S9500 系列 以太网交换机

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 S9500 系列以太网交换机（以下简称 S9500 系列）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、PoE、DHCP、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
S9500 系列 以太网交换机	4.1.3A(S9503)、4.3.1A(S9506、S9510)

约定

通用格式约定

格式	说明
宋体	正文采用宋体（正文）五号表示。
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。

格式	说明
[ ]	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。

配置过程约定

格式	说明
Inspur_config#**interface** *interface-type interface-number* Inspur_config_g3/1#	进入二层/三层物理接口或聚合组接口配置，均以进入 **gigaethernet 3/1** 为例。
Inspur_config#**interface vlan** *vlan-id* Inspur_config_v1#	进入三层物理接口或 VLAN 接口配置，均以进入 **vlan1** 为例。

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

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
- **monitor** 模式
- 接口基础配置
- **MTU** 配置
- **DDM**
- 端口限速
- 设备基础信息配置
- 恢复出厂设置
- 密码恢复
- ◆ 升级系统软件

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。
- 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 3 个级别。

- 0～1：参观级，用户可以执行 **telnet** 登陆，**ssh** 登陆等命令。
- 2～14：监控级，用户可以执行用于系统维护命令（**show**）等。
- 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，输入用户名和密码后，输入 enable 进入特权用户模式，在屏幕上显示：

```
Inspur#
```

在特权用户模式下，输入 **config** 命令，则可进入全局配置模式。

```
Inspur#config
Inspur_config#
```

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 name** 命令修改主机名。

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。

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，输入用户名和密码后，输入 **enable** 进入。	Inspur#
全局配置模式	在特权用户模式下，输入 **config** 命令。	Inspur_config#
二层物理接口配置模式	在全局配置模式下，使用 **interface { gigaEthernet | tgigaEthernet }***slot/port* 命令。	Inspur_config_gigaethernet 1/*interface*)# Inspur_config_tgigaEthernet 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 }***slot/port* 命令。	Inspur_config_if_range#

模式	进入方式	标识说明
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_l*lb-number*#
VLAN 配置模式	在全局配置模式下，输入 **vlan** *vlan-id* 命令。	Inspur_config_vlan*vlan-id*#
VLAN 接口配置模式	在全局配置模式下，使用 **interface vlan** *vlan-id* 命令。	Inspur_config_v*vlan-id*#
聚合组接口配置模式	在全局配置模式下，使用 **interface port-aggregator** *channel-number* 命令。	Inspur_config_p*channel-number*#
OSPF 配置模式	在全局配置模式下，使用 **router ospf** [*router-id*]命令。	Inspur_config_ospf_*router-id*)#
基本 **IP ACL** 配置模式	在全局配置模式下，使用 **ip access-list standard** *acl-name* 命令。	Inspur_config_std)#
扩展 **IP ACL** 配置模式	在全局配置模式下，使用 **ip access-list extended** *acl-name* 命令。	Inspur_config_ext)#
MAC ACL 配置模式	在全局配置模式下，使用 **mac access-list** *acl-name* 命令。	Inspur_config_macl)#
中文提示模式	在任意配置模式下，输入 **chinese** 命令。	Inspur#
英文提示模式	在任意配置模式下，输入 **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。
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。

快捷键	说明
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 **show run** 等。仅在分屏显示功能使能的情况下生效。
“Ctrl+E”	将光标移动到行尾。
“Ctrl+F”	作用同右光标键（→）。
“Ctrl+Z”	从其它模式退到特权用户模式。
“Space”	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。
“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：

```
aaa              Authentication, Authorization, Accounting
boot             system boot
bootrom           Bootrom
clear            Reset functions
clock            System time and date
config           Configuration from terminal interface
console           Console
copy             load configuration information
```

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：

```
authenticate            Authenticate function
authentication-keyid    Authentication keyid
peer                    Configure NTP peer
refclock-master         Set local clock as reference clock
server                  Configure NTP server
trust-keyid             Trusted authenticate keyid
```

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：

```
vlan1
<1-4094> vlan 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

错误提示信息	说明
Incomplete command..	未完成命令。
^ Unknown command	用‘^’标记的位置输入不合法。

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，如下表所示。

命令行信息显示特性功能键说明

功能键	说明
键入“**Space**”	继续显示下一屏信息。
键入“**Enter**”	继续显示下一行信息。

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：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：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：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。

序号	配置	说明
1	Inspur#**show** *command-string* | { **begin** | **include** | **exclude** } *expression*	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。

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、Web 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。

Telnet 方式：设备默认 IP 地址为 192.168.0.1。如需修改 IP 地址，需要先通过 Console 方式登录，在设备上配置 IP 地址，以及设置用户名和密码，再使用新 IP 地址进行远程 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。

1.2.2 通过 Console 口登录设备

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

缺省配置

设备上 Console 口的缺省配置如下。

功能	缺省值
传输速率	9600
流控方式	无流控
验证方式	不验证
停止位	1
数据位	8

通过 Console 口登录

当用户希望通过 PC 连接 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 1.2.1 通过 PC 连接 Console 口登录设备的组网示意图

图 1.2.2“超级终端”中的通信参数配置示意图

1.2.3 通过 Telnet 登录设备

简介

初始情况下，设备缺省管理 IP 地址为 192.168.0.1，子网掩码为 255.255. 0.0。设备的缺省用户名和密码为 admin/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。

有 SNMP 接口的设备，需使用 SNMP 接口进行 telnet 登录。无 SNMP 接口的设备，可以使用任意接口进入管理 VLAN 进行 telnet 登录。

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。如下图所示，交换机此时提供的是 Telnet Server 服务。

图 1.2.3 交换机作为 Telnet Server 设备的组网示意图

缺省配置

设备上 Telnet 服务器功能的缺省配置如下。

功能	缺省值
Telnet 服务器功能状态	使能
Telnet 服务器监听端口号	23
使能 **Telnet** 服务器功能的接口	所有接口

通过 **Telnet** 配置设备时，建议不要频繁修改设备的 **IP** 地址。修改 **IP** 地址可能导致当前 **Telnet** 连接断开，需根据新的 **IP** 地址重新建立 Telnet 连接。

配置 Telnet 服务器

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。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**interface vlan** *vlan-id* Inspur_config#**interface gigaethernet** *slot*/0	进入 **VLAN** 接口或带外接口配置模式，以下使用进入 **VLAN** 接口为例。
3	Inspur_config_v*vlan-id* #**ip address** *ip-address* [*ip-mask*] [*secondary*] Inspur_config-v*vlan-id* #**ipv6 address** *ipv6-address/prefix-length* [**eui-64**] Inspur_config_v*vlan-id* #**exit**	配置设备 **IP** 地址。
4	Inspur_config#**ip telnet access-list** { *ip-access-list-name*| *ipv6-access-list-name* }	配置 **Telnet** 的访问控制列表号，使用 **no** 格式恢复到缺省情况。
5	Inspur_config#**ip telnet max-user** *session-number*	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。
6	Inspur_config#**ip telnet listen-port** *port-id*	配置设备的 **TELNET** 侦听端口号。

配置 Telnet 客户端

请在作为 Telnet Client 的设备上进行以下配置。

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

1.2.4 通过 SSH 登录设备

简介

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。

设备支持基于密码和公钥两种认证方式。

基于密码认证方式：与登录设备认证使用同一数据库。SSH 客户端只需输入用户名和密码，就可以登录到远程 SSHv2 服务器。所有传输的数据都会被加密，但是可能会有其他服务器伪冒真正的服务器，无法避免伪冒服务器攻击。

基于公钥认证方式：SSHv2 客户端除需要输入用户名和密码外，还需要依靠密钥进行认证。登录前在 SSHv2 客户端创建一对密钥，包括主机公钥和主机私钥，并将公钥存入 SSHv2 服务器。登录认证过程和传输的数据都会被加密，避免了伪冒服务器攻击。

缺省配置

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	1024bit
密钥重协商周期	0h
SSH 采用的认证方式	password
SSH 认证超时时间	180s
SSH 认证允许失败次数	5
SSH 侦听端口号	22
SSH 会话功能状态	禁用
SSH 协议版本	v2
SSH 安全算法模式	禁止

配置 SSH 服务器

请在设备上进行以下配置。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**ip sshd key-bits** *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#**ip sshd enable**	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 ip sshd enable** 关闭 **SSHv2** 服务器。
4	Inspur_config#**ip sshd auth-method** { **password** | **rsa-key** }	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#**ip sshd timeout** *second*	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 180 秒。
6	Inspur_config#**ip sshd auth-retries** *times*	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 5 次。
7	Inspur_config#**ip sshd port** *port-number*	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。 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。
8	Inspur_config#**ip sshd access-class** { *ip-access-list-name* }	配置 **SSH** 的访问控制列表号。
9	Inspur_config#**ip sshd KexAlgorithms** *word*	指定允许的密钥交换算法，多个算法必须用逗号分隔。
10	Inspur_config#**ip sshd ciphers** *word*	指定允许的加密算法，多个算法必须用逗号分隔。
11	Inspur_config#**ssh -d** *ip address* **-l** *username* **-s** *password* [**-p** *port-id*]	配置通过 **ssh** 登录目标主机。

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 sshd	查看 SSH 进程信息
2	Inspur#show ssh	查看 SSH 连接信息

1.2.5 通过 Web 登录设备

简介

为了方便用户对设备进行配置和维护，设备支持 **Web** 网管功能。用户可以利用 **Web** 网管在图形界面下直观的管理和配置设备。

Web 网管支持以下两种文本传输协议：

HTTP（**Hypertext Transfer Protocol**，超文本传输协议）：用来在网络上传递 **Web** 页面信息。在设备上使能 **HTTP** 服务功能后，用户就可以通过 **HTTP** 协议登录设备，并利用 **Web** 界面访问、控制设备。

HTTPS（**Secure Hypertext Transfer Protocol**，安全的超文本传输协议）：利用 **SSL**（**Secure Sockets Layer**，安全套接层）协议保证合法客户端可以安全访问设备。客户端与设备之间交互的数据需要经过加密，保证了数据传输的安全性和完整性，从而实现对设备的安全管理。

配置 **Web** 网管功能后，远程用户可以通过 Web 浏览器登录设备并对其进行管理。如果禁止 **Web** 网管功能，则断开所有已经建立的 **HTTP** 连接。

缺省配置

设备上 **Web** 网管的缺省配置如下。

功能	缺省值
HTTP 功能状态	使能

配置 Web 网管功能

请在设备上进行以下配置。

序号	配置	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#ip http server	使能 **HTTP server** 功能，使用 **no** 格式禁止该功能。
3	Inspur_config#ip http http-access enable	使能 **HTTP** 功能，使用 **no** 格式禁止该功能。
4	Inspur_config#ip http ssl-access enable	使能 **HTTPS** 功能，使用 **no** 格式禁止该功能。

序号	配置	说明
5	Inspur_config#**ip http access-list** *access list name*	配置 **Web** 登录用户的 **IP** 访问列表。

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 http**	查看 **http** 信息。

1.2.6 管理登录用户

简介

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。

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。

缺省配置

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：**inspur**123 • 用户权限：15
新建用户权限	15

配置本地用户管理

请在设备上进行以下配置。

序号	配置	说明
1	Inspur_config#**username** *user-name* **password** *password*	创建或修改登录用户的用户名和明文形式密码。

序号	配置	说明
2	Inspur_config #**no username** *user-name*	删除用户。

配置本地密码管理

请在设备上进行以下配置。

序号	配置	说明
1	Inspur_config#**local***pass word*	进入本地密码配置态
2	Inspur_config-local*pass-word* #**non-user**	密码和用户名不同
3	Inspur_config-local*pass-word* #**validity** *time*	配置用户密码到期时间。
4	Inspur_config-local*pass-word* #**element** *[number] [lower-letter] [upper-letter] [special-character]*	配置账号或者修改密码时，增加密码的复杂度。
5	Inspur_config-local*pass-word* #**min-length** *min-length*	配置用户密码最小长度。
6	Inspur_config#**localauthor** *word*	进入本地授权策略配置
7	Inspur_config_locala*uthor_word#* **privilege configure** [*<0-15>*] [default]	配置命令优先级
8	Inspur_config#**username** *user-name* **password** *password* **pass-group** *word*	将该用户加入配置好的本地密码策略组
9	Inspur_config#**username** *user-name* **password** *password* **author-group** *word*	将该用户加入配置好的本地授权策略组

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 local-users**	查看设备的用户信息。

1.2.8 配置用户管理示例

组网需求

如下图所示，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：

创建用户 **user1**，明文密码为 aaAA123@。

配置用户 **user1** 的权限为 10 级。

图 1.2.4 用户管理组网示意图

配置步骤

步骤 1 创建用户本地授权组

```
Inspur_config#localauthor 123
Inspur_config_localauthor_123#privilege configure 10
Inspur_config_localauthor_123#exit
Inspur_config#
```

步骤 2 创建并配置用户权限。

```
Inspur_config#username user1 password aaAA123@ authen-group 123
```

检查结果

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。

```
Username:user1
Password:
Inspur>enable
Inspur#
```

如需删除默认的 inspur 账号，可使用如下命令：

```
Inspur_config#no username admin
```

1.3 Monitor 模式

1.3.1 简介

交换机的 **monitor** 模式是一种特殊的工作模式。

1.3.2 配置准备

场景

当设备的版本文件丢失或者升级版本错误时，可以进入 monitor 模式进行更改配置

1.3.3 进入 monitor 模式

交换机重启过程中长按 Ctrl+P 就可以进入到 monitor 模式

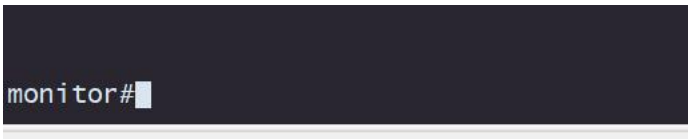


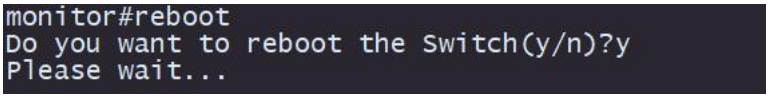
图 1.3.1　monitor 示例

1.3.4 退出 monitor 模式

在 monitor 模式下输入 reboot 或者断电重启都可以退出 monitor

序号	配置	说明
1	monitor#**reboot**	退出 **monitor** 模式。

图 1.3.2 退出 monitor 示例



1.4 接口基础配置

1.4.1 简介

交换机接口基础配置，是搭建网络的关键。通过启用 / 关闭接口，能掌控连接状态；设置速率与双工模式，匹配设备性能；配置 IP 地址实现网络通信；划分 VLAN 隔离广播域，增强安全性。

1.4.2 配置以太网接口

选定以太网接口

在全局配置模式下输入下列命令进入以太网接口配置状态。

序号	配置	说明
1	Inspur_config#**interface gigaethernet** *[slot/port]*	进入千兆以太网接口配置状态。
2	Inspur_config#**interface TgigaeEthernet** *[slot/port]*	进入万兆以太网接口配置状态。

序号	检查项	说明
1	Inspur_config#**show interface** *[type [slot/port]]*	显示详细接口状态。
2	Inspur_config#**show interface brief**	显示全部接口状态

检查

Inspur#**show interface gigaEthernet 3/1**

GigaEthernet3/1 is down, line protocol is down

protocolstatus upTimes 0, downTimes 0, alloc at 2000-1-1 0:1:31

Ifindex is 377, unique port number is 2

Hardware is Giga-FX, address is xxxx.xxxx.xxxx (bia xxxx.xxxx.xxxx)

MTU 9216 bytes, BW 1000000 kbit, DLY 10 usec

Encapsulation ARPA

Auto-duplex, 1000Mb/s, Flow-Control Off

5 minutes input rate 0 bits/sec, 0 packets/sec

5 minutes output rate 0 bits/sec, 0 packets/sec

Real time input rate 0.0%, 0 bits/sec, 0 packets/sec

Real time output rate 0.0%, 0 bits/sec, 0 packets/sec

peak input rate 0 bits/sec,

peak input rate 0 packets/sec,

peak output rate 0 bits/sec,

peak output rate 0 packets/sec,

Received 0 packets, 0 bytes

0 broadcasts, 0 multicasts

0 discard, 0 error, 0 PAUSE

0 align, 0 FCS, 0 symbol

0 jabber, 0 oversize, 0 undersize

0 carriersense, 0 collision, 0 fragment

0 L3 packets, 0 discards, 0 Header errors

0 URPF errors

Transmitted 0 packets, 0 bytes

0 broadcasts, 0 multicasts

0 discard, 0 error, 0 PAUSE

0 sqettest, 0 deferred, 0 oversize

0 single, 0 multiple, 0 excessive, 0 late

0 L3 forwards

Discard：丢弃数据包数。拥塞、**STP** 检查丢弃、**VLAN** 检查丢弃、**FP** 丢弃

indisc：收上来的报文是正确的，但是在这个端口的出站队列满了，没能力转发。报文多端口进，单端口出会出现这样的现象。

error：错误包

align：帧二进制长度不为 8 的倍数，无法通过 **FCS** 检测的帧，（不包括 **fragment** 或 **jabber**）
FCS：帧二进制长度为 8 的倍数，但没有通过 **FCS** 检测的帧，（不包括 **fragment** 或 **jabber**）

fragment：小于 64 字节，且有上计的 **alignment** 错误或 **FCS** 错误的报文总数。
jabber：大于 1518 字节，且有上计的 **alignment** 错误或 **FCS** 错误的报文总数。

oversize：大于 1518 字节的正常报文总数。

undersize：小于 64 字节的正常报文总数。

collision：对该以太网段上冲突总数的最好估计。

deferred：第一次传输的尝试由于线路繁忙被延后的帧数的统计。

single：经过一次冲突抑制之后最后成功传输的帧。

multiple：经过多次冲突抑制之后最后成功传输的帧。

late：在一个报文开始传输一个时隙后检测到冲突的计数。

excessive：由于冲突过多而传输失败的帧的计数。

配置 range 接口

序号	配置	说明
1	Inspur_config#**interface range** *type slot/port1 { -/, } port2[,port3[- port4]]*	进入 **range** 模式 1、槽位号为 **slot**; 2、端口号在任意一个“-”号前后两个值 **port1** 和 **port2** 3、**port2** 必须不小于 **port1**; 4、“-”号和“,”号的前后不能有空格。

配置速率

以太网的速率既可以通过自协商实现，也可以通过在 interface 下进行配置实现。

序号	配置	说明
1	Inspur_config_g3/1#**Speed** *{100|1000|auto}*	设置快速以太网的速率为 100M,1000M,或自协商。
2	Inspur_config_g3/1#**No speed**	恢复缺省设置，速率为自协商。

配置端口的双工模式

缺省时，以太网接口可以自动协商是半双工还是全双工。千兆端口的双工模式总是 auto。

序号	配置	说明
1	Inspur_config_g3/1#**duplex** *{full/auto}*	设置以太网的双工模式。
2	Inspur_config_g3/1#**No duplex**	恢复缺省设置，双工模式为自协商。

配置接口流量控制

在接口为全双工模式时，流量控制通过 802.3X 定义的 PAUSE 帧实现；在接口为半双工 模式时，通过背压实现。

序号	配置	说明
1	Inspur_config_g3/1#**flow-control on/off /auto**	打开/关闭接口流控。 注：对端接口也需要开启流控
2	Inspur_config_g3/1#**no flow-control**	恢复缺省设置，接口无流控。

1.4.3 配置逻辑接口

配置空（null）接口

整个系统只支持一个空接口。这个接口的功能类似于在大多数操作系统上应用的空设备。这个接口一直有效，但是从不转发或接收通信。空接口提供了过滤通信的一个可选方法，可以通过将不希望的网络通信路由到空接口，也可以起到访问控制列表的作用。

空接口的指定通过在全局配置态中使用下面命令：

序号	配置	说明
1	Inspur_config#**interface null** *0*	进入空接口配置状态 。

空接口可被用于使用接口类型作为参数的任何命令中。

配置回环接口

为指定一个回环接口，且进入接口配置态，在全局配置态中使用下面命令：

序号	配置	说明
1	Inspur_config#**interface loopback** *number*	进入回环接口配置状态。

配置聚合接口

通过下面的命令定义聚合接口：

序号	配置	说明
1	Inspur_config#**Interface port-aggregator** *number*	配置聚合接口。

配置 VLAN 接口

通过下面的命令定义VLAN 接口：

序号	配置	说明
1	Inspur_config#**Interface vlan** *number*	配置 **VLAN** 接口。

配置 SuperVlan 接口

定义SuperVlan 接口：

序号	配置	说明
1	Inspur_config#**Interface superVLAN** *number*	配置 **superVLAN** 接口。

1.4.4 配置接口公共属性

添加描述

若想向任意接口添加一条描述，在接口配置态中使用下面命令。

序号	配置	说明
1	Inspur_config_g3/1#**description** *string*	向当前配置接口中添加描述。

设置带宽

上层协议使用带宽信息来进行操作决策。在接口配置态中，使用如下命令为接口设置带宽：

序号	配置	说明
1	Inspur_config_g3/1#**bandwidth** *kilobps*	为当前配置接口设置带宽。

设置时延

上层协议使用时延信息来进行操作决策。在接口配置态中，使用如下命令向接口设置时延：

序号	配置	说明
1	Inspur_config_g3/1#**delay** *tensofmicroseconds*	为当前配置接口设置时延。

1.4.5 接口配置示例

接口描述示例

下面示例说明了如何添加有关接口的描述，此描述将出现在配置文件和接口命令显示中。

Inspur_config#**interface vlan 1**

Inspur_config_v1#**ip address 192.168.1.23 255.255.255.0**

接口描述示例

下面例子启用GigaEthernet 1/1 接口。

Inspur_config#Interface GigaEthernet1/1

Inspur_config_g1/1#shutdown

下面例子重新启用接口。

Inspur_config#interface GigaEthernet1/1

Inspur_config_g1/1#no shutdown

1.5 MTU 配置

1.5.1 简介

网络层一般要限制每次发送数据包的最大长度。任何时候网络层接收到一份要发送的 IP 数据包时，它要判断向本地哪个接口发送数据，并查询该接口获得其最大传输单元 MTU（Maximum Transmission Unit)。网络层把 MTU 值与要发送的 IP 数据包长度进行比较，如果 IP 数据包的长度比 MTU 值大，那么 IP 数据包就需要进行分片，分片后的数据包长度小于等于 MTU。

1.5.2 配置 MTU 大小

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**system mtu** *MTU size in bytes*	配置系统 **MTU** 大小。 系统 **MTU** 会在所有接口下生效。
3	Inspur_config#**interface** *[GigaEthernet | TGigaEthernet] interface number/port number*	进入接口配置模式。

序号	配置	说明
4	Inspur_config_g|tgx/x#**switchport mtu** *MTU size in bytes*	修改对应接口的 **MTU**。 注： 配置接口 **MTU** 后，全局 **MTU** 在该接口不再生效。

序号	检查项	说明
1	Inspur#**show system mtu**	显示系统 **MTU** 的大小。
2	Inspur#**show interface** *[GigaEthernet | TGigaEthernet] interface number/port number*	查看接口 **MTU** 大小。

1.5.3 修改 MTU 配置案例

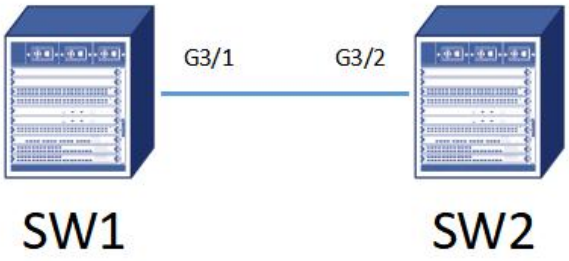


图 1.5.1**MTU** 配置案例

配置目标

将交换机 SW1 的 GigaEthernet 3/1 端口 MTU 值修改为 9216，将交换机 SW2 的系统 MTU 值修改为 9216。

配置步骤

交换机 SW1 配置

Inspur_SW1#**config**

Inspur_SW1_config#**interface gigaEthernet 3/1**

Inspur_SW1_config_g3/1#**switchport mtu 9216**

交换机 SW2 配置

Inspur_SW2#**coinfig**

Inspur_SW2_config#**system mtu 9216**

配置验证

Inspur_SW2#**show system mtu**

System MTU Jumbo size is 9216 bytes

Interface MTU Jumbo size(Byte)

g3/1 9216

Inspur_SW1#**show interface gigaEthernet 3/1**

GigaEthernet3/1 is down, line protocol is down

protocolstatus upTimes 0, downTimes 0, alloc at 2000-1-1 0:1:31

Ifindex is 377, unique port number is 2

Hardware is Giga-FX, address is xxxx.xxxx.xxxx (bia xxxx.xxxx.xxxx)

MTU 9216 bytes, BW 1000000 kbit, DLY 10 usec

Encapsulation ARPA

Auto-duplex, 1000Mb/s, Flow-Control Off

5 minutes input rate 0 bits/sec, 0 packets/sec

5 minutes output rate 0 bits/sec, 0 packets/sec

Real time input rate 0.0%, 0 bits/sec, 0 packets/sec

Real time output rate 0.0%, 0 bits/sec, 0 packets/sec

peak input rate 0 bits/sec,

peak input rate 0 packets/sec,

peak output rate 0 bits/sec,

peak output rate 0 packets/sec,

Received 0 packets, 0 bytes

0 broadcasts, 0 multicasts

0 discard, 0 error, 0 PAUSE

0 align, 0 FCS, 0 symbol

0 jabber, 0 oversize, 0 undersize

0 carriersense, 0 collision, 0 fragment

0 L3 packets, 0 discards, 0 Header errors

0 URPF errors

Transmitted 0 packets, 0 bytes

0 broadcasts, 0 multicasts

0 discard, 0 error, 0 PAUSE

0 sqettest, 0 deferred, 0 oversize

0 single, 0 multiple, 0 excessive, 0 late

0 L3 forwards

1.6 DDM

1.6.1 简介

DDM 检查功能缺省开启，可通过 show interface xxxx 显示相关端口上的光模块的 DDM 信息，如果没插光模块，则不显示。注意：开启后，CPU 占用率可能会略有上升，各机型依硬件设计不同而不同。检查的信息有各光模块的规格，波长，厂商信息，序列号，生产日期等等。如果光模块支持 Digitaldiagnostic monitoring 功能，则显示光模块的收发光功率，电压，偏置电流，温度以及相关阀值信息

1.6.2 禁止光口 DDM 检测功能

序号	配置	说明
1	Inspur_SW1#config	进入全局配置模式。
2	Inspur_SW1_config#ddm disable	禁止所有光口的 DDM 检查功能。
3	Inspur_SW1_config#no ddm disable	开启所有光口的 DDM 检查功能

序号	检查项	说明
1	Inspur#show ddm	查看所有端口的 DDM 信息。

1.6.3 使能光口自适应光模块功能配置

使能此功能后，端口会根据所插光模块类型来切换端口的工作模式到与所插光模块 相匹配的工作模式。比如万兆光口插千兆光模块，则会切到千兆光模式，千兆光口插百兆光模块，则会切换到百兆光模式。

由于万兆只有一种工作模式，而千兆有自适应和强制两种模式，所以在万兆口插千兆光模块时，会切到千兆光的缺省自适应模式，如果想指定切过去是切换到千兆光的强制模式，则需要在此命令后加配置参数 full 来指定。而百兆光只有一种工作模式，则无需带此参数。如果采用光转电模块，则必需配置此命令才能正常工作。

请在设备上进行以下配置。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config_tg3/1#**fiber-auto-config** *{full}*	使能光口的光模块自适应功能．如果带参数 **full,**则切 换过去是强制模式。
3	Inspur_config_tg3/1#**no fiber-auto-config**	关闭光口的光模块自适应功能。

1.7 端口限速

1.7.1 简介

端口限速是通过限制网络设备端口的带宽使用，确保网络资源的合理分配，避免因个别用户或应用占用过多带宽而影响整体网络性能。端口限速功能用于限制端口进出口的流量速率。进入特权模式下使用下面的命令限制端口的流量速率。

1.7.2 配置端口限速

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**interface** *[GigaEthernet | TGigaEthernet] interface number/port number*	进入接口配置模式。
3	Inspur_config_g|tgx/x#**switchport rate-limit** *{ band | bandwidth percent } { ingress | egress } [burst-size { high | middle | low }]*	配置端口的流量速率限制。 **band** 为要限制的流量速率，步长 64**Kbps**。 **percent** 为要限制的流量百分比。 **ingress** 表示对入口起作用。 **egress** 表示对出口起作用。 high, **middle, low** 是指报文缓冲区的大小。

1.7.3 端口限速配置案例

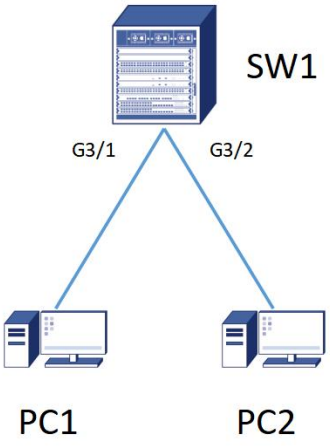


图 1.7.1 端口限速配置案例

配置目标

1.限制 **PC**1 端口的上行速率为 **10Mbps**。

2.使用带宽百分比限制方式，将 **PC**2 端口速率限制为 **50%**（假设端口带宽为 1**Gbps**）。

配置步骤

场景 1：基于固定速率的限速（单位：64kbps）。

配置命令：

Inspur_config# **interface GigabitEthernet 3/1**

Inspur_config_g3/1# **switchport rate-limit 156**

场景 2：基于带宽百分比的限速

配置命令：

Inspur_config# **interface GigabitEthernet 3/2**

Inspur_config_g3/2# **switchport rate-limit bandwidth 50**

1.8 配置设备基本信息

请在需要的设备上进行以下配置。

序号	配置	说明
1	Inspur_config#**hostname** *name*	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“\、’、<、>、&”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。

序号	配置	说明
2	Inspur_config#{ **chinese** | **english** }	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_config#**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。

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。

1.8.1 配置示例

配置设备名称

Inspur_config#**hostname switch**

switch_config#

配置切换语言模式

Inspur_config#**chinese**

Inspur_config#?

aaa -- 配置认证、授权或记录

aggregator-group -- 聚合配置

alias -- 定义命令别名

archive -- 配置备份

Inspur_config#**english**

Inspur_config#?

aaa -- AAA configuration

aggregator-group -- Aggregation configuration

alias -- Define alias for command

archive -- Configuration Backup

保存配置信息

Inspur#**write**

Saving current configuration...

OK!

Inspur#Jan 1 00:25:59 /startup-config is wrote, TID:8799adc0

1.9 恢复出厂

1.9.1 简介

设备在出厂时，通常会被安装一些基本的配置，称为出厂配置，用来保证设备在没有配置文件或者配置文件丢失、损坏的情况下，能够正常启动、运行。

1.9.2 配置准备

场景

当用户需要更改网络配置时，可以使用此命令将交换机恢复到出厂设置状态，以便重新配置网络。

当用户需要频繁更改交换机配置时，可以使用此命令将其恢复到出厂状态，以便更快地进行操作。

1.9.3 恢复出厂设置

enable 模式下恢复出厂设置

通过 console/vty 接口连接设备，输入用户名密码登录设备

序号	命令	说明
1	Inspur>**enable**	进入特权配置模式。
2	Inspur#**dir**	通过 **dir** 命令列出当前目录内容
3	Inspur#**delete startup-config**	通过 **delete** 命令删除全局配置文件
4	Inspur#**delete bvss-config**	通过 **delete** 命令删除堆叠文件（可选）
5	Inspur#**reboot**	重启设备

输入 reboot 命令以后根据提示输入 Y，然后重启设备即可恢复设备出厂设置。

monitor 模式下恢复出厂设置

在现场条件允许的情况下重启设备，在设备重启的过程中一直不停的按着 ctrl+p 让设备进入 monitor 模式，在 monitor 模式下输入

序号	命令	说明
1	monitor#**dir**	通过 **dir** 命令列出当前目录内容
2	monitor#**delete startup-config**	通过 **delete** 命令删除全局配置文件
3	monitor#**delete bvss-config**	通过 **delete** 命令删除堆叠文件（可选）
4	monitor#**reboot**	重启设备

输入 reboot 命令以后根据提示输入 Y，然后重启设备即可恢复设备出厂设置。

1.9.4 配置示例

enable 模式案例

Inspur>**enable**

Inspur#**dir**

Inspur#**delete startup-config**

Inspur#**delete bvss-config（可选）**

Inspur#**reboot**

输入 **reboot** 命令以后根据提示输入 **Y**，然后重启设备即可恢复设备出厂设置。

monitor 模式案例

monitor#**dir**

monitor#**delete startup-config**

monitor#**delete bvss-config （可选）**

monitor#**reboot**

输入 **reboot** 命令以后根据提示输入 Y，然后重启设备即可恢复设备出厂设置。

1.10 恢复密码

1.10.1 简介

交换机恢复密码是指在忘记交换机登录密码的情况下，无法登录设备进行配置。

1.10.2 配置准备

场景

网络管理员由于长时间未操作交换机，或者管理的交换机设备较多，可能会遗忘登录密码。这时候就需要恢复密码，以便能够重新登录交换机，进行配置修改、故障排查、功能升级等管理操作。

管理员离职或岗位变动，未进行密码交接，导致后续人员无法登录交换机，需要恢复密码来获取设备的管理权限。

1.10.3 恢复密码配置

明文密码恢复

通过 Console 口登录交换机，在条件允许的情况下重启交换机，在交换机重启的过程中一直不停的按 crtl+p，设备将进入 monitor# 模式，在 monitor# 模式下输入 more startup-config

请在设备上进行以下配置。

序号	配置	说明
1	monitor#more startup-config	查看当前交换机保存的配置

输入以上命令后，可以查看当前交换机保存的配置，在该配置中查找一条 username XXX

password 0 XXX 的命令，该命令就是关于交换机密码和用户名的配置命令。

密文密码恢复

通过 Console 口登录交换机，在条件允许的情况下重启交换机，在交换机重启的过程中一直不停的按 crtl+p，设备将进入 monitor# 模式，在 monitor# 模式下输入 more startup-config

序号	配置	说明
1	monitor#more startup-config	查看当前交换机保存的配置
2	monitor#service password-encryption	对系统中的密码进行加密

将 more startup-config 打印出来的所有信息复制（若底部出现--more--信息，说明底部还有信息未打印完，按空格可以打印将他们打印完），然后粘贴到一个 txt 文档中。在复制出来的配置中找到一条 service password-encryption，把这条命令删除掉。

此时我们设备还处在 monitor#模式，在此模式下输入 delete startup-config 即可将交换机的配置删除。

输入 reboot 重启交换机，等重启完成，不需要输入用户名密码即可登陆交换机。将刚才粘贴到 txt 文档中的配置进行复制，然后进入交换机 config#模式下，粘贴即可恢复之前的配置，然后可以自行配置用户名密码。（配置用户名密码的命令为：username XXX password XXX）

1.10.4 配置示例

明文示例

monitor#more startup-config

username admin password 0 admin

找到 username XXX password 0 XXX，此示例用户名为 admin，密码为 admin

密文示例

monitor#more startup-config

username admin password 7 101b433d384f

在 txt 文档中，删除 username admin password 7 101b433d384f 这条命令

monitor#more startup-config

恢复出厂重启后连删除 username admin password 7 101b433d384f 命令后的配置文档粘贴回去复原配置。

1.11 升级新系统软件

1.11.1 简介

升级的主要原因有以下几点：

- 修补漏洞：通过升级可以修补老版本存在的问题，提高设备的可靠性和安全性

- 支持新功能特性：厂商可以在后续软件版本中添加新的功能特性，满足用户的需求
- 提升性能：升级可以对交换机的驱动程序进行更新，使硬件更好的发挥性能

1.11.2 升级

简介

9500 系列交换机可以通过命令行升级，在进行升级前，需要确认好设备的主控以及准备好版本及 **tftp** 软件，该交换机是分布式的结构，每一块线卡都有 **bin** 文件，注意线卡文件版本是否与主控的版本同步。在升级时在主控的命令行界面进行升级。

判断主控

如果设备配置了两个主控板卡，则可以通过进入主控的命令行界面，能进入 **config** 模式的为主控，不能进入 **config** 模式的为备控，备控上的版本及线卡版本可通过主控进行同步。

配置交换机升级

请在设备上进行以下配置。

序号	命令	说明
1	Inspur#**copy tftp flash**	从 **tftp** 服务器上传文件到交换机（升级主控）
2	Inspur#**copy ftp flash**	从 **ftp** 服务器上传文件到交换机（升级主控）
3	Inspur#**copy tftp:***version name* **flash:** *switch.bin sever ip*	升级主控命令
4	Inspur#**copy tftp:***version name* **flash:***ls_bin sever ip*	升级线卡命令
5	Inspur#**update msu switch.bin**	更新备控目录中的版本文件（双主控）
6	Inspur#**update msu ls_bin**	更新备控目录中的显卡版本（双主控）
7	Inspur#**redundancy reload shelf**	整机重启

1.11.3 配置检查

配置完成后，请在设备上执行以下命令检查配置结果。

序号	命令	说明
1	Inspur#**dir**	查看 **flash** 文件目录和空闲空间
2	Inspur#**show version**	查看当前版本
3	Inspur#**show redundancy**	查看主备控运行状态
4	Inspur#**show oir-information**	查看线卡在线状态
5	Inspur#**through-pass slot** *number*	进入线卡

1.11.4 升级示例

配置步骤

步骤 1.电脑能够跟交换机通信

交换机的默认管理地址为 192.168.0.1，将电脑与交换机任意电口直连。电脑配置为同一网段即可

步骤 2 电脑使用 **tftb** 工具为交换机升级

（1）选择好路径之后点击 

按钮，启动 **tftp** 服务器。

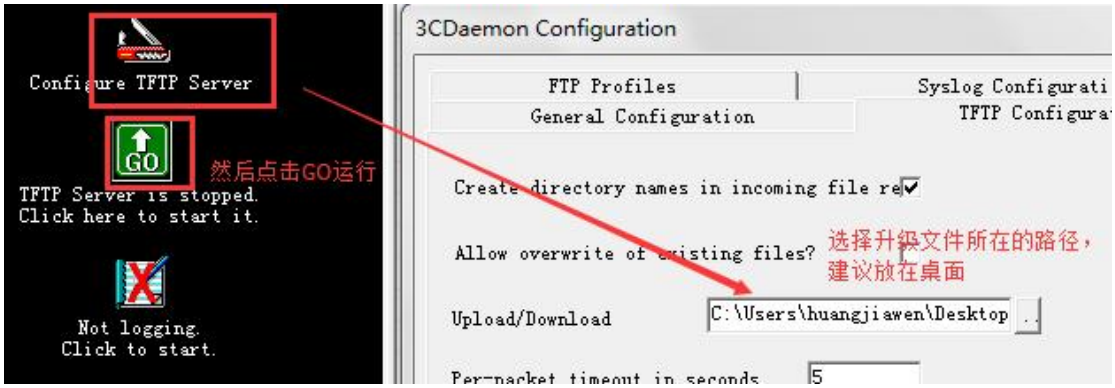


图 1.11.1

（2）运行后图标变成 

，查看右侧 **tftp** 服务器的地址（主机地址）是否和设备处于同一个网段。

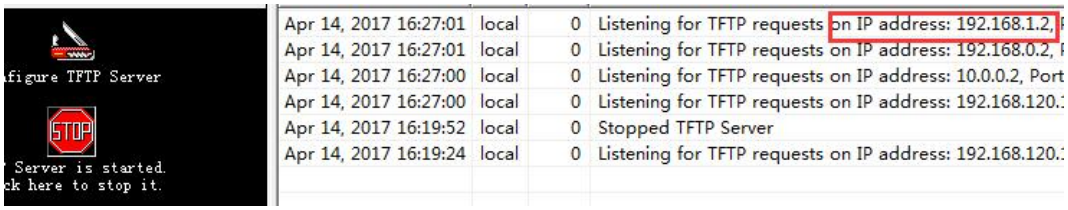


图 1.11.2

步骤 3 命令升级主控

（1）单独命令

Inspur#**copy tftp flash**

Source file name[]?*version.bin*

Remote-server ip address[]?*192.168.0.2*

Destination file name[INSPUR_MSU5020_11.0.1I_31509.bin]?**switch.bin**

（2）合并命令

Inspur#**copy tftp:***version.bin* **flash:switch.bin** *192.168.0.2*

步骤 4 升级线卡

Inspur#**copy tftp:***version.bin* **flash:ls_bin** *192.168.0.2*

注意：线卡版本与主控版本不一样

步骤 5 若交换机采用了双主控，则应将主控版本及线卡版本更新至备控

Inspur#**update msu switch.bin**

Inspur#**update msu ls_bin**

步骤 6 升级及同步线卡完成后，将交换机整机重启

Inspur#**redundancy reload shelf**

升级检查

步骤 1 交换机重启后，通过查看当前版本来确认是否升级成功

Inspur#**show version**

Internetwork Operating System Software

SWITCH Software, Version 4.1.3A Build 132777, RELEASE SOFTWARE

Compiled: 2024-10-15 16:56:24 by SYS, Image text-base: 0x108000

ROM: System Bootstrap, Version 0.1.9,hardware version:B

Serial num:0020077602685, ID num:0020077602685

System image file is "flash:/switch.bin"

步骤 2 查看线卡在线情况

Inspur#**show oir-information**

Slot 3 type SWITCH(present)

Monitor 模式升级

若升级失败导致无法进入系统，则可以在 **monitor** 模式下进行升级操作。进入 **monitor** 模式的方式见 1.3**monitor** 模式

步骤 1 查看主控的版本文件

monitor#**dir**

Directory of /:

1	tiger.blob	<FILE>	2084324	THU JAN 01 04:24:30 1970
2	1111	<FILE>	2626	WED JAN 07 06:38:02 1970
5	ifindex-config	<FILE>	232	SUN JAN 04 16:11:04 1970
0	startup-config	<FILE>	3656	SUN JAN 04 16:10:59 1970
4	config.db	<FILE>	133120	SUN JAN 04 16:11:02 1970
3	switch.bin	<FILE>	9007937	WED JAN 28 01:01:57 1970
6	123	<FILE>	2626	SUN JAN 11 18:59:08 1970
7	onu.zblob	<FILE>	550496	MON JAN 19 23:13:25 1970

free space 4767744

步骤 2 删除主控的版本文件

monitor#**format**　//该命令会清空内存的所有文件

monitor#**delete** *switch.bin*　//delete +删除的文件名，如 **switch.bin**

步骤 3 设置 **monitor** 模式下的管理 IP 地址

monitor#**ip address** *10.0.0.10 255.255.255.0*

步骤 4 电脑接在备控的 mgmt 接口，本地设置 ip 地址为 10.0.0.2，ping 管理地址，monitor 模式 下的管理地址 10.0.0.10

图 1.11.3

步骤 5 通过 tftp 把版本文件导入到主控。

参考前面的步骤通过 tftp 导入文件

步骤 6 重启主控

monitor# **reboot**

2 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**
- **privateVlan**
- **GVRP**

2.1 MAC 地址转发表

2.1.1 简介

以太网设备通过 **MAC** 地址转发规则实现快速转发。每台设备维护一个 **MAC** 地址转发表，记录 **MAC** 地址与接口的对应关系。所有入接口的报文都依据该表进行转发，这是实现二层报文快速转发的关键。**MAC** 地址转发表存储在设备缓存中，缓存容量决定了设备能够支持的 **MAC** 地址数量上限。

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**

MAC 地址的类型

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。如下图所示。

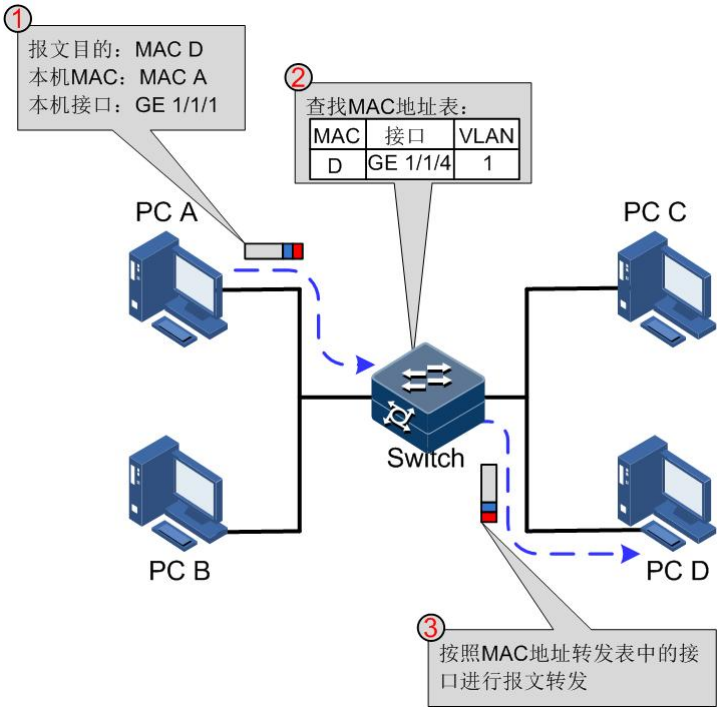


图 2.1.1 MAC 地址表转发示意图

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。

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。

2.1.2 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。

2.1.3 MAC 相关配置

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

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

配置静态 MAC 地址

请在设备上进行以下配置。

序号	命令	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config# [no] mac address-table static *mac-addr* vlan *vlan-id* interface *interface-id*	添加/删除一个静态 MAC 地址表项。 mac-addr 为 MAC 地址 ； vlan-id 为 VLAN 号，有效范围 1~4094 ； interface-id 为端口名称。

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。

配置黑洞 MAC 地址

请在设备上进行以下配置。

序号	命令	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#[no] mac address-table blackhole *mac-address* vlan *vlan-id*	配置/删除黑洞 MAC 地址。

配置 MAC 地址学习数目限制

请在设备上进行以下配置。

序号	命令	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#mac address-table dynamic maximum *<1-16448>*	配置全局动态 MAC 地址范围

配置 MAC 老化时间

请在设备上进行以下配置。

序号	命令	说明

序号	命令	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config# **mac address-table aging-time** {*0 / 10-1000000*}	配置 **MAC** 地址的老化时间。 0 表示 **MAC** 地址不老化 ； 10－1000000 以秒为单位的 **MAC** 地址老化时间。

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	命令	说明
1	Inspur#**show mac address-table**	查看 **MAC** 地址表项信息。
2	Inspur#**show mac address-table** { **static** | **dynamic** } [**vlan** *vlan-id*] [*interface-type interface-number*]	查看静态/动态 **MAC** 地址表项信息。
3	Inspur#**show mac address-table** *mac-address*	查看指定 **MAC** 地址表项信息。
4	Inspur#**show mac address-table blackhole**	查看黑洞 **MAC** 地址。
5	Inspur#**show mac address-table brief**	查看 **MAC** 地址表简单信息。
6	Inspur#**show mac address-table** [**vlan** *vlan-id*] [*interface-type interface-number*]	查看指定端口/**vlan** 的 **MAC** 地址表项信息。

维护

用户可以通过以下命令维护 MAC 地址转发表特性。

序号	命令	描述
1	Inspur# **clear mac address-table dynamic** [**address** *mac-addr* | **interface** *interface-id* | **vlan** *vlan-id*]	删除一个动态 **MAC** 地址表项。 dynamic 为动态学习的 **MAC** 地址 ； **mac-addr** 为 **MAC** 地址 ； **interface-id** 为端口名称 ； **vlan-id** 为 **VLAN** 号，范围 1-4094。

2.1.4 配置示例

组网需求

如下图所示，在 **Switch** A 上进行操作，在 GE 3/1 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。

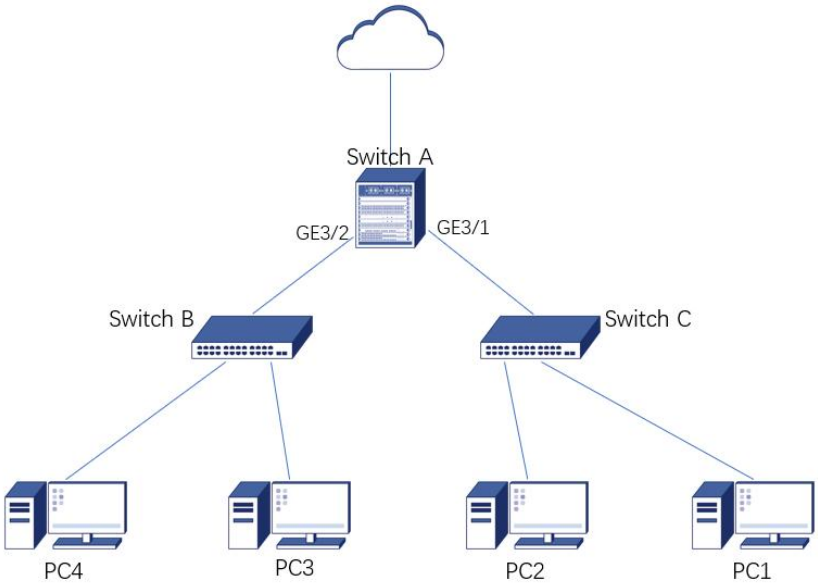


图 2.1.2**MAC** 应用组网示意图

配置步骤

1、创建 **VLAN** 10 并激活，将 GE 3/1 加入 **VLAN** 10。

```
Inspur#config
Inspur_config#vlan 10
Inspur_config#interface gigaEthernet 3/1
Inspur_config_g3/1#switchport mode access
Inspur_config_g3/1#switchport pvid 10
Inspur_config_g3/1#exit
```

2、在 GE 3/1 配置一条静态单播 **MAC** 地址 0001.0203.0405，所属 **VLAN** 10。

```
Inspur_config # mac address-table  static 0001.0203.0405 vlan 10 interface
gigaEthernet 3/1
```

3、配置 **MAC** 地址老化时间为 500s。

```
Inspur_config # mac address-table aging-time 500
```

检查结果

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

```
Inspur#show mac address-table
                  Mac Address Table (Total 1)
               ------------------------------------------

               Vlan    Mac Address      Type      Ports
               ----    -----------      ----      -----
                  10       0001.0203.0405    STATIC    g0/1
```

2.2 VLAN

2.2.1 简介

VLAN 概述

VLAN(Virtual Local Area Network)，即虚拟局域网，是一种通过将局域网内的设备逻辑地而不是物理地划分的交换网络。**IEEE** 于 1999 年颁布了用以标准化 **VLAN** 实现方案的 **IEEE** 802.1Q 协议标准草案。**VLAN** 技术允许将一个物理的 **LAN** 逻辑地划分成不同的广播域（**VLAN**），每一个 **VLAN** 都包含一组有着相同需求的设备，与物理上形成的 **LAN** 有着相同的属性，但由于它是逻辑地而不是物理地划分，所以同一个 **VLAN** 内的各个设备无须被放置在同一个物理空间，即，这些设备不一定属于同一个物理 **LAN** 网段，一个 **VLAN** 内部的广播和单播流量都不会转发到其他 **VLAN** 中，从而有助于控制流量、减少设备投资、简化网络管理、提高网络安全。

VLAN 划分

VLAN 划分有多种方式，例如基于接口、基于 **MAC** 地址、基于 **IP** 子网、基于协议划分等。

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 2-1。

表 2-1 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，则继续匹配基于 **IP** 子网 **VLAN**、基于接口 **VLAN**。

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。

基于协议划分 **VLAN**

基于协议划分 **VLAN** 是指根据数据帧所属的协议类型及封装格式对 **VLAN** 进行划分。

设备从接口接收到 **Untag** 报文后，会根据报文的协议域确定报文所属的 **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。

2.2.2 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**。

2.2.3VLAN 配置

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

功能	缺省值
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

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。

序号	命令	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**vlan** *vlan-id*	创建/进入 **VLAN**。 该命令也可用于批量创建 **VLAN**，**vlan-id** 使用逗号隔开，例如：(1,3,5,7) **Or** (1,3-5,7) **Or** (1-7)。
3	Inspur_config_vlan10#**name** *vlan-name*	配置 **VLAN** 名称。

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。

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。

序号	命令	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_g3/1#**switchport mode** { *access* | *trunk* }	配置接口模式为 **Access** 或 **Trunk**。

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。

序号	命令	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或聚合组配置模式。以下步骤以二层物理接口配置模式为例。
3	Inspur_config_g3/1#**switchport mode access** Inspur_config_g3/1#**switchport pvid** *vlan-id*	配置接口模式为 **Access**，并将 **Access** 接口加入 **VLAN**。

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。

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。

序号	命令	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_g3/1#**switchport mode trunk**	配置接口模式为 **Trunk**。
4	Inspur_config_g3/1#**switchport pvid** *vlan-id*	配置接口 **Native VLAN**。
5	Inspur_config_g3/1#**switchport trunk vlan-allowed** { **all** | [**add** | **remove**] *vlan-list* }	配置 **Trunk** 接口允许通过的 **VLAN**。
6	Inspur_config_g3/1#**switchport trunk vlan-untagged** { **all** | [**add** | **remove**] *vlan-list* }	配置 **Trunk** 接口可以去掉 **Tag** 的 **VLAN**。

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，对集群 **VLAN**、**GVRP** 动态 **VLAN** 等不生效。

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。

序号	命令	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**mac-vlan mac-address** *mac-addr* **vlan** *vlan-id* [priority] **[slot …]**	配置 **MAC** 地址与 **VLAN** 的关联
3	Inspur_config#**no mac-vlan mac-address** *mac-addr*	删除一个 **MAC VLAN** 表项
4	Inspur_config#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
5	Inspur_config_g3/1#[no] **switchport mac-vlan**	使能/关闭 **MAC-VLAN** 功能。

在端口模式为 **access** 时，若进来的报文通过 **MAC VLAN** 表项匹配到的 **VLAN** 不是端口的 **PVID**，报文会被丢弃。因此，若非需要，请勿将开启 **MAC VLAN** 功能的端口模式配置为 **access**。

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。

序号	命令	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**vlan** *vlan-id*	进入 **vlan** 配置模式。
3	Inspur_config_vlan10# **subnet {any |** *ip-addr mask* **} [slot …]**	配置一个 **Subnet VLAN** 表项及允许使用该表项的槽位。

序号	命令	说明
4	Inspur_config#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
5	Inspur_config_g3/1#**[no] switchport vlan-subnet enable**	在端口开启/关闭基于 **IP** 子网的 **VLAN** 功能。

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。

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。

序号	命令	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config# **protocol-vlan** *protocol_index* **frame-type { ETHERII | SNAP | LLC } ether-type** *etype-id*	添加一个协议模板。
3	Inspur_config#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
4	Inspur_config_g3/1# **switchport protocol-vlan** *protocol_index* **vlan** *vlan-id*	添加与协议模板的关联。

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	命令	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
6	Inspur#**show ip-subnet-vlan** { **all** | **vlan** *vlan-id* }	查看 **IP** 子网 **VLAN** 的配置信息。
7	Inspur#**show protocol-vlan all**	查看全部协议 **VLAN** 配置信息。
8	Inspur#**show protocol-vlan interface** *interface-type interface-number*	查看接口的协议 **VLAN** 配置信息。

2.2.4 配置示例

组网需求

如下图所示，**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；**PC 1** 和 **PC 2** 可以和 **PC 5** 通信。

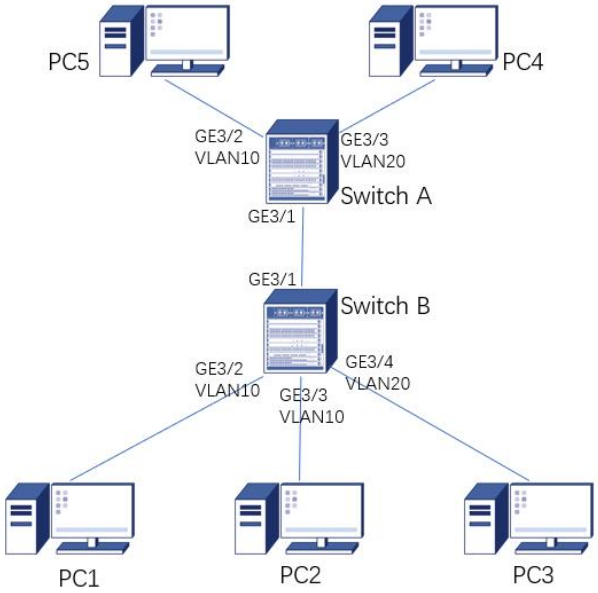


图 2.2.1 VLAN 和接口保护组网示意图

配置步骤

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# vlan 10,20
```

配置 Switch B。

```
Inspur#hostname SwitchB
SwitchB#config
SwitchB_config# vlan 10,20
```

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

```
SwitchB_config#interface gigaethernet 3/2
SwitchB_config_g3/2#switchport mode access
SwitchB_config_g3/2#switchport pvid 10
SwitchB_config_g3/2#exit
SwitchB_config#interface gigaethernet 3/3
```

```
SwitchB_config_g3/3#switchport mode access
SwitchB_config_g3/3#switchport pvid 10
SwitchB_config_g3/3#exit
SwitchB_config#interface gigaethernet 3/4
SwitchB_config_g3/4#switchport mode access
SwitchB_config_g3/4#switchport access vlan 20
SwitchB_config_g3/4#exit
SwitchB_config#interface gigaethernet 3/1
SwitchB_config_g3/1#switchport mode trunk
SwitchB_config_g3/1#switchport trunk vlan-allowed 10
SwitchB_config_g3/1#exit
```

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

```
SwitchA_config#interface gigaethernet 3/2
SwitchA_config_g3/2#switchport mode access
SwitchA_config_g3/2#switchport pvid 10
SwitchA_config_g3/2#exit
SwitchA_config #interface gigaethernet 3/3
SwitchA_config_g3/3#switchport mode trunk
SwitchA_config_g3/3#switchport trunk native vlan 20
SwitchA_config_g3/3#exit
SwitchA_config#interface gigaethernet 3/1
SwitchA_config_g3/1#switchport mode trunk
SwitchA_config_g3/1# switchport trunk vlan-allowed 10
```

检查结果

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

2.3 Private VLAN

2.3.1 简介

Private Vlan 解决了服务提供商在应用 **VLAN** 时所面临的问题：如果服务提供商给每一 个用户提供一个 **VLAN**，由于每一台设备最多支持 4094 个 **VLAN** 从而限制了服务提供商能 支持用户的总数量。

私有 VLAN 的类型和私有 VLAN 中端口的类型

私有 **VLAN(private vlan)**将一个 **VLAN** 的二层广播域划分成多个子域，每个子域都由一 个私有 **VLAN** 对组成：主 **VLAN(Primary VLAN)**和一个或若干个辅助 **VLAN(Secondary VLAN)**。一个私有 **VLAN** 域可以有多个私有 **VLAN** 对，每一个私有 **VLAN** 对代表一个子域。 在一个私有 **VLAN** 域中只有一个主 **VLAN**，所有的私有 **VLAN** 对共享同一个主 **VLAN**。每个 子域的辅助 **VLAN ID** 不同。

有一种类型的主 VLAN

主 **vlan(Primary VLAN)**：是一个与混杂端口相关联的 **VLAN**，**Private VLAN** 中只 能有一个 **Primary VLAN**，每个在 **Primary VLAN** 中的端口都是 **Primary VLAN** 的 成员。

有二种类型的辅助 VLAN

隔离 **VLAN(Isolated VLAN)**：同一个隔离 **VLAN** 中的端口不能互相进行二层通信。 一个私有 **VLAN** 域中只有一个隔离 **VLAN**。一个隔离 **vlan** 必须与一个 **Primary VLAN** 关联。

共用 **VLAN(Community VLAN)**：同一个共用 **VLAN** 中的端口可以互相进行二层通 信，但不能与其它共用 **VLAN** 中的端口进行二层通信。一个私有 **VLAN** 域中可以 有多个共用 **VLAN**。一个公共 **vlan** 必须与一个 **Primary VLAN** 相关联。

私有 VLAN 端口是如下类型的端口

混杂端口（**Promiscuous Port**）：属于主 **VLAN** 中的端口。可以与所有端口通讯， 包括同一个私有 **VLAN** 域中辅助 **VLAN** 的隔离端口和共用端口。

隔离端口**(Isolated Port)**：属于隔离 **VLAN** 中的主机端口**(Host Port)**。在同一个私 有 **VLAN** 域中，除了混杂端口外，隔离端口与其它的所有端口完全二层隔离，从 隔离端口收到的流量只能转发到混杂端口。

共用端口**(Community Port)**：属于共用 **VLAN** 中的主机端口**(Host Port)**。在一个私 有 **VLAN** 域中，同一个共用 **VLAN** 的共用端口可以互相进行二层通讯，也可以与 混杂端口进行二层通讯，不能与其它共用 **VLAN** 中的共用端口及隔离 VLAN 中的 隔离端口进行二层通讯。

私有 VLAN 对 VLAN TAG 中的字段的修改特性

此功能支持在 **VLAN** 的 **tag** 中修改 **VLAN ID** 和优先级字段，以及私有 **VLAN** 的出端口的报文是否带 **tag**。

2.3.2 配置准备

场景

隔离广播域：在数据中心网络中，可以将生产流量和测试流量分别配置在不同的 **Primary** 和 **Secondary VLAN** 中，从而隔离广播域，减少不必要的广播风暴。

增强安全性：在需要将某些服务器或设备与其他设备物理隔离的场景中，可以将这些设备配置在 **Isolated VLAN** 中，确保它们之间的通信不被其他网络段干扰或访问。

简化网络管理：通过将不同业务或部门流量分配到不同的 **Primary** 和 **Secondary VLAN** 中，可以简化网络管理和策略配置。

前提

一个私有 **VLAN** 对生效的条件如下：

1.具有主 **VLAN**。

2.具有辅助 **VLAN**。

3.辅助 **VLAN** 和主 **VLAN** 之间有关联。

4.主 **VLAN** 内有混杂端口。

2.3.3 相关配置

配置 Private VLAN

使用下面的命令来将 **VLAN** 配置成私有 **VLAN**

序号	命令	说明
1	Inspur_config#**vlan** *vlan-id*	进入 **VLAN** 模式进行配置
2	Inspur_config_vlan10#**private-vlan {primary|community|isolated}**	配置 **VLAN** 的私有 **VLAN** 属性
3	Inspur_config_vlan10#**no private-vlan {primary|community|isolated}**	清除 **VLAN** 的私有 **VLAN** 属性
4	Inspur#**show vlan private-vlan**	显示私有 **VLAN** 的配置信息

配置 Private VLAN 中的私有 VLAN 域的关联

使用下面的命令来关联私有 **VLAN** 中的主 **VLAN** 和辅助 **VLAN**

序号	命令	说明
1	Inspur_config#**vlan** *vlan-id*	进入主 **VLAN** 配置模式进行配置
2	Inspur_config_vlan10#**private-vlan association** {*svlist* | **add** *svlist* | **remove** *svlist*}	配置要关联的 **Secondary VLAN**
3	Inspur_config_vlan10#**no private-vlan association**	清除当前 **Primary VLAN** 与所有 **Secondary VLAN** 的关联

配置 Private VLAN 中的二层接口为私有 VLAN 的主机接口

使用下面的命令来配置 **Private VLAN** 中的二层接口为私有 **VLAN** 的主机接口

序号	命令	说明
1	Inspur_config#**Interface** *interface-type interface-name*	进入接口配置模式
2	Inspur_config_g3/1#**switchport mode private-vlan host**	配置二层接口为主机端口模式

