



## 配置指南-IP 地址及应用

---

本分册介绍 IP 地址及应用配置指南相关内容，包括以下章节：

1. IP 地址与服务
2. ARP
3. IPv6
4. DHCP
5. DHCPv6
6. DNS
7. FTP-Server
8. FTP Client
9. TFTP-Server
10. TUNNEL
11. 网络通信检测工具
12. TCP
13. 软件 IPv4/v6 快转

# 1 IP 地址与服务

## 1.1 概述

因特网协议（Internet Protocol，IP）使用逻辑虚拟的地址将数据包从源方发送到目的方，即 IP 地址。在网络层，路由设备使用 IP 地址完成数据包转发。

**i** 以下仅针对 IPv4 地址进行介绍。

### 协议规范

- RFC 1918：Address Allocation for Private Internets
- RFC 1166：Internet Numbers

## 1.2 典型应用

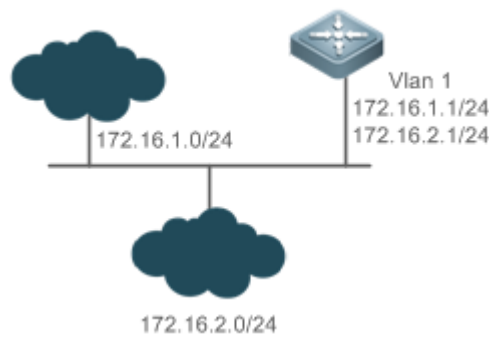
典型应用	场景描述
配置 IP 地址通信	两个网络使用同一个交换机接口进行通信

### 1.2.1 配置 IP 地址通信

#### 应用场景

交换机连接一个局域网，局域网分为两个网段：172.16.1.0/24 和 172.16.2.0/24。要求两个网段的计算机都可以通过交换机和因特网通信，并且两个网段的计算机之间可以互相通信。

图 1-1 IP 地址配置范例



## 功能部属

- 在 vlan1 口上配置两个 ip 地址，一个主 ip 地址，一个从 ip 地址。
- 在 172.16.1.0/24 网段中的主机上配置网关为 172.16.1.1，在 172.16.2.0/24 网段中的主机上配置网关为 172.16.2.1。

## 1.3 功能详解

### 基本概念

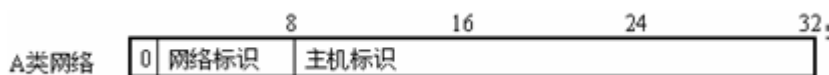
#### IP 地址

IP 地址由 32 位二进制组成，为了书写和描述方便，一般用十进制表示。十进制表示时，分为四组，每组 8 位，范围从 0~255，组之间用 “.” 号隔开，比如 “192.168.1.1” 就是用十进制表示的 IP 地址。

IP 地址顾名思义，自然是 IP 层协议的互连地址。32 位的 IP 地址由两个部分组成：1) 网络部分；2) 本地地址部分。根据网络部分的头几个比特位的值，目前使用中的 IP 地址可以划分成四大类。

A 类地址，最高比特位为 “0”，有 7 个比特位表示网络号，24 个比特位表示本地地址。这样总共有 128 个 A 类网络。

图 1-2



B 类地址，前两个最高比特位为 “10”，有 14 个比特位表示网络号，16 个比特位表示本地地址。这样总共有 16,384 个 B 类网络。

图 1-3



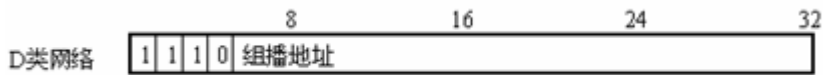
C 类地址，前三个最高比特位为 “110”，有 21 个比特位表示网络号，8 个比特位表示本地地址。这样总共有 2,097,152 个 C 类网络。

图 1-4



D 类地址，前四个最高比特位为 “1110”，其余比特位为组播地址。

图 1-5



**i** 前四个最高比特位为“1111”的地址是不允许分配的，这些地址称为 E 类地址，属于保留地址。

在建设网络过程中，进行 IP 地址规划时，一定要根据建设网络的性质进行 IP 地址分配。如果建设的网络需要与互联网连接，则需要到相应的机构申请分配 IP 地址。中国地区可以向中国互联网信息中心（CNNIC）申请，负责 IP 地址分配的最终机构为国际互联网名字与编号分配公司（ICANN, Internet Corporation for Assigned Names and Numbers）。如果建设的网络为内部私有网络，就不需要申请 IP 地址，但是也不能随便分配，最好分配专门的私有网络地址。

下表为保留与可用的地址列表：

类别	地址空间	状态
A 类网络	0.0.0.0~0.255.255.255	保留
	1.0.0.0~126.255.255.255	可用
	127.0.0.0~127.255.255.255	保留
B 类网络	128.0.0.0~191.254.255.255	可用
	191.255.0.0~191.255.255.255	保留
C 类网络	192.0.0.0~192.0.0.255	保留
	192.0.1.0~223.255.254.255	可用
	223.255.255.0~223.255.255.255	保留
D 类网络	224.0.0.0~239.255.255.255	组播地址
E 类网络	240.0.0.0~255.255.255.254	保留
	255.255.255.255	广播地址

其中专门有三个地址块提供给私有网络，这些地址是不会在互联网中使用的，如果分配了这些地址的网络需要连接互联网，则需要将这些 IP 地址转换成有效的互联网地址。下表为私有网络地址空间，私有网络地址由 RFC 1918 文档定义：

类别	地址空间	状态
A 类网络	10.0.0.0~10.255.255.255	1 个 A 类网络
B 类网络	172.16.0.0~172.31.255.255	16 个 B 类网络
C 类网络	192.168.0.0~192.168.255.255	256 个 C 类网络

关于 IP 地址、TCP/UDP 端口及其它编码的分配情况，请参考 RFC 1166 文档。

子网掩码

网络掩码也是一个 32 比特的数值，标识着该 IP 地址的哪几个比特为网络部分。网络掩码中，值为“1”的比特对应的 IP 地址比特位就是网络部分，值为“0”的比特对应的 IP 地址比特位就是主机地址部分。如 A 类网络对应的网络掩码为“255.0.0.0”。您可以利用网络掩码对一个网络进行子网划分，子网划分就是将主机地址部分的一些比特位也作为网络部分，缩小主机容量，增加网络的数量，这时的网络掩码就称为子网掩码。

广播报文

广播报文是指目标地址为某个物理网络上所有主机的数据包。锐捷产品支持两种类型广播报文：1) 定向广播，是指数据包接收者为一个指定网络的所有主机，目标地址的主机部分全为“1”；2) 淹没广播，是指数据包接收者为所有网络的主机，目标地址 32 比特位全为“1”。

### 📌 ICMP 报文

ICMP 是 ( Internet Control Message Protocol ) Internet 控制报文协议。它是 TCP/IP 协议族的一个子协议，用于在 IP 主机、网络设备之间传递控制消息，主要用于网络出现异常的时候通知相应设备。

### 📌 TTL

TTL ( Time-To-Live )，生存时间。指定数据包被路由器丢弃之前允许通过的网段数量。它是 IP 协议报文中的一个值，它告诉网络，数据包在网络中的时间是否太长而应被丢弃。

## 功能特性

功能特性	作用
IP 地址	用于配置接口 IP 地址，该接口才允许运行 IP 协议。
广播报文处理	设置 IP 广播地址，转发处理定向广播报文。
发送 ICMP 报文	控制 ICMP 协议报文的收发。
控制 ICMP 差错报文的发送速率	防止拒绝服务攻击。
IP MTU	用于配置接口 IP 报文的最大传输单元。
IP TTL	用于配置单播报文和广播报文的 TTL。
IP 源路由	用于对接收报文的源路由进行检查。
IP 地址池	用于 ppp 协商为对端分配 ip 地址

### 1.3.1 IP 地址

接口获取 IP 地址有以下方式：

- (1) 手工配置 IP 地址。
- (2) 利用 DHCP 协议获取 IP 地址。
- (3) 通过 PPP 协商获得 IP 地址。

这几种方式是互斥的，配置新的获取 IP 地址方式时会覆盖通过原有方式获取的 IP 地址。



利用 DHCP 协议获取 IP 地址请参见“DHCP”章节，以下仅介绍其他三种获取 IP 地址的方式。

### 📌 配置接口 IP 地址


一个设备只有配置了 IP 地址，才可以接收和发送 IP 数据包，接口配置了 IP 地址，说明该接口允许运行 IP 协议。

### 📌 接口配置多个 IP 地址

锐捷产品可以支持一个接口配置多个 IP 地址，其中一个为主 IP 地址，其余全部为次 IP 地址。次 IP 地址的配置理论上没有数目限制，但是次 IP 地址与主 IP 以及次 IP 地址之间必须属于不同网络。在网络建设中，会经常使用到次 IP 地址，通常在以下情况下应该考虑使用次 IP 地址：

- 一个网络没有足够多的主机地址。例如，现在一般局域网需要一个 C 类网络，可分配 254 台主机。但是当局域网主机超过 254 台时，一个 C 类网络将不够分配，有必要分配另一个 C 类网络地址。这样设备就需要连接两个网络，所以就可能需要配置多个 IP 地址。
- 许多旧的网络是基于第二层的桥接网络，没有进行子网的划分。次 IP 地址的使用可以使该网络很容易升级到基于 IP 层的路由网络。对于每个子网，设备都配置一个 IP 地址。
- 一个网络的两个子网被另外一个网络隔离开，可以创建一个被隔离网络的子网，通过配置次 IP 地址的方式，将隔离的子网连接起来。一个子网不能在设备的两个或两个以上接口出现。

#### 配置通过 PPP 协商获取 IP 地址

 本命令只在点对点接口上支持。

通过此配置，点对点接口可以通过 PPP 协商接受对端为自己分配的 IP 地址。

### 相关配置

#### 配置接口一个或多个 IP 地址

- 缺省情况接口没有配置 IP 地址。
- 通过 **ip address** 命令配置接口 IP 地址。
- 配置后根据冲突检测即可使用该 IP 地址进行通信。
- 通过 **ip address ip-address masksecondary** 可以配置多个次 IP 地址。

## 1.3.2 广播报文处理

### 工作原理

广播分两种，全广播，即 IP 地址为 255.255.255.255，由于会被路由器禁止传输，所以也叫本地网络广播。另一种是所有的主机位都为 1 的广播，例如：192.168.1.255/24，这种广播，通过配置是可以被转发的。

如果 IP 网络设备转发淹没广播（一般指目标 IP 地址为全“1”的广播报文），可能会引起网络的超负载，严重影响网络的运行，这种情况称为广播风暴。设备提供了一些办法能够将广播风暴限制在本地网络，阻止其继续扩张。但对于桥和交换机等基于二层网络设备，将转发和传播广播风暴。

解决广播风暴最好的办法就是给每个网络指定一个广播地址，这就是定向广播，这要求使用广播报文的 IP 协议尽可能应用定向广播而不是淹没广播进行数据传播。

关于广播问题的详细描述，请参见 RFC 919 和 RFC 922。

IP 定向广播报文是指目标地址为某个 IP 子网广播地址的 IP 报文，如目标地址为 172.16.16.255 的报文就称为定向广播报文。但是产生该报文的节点又不是目标子网的成员。

没有与目标子网直连的设备接收到 IP 定向广播报文，跟转发单播报文一样处理定向广播报文。当定向广播报文到达直连该子网的设备后，设备将把定向广播报文转换为淹没广播报文（一般指目标 IP 地址为全“1”的广播报文），然后以链路层广播方式发送给目标子网上的所有主机。

## 相关配置

### 配置 IP 广播地址

- 缺省情况下接口 IP 广播地址为 255.255.255.255。
- 如果需要定义其它地址的广播报文，可以在接口下配置 `ip broadcast-address` 命令。

### 允许转发定向广播

- 缺省情况接口不允许转发定向广播。
- 用户可以在指定的接口上，通过 `ip directed-broadcast` 命令配置接口允许转发定向广播，这样该接口就可以转发到直连网络的定向广播了。该命令只影响定向广播报文在目标子网的传输，而不影响其它定向广播报文的正常转发。
- 在接口上，用户还可以通过定义访问控制列表来控制转发某些定向广播。当定义了访问列表时，只有符合访问列表中定义的定向广播才会被转发。

## 1.3.3 发送 ICMP 报文

### 工作原理

#### ICMP 协议不可达消息

当设备接收到目标为自己的非广播报文，但是该数据包中采用了设备不能处理的 IP 协议，设备就向源地址发送 ICMP 协议不可达消息。另外，如果设备由于不知道路由而不能转发数据包时，也会发送 ICMP 主机不可达消息。

#### ICMP 重定向消息

路由有时会不够优化，使得设备从一个接口接收到的数据包，还要从该接口发送出去。如果设备将数据包从接收接口重新发送出去，设备就会给数据源发送一个 ICMP 重定向消息，告诉数据源到该目标地址的网关为同一子网上的另外一台设备。这样数据源就会将后续的数据包按照最佳的路径进行发送。

#### ICMP 掩码应答消息

网络设备有时需要知道互联网上某个子网的子网掩码，为了获取该信息，网络设备可以发送 ICMP 掩码请求消息，接收到 ICMP 掩码请求消息的网络设备就会发送掩码应答消息。

#### TTL 超时消息

设备转发 IP 报文时，如果报文的 TTL 超时了，设备需要向源端回应一个 TTL 超时的差错报文。

为了防止被其他设备 traceroute 到，进而遭受到攻击，可以关闭 TTL 超时差错报文的发送功能。关闭该功能后，设备收到 TTL 超时的报文，将不再回应 TTL 超时差错报文。

#### 时间戳查询

RFC 792 要求系统收到 ICMP 时间戳查询时，需要返回系统的当前时间。

为了防止攻击者通过该协议获取到系统的时间，从而攻击到一些基于时间认证的协议，可以关闭时间戳查询功能。关闭该功能后，设备收到时间戳查询报文直接丢弃，不再应答。

## 相关配置

#### 启用 ICMP 协议不可达消息

- 缺省情况接口启用 ICMP 协议不可达消息功能。
- 可通过 `[no] ip unreachable` 命令关闭或启用该功能。

#### 启用 ICMP 重定向消息

- 缺省情况接口启用 ICMP 协议重定向消息功能。
- 可通过 `[no] ip redirects` 命令关闭或启用该功能。

#### 启用 ICMP 掩码应答消息

- 缺省情况接口启用 ICMP 掩码应答消息功能。
- 可通过 `[no] ip mask-reply` 命令关闭或启用该功能。

#### 启用 TTL 超时消息

- 缺省情况启用 TTL 超时消息功能。
- 可通过全局模式下的 `[no] ip ttl-expires enable` 命令关闭或启用该功能。

#### 启用时间戳查询功能

- 缺省情况启用 ICMP 时间戳查询功能。
- 可通过全局模式下的 `[no] ip icmp timestamp` 命令关闭或启用该功能。

## 1.3.4 控制 ICMP 差错报文的发送速率

### 工作原理

为了防止拒绝服务攻击，对 ICMP 差错报文的发送速率进行限制，采用令牌桶算法。



如果 IP 报文需要分片，但是 IP 首部的不可分片位被设置了，设备会向源 IP 地址发送编号为 4 的 ICMP 目的不可达报文，这种 ICMP 差错报文的主要用途是路径 MTU 发现。为了防止其它 ICMP 差错报文太多导致发不出编号为 4 的 ICMP 目的不可达报文，从而导致路径 MTU 发现功能失效，对编号为 4 的 ICMP 目的不可达报文和其它 ICMP 差错报文分别限速。

## 相关配置

### 配置 IP 首部不可分片位触发的 ICMP 目的不可达报文的发送速率

- 缺省速率是 100 毫秒 10 个。
- 可通过 `ip icmp error-interval DF` 配置发送速率。

### 配置其它 ICMP 差错报文的发送速率

- 缺省速率是 100 毫秒 10 个。
- 可通过 `ip icmp error-interval` 配置发送速率。

## 1.3.5 IP MTU

### 工作原理

如果一个 IP 报文超过 IP MTU 的大小，RGOS 软件就会对报文进行拆分。所有在同一物理网段上的设备，其互联接口的 IP MTU 一定要一致。锐捷产品允许调整接口的链路 MTU 值，而且接口的链路 MTU 的变化会引起接口的 IP MTU 的变化，接口的 IP MTU 会自动与接口的链路 MTU 保持一致。但是反之不行，如果调整了接口的 IP MTU 值，接口的链路 MTU 不会跟着改变。

## 相关配置

### 设置 IP MTU

- 缺省情况接口 IP MTU 为 1500。
- 可通过 `ip mtu` 设置 IP 包最大传输单元(MTU)。

## 1.3.6 IP TTL

### 工作原理

IP 数据包从源地址向目的地址经过路由器间传播，设置一个 TTL 数值，每过一个路由器 TTL 值就减一，当减到零的时候，路由器就把这个包丢掉，这样可以防止无用的包在网络上无限传播下去，浪费网络带宽。

## 相关配置

### 设置 IP TTL

- 缺省情况接口 IP TTL 为 64。
- 可通过 `ip ttl` 设置接口的 IP TTL 值。

1.3.7 IP 源路由

工作原理

锐捷产品支持 IP 源路由。当设备接收到 IP 数据包时，会对 IP 报头的严格源路由、宽松源路由和记录路由等选项进行检查，这些选项在 RFC 791 中有详细描述。如果检测到该数据包启用了其中一个选项，就会执行响应的动作；如果检测到无效的选项，就会给数据源发送一个 ICMP 参数问题消息，然后丢弃该数据包。

开启 IP 源路由，在 IP 数据报选项中增加源路由选项，可用于测试某特定网络的吞吐率，也可以是数据报绕开出错的网络。然而，可能会导致诸如源地址欺骗(Source Address Spoofing)、IP 欺骗(IP Spoofing)等的网络攻击。




相关配置

配置 IP 源路由

- 缺省情况开启 IP 源路由功能。
- 可通过 `ip source-route` 开启或关闭该功能。

1.4 配置详解

配置项	配置建议&相关命令	
配置接口 IP 地址	 必须配置。用于配置 ip 地址，允许接口运行 IP 协议。	
	<code>ip address</code>	手工配置接口 IP 地址
配置广播报文处理方式	 可选配置。用于设置 IP 广播地址，允许转发定向广播报文。	
	<code>ip broadcast-address</code>	配置 IP 广播地址
	<code>ip directed-broadcast</code>	允许转发定向广播
配置发送 ICMP 报文	 可选配置。用于控制 ICMP 协议报文的收发。	
	<code>ip unreachable</code>	启用 ICMP 协议不可达和主机不可达消息
	<code>ip redirects</code>	启用 ICMP 重定向消息
	<code>ip mask-reply</code>	启用掩码应答消息
	<code>ip ttl-expires enable</code>	启用发送 TTL 超时差错报文功能
	<code>ip icmp timestamp</code>	启用时间戳查询功能
配置 ICMP 差错报文的发送速	 可选配置。	

率	<b>ip icmp error-interval DF</b>	配置 IP 首部不可分片位触发的 ICMP 目的不可达报文的发送速率
	<b>ip icmp error-interval</b>	配置其它 ICMP 差错报文和 ICMP 重定向报文的发送速率
设置 IP MTU	 可选配置。用于配置接口 IP 报文的最大传输单元。	
	<b>ip mtu</b>	设置 MTU 值
设置 IP TTL	 可选配置。用于配置单播报文和广播报文的 TTL。	
	<b>ip ttl</b>	设置 TTL 值
配置 IP 源路由	 可选配置。用于配置对接收报文的源路由进行检查。	
	<b>ip source-route</b>	启用 IP 源路由

### 1.4.1 配置接口 IP 地址

#### 配置效果

通过配置接口 IP 地址实现 IP 网络通信。

#### 注意事项

- 

#### 配置方法

##### 手工配置接口 IP 地址

- 必须配置。
- 在三层接口模式下配置。

##### 配置通过 PPP 协商获取接口 IP 地址

- 可选配置。
- 如果点对点接口上没有配置 IP 地址，且需要通过 PPP 协商获取 IP 地址时配置。
- 在三层接口模式下配置。

#### 检验方法

通过 **show ip interface** 可以看到配置的地址生效

## 相关命令

### 手工配置接口 IP 地址

【命令格式】 **ip address** *ip-address network-mask* [ **secondary** ]

【参数说明】 *ip-address* : 32 个比特位 IP 地址，8 位一组，以十进制方式表示，组之间用点隔开。

*network-mask* : 32 个比特位网络掩码，“1”表示掩码位，“0”表示主机位。每 8 位一组，以十进制方式表示，组之间用点隔开。

**secondary** : 表示配置的次 IP 地址。

【命令模式】 接口模式

【使用指导】 -

## 配置举例

### 给接口配置 IP 地址

【配置方法】 在接口 GigabitEthernet 0/0 配置 ip 地址 192.168.23.110 255.255.255.0

```
Ruijie#configure terminal
Ruijie(config)#interface gigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)# no switchport
Ruijie(config-if-GigabitEthernet 0/0)#ip address 192.168.23.110 255.255.255.0
```

【检验方法】 使用 **show ip interface** 可以看到接口 GigabitEthernet 0/0 添加地址成功

```
Ruijie# show ip interface gigabitEthernet 0/0
GigabitEthernet 0/0
  IP interface state is: UP
  IP interface type is: BROADCAST
  IP interface MTU is: 1500
  IP address is:
    192.168.23.110/24 (primary)
```

## 1.4.2 配置广播报文处理方式

### 配置效果

配置接口广播地址为 0.0.0.0，并允许转发定向广播报文。

### 注意事项

-

## 配置方法

### 配置 IP 广播地址

- 可选配置，有些老的主机可能只认 0.0.0.0 的广播地址，此时需要配置接口的广播地址为 0.0.0.0。
- 在三层接口模式下配置。

### 允许转发定向广播

- 可选配置，向处在一个广播域的全部主机发送广播，但是发送者并不处在这个广播域内，此时需要配置允许转发定向广播。
- 在三层接口模式下配置。

## 检验方法

通过 **show running-config interface** 可以看到配置生效

## 相关命令

### 配置 IP 广播地址

【命令格式】 **ip broadcast-address ip-address**

【参数说明】 *ip-address*：IP 网络的广播地址。

【命令模式】 接口模式

【使用指导】 目前 IP 广播报文的目标地址一般为全 “1”，表示为 255.255.255.255。RGOS 软件可以通过定义产生其它 IP 地址的广播报文，而且可以同时接收全 “1” 以及自己定义的广播包。

### 允许转发定向广播

【命令格式】 **ip directed-broadcast [ access-list-number ]**

【参数说明】 *access-list-number*：访问列表号，范围从 1-199，1300 - 2699。如果定义了访问列表号，只有匹配该访问列表的 IP 定向广播报文才转换。

【命令模式】 接口模式

【使用指导】 如果在接口上配置了 **no ip directed-broadcast**，RGOS 将丢弃接收到的直连网络的定向广播报文。

## 配置举例

【配置方法】 在设备端口 gigabitEthernet 0/1 配置 IP 广播报文的目标地址为 0.0.0.0，启用定向广播的转发。

```
Ruijie#configure terminal
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# no switchport
Ruijie(config-if-GigabitEthernet 0/1)#ip broadcast-address 0.0.0.0
Ruijie(config-if-GigabitEthernet 0/1)#ip directed-broadcast
```

【检验方法】 使用 **show ip interface** 可以看到接口 GigabitEthernet 0/1 配置成功

```
Ruijie#show running-config interface gigabitEthernet 0/1
ip directed-broadcast
ip broadcast-address 0.0.0.0
```

### 1.4.3 配置发送 ICMP 报文

#### 配置效果

启用接口 ICMP 协议不可达消息，ICMP 重定向消息以及掩码应答消息。

#### 注意事项

-

#### 配置方法

##### ▾ 启用 ICMP 协议不可达消息

- 缺省开启 ICMP 协议不可达消息。
- 可选配置，通过 **no ip unreachable**s 禁止该功能。
- 在三层接口模式下配置。

##### ▾ 启用 ICMP 重定向消息

- 缺省开启 ICMP 重定向消息。
- 可选配置，通过 **no ip redirects** 禁止该功能。
- 在三层接口模式下配置。

##### ▾ 启用 ICMP 掩码应答消息

- 缺省开启 ICMP 掩码应答消息。
- 可选配置，通过 **no ip mask-reply** 禁止该功能。
- 在三层接口模式下配置。

##### ▾ 启用 TTL 超时消息

- 缺省开启 TTL 超时消息。
- 可选配置，通过 **no ip ttl-expires enable** 禁止该功能。
- 在全局模式下配置。

##### ▾ 启用时间戳查询

- 缺省开启时间戳查询功能。
- 可选配置，通过 **no ip icmp timestamp** 禁止该功能。
- 在全局模式下配置。

## 检验方法

---

通过 **show ip interface** 可以看到配置生效。

通过 **show running-config** 可以看到 TTL 超时消息是否关闭。

通过 **show running-config** 可以看到时间戳查询功能是否关闭。

## 相关命令

---

### ▾ 启用 ICMP 协议不可达消息

- 【命令格式】 **ip unreachable**
- 【参数说明】 -
- 【命令模式】 接口模式
- 【使用指导】 -

### ▾ 启用 ICMP 重定向消息

- 【命令格式】 **ip redirects**
- 【参数说明】 -
- 【命令模式】 接口模式
- 【使用指导】 -

### ▾ 启用 ICMP 掩码应答消息

- 【命令格式】 **ip mask-reply**
- 【参数说明】 -
- 【命令模式】 接口模式
- 【使用指导】 -

### ▾ 关闭 TTL 超时消息

- 【命令格式】 **no ip ttl-expires enable**
- 【参数说明】 -
- 【命令模式】 全局模式
- 【使用指导】 -

### ▾ 关闭时间戳查询

- 【命令格式】 **no ip icmp timestamp**
- 【参数说明】 -

【命令模式】 全局模式  
【使用指导】 -

## 配置举例

【配置方法】 在设备端口 gigabitEthernet 0/1 启用 ICMP 协议不可达消息、ICMP 重定向消息以及 ICMP 掩码应答消息功能。

```
Ruijie#configure terminal
Ruijie(config)# no ip ttl-expires enable
Ruijie(config)# no ip icmp timestamp
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# no switchport
Ruijie(config-if-GigabitEthernet 0/1)# ip unreachable
Ruijie(config-if-GigabitEthernet 0/1)# ip redirects
Ruijie(config-if-GigabitEthernet 0/1)# ip mask-reply
```

【检验方法】 使用 **show ip interface** 可以看到接口 GigabitEthernet 0/1 配置成功

```
Ruijie#show running-config | include ip ttl-expires enable
no ip ttl-expires enable
Ruijie#show running-config | include ip icmp timestamp
no ip icmp timestamp
Ruijie#show ip interface gigabitEthernet 0/1
GigabitEthernet 0/1
    ICMP mask reply is: ON
    Send ICMP redirect is: ON
    Send ICMP unreachable is: ON
```

## 1.4.4 配置 ICMP 报文差错报文的发送速率

### 配置效果

配置 ICMP 差错报文的发送速率。

### 注意事项

-

### 配置方法

🔗 配置 IP 首部不可分片位触发的 ICMP 目的不可达报文的发送速率



- 可选配置。
- 在全局模式下配置。

#### 配置其它 ICMP 差错报文的发送速率

- 可选配置。
- 在全局模式下配置。

## 检验方法

执行 **show running-config** 可以看到配置生效。

## 相关命令

#### 配置 IP 首部不可分片位触发的 ICMP 目的不可达报文的发送速率

【命令格式】 **ip icmp error-interval DF milliseconds [bucket-size]**

【参数说明】 *milliseconds*：令牌桶的刷新周期，取值范围 0~2147483647，缺省值为 100，单位为毫秒。取值为 0 时，表示不限制 ICMP 差错报文的发送速率。

*bucket-size*：令牌桶中容纳的令牌数，取值范围 1~200，缺省值为 10。

【命令模式】 全局模式

【使用指导】 为了防止拒绝服务攻击，对 ICMP 差错报文的发送速率进行限制，采用令牌桶算法。

如果 IP 报文需要分片，但是 IP 首部的不可分片位被设置了，设备会向源 IP 地址发送编号为 4 的 ICMP 目的不可达报文，这种 ICMP 差错报文的主要用途是路径 MTU 发现。为了防止其它 ICMP 差错报文太多导致发不出编号为 4 的 ICMP 目的不可达报文，从而导致路径 MTU 发现功能失效，对编号为 4 的 ICMP 目的不可达报文和其它 ICMP 差错报文分别限速。

因为定时器的精度是 10 毫秒，建议用户把令牌桶的刷新周期配置成 10 毫秒的整数倍。如果令牌桶的刷新周期大于 0 小于 10，实际生效的刷新周期是 10 毫秒，例如配置 5 毫秒 1 个，实际效果是 10 毫秒 2 个；如果令牌桶的刷新周期不是 10 毫秒的整数倍，实际生效的刷新周期自动换算成 10 毫秒的整数倍，例如配置 15 毫秒 3 个，实际效果是 10 毫秒 2 个。

#### 配置其它 ICMP 差错报文的发送速率

【命令格式】 **ip icmp error-interval milliseconds [bucket-size]**

【参数说明】 *milliseconds*：令牌桶的刷新周期，取值范围 0~2147483647，缺省值为 100，单位为毫秒。取值为 0 时，表示不限制 ICMP 差错报文的发送速率。

*bucket-size*：令牌桶中容纳的令牌数，取值范围 1~200，缺省值为 10。

【命令模式】 全局模式

【使用指导】 为了防止拒绝服务攻击，对 ICMP 差错报文的发送速率进行限制，采用令牌桶算法。

因为定时器的精度是 10 毫秒，建议用户把令牌桶的刷新周期配置成 10 毫秒的整数倍。如果令牌桶的刷新周期大于 0 小于 10，实际生效的刷新周期是 10 毫秒，例如配置 5 毫秒 1 个，实际效果是 10 毫秒 2 个；如果令牌桶的刷新周期不是 10 毫秒的整数倍，实际生效的刷新周期自动换算成 10 毫秒的整数倍，例如配置 15 毫秒 3 个，实际效果是 10 毫秒 2 个。

## 配置举例

【配置方法】 配置 IP 首部不可分片位触发的 ICMP 目的不可达报文的发送速率为 1 秒 100 个，配置其它 ICMP 差错报文的发送速率为 1 秒 10 个。

```
Ruijie(config)# ip icmp error-interval DF 1000 100
Ruijie(config)# ip icmp error-interval 1000 10
```

【检验方法】 执行 **show running-config** 可以看到配置生效

```
Ruijie#show running-config | include ip icmp error-interval
ip icmp error-interval 1000 10
ip icmp error-interval DF 1000 100
```

## 1.4.5 配置 IP MTU

### 配置效果

调整 IP 包最大传输单元。

### 注意事项

-

### 配置方法

- 可选配置，所有在同一物理网段上的设备，当互联接口的 IP MTU 不一致时需要配置为一致。
- 在三层接口模式下配置。

### 检验方法

通过 **show ip interface** 可以看到配置生效

### 相关命令

#### 📄 配置 IP MTU

- 【命令格式】 **ip mtu bytes**
- 【参数说明】 **bytes**：IP 包最大传输单元，以字节为单位，范围 68~1500。
- 【命令模式】 接口模式
- 【使用指导】 -

## 配置举例

【配置方法】 将 gigabitEthernet 0/1 接口的 IP MTU 值设为 512 字节

```
Ruijie#configure terminal
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# no switchport
Ruijie(config-if-GigabitEthernet 0/1)#ip mtu 512
```

【检验方法】 使用 **show ip interface** 可以看到接口 GigabitEthernet 0/1 配置成功

```
Ruijie# show ip interface gigabitEthernet 0/1
IP interface MTU is: 512
```

## 1.4.6 配置 IP TTL

### 配置效果

修改接口的 IP TTL 值。

### 注意事项

-

### 配置方法

- 可选配置。
- 在三层接口模式下配置。

### 检验方法

通过 **show run-config** 可以看到配置生效

### 相关命令

#### 📄 配置 IP TTL

【命令格式】 **ip ttl value**

【参数说明】 *value* : TTL 值，取值范围是 0~255。

【命令模式】 全局模式

【使用指导】 -

## 配置举例

- 【配置方法】
- 配置本机发送的单播报文的缺省 TTL 值为 100。

```
Ruijie#configure terminal
Ruijie(config)#ip ttl 100
```

- 【检验方法】 通过 **show run-config** 可以看到配置生效

```
Ruijie#show running-config
ip ttl 100
```

## 1.4.7 配置 IP 源路由

### 配置效果

开启或关闭 IP 源路由信息的处理功能。

### 注意事项

-

### 配置方法

- 缺省情况下开启 IP 源路由功能。
- 可选配置，通过 **no ip source-route** 可关闭 IP 源路由功能。

### 检验方法

通过 **show run-config** 可以看到配置生效。

### 相关命令

#### 📄 配置 IP 源路由

- 【命令格式】 **ip source-route**
- 【参数说明】 -
- 【命令模式】 全局模式
- 【使用指导】 -

### 配置举例

【配置方法】      ●    关闭了 IP 源路由信息的处理功能。

```
Ruijie#configure terminal
Ruijie(config)#no ip source-route
```

【检验方法】      通过 **show run-config** 可以看到配置生效

```
Ruijie#show running-config
no ip source-route
```

# 1.5 监视与维护

## 清除各类信息

---

-

## 查看运行情况

---

作用	命令
显示接口 IP 信息	<b>show ip interface</b> [ <i>interface-type</i> <i>interface-number</i>   <b>brief</b> ]
显示 IP 报文统计值	<b>show ip packet statistics</b> [ <b>total</b>   <i>interface-name</i> ]
显示协议栈 IP 报文收发统计信息	<b>show ip packet queue</b>

## 查看调试信息

---

-

## 2 ARP

### 2.1 概述

在局域网中，每个 IP 网络设备都有两个地址：1）本地地址，由于它包含在数据链路层的帧头中，更准确地说应该是数据链路层地址，但实际上对本地地址进行处理的是数据链路层中的 MAC 子层，因此习惯上称为 MAC 地址，MAC 地址在局域网上代表着 IP 网络设备；2）网络地址，在互联网上代表着 IP 网络设备，同时它也说明了该设备所属的网络。

局域网上两台 IP 设备之间需要通信，必须要知道对方的 48 比特的 MAC 地址。根据 IP 地址来获知 MAC 地址的过程称为地址解析。地址解析的方式有两类：1）地址解析协议（ARP）；2）代理地址解析协议（Proxy ARP）。关于 ARP、Proxy ARP，分别在 RFC 826，RFC 1027 文档中描述。

ARP(Address Resolution Protocol，地址解析协议)是用来绑定 MAC 地址和 IP 地址的，以 IP 地址作为输入，ARP 能够知道其关联的 MAC 地址。一旦知道了 MAC 地址，IP 地址与 MAC 地址对应关系就会保存在设备的 ARP 缓存中。有了 MAC 地址，IP 设备就可以封装链路层的帧，然后将数据帧发送到局域网上去。缺省配置下，以太网上 IP 和 ARP 的封装为 Ethernet II 类型。

