知对端本机的链路状态。

其数据流如下：

- 发送时，设备从 NMS 获取所选择 TLV 需要的系统信息，以及从 LLDP MIB 中获得配置信息，生成 TLV，组成 LLDPDU，封装成 LLDP 报文发送给对端。
- 对端接收到 LLDP 报文后，对端设备会解析获得的各个 TLV 信息，如果有变更，将信息更新至 LLDP 的邻居 MIB 表中，并通知 NMS。

本端设备信息在邻居节点中老化时间 TTL（Time to live），可通过修改老化系数参数值调整，向邻居节点发送 LLDP 报文，邻居节点收到 LLDP 报文后，调整其邻居节点（即发送端）信息的老化时间。老化时间计算公式，TTL=Min{65535，(interval×hold-multiplier)}，其中：

- interval 表示设备向邻居节点发送 LLDP 报文的时间周期。
- hold-multiplier 表示设备信息在邻居节点的老化系数。

13.3.2 配置准备

场景

当用户通过 NView NNM 系统获取设备之间的连接信息，进行拓扑发现时，需要在设备之间使能 LLDP 功能，向邻居互相通告自己的信息，以及存储邻居信息，方便 NView NNM 系统查询。

前提

无

13.3.3 LLDP 的缺省配置

设备上 LLDP 的缺省配置如下。

功能	缺省值
LLDP 全局使能或禁止	禁止
接口 LLDP 功能状态	使能
延迟发送定时器	2s
周期发送定时器	30s
老化系数	4
重启定时器	2s
告警使能或禁止	使能
告警通知定时器	5s
LLDP 报文目的 MAC 地址	0180.c200.000e

13.3.4 使能全局 LLDP 功能

注意

禁止全局 LLDP 功能后，不能立即再使能，必须等重启定时器超时后才能再次使能。

通过 NView NNM 系统获取设备之间的连接信息，进行拓扑发现时，需要在设备之间使能 LLDP 功能，向邻居互相通告自己的信息，以及存储邻居信息，方便 NView NNM 系统查询。

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#lldp enable`	配置使能全局 LLDP 功能。

13.3.5 使能接口 LLDP 功能

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#interface` *interface-type interface-number*	进入物理层接口配置模式。

步骤	配置	说明
3	Inspur(config-gigaethernet1/1/*)#**lldp enable**	使能接口 LLDP 功能。

13.3.6 配置 LLDP 基本功能

注意

配置延时发送定时器和周期发送定时器时，延时发送定时器的取值要小于或等于周期发送定时器取值的四分之一。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**lldp message-transmission interval** *period*	（可选）配置 LLDP 报文的周期发送定时器。
3	Inspur(config)#**lldp message-transmission delay** *period*	（可选）配置 LLDP 报文的延迟发送定时器。
4	Inspur(config)#**lldp message-transmission hold-multiplier** *hold-multiplier*	（可选）配置 LLDP 报文老化系数。
5	Inspur(config)#**lldp restart-delay** *period*	（可选）配置重启定时器。即设备禁止全局 LLDP 功能后，需要等待重启定时器设定的时间后才能重新使能全局 LLDP 功能。

13.3.7 配置 LLDP 告警功能

当网络自身发生变化时，需要使能 LLDP 告警通知功能，及时向 NView NNM 系统发送拓扑信息更新告警。

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**lldp trap-interval** *period*	（可选）配置 LLDP 告警 Trap 周期发送定时器。

13.3.8 配置 TLV

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	Inspur(config-gigaethernet1/1/*)#**lldp tlv-select basic-tlv** { **all** | **port-description** | **system-capability** | **system-name** | **system-description** }	配置允许发布的基本 TLV。
4	Inspur(config-gigaethernet1/1/*)#**lldp tlv-select med-tlv** { **all** | **capability** | **inventory** | **network-policy**| **location-id** { **civic-address** *device-type country-code civic-address-type ca-value* | **elin-address** *tel-number* } }	配置允许发布的 MED TLV。
5	Inspur(config-gigaethernet1/1/*)#**lldp tlv-select dot1-tlv** { **all** | **port-vlan-id** | **vlan-name** [*vlan-id*] }	使能允许发布的 802.1 TLV 类型
6	Inspur(config-gigaethernet1/1/*)#**lldp tlv-select dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** }	使能允许发布的 802.3 TLV 类型

13.3.9 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show lldp local config**	查看 LLDP 本地配置信息。
2	Inspur#**show lldp local system-data** [*interface-type interface-number*]	查看 LLDP 本地系统信息。
3	Inspur#**show lldp remote** [*interface-type interface-number*] [**detail**]	查看 LLDP 邻居信息。
4	Inspur#**show lldp statistic** [*interface-type interface-number*]	查看 LLDP 报文统计信息。
5	Inspur#**show lldp tlv-select** [*interface-type interface-number*]	查看端口发送的可选 TLV 信息。

13.3.10 维护

用户可以通过以下命令维护 LLDP 特性。

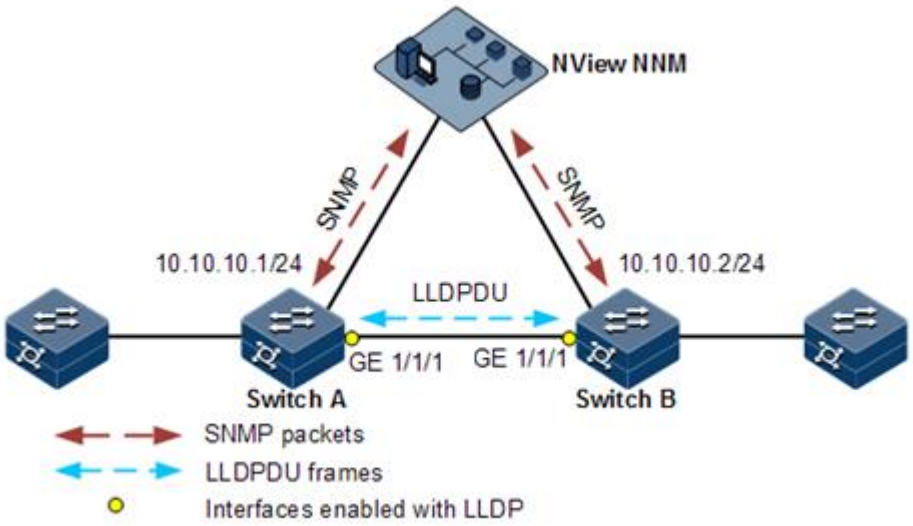
命令	说明
Inspur(config)#**clear lldp statistic** *interface-type interface-number*	清除 LLDP 统计信息。
Inspur(config)#**clear lldp remote-table** [*interface-type interface-number*]	清除 LLDP 邻居信息。
Inspur(config)#**clear lldp global statistic**	清除 LLDP 全局统计信息。

13.3.11 配置 LLDP 基本功能示例

组网需求

如图 13-9 所示，交换机和 NView NNM 系统相连，在 Switch A 和 Switch B 之间使能 LLDP 协议，则两设备之间二层链路的变化情况，可以通过 NView NNM 系统查询。如果邻居老化、新增邻居、邻居信息变化时会向 NView NNM 系统上报 LLDP 告警。

图13-9 配置 LLDP 基本功能组网示意图



配置步骤

步骤 1 配置全局使能 LLDP 并使能 LLDP 告警。

配置 Switch A。

Inspur#**hostname SwitchA**

```
SwitchA#config
SwitchA(config)#lldp enable
```

配置 Switch B。

```
Inspur#hostname SwitchB
SwitchB#config
SwitchB(config)#lldp enable
```

步骤 2 配置管理 IP 地址。

配置 Switch A。

```
SwitchA(config)#create vlan 1024 active
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport access vlan 1024
SwitchA(config-gigaethernet1/1/1)#exit
SwitchA(config)#interface vlan 1024
SwitchA(config-vlan1)#ip address 10.10.10.1 255.255.255.0
SwitchA(config-vlan1)#exit
```

配置 Switch B。

```
SwitchB(config)#create vlan 1024 active
SwitchB(config)#interface gigaethernet 1/1/1
SwitchB(config-gigaethernet1/1/1)#switchport access vlan 1024
SwitchB(config)#interface vlan 1024
SwitchB(config-vlan1)#ip address 10.10.10.2 255.255.255.0
SwitchB(config-vlan1)#exit
```

步骤 3 配置 LLDP 属性。

配置 Switch A。

```
SwitchA(config)#lldp message-transmission interval 60
SwitchA(config)#lldp message-transmission delay 9
SwitchA(config)#lldp trap-interval 10
```