序号	命令	说明
3	Inspur_config_g3/1#**no switchport mode**	清除二层接口的私有 **VLAN** 模式配置
4	Inspur_config_g3/1#**switchport private-vlan host-association** *p_vid s_vid*	关联二层主机接口与私有 **VLAN** 的关联
5	Inspur_config_g3/1#**no switchport private-vlan host-association**	清除二层主机接口与私有 **VLAN** 的关联

配置 Private VLAN 中的二层接口为私有 VLAN 的混杂接口

使用下面的命令来配置 **Private VLAN** 中的二层接口为私有 **VLAN** 的混杂接口

序号	命令	说明
1	Inspur_config#**Interface** *interface-type interface-name*	进入接口配置模式
2	Inspur_config_g3/1#**switchport mode private-vlan promiscuous**	配置二层接口为混杂端口模式
3	Inspur_config_g3/1#**no switchport mode**	清除二层接口的私有 **VLAN** 模式配置
4	Inspur_config_g3/1#**switchport private-vlan mapping** *p_vid{svlist | add svlist |* **remove** *svlist}*	关联二层混杂接口与私有 **VLAN** 的关联
5	Inspur_config_g3/1#**no switchport private-vlan mapping**	清除二层混杂接口与私有 **VLAN** 的关联

配置 Private VLAN 出端口报文中的相关字段修改

使用下面的命令来配置 **Private VLAN** 中出端口报文中的相关字段修改

序号	命令	说明
1	Inspur_config#**Interface** *interface-type interface-name*	进入接口配置模式
2	Inspur_config_g3/1#**switchport private-vlan tag-pvid** *vlan-id*	配置出端口报文 **tag** 中的 **vlan id** 字段
3	Inspur_config_g3/1#**switchport private-vlan tag-pri** *pri*	配置出端口报文 **tag** 中的 **priority** 字段
4	Inspur_config_g3/1#**[no] switchport private-vlan untagged**	配置出端口报文是否带 **tag**

Private VLAN 配置信息的显示

使用下面的命令来显示 **Private VLAN** 中的私有 **VLAN** 和二层接口的私有 **VLAN** 配置信息， 配置的模式为全局配置模式，接口配置模式和 **VLAN** 配置模式

序号	命令	说明
1	`Inspur#show vlan private-vlan`	显示私有 **VLAN** 的配置信息
2	`Inspur#show vlan private-vlan interface` *interface-type interface-name*	显示私有 **VLAN** 中的二层接口的 **VLAN** 配置信息

2.3.4 配置示例

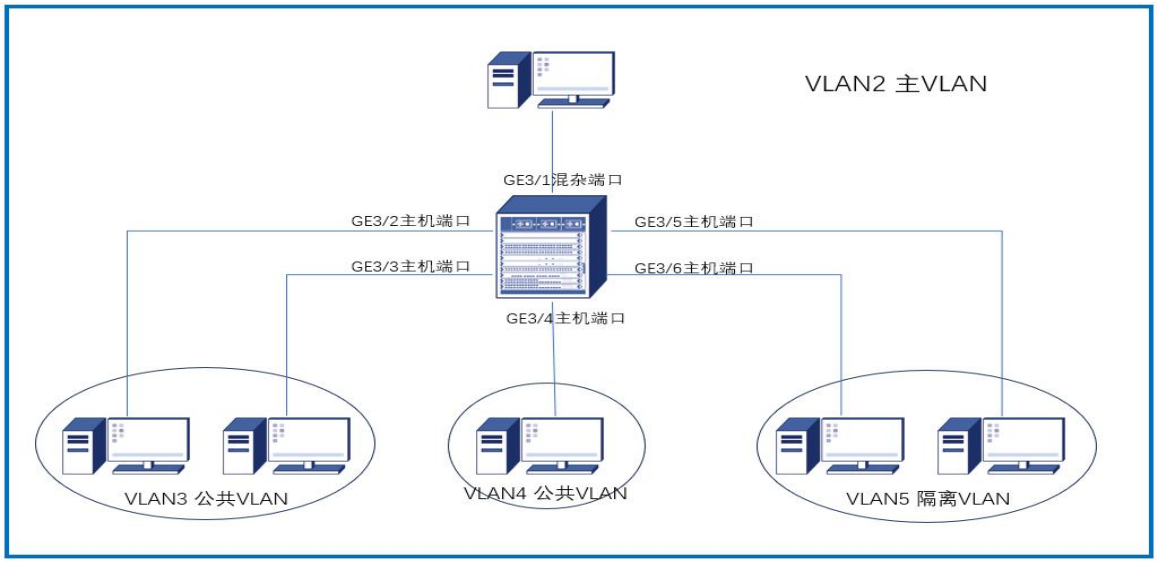


图 2.3.1Private VLAN 的典型配置图

通过一个典型的组网方式来说明 **Private VLAN** 的应用

如图 1 所示 **GE3/1** 为 **Primary VLAN 2** 下混杂端口，**GE3/2-GE3/6** 为主机端口，其中 **GE3/2**、**GE3/3** 为 Community VLAN 3 下的主机端口（公用端口），GE3/4 为 **Community VLAN 4** 下的主机端口（公用端口），**GE3/5**、**GE3/6** 为 **Isolated VLAN 5** 下的的主机端口（隔离端口）。

根据 **Private VLAN** 的概念，混杂端口 **GE3/1** 可以与该私有 **VLAN** 中的所有子 **VLAN** 域中的 主机接口互相进行二层通信，公用 **VLAN 3** 下的主机端口 **GE3/2**、**GE3/3** 可以互相二层通信，但不能与其他辅助 VLAN 中的主机端口进行二层通信，包括不同组的公用 **VLAN 4**，隔离 **VLAN 5** 下 的隔离端口 **GE3/5**、**GE3/6** 互相不能进行二层通信，它们只能与整个私有 **VLAN** 中的混杂端口 **GE3/1** 进行二层通信。

具体在交换机下的命令配置如下：

```
Inspur_config#interface GigaEthernet3/1
Inspur_config_g3/1#switchport mode private-vlan promiscuous
Inspur_config_g3/1#switchport private-vlan mapping 2 3-5
Inspur_config_g3/1#switchport pvid 2

Inspur_config#interface GigaEthernet3/2
Inspur_config_g3/2#switchport mode private-vlan host
Inspur_config_g3/2#switchport private-vlan host-association 2 3
Inspur_config_g3/2#switchport pvid 3
```

```
Inspur_config#interface GigaEthernet3/3
Inspur_config_g3/3#switchport mode private-vlan host
Inspur_config_g3/3#switchport private-vlan host-association 2 3
Inspur_config_g3/3#switchport pvid 3

Inspur_config#interface GigaEthernet3/4
Inspur_config_g3/4#switchport mode private-vlan host
Inspur_config_g3/4#switchport private-vlan host-association 2 4
Inspur_config_g3/4#switchport pvid 4

Inspur_config#interface GigaEthernet3/5
Inspur_config_g3/5#switchport mode private-vlan host
Inspur_config_g3/5#switchport private-vlan host-association 2 5
Inspur_config_g3/5#switchport pvid 5

Inspur_config#interface GigaEthernet3/6
Inspur_config_g3/6#switchport mode private-vlan host
Inspur_config_g3/6#switchport private-vlan host-association 2 5
Inspur_config_g3/6#switchport pvid 5

Inspur_config#vlan 2
Inspur_config_vlan2#private-vlan primary
Inspur_config_vlan2#private-vlan association 3-5

Inspur_config#vlan 3
Inspur_config_vlan3#private-vlan community

Inspur_config#vlan 4
Inspur_config_vlan4#private-vlan community

Inspur_config#vlan 5
Inspur_config_vlan5#private-vlan isolated

Inspur_config#show vlan private-vlan
```

2.4 GVRP

2.4.1 简介

GVRP （ **GARP VLAN Registration Protocol** ） 是 基 于 **GARP** （ **Generic Attribute Registration Protocol**）协议的一种具体的应用。它利用了 GARP 协议的工作机制维 护交换机中的 VLAN 信息，所有支持 **GVRP** 特性的交换机能够接收来自其他交换机 的 **VLAN** 注册信息，并动态更新本地的 **VLAN** 注册信息，包括当前的 **VLAN** 成员， 以及这些 **VLAN** 成员可以通过哪个端口到达等信息。同时所有支持 **GVRP** 特性的交 换机能够将本地的 **VLAN** 注册信息（包括动态 **VLAN** 信息和静态配置的 **VLAN** 信息） 向其他交换机传播，以达到同一交换网内所有支持 **GVRP** 特性的设备的 **VLAN** 信息 一致。

2.4.2 配置准备

场景

GVRP 是一种动态 **VLAN** 管理协议，主要用于简化 **VLAN** 配置和管理。它的使用场景主要集中在需要动态、灵活管理 **VLAN** 的网络环境中。以下是 **GVRP** 的主要使用场景：

1、大型企业网络

在大型企业网络中，通常需要配置大量的 **VLAN** 来隔离不同部门或业务流量。手动配置 **VLAN** 会非常繁琐且容易出错。**GVRP** 可以自动注册和传播 **VLAN** 信息，减少管理员的工作量。

2、服务提供商网络

服务提供商需要为不同客户提供独立的 **VLAN** 服务。**GVRP** 可以帮助动态分配和管理 **VLAN**，简化客户网络的配置。

3、多交换机环境

在由多台交换机组成的网络中，手动配置 **VLAN** 需要确保每台交换机的配置一致。**GVRP** 可以自动同步 **VLAN** 信息，避免配置不一致的问题。

4、简化网络管理

对于需要减少人工干预的网络环境，**GVRP** 可以显著降低管理复杂度，尤其是在 **VLAN** 数量较多或网络规模较大的情况下。

2.4.3 相关配置

全局开启/关闭 GVRP

在全局配置模式下进行下列配置：

序号	命令	说明
1	`Inspur_config# [no] gvrp`	开启/关闭全局 **GVRP**。

缺省不开启 GVRP 功能。

配置动态 VLAN 仅在注册的端口生效

在全局配置模式下进行下列配置：

序号	命令	说明
1	`Inspur_config# [no] gvrp dynamic-vlan-pruning`	使能/禁止动态 **VLAN** 仅在注册的端口生效。

开启该功能后，动态 **VLAN** 仅仅会在注册了该动态 **VLAN** 的端口生效，即如果一个 端口没有注册某个动态 **VLAN**，即便它是 **trunk** 口且允许该 **VLAN** 通过，这个端口也 不会归属于该动态 **VLAN**。

缺省不开启该功能。

端口开启/关闭 GVRP

在端口配置模式下进行下列配置：

序号	命令	说明

序号	命令	说明
1	Inspur_config#**Interface** *interface-type interface-name*	进入接口配置模式
2	Inspur_config# **[no] gvrp**	开启/关闭端口 **GVRP**。

在开启端口 **GVRP** 之前，请先开启全局 GVRP 功能，否则端口 **GVRP** 功能并不能 真正工作。并且只有在 **Trunk** 端口上才能配置 **GVRP** 功能，否则端口 **GVRP** 功能 也不会工作。

缺省状态下，端口 **GVRP** 功能开启。

GVRP 的监控与维护

请在管理态下进行下列操作：

序号	命令	说明
1	Inspur# **show gvrp statistics** [**interface** *interface-type interface-number*]	显示 **GVRP** 统计信息。
2	Inspur# **show gvrp status**	显示 **GVRP** 全局状态信息。
3	Inspur#**[no] debug gvrp { packet | event }**	开启/关闭 **GVRP** 数据包或事件调试开关。

2.4.4 配置示例

网络连接如图，为使 **Switch A** 和 **Switch B** 的 **VLAN** 配置信息达到一致，可在 **Switch A** 和 **Switch B** 上开启 **GVRP**，配置如下：

图 2.4.1

(1) 配置 Switch A 的与 Switch B 相连的端口为 Trunk：

SwitchA_config_g3/1# switchport mode trunk

(2) 开启 Switch A 的全局 GVRP

SwitchA_config#gvrp

(3) 开启 Switch A 端口的 GVRP

SwitchA_config_g3/1#gvrp

(4) 在 Switch A 上配置 VLAN 10，VLAN 20 和 VLAN 30

SwitchA_config#vlan 10,20,30

(5) 配置 Switch B 的与 Switch A 相连的端口为 Trunk

SwitchB_config_g3/1# switchport mode trunk

(6) 开启 Switch B 的全局 GVRP

SwitchB_config#gvrp

(7) 开启 Switch B 端口的 GVRP

SwitchB_config_g3/1#gvrp

(8) 在 Switch B 上配置 VLAN 40，VLAN 50 和 VLAN 60

SwitchB_config#vlan 40,50,60

3 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
- PIM-SM
- PIM-DM
- IGMP Snooping
- IGMP Proxy
- MLD Snooping

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。

组播方式传输如下图所示。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**。

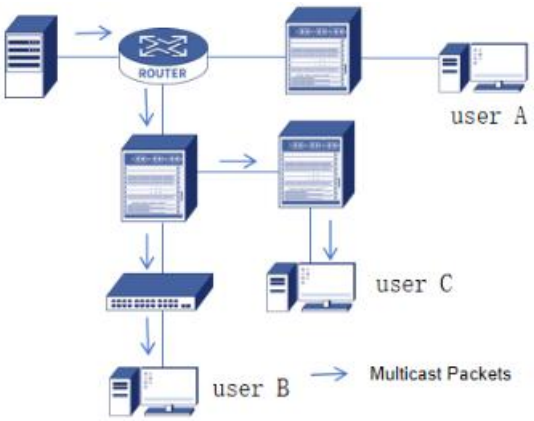


图 3.1.1 组播方式传输信息示意图

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，映射关系如下图所示。

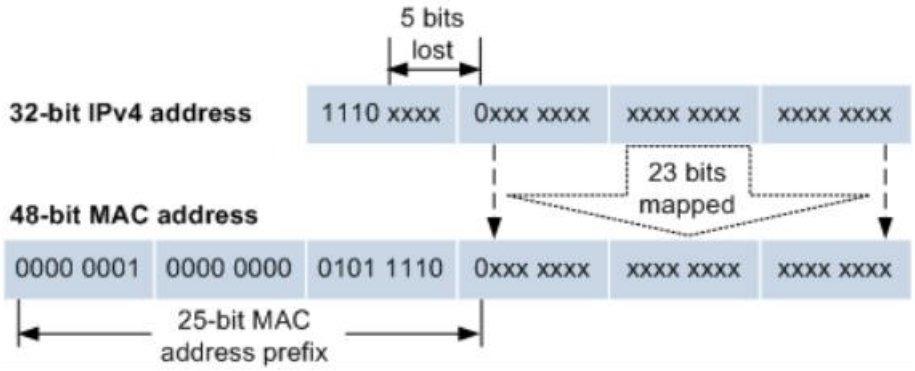


图 3.1.2 IPv4 组播地址和组播 MAC 地址的映射关系

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 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。

3.1 IGMP 基础配置

3.1.1 简介

IGMP 是一类针对多播组成员管理的协议，**IGMP** 即 **Internet Group Management Protocol** 的缩写。**IGMP** 是一种不对称的协议，它包括主机端和交换机端两方面的内容：主机端的协议规定了作为多播组成员的主机如何向交换机端 报告自身属于不同的多播组的身份，以及主机如何响应交换机端发送的 **Query** 报文的过程；交换机端的协议规定了支持 **IGMP** 的交换机端如何获得本地网络内主机的多播组成员身份，如何根据主机的 **Report** 报文更改交换机端保存的多播组成员信息。

通过 **IGMP** 交换机端协议在我们交换机中的实现，可以向交换机中的多播路由协议提供 当前网络内多播组的成员存在情况，以决定是否需要转发多播报文。综上所述，为使我们的交换机支持 **IP** 报文的多播过程，需要实现多播路由协议和 **IGMP** 交换机端协议。

3.1.2 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。

3.1.3 IGMP 配置

更改 IGMP 当前运行的版本

在端口配置态下进行以下配置。

序号	配置	说明
1	`Inspur_config_v1# ip igmp version` *version_number*	更改当前端口正在运行的 **IGMP** 的版本。

配置 IGMP 查询间隔

无论当前运行的 **IGMP** 协议的版本号为多少，多播交换机在开启了 **IGMP** 端功能的端口上都会每隔一段时间发送一次 **IGMP General Query** 报文，发送地址是 224.0.0.1，目的是希望获得 **IGMP** 主机响应的 **Report** 报文，从而获得此端口连接的网络上 **IGMP** 主机分别属于哪些多播组的信息。这个 **General Query** 报文发送间隔时间被称为 **IGMP** 查询间隔（**IGMP Query Interval**）。

序号	配置	说明
1	`Inspur_config_v1#ip igmp query-interval` *time*	更改当前端口的 **IGMP** 查询间隔大小，单位为 秒。
2	`Inspur_config_v1#no ip igmp query-interval`	恢复默认值。

配置 IGMP Querier 间隔

在正常运行情况下，同一网络内只存在一个 **querier**，即只有一个交换机在发送 **IGMP Query** 报文。对于 **IGMP** 协议版本 1，不存在 **querier** 选取的问题，因为 **IGMP** 版本 1 中哪台交换机能发送 **IGMP Query** 报文是由多播路由协议指定的。

对 **IGMP** 端协议版本 2 和版本 3 来说，采用同样的 **querier** 选取机制：即 **IP** 地址最小的交换机为此网络中的 **querier**，对于非 **querier** 来说，需要保存一个时钟，记录 **querier** 存在的时间，当此时钟超时后，非 **querier** 变为 **querier**，开始向外发送 **IGMP Query** 报文，直到此交换机收到 IP 地址比自己小的交换机发出的 **IGMP Query** 报文并再次变为非 **querier**。

在端口配置态下进行以下配置。

序号	配置	说明
1	Inspur_config_v1# **ip igmp querier-timeout** *time*	配置其他 **querier** 存在的时间间隔，单位为秒。
2	Inspur_config_v1#**no ip igmp querier-timeout**	恢复默认值。

配置 IGMP 最大响应时间

对 **IGMP** 端协议版本 2 和版本 3 而言，在发送 **IGMP General Query** 报文时，在 **IGMP** 报文中有专门的数据域指明了 **IGMP** 主机的最大响应时间，即 **IGMP** 主机必须在收到 **IGMP General Query** 报文后的最大响应时间间隔内发送对此 **General Query** 报文的响应报文。

IGMP 最大响应时间必须小于 **IGMP** 查询间隔，在使用此配置命令时，如果最大响应时间的值大于查询间隔 **(query-interval)** 时，系统会将最大响应时间的值自动调整为 **(query-interval - 1)** 秒。

在端口配置态下进行以下配置。

序号	配置	说明
1	Inspur_config_v1#**ip igmp query-max-response-time** *time*	配置 **IGMP** 最大响应时间，单位为秒。
2	Inspur_config_v1#**no ip igmp query-max-response-time**	恢复默认值。

配置 IGMP 最后一个组成员查询间隔

对 **IGMP** 端协议版本 2 和版本 3 而言，当发送针对某个特定多播组的 **Group Specific Query** 报文时，将使用最后一个组成员查询间隔作为 **IGMP Query** 报文中的主机 最大响应时间，即 **IGMP** 主机必须在收到 **Group Specific Query** 报文后的最后一个组成 员查询间隔内发送对此 **Query** 报文的响应报文。如果 **IGMP** 主机通过查询本身的状态发现不需要响应此 **Query** 报文，则在此时间间隔后过去后仍然不发送响应报文，则多播交 换机会对已经保存的多播组成员信息进行相应的更新。如果此时间间隔设置得过大，则 会造成 **IGMP** 主机多播组成员身份变化的延迟，如果此时间间隔设置得过小，又会造成 网络上 **IGMP** 报文的流量过大。

在端口配置态下进行以下配置。

序号	配置	说明
1	Inspur_config_v1#**ip igmp last-member-query-interval** *time*	配置 **IGMP** 最后一个组成员查询间隔，单位为毫秒。

IGMP 静态配置

在我们交换机对 **IGMP** 协议的实现中，除了协议规定的功能外，我们还支持端 口上的静态多播组配置。所谓“静态”是与 **IGMP** 主机端报告的“动态”信息相区别，对于 **IGMP** 主机来说，它的多播组成员关系可能是变化的，假设当前它只属于多播组 **group1**，希望接收发往多播组 **group1** 的多播报文；但经过一段时间后它可能又属于多播组 **group2**，还希望接收发往多播组 **group2** 的多播报文；而再经过一段时间之后，此 **IGMP** 主机可能不再属于任何一个多播组，所以说主机报告的多播组归属信息是动态变化的。

与上述“动态多播组”不同，某端口如果静态配置了属于某一个多播组，则除非使用 **no** 命令取消这种配置，多播协议将认为此端口始终需要接收发往这个多播组的多播报文。另外，为了提供和 **IGMP** 协议版本 3 更好的兼容，静态配置的多播组可以指定希望 接收来自哪些源地址的多播报文，即增加了多播报文接收的 **source-filter** 功能。可以在端口配置态下通过以下命令设置该端口的静态多播组：

在端口配置态下进行以下配置。

序号	配置	说明
1	Inspur_config_v1# **ip igmp static-group** { * | *group-address*} {**include** *source-address* / *<cr>* }	配置该端口下的静态多播组属性。

配置 IGMP Immediate-leave 列表

如果交换机某端口上已经启动了 **IGMP** 版本 2 且在此端口所连接的网络上仅存在一个 **IGMP** 主机，则可以通过配置 **IGMP Immediate-leave** 列表实现 IGMP 主机的“**Immediate Leave**”功能。根据 **IGMP** 版本 2 的规定，当某个主机要离开特定的多播组时，该主机将 向所有的多播交换机发送 **Leave** 报文，而多播交换机将发送 **Group Specific** 报文以确认 此端口上是否已经不再有主机需要接受发向这个多播组的多播报文。而如果配置了 “**Immediate Leave**”功能，则可以避免 **IGMP** 主机与多播交换机之间的报文交互，也可以 避免多播交换机维护的多播组成员身份变化的延迟。

因为在全局配置态和端口配置态下都能配置此条命令，但全局配置态下配置的此条命令的优先级要高于在端口配置态下配置的命令，如果先在全局配置态下配置了此命令，则后来在端口配置态下配置的命令将被忽略；如果先在端口配置态下配置了此条命令，则后来在全局配置态下配置的命令将删除原来在端口配置态下配置的命令。

请在设备上进行以下配置。

序号	配置	说明
1	Inspur_config#**ip access-list standard** *list-name*	创建名字为 **list-name** 的 **IP** 标准访问列表。
2	Inspur_config_std#**permit** *source-address*	在 **IP** 标准访问列表的配置模式下配置我们希 望实现“立即离开”功能的 **IGMP** 主机的 **IP** 地址。
3	Inspur_config#**int vlan** *1*	进入三层端口配置态
4	Inspur_config_v1# **ip igmp immediate-leave group-list** *list-name*	配置能实现“立即离开多播组”功能的 IGMP 主机的访问列表。

因为 **IGMP** 协议版本 1 和版本 3 对 **leave** 报文的处理流程和 **IGMP** 版本 2 的处理流程存在很大差异，所以上述配置命令对 **IGMP** 协议版本 1 和版本 3 无效。

Igmp 监控与维护

序号	配置	说明

1	Inspur#**show ip igmp groups**	显示 **IGMP** 缓存中多播组的信息。
2	Inspur#**show ip igmp interface** *type_number*	显示端口上 **IGMP** 的配置信息。

3.1.4 配置示例

Igmp 配置示例

图 3.1.3 igmp 组网图

步骤一：配置地址和 **vlan**

步骤二：配置 **igmp**

Inspur_config#**int vlan 10**

Inspur_config_v10#**ip igmp enable**

Inspur_config_v10#**ip igmp version 2**

检查配置

显示 **IGMP** 缓存中多播组的信息。

Inspur_config#**show ip igmp interface**

VLAN10 line protocol is up

Internet address is 192.168.10.1

Current IGMP router version is 2

Router plays role of querier on the interface now

IGMP is enable on the interface

IGMP query-interval is 60 seconds

IGMP max query response time is 10 seconds

IGMP Last member query response time is 1000 milliseconds

IGMP group expire time is 130 sec

IGMP querier timeout is 125 seconds

Multicast routing is enabled on the interface

显示端口上 IGMP 的配置信息。

Inspur_config#**show ip igmp groups**

Total igmp group number: 2

interface: VLAN10 : igmp group number: 2

Interface	Group address	Uptime	Expires	Last Reporter	Flags
VLAN10	239.255.255.250	00:00:00	00:02:10	192.168.10.10	R
VLAN10	224.0.0.252	00:00:03	00:02:07	192.168.10.10	R

3.2 PIM-DM

3.2.1 简介

PIM-DM（**Protocol Independent Multicast Dense Mode**）是一种密集模式的多播路由协议，缺省认为当组播源开始发送组播数据时，域内所有的网络节点都需要接收该数据。因而，**PIM-DM** 采用扩散-剪枝的方式进行组播数据包的转发。组播源开始发送数据时，沿路交换机向朝着源的 **RPF** 接口之外的所有 **PIM** 激活接口转发组播数据包。这样，**PIM-DM** 域中所有网络节点都会收到这些组播数据包。为了完成组播转发，沿路的交换机需要为组 **G** 和它的源 **S** 创建相应的组播路由项 **(S,G)**。**(S,G)**路由项包括组播源地址、组播组地址、入接口、出接口列表、定时器和标志等。

如果网络中某区域没有组播组成员，**PIM-DM** 协议会发送剪枝消息，将通往该区域的转发接口剪枝，并且建立剪枝状态。剪枝状态对应着超时定时器。当定时器超时时，剪枝状态又重新变为转发状态，组播数据得以再次沿着这些分支流下。另外，剪枝状态包含组播源和组播组的信息。当剪枝区域内出现了组播组成员时，为了减少反应时间，协议不必等待上游剪枝状态超时，而是主动向上游发送嫁接报文，以使剪枝状态变为转发状态。

只要源 **S** 仍然发送信息到 **G** 组，第一跳交换机就会周期性地向下面的初始广播树发送（**S**,**G**）状态刷新信息，以完成刷新。**PIM-DM** 的状态刷新机制，可以刷新下游的状态，使广播树分支的剪枝不会超时。

PIM-DM 在多路访问网络中，除了涉及 **DR** 的选举外，还引入了以下机制：使用断言机制来选举唯一的转发者以防向同一网段重复转发组播数据包；使用加入/剪枝抑制机制来减少冗余的加入/剪枝消息；使用剪枝否决机制来否决不应该的剪枝行为。

在 **PIM-DM** 域中，运行 **PIM-DM** 协议的交换机周期性的发送 **Hello** 消息，用以发现邻接的 **PIM** 交换机，进行叶子网络、叶子交换机的判断，并且负责在多路访问网络中进行指定交换机（**DR**）的选举。

为了适用于 **IGMPv1**，**PIM-DM** 负责进行 **DR** 的选取。当端口上所有 **PIM** 邻居都支持 **DRPriority** 时，选择优先级最高的成为 **DR**。如果优先级相同，则选择具有最大端口 **IP** 值的交换机为 **DR**；如果有交换机在 **hello** 报文中没有通告它的优先权，有多个交换机存在此情况，则选择端口 **IP** 值最高的交换机为 **DR**。

3.2.2 配置准备

场景

通过配置 **PIM-DM**，可以实现组播路由与数据转发。

3.2.3 PIM-DM 配置

调整定时器

路由协议使用几个计时器来判断发送 **hello** 报文、状态刷新控制包报文的频率 **Hello** 报文发送间隔时间的长短影响到邻居关系是否能正确建立。要调整计时器，在交换机 **vlan** 端口配置模式中使用如下命令：

在端口配置态下进行以下配置。

序号	配置	说明
1	Inspur_config_v1#**ip pim-dm hello-interval** *value*	经过多长时间（单位：秒）从端口向邻居发送 **hello** 报文。范围 1～65535，缺省值 20 秒。
2	Inspur_config_v1#**ip pim-dm state-refresh origination-interval** *value*	对于与源直连的第一跳交换机，是周期性发送状态刷新报文的间隔，仅仅对上游端口进行的配置生效；对于后 续交换机，是端口允许接收并处理状态刷新报文的时间 间隔。范围 1～65535， 缺省值 60 秒。

配置状态刷新

在管理模式，缺省情况下允许运行转发 **PIM** 密集模式状态刷新控制消息。端口配置态的配置命令，对于与源直连的第一跳交换机，是周期性发送状态刷新报文的间隔，此时仅仅对上游端口进行的配置生效；对于后续交换机，是端口允许接收并处理状态刷新报文的时间间隔。

在端口配置态下进行以下配置。

序号	配置	说明
1	Inspur_config_v1#**ip pim-dm state-refresh origination-interva l** *value*	在端口上收发状态刷新报文的时间间隔。
2	Inspur_config_v1#**no ip pim-dm state-refresh disable**	允许在端口上收发状态刷新报文。

配置过滤列表

PIM-DM 在缺省情况下没有设置过滤列表，包括邻居过滤列表以及组播边界过滤列表，都是在端口配置态下进行配置。

如果需要禁止某台交换机或者某个网段的交换机加入 **PIM-DM** 协商，就需要配置邻居过滤列表。为了禁止或者允许某些组通过本 **region**，就需要设置边界组过滤列表。

请在全局配置模式进行以下配置。

序号	配置	说明
1	Inspur_config#**ip access-list standard** *list-name*	创建名字为 **list-name** 的 **IP** 标准访问列表。
2	Inspur_config_std# **permit** *source-address*	在 **IP** 标准访问列表的配置模式下配置希望那些地址加入 **PIM-DM** 协商。

3	Inspur_config#**int vlan** *vlan_id*	进入三层端口配置态。
4	Inspur_config_v1#**ip pim-dm neighbor-filter** *access-list name*	配置邻居过滤列表。
5	Inspur_config_v1#**ip multicast boundary** *access-list name*	配置组过滤列表。

设置 DR 优先级

进行 **DR** 的选取，以便能适用于 **IGMPv1**。缺省情况下，交换机 **DR** 优先级为 1。当端口上所有 **PIM** 邻居都支持 **DR Priority** 时，选择优先级最高的成为 **DR**。如果优先级相同， 则选择具有最大端口 **IP** 值的交换机为 **DR**；如果有交换机在 **hello** 报文中没有通告它的优先权，有多个交换机存在此情况，则选择端口 **IP** 值最高的交换机为 **DR**。

在端口配置态下进行进行以下配置。

序号	配置	说明
1	Inspur_config_v1#**ip pim-dm dr-priority** *value*	在指定端口设置本地交换机 **DR** 优先级。

清除(S,G)信息

正常情况下，可能需要清除本地**MRT** 中的**(S,G)**表项或者清除通过**(S,G)**表项转发组播报文数的统计值。在全局配置模式下使用如下命令：

请在接口配置下进行以下配置。

序号	配置	说明
1	Inspur_config_v1#**clear ip mroute pim-dm** {* | *group* [source]}	清除本地 **MRT** 中的**(S,G)**表项，这个操作将删 除本地多播路由表中的全部或者部分表项，并可能影响正常的多播报文转发，本命令只能删 除上游端口是由 **PIM-DM** 多播路由协议创建的 **(S,G)**条目。

PIM-SM 监控与维护

序号	配置	说明
1	Inspur#**show ip pim-dm interface**	显示 **pim-dm** 端口信息
2	Inspur#**show ip pim-dm neighbor**	显示 **pim-dm** 邻居信息
3	Inspur#**show ip pim-dm sg-info**	显示 **pim-dm**（**S,G**）表项信息

3.2.4 pim-dm 配置示例

在以下例子中，要求通过 **pim-dm** 协议实现组播通信。

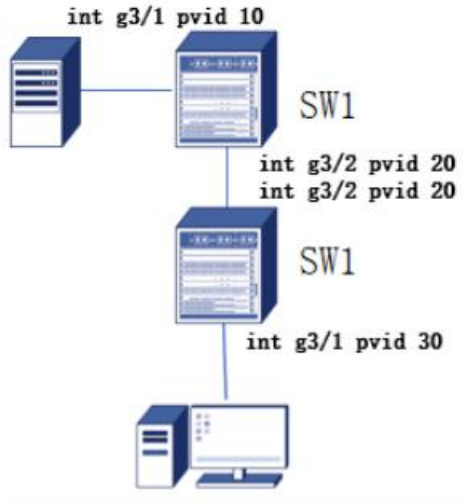


图 3.2.1 pim-dm 组网图

配置：

步骤 1：配置好 **vlan** 路由等，使组成员能够 **ping** 通服务器。

步骤 2：交换机开启 **pim-dm** 功能。

SW1：

Inspur#**config**

Inspur_config#**ip multicast-routing**

Inspur_config#**interface vlan 10**

Inspur_config_v10#**ip pim-dm**

Inspur_config_v10#**int vlan 20**

Inspur_config_v20#**ip pim-dm**

SW2：

Inspur#**config**

Inspur_config#**ip multicast-routing**

Inspur_config#**interface vlan *20***

Inspur_config_v20#**ip pim-dm**

步骤 3:**SW2** 开启 **igmp** 功能

Inspur_config#**interface vlan *30***

Inspur_config_v30#**ip igmp enable**

Inspur_config_v30#**ip igmp version *2***

pim-dm 监控

显示接口信息

Inspur#**show ip pim-dm interface**

PIM-DM Interface Table

Address	Interface	nbr_cnt	Intvl	Dr
10.10.10.1	v10	0	30	0.0.0.0

显示（**S**,**G**）表项信息

Inspur#show ip pim-dm sg-info

3.3 pim-sm

3.3.1 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。

3.3.2 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。

3.3.3 pim-sm 配置

启动/关闭全局组播

请在全局配置模式下进行以下配置。

序号	配置	说明
1	`Inspur_config#ip multicast-routing`	开启全局组播。
2	`Inspur_config#no ip multicast-routing`	关闭全局组播。

启动/关闭 pim-sm 进程

在全局使能了 **multicast-routing** 功能之后，还需要配置支持 **pim-sm** 的接口，才能在对应端口收发 **pim-sm** 协议消息。对于每一个三层端口，组播协议对端口具有独占性。也就是如果该端口上使能了其它组播协议，则不能再配置 **pim-sm**。

请在接口配置模式下进行以下配置。

序号	配置	说明
1	`Inspur_config_v10#ip pim-sm`	启动 **pim-sm** 进程。

2	Inspur_config_v10#**no ip pim-sm**	关闭 **pim-sm** 进程。

配置邻居过滤列表

pim-sm 在工作时也需要维护邻居关系，**pim-sm** 通过 **Hello** 消息来完成邻居的检测和相关参数的协商。交换机在使能了 **pim-sm** 功能的接口上周期性发送地的向所有 **pim** 交换机（224.0.0.13）以组播方式发送 **pim-sm hello** 报文，收到 **hello** 消息并且参数一致则建立邻居关系。如果一个交换机没有发送 **Hello** 消息却收到了 **Hello** 消息，则此交换机认为邻居存在，而对方如果没有收到 **hello** 报文，则认为邻居不存在。

可以在对应端口配置邻居过滤列表，对收到的 **hello** 报文进行邻居过滤检查。删除邻居过滤列表或者解禁刚才被否决的邻居，则需要等到下一个 **hello** 周期，才能获知邻居信息

请在设备上进行以下配置。

序号	配置	说明
1	Inspur_config_v10#**ip pim-sm nbr-filter** *nbr_permit*	配置 **pim-sm** 标准访问控制列表。
2	Inspur_config_v10#**no ip pim-sm nbr-filter** *nbr_permit*	关闭 **pim-sm** 标准访问控制列表。

RP 优先级

请在接口配置模式下进行以下配置。

序号	配置	说明
1	Inspur_config_v10#**ip pim-sm dr-pri** *value*	配置 **RP** 优先级。
2	Inspur_config_v10#**no ip pim-sm dr-pri**	恢复 **RP** 优先级默认值。

配置候选 DR

请在全局配置模式下进行以下配置。

序号	配置	说明
1	Inspur_config#**router pim-sm**	进入 **pim-sm** 视图。
2	Inspur_config_ps#**crp vlan** *vlan_id*	配置 **CRP** 地址。
3	Inspur_config_ps#**crp vlan** *vlan_id* **pri** *vlaue*	配置 **CRP** 优先级
4	Inspur_config_ps#**no crp vlan** *vlan_id*	取消 **CRP** 候选。

配置候选 BSR

请在全局配置模式下进行以下配置。

序号	配置	说明
1	Inspur_config#**router pim-sm**	进入 **pim-sm** 视图。
2	Inspur_config_ps#**cbsr vlan** *vlan_id* **hash-mask** *length* **priority** *pri_value*	配置候选 **BSR**，**length** 为 **hash** 长度，**pri_value** 为优先级。
3	Inspur_config_ps#**no cbsr vlan** *vlan_id*	取消 **CRP** 候选。

配置静态 RP

请在全局配置模式下进行以下配置。

序号	配置	说明
1	Inspur_config#**router pim-sm**	进入 **pim-sm** 视图。
2	Inspur_config_ps#**static-rp** *A.B.C.D*	配置候选静态 **RP**。
3	Inspur_config_ps#**no static-rp** *A.B.C.D*	取消配置 **RP**。

配置 SPT 切换阀值

交换机在数据转发时需要判断是否从 **RPT**(共享树)切换到 **SPT**(源树)，这个判断的依据就是 **SPT** 切换阀值(**spt-threshold**)，默认情况下接收端侧收到第一个数据报文后，就发生 **SPT** 切换。我们可以设置 **RPT** 到 **SPT** 切换的阀值，单位是 **KB/s**。一般情况下的处理是从 **RPT** 切换到 **SPT** 以后，不再进行回退操作。

请在全局配置模式进行以下配置。

序号	配置	说明
1	Inspur_config#**router pim-sm**	进入 **pim-sm** 视图。
2	Inspur_config_ps#**spt-threshold** *value*	配置 **SPT** 切换阈值。
3	Inspur_config_ps#**no spt-threshold** *value*	取消 **SPT** 切换阈值。

pim-sm 监控与维护

序号	配置	说明
1	Inspur#**show ip pim-sm interface**	显示端口 **pim-sm** 信息。
2	Inspur#**show ip pim-sm neighbor**	显示邻居信息。
3	Inspur#**show ip pim-sm bsr-router**	查看 **CRP/CBSR** 情况和运行状态。
4	Inspur#**show ip mroute pim-sm** [*group-address*] [*source-address*]	显示 **pim-sm** 的组播路由条目

5	Inspur#**clear ip mroute pim-sm** {*|[*group-address*] *[source-address*]}	*：清除所有 **pim-sm** 创建的多播路由。 **group-address**：删除相关组的多播路由。 **source-address**：删除相关源的多播路由。
6	Inspur#**debug ip pim-sm [hello|jp|register|assert|bsr|timer] [packet]**	开启调试打印开关。 **hello:**追踪 **hello** 模块发送接收报文信息。 **jp**：追踪 **join/prune** 报文信息。 **register**：追踪 **register** 报文信息。 **bsr:**追踪 **bsr** 报文信息。 **time**：追踪计时器信息。 **packet:**追踪状态机活动信息。

3.3.4 配置 pim-sm 示例

pim-sm 配置示例

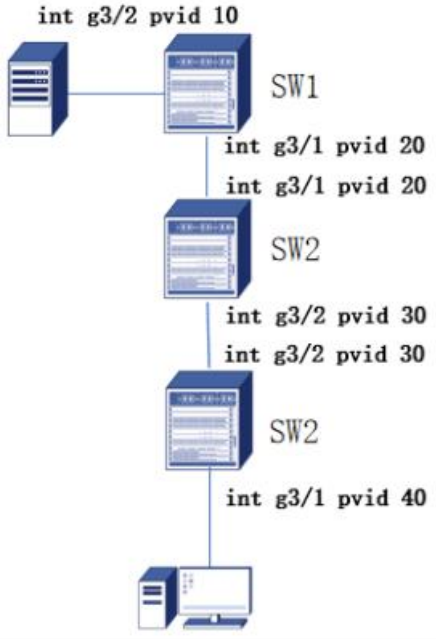


图 3.3.1 pim sm 组网图

前提：组成员能够 **ping** 通服务器。

步骤 1 开启交换机 **pim-sm** 功能。

SW1:

Inspur#**config**

Inspur_config#**ip multicast-routing**

Inspur_config#**interface vlan 10**

Inspur_config_v10#**ip pim-sm**

Inspur_config_v10#**quit**

Inspur_config#**interface vlan 20**

Inspur_config_v20#**ip pim-sm**

Inspur_config_v20#**quit**

SW2:

Inspur#**config**

Inspur_config#**ip multicast-routing**

Inspur_config#**interface vlan 20**

Inspur_config_v20#**ip pim-sm**

Inspur_config_v20#**quit**

Inspur_config#**interface vlan 30**

Inspur_config_v30#**ip pim-sm**

Inspur_config_v30#**quit**

SW3:

Inspur#**config**

Inspur_config#**ip multicast-routing**

Inspur_config#**interface vlan 30**

Inspur_config_v30#**ip pim-sm**

Inspur_config_v30#**quit**

Inspur_config#**quit**

步骤 2　配置静态 RP

SW1:

Inspur#**config**

Inspur_config#**router pim-sm**

Inspur_config_ps#**static-rp　192.168.20.1**　//RP 地址

SW2:

Inspur#**config**

Inspur_config#**router pim-sm**

Inspur_config_ps#**static-rp　192.168.20.1**　//RP 地址

SW3:

Inspur#**config**

Inspur_config#**router pim-sm**

Inspur_config_ps#**static-rp 192.168.20.1** //RP 地址

步骤 3 配置 igmp 功能

SW3:

Inspur_config#**int vlan 40**

Inspur_config_v40#**ip igmp enable**

Inspur_config_v40#**ip igmp version 2**

pim-sm 监控

显示端口 **pim-sm** 信息。

Inspur#**show ip pim-sm interface**

显示邻居信息。

Inspur#**show ip pim-sm neighbor**

显示 **pim-sm** 的组播路由条目。

Inspur#**show ip mroute pim-sm**

3.4 igmp snooping

3.4.1 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。

3.4.2 配置准备

场景

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。

3.4.3 igmp-snooping 配置

开启/关闭 vlan 的 igmp-snooping 功能

在全局配置模式下进行下列操作。

序号	配置	说明
1	Inspur_config#**ip igmp-snooping vlan** *vlan_id*	开启 **vlan** 的 **igmp-snooping** 功能。
2	Inspur_config#**no ip igmp-snooping vlan** *vlan_id*	恢复缺省设置。

增加/删除 vlan 的静态组播地址

静态组播地址的配置使一些不支持 **IGMP** 协议的主机也能接收到相应的组播报文。

在全局配置模式下进行下列操作。

序号	配置	说明
1	Inspur_config#**ip igmp-snooping vlan** *vlan_id* **static** *A.B.C.D* **interface** *intf*	增加 **vlan** 的静态组播地址。
2	Inspur_config#**no ip igmp-snooping vlan** *vlan_id* **static** *A.B.C.D* **interface** *intf*	删除 **vlan** 的静态组播地址。

VLAN 的 immediate-leave 特性

配置 **immediate-leave** 特性可以使交换机收到 **leave** 报文后立即从对应组播组的端口列表中删除相应的端口，而不再开启定时器等待是否还有其他主机加入了这个组播，如果同一端口下的其他主机也属于这个组但并不想离开，这些用户的组播通信可能会受到影响，此时不应启用 **immediate-leave** 功能。

在全局配置模式下进行下列操作。

序号	配置	说明
1	Inspur_config#**ip igmp-snooping vlan** *vlan_id* **immediate-leave**	配置 **vlan** 的 **immediate-leave** 特性。
2	Inspur_config#**no ip igmp-snooping vlan** *vlan_id* **immediate-leave**	恢复 **vlan** 的 **immediate-leave** 的特性为默认值。

配置 VLAN 的静态路由端口

配置静态的路由端口将组播报文发往该路由端口。交换机会把组播的 **report** 报文发送给 **vlan** 下的所有路由端口。

在全局配置模式下进行下列操作。

序号	配置	说明
1	Inspur_config#**ip igmp-snooping vlan** *vlan_id* **mrouter interface** *intf*	增加 **vlan** 的静态路由端口。
2	Inspur_config#**interface** *interface-type interface-number*	删除 **vlan** 的静态路由端口。

配置生成组播转发表时的 IPACL

配置 **IPACL** 可以制订交换机在收到 **igmp report** 报文后，生成组播转发表时的规则和限制。

在全局配置模式下进行下列操作。

序号	配置	说明
1	Inspur_config#**ip igmp-snooping policy** *word*	增加生成组播转发表时的 **IPACL**。
2	Inspur_config#**no ip igmp-snooping policy**	删除已配置的生成组播转发表时的 **IPACL**。

配置过滤目的地址未注册的组播报文的功能

当组播报文目标查找失败（**DLF**，即目的地址未通过 **igmp-snooping** 注册在交换芯片中）时，默认的处理方式是在报文所属的 vlan 内所有端口上进行转发，可以通过配置改变该处理方式，使其丢弃所有目的地址未注册在任何端口的组播报文。

在全局配置模式下进行下列操作。

序号	配置	说明
1	Inspur_config#**ip igmp-snooping dlf-drop**	丢弃组播目的地址查找失败的报文。
2	Inspur_config#**no ip igmp-snooping dlf-drop**	恢复默认设置。

配置 Router Age 定时器

Router Age 定时器用于监视 IGMP 查询者是否存在，**IGMP** 查询者维护通过发送查询报文来维护管理组播地址，**IGMP-snooping** 依赖 **IGMP** 查询者和主机之间的通信来工作。

在全局配置模式下进行下列操作。

序号	配置	说明
1	Inspur_config#**ip igmp-snooping timer router-age** *timer_value*	配置 **igmp-snooping** 的 **router age** 值。
2	Inspur_config#**no ip igmp-snooping timer router-age**	恢复默认值。

配置 Response Time 定时器

Response Time 定时器是当 **IGMP** 查询者发送查询报文后，主机报告组播的最晚时间，如果在该定时器老化后还没有收到报告报文，则交换机将删除该组播地址。

在全局配置模式下进行下列操作。

序号	配置	说明
1	Inspur_config#**ip igmp-snooping timer response-time** *timer_value*	配置 **igmp-snooping** 的 **Response Time** 值。
2	Inspur_config#**no ip igmp-snooping timer response-time**	恢复默认值。

配置 Response Time 定时器

当局域网中没有组播路由器且组播流量不需要路由时，可以通过 **IGMP querier** 来激活交换机自发 **query** 的功能，使得 **IGMP-snooping** 保持正常工作。

在全局配置模式下进行下列操作。

序号	配置	说明
1	Inspur_config#**ip igmp-snooping querier [address** *ip_adder*]	配置 **igmp-snooping** 的 **querier**，可选参数 **address** 为 **quert** 报文的源 **IP** 地址。
2	Inspur_config#**no ip igmp-snooping querier [address]**	关闭 **query** 功能。

配置 Querier Time 定时器

Querier Time 定时器是当交换机作为本地 **IGMP** 查询者发送查询报文的时间间隔，定时器老化后则在 **vlan** 内广播 **query** 报文。

在全局配置模式下进行下列操作。

序号	配置	说明

1	Inspur_config#**ip igmp-snooping querier querier-timer** *timer_value*	配置 **igmp-snooping** 的 **querier timer** 值。
2	Inspur_config#**no ip igmp-snooping querier querier-timer**	恢复默认值。

配置 IGMP-snooping 的端口下最大组播 IP 地址数量功能

如果配置 **IGMP-snooping** 的端口下最大组播 **IP** 地址数量功能则会在 **IGMP-snooping** 生成转发表项时判断该端口下已申请的组是否达到了该配置的数量，若超过该数目则不再生成该端口的表项。

在接口配置模式下进行下列操作。

序号	配置	说明
1	Inspur_config_g3/1#**ip igmp-snooping limit** *value*	配置 **igmp-snooping** 的端口下最大组播组数量。
2	Inspur_config#**no ip igmp-snooping limit**	恢复默认值。

igmp snooping 监控与维护

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-snooping**	显示 **igmp-snooping** 的配置信息。
2	Inspur#**show ip igmp-snooping timer**	显示 **igmp-snooping** 时钟信息。
3	Inspur#**show ip igmp-snooping groups**	显示 **igmp-snooping** 多播组信息。
4	Inspur#**show ip igmp-snooping statistics**	显示 **igmp-snooping** 统计信息。
5	Inspur#**debug ip igmp-snooping [packet|timer|event|error]**	开启 **igmp-snooping** 数据包/时钟调试/事件/错误打印开关，如果不指定具体调试开关，则所有调试开关被打开。
6	Inspur#**no debug ip igmp-snooping [packet|timer|event|error]**	关闭 **igmp-snooping** 数据包/时钟调试/事件/错误打印开关，如果不指定具体调试开关，则所有调试开关被关闭。

3.4.4 配置示例

igmp-snooping 配置示例

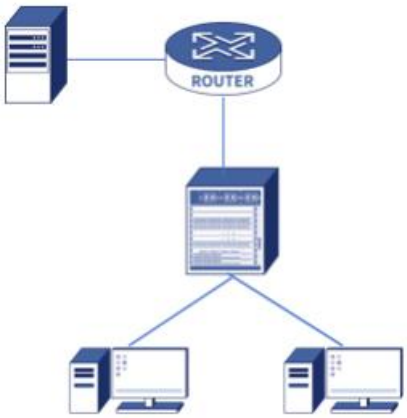


图 3.4 .1 igmp-snooping 示例图

步骤一：建立 **vlan**

步骤二：开启 **igmp-snooping**

Inspur_config#**ip** igmp-snooping vlan 10

igmp-snooping 监控

显示 **igmp-snooping** 的配置信息。

Inspur_config#**show ip igmp-snooping**

Global IGMP snooping configuration:

VLAN nodes : 10

IGMP version : V3

Max src-rec num : 32

Dlf-drop VLAN nodes :

Sensitive : Disabled

Querier : Disabled

Querier address : 10.0.0.200

Querier election : Disabled

Querier interval : 200s

Router age : 260s

Response time : 15s

Pull-stream : Disabled

Pull-stream address : 10.0.0.200

Report suppression : Disabled

Proxy leave : Disabled

VLAN Immediate-leave Querier IP Router Ports

---

10 Disabled none

显示 igmp snooping 多播组信息。

Inspur_config#show ip igmp-snooping group

Total number of groups: 1

Vlan Group Type Port(s)

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

10 239.255.255.250 IGMP g3/4

显示 **igmp snooping** 统计信息

Inspur_config#show ip igmp-snooping statistics

IGMP Snooping Message Statistics

L2 main messages sent OK : 25

L2 main messages sent failed : 0

L2 packets received : 1220

L2 packets sent : 4

L2 packets sent failed : 0

L2 link-status messages : 21

IGMP Snooping messages received: 28

IGMP packet messages received : 4

IGMP Snooping Packet Statistics

Received packets : 4

IGMP packets : 3

M-routing protocol packets : 0

Other packets : 0

Received IGMP general queries : 1

Received IGMPv2 specific queries : 0

Received IGMPv3 g specific queries : 0

Received IGMPv3 gs specific queries: 0

Received IGMPv1 reports : 0

3.5 igmp proxy

3.5.1 简介

在一些简单的网络拓扑中，与用户网段直接相连的交换机上并不需要运行复杂的组播路由协议，而透传主机 IGMP 报文又会导致上游接入设备管理太多用户。此时可以通过在与用户网段直接相邻的组播交换机上配置 **IGMP Proxy**（**IGMP** 代理）功能，使其收集下游用户的 **IGMP** 成员 **report/leave** 信息，将成员 **report/leave** 信息汇聚后代理下游主机统一上送给接入设备，并维护组成员关系，基于组成员关系进行组播转发。在上游接入设备看来，配置了 **IGMP Proxy** 功能的组播交换机就是一台主机。

3.5.2 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 proxy**，拦截主机和路由器之间的 **IGMP** 报文，减少网络负担。

需要注意的是：虽然 **IGMP proxy** 是基于 **IGMP snooping** 的一个功能模块，但两者的功能是互相独立的应用，开启关闭 **IGMP proxy** 不会影响 **IGMP snooping** 的功能，但必须开启 **IGMP snooping** 才能使用 **IGMP proxy** 的功能。

3.5.3 igmp-proxy 配置

开启/关闭 igmp-proxy 功能

当开启 **ip multicast routing** 后不能开启 **igmp proxy** 功能，若之前已经开启了 **igmp proxy** 则会被自动关闭，但关闭 **ip multicast routing** 后不会自动打开 **igmp proxy**，需要手动重新开启。

在全局配置下进行下列配置。

序号	配置	说明
1	`Inspur_config#ip igmp-proxy enable`	开启 `igmp proxy` 功能。

2	Inspur_config#**no ip igmp-proxy enable**	恢复缺省配置。

增加/删除 vlan 代理关系

avlan_map 指定的 **vlan** 之前不能被配置为被代理 **vlan**；同理 **cvlan_map** 之前也不能被配置为代理 **vlan**。

代理或者被代理 **vlan** 必须已经受 **igmp snooping** 控制。

在全局配置下进行下列配置。

序号	配置	说明
1	Inspur_config#**ip igmp-proxy agent-vlan** *avlan_map* **client-vlan map** *cvlan_map*	增加代理 **vlan** *avlan_map* 管理被代理 **vlan** *cvlan_map*。
2	Inspur_config#**no ip igmp-proxy agent-vlan** *avlan_map* **client-vlan map** *cvlan_map*	删除代理关系。

igmp-proxy 监控与维护

序号	配置	说明
1	Inspur#**show ip igmp-proxy**	显示 **igmp-proxy** 配置信息。
2	Inspu#**debug ip igmp-proxy** *[error|event|packet]*	开启 **igmp-proxy** 调试打印开关。
3	Inspur#**no debug ip igmp-proxy** *[error|event|packet]*	关闭 **igmp-proxy** 调试打印开关。

3.5.4 配置示例

igmp-proxy 配置示例

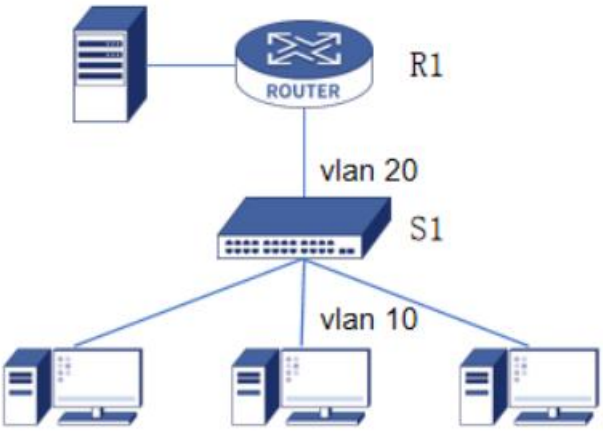


图 3.5.1

步骤 1：**S1** 配置好 **vlan**，并且组成员能够 ping 通服务器。

步骤 2：**S1** 开启 **igmp-snooping**

Inspur#**config**

Inspur_config#**ip igmp-snooping**

步骤 3：**S1** 开启 **igmp proxy**

Inspur_config#**ip igmp-proxy enable**

Inspur_config#**ip igmp-proxy agent-vlan 20 client-vlan map 10**

步骤 4：在路由器下游接口开启 **igmp** 功能。

igmp proxy 监控

显示 **igmp-proxy** 配置信息。

Inspur#show ip igmp-proxy

Global IGMP proxy configuration:

Global IGMP proxy: Enabled

Agent VLAN 20, allocated

Client VLANs: 10

3.6 MLD snooping

3.6.1 简介

MLD-Snooping 是一种 **IPv6** 二层组播协议，该协议侦听二层组播设备和用户主机之间发送的组播协议报文，维护组播报文出端口的信息，进而管理和控制组播数据报文的转发。

3.6.2 配置准备

场景

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 **MLD-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。

3.6.3 配置

开启/关闭 MLD-Snooping 功能

请在全局配置模式进行以下配置。

序号	配置	说明
1	Inspur_config#**ipv6 mld-snooping**	开启 **MLD-Snoooping** 组播功能。
2	Inspur_config#**no ipv6 mld-snooping**	关闭 **MLD-Snoooping** 组播功能。

增加/删除 VLAN 的静态组播地址

请在全局配置模式下进行以下配置。

序号	配置	说明
1	Inspur_config#**ipv6 mld-snooping vlan** *vlan_id* **staic** *X.X.X.X::X* **interface** *intf_name*	增加 **VLAN** 的静态组播功能。
2	Inspur_config#**no ipv6 mld-snooping vlan** *vlan_id* **staic** *X.X.X.X::X* **interface** *intf_name*	删除 **VLAN** 的静态组播功能。

配置 MLD-Snooping 的 Router Age 定时器

Router Age 定时器用于监视 **MLD-Snooping** 查询者是否存在，**MLD-Snooping** 查询者维护通过发送查询报文来维护管理组播地址，**MLD-Snooping** 依赖 **MLD-Snooping** 查询者和主机之间的通信来工作。

请在全局配置模式下进行以下配置。

序号	配置	说明
1	Inspur_config#**ipv6 mld-snooping timer router-age** *timer_value*	配置 **MLD-snooping** 的 **router age** 值。
2	Inspur_config#**no ipv6 mld-snooping timer router-age**	恢复 **MLD-snooping** 的 **router age** 为默认值。

配置 MLD-Snooping 的 Response Time 定时器

Response Time 定时器是当 **MLD-Snooping** 查询者发送查询报文后，主机报告组播的最晚时间，如果在该定时器老化后还没有收到报告报文，则交换机将删除该组播地址。

请在全局配置模式下进行以下配置。

序号	配置	说明
1	Inspur_config#**ipv6 mld-snooping timer response-time** *timer_vlaue*	配置 **MLD-snooping** 的 **response time** 值。
2	Inspur_config#**no ipv6 mld-snooping timer response-time** *timer_vlaue*	恢复 **MLD snooping** 的 **response time** 为默认值。

配置 MLD-Snooping 的 Querier

请在全局配置模式下执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur_config#**ipv6 mld-snooping querier [address** *ip_add***]**	查看安全 **MAC** 的接口配置信息。
2	Inspur_config#**no ipv6 mld-snooping querier [address** *ip_add***]**	查看安全 **MAC** 地址配置及学习情况。

配置静态的组播路由器端口

请在全局配置模式下执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur_config#**ipv6 mld-snooping vlan** *WORD* **mrouter interface** *inft_name*	在 **VLAN WORD** 下配置 **MLD-Snooping** 的静态组播路由器端口。
2	Inspur_config#**no ipv6 mld-snooping vlan** *WORD* **mrouter interface** *inft_name*	删除静态组播路由器端口。

开启/关闭立即离开功能

请在全局配置模式下执行以下命令检查配置结果。

序号	检查项	说明
1	Inspur_config#**ipv6 mld-snooping vlan** *WORD* **immediate-leave**	在 **vlan** 的快速离开功能。
2	Inspur_config#**no ipv6 mld-snooping vlan** *WORD* **immediate-leave**	恢复缺省配置。

MLD-Snooping 监控与维护

序号	检查项	说明
1	Inspur#**show ipv6 mld-snooping**	显示 **MLD-Snooping** 的配置信息。
2	Inspur#**show ipv6 mld-snooping timer**	显示 **MLD Snooping** 时钟信息。
3	Inspur#**show ipv6 mld-snooping groups**	显示 **MLD Snooping** 多播组信息。
4	Inspur#**show ipv6 mld-snooping statistics**	显示 **MLD Snooping** 统计信息。
5	Inspur#**show ipv6 mld-snooping vlan**	显示 **vlan** 的 **MLD Snooping** 的配置信息。
6	Inspur#**show ipv6 mld-snooping mac**	显示 **MLD-Snooping** 记录的组播 **mac** 地。

3.6.4 配置示例

MLD-Snooping 配置示例

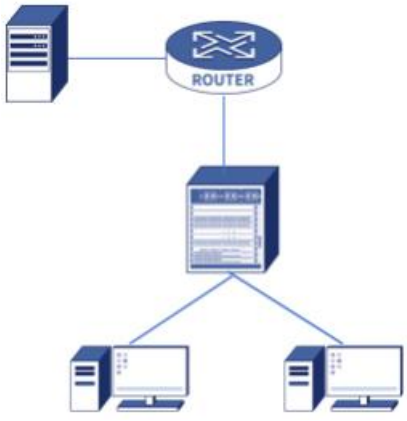


图 3.6.1 mld-snooping 示意图

配置步骤

第一步：配置好 **vlan** 以及地址。

第二步：开启 **MLD-Snooping** 功能。

Inspur>enable

Inspur#config

Inspur_config#ipv6 ml d-snooping

MLD-Snooping 维护

显示 **MLD-Snooping** 的配置信息。

Inspur_config#**s**how ipv6 mld-snooping

Global MLD snooping configuration:

Globally enable : Enabled

VLAN nodes : 1,10

MLD version : V1

Max src-rec num : 32

Querier : Disabled

Querier address : FE80::3FF:FEFE:FD00:1

Router age : 260s

Response time : 10s

Handle solicitation : Disabled

VLAN Immediate-leave Router Ports

---

1 Disabled

10 Disabled

显示 **MLD-Snooping** 统计信息。

Inspur_config#show ipv6 mld-snooping statistics

MLD Snooping Message Statistics

L2 main messages sent OK : 33

L2 main messages sent failed : 0

L2 packets received : 12

L2 packets sent : 12

L2 packets sent failed : 0

L2 link-status messages : 21

MLD Snooping messages received : 35

MLD packet messages received : 12

MLD Snooping Packet Statistics

Received packets : 12

MLD packets : 12

Other packets : 0

Received MLD general queries : 0

Received MLD specific queries : 0

Received MLDv2 g specific queries : 0

Received MLDv2 gs specific queries : 0

Received MLDv1 reports : 0

Received MLDv2 reports : 12

Received MLD dones : 0

Flooded queries : 0

Sent queries : 0

Forwarded and proxy-sent reports : 12

Forwarded and proxy-sent dones : 0

MLD Snooping Packet Drop

Badhdr packets : 0

Indiscard packets : 0

Intrnct packets : 0

Badver packets : 0

Inbadscope packets : 0

Tooshort packets : 0

Manyhdrs packets : 0

Checksum error packets : 0

MLD Snooping Hardware Operation Statistics

Total	: 0
Succeeded	: 0
Failed	: 0
Report/leave processing	: 0
Response timer expiring	: 0
Group creating/updating	: 0
Group deleting	: 0

4 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
- **STP**
- **RSTP**
- **MSTP**
- **PVST**
- 生成树参数配置
- 环路检测配置
- **Ether-ring**
- 端口备份
- 端口保护
- 端口镜像
- **VRRP** 配置
- 端口隔离
- **Keeplive** 功能

4.1 链路聚合

4.1.1 简介

端口聚合，即将几个属性相同的物理端口聚合绑定到一起形成一个逻辑上的通道。端口的聚合方式可以是将几个物理端口静态的聚合到一起而不管与这些物理端口相连的端口是否符合聚合的条件；而使用 LACP 协议进行聚合时，端口的聚合必须在与端口相连的对端和本端口都协商通过之后，端口才会聚合为一个逻辑通道。