#### 协议规范

- RFC826：An Ethernet Address Resolution Protocol
- RFC1027：Using ARP to implement transparent subnet gateways

### 2.2 典型应用

典型应用	场景描述
在局域网内提供地址解析协议服务	在同一网段中，主机学习其他设备的 MAC 地址，需要用到地址解析协议。
使用代理 ARP 实现透明的子网网关	通过代理地址解析服务，允许主机在不知道另一个网络是否存在的情况下和另一网络内的主机直接通讯。

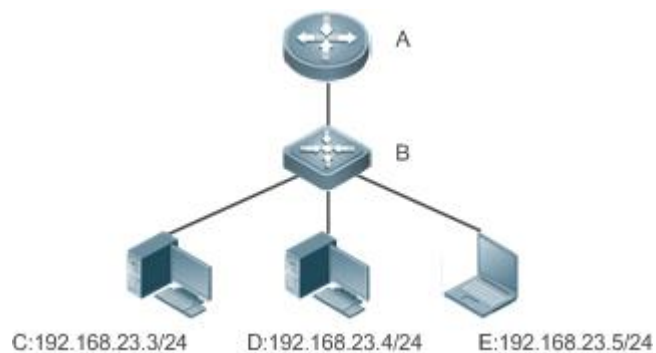
#### 2.2.1 在局域网内提供地址解析协议服务

#### 应用场景

在所有 IPv4 局域网内，都需要用到 ARP 协议。

- 主机需要通过 ARP 协议来学习其他设备的 MAC 地址，只有学到 MAC 地址后，主机才可以和其他设备通信。

图 2-1



【注释】 A 为路由器  
B 为交换机，作为用户主机网段的网关。  
C、D、E 为用户主机

## 功能部属

- 在局域网内运行 ARP 协议，实现 IP 地址和 MAC 地址的映射。

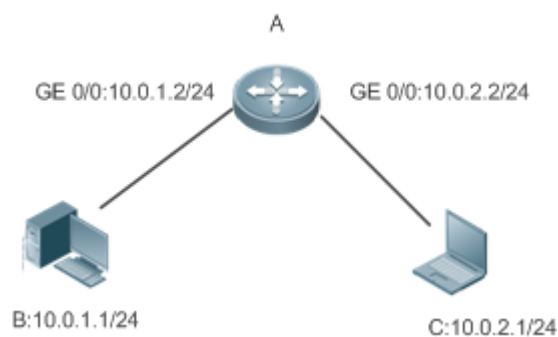
## 2.2.2 使用代理 ARP 实现透明的子网网关

### 应用场景

在不同的 IPv4 局域网内，实现透明的子网网关。

- 通过在设备上配置代理 ARP 的功能，实现不同网段内主机的直接通讯。

图 2-2



【注释】 A 为路由器，连接两个局域网  
B、C 为用户主机，不配置默认网关，在不同的子网

## 功能部属

- 在子网网关上运行代理 ARP 功能，可以帮助没有路由信息的主机获得其它子网 IP 地址的 MAC 地址。

## 2.3 功能详解

### 功能特性

功能特性	作用
静态 ARP	用户手工指定 IP 地址和 MAC 地址的映射，防止设备学到错误的 ARP 表项而影响网络。
ARP 属性设置	用户指定 ARP 表项的超时时间、ARP 请求重传次数和间隔、未解析 ARP 表项数上限。
可信任 ARP	防止 ARP 欺骗。
免费 ARP	检测 IP 地址冲突，以及让外围设备更新本机的 ARP。
代理 ARP	代理应答请求其他设备的 ARP 请求。
本地代理 ARP	代理应答一台设备请求子网内的其他设备的 ARP 请求
ARP 可信检测	通过 NDU（邻居不可达探测），保证学习的 ARP 表项正确。
ARP 防 IP 报文攻击	通过设置触发 ARP 设丢弃表项的 IP 报文个数，触发设置丢弃表项到硬件，来防止未知名单播报文大量送 CPU 对 CPU 造成冲击。
抑制往认证 VLAN 发送 ARP 请求	通过设置抑制往认证 vlan 发送广播 arp 请求报文，可以减少网络中 arp 广播报文的数量，改善网络环境

### 2.3.1 静态 ARP

静态 ARP 包括手工配置的静态 ARP 和认证下发的静态 ARP。手工配置的静态 ARP 优先级大于认证下发的静态 ARP。静态 ARP 能够防止设备学到错误的 ARP 表项而影响网络。

### 工作原理

静态 ARP，设备不会再去主动更新 ARP 表项，并且永久存在。

设备转发三层报文时，以太头部的目的 MAC 地址将采用静态配置的 MAC 地址来封装。

### 相关配置

#### 配置静态 ARP

手工配置的静态 ARP，在全局模式下，使用 `arp [vrf name] ip-address mac-address type` 命令配置静态 ARP 表项。缺省情况下用户没有配置任何静态 ARP 表项。用户可以将静态 ARP 表项绑定到不同的 VRF 下，也可以绑定在全局 VRF 下。ARP 封装只支持 Ethernet II 类型，用 arpa 表示。

### 2.3.2 ARP 属性设置

用户指定 ARP 表项的超时时间、ARP 请求重传次数和间隔、未解析 ARP 表项数上限、接口 ARP 学习数量限制、单板 ARP 学习数量限制。



## 工作原理

### 📌 ARP 超时设置

ARP 超时设置只对动态学习到的 IP 地址和 MAC 地址映射起作用。当一个 ARP 表项超时后，设备会发送单播 ARP 请求报文探测对方是否在线，假如能收到对方的 ARP 应答，则说明对方仍在线，该 ARP 表项不会删除，否则会删除该 ARP 表项。

超时时间设置得越短，ARP 缓冲中保存的映射表就越真实，但是 ARP 消耗网络带宽也越多。

### 📌 ARP 请求重传时间间隔和次数

IP 地址解析成 MAC 地址时连续发送 ARP 请求的时间间隔和次数。时间间隔越短，解析速率更快。次数越多，解析成功率更大，但是 ARP 消耗网络带宽也越多。

### 📌 未解析 ARP 表项的数量限制

在局域网中可能存在对网关的攻击，扫描网段，使网关生成大量未解析的 ARP 表项，从而使网关无法正常学习主机的 MAC 地址。为了防止这种攻击，用户可以配置未解析 ARP 表项的数量限制。

### 📌 接口 ARP 学习数量限制

改成通过配置指定接口的用户 ARP 表项个数，灵活控制 ARP 表项资源的按需分配，防止表项资源浪费。

## 相关配置

### 📌 ARP 超时设置

在接口模式下，使用命令 **arp timeout seconds** 配置 ARP 的超时时间。默认情况下超时时间为 3600 秒，用户可以根据实际情况重新调整。

### 📌 ARP 请求重传时间间隔和次数

- 在全局模式下，使用命令 **arp retry interval seconds** 配置 ARP 的重传时间间隔。默认情况下超时时间为 1 秒，用户可以根据实际情况重新调整。
- 在全局模式下，使用命令 **arp retry times number** 配置 ARP 的重传次数。默认情况下可以连续发送 5 次，用户可以根据实际情况重新调整。

### 📌 未解析 ARP 表项的数量限制

在全局模式下，使用命令 **arp unresolve number** 配置 ARP 的未解析表项数。默认为 arp 容量的最大值，用户可以根据实际情况重新调整。

### 📌 接口 ARP 学习数量限制

在接口模式下，使用命令 **arp cache interface-limit limit** 配置接口 ARP 的学习数量限制。默认不限制接口上 ARP 学习的数量，用户可以根据实际情况重新调整。此数量限制包含静态 ARP。

### 2.3.3 可信任 ARP

#### 工作原理

可信任 ARP 作为一类特殊 ARP，添加在交换机端的 ARP 表中，用于防止 ARP 欺骗。可信任 ARP 同时具有静态 ARP 和动态 ARP 两者的特征，其优先级高于动态 ARP 表项、并且低于静态 ARP 表项。可信任 ARP 具有类似于动态 ARP 的老化机制，在 ARP 老化时主动发送 ARP 请求报文探测主机是否存在，如果主机有应答则代表主机还是活动的，那么就更新 ARP 的老化时间，否则删除 ARP 表项。可信任 ARP 具有静态 ARP 的相关特征，即不会通过学习 ARP 报文动态更新 ARP 表项的 MAC、接口等相关字段。

可信任 ARP 是 GSN 客户端用户认证上线时，认证服务端通过接入交换机获取用户真实的 IP-MAC 关联信息，并根据用户的网关信息，在网关交换机上添加的。该过程对于网络管理员来说是透明的，不会对网络管理员的原有网络管理产生任何影响。

综上所述，因为可信任 ARP 来源真实有效，且不会被 ARP 报文动态更新，所以可以有效的防止针对网关的 ARP 欺骗。

#### 相关配置

##### 配置可信任 ARP 功能

- 全局模式下，使用命令 **service trustedarp** 打开可信任 arp 功能，缺省情况下该功能是关闭的。
- 全局模式下，使用命令 **arp trusted user-vlan vid1 translated-vlan vid2** 实现 VLAN 转换，缺省情况下没有任何 VLAN 转换。如果服务器下发的 VLAN 和可信任 ARP 表项生效的 VLAN 不同，则用户需要配置 VLAN 转换。
- 全局模式下，使用命令 **arp trusted aging** 允许可信任 ARP 老化。缺省情况下可信任 ARP 表项不允许老化。
- 全局模式下，使用命令 **arp trusted number** 设置可信任 ARP 表项的容量。缺省情况下为总容量的一半，用户可以根据实际情况更改容量。

### 2.3.4 免费 ARP

#### 工作原理

免费 ARP 报文是一种特殊的 ARP 报文，该报文的发送端 IP 地址和目标 IP 地址都是本机 IP 地址。免费 ARP 的主要用途有：

1. IP 地址冲突检测。当设备收到免费 ARP 报文后，如果发现报文中的 IP 地址和自己的 IP 地址相同，向发送免费 ARP 报文的设备返回一个 ARP 应答，告诉该设备 IP 地址冲突。
2. 当接口的 MAC 地址变化时，发送免费 ARP 通知其它设备更新 ARP 表项。

设备具有免费 ARP 报文学习功能。当设备收到免费 ARP 报文时，设备判断是否存在和免费 ARP 报文源 IP 地址对应的动态 ARP 表项，如果存在，根据免费 ARP 报文中携带的信息更新 ARP 表项。

#### 相关配置

### 配置免费 ARP

接口模式下，使用命令 **arp gratuitous-send interval seconds [number]** 允许接口定时发送免费 ARP 请求报文。缺省情况下接口上该功能是关闭的。一般在该接口充当下联设备网关时，需要开启这个功能，定时更新使下联设备的网关 mac，防止他人冒充网关。

## 2.3.5 代理 ARP

### 工作原理

设备的代理 ARP 功能可以帮助没有路由信息的主机，获得其它子网 IP 地址的 MAC 地址。比如设备接收到一个 ARP 请求，ARP 请求的发送者 IP 地址与目标 IP 地址不属于同一网段，而设备又知道所请求 IP 地址的路由，设备就会发送 ARP 响应，响应的 MAC 地址为设备自身的以太网 MAC 地址，这个过程就是代理 ARP 的功能。

### 相关配置

#### 配置代理 ARP

- 接口模式下，使用命令 **ip proxy-arp** 开启代理 ARP 功能。
- 缺省情况下路由器上开启了代理 ARP 功能，而交换机上关闭了代理 ARP 功能。

## 2.3.6 本地代理 ARP

### 工作原理

本地 ARP 代理指的是同一个 VLAN 内的代理，这里头的 VLAN 指的是普通 VLAN 或者 Sub VLAN。

设备开启本地代理 ARP 功能后，可以帮助主机获得子网内其他主机的 MAC 地址。比如在设备开启端口保护的情况下，不同端口下的用户被二层隔离，在开启本地 ARP 代理功能后，设备接收到一个 ARP 请求，就会代理发送 ARP 响应，响应的 MAC 地址为设备自身的以太网 MAC 地址，这样不同的主机之间的通信靠三层路由来实现。这个过程就是本地代理 ARP 的功能。

### 相关配置

#### 配置本地代理 ARP

- 接口模式下，使用命令 **local-proxy-arp** 开启本地代理 ARP 功能。
- 缺省情况下关闭本地代理 ARP 功能。
- 该命令只在 SVI 口上支持。

## 2.3.7 ARP 可信检测

### 工作原理

该命令用于防止 arp 欺骗导致无用的 arp 表项过多占用设备资源。在三层接口开启 arp 可信检测功能后，从该接口上收到 arp 请求报文：

1. 如果对应表项不存在，则创建动态 arp 表项，并经过 1 到 5 秒的一个随机时间后进入 NUD（邻居不可达探测），即将新学习的 arp 表项设置为老化状态并单播 arp 请求，在老化时间内收到对端 arp 更新，则保存表项，否则直接删除该表项。
2. 如果对应 arp 表项已经存在，则不进行 NUD 探测逻辑。
3. 如果已有的动态 arp 表项的 MAC 地址被更新，也走 NUD 探测逻辑。

该功能由于在 ARP 学习过程中增加了一个严格确认的过程，所以开启该功能会影响到 ARP 的学习性能。

关闭该功能后，arp 表项的学习和更新不再走 NUD 逻辑。

### 相关配置

#### 配置 ARP 可信检测

接口模式下，使用命令 **arp trust-monitor enable** 命令开启 ARP 可信检查功能，缺省情况下没有开启该功能。

## 2.3.8 ARP 防 IP 报文攻击

### 工作原理

在收到未解析的 IP 报文时，交换机设备不能够进行硬件转发，需要把报文送 CPU 进行地址解析，如果此类报文大量送 CPU，就会对 CPU 造成冲击，影响交换机其它业务的运行。

开启 ARP 防 IP 报文攻击后，在 ARP 请求期间，交换机 CPU 会统计收到的目的 IP 命中该 ARP 表项的报文个数，当这个个数等于配置的个数时，会设置一个丢弃表项到硬件，后续硬件收到所有该目的 IP 的报文都不会送 CPU；在地址解析完成时，更新上述表项为转发状态，使得交换机能够对该目的 IP 的报文进行硬件转发。

### 相关配置

#### 配置 ARP 防 IP 报文攻击

- 全局模式下，使用命令 **arp anti-ip-attack** 配置触发 ARP 丢弃表项的 IP 报文个数。
- 缺省情况下，在 3 个目的 IP 地址相同的未知名单播报文送 CPU 后，就会设置丢弃表项。

## 2.3.9 抑制往认证 VLAN 发送 ARP 请求

### 工作原理

在网关认证模式下，SuperVLAN 下的所有子 VLAN 默认都是认证 VLAN，认证 VLAN 下的认证用户需要在认证后才能上网。用户认证后会在设备上生成静态 ARP 表项，因此设备访问认证用户时，不需要往认证 VLAN 发送 ARP 请求。若设备需要访问免认证 VLAN 下的用户时，只需要往免认证 VLAN 发送 ARP 请求。

在网关认证模式下，设备默认开启了抑制往认证 VLAN 发送 ARP 请求的功能。如果设备需要访问认证 VLAN 下的免认证用户，需要关闭该功能。

### 相关配置

#### 配置抑制往认证 VLAN 发送 ARP 请求

- 接口模式下，使用命令 **arp suppress-auth-vlan-req** 开启抑制往认证 VLAN 发送 ARP 请求功能。
- 缺省情况下开启抑制往认证 VLAN 发送 ARP 请求功能。

## 2.4 配置详解

配置项	配置建议&相关命令	
配置静态 ARP	 可选配置，用于 IP 地址和 MAC 地址的静态绑定。	
	<b>arp</b>	定义静态 ARP
配置 ARP 属性	 可选配置，用于指定 ARP 表项的超时时间、ARP 请求重传次数和间隔、未解析 ARP 表项数上限、接口 ARP 学习数量限制	
	<b>arp timeout</b>	配置 ARP 超时时间
	<b>arp retry interval</b>	配置 ARP 请求重传时间间隔
	<b>arp unresolve</b>	配置未解析 ARP 表项的数量限制
	<b>arp cache interface-limit</b>	配置接口 ARP 学习数量限制
配置可信任 ARP	 可选配置，用于防止 ARP 欺骗。	
	<b>service trustedarp</b>	启用可信任 ARP 功能
	<b>arp trusteduser-vlan</b>	添加可信任 ARP 时进行 VLAN 转换
	<b>arp trusted aging</b>	允许可信任 ARP 老化
	<b>arp trusted</b>	调整可信任 ARP 的容量
配置免费 ARP	 可选配置，用于检测 IP 地址冲突，以及让外围设备更新本机的 ARP。	
	<b>arp gratuitous-send interval</b>	开启定时发送免费 ARP 的功能

配置代理 ARP	 可选配置，用于代理应答请求不同子网内其他设备的 ARP 请求。	
	<b>ip proxy-arp</b>	开启代理 ARP 功能。
配置本地代理 ARP	 可选配置，用于代理应答请求子网内其他设备的 ARP 请求。	
	<b>local-proxy-arp</b>	开启本地代理 ARP 功能。
<a href="#">配置 ARP 可信检测</a>	 可选配置，用于发送单播 ARP 请求确认，以保证学习 ARP 表项正确性。	
	<b>arp trusted-monitor enable</b>	开启 ARP 可信检测功能
配置 ARP 防 IP 报文攻击	 可选配置，防止 IP 报文大量送 CPU 对 CPU 造成冲击。	
	<b>arp anti-ip-attack</b>	配置触发 ARP 设丢弃表项的 IP 报文个数。
配置抑制往认证 VLAN 发送 ARP 请求	 可选配置，用于抑制往认证 VLAN 发送 ARP 请求。	
	<b>arp suppress-auth-vlan-req</b>	开启抑制往认证 VLAN 发 ARP 请求功能。

## 2.4.1 配置静态 ARP

### 配置效果

用户手工指定 IP 地址和 MAC 地址的映射，防止设备学到错误的 ARP 表项而影响网络。

### 注意事项

对于三层交换机，配置完静态 ARP 表项后，交换机必须在学习到该静态 ARP 表项的 MAC 地址对应的物理端口后才能进行正常的三层路由。

### 配置方法

#### 配置静态 ARP

- 可选配置
- 在汇聚设备上，可以通过静态绑定上联设备的 IP 和 MAC 地址的映射，防止设备因受到 ARP 攻击而更改掉上联设备的 ARP 表项的 MAC 地址，导致网络异常。
- 在全局模式下配置

### 检验方法

使用命令 **show running-config** 查看命令是否生效，或使用命令 **show arp static** 查看是否成功创建了静态 ARP 缓存表。

### 相关命令

## 配置静态 ARP

【命令格式】 **arp** [vrf name | oob] ip-address mac-address type

【参数说明】 **vrf name**：指定 VRF 实例，name 参数是 VRF 实例的名称。

**oob**：为 MGMT 口配置静态 ARP。

**ip-address**：与 MAC 地址对应的 IP 地址，分为四组十进制表示的数值，组之间用点隔开。

**mac-address**：数据链路层地址，48 个比特位组成。

**type**：ARP 封装类型。对于以太网接口，关键字为 arpa。

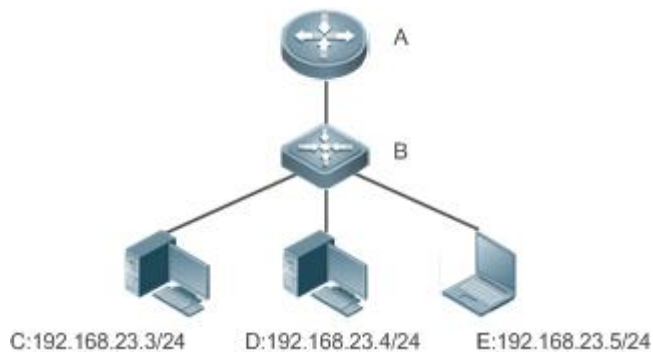
【命令模式】 全局模式

【使用指导】 RGOS 使用 ARP 缓冲表，根据 32 个比特位 IP 地址查找 48 个比特位的 MAC 地址。

由于大多数主机支持动态 ARP 解析，所以通常不需要配置静态 ARP 映射。利用 **clear arp-cache** 命令可以删除动态学习到的 ARP 映射。

## 配置举例

【网络环境】



【注释】 A 为路由器

B 为交换机，作为用户主机网段的网关。

C、D、E 为用户主机

【配置方法】 在设备 B 上配置静态 ARP 表项，静态绑定设备 A 的 IP 和 MAC 地址映射。

```
Ruijie(config)#arp 192.168.23.1 00D0.F822.334B arpa
```

【检验方法】 通过 **show arp static** 命令可查看静态 ARP 表项：

```
Ruijie(config)#show arp static
```

Protocol	Address	Age(min)	Hardware	Type	Interface
Internet	192.168.23.1<static>	00D0.F822.334B	arpa		

1 static arp entries exist.

## 常见配置错误

- 静态绑定的 MAC 地址错误。

## 2.4.2 配置 ARP 属性

### 配置效果

---

用户指定 ARP 表项的超时时间、ARP 请求重传次数和间隔、未解析 ARP 表项数上限、接口 ARP 学习数量限制、单板 ARP 学习数量限制。

### 注意事项

---

无

### 配置方法

---

#### 📄 ARP 超时设置

- 可选配置
- 局域网中如果用户上下线较频繁，则可以将 ARP 超时时间设置小一点，可以将无效的 ARP 表项尽早删除。
- 在接口模式下配置

#### 📄 ARP 请求重传时间间隔和次数

- 可选配置
- 在网络带宽资源不足时，可以将重传时间间隔配大，次数配小，以减少网络带宽的消耗。
- 在全局模式下配置

#### 📄 未解析 ARP 表项的数量限制

- 可选配置
- 在网络带宽资源不足时，可以将未解析 ARP 表项的数量配小，以减少网络带宽的消耗。
- 在全局模式下配置

#### 📄 接口 ARP 学习数量限制

- 可选配置
- 在接口模式下配置

### 检验方法

---

使用命令 **show arp timeout** 可以查看所有接口的老化超时时间。

使用命令 **show running-config** 查看 ARP 请求重传时间间隔和次数、未解析 ARP 表项是数量限制、接口 ARP 学习数量限制、单板 ARP 学习数量限制命令是否生效。



## 相关命令

---

### ▾ ARP 超时设置

- 【命令格式】 **arp timeout seconds**
- 【参数说明】 *seconds*：超时时间，以秒为计算单位，默认值为 3600，范围 0-2147483。
- 【命令模式】 接口模式
- 【使用指导】 ARP 超时设置只对动态学习到的 IP 地址和 MAC 地址映射起作用。超时时间设置得越短，ARP 缓存中保存的映射表就越真实，但是 ARP 消耗网络带宽也越多，所以需要权衡利弊。除非有特别的需要，否则一般不需要配置 ARP 超时时间。

### ▾ ARP 请求重传时间间隔和次数

- 【命令格式】 **arp retry interval seconds**
- 【参数说明】 *seconds*：<1-3600>，ARP 请求的重传时间可以设置为 1~3600 秒，默认值为 1 秒。
- 【配置模式】 全局模式
- 【使用指导】 当发现本设备有频繁的向外发送 ARP 请求，引起网络繁忙等其它问题时，可以将 ARP 请求的重传时间设置长一点，一般不要超过动态 ARP 表项的老化时间。

### ▾ 未解析 ARP 表项的数量限制

- 【命令格式】 **arp unresolve number**
- 【参数说明】 *number*：未解析 ARP 表项的最大个数，取值范围为< 1-8192>。默认值为 8192。
- 【配置模式】 全局模式
- 【使用指导】 当发现 ARP 缓存表中出现大量未解析表项，并且一段时间后还没有消失时，可以用此命令限制未解析表项的个数。

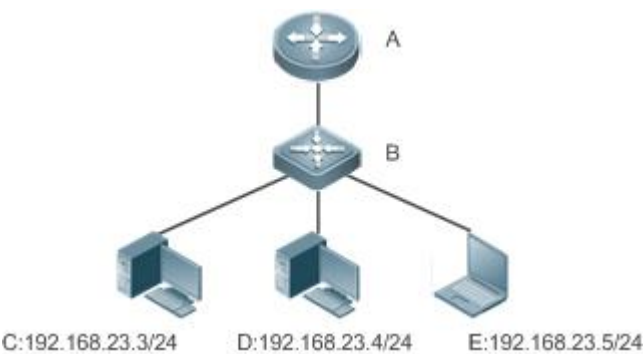
### ▾ 接口 ARP 学习数量限制

- 【命令格式】 **arp cache interface-limit limit**
- 【参数说明】 *limit*：指定接口所能学习的 ARP 数量最大限制，包括静态配置和动态学习的 ARP，取值范围为 0-设备支持的 ARP 表项容量，0 表示不限制接口 ARP 学习数量。
- 【配置模式】 接口模式
- 【使用指导】 限制接口的 ARP 学习数量，可防止恶意的 ARP 攻击，让设备生成大量的 ARP 表项，占用过多的表项资源。配置的值必须不小于当前接口已经学习到的 ARP 表项数量，否则配置不生效。该限制受限于设备支持的 ARP 容量。

## 配置举例

---

【网络环境】



【注释】 A 为路由器  
B 为交换机，作为用户主机网段的网关。  
C、D、E 为用户主机

【配置方法】

- 配置接口 GigabitEthernet 0/1 下的 ARP 超时时间为 60 秒
- 配置接口 GigabitEthernet 0/1 下的 ARP 学习数量限制为 300
- 配置 ARP 请求重传时间间隔为 3 秒
- 配置 ARP 请求重传次数为 4 次
- 配置未解析 ARP 表项数量限制为 4096
- 配置 slot 1 subslot 2 的 ARP 学习数量限制为 1000

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#arp timeout 60
Ruijie(config-if-GigabitEthernet 0/1)#arp cache interface-limit 300
Ruijie(config-if-GigabitEthernet 0/1)#exit
Ruijie(config)#arp retry interval 3
Ruijie(config)#arp retry times 4
Ruijie(config)#arp unresolve 4096
```

【检验方法】

- 通过 **show arp timeout** 查看接口的老化时间
- 通过 **show running-config** 查看 ARP 请求重传时间间隔和次数、未解析 ARP 表项是数量限制、接口 ARP 学习数量限制

```
Ruijie#show arp timeout
Interface                arp timeout(sec)
-----
GigabitEthernet 0/1      60
GigabitEthernet 0/2      3600
GigabitEthernet 0/4      3600
GigabitEthernet 0/5      3600
GigabitEthernet 0/7      3600
VLAN 100                 3600
VLAN 111                 3600
Mgmt 0                   3600

Ruijie(config)# show running-config
```

```
arp unresolve 4096
arp retry times 4
arp retry interval 3
!
interface GigabitEthernet 0/1
 arp cache interface-limit 300
```

## 常见配置错误

---

无

## 2.4.3 配置可信任 ARP

### 配置效果

---

可以有效的防止针对网关的 ARP 欺骗。

### 注意事项

---

可信任 ARP 只在交换机上支持。

### 配置方法

---

- 如果需要部署 GSN 方案，则应该执行此配置项。
- 部署 GSN 全局安全网络解决方案时，需要配置开启可信任 ARP 功能。
- 在全局模式下配置

### 检验方法

---

使用 **show arp trusted** 命令查看可信 ARP 表项；

使用 **show running** 命令查看可信任 ARP 的相关配置是否生效。

### 相关命令

---

#### 📌 启用可信任 ARP 功能

- 【命令格式】 **service trustedarp**
- 【参数说明】 -
- 【命令模式】 全局模式

【使用指导】 设备的可信任 ARP 功能是一种防止 ARP 欺骗的功能，作为 GSN 方案的一部分，需要和 GSN 方案一起使用。

#### 添加可信任 ARP 时进行 VLAN 转换

【命令格式】 **arp trusted user-vlan *vid1* translated-vlan *vid2***

【参数说明】 *vid1*：服务器设置的 VID

*vid2*：转换后的 VID

【配置模式】 全局模式

【使用指导】 要使此命令生效，首先启用可信任 ARP 功能。只有在服务器下发的 VLAN 和可信任 ARP 生效的 VLAN 不同时，才需要配置此命令。

#### 查看交换机上的可信任 ARP

【命令格式】 **show arp trusted [*ip* [*mask*]]**

【参数说明】 *ip*：IP 地址，显示指定 IP 地址的 ARP 表项；如果指定 **trusted** 关键字，则只显示可信任 ARP 表项，否则显示非可信任 ARP 表项。

*mask*：显示 IP 子网内的 ARP 表项；如果指定 **trusted** 关键字，则只显示可信任 ARP 表项，否则显示非可信任 ARP 表项。

【配置模式】 特权模式

【使用指导】 -

#### 删除交换机上的可信任 ARP

【命令格式】 **clear arp trusted [*ip* [*mask*]]**

【参数说明】 *ip*：IP 地址，显示指定 IP 地址的 ARP 表项；如果指定 **trusted** 关键字，则只显示可信任 ARP 表项，否则显示非可信任 ARP 表项。

*mask*：显示 IP 子网内的 ARP 表项；如果指定 **trusted** 关键字，则只显示可信任 ARP 表项，否则显示非可信任 ARP 表项。

【配置模式】 特权模式

【使用指导】 执行 **clear arp trusted** 会删除交换机上的所有的可信 ARP，可能导致用户不能上网。  
一般情况下使用 **clear arp trusted *ip*** 删除指定的可信任 ARP 表项。

#### 允许可信任 ARP 老化

【命令格式】 **arp trusted aging**

【参数说明】 -

【配置模式】 全局模式

【使用指导】 使用该命令后可信任 ARP 开始老化，老化时间和动态 ARP 老化时间相同。老化时间可以通过接口模式下 **arp timeout** 命令设置。

#### 调整可信任 ARP 的容量

【命令格式】 **arp trusted *number***

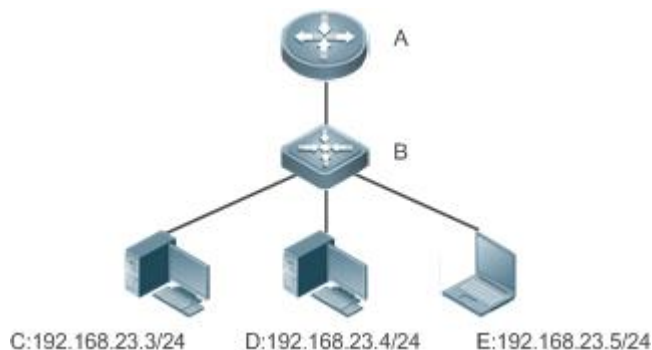
【参数说明】 *number*：取值范围最小为 10，最大为对应产品 arp 容量减去 1024，缺省可信 arp 的最大表项数为 arp 总容量的一半。

【配置模式】 全局模式

【使用指导】 要使此命令生效，首先启用可信任 ARP 功能。可信任 ARP 表项和其它表项共享内存，如果可信任表项占用过多，可能导致动态 ARP 表项空间不够。一般按需设置，不要设置得太大。

## 配置举例

### 【网络环境】



【注释】 A 为路由器  
B 为交换机，作为用户主机网段的网关。  
C、D、E 为用户主机

### 【配置方法】

- 开启可信任 ARP 功能
- 配置 VLAN 转换
- 配置可信任 ARP 表项运行老化
- 配置可信任 ARP 表项的容量为 1024

```
Ruijie(config)#service trustedarp
Ruijie(config)#arp trusted user-vlan 2-9 translated-vlan 10
Ruijie(config)#arp trusted aging
Ruijie(config)#arp trusted 1024
```

### 【检验方法】

- 通过 **show running-config** 查看上面的配置是否生效

```
Ruijie(config)# show running-config
service trustedarp
arp trusted user-vlan 2-9 translated-vlan 10
arp trusted aging
arp trusted 1024
```

## 常见配置错误

- 可信任 ARP 功能未开启，导致 ARP 表项下发失败

## 2.4.4 配置免费 ARP

## 配置效果

接口定时发送免费 ARP 报文。

## 注意事项

无

## 配置方法

- 可选配置
- 设备做用户网关时，为了防止因为 ARP 欺骗导致其他用户学习到错误的网关 MAC 后会一直上不了网，需要在接口上开启免费 ARP 功能。
- 在接口模式下配置

## 检验方法

使用 **show running-config interface [name]** 查看是否配置成功。

## 相关命令

### 📌 开启定时发送免费 ARP 的功能

【命令格式】 **arp gratuitous-send interval seconds [number]**

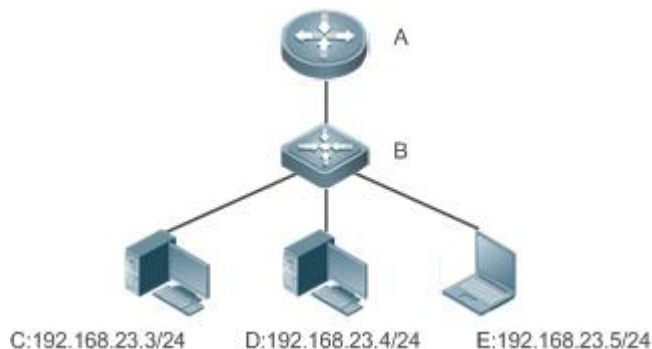
【参数说明】 *seconds*：发送免费 ARP 请求的时间间隔，单位秒，取值范围<1-3600>。  
*number*：发送免费 ARP 请求的数量，缺省值是 1，取值范围<1-100>。

【命令模式】 接口模式

【使用指导】 当设备的网络接口作为下联设备的网关时，如果下联设备中有冒充网关的行为，则可以在此接口配置定时发送免费 ARP 请求，公告自己才是真正的网关。

## 配置举例

【网络环境】



【注释】 A 为路由器

B 为交换机，作为用户主机网段的网关。

C、D、E 为用户主机

【配置方法】 配置 GigabitEthernet 0/0 口发送免费 ARP 功能，频率为每 5 秒发送一个免费 ARP 请求报文。

```
Ruijie(config-if-GigabitEthernet 0/0)#arp gratuitous-send interval 5
```

【检验方法】 使用 **show running-config interface** 命令查看配置是否生效