配置 Switch B。

```
SwitchB(config)#lldp message-transmission interval 60
SwitchB(config)#lldp message-transmission delay 9
SwitchB(config)#lldp trap-interval 10
```

检查结果

通过 **show lldp local config** 命令查看本地配置是否正确。

```
SwitchA#show lldp local config
System configuration:
------------------------------------------------------------------
LLDP enable status:               enable (default is disabled)
LldpMsgTxInterval:                60     (default is 30s)
LldpMsgTxHoldMultiplier:           4      (default is 4)
LldpReinitDelay:                  2      (default is 2s)
LldpTxDelay:                      9      (default is 2s)
LldpNotificationInterval:          10     (default is 5s)
LldpNotificationEnable:           enable (default is enabled)
```

```
------------------------------------------------------------------
Port            Status        Packet destination-mac
------------------------------------------------------------
GE1/1/1          enable        0180.C200.010e
GE1/1/2          enable        0180.C200.010e
GE1/1/3          enable        0180.C200.010e
GE1/1/4          enable        0180.C200.010e
GE1/1/5          enable        0180.C200.010e
GE1/1/6          enable        0180.C200.010e
……
SwitchB#show lldp local config
System configuration:
------------------------------------------------------------------
LLDP enable status:               enable (default is disabled)
LldpMsgTxInterval:                60     (default is 30s)
LldpMsgTxHoldMultiplier:           4      (default is 4)
LldpReinitDelay:                  2      (default is 2s)
LldpTxDelay:                      9      (default is 2s)
LldpNotificationInterval:          10     (default is 5s)
LldpNotificationEnable:           enable (default is enabled)
------------------------------------------------------------------
Port            Status        Packet destination-mac
------------------------------------------------------------
GE1/1/1          enable        0180.C200.000E
GE1/1/2          enable        0180.C200.000E
GE1/1/3          enable        0180.C200.000E
GE1/1/4          enable        0180.C200.000E
GE1/1/5          enable        0180.C200.000E
GE1/1/6          enable        0180.C200.000E
……
```

通过 **show lldp remote** 命令查看邻居信息是否建立。

```
SwitchA#show lldp remote
Port   ChassisId          PortId        SysName   MgtAddress     ExpiredTime
------------------------------------------------------------------------------
gigaethernet1/1/1  000E.5E02.B010    gigaethernet1/1/1        SwitchB
10.10.10.2    106
……
SwitchB#show lldp remote
Port           ChassisId     PortId    SysName   MgtAddress     ExpiredTime
------------------------------------------------------------------------------
gigaethernet1/1/1  000E.5E12.F120 gigaethernet1/1/1   SwitchA
 10.10.10.1 106
……
```

13.4 光模块数字诊断

13.4.1 简介

设备上光模块数字诊断支持对 SFP（Small Form-factor Pluggables，小型封装可插拔）光模块的诊断。

光模块数字诊断功能为系统提供一种性能监测手段，网络管理员通过分析该模块提供的监测数据，可以预测收发模块的寿命、隔离系统故障并在现场安装中验证模块的兼容性。

光模块数字诊断功能监控光模块的性能参数包括：

- 模块温度
- 内部供电电压
- 发送偏置电流
- 发送光功率
- 接收光功率

当性能参数达到了告警阈值或状态信息发生变化，会产生相应的 Trap 告警信息。

13.4.2 配置准备

场景

光模块故障诊断功能为用户提供一种对 SFP 光模块性能参数的检测手段，用户通过分析光模块的监测数据，可以预测其寿命、隔离系统故障并在现场安装中验证光模块的兼容性。

前提

无

13.4.3 光模块数字诊断的缺省配置

设备上光模块数字诊断的缺省配置如下。

功能	缺省值
全局光模块数字诊断功能状态	禁止
接口光模块数字诊断功能状态	使能
全局光模块数字诊断告警发送 Trap 功能	禁止
接口光模块数字诊断告警发送 Trap 功能	禁止
接口光模块数字诊断密码校验功能状态	禁止

13.4.4 配置使能光模块数字诊断

请在设备上进行以下配置。

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**transceiver ddm enable**	全局使能光模块数字诊断。
3	Inspur(config)#**transceiver ddm poll-interval** *interval*	配置光模块数字诊断轮询间隔时间
4	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
5	Inspur(config-gigaethernet1/1/*)#**transceiver ddm enable**	使能接口光模块数字诊断。 只有全局光模块数字诊断使能情况下，接口光模块数字诊断使能的光模块，才能进行数字诊断。

13.4.5 配置光模块数字诊断告警发送 Trap

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**snmp-server trap transceiver enable**	全局使能光模块数字诊断告警发送 Trap。
3	Inspur(config)#**interface** *interface-type interface-number*	进入物理层接口配置模式。
4	Inspur(config-gigaethernet1/1/*)#**transceiver trap enable**	使能接口光模块数字诊断告警发送 Trap。 只有全局光模块数字诊断告警发送 Trap 使能情况下，接口光模块数字诊断告警发送 Trap 使能的光模块，才能在产生告警时发送 Trap。

13.4.6 检查配置

配置完成后，请在设备上进行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show transceiver**	查看光模块数字诊断全局开关状态和接口开关状态信息。
2	Inspur#**show transceiver ddm** *interface-type interface-list* [**detail**]	查看光模块数字诊断性能参数。
3	Inspur#**show transceiver** *interface-type interface-list* **history** [**15m** | **24h**]	查看光模块数字诊断的历史信息。

序号	检查项	说明
4	Inspur#**show transceiver information** *interface-type interface-list*	查看光模块基本信息。
5	Inspur#**show transceiver threshold-violations** *interface-type interface-list*	查看光模块参数上次超过阈值的信息。

13.5 系统日志

13.5.1 简介

系统日志功能是指设备将系统信息和调试信息等内容以日志的形式记录并输出到指定的目的地，在设备发生故障时，方便用户查看和定位故障。

设备的系统消息和一些调试输出会被送至系统日志处理。系统日志根据用户的配置将信息送往不同的目的地，接收系统日志的目的地有以下几类。

- Console 控制台：将日志信息通过 Console 接口输出到本地控制台。
- Host 日志主机：将日志信息以日志文件形式输出到日志主机。
- Monitor 监控台：将日志信息输出到监控台，如 Telnet 终端。
- File 日志文件：将日志信息以日志文件形式输出到设备的 Flash 中。
- Buffer 缓冲区：将日志信息输出到缓冲区中。
- SNMP 服务器：将日志信息转化为 Trap 输出到 SNMP 服务器。

系统日志信息级别，根据严重程度分为 8 个等级，如表 13-4 所示。

表13-4 信息级别

严重等级	级别	说明
emergencies	0	系统不可以使用
alerts	1	需要立即处理
critical	2	严重状态
errors	3	错误状态
warnings	4	警告状态
notifications	5	正常但是很重要的状态
informational	6	通告事件
debugging	7	调试信息

说明

输出信息的严重等级是可手动设置的。根据配置的严重等级输出信息时，仅输出级别小于或等于所配置的严重等级的信息。比如，配置输出级别指定为 3（也可直接指定严重等级 errors）的信息输出，则级别为 0～3 的信息，即严重等级为 emergencies～errors 的信息均可以输出。

13.5.2 配置准备

场景

设备会将系统的登录成功失败、关键信息、调试信息、错误信息等生成系统日志，输出为日志文件或传送到日志主机、Console 接口或监控台，以便用户查看并定位故障。

前提

无

13.5.3 系统日志的缺省配置

设备上系统日志的缺省配置如下。

功能	缺省值
系统日志功能状态	使能
日志消息输出到 console 控制台功能	使能，缺省级别为 information（6）
日志信息输出到 host 日志主机功能	无，缺省级别为 information（6）
日志信息输出到 file 文件功能	禁止，固定级别为 debugging(7)
日志输出到 monitor 监控台功能	禁止，缺省级别为 information（6）
日志输出到 buffer 缓冲区功能	禁止，缺省级别为 information（6）
日志 Debug 级别	**low**
日志输出到历史表功能	禁止
日志历史表大小	1
日志转化为 Trap 功能	禁止，缺省级别为 warning（4）
日志缓冲区大小	4kB
系统日志发送速率	不限制

功能	缺省值
系统日志信息的时间戳	• debug：对 debug 级别(7 级)的 Syslog 信息没有时间戳 • log：对 0-6 级别的 Syslog 信息时间戳为绝对时间