交换机提供的端口聚合支持以下的运行模式和功能：

- 支持静态的聚合控制

将物理端口配置为捆绑到一个逻辑端口后，不去关心这些物理端口是否可以捆绑到一个逻辑端口，强制的认为这些端口可以捆绑到一个逻辑端口。

- 支持 LACP 动态协商的聚合控制

将物理端口配置为捆绑到一个逻辑端口后，通过 LACP 协议协商的物理端口才可以捆绑到一个逻辑端口，其它端口不会捆绑到该逻辑端口。

- 支持端口聚合的流量平衡

端口聚合后，聚合端口的数据流量分配到各个被聚合的物理端口上。

4.1.2 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。

4.1.3 链路聚合配置

配置用于聚合的逻辑通道

在将物理端口聚合绑定到一起之前，应该先创建一个逻辑端口，用于控制这些绑定 到一起的物理端口形成的通道。

序号	配置	说明
1	Inspur_config#**interface port-aggregator** *id*	配置聚合的逻辑通道。

物理端口的聚合

将多个物理端口聚合为一个逻辑通道，可以采用静态聚合，也可以使用 **LACP** 协议进行协商。

如果采用静态聚合，则只要该物理端口**linkUp**，并且聚合端口和物理端口的**VALN** 属性一致，该端口将会被聚合到逻辑通道中，不论当前端口是否符合端口聚合的条 件，也不论与该物理端口相连的端口是否符合聚合的条件。

使用LACP 协议，则端口的聚合必须在与端口相连的对端和本端口都协商通过之后， 端口才进行聚合。端口能够被聚合的首要条件是端口必须**LinkUp**，并且该端口协商 出来的是全双工模式；在聚合过程中，所有物理成员端口的Speed 必须保持一致， 即，如果已经有一个物理端口聚合成功，这时，第二个物理端口的Speed 必须与已 经聚合成功的物理端口的Speed 相同；同样所有物理端口与聚合端口的VALN 属性 也必须保持一致。

LACP 提供两种聚合方式，一种是**Active**，另一种是**Passive** 方式，在**Active** 方式 下交换机主动发起聚合协商过程，而Passive 方式则是被动的接受聚合协商过程， 在选择**LACP** 聚合时，如果端口聚合的两边都使用Passive 方式，则聚合是不会成 功，因为两端都会去等待对端发起聚合协商过程。

VALN 属性：端口的**PVID**、端口的**Trunk** 属性、端口**VLAN-Trunk** 时的**VLAN** 范围（**vlan-allowed**）和**Untag-VLAN** 范围（**vlan-untagged**）。 使用下面的命令对物理端口进行聚合：

序号	配置	说明
1	Inspur_config#**aggregator-group agg-id mode** { *lacp*|*static* }	物理端口的聚合选择。

选择端口聚合后的流量均衡方式

多个物理端口聚合到一起后为了保证所有的端口都能分担所有的数据流量，可以选择分担数据流量的方式，交换机最多提供8 种流量均衡策略：

- src-mac

根据源**MAC** 地址进行分担，即具有相同**MAC** 地址属性的报文将在一个物理端口上通过。

- dst-mac

根据目的MAC 地址进行分担，即具有相同**MAC** 地址属性的报文将在一个物理端口上通过。

- both-mac

根据源和目的**MAC** 地址进行分担，即具有相同**MAC** 地址属性的报文将在一个物理端口上通过。

- src-ip

根据源**IP** 地址进行分担，即具有相同**IP** 地址属性的报文将在一个物理端口上通过。

- dst-ip

根据目的**IP** 地址进行分担，即具有相同**IP** 地址属性的报文将在一个物理端口上通过。

- both-ip

根据源和目的**IP** 地址进行分担，即具有相同**IP** 地址属性的报文将在一个物理端口上通过。

- src-port

根据源端口进行负载均衡，报文从聚合端口的物理端口通过取决于报文进来的源端口。

- enhanced

根据聚合组成员数量进行负载均衡，报文从聚合端口的物理端口通过取决于当前聚合组的成员数量。目前只有**Broadcom V** 代码芯片支持模式。

序号	配置	说明
1	Inspur_config#**aggregator-group load-balance** { dst-mac | src-mac | both-mac | src-ip | dst-ip} | both-ip | src-port | enhanced }	配置流量均衡方式。

监控端口聚合的具体情况

为了监控端口聚合的状态，可以在管理模式下使用下面的命令：

序号	配置	说明
1	Inspur_config#**show aggregator-group** *id* { detail | brief | summary }	显示端口聚合的状态。

重要说明：

聚合口不支持增强分流算法，芯片不支持五元组

跨设备（堆叠）聚合口上配置的静态 **mac** 或学到的动态 **mac**，都会占用 2 条 **mac** 表项，实际表项只占用一条，不同板卡有多条显示属于正常情况

聚合口角色为根端口时，从聚合口进入的已知单播流量会洪泛，**mac** 同步机制问题。通过配置 **mac address-table rpc all agecheck**（**Inspur_config#**模式下）或 **clear mac address-table dynamic**（**Inspur#**模式下）可解决

4.4.4 配置示例

组网需求：

如图 4.1.1 所示，以太网交换机 **Inspur A** 使用 2 个端口（g3/1、g3/2）以聚合方式接入以太网交换机 **Inspur B** 。在聚合链路上实现负载分担。

本案例中介绍两种端口聚合方式。

拓扑图：

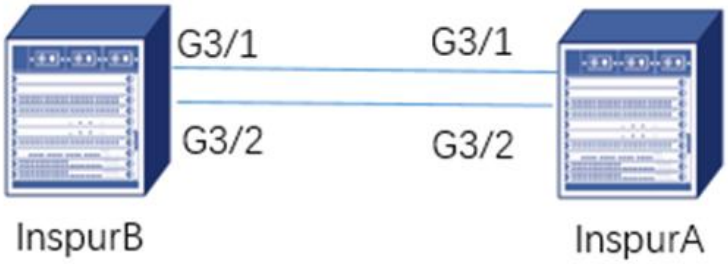


图 4.1.1 示意图

采用 LACP 协商模式的端口聚合

* 配置 **Inspur** A

• 在本地交换机上创建聚合组

InspurA_config#**int port-aggregator 1**
InspurA _config_p1#**exit**
InspurA _config#**int g3/1**
InspurA _config_g3/1#**aggregator-group 1 mode lacp**
InspurA_config_g3/1#**exit**
InspurA _config#**int g3/2**
InspurA _config_g3/2#**aggregator-group 1 mode lacp**
InspurA_config_g3/2#**exit**

* 配置 **Inspur** B

• 在本地交换机上创建聚合组

InspurB_config#**int port-aggregator 2**
InspurB _config_p2#**exit**
InspurB _config#**int g3/1**
InspurB_config_g3/1#**aggregator-group 2 mode lacp**
InspurB_config_g3/1#**exit**
InspurB _config#**int g3/2**
InspurB _config_g3/2#**aggregator-group 2 mode lacp**
InspurB_config_g3/2#**exit**
InspurA_config_g3/4#**exit**

采用静态端口聚合

* 配置 **Inspur A**

- 在本地交换机上创建聚合组

InspurA _config#**int port-aggregator 1**
InspurA _config_p1#**exit**
InspurA _config#**int g3/1**
InspurA _config_g3/1#**aggregator-group 1 mode static**
InspurA _config #**int g3/2**
InspurA _config _g3/2#**aggregator-group 1 mode static**
InspurA _config _g3/2#**exit**

* 配置 **Inspur B**

- 在本地交换机上创建聚合组

InspurB _config#**int port-aggregator 2**
InspurB _config_p1#**exit**
InspurB _config#**int g3/1**
InspurB _config_g3/1#**aggregator-group 2 mode static**
InspurB _config #**int g3/2**
InspurB _config _g3/2#**aggregator-group 2 mode static**
InspurB _config _g3/2#**exit**

查看聚合状态

- 查看本地聚合组及成员的状态

Inspur_config#**show aggregator-group 1 brief**

Aggregator-group brief infomation

Group: 1

System ID : 32768 00E0.0F64.C6AE Partner : 0 0000.0000.0000
Group ID : 32768 00E0.0F64.C6AF state : lineUp
Max Ports : 128 ports : 2

Flags: D - down A - Use In port-aggregator
U - Up I - Not In port-aggregator
d - default

G3/1(UA) G3/2(UA)

4.2 STP

4.2.1 简介

标准的生成树协议（**Spanning-Tree Protocol，STP**）定义于 **IEEE 802.1D**，它将一个由若干网桥连接组成的局域网拓扑简化为一棵单独的生成树，防止网络环路的产生，保证网络的稳定工作。

生成树算法和协议将任意的桥接局域网配置为简单连接的活动拓扑结构。在活动拓扑中，有些网桥端口可以转发帧，有些端口则处在阻塞状态而不能转发。处在阻塞状态的端口也可能被包含在活动拓扑中，当网络中出现设备失效、添加或移出时，它就会转入转发状态。

在生成树拓扑中，一个网桥被认为是根或者根桥（**Root**）。对每一个局域网段，都有一个网桥端口负责该网段到根桥的数据转发，该端口被认为是该局域网段的指派端口，而端口所在的网桥被认为是该局域网的指派网桥（**Designated Bridge**）。根桥是所有与之连接的局域网段的指派网桥。在每个网桥的端口中，到根桥最近的端口为该桥的根端口，且只有根端口和指派端口（如果存在）处于转发状态；还有一类端口并没有被关闭掉但是也不是根端口或指派端口，这一类端口为备用端口。

以下参数决定了稳定后的活动拓扑的结构：

(1) 每个网桥的唯一标识。

(2) 每个端口的路径开销。

(3) 网桥每个端口的端口标识。

优先级最高（标识符值最小）的网桥将被选为根桥。网络中每个网桥的端口都有一个根路径开销属性（**Root Path Cost**），即从根桥到该网桥经历的所有端口的路径开销的和的最小值。每个局域网段的指派端口就是指连接到该网段的且根路径开销最小的端口；如果若干个端口（连接到同一局域网段的不同网桥上）具有相同的根路径开销，则会首先比较它们所在网桥的标识，然后比较端口标识。按照这种方法，每个局域网段都只有一个指派端口（**Designated Port**），每个网桥上也只有一个根端口（**Root Port**）。

生成树拓扑使网络中不存在环路，保证网络的稳定性并具有故障恢复的能力。在以太网交换机被广泛使用的今天，**STP** 的作用也越发显得重要。因此，生成树协议是作为本公司交换机的一项基本功能而被提供的。

快速生成树协议（**Rapid Spanning-Tree Protocol，RSTP**）是对 **802.1D STP** 的一项重要更新。在网络中的网桥、网桥端口或者局域网段出现故障时，快速生成树协议实现了网络拓扑的快速收敛。网桥上新的根端口可以立即进入转发状态工作，同时，网桥之间的直接认可使指派端口也可以马上进行转发。**RSTP** 协议的配置请参见第 4.3 配置快速生成树协议（**RSTP**）。

本章描述了如何配置交换机支持的标准生成树协议。

4.2.2 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。

4.2.3 STP 配置

选择 STP 模式

序号	配置	说明
1	`Inspur_config#spanning-tree mode {sstp | pvst | rstp | mstp}`	进行的 STP 模式配置选择。

禁止/启动 STP

序号	配置	说明
1	Inspur_config#**no spanning-tree**	禁止运行 **STP**。
2	Inspur_config#**spanning-tree**	启动默认模式的 **STP**（**RSTP**）。
3	Inspur_config#**spanning-tree mode** { sstp | pvst | rstp | mstp }	启动某种模式的 **STP**。
4	Inspur_config_g3/1#**no spanning-tree**	禁止端口运行 **STP**。

配置网桥优先级

可以通过更改交换机的网桥优先级值来选择网络拓扑的生成树根。

序号	配置	说明
1	Inspur_config#**spanning-tree sstp priority** value	更改 **SSTP** 模式的网桥优先级值。（默认值 32768）

配置 Hello Time

序号	配置	说明
1	Inspur_config#**spanning-tree sstp hello-time** value	更改 **SSTP** 模式的 **Hello Time**。

配置 Max Age

通过配置 SSTP 的 Max Age 可以决定当该交换机作为根桥时生成树中报文的最大生存时间。

序号	配置	说明
1	Inspur_config#**spanning-tree sstp max-age** value	更改 **SSTP** 模式的最大生存时间。

配置 Forward Delay

通过配置 SSTP 的 Forward Delay 可以决定当该交换机作为根桥时网络中的所有交换机的状态跳转的时间间隔。

序号	配置	说明
1	Inspur_config#**spanning-tree sstp forward-time** value	更改 **SSTP** 模式的 **Forward time**。

配置端口优先级

当有环路形成时，STP 会将一些端口的状态跳转为 Blocking 状态，以断开环路。通过配置端口优先级和端口路径开销可以控制端口是否被阻塞。

序号	配置	说明

序号	配置	说明
1	Inspur_config#**spanning-tree port-priority** value	配置所有模式下端口的优先级。
2	Inspur_config# spanning-tree sstp port-priority value	更改 **SSTP** 模式的端口优先级。

配置端口路径开销

序号	配置	说明
1	Inspur_config#**spanning-tree cost** value	配置所有模式下端口的路径开销。
2	Inspur_config#**spanning-tree sstp cost** value	更改 **SSTP** 模式的端口路径开销。

监控 STP 状态

序号	配置	说明
1	Inspur_config#**show spanning-tree**	显示当前模式下生成树协议的状态。
2	Inspur_config#**show spanning-tree detail**	显示当前模式下生成树协议的状态。
3	Inspur_config#**show spanning-tree interface** {interface-type} number	显示当前模式 **STP** 下的端口信息。

配置 SNMP Trap

通过配置生成树协议的 **Trap** 功能，可以从主机的网管软件远程监测交换机生成树协议的变化。

S9500 以太网交换机的 **STP** 系列协议支持两种类型的 **Trap**：**newRoot** 和 **topologyChange**。当从非根交换机变为根交换机时，交换机发送 **newRoot Trap** 消息；当交换机检查到拓扑变化时，比如一个非边缘端口从非转发态变为转发态，会发送 **topologyChange Trap** 消息。

序号	配置	说明
1	Inspur_config#**spanning-tree management trap** { newroot | topologychange }	启用 **STP Trap**。 不指定 **Trap** 类型将同时启用两种 **Trap**。

4.2.4 配置示例

配置目标

如下图所示，三台设备 **Inspur A**、**Inspur B** 和 **Inspur 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 **Inspur A** 的优先级为 0。

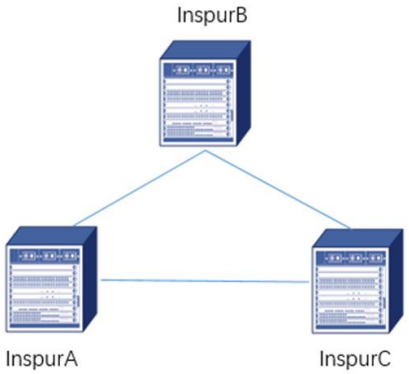


图 4.2.1STP 应用组网示意图

配置步骤

InspurB:
InspurB_config#**spanning-tree mode sstp**
InspurB_config#**spanning-tree sstp priority 0**
!

InspurA:
InspurA_config#**spanning-tree mode sstp**
!

InspurB:
InspurB_config#**spanning-tree mode sstp**
!

查看 Inspur A 生成树状态

InspurA_config#**show spanning-tree**

Spanning tree enabled protocol SSTP

SSTP
  Root ID Priority 0
           Address 8479.7339.64C3
           This bridge is the root
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID Priority 0
           Address 8479.7339.64C3
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface	Role	Sts	Cost	Pri.Nbr	Type
G3/1	Desg	FWD	4	128.2	P2p
G3/2	Desg	BLK	4	128.8	P2p

4.3 RSTP

4.3.1 简介

快速生成树协议（**Rapid Spanning Tree Protocol ， RSTP**） 用于在局域网中消除数据链路层物理环路，其核心是快速生成树算法。**RSTP** 由 IEEE 802.1D-1998 标准定义的 **STP**（**Spanning Tree Protocol**，生成树协议）改进而来，最早在 IEEE 802.1W-2001 中提出，并且在 IEEE 802.1D-2004 标准中替代了原来的 **STP** 协议。**RSTP** 完全向下兼容 **STP** 协议，除了和传统的 **STP** 协议一样具有避免回路、动态管理冗余链路的功能外，**RSTP** 极大的缩短了拓扑收敛时间，在理想的网络拓扑规模下，所有交换设备均支持 **RSTP** 协议且配置得当时，拓扑发生变化（链路 **UP/DOWN**）后恢复稳定的时间可以控制在秒级，而传统的拓扑稳定且能正常工作所需时间为 50 秒

4.3.2 配置准备

场景

在一个复杂的网络中，网络规划者由于冗余备份的需要，一般都倾向于在设备之间部署多条物理链路，其中一条作主用链路，其他链路作备份。这样就难免会形成环形网络，若网络中存在环路，可能会引起广播风暴和 MAC 表项被破坏。

4.3.3 RSTP 配置

禁止/启动 RSTP

序号	配置	说明
1	`Inspur_config#no spanning-tree mode`	关闭交换机的 **stp** 功能。
2	`Inspur_config#spanning-tree mode rstp`	开启 **RSTP**。

配置网桥优先级

可以通过更改交换机的网桥优先级值来选择网络拓扑的生成树根。

序号	配置	说明
1	`Inspur_config#spanning-tree rstp priority value`	更改 **RSTP** 模式的网桥优先级值。（默认值 32768）

配置 Hello Time

合适的 Hello Time 时间值可以保证网桥能够及时发现网络中的链路故障又不会占用过多的网络资源。

序号	配置	说明
1	`Inspur_config#spanning-tree sstp hello-time value`	更改 **RSTP** 模式的 **Hello Time**。

需要注意的是过长的 **Hello Time** 值会因为链路丢包而导致网桥长时间收不到 **Hello** 报文，那么网桥会认为链路发生了故障并且开始重新计算生成树，如果 **Hello Time** 过短则会导致网桥频繁

发送配置消息占用网络带宽，增加了网络负担和 **CPU** 负担，建议用户采用缺省值。 缺省情况下网桥的 **Hello Time** 为 2 秒。

配置 Forward Time

链路故障会引发网络重新进行生成树结构的计算，不过重新计算得到的新配置消息无法立刻传遍整个网络，如果新选出的根端口和指定端口立刻就开始数据转发的话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。根端口和指定端口重新开始数据转发之前要经历一个中间状态，中间状态经过 **Forward Delay** 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。网桥的 **Forward Delay** 特性与交换网络的网络直径有关，一般来说网络直径越大 **Forward Delay** 的时间就应该配置得越长。

序号	配置	说明
1	Inspur_config#**spanning-tree rstp forward-time** value	配置 **Forward Delay**

需要注意的是如果 **Forward Delay** 配置的过小可能会使网络出现暂时的冗余路径，如果 **Forward Delay** 配置的过大网络则可能会较长时间不能恢复连通，建议用户采用缺省值。缺省情况下网桥的 **Forward Delay** 为 15 秒。

配置 Max Age

Max Age 是用来判断配置消息是否过时的参数，用户可以根据实际的网络情况对其进行配置。

序号	配置	说明
1	Inspur_config#**spanning-tree rstp max-age** value	更改 **RSTP** 模式的最大生存时间。

链路故障，降低网络自适应能力。建议用户采用缺省值。 需要注意的是如果 **Max Age** 配置的过小，生成树计算就会比较频繁，而且有可能将网络拥塞误认为链路故障，如果 **Max Age** 配置的过大则很可能不能及时发现。 缺省情况下网桥的 **Max Age** 为 20 秒。

配置端口优先级

通过设定端口的优先级可以指定特定的以太网端口包含在生成树内，一般情况下配置的值越小端口的优先级就越高，该以太网端口就越有可能包含在生成树内，如果网桥所有的以太网端口采用相同的优先级参数值，则以太网端口的优先级高低就取决于该以太网端口的索引号。

序号	配置	说明
1	Inspur_config#**spanning-tree port-priority** value	配置所有模式下端口的优先级。
2	Inspur_config#**spanning-tree rstp port-priority** value	更改 **RSTP** 模式的端口优先级。

需要注意的是改变以太网端口的优先级会引起生成树重新计算。缺省情况下网桥所有以太网端口的优先级为 128。

配置端口路径开销

以太网端口的路径开销与该端口的链路速率有关，链路速率越大应该将该参数配置的越小，当该参数被配置为缺省值时，RSTP 协议可以自动检测当前以太网端口的链路速率并换算成相应的路径开销。

序号	配置	说明
1	Inspur_config#**spanning-tree cost** value	配置所有模式下端口的路径开销。
2	Inspur_config#**spanning-tree rstp cost** value	更改 **RSTP** 模式的端口路径开销。

需要注意的是配置以太网端口的路径开销会引起生成树重新计算，建议用户采用缺省值，让 **RSTP** 协议自己来计算当前以太网端口的路径开销。 缺省情况下网桥所有以太网端口的 **Path Cost** 在端口速率为 10Mbps 时为 2000000，在端口速率为 100Mbps 时为 200000。

配置边缘端口

运行 **RSTP** 协议的交换机之间如果是点到点的直接连接，它们可以通过握手机制快速建立拓扑。配置端口连接类型功能允许将端口的连接设置为点到点。

在默认情况下，协议会根据端口的双工属性决定其是不是使用了点到点的连接。如果端口工作在全双工模式，协议就会认为它是点到点的连接；如果端口工作在半双工模式，协议会认为它的连接是共享的。

如果确认端口所连的交换机运行着 **RSTP** 或者 **MSTP** 协议，可以将端口的连接类型设置为点到点，保证快速握手的进行。

序号	配置	说明
1	Inspur_config#**show spanning-tree**	配置点到点端口。 **force-true**：强制为点到点类型。 **force-false**：强制为非点到点类型。 **auto**：协议自动检测端口类型

配置 SNMP Trap

通过配置生成树协议的 **Trap** 功能，可以从主机的网管软件远程监测交换机生成树协议的变化。

S9500 以太网交换机的 **STP** 系列协议支持两种类型的 **Trap**：**newRoot** 和 **topologyChange**。当从非根交换机变为根交换机时，交换机发送 **newRoot Trap** 消息；当交换机检查到拓扑变化时，比如一个非边缘端口从非转发态变为转发态，会发送 **topologyChange Trap** 消息。

序号	配置	说明
1	Inspur_config#**spanning-tree management trap** {newroot|topologychange}	启用 **STP Trap**。 不指定 **Trap** 类型将同时启用两种 **Trap**。

4.3.4 配置示例

组网需求

如下图所示，三台设备 **Inspur A**、**Inspur B** 和 **Inspur 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 **Inspur A** 的优先级为 0，**Inspur B** 到 **Inspur A** 的开销改为 10。

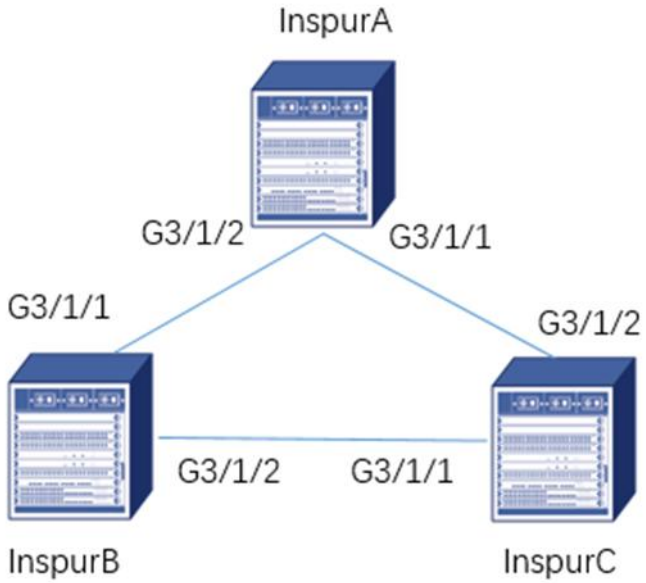


图 4.3.1 STP 应用组网示意图

配置步骤

在三台设备上均开启 **RSTP** 功能。

配置 **Inspur A**。

Inspur#**hostname InspurA**
InspurA#**config**
InspurA_config#**spanning-tree mode rstp**

配置 **Inspur B**。

Inspur#**hostname InspurB**
InspurB#**config**
InspurB_config#**spanning-tree mode rstp**

配置 **Inspur C**。

Inspur#**hostname InspurC**
InspurC#**config**
InspurC_config#**spanning-tree mode rstp**

配置三台设备的接口模式。

配置 **Inspur A**。

InspurA_config#**interface gigaethernet 3/1/1**
InspurA_config_gigaethernet3/1/1#**Inspurport mode trunk**
InspurA_config_gigaethernet3/1/1#**exit**
InspurA_config#**interface gigaethernet 3/1/2**
InspurA_config_gigaethernet3/1/2#**Inspurport mode trunk**

InspurA_config_gigaethernet3/1/2#**exit**

配置 **Inspur B**。

InspurB_config#**interface gigaethernet 3/1/1**
InspurB_config_gigaethernet3/1/1#**Inspurport mode trunk**
InspurB_config-gigaethernet3/1/1#**exit**
InspurB_config#**interface gigaethernet 3/1/2**
InspurB_config_gigaethernet3/1/2#**Inspurport mode trunk**
InspurB_config_gigaethernet3/1/2#**exit**

配置 **Inspur C**。

InspurC_config#**interface gigaethernet 3/1/1**
InspurC_config_gigaethernet3/1/1#**Inspurport mode trunk**
InspurC_config_gigaethernet3/1/1#**exit**
InspurC_config#**interface gigaethernet 3/1/2**
InspurC_config_gigaethernet3/1/2#**Inspurport mode trunk**
InspurC_config_gigaethernet3/1/2#**exit**

配置生成树优先级及接口路径开销。

配置 **Inspur A**。

InspurA_config#**spanning-tree priority 0**
InspurA_config#**interface gigaethernet 3/1/2**
InspurA_config_gigaethernet3/1/2#**spanning-tree cost 10**

配置 **Inspur B**。

InspurB_config#**interface gigaethernet 3/1/1**
InspurB_config_gigaethernet3/1/1#**spanning-tree cost 10**

检查结果

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

InspurA#**show spanning-tree**

```
Spanning tree enabled protocol RSTP(2004)

RSTP
  Root ID      Priority    32768
               Address     8479.7339.64C3
               This bridge is the root
               Hello Time 2 sec   Max Age 20 sec   Forward Delay 15 sec

  Bridge ID    Priority    32768
               Address     8479.7339.64C3
               Hello Time 2 sec   Max Age 20 sec   Forward Delay 15 sec

Interface          Role Sts Cost      Pri.Nbr  Type
---------------- ---- --- --------- -------- ----------------------
G3/1/1               Desg FWD 20000     128.2    Edge
G3/1/2               Desg FWD 20000     128.8    Edge
```

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

InspurA#**show spanning-tree interface g0/2**

```
  Port 2 (gigaethernet 3/1/1) of RSTP is Forwarding
    Edge port(TRUE), Link type is auto ptop
    Port Identifier 128.2, Port role DesignatedPort
    Port path cost 10, Port priority 128
    Designated root has priority 32768, address 8479.7339.64C3
```

```
Designated bridge has priority 32768, address 8479.7339.64C3
Designated port id is 128.2, designated path cost 0
Timers: message age 0, forward delay 15, hello 2
        message expires in 0 seconds
Number of transitions to forwarding state: 1
        last transitions occurred 09:22:03 ago
sent BPDU :         16695
            TCN:    0, RST:    16695, Config BPDU:    0
received BPDU : 0
            TCN:    0, RST:    0, Config BPDU:    0
```

4.4 MSTP

4.4.1 简介

MSTP（Multiple Spanning Tree Protocol）多生成树协议，用来在桥接局域网中建立简单而完整的拓扑结构。**MSTP** 可以与早期的 **STP（Spanning Tree Protocol）**和 **RSTP（RapidSpanning Tree Protocol）**相兼容。

STP 和 **RSTP** 都只能在网络中建立单独的生成树拓扑，所有 **VLAN** 的报文沿着唯一的生成树进行转发。**STP** 收敛过慢，**RSTP** 通过握手机制保证网络拓扑快速稳定。**MSTP** 继承了 **RSTP** 的快速握手机制，同时，在保证网络拓扑快速建立的基础上，**MSTP** 允许将不同的 **VLAN** 划分到不同的生成树中去，从而在网络中建立多个树状拓扑。

在 **MSTP** 建立的网络中，属于不同 **VLAN** 的帧可以在不同的路径上转发，实现了 **VLAN** 数据的负载均衡。 与按 **VLAN** 划分 **STP（per-VLAN Spanning Tree，PVST）**不同的是，**MSTP** 还允许将多个 **VLAN** 划分到同一个生成树拓扑中去，这样可以有效减少支持大量 **VLAN** 所需的生成树的数目。

4.4.2 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。

4.4.3 MSTP 配置

MSTP 的缺省配置

设备上 **MSTP** 的缺省配置如下。

属性	默认设置
生成树协议模式	**RSTP**（**PVST**，**SSTP** 和 **MSTP** 没有启动）。
区域名称	交换机 **MAC** 地址的字符串形式。
区域修订级别	0
多生成树配置表	所有 **VLAN** 都映射在 **CIST**（**MST00**）中。

生成树优先级（**CIST** 和所有 **MSTI**）	32768
生成树端口优先级（**CIST** 和所有 **MSTI**）	128 100 **Mbps**：200000 10 **Mbps**：2000000
Hello Time	2 秒
Forward Delay	15 秒
Maximum-aging Time	20 秒
最大跳数	20
生成树端口路径开销（**CIST** 和所有 **MSTI**）	1000 **Mbps**：20000

启动和停止多生成树协议

生成树协议在默认情况下会以 **RSTP** 模式启动，当不需要运行 **spanning-tree** 时可以停止其运行。

序号	配置	说明
1	Inspur_config#**spanning-tree mode mstp**	启动 **MSTP** 多生成树协议。

配置多生成树区域

交换机所处的多生成树区域，由配置名称、修订号以及 **VLAN** 与 **MSTI** 映射关系这三项属性决定，通过区域配置命令可以分别对其进行设置。需要注意的是，三项属性中任何一项的变化都会导致交换机所处区域的变化。

在初始情况下，多生成树配置名称等于交换机 **MAC** 地址的字符串形式，修订号为 0，并且所有的 **VLAN** 都被映射在 **CIST（MST00）**中。由于不同交换机的 **MAC** 地址都是不同的，因此初始情况下所有运行多生成树协议的交换机都是处在不同的区域中。通过执行 **spanning-tree mstp instance instance-id vlan vlan-list** 命令，可以创建一个新的 **MSTI**，并将指定的 **VLAN** 映射给它；如果该 **MSTI** 被删除，这些 **VLAN** 会被重新映射到 **CIST** 中。

序号	配置	说明
1	Inspur_config#**spanning-tree mstp revision** value	设置多生成树配置修订号。
2	Inspur_config#**spanning-tree mstp name** String	设置多生成树配置名称。 **string** 表示配置名称字符串，最多可包含 32 个字符，大小写敏感。默认值为交换机 **MAC** 地址的字符串形式。

序号	配置	说明
3	Inspur_config#**spanning-tree mstp instance** instance-id **vlan** vlan-list	将 **VLAN** 映射到 **MSTI**。 **instance-id**：生成树实例号，表示一个 **MSTI**。**vlan-list**：映射到该生成树的 **VLAN** 列表。范围 1-4094。**instance-id** 为单独的值，仅表示一个生成树实例；**vlan-list** 可以表示一组 **VLAN**，比如：”1,2,3”、”1-5”、“1,2,5-10”等。

配置网络根桥

在 **MSTP** 协议中，每个生成树实例都有一个网桥标识属性（**Bridge ID**），网桥标识中包含有该交换机的优先级值以及 **MAC** 地址。在网络生成树拓扑建立过程中，网桥标识较小的交换机会被选为网络（或区域）的根。

多生成树协议允许通过配置将交换机设为网络的根。**Spanning-tree mstp instance-idroot** 配置命令可以将交换机在某个生成树实例中的优先级从默认的 32768 设置为一个足够小的值，保证交换机在该生成树实例中成为根。

通常情况下，当执行上述命令后，协议会自动检查当前网络根桥的网桥标识，然后把网桥标识的优先级字段设置为 24576，如果这个值可以保证当前交换机成为生成树实例的根。

如果网络根桥的优先级比 24576 更小，那么协议会自动把当前网桥的生成树优先级设置为比根桥优先级小 4096 的一个值。需要注意的是，4096 是网桥优先级值的步长。

设置根桥时，可以通过 **diameter** 子命令设置多生成树网络的网络直径，该关键字仅在生成树实例号为 0 时有效。设定网络直径以后，为了保证网络收敛的稳定，协议会自动根据这个值来计算合适的生成树协议时间参数，包括：**Forward Delay** 以及 **MaximumAge**。**Hello-time** 子命令可以用来设置新的 **Hello Time** 时间，以取代默认设置。

序号	配置	说明
1	Inspur_config#**spanning-tree mstp** instance-id **root primary** {diameter net-diameter { hello-time seconds}value	设置交换机在指定生成树实例中为根。 **instance-id**：生成树实例号； **net-diameter**：可选参数，网络直径，当 **instance-id** 为 0 时有效，范围：2 - 7； **seconds**：可选参数，**Hello Time**，范围：1 - 10 秒。

配置次要根桥

为网络配置根桥以后，可以通过 **spanning-tree mstp instance-id root secondary** 命令设置一台或多台交换机成为网络的次要根桥（或称备份根桥）。如果根桥因为某些原因不能工作，次要根桥会接替成为网络的根。

与配置主要根桥不同，执行配置次要根桥的命令后，协议会将交换机的生成树优先级直接设置为 28672，这样，在网络中其它交换机的优先级都为默认的 32768 的情况下，当前交换机就可以成为次要根桥。

配置次要根桥时，仍然可以通过 **diameter** 和 **hello-time** 子命令来更新生成树协议的时间参

数。当次要根桥成为主要根桥开始工作后，这些参数将会开始起作用。

序号	配置	说明
1	Inspur_config#**spanning-tree mstp instance-id root secondary** [diameter net-diameter {hello-time seconds}]	设置交换机在指定生成树实例中为根。 **instance-id**：生成树实例号； **net-diameter**：可选参数，网络直径，当 **instance-id** 为 0 时有效，范围：2 – 7； **seconds**：可选参数，**Hello Time**，范围：1 – 10 秒。

配置网桥优先级及时间参数

配置网桥优先级在某些情况下可以更直接的将交换机设置为网络的根，而不需通过 **root** 子命令。交换机在每个生成树实例中的优先级值是相互独立的，可以独立配置。

生成树协议的时间参数包括下列几项：

Hello Time： 交换机作为网络根桥时向指派端口发送配置信息的时间间隔；

Forward Delay：**STP** 模式下，端口从 **Blocking** 状态到 **Learning** 状态，以及从 **Learnin** 状态到 Forwarding 状态经历的时间；

MAX AGE: 生成树配置信息的最大生存期。

为了减少网络拓扑震荡，时间参数之间应该符合以下条件的要求：

2 x (fwd_delay - 1.0) >= max_age

max_age >= (hello_time + 1) x 2

序号	配置	说明
1	Inspur_config#**spanning-tree mstp** instance-id **priority** value	设置交换机的优先级值。 **instance-id**：生成树实例号； **value**：网桥优先级，可为下列值之一：0，4096，8192，12288，16384，20480，24576，28672，32768，36864，40960，45056，49152，53248，57344，61440。
2	Inspur_config#**spanning-tree mstp hello-time** seconds	设置 **Hello Time** 参数。 **seconds**：范围：1
3	Inspur_config#**spanning-tree mstp forward-time** seconds	设置 **Forward Delay** 参数。
4	Inspur_config#**spanning-tree mstp max-age** seconds	设置 **Max Age** 参数。 **seconds**：范围：6 – 40 秒，默认值 20 秒。

建议通过设置根桥或者设置网络直径的方法来修改生成树协议的时间参数，以保证其合理性。即使新设置的时间参数不符合上述公式的要求，仍然会在协议中生效。配置时请注意控制台的提示。

配置边缘端口

边缘端口表示该端口连接着网络上的终端设备，一个强制的边缘端口在 **Link Up** 之后会立刻进入转发状态。在端口配置模式下。

序号	配置	说明
2	Inspur_config# **spanning-tree mstp edge**	将端口配置为边缘端口。

配置端口路径开销

MSTP 协议中端口路径开销的默认值是根据端口的连接速率计算出来的。如果两台交换机之间形成环路，路径开销较小的端口会进入 **Forwarding** 状态，路径开销越小表示端口的速率越高。如果所有端口的路径开销都相同，端口号较小的端口会优先进入转发状态。

序号	配置	说明
1	Inspur_config#**spanning-tree cost** value	设置端口在所有生成树实例中的路径开销。**value**：端口路径开销，范围 1 – 200000000。
2	Inspur_config_g3/1#**spanning-tree mstp** ***instance-id*** **cost** *cost*	设置端口路径开销。 **instance-id**：生成树实例号； **cost**：路径开销值，范围 1 – 200000000。

配置网络直径

网络直径表示网络上两台主机之间跨越交换机的最大数目，它反映了网络的规模。

可以通过 **spanning-tree mstp diameter net-diameter** 命令设置多生成树协议的网络直径。网络直径参数仅对 **CIST** 有效，设置后，生成树协议的三个时间参数会被自动更新为较优的值。

序号	配置	说明
1	Inspur_config#**spanning-tree mstp diameter** net-diameter	设置网络直径参数。 **net-diameter**：范围：2 – 7，默认值为 7。

网络直径参数在交换机中并没有作为一项单独的设置而被保存，只有通过设置网络直径而修改的时间参数才会被保存。

配置最大跳数

序号	配置	说明
1	Inspur_config#**spanning-tree mstp max-hops** hop-count	设置最大跳数。 **hop-count**：范围：1

配置端口优先级

如果交换机的两个端口之间形成环路，优先级较高的端口会进入 **Forwarding** 状态，较低的则被阻塞。如果所有端口的优先级都相同，那么端口号较小的端口将优先进入 **Forwarding** 状态。

序号	配置	说明
1	Inspur_config_g3/1#**spanning-tree mstp** *instance-id* **port-priority** *priority*	设置端口优先级。 **instance-id**：生成树实例号； **priority**：端口优先级，为下列值之一：0，16，32，48，64，80，96，112，128，144，160，176，192，208，224，240。
2	Inspur_config#**spanning-tree port-priority** *value*	设置端口优先级。 **instance-id**：生成树实例号； **priority**：端口优先级，为下列值之一：0，16，32，48，64，80，96，112，128，144，160，176，192，208，224，240。

配置端口路径开销

MSTP 协议中端口路径开销的默认值是根据端口的连接速率计算出来的。如果两台交换机之间形成环路，路径开销较小的端口会进入 **Forwarding** 状态，路径开销越小表示端口的速率越高。如果所有端口的路径开销都相同，端口号较小的端口会优先进入转发状态。

序号	配置	说明
1	Inspur_config#**spanning-tree cost** value	设置端口路径开销。 **instance-id**：生成树实例号； **cost**：路径开销值，范围 1 – 200000000。
2	Inspur_config#**spanning-tree mstp** *instance-id* **cost** *cost*	设置端口路径开销。 **instance-id**：生成树实例号； **cost**：路径开销值，范围 1 – 200000000。

配置端口连接类型

运行 **MSTP** 协议的交换机之间如果是点到点的直接连接，它们可以通过握手机制快速建立拓扑。配置端口连接类型功能允许将端口的连接设置为点到点。

在默认情况下，协议会根据端口的双工属性决定其是不是使用了点到点的连接。如果端口工作在全双工模式，协议就会认为它是点到点的连接；如果端口工作在半双工模式，协议会认为它的连接是共享的。

如果确认端口所连的交换机运行着 **RSTP** 或者 **MSTP** 协议，可以将端口的连接类型设置为点到点，保证快速握手的进行。

序号	配置	说明
1	Inspur_config_g3/1#**spanning-tree mstp point-to-point force-true**	设置端口连接方式为点到点。

序号	配置	说明
2	Inspur_config_g3/1#spanning-tree mstp point-to-point force-false	设置端口连接方式为非点到点。
3	Inspur_config_g3/1#spanning-tree mstp point-to-point auto	自动检测端口的连接方式（默认）。

激活多生成树兼容模式

本公司交换机支持的 **MSTP** 协议是基于 IEEE 802.1Q 标准实现的，为了与某些其它的 **MSTP** 实现兼容--主要是 **Cisco** 交换机在早期支持的 **MSTP** 协议可以工作在多生成树兼容模式。工作在 **MSTP** 兼容模式的交换机可以识别其它多生成树协议的报文结构，检查其中包含的多生成树区域标识信息，并与之建立多生成树区域。

MSTP 兼容模式的工作方式与 **STP** 兼容模式相同，都是依赖 **MSTP** 的协议转换机制实现的：如果交换机的一个端口收到兼容模式的 **BPDU**，该端口就会自动迁移到该模式运行，发送兼容模式的 **BPDU**。如果希望将端口恢复为标准的多生成树模式，请使用 **spanning-tree mstp migration-check** 命令。

序号	配置	说明
1	Inspur_config#spanning-tree mstp mst-compatible	激活交换机的 MST 兼容模式。

兼容模式的主要作用是使交换机可以与运行其它**MSTP** 协议的交换机建立多生成树区域，在实际组网时，请确保交换机具有相同的配置名称和修订号，并建议将运行其它**MSTP** 协议的交换机配置为**CIST** 的根，以保证交换机可以通过接收报文而进入兼容模式。

如果没有激活MST 兼容模式，交换机将不会解析兼容**BPDU** 的全部内容，而是仅将其当 作普通的**RSTP BPDU** 对待，这样交换机就不能与相连的兼容**MSTP** 交换机处在同一区 域中。

对一个已经处在兼容模式的端口，即使通过全局命令关闭交换机的兼容模式，该端口也不会自动恢复到发送标准的**MST BPDU**，这时，请使用**migration-check** 命令。

配置端口的 TCN 限制

配置端口的 **TCN** 限制可以使端口不传播拓扑变化到其它端口。

序号	配置	说明
1	Inspur_config-g3/1#spanning-tree mstp restricted-tcn	使端口不传播拓扑变化到其它端口

配置端口的角色限制

配置端口的角色限制可以使端口不被选为根端口。在端口配置模式下。

序号	配置	说明
1	Inspur_config_g3/1#spanning-tree mstp restricted-role	使端口不被选为根端口

查看多生成树协议信息

在监控模式、全局配置模式以及端口配置模式下，使用下面的命令查看多生成树协议的各种信息：

序号	配置	说明
1	Inspur_config#**show spanning-tree**	查看生成树协议信息。 （**SSTP，PVST，RSTP，MSTP** 通用）
2	Inspur_config#**show spanning-tree detail**	查看生成树协议详细信息。 （**SSTP，PVST，RSTP，MSTP** 通用）
3	Inspur_config#**show spanning-tree interface** *interface-type interface-number*	查看生成树协议端口信息。 （**SSTP，PVST，RSTP，MSTP** 通用）
4	Inspur_config#**show spanning-tree mstp**	查看所有多生成树实例。
5	Inspur_config#**show spanning-tree mstp region**	查看多生成树区域配置。
6	Inspur_config#**show spanning-tree mstp instance** *instance-id*	查看某一个多生成树实例信息。
7	Inspur_config#**show spanning-tree mstp detail**	查看多生成树详细信息。
8	Inspur_config#**show spanning-tree mstp interface** *interface-type interface-number*	查看多生成树端口配置。
9	Inspur_config#**show spanning-tree mstp protocol-migration**	查看端口的协议转换状态。

4.4.4 配置 MSTP 示例

1. 组网需求

如下图所示，三台交换机设备组成环形网络运行 MSTP 协议

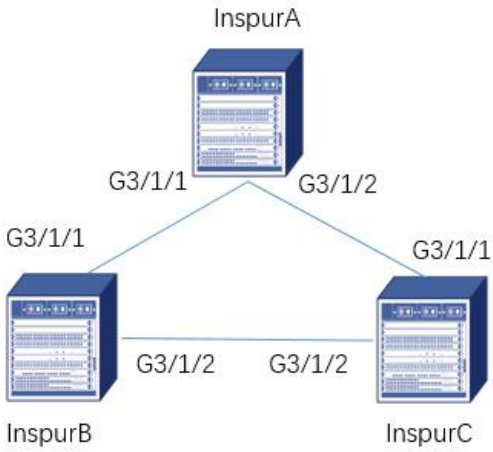


图 4.4.1 MSTP

配置序号

1.在三台交换机上分别创建 **VLAN 3** 和 **VLAN** 4 并激活，

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

3. **Inspur A**、**Inspur B**、**Inspur C** 设置生成树模式为 **MSTP**，并开启生成树协议。

配置 Inspur A

Inspur_config#spanning-tree mode mstp

Inspur_config#spanning-tree mstp name A

Inspur_config#spanning-tree mstp instance 1 **vlan** 3

Inspur_config#spanning-tree mstp instance 2 **vlan** 4

Inspur_config#spanning-tree mstp 1 priority 0

Inspur_config#spanning-tree mstp 2 priority 4096

Inspur_config#interface gigaEthernet3/1/1

Inspur_config_ GE 3/1/1#**Switchport** mode trunk

Inspur_config#Exit

Inspur_config#interface gigaEthernet3/1/2

Inspur_config_ GE 3/1/2#**Switchport** mode trunk

配置 Inspur B

Inspur_config#spanning-tree mode mstp

Inspur_config#spanning-tree mstp name 1

Inspur_config#spanning-tree mstp instance 1 vlan 3

Inspur_config#spanning-tree mstp instance 2 vlan 4

Inspur_config#spanning-tree mstp 1 priority 4096

Inspur_config#spanning-tree mstp 2 priority 8192

Inspur_config#interface gigaEthernet3/1/1

Inspur_config_g3/1/1#Switchport mode trunk

Inspur_config#Exit

Inspur_config#interface gigaEthernet3/1/2

Inspur_config_g3/1/2#Switchport mode trunk

配置 Inspur C

Inspur_config#spanning-tree mode mstp

Inspur_config#spanning-tree mstp name 1

Inspur_config#spanning-tree mstp instance 1 vlan 3

Inspur_config#spanning-tree mstp instance 2 vlan 4

Inspur_config#spanning-tree mstp 1 priority 8192

Inspur_config#spanning-tree mstp 2 priority 0

Inspur_config#interface gigaEthernet3/1/1

Inspur_config_g3/1/1#Switchport mode trunk

Inspur_config#Exit

Inspur_config#interface gigaEthernet3/1/2

Inspur_config_g3/1/2#Switchport mode trunk

3.通过 show spanning-tree 来查看生成树状态

InspurA
Inspur_config#show spanning-tree

Spanning tree enabled protocol MSTP

MST00

Root ID Priority 32768

Address 8479.73BB.29A2

Port TGigaEthernet0/2

Cost 0

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768 (priority 32768 mst-id 0)

Address 8479.73BB.3908

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Pri.Nbr Type

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

tg0/1 Altn BLK 2000 128.81 P2p

tg0/2 Root FWD 2000 128.82 P2p

tg0/11 Desg FWD 2000 128.91 Edge

MST01

Root ID Priority 1

Address 8479.73BB.3908

This bridge is the root

Bridge ID Priority 1 (priority 0 mst-id 1)

Address 8479.73BB.3908

Interface Role Sts Cost Pri.Nbr Type

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

G3/1/1 Desg FWD 2000 128.81 P2p

G3/1/2 Desg FWD 2000 128.82 P2p

MST02

Root ID Priority 2

Address 8479.73BB.29A2

Port TGigaEthernet0/2

Cost 2000

Bridge ID Priority 4098 (priority 4096 mst-id 2)

Address 8479.73BB.3908

Interface Role Sts Cost Pri.Nbr Type

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

G3/1/1 Desg FWD 2000 128.81 P2p

G3/1/2 Root FWD 2000 128.82 P2p

InspurB

Inspur_config#show spanning-tree

Spanning tree enabled protocol MSTP

MST00

Root ID Priority 32768

Address 8479.73BB.29A2

Port TGigaEthernet0/3

Cost 0

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768 (priority 32768 mst-id 0)

Address 8479.73BB.2F56

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface	Role	Sts	Cost	Pri.Nbr	Type
G3/1/1	Desg	FWD	2000	128.81	P2p
G3/1/2	Root	FWD	2000	128.83	P2p

MST01

Root ID Priority 1

Address 8479.73BB.3908

Port TGigaEthernet0/1

Cost 2000

Bridge ID Priority 4097 (priority 4096 mst-id 1)

Address 8479.73BB.2F56

Interface	Role	Sts	Cost	Pri.Nbr	Type
G3/1/1	Root	FWD	2000	128.81	P2p
G3/1/2	Desg	FWD	2000	128.83	P2p

MST02

Root ID Priority 2

Address 8479.73BB.29A2

Port TGigaEthernet0/3

Cost 2000

Bridge ID Priority 8194 (priority 8192 mst-id 2)

Address 8479.73BB.2F56

Interface	Role	Sts	Cost	Pri.Nbr	Type
G3/1/1	Altn	BLK	2000	128.81	P2p
G3/1/2	Root	FWD	2000	128.83	P2p

Inspurc

Inspur_config#show spanning-tree

Spanning tree enabled protocol MSTP

MST00

```
  Root ID     Priority    32768
              Address     8479.73BB.29A2
              This bridge is the root
              Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32768  (priority 32768 mst-id 0)
              Address     8479.73BB.29A2
              Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
Interface        Role Sts Cost      Pri.Nbr Type
---------------- ---- --- --------- -------- --------------------------
G3/1/1           Desg FWD 2000      128.82   P2p
G3/1/2           Desg FWD 2000      128.83   P2p
MST01
  Root ID     Priority    1
              Address     8479.73BB.3908
              Port        TGigaEthernet0/2
              Cost        2000
  Bridge ID   Priority    8193  (priority 8192 mst-id 1)
              Address     8479.73BB.29A2
Interface        Role Sts Cost      Pri.Nbr Type
---------------- ---- --- --------- -------- --------------------------
G3/1/1           Root FWD 2000      128.82   P2p
G3/1/2           Altn BLK 2000      128.83   P2p
MST02
  Root ID     Priority    2
              Address     8479.73BB.29A2
              This bridge is the root
  Bridge ID   Priority    2  (priority 0 mst-id 2)
              Address     8479.73BB.29A2
Interface        Role Sts Cost      Pri.Nbr Type
---------------- ---- --- --------- -------- --------------------------
G3/1/1           Desg FWD 2000      128.82   P2p
G3/1/2           Desg FWD 2000      128.83   P2p
```

4.5 PVST

4.5.1 简介

SSTP 模式下，整个网络仅有一个生成树实例，交换机端口在生成树中的状态将决定它在所有 **VLAN** 中的状态。在网络中存在多个 **VLAN** 的情况下，单生成树协议与 **VLAN** 拓扑的这种隔离状态可能导致部分网络的正常通信被阻塞。

交换机支持在一定数目的 **VLAN** 上运行独立的 **SSTP**，保证端口可以在不同的 **VLAN** 中具有不同的状态。同时也可以实现 **VLAN** 之间的流量均衡。

需要注意的是，可以独立运行生成树协议的 **VLAN** 数目取决于实际版本，超出数目限制的其它 **VLAN** 拓扑将不受 **STP** 控制。

4.5.2 配置准备

场景

VLAN 隔离与冗余：中小型企业通常会根据部门或业务功能划分 **VLAN**，PVST 为每个 **VLAN** 提供独立的生成树实例，能实现不同 **VLAN** 之间的隔离，并且每个 **VLAN** 都有自己的冗余路径。比如财务部门和销售部门属于不同 **VLAN**，**PVST** 可确保每个部门的网络在链路出现故障时都能快速切换到备用路径，不影响业务运行。

负载均衡需求：企业内部可能有多种业务流量，如数据传输、视频会议等，通过 **PVST** 可以根据不同 **VLAN** 的流量特点，将流量分配到不同的物理链路上，实现负载均衡，提高网络资源的利用率，避免某条链路因流量过大而出现拥塞。

4.5.3 PVST 配置

VLAN STP 配置任务

序号	配置	说明
1	Inspur_config#**spanning-tree mode pvst**	启动按 **VLAN** 分配 STP 的模式。
2	Inspur_config#**spanning-tree vlan** vlan-list	为指定 **VLAN** 分配 STP 实例。 **vlan-list**：**VLAN** 列表（下同）。
3	Inspur_config#**spanning-tree vlan** vlan-list **priority** value	配置指定 **VLAN** 中生成树的优先级。
4	Inspur_config#**spanning-tree vlan** vlan-list **forward-time** value	配置指定 **VLAN** 的 **Forward Delay**。
5	Inspur_config#**spanning-tree vlan** vlan-list **max-age** value	配置指定 **VLAN** 的 **Max-age**。
6	Inspur_config#**spanning-tree vlan** vlan-list **hello-time** value	配置指定 **VLAN** 的 **Hello-time**
7	Inspur_config_g3/1#**spanning-tree vlan** vlan-list **cost** value	配置端口在指定 **VLAN** 的路径开销。
8	Inspur_config_g3/1#**spanning-tree vlan** vlan-list **port-priority** value	配置端口在 **VLAN** 中的优先级。

监控 PVST 信息

序号	配置	说明
1	Inspur_config#show spanning-tree vlan vlan-list	查看 VLAN 中生成树状态。
2	Inspur_config#show spanning-tree pvst instance-list	查看 PVST 实例与 VLAN 的对应关系

4.6 生成树参数配置

4.6.1 简介

本公司交换机的生成树协议模块支持七种额外的附加功能（下称为“可选特性”），这些功能在缺省情况下是没有配置的，各种生成树协议模式对可选特性的支持情况如下表所示。

可选特性	Single STP	PVST	RSTP	MSTP
Port Fast	Yes	Yes	No	No
BPDU Guard	Yes	Yes	Yes	Yes
BPDU Filter	Yes	Yes	No	No
Uplink Fast	Yes	Yes	No	No
Backbone Fast	Yes	Yes	No	No
Root Guard	Yes	Yes	Yes	Yes
Loop Guard	Yes	Yes	Yes	Yes

4.6.2 配置准备

场景

在使用生成树的过程中，会用到其他附加特性配置。

4.6.3 生成树参数配置

配置 Port Fast

Port Fast 特性在 **SSTP/PVST** 模式下使一个端口立刻进入 **Forwarding** 状态而不需经过从 **Listening** 到 **Learning** 的状态等待。其它生成树模式下该功能无效。

序号	配置	说明
1	Inspur_config#spanning-tree portfast default	全局启动 Port Fast 功能，对所有端口有效。

序号	配置	说明
2	Inspur_config#spanning-tree portfast	对当前端口启动 Port

配置 BPDU Guard

BPDU Guard 特性在端口收到 **BPDU** 时执行保护动作，配置了该特性的端口不会再发送 **BPDU**。

在不同的生成树协议模式下，**BPDU Guard** 的行为有所不同。在 **SSTP/PVST** 模式下，一个配置了 **BPDU Guard** 和 **Port Fast** 特性的端口如果收到 **BPDU**，该端口会被强制 **shutdown**，此后用户只能通过手动配置将其恢复。在 **RSTP/MSTP** 模式下，一个配置了 **BPDU Guard** 的端口如果收到 **BPDU**，该端口会在一段时间内被设置为 **Blocking** 状态。

序号	配置	说明
1	Inspur_config#spanning-tree portfast bpduguard	全局启动 BPDU Guard 功能，对所有端口有效。
2	Inspur_config_g3/1#spanning-tree bpduguard enable	启动端口的 BPDU Guard 功能
3	Inspur_config_g3/1#spanning-tree bpduguard disable	关闭端口的 BPDU Guard 功能，不影响全局配置。

配置 BPDU Filter

BPDU Filter 特性可以在 **SSTP/PVST** 模式下使交换机的端口不向外发送 **BPDU**，同时也是对 **Port Fast** 端口的另一种保护手段。

序号	配置	说明
1	Inspur_config#spanning-tree portfast bpdufilter	全局启动 BPDU Filter 功能，对所有端口有效。
2	Inspur_config_g3/1#spanning-tree bpdufilter enable	启动端口的 BPDU Filter 特性。
3	Inspur_config_g3/1#panning-tree bpdufilter disable	关闭端口的 BPDU Filter 特性，不影响全局配置。

配置 Uplink Fast

Uplink Fast 特性在交换机到网络根桥的连接中断的情况下，使新的根端口快速进入 **Forwarding** 状态。 **Uplink Fast** 特性仅在 **SSTP/PVST** 模式下有效。

序号	配置	说明
1	Inspur_config#spanning-tree uplinkfast	启动 Uplink Fast 特性。

配置 Backbone Fast

Backbone Fast 特性是对 **Uplink Fast** 技术的补充。**Uplink Fast** 在到达指派交换机的直接连接中断的情况下使冗余线路快速开始工作，而 **Backbone Fast** 则可以检测上一层网络中发生的、非直连的网络中断，并加速端口的状态变化。**Backbone Fast** 特性仅在 **SSTP/PVST** 模式下有效。

序号	配置	说明
1	Inspur_config#spanning-tree backbonefast	启动 Backbone Fast 特性。

配置 Root Guard

Root Guard 特性可以防止一个端口因为收到高优先级的 **BPDU** 而变为 **Root** 端口。

Root Guard 特性在 **SSTP/PVST** 和 **RSTP/MSTP** 中的行为有所不同。在 **SSTP/PVST** 模式下，**Root** 端口总是会被 **Root Guard** 阻塞；而在 **RSTP/MSTP** 中，端口只有在收到更高级的 **BPDU** 之后才会被 **Root Guard** 阻塞，一个原本就具有 **Root** 角色的端口是不会被阻塞的。

序号	配置	说明
1	Inspur_config#spanning-tree guard root	在端口启动 Root Guard。
2	Inspur_config#spanning-tree guard none	关闭端口的 Root Guard 和 Loop Guard 特性。

配置 Loop Guard

Loop Guard 特性在一个 **Root Port** 或 **Alternate Port** 变为 **Designated Port** 之后对其进行保护，该功能可以防止因为端口无法持续收到 **BPDU** 而造成环路。 **STP** 可选特性配置 **Loop Guard** 特性在 **SSTP/PVST** 和 **RSTP/MSTP** 中的行为有所不同。在 **SSTP/PVST** 模式下，**Designated** 端口总是会被 **Loop Guard** 阻塞；而在 **RSTP/MSTP** 中，端口只在因为不能收到 **BPDU** 而变为 **Designated** 端口之后才会被阻塞，一个因为收到低优先级 **BPDU** 而具有 **Designated** 角色的端口是不会被 **Loop Guard** 阻塞的。

序号	配置	说明
1	Inspur_config#spanning-tree loopguard default	全局启动 Loop Guard 特性，对所有端口有效。
2	Inspur_config_g3/1#spanning-tree guard none	启动端口的 Loop Guard 特性。
3	Inspur_config_g3/1#spanning-tree guard none	关闭端口的 Root Guard 和 Loop Guard 特性。

配置地址表老化保护

在网络拓扑变化频繁的情况下，配置地址表老化保护功能可以避免生成树协议因频繁更新

MAC 地址表而影响通信。

快速收敛的生成树协议，比如 **RSTP** 和 **MSTP**，在检测到生成树拓扑发生变化时，会对交换机的 **MAC** 地址表执行清除操作，删除旧的 **MAC** 地址，加速 **MAC** 地址的更新，从而确保通信可以快速恢复。在缺省配置下，交换机通过 **MAC** 地址表快速老化的方式完成清除操作。对于大多数型号的交换机，地址表的快速老化可以在 1 秒钟以内完成，并且对设备 **CPU** 的性能影响极小。

开启地址表老化保护功能之后，**STP** 协议会在执行第一次老化后启动保护定时器，定时器超时之前（缺省为 15 秒）不会再执行老化。若在 15 秒内又发生了网络拓扑变化，协议会在定时器超时之后自动执行第二次老化。

序号	配置	说明
1	Inspur_config#**spanning-tree fast-aging**	启动/关闭地址表老化功能。
2	Inspur_config#**spanning-tree fast-aging protection**	启动/关闭地址表老化保护功能。
3	Inspur_config#**spanning-tree fast-aging protection time** value	配置地址表老化保护的时间。在此时间之内，生成树协议只能执行一次地址表老化。 缺省为 15 秒。

配置 FDB-Flush

交换机的快速生成树协议（**RSTP** 和 **MSTP**）在缺省配置下使用地址表快速老化的方式清除旧的 **MAC** 地址，而非 **FDB-Flush**。

序号	配置	说明
1	Inspur_config#**spanning-tree fast-aging flush-fdb**	开启 **FDB-Flush**

需要注意的是 **FDB-Flush** 与快速老化功能相互独立，可以在配置 **no spanning-treefast-aging** 的同时配置 **FDB-Flush**。但快速老化保护功能对 **FDB-Flush** 无效。

配置 BPDU Terminal

默认情况下，在无生成树运行的情况下，我司设备会对收到的 **BPDU** 进行转发。**BPDUTerminal** 功能可以在无生成树运行的情况下禁止转发 **BPDU**。

序号	配置	说明
1	Inspur_config#**spanning-tree bpdu-termina**	开启 **BPDU Terminal**。

4.7 环路检测

4.7.1 简介

网络中的环路会导致设备对广播、组播以及未知单播等报文进行重复发送，造成网络资源的浪费甚至导致网络瘫痪。为了能够及时发现二层网络中的环路问题，以避免对整个网络造成严重影响，需要提供一种检测功能，使网络中出现环路时能及时通知用户检查网络连接和配置情况，并能够将出问题的端口进行受控操作。**Loopback Detection**（环路检测）功能可以检测设备的端口是否发生环回，它通过从端口定时发送检测报文，并检测该报文是否能够从发出去的接口送回来。当设备发现接口存在环回情况，可以及时通过发送告警信息到网管系统，使管理人员及时发现并解决网络问题，避免长时间断网现象。此外，设备还可以进行端口受控，根据需求选择配置阻端接口、禁止端口 **MAC** 学习、关闭端口（**error-disable**）三种处理方式，能迅速将环回对网络的影响降低至最小。

本公司交换机支持的环路检测特性比较丰富，主要有：

- 支持配置端口的环路检测功能
- 支持配置环路检测报文的目的 **MAC** 地址，可以对每个端口发送的环路检测报文进行配置
- 支持配置端口对指定的 **VLAN** 进行环路检测，最多支持对 10 个 **VLAN** 进行环路检测
- 支持配置端口环路检测报文的发送周期和端口进行受控操作后的恢复周期
- 支持对端口进行受控操作，主要有阻塞端口、禁止端口的 **MAC** 地址学习、关闭端口（**error-disable**）三种处理方式
- 支持对端口默认是否存在环路进行配置操作

4.7.2 配置准备

场景

端口环路检测功能用于检测端口下是否存在环路。可以设置端口发送环路检测报文的时间间隔。

4.7.3 环路检测配置

配置全局的环路检测功能

全局打开或关闭环路检测功能，全局命令默认对所有物理端口生效。全局配置相当于一个开关，只有当全局命令开启后，端口上开启的环路检测功能才会生效。如果端口上未开启环路检测功能，则端口配置不生效。

序号	配置	说明
1	Inspur_config#**loopback-detection**	开配置全局环路检测功能

配置端口的环路检测功能

在指定端口上打开或关闭环路检测功能。需要全局上开启环路检测功能后，端口配置才会生效。

序号	配置	说明
1	Inspur_config_g3/1#**loopback-detection enable**	配置端口环路检测功能

配置端口对指定 VLAN 进行环路检测

配置对指定 **VLAN** 的环回检测功能后，端口会定时发送多份带指定 **VLAN Tag** 的检测报文，一个接口最多可发送 10 份带指定 **VLAN Tag** 的检测报文。

需要注意的是端口必须存在于所配置的 **VLAN** 内，否则配置失效，且配置的 **VLAN** 必须创建，具体为，如果端口在 **VLAN2-VLAN8** 内进行环路检测，如果端口配置成 **trunk** 模式，且 **trunk vlan-allowed** 为 **VLAN** 5-8，那么交换机发出的带 2-4**tag** 的报文会无法从端口出去导致配置失效，同时 **trunk vlan-untagged** 需要配置为包括 2-8 使出去的报文都能带上 **vlan tag**，且相关 **VLAN** 必须创建，否则那些带该 **VLAN id** 的 **tag** 会失效。