```
Ruijie#sh running-config interface gigabitEthernet 0/0
```

```
Building configuration...
Current configuration : 127 bytes
!
interface GigabitEthernet 0/0
 duplex auto
 speed auto
 ip address 30.1.1.1 255.255.255.0
 arp gratuitous-send interval 5
```

## 常见配置错误

无

## 2.4.5 配置代理 ARP

### 配置效果

设备代理应答非本机的 ARP 请求报文。

### 注意事项

三层交换机缺省关闭代理 ARP 功能，路由器缺省开启代理 ARP 功能。

### 配置方法

- 可选配置。
- 没有路由信息的主机需要获得其它子网 IP 地址的 MAC 地址，设备需要开启代理 ARP 功能，代理应答 ARP。
- 在接口模式下配置

### 检验方法

使用 **show ip interface [name]**命令查看是否配置成功。

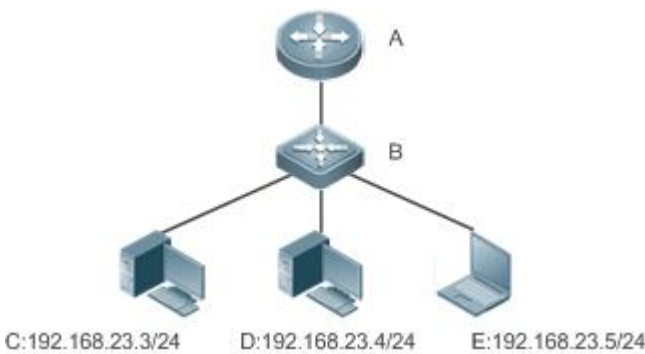
相关命令

开启代理 ARP 功能

- 【命令格式】 `ip proxy-arp`
- 【参数说明】 -
- 【命令模式】 接口模式
- 【使用指导】 -

配置举例

【网络环境】



【注释】 A 为路由器  
B 为交换机，作为用户主机网段的网关。  
C、D、E 为用户主机

【配置方法】 配置 GigabitEthernet 0/0 口开启代理 ARP 功能  
Ruijie(config-if-GigabitEthernet 0/0)#ip proxy-arp

【检验方法】 使用 **show ip interface** 命令查看是否配置成功  
Ruijie#show ip interface gigabitEthernet 0/0  
GigabitEthernet 0/0  
IP interface state is: DOWN  
IP interface type is: BROADCAST  
IP interface MTU is: 1500  
IP address is:  
No address configured  
IP address negotiate is: OFF  
Forward direct-broadcast is: OFF  
ICMP mask reply is: ON  
Send ICMP redirect is: ON  
Send ICMP unreachable is: ON  
DHCP relay is: OFF  
Fast switch is: ON



```
Help address is: 0.0.0.0
Proxy ARP is: ON
ARP packet input number: 0
  Request packet      : 0
  Reply packet       : 0
  Unknown packet     : 0
TTL invalid packet number: 0
ICMP packet input number: 0
  Echo request       : 0
  Echo reply        : 0
  Unreachable       : 0
  Source quench     : 0
  Routing redirect  : 0
```

## 常见配置错误

---

无

## 2.4.6 配置本地代理 ARP

### 配置效果

---

设备代理应答子网内非本机的 ARP 请求报文。

### 注意事项

---

只在 SVI 口下支持。

### 配置方法

---

- 可选配置。
- 在开启端口保护时，如果有需要 VLAN 内的主机通信，则需要配置本地 ARP 代理。
- 在接口模式下配置

### 检验方法

---

使用 **show run interface [name]** 命令查看是否配置成功。

### 相关命令

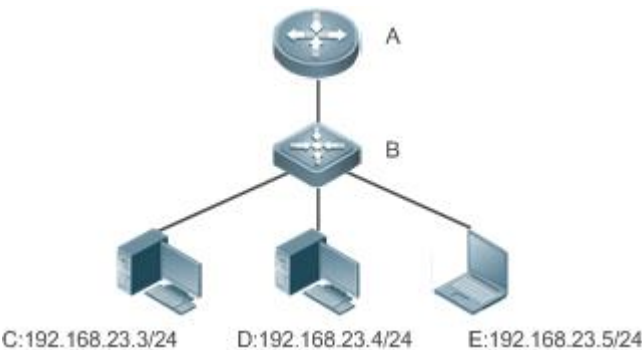
---

开启本地代理 ARP 功能

- 【命令格式】 local-proxy-arp
- 【参数说明】 -
- 【命令模式】 接口模式
- 【使用指导】 -

配置举例

【网络环境】



- 【注释】 A 为路由器
- B 为交换机，作为用户主机网段的网关。
- C、D、E 为用户主机

【配置方法】 配置 VLAN 1 口开启代理 ARP 功能

```
Ruijie(config-if-VLAN1)#local-proxy-arp
```

【检验方法】 使用 show ip interface 命令查看是否配置成功

```
Ruijie#show running-config interface vlan 1

Building configuration...
Current configuration : 53 bytes

interface VLAN 1
ip address 192.168.1.2 255.255.255.0
local-proxy-arp
```

常见配置错误

无

## 2.4.7 配置 ARP 可信检测

### 配置效果

开启 arp 可信检测功能，在收到 arp 请求报文后，如果对应表项不存在，进入 NUD（邻居不可达探测）。如果已有的动态 arp 表项的 MAC 地址被更新，马上走 NUD 探测逻辑，起到防止 arp 攻击的作用。

### 注意事项

该功能由于在 ARP 学习过程中增加了一个严格确认的过程，所以开启该功能会影响到 ARP 的学习性能。

### 配置方法

- 可选配置。
- 如果有要求严格学习 ARP 表项的需求时，设备上可以开启 arp 可信功能，设备在收到 arp 请求报文后，如果之前不存在对应 arp 表项，则需要发送单播 ARP 请求报文，在确认对端真实存在后才学习 ARP 表项，否则不学习 ARP 表项。在 arp 表项的 mac 地址发生了变化后，马上走 NUD 探测，防止 arp 欺骗。
- 在接口模式下配置

### 检验方法

使用 **show running-config interface [name]** 查看是否配置成功。

### 相关命令

#### 🔽 开启 ARP 可信检测功能

【命令格式】 **arp trust-monitor enable**

【参数说明】 -

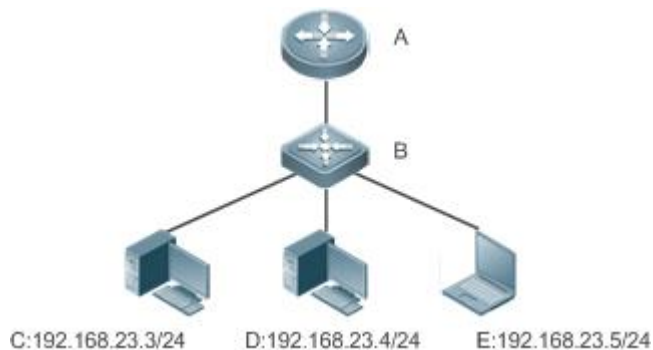
【命令模式】 接口模式

【使用指导】

- ❗ 开启该功能，如果对应 arp 表项已经存在，且 mac 地址没发生更新，则不进行 NUD 探测逻辑。
- ❗ 开启该功能，如果已有的动态 arp 表项的 mac 地址被更新，则马上走 NUD 探测逻辑。
- ❗ 关闭该功能后，arp 表项的学习和更新不需要 NUD 过程。

### 配置举例

## 【网络环境】



【注释】 A 为路由器  
B 为交换机，作为用户主机网段的网关。  
C、D、E 为用户主机

【配置方法】 配置 GigabitEthernet 0/0 口开启 ARP 可信检测功能

```
Ruijie(config-if-GigabitEthernet 0/0)#arp trust-monitor enable
```

【检验方法】 使用 **show running-config interface** 查看是否配置是否生效

```
Ruijie#show running-config interface gigabitEthernet 0/0
```

```
Building configuration...
Current configuration : 184 bytes
!
interface GigabitEthernet 0/0
 duplex auto
 speed auto
 ip address 30.1.1.1 255.255.255.0
 arp trust-monitor enable
```

## 常见配置错误

无

## 2.4.8 配置 ARP 防 IP 报文攻击

### 配置效果

交换机 CPU 收到配置个数的目的 IP 命中该 ARP 表项的报文时，后续所有该目的 IP 的报文都不会送 CPU。

### 注意事项

只在交换机产品上支持。

## 配置方法

- 可选配置。
- 在交换机产品上，默认情况下，在 3 个未知名单播报文送 CPU 后设置丢弃表项。通过此命令用户可以针对具体网络环境调整这个参数，也可以关闭该功能。
- 在全局模式下配置。

## 检验方法

使用 **show run** 命令查看是否配置成功。

## 相关命令

### 配置 ARP 防 IP 报文攻击

【命令格式】 **arp anti-ip-attack num**

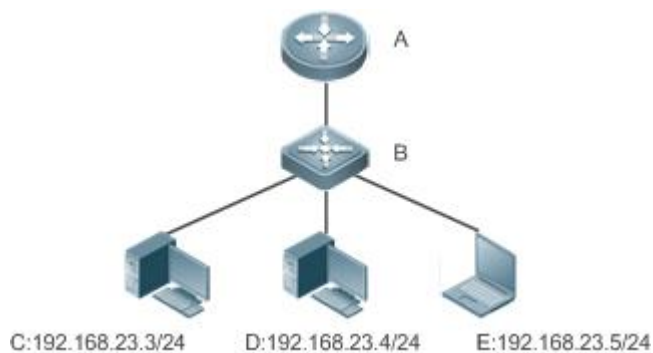
【参数说明】 num：设置触发 ARP 设丢弃表项的 IP 报文个数，取值范围<0-100>。  
0 表示关闭 ARP 防 IP 报文攻击功能。缺省值为 3。

【命令模式】 全局模式

【使用指导】  如果硬件路由资源比较充分，**arp anti-ip-attack num** 可以设置得小一些。在硬件路由资源比较紧张的情况下，要优先满足正常路由的使用，可以将 **arp anti-ip-attack num** 设置得比较大，或者关闭该功能。

## 配置举例

### 【网络环境】



【注释】 A 为路由器  
B 为交换机，作为用户主机网段的网关。  
C、D、E 为用户主机

【配置方法】 在设备 B 上配置 ARP 防 IP 报文攻击。

```
Ruijie(config)#arp anti-ip-attack 10
```

【检验方法】 使用 **show running-config** 查看配置是否生效

```
Ruijie#show running-config

Building configuration...

Current configuration : 53 bytes
arp anti-ip-attack 10
```

## 常见配置错误

---

无

## 2.4.9 配置抑制往认证 VLAN 发送 ARP 请求

### 配置效果

---

设备不往认证 VLAN 发送 ARP 请求报文。

### 注意事项

---

只在 SVI 口下支持。

### 配置方法

---

- 可选配置。
- 在开启网关认证模式下，设备默认不往认证 VLAN 发送 ARP 请求报文。若需要往认证 VLAN 发送 ARP 请求，使用该命令的 no 形式取消该功能。
- 在接口模式下配置

### 检验方法

---

使用 **show run interface [name]**命令查看是否配置成功。

### 相关命令

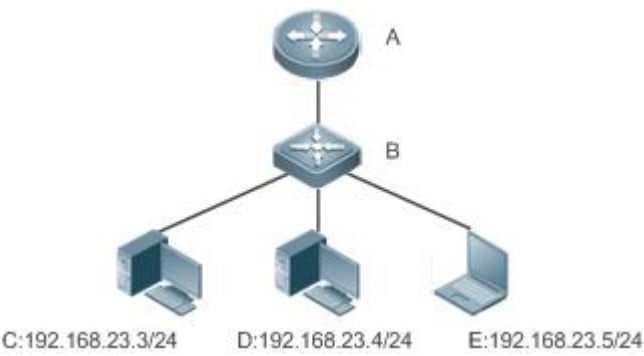
---

#### 🔗 抑制往认证 VLAN 发送 ARP 请求

- 【命令格式】 **arp suppress-auth-vlan-req**
- 【参数说明】 -
- 【命令模式】 接口模式
- 【使用指导】 -

配置举例

【网络环境】



【注释】 A 为路由器  
B 为交换机，作为用户主机网段的网关。  
C、D、E 为用户主机

【配置方法】 配置 VLAN 2 口关闭抑制往认证 VLAN 发送 ARP 请求的功能。  
Ruijie(config-if-VLAN2)#no arp suppress-auth-vlan-req

【检验方法】 使用 **show running-config interface [name]**查看配置是否生效