13.5.4 配置系统日志基本信息

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**logging on**	（可选）配置使能系统日志功能。
3	Inspur(config)#**logging time-stamp** { **debug** | **log** } { **datetime** | **none** | **uptime** }	（可选）配置系统日志的时间戳。 可选参数 **debug** 用于指定 debug 级别（7 级）的系统日志时间戳，缺省情况下该类系统日志没有时间戳； 可选参数 **log** 用于指定 0～6 级的系统日志时间戳，缺省情况下该类系统日志采用 **date-time** 作为时间戳。
4	Inspur(config)#**logging rate-limit** *log-num*	（可选）配置系统日志的发送速率。
5	Inspur(config)#**logging sequence-number**	（可选）配置系统日志的系列号。 序列号仅对日志输出到控制台、监控台、日志文件、日志缓冲区有意义，对日志主机和历史表无意义。
6	Inspur(config)#**logging discriminator** *discriminator-number* { **facility** | **mnemonics** | **msg-body** } { { **drops** | **includes** } *key* | **none** }	（可选）创建并配置系统日志的过滤器。 过滤器可以配置成功后，可以配合日志输出方向（控制台、监控台、日志文件、日志缓冲区）对日志信息进行过滤输出。
7	Inspur(config)#**logging buginf** [**high** | **normal** | **low** | **none**]	（可选）配置发送 Debug 级别日志。

13.5.5 配置系统日志输出

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。

步骤	配置	说明
2	Inspur(config)#**logging console** [*log-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings** | **discriminator** *discriminator-number*]	（可选）配置系统日志输出方向为 Console 控制台。
3	Inspur(config)#**logging host** { *ip-address* | *ipv6-address* } [*log-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings** | **discriminator** *discriminator-number*]	（可选）配置系统日志输出方向为日志主机。 最多可配置 10 个日志主机。
	Inspur(config)#**logging** [**host** { *ip-address* | *ipv6-address* }] **facility** { **alert** | **audit** | **auth** | **clock** | **cron** | **daemon** | **ftp** | **kern** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **lpr** | **mail** | **news** | **ntp** | **security** | **syslog** | **user** | **uucp** }	（可选）配置发送到日志主机的日志信息的 facility 字段。 前提条件是系统创建了日志主机，否则配置失败。 此配置适用于设备上配置的所有日志主机。
4	Inspur(config)#**logging monitor** [*log-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings** | **discriminator** *discriminator-number*]	（可选）配置系统日志输出方向为监控台。
5	Inspur(config)#**logging file** [**discriminator** *discriminateor-number*]	（可选）配置系统日志输出方向为设备的 Flash。 严重级别固定为 warning（4），不允许配置。
6	Inspur(config)#**logging buffered** [*log-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings** | **discriminator** *discriminator-number*]	（可选）配置系统日志输出方向为缓冲区。
	Inspur(config)#**logging buffered size** *size*	（可选）配置系统日志缓冲区的大小。
7	Inspur(config)#**logging history**	（可选）配置系统日志输出到日志历史表。 输出信息级别采用转化为 Trap 的级别。
	Inspur(config)#**logging history size** *size*	（可选）配置日志历史表的大小。
	Inspur(config)#**logging trap** [*log-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings** | **discriminator** *discriminator-number*]	（可选）配置使能将历史表中的一定级别的日志转化为 Trap。 前提条件是系统日志输出到日志历史表中功能使能，否则没有系统日志转化为 Trap。

13.5.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show logging**	查看系统日志配置的相关信息。
2	Inspur#**show logging buffer**	查看系统日志缓冲区信息。
3	Inspur#**show logging discriminator**	查看过滤器信息。
4	Inspur#**show logging file**	查看系统日志文件内容，。
5	Inspur#**show logging history**	查看系统日志历史表信息。

13.5.7 维护

用户可以通过以下命令，维护系统日志特性的运行情况和配置情况。

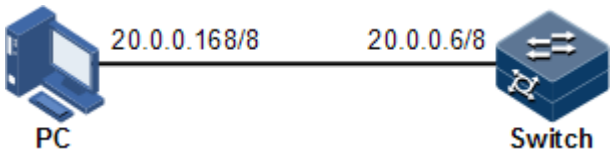
命令	描述
Inspur(config)#**clear logging buffer**	清除缓冲区中的日志信息。
Inspur(config)#**clear logging statistics**	清除日志的统计信息。

13.5.8 配置系统日志输出到日志主机示例

组网需求

如图 13-10 所示，配置系统日志功能，将设备上的日志信息输出到日志主机，以便用户随时查看。

图13-10 系统日志输出到日志主机组网示意图



配置步骤

步骤 1 配置设备的 IP 地址。

```
Inspur#config
Inspur(config)#interface vlan 1
Inspur(config-vlan1)#ip address 20.0.0.6 255.0.0.0
```

```
Inspur(config-vlan1)#exit
```

步骤 2 配置系统日志输出到日志主机 PC 上。

```
Inspur(config)#logging on
Inspur(config)#logging time-stamp log datetime
Inspur(config)#logging rate-limit 2
Inspur(config)#logging host 20.0.0.168 warnings
```

检查结果

通过 **show logging** 命令查看系统日志配置是否正确。

```
Inspur#show logging
Syslog logging:         enable
Dropped Log messages:    0
Dropped debug messages:  0
Rate-limited:           2 messages per second
Squence number display:  disable
Debug level time stamp:  none
Log level time stamp:    datetime
Log buffer size:        4kB
Debug level:            low
Syslog history logging:  disable
Syslog history table size:1
Dest     Status   Level           LoggedMsgs  DroppedMsgs  Discriminator
-------------------------------------------------------------------------
---
buffer   enable   informational(6)  10         0           0
console  enable   informational(6)  10         0           0
trap     disable  warnings(4)      0          0           0
file     enable   debugging(7)     17         0           0
Log host information:
Max number of log server:    10
Current log server number:   1
Target Address     Level           Facility      Sent     Drop
Discriminator
-------------------------------------------------------------------------
--------------
20.0.0.168        warnings(4)      local7       0        0        0
```

13.6 配置告警管理

13.6.1 配置准备

场景

设备发生故障时，由告警管理模块来收集设备故障信息，以日志等形式输出告警的发生时间、告警的名称和描述信息等，帮助用户快速进行问题定位。

如果设备上配置网管系统，告警信息可以直接上报网管系统，给出告警产生的可能原因和处理建议，帮助用户及时处理故障。

如果设备上配置了硬件监控功能。当设备运行环境出现异常时，会记录硬件监控告警表、产生 Syslog 系统日志或发送 Trap 等告警信息，通知用户进行相应处理，防止故障发生。

告警管理方便用户直接在设备上进行告警抑制，告警自动上报，告警监控，告警反转，告警延迟，告警存储模式，清除告警，查看告警等配置。

前提

如果设备上需要配置硬件监控功能时：

- 以 Syslog 方式输出时，告警信息会生成系统日志。当需要把告警信息发送到系统日志主机时，设备上需要配置系统日志主机的 IP 地址等信息。
- 需要把告警信息以 Trap 方式发送到网管中心时，设备上需要配置网管中心的 IP 地址等信息。

13.6.2 配置告警基本功能

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**alarm inhibit** { **enable** | **disable** }	（可选）使能告警抑制，使用 disable 格式禁用该功能。 缺省情况下，设备已经使能告警抑制功能。
3	Inspur(config)#**alarm auto-report all enable**	（可选）使能所有告警自动上报功能。
	Inspur(config)#**alarm auto-report** *alarm-restype alarm-restype-value* **enable**	（可选）使能指定告警源的告警自动上报功能
	Inspur(config)#**alarm auto-report type** *alarm-type* **enable**	（可选）使能指定告警类型的告警自动上报功能
	Inspur(config)#**alarm auto-report type** *alarm-type alarm-restype alarm-restype-value* **enable**	（可选）使能指定告警源和指定告警类型的告警自动上报功能。
4	Inspur(config)#**alarm monitor all enable**	（可选）使能告警监控。
	Inspur(config)#**alarm monitor** *alarm-restype alarm-restype-value* **enable**	（可选）使能指定告警源的告警监控功能。
	Inspur(config)#**alarm monitor type** *alarm-type* **enable**	（可选）使能指定告警类型的告警监控功能。
	Inspur(config)#**alarm monitor type** *alarm-type alarm-restype alarm-restype-value* **enable**	（可选）使能指定告警源和指定告警类型的告警监控功能