序号	配置	说明
1	Inspur_config_g3/1# **loopback-detection vlan-control** *vlanlist*	配置端口对指定 **VLAN** 进行环路检测

配置端口的环路检测周期（报文发送周期、端口受控恢复周期）

序号	配置	说明
1	Inspur_config_g3/1#**loopback-detection hello-time** *time*	配置端口环路检测报文发送的周期

由于网络是处于一个时刻变化中，因此环路检测是一个持续的过程。端口以一定的时间间隔周期性的发送环路检测报文。这个时间间隔即环路检测报文的发送周期，系统默认时间为 3 秒。

序号	配置	说明
1	Inspur_config_g3/1#**loopback-detection recovery-time** *time*	配置端口环路检测报文发送的周期

设置当环路消失后，端口的自动恢复时间。默认当端口 10 秒内没有收到发出去的环路检测报文，就认为环路消失。建议恢复时间至少是报文发送时间的 3 倍；如果发送周期配置的很小，恢复时间建议至少比发送周期多 10S。

配置端口的受控功能

序号	配置	说明
1	Inspur_config_g3/1#**loopback-detection control {block|learning|shutdown}**	配置端口的环路检测受控功能

当端口检测到该端口下的网络存在环路时，可以根据配置的受控功能来对端口进行相应的受控操作，端口的受控状态有 **block**（堵塞端口），**nolearn**（禁止 MAC 地址学习），**shutdown**（**error-disable** 关闭端口），**trap**（接口只上报告警）。当配置了任何一种受控状态且发现端口下存在环路时，都会发送 trap 告警信息。缺省情况下为 **trap** 配置。

全局开启环路检测之后，通过开启环路检测功能的端口发送环路检测报文后，该端口又收到了之前发送的环路检测报文，则会该端口进行下面四种受控操作：

Block：堵塞端口.当检测到环路时，将该端口与其它端口隔离，进入该端口的数据报文无法转

发给其它端口。使该端口处于 **protocol down** 状态同时老化该端口的 **MAC** 地址表。

Nolearn：禁止端口 **MAC** 地址学习。当检测到环路时，该端口将不再进行 **MAC** 地址学习同时老化该端口的 **MAC** 地址表。

shutdown: 关闭端口。当检测到环路时，除了发送 **trap** 告警信息和老化端口的 **MAC** 地址表，还将自动关闭该端口（**error-disable**），使其不能收发报文。直到 **err-disable-recover** 时间到。

Trap： 端口只上报告警：当检测到环路时，端口只上报告警和老化端口的 **MAC** 地址，无其他动作，端口的默认受控配置即为 **trap** 操作。

当端口在 **block** 状态时，将无法转发进入该端口的数据报文，同时端口会继续发送环路检测报文，当检测到环路消失时，端口将自动恢复。默认在 10s 内没收到发出去的环路检测报文，认为环路消失。当端口处在 **block** 状态时。

Block 状态时，端口协议为 **down**，而 **shutdown** 状态时，端口链路直接 **down**。

配置端口环路检测帧的上限值

序号	配置	说明
1	Inspur_config_g3/1#**loopback-detection frames-threshold** *frames-threshold*	配置端口环路检测帧的上限值

当端口的受控配置为 **block**，开启端口的帧数检测功能时，如果收到的本端口发送的环路检测报文大于设置的帧数阈值，则端口 **err-disable shutdown**，系统默认值为 10。

配置端口的帧数检测功能

序号	配置	说明
1	Inspur_config_g3/1#**loopback-detection frames-monitor**	配置端口帧数检测功能

配置端口发送的环路检测报文的目的 MAC 地址

序号	配置	说明
1	Inspur_config_g3/1#**loopback-detection dest-mac** *Mac-address*	配置端口发送环路检测报文的目的 MAC 地址

系统默认发出的环路检测报文的目的 **MAC** 地址为 01-80-C2-00-00-0a，如果用户进行了配置则按照用户配置的 **MAC** 地址作为环路检测报文的目的 MAC 地址。

配置端口默认存在环路问题

序号	配置	说明
1	Inspur_config_g3/1#**loopback-detection existence**	配置端口默认是否存在环路问题

主要为配置当端口起来和端口环路检测功能生效的时候是否认为该端口下存在环路问题。当端口的受控功能配置为 **shutdown** 时，不宜将端口下配置成存在环路问题，因为处于 **shutdown** 状态的话端口已经不转发报文了。默认配置为认为端口下不存在环路。

监控环路检测信息

主要用来显示全局的一些环路检测配置和信息，主要包括全局的配置，以及各个端口下是否发现环路问题，以及端口的一些配置信息。

序号	配置	说明
1	Inspur_config#**show loopback-detection interface** *intf*	显示端口的环路检测配置信息
2	Inspur_config#**show loopback-detection**	显示全局的环路检测配置信息

4.7.4 配置环路检测示例

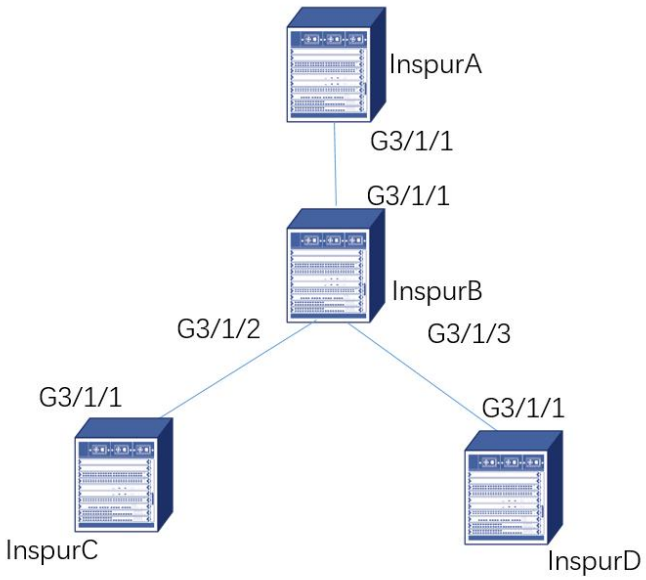


图 4.7.1 环路检测

如图 4.8 所示，交换机 **InspurA** 的端口进行对指定 **VLAN**（1,2,3）的环路检测，需要在各个交换机上进行这样的配置：

交换机 InspurA：

Inspur_config_g3/1/1#**switchport trunk vlan-untagged 1-3**

Inspur_config_g3/1/1#**switchport mode trunk**

Inspur_config_g3/1/1#**loopback-detection enable**

Inspur_config_g3/1/1#**loopback-detection control block**

Inspur_config_g3/1/1#**loopback-detection vlan-control 1-5**

Inspur_config#**loopback-detection**

Inspur_config#**vlan 1-3**

交换机 InspurB：

Inspur_config_g3/1/1#**switchport mode trunk**

Inspur_config_g3/1/2#**switchport mode trunk**

Inspur_config_g3/1/3#**switchport mode trunk**

Inspur_config#**vlan1-3**

交换机 InspurC

Inspur_config_g3/1/1#**switchport pvid 3**

如果连接的 **InspurC** 网络存在环路，如 **InspurC** 在某个端口下存在环路且该端口的 **PVID** 为 3，则会报文会回传到 **InspurA** 的 G3/1/1，**InspurA** 发现环路问题后会对端口 G3/1/1 进行 **block** 受控操作。

4.8 端口镜像

4.8.1 简介

端口镜像是将网络设备上指定端口接收或发送的报文复制到目的端口，可以只复制端口接收或者发送的报文，也可以同时复制接收和发送的报文。指定端口称为镜像端口，目的端口称为观察端口。

4.8.2 配置准备

场景

为了方便对交换机进行管理，可以通过配置端口镜像，使用交换机某一个端口来对流经一组端口的流量进行观察。

4.8.3 端口镜像配置

配置端口镜像

端口镜像可以分为本地镜像和远程镜像。本地镜像是指将报文复制到本设备的端口，远程镜像功能可以使报文跨越多个网络设备、送达远端设备。端口镜像以镜像组的方式进行配置，相关的概念包括源端口、目的端口、远程镜像 **VLAN**、远程镜像 **TPID**、**VLANDISABLE-LEARNING** 等。

序号	配置	说明
1	Inspur_config#**mirror session** session_number {**destination** {interface interface-id} [**rspan** vid [tpid]] | **source** {interface interface-id [, | -] [rx | tx both] }	配置端口镜像。 session-number 为端口镜像编号 。 destination 为镜像目的端口 。 vid 为远程镜像 tag 的 vid。 tpid 为远程镜像 tag 的 tpid source 为镜像源端口 。 Interface-id 为端口号。 rx 表示只镜像输入数据。tx 表示只镜像输出数据，both 表示输入输出数据均镜像。

配置远程镜像 vlan

在远程镜像中，通过远程镜像 **vlan** 来识别不同远程镜像组之间的报文。同时，为了将镜像报文送到从本地设备送至远端设备，需要在中间设置上关闭远程镜像 **vlan** 的 **macaddress** 学习能力，实现镜像报文在中间设备上的广播，从而将报文送达远端。在配置远程镜像 **vlan** 之前，需要先创建该 **vlan**。

序号	配置	说明
1	Inspur_config#**vlan disable-learning** { word | **add** word |**remove** word}	|配置远程镜像 **vlan**。 **word** 为 **vlan** 信息

查看端口镜像配置

序号	配置	说明
1	Inspur_config#**show mirror** [session session_number]	显示端口镜像信息。**session-number** 为端口镜像编号(1-4)。

4.8.4 配置端口镜像示例

把 InspurA 的 G3/1 口流量镜像到 G3/2 的服务器上。

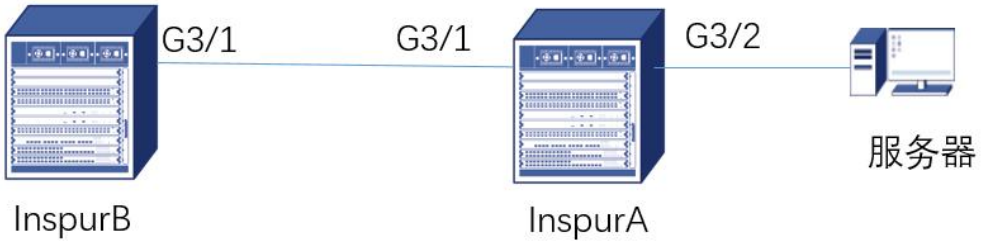


图 4.8.1

InspurA 配置

Inspur_config#**mirror session 1 destination interface g3/2**

Inspur_config#**mirror session 1 source interface g3/1 both**

4.9 VRRP

4.9.1 简介

虚拟路由冗余协议(**Virtual Router Redundancy Protocol**) 消除了在静态缺省路由环境下的单点服务失败的风险。**VRRP** 可避免静态指定网关的缺陷。通过 **VRRP**，一组路由交换机可以一起协同工作，共同组成一台虚拟路由交换机。该虚拟路由交换机对外配有一个虚拟 **IP** 地址和虚拟 **MAC** 地址，**VRRP** 从路由交换机组中选出一台作为 **master**，负责转发数据包。当主路由交换机发生故障时，备份路由交换机会迅速接管主路由交换机，主机不必改变缺省网关地址，且此过程对于终端系统是透明的。这样就提供了在故障发生时更快、更有效的解决方法。

4.9.2 配置准备

场景

可以在主机的下一跳设备出现故障时，及时将业务切换到备份设备，从而保障网络通信的连续性和可靠性。

4.9.3 VRRP 配置

配置 VRRP 虚拟 IP 地址

序号	配置	说明
1	Inspur_config_v1#**vrrp** vrid **associate** virtual-address address-mask	配置端口下 **VRRP** 的虚拟 IP 地址

配置 **VRRP** 的虚拟地址后就开启了该虚拟路由交换机，虚拟地址必须和该端口的 **primary IP** 地址在同一网段，否则虚拟路由交换机将一直停在 **Init** 状态。当虚拟地址和端口 **primary IP** 地址一致时，系统将自动提升该虚拟路由交换机的优先级为 255。

配置 VRRP 验证方式

序号	配置	说明
1	Inspur_config_v1#**vrrp** vrid **authentication** WORD	配置 **VRRP** 验证方式为 **simple-text**。

simple-text 验证方式下，验证字符串将以明码方式放入报文里转发出去，接收者将报文中携带的验证字符串和本地配置的验证字符串匹配检验，验证字符串不超过 8 个字符。 缺省状态下，**VRRP** 不进行验证。

配置 VRRP 优先级抢占

序号	配置	说明
1	Inspur_config_v1#**vrrp** vrid **preempt** [delay second]	配置 **VRRP** 优先级抢占。

优先级抢占只对处于 **Backup** 下的路由交换机有效，当收到由 **master** 路由交换机发送来的 **advertise** 报文后，当检测到 **master** 的优先级没有本地配置的优先级高时，如果 **Backup** 路由交换机配置了优先级抢占，**Backup** 路由交换机将从 **Backup** 状态跃迁到 **master** 状态，并向外发送 **advertise** 报文。反之，则继续停留在 **Backup** 状态。 缺省方式是优先级抢占。

配置 VRRP 协议报文 mac 地址

序号	配置	说明
1	Inspur_config_v1#**vrrp** vrid **source-mac-use-system**	配置 **VRRP** 组使用系统 **mac** 地址发送报文。

默认情况下，**VRRP** 的协议报文使用协议 **mac** 地址作为源地址发送；配置该命令后，**VRRP** 的协议报文使用系统 **mac** 地址作为源地址发送。

配置 VRRP 优先级

序号	配置	说明
1	Inspur_config_v1#**vrrp** vrid **priority** value (**1~254**)	配置 **VRRP** 优先级。

当虚拟地址和端口地址一致时，**VRRP** 会自动提升优先级为 255，当虚拟地址或者端口地址发生变化后，优先级值会自动恢复到原来配置的值。

配置 VRRP 时钟值

序号	配置	说明
1	Inspur_config_v1#**vrrp** vrid **timers advertise** { value | **dsec** value | **csec** value }	配置 **VRRP** 时钟值。

配置 VRRP 监控对象

序号	配置	说明
1	Inspur_config_v1#**vrrp** vrid **track interface** intf-id value	配置 **VRRP** 监控本地端口状态。
2	Inspur_config_v1#**vrrp** vrid **track ip** ip-address value	配置 **VRRP** 监控到指定地址的状态。

通过配置监控功能，**VRRP** 组能够针对链路状态的变化适时调整其优先级，提供了主线路状态变化时切换至备用线路的机会。这种链路状态变化不是指 **VRRP** 路由交换机本身是否可达，而是经由该 **VRRP** 路由交换机的目的链路是否可达。

VRRP 支持两种监控对象。第一种是监控端口状态，当被监控的端口链路状态为 **down** 时，

主动降低本身的优先级；第二种是监控到指定节点的状态，当不可达时，主动降低本身的优先级。

配置 VRRP BFD 快速检测

序号	配置	说明
1	Inspur_config_v1#**vrrp** vrid **bfd fast-detect peer** A.B.C.D	配置 **VRRP BFD** 快速检测。

VRRP 的监控与维护

序号	配置	说明
1	Inspur_config#**show vrrp** { brief | [interface vlan_intf] [detail]}	显示 **VRRP** 信息。

4.9.4 配置 VRRP 示例

使 **InspurA** 上业务起到冗余作用

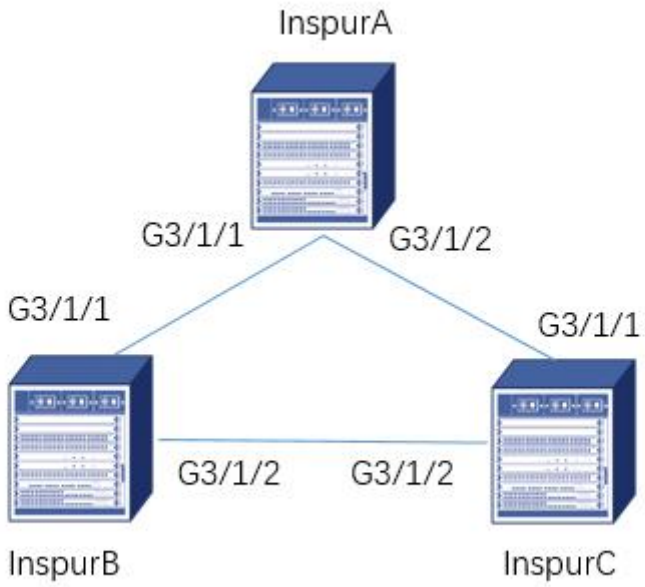


图 4.9.1

InspurB:

Inspur_config#**int vlan 1**

Inspur_config_v1#**vrrp 1 associate 192.168.1.254 255.255.255.0**

Inspur_config_v1#**vrrp 1 priority 150**

Inspur_config#**int vlan 2**

Inspur_config_v2#**vrrp 2 associate 192.168.2.254 255.255.255.0**

Inspur_config_v2#**vrrp 2 priority 150**

Inspur_config#**int vlan 3**

Inspur_config_v3#**vrrp 3 associate 192.168.3.254 255.255.255.0**

Inspur_config_v3#**vrrp 3 priority 150**

InspurC:

Inspur_config#**int vlan 1**

Inspur_config_v1#**vrrp 1 associate 192.168.1.254 255.255.255.0**

Inspur_config#**int vlan 2**

Inspur_config_v2#**vrrp 2 associate 192.168.2.254 255.255.255.0**

Inspur_config#**int vlan 3**

Inspur_config_v3#**vrrp 3 associate 192.168.3.254 255.255.255.0**

维护 vrrp

Inspur#**show vrrp brief**

Interface Grp Prio Pree State Master addr Virtual addr

v10 10 150 Y Master 192.168.10.1 192.168.10.254

4.10 端口隔离

4.10.1 简介

端口隔离（**Port Isolation**） 是一种网络技术，用于限制同一交换机上不同端口之间的通信，确保某些端口之间无法直接通信，从而增强网络的安全性和灵活性。端口隔离通常用于多租户环境、公共网络或需要严格隔离的场景。

4.10.2 配置准备

场景

在正常情况下，交换机的不同端口间的数据包能够自由的转发。在某些情况下，需要禁止端口之间的数据流，端口隔离功能就是提供这种控制的。隔离端口之间不能进行数据通信，非隔离端口之间以及隔离端口和非隔离端口之间的数据包仍然能够正常转发。

4.10.3 端口隔离配置

端口隔离配置

序号	配置	说明
1	`Inspur_config_g3/1#Switchport protected`	开启/取消端口隔离功能

4.10.4 配置端口隔离示例

1.非基于组的隔离

隔离端口之间不能进行数据通信:

例如 1 和 2 是隔离端口 则 1 和 2 之间不可以通信非隔离端口之间以及隔离端口和非隔离端口之间的数据包仍然能够正常转发;

例如 3 是非隔离的端口，非隔离的端口它们之间可以通信，同样 1 和 3，2 和 3 也可以通信;

Inspur_config#**int g3/1**

Inspur_config_g3/1#**switchport protected**

Inspur_config_g3/1#int g0/2

Inspur_config-g3/2#switchport protected

2.基于组的隔离

组内隔离端口之间不能进行数据通信 //一个组内的端口不能通信但可以和组外任意端口之间进行数据通信

Inspur_config#**port-protected18**

Inspur_config#**int g3/1**

Inspur_config_g3/1#**switchport protected 10**

Inspur_config_gi3/1#**int g3/2**

Inspur_config_g3/2#**switchport protected 10**

4.11 Keepalive

4.11.1 简介

Keepalive 环路检测是一种用于检测网络中是否存在环路的机制。环路（**Loop**）是指数据包在网络中无限循环，导致网络拥塞、性能下降甚至瘫痪。**Keepalive** 环路检测通过发送特定的探测包（如 **Keepalive** 报文）并结合网络设备的响应行为，判断是否存在环路。

4.11.2 配置准备

场景

在以太网交换机中，**Keepalive** 环路检测用于防止广播风暴。

4.11.3 Keepalive 配置

Keepalive 配置

序号	配置	说明
1	Inspur_config_g3/1#**keepalive** [second]	配置端口发送环路检测报文时间间隔。**second** 为发送报文的时间间隔。范围为 0-32767，默认为 12.

4.11.4 配置 Keepalive 示例

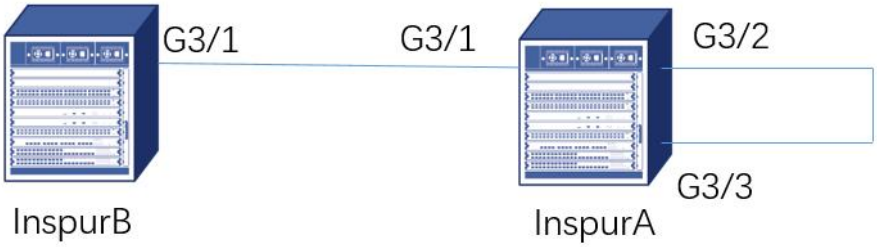


图 4.11.1

将 **InspurA** 的 G3/2 和 G3/3 端口相连，形成回环，在 **InspurB** 的 G3/1 端口配置 **keepalive**。

InspurB 配置：

Inspur_config#**interface GigaEthernet3/1**

Inspur_config_g3/1#**keepalive**

5 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。

- **IP** 访问列表
- **IP v6** 访问列表
- **MAC** 访问列表
- **802.1x**
- **AAA**
- **DOS** 防攻击配置
- **IP** 防攻击配置
- 防止攻击
- 风暴抑制
- **DHCP**
- **DHCP Snooping**
- **DHCPv6**
- **BFD** 配置
- **flow-control**

5.1 IP 访问列表

5.1.1 简介

IP 访问列表是应用 **IP** 地址的允许和禁止条件的有序集合。本公司路由交换机的 **ROS** 软件在访问列表中逐个按规则测试地址。第一个匹配决定是否该软件接受或拒绝该地址。

因为在第一个匹配之后，该软件停止了匹配规则，所以条件的先后次序是重要的。如果没有规则匹配，拒绝该地址。 在使用访问列表中有以下两个步骤：

(1) 通过指定访问列表名及访问条件，建立访问列表。

(2) 将访问列表应用到端口。

5.1.2 配置准备

场景

过滤报文帮助控制包在网络中的运动。这样的控制可以帮助限制网络传输并通过一定的用户或设备限制网络使用。为了从交叉指定的端口中使包有效或无效，本公司路由交换 机提供了访问列表。可以用以下方式使用访问列表：

- 控制在端口上的包传输
- 控制虚拟终端线路访问
- 限制路由更新内容 。

5.1.3 配置 IP 访问列表

请在设备上进行以下配置。步骤 2～步骤 3 请根据需要选择配置。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	**Inspur_config#ip access-list standard** *name*	使用名字定义一个标准的 **IP** 访问列表。
3	**Inspur_config_std# deny** *{source [source-mask] | any}* or **permit** *{source [source-mask] | any}*	在标准访问列表配置模式下，指定一个或多个允许或不允许条件。这决定该包通过还是不通过。
4	**Inspur_config#**Exit	退出访问列表配置模式。
5	**Inspur_config#ip access-list extended** *name*	使用名字定义一个扩展的 **IP** 访问列表。

序号	配置	说明
6	**Inspur_config_ext# {deny | permit}** *protocol source source-mask destination destination-mask* **[precedence** *precedence*] **[tos** *tos*] **{deny | permit}** *protocol* **any any**	在扩展访问列表配置模式下，指定一个或多个 允许或不允许条件。这决定该包通过还是不通过。（**precedence** 表示 **ip** 包优先级，**TOS** 表示 **Type of Service**）
7	**Inspur_config#**Exit	退出访问列表配置模式。

将访问列表应用到端口

配置时间段

请在设备上进行以下配置。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**Time-range time** Inspur_config_tr#**periodic weekdays** *00:00 to 08:00* Inspur_config_tr#**periodic weekdays** *11:00 to 23:59*	创建时间段，可应用于 **ACL** 规则。

重要说明：

匹配 **ttl** 的 **acl** 不支持 **gt/lt** 参数，为硬件限制

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_config#**show ip access-list** *[name]*	查看 **ACL** 信息。
2	Inspur#**show time-range** [*time-range-name*]	查看时间段配置相关信息。
3	Inspur_config#**show ip access-list** *[name]* config-list	查看本地访问控制 **ACL** 列表信息。

5.1.4 扩展 IP 访问列表示例

在以下例子中，第一行允许新来的 **TCP** 与主机 130.2.1.2 的 **SMTP** 端口连接。

ip access-list extended aaa

permit tcp any 130.2.1.2 255.255.255.255 eq 25

interface g1/10

ip access-group aaa

5.2 IPv6 访问列表

5.2.1 简介

IPv6 访问列表是应用 **IPv6** 地址的允许和禁止条件的有序集合。本公司路由交换机的 **ROS** 软件在 **IPv6** 访问列表中逐个按规则测试 **IPv6** 地址。第一个匹配决定是否该软件接受或拒绝该地址。

因为在第一个匹配之后，该软件停止了匹配规则，所以条件的先后次序是重要的。如果没有规则匹配，默认拒绝该地址。

在使用 **IPv6** 访问列表中有以下两个步骤：

1.建立访问列表

通过指定访问列表名及访问条件，建立 **IPv6** 访问列表。条件可以基于 **IPv6** 源地址、目的地址、协议类型或其他字段。

2.将访问列表应用到接口

创建的 **IPv6** 访问列表需要应用到相应的接口上，以控制进入（**inbound**）或离开（**outbound**）该接口的流量。

5.2.2 配置准备

场景

过滤报文帮助控制包在网络中的运动。这样的控制可以帮助限制网络传输并通过一定的 用户或设备限制网络使用。为了从交叉指定的端口中使包有效或无效，本公司路由交换 机提供了访问列表。可以用以下方式使用访问列表：

- 控制在端口上的包传输
- 控制虚拟终端线路访问
- 限制路由更新内容 。

5.2.3 配置 IPv6 访问列表

请在设备上进行以下配置。步骤 2～步骤 3 请根据需要选择配置。

序号	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur_config# ipv6 access-list standard` *`name`*	使用名字定义一个 **IPv6** 访问列表。

序号	配置	说明
3	Inspur_ config_ipv6acl# **deny** *{source [source-mask] | any}* or **permit** *{source [source-mask] | any}*	在标准访问列表配置模式下，指定一个或多个允许或不允许条件。这决定该包通过还是不通过。
4	Inspur_ config_ipv6acl#**Exit**	退出访问列表配置模式。

将访问列表应用到端口

请在设备上进行以下配置。

序号	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，以下以物理接口模式为例进行说明。
3	Inspur_config_g0/1#**ipv6 access-group** *Inspur*	在接口上应用 **ACL**。
4	Inspur_config_g0/1#**exit**	返回全局配置模式。

配置时间段

请在设备上进行以下配置。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**Time-range time** Inspur_config_tr#**periodic weekdays** *00:00 to 08:00* Inspur_config_tr#**periodic weekdays** *11:00 to 23:59*	创建时间段，可应用于 **ACL** 规则。

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_config#**show ip access-list** *[name]*	查看 **ACL** 信息。
2	Inspur#**show time-range** [*time-range-name*]	查看时间段配置相关信息。
3	Inspur_config#**show ip access-list** *[name]* config-list	查看本地访问控制 **ACL** 列表信息。

5.2.4 扩展 IPv6 访问列表示例

在以下例子中，拒绝 2001:1::2/128 主机与 1000 2002:1::2 主机的 udp 的 2000 端口号连接。

```
ipv6 access-list 1
 deny udp 2001:1::2/128 eq 1000 2002:1::2/128 eq 2000 sequence 20
 permit ipv6 any any sequence 30
interface  g1/10
ipv6 access-group 1
```

5.3 MAC 访问列表

5.3.1 简介

MAC 访问控制列表（**ACL**）是基于 **MAC** 地址的允许或禁止条件的有序集合，用于控制二层网络设备（如交换机）对以太网帧的转发决策。设备会按照规则的顺序逐一匹配帧的源或目的 **MAC** 地址，首个匹配的规则将决定是否允许或拒绝该帧通过。若未匹配任何规则，默认行为是拒绝该帧。

5.3.2 配置准备

场景

- 防止非法设备接入网络
- 限制设备间的二层通信
- 隔离广播风暴或未知单播泛洪。

5.3.3 配置 MAC 访问列表

请在设备上进行以下配置。步骤 2～步骤 3 请根据需要选择配置。

序号	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur_config#[no] mac access-list` *name*	添加/删除一个 **MAC** 访问列表。**name** 为 **MAC** 访问列表的名称。

序号	配置	说明
3	Inspur-config-macl#**[no] {deny | permit} {any | host** *src-mac-addr*} **{any |** *dst-mac-addr*}[*ethertype*]	添加/删除一个 **MAC** 访问列表条目，可以重复该命 令来添加/删除多个 **MAC** 访问列表条目。 **any** 表示匹配任何 **MAC** 地址；**src-mac-addr** 为源 **MAC** 地址； **dst-mac-addr** 为目的 **MAC** 地址； **ethertype** 为匹配的以太网数据包的类型。
4	Inspur-config-macl#**Exit**	退出 **MAC** 访问列表配置模式。

将访问列表应用到端口

请在设备上进行以下配置。

序号	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，以下以物理接口模式为例进行说明。
3	Inspur_config_g0/1#**[no] mac access-group** *name*	在接口上应用 **ACL**。
4	Inspur_config_g0/1#**exit**	返回全局配置模式。

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_config#**show mac access-list** *[name]*	查看 **ACL** 信息。

5.3.4 扩展 MAC 访问列表示例

在以下例子中，拒绝主机 bc60.6bb6.1111 与 bc60.6bb6.2222 主机的通信。

```
mac access-list mac
    deny host bc60.6bb6.1111 host bc60.6bb6.2222
    permit any any
interface gigaEthernet 3/5
    mac access-group mac
```

5.4 802.1x

5.4.1 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，如下图所示，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。

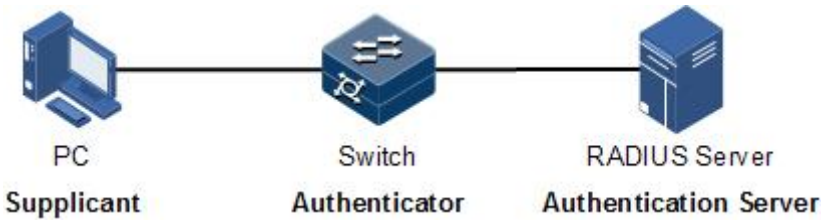


图 5.4.1 802.1x 认证体系结构

接口接入控制模式

802.1x 定义了三种端口的控制方式：强制认证通过、强制认证不通过和启动 802.1x 认证。强制认证通过，表示端口已经认证通过，不需要在使用任何认证过程对端口进行认 证，所有的用户都可以通过该端口进行数据访问控制；该模式是端口的默认模式。 强制认证不通过，表示端口认证不通过，即使使用任何认证手段对端口进行认证， 该端口都不会认证通过，所有的用户都无法通过该端口进行数据访问控制。 启动 802.1x 认证，即端口将运行 802.1x 认证协议，对访问该端口的用户进行 802.1x 认证，只有认证通过后用户都可以通过该端口进行数据访问控制。启动端口的 802.1x 的认证后还要配置 AAA 的认证方法。

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：

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；

认证者向申请者发送 **EAP-Request/Identity** 报文，询问请求者的用户名；

申请者响应一个 **EAP-Response/Identity** 给认证者，其中包括用户名信息；

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；

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；

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；

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。

5.4.2 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。

5.4.3 配置 802.1x 认证

配置端口的 802.1x 认证

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。

在配置 802.1x 前，必须将 802.1x 功能使能，使用下面的命令可以使能 802.1x。

序号	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# **aaa authentication dot1x** {*default* | *list name*} **method**	配置 802.1x 的 AAA 认证。
4	Inspur_config#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
5	Inspur_config_g3/1#**dot1x port-control auto**	使能接口 802.1x 功能。
6	Inspur_config_g3/1#**dot1x port-control force-authorized**	配置端口强制认证通过。。
7	Inspur_config_g3/1#**dot1x port-control force-unauthorized**	使能端口强制认证不通过。

配置 802.1x 多主机端口认证

请在设备上进行以下配置。

激活 802.1x 多主机端口认证，可以在接口配置模式下使用下面的任意一个命令：

序号	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。

序号	配置	说明
3	Inspur_config_g3/1#**dot1x authentication multiple-hosts**	配置 802.1x 多主机端口认证。只需要一台主机 认证通过，端口就 up。
4	Inspur_config_g3/1#**dot1x authentication multiple-auth**	设置 802.1x 多主机端口认证。需要所有主机都 认证通过，端口才 **up**。

配置 802.1x 重认证

重认证功能是在认证通过后，为了保证认证客户端的合法性，间隔一段时间后还会向客户端进行 认证，这时就需要启动重认证功能。启动重认证功能，当端口认证通过以后，将会周期性的向主机进行认证请求。

请在设备上进行以下配置。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**dot1x re-authentication**	进入二层物理接口配置模式。
3	Inspur_config#**dot1x timeout re-authperiod** *time*	配置重认证的周期。
4	Inspur_config#**dot1x reauth-max** *time*	配置重认证失败后的重试次数。

配置控制 802.1x 发送频率

请在设备上进行以下配置。

802.1x 认证过程中，它会向客户主机发送数据报文，通过控制 802.1x 发送频率可以 调节数据发送以保证客户主机的响应。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**idot1x timeout tx-period** *time*	设定 802.1x 报文发送频率。

配置 802.1x 用户绑定

请在设备上进行以下配置。

802.1x 认证时，可以将用户与某一个端口进行绑，保证端口访问的安全。启动 802.1x 用户绑定功能，可以在接口配置模式下使用下面的命令：

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

序号	配置	说明
2	Inspur_config#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
3	Inspur_config_g3/1#**dot1x user-permit** *User name*	配置重认证定时器时间。

配置 802.1x 端口的认证方法

802.1x 认证时不同的端口可以使用不同的认证方法，缺省时，802.1x 认证使用 default 方法。 配置 802.1x 认证方法，可以在接口配置模式下使用下面的命令：

序号	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_g3/1#**dot1x authentication method** *name*	配置 802.1x 认证方法。

配置 802.1x 端口的认证类型

802.1x 认证时可以选择认证类型，该类型将决定 AAA 使用 Chap 或 Eap 认证(eap

认证支持 **md5-challenge** 和 eap-tls 方式)；使用 **Chap** 时 **MD5** 所需的 **challenge** 将在本地产生，而使用 **Eap** 时 **challenge** 将认证服务器上产生；每一个端口只使用一种认证类型，默认情况下该类型使用全局配置的认证类型，当端口配置了认证类型时就一直使用该认证类型，除非使用 **No** 命令恢复到默认值。

eap-tls 采用电子证书作为认证凭证，遵循 **tls(Translation Layer Security)**中 **handshake** 协议规范，具有更好的安全性。

配置认证类型，可以在全局配置模式下使用下面的命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config# **dot1x authen-type** {*chap*|*eap*}	选择 **chap** 或 **eap**
3	Inspur_config#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
4	Inspur_config_g3/1#**dot1x authentication type** {*chap*/*eap*}	选择 **chap** 或 **eap** 或使用全局下的配置类型。

配置 802.1x 记帐

采用 **dot1x** 认证的同时，可以进行记帐，实现机制是，在 **dot1x** 认证通过后，判断是否在该认证接口下打开了记帐功能，如果是，则使用 AAA 接口发送记帐请求，在收到 AAA 模块的请求成功信息后，该接口才可以通过报文。

记帐方法可以采用 AAA 配置中各种记帐方法，相关内容请参考 AAA 配置

为了保证记帐信息的准确性，在记帐开始后，**dot1x** 会周期性的使用 AAA 接口向 **server** 端发送 **update** 信息，但根据 AAA 配置的不同，AAA 模块决定是否真正发送该报文。

同时，请打开 **dot1x** 重认证功能，确保 **supplicant** 出现异常时，能够被交换机知晓。

为了打开 **dot1x** 记帐功能及配置记帐采用的方法，可以在接口配置模式下使用下面的命令：

序号	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_g3/1#**dot1x accounting enable**	打开 **802.1x** 记帐功能。
4	Inspur_config_g3/1#**dot1x accounting method** *{method name}*	配置记帐方法，缺省为 **default**。
5	Inspur_config#**aaa accounting update periodic** *<30-120>*	发送记录更新信息的时间间隔（秒）

配置 802.1x guest-vlan

guest-vlan 功能可以在客户端没有响应时，给予相应端口有限的访问权限（例如下载客户端软件）。**guest-vlan** 可以是系统中任何一个已配置的 **vlan**，如果配置的 **guest-vlan** 不满足该条件，则该端口无法进入该 **guest-vlan**。

认证失败没有访问权限。

全局模式下打开 **guest-vlan** 功能，使用下面的命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**dot1x guest-vlan**	在所有端口下打开 **guest-vlan** 功能。

初始时，每个端口的 **guest-vlan id** 为 0,此时即使打开了全局 **guest-vlan** 功能，也不 起作用，只有在端口配置模式下，配置了 **guest-vlan id** 后，**guest-vlan** 才其作用。

端口模式下使用下面命令配置 guest-vlan id:

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

序号	配置	说明
2	Inspur_config#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
3	Inspur_config_g3/1#**dot1x guest-vlan** *{id(1-4094)}*	在端口下配置 **guest-vlan** 的 **vlan id**。

配置禁止拥有多网卡的 Supplicant

禁止拥有多张网络适配器的 Supplicant 端，防止代理的发生。可以在端口配置模式 下使用下面的命令：

序号	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_g3/1#**dot1x forbid multi-network-adapter**	禁止拥有多张网络适配器的 **Supplicant** 端。。

配置 802.1x 恢复默认选项

将所有的全局配置恢复到默认配置。可以在全局配置模式下使用下面的命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**dot1x default**	将所有的全局配置恢复到默认配置。

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-number*]	查看全局或接口 802.1x 配置信息。
2	Inspur#**show dot1x statistics**	查看接口 802.1x 统计信息。

5.4.4 配置 802.1x 示例

组网需求

为了使用户访问外部网络，如下图所示，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。

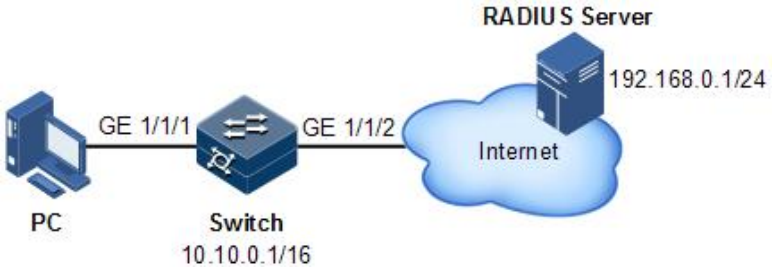


图 5.4.2　802.1x 应用组网示意图

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_v1#**ip address 10.10.0.1 255.255.0.0**

Inspur_config_v1#**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_g3/1#**dot1x enable**

步骤 3 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_g3/1#**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_g3/1)#**dot1x reauthentication enable**

Inspur_config_g3/1#**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: 5(s)
SuppTimeout: 30(s)
ReAuthPeriod: 600(s)
TxPeriod: 30(s)
KeepalivePeriod: 60(s)
MaxUserNum: 512
GuestVlanID: 0
AuthFree Protocol: None
```

5.5 AAA

5.5.1 简介

AAA

AAA（**Authentication**、**Authorization**、**Accounting**，认证、授权、计费）是网络安全的一种管理机制，提供了认证、授权、计费三种安全功能。

认证：确认访问网络的远程用户的身份，判断访问者是否为合法的网络用户。

授权：对不同用户赋予不同的权限，限制用户可以使用的服务。例如，管理员授权办公用户才能对服务器中的文件进行访问和打印操作，而其它临时访客不具备此权限。

计费：记录用户使用网络服务过程中的所有操作，包括使用的服务类型、起始时间、数据流量等，用于收集和记录用户对网络资源的使用情况，并可以实现针对时间、流量的计费需求，也对网络起到监视作用。

AAA 采用客户端/服务器结构，客户端运行于 **NAS**（**Network Access Server**，网络接入服务器）上，负责验证用户身份与管理用户接入，服务器上则集中管理用户信息。

AAA 可以通过多种协议来实现，这些协议规定了 **NAS** 与服务器之间如何传递用户信息。目前设备支持 **RADIUS**（**Remote Authentication Dial-In User Service**，远程用户拨号认证服务）协议和 **TACACS+**（**Terminal Access Controller Access Control System**，终端访问控制器访问控制系统）。

RADIUS

RADIUS（**Remote Authentication Dial In User Service**，远程用户拨号认证服务）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。

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。

TACACS+

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。

5.5.2 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 **RADIUS/TACACS+**服务器对用户进行认证和计费。本设备可以作为 **RADIUS/TACACS+**服务器的代理设备，根据 **RADIUS/TACACS+**服务器反馈的结果对用户访问进行授权。**TACACS+**较 **RADIUS** 更加安全、可靠。

5.5.3 配置 AAA 功能

AAA 认证的一般配置过程 要配置 AAA 认证，需要完成下列配置过程：

- 如果使用的是安全服务器，需要配置安全协议参数，如 **RADIUS**、**TACACS**＋。
- 使用 **aaa authentication** 命令定义认证方法列表。
- 如果需要的话，把方法列表应用到特定的端口或是线路上。

配置 AAA 登录认证

AAA 安全服务使得使用各种认证方法变得更容易了，不论决定使用哪种登录方法，都使用 **aaa authentication** 命令开启 AAA 认证。在 **aaa authentication login** 命令中，创建一张或是多张认证方法的列表，这些列表在登录时使用。使用线路配置命令 **login authentication** 来应用这些列表。

配置时，从全局配置模式开始，使用如下命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**aaa authentication login** *{default | list-name}method1 [method2...]*	创建全局认证列表。
3	Inspur_config#**line [console | vty]** *line-number [ending-line-number]*	配置 **RADIUS** 认证、计费服务器的 **IP** 地址、协议端口号、**key** 和源 **IP** 信息。
4	Inspur_config# **login authentication** *{default | list-name}*	应用该认证列表于某条或是某几个线路上。(在线路模式下)

关键字 **list-name** 是用来命名所创建的列表的任何字符串。关键字 **method** 指定认证过程 所采用的实际方法。仅当前面所用的方法返回认证错误时，才会使用其他的认证方法， 如果前面的方法指明认证失败了，则不再使用其他的认证方法。如果要指定即使所有的 方法都返回认证错误仍能成功登录，只要在命令行中指定 none 作为最后一个认证方法。 使用 **default** 参数可建立一个缺省的列表，缺省列表自动的应用于所有的接口。

例如：指定 **RADIUS** 作为用户登录时的缺省认证方式

使用下面的命令： **aaa authentication login default group radius**

注意：

- 由于关键字 **none** 使得登录的任何用户都可成功的通过认证，所以应当将该关键字作

为备用的认证方法。

- 登陆时，如果找不到认证方法列表的话，除 **console** 口登陆以外，其它任何形式的登陆将以认证失败结束。

下表列出了目前支持的登录认证方式：

关键字	说明
enable	使用 **enable** 口令进行认证。
group name	使用命名的服务器组进行认证。
group radius	使用 **RADIUS** 认证。
line	使用线路密码进行认证。
local	使用本地数据库进行认证。
local-case	使用本地用户名数据库进行认证(用户名区分大小写)。
none	认证无条件通过。

(1)使用 **enable** 口令进行登录认证

在 **aaa authentication login** 命令中使用 **enable** 方法关键字指定 **enable** 口令作为登录认证方法，

例如：在没有定义其他方法时，指定 enable 口令作为登录时用户认证的方法，使用下面的命令：

aaa authentication login default enable

(2) 使用线路口令进行登录认证

在使用 **aaa authentication login** 命令时，用 **line** 方法关键字指定线路口令作为登录时的认证方法。

例如，在用户登录时指定线路口令为用户认证方法，并且不定义,任何其他方法，可以输入下面的命令：

aaa authentication login default line

在能够使用线路口令进行注册认证之前，需要定义一条线路口令。

(3) 使用本地口令进行登录认证

在使用 **aaa authentication login** 命令时，用 local 方法关键字指定使用本地用户名数据库作为登录认证方法。例如，在用户注册时指定本地用户名数据库作为用户认证方法，并且不定义任何其他方法，可以输入下面的命令行：

aaa authentication login default local

(4) 使用 **RADIUS** 进行登录认证

在使用 **aaa authentication login** 命令时，用 **radius** 方法关键字指定 **RADIUS** 作为登录认证方

法。

例如在用户登录时指定 **RADIUS** 为用户认证方法，并且不定义任何其他方法，可以输入下面的命令：

aaa authentication login default radius

在能使用 **RADIUS** 作为注册认证方法之前，需要首先配置 **RADIUS** 服务

配置在进入特权级别时开启口令保护

使用 **aaa authentication enable default** 命令创建一个认证方法列表，这些方法决定了某 个用户是否可以执行特权级别的 **EXEC** 命令。可以至多指定四种认证方法。仅当前面所 用的方法返回认证错误时，才会使用其他的认证方法。如果前面使用的方法返回认证失 败，则不再使用其他的认证方法，如果指定即使所有的方法都返回错误仍能成功认证， 只需在命令中指定 **none** 作为最后一个认证方法。

配置时，在全局配置模式下使用下面的命令：

序号	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur_config#aaa authentication enable` *`default method1 [method2...]`*	在用户进入特权级别时开启口令认证。

关键字 method 指定认证过程使用的实际方法，在认证时依输入的次序使用。

下表列出了所支持的口令保护认证方法：

关键字	说明
`enable`	使用 **`enable`** 口令进行认证。
`group name`	使用命名的服务器组进行认证。
`group radius`	使用 **`RADIUS`** 认证。
`line`	使用线路密码进行认证。
`none`	认证无条件通过。

当配置了 **enable** 认证方法为远端认证时，使用 RADIUS 进行认证，如下面介绍：

使用 **RADIUS** 进行 **enable** 认证：

认证的用户名为**$ENABLE level$**，其中 level 是指用户要进入的特权级别，即 enable

命令后的特权级别的数字，举例来说，如果某用户要进入级别为 7 的特权级别，需要输入命令 **enable** 7，如果此时配置了使用 **RADIUS** 进行认证，则提交给 **Radius-server host** 的用户名为 **$ENABLE7$**，缺省条件下 **enable** 进入的特权级别均为 15，即在使用 **RADIUS** 进行认证时，提交给 **Radius-server host** 的用户名为**$ENABLE15$**。这就需要预先在 **Radius-server host** 上配置相应的用户名和密码，特别要指出的是：

在 **Radius-server host** 的用户数据库中，要指明用于特权认证的用户的服务类型（**Service-Type**）为 6，即 **Admin-User**。

配置 AAA 认证消息标语

支持使用可配置的、个性化的登陆及登陆失败标语。即在用户登陆进入系统将用 AAA 认证时，以及无论什么原因认证失败时，将显示所配置的消息标语。

全局配置模式下，使用下述命令配置注册标语：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**aaa authentication banner** *delimiter text-string delimiter*	配置一个个性化的登陆注册标语。

全局配置模式下，使用下述命令配置登陆失败标语:

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**aaa authentication fail-message** *delimiter text-string delimiter*	配置一个个性化的登陆失败的标语。

注意:

创建标语时，需要配置一个定界符号”，然后再配置文本字符串本身，该定界符号的作用 是通知系统下面的文本字符串将被作为标语显示。定界字符在文本字符串的尾部重复出现，表示标语结束。。

配置改变提示输入用户名时的字符串

使用 **aaa authentication username-prompt** 命令可以改变提示用户输入用户名时所显示的缺省文本。该命令的 **no** 形式恢复口令提示为如下形式的缺省值：

aaa authentication username-prompt 不改变远程 **TACACS＋**或是 **RADIUS** 服务器所提供的任何提示信息。

配置时，在全局模式下使用下面的命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**aaa authentication username-prompt** *text-string*	在提示用户输入用户名时改变缺省的显示文本。

配置本地特权级别认证数据库

创建基于本地的密码数据库，用于控制用户获取各种特权级别，要建立本地各种特权级别的 **enable** 密码数据库，可以在全局配置模式下，使用下面命令进行配置，删除时，利用该命令的 **no** 形式：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**enable password** { [*encryption-type*] **encrypted-password**} [**level** *level*]	建立本地各种特权级别的 **enable** 密码数据库

配置 AAA exec 授权

使用 **aaa authorization** 命令开启 AAA 授权。在 **aaa authorization exec** 命令中，创建一 张或是多张授权方法的列表，开启 **EXEC** 授权，以决定是否允许用户运行 **EXEC** 外壳程 序，或者授于用户在进入 **EXEC** 外壳程序时的特权级别。使用线路配置命令 **login authorization** 来应用这些列表。

配置时，从全局配置模式开始，使用如下命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**aaa authorization exec** *{default | list-name}method1 [method2...]*	创建全局授权列表。
3	Inspur_config#**line [console | vty]** *line-number [ending-line-number]*	进入某个线路的配置状态。
4	Inspur_config_line#**login authorization** *{default | list-name}*	应用该授权列表表于某条或是某几个线路上。

关键字 **list-name** 是用来命名所创建的列表的任何字符串。关键字 **method** 指定授权过程 所采用的实际方法。仅当前面所用的方法返回授权错误时，才会使用其他的授权方法， 如果前面的方法指明授权失败了，则不再使用其他的授权方法。如果要指定即使所有的 方法都返回授权错误仍能进入 **EXEC shell**，只要在命令行中指定 **none** 作为最后一个授权方法。 使用 **default** 参数可建立一个缺省的列表，缺省列表自动的应用于所有的接口。

例如：指定 **RADIUS** 作为 **exec** 的缺省授权方式，使用下面的命令：

aaa authorization exec default group radius

注意：

授权时，如果找不到授权方法列表的话，将不再进行授权服务，并允许授权通过。

5.5.4 配置 RADIUS 功能

配置交换机与 RADIUS 服务器的通信

RADIUS 服务器通常是运行由 **Livingston**、**Merit**、 **Microsoft** 或另外的软件提供商提供的 **RADIUS** 服务器软件的多用户系统，**RADIUS** 服务器和交换机使用共享的密钥来加密口令并交换响应。使用 radius-server host 命令来指定 **RADIUS** 服务器，使用 **radius-server key** 命令来指定共享密钥。

配置时，在全局配置模式下使用下述命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**radius-server host** *ip-address* **[auth-port** *port-number***][acct-port** *port-number***]**	指定远程 RADIUS 服务器的 IP 地址，指定认证和记录的目的端口号。
3	Inspur_config#**radius-server key** *string*	指定交换机和 RADIUS 服务器之间使用的共享密钥。

另外为了定制交换机和 RADIUS 服务器之间的通信，请使用下述可选的 radius 全局配置命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**radius-server retransmit** *retries*	指定交换机在放弃重试之前向服务器传输每个 RADIUS 请求的次数。
3	Inspur_config#**radius-server timeout** *seconds*	指定交换机在重新传输 RADIUS 请求之前，对应答应等待的秒数。
4	Inspur_config#**radius-server deadtime** *minutes*	当 RADIUS 服务器不对认证请求作出反应时，需要将此台服务器标志为“死亡”的持续时间。

配置交换机使用厂商专用的 RADIUS 属性

Internet 工程任务组（**IETF**）草案标准通过使用厂商专用属性（**Attribute26**），为在网络 访问服务器和 **RADIUS** 服务器之间交互基于厂商的专用扩展属性提供了一种方法。厂商 专用属性（**VSA**）允许厂商支持属于它们自己的不适合于普遍用途的扩展属性。有关厂 商 **ID** 和厂商专用属性的更多信息，请参 **RFC 2138**：远程认证拨号用户服务（**RADIUS**）。

要使网络访问服务器，使其能够识别和使用厂商专用属性，请在全局配置模式下使用下述命令：

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

序号	配置	说明
2	Inspur_config#**radius-server vsa send** *[authentication]*	使网络访问服务器能够如同 RADIUS IETF 属性 26 所定义的那样去识别和使用厂商专用属性。。

配置 RADIUS 认证

在标识了 **RADIUS** 服务器并定义了 **RADIUS** 认证密钥之后，就需要为 **RADIUS** 认证定义 方法列表。由于 **RADIUS** 认证是通过 **AAA** 来进行的，所以需要输入 **aaa authentication** 命令，指定 **RADIUS** 作为认证方法。

配置 RADIUS 授权

利用 **AAA** 授权可以设置参数、限制用户的网络访问。使用 **RADIUS** 的授权提供了一种远 程访问控制的方法，包括一次性授权或对每个服务的授权。因为 **RADIUS** 授权是通过 **AAA** 进行的，所以需要使用 **aaa authorization** 命令，指定 **RADIUS** 作为授权方法。

配置 RADIUS 记录

AAA 记录特性让我们能够追踪用户正在访问的服务及他们占用的网络资源数量。由于 **RADIUS** 记录特性是通过 **AAA** 提供的，所以需要使用 **aaa accounting** 命令，指定 **RADIUS** 作为记录方法。

5.5.5 配置 TACACS+功能

配置指定 TACACS+服务器

tacacs-server 命令使你能够指定 **TACACS**+服务器的 **IP** 地址。由于 **TACACS**+软件按照 配置的顺序搜索主机，这一特色对于设置不同的服务器优先级是有用的。

为了指定 **TACACS**+主机，以全局配置模式使用下述命令

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**tacacs-server host** *ip-address*[**single-connection| multi-connection**][**port** *integer*] [**timeout** *integer*] [**key** *string*]	指定 TACACS+服务器 IP 地址及相应属性。

使用 **tacacs-server** 命令，还可以配置下述选项：

- 使用 tacacs-server 命令，还可以配置下述选项：
- 使用 single-connection 关键字指定采用单一连接,这样做允许服务器程序处理更多的

TACACS＋操作，可能更有效。multi-connection 则是指示采用多条 TCP 连接。

- 使用 port 参数，指定 TACACS+服务器程序使用的 TCP 端口号。缺省的端口号是 49。
- 使用 timeout 参数，指定路由器等待服务器回应的时间上限（以秒为单位）。
- 使用 key 参数指定对报文进行加密和解密的密钥

注意：

使用 **tacacs-server** 后接 **host**，再接 **timeout** 等命令指定的超时值将覆盖 **tacacs-server timeout** 命令设置的全局超时值； 使用 **tacacs-server** 指定的加密密钥将覆盖使用全局配 置命令 **tacacs-server key** 设置的缺省密钥。所以可以使用本命令配置唯一的 **TACACS+** 连接来加强网络的安全性。

配置 TACACS+加密密钥

为了设置 **TACACS**+报文加密密钥，在全局配置模式使用下述命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**tacacs-server key** *keystring*	设置与 TACACS+服务器所使用密钥相匹配的加密密钥。

注意：

为了成功地进行加密，必须对 TACACS+服务器程序配置相同的密钥。

配置使用 TACACS+进行认证

在标识了 **TACACS**+服务器并定义了与之相联系的加密密钥后，就需要为 **TACACS**+认证 定义方法列表。由于 **TACACS**+认证通过 **AAA** 进行操作，所以需要设置 **aaaauthentication** 命令指定 **TACACS**+作为其认证方法。

配置使用 TACACS+进行授权

AAA 授权使得能够设置参数限制用户的网络访问权限。**TACACS**+授权，可以应用于命令、网络连接和 **EXEC** 会话等服务。由于 **TACACS**+授权是通过 **AAA** 提供的，所以需要配置 **aaa authorization** 命令指定 **TACACS**+作为授权方法。

配置使用 TACACS+进行记录

AAA 记录使得能够跟踪用户正在使用的服务以及他们消耗的网络资源的数量。由于 **TACACS**+记录是通过 **AAA** 提供的，所以需要配置 **aaaaccounting** 命令指定 **TACACS**+ 作为记录方法。

5.5.6 AAA 认证配置示例

RADIUS 认证示例

下面是一个使用 AAA 命令集定义通用配置的示例：

```
radius-server host 1.2.3.4
 radius-server key myRaDiUSpassWoRd
 username root password AlongPassword
 aaa authentication login admins group radius local
 line vty 1 16
 login authentication admins
```

在这个示例中，各命令行的意义为：

radius-server host 命令定义 RADIUS 服务器的 IP 地址；**radius-server key** 命令定义网络访问服务器和 RADIUS 服务器主机之间的共享密钥；**aaa authentication login admins group radius local** 命令定义了认证方法列表 **admins**，它指定首先通过 RADIUS 进行认证，然后（若 RADIUS 服务器不响应）使用本地认证；**login authentication admins** 命令指定在登录认证中运用 **admins** 方法列表；

TACACS+认证示例

TACACS+认证示例：

下述示例配置 login 认证由 TACACS+完成：

```
aaa authentication login test group tacacs+ local
 tacacs-server host 1.2.3.4
 tacacs-server key testkey
 line vty 0
 login authentication test
```

在这个示例中：

aaa authentication 命令定义了运行在 **vty0** 上使用的认证方法列表 **test**。关键字 **tacacs+** 意味着认证通过 TACACS+进行，如果 TACACS+在认证期间不响应，则关键字 **local** 指示使用网络访问服务器上的本地数据库进行认证。

tacacs-server host 命令标识 TACACS+服务器的 IP 地址为 1.2.3.4。**tacacs-server key** 命令定义共享的加密密钥为 **testkey**。

下述示例将 TACACS+配置为 login 认证时使用的安全协议，但是不再使用方法列表 test，

而是使用方法列表 default：