```
Ruijie#show running-config interface vlan 2

Building configuration...
Current configuration : 53 bytes

interface VLAN 2
ip address 192.168.1.2 255.255.255.0
no arp suppress-auth-vlan-req
```

常见配置错误

无

2.5 监视与维护

清除各类信息

在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。


作用	命令
----	----

清除动态 ARP 表项。在网关认证模式下，不会删除认证 VLAN 下的动态 ARP 表项。	<b>clear arp-cache</b>
---	------------------------

## 查看运行情况

作用	命令
显示 ARP 表。	<b>show arp</b> [detail][ <i>interface-type interface-number</i> ][ <b>vrf</b> <i>vrf-name</i> ] [ <i>ip [mask]   mac-address   static   complete   incomplete</i> ]    <b>subvlan</b> { <i>subvlan-number</i>   <b>min-max min_value max_value</b> }
显示 ARP 表	<b>show ip arp</b> [ <i>vrf vrf-name</i> ]
显示可信任 ARP 表	<b>show arp</b> [detail] <b>trusted</b> [ <i>ip [mask]</i> ]
显示 ARP 表项相应计数	<b>show arp counter</b>
显示动态 ARP 表项的老化时间	<b>show arp timeout</b>

## 查看调试信息

 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
显示 ARP 报文的收发情况	<b>debug arp</b>
显示 ARP 表项的创建删除情况	<b>debug arp event</b>



## 3 IPv6

### 3.1 概述

随着 Internet 的迅速增长以及 IPv4 地址空间的逐渐耗尽,IPv4 的局限性就越来越明显。对新一代互联网络协议( Internet Protocol Next Generation - IPng ) 的研究和实践已经成为热点, Internet 工程任务工作小组(IETF)的 IPng 工作组确定了 IPng 的协议规范,并称之为"IP 版本 6" ( IPv6 ),该协议的规范在 RFC2460 中有详细的描述。

#### IPv6 的主要特点

---

##### ➤ 更大的地址空间

地址长度由 IPv4 的 32 位扩展到 128 位,约有  $2^{128}$  个地址,IPv6 采用分级地址模式,支持从 Internet 核心主干网到企业内部子网等多级子网地址分配方式。

##### ➤ 简化了报头格式

新 IPv6 报文头的设计原则是力图将报文头开销降到最低,因此将一些非关键性字段和可选字段从报文头中移出,放到扩展的报文头中,虽然 IPv6 地址长度是 IPv4 的四倍,但报头仅为基本 IPv4 首部的两倍。改进的 IPv6 报文头在设备转发时拥有更高的效率,例如 IPv6 报文头中没有校验和,IPv6 设备在转发中不需要去处理分片(分片由发起者完成)。

##### ➤ 高效的层次寻址及路由结构

IPv6 采用聚合机制,定义非常灵活的层次寻址及路由结构,同一层次上的多个网络在上层设备中表示为一个统一的网络前缀,这样可以显著减少设备必须维护的路由表项,这也大大降低了设备的选路和存储开销。

##### ➤ 简单的管理:即插即用

通过实现一系列的自动发现和自动配置功能,简化网络节点的管理和维护。比如邻接节点发现( Neighbor Discovery )、最大传输单元发现( MTU Discovery )、路由器通告( Router Advertisement )、路由器请求( Router Solicitation )、节点自动配置( Auto-configuration )等技术就为即插即用提供了相关的服务。特别要提到的是 IPv6 支持全状态和无状态两种地址配置方式,在 IPv4 中,动态主机配置协议 DHCP 实现了主机 IP 地址及其相关配置的自动设置,IPv6 承继 IPv4 的这种自动配置服务,并将其称为全状态自动配置(Stateful Autoconfiguration)(参见 DHCPv6)。除了全状态自动配置,IPv6 还采用了一种被称为无状态自动配置( Stateless Autoconfiguration )的自动配置服务。在无状态自动配置过程中,主机自动获得链路本地地址、本地设备的地址前缀以及其它一些相关的配置信息。

##### ➤ 安全性

IPSec 是 IPv4 的一个可选扩展协议,但是在 IPv6 中它是 IPv6 的一个组成部分,用于提供 IPv6 的安全性。目前,IPv6 实现了认证头( Authentication Header, AH )和封装安全载荷( Encapsulated Security Payload, ESP )两种机制。前者实现数据的完整性及对 IP 包来源的认证,保证分组确实来自源地址所标记的节点;后者提供数据加密功能,实现端到端的加密。

##### ➤ 更好的 QoS 支持

IPv6 包头的新字段定义了数据流如何识别和处理。IPv6 包头中的流标识 ( Flow Label ) 字段用于识别数据流身份 , 利用该字段 , IPv6 允许用户对通信质量提出要求。设备可以根据该字段标识出同属于某一特定数据流的所有包 , 并按需对这些包提供特定的处理。

用于邻居节点交互的新协议

IPv6 的邻居发现协议 ( Neighbor Discovery Protocol ) 使用一系列 IPv6 控制信息报文 ( ICMPv6 ) 来实现相邻节点 ( 同一链路上的节点 ) 的交互管理。邻居发现协议以及高效的组播和单播邻居发现报文替代了以往基于广播的地址解析协议 ARP、ICMPv4 路由器发现等报文。

可扩展性

IPv6 特性具有很强的可扩展性 , 新特性可以添加在 IPv6 包头之后的扩展包头中。不像 IPv4 , 包头最多只能支持 40 字节的可选项 , IPv6 扩展包头的大小仅受到整个 IPv6 包最大字节数的限制。

协议规范

- RFC4291 - IPVersion6AddressingArchitecture.
- RFC2460 - Internet Protocol, Version 6 (IPv6) Specification
- RFC4443 - Internet Control Message Protocol (ICMPv6)for the Internet Protocol Version 6 (IPv6) Specification
- RFC4861 - Neighbor Discovery for IP version 6 (IPv6)
- RFC4862 - IPv6 Stateless Address Autoconfiguration
- RFC5059 - Deprecation of Type 0 Routing Headers in IPv6

3.2 典型应用

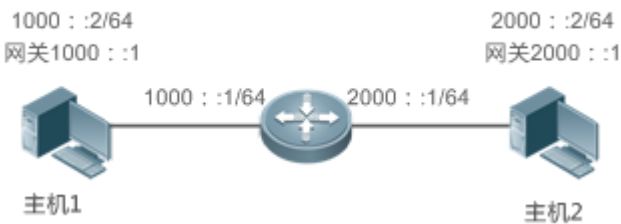
典型应用	场景描述
IPv6 地址通讯	两台 PC 使用 IPv6 地址进行通信

3.2.1 IPv6 地址通讯

应用场景

如下图所示 , 主机 1 和主机 2 可以通过 IPv6 地址进行通信。

图 3-1



### 功能部属

主机可以使用无状态地址自动配置也可以使用 DHCPv6 分配地址，配置完地址后，即可以使用 IPv6 地址进行通讯。

## 3.3 功能详解

### 功能特性

功能特性	作用
IPv6 地址格式	IPv6 的地址格式使其具有更大的地址空间，及灵活的表示方法。
IPv6 地址类型	IPv6 通过地址标识来区分其网络应用。
IPv6 包头结构	IPv6 通过简化固定报头、扩展选项报头，提高了设备处理数据包的速度，也提高了其转发性能。
<a href="#">IPv6 路径 MTU 发现</a>	主机动态的发现并调整发送数据路径上的 MTU 的大小，节省了路由器的资源，提高了 IPv6 网络的效率。
IPv6 邻居发现	完成路由器发现、前缀发现、参数发现、地址自动配置、地址解析（相当于 ARP）、确定下一跳、邻居不可达检测、地址冲突检测和重定向。
IPv6 源路由	用来指定报文经过哪些中间节点到达目的地址，类似于 IPv4 的宽松源路由选项和宽松记录路。
控制 ICMPv6 差错报文的发送速率	防止拒绝服务攻击。
IPv6 HOP-LIMIT	防止无用的单播报文在网络上无限传播下去，浪费网络带宽
抑制往认证 vlan 发送广播 NS 报文	网关认证模式下，设备抑制往认证 VLAN 发送广播 NS 请求的功能
MGMT 口支持缺省网关	给 MGMT 口配置缺省网关，为 MGMT 口生成一条默认路由

### 3.3.1 IPv6 地址格式

IPv6 地址格式 IPv6 地址的基本表达方式是 X:X:X:X:X:X:X:X，其中 X 是一个 4 位十六进制整数(16 位)。每一个数字包含 4 个比特，每个整数包含 4 个十六进制数字，每个地址包括 8 个整数，一共 128 位。下面是一些合法的 IPv6 地址：

2001:ABCD:1234:5678:AAAA:BBBB:1200:2100

800:0:0:0:0:0:0:1

1080:0:0:0:8:800:200C:417A

这些整数是十六进制整数，其中 A 到 F 表示的是 10 到 15。地址中的每个整数都必须表示出来，但起始的 0 可以不必表示。某些 IPv6 地址中可能包含一长串的 0 (就像上面的第二和第三个例子一样)。当出现这种情况时，允许用“::”来表示这一长串的 0。即地址 800:0:0:0:0:0:0:1 可以被表示为：800::1

这两个冒号表示该地址可以扩展到一个完整的 128 位地址。在这种方法中，只有当 16 位组全部为 0 时才会被两个冒号取代，且两个冒号在地址中只能出现一次。

在 IPv4 和 IPv6 的混合环境中还有一种混合的表示方法。IPv6 地址中的最低 32 位可以用于表示 IPv4 地址，该地址可以按照一种混合方式表达，即 X:X:X:X:X:X:d.d.d.d，其中 X 表示一个 16 位整数，而 d 表示一个 8 位的十进制整数。例如，地址 0:0:0:0:0:0:192.168.20.1 就是一个合法的 IPv6 地址。使用简写的表达方式后，该地址也可以表示为 ::192.168.20.1。典型代表是 IPv4 兼容 IPv6 地址和 IPv4 映射 IPv6 地址，IPv4 兼容 IPv6 地址前 96 比特是 0，表示法为 “::A.B.C.D”，例如 “::1.1.1.1”，目前 IPv4 兼容地址已被废除；IPv4 映射 IPv6 地址表示法为 “::FFFF:A.B.C.D”，用于把 IPv4 地址表示为 IPv6 地址，如把 IPv4 地址 “1.1.1.1” 映射到 IPv6 地址 “::FFFF:1.1.1.1”。

由于 IPv6 地址被分成两个部分：子网前缀和接口标识符，因此可以按照类似 CIDR 地址的方式被表示为一个带额外数值的地址，其中该数值指出了地址中有多少位是代表网络部分(网络前缀)，即 IPv6 节点地址中指出了前缀长度，该长度与 IPv6 地址间以斜杠区分，例如：12AB::CD30:0:0:0/60，这个地址中用于选路的前缀长度为 60 位。

## 相关配置

### 配置 IPv6 地址

- 缺省情况接口没有配置 IPv6 地址。
- 可通过 **ipv6 address** 命令配置接口 IPv6 地址。
- 配置后根据冲突检测即可使用该 IPv6 地址进行通信。

### 3.3.2 IPv6 地址类型

RFC4291 定义了三种 IPv6 地址类型：

- 单播(Unicast)：单个接口的标识符。送往一个单播地址的包将被传送至该地址标识的接口上。
- 组播(Multicast)：一组接口(一般属于不同节点)的标识符。送往一个组播地址的包将被传送至加入该组播地址的所有接口上。
- 泛播(Anycast)：一组接口的标识符。送往一个泛播地址的包将被传送至该地址标识的接口之一(根据选路协议选择“最近”的一个)。



在 IPv6 中已经没有定义广播地址。

下面逐一介绍这几类地址：

#### 单播地址 ( Unicast Addresses )

单播地址分为未指定地址、环回地址、链路本地地址、站点本地地址和全球单播地址。目前，站点本地地址被废除了，除了未指定地址、环回地址和链路本地地址以外的单播地址，都是全球单播地址。

- 未指定地址

未指定地址是 0:0:0:0:0:0:0:0，通常简写为::，常见的两个用途是：

3. 若主机启动时没有单播地址，则以未指定地址作为源地址，发送路由器请求，从网关获取前缀信息，从而自动生成单播地址。
4. 给主机配置 IPv6 地址时，检测地址是否和同网段其它主机的地址冲突，则以未指定地址作为源地址发送邻居请求（相当于免费 ARP）。

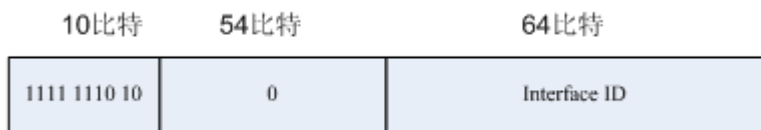
- 环回地址

环回地址是 0:0:0:0:0:0:0:1，通常简写为::1，相当于 IPv4 地址 127.0.0.1，一般在节点给自身发报文时使用。

- 链路本地地址

链路本地地址的格式如下：

图 3-2

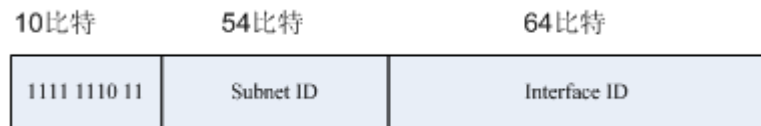


链路本地地址用于单个网络链路上给主机编号。前缀的前 10 位标识的地址即链路本地地址。设备永远不会转发源地址或者目的地址带有链路本地地址的报文。该地址的中间 54 位置成 0。后 64 位表示接口标识符，地址空间的这部分允许单个网络连接多达（2 的 64 次方减 1）个主机。

- 站点本地地址

站点本地地址的格式如下：

图 3-3



站点本地地址可以用在站点内传送数据，设备不会将源地址或者目的地址带有站点本地地址的报文转发到 Internet 上，即这样的包只能在站点内转发，而不能把包转发到站点外去。站点可以理解为一个公司的局域网，这种地址类似于 IPv4 的私有地址，如 192.168.0.0/16。RFC3879 已经废除了站点本地地址。对于新的实现，不再支持该前缀，统一视为全球单播地址；对于已经实现和部署的，可以继续用这个前缀。

- 全球单播地址

全球单播地址格式如下：

图 3-4



全球单播地址中有一类地址是嵌入 IPv4 地址的 IPv6 地址，用于 IPv4 节点和 IPv6 节点互通，分为 IPv4 兼容 IPv6 地址和 IPv4 映射 IPv6 地址两种。

IPv4 兼容 IPv6 地址格式（IPv4-compatible IPv6 address）

图 3-5



IPv4 映射 IPv6 地址格式（IPv4-mapped IPv6 address）

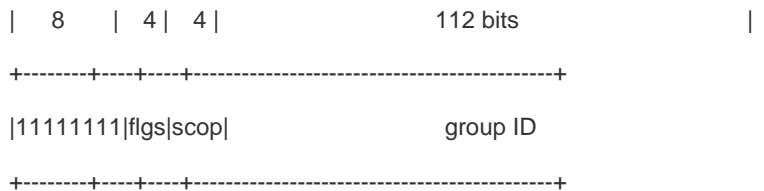
图 3-6



IPv4 兼容 IPv6 地址主要是用在自动隧道上，这类节点既支持 IPv4 也支持 IPv6，IPv4 兼容 IPv6 地址通过 IPv4 设备以隧道方式传送 IPv6 报文，目前 IPv4 兼容 IPv6 地址已被废除。而 IPv4 映射 IPv6 地址则被 IP6 节点用于访问只支持 IPv4 的节点，例如当一个 IPv4/IPv6 主机的 IPv6 应用程序请求解析一个主机名字（该主机只支持 IPv4）时，那么名字服务器内部将动态生成 IPv4 映射的 IPv6 地址返回给 IPv6 应用程序。

### 组播地址（Multicast Addresses）

IPv6 组播的地址格式如下：



地址格式中的第 1 个字节为全“1”代表是一个组播地址。

#### ● 标志字段：

由 4 个比特位组成。目前只指定了第 4 位，该位用来表示该地址是由 Internet 编号机构指定的知名的组播地址，还是特定场合使用的临时组播地址。如果该标志位为“0”，表示该地址为知名组播地址；如果该位为“1”，表示该地址为临时地址。其他 3 个标志位保留将来用。

#### ● 范围字段：

由 4 个比特位组成，用来表示组播的范围。即组播组是包括本地节点、本地链路、本地站点，还包括 IPv6 全球地址空间中任何位置的节点。

● 组标识符字段：

长 112 位，用于标识组播组。根据组播地址是临时的还是知名的以及地址的范围，同一个组播标识符可以表示不同的组。

IPv6 的组播地址是以 FF00::/8 为前缀的这类地址。一个 IPv6 的组播地址通常标识一系列不同节点的接口。当一个报文发送到一个组播地址上时，那么该报文将分发到标识有该组播地址的每个节点的接口上。一个节点(主机或者设备)必须加入下列的组播：

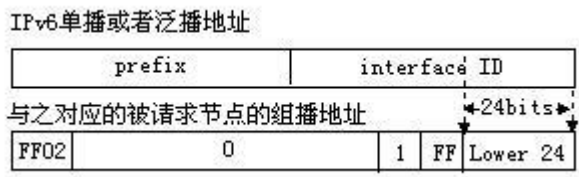
- 5. 本地链路所有节点组播地址 FF02::1
- 6. 被请求节点的组播地址，前缀为 FF02:0:0:0:0:1:FF00:0000/104

如果是设备那么还必须加入本地链路所有设备的组播地址 FF02::2。

被请求节点的组播地址是对应于 IPv6 单播(unicast)和泛播(anycast)地址的，IPv6 节点必须为配置的每个单播地址和泛播地址加入其相应的被请求节点的组播地址。被请求节点的组播地址的前缀为 FF02:0:0:0:0:1:FF00:0000/104，另外 24 位由单播地址或者泛播地址的低 24 比特组成，例如对应于单播地址 FE80::2AA:FF:FE21:1234 的被请求节点的组播地址是 FF02::1:FF21:1234，

被请求节点组播地址通常用于邻居请求(NS)报文中，被请求节点组播地址的格式如下：

图 3-7



📌 泛播地址 ( Anycast Addresses )

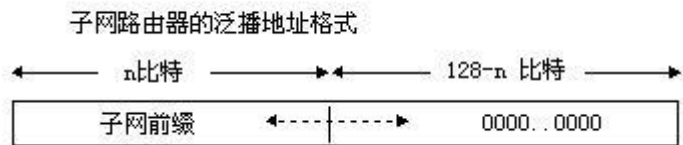
泛播地址与组播地址类似，同样是多个节点共享一个泛播地址，不同的是只有一个节点期待接收给泛播地址的数据包而组播地址成员的所有节点均期待着接收发给该地址的所有包。泛播地址被分配在正常的 IPv6 单播地址空间，因此泛播地址在形式上与单播地址无法区分开，一个泛播地址的每个成员，必须显式地加以配置，以便识别是泛播地址。

⚠ 泛播地址只能分配给设备，不能分配给主机，并且泛播地址不能作为报文的源地址。

在 RFC2373 中预定义了一个泛播地址，称之为子网路由器的泛播地址。下图显示了子网路由器的泛播地址格式，这类地址由子网前缀后面跟着一系列的 0(作为接口标识符)组成。

其中子网前缀标识了一个指定的链路(子网)，送给子网路由器泛播地址的报文将被分发到在该子网上的一个设备。子网路由器的泛播地址通常是被用于一个节点上的应用程序需要和远程子网的一个设备通信而使用。

图 3-8



## 相关配置

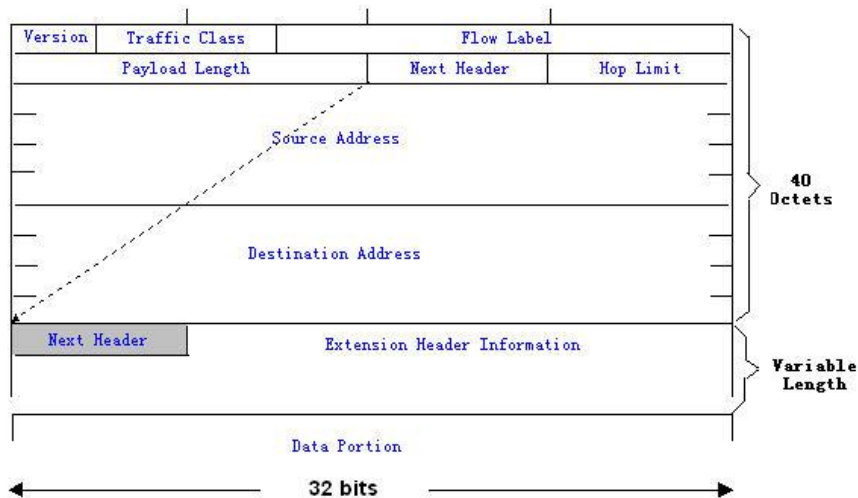
### 配置 IPv6 地址

- 缺省情况接口没有配置 IPv6 地址。
- 可通过 `ipv6 address` 命令配置接口 IPv6 单播地址和泛播地址。
- 接口 up 之后将会自动加入相应的组播组。

### 3.3.3 IPv6 包头结构

IPv6 包头格式如下图：

图 3-9



在 IPv4 中，所有包头以 4 字节为单位。在 IPv6 中，包头以 8 字节为单位，包头的总长度是 40 字节。IPv6 包头定义了以下字段：

- 版本(Version)：

长度为 4 位，对于 IPv6 该字段必须为 6。

- 类别(Traffic Class)：

长度为 8 位，指明为该包提供了某种服务，相当于 IPv4 中的“TOS”。



- 流标签(Flow Label)：

长度为 20 位，用于标识属于同一业务流的包，一个节点可以同时作为多个业务流的发送源，流标签和源节点地址唯一标识了一个业务流。

- 净荷长度(Payload Length)：

长度为 16 位，其中包括包净荷的字节长度，同时也包含了各个 IPv6 扩展选项的长度(如果存在)，换句话说就是包含了除 IPv6 头本身外的 IPv6 包的长度。

- 下一个头(Next Header)：

这个字段指出了 IPv6 头后所跟的头字段中的协议类型。与 IPv4 协议字段类似，下一个头字段可以用来指出高层是 TCP 还是 UDP，它也可以用来指明 IPv6 扩展头的存在。

- 跳数(Hop Limit)：

长度为 8 位。每当设备对包进行一次转发之后，这个字段就会被减 1，如果该字段达到 0，这个包就将被丢弃。它与 IPv4 包头中的生存期字段类似。

- 源地址(Source Address)：

长度为 128 位，指出了 IPv6 包的发送方地址。

- 目的地址(Destination Address)：

长度为 128 位，指出了 IPv6 包的接收方地址。

IPv6 的扩展头，目前 IPv6 定义了下列的扩展头：

- 逐跳选项头(Hop-by-Hop Options)：

此扩展头必须紧随在 IPv6 头之后，它包含包所经过的路径上的每个节点都必须检查的选项数据。

- 路由选项头 ( Routing ( Type 0 ))：

此扩展头指明包在到达目的地途中将经过哪些节点，它包含包沿途经过的各节点的地址列表。IPv6 头的最初目的地址是选路头的一系列地址中的第一个地址，而不是包的最终目的地址。IPv6 头部目的地址对应的节点接收到该包之后，对 IPv6 头和选路头进行处理，并把包发送到选路头列表中的第二个地址，如此继续，直到包到达其最终目的地。

- 分片头 ( Fragment )：

此扩展头用于源节点对长度超出源节点和目的节点路径 MTU 的包进行分片。

- 目的地选项头 ( Destination Options )：

此扩展头代替了 IPv4 选项字段，目前唯一定义的目的地选项是在需要时把选项填充为 64 位 ( 8 字节 ) 的整数倍，此扩展头可以用来携带由目的地节点检查的信息。

- 上层扩展头(Upper-layer header)：

指明了上层传输数据的协议，如 TCP(6)、UDP(17)。

此外还有身份验证头(Authentication )和封装安全性净荷(Encapsulating Security Payload )的扩展头，这将放到 IPSec 章节描述。

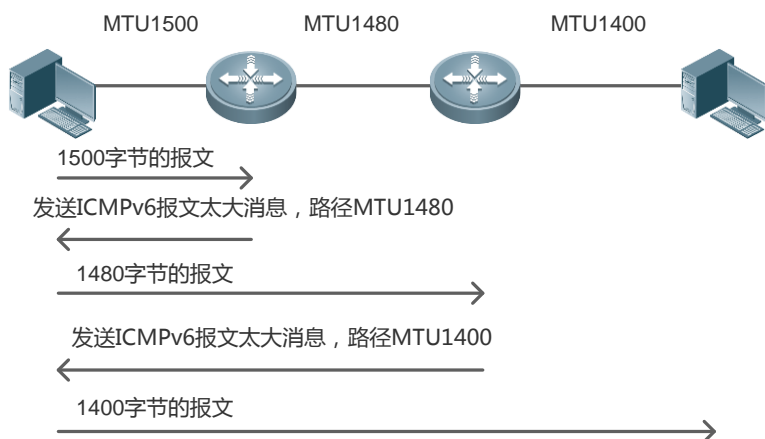
## 相关配置

无

### 3.3.4 IPv6 路径 MTU 发现

和 IPv4 的路径 MTU 发现类似，IPv6 的路径 MTU 发现允许一台主机动态的发现并调整发送数据路径上的 MTU 的大小。另外，当主机要发送的数据包的大小如果比发送数据路径上的 MTU 大时，那么将由主机自行负责分片。这种由主机分片的行为使得设备无需处理分片从而节省了 IPv6 设备的资源，同时也提高了 IPv6 网络的效率。

图 3-10



如上图，当主机要发送的报文的长度比路径 MTU 大时，路由器丢弃报文，并且向主机发送一个 ICMPv6 报文太大消息，把 MTU 告诉主机，然后主机根据新的路径 MTU 对报文进行分片。这种由主机分片的行为使得路由器不需要对报文进行分片从而节省了路由器的资源，同时也提高了 IPv6 网络的效率。

## 相关配置

### 配置接口 IPv6 MTU

- 以太网接口的默认 IPv6 MTU 是 1500。
- 可通过 `ipv6 mtu` 命令修改接口的 IPv6 MTU 值。

### 3.3.5 IPv6 邻居发现

邻居发现协议是 IPv6 协议的一个基本的组成部分，它的主要功能有路由器发现、前缀发现、参数发现、地址自动配置、地址解析（相当于 ARP）、确定下一跳、邻居不可达检测、地址冲突检测和重定向。邻居发现定义了 5 种 ICMP 报文：“路由器请求”，ICMP 类型为 133；路由器公告，ICMP 类型为 134；邻居请求，相当于 ARP 请求，ICMP 类型为 135；邻居公告，相当于 ARP 应答，ICMP 类型为 136；ICMP 重定向报文，ICMP 类型为 137”。

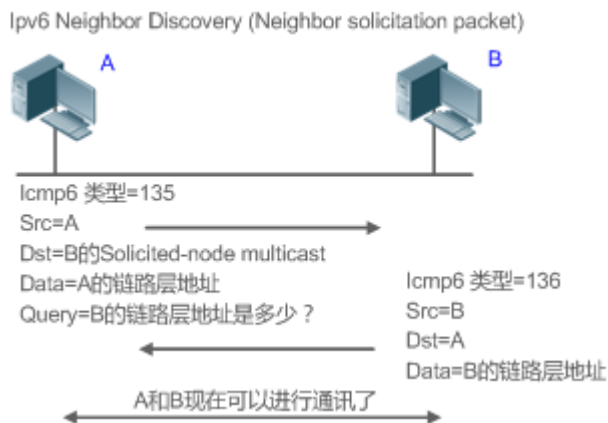
上述五种 ICMP 报文都会携带一个或者多个的选项，这些选项在某些情况下是可选，事实上，有些情况下选项实际上就是报文的全部意义所在，邻居发现主要定义五种选项：“源链路层地址选项”，类型=1；“目标链路层地址选项”，类型=2；“前缀信息选项”，类型=3；“重定向的首部选项”，类型=4；“MTU 选项” 类型=5；

#### 地址解析

当一个节点要与另外一个节点通信时，那么该节点必须获取对方的链路层地址，此时就要向该节点发送邻居请求(NS)报文,报文的目的地址是对应于目的节点的 IPv6 地址的被请求多播地址，发送的 NS 报文同时也包含了自身的链路层地址。当对应的节点收到该邻居请求后发回一个响应的报文称之为邻居公告报文(NA)，其目的地址是邻居请求的源地址，内容为被请求的节点的链路层的地址。当源节点收到该应答报文后就可以和目的节点进行通讯了。

下图是地址解析的过程：

图 3-11



#### 邻居不可达检测

当一个邻居被认为可到达的时间到期以后，如果有 IPv6 单播报文需要发送给这个邻居，将执行邻居不可达检测 (Neighbor Unreachability Detection)。

邻居不可达检测和向邻居发送 IPv6 报文可以同时进行，在检测过程中，继续向该邻居转发 IPv6 报文。

#### 地址冲突检测

当给主机配置 IPv6 地址以后，想知道这个 IPv6 地址在链路上是不是唯一的，需要执行地址冲突检测，发送源 IPv6 地址是未指定地址的邻居请求。

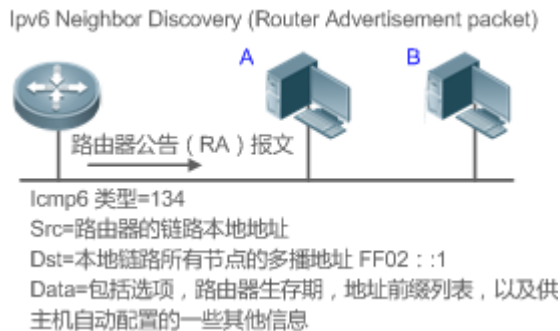
如果设备检测到地址冲突，该地址将被设置为冲突状态，设备将不能接收目的地址为该地址的 ipv6 报文，同时设备会为该冲突的地址起一个定时器，定时进行地址冲突检测，如果重新检测没有冲突，该地址将可以正常使用。

## ➤ 路由器，前缀和参数发现

路由器公告报文(RA)在设备上定期被发往链路本地所有节点的。

路由器公告报文发送如下图：

图 3-12



路由器公告报文中通常包含如下内容：

- 一个或者多个 IPv6 地址前缀（用于 on-link 确定，或无状态地址自动配置）
- IPv6 地址前缀的有效期。
- 主机自动配置使用的方式(有状态还是无状态)。
- 作为缺省设备的信息(即决定本设备是否要作为缺省设备，如果是那么还宣布自己充当缺省设备的时间)。
- 提供给主机配置的一些其它信息如跳数限制、MTU、邻居请求重传间隔时间等。

路由器公告报文同时也用来应答主机发出的路由器请求(RS)报文，路由器请求报文允许主机一旦启动后可以立即获得自动配置的信息而无需等待设备发出的路由器公告报文(RA)。当主机刚启动时如果没有单播地址，那么主机发出的路由器请求报文将使用未指定地址(0:0:0:0:0:0:0:0)作为请求报文的源地址，否则使用已有的单播地址作为源地址，路由器请求报文使用本地链路所有设备组播地址(FF02::2)作为目的地址。作为应答路由器请求(RS)报文的路由器公告(RA)报文将使用请求报文的源地址作为目的地址(如果源地址是未指定地址那么将使用本地链路所有节点组播地址 FF02::1)。

在路由器公告报文中下列参数是可以被配置的：

- Ra-interval 路由器公告报文的发送间隔。
- Ra-lifetime 路由器生存期，即设备是否充当本地链路的缺省路由器以及充当该角色的时间。
- Prefix 本地链路的 IPv6 地址前缀，用于 on-link 确定，或无状态地址自动配置，包括前缀的其它参数配置。
- Ns-interval 邻居请求报文重传的时间间隔。
- Reachabletime 检测到邻居可到达事件后认为邻居是可到达的所维持的时间。
- Ra-hoplimit 路由器公告(RA)报文跳数的值，用于设置主机发送单播报文的 hop-limit
- Ra-mtu 路由器公告(RA)报文的 MTU 字段的值
- Maneged-config-flag 决定了收到该路由器公告的主机是否要使用全状态自动配置来获取地址
- Other-config-flag 决定了收到该路由器公告的主机是否将使用 dhcpv6 来获取除 IPv6 地址以外的其他信息进行自动配置。

以上这些参数在 IPv6 接口属性中进行配置。

### ↘ 重定向

当路由器收到 IPv6 报文以后，发现存在更优的下一跳，就发送 ICMP 重定向报文把更优的下一跳告诉主机，下一次主机直接把 IPv6 报文发给更优的下一跳。

### ↘ 未解析的邻居表项的最大数量

- 为防止恶意扫描网段，生成大量的未解析邻居表项，占用过多的内存，可配置限制未解析的邻居表项的最大数量

### ↘ 处理 ND 选项最大数量

- 为防止伪造 ND 报文携带无穷的 ND 选项，设备处理占用过多的 CPU，可配置限制 ND 选项最大数量

### ↘ 接口邻居学习表项数量

- 为防止邻居学习攻击，占用设备邻居表项，占用内存且影响转发性能，可配置限制接口邻居学习表项数量

## 相关配置

### ↘ 配置 IPv6 重定向

- 缺省情况 IPV6 的接口上允许发送 ICMPv6 重定向报文
- 可以使用接口配置模式命令 “no ipv6 redirects” 禁止接口发送重定向报文

### ↘ 配置 IPv6 地址冲突检测

- 缺省情况接口上为 IPV6 地址执行地址冲突检测时会发送的 1 个邻居请求(NS)报文
- 可以使用接口配置模式命令 “ipv6 nd dad attempts value” 配置 DAD 连续发送的 NS 报文个数，0 表示阻止为该接口上的 Ipv6 地址启动地址冲突检测
- 使用 “no ipv6 nd dad attempts” 恢复默认配置
- 缺省情况设备对已经冲突 IPv6 地址会定时执行地址冲突检测，时间间隔为 60s
- 可以使用全局配置模式命令 “ipv6 nd dad retry value” 配置重复地址冲突检测的时间间隔，0 表示关闭设备进行重复冲突地址检测功能。
- 使用 “no ipv6 nd dad retry” 恢复默认配置

### ↘ 配置邻居可达时间

- 缺省情况 IPv6 邻居默认可达时间为 30s
- 可以使用接口配置模式命令 “ipv6 nd reachable-time milliseconds” 修改可达时间

### ↘ 配置邻居 stale 状态时间

- 缺省情况 IPv6 邻居默认 stale 状态持续时间 1h，到期后将进行邻居不可达检测

- 可以使用接口配置模式命令 “**ipv6 nd stale-time seconds**” 修改 stale 状态持续时间

#### 配置前缀信息

- 缺省情况 RA 公告的前缀是在该接口上通过 **ipv6 address** 命令配置的前缀
- 可以使用接口配置模式命令 “**ipv6 nd prefix**” 添加或删除可公告的前缀及前缀参数

#### 配置 RA 抑制功能

- 缺省情况 IPv6 的接口上不会发送路由器公告报文
- 可以使用接口配置模式命令 “**no ipv6 nd suppress-ra**” 关闭 RA 抑制功能

#### 配置未解析的邻居表项的最大数量

- 默认值为 0，表示不限制，即受限于设备支持的 ND 表项容量
- 使用全局配置模式下命令 **ipv6 nd unresolved number** 限制未解析邻居数量，表项超过该限制后，将不为后续报文进行主动解析

#### 配置处理 ND 选项最大数量

- 使用全局配置模式下命令 **ipv6 nd max-opt value** 限制处理邻居选项个数，默认值为 10

#### 配置接口可学习邻居表项的数量

- 使用接口配置模式下命令 **ipv6 nd cache interface-limit value** 限制接口可学习的邻居数量，默认值为 0，表示不限制

### 3.3.6 IPv6 源路由

#### 工作原理

IPv6 报文通过路由首部被发送者用来指定报文经过哪些中间节点到达目的地址，类似于 IPv4 的宽松源路由选项和宽松记录路由选项，格式为：

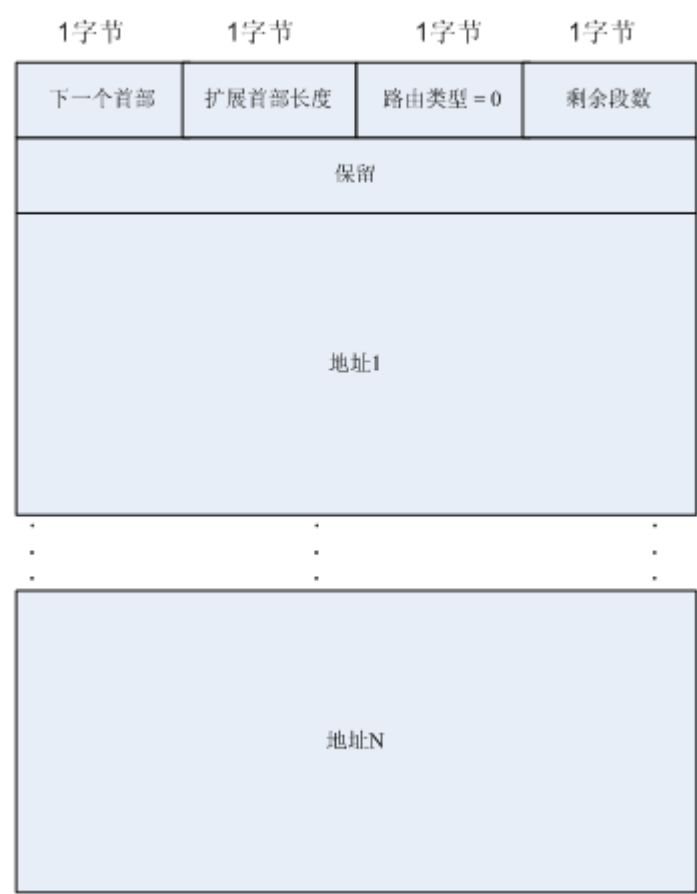
图 3-13

1字节	1字节	1字节	1字节
下一个首部	扩展首部长度	路由类型	剩余段数
各种路由类型特定的数据			

其中剩余段数用来指明报文从当前节点到最终目的地址，还需要经过多少个路由首部指明的中间节点，不包括路由首部没有列出的中间节点。

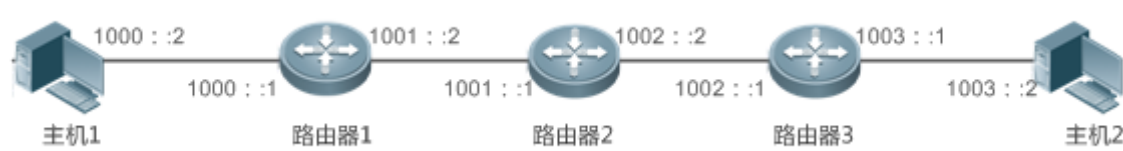
目前定义了两种路由类型：0 和 2。类型 2 路由首部用于移动通信。RFC2460 定义了类型 0 路由首部（类似于 IPv4 的宽松源路由选项），格式如下图所示。

图 3-14



下面举例说明类型 0 路由首部的应用，如图 3-15 所示。

图 3-15



主机 1 发报文给主机 2，指明要经过路由器 2 和 3，转发过程中报文 IPv6 首部和路由首部的相关字段变化如下表所示：

传输节点	IPv6 首部的相关字段	类型 0 路由首部的相关字段
主机 1	源地址=1000::2 目的地址=1001::1（路由器 2 的地址）	剩余段数=2 地址 1=1002::1（路由器 3 的地址） 地址 2=1003::2（主机 2 的地址）
路由器 1	无变化	
路由器 2	源地址=1000::2	剩余段数=1

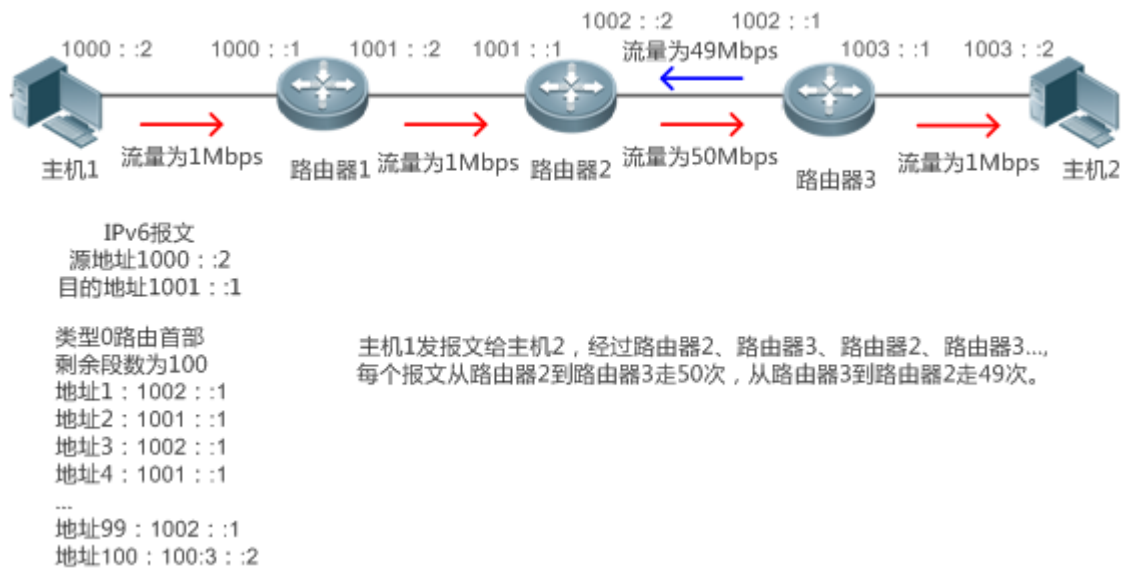
	目的地址=1002::1（路由器 3 的地址）	地址 1=1001::1（路由器 2 的地址） 地址 2=1003::2（主机 2 的地址）
路由器 3	源地址=1000::2 目的地址=1003::2（主机 2 的地址）	剩余段数=0 地址 1=1001::1（路由器 2 的地址） 地址 2=1002::1（路由器 3 的地址）
主机 2	无变化	

具体过程如下：

- 主机 1 发出报文，目的地址是路由器 2 的地址 1001::1，在类型 0 路由首部中填上路由器 3 的地址 1002::1 和主机 2 的地址 1003::2，剩余段数是 2。
- 路由器 1 只是简单地把报文转发给路由器 2。
- 路由器 2 把 IPv6 首部的目的地址和路由首部的地址 1 交换，即现在目的地址是路由器 3 的地址 1002::1，路由首部的地址 1 是路由器 2 的地址 1001::1，剩余段数是 1。修改完以后，路由器 2 把报文转发给路由器 3。
- 路由器 3 把 IPv6 首部的目的地址和路由首部的地址 2 交换，即现在目的地址是主机 2 的地址 1003::2，路由首部的地址 2 是路由器 3 的地址 1002::1，剩余段数是 0。修改完以后，路由器 3 把报文转发给主机 2。

类型 0 路由首部有可能被利用进行拒绝服务攻击，如下图所示，主机 1 以 1Mbps 的速度向主机 2 发报文，故意构造一个路由首部，使报文在路由器 2 和路由器 3 之间多次往返，从路由器 2 到路由器 3 走 50 次，从路由器 3 到路由器 2 走 49 次，这时路由首部产生流量放大效应：“路由器 2 到路由器 3 方向的流量为 50Mbps，路由器 3 到路由器 2 方向的流量为 49Mbps”。由于存在这个安全问题，RFC5095 废除了类型 0 路由首部。

图 3-16



## 相关配置

### 配置 IPv6 源路由



- 缺省情况不支持类型 0 路由首部
- 可以使用全局配置模式命令 “**ipv6 source-route**” 打开这项功能

### 3.3.7 控制 ICMPv6 差错报文的发送速率

#### 工作原理

ICMPv6 差错报文是由目标节点或者中间路由器发送，用于报告在转发和传送 IPv6 数据包过程中出现的错误。主要包括下面四种类型的差错报文：目标不可达（Destination unreachable）、报文太大（Packet too big）、超时（Time exceeded）、参数问题（Parameter problem）。

往设备发送非法 IPv6 报文，设备会丢弃这些报文，并向源 IPv6 地址发送相应的 ICMPv6 差错报文。如果受到 IPv6 非法报文攻击，可能出现设备一直在应答 ICMPv6 差错报文而耗尽设备资源，这样设备将不能正常提供服务，针对这种攻击，可以对 ICMPv6 差错报文的发送速率进行限制。

如果转发的 IPv6 报文的长度超过出口的 IPv6 MTU，路由器会丢弃 IPv6 报文，并且向源 IPv6 地址发送 ICMPv6 报文太大消息，这种 ICMPv6 差错报文的主要用途是 IPv6 路径 MTU 发现。为了防止其它 ICMPv6 差错报文太多而将 ICMPv6 报文太大消息限速过滤掉，从而导致 IPv6 路径 MTU 发现功能失效，对 ICMPv6 报文太大消息和其它 ICMPv6 差错报文分别限速。

ICMPv6 重定向报文不属于 ICMPv6 差错报文，我司把 ICMPv6 重定向报文和其它 ICMPv6 差错报一起限速。

#### 相关配置

##### 配置 ICMPv6 报文太大消息的发送速率

- 缺省速率是 100 毫秒 10 个。
- 可通过 **ipv6icmp error-interval too-big** 配置发送速率。

##### 配置其它 ICMPv6 差错报文的发送速率

- 缺省速率是 100 毫秒 10 个。
- 可通过 **ipv6icmp error-interval** 配置发送速率。

### 3.3.8 IPv6 HOP-LIMIT

#### 工作原理

IPv6 数据包从源地址向目的地址经过路由器间传播，设置一个 hop-limit 数值，每过一个路由器 hop-limit 值就减一，当减到零的时候，路由器就把这个包丢掉，这样可以防止无用的包在网络上无限传播下去，浪费网络带宽。其功能类似于 IPv4 的 TTL。

#### 相关配置

##### 设置 IPv6 hop-limit

- 缺省情况设备 IPv6 HOP-LIMIT 为 64。
- 可通过 **ipv6 hop-limit** 设置设备的 IPv6 HOP-LIMIT 值。

### 3.3.9 抑制往认证 vlan 发送广播邻居请求（NS）报文

#### 工作原理

在网关认证模式下，SuperVLAN 下的所有子 VLAN 默认都是认证 VLAN，认证 VLAN 下的认证用户需要在认证后才能上网。用户认证后会在设备上生成静态 ND 表项，因此设备访问认证用户时，不需要往认证 VLAN 发送 NS 请求。若设备需要访问免认证 VLAN 下的用户时，只需要往免认证 VLAN 发送 ARP 请求。

在网关认证模式下，设备默认开启了抑制往认证 VLAN 发送 NS 请求的功能。如果设备需要访问认证 VLAN 下的非认证用户，需要关闭该功能。

#### 相关配置

##### ✎ 设置抑制往认证 vlan 发送广播 NS 报文

- 接口模式下，使用命令 **ipv6 nd suppress-auth-vlan-ns** 开启抑制往认证 VLAN 发送 NS 请求功能。
- 缺省情况下开启抑制往认证 VLAN 发送 NS 请求功能。
- 只支持在 SVI 接口上配置，且只有网关认证模式下才生效

### 3.3.10 MGMT 接口支持缺省网关

#### 工作原理

给 MGMT 口配置缺省网关，为 MGMT 口生成一条默认路由。


#### 相关配置

##### ✎ 设置 MGMT 口的缺省网关

- 接口模式下，使用命令 **ipv6 gateway ipv6-address** 配置 MGMT 口的缺省网关。
- 缺省情况下，MGMT 口没有配置缺省网关

### 3.4 配置详解

配置项	配置建议&相关命令	
配置 IPv6 地址	 必须配置，用于配置 ipv6 地址，启用 IPv6 协议。	
	ipv6 enable	打开接口的 IPv6 协议
	ipv6 address	配置接口 IPv6 的单播地址
配置 IPv6 邻居发现	 可选配置，用于限制接口 IPv6 重定向功能。	
	ipv6 redirects	打开该接口的 IPv6 重定向功能
	 可选配置，用于设置 DAD 检测。	
	ipv6 nd dad attempts	配置冲突检测时要连续发送的邻居请求(NS)报文的数量。
	 可选配置，用于设置邻居发现的各种参数。	
	ipv6 nd reachable-time	设置邻居被认为可到达的时间
	ipv6 nd prefix	设置路由器公告(RA)报文中所要公告的地址前缀
	ipv6 nd suppress-ra	设置是否在该接口上阻止路由器公告 ( RA ) 报文发送
	 可选配置，用于设置未解析邻居的最大数量。	
	ipv6 nd unresolved	设置未解析邻居的最大数量
	 可选配置，用于设置处理 ND 报文的选项最大数量	
	ipv6 nd max-opt	设置处理 ND 选项最大数量
	 可选配置，用于限制接口可学习的邻居数量	
	ipv6 nd cache interface-limit	设置接口可学习邻居数量
<a href="#">配置路径 MTU 发现</a>	 可选配置，用于限制接口发送 IPv6 报文的 mtu。	
	ipv6 mtu	设置 IPv6 MTU 值
配置 IPv6 源路由	 可选配置，用于开启支持 IPv6 源路由功能。	
	ipv6 source-route	配置设备转发带有路由首部的 IPv6 报文。
配置 ICMPv6 差错报文的发送速率	 可选配置。	
	ipv6 icmp error-interval too-big	配置 ICMPv6 报文太大消息的发送速率。
	ipv6 icmp error-interval	配置其它 ICMPv6 差错报文和 ICMPv6 重定向报文的发送速率。
配置设备 IPv6 HOP-LIMIT	 可选配置，用于限制接口发送 IPv6 单播报文的转发跳数。	
	ipv6 hop-limit	设置 IPv6 HOP-LIMIT 值。

配置抑制往认证 vlan 发送广播 NS 报文	 可选配置，用于网关认证模式下，抑制往免认证 vlan 发送广播 ns 报文。	
	<b>ipv6</b> <b>suppress-auth-vlan-ns</b>	<b>nd</b> 设置抑制往免认证 vlan 发送广播 ns 报文。
配置 MGMT 口缺省网关	 可选配置，用于给 mgmt 口配置缺省网关。	
	<b>ipv6 gateway</b> <i>ipv6-address</i>	设置 mgmt 口的缺省网关。

### 3.4.1 配置 IPv6 地址

#### 配置效果

通过配置接口 IPv6 地址实现 IPv6 网络通信。

#### 注意事项

无

#### 配置方法

##### 打开接口的 IPv6 协议

- 可选配置，若不想通过配置 IPv6 地址来开启接口 IPv6 协议，则必须配置 **ipv6 enable** 来开启接口 IPv6 功能。

##### 配置接口 IPv6 的单播地址

- 必须配置。

#### 检验方法

通过 **show ipv6 interface** 可以看到配置的地址生效

#### 相关命令


##### 打开接口的 IPv6 协议

【命令格式】 **ipv6 enable**

【参数说明】 -

【命令模式】 接口模式

【使用指导】 有 2 种方式可以打开接口上的 IPv6 功能，一是在接口下配置 **ipv6 enable** 命令，二是直接在接口下配置了 IPv6 地址。

 如果接口已经被绑定到没有配置 IPv6 地址族的多协议 VRF，那么不允许在接口上打开 IPv6 功能，必须

先给多协议 VRF 配置 IPv6 地址族，然后才能在接口上打开 IPv6 功能。

如果在接口上配置了 IPv6 地址那么接口的 IPv6 功能就会自动打开，即使使用 **no ipv6 enable** 也不能关闭 IPv6 功能。

## 配置接口 IPv6 的单播地址

【命令格式】 **ipv6 address***ipv6-address/prefix-length*

**ipv6 address***ipv6-prefix/prefix-length***eui-64**

**ipv6 address***prefix-name sub-bits/prefix-length* [**eui-64**]

【参数说明】 *ipv6-address*：IPv6 地址，必须遵循 RFC4291 定义的地址形式，每个地址域之间用冒号隔开，每个域占 16 比特，用十六进制数表示。

*ipv6-prefix*：IPv6 地址前缀，必须遵循 RFC4291 定义的地址形式，每个地址域之间用冒号隔开，每个域占 16 比特，用十六进制数表示。

*prefix-length*：IPv6 前缀的长度即 IPv6 地址中代表网络的部分。

*prefix-name*：通用前缀的名字。使用这个指定的通用前缀生成接口地址。

*sub-bits*：子前缀比特与主机比特的值。这个值与通用前缀中的前缀合并生成接口地址。这个值的表示法要遵循 RFC4291 描述的冒号表示法。

*eui-64*：表示生成的 IPv6 地址由配置的地址前缀和 64 比特的接口 ID 标识符组成。

【命令模式】 接口模式

【使用指导】

❗ 如果接口已经被绑定到没有配置 IPv6 地址族的多协议 VRF，那么不允许给接口配置 IPv6 地址，必须先给多协议 VRF 配置 IPv6 地址族，然后才能给接口配置 IPv6 地址。

当一个 IPv6 接口被创建并且链路状态为 UP 时那么系统将为该接口自动生成链路本地地址。

接口的 IPv6 地址也可以使用通用前缀机制生成。其机制就是 IPv6 地址=“通用前缀”+“子前缀”+“主机比特”。通用前缀可以使用 **ipv6 general-prefix** 命令配置，也可能通过 DHCPv6 客户端的 PD(前缀发现)功能学习到(参见 DHCPv6 配置指南)。“子前缀”+“主机比特”就是使用本命令的 *sub-bits/prefix-length* 参数配置。使用 **no ipv6 address** 如果不指定删除具体的地址，那么将删除所有手工配置的地址。

使用 **no ipv6 address***ipv6-prefix/prefix-length***eui-64** 可以删除使用命令 **ipv6 address***ipv6-prefix/prefix-length***eui-64** 配置的地址。

## 配置举例

### 给接口配置 IPv6 地址

【配置方法】 在接口 GigabitEthernet 0/0 开启 IPv6 协议，并添加 ipv6 地址 2000::1

```
Ruijie(config)#interface gigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2000::1/64
```

【检验方法】 使用 **show ipv6 interface** 可以看到接口 GigabitEthernet 0/0 添加地址成功

```
Ruijie(config-if-GigabitEthernet 0/0)#show ipv6 interface gigabitEthernet 0/0

interface GigabitEthernet 0/0 is Down, ifindex: 1, vrf_id 0
```

```
address(es):
  Mac Address: 00:00:00:00:00:00
  INET6: FE80::200:FF:FE00:1 [ TENTATIVE ], subnet is FE80::/64
  INET6: 2000::1 [ TENTATIVE ], subnet is 2000::/64
Joined group address(es):
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<160--240>
ND router advertisements live for 1800 seconds
```

## 常见错误

---

无

### 3.4.2 配置路径 MTU 发现

## 配置效果

---

本地发送 IPv6 报文时根据路径 MTU 分片。

## 注意事项

---

接口 IPv6 MTU 的配置范围受接口 MTU 限制，最大值是接口 MTU。

## 配置方法

---

### 📌 设置接口 IPv6 MTU 值

- 可选配置。

## 检验方法

---

- 通过 **show run** 命令查看配置是否正确。
- 通过 **show ipv6 interface** 命令查看接口 IPv6 MTU 配置是否正确。

## 相关命令

### 设置接口 IPv6 MTU 值

- 【命令格式】 **ipv6 mtu bytes**
- 【参数说明】 *bytes* : IPv6 包最大传输单元，以字节为单位，范围 1280~1500。
- 【命令模式】 接口模式
- 【使用指导】 -

## 配置举例

### 配置接口 IPv6 MTU

- 【配置方法】 修改接口 IPv6 MTU 为 1300。

```
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 mtu 1300
```

- 【检验方法】 通过 **show ipv6 interface** 查看配置是否生效。