步骤	配置	说明
5	Inspur(config)#**alarm monitor-level** { **critical** | **major** | **minor** | **warning** }	（可选）配置告警监控的级别。
6	Inspur(config)#**alarm inverse** *interface-type interface-number* { **none** | **auto** | **manual** }	（可选）配置告警反转模式。 缺省情况下，设备采用 **none** 模式，即不反转模式。
7	Inspur(config)#**alarm** { **active** | **clear** } **delay** *second*	（可选）配置告警延时。 缺省情况下，设备的告警延时是 0 秒。
8	Inspur(config)#**alarm active storage-mode** { **loop** | **stop** }	（可选）配置告警存储模式。 缺省情况下，设备采用 **stop** 模式，即停止模式。
9	Inspur(config)#**alarm clear all**	（可选）清除所有当前告警
	Inspur(config)#**alarm clear index** *index-value*	（可选）清除指定告警索引的当前告警
	Inspur(config)#**alarm clear** *alarm-restype alarm-restype-value*	（可选）清除指定告警源的当前告警。
	Inspur(config)#**alarm clear type** *alarm-type*	（可选）清除指定告警类型的当前告警。
	Inspur(config)#**alarm clear type** *alarm-type alarm-restype alarm-restype-value*	（可选）清除指定告警类型和告警源的当前告警
10	Inspur(config)#**alarm syslog enable**	（可选）使能告警向系统日志输出。 缺省情况下，设备未使能告警向系统日志输出。
11	Inspur(config)#**alarm correlation-Inhibit** { **enable** | **disable** }	（可选）使能相关性告警抑制功能，使用 **disable** 格式禁用该功能。

说明

支持告警模块的功能均可采用配置使能或禁用针对本模块的告警监控、告警自动上报、告警清除功能。

13.6.3 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show alarm management** [*alarm_type*]	查看当前告警参数配置信息。 使用本命令可查看的告警参数信息包含告警抑制、告警反转模式、告警延迟、告警存储模式，告警缓冲区可存储告警的最大条数，以及告警日志可存储告警的最大条数。
2	Inspur#**show alarm log**	查看告警管理模块的配置信息。
3	Inspur#**show alarm management statistics**	查看告警管理模块的统计信息。
4	Inspur#**show alarm active**	查看当前告警表信息。

13.7 硬件环境监控

13.7.1 简介

硬件环境监控主要是对设备的运行环境进行监控，监控的告警事件包括：

- 电源状态告警；
- 温度超出阈值告警；
- 电压超出阈值告警；
- 接口状态异常告警；
- Flash 监控告警。

当产生告警时，有多种方式通知用户，告警事件输出方式如下：

- 记录设备硬件环境监控告警缓冲区；
- 输出 Syslog 系统日志；
- 向网管中心发送 Trap；

用户获知告警事件发生后可以采取相应的措施，预防故障的发生。

告警事件

- 电源监控告警

电源状态告警具体有 2 种：

- 电源电压异常告警

电源电压值超过预定电压值 12V 的 20%或低于预定电压值 12V 的 20%时产生告警，反之电压值恢复正常时也会产生告警，支持记录硬件监控告警表、Trap、Syslog 和继电器输出方式。

- 电源状态改变告警

电源状态改变指电源在位转变成电源不在位，或电源不在位转变为电源在位。设备支持双电源，所以电源状态改变告警区分为双电源中的一个电源状态改变和设备掉电两种告警事件。

- 双电源中的一个电源状态改变，告警事件通知用户是电源 1 还是电源 2 状态改变，支持记录硬件环境监控告警表、Trap、Syslog 和继电器输出方式。
- 设备掉电，表示双电源都掉电，即双电源都转变为不在位状态，支持记录硬件环境监控告警表、Trap、Syslog 和继电器输出方式。

- 温度超出阈值告警

设备支持温度超出阈值告警事件，当设备当前温度低于低温阈值时，产生低温告警事件，支持记录硬件环境监控告警表、Trap、Syslog 和继电器输出方式。

当设备当前温度高于高温阈值时产生高温告警事件，其输出方式和低温告警一样。

- 电压超出阈值告警

设备支持检测电压超出阈值告警事件，当监控的当前电压值低于低压阈值时，产生低压告警事件，支持记录硬件环境监控告警表、Trap、Syslog 和继电器输出方式。

当监控电压的当前电压值高于高压阈值时产生高压告警事件，其输出方式和低压告警一样。

说明

系统只监测 3.3V 主芯片电压。

- 接口状态告警

每个接口有两种告警事件：

- 接口 link-fault 告警：链路故障告警，表示对端链路信号丢失。该告警事件只针对光口，电口没有该功能。
- 接口 link-down 告警：接口状态 Down 告警。

接口的两种告警事件均支持记录硬件环境监控告警表、Trap、Syslog 和继电器输出方式。

告警输出方式

硬件环境监控告警的输出方式：

- 硬件环境监控告警缓冲区输出，即记录到硬件环境监控告警表
  - 硬件环境监控当前告警表，记录设备当前未被清除的或未恢复的告警信息。
  - 硬件环境监控历史告警表，记录当前的、已恢复的和已手动清除的告警信息。

硬件环境监控告警信息会自动记录在硬件环境监控当前告警表和硬件环境监控历史告警表，不用手动设置。

- Trap 输出

告警信息以发送 Trap 方式输出到网管中心。

Trap 输出有全局的开关，在监控的各种告警事件下也存在各自的 Trap 告警输出开关，当全局开关和监控的告警事件下的开关同时使能时，告警才能产生 Trap 输出。

Trap 信息的内容如表 13-5 所示。

表13-5 Trap 信息内容说明

字段	说明
告警状态	• asserted（当前正在发生告警） • cleared（告警恢复） • clearall（清除所有的告警信息）
告警源	• device（全局告警） • 接口号（接口状态告警）
时间戳	告警产生的时间，以绝对时间的形式表示
告警事件类型	• dev-power-down（设备掉电告警） • power-abnormal（电源异常告警，双电源中的一个电源掉电） • high-temperature（高温告警） • low-temperature（低温告警） • high-volt（高压告警） • low-volt（低压告警） • link-down（接口 LinkDown 告警） • link-falut（接口 LinkFault 告警） • all-alarm（清除所有告警信息）

- Syslog 系统日志输出

告警信息记录到 Syslog 系统日志。

Syslog 方式输出时有全局的开关，在监控的各种告警事件下也存在各自的 Syslog 告警输出开关。当全局开关和监控的告警事件下的开关同时使能时，告警才能产生 Syslog 输出。

Syslog 系统日志内容如表 13-6 所示。

表13-6 Syslog 信息内容说明

字段	说明
Facility	产生告警的模块名，硬件环境监控模块固定是 alarm
Severity	级别，同系统日志定义的级别，参见表 13-4 相关内容
Mnemonics	告警事件类型，具体类型说明，参见表 13-5 相关内容

字段	说明
Msg-body	正文，描述发生的告警事件内容

13.7.2 配置准备

场景

设备硬件环境监控提供设备运行环境监控功能，用户可以配置硬件环境监控功能进行故障监控。当设备运行环境出现异常时，会记录硬件环境监控告警表、产生 Syslog 系统日志或发送 Trap 等告警信息，通知用户进行相应处理，防止故障发生。

前提

硬件环境监控告警输出：

- 以 Syslog 方式输出时，告警信息会生成系统日志。当需要把告警信息发送到系统日志主机时，设备上需要配置系统日志主机的 IP 地址等信息。
- 需要把告警信息以 Trap 方式发送到网管中心时，设备上需要配置网管中心的 IP 地址等信息。

13.7.3 硬件环境监控的缺省配置

设备上硬件环境监控的缺省配置如下。

功能	缺省值
全局硬件环境监控告警 Syslog 输出	禁止
全局硬件环境监控告警 Trap 输出	禁止
电源掉电事件告警	• Trap 输出功能使能 • Syslog 系统日志输出功能使能 • Relay 输出功能使能
温度告警输出	• Trap 输出功能使能 • Syslog 系统日志输出功能使能 • Relay 输出功能使能
电压告警输出	
接口 link-down 事件告警输出	• Trap 输出功能使能 • Syslog 系统日志输出功能使能 • Relay 输出功能禁止
接口 link-fault 事件告警	• Trap 输出功能禁止 • Syslog 系统日志输出功能禁止 • Relay 输出功能禁止

功能	缺省值
高温告警阈值	90ºC
低温告警阈值	-10ºC
高电压阈值	3450mV
低电压阈值	3150mV

13.7.4 配置使能全局硬件环境监控

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**logging alarm**	（可选）使能全局硬件环境监控告警 Syslog 输出。
3	Inspur(config)#**snmp-server alarm-trap enable**	（可选）使能全局硬件环境监控告警发送 Trap。