```
aaa authentication login default group tacacs+ local
 tacacs-server host 1.2.3.4
```

tacacs-server key goaway

在这个示例中：

aaa authentication 命令定义 **login** 认证时使用的默认认证方法列表 **default**。如果需要认证，那么关键字 **tacacs+**意味着认证通过 **TACACS+**进行，如果 **TACACS+**在认证期间不响应，则关键字 **local** 指示使用网络访问服务器上的本地数据库进行认证。

tacacs-server host 命令标识 **TACACS+**服务器程序的 **IP** 地址为 1.2.3.4。**tacacs-server key** 命令定义共享的加密密钥为 **goaway**。

TACACS+授权示例：

aaa authentication login default group tacacs+ local

aaa authorization exec default group tacacs+

tacacs-server host 10.1.2.3

tacacs-server key goaway

在这个示例中：

aaa authentication 命令定义 **login** 认证时使用的默认认证方法列表 **default**。如果需要认证，那么关键字 **tacacs+**意味着认证通过 **TACACS+**进行，如果 **TACACS+**在认证期间不响应，则关键字 **local** 指示使用网络访问服务器上的本地数据库进行认证。

aaa authorization 命令配置通过 **TACACS+**进行网络服务授权。

tacacs-server host 命令标识 **TACACS+**服务器 **IP** 地址为 10.1.2.3。**tacacs-server key** 命令定义共享的加密密钥为 **goaway**。

TACACS+计费示例：

下述示例配置 login 认证的方法列表使用 TACACS+作为方法之一，并配置通过 TACACS+

进行计费：

aaa authentication login default group tacacs+ local

aaa accounting exec default start-stop group tacacs+

tacacs-server host 10.1.2.3

tacacs-server key goaway

在这个示例中：

aaa authentication 命令定义 **login** 认证时使用的默认认证方法列表 **default**。如果需要认证，那么关键字 **tacacs+**意味着认证通过 **TACACS+**进行，如果 **TACACS+**在认证期间不响应，则关键字 **local** 指示使用网络访问服务器上的本地数据库进行认证。

aaa accounting 命令配置通过 **TACACS+**进行网络服务的计费。在这个示例中，计费服务开始和结束时的相应信息，发送到 **TACACS+**服务器。

tacacs-server host 命令标识 **TACACS+**服务器的 **IP** 地址为 10.1.2.3。**tacacs-server key** 命

令定义共享的加密密钥为 goaway

5.6 DOS 防攻击配置

5.6.1 简介

分布式拒绝服务攻击（**DDoS**）和单一来源的拒绝服务攻击（**DoS**）已成为影响网络正常运行的主要安全威胁之一。这些攻击通过大量伪造的流量或特定攻击手段，迅速消耗网络带宽、计算资源或目标设备的处理能力，导致网络瘫痪或服务不可用。为此，交换机设备通常需要配备强大的防御功能，以保障网络的稳定性和安全性。

Inspur 交换机提供了多种 **DoS** 防护机制，通过灵活配置和精细化策略，能够有效识别并防止各类 **DoS** 攻击类型。这些防护措施不仅针对常见的 **ICMP**、**TCP** 等攻击方式，还包括更为复杂的如 **Smurf** 攻击、**SYN** 洪水攻击等，能够实现对网络安全的全面防护。通过配置相关的防御策略，设备能够及时检测并阻止恶意流量，保障网络环境的正常运行。

5.6.2 配置准备

为了有效应对 **DoS**（拒绝服务）攻击，保障网络设备和数据的安全，交换机提供了多种防御措施。这些防护措施可以帮助识别并阻止各种类型的恶意流量，防止网络资源被滥用，确保设备和网络的稳定运行。为实现这一目标，设备提供了多种 **DoS** 防护配置选项，通过合理配置可以有效防范不同类型的攻击。

在进行 **DoS** 防护配置前，需要了解以下几点准备工作：

明确防护需求：根据网络环境的具体需求，确定需要防护的 **DoS** 攻击类型。例如，是否需要防止 **ICMP DoS** 攻击（如 **Ping** 洪水攻击）、**SYN** 洪水攻击、**TCP** 头部非法攻击等。通过对网络流量的分析，了解可能遭遇的攻击类型，从而定制防护策略。

配置相关接口与端口：**DoS** 防护配置通常与网络设备的端口、接口及 **VLAN** 相关。根据网络架构，识别关键的网络接口和端口，并确保防护策略能够有效应用到这些端口上。

启用流量监控：在实施 **DoS** 防护配置之前，确保启用适当的流量监控工具和日志记录机制。这将帮助及时识别异常流量，并为防护策略的调整提供依据。

选择适合的防护方式：根据不同的 **DoS** 攻击类型，选择合适的防护方式。例如：

- 对于 Ping 洪水攻击（Ping Flood），可启用 pingflood 防护；
- 对于 TCP 的 SYN 洪水攻击，可启用 synflood 防护；
- 对于 TCP 头部异常的攻击，可以启用 tcpflags 防护；
- 对于 IP 报文的分包攻击，可以启用 ipv4firstfrag 和 tcpfrag 防护等。

5.6.3 配置 DOS 防攻击

配置全局 DoS 防护

在全局配置模式使用下述命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**dos enable all**	抵御不同种类的 **dos** 攻击

配置 ICMP DoS 攻击检测

在全局配置模式使用下述命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**dos enable icmp** *<0-1023>*	配置 **ICMP dos** 攻击检测

配置 IP 源地址为目的地址的报文丢弃：

在全局配置模式使用下述命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**dos enable ip**	丢弃源 **IP** 等于目的 **IP** 的报文

配置检查 IP 报文的第一个分包

在全局配置模式使用下述命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config# **dos enable ipv4firstfrag**	配置允许检查 **ip** 报文的第一个分包。

配置源端口号等于目的端口号的 TCP/UDP 报文丢弃

在全局配置模式使用下述命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**dos enable l4port**	丢弃源端口号等于目的端口号的 **TCP/UDP** 报文。

配置 Ping 洪水防护

在全局配置模式使用下述命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**dos enable pingflood**	防护用于阻止通过大量 **Ping** 请求来使目标网络设备崩溃的 **DoS** 攻击。

配置 SYN 泛洪防护

在全局配置模式使用下述命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**dos enable synflood**	防护用于防止通过大量 **SYN** 请求来使目标设备的 **TCP** 连接资源耗尽的 **SYN** 洪水攻击。

配置丢弃非法 TCP 头部的 TCP 报文

在全局配置模式使用下述命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**dos enable tcpflags**	配置用于丢弃带有非法 **TCP** 头部的 **TCP** 报文，以防止基于 **TCP** 标志位的攻击。

配置 TCP 分包 DoS 攻击检测

在全局配置模式使用下述命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config# **dos enable tcpfrag** *<0-255>*	使能 **TCP** 分包 **dos** 攻击检测

配置 TCP Smurf 攻击防护

在全局配置模式使用下述命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**tacacs-server key** *keystring*	设置与 **TACACS+**服务器所使用密钥相匹配的加密密钥。

配置 ICMP Smurf 攻击防护

在全局配置模式使用下述命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**dos enable icmpsmurf**	配置防护用于防止 **ICMP Smurf** 攻击。

配置 IP Smurf 攻击防护：

在全局配置模式使用下述命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**dos enable ipsmurf**	配置防护用于防止 **IP Smurf** 攻击

配置检查

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#**config**	进入全局配置模式。
2	Inspur#**show dos**	显示 **dos** 信息。

5.6.4 配置 DOS 防攻击示例

在全局状态下配置抵御带非法 **flag** 的 **TCP** 报文攻击，并显示用户配置。

config

dos enable tcpflags

show dos

在全局状态下配置抵御源、目的 **IP** 地址相等的 **IP** 报文攻击。

config

dos enable ip

在全局状态下配置抵御最大长度超过 255 的 **ICMP** 报文攻击。

config

dos enable icmp 255

5.7 IP 防攻击配置

5.7.1 简介

为保证网络带宽的合理利用，本公司系列交换机提供了防止恶意 IP 流量大量占用网络带 宽的功能。针对目前最常见的攻击形式，对一段时间内大量发送 ICMP、IGMP 或者 IP 报文的主机进行通信限制，不对这些主机提供任何网络服务。使用该功能可以防止恶意 报文大量占用网络带宽导致网络拥塞的问题。

5.7.2 配置准备

场景

当某台主机在任意指定时间间隔内发送的 **IGMP**, **ICMP** 或者 **IP** 报文数量超过门限时，我 们就认为它对网络造成了攻击。 用户可以选择防止攻击的类型（**ICMP**, **IGMP** 或者 **IP**）、应用防攻击功能的端口和攻击检 测参数。因此用户需要进行的配置任务有：

- 配置 IP 防攻击类型
- 配置 IP 攻击检测参数

5.7.3 配置 IP 防攻击

配置 IP 攻击检测参数

序号	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur_config#ip verify log-enable`	开启/关闭攻击检测的系统日志
3	`Inspur_config#ip verify filter` *`time`*	当识别出攻击源后，对攻击源进行停止服务， 调整单位是秒，默认时间为 180 秒

配置 IP 攻击检测类型

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**ip verify icmp ping-flood** *value*	限制 **ping** 包接收，检测门限为 **value** 个报文
3	Inspur_config#**ip verify icmp ping-sweep** *time*	限制 **ping** 扫描，检测周期为 **time**，单位为秒
4	Inspur_config#**ip verify tcp syn-flood** *value*	限制 **tcp syn** 包接收，检测门限为 **value** 个报文
5	Inspur_config#**ip verify tcp syn-sweep** *time*	限制 **tcp syn** 端口扫描，检测周期为 **time**，单位为秒
6	Inspur_config#**ip verify tcp fin-scan** *time*	限制 **tcp stealth fin** 扫描，检测周期为 **time**，单位为秒
7	Inspur_config#**ip verify tcp rst-flood** *value*	限制 **tcp rst** 包接收，检测门限为 **value** 个报文
8	Inspur_config#**ip verify udp udp-flood** *value*	限制 **udp** 包接收，检测门限为 **value** 个报文
9	Inspur_config#**ip verify udp udp-sweep** *time*	限制 **udp** 扫描，检测周期为 **time**，单位为秒
10	Inspur_config#**ip verify attack Xmas-Tree** *time*	过滤 **Xmas-Tree** 扫描攻击，检测周期为 **time**，单位为秒
11	Inspur_config#**ip verify attack Null-scan** *time*	过滤 **Null** 扫描攻击，检测周期为 **time**，单位为秒
12	Inspur_config#**ip verify attack Land**	过滤 **Land** 攻击
13	Inspur_config#**ip verify attack Smurf**	过滤 **Smurf** 攻击
14	Inspur_config#**ip verify attack WinNuke**	过滤 **WinNuke** 攻击
15	Inspur_config#**ip verify attack TearDrop**	过滤 **TearDrop** 攻击
16	Inspur_config#**ip verify attack Fraggle**	过滤 **Fraggle** 攻击

配置 IP 防攻击功能

当防攻击的全部参数配置完毕后，就可以启动防止攻击功能了。需要指出的是，防止攻击功能是需要消耗少量处理器资源的。如果关闭攻击检测功能，所有被阻塞的攻击源将被解除阻塞。

序号	配置	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#ip verify enable	开启/关闭攻击检测

配置检查

当您启用防止攻击功能后，可以通过命令查看该功能的工作情况。

序号	配置	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#show ip verify status	显示当前 IP 攻击检测状态、防御状态以及攻击者的信息
3	Inspur_config#show ip verify config	显示当前 IP 攻击检测配置

5.7.4 配置示例

请在设备上进行以下配置。用户希望打开防止端口扫描攻击功能，要求任何主机在任何 15 秒内扫描端口超过一次扫描单位时就认为是攻击，对攻击源阻塞网络服务 10 分钟，则应该如下配置：

ip verify icmp ping-sweep 15

ip verify tcp syn-sweep 15

ip verify udp udp-sweep 15

ip verify enable

ip verify log-enable

ip verify filter 600

5.8 防止攻击配置

5.8.1 简介

为保证网络带宽的合理利用，确保网络用户以及设备自身的正常工作，我司以太网交换机系列产品提供了防攻击功能（Filter），用于对恶意流量进行检测和抑制。Filter 能够识别交换机端口上接收的报文，并按照报文类型进行统计。针对目前常见的攻击形式，Filter 可以统计出一段时间内某个主机发送的 ARP、IGMP 或者 IP 报文的数目，一旦数目超限，设备便不再转发该主机的报文。Filter 通过阻塞源地址的方式限制来自特定主机的报文。对于 ARP 攻击，Filter 阻塞源 MAC 地址；而对于 IP 类型的攻击，比如 Ping 扫描和 TCP/UDP 端口扫描，Filter 会阻塞源 IP 地址。

Filter 的模式决定了交换机如何限制已经确定的攻击源，有两种模式可以选择：

- 源地址定时阻塞（Raw）

Raw 模式下，从确定攻击源时开始，交换机会在预先设定的阻塞时间（block-time）内丢弃来自攻击源的报文。超过阻塞时间之后，自动解除对攻击源地址的限制，并启动新一轮统计。

Raw 模式严格按照源地址阻塞报文。比如，在攻击源的 MAC 地址被阻塞之后，所有源 MAC 地址等于该地址的报文，无论 ARP、ICMP、DHCP 或其它类型，都会被丢弃。

- 源地址阻塞加轮询，或称混合模式（Hybrid）

阻塞攻击源之后，交换机继续对来自攻击源的报文进行计数，并在预先设定的轮询时间（Polling Interval）到达时检查这段时间攻击源发送的报文是否仍然超过限制，若超过限制，说明攻击源仍然存在，则保持阻塞状态，若没有超过限制，说明攻击可能已经停止，此时便解除阻塞。在混合模式下，可以对初次确定攻击源时的报文限制数目和轮询检查时的报文限制数目分别进行配置。。使用该功能可以防止恶意 报文大量占用网络带宽导致网络拥塞的问题。

5.8.2 配置准备

场景

为了实现对攻击报文的持续统计，混合模式在阻塞源地址的同时会匹配报文类型。比如，一台主机因发起 ARP 攻击而被阻塞了 MAC 地址，除非该主机也被识别为存在 IP 攻击，否则来自该主机的 IP 报文仍然会被交换机转发。

请根据应用环境选择 Filter 的模式。如果希望对攻击源进行严格的控制，并相对减轻交换机 CPU 的负担，请使用 Raw 模式；如果希望灵活的控制攻击源，并在攻击停止后尽快恢复主机的通信，请使用混合模式。需要注意的是，混合模式交换机能够支持的 Filter 数目是有限的，在数目不足的情况下，会自动使用 Raw 模式阻塞攻击源。

5.8.3 配置防止攻击

当某台主机在任意指定时间间隔内发送的 IGMP,ARP 或者 IP 报文数量超过门限时，就认为它对网络造成了攻击。 Filter 支持选择需要统计的报文类型（ARP，IGMP，IP 等）、应用防攻击功能的端口和攻击检测参数。

配置攻击检测参数

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**filter period** *time*	开启/关闭攻击检测的系统日志
3	Inspur_config#**filter threshold [arp | bpdu | dhcp | igmp | ip | icmp]** *value*	配置各种报文类型的攻击检测门限为 **value** 个报文。
4	Inspur_config#**filter block-time** *time*	配置 **Raw** 模式下对攻击源地址进行阻塞的时间，以秒为单位。

序号	配置	说明
5	Inspur_config#**filter polling period** *time*	配置 **Hybrid** 模式下轮询检查攻击源的周期，单位秒。
6	Inspur_config#**filter polling threshold [arp | bpdu | dhcp | igmp | ip | icmp]** *value*	配置 **Hybrid** 模式轮询检查时的攻击报文门限值
7	Inspur_config#**filter polling auto-fit**	配置 **Hybrid** 模式轮询检查的 **period** 和 **threshold** 参数自动适应攻击源检测的对应参数。该命令缺省有效，轮询的周期等于攻击检测周期，轮询的报文门限值等于攻击检测报文门限值的四分之三。

配置攻击检测类型

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**filter dhcp**	全局启动 **DHCP** 报文攻击检测。
3	Inspur_config#**filter icmp**	全局启动 **ICMP** 报文攻击检测。
4	Inspur_config#**filter igmp**	全局启动 **IGMP** 报文攻击检测。
5	Inspur_config#**filter ip source-ip**	全局启动 **IP** 攻击检测。
6	Inspur_config#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
7	Inspur_config_g3/1#**filter arp**	启动端口的 **ARP** 报文攻击检测。
8	Inspur_config_g3/1#**filter bpdu**	启动端口的 **BPDU** 报文攻击检测。
9	Inspur_config_g3/1#**filter dhcp**	启动端口的 **DHCP** 报文攻击检测。
10	Inspur_config_g3/1#**filter icmp**	启动端口的 **ICMP** 报文攻击检测。
11	Inspur_config_g3/1#**filter ip source-ip**	启动端口的 **IP** 报文攻击检测。

注意：

ARP 攻击将一个“主机 **MAC** 地址+来源端口”二元组作为一个攻击源。也就是说，对 于相同的 **MAC** 地址但从不同端口来的报文，计数不会被累加。而 **IGMP** 和 **IP** 攻击都 将“主机 **IP**+来源端口”作为攻击源。

1、防止 **IGMP** 攻击和防止 **IP** 攻击功能不能同时启动。

2、**IP**、**ICMP** 和 **DHCP** 报文攻击检测需要同时在全局和端口模式配置之后才生效。

配置启用防止攻击功能

当防攻击的全部参数配置完毕后，就可以启动防止攻击功能了。需要指出的是，防止攻击功能是需要消耗少量处理器资源的。如果关闭攻击检测功能，所有被阻塞的攻击源将被解除阻塞。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**filter enable**	启用防止攻击功能
3	Inspur_config#**filter mode [raw | hybrid]**	配置 **Filter** 的模式，**Raw** 或者 **Hybrid**。

注意：

关闭攻击检测功能后，会解除所有被阻塞的攻击源。

配置检查

当您启用防止攻击功能后，可以通过命令查看该功能的工作情况。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**show filter**	查看 **Filter** 的参数设置、被阻塞的攻击源以及正在统计的报文条目。
3	Inspur_config#**show filter summary**	查看 **Filter** 的参数设置和摘要信息。

5.8.4 配置示例

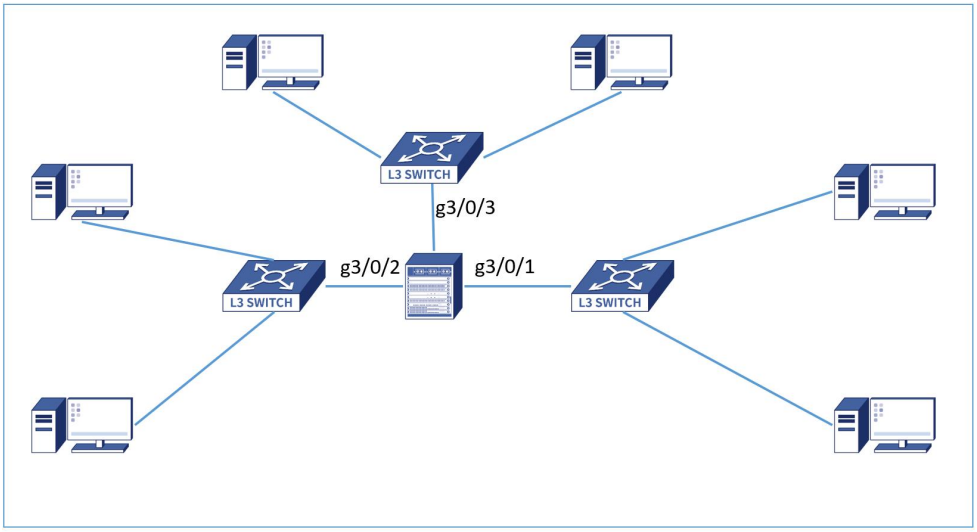


图 5.8.1

请在设备上进行以下配置。用户希望打开防止端口扫描攻击功能，要求任何主机在任何 15 秒内扫描端口超过一次扫描单位时就认为是攻击，对攻击源阻塞网络服务 10 分钟，则应该如下配置：

配置 **Filter** 的参数，判断攻击源的标准为主机 10 秒钟发送超过 100 个 **ARP** 报文：

Inspur# config

Inspur_config# filter period 10

Inspur_config# filter threshold arp 100

配置四个端口的 **ARP** 攻击检测：

Inspur_config# interface range g3/0/1-3/0/3

Inspur_config_intf# filter arp

配置使用 **Raw** 模式，然后启动

Inspur_config# filter mode raw

Inspur_config# filter enable

5.9 风暴抑制

5.9.1 简介

风暴抑制是用于控制广播、未知组播以及未知单播报文，防止这类报文引起广播风暴的安全技术。

通过阻塞报文或关闭接口来阻断广播、未知组播或未知单播报文的流量。此外，风暴控制还支持通过抑制报文来控制报文的平均速率。当流量超过指定的阈值时，系统会执行对应的风暴控制动作。

5.9.2 配置准备

场景

当设备某个二层以太网接口收到广播、未知组播或未知单播报文时，如果根据报文的目的 **MAC** 地址设备不能明确报文的出接口，设备会向同一 **VLAN** 内的其他二层以太接口转发这些报文，这样可能导致广播风暴，降低设备转发性能。风暴控制功能，则可以有效地控制这几类报文流量。

5.9.3 配置风暴抑制功能

配置风暴抑制

请在设备上进行以下配置。

序号	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_g3/1#**storm-control { broadcast | multicast | unicast } threshold** *count*	配置端口的风暴限速功能。 **unicast** 表示对单播起作用； **multicast** 表示对组播起作用； **broadcast** 表示对广播起作用； **count** 表示待配置的阀值。。
4	Inspur_config_g3/1#**storm-controlmode{kbps|pps}**	配置端口风暴控制阈值单位。 **mode** 单位 **kbps** 或者 **pps**。
5	Inspur_config_g3/1#**storm-control { broadcast | multicast } action {shutdown|block|resume}**	配置端口的风暴控制动作。 **shutdown** 表示流量到阈值后端口关闭； **block** 表示流量到阈值后端口阻塞； **resume** 表示复原因风暴控制阻塞或关闭的端口。
6	Inspur_config_g3/1#**storm-control { broadcast |multicast } auto-resume** *[second]*	配置端口的风暴控制 **auto-resume** 功能。 单位为秒，不输入默认为 60 秒
7	Inspur_config_g3/1#**storm-control notify{log|trap}**	配置端口的风暴控制上报告警功能。 **log** 表示 **syslog** 打印输出； **trap** 表示发送 **snmp-trap**。

配置检查

可以通过以下命令查看该功能的工作情况。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**show storm-control**	显示风暴控制
3	Inspur_config#**show storm-control { broadcast | multicast } action**	显示广播风暴控制行为

5.9.4 配置示例

组网需求

如下图所示，当 **SW**1 的 **GE** 3/0/1 和 **GE** 3/0/2 接口接收到大量的未知单播或广播报文，**SW**1 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 **SW**1 的转发性能。

为限制广播风暴对 **SW**1 的影响，需要在 **SW**1 的 **GE** 3/0/1 和 **GE** 3/0/2 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，且打开上报告警功能。并配置风暴控制动作为 **shutdown**，报文在阈值下后 120**s** 后会自动恢复。

interface range g3/1-2

storm-control broadcast threshold 100

storm-control notify log

storm-control broadcast action shutdown

storm-control broadcast auto_resume 120

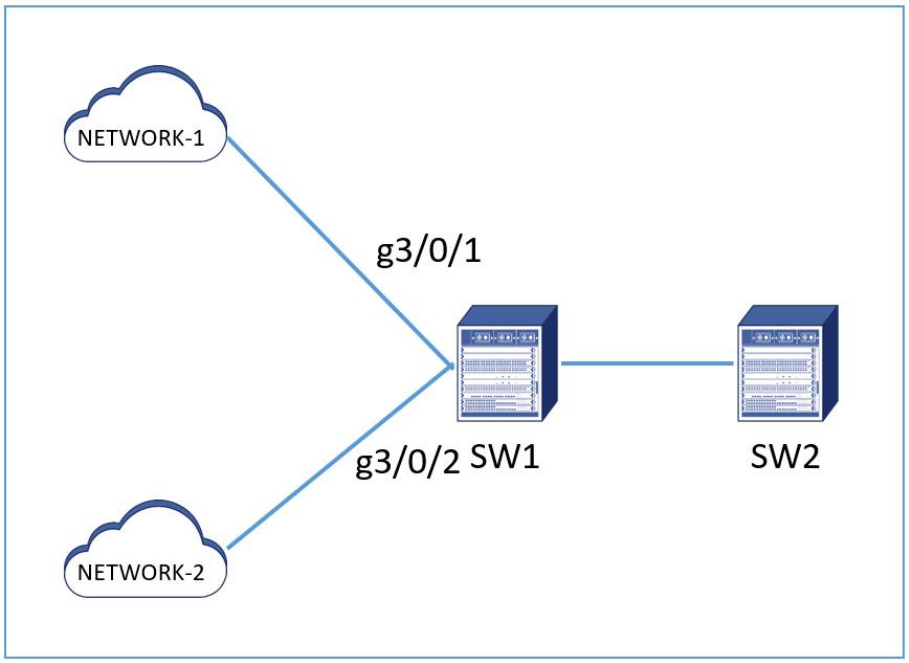


图 5.9.1 风暴抑制应用组网示意图

检查结果

通过 **show storm-control** 查看风暴抑制配置是否正确。

```
Inspur_config_if_range#show storm-control
Port     bc_mode     level      mc_mode     level      uc_mode    level
-------------------------------------------------------------------------
g3/1     broadcast     100      multicast       0      unicast        0
g3/2     broadcast     100      multicast       0      unicast        0
```

5.10 DHCP

5.10.1 简介

动态主机配置协议 DHCP（Dynamic Host Configuration Protocol）是一种用于集中对用户 IP 地址进行动态管理和配置的技术。即使规模较小的网络，通过 DHCP 也可以使后续增加网络设备变得简单快捷。

DHCP 是在 BOOTP（BOOTstrap Protocol）基础上发展而来，但 BOOTP 运行在相对静态（每台主机都有固定的网络连接）的环境中，管理员为每台主机配置专门的 BOOTP 参数文件，该文件会在相当长的时间内保持不变。DHCP 从以下两方面对 BOOTP 进行了扩展：

- DHCP 允许计算机动态地获取 IP 地址，而不是静态为每台主机指定地址。
- DHCP 能够分配其他配置参数，例如客户端的启动配置文件，使客户端仅用一个消息就获取它所需要的所有配置信息。

5.10.2 配置准备

场景

只有跟 DHCP 客户端在同一个网段的 DHCP 服务器才能收到 DHCP 客户端广播的 DHCP DISCOVER 报文。当 DHCP 客户端与 DHCP 服务器不在同一个网段时，必须部署 DHCP 中继来转发 DHCP 客户端和 DHCP 服务器之间的 DHCP 报文。

5.10.3 配置 DHCP Client

配置指定的 DHCP-Server 地址

可以根据需要，调整 DHCP 协议交互时的参数，在全局配置方式下执行下列命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**ip dhcp-server** *ip-address*	指定 **DHCP** 服务器的 **IP** 地址。

配置 DHCP 协议参数

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**ip dhcp client minlease** *seconds*	指定最小可接受的租用时间。

序号	配置	说明
3	Inspur_config#**ip dhcp client retransmit** *count*	指定协议报文的重传次数。
4	Inspur_config#**ip dhcp client select** *seconds*	指定 **SELECT** 间隔时间
5	Inspur_config#**ip dhcp client class_identifier** *WORD*	指定供应商分类编码
6	Inspur_config#**ip dhcp client client_identifier hrd_ether**	指定客户端 **ID** 为以太网类型
7	Inspur_config#**ip dhcp client timeout_shut**	指定客户端超时断开端口
8	Inspur_config#**ip dhcp client retry_interval** *minutes*	没有服务器响应时重新申请地址的时间间隔

配置 fallback 获取地址

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**ip address dhcp fallback** *<ip-address> <mask>*	通过 **DHCP** 协议来配置该以太网接口的 **IP** 地址，如果十秒内没有获取到则配置 **fallback** 子 命令的静态 **IP** 地址

配置检查

可以查看路由交换机当前发现的 **DHCP-Server**（包括手工指定的）的相关信息

在管理态下执行下列命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**show dhcp server**	显示路由交换机所知 **DHCP** 服务器的相关信息。
3	Inspur_config#**show dhcp lease**	显示路由交换机当前所使用的 **IP** 地址资源及其相关信息。

5.10.4 配置 DHCP Server

打开 DHCP Server 服务

打开 **DHCP Server** 服务，为 **DHCP Client** 分配 **IP** 地址等参数，在全局配置态下执行下列命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**ip dhcpd enable**	打开 **DHCP Server** 服务

配置 DHCP Server 中继

DHCP 服务器也支持 **relay** 操作，对于自身不能分配的地址请求，配置了 **ip helper-address** 的端口将转发 **DHCP** 请求）：

序号	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_g3/1#**ip helper-address** *ip-address*	配置中继地址。

配置 ICMP 检测参数

可以根据需要，调整 **Server** 进行地址检测时，发送的 **ICMP** 报文的参数： 配置发送 **ICMP** 报文个数，在全局配置状态下，执行下列命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**ip dhcpd ping packets** *pkgs*	指定地址检测是发送 **ICMP** 报文的个数
3	Inspur_config#**ip dhcpd ping timeout** *timeout*	指定等待 **ICMP** 报文响应的超时时间

配置保存 database 的参数

配置每隔多长时间将地址分配信息保存到 **agentdatabase** 中，在全局配置状态下，执行下列命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**ip dhcpd write-time** *time*	指定每隔多长时间将地址分配信息保存到 **agent database** 中。

配置 DHCP Server 地址池

添加 **DHCPServer** 地址池，在全局配置态下执行下列命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**ip dhcpd pool** *name*	添加 **DHCP Server** 地址池，并进入 **DHCP** 地址池配置态。

配置 DHCP Server 地址池参数

在 **DHCP** 地址池配置态下，可以执行以下命令来配置相关参数：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**ip dhcpd pool** *name*	添加 **DHCP Server** 地址池，并进入 **DHCP** 地址池配置态。
3	Inspur_config_dhcp#**network** *ip-addr netsubnet*	配置用于自动分配的地址池的网络地址
4	Inspur_config_dhcp#**range** *low-addr high-addr*	配置用于自动分配的地址区域
5	Inspur_config_dhcp#**default-router** *ip-addr …*	配置分配给客户机的缺省路由
6	Inspur_config_dhcp#**dns-server** *ip-addr …*	配置分配给客户机的 **DNS** 服务器地址
7	Inspur_config_dhcp#**domain-name** *name*	配置分配给客户机的域名。
8	Inspur_config_dhcp#**lease** *{days [hours][minutes] | infinite }*	配置分配给客户机的地址的时间期限
9	Inspur_config_dhcp#**netbios-name-server** *ip-addr…*	配置分配给客户机的 **netbios** 名字服务器地 址。
10	Inspur_config_dhcp#**hw-access deny** *hardware-address*	拒绝为 **mac** 地址为“**hardware-address**”的 主机分配 **ip** 地址

配置检查

查看 DHCP Server 当前的地址分配信息，在管理态下执行下列命令

序号	配置	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#show ip dhcpd binding	显示 DHCPServer 当前的地址分配信息。
3	Inspur_config#show ip dhcpd statistic	显示 DHCPServer 当前的统计信息
4	Inspur_config#clear ip dhcpd binding *{ip-addr|*}*	删除指定的地址分配信息。
5	Inspur_config#clear ip dhcpd statistic	删除 DHCPServer 当前的统计信息。

5.10.5 配置示例

- **DHCP Client** 配置示例:

  下面是 **DHCPClient** 配置示例。

  1. 获取一个 **IP** 地址示例

  以下例子将为 **vlan**11 接口通过 **DHCP** 协议分配一个 **IP** 地址。

  !

  interface vlan 11

  ip address dhcp

  2. 使用 **fallback** 获取 **IP** 地址

  以下例子将为 **vlan**1 接口通过 **DHCP** 协议分配一个 **IP** 地址，如果十秒内没有获取到地址

  则配置 **fallback** 子命令下的静态 **IP** 地址。

  !

  Interface vlan1

  Ip address dhcp fallback 192.168.0.1 255.255.255.0

- DHCPServer 配置示例:

  以下例子将 **ICMP** 检测包的超时时间设为 200**ms**，配置一个名为 1 的地址池，并打开 **DHCP Server** 服务。

  ip dhcpd ping timeout 2

  ip dhcpd pool 1

  network 192.168.20.0 255.255.255.0

  range 192.168.20.211 192.168.20.215

  domain-name my315

  default-router 192.168.20.1

dns-server 192.168.1.3 61.2.2.10

netbios-name-server 192.168.20.1

lease 1 12 0

!

ip dhcpd enable

5.11 DHCP-Snooping

5.11.1 简介

DHCP Snooping 是 DHCP（Dynamic Host Configuration Protocol）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 地址等参数的对应关系，防止网络上针对 DHCP 攻击。

5.11.2 配置准备

场景

DHCP 协议（RFC2131）在应用的过程中遇到很多安全方面的问题，网络中存在一些针对 DHCP 的攻击，如 DHCP Server 仿冒者攻击、DHCP Server 的拒绝服务攻击、仿冒 DHCP 报文攻击等。

为了保证网络通信业务的安全性，可引入 DHCP Snooping 技术，在 DHCP Client 和 DHCP Server 之间建立一道防火墙，以抵御网络中针对 DHCP 的各种攻击。

5.11.3 配置 DHCP-snooping 功能

开启 DHCP-snooping 功能

请在设备上进行以下配置。

序号	配置	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#ip dhcp-relay snooping	开启 DHCP-snooping 功能。

该命令是启动 **DHCPsnooping** 功能的全局控制命令。配置该命令，则交换机侦听所有 **DHCP** 报文，形成相应的绑定关系。

注意：如果客户端是在配置该命令之前通过此交换机获取地址，则交换机不能添加相应的绑定关系

在 VLAN 上启动 DHCP-snooping

在 **VLAN** 上启动 **DHCP snooping** 功能，则对属于整个 **VLAN** 的所有非信任物理端口收到的

DHCP 报文进行合法化检查。对于 **VLAN** 内的非信任物理端口收到的 **DHCP** 响应报文将丢弃，防止用户非法伪造或者误配的 **DHCP** 服务器提供地址分配；对于非信任端口的 **DHCP** 请求报文，如果报文发送 **MAC** 地址和报文内的硬件地址字段不匹配，认为是用户故意伪造的用于 **DHCPDOS**（拒绝服务）的攻击报文， 交换机也将丢弃。

在全局配置模式下进行下列配置

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**ip dhcp-relay snooping vlan** *vlan_id*	在 **VLAN** 上开启 **DHCP-snooping** 功能。

在 VLAN 上启动 DHCP 防攻击功能

在 VLAN 上启动 DHCP 防攻击功能，配置了 DHCPsnooping 特定 VLAN 下的允许 最大 dhcpclient 用户数，执行先到先分配的原则，当 vlan 内的用户数达到配置的允 许最大值后，就不允许新的 client 进行分配。

在全局配置模式下进行下列配置：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**ip dhcp-relay snooping vlan** *vlan_id* **max-client** *numbe*	在 **VLAN** 上启动 **DHCP** 防攻击功能

配置接口为 DHCP 信任接口

配置接口为 DHCP 信任接口，则该接口收到的 DHCP 报文不进行检查。缺省情况下接口为非信任接口。

在物理接口配置模式下进行下列配置：

序号	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_g3/1#**dhcp snooping trust**	配置接口为 **DHCP** 信任接口

开启绑定表快速更新功能

默认情况下此功能关闭。没有开启此功能时，如果在一个端口下已经绑定了客户端 A， 相同的 mac 地址在其他端口的 dhcp 请求会被认为是伪造 mac 攻击，即使客户端 A 已经下线（没有 release 地址）。 开启此功能后，同一个客户端 A，在其他端口上如果在发送 dhcp 请求报文，dhcp snooping 会将原来端口上的 A 的绑定信息删除，不认为此行为是攻击行为。 建议在客户端会频繁更换端口的环境下，且 dhcpserver 分配的地址租约无法改动为较短时间的时候才考虑使用此功能。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**dp dhcp-relay snoopin rapid-refresh-bind**	开启绑定表快速更新功能

在 VLAN 上启动 DAI 功能

在属于某个 VLAN 的所有物理端口进行 ARP 动态监测，如果该接口收到的 ARP 报文的源 MAC 和源 IP 地址不满足接口上配置的 MAC 和 IP 地址绑定关系，则拒绝处理该报文。接口上配置的绑定关系可以是 DHCP 动态绑定的，也可以是手工配置的。 如果物理接口上没有配置任何 MAC 和 IP 地址绑定，则交换机拒绝转发所有 ARP 报文。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式
2	Inspur_config#**ip arp inspection vlan** *vlanid*	对 **VLAN** 内的所有非信任端口启动动态 **ARP** 监测

配置接口为 ARP 监测信任接口

对于 **ARP** 监测信任接口，不启动 **ARP** 监测功能。接口默认为非信任接口。

在接口配置模式下进行下列配置：

序号	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_g3/1#**arp inspection trust**	配置接口为 **ARP** 监测信任接口

在 VLAN 上启动 IP 源地址监测功能

启动 IP 源地址监测的 VLAN，属于该 VLAN 的所有物理端口收到的 IP 报文的源 MAC 和源 IP 地

址不满足接口上配置的 MAC 和 IP 地址绑定关系，则该报文被拒绝处理。

接口上配置的绑定关系可以是 DHCP 动态绑定的，也可以是手工配置的。如果此物理接口上没有配置任何 MAC 和 IP 地址绑定，则交换机拒绝转发所有该接口收到的 IP 报文。

在全局配置模式下进行下列配置：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式
2	Inspur_config#**ip verify source vlan** *vlanid*	对 **VLAN** 内的所有非信任接口启动报文源 **IP** 地址检查功能

注意：如果收到的是 **DHCP** 报文（也是 **IP** 报文），则因为配置了全局 **snooping** 进行软件转发。

配置接口为 IP 源信任接口

对于 **IP** 源地址信任接口，不启动源地址检查功能。 在接口配置模式下进行下列配置

序号	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_g3/1#**ip-source trust**	配置接口为 **IP** 源地址信任接口

配置 DHCP-snooping Option82 选项格式

Option82 选项将可以携带本地信息给服务器，帮助服务器来分配给客户端地址。

在全局模式下进行下列配置：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式
2	Inspur_config#**ip dhcp-relay snooping information option**	配置 **DHCP-snooping** 转发 **DHCP** 报文将携带 **option**82 选项，选项为默认格式。

如果想要指定 **option**82 格式，则在全局模式下进行下列配置：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式

序号	配置	说明
2	Inspur_config#**ip dhcp-relay snooping information option format {***snmp-ifindex/manual/cm-type/hn-type[host]/hw-type/custom-template/ukr-type***}**	配置 **DHCP-snooping** 转发 **DHCP** 报文将携带 **option**82 选项，选项为 **SNMP-IFINDEX** 格式、手动配置格式、**CM-TYPE** 格式、**cisco** 格式、**hw-type** 格式、**custom-template** 格式或者 **ukr-type** 格式。。

如果配置了手动模式填写 **option**82，在接口配置模式下进行下列配置 **circuit-id** 子选项：

序号	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_g3/1#**dhcp snooping information circuit-id string** *[STRING]*	如果配置了 **option**82 为手动格式，则配置 **DHCP-snooping** 转发 **DHCP** 报文将携带 **option**82 选项，选项内容为 **STRING** 所写的字符串。此命 令在连接 **client** 的端口上配置。
4	Inspur_config_g3/1#**dhcp snooping information circuit-id hex***[xx-xx-xx-xx-xx-xx]*	如果配置了 **option**82 为手动格式，则配置 **DHCP-snooping** 转发 **DHCP** 报文将携带 **option**82 选项，选项内容为所写十六进制。此命令在连接 **client** 的端口上配置。

如果配置了手动模式填写 **option**82，在接口配置模式下进行下列配置 **remote-id** 子选项：

序号	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_g3/1#**dhcp snooping information remote-idstring***[STRING]*	如果配置了 **option82** 为手动格式，则配置 **DHCP-snooping** 转发 **DHCP** 报文将携带 **option82** 选项，选项内容为 **STRING** 所写的字符串。此命令在连接 **client** 的端口上配置。
4	Inspur_config_g3/1#**dhcp snooping information remote-id hex***[xx-xx-xx-xx-xx-xx]*	如果配置了 **option82** 为手动格式，则配置 **DHCP-snooping** 转发 **DHCP** 报文将携带 **option82** 选项，选项内容为所写十六进制。此命令在连接 **client** 的端口上配置。

如果配置了手动模式填写 **option**82，在接口配置模式下进行下列配置 **vendor-specific** 子选项：

序号	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_g3/1#**dhcp snooping information vendor-specific string** *STRING*	如果配置了 **option**82 为手动格式，则配置 **DHCP-snooping** 转发 **DHCP** 报文将携带 **option**82 选项，选项内容为 **STRING** 所写的字符串。此命令在连接 **client** 的端口上配置。
4	Inspur_config_g3/1#**dhcp snooping information vendor-specific hex***[xx-xx-xx-xx-xx-xx]*	如果配置了 **option**82 为手动格式，则配置 **DHCP-snooping** 转发 **DHCP** 报文将携带 **option**82 选项，选项内容为所写十六进制。此命令在连接 **client** 的端口上配置。

配置 DHCP-snooping Option82 报文策略

可以配置收到已经携带 **option**82 选项的 **dhcp** 请求包后采取的策略。

Drop 策略：在端口模式下输入下列命令，配置丢弃包含 **option**82 选项的请求包：

序号	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_g3/1#**dhcp snooping information drop**	配置丢弃包含 **option**82 选项的请求包。

Append 策略：在端口模式下输入下列命令，配置追加包含 **option**82 选项的请求包：

序号	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_g3/1#**dhcp snooping information append**	端口开启追加 **option**82 选项。
4	Inspur_config_g3/1#**dhcp snooping information append first-subop9-param** *{ hex xx-xx-xx-xx-xx-xx | vlan ip | hostname }*	**Option**82 **vendor-specific**（**suboption**9）子选项所带的第一个参数。

序号	配置	说明
5	Inspur_config_g3/1#**dhcp snooping information append second-subop9-param** *{ hex xx-xx-xx-xx-xx-xx | vlan ip | hostname }*	**Option82 vendor-specific**（**suboption9**）子选项所带的第二个参数

手工配置接口绑定

对于不使用 **DHCP** 获取地址的主机，在交换机接口上可以手工配置添加绑定条目使主机正常访问网络。手工配置的绑定条目比动态配置的绑定条目优先级要高，如果配置条目的 **MAC** 地址与动态配置条目的 **MAC** 地址相同，则手工配置的更新动态配置条目。接口绑定条目以 **MAC** 地址为唯一索引。

在全局配置模式下进行下列配置：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式
2	Inspur_config#**ip source binding** *MAC IP* **interface** *name vlanvlan-id*	手工配置接口绑定。

配置检查

可以通过以下命令查看该功能的工作情况。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**show ip dhcp-relay snooping**	显示 **DHCP-snooping** 的配置信息
3	Inspur_config#**show ip dhcp-relay snooping binding**	显示在接口生效的地址绑定条目
4	Inspur_config#**show ip dhcp-relay snooping binding all**	显示 **DHCP-snooping** 生成的所有绑定条目
5	Inspur_config#**show ip dhcp-relay snooping statistics**	显示 **DHCP-snooping** 相关的统计信息

5.11.4 配置示例

组网需求

如下图所示，当 **SW**1 的 **GE** 3/0/1 和 **GE** 3/0/2 接口接收到大量的未知单播或广播报文，**SW**1 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 **SW**1

的转发性能。

为限制广播风暴对 **SW**1 的影响，需要在 **SW**1 的 **GE** 3/0/1 和 **GE** 3/0/2 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，且打开上报告警功能。并配置风暴控制动作为 **shutdown**，报文在阈值下后 120**s** 后会自动恢复。

interface range g3/1-2

storm-control broadcast threshold 100

storm-control notify log

storm-control broadcast action shutdown

storm-control broadcast auto_resume 120

风暴抑制应用组网示意图

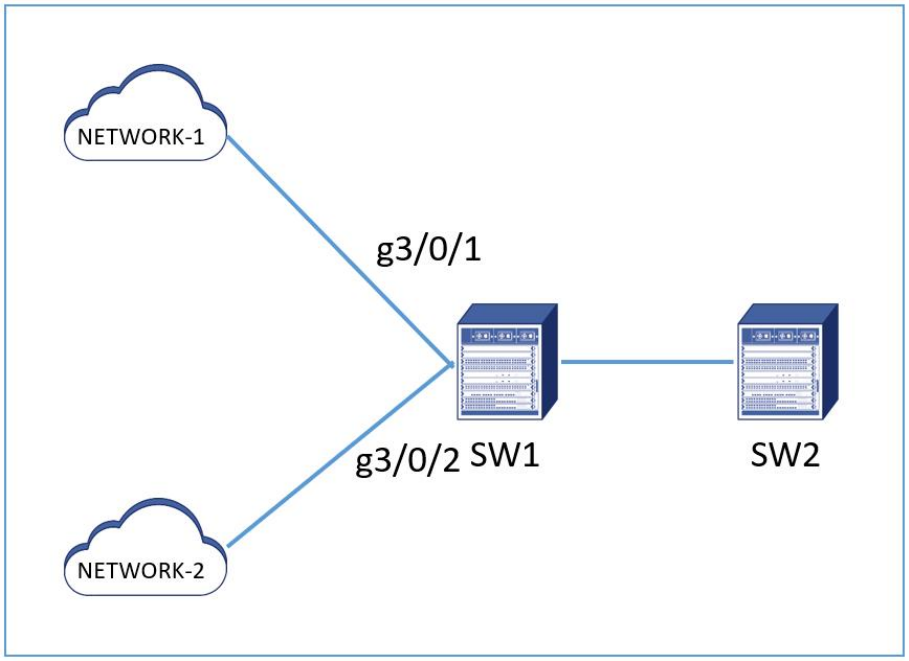


图 5.12.1

检查结果

通过 **show storm-control** 查看风暴抑制配置是否正确。

```
Inspur_config_if_range#show storm-control
Port     bc_mode     level       mc_mode     level       uc_mode    level
-------------------------------------------------------------------------
g3/0/1     broadcast     100       multicast       0       unicast       0
g3/0/2     broadcast     100       multicast       0       unicast       0
```

5.12 DHCPv6

5.12.1 简介

DHCPv6 是一种运行在客户端和服务器之间的协议，与 IPv4 中的 DHCP 一样，所有的协议报文都是基于 UDP 的。但是由于在 IPv6 中没有广播报文，因此 DHCPv6 使用组播报文，客户端也无需配置服务器的 IPv6 地址。

5.12.2 配置准备

场景

IPv6 协议具有地址空间巨大的特点，但同时长达 128 比特的 IPv6 地址又要求高效合理的地址自动分配和管理策略。

目前 IPv6 地址的分配方法有以下几种：

- 手动配置。手动配置 IPv6 地址/前缀及其他网络配置参数（DNS、NIS、SNTP 服务器地址等参数）。
- 无状态自动地址分配。由接口 ID 生成链路本地地址，再根据路由通告报文 RA（Router Advertisement）包含的前缀信息自动配置本机地址。
- 有状态自动地址分配，即 DHCPv6 方式。DHCPv6 又分为如下两种:
  - DHCPv6 有状态自动分配。DHCPv6 服务器自动分配 IPv6 地址/PD 前缀及其他网络配置参数（DNS、NIS、SNTP 服务器地址等参数）。
  - DHCPv6 无状态自动分配。主机 IPv6 地址仍然通过路由通告方式自动生成，DHCPv6 服务器只分配除 IPv6 地址以外的配置参数，包括 DNS、NIS、SNTP 服务器等参数。

5.12.3 配置 DHCP v6

配置 DHCPv6 client PD 前缀

启动 **DHCPv6 pd client** 功能的控制命令后。配置该命令，则设备发送 **DHCPv6** 前缀代理请求。 其中 **prefix_name** 可以被当做前缀来使用，譬如在配置 **ipv6** 端口地址的时候。

在端口配置模式下进行下列配置：

序号	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_g3/1#ipv6 dhcp client` *{pd prefix_name | hint | stateless | rapid-commit}*	开启 **DHCPv6 pd client** 功能

配置 DHCPv6 client NA

该命令是启动 **DHCPv6 naclient** 功能的控制命令。配置该命令，则设备发送 **DHCPv6 NA** 请求。**Server** 端回应 **na** 地址后，设备通知 **nd** 获取对应的前缀长度。

在端口配置模式下进行下列配置：

序号	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_v1#**ipv6 dhcp client na**	开启 **DHCPv6 na client** 功能。

配置 dhcpv6 中继功能

序号	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_v1#**ipv6 dhcp relay destination** *ipv6_address*	开启 **DHCP v6 relay** 功能。

注意：

ipv6 dhcp relay destination 命令用于配置 **relay** 的目的地址。可以是另外的 **relay agent** 的 地址也可以是服务器的地址。 如果需要配置多个目的地址，可以多次配置该命令。**DHCPv6** 的 **client**、**relay**、**server** 功能在一个接口上是互斥的，也就是说在一个接口上只能配置成一种模式。

5.12.4 配置 dhcpv6 服务器功能

配置 ipv6 前缀池

配置前缀池是为了让 **dhcpv6** 的地址池调用，来分配前缀地址。在全局配置态下执行下列命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**ipv6 local pool** *poolname prefix/prefix-length assigned-length*	配置 **ipv6** 前缀池。

配置 dhcpv6 前缀服务器功能

此功能打开需要先配置一个 **ipv**6 前缀池，

例如： **ipv**6 **local pool pd**1 100::1/56 64

在全局配置模式下进行下列配置，进入 **dhcp v**6 池特殊配置模式：

ipv6 **dhcp pool dhpool**1

在 **dhcp v**6 特殊配置下进行下列配置：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**prefix-delegation pool pool name**	指定 **ipv**6 前缀池
3	Inspur_config_dhcpv6#**prefix-delegation** *ipv6_prefix/prefix_length client_DUID* **[iaid** *IAID***]**	指定 **ipv**6 前缀
4	Inspur_config_dhcpv6#**ipv6 dhcp server** *poolname [allow-hint | preference num| rapid-commit]*	打开 **dhcpv**6 **server** 功能。

配置 dhcpv6 地址服务器功能

在 **dhcpv**6 池特殊配置模式态下进行下列配置::

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config_dhcpv6#**non-temporary-address range** *ipv6_address_start ipv6_address_end*	配置 **ipv**6 地址。

配置 DNS 服务器

在 **dhcpv**6 池特殊配置模式态下进行下列配置：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config_dhcpv6#d**ns-server** *ipv6_address*	配置分配给 **client** 的 **dns** 服务器地址。

配置 DNS IPv6 域名

在 **dhcpv**6 池特殊配置模式态下进行下列配置：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config_dhcpv6#**ip dhcpd pool** *name*	配置分配给 **client** 的 **dns** 域名。。

配置租约时间

在 **dhcpv**6 池特殊配置模式态下进行下列配置：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config_dhcpv6#**lifetime valid-time preferred-time**	配置分配给 **client** 的租约时间。
3	Inspur_config_dhcpv6#**Lifetime infinite**	分配给 **client** 的时间不限

5.12.5 配置示例

DHCPv6 **Server** 配置示例:

配置一个 **dhcpv**6 地址池，前缀为 6666::/64 80，租期不限，**dns** 为 8888::8888。

```
ipv6 local pool admin 6666::/64 80
!
ipv6 dhcp pool bdcom
   non-temporary-address range 6666::100 6666::200
   prefix-delegation pool admin
   dns-server 8888::8888
   lifetime infinite
!
ipv6 dhcp enable
```

5.13 BFD

5.13.1 简介

BFD（**Bidirectional Forwarding Detection**，双向转发检测）是一套全网统一的检测机制，用于快速检测、监控网络中链路或者 **IP** 路由转发的连通状况。为了提升现有网络性能， 相邻协议之间必须能快速检测到通信故障，从而更快的建立起备用通道恢复通信。

5.13.2 配置准备

场景

减小设备故障对业务的影响，提高网络的可靠性，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。

5.13.3 配置 BFD

激活接口 BFD 功能

BFD 会话建立前 **BFD** 控制报文以不小于 1 秒的时间间隔周期发送以减小报文流量。在会话建立后 则以协商的时间间隔发送 **BFD** 控制报文以实现快速检测。在 **BFD** 会话建立的同时，**BFD** 控制报 文发送时间间隔以及检测时间也会通过报文交互协商确定。在 **BFD** 会话有效期间，这些定时器可 以随时协商修改而不影响会话状态。**BFD** 会话不同方向的定时器协商是分别独立进行的，双向定 时器时间可以不同。**BFD** 控制报文发送时间间隔为本端 **min_tx_interval** 与对端 **min_rx_interval** 之中的最大值，也就是说比较慢的一方决定了发送频率。 检测时间为对端 **BFD** 控制报文中的 **DetectMult**（即对端配置的检测系数）乘以经过协商的对端 **BFD** 控制报文发送时间间隔。如果加大本端 **min_tx_interval**，那么本端实际发送 **BFD** 控制报文的时间 间隔必须要等收到对端 **F** 字段置位的报文后才能改变，这是为了确保在本端加大 **BFD** 控制报文发送时间间隔前对端已经加大了检测时间，否则可能导致对端检测定时器错误超时。 如果减小本端 **min_rx_interval**，那么本端检测时间必须要等收到对端 **F** 字段置位的报文后才能改 变，这是为了确保在本端减小检测时间前对端已经减小了 **BFD** 控制报文发送间隔时间，否则可能导致本端检测定时器错误超时。然而如果减小 **min_tx_interval**，本端 **BFD** 控制报文发送时间间隔 将会立即减小；加大 **min_rx_interval**，本端检测时间将会立即加大。

缺省情况下，接口 **bfd** 功能未激活。 在使能接口 **bfd** 功能后，各动态协议配置的 **bfd** 检测功能才能生效。

使用下面的 **BFD** 配置命令来达到上述目的：

序号	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_v1#bfd enable *<cr>* / {min_tx_interval *<tx_value>* min_rx_interval *<rx_value>* multi *<m_value>*	激活接口 **BFD** 功能。

激活接口 bfd echo 功能

缺省情况下，接口 **bfdecho** 功能未激活。

bfd echo（回声）功能激活后，支持 **bfdecho** 功能的邻居 **up** 以后控制报文按照 **slow-timers** 配置的时间间隔发送，连通性检测功能由回声报文完成，回声报文发送时间间隔为 **bfd min_echo_rx_interval** 命令配置的时间。

使用下面的 **BFD** 配置命令来达到上述目的：

序号	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_v1#bfd echo enable *<cr>|<number>*	激活 bfd echo（回声）功能。。

配置检查

配置完成后，使用下面的管理命令显示各种 **BFD** 统计信息：

序号	配置	说明
1	Inspur#config	进入全局配置模式。
2	Inspur#show bfd interfaces details	显示系统中的激活 BFD 功能接口列表 。
3	Inspur#show bfd neighbors details	显示系统中 BFD 邻居详细信息。

5.13.4 配置示例

在接口下配置 bfd，将发送和接收时间分别改为 200ms 和 300ms，倍数为 5；

```
bfd enable min_tx 200 min_rx 300 multi 5
```

5.14 flow-control

5.14.1 简介

交换机的流量控制机制：流量控制用于防止在端口阻塞的情况下丢帧，当发送或者接收缓冲区开始溢出时通过阻塞信号发送回源地址实现。流量控制可以有效的防止由于网络中瞬间的大量数据对网络带来的冲击。

5.14.2 配置准备

场景

流量的控制有两种方式：
1、在半双工方式下，通过反向压力即我们通常说的背压计数实现的，这种计数是通过向发送源发送 jamming 信号使得信息源降低发送速度。
2、在全双工方式下，流量控制一般遵循 IEEE 802.3X 标准，是由交换机向信息源发送 pause 帧令其暂停发送。
pause：当接口开启流量控制机制后，当接口出现拥塞时，会给上联设备接口发送 pause 帧，通知上联端口停止发包。

5.14.3 配置 flow-control

配置接口流量控制

在接口为全双工模式时，流量控制通过 802.3X 定义的 PAUSE 帧实现；在接口为半双工模式时，通过背压实现。

请在设备上进行以下配置：

序号	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_g3/1#**flow-control** *[on off auto]*	配置接口流控。

配置检查

配置完成后，使用下面的管理命令显示各种 **BFD** 统计信息：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur#**show flow-control**	显示流控状态
3	Inspur#**show flow-control interface** *interface-type interface-number*	显示具体接口流控状态。

5.14.4 配置示例

在设备的接口打开流控；防止由于网络中瞬间的大量数据对网络带来的冲击。
Inspur#conf

Inspur_config#int g3/5

Inspur_config_g3/5#flow-control auto

6 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 配置
- NTP
- 系统日志
- 告警管理
- CPU 监控
- 内存监控
- 风扇监控
- Ping
- Traceroute
- PDP

6.1 SNMP

6.1.1 简介

SNMP 系统包括下面 3 个部分：

SNMP 管理端 (NMS)

SNMP 代理 (AGENT)

管理信息库 （MIB）

SNMP 是应用层协议。 它提供了在 SNMP 管理端和代理之间进行通信的报文格式。

SNMP 管理端可以是网络管理系统（ NMS， 如 CiscoWorks） 的一部分。 代理和 MIB 驻留在系统上。 配置系统上的 SNMP， 需要定义管理端和代理间的关系。

SNMP 代理包含 MIB 变量，SNMP 管理端可以查询或改变这些变量的值。管理端可以从代理处得到变量值，或者把变量值存储到代理处。代理从 MIB 收集数据。 MIB 是设备参数和网络数据的信

息库。代理也能响应管理端的读取或设置数据的请求。SNMP 代理可以主动向管理端发送陷阱（trap）。陷阱是针对网络的某一条件而向 SNMP 管理端报警的消息。 陷阱能指出不正确的用户认证、 重启、 链路状态（启动或关闭）、 TCP 连接的关闭、与邻近系统连接的丢失或其它重要的事件。

1.SNMP 通告

特殊事件发生时系统能向 SNMP 管理端发送通知(inform)。 例如，当代理系统遭遇一个错误条件时， 它可能向管理端发送一个消息。

SNMP 通告可以作为陷阱（trap） 或通知请求（inform request）来发送。由于接收方收到一个陷阱时不发送任何应答，导致发送方不能确定是否陷阱已经被接收，所以陷阱不可靠。与此相对的是，接收通知请求的 SNMP 管理端用 SNMP 响应 PDU 作为这个消息的应答。如果管理端没有收到一个通知请求，也不会发送响应。如果发送方没有收到应答，那么可以重新发送通知请求。这样，通告更可能到达它们计划中的目的地。

因为通知请求更加可靠，所以它们消耗了系统和网络的更多的资源。陷阱只要一发出便被丢弃。与此不同的是，通知请求必须保留在内存中，直到收到响应或者请求超时。另外，陷阱只发送一次，而通知请求可以重新发送多次。重新发送增加了网络通信量并在网络上产生更多的负荷。因此，陷阱和通知请求在可靠性和资源间提供了平衡。如果 SNMP 管理端非常需要收到每个通知，可使用通知请求；如果关心网络的通信量或系统的内存，并且不必收到每个通知，可使用陷阱。

2.协议版本:目前，SNMP 协议共有 v1、v2c 和 v3 三个版本。

SNMPv1---简单网络管理协议，一个完全的 Internet 标准，在 RFC1157 中定义。

SNMPv2C---SNMPv2 的基于团体的管理框架，Internet 试验协议，在 RFC1901 中定义。

SNMPv3---简单网络管理协议版本 3， 在 RFC3410 中定义。

SNMPv1 使用基于团体的安全形式。能访问代理 MIB 的管理端团体用 IP 地址访问控制列表和口令来定义。

SNMPv3 通过对 SNMP 报文进行认证和加密操作来提供对设备访问的安全性。SNMPv3 提供了下列安全特性：

消息完整性：保证消息在传输过程中没有被篡改

认证：确保消息的来源地的合法性

加密：对消息题进行加密，未经认证的主机即使窃取到消息也无法解密阅读

SNMPv3 提供安全模型和安全级别。安全模型是指一种认证策略，通过配置用户名和该用户所属的组来实现。安全级别是指安全模型中支持的不同的认证方式。SNMPv3 基于用户的安全模型支持三种安全级别， 按照从高到低的顺序排列分别是认证并加密、认证不加密和不认证；通过使用 MD5 或 SHA 散列算法计算认证密钥的摘要值在网络间传送并在 SNMP 引擎比对来实现密码不被泄漏， 使用 DES 加密算法对报文进行加密保证设备不被第三者窃听。通过配置用户/密码对和用户所属的组来实现管理者对设备的身份认证，通过配置组和视图决定组内的用户不同操作对于管理信息库的访问权限； 组同时限制了组内用户的最低安全级别。

3.所支持的 MIB

本公司系统的 SNMP 支持所有的 MIB II 变量（在 RFC1213 中讲述）和 SNMP 陷阱（RFC1215 中讲述）。本公司系统为每个系统提供了自己私有的 MIB 扩充。

6.1.2 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。

6.1.3 SNMP 配置

配置 SNMP 视图

SNMP 视图用于规定管理信息库的访问权限：允许访问和拒绝访问。

使用下面的命令配 置 SNMP 视图

序号	命令	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#snmp-server view *name oid* [excluded / included]	创建 SNMP 视图，并配置访问的 MIB 变量范围。

SNMP 视图中可以访问的子集为所有配置了允许访问的管理信息库的对象除去所有配置了拒绝访问的对象；未配置的对象默认权限为不可访问。

配置了 SNMP 视图后，可以将 SNMP 视图应用到 SNMP 团体名的配置中，用以限定该团体名的可访问对象的子集。

为 SNMP 团体创建或修改访问控制

使用SNMP 团体字符串定义 SNMP 管理端和代理的关系。团体字符串类似于允许访问系统上代理的口令。可选的是可以指定下面一个或多个与团体字符串相关联的特性：

允许使用团体字符串获得代理访问权的SNMP 管理端的IP 地址访问列表。定义对指定团体有访问权的所有MIB 对象子集的MIB 视图。指定团体对有访问权的MIB 对象的读写权限。在全局配置模式下使用下面的命令来配置团体字符串：

序号	命令	说明
1	Inspur_config#snmp-server community [0|7] *string*[view *view-name*] [ro | rw] [*word*]	定义团体访问字符串。

可以配置一个或多个团体字符串。使用 no snmp-server community 命令除去给定的团体字符串。

设置该系统管理员的联系方法和系统所在位置

sysContact 和sysLocation 都是MIB 中system 组中的管理变量，分别定义了被管理该节点（系统）的联系人标识和实际位置。这些信息可以通过配置文件进行访问。

在全局配置模式下使用下面的一个或多个命令：

序号	命令	说明
1	Inspur_config#**snmp-server contact** *text*	设置节点联系人字符串。
2	Inspur_config#**snmp-server location** *text*	设置节点位置字符串。

定义 SNMP 代理数据包的最大长度

当SNMP 代理接收请求或发出响应时，可以设置数据包的最大许可长度。

在全局配置模 式下使用下面的命令：

序号	命令	说明
1	Inspur_config#**snmp-server packetsize** *byte-count*	设定数据包的最大许可长度。

监视SNMP 状态

在全局配置模式下使用下面的命令，监视SNMP 输入和输出统计，包括非法团体字符串条目，错误和请求变量的数量。

序号	命令	说明
1	Inspur_config#**show snmp**	监视 **SNMP** 状态。

配置 SNMP 陷阱

使用下面的命令配置系统发送 SNMP 陷阱（第二个任务是可选的）：配置系统发送陷阱

在全局配置模式下使用下面的命令配置系统向一个主机发送陷阱。

序号	命令	说明
1	Inspur_config#**snmp-server host|hostv6** *host community-string [trap-type]*	指定陷阱消息的接收者。
2	Inspur_config#**snmp-server host|hostv6** *host* **[vrf** *word***]** **[udp-port** *port-num***] [permit|deny** *event-id***]** **{{version [v1 | v2c | v3]} | {[informs | traps] | [auth |noauth]}}** *community-string/user* **[authentication | configure| snmp]**	指定陷阱消息的接收者，以及陷阱信息的版本

系统开机后，SNMP 代理自动启动，所有类型的陷阱被激活。 使用 snmp-server host 命令指定哪个主机将要接收哪些类型的陷阱。

有些陷阱需要通过其它命令来控制。例如，如果要在接口打开或关闭时会发送 SNMP 链路陷阱， 需在接口配置模式下使用 snmp trap link-status 激活链路陷阱。使用接口配置命令 no snmp trap link-stat 关闭这些陷阱。为了使主机收到陷阱，必须为该主机配置 snmp-server host

命令。

改变陷阱运行参数作为可选项，可以指定产生陷阱的源接口，为每个主机指定消息（数据包）队列长度或重发间隔的值。

在全局配置模式下使用下面可选命令改变陷阱运行参数：

序号	命令	说明
1	Inspur_config#**snmp-server trap-source** *interface id*	指定产生陷阱消息的源接口。该命令为信息也设置源 **IP** 地址。
2	Inspur_config#**snmp-server queue-length** *length*	为每个陷阱主机建立消息队列长度。缺省为 10。
3	Inspur_config#**snmp-server trap-timeout** *seconds*	定义重发队列中重发陷阱消息的频率。缺省为 30 秒。

SNMP 绑定源地址

在全局配置模式下使用下面的命令，设置 SNMP 报文的源地址功能。

序号	命令	说明
1	Inspur_config#**snmp source-addr** *ip address*	设置 **SNMP** 报文的源地址

SNMP 配置侦听端口

全局模式下使用下面命令，配置 SNMP 代理的侦听端口号。

序号	命令	说明
1	Inspur_config#**snmp-server udp-port** *portnum*	设置 **SNMP** 代理的侦听端口号

配置 SNMPv3 组

通过下面的命令配置组

序号	命令	说明
1	Inspur_config#**snmp-server group** [*groupname* { **v3 [auth | noauth | priv]**}][**read** *readview*][**write** writeview] [**notify** notifyview] [**access** access-list]	配置一个 **SNMPv3** 组。默认情况下可以读 **internet** 子树下 所有叶子，不可以写任何叶子。

配置 SNMPv3 用户

通过下面的命令配置一个本地用户，管理者访问设备时，必须使用设备上配置的用户名和密码进行访问。用户的安全级别不能低于用户所属的组的安全级别，否则用户不能通过认证

序号	命令	说明

序号	命令	说明
1	Inspur_config#**snmp-server user** *username groupname* **{ v3 priv [des | aes128 | aes256 | aes256-c] auth [md5 | sha | sha256]** *priv-password auth-password* **}**	配置一个本地 **SNMPv3** 用户

配置共同体密文显示

使用全局配置模式命令 snmp-server encryption 使已经配置的 snmp 共同体，SHA 加密密码和 MD5 加密密码密文显示，该命令为一次性命令不做保存，不可用 NO 命令取消。命令格式如下

序号	命令	说明
1	Inspur_config#**snmp-server encryption**	使 **snmp** 共同体，**SHA** 加密密码和 **MD5** 加密密码密文显示。用于保证密码安全性

配置陷阱源地址

使用全局配置模式命令 snmp-server trap-source 指定一个接口用于所有陷阱的源地址。 使用该命令的 no 形式除去这样一个接口。

序号	命令	说明
1	Inspur_config#**snmp-server trap-source** *interface*	当从 **SNMP** 服务器发出 **SNMP** 陷阱时，无论当时在哪个接口发出，它都有一个的陷阱地址。如果想用该陷阱地址进行跟踪，可使用该命令。

配置陷阱发送超时时间

使用全局配置模式命令 snmp-server trap-timeout 定义重发陷阱消息的超时值。

序号	命令	说明
1	Inspur_config#**snmp-server trap-timeout** *seconds*	在交换机软件试图发送陷阱之前，它查找到 目标地址的路由。如果没有路由，陷阱存入重发队列中。命令 **server trap-timeout** 决定了重发的间隔。

配置陷阱绑定主机名称

该设置用于 snmp 发送 trap 时在绑定变量中添加 hostname 信息

序号	命令	说明
1	Inspur_config#**snmp-server trap-add-hostname**	在特定的时候，网管主机需要定位 **trap** 来自哪个主机，这来命令可以起到很大的帮助。

配置将陷阱发送记录为 log

设置设备把 trap 的发送记录记为 logs。

序号	命令	说明
1	Inspur_config#**snmp-server trap-logs**	启用 **snmp trap** 的发送 log 记录后，可以向 log 服务器发送，设备的 trap 发送记录，可以增 加对设备运行状态的了解

配置 snmp 饱和攻击防御

设置开启 snmp 遭受不断尝试密码时的防护功能，设置 snmp sever 在五分钟内错误 commuity 登录的重复次数

序号	命令	说明
1	Inspur_config#**snmp-server set-snmp-dos-max** *retry times*	设置 **snmp** 错误请求五分钟内最大重试次数

需要配合 snmp-server host 使用

配置发送心跳 trap

使用全局配置模式命令 snmp-server keep-alive 配置设备定时的发送心跳 trap。时间间隔为 times

序号	命令	说明
1	Inspur_config#**snmp-server keep-alive** *times*	定期向指定 **trap host** 发送心跳 **trap**

配置设备网元编码

使用全局配置模式命令 snmp-server necode 设置管理节点的信息（设备唯一标识符）。 使用 no 形式除去设备标识信息

序号	命令	说明
1	Inspur_config#**snmp-server necode** *text*	与 **snmp** 私有 **MIB** 变量的值对应。

配置陷阱事件列表

使用全局配置模式命令 snmp-server event-id 创建和设置 event 列表，使用 no 命令删除

序号	命令	说明
1	Inspur_config#**snmp-server event-id** *number* **trap-oid** *oid*	在 **host** 配置中使用，用于发送 **trap** 时的过滤。

配置 getbulk 请求的最大处理时间

使用全局配置模式命令 snmp-server getbulk-timeout 设置 getbulk 请求的最大处理时间，若超过此时间无法处理完成所有的 getbulk 请求，则直接返回现有结果。使用 no 命令删除。

序号	命令	说明
1	Inspur_config#**snmp-server getbulk-timeout** *seconds*	设置 **getbulk** 请求的最大处理时间，若超过 此时间无法处理完成所有的 **getbulk** 请求，则直接返回现有结果。

配置 getbulk 请求的 cpu 间歇时间

使用全局配置模式命令 snmp-server getbulk-delay 设置 snmp 代理在处理 getbulk 请求时，为防止 snmp 占用过多 cpu 设置 snmp 任务挂起的时间。单位为百分之一秒。使用 no 命令删除。

序号	命令	说明
1	Inspur_config#**snmp-serve getbulk-delay** *ticks*	**snmp** 代理在处理 **getbulk** 请求时，为防止任务占用过 多 **cpu** 设置 **snmp** 任务挂起时间，单位为百分之一秒。

显示 snmp 运行信息

使用命令 show snmp 监视 SNMP 输入和输出统计，包括非法团体字符串条目，错误和 请求变量的数量。 使用命令 show snmp host 显示 SNMP 陷阱主机信息。使用命令 show snmp view 显示 SNMP 视图信息。使用命令 show snmp mibs 显示 mib 注册信息。使用命令 show snmp group 显示 SNMP 组信息。使用命令 show snmp user 显示 SNMP 用户信息。

序号	命令	说明
1	Inspur_config#**show snmp** *host*	显示 **SNMP** 陷阱主机信息。
2	Inspur_config#**show snmp** *view*	显示 **SNMP** 视图信息。
3	Inspur_config#**show snmp** *mibs*	显示 **SNMP MIB** 注册的信息。

序号	命令	说明
4	Inspur_config#**show snmp** *group*	显示 **SNMP** 组信息。
5	Inspur_config#**show snmp** *user*	显示 **SNMP** 用户信息。

显示 snmp 调试信息

显示 SNMP 事件、报文发送、接收过程和出错信息。

命令	说明
Inspur#**debug snmp** *error*	打开 **SNMP** 出错信息的调试开关。
Inspur#**debug snmp** *event*	打开 **SNMP** 事件的调试开关。
Inspur#**debug snmp** *packet*	打开 **SNMP** 输入输出报文的调试开关。

6.1.4 配置示例

示例 1