```
Ruijie(config-if-GigabitEthernet 0/0)#show ipv6 interface
```

```
interface GigabitEthernet 0/ is Down, ifindex: 1, vrf_id 0
address(es):
  Mac Address: 00:d0:f8:22:33:47
  INET6: FE80::2D0:F8FF:FE22:3347 [ TENTATIVE ], subnet is FE80::/64
  INET6: 1020::1 [ TENTATIVE ], subnet is 1020::/64
  INET6: 1023::1 [ TENTATIVE ], subnet is 1023::/64
Joined group address(es):
MTU is 1300 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<160--240>
ND router advertisements live for 1800 seconds
```

## 常见配置错误

无

### 3.4.3 配置 IPv6 邻居发现

#### 配置效果

---

配置 ND 协议相关属性，比如配置 ipv6 重定向功能，配置 DAD 检测等。

#### 注意事项

---

接口默认是抑制发送 RA 报文，要设备能够发送 RA 报文必须在接口模式下配置 no ipv6 nd suppress-ra。

#### 配置方法

---

##### ✎ 打开该接口的 IPv6 重定向功能

- 可选配置，缺省已开启。
- 当需要关闭接口 IPv6 重定向功能时，使用 “no ipv6 redirects”。

##### ✎ 配置冲突检测时要连续发送的邻居请求(NS)报文的数量

- 可选配置。
- 如果需要阻止为该接口上的 Ipv6 地址启动地址冲突检测或者修订 DAD 连续发送邻居请求(NS)报文个数，可使用该配置。

##### ✎ 设置邻居被认为可到达的时间

- 可选配置。
- 如果需要修改邻接可达时间，可使用该配置。

##### ✎ 设置路由器公告(RA)报文中所要公告的地址前缀

- 缺省情况 RA 公告的前缀是在该接口上通过 ipv6 address 命令配置的前缀

##### ✎ 设置是否在该接口上阻止路由器公告 ( RA ) 报文发送

- 可选配置。
- 如果需要设备能发送路由器公告，可使用该命令来配置。

##### ✎ 配置未解析的邻居表项的最大数量

- 可选配置。
- 如果设备受到扫描攻击而创建大量未解析邻居表项，消耗表项资源，可以使用该命令限制未解析邻居的数量。

##### ✎ 配置处理 ND 选项最大数量

- 可选配置
- 如果环境要求设备能够处理更多的选项内容，可使用该命令来配置。



## 配置接口可学习邻居表项的数量

- 可选配置
- 如果环境中 IPv6 主机数可控制，可以使用该功能限制接口的学习邻居个数，防止网络中进行 ND 学习攻击，使得设备学习表项占用内存影响性能。

## 检验方法

通过以下命令查看配置是否正确：

- **show ipv6 interface** *interface-type interface-num* 可查看接口重定向功能，邻居可达时间、邻居请求发送间隔等信息是否配置生效
- **show ipv6 interface** *interface-type interface-num ra-inifo* 可查看路由器公告配置的前缀及其他信息是否正确
- **show run**

## 相关命令

### 打开该接口的 IPv6 重定向功能

- 【命令格式】 **ipv6 redirects**
- 【参数说明】 -
- 【命令模式】 接口模式
- 【使用指导】 所有 ICMPv6 的错误报文的数据包传输速率是有限制的，缺省每秒钟最多可以发送 10 个错误 ICMPv6 错误报文(10pps)。

### 配置冲突检测时要连续发送的邻居请求(NS)报文的数量

- 【命令格式】 **ipv6 nd dad attempts** *value*
- 【参数说明】 *value*：邻居请求(NS)报文的数量
- 【命令模式】 接口模式
- 【使用指导】 当在接口上配置一个新的 IPV6 地址前要为其启动地址冲突检测，此时该地址处于“tentative”（试验）的状态。地址冲突过程执行完了，如果没有检测到冲突，那么该地址就可以被正确使用，如果检测到冲突了，并且该地址所使用的接口标识符是使用 EUI-64 的标识符，那么表明在该链路上存在链路层地址出现重复，那么此时系统会自动关闭该接口（即阻止在该接口上进行 IPV6 的相关操作），此时必须手工去修改并配置新的地址，并通过再次 down/up 接口重新启动地址冲突检测。任何情况下当一个接口从 down 状态变为 up 状态时都会为该接口上的地址重新启动地址冲突检测。

### 设置邻居被认为可到达的时间

- 【命令格式】 **ipv6 nd reachable-time** *milliseconds*
- 【参数说明】 *milliseconds*：邻居被认为可到达的时间，以毫秒为单位，范围：0-3600000。缺省为 30 秒。
- 【命令模式】 接口模式
- 【使用指导】 设备通过该配置的时间来检测不可用的邻居，所设置的时间越短意味着可以更快的检测到邻居失效，但是将浪费更多的网络带宽、消耗设备更多的资源。因此不建议将该时间配置的过小。

配置的值将在路由器公告报文(RA)中被发布出去，同时该值也被设备自身使用。如果设置的值为 0 表示设备未指定该时间，即使用缺省值。

## 设置路由器公告(RA)报文中所要公告的地址前缀

【命令格式】 **ipv6 nd prefix** {*ipv6-prefix/prefix-length* | **default**} [[*valid-lifetime* {**infinite** | *preferred-lifetime* } ] | [*at valid-datepreferred-date*] | [**infinite**(**infinite** | *preferred-lifetime*))] [**no-advertise**] | [[ **off-link** ] [**no-autoconfig** ]]

【参数说明】 *ipv6-prefix* : IPv6 的网络号，必须遵循 RFC4291 的地址表示形式。

*prefix-length* : IPv6 前缀的长度，注意前面必须加上 ' / ' 。

*valid-lifetime* : 主机收到路由器公告的前缀后认为有效的时间，取值范围 0-4294967295。缺省 30 天。

*preferred-lifetime* : 主机收到路由器公告的前缀后认为首选有效的时间，取值范围 0-4294967295，缺省 7 天。

*at valid-date preferred-date* : 设置公告前缀有效和首选有效的截止时间，截止时间是以日、月、年、小时、分钟表示的。

**infinite** : 表示永远都有效。

**default** : 设置要使用的缺省参数配置。

**no-advertise** : 表示该前缀不被路由器公告。

**off-link** : 主机在发送 IPV6 报文时如果目的地址的前缀匹配前缀那么认为该目的地是在同一链路(on-link)上是可直接到达的。设置了该选项表示该前缀不用来做 on-link 的判断。

**no-autoconfig** : 该选项指示主机收到该路由器公告中的前缀不能用于地址自动配置。

【命令模式】 接口模式

【使用指导】 通过该命令可以分别配置每一个前缀的各个参数，包括是否要公告该前缀，缺省情况下路由器公告报文中(RA)公告的前缀是在该接口上通过 **ipv6 address** 命令配置的前缀，如果要增加其它前缀可以使用该命令进行配置。

**ipv6 nd prefix default** 设置该接口上使用的缺省配置参数，即新增加一个前缀时，如果没有指定任何参数，那么将使用 **ipv6 nd prefix default** 所设置的参数做为配置的前缀的参数。注意一旦为该前缀指定了某个参数以后将不再认为使用缺省参数配置。即以后使用 **ipv6 nd prefix default** 改变缺省参数配置时不会去修改该前缀的配置，而只修改完全使用缺省参数配置的前缀。

*at valid-datepreferred-date* 前缀的有效时间有 2 种指定方式：一种是在公告报文中每个前缀指定一个固定的时间；另外一种是指定截止时间，使用该方式那么每次发出去的公告报文中的前缀的有效时间将采用递减的方式，直到值为 0。

## 设置是否在该接口上阻止路由器公告 ( RA ) 报文发送

【命令格式】 **ipv6 nd suppress-ra**

【参数说明】 -

【命令模式】 接口模式

【使用指导】 当要在一个接口上抑制路由器公告报文发送时可以使用 **ipv6 suppress-ra** 命令

## 设置未解析的邻居表项的最大数量

【命令格式】 **ipv6 nd unresolved** *number*

【参数说明】 *number* : 表示未解析邻居表项限制数

【命令模式】 全局模式

【使用指导】 为了防止恶意扫描攻击导致生成大量未解析的 ND 表项，占用表项资源，可以通过配置限制未解析的 ND 表项

的个数。

#### 📌 设置可处理 ND 选项数量

【命令格式】 **ipv6 nd max-opt***value*

【参数说明】 *value*：支持的选项个数

【命令模式】 全局模式

【使用指导】 配置设备处理 ND 选项数量限制，比如链路层地址选项，MTU 选项，重定向选项，前缀选项。

#### 📌 设置接口可学习邻居表项数量

【命令格式】 **ipv6 nd cache interface-limit***value*

【参数说明】 *value*：接口所能学习的邻居最大限制

【命令模式】 接口模式

【使用指导】 限制接口的邻居学习数量，可防止恶意的邻居攻击，让设备生成大量的邻居表项，占用过多的内存。配置的值必须不小于当前接口已经学习到的邻居数，否则配置不生效。该限制受限于设备支持 ND 容量。

### 配置举例

#### 📌 打开接口的 IPv6 重定向功能

【配置方法】 开启接口 IPv6 重定向功能。

```
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 redirects
```

【检验方法】 通过 **show ipv6 interface** 查看配置是否生效。

```
Ruijie#show ipv6 interface gigabitEthernet 0/0
```

```
interface GigabitEthernet 0/0 is Down, ifindex: 1, vrf_id 0
  address(es):
    Mac Address: 00:00:00:00:00:00
    INET6: FE80::200:FF:FE00:1 [ TENTATIVE ], subnet is FE80::/64
  Joined group address(es):
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds<160--240>
  ND router advertisements live for 1800 seconds
```

#### 📌 配置 IPv6 地址冲突检测

【配置方法】 配置 DAD 检测要连续发送 3 个 NS 报文。

```
Ruijie(config-if-GigabitEthernet 0/0)# ipv6 nd dad attempts 3
```

【检验方法】 通过 **show ipv6 interface** 查看配置是否生效。

```
Ruijie#show ipv6 interface gigabitEthernet 0/0

interface GigabitEthernet 0/0 is Down, ifindex: 1, vrf_id 0
  address(es):
    Mac Address: 00:00:00:00:00:00
    INET6: FE80::200:FF:FE00:1 [ TENTATIVE ], subnet is FE80::/64
  Joined group address(es):
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 3
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds<160--240>
  ND router advertisements live for 1800 seconds
Ruijie(config-if-GigabitEthernet 0/0)#
```

## ✎ 手工配置路由器公告的前缀信息

【配置方法】 为接口添加一个前缀 1234::/64。

```
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 nd prefix 1234::/6
```

【检验方法】 通过 **show ipv6 interface** 查看配置是否生效。

```
Ruijie#show ipv6 interface gigabitEthernet 0/0 ra-info

GigabitEthernet 0/0: DOWN (RA is suppressed)
  RA timer is stopped
  waits: 0, initcount: 0
  statistics: RA(out/in/inconsistent): 0/0/0, RS(input): 0
  Link-layer address: 00:00:00:00:00:00
  Physical MTU: 1500
  ND router advertisements live for 1800 seconds
  ND router advertisements are sent every 200 seconds<160--240>
  Flags: !M!0, Adv MTU: 1500
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit time is 0 milliseconds
  ND advertised CurHopLimit is 64
  Prefixes: <total: 1>
    1234::/64(Def, CFG, vltime: 2592000, pltime: 604800, flags: LA)
```

### 配置路由器公告的前缀从前缀池获取

【配置方法】 配置路由器公告的前缀从前缀池 “ra-pool” 获取

```
Ruijie(config-if-GigabitEthernet 0/0)#peel default ipv6 pool ra-pool
```

【检验方法】 通过 **show run** 查看配置是否生效。

```
Ruijie(config-if-GigabitEthernet 0/0)#show run interface gigabitEthernet 0/0

Building configuration...
Current configuration : 125 bytes

interface GigabitEthernet 0/0
  ipv6 enable
  no ipv6 nd suppress-ra
  peel default ipv6 pool ra-pool
!
```

### 配置关闭路由器公告抑制功能

【配置方法】 关闭接口抑制路由器公告功能

```
Ruijie(config-if-GigabitEthernet 0/0)# no ipv6 nd suppress-ra
```

【检验方法】 通过 **show run** 查看配置是否生效。

```
Ruijie(config-if-GigabitEthernet 0/0)#show run interface gigabitEthernet 0/0

Building configuration...
Current configuration : 125 bytes

interface GigabitEthernet 0/0
  ipv6 enable
  no ipv6 nd suppress-ra
!
```

### 配置未解析的邻居表项的最大数量

【配置方法】 配置未解析的邻居表项的最大数量为 200

```
Ruijie(config)# ipv6 nd unresolved 200
```

【检验方法】 通过 **show run** 查看配置是否生效。

```
Ruijie#show run

ipv6 nd unresolved 200
!
```

### 配置可处理 ND 选项数量

【配置方法】 配置可处理 ND 选项数量为 20

```
Ruijie(config)# ipv6 nd max-opt20
```

【检验方法】 通过 **show run** 查看配置是否生效。

```
Ruijie#show run

ipv6 nd max-opt20
!
```

#### 📌 配置接口可学习邻居表项数量

【配置方法】 配置接口可学习邻居表项数量 100

```
Ruijie(config-if-GigabitEthernet 0/1)# ipv6nd cache interface-limit 100
```

【检验方法】 通过 **show run** 查看配置是否生效。

```
Ruijie#show run

!
interface GigabitEthernet 0/1
  ipv6nd cache interface-limit 100
!
```

### 常见配置错误

---

无

## 3.4.4 配置 IPv6 源路由

### 配置效果

---

RFC5095 废除了类型 0 路由首部。锐捷的解决方法是缺省情况不支持类型 0 路由首部，管理员可以使用全局配置模式命令“ipv6 source-route”打开这项功能。

### 注意事项

---

无

### 配置方法

---

#### 📌 配置设备转发带有路由首部的 IPv6 报文

- 可选配置。
- 如果需要开启 IPv6 源路由功能，可使用该配置。

## 检验方法

---

向设备发送带有 0 路由首部的报文，设备能够正常转发。

## 相关命令

---

### 配置设备转发带有路由首部的 IPv6 报文

【命令格式】 **ipv6 source-route**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 因为类型 0 路由首部有安全隐患：使设备很容易遭受拒绝服务攻击，所以在缺省情况下禁止转发带有路由首部的 IPv6 报文，但是仍然处理最终目的地址是本机的带有类型 0 路由首部的 IPv6 报文。

## 配置举例

---

### 配置支持 IPv6 类型 0 路由。

【配置方法】 开启支持 IPv6 类型 0 路由功能。

```
Ruijie(config)#ipv6 source-route
```

【检验方法】 使用 **show run** 查看配置是否生效。

```
Ruijie#show run | inc ipv6 source-route  
ipv6 source-route
```

## 常见配置错误

---

无

## 3.4.5 配置 ICMPv6 差错报文的发送速率

### 配置效果

---

配置 ICMPv6 差错报文的发送速率。

### 注意事项

---

-

### 配置方法

---

### 配置 ICMPv6 报文太大消息的发送速率

- 可选配置。
- 如果设备收到大量 IPv6 报文的长度超过出口的 IPv6 MTU，并因发送 ICMPv6 报文太大消息而消耗较大 CPU 的情况，可以使用该配置限制该差错报文的发送。

### 配置其它 ICMPv6 差错报文的发送速率

- 可选配置。
- 如果设备收到大量非法 IPv6 报文，并因此而产生大量 ICMPv6 差错报文时，可以使用该配置限制差错报文发送速率（该命令不会影响 ICMPv6 报文太大差错报文的发送速率）

## 检验方法

执行 **show running-config** 可以看到配置生效。

## 相关命令

### 配置 ICMPv6 报文太大消息的发送速率

【命令格式】 **ipv6 icmp error-interval too-big milliseconds [bucket-size]**

【参数说明】 *milliseconds*：令牌桶的刷新周期，取值范围 0~2147483647，缺省值为 100，单位为毫秒。取值为 0 时，表示不限制 ICMPv6 差错报文的发送速率。

*bucket-size*：令牌桶中容纳的令牌数，取值范围 1~200，缺省值为 10。

【命令模式】 全局模式

【使用指导】 为了防止拒绝服务攻击，对 ICMPv6 差错报文的发送速率进行限制，采用令牌桶算法。

如果转发的 IPv6 报文的长度超过出口的 IPv6 MTU，路由器会丢弃 IPv6 报文，并且向源 IPv6 地址发送 ICMPv6 报文太大消息，这种 ICMPv6 差错报文的主要用途是 IPv6 路径 MTU 发现。为了防止其它 ICMPv6 差错报文太多导致发不出 ICMPv6 报文太大消息，从而导致 IPv6 路径 MTU 发现功能失效，对 ICMPv6 报文太大消息和其它 ICMPv6 差错报文分别限速。

因为定时器的精度是 10 毫秒，建议用户把令牌桶的刷新周期配置成 10 毫秒的整数倍。如果令牌桶的刷新周期大于 0 小于 10，实际生效的刷新周期是 10 毫秒，例如配置 5 毫秒 1 个，实际效果是 10 毫秒 2 个；如果令牌桶的刷新周期不是 10 毫秒的整数倍，实际生效的刷新周期自动换算成 10 毫秒的整数倍，例如配置 15 毫秒 3 个，实际效果是 10 毫秒 2 个。

### 配置其它 ICMPv6 差错报文的发送速率

【命令格式】 **ipv6 icmp error-interval milliseconds [bucket-size]**

【参数说明】 *milliseconds*：令牌桶的刷新周期，取值范围 0~2147483647，缺省值为 100，单位为毫秒。取值为 0 时，表示不限制 ICMPv6 差错报文的发送速率。

*bucket-size*：令牌桶中容纳的令牌数，取值范围 1~200，缺省值为 10。

【命令模式】 全局模式

【使用指导】 为了防止拒绝服务攻击，对 ICMPv6 差错报文的发送速率进行限制，采用令牌桶算法。



因为定时器的精度是 10 毫秒，建议用户把令牌桶的刷新周期配置成 10 毫秒的整数倍。如果令牌桶的刷新周期大于 0 小于 10，实际生效的刷新周期是 10 毫秒，例如配置 5 毫秒 1 个，实际效果是 10 毫秒 2 个；如果令牌桶的刷新周期不是 10 毫秒的整数倍，实际生效的刷新周期自动换算成 10 毫秒的整数倍，例如配置 15 毫秒 3 个，实际效果是 10 毫秒 2 个。

## 配置举例

### 配置 ICMPv6 差错报文的发送速率

【配置方法】 配置 ICMPv6 报文太大消息的发送速率为 1 秒 100 个，配置其它 ICMPv6 差错报文的发送速率为 1 秒 10 个。

```
Ruijie(config)#ipv6 icmp error-interval too-big 1000 100
Ruijie(config)#ipv6 icmp error-interval 1000 10
```

【检验方法】 执行 **show running-config** 可以看到配置生效。

```
Ruijie#show running-config | include ipv6 icmp error-interval
ipv6 icmp error-interval 1000 10
ipv6 icmp error-interval too-big 1000 100
```

## 常见配置错误

无

## 3.4.6 配置 IPv6 HOP-LIMIT

### 配置效果

配置发送单播报文的跳数，避免报文在网络上无限传播下去。

### 注意事项

-

### 配置方法

#### 设置 IPv6 HOP-LIMIT 值

- 可选配置
- 如果需要修订单播报文的转发跳数，可以使用该配置

### 检验方法

- 通过 **show running-config** 命令查看配置是否正确。
- 本地发送 ipv6 单播报文，抓包可以看到 ipv6 首部的 hop-limit 字段值与配置的一致。

## 相关命令

### 设置 IPv6 HOP-LIMIT 值

- 【命令格式】 **ipv6 hop-limit value**
- 【参数说明】 *value*：设备发送单播报文的跳数值，范围 1~255。
- 【命令模式】 全局模式
- 【使用指导】 -

## 配置举例

### 配置 IPv6 HOP-LIMIT

- 【配置方法】 修改设备 IPv6 HOP-LIMIT 为 250。
- ```
Ruijie(config)#ipv6 hop-limit 250
```
- 【检验方法】 通过 **show running-config** 查看配置是否生效。
- ```
Ruijie#show running-config
ipv6 hop-limit 254
```

## 常见配置错误

无

### 3.4.7 配置抑制往认证 vlan 发送广播邻居请求（NS）报文

## 配置效果

抑制在 SVI 口上往认证 vlan 发送广播邻居请求（NS）报文。

## 注意事项

只支持 SVI 口配置，且在网络认证模式下才生效。

## 配置方法

### 配置抑制往免认证 vlan 发送广播 NS 报文

- 可选配置

- 网关认证模式下，如果希望设备能往认证 vlan 发送广播 NS 报文，可使用该配置

## 检验方法

- 通过 **show running-config** 命令查看配置是否正确。

## 相关命令

### 设置抑制往免认证 vlan 发送广播 NS 报文

- 【命令格式】 **ipv6 nd suppress-auth-vlan-ns**
- 【参数说明】 -
- 【命令模式】 接口模式
- 【使用指导】 使用改命令的 no 形式，可以关闭该功能。

## 配置举例

### 配置关闭抑制往免认证 vlan 发送广播 NS 报文

- 【配置方法】 配置关闭抑制往免认证 vlan 发送广播 ns 报文。  

```
Ruijie(config-if-VLAN 2)#no ipv6 nd suppress-auth-vlan-ns
```
- 【检验方法】 通过 **show running-config interface vlan 2** 查看配置是否生效。  

```
Ruijie#show running-config interface vlan 2  
no ipv6 nd suppress-auth-vlan-ns
```

## 常见配置错误

无

## 3.4.8 配置 MGMT 口缺省网关

### 配置效果

配置 mgmt 口缺省网关，生成一条默认路由出口是 mgmt 口，下一跳是配置的网关。

### 注意事项

MGMT 口才支持。

### 配置方法

### 配置 MGMT 口缺省网关

- 可选配置
- 如果需要为 MGMT 配置一条默认路由并指定下一跳，可以使用该配置

### 检验方法

- 通过 **show running-config** 命令查看配置是否正确。

### 相关命令

#### 设置 MGMT 口缺省网关

- 【命令格式】 **ipv6 gateway ipv6-address**
- 【参数说明】 -
- 【命令模式】 接口模式
- 【使用指导】 只在 MGMT 口支持

### 配置举例

#### 配置 MGMT 口缺省网关为 2000::1

- 【配置方法】 配置 MGMT 口缺省网关为 2000::1。

```
Ruijie(config)# interface mgmt 0
Ruijie(config-mgmt)# ipv6gateway 2000::1
```

- 【检验方法】 通过 **show running-configinterface vlan 2** 查看配置是否生效。