说明

- 当全局硬件环境监控告警 Syslog 输出使能，监控的告警事件下以 Syslog 方式输出同时使能时，告警事件才能产生 Syslog。
- 当全局硬件环境监控告警发送 Trap 使能，监控的告警事件下以 Trap 方式输出同时使能时，告警事件才能发送 Trap。
- 当全局硬件环境监控告警 Relay 输出使能，监控的告警事件下以 Relay 方式输出同时使能时，告警事件才能产生 Relay。

13.7.5 配置温度监控告警

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**alarm temperature** { **high** *high-value* | **low** *low-value* | **notifies** | **syslog** }	使能温度告警输出，并配置温度告警输出方式，或温度告警阈值。 • 高温阈值 high-value 必须高于低温阈值 low-value； • 低温阈值 low-value 必须低于高温阈值 high-value。

13.7.6 配置电压监控告警

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**alarm voltage** { **high** *high-value* | **low** *low-value* | **notifies** | **syslog** }	使能电压告警输出，并配置电压告警输出方式，或电压告警阈值。 **说明** 设备只监控 3.3V 主芯片电压。
3	Inspur(config)#**alarm power-supply** { **notifies** | **syslog** }	使能电源告警功能，并配置告警输出方式。

13.7.7 手动清除全部硬件环境监控告警事件

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**clear alarm**	配置手动清除告警。 **说明** • 执行该命令，可清除当前告警表中所有告警信息，并在历史告警表中生成一条告警类型是 all-alarm 的告警信息。 • 如果告警全局发送 Trap 使能，则该条 all-alarm 告警信息会以 Trap 方式输出；如果全局 Syslog 使能，则该条 all-alarm 告警信息会以 Syslog 方式输出。如果全局 Relay 使能，则该条 all-alarm 告警信息会以继电器方式输出。

13.7.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show alarm**	查看全局硬件环境监控告警配置信息。

序号	检查项	说明
2	Inspur#show alarm currrent	查看硬件环境监控当前告警信息。
3	Inspur#show alarm history	查看硬件环境监控历史告警信息。
4	Inspur#show environment [temperature | voltage | power]	查看设备当前的电源、温度、电压告警等当前环境信息。

13.8 CPU 监控

13.8.1 简介

设备支持 CPU 监控功能，可以实时监控系统中各任务的状态、CPU 利用率和堆栈使用情况，帮助网管人员快速定位故障。

CPU 监控可以提供以下功能：

- 查看 CPU 利用率

提供查看各周期（5 秒，1 分钟，10 分钟，2 小时）内各任务的 CPU 占用时间和利用率。可以静态显示，也可以动态显示各周期内 CPU 总的利用率。

提供查看所有任务的运行状态信息和指定任务的详细运行状态信息。

提供查看各周期内 CPU 历史利用率。

提供查看死亡任务信息。

- CPU 利用率门限告警

在指定的采样周期内，系统的 CPU 利用率从低于下限阈值上升到高于上限阈值或者从高于上限阈值下降到低于下限阈值时，会产生告警并发送 Trap，Trap 信息会提供最近某个周期（5 秒，1 分钟，10 分钟）内 CPU 利用率最高的 5 个任务序号及其 CPU 利用率。

13.8.2 配置准备

场景

CPU 监控功能可以实时监控系统中各任务的状态、CPU 利用率和堆栈使用情况，提供 CPU 利用率门限值告警，方便及时发现并消除隐患，或帮助网管人员进行故障定位。

前提

在配置 CPU 监控之前，需完成以下任务：

- 当需要把 CPU 监控告警信息以 Trap 方式输出时，需在设备上配置 Trap 输出目标主机地址，即网管中心的 IP 地址等信息。

13.8.3 CPU 监控的缺省配置

设备上 CPU 监控的缺省配置如下。

功能	缺省值
CPU 利用率告警 Trap 输出	使能
CPU 利用率告警的上限阈值	99%
CPU 利用率告警的恢复阈值	79%
CPU 利用率采样周期	60s

13.8.4 配置 CPU 监控告警

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**cpu threshold recovering** *recovering-threshold-value* **rising** *rising-threshold-value*	（可选）配置 CPU 告警恢复阈值和上限阈值。
3	Inspur(config)#**cpu interval** *interval-value*	（可选）配置 CPU 告警采样时间间隔。

13.8.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

步骤	配置	说明
1	Inspur#**show cpu-utilization** [**dynamic** | **history** { **10min** | **1min** | **2hour** | **5sec** }]	查看 CPU 利用率。
2	Inspur#**show process** [**cpu** | **sorted** { **priority** | **name** } | *taskname*]	查看各任务状态信息。
3	Inspur#**show process cpu** [**sorted** [**10mins** | **1min** | **5secs** | **invoked**]]	查看各任务的 CPU 利用率。
4	Inspur#**show process dead**	查看死亡任务信息。
5	Inspur#**show process pid** *range*	查看指定任务信息。

13.9 电缆诊断

13.9.1 简介

设备支持电缆诊断功能，可以对线路进行检测。

电缆诊断可查询的结果如下：

- 发送线缆的检测结果；
- 发送线缆的错误位置；
- 接收线缆的检测结果；
- 接收线缆的错误位置。

13.9.2 配置准备

场景

使能设备的电缆诊断功能，可及时了解设备电缆线路的运行状态，及早定位并排除设备电缆故障。

前提

无

13.9.3 配置电缆诊断功能

请在需要配置电缆诊断的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**test cable-diagnostics** *interface-type interface-number*	使能接口的电缆诊断功能。
2	Inspur(config)#**test cable-diagnostics noshutdown** { **enable** | **disable** }	使能接口电缆诊断不重启接口的功能，使用 **disable** 格式禁用该功能。

13.9.4 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show cable-diagnostics** [*interface-type interface-number*]	查看接口的电缆诊断信息。

13.10 配置内存监控

13.10.1 配置准备

场景

内存利用率监控功能可以实时监控系统的内存利用率，提供内存利用率阈值告警，方便及时发现并消除隐患，或帮助网管人员进行故障定位。

前提

当用户需要把内存利用率监控告警信息以 Trap 方式输出时，应首先在设备上配置 Trap 输出目标主机地址，即网管中心的 IP 地址等信息。

13.10.2 配置内存监控

请在设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**memory threshold recovering** *recovering-threshold-value* **rising** *rising-threshold-value*	配置内存监控告警上下门限。
3	Inspur(config)#**memory interval** *Observation-interval-value*	配置内存告警采样时间间隔。

13.10.3 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show memory**	查看内存信息。

13.11 风扇监控

13.11.1 简介

设备支持风扇监控功能，可以对风扇的转速和温度进行监控，当设备监控到风扇的转速和温度出现异常时，会产生告警并发送 Trap 信息。

设备对风扇的监控模式有两种：

- 强制监控，即强制设定风扇的转速；
- 自动监控，即风扇根据温度的变化自动调节转速。

在自动监控模式下，设备将风扇的转速分为四个等级，每个等级分别对应一组温度范围，设备会依据环境温度的不同，对风扇转速进行相应的调整。

13.11.2 配置准备

场景

当设备安放于比较炎热的环境时，过高的温度会影响设备的散热性能，此时需要配置风扇监控功能，使设备的风扇能够依据周围的环境温度自动调节，以维护设备的正常运转。

前提

无

13.11.3 配置风扇监控功能

请在需要配置风扇监控功能的设备上进行以下配置。

步骤	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur(config)#**fan-monitor mode { auto | enforce }**	配置设备对风扇转速的监控模式。 缺省情况下，设备对风扇的监控模式为**auto**。
3	Inspur(config)#**fan-monitor enforce level** *level*	（可选）配置强制监控模式下的风扇转速。
4	Inspur(config)#**fan-monitor trap send enable**	（可选）使能风扇监控告警发送 Trap 功能。

13.11.4 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur#**show fan-monitor information**	查看风扇监控配置的相关信息是否正确。
2	Inspur#**show fan-monitor status**	查看当前的风扇状态信息是否正常。

13.12 性能统计

13.12.1 简介

性能统计用于监测设备的接口，对服务报文进行统计，使用户了解网络性能。性能统计功能提供基于接口或业务流两类测量点的短周期或长周期统计。短周期统计周期为 15 分钟，长周期统计周期为 24 小时。一个统计周期内统计的数据，以数据块的形式按照写入周期，保存到 Flash 存储器中，方便用户查看。