```
snmp-server community public RO

snmp-server community private RW

snmp-server host 192.168.10.2 public
```

在这个例子中配置了对所有 MIB 变量有读权限的团体字符串 public 与对所有 MIB 变量有读写权限的团体字符串 private。用户可以用团体字符串 public 读系统中 MIB 变量，用 private 读系统中的 MIB 变量与写系统中可写的 MIB 变量。它还指定了当系统需要发送陷阱消息时，用团体字符串 public 向 192.168.10.2 发送陷阱消息。例如当系统的某个端口 down 时，系统会向 192.168.10.2 发送一条 linkdown 的陷阱消息。

示例 2

```
snmp-server group getter v3 auth

snmp-server group setter v3 priv write v-write

snmp-server user get-user getter v3 auth sha 12345678

snmp-server user set-user setter v3 encrypted auth md5 12345678 snmp-server
view v-write internet included
```

使用 SNMPv3 对设备进行管理。组 getter 可以对设备信息进行浏览，组 setter 可以对设备进行设置操作。用户 get-user 属于组 getter，安全级别为认证不加密，口令为 12345678， 时用 sha 算法进行口令摘要；用户 set-use 属于组 setter，安全级别为认证并加密，口令为 12345678，使用 md5 算法进行口令摘要。

6.2 RMON

6.2.1 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。

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。

6.2.2 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。

6.2.3 RMON 配置

配置交换机 RMon 告警功能

可以通过命令行或SNMP 网管配置RMon 告警功能；如果通过SNMP 网管配置，还需要对交换机的SNMP 进行配置。告警功能配置完成后，设备可以监控系统中某些统计值。 配置RMon 告警功能步骤如下：

请在设备上进行以下配置。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**rmon alarm** *index variable interval* {**absolute** | **delta**} **rising-threshold** *value* [*eventnumber*] **falling-threshold** *value* [*eventnumber*] [**owner** *string*] [**repeat**]	增加一个 **RMon** 告警表项。 **index** 为该表项的索引， 有效范围 1~65535 。 **variable** 为被监测 **MIB** 中对象， 必须是系统中一个有效的 **MIB** 对 象， 并且 只有 类 型为 **INTEGER** 、 **Counter** 、 **Gauge** 或 **TimeTicks** 的对象才能被检测。 **interval** 为 取 样 的 间 隔 时 间 ， 以 秒 为 单 位 ， 有 效 范 围 1~2147483647。 使用 **absolute** 来直接监测 MIB 对象的取值； 使用 **delta** 来监测两次取样之间 **MIB** 对象值的变化。 **value** 用于表示产生告警的阈值， 对应的 **eventnumber** 表示到 达该阈值时产生的事件的索引； **eventnumber** 是可选的。 **owner string** 可以用来描述该告警的一些描述性信息。 **repeat** 用来控制允许重复触发事件。
3	Inspur_config#**exit**	退回到管理模式
4	Inspur#**write**	保存配置 。

配置完成一条告警表项后，设备会每隔interval 秒获取variable 指定的oid 的值，并根据告警类型（absolute 或delta）与前次值进行比较，如果本次统计值比前次大并且超出rising-threshold 指定的阈值则会引发索引为eventnumber 的事件（如果eventnumber 为零或事件表不存在索引为eventnumber 的事件则不引发），下降亦然；如果无法获取 variable 指定的oid，则本行告警表项状态被设置为invalid。当使用rmon alarm 命令多次配置相同index 的告警表项时，只有最后一次配置的参数有效；使用no rmon alarm index 命令删除索引为index 的告警表项。

配置交换机 RMON 事件功能

请在设备上进行以下配置。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**rmon event index [description** *string*] **[log] [owner** *string*] **[trap** *community*] **[ifctrl** *interface*]	增加一个 **RMon** 事件表项。 **index** 为该表项的索引，有效范围 1~65535 。 **description** 表示该事件的描述信息 。 **log** 表示该事件被引发时在 **log** 表中增加一条信息 。 **trap** 表示该事件被引发时产生一条 **trap**，**community** 为团体名称。 **ifctrl interface** 配置事件控制关闭的端口。 **owner string** 可以用来描述该事件的一些描述性信息。
3	Inspur_config#**exit**	退回到管理模式。
4	Inspur**write**	保存配置。

配置RMon 事件后，当触发RMon 告警时，首先更新本事件表项的eventLastTimeSent 域 为当时的sysUpTime；如果该事件配置了log 属性，则向log 表中增加一条信息；如果配 置了trap 属性，则以community 为团体名称发出一条trap。当使用rmon event 命令多次配置相同index 的事件表项时，只有最后一次配置的参数有效；使用no rmon event index 命令删除索引为index 的事件表项。

配置交换机 RMon 统计功能

RMon 统计组用于监测设备上每一个接口上的统计信息。RMon 统计功能配置步骤如下：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**interface g3/1**	进入端口模式。 **iftype** 为端口的类型。 **ifid** 为接口的 **id**。
3	Inspur_config_g3/1#**rmon collection stats**index [**owner** string]	在该接口上使能统计功能。 **index** 为统计表项索引 。 **owner string** 可以用来描述该统计表的一些描述性信息。
4	Inspur_config_3/1#**exit**	退回到全局模式。
5	Inspur_config#**exit**	退回到管理模式。
6	Inspur#**write**	保存配置。

当使用rmon collection stats 命令多次配置相同index 的事件表项时，只有最后一次配置

的参数有效；使用no rmon collection stats index 命令删除索引为index 的统计表项。

配置交换机RMON 历史功能

RMON 历史组用于收集设备上一个接口上的不同时间段的统计信息。RMon 统计功能配置 步骤如下：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**interface g3/1**	进入端口模式 **iftype** 为端口的类型 **ifid** 为接口的 **id**
3	Inspur_config_g3/1#**rmon collection history** *index* [**buckets** *bucket-number*] [**interval** *second*] [**owner** *owner-name*]	在该接口上使能历史功能 **index** 为该历史表项索引 在所有该历史记录控制表项收集的数据中，最近 **bucket-number** 条表项需要保留，用户可以浏览以太网历史记录表获取这些统计值；默认值为 50 条。**second** 为每两次获取统计数据的间隔时间，默认值为 1800 秒（半小时）。**owner string** 可以用来描述该历史控制表的一些描述性信息
4	Inspur_config_g3/1#**exit**	退回到全局模式
5	Inspur_config#**exit**	退回到管理模式
6	Inspur#**write**	保存配置

增加一个历史控制表项后，设备会每隔 second 秒从指定的接口上获取一次统计值，将结 果作为表项增加到以太网历史记录表中。当使用 rmon collection history index 命令多次 配置相同 index 的历史表项时，只有最后一次配置的参数有效；使用 no rmon history index 命令删除索引为 index 的历史控制表项。注意 bucket-number 过大和 interval second 过小都会过多占用系统资源。

显示交换机RMON 配置

使用 show 命令显示交换机 RMON 配置。

序号	检查项	说明

序号	检查项	说明
1	Inspur#show rmon [alarm] [event] [statistics] [history]	显示 rmon 配置信息 alarm 表示显示告警表项配置 event 表示显示事件表项配置，同时显示由于事件被引发而导致 log 表中包含的表项 statistics 表示显示统计表项配置，同时显示设备收集到的该接口上的统计值 history 表示显示历史表项配置，同时显示设备收集到的该接口上最近指定个数时间间隔内的统计值

6.2.4 配置示例

示例

```
Inspur#config
Inspur_config#rmon event 1 log description High-ifOutErrors owner system
```

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#show rmon event
  Event 1 is valid, owned by system
  Description is High-ifOutErrors
  Event firing causes log, last fired 0:00:00:00
```

show rmon event 解释：事件 1 有效，事件属于 system，描述为 High-ifOutErrors，事件触发原因日志，上次触发时间 0:00:00:00

6.3 LLDP

6.3.1 LLDP 简介

802.1AB 链接层发现协议（Link Layer Discovery Protocol），能够使企业网络的故障 查找变得更加容易，并加强网络管理工具在多厂商环境中发现和保持精确网络拓扑结构 的能力。它可使邻近设备向其他设备发出其状态信息的通知，并且所有设备的每个端口 上都存储着定义自己的信息，如果需要还可以向与它们直接连接的近邻设备发送更新的 信息，近邻的设备会将信息存储在标准的 SNMP MIBs。网络管理系统可从 MIB 处查询出 当前第二层的连接情况。LLDP 不会配置也不会控制网络元素或流量，它只是报告第二层的配置。

简单说来，LLDP 是一种邻近发现协议。它为以太网网络设备，如交换机、路由器和 无线局域网接入点定义了一种标准的方法，使其可以向网络中其他节点公告自身的存在，并保存各个邻近设备的发现信息。例如设备配置和设备识别等详细信息都可以用该协议 进行公告。具体来说，LLDP 定义了一个通用公告信息集、一个传输公告的协议和一种用来存储所收到的公告信息的方法。要公告自身信息的设备可以将多条公告信息放在一个 局域网数据包内传输，传输的形式为类型长度值（TLV）域。

TLV 包含三个必须的 TLV：Chassis ID TLV、Port ID TLV 和 Time To Live TLV，五个可选的 TLV ： Port Description、System Name、System Description、System Capabilities、Management Address，以及三项扩展的 TLV：DOT1（Port Vlan ID、Protocol Vlan ID、Vlan Name、Protocol Identity）、DOT3（MAC/PHY Configuration/Status、Power Via MDI、Link Aggregation、Max Frame Size）、MED（MED Capability、Network Policy、Location Identification、Extended Power-via-MDI、Inventory(Hardware Revision、Firmware Revision、Software Revision、Serial Number、Manufacturer Name、Mode Name、Assert ID)）。

LLDP 是单向协议，一个 LLDP 代理能够通过与之关联的 MSAP 发送自己系统状态 和自身功能，也可接收邻接设备的当前系统状态和功能。但是，LLDP 代理不能通过此协议请求对方任何信息。LLDP 代理其发送和接收信息互不影响，可以只配置实现发送或接收功能，或两者都有。

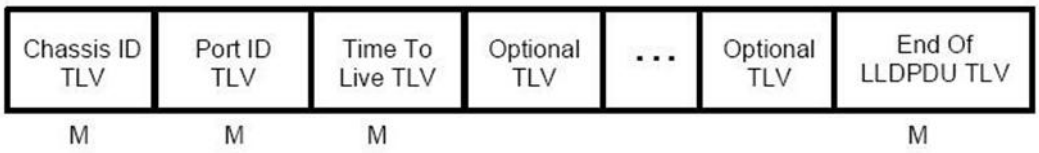
协议初始化：本地 LLDP 代理可能配置为只接收帧，只发送帧，既接收又发送帧，所以对帧接收和发送需要独立的协议初始化处理。在没有配置说明只接收或只发送的情况下，LLDP 代理默认为可接收可发送模式。

LLDP 发送模式初始化：在接口模式下配置接口是否为可发送帧模式。当配置为可发送帧模式时，在本地系统中一个或多个信息元素（管理对象）状态或值发生变化和发送计时器超时两种情况下， 自动发送 LLDP 信息；当为不可发送帧时，接口不向邻居发送 LLDP 报文。

LLDP 接收模式初始化:在接口模式下配置接口是否为可接收帧模式。当配置为可接收帧模式时，能够接收 周围邻居发送的 LLDP 报文，并将其中的 tlv 内容存入远端 MIB 中；当为不可接收帧时，接口接收到邻居发送 LLDP 报文后直接丢弃。

LLDP PDU 报文结构说明

LLDP PDU 应该按照顺序包含三个必须的 TLV，后面为一个或多个可选 TLV，最后为结束 TLV。如图 1 所示：



M 为必须包含的 TLV。

图 1 LLDP PDU 格式

(1) 三个必须的 TLV 应该在 LLDP PDU 的开始依次出现，其顺序为：

1. Chassis ID TLV
2. Port ID TLV
3. Time To Live TLV

(2) 由网络管理选择可选的 TLV，顺序任意，包括：

4. Port Description
5. System Name
6. System Description

7. System Capabilities

8. Management Address

以及 3 项扩展的 TLV，有 DOT1：

9. Port Vlan ID

10. Protocol Vlan ID

11. Vlan Name

12. Protocol Identity

DOT3：

13. MAC/PHY Configuration/Status

14. Power Via MDI

15. Link Aggregation

16. Max Frame Size

MED（默认情况下，MED 的 TLV 是不被发送的，当收到包含 MED TLV 的 LLDP 报文后，才会发送含有 MED TLV 的 LLDP 报文）：

17. MED Capability（若添加了 MED 扩展 TLV，则此 TLV 是必须的）

18. Network Policy

19. Location Identification

20. Extended Power-via-MDI

21. Inventory（包含 Hardware Revision、Firmware Revision、Software Revision、Serial Number、Manufacturer Name、Mode Name、Assert ID）

(3) 结束 TLV 应该为 LLDP PDU 中最后一个 TLV。

6.3.2 配置准备

场景

当用户通过 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 NNM 系统查询。

6.3.3 LLDP 配置

禁止/启动 LLDP

默认情况下 LLDP 关闭，当需要运行 LLDP 时可以开启 lldp 让其运行。开启 LLDP 功能后，本地端口定期向外发送 lldp 帧以通知对端本地端口的信息。

在全局配置模式下使用下面的命令开启 lldp：

序号	配置	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#lldp run	运行 lldp 功能

使用下面的命令禁止lldp：

序号	配置	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#no lldp run	关闭 lldp 功能

注意：只有开启了 lldp 功能才能对接收到的 lldp 报文进行处理，否则 lldp 帧将被直接转发。

配置 holdtime

正常情况下，MIB 中存储的远端信息在老化前都会更新，但由于更新帧发送过程中可能丢失，引起 MIB 中信息老化。为了防止此情况，设置 TTL 值使在老化时间内，多次发送更新 LLDP 帧。可以通过更改交换机的 holdtime 来控制发送 lldp 报文的 ttl 超时时间。

在全局配置模式下使用下面的命令可以配置 lldp 的 holdtime：

序号	配置	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#lldp holdtime *time*	配置 lldp 的超时时间，取值范围：<0-65535>，默认为 120 秒

恢复超时时间的默认配置：

序号	配置	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#no lldp holdtime	将超时时间恢复成默认值，默认为 120 秒

注意：超时时间应该比 lldp 报文发送的间隔时间要长，这样才能够保证在收到下一个 lldp 帧时，前面的邻居信息没有老化丢失。

配置 timer

通过配置 lldp 的 timer 可以控制交换机发送报文的间隔时间。

在全局配置模式下使用下面的命令可以配置 lldp 的 timer：

序号	配置	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#lldp timer *time*	配置 lldp 帧发送间隔。取值范围：<5-65534>，默认为 30 秒

恢复发送间隔的默认值：

序号	配置	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#no lldp timer	恢复为默认的间隔时间， 默认为 30 秒

配置 reinit

在本地系统中一个或多个信息元素（管理对象）状态或值发生变化和发送计时器超时两种情况下，自动发送 LLDP 信息。由于单个信息变化即需要发送 LLDP 帧，可能连续的一系列信息改变触发许多 LLDP 帧发送，每个帧中只报告一个变化，为了避免这种情况，网络管理定义了两个连续发送 LLDP 帧间的等待时间。通过配置 lldp 的 reinit 可以控制连续两个 lldp 报文发送的间隔时间

序号	配置	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#lldp reinit *time*	配置 lldp 连续发送报文的间隔时间。取值范围：<2-5>，默认为 2 秒

恢复 reinit 的默认值：

序号	配置	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#no lldp reinit	恢复为默认的连续报文发送间隔，默认为 2 秒

配置选择需要发送的 TLV

通过配置 lldp 的 tlv-select 可以选择需要发送的 TLV 进行发送. 默认情况下全部 TLV 都被发送。

在全局配置模式下使用下面的命令可以配置添加要发送的 tlv：

序号	配置	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#lldp tlv-select management-address	可选。发送管理地址 tlv，管理地址应该方便管理使用，一般为三层 IP 地址。
3	Inspur_config#lldp tlv-select port-description	可选。发送端口描述 tlv。端口描述采用数字或字母来描述端口。
4	Inspur_config#lldp tlv-select system-capabilities	可选。发送系统性能 tlv，系统性能是指发送报文的系统是交换机/路由器或是其它。

序号	配置	说明
5	Inspur_config#**lldp tlv-select system-description**	可选。发送系统描述 **tlv**，系统描述由数字字母组成的网络实体的文本描述。系统描述应该包括系统的全名，系统硬件类型的版本定义，软件操作系统，网络软件。
6	Inspur_config#**lldp tlv-select system-name**	可选。发送系统名称 **tlv**。系统名域为由数字字母 组成的系统管理者指定的名称。系统名应该为系统管理者名称,即交换机名称。

在全局配置模式下使用下面的命令可以配置删除要发送的 tlv：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**no lldp tlv-select management-address**	可选。发送管理地址 **tlv**，管理地址应该方便管理使用，一般为三层 IP 地址。
3	Inspur_config#**no lldp tlv-select port-description**	可选。发送端口描述 **tlv**。端口描述采用数字或字母来描述端口。
4	Inspur_config#**no lldp tlv-select system-capabilities**	可选。发送系统性能 **tlv**，系统性能是指发送报文的系统是交换机/路由器或是其它。
5	Inspur_config#**no lldp tlv-select system-description**	可选。发送系统描述 **tlv**，系统描述由数字字母组成的网络实体的文本描述。系统描述应该包括系统的全名，系统硬件类型的版本定义，软件操作系统，网络软件。
6	Inspur_config#**no lldp tlv-select system-name**	可选。发送系统名称 **tlv**。系统名域为由数字字母 组成的系统管理者指定的名称。系统名应该为系统管理者名称。即交换机名称。

指定端口配置选择需要发送的扩展 TLV

通过端口配置 lldp 的 dot1-tlv-select/ dot3-tlv-select/ med-tlv-select 可以选择需要发送的扩展 TLV 进行发送. 默认情况下 DOT1 和 DOT3 的 TLV 都被发送，MED 的 TLV 不被发送。

在接口配置模式下使用下面的命令可以配置添加要发送的 tlv：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**interface** *tgigaEthernet 3/1*	进入到端口配置模式。
3	Inspur_config_tg3/1#**lldp dot1-tlv-select port-vlan-id**	可选，发送 802.1 组织自定义 **tlv**，通知端口的 **PVID**。

序号	配置	说明
4	Inspur_config_tg3/1#**lldp dot1-tlv-select protocol-vlan-id**	可选，发送 802.1 组织自定义 **tlv**，通知端口的 **PPVID**。
5	Inspur_config_tg3/1#**lldp dot1-tlv-select vlan-name**	可选，发送 802.1 组织自定义 **tlv**，通知端口的 **vlan name**。
6	Inspur_config_tg3/1#**lldp dot1-tlv-select protocol-identity**	可选，发送 802.1 组织自定义 **tlv**，通知端口的 **Protocol-identity**。
7	Inspur_config_tg3/1#**lldp dot3-tlv-select macphy-confg**	可选，发送 802.3 组织自定义 **tlv**，包含以下内容： **a**）物理层具有的比特率和通信模式 **(duplex)**； **b**）目前的 **duplex** 和设置的比特率； **c**）表明设置是连接初始化阶段自动协商的结果。
8	Inspur_config_tg3/1#**lldp dot3-tlv-select power**	可选，发送 802.3 组织自定义 **tlv**，显示端口通过 链路允许电源被提供给连接无电源的系统。
9	Inspur_config_tg3/1#**lldp dot3-tlv-select link-aggregation**	可选，发送 802.3 组织自定义 **tlv**，指示端口链路 是否能够被聚合，若是，则指示端口辨别聚合。
10	Inspur_config_tg3/1#**lldp dot3-tlv-select max-frame-size**	可选，发送 802.3 组织自定义 **tlv**，指示端口最大 支持帧的大小（字节）。
11	Inspur_config_tg3/1#**lldp med-tlv-select network-policy**	可选，发送 **MED** 自定义 **tlv**，显示端口能有效的 发现和诊断 **VLAN** 配置的错误匹配的流，还有相关的 2 层和 3 层的属性。
12	Inspur_config_tg3/1#**lldp med-tlv-select location**	可选，发送 **MED** 自定义 **tlv**，指定了地址，包括： a）基于坐标的 **LCI**，在 **IETF RFC** 3825 [6]里定义； b）城市地址 **LCI**，在 **IETF (refer to ANNEX B)**里定义； c）紧急呼叫服务 **ELIN** 号码；
13	Inspur_config_tg3/1#**lldp med-tlv-select power-management**	可选，发送 **MED** 自定义 **tlv**，显示经由媒介依赖 端口的扩展电源发现使能媒介终端和网络连通 设备广告详细的电源信息。
14	Inspur_config_tg3/1#**lldp med-tlv-select inventory**	可选，发送 **MED** 自定义 **tlv**，显示发现使能跟踪 和鉴定终端相关的详细清单属性。

在全局配置模式下使用下面的命令可以配置删除要发送的 tlv：

序号	配置	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#interface interface-type interface-number	进入到端口配置模式。（后续使用 tg3/1 接口）
3	Inspur_config_tg3/1#no lldp dot1-tlv-select port-vlan-id	可选，发送 802.1 组织自定义 tlv，通知端口的 PVID。
4	Inspur_config_tg3/1#no lldp dot1-tlv-select protocol-vlan-id	可选，发送 802.1 组织自定义 tlv，通知端口的 PPVID。
5	Inspur_config_tg3/1#no lldp dot1-tlv-select vlan-name	可选，发送 802.1 组织自定义 tlv，通知端口的 vlan name。
6	Inspur_config_tg3/1#no lldp dot1-tlv-select protocol-identity	可选，发送 802.1 组织自定义 tlv，通知端口的 Protocol-identity。
7	Inspur_config_tg3/1#no lldp dot3-tlv-select macphy-confg	可选，发送 802.3 组织自定义 tlv，包含以下内容： a）物理层具有的比特率和通信模式（duplex）； b）目前的 duplex 和设置的比特率； c）表明设置是连接初始化阶段自动协商的结果。
8	Inspur_config_tg3/1#no lldp dot3-tlv-select power	可选，发送 802.3 组织自定义 tlv，显示端口通过 链路允许电源被提供给连接无电源的系统。
9	Inspur_config_tg3/1#no lldp dot3-tlv-select link-aggregation	可选，发送 802.3 组织自定义 tlv，指示端口链路 是否能够被聚合，若是，则指示端口辨别聚合。
10	Inspur_config_tg3/1#no lldp dot3-tlv-select max-frame-size	可选，发送 802.3 组织自定义 tlv，指示端口最大 支持帧的大小（字节）。
11	Inspur_config_tg3/1#no lldp med-tlv-select network-policy	可选，发送 MED 自定义 tlv，显示端口能有效的 发现和诊断 VLAN 配置的错误匹配的流，还有相 关的 2 层和 3 层的属性。
12	Inspur_config_tg3/1#no lldp med-tlv-select location	可选，发送 MED 自定义 tlv，指定了地址，包括： a）基于坐标的 LCI，在 IETF RFC 3825 [6]里定义； b）城市地址 LCI，在 IETF（refer to ANNEX B)里定义； c）紧急呼叫服务 ELIN 号码；

序号	配置	说明
13	Inspur_config_tg3/1#**no lldp med-tlv-select power-management**	可选，发送 **MED** 自定义 **tlv**，显示经由媒介依赖 端口的扩展电源发现使能媒介终端和网络连通 设备广告详细的电源信息。
14	Inspur_config_tg3/1#**no lldp med-tlv-select inventory**	可选，发送 **MED** 自定义 **tlv**，显示发现使能跟踪 和鉴定终端相关的详细清单属性。

发送 / 接收状态配置

Lldp 系统可工作在以下几种模式下：仅可发送模式，仅可接收模式和可发送可接收模式．默认情况下为可发送接收模式，通过下面的命令可改变 lldp 的工作模式。

在接口配置态下使用下面的命令配置 lldp 的工作模式为禁止发送接收模式：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**interface** *interface-type interface-number*	进入到端口配置模式（后续使用 tg3/1 接口）
3	Inspur_config_tg3/1#**no lldp transmit**	配置端口为禁止发送 **lldp** 帧模式
4	Inspur_config_tg3/1#**no lldp receive**	配置端口为禁止接收 **lldp** 帧模式

在接口配置态下使用下面的命令配置 lldp 的工作模式为可发送接收模式：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**interface** *interface-type interface-number*	进入到端口配置模式（后续使用 tg3/1 接口）
3	Inspur_config_tg3/1#**lldp transmit**	配置端口为可发送 **lldp** 帧模式
4	Inspur_config_tg3/1#**lldp receive**	配置端口为可接收 **lldp** 帧模式

注意： 除上述模式外，还可将端口配置为仅发送或仅接收模式。

指定端口管理 ip 地址

在端口配置状态下面用户可以任意配置 lldp 报文发送的端口的管理地址，该管理地址应该是一个和端口相关的 ip 地址，这样才能够保证管理地址的正常通信。

在接口配置态下使用下面的命令配置管理 ip 地址：

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

序号	配置	说明
2	Inspur_config#**interface** *interface-type interface-number*	进入到端口配置模式（后续使用 tg3/1 接口）
3	Inspur_config_tg3/1# **lldp management-ip** *A.B.C.D*	配置端口管理 **ip** 地址

注意：使用 no lldp management-ip 可以恢复端口默认的管理地址，默认的管理地 址为端口 pvid 对应的 vlan 接口的 ip 地址，当对应的 vlan 接口不存在时，管理地址值为 0.0.0.0。

发送 trap 通知到 mib 库

发送 trap 通知到 lldp mib 库或 ptopo mib 库。

在全局配置态下使用下面的命令发送 trap 通知到 lldp mib 库或 ptopo mib 库

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**lldp trap-send lldp-mib**	发送 **trap** 通知到 **lldp mib** 库
3	Inspur_config#**lldp trap-send ptopo-mib**	发送 **trap** 通知到 **ptopo mib** 库

配置 location 信息

通过 location 信息的配置， 来确定本机的地址信息。

在全局配置模式下使用下面的命令可以配置 location 信息：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**location elin identifier** *id WORD*	配置 **location elin** 信息，**id** 为 **elin identifier** 号， **WORD** 是 **elin** 信息，取值 10-25**bytes**
3	Inspur_config#**location civic identifier** *id*	进入 **location** 配置模式
4	Inspur_config_civic#**language** *WORD*	设置语言
5	Inspur_config_civic#**state** *WORD*	设置州（行政区，区，省，管区）名
6	Inspur_config_civic#**county** *WORD*	设置县名
7	Inspur_config_civic#**city** *WORD*	设置城市名
8	Inspur_config_civic#**division** *WORD*	设置地区名
9	Inspur_config_civic#**neighborhood** *WORD*	设置邻居名

序号	配置	说明
10	Inspur_config_civic#**street** *WORD*	设置街道名
11	Inspur_config_civic#**leading-street-dir** *WORD*	设置主街道方向，比如 **N**（北）
12	Inspur_config_civic#**trailing-street-suffix** *WORD*	设置小路下标，比如 **SW**
13	Inspur_config_civic#**street-suffix** *WORD*	设置街道下标，比如 **Platz** 大道
14	Inspur_config_civic# **number** *WORD*	设置街道号，比如 **123** 号
15	Inspur_config_civic# **street-number-suffix** *WORD*	设置街道号下标，比如 **A** 路 1/2 号
16	Inspur_config_civic#**landmark** *WORD*	设置地标信息，比如哥伦比亚大学
17	Inspur_config_civic#**additional-location** *WORD*	设置增加的位置信息
18	Inspur_config_civic#**name** *WORD*	设置居民信息，比如 **Joe** 的理发店
19	Inspur_config_civic#**postal-code** *WORD*	设置邮编
20	Inspur_config_civic#**building** *WORD*	设置楼信息
21	Inspur_config_civic#**unit** *WORD*	设置单元信息
22	Inspur_config_civic#**floor** *WORD*	设置楼层信息
23	Inspur_config_civic#**room** WORD	设置房间信息
24	Inspur_config_civic#**type-of-place** WORD	设置地点类型，比如办公室
25	Inspur_config_civic#**postal-community** *WORD*	设置邮局名
26	Inspur_config_civic#**post-office-box** *WORD*	设置邮箱名，比如 12345
27	Inspur_config_civic#**additional-code** *WORD*	设置增加的代码
28	Inspur_config_civic#**country** *WORD*	设置国家名
29	Inspur_config_civic#**script** *WORD*	设置脚本信息

在全局配置模式下使用下面的命令可以配置删除 **location** 信息：

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

序号	配置	说明
2	Inspur_config#**no location elin identifier** id	删除 elin identifier 号为 id 的 location elin 信息
3	Inspur_config#**no location civic identifier** id	删除 civic identifier 号为 id 的 location civic 信息
4	Inspur_config#**location civic identifier** *id*	进入 **location** 配置模式
5	Inspur_config_civic#**no language**	删除语言
6	Inspur_config_civic#**no state**	删除州（行政区，区，省，管区）名
7	Inspur_config_civic#**no county**	删除县名
8	Inspur_config_civic#**no city**	删除城市名
9	Inspur_config_civic#**no division**	删除地区名
10	Inspur_config_civic#**no neighborhood**	删除邻居名
11	Inspur_config_civic#**no street**	删除街道名
12	Inspur_config_civic#**no leading-street-dir**	删除主街道方向，比如 **N**（北）
13	Inspur_config_civic#**no trailing-street-suffix**	删除小路下标，比如 **SW**
14	Inspur_config_civic#**no street-suffix**	删除街道下标，比如 **Platz** 大道
15	Inspur_config_civic#**no number**	删除街道号，比如 123 号
16	Inspur_config_civic#**no street-number-suffix**	删除街道号下标，比如 **A** 路 1/2 号
17	Inspur_config_civic#**no landmark**	删除地标信息，比如哥伦比亚大学
18	Inspur_config_civic#**no additional-location**	删除增加的位置信息
19	Inspur_config_civic#**no name**	删除居民信息，比如 **Joe** 的理发店
20	Inspur_config_civic#**no postal-code**	删除邮编
21	Inspur_config_civic#**no building**	删除楼信息
22	Inspur_config_civic#**no unit**	删除单元信息
23	Inspur_config_civic#**no floor**	删除楼层信息
24	Inspur_config_civic#**no room**	删除房间信息

序号	配置	说明
25	Inspur_config_civic#**no type-of-place**	删除地点类型，比如办公室
26	Inspur_config_civic#**no postal-community**	删除邮局名
27	Inspur_config_civic#**no post-office-box**	删除邮箱名，比如 12345
28	Inspur_config_civic#**no additional-code**	删除增加的代码
29	Inspur_config_civic#**no country**	删除国家名
30	Inspur_config_civic#**no script**	删除脚本信息

指定端口配置 location 信息

为端口配置 **location** 信息，在 **TLV** 信息中承载 **location** 信息。在接口配置态下使用

下面的命令配置 **location** 信息：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**interface** *interface-type interface-number*	进入到端口配置模式（后续使用 tg3/1 接口）
3	Inspur_config_tg3/1#**location civic id**	为端口配置 civic 为 id 的 location 信息
4	Inspur_config_tg3/1#**location elin id**	为端口配置 elin 为 id 的 location 信息

在接口配置态下使用下面的命令删除端口 location 信息：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**interface** *interface-type interface-number*	进入到端口配置模式（后续使用 tg3/1 接口）
3	Inspur_config_tg3/1#**no location civic**	删除端口配置 civic 的 location 信息
4	Inspur_config_tg3/1#**no location elin**	删除端口配置 elin 的 location 信息

显示命令配置

序号	配置	说明

序号	配置	说明
1	Inspur#show lldp errors	显示 lldp 模块的出错信息
2	Inspur# show lldp interface *interface-type interface-number*	显示端口的状态信息，即发送和接收模式
3	Inspur#show lldp neighbors	显示接收邻居的简略信息
4	Inspur#show lldp neighbors detail	显示接收邻居的详细信息
5	Inspur#show lldp traffic	显示发送和接收的各种统计信息
6	Inspur#show location elin	显示 location elin 信息
7	Inspur#show location civic	显示 location civic 信息

清除命令配置

通过清除命令可以清除接收到的邻居列表和各种统计信息。 在管理配置命令模式下，使用下面的命令配置：

序号	配置	说明
1	Inspur#clear lldp counters	清除各种统计计数
2	Inspur#clear lldp table	清除接收到的邻居信息

6.3.4 配置示例

网络环境需求

在两台交换机相连的端口上配置 LLDP 协议。

网络拓扑图

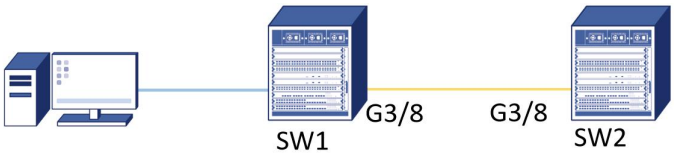


图 6.3.1 网络拓扑图

配置步骤

基本配置

配置交换机 S1： Inspur_config# hostname SW1

SW1_config#lldp run

SW1_config#

配置交换机 S2： Inspur_config# hostname SW2

SW2_config#lldp run

SW2_config#

大概一分钟以后可在交换机 SW1 上查看到邻居 SW2 信息，默认不发送 MED-TLV 信息。

在 S1 上验证：

```
SW1_config#show lldp neighbors
Capability Codes:
        (R)Router,(B)Bridge,(C)DOCSIS Cable Device,(T)Telephone
        (W)WLAN Access Point, (P)Repeater,(S)Station,(O)Other

Device-ID       Local-Intf      Hldtme      Port-ID      Capability
SW2             TGi3/8          106         TGi3/8       R B

Total entries displayed: 1
SW1_config#show lldp neighbors detail
local port id: TGigaEthernet3/8
chassis id: bc60.6bb6.1ef0
chassis id subtype: MAC address
port id: TGi3/8
port id subtype: locally assigned
port description: TGigaEthernet3/8
system name: SW2

system description: Inspur(tm) S9503-MU-24S8X Software, Version 4.1.3A
Serial: 0020077602685, Copyright(c) 2015-2024 Inspur Networking
Technology(Shandong) Co., Ltd. All rights reserved.
Compiled: 2024-10-15 16:56:24 by SYS

Time remaining: 107
system capabilities: R B
enabled capabilities: R B
```

```
Management Address:
   IP: 192.168.1.77
Port VLAN ID: 1
Auto Negotiation: supported,not enabled
Physical media capabilities:
   1000baseX(FD)
   1000baseX(HD)
   100baseTX(FD)
   100baseTX(HD)
Operational MAU type: Four-pair Category 5 UTP, half duplex mode(30)

MED Information:

  MED Codes:
        (CA)Capabilities, (NP)Network Policy, (LI)Location Identification
        (PS)Power via MDI - PSE, (PD)Power via MDI - PD, (IN)Inventory

  Hardware Revision: 0.1.9
  Firmware Revision: 0.1.9
  Software Revision: 4.1.3A
  Serial Number: 0020077602685
  Manufacturer Name: Inspur
  Model Name: S9503-MU-24S8X
  Asset ID: S77602685
  Capabilities: CA,NP,LI,IN
  Device type: Network Connectivity
  Network Policy: Voice
    Policy: Unknown
  Power requirements - not advertised
----------------------------------------
```

Total entries displayed: 1

TLV 配置

配置交换机 SW1： Inspur_config# hostname SW1

SW1_config#lldp run

SW1_config#

配置交换机 SW2： Inspur_config# hostname SW2

SW2_config#lldp run

SW2_config#no lldp tlv-select system-name

SW2_config#interface tgigaEthernet 3/8

SW2_config_tg3/8#no lldp dot1-tlv-select port-vlan-id

SW2_config_tg3/8#no lldp dot3-tlv-select max-frame-size

SW2_config_tg3/8#

大概一分钟以后可在交换机 A 上查看到邻居 B 信息，与 1.4.3.1 基本配置中所显示的信息有所区别，分别用红色和蓝色来区分。

在 SW1 上验证：SW1_config#show lldp neighbors

Capability Codes:

(R)Router,(B)Bridge,(C)DOCSIS Cable Device,(T)Telephone

(W)WLAN Access Point, (P)Repeater,(S)Station,(O)Other

Device-ID	Local-Intf	Hldtme	Port-ID	Capability
bc60.6bb6.1ef0	TGi3/8	95	TGi3/8	R B

Total entries displayed: 1

SW1_config#show lldp neighbors Detail

local port id: TGigaEthernet3/8

chassis id: bc60.6bb6.1ef0

chassis id subtype: MAC address

port id: TGi3/8

port id subtype: locally assigned

port description: TGigaEthernet3/8

system name: -- not advertised

system description: Inspur(tm) S9503-MU-24S8X Software, Version 4.1.3A

Serial: 0020077602685, Copyright(c) 2015-2024 Inspur Networking Technology(Shandong) Co., Ltd. All rights reserved.

Compiled: 2024-10-15 16:56:24 by SYS

Time remaining: 96

system capabilities: R B

enabled capabilities: R B

Management Address:

IP: 192.168.1.77

Port VLAN ID -- not advertised

PPVID: 1

VLAN 1 name: Default

Auto Negotiation: supported,not enabled

Physical media capabilities:

1000baseX(FD)

1000baseX(HD)

100baseTX(FD)

100baseTX(HD)

Operational MAU type: Four-pair Category 5 UTP, half duplex mode(30)

Link Aggregation:

Aggregation capability: capable of being aggregated

Aggregation status: not currently in aggregation

Total entries displayed: 1

Location 配置

配置交换机 SW1：Inspur_config# hostname SW1

SW1_config#lldp run

SW1_config#

配置交换机 SW2：Inspur_config# hostname SW2

SW2_config#lldp run

SW2_config#location elin identifier 1 1234567890//配置 elin 信息

SW2_config#location civic identifier 1 //进入 location 配置模式

SW2_config_civic#language English

SW2_config_civic#city Shandong

SW2_config_civic#street Curie

SW2_config_civic#script EN //以上配置 civic 信息

SW2_config_civic#quit

SW2_config#interface tgigaEthernet 3/8

SW2_config_tg3/8#location elin 1//为端口指定 elin id

SW2_config_tg3/8#location civic 1 //为端口指定 civic id

Switch_config_g1/8#show location elin //显示 elin 配置信息

在 S2 上验证：

SW2_config#show location elin //显示 elin 配置信息

elin information:

  elin 1: 1234567890

total: 1

在 S1 上验证：

SW1_config#show lldp neighbors

Capability Codes:

(R)Router,(B)Bridge,(C)DOCSIS Cable Device,(T)Telephone

(W)WLAN Access Point, (P)Repeater,(S)Station,(O)Other

Device-ID	Local-Intf	Hldtme	Port-ID	Capability
SW2	TGi3/8	105	TGi3/8	R B

```
Total entries displayed: 1
SW1_config#show lldp neighbors detail

local port id: TGigaEthernet3/8
chassis id: bc60.6bb6.1ef0
chassis id subtype: MAC address
port id: TGi3/8
port id subtype: locally assigned
port description: TGigaEthernet3/8
system name: SW2

system description: Inspur(tm) S9503-MU-24S8X Software, Version
4.1.3A
Serial: 0020077602685, Copyright(c) 2015-2024 Inspur Networking
Technology(Shandong) Co., Ltd. All rights reserved.
Compiled: 2024-10-15 16:56:24 by SYS

Time remaining: 107
system capabilities: R B
enabled capabilities: R B
Management Address:
   IP: 192.168.1.77

Port VLAN ID: 1
PPVID: 1
VLAN 1 name: Default
Auto Negotiation: supported,not enabled
Physical media capabilities:
   1000baseX(FD)
   1000baseX(HD)
   100baseTX(FD)
```

```
        100baseTX(HD)

    Operational MAU type: Four-pair Category 5 UTP, half duplex
mode(30)


    Link Aggregation:

            Aggregation capability: capable of being aggregated

            Aggregation status: not currently in aggregation

    Maximum frame size: 1500

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


    Total entries displayed: 1
```

6.4 NTP

6.4.1 NTP 简介

NTP网络时间协议（Network Time Protocol）是用来使计算机时间同步化的一种协议，可用于分布式时间服务器和客户端之间进行时间同步。它可以提供高精度的时间校正，且可通过加密认证方式防止恶意的协议攻击。客户端和服务器端采用UDP协议进行通信，端口号为123。

6.4.2 配置准备

场景

配置设备的系统时间，保证系统时间的精准。
多台设备之间的日志时间戳一致。
安全事件（如防火墙日志）的时间同步，便于追踪和分析。

6.4.3 NTP 配置

配置设备作为 NTP 服务器

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**ntp master primary**	配置设备作为原始 **NTP** 服务器（**stratum = 1**），在设备无上级 **NTP** 服务器的情况下采用该配置

序号	配置	说明
3	Inspur_config#**ntp master secondary**	为工作在对等体模式下的交换机设备配置 **NTP** 对等体地址、版本号、最大轮询时间间隔和最小轮询时间间隔。

配置设备为 NTP 客户端

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**ntp client enable**	配置设备作为 **NTP** 客户端，从 **NTP** 服务器同步时间。
3	Inspur_config# **ntp server** *ip-address* [**version** *number* |**key** *keyed* | **vrf** *vrf-name*]*	配置 **NTP** 服务器 **IP** 地址，可指定版本号、密钥号以及所属 **vrf** 实例

配置 NTP 认证功能

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**ntp authentication enable**	打开认证功能（默认关闭）
3	Inspur_config#**ntp authentication key** *keyid* **md5** *password*	配置 **NTP md5** 认证 keyid 和对应密钥
4	Inspur_config# **ntp authentication trusted-key** *keyid*	配置 **keyid** 对应密钥为可信密钥

配置 NTP 关联

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config# **ntp server** *ip-address* [**version** *number* |**key** *keyed* | **vrf** *vrf-name*]*	配置 **NTP** 服务器 **IP** 地址，可指定版本号、密钥 号以及所属 **vrf** 实例
3	Inspur_config# **ntp peer** *ip-address* [**version** *number* | **key** *keyid* | **vrf** *vrf-name*]*	配置设备 **NTP** 对等体 **IP** 地址，可指定版本号、 密钥号以及所属 **vrf** 实例

重要说明：

1. 只有在设备自己取得时间同步的前提下才能给 **NTP** 客户端提供时间服务，否则以该设备作

为服务器的客户端设备无法获得时间同步

2. 需要 **NTP** 认证时，通信双方必须同时打开 **NTP** 认证功能，并且保证配置相同的 **keyid** 和密钥，同时必须指定 **keyid** 为可信任的，否则时间同步失败

配置NTP 轮询时间

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**ntp query-interval** *offset-seconds*	配置 **ntp** 轮询服务器的时间间隔

重要说明：

1.只有配置了 **ntp peer** 或者 **ntp server** 的情况下 **ntp query-interval** 才能正常工作，如果 **ip** 地址 没有配置或者配置没有成功的话，**ntp query-interval** 的配置是没有什么意义的。

显示命令配置

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**show ntp status**	显示 NTP 状态
3	Inspur_config#**show ntp timers**	显示 NTP 定时器状态
4	Inspur_config#**show ntp associations** [**detail**]	显示 NTP 关联状态及显示每个 NTP 关联详细信息

重要说明：

设备重启，系统时间会丢失，为硬件限制

6.4.3 配置示例

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：

- SW1 作为时钟同步系统的主时钟。
- SW2 作为时钟同步系统的客户端，需设置上层的 S1 为 NTP 服务器。

图 6.4 NTP 组网示意图

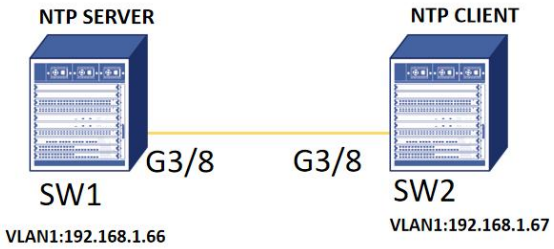


图 6.4.1

配置步骤

步骤 1：配置 SW1。

```
Inspur#config
Inspur_config#hostname SW1
SW1_config#ntp master primary
```

步骤 2：配置 SW2。

```
Inspur#config
Inspur_config#hostname SW2
SW2_config#ntp server 192.168.1.66
SW2_config#ntp client enable
```

检查结果

查看 SW1:通过 **show ntp status** 查看 SW1 配置是否正确。

```
SW1_config#show ntp status
Time-zone: GMT+0:00, UTC
Current time: 2025-02-11 10:12:46
Clock Status: synchronized
Clock Stratum: 1
Leap Indicator: 0
Reference ID: LOCL
Clock Jitter: 0.000000
Clock Precision: -18
Clock Offset: 0.000 ms
Root Delay: 0.000 ms
Root Dispersion: 0.000 ms
Packets Sent: 6
Packets Received: 6 (bad version: 0)
Reference Time: 1970-01-01 00:00:00
Last Update Time: 1970-01-01 00:00:00
```

查看 SW2:通过 **show ntp status** 查看 SW2 配置是否正确。

```
SW2_config#show ntp status

Time-zone: GMT+0:00, UTC
```

```
Current time: 2025-02-11 10:15:42
Clock Status: synchronized
Clock Stratum: 2
Leap Indicator: 0
Reference ID: 192.168.1.66
Clock Jitter: 0.000000
Clock Precision: -18
Clock Offset: 447.215 ms
Root Delay: 0.500 ms
Root Dispersion: 8385.134 ms
Packets Sent: 34
Packets Received: 34 (bad version: 0)
Reference Time: 2025-02-11 10:15:31
Last Update Time: 2025-02-11 10:15:26
```

通过 **show ntp associations** 查看 SW2 的 NTP 会话信息。

```
SW2_config#show ntp associations

 ip address      reference clock  st  poll   reach  delay   offset   dispersion
---------------------------------------------------------------------------------
*192.168.1.66    LOCL             1   8      37     0.48    447.72   437.9
---------------------------------------------------------------------------------
Notes: * system peer(master), poll(s), delay(ms), offset(ms), dispersion(ms)

Total Associations: 1
```

6.5 系统日志

6.5.1 系统日志简介

设备在运行过程中，主机软件中的日志模块会对运行中的各种情况进行记录，从而形成日志信息。

日志信息主要用于查看设备的运行状态、分析网络的状况以及定位问题发生的原因，为系统进行诊断和维护提供依据。

系统日志信息级别，根据严重程度分为 8 个等级，如下表所示。

信息级别

严重等级	级别	说明
emergencies	0	系统不可用
alerts	1	需要马上行动
critical	2	临界情况
errors	3	错误情况
warnings	4	警告情况
notifications	5	正常但很重要的情况
informational	6	报告性信息
debugging	7	调试信息

6.5.2 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。

6.5.3 配置系统日志

配置系统日志基本信息

请在设备上进行以下配置。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**logging on**	配置使能系统日志功能。
3	Inspur_config#**service timestamps** [log|debug] [*uptime*| *datetime*]	配置系统在 debug 或记录日志信息时附加时间戳。 缺省开启：**service timestamps log date** **service timestamps debug date**
4	Inspur_config#**logging source-interface** [*vlan* / *Null*]	设置日志交互的源地址端口

日志信息记录到指定的 IPV4syslog 服务器上

请在设备上进行以下配置。

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

序号	配置	说明
2	Inspur_config#**logging** *A.B.C.D*	使用 logging 命令将指定级别的日志信息记录到 IPV4syslog 服务器上。

日志信息记录到指定的 IPV6syslog 服务器上

请在设备上进行以下配置。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**logging** *X:X:X::X*	使用 logging 命令将指定级别的日志信息记录到 IPV6syslog 服务器上。

设置日志缓存容量

请在设备上进行以下配置。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**logging buffered** *size*	设置日志缓存容量，范围：4096-2147483647 字节。

禁止所有的记录。

请在设备上进行以下配置。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2.	Inspur_config#**no logging on**	使用 **no logging on** 来禁止所有的记录。

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 start** *hour minute year month day* **file** [*file_name*]	查看某年某月某某时的日志信息。
3	Inspur#**show logging file**	查看系统日志文件内容

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	清除日志信息
Inspur_config#clear logging-file	清除日志文件

6.5.3 配置示例

组网需求

如下图所示，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。

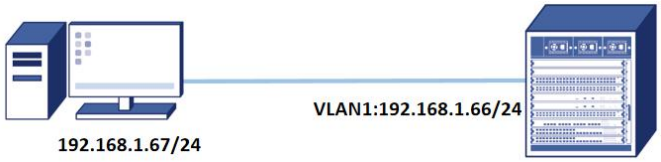


图 6.5.1 系统日志输出到日志主机组网示意图

配置步骤

步骤 1 配置设备的 IP 地址。

```
Inspur#config
Inspur_config#interface vlan 1
Inspur_config_v1#ip address 192.168.1.66 255.255.255.0
Inspur_config_v1)#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 192.168.1.77
```

检查结果

通过 show logging 命令查看系统日志配置是否正确。

```
Inspur_config#show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: level debugging, 56 messages logged
    Monitor logging: level errors, 0 messages logged
    Buffer logging: disabled
```

```
Trap logging: level informational, 1 message lines logged
```

6.6 CPU 监控

6.6.1 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（1 秒，1 分钟，5 分钟）内各任务的 CPU 利用率。

  提供查看设备当前运行的任务或进程状态。

  提供 CPU 限速配置信息。

- CPU 利用率门限告警

  设置相应的阈值，在超过该阈值时进行告警。

6.6.2 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。

6.6.3 配置 CPU 监控

配置 CPU 监控告警

请在设备上进行以下配置。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**threshold** [*slot number*] **cpu-threshold** *percentage*	**CPU** 监控利用率预警阈值，阈值取值范围：1-99%。

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	配置	说明
1	Inspur#**config**	进入全局配置模式。

序号	配置	说明
2	Inspur_config#**show cpu**	查看 CPU 利用率信息。
3	Inspur_config#**show cpu-threshold** [**configuration** | **statistics** | **rate**]	查看显示 CPU 限速信息的配置信息/统计信息/速率信息。
4	Inspur_config#**show cpu-util** [*slot*]	查看当前 CPU 利用率/

6.7 内存监控

6.7.1 简介

在网络运行中，内存占用率过高常常会导致业务异常。在设备处理数据的过程中，如果能够对内存出现高占用率的情况及时告警，可以更有效地监控内存的使用情况，优化系统性能，以保证系统一直处于良性运作。

6.7.2 配置准备

场景

实时监控系统的内存利用率，根据提供的阈值告警，及时发现并消除隐患。

6.7.3 配置内存监控

配置内存监控告警

请在设备上进行以下配置。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**threshold** [*slot number*] **mem-threshold** *percentage*	内存监控利用率预警阈值，阈值取值范围：1-99%。

6.7.4 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	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**show mem-util** [*slot*]	查看当前 **memory** 利用率

6.8 风扇监控

6.8.1 简介

设备支持风扇监控功能，可以对风扇的状态进行监控，当设备监控到风扇出现异常时，会产生告警信息。

6.8.2 配置准备

场景

实时监控设备风扇状态，根据提供的风扇告警，及时发现并消除隐患。

6.8.3 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。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config# **fan-config warning-threshold** *fan_number*	配置风扇告警阀值，当损坏风扇数量超过阀值后报警
3	Inspur_config#**fan-detect**	检测风扇

6.8.4 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-status**	查看风扇状态

6.9 Ping

6.9.1 简介

ping 是一种常用的网络工具，用于测试主机之间的连通性。它通过发送 ICMP（Internet Control Message Protocol）回显请求报文到目标主机，并等待其返回 ICMP 回显应答报文，从而判断网络是否通畅以及测量往返时间（RTT）。

工作原理

发送请求：源主机向目标主机发送 ICMP Echo Request 报文。

接收响应：如果目标主机可达且未屏蔽 ICMP 请求，它会返回 ICMP Echo Reply 报文。

计算时间：源主机根据发送和接收的时间差计算往返时间（RTT）。

6.9.2 配置 IPv4 Ping 功能

请在设备上进行以下操作。

序号	配置	说明
1	Inspur# **ping** [-a][-d] [**-f**] [**-i** {*source-ip-address*}] [**-m** {*source-interface*}] [**-j** *host1* [*host2 host3 …*]] [**-k** *host1* [*host2, host3 …*]] [**-l** *length*] [**-n** *number*] [**-r** *hops*] [**-s** *tos*] [**-t** *ttl*] [**-v**] [**-w** *waittime*] [**-b** *time*] [**-c**] [**-vrf** *vpnname*] *WORD*	通过 **ping** 命令测试 IPv4 网络的连通性。

Ping 命令参数解释

序号	参数	说明
1	**-a**	一直 **ping**，直到被中断
2	**-d**	不使用路由表， 直接路由到端口
3	**-f**	置 **DF**（报文不分片）位。如果用户要求发送的报文大于路径 **MTU**，报文会被路径上的路由交换机丢弃，并向源主机发送 **ICMP** 出错报文。如果发现网络性能问题，可能是由于其中的一个节点配置了较小的 **MTU**。可以使用这个选项确定路径上的最小 **MTU**。缺省：不置位。
4	**-i**	设置报文采用的源 **IP** 地址或者某个接口的 IP 地址。缺省：发送接口的主 **IP** 地址。
5	**source-ip-address**	报文采用 **source-ip-address** 作为源 IP 地址。
6	**-m**	报文指定端口地址。
7	**source-interface**	报文采用 **source-interface** 接口的 IP 地址作为源地址。
8	**-j** *host1 [host2 host3…]*	设置松弛源路由。缺省：不设置。
9	**-k** *host1 [host2 host3…]*	设置严格源路由。缺省：不设置。
10	**-l** *length*	设置报文中 ICMP 数据的长度。缺省：56 字节。
11	**-n** *number*	设置发送的总报文数。缺省：5 个报文。
12	**-r** *hops*	记录路由，最多记录 **hops** 条路由。缺省：不记录路由。
13	**-s** *tos*	设置报文的 **IP TOS** 为 **tos**。缺省：0

序号	参数	说明
14	**-t** *ttl*	设置报文的 **IP TTL** 为 **ttl**。缺省：255。
15	**-v**	详细输出。缺省：简要输出。
16	**-w** *waittime*	每个报文等待应答的时间。 缺省： 2 秒。
17	**-b** *time*	两个 **ping** 报文之间的间隔时间。
18	**-c**	详细输出。
19	**-vrf**	所在的 vpn 名称。
20	**WORD**	目的地址或主机名

重要说明：

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“q”或“Q”键强制中断执行过程后才能进行其他操作。

6.9.3 配置 IPv6 Ping 功能

请在设备上进行以下操作。

序号	配置	说明
1	Inspur#**ping6** [**-a**|**-l** *data_bytes*|**-n** *times*|**-v**| **-w** *seconds*|**-b** *ms*|-i *Source_address*] WORD	通过 **ping6** 命令测试 IPv6 网络的连通性。

Ping6 命令参数解释

序号	参数	说明
1	**-a**	一直 **ping**，直到被中断
2	**-l**	数据长度,数据字节缺省 56
3	**-n**	发送的 **echo** 请求报文数
4	**-v**	设置报文采用的源 **IP** 地址或者某个接口的 IP 地址。缺省：发送接口的主 **IP** 地址。
5	**-w**	报文采用 **source-ip-address** 作为源 IP 地址。
6	**-b**	报文指定端口地址。
7	**-i**	报文采用 **source-interface** 接口的 IP 地址作为源地址。
8	**WORD**	设置松弛源路由。缺省：不设置。

重要说明：

在 ping6 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“q”或“Q”键强制中断执行过程后才能进行其他操作。

6.10 Traceroute

6.10.1 简介

Traceroute 是一种网络诊断工具，用于追踪数据包从源设备到目标设备的路径。它通过显示数据包经过的每一跳（hop）来帮助识别网络路径中的问题，如延迟、丢包或路由错误。

工作原理

发送探测包：Traceroute 发送一系列数据包（通常是 ICMP 或 UDP），并逐步增加 TTL（Time to Live）值。

TTL 过期：每经过一个路由器，TTL 减 1，当 TTL 为 0 时，路由器丢弃数据包并返回一个 ICMP "Time Exceeded" 消息。

记录路径：源设备通过接收到的 ICMP 消息确定每一跳的 IP 地址和往返时间（RTT）。

配置 IPv4 Traceroute 功能

请在设备上进行以下操作。

序号	配置	说明
1	Inspur# **traceroute [-i** *source-ip-address* **] [-m** *source-interface***}] [-j** *host1* **[***host2 host3 …***]] [-k host1 [host2,host3 …]] [-p** *port-number***] [-q** *probe-count***] [-r** *hops***] [-t** *min max***] [-vrf** *name***] [-w** *waittime***] [-x** *icmp***] WORD**	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。

traceroute 命令参数解释

序号	参数	说明
1	**-i** *source-ip-address*	设置报文采用的源 **IP** 地址
2	**-m** *source-interface*	设置报文发送的端口
3	**-j** *host1 [host2 host3…]*	设置松弛源路由。缺省：不设置。
4	**-k** *host1 [host2 host3…]*	设置严格源路由。缺省：不设置。
5	**-p** *port-number*	设置发送 **UDP** 报文的目的端口号。缺省：33434。
6	**-q** *probe-count*	设置每次探测的报文数。缺省：3 个报文。

序号	参数	说明
7	**-r** *hops*	记录路由，最多记录 hops 条路由。缺省：不记录路由。
8	**-t** *min max*	设置报文的最小和最大 IP TTL 为 min 和 max。 缺省：最小为 1，最大 255。
9	**-vrf** *name*	设置 **VPN** 路由转发对象名称
10	**-w** *waittime*	每个报文等待应答的时间。缺省：3 秒。
11	**-x** *icmp*	设置探测报文为 **ICMP ECHO** 报文。缺省：**UDP** 报文
12	**WORD**	目的地址或主机名
13	**-h**	报文指定下一跳 IP 地址

重要说明：

在 **traceroute** 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“q”或“Q”键强制中断执行过程后才能进行其他操作。

配置 IPv6 Traceroute 功能

请在设备上进行以下操作。

序号	配置	说明
1	Inspur# **traceroute6** [**-i** *source-ip-address*] [**-p** *port-number*] [**-q** *probe-count*] [**-t** *min max*] [**-vrf** *name*] [**-w** *waittime*] [**-x** *icmp*] **WORD**	通过 **traceroute6** 命令测试 IPv6 网络的连通性并查看报文经过的网络节点。

traceroute 命令参数解释

序号	参数	说明
1	**-i** *source-ip-address*	设置报文采用的源 **IP** 地址
2	**-p** *port-number*	设置发送 **UDP** 报文的目的端口号。缺省：33434。
3	**-q** *probe-count*	设置每次探测的报文数。缺省：3 个报文。
4	**-t** *min max*	设置报文的最小和最大 **IP TTL** 为 **min** 和 **max**。 缺省：最小为 1，最大 255。
5	**-w** *waittime*	每个报文等待应答的时间。缺省：3 秒。
6	**-x** *icmp*	设置探测报文为 **ICMP ECHO** 报文。缺省：**UDP** 报文

序号	参数	说明
7	WORD	目的地址或主机名

重要说明：

在 traceroute6 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“q”或“Q”键强制中断执行过程后才能进行其他操作。

6.11 PDP

6.11.1 简介

PDP 协议专门用于发现网络设备的两层协议，用于网管程序发现已知设备的所有邻居，使用 PDP，能够学到邻居设备的设备类型和 SNMP 代理地址。通过 PDP 发现邻居设备，网管程序能够用 SNMP 询问邻居设备以获得网络拓扑结构。

本公司交换机上的 PDP 功能能够实现发现邻居设备的功能，但不能接受 SNMP 询问邻居设备，所以交换机只能处于网络边缘，否则将不能获得完整的网络拓扑结构。

交换机上的 PDP 能够配置于所有的 SNAP 上（如以太网等）。

6.11.2 配置准备

场景

通过 PDP 发现邻居设备，网管程序通过 SNMP 询问邻居设备以获得网络拓扑结构。

6.11.3 PDP 配置

交换机 PDP 默认配置

功能	默认设置
PDP 全局配置状态	未启动。
PDP 端口配置状态	启动。
PDP 时钟（发送报文频率）	60 秒。
PDP 信息保存	180 秒。
PDP 版本	2。

设置 PDP 时钟和信息保存时间

设置 PDP 发送报文的频率和 PDP 信息保存时间时， 可以在全局配置模式下使用下面的命令：

序号	配置	说明

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config# **pdp timer** *seconds*	配置 **PDP** 发送报文的频率
3	Inspur_config# **pdp holdtime** *seconds*	配置 **PDP** 信息保存时间。

设置 PDP 的版本

设置 PDP 支持的版本时，可以在全局配置模式下使用下面的命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config# **pdp version** *[1|2]*	配置 **PDP** 的版本。