```
Ruijie#show running-config interface mgmt 0
Ipv6 gateway 2000::1
```

### 常见配置错误

无

## 3.5 监视与维护

### 清除各类信息


 在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

作用	命令
清除动态学习到的邻居。	<b>clear ipv6 neighbors</b> [ <i>vrfvrf-name</i> ] [ <b>oob</b> ] [ <i>interface-id</i> ]

## 查看运行情况

作用	命令
显示接口上关于 IPv6 的信息	<b>show ipv6 interface</b> [[ <i>interface-id</i> ] [ <i>ra-info</i> ] ] [brief [ <i>interface-id</i> ]]
显示邻居的信息	<b>show ipv6 neighbors</b> [ <i>vrfvrf-name</i> ] [ <b>verbose</b> ][ <i>interface-id</i> ] [ <i>ipv6-address</i> ] [static] [oob]

## 查看调试信息

 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
查看 ND 学习情况	<b>debug ipv6 nd</b>

## 4 DHCP

### 4.1 概述

DHCP ( Dynamic Host Configuration Protocol , 动态主机设置协议 ) 是一个局域网的网络协议，使用 UDP 协议工作，被广泛用来动态分配可重用的网络资源，如 IP 地址。

DHCP 是基于 Client/Server 工作模式，DHCP 客户端通过发送请求消息向 DHCP 服务器获取 IP 地址，等其他配置信息。当 DHCP 客户端与服务器不在同一个子网上，必须有 DHCP 中继代理 ( DHCP Relay ) 来转发 DHCP 请求和应答消息。

#### 协议规范

- RFC2131 : Dynamic Host Configuration Protocol
- RFC2132 : DHCP Options and BOOTP Vendor Extensions
- RFC3046 : DHCP Relay Agent Information Option

### 4.2 典型应用

典型应用	场景描述
在局域网内提供 DHCP 服务	为局域网内下游用户分配地址。
设备启动 DHCP Client 功能	局域网内下游多设备启动 DHCP Client 功能。
MPLS 环境下的 DHCP Server 典型应用	L2vpn/L3vpn 环境下 DHCP Server 的应用。
AM 规则在 DHCP-server 中的典型应用	Supervlan 场景下 DHCP Server 的应用。
有线场景中 DHCP Relay 典型应用	有线场景中跨网段的用户申请 IP 上网。
AM 规则在 DHCP Relay 中的典型应用	Supervlan 场景中跨网段的用户申请 IP 上网。

#### 4.2.1 在局域网内提供 DHCP 服务

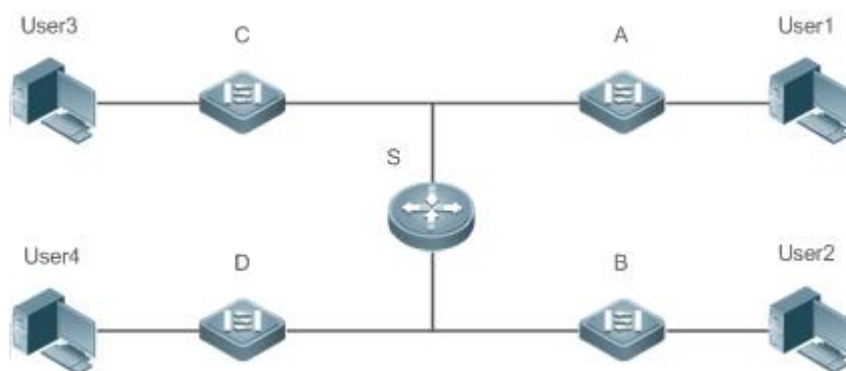
##### 应用场景

在一个局域网内，为四个用户分配 IP 地址。

以下图为例，为 User1、User2、User3 、User4 分配 IP 地址。

- User1、User2、User3 、User4 通过 A、B、C、D 与 Server 相连

图 4-1



【注释】 S 为出口网关设备，作 DHCP-Server。  
 A、B、C、D 为接入交换机，作二层透传  
 User1、User2、User3、User4 为用户

## 功能部署

- Server(S)上运行 DHCP-Server 服务
- 在 A、B、C、D 上实行二层 VLAN 透传功能
- User1、User2、User3、User4 上主动发起 DHCP-Client 请求

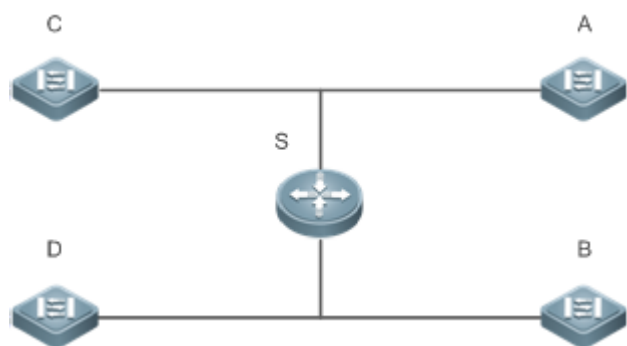
## 4.2.2 设备启动 DHCP Client 功能

### 应用场景

在一个局域网内，A、B、C、D 四个接入设备向 S 请求地址

以下图为例，A、B、C、D 接口上开启 DHCP-Client 功能，请求 IP 地址。

图 4-2



【注释】 S 为出口网关设备，作 DHCP-Server。  
A、B、C、D 为接入交换机，接口启动 DHCP-Client 功能

## 功能部署

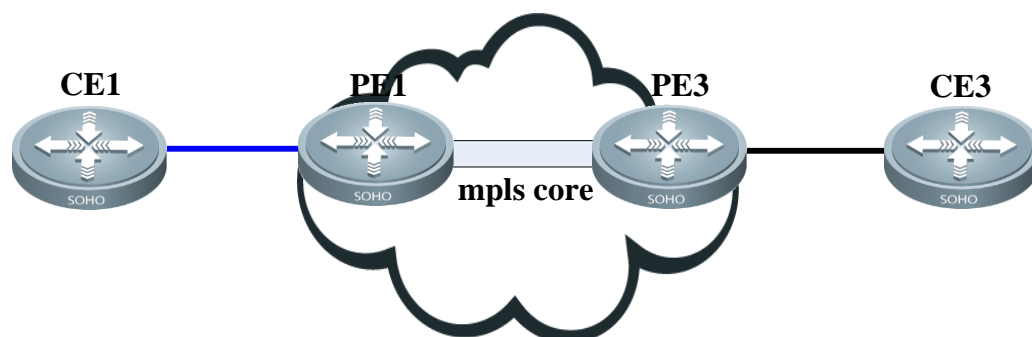
- Server(S)上运行 DHCP-Server 服务
- 在 A、B、C、D 在接口上开启 DHCP-Client 功能

### 4.2.3 MPLS 环境下的 DHCP Server 典型应用

#### 应用场景

如下图所示，如果在 L3VPN 环境下，PE1 为 DHCP-Server，CE1 为 DHCP-Client，这种场景下无影响；如果在 L2VPN 环境下，PE1 为 DHCP-Server，CE1 为 DHCP-Client，这种场景下有影响，PE1 的 AC 侧接口上无法配置 IP 地址，导致 DHCP 报文无法到达 Server 模块

图 4-3 MPLS 组网拓扑图(L2VPN/L3VPN)



【注释】 在一个 MPLS core 域内，PE1，PE3 组成一个 VPLS 网络。CE1，CE3 分别被 PE1，PE3 接入到同一个 VPLS，CE1 多归(Multi-Homing)到 PE1 和 PE3 并且接入同一个 VPLS 域。PE1 上启动 DHCP-Server

## 功能部署

- 配置 PE1、PE3 为 L3VPN 的场景，并在 PE1 启动 DHCP-Server 功能。
- CE1 上启动 DHCP-Client。

### 4.2.4 AM 规则在 DHCP-Server 中的典型应用

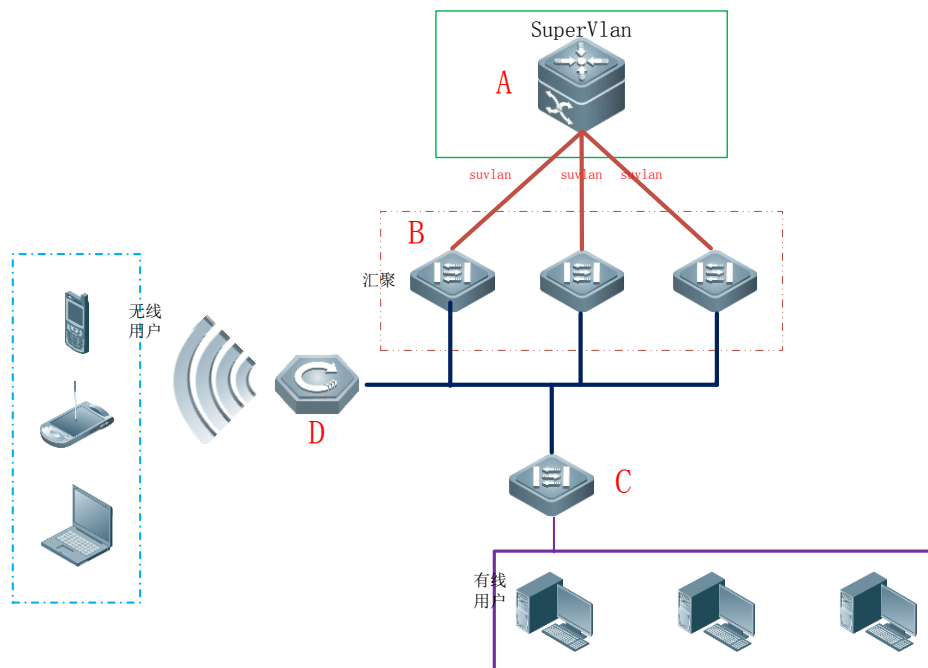
#### 应用场景



如下图 1-4 所示，设备 A 作为核心交换设备，配置 Supervlan 场景、AM 过滤规则及启动 Dhcp-Server，B 作为汇聚交换设备层，C 用作接入交换设备，D 作为无线接入交换设备。主要需求如下：

- 基于 vlan+port 的 AM 规则进行动态地址分配
- 基于 vlan 的 AM 规则进行静态地址分配
- 基于缺省 AM 规则进行动态地址分配

图 4-4 AM 规则在 DHCP-Server 中的组网拓扑图



- 【注释】
- A 作为核心设备。
  - B 作为汇聚设备。
  - C 作为有线接入设备。
  - D 作为无线接入设备。

## 功能部署

- 在 A 上配置 AM 规则、启动 Dhcp-Server 服务、创建 Supervlan。
- 在 B、C 上创建 Vlan，对有线用户 DHCP 报文透传至设备 A，进行地址获取。
- 在 D 上启动无线功能，将无线用户 DHCP 报文透传至设备 A，进行地址获取。

## 4.2.5 有线场景中 DHCP Relay 典型应用

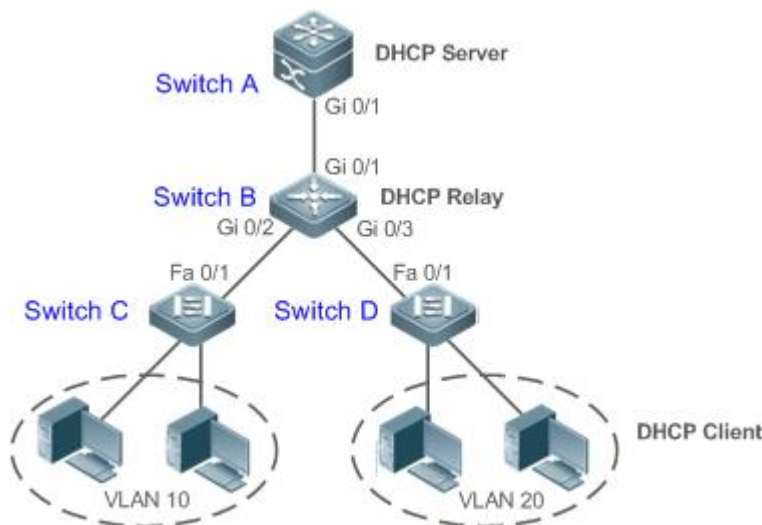
### 应用场景

如下图所示，Switch C 和 Switch D 作为接入设备，分布着 VLAN 10 和 VLAN 20 的 PC 用户，Switch B 作为网关设备，Switch A 作为核心设备。主要需求如下：

Switch A 可以充当 DHCP Server，为不同 VLAN 用户动态分配不同网段的 IP 地址。

Switch C 和 Switch D 下的接入用户可以跨网段动态获取 IP 地址。。

图 4-5DHCP Relay 组网拓扑图



- 【注释】 Switch C 与 Switch D 作为接入设备。  
Switch B 作为网关设备。  
Switch A 作为核心设备。

## 功能部署

- 配置 Switch B 和 Switch C、D 之间的二层通信。
- 在 Switch B 上，指定 DHCP 服务器地址，并开启 DHCP Relay 功能。
- 在 Switch A 上，分别为 VLAN 10 和 VLAN 20 的用户创建 DHCP 地址池，开启 DHCP Server 功能。

## 4.2.6 AM 规则在 DHCP Relay 中的典型应用

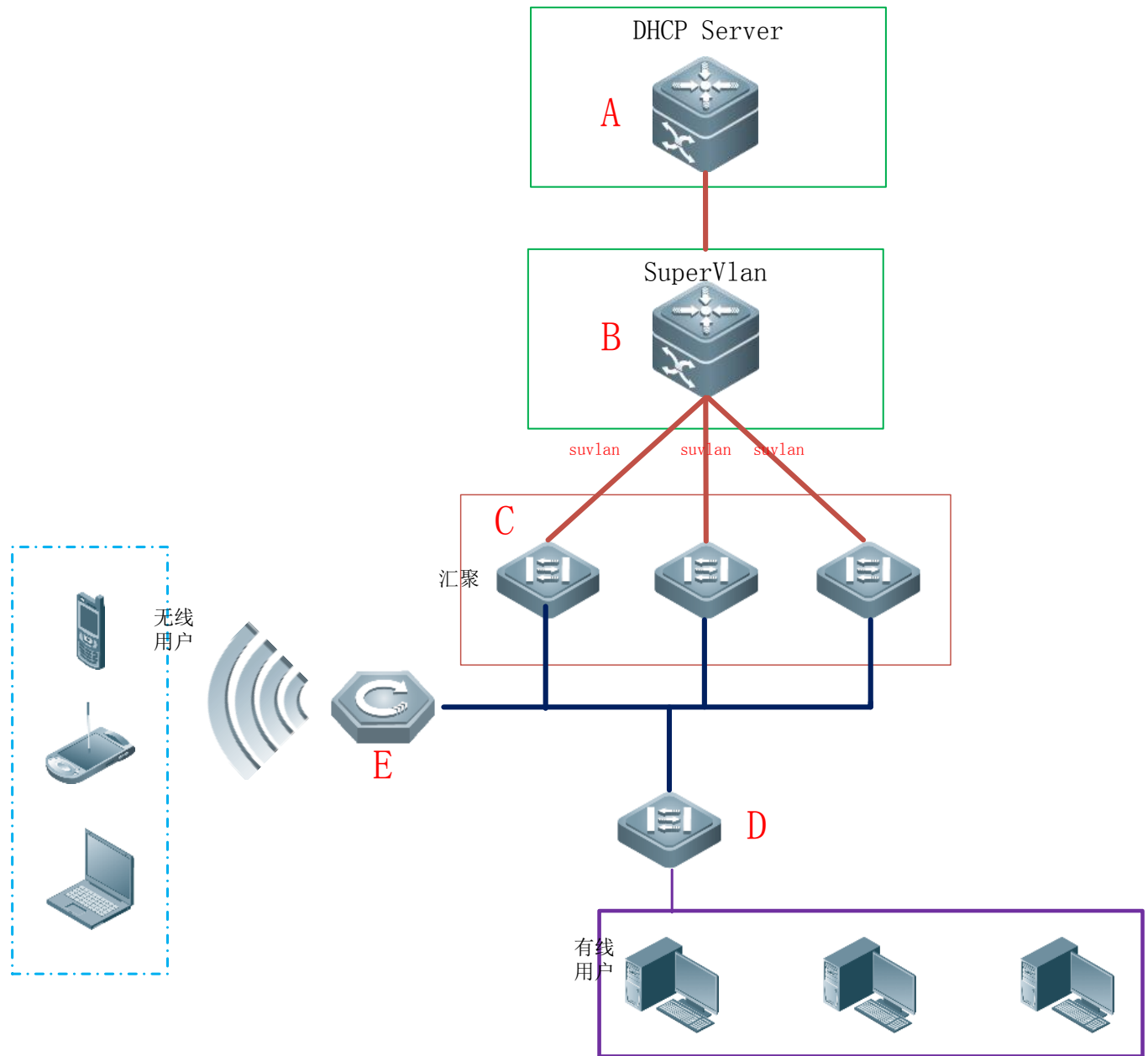
### 应用场景

如下图 1-7 所示，设备 A 作为 DHCP Server 设备，设备 B 作为核心交换设备，配置 Supervlan 场景、AM 过滤规则及启动 Dhcp Relay，C 作为汇聚交换设备层，D 用作接入交换设备，E 作为无线接入交换设备。主要需求如下：

- 基于 vlan+port 的 AM 规则进行选择客户端子网作为中继报文 Giaddress，并转发报文给 DHCP Server 分配对应客户端子网的地址

- 基于缺省 AM 规则进行选择客户端子网作为中继报文 Giaddress，并转发报文给 DHCP Server 分配对应客户端子网的地址

图 4-6 AM 规则在 DHCP Relay 中的组网拓扑图



- 【注释】
- A 作为核心设备。
  - B 作为核心设备。
  - C 作为汇聚设备。
  - D 作为有线接入设备。
  - E 作为无线接入设备。

## 功能部属

---

- 在 A 上启动 Dhcp Server 服务。
- 在 B 上配置 AM 规则、启动 Dhcp Relay 服务、创建 Supervlan。
- 在 C、D 上创建 Vlan，对有线用户 DHCP 报文透传至设备 B，进行地址获取。
- 在 E 上启动无线功能，将无线用户 DHCP 报文透传至设备 B，进行地址获取。

## 4.3 功能详解

### 基本概念

---

#### 📌 DHCP 服务器

锐捷产品的 DHCP 服务器完全根据 RFC 2131 来实现的，主要功能就是为主机分配和管理 IP 地址。

#### 📌 DHCP 客户端

DHCP 客户端可以让设备自动地从 DHCP 服务器获得 IP 地址以及其它配置参数。

#### 📌 DHCP 中继

当 DHCP 客户端与服务器不在同一个子网上，就必须有 DHCP 中继代理来转发 DHCP 请求和应答消息。

#### 📌 租约

租约是客户机可使用指派的 IP 地址期间 DHCP 服务器指定的时间长度。租用给客户时，租约是活动的。在租约过期之前，客户机一般需要通过服务器更新其地址租约时间。当租约期满或在服务器上删除时，租约是非活动的。租约期限决定租约何时期满以及客户需要用服务器更新它的次数。

#### 📌 排除地址

排除地址是指从 DHCP 服务器中排除指定的一些 IP 地址序列，排除地址作用是为了确保在这些地址都不会是由 DHCP 服务器提供给 DHCP 客户机。

#### 📌 地址池

地址池是指 DHCP 服务器可分配给用户的地址集合，所有分配给用户的地址都从管理员配置的池中取出的。

#### 📌 选项类型

选项类型是 DHCP 服务器在向 DHCP 客户机提供租约服务时指派的配置参数。例如，某些公用选项包括默认网关（路由器）、WINS 服务器和 DNS 服务器的 IP 地址。DHCP-Server 还允许配置其它选项。虽然大多数选项都是在 RFC 2132 中预定义的，但若需要的话，可添加自定义选项类型。

## 功能特性

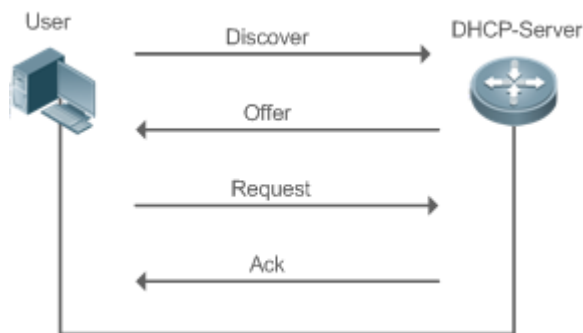
功能特性	作用
DHCP 服务器	设备启用 DHCP Server 功能，可以为主机动态分配 IP 地址和提供主机配置参数。
DHCP 中继代理	设备启用 DHCP Relayr 功能，可以在不同网段之间转发 DHCP 请求和应答消息。
DHCP 客户端	设备启用 DHCP Client 功能，可以自动从 DHCP 服务器获取 IP 地址以及其它配置参数。
AM 规则	设备启用 AM 功能，可以依据该规则进行地址分配

### 4.3.1 DHCP 服务器

#### 工作原理

##### ↳ DHCP 工作的基本流程

图 4-7



DHCP 请求 IP 地址的过程如下：

11. 主机发送 DHCPDISCOVER 广播包在网络上寻找 DHCP 服务器；
12. DHCP 服务器向主机发送 DHCPOFFER 单播/广播(依据主机报文相关属性确定)数据包，包含 IP 地址、MAC 地址、域名信息以及地址租期；
13. 主机发送 DHCPREQUEST 广播包，正式向服务器请求分配已提供的 IP 地址；
14. DHCP 服务器向主机发送 DHCPACK 单播包，确认主机的请求。

**i** DHCP 客户端可以接收到多个 DHCP 服务器的 DHCPOFFER 数据包，然后可能接受任何一个 DHCPOFFER 数据包，但客户端通常只接受收到的第一个 DHCPOFFER 数据包。另外，DHCP 服务器 DHCPOFFER 中指定的地址不一定为最终分配的地址，通常情况下，DHCP 服务器会保留该地址直到客户端发出正式请求。

正式请求 DHCP 服务器分配地址 DHCPREQUEST 采用广播包，是为了让其它所有发送 DHCPOFFER 数据包的 DHCP 服务器也能够接收到该数据包，然后释放已经 OFFER（预分配）给客户端的 IP 地址。

如果发送给 DHCP 客户端的 DHCPOFFER 信息包中包含无效的配置参数，客户端会向服务器发送 DHCPDECLINE 信息包拒绝接受已经分配的配置信息。

在协商过程中，如果 DHCP 客户端没有及时响应 DHCP OFFER 信息包，DHCP 服务器会发送 DHCP NAK 消息给 DHCP 客户端，导致客户端重新发起地址请求过程。

在网络建设中，应用锐捷产品 DHCP 服务器，可以带来以下好处：

- 降低网络接入成本。一般采用静态地址分配的接入费用比较昂贵，应用动态地址分配的接入成本较低。
- 简化配置任务，降低网络建设成本。采用动态地址分配，大大简化了设备配置，对于在没有专业技术人员的地方部署设备，更是降低了部署成本。
- 集中化管理。在对多个子网进行配置管理时，有任何配置参数的变动，只需要修改和更新 DHCP 服务器的配置即可。

## 📌 地址池

Server 收到来自 Client 请求报文，首先选择出一个合法有效地址池，并在该池中通过 PING 机制确认一个可用的地址，接着下发该池相关配置信息与地址至客户端，同时本地保存该租约信息在，以供该客户端续租时检查有效性使用；由此完成整个租约分配流程。

地址池中可以带有各种配置参数，以下列举几个常用的：

- 地址池范围，可以分配给用户的地址范围
- 网关地址，通告用户网关地址，最多可以有八个
- DNS 地址，通告用户 DNS 地址，最多可以有八个
- 租约周期，通告用户地址何时老化，用户何时该请求续租

## 📌 VRRP 监控功能

在 VRRP (Virtual Router Redundancy Protocol，虚拟路由冗余协议)应用场景下，DHCP 提供配置命令来决定是否监控当前接口的 VRRP 状态。对于配置了 VRRP 地址的接口，当配置监控 VRRP 状态后，DHCP 服务器仅对处于 Master 状态的设备接口上来的 DHCP 客户端请求报文进行处理，处于备份(Backup)状态的接口请求报文将被丢弃。而对于没配置 VRRP 地址的接口，DHCP 服务器不再监控 VRRP 状态，所有 DHCP 请求报文都会得到处理。VRRP 监控命令只能在三层口上配置，默认情况下 VRRP 监控功能关闭，即只有主机处理 DHCP 业务备机不处理。

## 📌 基于 vlan+端口+ip-range 地址分配功能

在部署地址池的环境下，为每个 vlan+端口号来分配指定 ip-range 的地址功能(在满足正常动态地址分配逻辑后，才能从本配置中选择有效地址)。主要有三种应用场景：1.只有全局默认配置；2.只有基于 vlan+端口+ip-range 的配置；3.上述两种配置均有；场景 1 有全局配置，默认分配全局配置的区间地址；场景 2 来自指定 vlan+端口的用户分配指定区间的地址，其余则用户无地址分配；场景 3 满足场景 2 的分配指定区间地址，其余用户分配全局默认配置地址。

## 📌 基于 ARP 检测用户下线

DHCP 提供配置命令来决定是否基于 ARP 检测用户下线。当配置了基于 ARP 检测用户下线时，用户下线后，DHCP 服务器会收到 ARP 老化通告，开始回收地址。如果一段时间内（默认 5 分钟），用户没有重新上线，DHCP 服务器就回收该地址，分配给新用户；如果在该段时间内重新上线，用户可以继续使用该地址。

## 📌 添加伪服务器检测功能

如果网络中私自部署 DHCP 服务器，当客户端申请地址时，会与这台服务器进行交互，导致客户端分配到错误的 IP 地址。这台服务器称为伪服务器。DHCP 提供配置命令来决定是否开启伪服务器检测功能。当配置伪服务器检测功能时，DHCP 会检查

接收到的 DHCP 报文中是否携带 Option 54（Server Identifier Option，服务器标识选项）。如果携带该选项，并且选项内容与真实 DHCP 服务器标识不相符，则记录此伪服务器的 IP 地址和接收到报文的端口信息。伪服务器检测只是一种事后检测的安全功能，并不能预防非法 DHCP 服务器给客户端分配地址。

## 相关配置

### 全局启动 DHCP-Server 服务

- 缺省情况下，该服务关闭。
- 全局使用 **service dhcp** 开启该服务。
- 必须在全局使用 **service dhcp** 功能，才能进行 DHCP 服务。

### 配置地址池

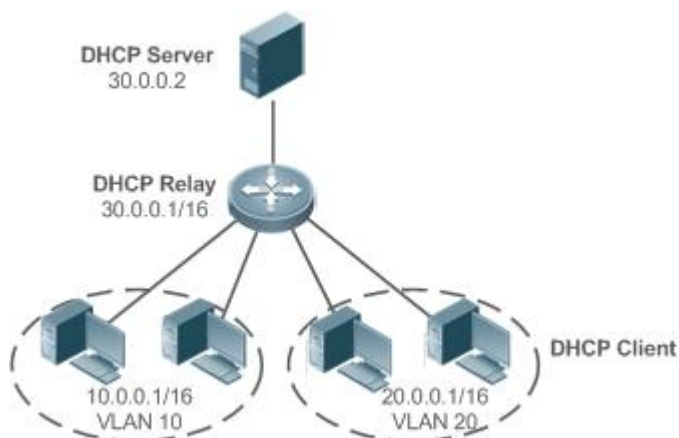
- 缺省情况下，无地址池。
- 使用 **ip dhcp pool** 命令可以进入到地址池配置模式，进行地址范围、网关地址、DNS 等信息配置。
- 不配置地址池范围将无地址可分配，无法下发任何地址。

## 4.3.2 DHCP 中继代理

### 工作原理

DHCP 请求报文的源 IP 地址为 255.255.255.255，这种类型报文的转发局限于子网内。为了实现跨网段的动态 IP 地址分配，DHCP 中继就产生了。DHCP 中继将收到的 DHCP 请求报文以单播方式转发给 DHCP 服务器，同时将收到的 DHCP 响应报文转发给 DHCP 客户端。DHCP 中继相当于一个转发站，负责沟通位于不同网段的 DHCP 客户端和 DHCP 服务器，即转发客户端 DHCP 请求报文、转发服务端 DHCP 应答报文。这样就实现了只要安装一个 DHCP 服务器，就可以实现对多个网段的动态 IP 管理，即 Client—Relay—Server 模式的 DHCP 动态 IP 管理。如图所示：

图 4-8 DHCP Relay 应用场景



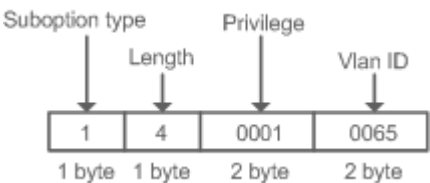
VLAN 10和VLAN 20分别对应 10.0.0.1/16和 20.0.0.1/16的网络,而 DHCP 服务器在 30.0.0.1/16的网络上,30.0.0.2的 DHCP 服务器要对 10.0.0.1/16和 20.0.0.1/16的网络进行动态 IP 管理,只要在作为网关的设备上打开 DHCP 中继功能,并配置 30.0.0.2 为 DHCP 服务器的 IP 地址。

📌 DHCP Relay Agent Information(option 82)

根据 RFC3046 的定义,中继设备进行 DHCP Relay 时,可以通过添加 option 的方式来详细的标明 DHCP 客户端的一些网络信息,从而使服务器可以根据更精确的信息给用户分配不同权限的 IP,根据 RFC3046 的定义,所使用 option 选项的选项号为 82,故也被称作 option 82。锐捷实现的 Relay agent information 目前存在四种应用方案,下面分别对四种应用方案进行说明:

- 15. Relay agent information option dot1x: 此种应用方案需要结合 802.1x 认证以及锐捷产品 RG-SAM。DHCP 中继根据 RG-SAM 在 802.1x 认证过程中下发的 IP 权限,以及 DHCP 客户端所属 vid,组合构成 Circuit ID 子选项。选项格式如图 4-9 所示:

图 4-9 选项格式



- 16. Relay agent information option82: 此种 option 的应用不需要结合其他协议模块的运行。DHCP 中继根据接收 DHCP 请求报文的实体端口,以及设备自身的物理地址信息,组合构成 option82 选项。选项格式如下图所示:

图 4-10 Agent Circuit ID

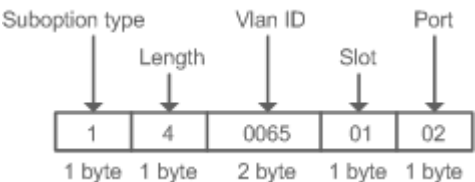
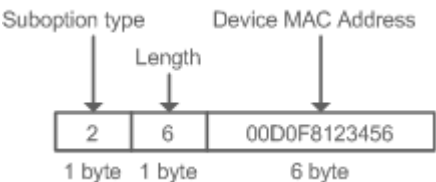


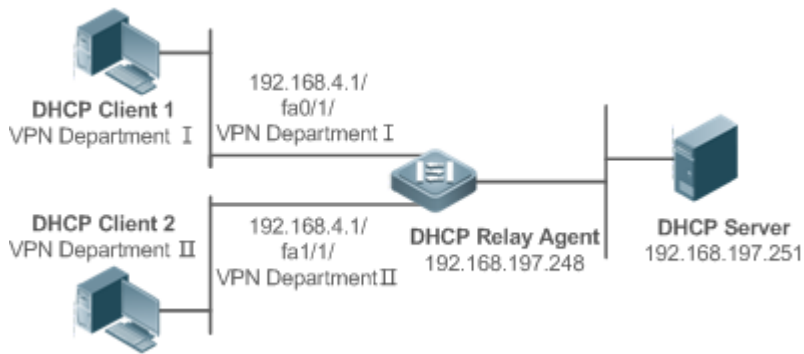
图 4-11 Agent Remote ID



- 17. Relay agent information option vpn: 此种 option 的应用需要结合 MPLS VPN 相关功能。

图 4-12 MPLS VPN 环境中应用

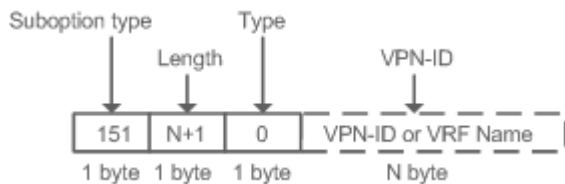




如图 4-12 所示，在 MPLS VPN 环境中，DHCP Client 1 和 DHCP 中继上的 fa0/1 口相连，DHCP Client 2 和 DHCP 中继上的 fa1/1 相连，接口 fa0/1 和接口 fa1/1 分别属于不同的 VRF，DHCP Client 1 和 DHCP Client 2 通过 DHCP 获取地址。按照网络规划，VPN DepartmentI 和 VPN DepartmentII 使用重叠网段 192.168.4.0/24，在该应用环境下，传统的 DHCP 应用根本无法支持该部署。为了实现在 MPLS VPN 环境下对 DHCP 中继的支持，在 DHCP 中继中引入了 option vpn 选项，该选项包括 VPN-ID、Subnet-Selection 以及 Server-Identifier-Override 三个子选项，简单说明一下这三个子选项的意义：

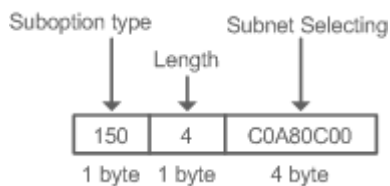
- **VPN-ID**：在接收到 DHCP 请求报文时，将 DHCP 客户端所属的 VPN 信息，以选项形式加入 DHCP 请求报文中。DHCP 服务器发送响应报文时，将该选项信息原样保留，DHCP 中继根据该选项，将 DHCP 响应报文转发到正确的 VRF 中。选项格式如下图所示：

图 4-13 VPN-ID



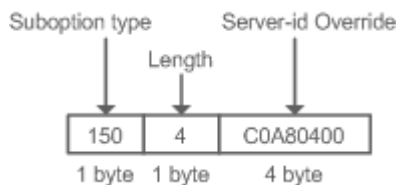
- **Subnet-Selection**：在传统的 DHCP 中继环境中，通过 gateway address[giaddr]字段表示客户端所在的网络信息以及 DHCP 服务器与 DHCP 中继的通讯地址。在 MPLS VPN 环境中，将 giaddr 修改为 DHCP 中继连接 DHCP 服务器的接口 IP，使 DHCP 服务器可以与 DHCP 中继直接通讯。但是客户端的子网信息必须通过新的选项 Subnet-Selection 来表示。选项格式如下图所示：

图 4-14 Subnet-Selection



- **Server-Identifier-Override**：在 MPLS VPN 环境下，DHCP 客户端后续的请求报文都无法直接发送到 DHCP 服务器。DHCP 中继使用该选项携带 DHCP 中继与 DHCP 客户端直连的接口地址信息，DHCP 服务器发送响应报文的时候，用该选项覆盖 Server-identifier 选项信息。从而使 DHCP 客户端在与 DHCP 服务器交互的过程中，能够将报文送往 DHCP 中继，然后由 DHCP 中继将报文转发到 DHCP 服务器。选项格式如下图所示：

图 4-15 Server-Identifier-Override



18. Relay agent information option82：此种 option 的应用不需要结合其他协议模块的运行。与之前的 option82 相比较，其选项的填充内容有所改变，且支持自定义的内容填充；默认情况下，DHCP 中继根据接收 DHCP 请求报文的实体端口信息，以及设备自身的物理地址信息和设备名称，组合构成 option82 选项。选项格式如下图所示：

图 1-18 Option82.1-circuit-id

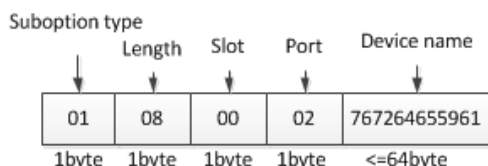
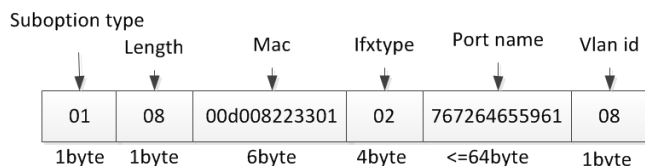


图 1-19 Option82-remote-id



## DHCP Relay Check Server-id 功能

在 DHCP 应用环境中，通常会为每一个网络配备多个 DHCP 服务器，从而进行备份，防止因为一台服务器的工作不正常影响网络的正常使用。在 DHCP 获取的四个交互过程中，当 DHCP 客户端在发送 DHCP REQUEST 时已经选定了服务器，此时会在请求的报文中携带一个 server-id 的 option 选项，在某些特定的应用环境中为了减轻网络服务器压力，需要我们 Relay 能够使能此选项，只把请求报文发给此选项里的 DHCP 服务器，而不是发送给每一个配置的 DHCP 服务器，上述就是 DHCP Relay check server-id 功能。

## DHCP Relay suppression 功能

在指定接口上配置命令 `ip DHCP Relay suppression` 后，将屏蔽该接口上收到的 DHCP 请求报文；而对于其他接口上收到的 DHCP 请求报文，则正常转发。

## 相关配置

### 启动设备上的 DHCP Relay 功能

- 缺省情况下，设备上的 DHCP Relay 功能关闭。
- 使用 **service dhcp** 命令可以启动设备上的 DHCP Relay 功能。
- 必须在设备上启用 DHCP Relay 功能，DHCP Relay 才能正常工作。

### 配置 DHCP 服务器的 IP 地址

- 缺省情况下，无 DHCP 服务器的 IP 地址表项。
- 使用 **ip helper-address** 命令可以添加 DHCP 服务器地址表项，DHCP 服务器地址可以全局配置，也可以在三层接口上配置。全局或者每个三层接口上最多可以配置 20 个 DHCP 服务器地址。
- 在接口上收到 DHCP 请求报文时，首先使用接口上的 DHCP 服务器列表；如果接口上面没有配置 DHCP 服务器列表，则使用全局配置的 DHCP 服务器列表。

### 启动 DHCP option 82 功能

- 缺省情况下，设备上的 DHCP option 82 功能关闭。
- 使用 **ip dhcp relay information option82** 命令可以启动设备上的 DHCP option 82 功能。

### 启动 DHCP Relay check server-id 功能

- 缺省情况下，设备上的 DHCP Relay check server-id 功能关闭。
- 使用 **ip dhcp relay check server-id** 命令可以启动设备上的 DHCP Relay check server-id 功能。

### 启动 DHCP Relay suppression 功能

- 缺省情况下，所有接口上 DHCP Relay suppression 功能关闭。
- 使用 **ip dhcp relay suppression** 命令可以启动对应接口上的 DHCP Relay suppression 功能。

### 启动 DHCP Relay multiple-giaddr 功能

- 缺省情况下，DHCP Relay 支持多 giaddr IP 功能关闭。
- 使用 **ip dhcp relay multiple-giaddr** 命令可以启动 DHCP Relay 支持多 giaddr IP 功能。

### 启动 DHCP Relay 网关自动切换功能

- 缺省情况下，DHCP Relay 网关自动切换功能关闭。
- 使用 **ip dhcp smart-relay** 命令可以启动网关自动切换功能。

## 4.3.3 DHCP 客户端

### 工作原理

Client 状态机进入 Init 状态，主动发出广播 Discover 报文，之后 Client 有可能收到多份 Offer，进入 Offer 选择阶段选择一份最优的 Offer 后给予该服务器响应，此后在地址的老化 1/2、4/5 周期内还会发出续租等报文请求对地址的继续使用。

### 相关配置

#### 接口上启动 DHCP-Client 功能

- 缺省情况下，该服务关闭。

- 接口模式下使用 **ip address dhcp** 开启功能。
- 必须开启客户端功能，才能进行 DHCP 服务。
- 该功能只在三层接口上有效，如 SVI、Router Port 等；

#### 4.3.4 AM 规则

##### 工作原理

AM 规则用于规划不同 vlan + port/vlan 上来的 DHCP 客户端请求的 IP 范围，可快速定位出问题的 DHCP 客户端所属的 vlan + port/vlan，也可以更有效地分配地址池的地址。使用 AM 规则后，所有来自配置 vlan + port/vlan 的 DHCP 客户端能够正常获得地址；反之，若 DHCP 客户端来源未配置 vlan + port/vlan 时：如果配置了缺省 AM 规则，DHCP 客户端将获得缺省区间中的地址，如果未配置缺省 AM 规则，DHCP 客户端无法获得地址。

##### 相关配置

##### 在全局配置模式下进入 AM 规则配置模式

- 全局配置模式下使用 **address-manage** 进入 AM 配置模式；
- 使用 **match ip default** 命令配置缺省 AM 规则；
- 使用 **match ip** 命令配置基于 vlan+port/vlan 的 AM 规则；





## 4.4 配置详解

### 配置 DHCP 服务器

配置项	配置建议 & 相关命令	
配置 DHCP 服务器动态分配 IP 地址	 必须配置，用于启用 DHCP 服务器实现动态 IP 地址分配。	
	<b>service dhcp</b>	启动 DHCP-SERVER 功能
	<b>ip dhcp pool</b>	配置地址池
	<b>network</b>	配置 DHCP 地址池的网络号和掩码
	 可选配置，用于设置地址池相关属性。	
	<b>default-router</b>	配置客户端缺省网关
	<b>lease</b>	配置地址租期
	<b>next-server</b>	配置客户端启动的下载服务器地址
	<b>bootfile</b>	配置客户端启动文件
	<b>domain-name</b>	配置客户端的域名
	<b>dns-server</b>	配置域名服务器

	<b>netbios-name-server</b>	配置 NetBIOS WINS 服务器
	<b>netbios-node-type</b>	配置客户端 NetBIOS 节点类型
	<b>lease-threshold</b>	配置地址池告警门限值
	<b>option</b>	配置自定义选项
	<b>pool-status</b>	配置地址池启用或关闭
配置 DHCP 服务器手工地址绑定	 可选配置，用于为客户静态配置 IP 地址。	
	<b>ip dhcp pool</b>	配置地址池名并进入地址池配置模式
	<b>host</b>	配置客户端主机的 IP 地址和网络掩码
	<b>hardware-address</b>	配置客户端的硬件地址
	<b>client-identifier</b>	配置客户端的唯一标识
	<b>client-name</b>	配置客户端的名字
配置 DHCP 服务器全局属性	 可选配置，用于设置 DHCP 服务器相关属性。	
	<b>ip dhcp excluded-address</b>	配置排除地址
	<b>ip dhcp force-send-nak</b>	配置 DHCP 服务器强制回复 NAK
	<b>ip dhcp monitor-vrrp-state</b>	配置监控 VRRP 状态
	<b>ip dhcp ping packets</b>	配置 Ping 包次数
	<b>ip dhcp ping timeout</b>	配置 Ping 包超时时间
	<b>ip dhcp server arp-detect</b>	配置 DHCP 服务器检测用户下线
配置 DHCP 服务器 AM 规则	 可选配置，用于设置 DHCP 服务器相关属性。	
	<b>match ip default</b>	配置基于 vlan/port 规则下的缺省 AM 规则
	<b>match ip ip-address</b>	配置基于 vlan/port 规则下的 AM 规则

## 配置 DHCP 中继代理

配置项	配置建议 & 相关命令	
配置 DHCP Relay 基本功能	 必须配置。用于建立 DHCP Relay 服务。	
	<b>service dhcp</b>	启动 DHCP Relay 功能
	<b>ip helper-address</b>	配置 DHCP 服务器的 IP 地址
配置 DHCP Relay option 82 功能	 可选配置。结合设备自身物理接口信息,给用户分配不同权限 IP。该功能与 <b>dhcp option dot1x</b> 不可以同时使用。	
	<b>ip dhcp relay information option82</b>	启用 DHCP option82 功能
配置 DHCP Relay check server-id 功能	 可选配置。DHCP Relay 仅将 DHCP 请求报文转发到 option server-id 中指定的服务器。	
	<b>ip dhcp relay check server-id</b>	启用 DHCP Relay check server-di 功能
配置 DHCP Relay suppression 功能	 可选配置。屏蔽对应接口地址上 DHCP 请求报文。	

	<b>ip dhcp relay suppression</b>	启用 DHCP Relay suppression 功能
<a href="#">配置网关 IP 自动切换功能</a>	 可选配置。使能网关自动切换功能。	
	<b>ip dhcp smart-relay</b>	配置网关启动切换功能

#### 配置 DHCP 客户端

配置项	配置建议 & 相关命令	
配置 DHCP 客户端	 必须配置，用于启用 DHCP 客户端	
	<b>ip address dhcp</b>	使得以太网或者 PPP、HDLC、FR 封装的接口能够通过 DHCP 获得 IP 地址信息

### 4.4.1 配置 DHCP 服务器动态分配 IP 地址

#### 配置效果

向所有 dhcp-client 提供 dhcp 服务，包括地址、网关等信息下发

#### 注意事项

DHCP 服务器和 DHCP 中继共用 **service dhcp** 这条命令，但是这两个功能是互斥的，两者之间的切换依赖于是否配置了 DHCP 地址池。

#### 配置方法

##### 启动 DHCP-SERVER 功能

- 实现动态分配地址功能，为必选配置。
- 在配置模式下执行 **service dhcp** 命令。

##### 配置地址池

- 创建地址池，为必选配置。
- 在配置模式下执行 **ip dhcp pool** 命令。

##### 配置 DHCP 地址池的网络号和掩码

- 动态分配地址范围，为必选配置。
- 在地址池模式下执行 **network** 命令。

##### 配置客户端缺省网关

- 用于通告客户端网关地址，为可选配置。
- 在地址池模式下执行 **default-router** 命令。

### 配置地址租期

- 用于通告客户端租约老化周期，默认值为 24h，为可选配置。
- 在地址池模式下执行 **lease** 命令。

### 配置客户端启动的下载服务器地址

- 用于通告客户端 TFTP 服务器地址，为可选配置。
- 在地址池模式下执行 **next-server** 命令。

### 配置客户端的域名

- 用于通告客户端的域名，为可选配置。
- 在地址池模式下执行 **domain-name** 命令。

### 配置域名服务器

- 用于通告客户端 dns 地址，为可选配置。
- 在地址池模式下执行 **dns** 命令。

### 配置 NetBIOS WINS 服务器

- 用于通告 windows 客户端 dns 地址，为可选配置。
- 在地址池模式下执行 **netbios-name-server** 命令。

### 配置客户端 NetBIOS 节点类型

- 用于通告 windows 客户端节点类型，为可选配置。
- 在地址池模式下执行 **netbios-name-type** 命令。

### 配置地址池告警门限值

- 用于管理租约数量，达到限制时打印警告，默认为 90%，为可选配置。
- 在地址池模式下执行 **lease-threshold** 命令。

### 配置自定义选项

- 用于通告客户端配置信息，为可选配置。
- 在地址池模式下执行 **option** 命令。

### 配置地址池启用或关闭

- 用于配置地址池是否可用，默认为开启，为可选配置。
- 在地址池模式下执行 **pool-status** 命令。

## 检验方法

利用 DHCP 客户端与 DHCP 服务器进行连接

- 检查客户端是否能取到服务器上配置的相关信息

## 相关命令

### 启动 DHCP-SERVER 功能

- 【命令格式】 **service dhcp**
- 【参数说明】 -
- 【命令模式】 全局模式
- 【使用指导】 启用 DHCP 服务器和 DHCP 中继代理功能，DHCP 服务器和 DHCP 中继共用 **service dhcp** 这条命令，两功能可以同时存在，但是报文是通过 Relay 转发还是直接由 Server 处理，取决于设备上是否配置了合法有效的地址池，如果存在地址池则由 Server 处理，不存在由 Relay 转发。

### 配置地址池

- 【命令格式】 **ip dhcp pool dhcp-pool**
- 【参数说明】 *pool-name*：地址池名称
- 【命令模式】 全局模式
- 【使用指导】 要给用户下发地址，首先要配置地址池名并进入地址池配置模式

### 配置 DHCP 地址池的网络号和掩码

- 【命令格式】 **network network-number mask [low-ip-address high-ip-address]**
- 【参数说明】 *network-number*: DHCP 地址池的 IP 地址网络号  
*mask*: DHCP 地址池的 IP 地址网络掩码。如果没有定义掩码，缺省为自然网络掩码
- 【命令模式】 DHCP 地址池配置模式
- 【使用指导】 进行动态地址绑定的配置，必须配置新建地址池的子网及其掩码，为 DHCP 服务器提供了一个可分配给客户端的地址空间。DHCP 在分配地址池中的地址，是按顺序进行的，如果该地址已经在 DHCP 绑定表中或者检测到该地址已经在该网段中存在，就检查下一个地址，直到分配一个有效的地址。  
锐捷无线产品中新增了可以配置地址池的网段范围，指明可以分配的网段中的起始地址和终止地址，该配置为可选配置。在不指明起始地址和终止地址的情况下，地址池的可分配的 IP 地址范围为该网段内的所有 IP 地址。锐捷产品的 DHCP 动态地址池中，地址的分配是以客户端的物理地址和客户端 ID 为索引的，这意味着 DHCP 动态地址池中不可能存在相同客户端的两份租约；如果客户端和服务端之间的网络拓扑存在路径上的冗余[客户端可以通过直连路径，同时也可以通过中继路径到达服务器]，就会导致服务器分配地址出现问题，可能导致地址分配失败；  
因此，为了避免上述问题，要求网络管理员在构建网络的时候，通过其它的方式，如调整物理链路或者网络路径，来避免这种客户端到服务器的路径冗余

### 配置客户端缺省网关

- 【命令格式】 **default-router address [address2...address8]**
- 【参数说明】 *address*：定义客户端默认网关的 IP 地址。要求至少配置一个  
*ip-address2...ip-address8*：(可选) 最多可以配置 8 个网关
- 【命令模式】 DHCP 地址池配置模式
- 【使用指导】 配置客户端默认网关，这个将作为服务器分配给客户端的默认网关参数。缺省网关的 IP 地址必须与 DHCP 客户端的 IP 地址在同一网络



## 配置地址租期

- 【命令格式】 **lease** {*days* [*hours*] [*minutes*] | **infinite**}
- 【参数说明】 *days* : 定义租期的时间，以天为单位  
*hours*: (可选) 定义租期的时间，以小时为单位。定义小时数前必须定义天数  
*minutes*: (可选) 定义租期的时间，以分钟为单位。定义分钟前必须定义天数和小时数  
**infinite**: 定义没有限制的租期
- 【命令模式】 DHCP 地址池配置模式
- 【使用指导】 DHCP 服务器给客户端分配的地址，缺省情况下租期为 1 天。当租期快到时客户端需要请求续租，否则过期后就不能使用该地址

## 配置客户端启动文件

- 【命令格式】 **bootfile** *filename*
- 【参数说明】 *file-name* : 定义用于启动的文件名
- 【命令模式】 DHCP 地址池配置模式
- 【使用指导】 客户端启动文件是客户端启动时要用到的启动映像文件。启动映像文件通常是 DHCP 客户端需要下载的操作系统

## 配置客户端的域名

- 【命令格式】 **domain-name** *domain*
- 【参数说明】 *domain-name*: 定义 DHCP 客户端的后缀域名字符串
- 【命令模式】 DHCP 地址池配置模式
- 【使用指导】 可以指定客户端的域名，这样当客户端通过主机名访问网络资源时，不完整的主机名会自动加上域名后缀形成完整的主机名

## 配置域名服务器

- 【命令格式】 **dns-server** { *ip-address* [ *ip-address2*...*ip-address8* ] }
- 【参数说明】 *ip-address*: 定义 DNS 服务器的 IP 地址。要求至少配置一个  
*ip-address2*...*ip-address8*: (可选) 最多可以配置 8 个 DNS 服务器
- 【命令模式】 DHCP 地址池配置模式
- 【使用指导】 当客户端通过主机名访问网络资源时，需要指定 DNS 服务器进行域名解析。要配置 DHCP 客户端可使用的域名服务器

## 配置 NetBIOS WINS 服务器

- 【命令格式】 **netbios-name-server** *address* [*address2*...*address8*]
- 【参数说明】 *address*: 定义 WINS 服务器的 IP 地址。要求至少配置一个  
*ip-address2*...*ip-address8*: (可选) 最多可以配置 8 个 WINS 服务器
- 【命令模式】 DHCP 地址池配置模式
- 【使用指导】 WINS 是微软 TCP/IP 网络解析 NetBIOS 名字到 IP 地址的一种域名解析服务。WINS 服务器是一个运行在 Windows NT 下的服务器。当 WINS 服务器启动后，会接收从 WINS 客户端发送的注册请求，WINS 客户端关闭时，会向 WINS 服务器发送名字释放消息，这样 WINS 数据库中与网络上可用的计算机就可以保持一致了

## 配置客户端 NetBIOS 节点类型

【命令格式】 **netbios-node-type** *type*

【参数说明】 *type*: 定义 NetBIOS 节点类型，有两种方式  
数字定义，范围从 0~FF，十六进制数，但只能取以下值：

- 1，代表 b-node
- 2，代表 p-node
- 4，代表 m-node
- 8，代表 h-node

字符串定义：

- b-node，广播型节点
- p-node，对等型节点
- m-node，混合型节点
- h-node，复合型节点

【命令模式】 DHCP 地址池配置模式

【使用指导】 微软 DHCP 客户端 NetBIOS 节点类型有四种：1) Broadcast，广播型节点，通过广播方式进行 NetBIOS 名字解析；2) Peer-to-peer，对等型节点，通过直接请求 WINS 服务器进行 NetBIOS 名字解析；3) Mixed，混合型节点，先通过广播方式请求名字解析，后通过与 WINS 服务器连接进行名字解析；4) Hybrid，复合型节点，首先直接请求 WINS 服务器进行 NetBIOS 名字解析，如果没有得到应答，就通过广播方式进行 NetBIOS 名字解析。

缺省情况下，微软操作系统的节点类型为广播型或者复合型。如果没有配置 WINS 服务器，就为广播型节点；如果配置了 WINS 服务器，就为复合型节点

## 配置自定义选项

【命令格式】 **option code** { *ascii string* | *hex string* | *ip ip-address* }

【参数说明】 *code*: 定义 DHCP 选项代码

*ascii string*: 定义一个 ASCII 字符串

*hex string*: 定义十六进制字符串

*ip ip-address*: 定义 IP 地址列表

【命令模式】 DHCP 地址池配置模式

【使用指导】 DHCP 提供了一个机制，允许在 TCP/IP 网络中将配置信息传送给主机。DHCP 报文专门有 option 字段，该部分内容可为变化内容，用户可以根据实际情况进行定义，DHCP 客户端必须能够接收携带至少 312 字节 option 信息的 DHCP 报文。另外 DHCP 报文中的固定数据字段也称为一个选项

在 WLAN 无线应用环境中，AP 上的 DHCP 客户端会动态申请获取 AC 的 IP 地址列表，可以通过在 DHCP 服务器上配置自定义选项携带 AC 的 IP 地址列表来实现

## 配置地址池启用或关闭

【命令格式】 **pool-status** {*enable* | *disable*}

【参数说明】 **enable**: 启用地址池

**disable**: 关闭地址池

默认为开启

【命令模式】 DHCP 地址池配置模式

【使用指导】 在锐捷无线产品中新增了可配置 DHCP 地址池是否启用命令，通过配置命令可以启用或关闭对应地址池服务

## 配置举例

### 配置地址池

- 【配置方法】
- 定义了一个地址池 net172
  - 地址池网段为 172.16.1.0/24
  - 缺省网关为 172.16.1.254
  - 地址租期为 1 天
  - 排除 172.16.1.2~172.16.1.100 地址