- 基于接口的性能统计：
  - 接口的短/长周期性能统计：包括业务口和管理口的短/长周期性能统计。
  - 接口的短/长周期性能统计数据存储：包括业务口和管理口的短/长周期性能统计数据，按配置的写入周期保存于 Flash 中。
- 基于业务流的性能统计：
  - 业务流的短/长周期性能统计：包括服务 VLAN 或优先级的短/长周期性能统计。
  - 业务流的短/长周期性能统计数据存储：包括服务 VLAN 或优先级的短/长周期性能统计数据，按配置的写入周期保存于 Flash 中。

13.12.2 配置准备

场景

用户需要了解设备性能时，使用性能统计功能，可以实现对接口或业务流进行报文统计，向用户提供对报文的历史和当前统计信息。

前提

无

13.12.3 性能统计的缺省配置

功能	缺省值
性能统计功能	使能
存储的数据块个数	16

13.12.4 配置性能统计

步骤	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur(config)#performance statistics interval buckets` *buckets-number*	配置统计 Flash 文件中存储的数据块个数。

步骤	配置	说明
3	Inspur(config)#**interface** *interface-type interface-number* Inspur(config-gigaethernet1/1/*)#**performance statistics** [**vlan** *vlan-id* [**cos** *statistics-cos*]] { **enable** | **disable** }	接口配置模式下使能性能统计功能，使用 **disable** 格式禁止该功能。

说明

进行性能统计的时间与命令配置的时间无关，与系统时间相关。性能统计功能以 15 分钟作为一个周期，完成一次统计。例如：在进行首次统计时，若在第 5 分钟使能性能统计功能，则在 15 分钟开始统计，30 分钟完成本次统计。

13.12.5 检查配置

序号	检查项	说明
1	Inspur#**show performance statistics interval buckets** Inspur#**show performance statistics interface** *interface-type interface-number* { **current** | **history** } Inspur#**show interface** *interface-type interface-number* **vlan** *vlan-id* [**cos** *cos-value*] { **current** | **history** }	查看性能统计信息。

13.12.6 维护

命令	说明
Inspur(config)#**clear performance statistics histroy**	清除性能统计信息。

13.13 Ping

13.13.1 简介

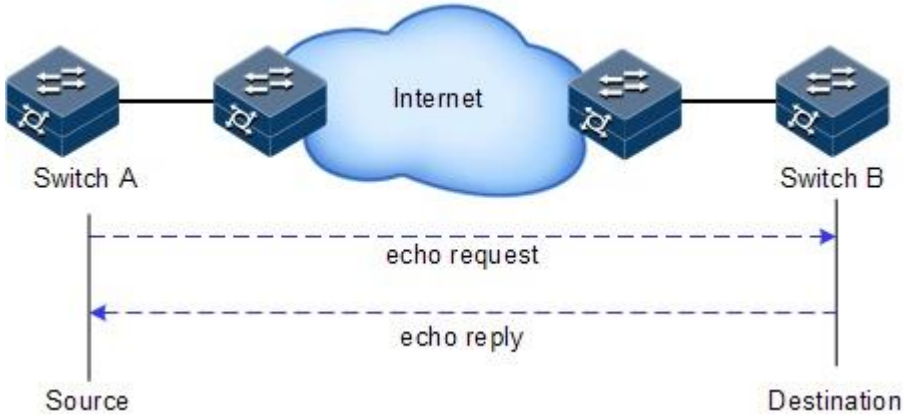
Ping 的名字源于声纳定位操作，用于检测网络连接是否正常。

Ping 功能一般借助 ICMP echo 报文来实现。首先发送 echo request 报文到某个地址，然后等待该地址对应的设备响应 echo reply 报文，当 echo request 到达目标地址以后，在

一个有效的时间内返回 echo reply 报文给源地址，则说明目的地可达。如在有效时间内没有收到回应，则在发送端显示超时，并表明目的地不可达。

Ping 功能实现原理如图 13-11 所示。

图13-11 Ping 功能实现原理组网示意图



13.13.2 配置 Ping 功能

请在设备上进行以下操作。

步骤	配置	说明
1	Inspur#**ping** [**vrf** *name*]*ip-address* [**count** *count*] [**size** *size*] [**waittime** *period*] [**source** *ip-address*]	（可选）通过 **ping** 命令测试 IPv4 网络的连通性。
2	Inspur#**ping ipv6** *ipv6-address* [**count** *count*] [**size** *size*] [**waittime** *period*]	（可选）通过 **ping** 命令测试 IPv6 网络的连通性。

说明

在 **ping** 命令执行的过程中，无法对设备进行其他操作，只有等待执行过程结束或者通过“Ctrl＋C”键强制中断执行过程后才能进行其他操作。

13.14 Traceroute

13.14.1 简介

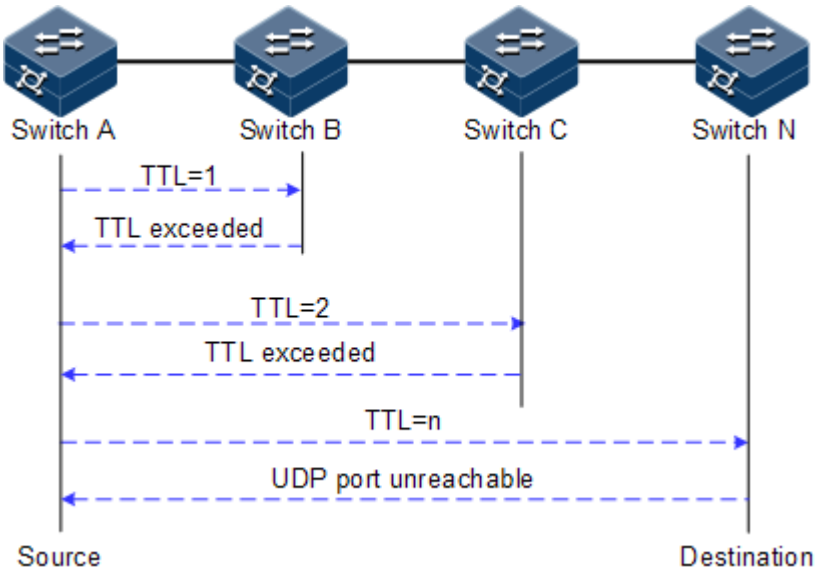
Traceroute 和 Ping 一样，是网络管理中常用的维护手段。Traceroute 功能常用于测试报文从发送端到目的端所经过的网络节点，检测网络连接是否可达，并分析网络中的故障点。

Traceroute 的执行过程如下：

- 首先发送一份 TTL 为 1 的嗅探报文（其中报文的 UDP 端口号是目的端的任何一个应用程序都不可能使用的端口号）。
- 到达第 1 跳时 TTL 减 1，由于 TTL 的值为 0，第 1 跳设备发回一个 ICMP 超时报文，指明此报文不能被发送。
- 发送主机将 TTL 加 1 后重新发送此报文。
- 到达第 2 跳时由于 TTL 的值被减为 0，第 2 跳设备发回一个 ICMP 超时报文，指明此报文不能被发送。

以上步骤循环进行，直到到达目的主机，目的主机并不会送回 ICMP 超时报文，由于目的主机的端口号没有被使用，目的主机会发送端口不可达报文，测试结束。这样，发送主机就能够记录每一个 ICMP TTL 超时报文的源地址，根据得到的回应报文分析出到达目的地所经历的路径。Traceroute 功能实现原理如图 13-12 所示。

图13-12 Traceroute 功能实现原理组网示意图



13.14.2 配置 Traceroute 功能

请在设备上进行以下操作。

步骤	配置	说明
1	Inspur#**traceroute** [**vrf** *name*] *ip-address* [**firstttl** *first-ttl*] [**maxttl** *max-ttl*] [**port** *port-number*] [**waittime** *period*] [**count** *times*] [**size** *size*]	（可选）通过 **traceroute** 命令测试 IPv4 网络的连通性并查看报文经过的网络节点。
2	Inspur#**traceroute ipv6** *ipv6-address* [**firstttl** *fitst-ttl*] [**maxttl** *max-ttl*] [**port** *port-id*] [**waittime** *second*] [**count** *times*] [**size** *size*]	（可选）通过 **traceroute** 命令测试 IPv6 网络的连通性并查看报文经过的网络节点。

14 附录

本章介绍了本文档中涉及的缩略语和术语。

- 术语
- 缩略语

14.1 术语

B

半双工	Half-duplex	半双工指在同一时间只能在同一个方向进行的双向通信。一方在接受信息，而另一方在发送信息的通信，即为半双工。
保护地线	Protection Ground Wire	连接设备和保护地的线缆，通常为黄绿相间的同轴线缆。
标签	Label	线缆、机箱以及警告标识。