启动交换机上的 PDP

PDP 在默认配置下是没有启动的， 如果要使用 PDP， 可以在全局配置模式下使用下面的命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**pdp run**	配置 **PDP** 的版本。

启动交换机端口上的 PDP

在全局开启了 PDP，端口下默认启动 PDP，在接口配置模式下使用下面的命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**interface tgigaEthernet 3/1**	进入到端口配置模式。
3	Inspur_config_tg3/1#**pdp enable**	启动交换机端口上的 **PDP** 功能。

监控和管理 PDP

配置完成后，请在设备上执行以下命令检查配置结果。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**show pdp traffic**	显示交换机接收和发送的 **PDP** 报文计数。

序号	配置	说明
3	Inspur_config#show pdp neighbor [detail]	显示交换机通过 PDP 发现的邻居。

6.11.4 配置示例

网络环境需求

在两台交换机相连的端口上配置 PDP 协议。

网络拓扑图

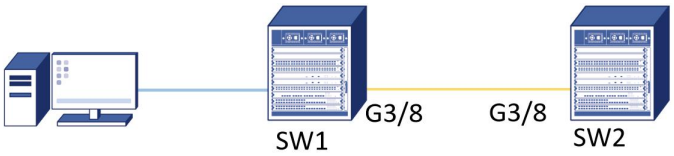


图 6.11.1 图 6-1 网络拓扑图

配置步骤

基本配置

配置交换机 SW1： Inspur_config# hostname SW1

SW1_config#pdp run

SW1_config#

Switch_config#pdp timer 30

Switch_config#pdp holdtime 90

Switch_config#pdp version 1

配置交换机 SW2： Inspur_config# hostname SW2

SW2_config#pdp run

SW2_config#

在 SW1 上验证：Inspur_config#show pdp neighbor

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge

S - Switch, H - Host, I - IGMP, r - Repeater

Device-ID Local-Intf Hldtme Port-ID Platform Capability

Inspur TGi3/8 80 TGi3/8 Inspur S9503-MU-24 R S

Inspur_config#show pdp neighbor detail

Device ID: Inspur

Entry address(es): IP address: 192.168.1.2

Platform: Inspur S9503-MU-24S8X Software, RISC processor, Capabilities: Router Switch

Interface: TGigaEthernet3/8, Port ID(outgoing port): TGigaEthernet3/8

Holdtime : 81 sec

Version :

Inspur(tm) S9503-MU-24S8X Software, Version 4.1.3A

Serial: 0020077602685, System Address: BC606BB61EF0

Compiled: 2024-10-15 16:56:24 by SYS

7 IP 业务

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。

- **IP** 基础配置
- **ARP**
- 静态路由
- 路由映射
- **OSPFv2**
- **OSPFv3**
- **BGP/BGP4+**
- **RIP**
- **VRF**

7.1 IP 基础配置

7.1.1 简介

Internet 协议(IP)是一个以报文形式在计算机网络中交换数据的协议。IP 具有寻址、分片、重组和协议复用功能。它是所有其它 IP 协议（统称为 IP 协议族）的基础。作为网络层协议，IP 包括用于路由的寻址和控制信息。

传输控制协议（TCP）建立在 IP 之上。TCP 是面向连接的协议，所以它规定了数据传输中数据和确认信息的格式。TCP 还规定了计算机用来确认数据正确到达的方法。TCP 允许在同一个系统中的多个应用程序同时进行通信，因为它可以把收到的数据分别送往各个应用程序。

7.1.2 配置准备

为每一个 VLAN 接口、三层以太网接口，或 LOOPBACK 接口配置 IP 地址。

为 VLAN 接口配置 IP 地址前，需要先创建指定 VLAN 并激活。

7.1.3 配置接口 IP 地址

请在设备上进行以下配置。

序号	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。以下以 **VLAN** 接口配置模式为例进行说明。
3	Inspur_config_v1#**ip address** *ip-address mask*	配置接口的主 **IP** 地址，掩码（**mask**）表示 **IP** 地址中的网络部分。 可以使用 **no ip address** 命令删除接口的 **IP** 地址配置。
4	Inspur_config_v1#**ip address** *ip-address mask* **secondary**	配置接口的从 **IP** 地址，掩码（**mask**）表示 **IP** 地址中的网络部分。 可以使用 **no ip address** ***ip-address*** **sub** 命令删除从 IP 地址配置。

配置接口 IPv6 地址

IPv6 协议在默认状态下未启用。如需在某个 **VLAN** 端口中使用 **IPv6** 协议，应在 **VLAN** 端口配置态下使能 **IPv6** 协议。**IPv6** 协议的使能通过配置 **IPv6** 地址实现。如某个 **VLAN** 端口下至少配置有一个 **IPv6** 地址，则该 **VLAN** 端口可以处理 **IPv6** 报文、与 其他 **IPv6** 设备通信。反之如不存在任何 **IPv6** 地址，则协议不会使能。

请在设备上进行以下配置。

序号	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。以下以 **VLAN** 接口配置模式为例进行说明。
3	Inspur_config_v1#**ipv6 enable**	使能 **IPV6**。自动配置一个链路本地地址
4	Inspur_config_v1#**ipv6 address** *fe80::x* **link-local**	手工配置一个链路本地地址
5	Inspur_config_v1#**ipv6 address** *ipv6-address/prefix-length* [**eui-64**]	配置 **VLAN** 接口的 **IPv6** 地址。

7.1.4 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 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。
3	Inspur#show ip interface vLAN *vlan-id*	查看三层接口详细信息。

7.1.5 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，使下图中的主机和设备之间能够相互 Ping 通。

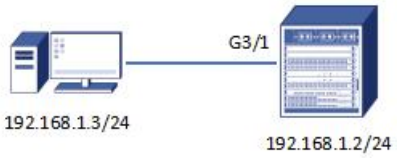


图 7.1.1 配置 VLAN 接口组网示意图

配置步骤

步骤 2 创建 VLAN 10，并将接口 GE 3/1 加入 VLAN 10。

```
Inspur#config
Inspur_config#vlan 10
Inspur_config#interface gigaethernet 3/1
Inspur_config_g3/1#switchport pvid  10
Inspur_config_g3/1#exit
```

步骤 3 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#int vlan 10
Inspur_config_v10#ip address 192.168.1.2 255.255.255.0
```

检查结果

通过 show vlan id 命令查看 VLAN 和物理接口的绑定关系是否正确。

```
Inspur_config#show vlan id  10
VLAN id: 10, Name: VLAN0010
Mode: Static, Total Ports: 1
Interface       Attributes
g3/1            Access
```

通过 **show ip interface brief** 命令查看三层接口配置是否正确。

```
Inspur_config#show ip interface brief
Interface                  IP-Address      Method  Protocol-Status
GigaEthernet3/0            unassigned      manual  down
Null0                      unassigned      manual  up
VLAN10                      192.168.1.2    manual  up   .
```

通过 **ping** 命令查看设备和 PC 之间是否能够互通。

```
Inspur_config#ping 192.168.1.3
PING 192.168.1.1 (192.168.1.1): 56 data bytes
!!!!!
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
```

7.2 ARP

7.2.1 简介

在局域网中，当主机或其它三层网络设备有数据要发送给另一台主机或三层网络设备时，它需要知道对方的网络层地址（即 IP 地址）。但是仅有 IP 地址是不够的，因为 IP 报文必须封装成帧才能通过物理网络发送，因此发送方还需要知道接收方的物理地址（即 MAC 地址），这就需要一个从 IP 地址到 MAC 地址的映射。ARP 即可以实现将 IP 地址解析为 MAC 地址。主机或三层网络设备上会维护一张 ARP 表，用于存储 IP 地址和 MAC 地址的关系。

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。

7.2.2 配置准备

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。

7.2.3 配置 ARP 相关功能

配置静态 ARP 表项

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。

序号	配置	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#arp *ip-address hardware-address* vlan *vlan-id* [alias]	配置静态 ARP 映射，静态 ARP 映射会永久保留在 ARP 缓存中，Alias（可选）交换机回答对这一 IP 地址的 ARP 请求。

配置动态 ARP 表项

请在需要配置的设备上进行以下配置。

序号	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
3	Inspur_config_v*#arp timeout *seconds*	配置该 VLAN 接口 ARP 缓存中动态 ARP 表项的存在时间。
4	Inspur_config_v*#arp dynamic	配置动态学习 ARP 功能。
5	Inspur_config_v*#arp send-gratuitous [interval *value*]	配置接口免费 ARP 学习功能。interval 设置发送免费 ARP 的间隔，缺省 120 秒，范围 1-600 秒

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。

序号	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_v*#**ip proxy-arp**	在接口上进行代理 **ARP**。

7.2.4 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 arp** [*address netmask* | *vlan-id*]	显示所有 **ARP** 表项，包括接口 **IP** 地址的 **ARP** 映射，用户配置的静态 **ARP** 映射，动态 **ARP** 映射。
2	Inspur#**show arp statistic** [**vlan** *vlan-id*]	显示 **ARP** 相关统计表项

7.2.5 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。

序号	命令	描述
1	Inspur#**clear arp-cache** [*ip-address vlan* | *mask*]	清除动态 ARP 缓存。
2	Inspur#**clear arp statistics** [**vlan** *vlan-id*]	清除 ARP 统计信息。

7.2.6 配置 ARP 示例

组网需求

如下图所示，交换机设备连接主机，通过接口 **GE 3/1** 连接上游的 **Router**。**Router** 的 **IP** 地址为 **192.168.1.1/24**，**MAC** 地址为 **bc60:6bb6:1ef0**。

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。

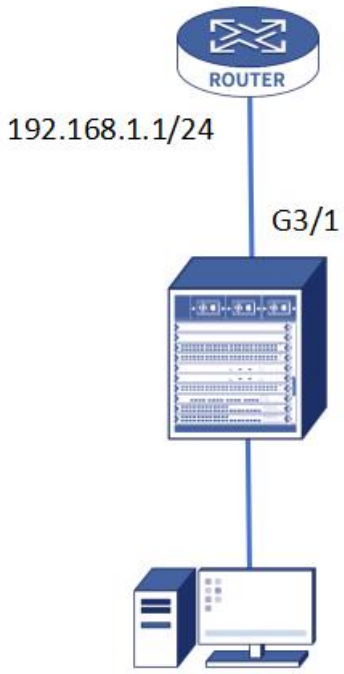


图 7.2.1 图 1-1 配置 ARP 组网示意图

配置步骤

配置增加一条 ARP 静态表项。

```
Inspur#config

Inspur_config#arp 192.168.1.1 bc:60:6b:b6:1e:f0 VLAN  1
```

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。

7.3 静态路由

7.3.1 简介

路由是数据通信网络中最基本的要素。路由信息就是指导报文发送的路径信息，路由的过程就是报文转发的过程。

缺省路由

缺省路由（也叫默认路由）是另外一种特殊的路由。简单来说，缺省路由是没有在路由表中找到匹配的路由表项时才使用的路由。如果报文的目的地址不能与路由表的任何目的地址相匹配，那么该报文将选取缺省路由进行转发。如果没有缺省路由且报文的目的地址不在路由表中，那么该报

文将被丢弃，并向源端返回一个 **ICMP**（**Internet Control Message Protocol**）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。

7.3.2 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。静态路由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。

7.3.3 配置静态路由

请在设备上进行以下配置。

序号	配置	说明
1	`Inspur#config`	进入全局配置模式。
2	`Inspur_config#ip route default { next-hop | interface } [ distance ] [ tag tag ] [ global ] [ description ]`	配置 **IPv4** 缺省路由。 **Distance**：管理距离（1-255 默认为 1） **tag tag**：设定一个 **tag**，用于 **match** 时进行匹配，并对路由进行控制 **Global**：下一跳地址依赖于全局路由表中的路由 **Description**：对本静态路由条目的描述
3	`Inspur_config#ip route ip-address ip-mask { next-hop | interface } [ distance ] [ tag tag ] [ global ] [ description ]`	配置 IPv4 静态路由。 **Distance**：管理距离（1-255 默认为 1） **tag tag**：设定一个 **tag**，用于 **match** 时进行匹配，并对路由进行控制 **Global**：下一跳地址依赖于全局路由表中的路由 **Description**：对本静态路由条目的描述

4	Inspur_config#**ip route bfd { static { next-hop | { [vrf** *name* **] *ip-address* } } | query** *interval* **| reply** *interval* **}**	配置 IPv4 静态路由。 **Static**：启动静态路由的双向链路查询功能 **next-hop**：启用基于网关查询的静态路由双向链路检测功能 **ip-address**：查询网关地址 **Query**：配置查询时间间隔 **Reply**：从发送查询报文到收到回应报文的最大时间间隔 **Interval**：配置的时间间隔 **Vrf**：在 **VRF** 下启用静态 **BFD**
5	Inspur_config#**ip route load-balance**	配置权重路由均衡。
6	Inspur_config_v1#**ip route-weight** *value*	配置出端口基于数据流的路由权重。 **Value**：指定权重值。参数范围 **1-4294967295**

7.3.4 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 ip route [** *ip-address* **| all | detail | protocol | bfd | summary | vrf** *vrf_name* **| information]**	查看 **IPV4** 路由表的内容。 **ip-address**：显示特定的路由。显示所有能够到达地址（或者网络） **All**：现实所有路由条目，包括非激活的路由条目 **Detail**：显示路由的详细信息 **Summary**：显示所有激活路由的汇总信息 **Protocol**：路由协议名或关键词：**connected**、**static**、**bgp**、**ospf**、**beigrp** 或 **rip** 等 **Bfd**：静态路由下一跳双向侦测 **vrf**：显示 VPN 路由 **Information**：显示路由全局统计信息

2	Inspur#**show ip fib** { **route** [**no-adv**] | **summary** | **vrf** *vrf-name* | **nexthop** }	查看快速转发表中的路由。 **Fib**：快速转发表 **Route**：显示快速转发表中的路由 **no-adv**：显示尚未同步到线卡的路由 **summary**：显示 FIB 表的统计信息 **vrf**：显示指定 **vrf** 的 **FIB** 表中的路由

7.3.5 配置静态路由示例

组网需求

配置静态路由，使下图中的任意两台主机或交换机设备之间能够相互 Ping 通。

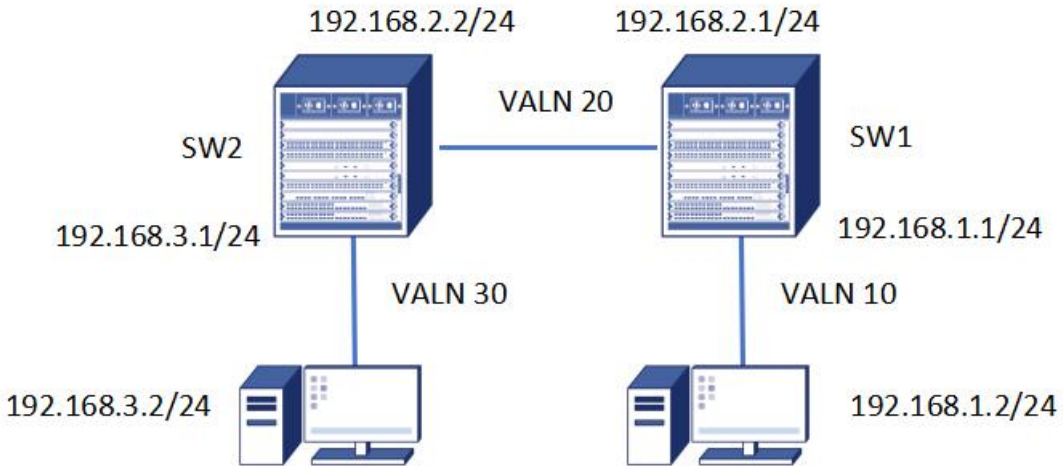


图 7.3.1 配置静态路由组网示意图

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 **SW1** 上配置静态路由。

```
Inspur#hostname SW1

SW1#config

SW1_config#ip route 192.168.3.0 255.255.255.0 192.168.2.2
```

步骤 3　在 SW2 上配置静态路由。

```
Inspur#hostname SW2
```

```
SW2#config

SW2_config#ip route 192.168.1.0 255.255.255.0 192.168.2.1
```

检查结果

通过 **show ip route** 命令查看两台设备路由表信息。

通过 **ping** 命令检测所有设备之间是否均能两两互通。

7.4 路由映射

7.4.1 简介

路由映射（route-map）用来修改路由的属性、过滤路由。常用于动态路由协议的策略，如 redistribute 路由、过滤路由、设置路由属性进行策略路由等。

route-map 以名字标识，同一个 route-map 下可以有多个条目。系统中 route-map 的总数仅受系统的资源限制。同一 route-map 下的各条目都可以指定序号或系统自动生成序号。 每一条目都有一性质（deny/permit），每一条目下可以配置匹配规则（用 match 命令）、设置规则（用 set 命令）、退出策略（用 on-match 命令）。

为了实现路由策略，首先需要定义一系列的匹配规则，即要实施路由策略的路由信息的特征，然后再将它们应用于路由的发布、接收和引入等过程中。可以将路由信息中的不同属性作为匹配依据进行设置，如目的地址、发布路由信息的路由设备地址等。

匹配规则分类

匹配规则用来检查目标的某一属性是否满足一定规则。如果目标满足本条目下所有匹配 规则，则认为该目标匹配本条目成功，否则匹配本条目失败。如果一个条目下未配置匹配规则，则任何目标都匹配本条目。如果匹配规则是用其他列表（如 access-list、prefix-list、 community-list、aspath-list 等）来检查目标是否匹配的，那么应用该列表的返回值就是该匹配规则的结果。

设置规则用来设置目标的某一属性。如果目标匹配本条目成功，且本条目的性质为 permit，则用本条目下配置的设置规则来修改目标的属性；如果目标匹配本条目成功，且本条目的性质为 deny，则检查退出策略；如果目标匹配本条目失败，则进行下一条目的检查。

7.4.2 配置准备

场景

路由策略可以实现对路由信息的发布、接收和引入进行控制，并对通过路由策略的路由属性进行修改。

为了实现路由策略，首先定义将要实施路由策略的路由特征，即定义一组匹配规则和设置规则，然后将它们应用于 **RIP**、**OSPF** 等路由的发布、接收和引入过程的路由策略中。

7.4.3 配置路由映射

配置 IPv4 前缀列表

前缀列表（**prefix-list**）是用来过滤网络前缀的一组规则的集合。每一条规则含有五个元素：序号（**sequence**）、性质（**deny/permit**）、前缀和长度（**a.b.c.d/n**）、下限（**ge x**）、上限（**ley**）。所有规则按序号从小到大排列。应用前缀列表时，从序号最小的规则开始检查，如果匹配成功，则停止其他规则的匹配，返回该规则的性质（**deny/permit**）。

序号	配置	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#ip prefix-list *name* [seq *seq_number*] [deny | permit] [*ip-address/mask* | any] [ge *value*] [le *value*]	创建一个 prefix-list（前缀列表）或增加一条 prefix-list 规则。
3	Inspur_config#ip prefix-list *name* description *strings*	配置 prefix list 的描述。

配置 IPv6 前缀列表

请在设备上进行以下配置。

序号	配置	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#ipV6 prefix-list *name* [seq *seq_number*] [deny | permit] [*ip-address/mask* | any] [ge *value*] [le *value*]	创建一个 prefix-list（前缀列表）或增加一条 prefix-list 规则。
3	Inspur_config#ipv6 prefix-list *name* description *strings*	配置 IPv6 前缀列表的描述信息。

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。

配置路由映射表

请在设备上进行以下配置。

序号	配置	说明
1	Inspur#config	进入全局配置模式。

2	Inspur_config#**route-map** *name* [**seq**] [**deny** | **permit**]	创建一个路由映射（**route-map**）或定义一条路由映射条目。
3	Inspur_config_route_map#**match as-path** *as-path-list-name*	设置一条 **route-map** 匹配规则，通过 **as-pathlist** 来检查 **BGP** 路由属性。 用指定的 **AS** 路径列表来匹配目标。只适用于 **BGP** 路由。用来过滤 **BGP** 路由的 **AS_PATH** 属性。
4	Inspur_config_route_map#**match community** *community-list-name*	设置一条 **route-map** 匹配规则，通过 **community list** 来检查 **BGP** 路由属性。
5	Inspur_config_route_map#**match ip address** *name*	设置一条 **route-map** 匹配规则，通过 **ip access list** 来匹配路由目的网络地址。
6	Inspur_config_route_map#**match ip next-hop** *ip-address*	设置一条 **route-map** 匹配规则，检查路由的 **nexthop** 地址是否与指定的 **nexthop** 地址匹配。
7	Inspur_config_route_map#**match ip address prefix-list** *name*	设置一条 **route-map** 匹配规则，通过 **ip prefix list** 来匹配路由目的网络地址。
8	Inspur_config_route_map#**match tag** *value*	设置一条 **route-map** 匹配规则，检查路由的 **tag** 是否与指定的 **tag** 匹配。
9	Inspur_config_route_map#**match metric** *value*	设置一条 **route-map** 匹配规则，检查路由的 **metric** 是否与指定的 **metric** 匹配。
10	Inspur_config_route_map#**match length** *minimum-length maximum-length*	设置一条 **route-map** 匹配规则，匹配报文长度。
11	Inspur_config_route_map#**match ipv6 address** *name*	设置一条 **route-map** 匹配规则，通过 **ipv6 access list** 来匹配路由目的网络地址。
12	Inspur_config_route_map#**match ipv6 address prefix-list** *name*	设置一条 **route-map** 匹配规则，通过 **ipv6 prefix list** 来匹配路由目的网络地址。
13	Inspur_config_route_map#**match ipv6 next-hop** *ip-address*	设置一条 **route-map** 匹配规则，检查路由的 **nexthop** 地址是否与指定的 **nexthop** 地址匹配。
14	Inspur_config_route_map#**set aggregator as** *as-number*	配置一条 **route-map** 设置规则，设置 **BGP** 路由的 **aggregator** 属性。

15	Inspur_config_route_map#**set as-path prepend** *as*	配置一条 **route-map** 设置规则，在 **BGP** 路由的 **as-path** 属性前添加 **AS**。
16	Inspur_config_route_map#**set interface** interface-name	为策略路由设置出端口,用来给策略路由设置缺省的出端口。
17	Inspur_config_route_map#**set ip default next-hop** *ip-address* **[load-balance]**	为策略路由设置缺省的 **nexthop**,只有当该 **nexthop** 可到达时才认为有效，可以被设置为路由
18	Inspur_config_route_map#**set ip precedence** *0-7*	为策略路由设置 **precedence**,**IP** 报文的 **Precedence** 定义 **routine:0** **Priority:1 immediate:2 flash:3** **flash-override:4 critical:5** **Internet:6 network:7**
19	Inspur_config_route_map#**set ip next-hop** *ip-address* **[load-balance]**	配置一条 **route-map** 设置规则，用于设置路由的 **next-hop** 地址。

配置策略路由 PBR

策略路由可以应用于本地发出的报文或转发的报文。对于本地发出的报文应用策略路由我们称之为本地策略路由。

用于策略路由的 **Route-map** 可以根据通过 **Access-list** 或报文长度来匹配报文，通过设置 **nexthop** 或出端口来进行策略路由。通过使用 **Access-list**，可以满足各种策略需要，如根 据源地址路由、根据应用路由等。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**ip local policy route-map** *name*	配置打开本地报文的策略路由功能。
3	Inspur_config_v1#**ip policy route-map** *name*	配置打开端口上的策略路由功能。通过在报文入端口上配置，就可以实现从该端口收到的报文的策略路由。

7.4.4 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 ip prefix-list [summary | detail** *prefix-name* **]**	查看 **IP** 前缀列表信息。
2	Inspur#**show ipv6 prefix-list [summary | detail** *prefix-name* **]**	查看 **IPv6** 前缀列表信息。

3	Inspur#**show route-map** [*map-name*]	查看路由映射表配置信息。
4	Inspur#**show ip local policy**	查看本地策略路由的配置状态。
5	Inspur#**show ip policy**	查看显示端口策略路由的配置状态。

7.4.5 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。

序号	命令	描述
1	Inspur#**clear ip prefix-list** [*prefix-name* [*ip-address/mask*]]	清除指定 **prefix-list** 的统计信。
2	Inspur#**clear ipv6 prefix-list** [*prefix-name* [*ipv6-address/mask*]]	清空 **IPv6** 前缀列表的统计信息。

7.5 OSPFv2

7.5.1 简介

OSPF（Open Shortest Path First，开放最短路径优先）是 IETF 的 OSPF 工作组的开发的 IGP 路由协议，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。下面列出了实现中的一些关键特征：

路由转发：即被任何一种路由协议学习生成的路由都可以被转发到其他路由协议 域。在自治域内，这表示 OSPF 能输入 RIP 学习到的路由。OSPF 学习到的路由也可以输出到 RIP。在自治域间，OSPF 能输入 BGP 学习到的路由； OSPF 路由也能输出到 BGP 中去。

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。

认证：在一个域内的邻接路由交换机之间，支持明文与 MD5 认证。

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 BFD for OSPF。

OSPF 要求在全部域内路由交换机、**ABR** 与 **ASBR** 之间进行交换路由数据。为了简化配置，可以让它们全部工作在默认参数，不需认证等；但如果要修改某些参数，则必须保证在所有路由交换机

上的参数一致。

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：

广播类型（Broadcast）：当链路层协议是 Ethernet 或 FDDI（Fiber Distributed Data Interface）时，缺省情况下，OSPF 认为网络类型是 Broadcast。在该类型的网络中：通常以组播形式发送 Hello 报文、LSU 报文和 LSAck 报文。其中，224.0.0.5 的组播地址为 OSPF 设备的预留 IP 组播地址；224.0.0.6 的组播地址为 OSPF DR/BDR 的预留 IP 组播地址。以单播形式发送 DD 报文和 LSR 报文。

NBMA 类型（Non-Broadcast Multi-Access）：当链路层协议是帧中继或 X.25 时，缺省情况下，OSPF 认为网络类型是 NBMA。在该类型的网络中，以单播形式发送协议报文（Hello 报文、DD 报文、LSR 报文、LSU 报文、LSAck 报文）。

点到多点 P2MP 类型（Point-to-Multipoint）：没有一种链路层协议会被缺省的认为是 P2MP 类型。点到多点必须是由其他的网络类型强制更改的。常用做法是将非全连通的 NBMA 改为点到多点的网络。在该类型的网络中：以组播形式（224.0.0.5）发送 Hello 报文。以单播形式发送其他协议报文（DD 报文、LSR 报文、LSU 报文、LSAck 报文）。

点到点 P2P 类型（Point-to-Point）：当链路层协议是 PPP、HDLC 或 LAPB 时，缺省情况下，OSPF 认为网络类型是 P2P。在该类型的网络中，以组播形式（224.0.0.5）发送协议报文（Hello 报文、DD 报文、LSR 报文、LSU 报文、LSAck 报文）。

路由设备 ID 号

Router ID 是用于在自治系统中唯一标识一台运行 OSPF 的路由器的 32 位整数。每个运行 OSPF 的路由器都有一个 Router ID。Router ID 的格式和 IP 地址的格式是一样的。

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：

如果一个 **loopback** 接口配置了 **IP** 地址，则路由交换机使用 **IP** 地址作为它的路由交换机 **ID**，由于 **loopback** 接口永远不会 Down,所有使得路由表具有较大的稳定性。

若没有配置 IP 地址的 **Loopback** 接口，OSPF 使用配置在接口的最大 **IP** 地址作为它的路由交换机 **ID**。如果与这个 IP 地址相连的接口变为 **DOWN** 状态，或者该 **IP** 地址被删除，**OSPF** 进程将重新计算新的路由交换机 **ID** 并且重新从所有接口发送路由信息。若 **IP** 地址已经被其它 **OSPF** 进程选用，则不能被该进程选用；

DR 和 BDR 选举

在广播网络和 NBMA 网络中，任意两台路由器之间都要传递路由信息。网络中有 n 台路由器，则需要建立 n*(n-1)/2 个邻接关系。这使得任何一台路由器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 定义了 DR。通过选举产生 DR 后，所有其他设备都只将信息发送给 DR，由 DR 将网络链路状态 LSA 广播出去。

为了防止 DR 发生故障，重新选举 DR 时会造成业务中断，除了 DR 之外，还会选举一个备份指定路由器 BDR。这样除 DR 和 BDR 之外的路由器（称为 DR Other）之间将不再建立邻接关系，也不再交换任何路由信息，这样就减少了广播网和 NBMA 网络上各路由器之间邻接关系的数量。

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。

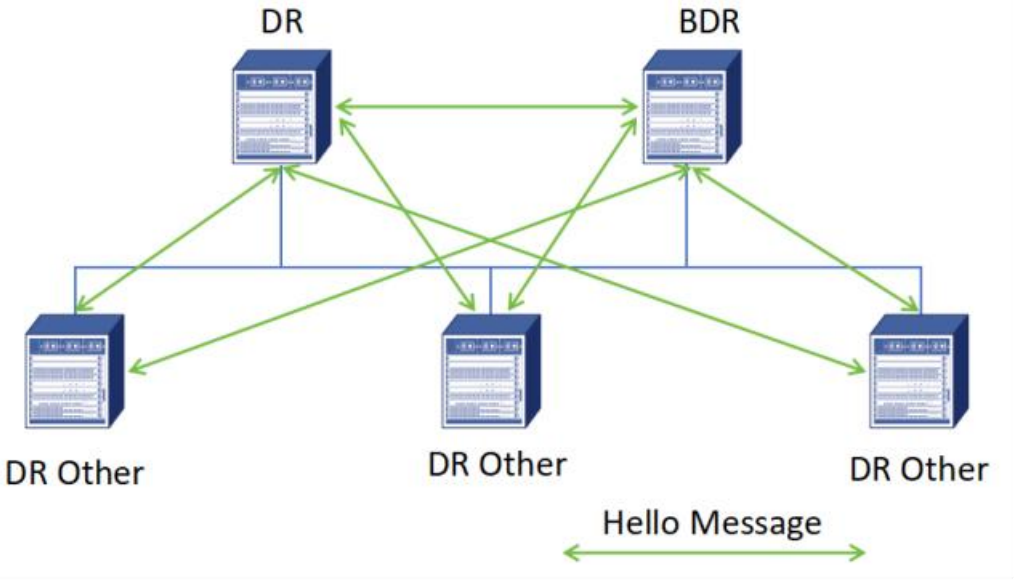


图 7.4.1 广播类型接口角色示意图

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 的报文类型可以分为以下五种：

Hello 报文：周期性发送，用来发现、建立和维持 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 报文（Database Description，数据库描述）报文：用来协商主从关系，在两台路由器交换 DD 报文的过程中，一台为 Master，另一台为 Slave。由 Master 规定起始序列号，每发送一个 DD 报文序列号加 1，Slave 方使用 Master 的序列号作为确认。DD 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 报文（Link State Request，链路状态请求）报文：向对方请求所需的 LSA。两台路由器互相交换过 DD 报文之后，需要发送 LSR 报文（Link State Request packet）向对方请求更新 LSA。LSR 报文里包括所需要的 LSA 的摘要信息。

LSU 报文（Link State Update，链路状态更新）报文：用来向对端路由器发送其所需要的 LSA

或者泛洪本端更新的 LSA，其报文内容是多条完整的 LSA 的集合。为了实现泛洪的可靠性传输，需要 LSAck 报文对其进行确认，对没有收到确认报文的 LSA 进行重传，重传的 LSA 是直接发送到邻居的。

LSAck 报文（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，用于描述设备的链路状态和开销，在路由器所属的区域内传播。

Network LSA（Type2）：由 DR 产生，用于描述本网段的链路状态，在所属的区域内传播。

Network Summary LSA（Type3）：由 ABR（Area Border Router，区域边界路由设备）产生，用来描述区域间的路由信息。

ASBR Summary LSA（Type4）：由 ABR 发布，描述到 ASBR 的路由信息，并通告给除 ASBR 所在区域的其他相关区域。

AS External LSA（Type5）：由 ASBR 产生，描述到 AS 外部的路由，通告到除 Stub 区域和 NSSA 区域以外所有的区域。

邻居和邻接

OSPF 路由设备启动后，开启了 OSPF 功能的接口会周期性地发送 Hello 报文，与网络中其他收到 Hello 报文的路由器协商报文中的指定参数，包括区域号、验证模式、发送 Hello 报文的时间间隔、路由器失效时间等参数。如果协商一致，则在返回的 Hello 报文的邻居列表中添加发送该 Hello 报文的设备的 Router ID，双方建立双向通信，邻居关系建立。邻居关系建立后，如果在路由器失效时间内没有收到邻居发来的 Hello 报文，则中断邻居关系。。

OSPF 邻接关系位于邻居关系之上，两端需要进一步交换 DD 报文、交互 LSA 信息时才建立邻接关系。

并非所有邻居都会建立邻接关系，是否建立邻接关系主要取决网络类型和 DR/BDR。在 P2P 链路和 P2MP 链路上，每一台设备都需要交换 LSA 信息，因此只存在邻接关系。在广播链路和 NBMA 链路上，因为 DR Other 之间不需要交换 LSA 信息，所以建立的是邻居关系。而 DR 与 BDR 之间，DR、BDR 与 DR Other 之间需要交互 LSA 信息，所以建立的是邻接关系

OSPF 的运行过程

OSPF 协议中，路由的计算过程如下：

1.运行 OSPF 协议后，会从所有启动 OSPF 协议的接口上发送 Hello 报文。如果两台路由器共享一条公共数据链路，并且能够成功协商各自 Hello 报文中所指定的某些参数，就能形成邻居关系。。

2.形成邻居关系的设备之间进一步交互 LSA 形成邻接关系。每台设备根据自己周围的网络拓扑结构生成 LSA，LSA 描述了路由器所有的链路、接口、邻居及链路状态等信息 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。

3. 通过 LSA 的泛洪，设备会把收到的 LSA 汇总记录在 LSDB 中。最终，所有路由器都会形成同样的 LSDB。LSA 是对路由器周围网络拓扑结构的描述，而 LSDB 则是对整个自治系统的网络拓扑结构的描述，LSDB 是 LSA 的汇总。

4. 当 LSDB 同步完成之后，每一台设备都将以其自身为根，使用 SPF 算法来计算一个无环路的拓扑图来描述它所知道的到达每一个目的地的最短路径（最小的路径代价）。这个拓扑图就是最短路径树，有了这棵树，路由器就能知道到达自治系统中各个节点的最优路径。

5. 根据 SPF 算法得出最短路径树后，每台设备将计算得出的最短路径加载到 OSPF 路由表形成指导数据转发的路由表项，并且实时更新。同时，邻居之间交互 Hello 报文进行保活，维持邻居关系或邻接关系，并且周期性地重传 LSA。

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，并使得运行 **SPF** 算法的复杂度增加导致 **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 **LSA** 泛洪严重，降低网络带宽利用率，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，将 **LSA** 泛洪限制在一个区域内，提高网络的利用率和路由的收敛速率；每个区域内的路由器数量减少，维护的 **LSDB** 规模降低，**SPF** 计算也仅限于区域内的 **LSA**；每台路由器需要维护的路由表也越来越小。 此外，多区域提高了网络的扩展性，有利于组建大规模的网络。

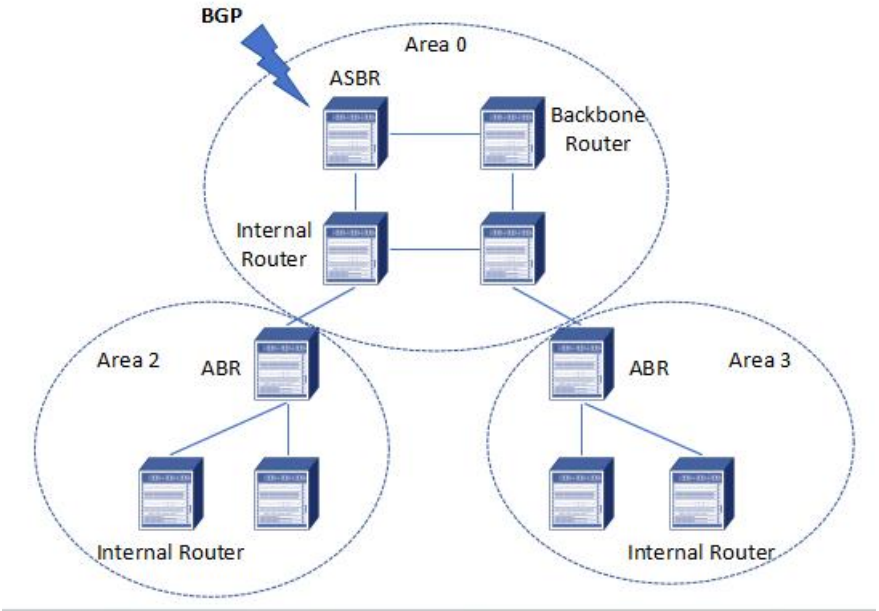


图 1-1OSPF 区域及路由设备类型

区域是从逻辑上将路由器划分为不同的组，每个组用区域号（**Area ID**）来标识。区域的边界是路由器，而不是链路。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。

路由设备的类型

如上图所示，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

骨干区域：连接所有其他 OSPF 区域的中央区域，用 Area 0 表示。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：

骨干区域自身必须保持连通。

所有非骨干区域必须与骨干区域保持连通。

OSPF 虚连接

虚连接（Virtual link）是指在两台 ABR 之间通过一个非骨干区域建立的一条逻辑上的连接通道。

根据 RFC 2328，在部署 OSPF 时，要求所有的非骨干区域与骨干区域相连，否则会出现有的区域不可达的问题。但是在实际应用中，可能会因为各方面条件的限制，无法满足所有非骨干区域与骨干区域保持连通的要求，此时可以通过配置 OSPF 虚连接来解决这个问题。

虚连接相当于在两个 ABR 之间形成了一个点到点的连接，因此，虚连接的两端和物理接口一样可以配置接口的各参数，如发送 Hello 报文间隔等。为虚连接两端提供一条非骨干区域内部路由的区域称为传输区域（Transit Area）。配置虚连接时，必须在两端同时配置方可生效。

Stub 区域

Stub 区域是一些特定的区域，Stub 区域的 ABR 不传播它们接收到的自治系统外部路由，因此这些区域中路由器的路由表规模以及路由信息传递的数量都会大大减少。Stub 区域是一种可选的配置属性，但并不是每个区域都符合配置的条件。一般情况下，Stub 区域位于自治系统的边界，是只有一个 ABR 的非骨干区域，为保证到自治系统外的路由依旧可达，Stub 区域的 ABR 将生成一条缺省路由，并发布给 Stub 区域中的其他非 ABR 路由器。

骨干区域不能配置成 **Stub** 区域。

如果要将一个区域配置成 Stub 区域，则该区域中的所有路由器都要配置 **Stub** 区域属性。

Stub 区域内不能存在 **ASBR**，因此自治系统外部的路由不能在本区域内传播。

虚连接不能穿过 **Stub** 区域。

7.5.2 配置 OSPF

请在设备上进行以下配置。

序号	配置	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#router ospf *process-id* [vrf *WORD*]	启动一个 OSPF 进程，并进入 OSPF 配置模式。
3	Inspur_config_ospf_1#network *address mask* area area-id	配置 OSPF 运行的接口以及接口的区 域 ID。
4	Inspur_config_ospf_1#router-id *address*	配置运行 OSPF 路由交换机 ID。

配置 OSPF 的接口参数

请在设备上进行以下配置。

序号	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_v1#ip ospf cost *cost*	配置接口的路由开销。 缺省情况下，未配置接口路由开销。
4	Inspur_config_v1#ip ospf retransmit-interval *seconds*	配置属于同一个 OSPF 接口的邻居之间重传 LSA 的秒数。
5	Inspur_config_v1#ip ospf transmit-delay *seconds*	配置在一个 OSPF 接口传输 LSA 的估计时间（秒为单位）。
6	Inspur_config_v1#ip ospf priority *number*	配置路由交换机成为 OSPF DR 路由交换机的优先值。
7	Inspur_config_v1#ip ospf hello-interval *seconds*	配置在 OSPF 接口发送 hello 包的时间间隔。
8	Inspur_config_v1#ip ospf dead-interval *seconds*	在这个规定的时间间隔内，未收到邻居的 HELLO 包，则认为邻居路由交换机已关机。
9	Inspur_config_v1#ip ospf password *key*	为一个网段内的邻接路由的认证口令。它使用 OSPF 的简单的口令认证。
10	Inspur_config_v1#ip ospf message-digest-key *keyid* md5 *key*	要求 OSPF 使用 MD5 认证。
11	Inspur_config_v1#ip ospf passive	在端口上不发送 HELLO 报文。

12	Inspur_config_v1#**ip ospf demand-circuit**	指定接口为按需电路。 配置为按需电路后，可以抑制 hello 报文以及周期性的链路状态更新报文，当网络拓扑稳 定后，可以关闭底层的链路。
13	Inspur_config_v1#**ip ospf transmit-delay**	设置在接口上传送链路状态广播的时延值。

配置带宽参考值

请在设备上进行以下配置。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**router ospf** *process-id* [**vrf** *WORD*]	启动一个 OSPF 进程，并进入 OSPF 配置模式。
3	Inspur_config_ospf_1#**auto-cost reference-bandwidth** *value*	配置计算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 100**Mbps**。 ***Value***：取值范围为 1～ 4294967，单位为 **Mbps**。

如果没有配置链路的开销值，**OSPF** 将根据链路带宽来计算开销（开销＝带宽参考值÷带宽，当计算出来的开销值大于 65535 时，开销取最大值 65535）。 如果配置了链路的开销值，**OSPF** 不再根据链路带宽来计算开销，而是使用配置的链路开销值。

配置 OSPF 管理距离

请在设备上进行以下配置。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**router ospf** *process-id* [**vrf** *WORD*]	启动一个 **OSPF** 进程，并进入 **OSPF** 配置模式。

3	Inspur_config_ospf_1#**distance** *value* [*network mask*] [*access-list-name*]	基于路由的通告路由器的 **router-id** 和目的网段设置 **ospf** 路由的管理距离。 **Value**：管理距离，取值范围为 1~255。 **Network**：通告路由器的 router-id 所在的网段。 **Mask**：通告路由器的 router-id 所在的网段的掩码 **access-list-name**：访问列表名
4	Inspur_config_ospf_1#**distance ospf** { [**intra-area** dist1] [**inter-area** dist2] [**external** dist3] }	基于类型定义 ospf 路由的管理距离。 缺省： **intra-area**: 110 **inter-area**: 110 **external**: 150

配置 OSPF 网络类型

请在设备上进行以下配置。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**router ospf** *process-id* [**vrf** *WORD*]	启动一个 **OSPF** 进程，并进入 **OSPF** 配置模式。
3	Inspur_config_ospf_1#**ip ospf network** { **broadcast** | **non-broadcast** | **point-to-multipoint** | **point-to-point** }	配置 **OSPF** 的网络类型 **Broadcast**:设定为广播类型 **non-broadcast**:设定为非广播类型 **point-to-multipoint**:设定为点到多点方式 **point-to-point**:设定为点到点方式

配置 OSPF 域参数

请在设备上进行以下配置。

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

2	Inspur_config#**router ospf** *process-id* [**vrf** *WORD*]	启动一个 **OSPF** 进程，并进入 **OSPF** 配置模式。
3	Inspur_config_ospf_1#**area** *area-id* **authentication simple**	激活 **OSPF** 区域认证。
4	Inspur_config_ospf_1#**area** *area-id* **authentication message-digest**	使 **OSPF** 使用 **MD5** 进行认证。
5	Inspur_config_ospf_1#**area** *area-id* **stub [no-summary]**	定义一个 **stub** 区域 **no-summary**:不向末梢区域发送 **Summary LSA**
6	Inspur_config_ospf_1#**area** *area-id* **default-cost** *cost*	为 **Stub** 区域的默认路由设定权值。

配置 OSPF 路由汇总

请在需要的设备上进行以下配置。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**router ospf** *process-id* [**vrf** *WORD*]	启动一个 **OSPF** 进程，并进入 **OSPF** 配置模式。
3	Inspur_config_ospf_1#**area** *area-id* **range** *address mask*	配置 **OSPF** 域内路由的汇总，设定汇总路由的地址范围。
4	Inspur_config_ospf_1#**summary-address** *prefix mask* [**not advertise**]	描述覆盖分发路由的地址与掩码，仅仅一条汇总路由被广播。 **not advertise**：不发布
5	Inspur_config_ospf_1#**default-information originate** [**always** | **metric-type** [**1** | **2**] | **metric** *cost* | **route-map** *map-name*]	强制 **ASBR** 生成默认路由进入 **OSPF** 路由域。
6	Inspur_config_ospf_1#**default-metric** *value*	设定引入路由的缺省路由权重。 **Value**：所要设定的路由权值。 取值范围：1~16777214。
7	Inspur_config_ospf_1#**maximum-paths** *value*	设等价路由的下一跳的最大数量取值范围 1-8.

配置路由计算的计时器

请在需要的设备上进行以下配置。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**router ospf** *process-id* [**vrf** *WORD*]	启动一个 **OSPF** 进程，并进入 **OSPF** 配置模式。
4	Inspur_config_ospf_1#**timers delay-timer** *delaytime*	设定在一个域中路由计算的时间延迟。 **Delaytime**：时延时间，范围 0-65535 秒
5	Inspur_config_ospf_1#**timers hold-timer** *holdtime*	设定在一个域中路由计算的最小时间间隔。 **Holdtime**：时延时间，范围 0-65535 秒

配置 OSPF 平滑重启功能

请在设备上进行以下配置。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**router ospf** *process-id* [**vrf** *WORD*]	进入 VLAN 接口配置模式或者三层物理接口配置模式。以下步骤以三层 VLAN 配置模式为例。
3	Inspur_config_ospf_1#**graceful-restart** { **interval** *period* | **ietf** [**helper** { **disable** | **strict-lsa-checking** }] }	设置 **OSPF** 平滑重启功能及相关参数。 **Ietf**：使能 **IETF** 标准的平滑重启能力（基于 **rfc**3623），默认关闭。 **interval period**：(任选项)配置平滑重启的时间上限，取值范围 40~1800s，默认取值 120s **helper disable**：(任选项)关闭 **GRhelper** 能力，缺省情况下，设备可以作任一 **OSPF** 邻居的 **GRHelper** **helper strict-lsa-checking**：(任选项) 开启 **strict-lsa-checking** 能力，当 **GR Helper** 检测到有 **LSA** 发生变化时，退出 **HelpMode**，默认关闭。

配置 OSPF NSSA 区域

请在需要的设备上进行以下配置。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**router ospf** *process-id* [**vrf** *WORD*]	启动一个 **OSPF** 进程，并进入 **OSPF** 配置模式。
3	Inspur_config_ospf_1#**area** *area-id* **nssa** [**default-information-originate** [**metric** *value* | **metric-type** { *1* | *2* }] | **no-redistribute** | **no-summary** | **translate-always**]	配置一个区域为 **NSSA** 区域。 **area-id**：配置 **NSSA** 的区域 **id**。可以是十进制，也可以是一个 **ip** 地址 **default-information-Originate**：对于 **ABR**，配置该命令后，若没有配置 **no-summary** 命令，不论本地是否存在缺省路由，都会生成一条 **Type-7LSA** 向区域内发布缺省路由，但是若配置了 **no-summary**，会生成一条 **Type-3 LSA** 向区域内发布缺省路由；对于 **ASBR**，配置后，只有当主路由表存在缺省路由时，才产生 **Type-7 LSA** 向区域内发布缺省路由。 **Metric**：默认路由的 **metric**。 **metric-type**：默认路由的 **metric** 类型。 **no-redistribute**：用于禁止将 **AS** 外部路由以 **Type-7 LSA** 的形式引入到 **NSSA** 区域中，通常只用在既是 **NSSA** 区域的 **ABR**，也是 OSPF 自治系统的 **ASBR** 的 路由器上。 **no-summary**：只用于 **NSSA** 区域的 **ABR**，禁止 **ABR** 路由器发送 **Type-3 LSA** 到 **NSSA** 区域，配置后，**NSSA ABR** 只通过生成一条 **Type-3 LSA** 向区域内发布一条缺省路由，不再向区域内发布任何其它 **Type-3 LSA**（这种区域又称为 **NSSA Totally Stub** 区域）。 **translate-always**：只用于 **NSSA** 区域的 **ABR**，设置该 **ABR** 总是担任将 **Type-7 LSA** 翻译成 **Type-5 LSA** 的角色。

4	Inspur_config_ospf_1#**area** *area-id* **nssa-range** *address mask* [**advertise** | **not-advertise** | **tag** *value* | *cost*]	翻译 **Type-7 LSA** 时进行路由聚合。 **area-id**：配置 **NSSA** 的区域 **id**。可以是十进制，也可以是一个 **ip** 地址 **.** **Address**：聚合路由的目的 IP 地址。 **Mask**：聚合路由的网路掩码。 **advertise**：聚合后发布。 **not-advertise**：聚合后不发布。 **Tag**：聚合路由的标识。 **value**：路由标识值，取值范围为 0～4294967295，缺省值为 0 **Cost**：聚合路由的开销，取值范围为 0～16777215
5	Inspur_config_ospf_1#**area** *area-id* **nssa-translate-interval** *interval*	配置一个时间间隔，该值表示当一个被选举的 **Type-7LSA** 的翻译者，由于某些原因，其翻译角色被别人代替后，其继续履行翻译功能的时间。

配置 OSPF 虚连接

在需要的设备上进行以下配置。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**router ospf** *process-id* [**vrf** *WORD*]	启动一个 **OSPF** 进程，并进入 **OSPF** 配置模式。

3	Inspur_config_ospf_1#**area** area-id **virtual-link** neighbor-ID [**authentication** simple | message-digest] [**dead-interval** dead-value][**hello-interval** hello-value][**retransmit-interval** retrans-value][**transdly** dly-value][**password** [0 | 1] pass-string] [message-digest-key key-id **MD5** [0 | 1] md5-string]	配置一条 **virtual link**。 **area-id**：指定 **virtual link** 的 **transit-area**。 **neighbor-id**：**virtual-link** 对端路由器的 **ospf router-id**。 **Simple**：配置 **virtual-link** 使用明文认证，在 **virtual-link** 的两端所配置的类型必须一致。 **message-digest**：配置 **virtual-link** 使用 **md5** 认证，在 **virtual-link** 的两端所配置的类型必须一致。 **dead-value**：本路由器认为邻居死亡的时间间隔，单位：秒．在 **virtual link** 的两端所配置的值必须一致。 **hello-value**：路由器在 **virutal-link** 上发送 **Hello** 报文的时间间隔，单位:秒．在 **virtual link** 的 两端所配置的值必须一致。 **retrans-value**：路由器在 **virtual-link** 上重传报文的时间间隔．单位:秒.在 **virtual-link** 的两端所配置的值必须一致。 **dly-value**：路由器在 **virtual-link** 上通告 **LSA** 时的 **delay** 值．单位：秒.在 **virtual-link** 的两端 所配置的值必须一致。 **pass-string**：如果 **virutual-link** 使用明文认证，那么配置口令.最大 8 个字符．在 **virtual-link** 的两端所配置的值必须一致。
4	Inspur_config_ospf_1#**area** area-id **virtual-link** neighbor-ID [**authentication** simple | message-digest] [**dead-interval** dead-value][**hello-interval** hello-value][**retransmit-interval** retrans-value][**transdly** dly-value][**password** [0 | 1] pass-string] [message-digest-key key-id **MD5** [0 | 1] md5-string]	**key-id**：如果 **virtual-link** 使用 **MD5** 认证，所使用的 **MD5 key**。 有效范围:1-255．在 **virtual-link** 的两端所配置的值必须一致。 **MD5-String**：设置 **MD5** 口令，最大 16 个字符．在 **virtual-link** 的两端所配置的值必须一致。 **0 | 1** ：0 表示后面配置的字符串是密钥的明文形式；1 表示后面配置的字符串是密钥的加密形式。

7.5.3 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 ospf [*process-id*]	查看 OSPF 路由进程的基本信息。
2	Inspur#show ip ospf [*process-id*] database	查看 OSPF 数据库信息。
3	Inspur#show ip ospf border-routers	显示 ABR 与 ASBR 的内部路由表项。
4	Inspur#show ip ospf interface	显示有关 OSPF 接口的信息。

7.5.4 OSPF 配置举例

网络环境需求

有三台交换机 SW1、SW2 和 SW3，其中 SW1 和 SW2 分别连接网络 1.1.1.1/32 和 3.3.3.3/32（LoopBack 0 模拟），现需要使用 OSPF 实现这两个网络的互通

网络拓扑图

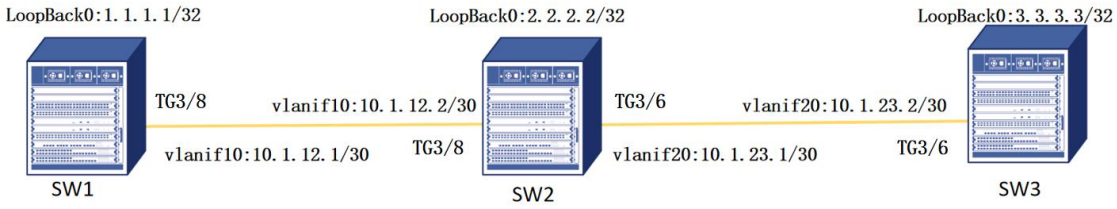


图 7-1 网络拓扑图

配置步骤

基本配置

配置交换机 SW1：Inspur_config#hostname SW1

SW1_config#interface loopback 0

SW1_config_l0#ip address 1.1.1.1 255.255.255.255

SW1_config_l0#exit

SW1_config#interface vLAN 10

SW1_config_v10#ip address 10.1.12.1 255.255.255.252

SW1_config_v10#exit

SW1_config#router ospf 1

SW1_config_ospf_1#router-id 1.1.1.1

SW1_config_ospf_1#network 1.1.1.1 255.255.255.255 area 0

SW1_config_ospf_1#network 10.1.12.1 255.255.255.252 area 0

SW1_config#interface tgigaEthernet 3/8

SW1_config_tg3/8#switchport mode trunk

配置交换机 SW2：Inspur_config#hostname SW2

SW2_config#interface loopback 0

SW2_config_l0#ip address 2.2.2.2 255.255.255.255

SW2_config_l0#exit

SW2_config#interface vLAN 10

SW2_config_v10#ip address 10.1.12.2 255.255.255.252

SW2_config_v10#exit

SW2_config#interface vLAN 20

SW2_config_v20#ip address 10.1.23.1 255.255.255.252

SW2_config_v20#exit

SW2_config#router ospf 1

SW2_config_ospf_1#router-id 2.2.2.2

SW2_config_ospf_1#network 2.2.2.2 255.255.255.255 area 0

SW2_config_ospf_1#network 10.1.12.2 255.255.255.252 area 0

SW2_config_ospf_1#network 10.1.23.1 255.255.255.252 area 1

SW2_config_ospf_1#exit

SW2_config#interface tgigaEthernet 3/8

SW2_config_tg3/8#switchport mode trunk

SW2_config_tg3/8#exit

SW2_config#interface tgigaEthernet 3/6

SW2_config_tg3/6#switchport mode trunk

配置交换机 SW3：Inspur_config#hostname SW3

SW3_config#interface loopback 0

SW3_config_l0#ip address 3.3.3.3 255.255.255.255

SW3_config_l0#exit

SW3_config#interface vLAN 20

```
SW3_config_v20#ip address 10.1.23.2 255.255.255.252
SW3_config_v20#exit
SW3_config#router ospf 1
SW3_config_ospf_1#router-id 3.3.3.3
SW3_config_ospf_1#network 3.3.3.3 255.255.255.255 area 1
SW3_config_ospf_1#network 10.1.23.2 255.255.255.252 area 1
SW3_config_ospf_1#exit
SW3_config#interface tgigaEthernet 3/6
SW3_config_tg3/8#switchport mode trunk
```

在 SW2 上查看 OSPF 邻居表：

```
SW2_config#show ip ospf neighbor
```

```
--------------------------------------------------------------------------------

                                OSPF process: 1


                                    AREA: 0
Neighbor ID     Pri   State           DeadTime   Neighbor Addr   Interface
1.1.1.1         1     FULL/DR         40         10.1.12.1       VLAN10

                                    AREA: 1
Neighbor ID     Pri   State           DeadTime   Neighbor Addr   Interface
3.3.3.3         1     FULL/BDR        33         10.1.23.2       VLAN20
--------------------------------------------------------------------------------
```

在 SW1 上查看 OSPF 路由表：

```
SW1_config#show ip route
max_rtlimit:16384       static_nh_limit:8
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
```

```
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2, IA - ISIS inter-level
       I - IPSEC type
VRF ID: 0