```
Ruijie(config)# ip dhcp excluded-address 172.16.1.2 172.16.1.100
Ruijie(dhcp-config)# ip dhcp pool net172
Ruijie(dhcp-config)# network 172.16.1.0 255.255.255.0
Ruijie(dhcp-config)# default-router 172.16.1.254
Ruijie(dhcp-config)# lease 1
```

- 【检验方法】 1.show run 查看

```
Ruijie(config)#show run | begin ip dhcp
ip dhcp excluded-address 172.16.1.2 172.16.1.100
ip dhcp pool net172
network 172.16.1.0 255.255.255.0default-router 172.16.1.254
lease 1
```

## 4.4.2 配置 DHCP 服务器手工地址绑定

### 配置效果

向某些特定的 dhcp-client 下发特定的 ip 地址及其它配置信息

### 注意事项

无

### 配置方法

#### 配置地址池名并进入地址池配置模式

- 创建地址池，为必选配置。
- 在配置模式下执行 **ip dhcp pool** 命令。

### 配置客户端主机的 IP 地址和网络掩码

- 配置静态 ip 地址及网络掩码，必选配置。
- 在地址池模式下执行 **host** 命令。

### 配置客户端的硬件地址

- 配置静态 mac 地址，可选配置。
- 在地址池模式下执行 **hardware** 命令。

### 配置客户端的唯一标识

- 配置静态用户 uid，可选配置。
- 在地址池配置下执行 **client-identifier** 命令。

### 配置客户端的名字

- 配置静态用户名字，可选配置。
- 在地址池模式下执行 **host-name** 命令。

## 检验方法

对应的用户上线，判断是否能取到相应地址。

## 相关命令

### 配置地址池

- 【命令格式】 **ip dhcp pool** *dhcp-pool*
- 【参数说明】 *pool-name*：地址池名称
- 【命令模式】 全局模式
- 【使用指导】 要给用户下发地址，首先要配置地址池名并进入地址池配置模式

### 手工地址绑定

- 【命令格式】 **host** *ip-address* [*netmask*]  
**client-identifier** *unique-identifier*  
**client-name** *name*
- 【参数说明】 *ip-address*: 定义 DHCP 客户端主机的 IP 地址  
*netmask*: 定义 DHCP 客户端主机的网络掩码  
*unique-identifier*：定义客户端硬件地址，如 aabb.bbbb.bb88;定义客户端的标识，如 01aa.bbbb.bbbb.88  
*name*: (可选) 用标准的 ASCII 字符定义客户端的名字，名字不要包括域名。如定义 mary 主机名，不可定义成 mary.rg.com
- 【命令模式】 DHCP 地址池配置模式
- 【使用指导】 地址绑定是指 IP 地址和客户端 MAC 地址的映射关系。地址绑定有两种：1) 手工绑定，就是在 DHCP 服务器数据库中，通过手工定义将 IP 地址和 MAC 地址进行静态映射，手工绑定其实是一个特殊地址池；2) 动态

绑定，DHCP 服务器接收到 DHCP 请求时，动态地从地址池中分配 IP 地址给客户端，而形成的 IP 地址和 MAC 地址映射。

要定义手工地址绑定，首先需要为每一个手动绑定定义一个主机地址池，然后定义 DHCP 客户端的 IP 地址和硬件地址或客户端标识。硬件地址就是 MAC 地址。客户端标识，微软客户端一般定义客户端标识，而不定义 MAC 地址，客户端标识包含了网络媒介类型和 MAC 地址。关于媒介类型的编码，请参见 RFC 1700 中关于“Address Resolution Protocol Parameters”部分内容。以太网类型为“01”

## 配置举例

### 动态地址池

- 【配置方法】
- 地址池 vlan1 20.1.1.0 255.255.255.0
  - 缺省网关为 20.1.1.1
  - 租约时间为 1 天

```
Ruijie(config)# ip dhcp pool vlan1
Ruijie(dhcp-config)# network 20.1.1.0 255.255.255.0
Ruijie(dhcp-config)# default-router 20.1.1.1
Ruijie(dhcp-config)# lease 1 0 0
```

【检验方法】

```
1. show run 查看
Ruijie(config)#show run | begin ip dhcp
ip dhcp pool vlan1
network 20.1.1.0 255.255.255.0
default-router 20.1.1.1
lease 1 0 0
```

### 手工绑定配置

- 【配置方法】
- 主机地址 172.16.1.101，掩码为 255.255.255.0
  - 主机名 Billy.rg.com
  - 缺省网关为 172.16.1.254
  - MAC 地址为 00d0.df34.32a3

```
Ruijie(config)# ip dhcp pool Billy
Ruijie(dhcp-config)# host 172.16.1.101 255.255.255.0
Ruijie(dhcp-config)# client-name Billy
Ruijie(dhcp-config)# hardware-address 00d0.df34.32a3 ethernet
Ruijie(dhcp-config)# default-router 172.16.1.254
```

【检验方法】

```
1. show run 查看
Ruijie(config)#show run | begin ip dhcp
ip dhcp pool Billy
```

```
host 172.16.1.101 255.255.255.0
client-name Billy
hardware-address 00d0.df34.32a3 ethernet
default-router 172.16.1.254
```

### 4.4.3 配置 DHCP 服务器 AM 规则

#### 配置效果

配置该命令后，可依据端口+VLAN 按区间进行地址分配

#### 注意事项

锐捷产品目前版本支持以太网接口、千兆口以及 FR、PPP、HDLC 接口上的配置。

#### 配置方法

##### 配置地址管理功能

- 进入到地址管理模式，为必选配置。
- 在配置模式下执行 **address-manage** 命令。

##### 配置 AM 规则

- 配置基于端口+VLAN 的 AM 规则，为必选配置。
- 在配置模式下执行 **match ip** 命令。

#### 检验方法

查看不同 vlan、端口下的用户是否取到有效地址

#### 相关命令

##### 配置缺省区间

【命令格式】 **match ip default** *ip-address netmask*

【参数说明】 *ip-address*: 网络地址  
*netmask*: 地址掩码

【命令模式】 address-manage 模式下

【使用指导】 配置该命令后所有来自未配置 vlan + port 的 DHCP 客户端将取得缺省区间内的地址，如果无该配置命令同时也无任何其它 vlan + port 配置，则按正常流程分配地址。

## 配置基于 vlan/port 规则下的动态地址分配

- 【命令格式】 **match ip** *ip-address netmask interface* [**add/remove**] **vlan** *vlan-list*
- 【参数说明】 *ip-address*: 网络地址  
*netmask*: 地址掩码  
*interface*: 接口名称  
*add/remove*: 添加或删除指定 vlan  
*vlan-list*: vlan 索引
- 【命令模式】 address-manage 模式下
- 【使用指导】 配置该命令后来自指定 vlan + port 的 DHCP 客户端将取得配置区内地址。

## 配置基于 vlan 规则下的静态地址分配

- 【命令格式】 **match ip** *ip-address netmask* [**add/remove**] **vlan** *vlan-list*
- 【参数说明】 *ip-address*: 网络地址  
*netmask*: 地址掩码  
*add/remove*: 添加或删除指定 vlan  
*vlan-list*: vlan 索引
- 【命令模式】 address-manage 模式下
- 【使用指导】 在 supervlan 场景下，满足 Dhcp 静态地址池配置的用户，无论在哪个 subvlan 下都只分配该静态地址；此时 AM 无需基于所有 subvlan/port 对该地址进行配置，只需要配置该地址在对应的 vlan 区间生效即可。该规则当前只对静态地址分配生效，动态地址不生效。

## 配置举例

### AM 规则配置

- 【配置方法】
- 配置缺省规则规则
  - 配置指定 vlan+port+地址区间规则
  - 配置指定 vlan+地址区间规则

```
Ruijie(config)# address-manage
Ruijie(config-address-manage)# match ip default 172.50.128.0 255.255.128.0
Ruijie(config-address-manage)# match ip 10.1.5.0 255.255.255.0 Gi5/3 vlan 1005
Ruijie(config-address-manage)# match ip 10.1.6.0 255.255.255.0 vlan 1006
```

- 【检验方法】 1 : **show run** 查看

```
address-manage
match ip default 172.50.128.0 255.255.128.0
match ip 10.1.5.0 255.255.255.0 Gi5/3 vlan 1005
match ip 10.1.6.0 255.255.255.0 vlan 1006
```

## 4.4.4 配置 DHCP 服务器全局属性

### 配置效果

---

开启服务器一些特定的功能，如 ping 机制、强制 nak 等。

### 注意事项

---

Nak 命令的配置可能引起网络中其它服务器的功能异常。

### 配置方法

---

#### 配置排除地址

- 配置某些地址或地址段不可用，为可选配置。
- 在配置模式下执行 **ip dhcp excluded-address** 命令

#### 配置 DHCP 服务器强制回复 NAK

- 针对某些用户的错误地址请求，服务器回复 nak 报文，可选配置。
- 在配置模式下执行 **ip dhcp force-send-nak** 命令。

#### 配置监控 VRRP 状态

- 启动该功能后，主机 server 处理 DHCP 相关报文，备机 server 则不处理 DHCP 相关报文，可选配置。
- 在配置模式下执行 **ip dhcp monitor-vrrp-state** 命令。

#### 配置 Ping 包次数

- 检查地址的可达性，执行 ping 操作，默认值为 2，可选配置。
- 在配置模式下执行 **ip dhcp ping packet** 命令。

#### 配置 Ping 包超时时间

- 检查地址的可达性，设置 ping 返回时长，默认值为 500ms，可选配置。
- 在配置模式下执行 **ip dhcp ping timeout** 命令。

#### 配置 DHCP 服务器检测用户下线

- 用于配置 DHCP 服务器是否检测用户下线。如果用户下线后一段时间内没有重新上线，则回收分配给该用户的地址。
- 在配置模式下执行 **ip dhcp server arp-detect** 命令。

### 检验方法

---

启动 **dhcp-server** 下发地址过程中可检验。



## 相关命令

### 配置排除地址

- 【命令格式】 **ip dhcp excluded-address** *low-ip-address* [*high-ip-address*]
- 【参数说明】 *low-ip-address*: 排斥 IP 地址范围的起始 IP 地址  
*high-ip-address*: 排斥地址范围的结束 IP 地址
- 【命令模式】 全局模式
- 【使用指导】 如果没有特别配置, DHCP 服务器会试图将在地址池中定义的所有子网地址分配给 DHCP 客户端。因此, 如果想保留一些地址不分配, 比如已经分配给服务器或者设备了, 必须明确定义这些地址是不允许分配给客户端的; 配置 DHCP 服务器, 一个好的习惯是将所有已明确分配的地址全部不允许 DHCP 分配, 这样可以带来两个好处: 1) 不会发生地址冲突; 2) DHCP 分配地址时, 减少了检测时间, 从而提高 DHCP 分配效率

### 配置 DHCP 服务器强制回复 NAK

- 【命令格式】 **ip dhcp force-send-nak**
- 【参数说明】 -
- 【命令模式】 全局配置模式
- 【使用指导】 在无线应用中, DHCP 客户端的移动性较大, DHCP 客户端会经常性的从一个网络移动到另一个网络中。当 DHCP 服务器在收到客户端的 Request 续租报文时, 发现客户端的网段发生更改或者是租约超时时会给予回复 NAK, 要求客户端重新获取 IP 地址, 避免客户端不断发送 Request 报文直至超时后重新获取 IP 地址, 延长 IP 地址获取时间。
- 但是, DHCP 服务器发送 NAK 报文的前提是该 DHCP 客户端在自己的管理范围之内, 也就是可以查找到对应的租约记录信息。当 DHCP 客户端从另一个网络环境中移入时, DHCP 服务器将无法在本地查找到对应的租约记录信息, 不予回复 NAK, 此时 DHCP 客户端需要不断发送 Request 报文直至超时后重新获取 IP 地址, 导致 IP 地址获取时间变长。在 DHCP 服务器重启时丢失客户端租约, 而客户端要求续租时也会遇到类似情况。在这种情况下, 可以通过配置命令强制让 DHCP 服务器在查找不到租约记录时也给予回复 NAK 报文, 触发客户端快速获取到 IP 地址, 注意: 默认情况下该条命令关闭; 在开启该命令的时候, 在同一广播域内, 不允许开启多台 DHCP 服务器

### 配置 Ping 包次数

- 【命令格式】 **ip dhcp ping packets** [*number*]
- 【参数说明】 *Number*: (可选) 范围从 0 到 10, 0 表示关闭 ping 操作。缺省 ping 两个包
- 【命令模式】 全局配置模式
- 【使用指导】 缺省情况, 当 DHCP 服务器试图从地址池中分配一个 IP 地址时, 会对该地址执行两次 Ping 命令(一次一个数据包)。如果 Ping 没有应答, DHCP 服务器认为该地址为空闲地址, 就将该地址分配给 DHCP 客户端; 如果 Ping 有应答, DHCP 服务器认为该地址已经在使用, 就试图分配另外一个地址给 DHCP 客户端, 直到分配成功

### 配置 Ping 包超时时间

- 【命令格式】 **ip dhcp ping timeout** *milliseconds*
- 【参数说明】 *milli-seconds*: DHCP 服务器等待 ping 应答的时间(以毫秒计)。取值范围为 100 到 10000

- 【命令模式】 全局配置模式
- 【使用指导】 缺省情况下，DHCP 服务器 Ping 操作如果 500 毫秒没有应答，就认为没有该 IP 地址主机存在。可以通过调整 Ping 包超时时间，改变服务器 Ping 等待应答的时间

#### 配置基于 ARP 检测用户下线

- 【命令格式】 **ip dhcp server arp-detect**
- 【参数说明】 -
- 【命令模式】 全局配置模式
- 【使用指导】 缺省情况下，DHCP 服务器不会基于 ARP 检测用户下线。配置该命令后，DHCP 服务器可以检测用户的下线。如果用户在一段时间内（默认 5 分钟）未重新上线，DHCP 服务器就回收分配给该用户的地址。

### 配置举例

#### 配置 ping 机制

- 【配置方法】
- 配置 ping 次数为 5
  - 配置 ping 超时时长为 800ms

```
Ruijie(config)# ip dhcp ping packet 5
Ruijie(config)# ip dhcp ping timeout 800
```

- 【检验方法】 1.show run 查看

```
Ruijie(config)#show run | begin ip dhcp
ip dhcp ping packet 5
ip dhcp ping timeout 800
```

#### 配置排除地址

- 【配置方法】
- 排除 192.168.0.0 – 192.168.255.255 的所有地址

```
Ruijie(config)# ip dhcp excluded-address 192.168.0.0 192.168.255.255
```

- 【检验方法】 1.show run 查看

```
Ruijie(config)#show run | begin ip dhcp
ip dhcp excluded-address 192.168.0.0 192.168.255.255
```

## 4.4.5 配置 DHCP Relay 基本功能

### 配置效果

- 建立 Client—Relay—Server 模式的 DHCP 动态 IP 管理，解决 DHCP 客户端与 DHCP 服务器不在同一网段时 DHCP 客户端与在其他网段的 DHCP 服务器通讯问题。

## 注意事项

- DHCP Relay 需要借助网络中现有的单播路由。因此，网络中必须配置 IPv4 单播路由。

## 配置方法

### 启动 DHCP Relay 功能

- 必须配置。
- 若无特殊要求，应在设备上启动 DHCP Relay 功能。

### 配置 DHCP 服务器的 IP 地址

- 必须配置。
- 应在设备上启动 DHCP 服务器的 IP 地址。

## 检验方法

- 检查用户主机能否通过 DHCP Relay 成功获取到 IP 地址。

## 相关命令


### 启动 DHCP Relay 功能

- 【命令格式】 **service dhcp**
- 【参数说明】 -
- 【命令模式】 全局模式
- 【使用指导】 -

### 配置 DHCP 服务器的 IP 地址

- 【命令格式】 **ip helper-address { cycle-mode | [ vrf { vrf-name } ] A.B.C.D }**
- 【参数说明】 *cycle-mode* : 开启 dhcp 请求报文转发所有 dhcp 服务器  
*vrf-name* : **vrf 名称**  
*A.B.C.D*: Server 的 ip 地址
- 【命令模式】 全局模式、接口模式
- 【使用指导】 配置接口必须是三层接口，包括：路由口、L3AP、SVI、loopback 接口。  
所有配置接口应 IPv4 单播路由可达。

## 配置举例

 以下配置举例，仅介绍与 DHCP Relay 相关的配置。

## 有线场景中 DHCP Relay 配置

【网络环境】

图 4-16



【配置方法】

- 用户设备启动通过 DHCP 获取地址的功能。
- 在作为 DHCP Relay Agent 的网络设备中启动 DHCP Relay 功能。
- 配置 DHCP Server。

**A** 用户设备启动 DHCP 获取地址的功能。

**B** # 启用 DHCP 中继代理

```
Ruijie(config)# service dhcp
```

# 添加一个全局的 DHCP 服务器的地址

```
Ruijie(config)# ip helper-address 172.2.2.1
```

# 配置与用户设备连接的端口的 IP 地址

```
Ruijie(config)# interface gigabitEthernet 0/1
```

```
Ruijie(config-if)# ip address 192.1.1.1 255.255.255.0
```

# 配置与 Server 设备连接的端口的 IP 地址

```
Ruijie(config)# interface gigabitEthernet 0/2
```

```
Ruijie(config-if-gigabitEthernet 0/2)# ip address 172.2.2.2 255.255.255.0
```

**C** # 启用 DHCP SERVER 功能

```
Ruijie(config)# service dhcp
```

# 添加一个客户端地址池

```
Ruijie(config)# ip dhcp pool relay
```

```
Ruijie (dhcp-config)#network 192.1.1.0 255.255.255.0
```

```
Ruijie (dhcp-config)#default-router 192.1.1.1
```

# 配置与 relay 设备连接的端口的 IP 地址

```
Ruijie(config)# interface gigabitEthernet 0/1
```

```
Ruijie(config-if-gigabitEthernet 0/2)# ip address 172.2.2.1 255.255.255.0
```

【检验方法】 查看用户是否能获取到 IP 地址。

- 检查用户设备是否能获取到 IP 地址。
- 检查 DHCP Relay 配置是否正确。

**A** 用户设备能获取到 IP 地址

**B** 登录到 DHCP Relay Agent 设备后在特权模式下用 **show running-config** 命令显示 DHCP Relay 配置

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

```
service dhcp
```

```
ip helper-address 172.2.2.1
```

```
!
```

```
interface GigabitEthernet 0/1
```

```
ip address 192.1.1.1 255.255.255.0
```

```
!  
interface GigabitEthernet 0/2  
ip address 172.2.2.2 255.255.255.0  
!
```

## 常见错误

- IPv4 单播路由配置错误。
- 没有启动 DHCP Relay 功能。
- 没有配置 DHCP Relay 与 DHCP Service 之间的路由。
- 没有配置 DHCP 服务器 IP 地址。

## 4.4.6 配置 DHCP Relay option 82 功能

### 配置效果

- 中继设备进行 DHCP Relay 时，可以通过添加 option 的方式来详细的标明 DHCP 客户端的一些网络信息，从而使服务器可以根据更精确的信息给用户分配不同权限的 IP。

### 注意事项

- 必须配置 DHCP Relay 基本功能。

### 配置方法

#### 📌 启动 DHCP Relay 基本功能

- 必须配置。
- 若无特殊要求，应在设备上启动 DHCP Relay 基本功能。

#### 📌 启动 DHCP option82 功能

- 缺省情况下，设备上的 DHCP option 82 功能关闭。
- 使用 **ip dhcp relay information option82** 命令可以启动或关闭设备上的 DHCP option 82 功能。

### 检验方法

- 检查客户端获取到的 IP 地址，是否是根据 option 82 规则分配。。

## 相关命令

### 配置 DHCP option82 功能

- 【命令格式】 **ip dhcp relay information option82**
- 【参数说明】 -
- 【命令模式】 全局模式
- 【使用指导】 -

## 配置举例

### 启动 DHCP option 82 功能。

- 【配置方法】
  - 启动 DHCP option 82 功能
  - 配置相关的子选项命令

```
Ruijie(config)# ip dhcp relay information option82
```

- 【检验方法】 登录到 DHCP Relay Agent 设备后在特权模式下用 **show running-config** 命令显示 DHCP Relay 配置。

```
Ruijie#show ru | incl ip dhcp relay  
ip dhcp relay information option82
```

## 常见配置错误

- DHCP Relay 基本功能没有配置，或配置失败。

### 4.4.7 配置 DHCP Relay check server-id 功能

## 配置效果

- 当配置命令 **ip dhcp relay check server-id** 后，DHCP Relay 仅将 DHCP 请求报文转发到 option server-id 中指定的服务器。如果没有配置该命令，则向所有配置的 DHCP 服务器转发 DHCP 请求报文。

## 注意事项

- 必须配置 DHCP Relay 基本功能。

## 配置方法

### 启动 DHCP Relay check server-id 功能

- 缺省情况下，设备上的 DHCP Relay check server-id 功能关闭。

- 使用 **ip dhcp relay check server-id** 命令可以启动设备上的 DHCP Relay check server-id 功能。

## 检验方法

DHCP Relay 是否仅将 DHCP 请求报文转发到 option server-id 中指定的服务器。

## 相关命令

### 配置 DHCP Relay check server-id 功能

- 【命令格式】 **ip dhcp relay check server-id**
- 【参数说明】 -
- 【命令模式】 全局模式
- 【使用指导】 -

## 配置举例

### 配置 DHCP Relay check server-id 功能。

- 【配置方法】
  - 配置 DHCP Relay 基本功能。略
  - 在对应接口上配置 DHCP Relay check server-id 功能。

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp relay check server-id
```

- 【检验方法】 登录到 DHCP Relay Agent 设备后在特权模式下用 **show running-config** 命令显示 DHCP Relay 配置。

```
Ruijie# show running-config | include check server-id
ip dhcp relay check server-id
Ruijie#
```

## 常见配置错误

- DHCP Relay 基本功能没有配置，或配置失败。

## 4.4.8 配置 DHCP Relay suppression 功能

## 配置效果

- 在指定接口上配置命令 **ip dhcp relay suppression** 后，将屏蔽该接口上收到的 DHCP 请求报文；而对于其他接口上收到的 DHCP 请求报文，则正常转发。

## 注意事项

- 必须配置 DHCP Relay 基本功能。

## 配置方法

### 启动 DHCP Relay suppression 功能

缺省情况下，设备上所有接口的 DHCP Relay suppression 功能关闭。

使用 **ip dhcp relay suppression** 命令可以启动设备上的 DHCP Relay suppression 功能。

## 检验方法

- 接口上收到的 DHCP 请求报文是否被过滤。

## 相关命令

### 配置 DHCP Relay suppression 功能

- 【命令格式】 **ip dhcp relay suppression**
- 【参数说明】 -
- 【命令模式】 接口模式
- 【使用指导】 -

## 配置举例

### 配置 DHCP Relay suppression 功能。

- 【配置方法】
  - 配置 DHCP Relay 基本功能。略
  - 在对应接口上配置 DHCP Relay suppression 功能。

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip dhcp relay suppression
Ruijie(config-if-GigabitEthernet 0/1)#end
Ruijie#
```

- 【检验方法】 登录到 DHCP Relay Agent 设备后在特权模式下用 **show running-config** 命令显示 DHCP Relay 配置。

```
Ruijie# show running-config | include relay suppression
ip dhcp relay suppression
Ruijie#
```

## 常见配置错误



DHCP Relay 基本功能没有配置，或配置失败。

## 4.4.9 配置 DHCP Relay 支持多 giaddr IP 功能

### 配置效果

- 配置命令 `ip dhcp relay multiple-giaddr` 后，开启支持多 giaddr IP 功能。

### 注意事项

- 必须配置 DHCP Relay 基本功能。

### 配置方法

#### 启动 DHCP Relay multiple-giaddr 功能

缺省情况下，功能关闭。

使用 `ip dhcp relay multiple-giaddr` 命令可以启动功能。

### 检验方法

- 接口上配置了多个 IP 地址时的 DHCP 请求报文是否可以带上不同的 IP 地址转发给 DHCP 服务器。

### 相关命令

#### 配置 DHCP Relay multiple-giaddr 功能

- 【命令格式】 `ip dhcp relay multiple-giaddr`
- 【参数说明】 -
- 【命令模式】 全局模式
- 【使用指导】 -

### 配置举例

#### 配置 DHCP Relay multiple-giaddr 功能。

- 【配置方法】
  - 配置 DHCP Relay 基本功能。略
  - 配置 DHCP Relay multiple-giaddr 功能。

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp relay multiple-giaddr
```

【检验方法】 登录到 DHCP Relay Agent 设备后在特权模式下用 **show running-config** 命令显示 DHCP Relay 配置。

```
Ruijie# show running-config
ip dhcp relay multiple-giaddr
```

## 常见配置错误

DHCP Relay 基本功能没有配置，或配置失败。

### 4.4.10 配置 DHCP Relay 支持网关自动切换功能

#### 配置效果

- 配置命令 **ip dhcp smart-relay** 后，开启网关自动切换功能。

#### 注意事项

- 必须配置 DHCP Relay 基本功能。

#### 配置方法

##### 启动 DHCP Relay 网关自动切换功能

缺省情况下，功能关闭。

使用 **ip dhcp smart-relay** 命令可以启动功能。

#### 检验方法

- 接口上配置了多个 IP 地址，DHCP-RELAY 转发 DISCOVER 报文 3 个，没有收到应答报文，切换网关地址。

#### 相关命令

##### 配置 DHCP Relay 网关自动切换功能

- 【命令格式】 **ip dhcp smart-relay**
- 【参数说明】 -
- 【命令模式】 全局模式
- 【使用指导】 -

## 配置举例

### 配置 DHCP Relay 网关启动切换功能。

#### 【配置方法】

- 配置 DHCP Relay 基本功能。略
- 配置 DHCP Relay 网关启动切换功能。

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp smart-relay
```

【检验方法】 登录到 DHCP Relay Agent 设备后在特权模式下用 **show running-config** 命令显示 DHCP Relay 配置。

```
Ruijie# show running-config
ip dhcp smart-relay
```

## 常见配置错误

DHCP Relay 基本功能没有配置，或配置失败。

### 4.4.11 配置 DHCP Relay 指定源地址功能

## 配置效果

- 在指定接口上配置命令 **ip dhcp relay source** 后，就指定 Relay 报文的源地址。

## 注意事项

- 必须配置 DHCP Relay 基本功能。
- 一个接口下只能指定一个 Relay 报文的源地址。
- 该功能需配合 option82 功能一起使用，给客户端分配正确的子网地址。

## 配置方法

### 启动 DHCP Relay 指定源地址功能

缺省情况下，不指定 DHCP Relay 报文的源地址。

使用 **ip dhcp relay source ip-address** 命令可以指定 Relay 报文的源地址。

## 检验方法

- 接口上配置了指定源地址时，发给的 DHCP 服务器的 Relay 报文的源地址即配置的地址。

## 相关命令

### 配置 DHCP Relay 指定源地址功能

- 【命令格式】 **ip dhcp relay source ip-address**
- 【参数说明】 *ip-address* : relay 报文的源地址。
- 【命令模式】 接口模式
- 【使用指导】 -

## 配置举例

### 配置 DHCP Relay 指定源地址功能。

- 【配置方法】
  - 配置 DHCP Relay 基本功能。略
  - 在对应接口上配置 DHCP Relay 指定源地址功能。

```
Ruijie(config-if)# ip dhcp relay source 1.1.1.1
```

- 【检验方法】 登录到 DHCP Relay Agent 设备后在特权模式下用 **show running-config** 命令显示 DHCP Relay 配置。

## 常见配置错误

DHCP Relay 基本功能没有配置，或配置失败。

## 4.4.12 配置 DHCP 客户端

### 配置效果

设备启动 dhcp-client，可动态取得地址及其它需求配置。

### 注意事项

锐捷产品目前版本支持以太网接口以及 FR、PPP、HDLC 接口上的 DHCP 客户端。

### 配置方法

在接口上执行 **ip address dhcp** 命令

### 检验方法

查看接口是否取到 ip 地址

相关命令

配置 DHCP 客户端

- 【命令格式】 ip address dhcp
- 【参数说明】 -
- 【命令模式】 接口配置模式
- 【使用指导】
  - 锐捷产品支持以太网端口通过 DHCP 获得动态分配的 IP 地址
  - 锐捷产品支持 ppp 封装的端口通过 DHCP 获得动态分配的 IP 地址
  - 锐捷产品支持 FR 封装的端口通过 DHCP 获得动态分配的 IP 地址
  - 锐捷产品支持 HDLC 封装的端口通过 DHCP 获得动态分配的 IP 地址

配置举例

DHCP 客户端配置

- 【配置方法】 1：为设备接口 FastEthernet 0/0 配置 DHCP 自动分配地址


```
Ruijie(config)# interface FastEthernet0/0
Ruijie(config-if-FastEthernet 0/0)#ip address dhcp
```

- 【检验方法】 1：show run 查看