D

单模光纤	Single Mode Fiber	单模光纤指在同一条光纤中只能传输单个模式光信号的光纤。
第一英里以太网	EFM（Ethernet in the First Mile）	遵循 IEEE 802.3ah 协议，是一种链路级以太网 OAM 技术，针对两台直连设备之间的链路，提供链路连通性检测功能、链路故障监控功能、远端故障通知功能等。EFM 主要用于用户接入的网络边缘的以太网链路。
电气和电子工程师协会	IEEE（Institute of Electrical and Electronics Engineers）	一个国际性的电子技术与信息科学工程师的协会，是世界上最大的专业技术组织之一（成员人数）。
动态 ARP 检测	DAI（Dynamic ARP Inspection）	一种能够验证网络中 ARP 地址解析协议数据报的安全特性。通过 DAI，网络管理员能够拦截、记录和丢弃具有无效 MAC 地址/IP 地址绑定的 ARP 数据包，以防止网络中常见的 ARP 欺骗攻击。

动态主机配置协议	DHCP（Dynamic Host Configuration Protocol）	在网络中动态分配 IP 地址的技术。它可以自动地为网络中的所有客户端分配 IP 地址，从而减轻管理员的工作量，实现 IP 地址集中管理。
多模光纤	Multi-mode Fiber	多模光纤指在同一条光纤中能够传输多个模式光的光纤。

F

访问控制列表	ACL（Access Control List）	访问控制列表是由 permit | deny 语句组成的一系列有顺序的规则，设备根据这些规则判断哪些数据包可以接收，哪些数据包需要拒绝。
服务质量	QoS（Quality of Service）	一种网络安全机制，是用来解决网络延迟和阻塞问题的一种技术。当网络过载或拥塞时，QoS 能确保重要业务不被延迟或丢弃，同时保证网络高效运行。

G

GFP 封装	GFP Encapsulation	GFP 是一种通用映射技术，它可将变长或定长的数据分组，进行统一的适配处理，实现数据业务在多种高速物理传输通道中的传输。
故障转移	Failover	提供了一种端口联动方案，可以扩展链路备份的范围。该功能通过监控上行链路并对下行链路进行同步设置，使上层设备的故障迅速传达给下层，从而触发主备切换，避免因上行链路故障无法被下层设备感知而出现的流量丢失。
挂耳	Ear hanging	机箱侧面的部件，用于把机箱安装在机柜中。
光纤配线架	ODF（Optical Distribution Frame）	光缆和光通信设备之间的配线连接设备。它是光传输系统中一个重要的配套设施，主要用于光缆终端的光纤熔接、光连接器安装、光路的调接、多余尾纤的存储及光缆的保护等。

H

互联网编号分配委员会	IANA（Internet Assigned Numbers Authority）	主要职能是分配和维护在互联网技术标准（或协议）中的唯一编码和数值，如 IP 地址，组播地址等。

J

激光器自动关断	ALS（Automatic Laser Shutdown）	当光接口的光纤被拔出或光发射器的输出功率过大时，光接口自动关断激光器，防止出现维护或运行风险。

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

K

开放最短路径优先	OSPF（Open Shortest Path First）	一种内部网关动态路由协议，用于在单一自治系统内决策路由。
快速生成树协议	RSTP（Rapid Spanning Tree Protocol）	RSTP 是为了弥补 STP（Spanning Tree Protocol，生成树协议）收敛速度慢的不足而开发的。RSTP 在 STP 的基础上进行了改进，实现了网络拓扑快速收敛。

L

链路汇聚控制协议	LACP（Link Aggregation Control Protocol）	一种实现链路动态汇聚的协议。LACP 协议通过 LACPDU（Link Aggregation Control Protocol Data Unit，链路汇聚控制协议数据单元）与对端交互信息。
链路聚合	Link Aggregation	通过将多个物理以太网端口聚合在一起形成一个逻辑上的聚合组，并把同一聚合组内的多条物理链路视为一条逻辑链路。链路聚合可以实现流量在聚合组各成员端口之间负载分担，在有效的提高了设备之间链路可靠性的同时，还在不进行硬件升级的条件下增大了带宽。

M

密码认证协议	PAP（Password Authentication Protocol）	PPP 认证协议中的密码认证协议，是一种 2 次握手协议，在网络上采用明文方式传输用户名和密码。

Q

全双工	Full-duplex	通信链路上双方可以同时发送和接收数据。
QinQ	Stacked VLAN 或 Double VLAN	是 802.1Q 的扩展，IEEE 在 802.1ad 标准中定义。在运营商的骨干网络（公网）中，报文携带两层的 VLAN Tag：公网 VLAN Tag 和私网 VLAN Tag。公网中私网 VLAN Tag 被当作报文数据部分进行传输。可以分为基本 QinQ 和灵活 QinQ 两种类型。

S

生成树协议	STP（Spanning Tree Protocol）	STP 可以在局域网中消除网络环路，并实现数据链路备份功能。在逻辑上阻断环路，防止广播风暴的产生。当未阻断的链路出现故障时，阻断的链路会被重新激活，充当备份线路的功能。
私有 VLAN	PVLAN（Private VLAN）	PVLAN 采用两层 VLAN 隔离技术，只有上层 VLAN 全局可见，下层 VLAN 相互隔离。如果将交换机或 IP DSLAM 设备的每个端口划为一个（下层）VLAN，则实现了所有端口的隔离。

T

挑战握手认证协议	CHAP（Challenge-Handshake Authentication Protocol）	PPP 认证协议中的挑战握手认证协议，是一种 3 次握手验证协议，只在网络上传输用户名，而不传输用户密码。

V

VLAN 映射	VLAN Mapping	主要功能是将以太网业务报文中的私网 VLAN Tag 替换为运营商的 VLAN Tag，使其按照运营商的 VLAN 转发规则进行传输。在报文从运营商网络转发到对端用户私网时，再按照同样的规则将 VLAN Tag 恢复为原有的用户私网 VLAN Tag，使报文正确到达目的地。

W

网络时间协议	NTP（Network Time Protocol）	由 RFC1305 定义的时间同步协议，用来在分布式时间服务器和客户端之间进行时间同步。使用 NTP 的目的是快速对网络内所有具有时钟的设备进行时钟同步，从而使设备能够提供基于统一时间的不同应用。同时 NTP 还能保证很高的精度（误差在 10ms 左右）。

X

虚拟局域网	VLAN（Virtual Local Area Network）	是为解决以太网的广播问题和安全性而提出的一种协议。是一种通过将局域网内的设备逻辑地而不是物理地划分成一个个网段，从而实现多个互不影响的虚拟工作组的二层隔离技术。

Y

以太网承载 PPP 协议	PPPoE（Point-to-point Protocol over Ethernet）	通过 PPPoE 协议，远端接入设备能够实现对每个接入用户的控制和计费。

以太网环网保护倒换	ERPS（Ethernet Ring Protection Switching）	基于 ITU-T G.8032 标准的 APS（Automatic Protection Switching，自动保护倒换）协议，是一种专门应用于以太网环的链路层协议，正常情况下，它在以太网环中能够防止数据环路引起的广播风暴，当以太网环上链路或设备故障时，能迅速切换到备份链路，保证业务快速恢复。
因特网工程任务组	IETF（Internet Engineering Task Force）	成立于 1985 年底，是全球互联网最具权威的技术标准化组织，主要任务是负责互联网相关技术规范的研发和制定。
远程用户拨号认证系统	RADIUS（Remote Authentication Dial In User Service）	网络中对用户进行认证和计费的协议。

Z

自动保护倒换	APS（Automatic Protection Switched）	自动保护倒换技术是通过对传输线路变化的实时监视、告警信息的自动分析，能够及时发现故障及隐患，在出现严重故障时，快速将工作通道自动切换到备用通道，在极短的时间内恢复通信，完成对故障的快速反应和恢复机制。
自协商	Auto-Negotiation	自协商指接口根据协商结果自动选择接口速率和双工模式。

14.2 缩略语

A

AAA	Authentication，Authorization and Accounting	认证、授权和计费
ABR	Area Border Router	区域边界路由器
AC	Alternating Current	交流电
ACL	Access Control List	访问控制列表
ANSI	American National Standards Institute	美国国家标准协会
APS	Automatic Protection Switching	自动保护倒换
ARP	Address Resolution Protocol	地址解析协议
AS	Autonomous System	自治系统
ASCII	American Standard Code for Information Interchange	美国信息交换标准码
ASE	Autonomous System External	外部自治系统
ATM	Asynchronous Transfer Mode	异步传输模式