C       1.1.1.1/32          is directly connected, Loopback0
O       2.2.2.2/32          [110,2] via 10.1.12.2(on VLAN10)
O IA    3.3.3.3/32          [110,12] via 10.1.12.2(on VLAN10)
C       10.1.12.0/30        is directly connected, VLAN10
O IA    10.1.23.0/30        [110,2] via 10.1.12.2(on VLAN10)
```

7.6 OSPFv3

7.6.1 简介

OSPF（Open Shortest Path First）是 IETF 组织开发的一个基于链路状态的内部网关协议（Interior Gateway Protocol）。目前针对 IPv4 协议使用的是 OSPF Version 2，针对 IPv6 协议使用 OSPF Version 3。

OSPFv3 在 OSPFv2 基础上进行了修改，是一个独立的路由协议。

OSPFv3 在 Hello 报文、状态机、LSDB、洪泛机制和路由计算等方面的工作原理和 OSPFv2 保持一致。

OSPFv3 协议把自治系统划分成逻辑意义上的一个或多个区域，通过 LSA（Link State Advertisement）的形式发布路由。

OSPFv3 依靠在 OSPFv3 区域内各设备间交互 OSPFv3 报文来达到路由信息的统一。

OSPFv3 报文封装在 IPv6 报文内，可以采用单播和组播的形式发送。

OSPFv3 报文类型

Hello 报文：周期性发送，用来发现和维持 OSPFv3 邻居关系

DD 报文（Database Description packet）：描述了本地 LSDB 的摘要信息，用于两台设备进行数据库同步。

LSR 报文（Link State Request packet）：用于向对方请求所需的 LSA。设备只有在 OSPFv3 邻居双方成功交换 DD 报文后才会向对方发出 LSR 报文。

LSU 报文（Link State Update packet）：向对方发送其所需要的 LSA。

LSAck 报文（Link State Acknowledgment packet）：用来对收到的 LSA 进行确认。

LSA 类型

Router-LSA（Type1）：设备会为每个运行 OSPFv3 接口所在的区域产生一个 LSA，描述了设备的链路状态和开销，在所属的区域内传播。

Network-LSA（Type2）：由 DR 产生，描述本链路的链路状态，在所属的区域内传播。

Inter-Area-Prefix-LSA（Type3）：由 ABR 产生，描述区域内某个网段的路由，并通告给其他相关区域。

Inter-Area-Router-LSA（Type4）：由 ABR 产生，描述到 ASBR 的路由，通告给除 ASBR 所在区域的其他相关区域。

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 区域和 NSSA 区域）。

NSSA LSA（Type7）：由 ASBR 产生，描述到 AS 外部的路由，仅在 NSSA 区域内传播。

Link-LSA（Type8）：每个设备都会为每个链路产生一个 Link-LSA，描述到此 Link 上的 link-local 地址、IPv6 前缀地址，并提供将会在 Network-LSA 中设置的链路选项，它仅在此链路内传播。

Intra-Area-Prefix-LSA（Type9）：每个设备及 DR 都会产生一个或多个此类 LSA，在所属的区域内传播。设备产生的此类 LSA，描述与 Router-LSA 相关联的 IPv6 前缀地址。DR 产生的此类 LSA，描述与 Network-LSA 相关联的 IPv6 前缀地址。

OSPFv3 路由类型

AS 区域内和区域间路由描述的是 AS 内部的网络结构，AS 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。OSPFv3 将引入的 AS 外部路由分为 Type1 和 Type2 两类。

Intra Area Routes：区域内路由。从区域内生成的且目的地属于该区域的路由。

Inter Area Routes：区域间路由。来自其他区域的路由。

External Routes：外部路由。引入其他路由协议或不同 OSPF 进程的路由。根据路由开销的计算方式，外部路由可以分为以下两类：第一类外部路由（Type1 External）：第一类外部路由的开销=本设备到相应的 ASBR 的开销+ASBR 到该路由目的地址的开销。第二类外部路由（Type2 External）：第二类外部路由的开销=ASBR 到该路由目的地址的开销。对于同一目的地址，第一类的外部路由的优先级要大于第二类外部路由。

OSPFv3 路由聚合

通过路由聚合，可以减少路由信息，从而减小路由表的规模，提高设备的性能。

OSPFv3 路由聚合过程如下：区域间路由聚合;区域间路由聚合在 ABR 上完成，主要用于聚合 AS 内区域之间的路由。ABR 向其它区域发送路由信息时，以网段为单位生成 Type3 LSA。如果该区域中存在一些连续的网段，则可以通过命令将这些连续的网段聚合成一个网段。这样 ABR 只发送一条聚合后的 LSA，所有属于命令指定的聚合网段范围的 LSA 将不会再被单独发送出去。

外部路由聚合:外部路由聚合在 ASBR 上完成，主要用于聚合 OSPF 引入的外部路由。ASBR 将对引入的聚合地址范围内的 Type5 LSA 进行聚合。当配置了 NSSA 区域时，还要对引入的聚合地址范围内的 Type7 LSA 进行聚合。

如果本地设备既是 ASBR 又是 ABR，则对由 Type7 LSA 转化成的 Type5 LSA 进行聚合处理。

7.6.2 配置 OSPFv3

请在设备上进行以下配置。

序号	配置	说明
1	Inspur#config	进入全局配置模式。

序号	配置	说明
2	Inspur_config#**router ospfv3** *process-id*	启动一个 **OSPFv3** 进程，并进入 **OSPFv3** 配置模式。
3	Inspur_config_ospfv3_1#**router-id** *address*	配置运行 **OSPF** 路 v3 交换机 **ID**。
4	Inspur_config#**int vlan** vlan-id	进入 **VLAN** 接口配置模式。
5	Inspur_config_v1#**ipv6 ospf** process-id **area** area-id	这个命令在接口上使能 **OSPFv3** 协议。

在启动 OSPFv3 之前，需要先使能 IPv6 报文转发 **ipv6 unicast-routing** 功能。

配置 OSPF 的接口参数

请在设备上进行以下配置。

序号	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_v1#**ipv6 ospf cost** *cost*	配置 **OSPFv3** 接口发送包的开销值。
4	Inspur_config_v1#**ipv6 ospf retransmit-interval** *secondsds*	配置邻居之间重传 **LSA** 的时间值.
5	Inspur_config_v1#**ipv6 ospf transmit-delay** *seconds*	配置在一个 **OSPFv3** 接口传输 **LSA** 的延迟时间。
6	Inspur_config_v1#**ipv6 ospf priority** *number*	配置路由交换机成为 **OSPF DR** 路由交换机的优先值。
7	Inspur_config_v1#**ipv6 ospf hello-interval** *seconds*	配置在 **OSPFv3** 接口发送 **hello** 包的时间间隔。
8	Inspur_config_v1#**ipv6 ospf dead-interval** *seconds*	在这个规定的时间间隔内，未收到邻居的任何 **OSPFv3** 报文，则认为邻居交换机已关机。
9	Inspur_config_v1#**ipv6 ospf database-filter all out**	指定接口过滤需要发出的 **LSA**。
10	Inspur_config_v1#**ipv6 ospf mtu-ignore**	配置接口在发送的 **DD** 报文中，将 **MTU** 域的值设置为 0， 同时忽略 **MTU** 检查，不检查接收到的 **DD** 报文的 **MTU** 域。

序号	配置	说明
11	Inspur_config_v1#**ipv6 ospf neighbor** *router-id ipv6-address* [**cost** *number*] [**database-filter all out**] [**poll-interval** *seconds*] [**priority** *number*] [**instance** *instance-id*]	配置非广播网络接口上的 **OSPF** 邻居。 **router-id**：邻居的 **router-id** **ipv6-address**：邻居的链路本地地址 **cost number**：邻居的花费，取值范围是 1~65535 **database-filter all out**：过滤发送出去的 **LSA** **poll-interval seconds**：邻居的查询时间间隔 **priority number**：邻居的优先级，取值范围是 0~255 **instance instance-id**：指定接口所属的 **ospf** 实例号，缺省值为 0
12	Inspur_config_v1#**ipv6 ospf network** { **broadcast** | **non-broadcast** | **point_to_multipoint** | **point-to-point** } [**instance** *instance-id*]	设置接口的网络类型。 **Broadcast**：设置接口的网络类型为广播类型 **Nonbroadcast**：设置接口的网络类型为非广播 **NBMA** 类型 **point-to-multipoint**：设置接口的网络类型为点到多点 **point-to-point**：设置接口的网络类型为点到点 **instance instance-id**：指定接口所属的 **ospf** 实例号，缺省值为 0

配置 OSPFv3 域参数

请在设备上进行以下配置。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**router ospfv3** *process-id* [**vrf** *WORD*]	启动一个 **OSPF** 进程，并进入 **OSPF** 配置模式。

序号	配置	说明
3	Inspur_config_ospfv3_1#**area** *area-id* **nssa** [**default-information-originate** [**metric** *value*] [**metric-type** { 1 | 2 }]] [**interval** *value*] [**no-redistribute**] [**no-summary**] [**range** { *ipv6-prefix/prefix-length* } [**advertise** | **not-advertise**]] [**translator** { **always** | **candidate** }]	配置一个区为 **NSSA** 区域 **area-id:** 设置 **nssa** 区域的 **ID**。可以是十进制，也可以是一个 **IP** 地址 **default-informat ion-originate:** 向 **NSSA** 区域发送默认路由。配置该命令后，如果是 **NSSA** 区域的非 **ABR**，需要本机器上有一条 **IPv6** 默认路由，才会向 **NSSA** 区域发送默认路由；在 **ABR** 上，无论本机器上是否有一条 **IPv6** 默认路由，都会向 **NSSA** 区域发送默认路由 **metric value:** 默认路由的花费，取值范围 1~16777214 **metric-type:**{ 1 | 2 } 默认路由的花费类型 **interval value:NSSA** 翻译者角色的稳定时间，取值范围 1~65535 **no-redistribute:** 不向 **NSSA** 区域重发布路由 **no-summary:** 禁止 **ABR** 交换机发送汇总链路到 **NSSA** 域 **range** 类型 7 的 **LSA** 翻译成类型 5 的 **LSA** 时进行汇总 **Translator:NSSA** 翻译者角色，**always** 表示始终为翻译者，**candidate** 表示可以被选为翻译者
4	Inspur_config_ospfv3_1#**area** *area-id* **default-cost** *cost*	指定发送到 **NSSA** 或者 **STUB** 区域的缺省汇总路由的代价,缺省值为 1
5	Inspur_config_ospfv3_1#**area** *area-id* **stub [no-summary]**	配置一个区为 **stub** 区域 **no-summary:** 禁止 **ABR** 交换机发送汇总链路到 **stub** 域

配置 OSPFv3 虚连接

对于没有和骨干区域直接相连的非骨干区域，或者不连续的骨干区域，可以使用 OSPFv3 的虚链路建立逻辑上的连通性。为了建立一条虚链路， 必须在这个虚链路的两端都进行 配置，如果只在一端配置，这个虚链路将无法工作。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**router ospfv3** *process-id* [**vrf** *WORD*]	启动一个 **OSPF** 进程，并进入 **OSPF** 配置模式。

序号	配置	说明
3	Inspur_config_ospfv3_1#**area** *area-id* **virtual-link** *neighbor-ID* [**dead-interval** *dead-value*][**hello-interval** *hello-value*][**retransmit-interval** *retrans-value*][**transmit-delay** *dly-value*]	配置一条 **virtual link**。 **area-id**：指定 **virtual link** 的 **transit-area**。 **neighbor-id**：**virtual-link** 对端路由器的 **ospf router-id**。 **dead-value**：本路由器认为邻居死亡的时间间隔，单位：秒。在 **virtual link** 的两端所配置的值必须一致；默认 40s。 **hello-value**：路由器在 **virutal-link** 上发送 Hello 报文的时间间隔，单位:秒。在 **virtual link** 的两端所配置的值必须一致；默认 10s。 **retrans-value**：路由器在 **virtual-link** 上重传报文的时间间隔。单位：秒。在 **virtual-link** 的两端所配置的值必须一致；默认 5s。 **dly-value**：路由器在 **virtual-link** 上通告 **LSA** 时的 **delay** 值。单位：秒。在 virtual-link 的两端所配置的值必须一致；默认 1s。
4	Inspur_config_ospfv3_1#**no area** *area-id* **virtual-link** *neighbor-ID*	删除指定的 **virtual link**。

7.6.3 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 ipv6 ospf** [*process-id*]	查看 **OSPFv3** 路由进程的基本信息。
2	Inspur#**show ipv6 ospf** [*process-id*] **database**	查看 **OSPFv3** 数据库信息。
3	Inspur#**show ipv6 ospf interface**	显示有关 OSPFv3 接口的信息。
4	Inspur#**show ipv6 ospf virtual-links**	显示 OSPFv3 的虚链路信息。
5	Inspur#**show ipv6 ospf route**	显示 OSPFv3 的路由信息。

7.6.4 OSPFv3 配置举例

有三台交换机 SW1、SW2 和 SW3，其中 SW1 和 SW2 分别连接网络 1111::1/128 和 3333::3/128（LoopBack 0 模拟），现需要使用 OSPF 实现这两个网络的互通

网络拓扑图

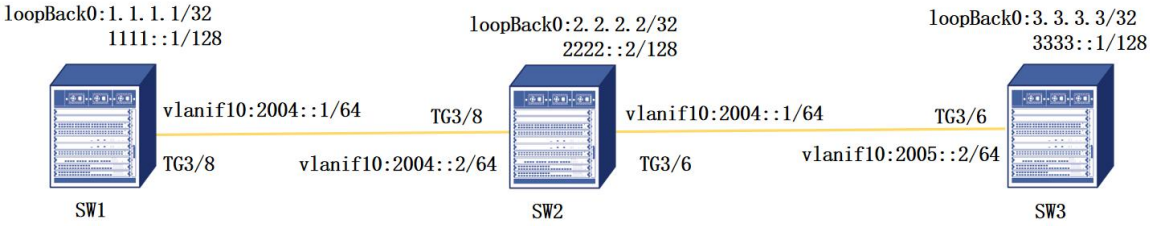


图 7-1 网络拓扑图

配置步骤

基本配置

配置交换机 SW1：Inspur_config#hostname SW1

SW1_config#ipv6 unicast-routing

SW1_config#interface loopback 0

SW1_config_l0#ip address 1.1.1.1 255.255.255.255

SW1_config_l0#ipv6 enable

SW1_config_l0#ipv6 address 1111::1/64

SW1_config_l0#ipv6 ospf 1 area 0

SW1_config_l0#exit

SW1_config#interface vLAN 10

SW1_config_v10#ipv6 enable

SW1_config_v10#ipv6 address 2004::1/64

SW1_config_v10# ipv6 ospf 1 area 0

SW1_config_v10#exit

SW1_config#router ospfv3 1

SW1_config_ospfv3_1#router-id 1.1.1.1

SW1_config_ospfv3_1#exit

SW1_config#interface tgigaEthernet 3/8

SW1_config_tg3/8#switchport mode trunk

配置交换机 SW2：Inspur_config#hostname SW2

SW2_config#ipv6 unicast-routing

SW2_config#interface loopback 0

```
SW2_config_l0#ip address 2.2.2.2 255.255.255.255
SW2_config_l0#ipv6 enable
SW2_config_l0#ipv6 address 2222::1/128
SW2_config_l0#ipv6 ospf 1 area 0
SW2_config_l0#exit
SW2_config#interface vLAN 10
SW2_config_v10#ipv6 enable
SW2_config_v10#ipv6 address 2004::2/64
SW2_config_v10# ipv6 ospf 1 area 0
SW2_config_v10#exit
SW2_config#interface vLAN 20
SW2_config_v10#ipv6 enable
SW2_config_v10#ipv6 address 2005::1/64
SW2_config_v10# ipv6 ospf 1 area 1
SW2_config_v10#exit
SW2_config#router ospfv3 1
SW2_config_ospfv3_1#router-id 2.2.2.2
SW2_config_ospfv3_1#exit
SW2_config#interface tgigaEthernet 3/8
SW2_config_tg3/8#switchport mode trunk
SW2_config_tg3/8#exit
SW2_config#interface tgigaEthernet 3/6
SW2_config_tg3/8#switchport mode trunk
```

配置交换机 SW3：Inspur_config#hostname SW3

```
SW3_config#ipv6 unicast-routing
SW3_config#interface loopback 0
SW3_config_l0#ip address 3.3.3.3 255.255.255.255
SW3_config_l0#ipv6 enable
SW3_config_l0#ipv6 address 3333::3/128
SW3_config_l0#ipv6 ospf 1 area 0
```

```
SW3_config_l0#exit
SW3_config#interface vLAN 20
SW3_config_v20#ipv6 enable
SW3_config_v20#ipv6 address 2005::2/64
SW3_config_v20# ipv6 ospf 1 area 0
SW3_config_v20#exit
SW3_config#router ospfv3 1
SW3_config_ospfv3_1#router-id 3.3.3.3
SW3_config_ospfv3_1#exit
SW3_config#interface tgigaEthernet 3/6
SW3_config_tg3/8#switchport mode trunk
```

在 SW2 上查看 OSPF 邻居表：

```
SW2_config_l0#show ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface        Instance ID
1.1.1.1           1   Full/Backup     00:00:35    VLAN10           0
3.3.3.3           1   Full/Backup     00:00:35    VLAN20           0
```

在 SW1 上查看 OSPF 路由表：

```
SW1_config_l0#show ipv6 route
Codes: C - Connected, L - Local, S - Static, R - Ripng, B - BGP, O - OSPF
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1,              OE2 - OSPF external type 2
       OIA - OSPF inter area,                   DHCP - DHCP type
       L1 - IS-IS level-1, L2 - IS-IS level-2
       <s> - STALE
       [N] - no arp/nd, [E] - add exf [Ns] - hw exf not support
       [T] - to be add later, [F] - add exf fail
VRF ID: 0

C      1111::1/128[1]
```

```
        is directly connected, LC,Loopback0
C       2004::/64[1]
        is directly connected, C,VLAN10
C       2004::1/128[1]
        is directly connected, L,VLAN10
OIA     2005::/64[1]
        [110,2] via fe80::be60:6bff:feb6:2b71(on VLAN10)
O       2222::2/128[1]
        [110,1] via fe80::be60:6bff:feb6:2b71(on VLAN10)
OIA     3333::3/128[1]
        [110,12] via fe80::be60:6bff:feb6:2b71(on VLAN10)
C       fe80::/10[1]
        is directly connected, L,Null0
C       fe80::/64[1]
        is directly connected, C,VLAN10
C       fe80::be60:6bff:feb6:1ef0/128[1]
        is directly connected, L,VLAN10
C       fe80::/64[1]
        is directly connected, C,Loopback0
C       fe80::be60:6bff:feb6:1ef0/128[1]
        is directly connected, L,Loopback0
```

7.7 BGP/BGP4+

7.7.1 BGP 简介

BGP 概述

边界网关协议 BGP（Border Gateway Protocol）是一种实现自治系统 AS（Autonomous System）之间的路由可达，并选择最佳路由的距离矢量路由协议。

在 BGP 中，每条路由都包含一个网络号、该路由传递所通过的自治系统列表(称作自治系统路径 as-path)、以及其他属性列表。BGP 的基本功能是同其它 BGP 系统交换网络可达性信息，包括有关 AS 路径表的信息。该信息能够用于构造能消除路由环路的 AS 连通图，并且能用 AS 连通图实施 AS 级的路由策略。

BGP 基本概念

自治系统 AS

AS 是指在一个实体管辖下的拥有相同选路策略的 IP 网络。BGP 网络中的每个 AS 都被分配一个唯一的 AS 号，用于区分不同的 AS。

BGP 分类

BGP 按照运行方式分为 EBGP（External/Exterior BGP）和 IBGP（Internal/Interior BGP）。 EBGP：运行于不同 AS 之间的 BGP 称为 EBGP。为了防止 AS 间产生环路，当 BGP 设备接收 EBGP 对 等体发送的路由时，会将带有本地 AS 号的路由丢弃。

IBGP：运行于同一 AS 内部的 BGP 称为 IBGP。为了防止 AS 内产生环路，BGP 设备不将从 IBGP 对等体学到的路由通告给其他 IBGP 对等体，并与所有 IBGP 对等体建立全连接。

BGP 报文交互中的角色

BGP 报文交互中分为 Speaker 和 Peer 两种角色。

Speaker：发送 BGP 报文的设备称为 BGP 发言者（Speaker），它接收或产生新的报文信息，并发布（Advertise）给其它 BGP Speaker。

Peer：相互交换报文的 Speaker 之间互称对等体（Peer）。若干相关的对等体可以构成对等体组（Peer Group）。

BGP 的路由器号（Router ID）

BGP 的 Router ID 是一个用于标识 BGP 设备的 32 位值，通常是 IPv4 地址的形式，在 BGP 会话建立时发送的 Open 报文中携带。对等体之间建立 BGP 会话时，每个 BGP 设备都必须有唯一的 Router ID，否则对等体之间不能建立 BGP 连接。

BGP 工作原理

BGP 对等体的建立、更新和删除等交互过程主要有 5 种报文、6 种状态机和 5 个原则。

BGP 的报文

BGP 对等体间通过以下 5 种报文进行交互，其中 Keepalive 报文为周期性发送，其余报文为触发式发送：

Open 报文：用于建立 BGP 对等体连接。

Update 报文：用于在对等体之间交换路由信息。

Notification 报文：用于中断 BGP 连接。

Keepalive 报文：用于保持 BGP 连接。

Route-refresh 报文：用于在改变路由策略后请求对等体重新发送路由信息。只有支持路由刷新能力的 BGP 设备会发送和响应此报文。

BGP 状态机

BGP 对等体的交互过程中存在 6 种状态机：空闲（Idle）、连接（Connect）、活跃（Active）、Open 报文已发送（OpenSent）、Open 报文已确认（OpenConfirm）和连接已建立（Established）。在 BGP 对等体建立的过程中，通常可见的 3 个状态是：Idle、Active 和 Established。

BGP 对等体的交互过程

BGP 设备将最优路由加入 BGP 路由表，形成 BGP 路由。BGP 设备与对等体建立邻居关系后，采取以下交互原则：

从 IBGP 对等体获得的 BGP 路由，BGP 设备只发布给它的 EBGP 对等体。

从 EBGP 对等体获得的 BGP 路由，BGP 设备发布给它所有 EBGP 和 IBGP 对等体。

当存在多条到达同一目的地址的有效路由时，BGP 设备只将最优路由发布给对等体。

路由更新时，BGP 设备只发送更新的 BGP 路由。

所有对等体发送的路由，BGP 设备都会接收。

7.7.2 BGP 配置准备

BGP（边界网关协议）是一种用于在不同自治系统（AS）之间交换路由信息的协议，广泛应用于以下场景：

ISP 运营商互联，BGP 帮助 ISP 确定最优路径，提高传输效率；企业之间通过 BGP 互联，提升网络可靠性；数据中心互联，多个数据中心之间需要高效路由，确保低延迟和高可用性。

7.7.3 BGP 配置

激活 BGP 路由选择

对于外部网关路由协议而言，用 network 路由器配置命令配置一个 IP 网络，仅能控制哪些网络能得到通告。这恰恰同内部网关协议(IGP)相反，它是用 network 命令决定发送更新到何处。

network 命令用于把 IGP 路由引入到 BGP 路由表中。

在全局配置模式下进行以下配置。

序号	配置	说明
1	Inspur_config#**router bgp** *autonomous_system*	激活 BGP 路由。
2	Inspur_config_bgp#network network_number/mask_len **route-map** route-map_name	将网络标记位本地自治系统并将其列入 BGP 列表中。

配置 BGP 邻居

配置 BGP 邻居是为了建立交换路由信息的对象。BGP 支持两种邻居，内部邻居和外部邻居。内部邻居在同一 AS 内，外部邻居在不同 AS。通常，外部邻居彼此相邻，共享一个子网；而内部邻居可能在统一 AS 的任何地方。BGP4+与 BGP 相同。

请在全局配置模式下进行以下配置

序号	配置	说明
1	Inspur_config#**neighbor** *ip_address* **remote-as** *number*	指定一个 BGP 邻居。

BGP 软重置

清除 BGP 会话会导致高速缓存无效并对网络的运作产生巨大的影响，软重置功能是的不必清除 BGP 会话就允许配置和激活策略。BGP4+与 BGP 相同。

在 BGP 路由模式下进行以下配置。

序号	配置	说明
1	Inspur_config_bgp# **neighbor** *ip_address* **soft-reconfiguration inbound**	配置 **BGP** 软重置。

复位 BGP 连接

一旦定义了两个路由器为 BGP 邻居，它们将会建立一个 BGP 连接，并交换路由选择信息。如果随后改变了 BGP 路由策略，或者其他的配置改变，则必须复位 BGP 连接以使配置变化生效。BGP4+与 BGP 相同。

请在特权模式下配置以下命令

序号	配置	说明
1	Inspur# **clear ip bgp ***	复位所有 **BGP** 连接。
2	Inspur#**clear ip bgp** *address*	重建一个特定的 **BGP** 连接。

配置 BGP 路由权重

BGP 路由权重是赋给 BGP 路由的一个数字一遍能够控制路由选择过程。权重取值范围是 0-65535.本地生成的 BGP 路由默认权重为 32768，从邻居获知的路由权重为 0，管理者可以通过改变路由的权重实施路由策略。BGP4+与 BGP 相同。

在 BGP 路由模式下进行以下配置。

序号	配置	说明
1	Inspur_config_bgp#**neighbor** *ip-address* **weight** *number*	给来自一个邻居的所有路由指定一个权重。

配置 BGP 与 IGP 的同步

如果允许另一个 AS 通过你的 AS 到第三个 AS 传送数据，则你的 AS 内部路由状态同它广播给其他 AS 的路由信息保持一致是十分重要的。因此需要 BGP 与 IGP 同步，默认情况下同步被激活。

某些情况下不需要同步，则可以取消同步功能，取消该特征能使得 BGP 收敛更快，取消同步时，也应该使用 clear ip bgp 清除 BGP 会话。BGP4+与 BGP 相同。

在 BGP 路由模式下进行以下配置。

序号	配置	说明
1	Inspur_config_bgp#**no synchronization**	取消 **BGP** 与 **IGP** 之间的同步。

配置基于端口进行 BGP 路由过滤

配置基于端口过滤 BGP 路由可以使用访问控制列表等方式。BGP4+与 BGP 相同。

在全局配置模式下进行以下配置。

序号	配置	说明
1	Inspur_config#**filter vlan {in|out} {access-list** *access-lis_name*} **{prefix-list** *prefix-list_name*} **{gateway** *access-list_name*}	基于端口过滤 BGP 路由。

配置基于邻居进行 BGP 路由过滤

1）同 ip as-path 全局配置命令和 neighbor filter-list 命令一起使用 Aspath 列表过滤器。BGP4+与 BGP 相同。

在全局模式下进行配置。

序号	配置	说明
1	Inspur_config#**ip as-path access-list** *aspaths-list_name* **{permit|deny}** *as-regular-expression*	定义一个与 **BGP** 有关的访问表。
2	Inspur_config#**router bgp** *autonomous-system*	进入路由器配置模式。
3	Inspur_config_bgp#**neighbor** *ip_address* **filter-list** *aspath-list_name* {**in|out**}	建立一个 **BGP** 过滤器。

同 ip access-list 全局配置命令和 neighbor distribute-list 命令一起使用访问列表。BGP4+与 BGP 相同。

在全局模式下进行配置。

序号	配置	说明
1	Inspur_config#**ip access-list standard** *access-list_name*	定义一个访问列表。
2	Inspur_config#**router bgp** *autonomous-system*	进入路由器配置模式。

序号	配置	说明
3	Inspur_config_bgp#**neighbor** *ip_address* **distribute-list** *access-list_name* {**in**|**out**}	建立一个 **BGP** 过滤器。

同 ip prefix-list 全局配置命令和 neighbor prefix-list 命令一起使用前缀列表。BGP4+与 BGP 相同。

在全局模式下进行配置。

序号	配置	说明
1	Inspur_config#**ip prefix-list** *prefix-list_name* sequence-number **{permit|deny}** *A.B.C.D/n* **ge** *x* **le** *y*	定义一个前缀列表。
2	Inspur_config#**router bgp** *autonomous-system*	进入路由器配置模式。
3	Inspur_config_bgp#**neighbor** *ip_address* **prefix-list** *prefix-list_name* {**in**|**out**}	建立一个 **BGP** 过滤器。

使用路由映像过滤和修改路由更新

可以在每个邻居的基础上使用路由映像过滤路由更新和修改参数属性。路由映像既可以用于入站更新又可以用于出站更新。只有通过路由映像的路由才在发送路由更新或接收路由更新时处理。BGP4+与 BGP 相同。

在 BGP 路由模式下进行以下配置。

序号	配置	说明
1	Inspur_config_bgp#**neighbor** {ip-address} **route-map** *route-map-name* **{in|out}**	把路由映像应用于入站或出站路由。

配置聚合地址

无类型域间路由能够创建聚合路由以使路由表最小化。BGP4+与 BGP 相同。

在 BGP 路由模式下进行以下配置。

序号	配置	说明
1	Inspur_config_bgp#**aggregate-address** network/len	在 **BGP** 路由表中创建聚合地址。
2	Inspur_config_bgp#**aggregate-address** network/len **summary-only**	只广播汇总路由。

调整 BGP 定时器

在全局配置模式下进行以下配置。BGP4+与 BGP 相同。

在 BGP 路由模式下进行以下配置。

序号	配置	说明
1	Inspur_config_bgp#**neighbor** {ip-address|peer group-name} **timers** *keepalive_holdtime*	为指定的对等体或对等组设置 **keepalive** 和 **holdtime** 定时器。
2	Inspur_config_bgp#**no neighbor timers**	恢复缺省值。

关闭对等体

在全局配置模式下进行以下配置。BGP4+与 BGP 相同。

在 BGP 路由模式下进行以下配置。

序号	配置	说明
1	Inspur_config_bgp#**neighbor {ip-address} shutdown**	关闭 **BGP** 邻居。
2	Inspur_config_bgp#**no neighbor {ip-address} shutdown**	激活 **BGP** 邻居。

监视与维护 BGP

清除 BGP 路由表和数据库。BGP4+与 BGP 相同。

在特权配置模式下进行以下配置。

序号	配置	说明
1	Inspur#**clear ip bgp ***	复位所有 **BGP** 连接。
2	Inspur#**clear ip bgp as-number**	复位指定自治系统的 **BGP** 连接。
3	Inspur#**clear ip bgp address**	复位指定邻居的 **BGP** 连接。
4	Inspur#**clear ip bgp** *address* **soft**	清除指定邻居的数据库。
5	Inspur#**clear ip bgp aggregates**	清除路由聚合产生的路由。
6	Inspur#**clear ip bgp networks**	清除 **network** 命令产生的路由
7	Inspur#**clear ip bgp redistribute**	清除转发产生的路由。

显示路由表和统计系统信息。BGP4+与 BGP 相同。

序号	配置	说明
1	Inspur#**show ip bgp**	显示系统中的 **BGP** 路由表。
2	Inspur#**show ip bgp prefix-list**	显示匹配指定前缀列表的路由。
3	Inspur#**show ip bgp community**	显示团体属性的统计信息。

4	Inspur#show ip bgp network	显示指定 BGP 路由。
5	Inspur#show ip bgp neighbor *address*	显示指定邻居的 TCP 和 BGP 连接的详细信息。
6	Inspur#show ip bgp summary	显示所有 BGP 连接的状态。
7	Inspur#show ip bgp paths	显示数据库中所有的 BGP 路径信息。
8	Inspur#show ip bgp *A.B.C.D/n*	显示到指定地址/子网的路由

在特权配置模式下进行以下配置。

跟踪 BGP 信息

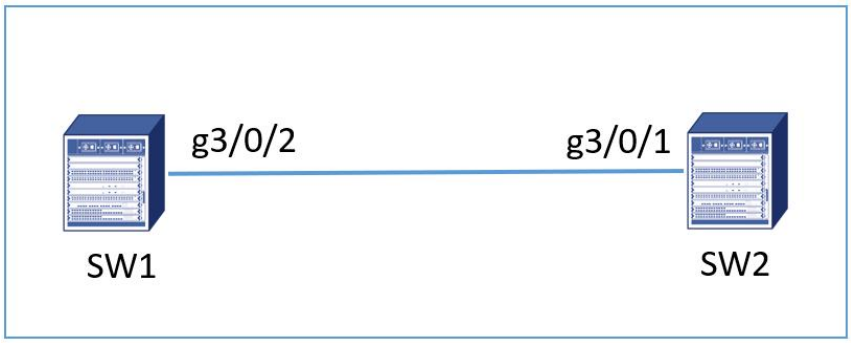
在特权配置模式下进行以下配置。BGP4+与 BGP 相同。

序号	配置	说明
1	Inspur#debug ip bgp	跟踪一般的 BGP 信息。
2	Inspur#debug ip bgp all	跟踪所有的 BGP 信息。
3	Inspur#debug ip bgp fsm	跟踪 BGP 状态机。
4	Inspur#debug ip bgp keepalive	跟踪 BGP 的 keepalive 报文。
5	Inspur#debug ip bgp open	跟踪 BGP 的 open 报文。
6	Inspur#debug ip bgp update	跟踪 BGP 的 update 报文。

7.7.4 配置示例

配置示例

建立一个 SW1 和 SW2 的 ibgp 邻居，as 号为 100，并宣告直连路由；



SW1：

Inspur>ena

Inspur#conf

Inspur_config#int v2

Inspur_config_v2#ip add 192.168.10.1 255.255.255.0

Inspur_config_v2#exit

Inspur_config#router bgp 100

Inspur_config_bgp#neighbor 192.168.10.2 remote-as 100

Inspur_config_bgp#network 192.168.10.0

SW2：

Inspur>ena

Inspur#conf

Inspur_config#int v2

Inspur_config_v2#ip add 192.168.10.2 255.255.255.0

Inspur_config_v2#exit

Inspur_config#router bgp 100

Inspur_config_bgp#neighbor 192.168.10.1 remote-as 100

Inspur_config_bgp#network 192.168.10.0

检查配置

Inspur_config#show ip bgp neighbors

BGP neighbor is 192.168.10.2, remote AS 100, local AS 100, internal link

BGP version 4, remote router ID 10.1.1.1

BGP state = Established, up for 00:00:29

Last read 00:01:44, hold time is 90, keepalive interval is 30 seconds

Wait EOR:none

Sync time 00:00:28

Neighbor capabilities:

Four-octet AS: advertised and received

Route refresh: advertised and received (old and new)

Address family IPv4 Unicast: advertised and received

Received 1 messages, 0 notifications, 0 in queue

Sent 2 messages, 0 notifications, 0 in queue

Route refresh request: received 0, sent 0

Minimum time between advertisement runs is 1 seconds

For address family: IPv4 Unicast

0 accepted prefixes

Connections established 1; dropped 0

Last reset never

Local host: 192.168.10.1, Local port: 179

Foreign host: 192.168.10.2, Foreign port: 23638

Nexthop: 192.168.10.1

Nexthop global: ::ffff:192.168.10.1

Nexthop local: ::

BGP connection: non shared network

Connections fd: 73, so_gencnt: 129

Read thread: on Write thread: off

7.8 RIP

7.8.1 简介

路由信息协议 RIP 是一个相对过时但仍然普遍使用的内部网关协议（IGP），主要应用于规模较小的同质型网络。RIP 是一个经典的距离向量路由协议，出现在 RFC 1058 中。

RIP 通过用户数据报协议 UDP 数据分组的广播来交换路由信息。在路由器中，每 30 秒钟发送一次路由信息的更新。如果一台路由器在 180 秒内没有接收到来自相邻路由器的更新，便把路由表中来自该路由器的路由标记为“不可用的”。如果接下去的 120 秒内仍然没有接收到更新，便把这些路由从路由表中删除。

RIP 使用跳跃计数（hop count）来作为衡量不同路由的权值。这个跳跃计数是指一个分组从信源到达信宿所经过的路由器的数目。直接相连网络的路由权值为 0，不可到达网络的路由权值为 16。由于 RIP 使用的路由权值范围较小，所以对大规模的网络就显得不大适合。

如果路由器有一条缺省路由，RIP 就宣告通向伪网络 0.0.0.0 的路由。实际上，网络 0.0.0.0 并不存在，它只是用来在 RIP 中实现缺省路由的功能。如果 RIP 学习到了一条缺省路由，或者路由器中设置了默认网关并配置了缺省权值，路由器都将宣告这个缺省的网络。

RIP 向指定网络中的接口发送路由更新。如果一个接口所在的网络没有被指定，该网络不会在任何 RIP 更新中宣告。

7.8.2 配置准备

场景

RIP 主要应用于规模较小的网络中，例如校园网以及结构较简单的地区性网络。

7.8.3 RIP 配置

启动 RIP 实例

要激活 RIP 实例，进入全局配置模式，按以下步骤进行：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**router rip process-id** [*vrf vrf-name*]	建立 **RIP** 实例，进入路由器 **RIP** 实例配置模式。

生成 RIP 实例接口

启动 RIP 实例后，只有接口关联到实例下才能生成 RIP 的直连网段，以及用这些接口和邻居交换路由信息。实例要关联接口，在接口的配置态，按以下步骤进行：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**interface vlAN 1**	进入到端口配置模式。
3	Inspur_config_v1#**ip rip** *process-id* **enable**	将接口关联到 **process-id** 实例中。

重要说明：

1. 为 **RIP** 的激活接口（生成接口的直连路由，接口能够收发 **RIP** 协议报文），需要满足：接口关联到 **RIP** 实例，接口上有合法的 **ip** 地址，接口的状态 **up**。

2. 一个接口中 **enable** 一个 **RIP** 实例的时候，若该接口被指定了 **vrf**，而实例的 **vrf** 和接口上的 **vrf** 不一致，该接口不能够成为 **RIP** 的激活接口，直到修订了接口的 **vrf**。

3. 一个接口关联了一个尚未创建的 **RIP** 实例，将会以接口上的 vrf（若被指定了 **vrf**）和 **enable** 的 **process-id** 创建 RIP 实例。

4. 每个接口只能属于一个 **RIP** 实例。

允许 RIP 路由更新分组的单目广播

RIP 通常是一个广播型协议，如果要使 RIP 路由更新能够到达非广播型网络，你必须对交换机进行配置以允许路由信息的交换。要达到这样的目的，在路由配置模式中使用如下命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**router rip process-id** [*vrf vrf-name*]	建立 **RIP** 实例，进入路由器 **RIP** 实例配置模式。
3	Inspur_config_rip_1#**neighbor** *A.B.C.D*	定义一个邻居路由器，与之交互路由信息。

重要说明：

如果你想控制哪些接口可以用来交换路由信息，可以使用命令 **ip rip passive** 指定在某个（某些）接口上禁止路由更新的发送。如果参考在“配置 **IP** 路由中与协议无关的命令”一章中的

“过滤路由信息”中关于路由过滤的讨论。

对路由权值应用偏移量

偏移量列表是用来对那些由 RIP 学习到的入站和出站路由增加一个偏移量。这就提供了一个本地的机制来增加路由权值。另外，你还可以使用访问列表或接口来限制偏移量列表。要增加路由权值，在路由配置模式中使用如下命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**router rip process-id** [*vrf vrf-name*]	建立 **RIP** 实例，进入路由器 **RIP** 实例配置模式。
3	Inspur_config_rip_1#**offset** {[*interface-type number*]|* } **{in|out}** *access-list-name offset*	对路由权值增加一个偏移量。

调整计时器

路由协议使用几个计时器来判断发送路由更新的频率、多长时间内路由变为无效以及其它参数。你可以调整这些计时器使路由协议的性能更适合网络互联的需要。

也有可能调整路由协议来加速各种 IP 路由算法的收敛时间，做到向冗余路由器的快速备份，以达到在需要快速恢复（quick recovery）的场合中向终端用户保证最小的崩溃时间。要调整计时器，在路由配置模式中使用如下命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**router rip process-id** [*vrf vrf-name*]	建立 **RIP** 实例，进入路由器 **RIP** 实例配置模式。
3	Inspur_config_rip_1#**timers holddown** *value*	经过多长时间（单位：秒）从路由表中删除某一条路由。
4	Inspur_config_rip_1#**timers expire** *value*	经过多长间隔（单位：秒）路由被宣告为无效。
5	Inspur_config_rip_1# **timers update** *value*	发送路由更新的频率（发送更新的间隔，单位：秒）。

指定 RIP 版本号

缺省情况下（没有配置全局和端口上的 version），路由器接收 RIP-1 和 RIP-2 的分组，向外发送分组的时候，若端口有 peer 则依据 RIP 的自适应规则，（一个端口上若只有一个 peer 或者有多个 peer 但 peer 彼此的 version 都一致，则按 peer 的 version 响应；若同一个端口上有多个 peer 但 peer 彼此的 version 不一致，则依据系统的 RIP 缺省情况处理），若没有 peer 则发送缺省的 RIP-2 的分组。通过配置，可以使路由器仅发送和接收 RIP-1 的分组，或者仅发送和接收 RIP-2 的分组。要达到这样的目的，在路由配置模式中使用如下命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**router rip process-id** [*vrf vrf-name*]	建立 **RIP** 实例，进入路由器 **RIP** 实例配置模式。
3	Inspur_config_rip_1#**version** {1 | 2}	配置路由器仅仅发送和接受 RIP-1 或 RIP-2 的分组。

上述的任务控制 RIP 的缺省行为。你也可以配置某一特定接口来改变这个缺省行为。要控制接口发送 RIP-1 分组还是 RIP-2 分组，以及要控制发送 request 的时候的分组，在接口配置模式下使用如下命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**interface vlAN** 1	进入到端口配置模式。
3	Inspur_config_v1#**ip rip send version** 1	配置接口仅仅发送 RIP-1 的分组。
4	Inspur_config_v1#**ip rip send version** 2	配置接口仅仅发送 RIP-2 的分组。
5	Inspur_config_v1#**ip rip send version compatibility**	广播发送 RIP-2 更新报文。
6	Inspur_config_v1#**ip rip v1demand**	在发送 request 的时候发送 RIP-1 的分组。
7	Inspur_config_v1#**ip rip v2demand**	在发送 request 的时候发送 RIP-2 的分组。

同样，要控制接口接收 RIP-1 分组还是 RIP-2 分组，在接口配置模式下使用如下命令：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**interface vlAN** 1	进入到端口配置模式。
3	Inspur_config_v1#**ip rip receive version** 1	配置接口仅仅发送 RIP-1 的分组。
4	Inspur_config_v1#**ip rip receive version** 2	配置接口仅仅发送 RIP-2 的分组。
5	Inspur_config_v1#**ip rip receive version** 1 2	广播发送 RIP-2 更新报文。

激活接口的“聋”“哑”状态

在缺省情况下 RIP 覆盖的接口是可以发送和接收路由更新的，通过配置可以灵活应用 RIP 协议，让 RIP 接口处于只接收不发送或者只发送不接受状态。

要配置接口的聋哑状态，要在接口配置模式下进行：

序号	配置	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#interface vlAN 1	进入到端口配置模式。
3	Inspur_config_v1#ip rip passive	接口不发送 rip 协议分组。
4	Inspur_config_v1#ip rip deaf	接口不接受 rip 协议分组。

激活 RIP 认证

RIP-1 不支持认证。如果你在发送和接收 RIP-2 的分组，你可以在接口上激活 RIP 认证功能。

在 RIP 激活的接口上，我们支持多种认证模式：明文认证、MD5 认证、动态认证（md5 和 sha1）。每个 RIP-2 分组中缺省时使用明文认证。

注意：如果处于安全的目的，不要在 RIP 分组中使用明文验证，这是因为未经加密的认证密钥发送在每个 RIP-2 分组中。如果在不涉及安全问题的情况下（例如：要保证配置错误的主机不能参与路由），可以使用明文验证。

要配置 RIP 明文认证，在接口配置模式下，按如下步骤进行：

序号	配置	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#interface vlAN 1	进入到端口配置模式。
3	Inspur_config_v1#ip rip authentication simple	配置接口使用明文认证。
4	Inspur_config_v1#ip rip password [*string*]	配置明文认证密钥。

要配置 RIP 的 MD5 认证，在接口配置模式下，按如下步骤进行：

序号	配置	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#interface vlAN 1	进入到端口配置模式。
3	Inspur_config_v1#ip rip authentication md5	配置接口使用 MD5 认证。
4	Inspur_config_v1#ip rip md5-key [*key-ID*] md5 [*key*]	配置 MD5 认证密钥和认证 ID。

要配置 RIP 的动态认证，在接口配置模式下，按如下步骤进行：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**interface vlAN** 1	进入到端口配置模式。
3	Inspur_config_v1#**ip rip authentication dynamic**	配置接口使用动态认证（**md5** 和 **sha1**）。
4	Inspur_config_v1#**ip rip dynamic-key** [*key-ID*] **{ md5 | sha1 }** [*key*] xxxx-xx-xx-xx-xx:xx xx:xx	配置动态认证密钥和认证 **ID**。

RIP 认证配置完毕后，建议在接口配置模式下，按如下步骤进行：

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**interface vlAN** 1	进入到端口配置模式。
3	Inspur_config_v1#**ip rip authentication commit**	认证通不过时尽快老化对端 peer 和从对端学到的路由。

禁止路由汇总

RIP-2 在缺省情况下支持自动路由汇总。在穿越有类别网络边界时汇总 RIP-2 路由。RIP-1 自动路由汇总功能总处于激活状态。

如果有一个分离的子网，就要禁止路由汇总来宣告这个子网。如果路由汇总被禁止，在穿越由类别网络边界时，路由器将传送子网和主机的路由信息。在路由配置模式下，使用下面命令来禁止自动汇总。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**router rip process-id** [*vrf vrf-name*]	建立 **RIP** 实例，进入路由器 **RIP** 实例配置模式。
3	Inspur_config_rip_1#**no auto-summary**	禁止自动汇总。

禁止可信源 IP 地址验证和零域验证

缺省情况下，路由器会对收到的 RIP 路由更新的可信源 IP 地址进行验证。如果这个地址非法，将丢弃这个路由更新。

如果你有一台路由器希望接收来自它的更新，但是你并没有在接受端的路由器的接口上关联对应的 rip 实例，那么就可以禁止这个功能。但在正常情况下，推荐你不要使用这个命令。在路由器配置模式下使用如下命令将禁止对入站路由更新的可信源 IP 地址进行验证的缺省功能。

在缺省情况下，路由器会对收到的 version 1 下路由条目的必须为零的字段进行验证。如果相应

的字段不能通过零域的合法性检验，该路由条目将被丢弃。如果配置不进行该项验证，将可能导致本地学习到对端发送过来的错误的路由信息

序号	配置	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#no validate-update-source	禁止对入站 RIP 路由更新的可信源 IP 地址的验证。
3	Inspur_config_rip_1#no check-zero-domain	禁止对入站 RIP 路由更新的必须为零字段的验证。

最大等价路由数

在缺省情况下，RIP 路由信息最多允许生成 4 条等价路由。当从多个邻居学习到某个或某些相同网段的路由信息生成等价路由时，若某个网段的等价路由数大于当前最大等价路由数将不能添加到 RIP database 中。

在路由配置模式下使用如下命令对 RIP 本地路由表中最大等价路由数进行配置：

序号	配置	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#maximum-nexthop number	配置 RIP 路由信息最大等价路由数。
3	Inspur_config_rip_1#no maximum-nexthop	恢复缺省最大等价路由数。

激活或禁止水平分割

正常情况下，与广播型 IP 网络相连并使用距离向量路由协议的路由器采用水平分割机制来减小路由环路的可能性。水平分割阻塞路由信息向接收到该路由信息的接口进行宣告。这样做可以优化多个路由器间的通信（尤其是在环路打破的时候）。但是，对于非广播型网络（例如帧中继），情况并非那么理想。此时，你可能要禁止水平分割。

如果一个接口配置了辅助的 IP 地址并且激活了水平分割，路由更新的信源 IP 地址可能不包括每一个辅助地址。一条路由更新中的信源 IP 地址只包括一个网络号（除非水平分割被禁止）。

要激活或禁止水平分割，在接口配置模式下使用如下命令：

序号	配置	说明
1	Inspur#config	进入全局配置模式。
2	Inspur_config#interface vlAN 1	进入到端口配置模式。
3	Inspur_config_v1#ip rip split-horizon {simple | poisoned}	激活水平分割。
4	Inspur_config_v1#no ip rip split-horizon {simple | poisoned}	禁止水平分割。

在缺省情况下，对于点对点接口，水平分割是激活的；对于点对多点接口，水平分割是禁止的。可选参数 simple 和 poisoned 分别表示简单水平分割和带毒性逆转的水平分割。

请参考本章中“水平分割举例”一节中关于使用水平分割的具体例子。

注意：

在一般情况下，推荐你不要改变缺省状态，除非你能肯定你的应用程序需要状态的改变才能正确地宣告路由。记住：如果水平分割在一个串行接口上被禁止（并且与该接口相连的是一个分组交换网），你必须对该网络上任何相关多目广播组中的路由器禁止水平分割。

监视和维护 RIP

监视和维护 RIP，可以显示网络的统计信息，如：RIP 协议参数配置、使用网络、网络通信实时跟踪等。这些信息能帮助你判断网络资源的利用，解决网络问题。能了解网络节点的可达性。

在管理态输入命令，使用下面的命令，可以显示各种路由统计信息。

序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**show ip rip**	显示所有 **RIP** 实例当前状态。
3	Inspur_config#**Show ip rip** *process-id*	显示具体某个 **RIP** 实例的当前状态
4	Inspur_config#**show ip rip** *process-id* **database**	显示某个 **RIP** 实例的所有路由。
5	Inspur_config# **how ip rip** *process-id* **protocol**	显示某个 **RIP** 实例协议相关信息。
6	Inspur_config# **how ip rip** *process-id* ***summary***	显示某个 **RIP** 实例协议相关信息。
7	Inspur_config#**show ip rip** *process-id* **peer**	显示 **RIP peer** 信息
8	Inspur_config#**Show ip rip** *process-id* **interface**	显示某个 **RIP** 实例全部的接口及接口状态

在管理态输入命令，使用下面的命令，可以跟踪路由协议信息。

序号	配置	说明
1	Inspur#**debug ip rip database**	跟踪 RIP 路由加入路由表、从路由表中删除路由、路由改变等过程信息。
2	Inspur# **debug ip rip packet**	跟踪 RIP 报文的接收和发送
3	Inspur# **Debug ip rip message**	跟着 RIP 事件，如定时器超时

7.8.4 配置示例

网络环境需求

在两台交换机相连三层端口上配置 RIP 协议。

网络拓扑图

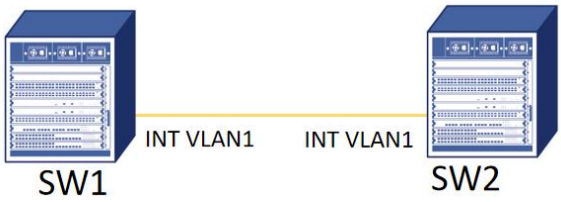


图 7-1 网络拓扑图

配置步骤

基本配置

配置交换机 SW1：Inspur_config#hostname SW1

```
SW1_config#interface vLAN 1
SW1_config_v1#ip address 192.168.1.77 255.255.255.0
SW1_config_v1#ip rip 1 enable
SW1_config_v1# exit
SW1_config#interface loopback 0
SW1_config_l0#ip address 10.1.1.1 255.0.0.0
SW1_config_l0#ip rip 1 enable
SW1_config_l0#exit
SW1_config#router rip 1
```

配置交换机 SW2：Inspur_config#hostname SW2

```
SW2_config#interface vLAN 1
SW2_config_v1#ip address 192.168.1.66 255.255.255.0
SW2_config_v1#ip rip 1 enable
SW2_config_v1# exit
SW2_config#interface loopback 0
SW2_config_l0#ip address 20.1.1.1 255.0.0.0
SW2_config_l0#ip rip 1 enable
```

```
SW2_config_l0#exit
SW2_config#router rip 1
```

在 SW1 上查询 RIP 路由：

```
SW1_config#show ip rip 1 database
 10.0.0.0/8          directly connected  Loopback0
 20.0.0.0/8          [120,1]  via 192.168.1.66 (on VLAN1)  00:00:04
 192.168.1.0/24      directly connected  VLAN1
```

7.9 VRF

7.9.1 简介

VRF 即虚拟路由转发，本质是一种虚拟化技术，也叫 VPN 实例 。它通过在三层转发设备上创建多张路由表，实现多状态路由虚拟化，隔离不同网络流量，提升网络安全性、简化管理以及便于网络测试。在多租户环境、企业网络等场景发挥重要作用，能解决 IP 地址冲突、提升网络性能。

7.9.2 配置准备

场景

大型企业往往有多种不同业务，如生产业务、办公业务、研发业务等，不同业务对网络的安全性、性能等要求不同。通过配置 VRF，能将不同业务的流量隔离在各自的虚拟网络中，防止相互干扰和数据泄露，例如生产业务的敏感数据不会被办公网络的用户误访问，同时可针对不同业务的 VRF 进行独立的 QoS 配置、访问控制等，保障关键业务的网络性能。

7.9.3 VRF 配置

序号	配置	说明
1	Inspur#**config**	进入交换机配置模式。
2	Inspur_config#**ip vrf** *vrf-name*	创建 **VRF**，并进入 VRF 配置模式。 vrf-name：**VRF** 名称，最多 31 个字符。
3	Inspur_config_vrf#rd *route-distinguisher*	制定 **VRF** 的路由区分符。 route-distinguisher：路由区分符，由自治域号与任 意数字组成，或 **IP** 地址与任意数字组成。

序号	配置	说明
4	Inspur_config_vrf#route-target **{ export | import | both }** *route-target-extened-community*	创建 **VRF** 的输入和输出目标 **VPN** 扩展属性。 route-target-extended-community：由自治域号与 任意数字组成，或 **IP** 地址与任意数字组成。
5	Inspur_config_v1#**ip vrf forwarding** *vrf-name*	将三层接口与 **VRF** 关联。 vrf-name：**VRF** 名称。
6	Inspur_config_v1#**ip address** *ip-address subnet-mask*	配置接口 IP 地址。
7	Inspur_config_v1#**exit**	退出端口配置模式。
8	Inspur_config#**ip exf**	启动 **IP** 硬件路由功能。
9	Inspur_config_vrf#**import map** *WORD*	配置加入 **VRF** 路由表中的路由的 **route-map** 过滤。
10	Inspur_config_vrf#**export map** *WORD*	将符合 **route-map** 条件的目标 **VPN** 扩展属性加入到 **VRF** 的输出目标 **VPN** 扩展属性中。
11	Inspur_config_vrf#**description** *LINE*	配置 **VRF** 的描述说明。
12	Inspur_config#**ip route** [**vrf** vrf-name] dest mask { type num | nexthop } *[distance]*	配置 **VRF** 静态路由。

维护与监视

序号	配置	说明
1	Inspur#**show ip vrf**	显示 **VRF** 及所关联的端口信息。
2	Inspur#**show ip vrf** [{**brief** | **detail** | **interface**}] *vrf-name*	显示 **VRF** 配置信息及相关联的端口信息。
3	Inspur#**show ip route vrf** *vrf-name*[A.B.C.D | all | beigrp | bgp | ospf | rip | connect | static | summary]	显示 **VRF** 路由表中路由信息。

7.9.4 VRF 配置示例

在交换机上配置 VRF

```
Inspur#config
Inspur_config#ip vrf vpn1
Inspur_config_vrf_vpn1#rd 100:1
Inspur_config_vrf_vpn1#route-target export 100:1
Inspur_config_vrf_vpn1#route-target import 100:1
Inspur_config_vrf_vpn1#exit
Inspur_config#ip vrf vpn2
Inspur_config_vrf_vpn2#rd 100:2
Inspur_config_vrf_vpn2#route-target export 100:2
Inspur_config_vrf_vpn2#route-target import 100:2
Inspur_config_vrf_vpn2#exit
```

8 堆叠

8.1 堆叠配置指导

8.1.1 简介

BVSS 一般是指 Brilliant Virtual Switch System（灵活虚拟交换系统技术）。BVSS 是软件虚拟化技术，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。虚拟化技术是一种集中管理的端口扩展技术。用户可以把启用虚拟化功能的交换机，利用虚拟化线卡及连接线把它们连接在一起构成虚拟设备。

需要相同型号、相同软件版本的设备才可以组成 BVSS。BVSS 中的成员设备最多为 2 台。

8.1.2 BVSS 的优点

BVSS 主要具有以下优点：

- 带宽充分利用并成倍增加。堆叠可实现跨设备或线卡的链路聚合，不用阻塞端口，使链路带宽倍增，实现负载均衡，并且大大提高网络的可靠性。
- 简化网络拓扑，减少网络故障。不需要配置生成树和 vrrp，所以不存在收敛带来的业务中断。
- 大大缩短故障恢复时间。堆叠组中成员之间的故障切换为毫秒级别（50-200ms），大大的缩短了故障的恢复时间。
- 简化管理。多台设备在逻辑上成为一台设备，管理员可统一进行管理。

8.1.3 BVSS 的应用

如下图所示，Switch A 和 Switch B 组成 BVSS，对上、下层设备来说，它们就是一台设备。

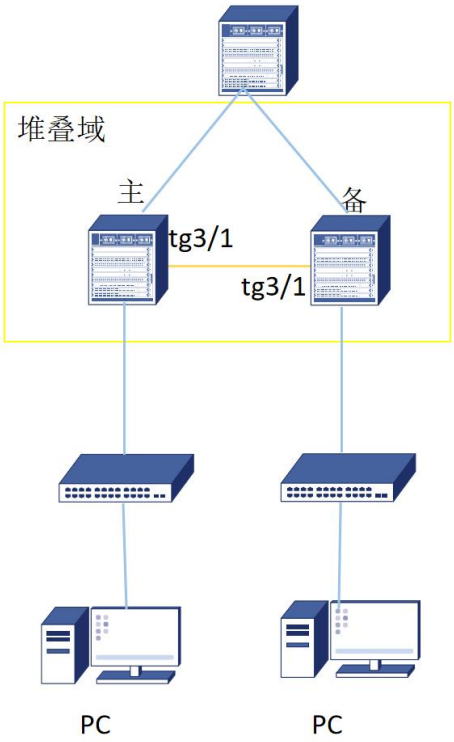


图 8-1Bvss 组网应用示意图

8.1.4 BVSS 基本概念

如下图所示，将 Switch A 和 Switch B 物理连线，进行必要的配置后，就能形成虚拟化的 BVSS。BVSS 统一管理 Switch A 和 Switch B 的物理资源和软件资源。

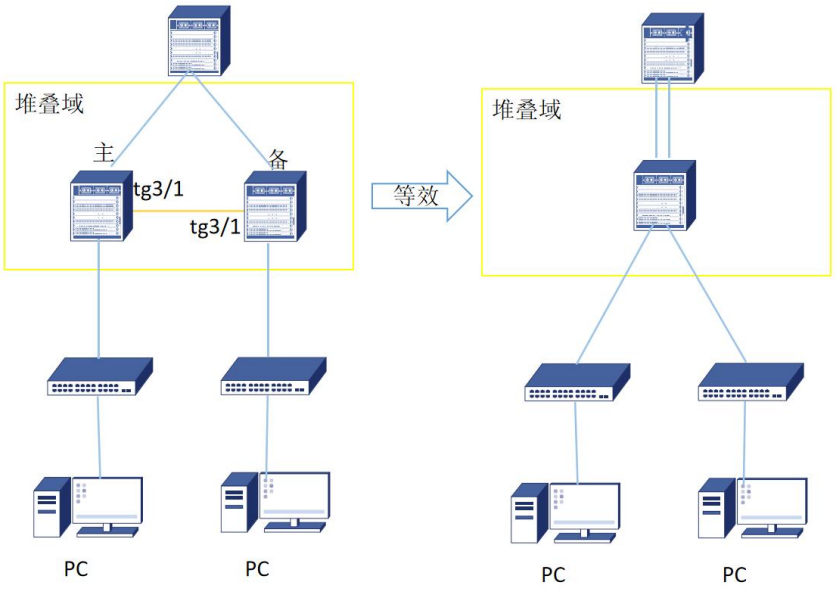


图 8-2BVSS 虚拟化示意图

BVSS 虚拟化技术涉及如下基本概念：

堆叠域

堆叠域（stacking domain）是堆叠组的一个属性，在一个网络中用来区分不同的堆叠组。只有具有相同堆叠域的交换机才能进行堆叠形成堆叠组，一台设备只能属于一个堆叠域。堆叠域的取值范围为 1-255，缺省堆叠域的值为 0。

注：0 是一个无效值，如果两台设备都缺省为 0，则无法堆叠起来

成员编号

堆叠组里的每一个成员设备都需要一个成员编号（stacking member-id）来标示，以区分其他成员设备。在每一个堆叠组中，每个成员设备的编号必须是唯一的，如果在同一个堆叠域中存在两个成员设备的编号相同，则不能形成堆叠组，在堆叠模式中，端口编号采用三维格（tengigabitEthernet 1/1/1 ），第一维表示成员设备编号。

成员优先级

成员优先级是堆叠组中成员设备的一个属性，主要用于设备角色的选举过程中确定成员设备的角色。成员设备的优先级越高（数值越大），当选为主设备的可能性就越大。成员设备的优先级的取值范围为 1 - 255，缺省为 0。在第一次堆叠协商过程中，优先级越高的设备选为主设备。

注：0 是一个无效值，如果两台设备都缺省为 0，则无法堆叠起来

堆叠模式

框式设备只支持一种堆叠模式：普通模式。在普通模式中，我们允许最多两台设备以单链路相连构成堆叠。缺省情况下设备是独立模式，不做堆叠模式。

8.1.5 角色选举

角色：主设备，备设备，候选设备。

目前角色选举的遵循如下原则：

(1)比较设备优先级，优先级高的（数值大）优先；

(2)设备的运行时间长的优先，运行时间差别小于 2 分钟的认为相同（2 分钟为暂定值，主要为了避免堆叠组整体重启后，带有重配置的主设备启动慢于非主设备而引起主设备变化）；

(3)设备的 mac 地址，小的优先。

8.1.6 成员设备退出

如果离开的是主设备，备设备升为主设备时，会将自己的优先级、运行时间提升为与原主设备相同，同时，会启动一个旧主设备保存定时器（默认为 3 分钟，可通过命令配置为 3-10 分钟），在该定时器超时之前，若原主设备又加入了堆叠组，则原主设备作为备设备；若定时器超时之后原主设备才加入堆叠组，则会重新选举主设备。

如果离开的是备设备，优先的候选设备自动升级为备设备。

8.1.7 相关协议

RNP 协议

RNP（Role Negotiation Protocol，角色协商协议）主要用于在虚拟化域中协商各个成员设备的角色。设备在虚拟化域中的角色分为三种：全局主设备、全局备设备和全局候选设备。

默认设备运行在 BVSS 模式下是默认开启 RNP 协议的。当设备启动完成后根据设备的优先级进行选举主设备和备设备的过程就是由 RNP 完成的。

SGNP 协议

SGNP（SL Group Negotiation Protocol，SL 组协商协议）主要用于在虚拟化系统中的相邻设备间协商虚拟化链路组的成员端口。有两个虚拟化链路组：组 1 和组 2。只有为端口配置所属的虚拟化链路组后，端口才能成为虚拟化链路组的成员端口。在开启 BVSS 模式后把堆叠板卡端口配置加入堆叠链路组。如果不配置，则两台设备无法进行交互，则无法形成虚拟化。而且在配置时如果先开启了 BVSS 模式，然后在进行配置时，已经不能配置。

该协议也是默认开启的协议，不需要开启，只需要把端口划入链路组即可。

8.1.8 BVSS 配置

通过 console 接口连接设备，输入用户名密码登录设备进行配置

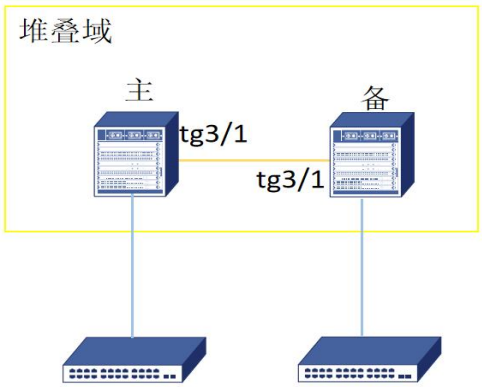
序号	配置	说明
1	Inspur#**config**	进入全局配置模式。
2	Inspur_config#**bvss**	进入 **BVSS** 配置模式

序号	配置	说明
3	Inspur_config_bvss#*[no]* **bvss enable**	开启/关闭堆叠管理
4	Inspur_config_bvss#*[no]* **bvss mode normal**	开启/关闭堆叠模式普通模式
5	Inspur_config_bvss#**bvss domain-id** *id*	配置堆叠域 **id**，取值范围为 1-255。
6	Inspur_config_bvss#**bvss member-id** *id*	配置堆叠成员编号 **id**，取值范围为 1-2
7	Inspur_config_bvss#**bvss priority** *priority*	配置堆叠设备优先级，取值范围为 1-255
8	Inspur_config_bvss#**bvss sgnp neighbour-timeout** *time*	配置 **sgnp** 邻居超时时间
9	Inspur_config_bvss#**bvss rnp old-master-timeout** *time*	配置 **rnp** 超时时间
10	Inspur_config_bvss#**bvss slot** *slot-id*	指定槽位为堆叠板卡
11	Inspur_config_bvss#**bvss interface** *number* **slot** *slot-number* **port** *port-number*	配置虚拟化端口
12	Inspur_config_bvss#**interface tgigaEthernet** *number*	进入堆叠口
13	Inspur_config_tg3/1#**bvss-link-group** *group-id*	配置堆叠口 **group** 组
14	Inspur_config_tg3/1#**exit**	退出堆叠口
15	Inspur_config_bvss#**exit**	退出 **BVSS** 模式
16	Inspur#**write bvss-config**	保存堆叠配置

序号	检查项	说明
1	Inspur#**show bvss current-config**	查看当前堆叠配置
2	Inspur#**show bvss rnp**	查看 **rnp** 信息
3	Inspur#**show bvss sgnp**	查看 **sgnp** 信息

8.1.9 BVSS 配置示例

以下图为例，两台 S9503 做堆叠虚拟为一台设备，堆叠组的 domain-id 为 1，主设备 member-id 为 1、优先级为 240、堆叠口为 tg3/1，备设备 member-id 为 2、优先级为 200、堆叠口为 tg3/1



主设备：

```
Inspur_config#
Inspur_config#bvss
Inspur_config_bvss#bvss enable
Please write bvss configuration and reboot switch, if not bvss function invalid.
Inspur_config_bvss#bvss mode normal
Inspur_config_bvss#bvss domain-id 1
Inspur_config_bvss#bvss member-id 1
Inspur_config_bvss#bvss priority 240
Inspur_config_bvss#bvss sgnp neighbour-timeout 10
Inspur_config_bvss#bvss rnp old-master-timeout 10
Inspur_config_bvss#bvss slot 3
Inspur_config_bvss#bvss interface 1 slot 3 port 1
Inspur_config_bvss#interface tgigaEthernet 3/1
Inspur_config_tg3/1#bvss-link-group 1
Inspur_config_tg3/1#exit
Inspur_config_bvss#exit
Inspur#write bvss-config
```

备设备

```
Inspur_config#
Inspur_config#bvss
Inspur_config_bvss#bvss enable
Please write bvss configuration and reboot switch, if not bvss function invalid.
Inspur_config_bvss#bvss mode normal
Inspur_config_bvss#bvss domain-id 1
Inspur_config_bvss#bvss member-id 2
Inspur_config_bvss#bvss priority 200
Inspur_config_bvss#bvss sgnp neighbour-timeout 10
Inspur_config_bvss#bvss rnp old-master-timeout 10
Inspur_config_bvss#bvss slot 3
Inspur_config_bvss#bvss interface 1 slot 3 port 1
Inspur_config_bvss#interface tgigaEthernet 3/1
Inspur_config_tg3/1#bvss-link-group 2
Inspur_config_tg3/1#exit
Inspur_config_bvss#exit
Inspur#write bvss-config
```

保存配置后，需要等待 3 分钟左右，等它们之间的配置同步完成之后断电重启俩台设备，设备重启完成后会自动开始堆叠

调式维护

查看当前堆叠配置

```
Inspur#show bvss current-config
bvss configuration information:
 bvss enable: TRUE          //已开启堆叠
 bvss domain-id: 1          //堆叠域为 1
 bvss member-id : 1         //成员 ID 为 1
 bvss mode: normal         //堆叠模式为普通
 bvss priority: 240          //优先级为 240
 bvss mac-address mode: use-active-member   //堆叠组 MAC 为主设备 MAC
```

查看 rnp 信息

```
Inspur#show bvss rnp
  RNP is running. CfgPri 240, SwitchType 0x107b, Slot 0
  System started, ignoreTimeoutCnt 0
  DomainId 1, MemberId 1, LoopTopology 0, Merge 0, Master State
  MasterMemId 1, BackupMemId 2, MasterGlbMacAddr 00e0.0f62.0035
  OldMasterMemberId 0, OldMasterWhile 0, txAdvPduCnt 3353
  bvss link group 1 is usable, bvss link group 2 is not usable.
  Pri info for member 1 (SwitchType 107b, slot 0):
    Priority 240, RunningTime 17097, MAC 00e0.0f62.0035
    //成员 1 优先级，运行时间，MAC 地址
  Pri info for member 2 (SwitchType 107b, slot 0):
    Priority 200, RunningTime 4198, MAC fcfa.f736.c300
    //成员 1 优先级，运行时间，MAC 地址
```

注意：

能看到所有成员信息即堆叠成功

查看 sgnp 信息

```
Inspur#show bvss sgnp
  SGNP is running, Running Time 2143, NeighbourTimeout 5, Started TMP
  bvss Role notified, System started, ignoreTimeoutCnt 4136
  DomainId 1, MemberId 2, bvss Mode 3, LoopTopology 0
  MAC Addr:fcfa.f736.c300, portMap:1-2
  bvss link group info for group 1:
    cfgMemberPt: ; validMemberPt:
    peerMemberId 0, peerGroupId 0
  bvss link group info for group 2:
    cfgMemberPt: 1-2; validMemberPt: 1-2
    peerMemberId 1, peerGroupId 1
  bvss port info for port 1:
```

```
  slotId 0, groupId 2, peerPortId 1, peerSlotId 0, peerGroupId 1
bvss port info for port 2:
  slotId 0, groupId 2, peerPortId 2, peerSlotId 0, peerGroupId 1
```