AWG	American Wire Gauge	美国线缆标准

B

BC	Boundary Clock	边界时钟
BDR	Backup Designated Router	备份指定路由器
BITS	Building Integrated Timing Supply System	通信楼综合定时供给系统
BOOTP	Bootstrap Protocol	自举协议
BPDU	Bridge Protocol Data Unit	网桥协议数据单元
BTS	Base Transceiver Station	基站收发信台

C

CAR	Committed Access Rate	承诺访问速率
CAS	Channel Associated Signaling	随路信令
CBS	Committed Burst Size	承诺突发数据量
CE	Customer Edge	用户网边缘
CHAP	Challenge Handshake Authentication Protocol	挑战握手认证协议
CIDR	Classless Inter-Domain Routing	无类域间路由
CIR	Committed Information Rate	承诺信息速率
CIST	Common Internal Spanning Tree	公共内部生成树
CLI	Command Line Interface	命令行接口
CoS	Class of Service	服务等级
CPU	Central Processing Unit	中央处理器
CRC	Cyclic Redundancy Check	循环冗余校验
CSMA/CD	Carrier Sense Multiple Access/Collision Detection	载波侦听多路访问
CST	Common Spanning Tree	公共生成树

D

DAI	Dynamic ARP Inspection	动态 ARP 检测
DBA	Dynamic Bandwidth Allocation	动态带宽分配
DC	Direct Current	直流电

DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DiffServ	Differentiated Service	区分服务
DNS	Domain Name System	域名系统
DRR	Deficit Round Robin	差额循环调度
DS	Differentiated Services	差分服务
DSL	Digital Subscriber Line	数字用户线

E

EAP	Extensible Authentication Protocol	PPP 扩展认证协议
EAPoL	EAP over LAN	基于局域网的 EAP
EFM	Ethernet in the First Mile	第一英里以太网
EMC	Electro Magnetic Compatibility	电磁兼容
EMI	Electro Magnetic Interference	电磁干扰
EMS	Electro Magnetic Susceptibility	电磁敏感性
ERPS	Ethernet Ring Protection Switching	以太网环网保护倒换
ESD	Electro Static Discharge	静电释放
EVC	Ethernet Virtual Connection	以太网虚连接

F

FCS	Frame Check Sequence	帧校验序列
FE	Fast Ethernet	快速以太网
FIFO	First Input First Output	先入先出
FTP	File Transfer Protocol	文件传输协议

G

GARP	Generic Attribute Registration Protocol	通用属性注册协议
GE	Gigabit Ethernet	千兆以太网
GMRP	GARP Multicast Registration Protocol	基于 GARP 的组播注册协议
GPS	Global Positioning System	全球定位系统
GVRP	Generic VLAN Registration Protocol	通用 VLAN 注册协议

H

HDLC	High-level Data Link Control	高级数据链路控制
HTTP	Hyper Text Transfer Protocol	超文本传输协议

I

IANA	Internet Assigned Numbers Authority	互联网编号分配委员会
ICMP	Internet Control Message Protocol	Internet 控制报文协议
IE	Internet Explorer	IE 浏览器
IEC	International Electro technical Commission	国际电子技术委员会
IEEE	Institute of Electrical and Electronics Engineers	电气和电子工程师协会
IETF	Internet Engineering Task Force	因特网工程任务组
IGMP	Internet Group Management Protocol	因特网组管理协议
IP	Internet Protocol	网络互联协议
IS-IS	Intermediate System to Intermediate System Routing Protocol	中间系统到中间系统的路由选择协议
ISP	Internet Service Provider	Internet 服务提供商
ITU-T	International Telecommunications Union - Telecommunication Standardization Sector	国际电信联盟远程通信标准化组织

L

LACP	Link Aggregation Control Protocol	链路汇聚控制协议
LACPDU	Link Aggregation Control Protocol Data Unit	链路聚合控制协议数据单元
LAN	Local Area Network	局域网
LCAS	Link Capacity Adjustment Scheme	链路容量调整机制
LLDP	Link Layer Discovery Protocol	链路层发现协议
LLDPDU	Link Layer Discovery Protocol Data Unit	链路层发现协议数据单元

M

MAC	Medium Access Control	媒体访问控制
MDI	Medium Dependent Interface	介质相关接口
MDI-X	Medium Dependent Interface cross-over	介质相关交叉接口
MIB	Management Information Base	管理信息库
MSTI	Multiple Spanning Tree Instance	多生成树实例
MSTP	Multiple Spanning Tree Protocol	多生成树协议

MTBF	Mean Time Between Failure	平均无故障工作时间
MTU	Maximum Transmission Unit	最大传输单元
MVR	Multicast VLAN Registration	组播 VLAN 注册

N

NMS	Network Management System	网络管理系统
NNM	Network Node Management	网络节点管理
NTP	Network Time Protocol	网络时间协议
NView NNM	NView Network Node Management	NView 网络节点管理系统

O

OAM	Operation，Administration and Management	操作、管理和维护
OC	Ordinary Clock	普通时钟
ODF	Optical Distribution Frame	光纤配线架
OID	Object Identifiers	对象标识符
Option 82	DHCP Relay Agent Information Option	DHCP 中继代理信息选项
OSPF	Open Shortest Path First	开放最短路径优先

P

P2MP	Point to Multipoint	点到多点
P2P	Point-to-Point	点到点
PADI	PPPoE Active Discovery Initiation	PPPoE 活动发现发起报文
PADO	PPPoE Active Discovery Offer	PPPoE 活动发现提供报文
PADS	PPPoE Active Discovery Session-confirmation	PPPoE 活动发现会话确认报文
PAP	Password Authentication Protocol	密码认证协议
PDU	Protocol Data Unit	协议数据单元
PE	Provider Edge	运营商边缘
PIM-DM	Protocol Independent Multicast-Dense Mode	密集模式独立组播协议
PIM-SM	Protocol Independent Multicast-Sparse Mode	稀疏模式独立组播协议
Ping	Packet Internet Grope	因特网包探索器
PPP	Point to Point Protocol	点对点协议

PPPoE	PPP over Ethernet	以太网承载 PPP 协议
PTP	Precision Time Protocol	精确时钟同步协议

Q

QoS	Quality of Service	服务质量

R

RADIUS	Remote Authentication Dial In User Service	远程用户拨号认证系统
RCMP	Inspur Cluster Management Protocol	浪潮思科集群管理协议
RED	Random Early Detection	随机早期检测
RH	Relative Humidity	相对湿度
RIP	Routing Information Protocol	路由信息协议
RMON	Remote Network Monitoring	远端网络监控
RNDP	Inspur Neighbor Discover Protocol	浪潮思科邻居发现协议
ROS	Inspur Operating System	浪潮思科操作系统
RPL	Ring Protection Link	环保护链路
RRPS	Inspur Ring Protection Switching	浪潮思科环保护倒换
RSTP	Rapid Spanning Tree Protocol	快速生成树协议
RSVP	Resource Reservation Protocol	资源预留协议
RTDP	Inspur Topology Discover Protocol	浪潮思科拓扑收集协议

S

SCADA	Supervisory Control And Data Acquisition	数据采集与监视控制系统
SF	Signal Fail	信号失效
SFP	Small Form-factor Pluggable	小封装可插拔
SFTP	Secure File Transfer Protocol	安全文件传输协议
SLA	Service Level Agreement	服务等级规约
SNMP	Simple Network Management Protocol	简单网络管理协议
SNTP	Simple Network Time Protocol	简单网络时间协议
SP	Strict-Priority	严格优先级调度
SPF	Shortest Path First	最短路径优先

SSHv2	Secure Shell v2	安全外壳协议版本 2
STP	Spanning Tree Protocol	生成树协议

T

TACACS+	Terminal Access Controller Access Control System	终端访问控制器访问控制系统
TC	Transparent Clock	透传时钟
TCP	Transmission Control Protocol	传输控制协议
TFTP	Trivial File Transfer Protocol	普通文件传输协议
TLV	Type Length Value	类型、长度和取值
ToS	Type of Service	服务类型
TPID	Tag Protocol Identifier	标签协议标识
TTL	Time To Live	生存时间

U

UDP	User Datagram Protocol	用户数据包协议
UNI	User Network Interface	用户侧接口
USM	User-Based Security Model	基于用户的安全模型

V

VLAN	Virtual Local Area Network	虚拟局域网
VRRP	Virtual Router Redundancy Protocol	虚拟路由冗余协议

W

WAN	Wide Area Network	广域网
WRR	Weight Round Robin	加权循环调度