```
Ruijie(config)#show run | begin ip address dhcp
ip address dhcp
```

4.5 监视与维护

清除各类信息


 在设备运行过程中执行 clear 命令，可能因为重要信息丢失而导致业务中断。

作用	命令
清除 DHCP 地址绑定	clear ip dhcp binding { address   * }
清除 DHCP 地址冲突	clear ip dhcp conflict { address   * }
清除 DHCP 服务器统计状态	clear ip dhcp server statistics
清除 DHCP 中继统计状态	clear ip dhcp relay statistics
清除 DHCP 服务器性能统计信息	clear ip dhcp server rate

查看运行情况

作用	命令
显示 DHCP 租约信息	<b>show dhcp lease</b>
显示 dhcp 用的套接字	<b>show ip dhcp socket</b>
显示已经分配的地址	<b>show ip dhcp binding</b>
显示创建的地址池	<b>show ip dhcp pool</b>
显示 dhcp-server 统计信息	<b>show ip dhcp server statistic</b>
显示 dhcp-relay 统计信息	<b>show ip dhcp relay statistic</b>
显示冲突地址	<b>show ip dhcp conflict</b>

## 查看调试信息

 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
DHCPagent 调试开关	<b>debug ip dhcp server agent</b>
DHCP 热备调试开关	<b>debug ip dhcp server ha</b>
DHCP 地址池调试开关	<b>debug ip dhcp server pool</b>
DHCP VRRP 调试开关	<b>debug ip dhcp server vrrp</b>
DHCP 打开所有调试开关	<b>debug ip dhcp server all</b>
DHCP 报文调试开关	<b>debug ip dhcp client</b>
DHCP Relay 事件调试开关。	<b>debug ip dhcp relay</b>

## 5 DHCPv6

### 5.1 概述

DHCPv6 ( Dynamic Host Configuration Protocol for IPv6 , IPv6 动态主机配置协议 ) 是一种允许 DHCP Server 将配置信息 ( 如 IPv6 网络地址 ) 传递给 IPv6 节点的协议。

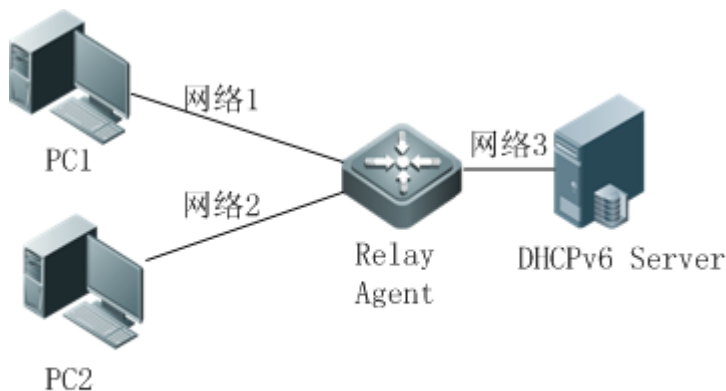
与其他 IPv6 地址分配方法 ( 手工配置、无状态的地址自动配置 ) 相比, DHCPv6 提供了分配地址、Prefix Delegation ( 前缀代理 )、配置参数分配的功能。

- DHCPv6 是一种全状态的地址自动配置协议, 提供了灵活地添加和重复使用网络地址的功能, 能够记录分配的地址, 增强了网络的管理性。
- 通过使用 DHCPv6 的前缀代理, 上游网络设备可以为下游网络设备分派地址前缀, 实现了灵活的站点级别的自动配置, 可以灵活地控制站点地址空间。
- DHCPv6 的配置参数分配可以解决在无状态地址自动配置协议下无法获取参数的问题, 为主机提供如 DNS 服务器地址和域名等配置信息。

DHCPv6 是一种 Client/Server 模型的协议。DHCPv6 Client 用于获取各类配置信息; DHCPv6 Server 用于提供各类配置信息。如果 DHCPv6 Client 和 DHCPv6 Server 不在同一网络链路时, 还可以通过 DHCPv6 Relay 进行交互。

DHCPv6 Client 通常是通过链路范围内保留组播地址来发现 DHCPv6 Server, 因此 DHCPv6 Client 和 DHCPv6 Server 必须能够直接通信, 也就是说需要部署在相同的链路内。这给实际用户会带来管理上的不方便, 经济上的浪费 ( 如果每个子网都部署一台 DHCPv6 Server ), 升级不方便等麻烦。而 DHCPv6 Relay Agent 功能, 允许 DHCPv6 Client 发送报文到处于不同链路上的 DHCPv6 Server, 从而解决这些问题。DHCP Relay Agent 通常都可以部署在 DHCPv6 Client 的链路内, 主要用来中继 DHCPv6 Client 和 DHCPv6 Server 之间的交互报文。DHCP Relay Agent 对于客户端而言是透明的。

图 5-1



DHCPv6 Client

 下文仅介绍 DHCPv6 的相关内容。

## 协议规范

- RFC3315 : Dynamic Host Configuration Protocol for IPv6
- RFC3633 : IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) Version 6
- RFC3646 : DNS Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC3736 : Stateless DHCP Service for IPv6
- RFC5417 : Control And Provisioning of Wireless Access Points (CAPWAP) Access Controller DHCP Option

## 5.2 典型应用

典型应用	场景描述
请求分配地址、配置参数	DHCPv6 Client 向 DHCPv6 Server 请求地址信息 ; DHCPv6 Server 为其分配地址和配置参数
请求分配前缀	DHCPv6 Client 向 DHCPv6 Server 请求前缀信息 ; DHCPv6 Server 为其分配前缀, DHCPv6 Client 再以该前缀配置 IPv6 地址
中继服务	通过 DHCPv6 中继, 使处于不同链路上的 DHCPv6 Client 和 DHCPv6 Server 进行通信。

### 5.2.1 请求分配地址、配置参数

#### 应用场景

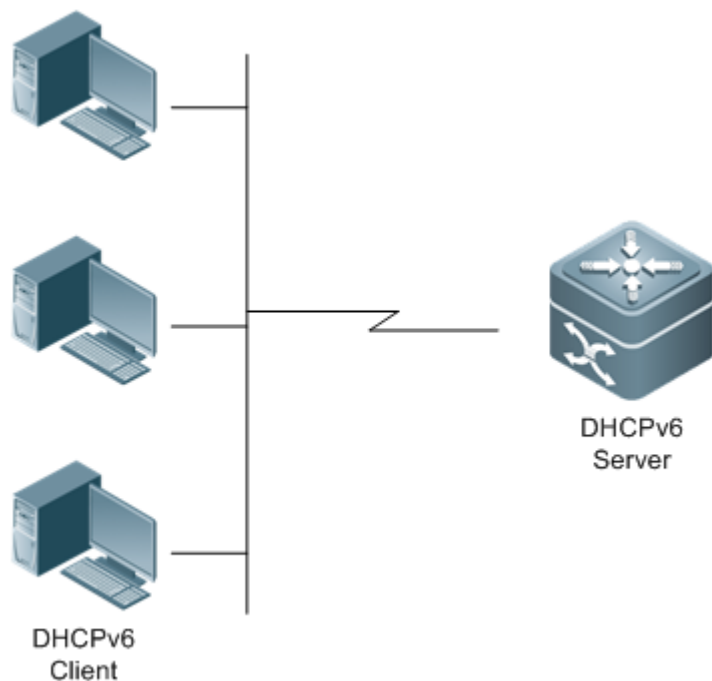
在一个子网内, DHCPv6 Client 向 DHCPv6 Server 请求地址信息 ; DHCPv6 Server 为其分配地址和配置参数

以下图为例 :

- DHCPv6 Server 上配置了可供分配的 IPv6 地址和 DNS Server、域名等配置参数信息。
- 主机作为 DHCPv6 Client 向 DHCPv6 Server 请求分配 IPv6 地址, DHCPv6 Server 收到请求后, 从配置的地址中选择一个可用的分配给主机。
- 主机还可以向 DHCPv6 Server 请求分配 DNS Server、域名等配置参数信息。

图 5-2





## 功能部署

- 在子网内主机运行 DHCPv6 Client，获取 IPv6 地址和参数。
- 在 DHCP Server 设备上运行 DHCPv6 Server 并配置地址及参数，实现地址和参数的分配。

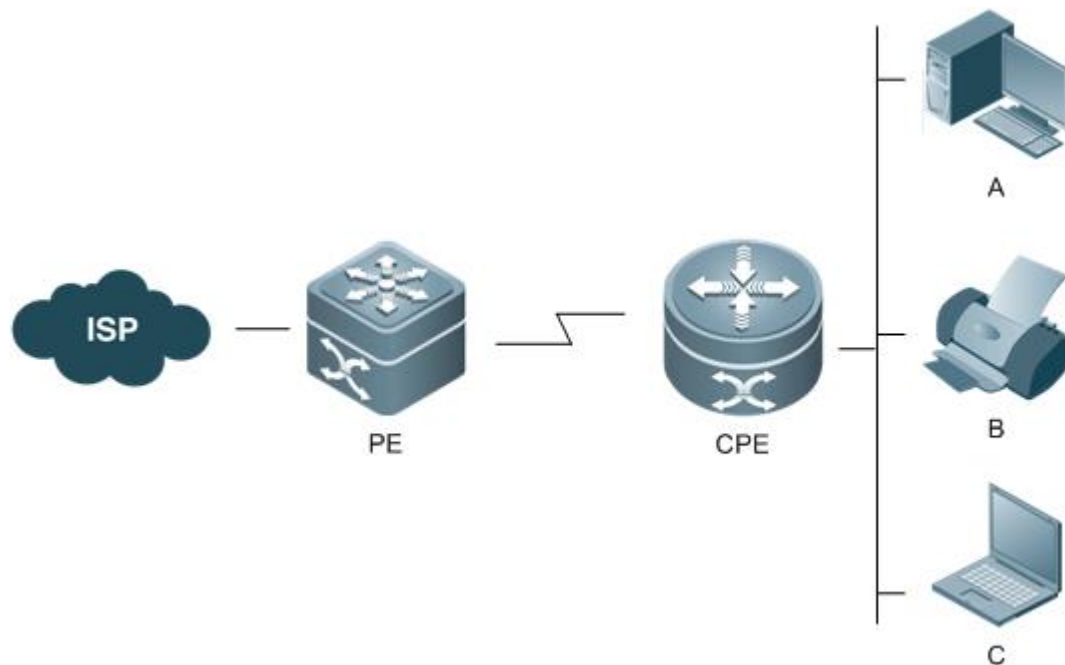
## 5.2.2 请求\分配前缀

### 应用场景

以下图为例，上游设备（PE）为下游设备（CPE）分配 IPv6 地址前缀，CPE 根据得到的地址前缀为内部子网生成新的地址前缀，CPE 内部子网内的主机就以新的地址前缀通过 RA（Router Advertisement）完成自己的地址配置。

- PE 作为 DHCPv6 Server 提供前缀代理服务，配置好地址前缀信息。
- CPE 作为 DHCPv6 Client 向 PE 请求地址前缀，在获取到地址前缀后，为内部子网生成新的地址前缀，并向内部子网内主机发送 RA（Router Advertisement）。
- CPE 内部子网内的主机就可以根据 CPE 发送的 RA 完成自己的地址配置。

图 5-3



【注释】 PE ( Provider Edge ) , 作为 DHCPv6 Server , 又叫 Delegating Router , 提供前缀信息。  
CPE ( Customer Premises Equipment ) , 作为 DHCPv6 Client , 又叫 Requesting Router , 请求前缀信息。  
A、B、C 为各种类型主机

## 功能部署

- 在 PE 运行 DHCPv6 Server , 实现前缀代理服务。
- 在 CPE 运行 DHCPv6 Client , 实现地址前缀的获取。
- 在 CPE 和主机之间部署 IPv6 ND , 实现通过 RA 配置子网内主机地址。

### 5.2.3 中继服务

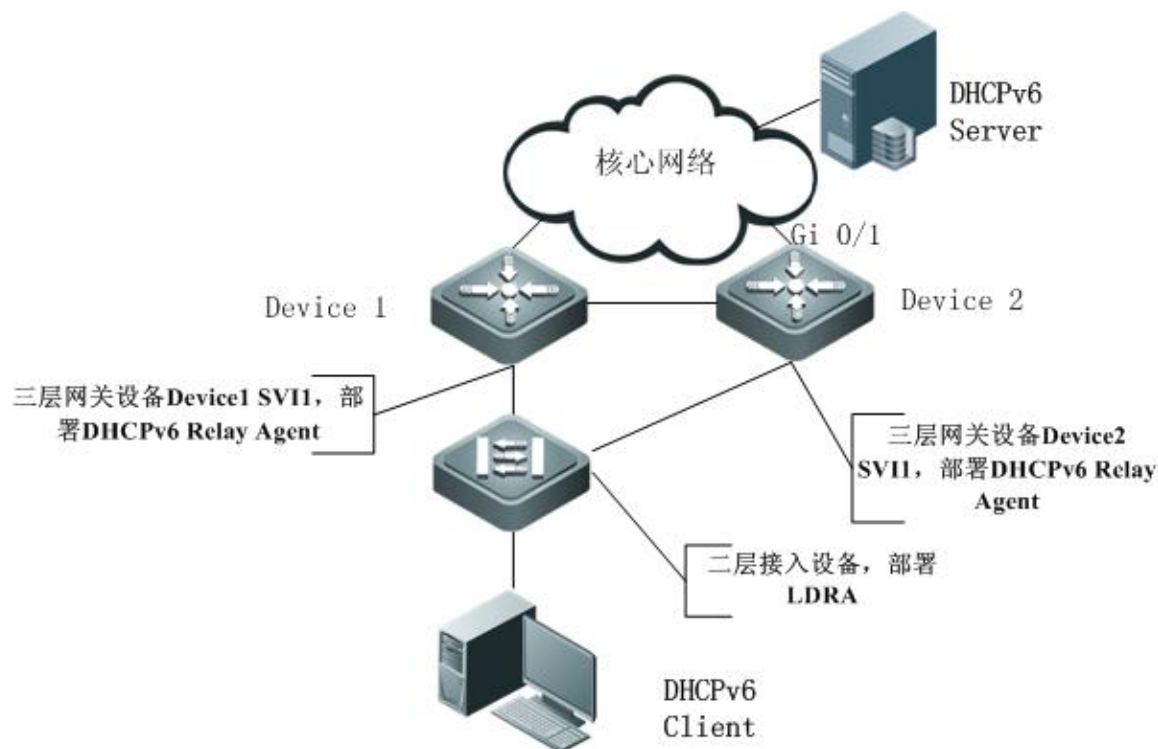
## 应用场景

DHCPv6 Relay Agent 为处于不同链路上的 DHCPv6 Client 和 DHCPv6 Server 提供中继服务, 使得二者可以进行通信。

以下图为例：

- Device1 开启 DHCPv6 Relay Agent 并且目的地址指向 3001::2；
- Device2 由于希望通过下一级 Relay 继续处理转到其他服务器, 所以开启 DHCPv6 Relay Agent 并且目的地址指向 FF02::1:2 ( 所有服务器和 Relay 组播地址 ), 出接口指定为上联目标地址的三层接口为 gi 0/1。

图 5-4



## 功能部署

- 在 Device1 上启用 DHCPv6 Relay Agent，并将地址指定为 3000::1。
- 在 Device2 上启用 DHCPv6 Relay Agent，并将地址指定为 FF02::1:2。

## 5.3 功能详解

### 基本概念

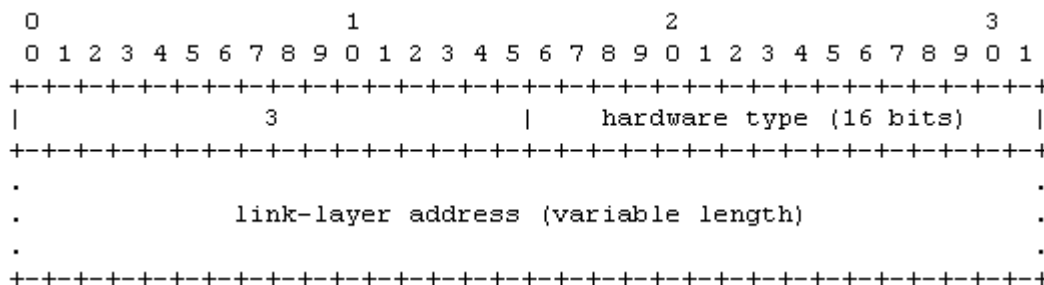
#### 📌 DUID

DUID ( DHCP Unique Identifier ) 即 DHCP 唯一标识。RFC3315 中明确定义，每一台 DHCPv6 设备 ( 包括客户端、中继和服务器 ) 都必须拥有一个 DHCPv6 唯一标识，并用于在设备之间交换 DHCPv6 消息时相互验证。

RFC3315 上规定了三种类型的 DUID：

- DUID-LLT：DUID Based on Link-Layer address plus Time，链路地址加时间。
- DUID-EN：DUID Assigned by Vendor Based on Enterprise Number，厂商私有 ID 加企业内部编号。
- DUID-LL：Link-Layer address，链路地址。

锐捷 DHCPv6 设备采用的 DUID 类型是 DUID-LL。DUID-LL 的结构如下：



其中，DUID type 为 DUID 类型，DUID-LL 类型取值为 0x0003；Hardware type 为硬件类型，设备支持的硬件类型为以太网，取值为 0x0001；Link layer address 为链路层地址，取值为设备的 MAC 地址。

## 标识联盟 (IA)

在 DHCPv6 中 Server 分配给 Client 的地址信息是一个集合 (Identity association, IA)，DHCPv6 Server 以 IA 为单位进行地址分配，每一个 IA 都由 IAID 唯一标识。IAID (Identity association identifier) 由 DHCPv6 Client 生成。IA 与 Client 成——对应关系，一个 IA 中可以包含多个地址，Client 可以将 IA 中的地址分配给设备上的其他接口。IA 中可以包含的地址有以下三类：

- NA：Non-temporary Addresses，全球唯一地址；
- TA：Temporary Addresses，临时地址（基本没有相关应用）；
- PD：Prefix Delegation，前缀空间；

因此根据 IA 中包含的地址不同，IA 又分为 IA\_NA、IA\_TA、IA\_PD 三种类型 (IA-Type)。锐捷 DHCPv6 Server 支持分配 IA\_NA 和 IA\_PD，不支持 IA\_TA。

## 绑定 (Binding)

DHCPv6 的绑定 (DHCPv6 Binding) 是一组可管理的信息结构。在 Server 上的绑定中，记录着分配给每个 Client 的 IA 和其他配置信息。每个 Client 可以申请多个绑定，Server 上的绑定以绑定表的形式组织，包含 IA 的绑定以 DUID、IA-Type、IAID 为索引，包含配置信息的绑定以 DUID 为索引。

## 地址冲突

DHCPv6 的地址冲突 (DHCPv6 conflict) 是指当 DHCPv6 Client 自身分配的地址存在冲突，Client 发送 Decline 报文通知 Server 本地址存在重复绑定，Server 将本地址添加到地址冲突队列中。只要存在于该队列中的地址，之后 Server 将不再把该地址分配出去，Server 支持查看和清除地址冲突队列中的地址信息的功能。

## 报文类型

RFC3315 规定 DHCPv6 使用 546 和 547 端口和 UDP 进行报文交互，DHCPv6 Client 在 546 端口上接收报文，DHCPv6 Server 和 DHCPv6 Relay 在 547 端口上接收报文。RFC3315 定义 DHCPv6 Server、DHCPv6 Client、DHCPv6 Relay 之间可以收发的报文类型，如下：

- DHCPv6 Client 允许发送给 DHCPv6 Server 的报文类型包括：Solicit、Request、Confirm、Renew、Rebind、Release、Decline、Information-request。
- DHCPv6 Server 允许发送给 DHCPv6 Client 的报文类型包括：Advertise、Reply、Reconfigure。
- DHCPv6 Relay 允许发送给 DHCPv6 Relay 或 DHCPv6 Server 的报文类型包括：Relay-forward。
- DHCPv6 Server 或 DHCPv6 Relay 允许发送给 DHCPv6 Relay 的报文类型包括：Relay-reply。

- ✔ 锐捷 DHCPv6 Server 不支持 Reconfigure 报文类型。
- ✔ 锐捷 DHCPv6 Client 不支持 Confirm、Reconfigure 报文类型。

功能特性

功能特性	作用
请求\分配地址	通过 Client/Server 模式在网络中动态获取\分配 IPv6 地址。
请求\分配前缀	通过 Client/Server 模式在网络中动态获取\分配 IPv6 前缀。
无状态服务	为网络中主机提供无状态的参数自动配置服务。
中继服务	通过 Relay 为不在同一网络中的主机提供 DHCPv6 Server 服务。

5.3.1 请求\分配地址

DHCPv6 Client 可以向网络中的 DHCPv6 Server 请求 IPv6 网络地址信息。  
DHCPv6 Server 配置可用的地址后，可以为网络中的主机提供 IPv6 网络地址，并记录所分配的地址，能够提高网络管理性。

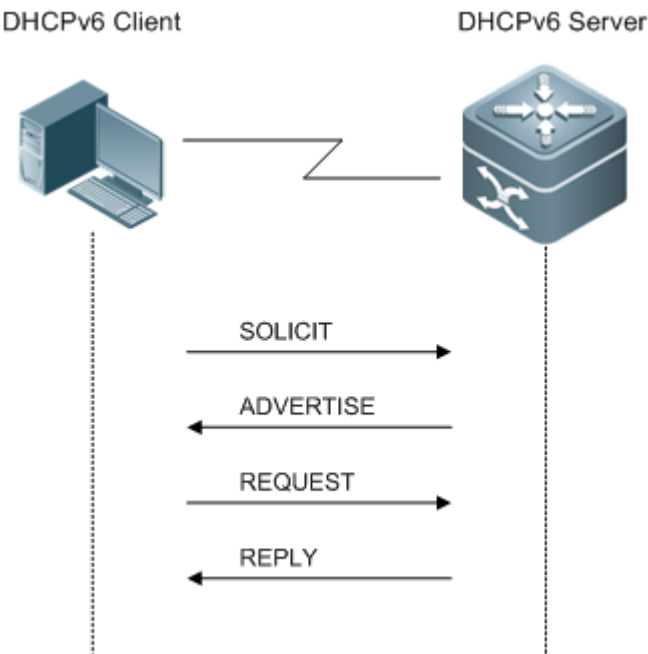
工作原理

网络中主机作为 DHCPv6 Client 与 DHCPv6 Server 通过消息交互完成地址的分配、更新、确认、释放等操作。

四次消息交互

四次消息交互的过程如图所示：

图 5-5

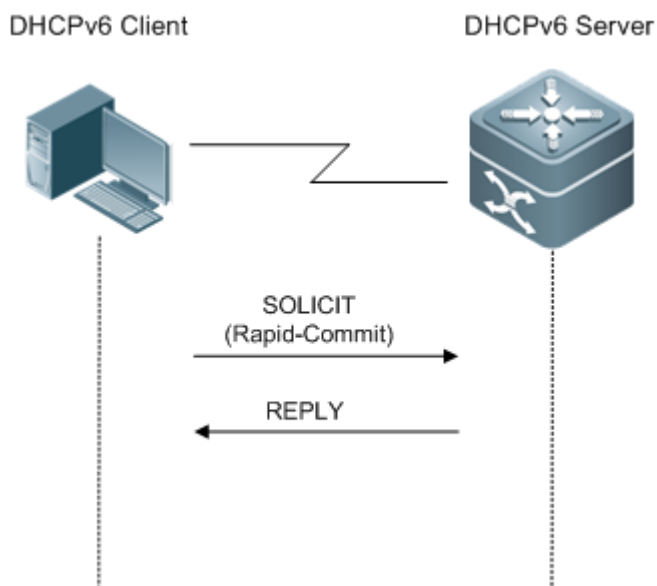


- DHCPv6 Client 在本链路内发送一个目的地址为 FF02::1:2，目的端口 547 的 SOLICIT 消息来请求地址分配、前缀分配、配置参数分配。本链路内的所有 DHCPv6 Server 或者 DHCPv6 Relay Agent 都会收到 SOLICIT 消息。
- DHCPv6 Server 收到 SOLICIT 消息后，如果本地可以提供 SOLICIT 消息里的请求信息，则以单播方式回应一个 ADVERTISE 消息，包含了 DHCPv6 Server 所能提供的地址、前缀、配置参数等信息。
- DHCPv6 Client 可能收到多个 DHCPv6 Server 发送的 ADVERTISE 消息。选择最合适的 DHCPv6 Server 后，DHCPv6 Client 发送一个目的地址为 FF02::1:2，目的端口 547 的 REQUEST 消息请求地址分配、前缀分配、配置参数分配。
- DHCPv6 Server 收到 REQUEST 消息后，本地创建绑定信息，并单播回应一个 REPLY 消息，包含了 DHCPv6 Server 将要分配给 DHCPv6 Client 的地址、前缀、配置参数等信息。DHCPv6 Client 根据 REPLY 消息里的信息完成地址分配、前缀分配或配置参数分配。

## 二次消息交互

如果 DHCPv6 Client 需要更短的配置时间时，可以通过两次消息交互完成地址、前缀、参数配置。

图 5-6



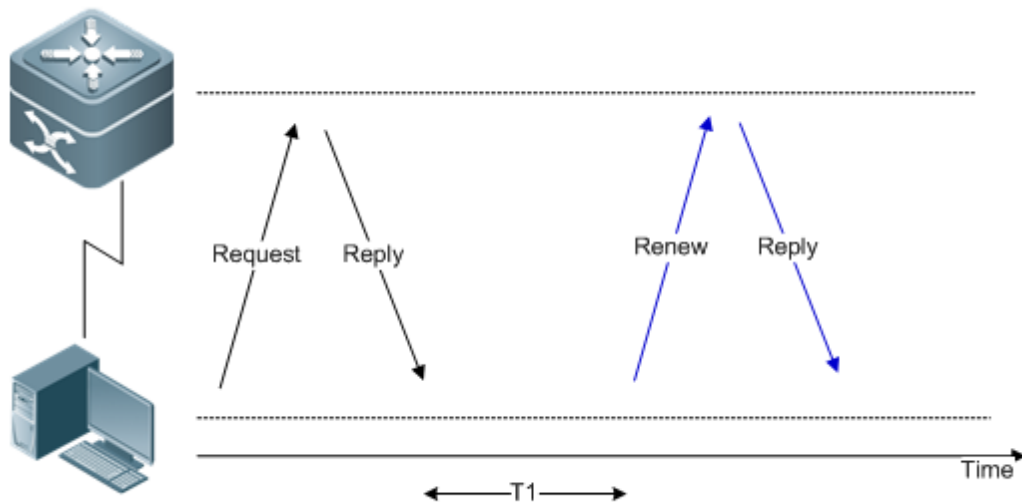
- DHCPv6 Client 在本地链路内发送一个目的地址为 FF02::1:2，目的端口为 547 的 SOLICIT 消息，同时 SOLICIT 消息里面包含 Rapid Commit 选项，来请求地址分配、前缀分配、配置参数消息分配。
- 如果 DHCPv6 Server 支持处理 Rapid Commit 选项，在本地创建绑定信息，并单播回应一个 REPLY 消息，包含了将要分配给 DHCPv6 Client 的地址、前缀、配置参数等信息。DHCPv6 Client 根据 REPLY 消息里的信息完成配置。

## 更新和重新绑定

DHCPv6 Server 在发给 DHCPv6 Client 消息中的 IA 中提供了控制地址和更新的参数 T1 和 T2。

图 5-7

## DHCPv6 Server

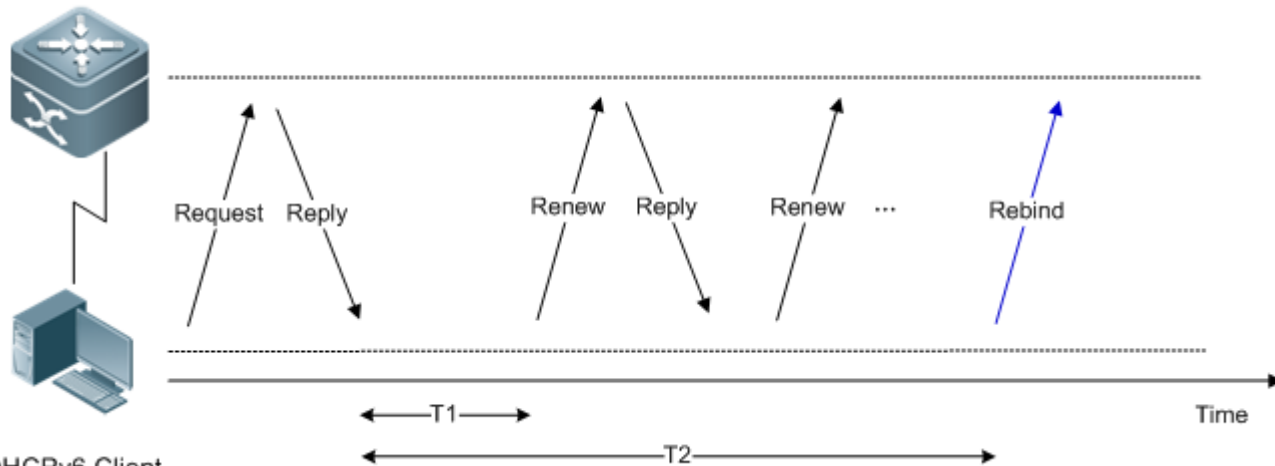


## DHCPv6 Client

- $T1$  的值表示在  $T1$  秒后 ,DHCPv6 Client 需要向 DHCPv6 Server 发送一个 Renew 多播消息进行地址和前缀的更新。Renew 消息里包含了 DHCPv6 Server 的 DUID , 需要更新的 IA 信息等内容。
- DHCPv6 Server 收到 Renew 消息后, 如果 Renew 消息中的 DUID 值等于本设备的 DUID 值, 则更新本地的绑定, 并以单播的方式回应一个 Reply 消息, 包含新的  $T1$  和其他参数值。

图 5-8

## DHCPv6 Server



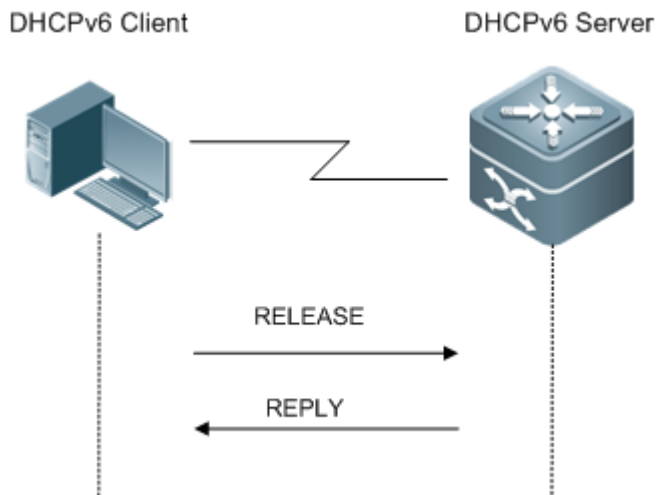
## DHCPv6 Client

- $T2$  的值表示 DHCPv6 Client 向 DHCPv6 Server 发送 Renew 消息后, 一直没有收到响应, 当到达  $T2$  时间后, 需要向 DHCPv6 Server 发送一个 Rebind 多播消息进行地址和前缀的重新绑定。
- DHCPv6 Server ( 可能是新的 DHCPv6 Server ) 收到 Rebind 后, 根据 Rebind 的内容单播回应一个 Reply 报文。

### 释放

如果 DHCPv6 Client 需要释放一个地址或前缀时，通过向 DHCPv6 Server 发送一个 Release 消息通知 DHCPv6 Server 不再使用的地址或前缀，以便 DHCPv6 Server 能够将这些地址和前缀再次分配给其他 DHCPv6 Client。

图 5-9

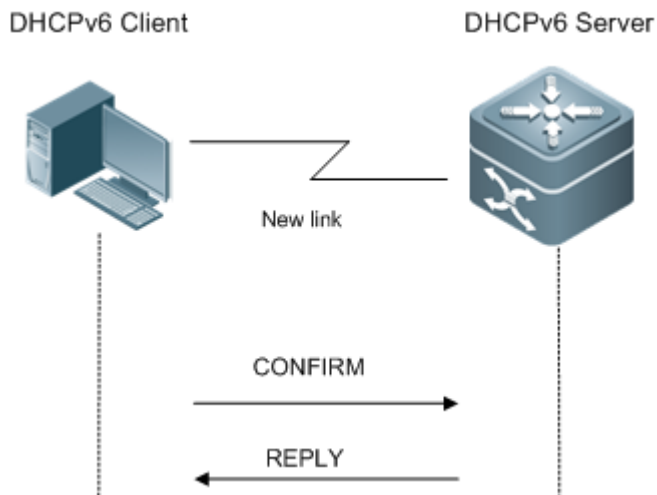


- DHCPv6 Server 收到 Release 消息后，根据 Release 消息里的地址或前缀信息移除相关绑定，并回复一个携带状态选项的 Reply 消息给 DHCPv6 Client。

#### 确认

DHCPv6 Client 如果移动到新的链路（如发生重启），则会发送一个 Confirm 消息来向新链路里的 DHCPv6 Server 确认原来的地址是否仍然可用。

图 5-10



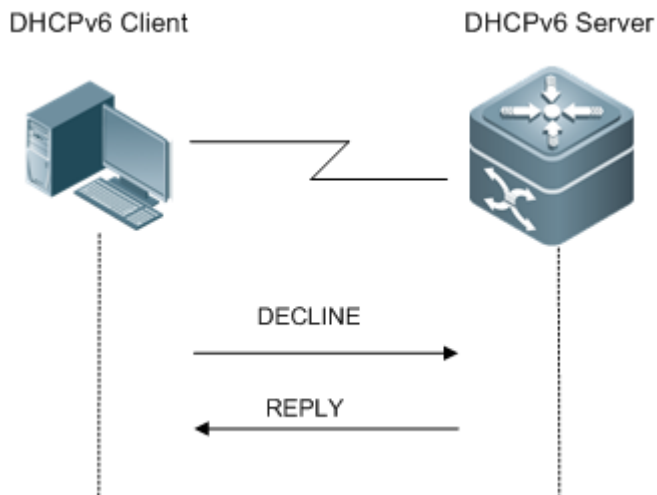
- DHCPv6 Server 收到 Confirm 消息后，根据 Confirm 消息里的地址信息进行确认，并回复一个携带状态选项的 Reply 消息给 DHCPv6 Client。如果确认失败，DHCPv6 Client 可能重新发起地址分配请求。

#### 地址冲突



DHCPv6 Client 完成地址分配后，如果在链路上检测到所分配地址已被使用，则发送 Decline 消息通知 DHCPv6 Server 存在地址冲突。

图 5-11




- DHCPv6 Client 在 Decline 消息里包含冲突地址的 IA 信息。
- DHCPv6 Server 收到 Decline 消息后，将 Decline 消息里的地址标记为 “declined”，不会在后续的地址分配中使用这些地址，然后回复一个携带状态选项的 Reply 消息给 DHCPv6 Client。标记为 “declined” 的地址，可以通过手工清除，以便可以重新分配。

## 相关配置

### ▮ 启用接口上的 DHCPv6 Server 功能

- 缺省情况下，接口上的 DHCPv6 Server 功能未启用。
- 使用 **ipv6 dhcp server** 命令可以启用或停用接口上的 DHCPv6 Server 功能。

 只能在三层接口上启用 DHCPv6 Server 功能。

### ▮ DHCPv6 Server 分配地址

- 缺省情况下，DHCPv6 Server 没有创建信息池和配置可分配的地址。
- 使用 **ipv6 dhcp pool** 命令可以创建信息池。
- 使用 **iana-address** 命令可以配置可分配的地址，以及地址的 preferred lifetime 和 valid lifetime 值。

### ▮ DHCPv6 Server 清除冲突地址

- 缺省情况下，DHCPv6 Server 检测到的冲突地址不会清除。
- 使用 **clear ipv6 dhcp conflict** 命令可以清除冲突的地址，以便在后续的地址分配中可以继续使用这些地址。

### ▮ 启用接口上的 DHCPv6 Client 请求地址功能

- 缺省情况下，接口上的 DHCPv6 Client 地址请求功能未启用。

- 使用 **ipv6 dhcp client ia** 命令可以启用或停用接口上的 DHCPv6 Client 请求地址功能。

 只能在三层接口上启用 DHCPv6 Client 请求地址功能。

### 5.3.2 请求\分配前缀

在 DHCPv6 Server 上配置可用的前缀，通过使用 DHCPv6 的前缀代理，上游网络设备可以为下游网络设备分派地址前缀，实现了灵活的站点级别的自动配置，可以灵活地控制站点地址空间。

#### 工作原理

下游网络设备作为 DHCPv6 Client 与 DHCPv6 Server 通过消息交互完成前缀的分配、更新、释放等操作。下游网络设备通过与分配地址一样的机制进行四次消息交互、两次消息交互获取前缀信息，进行前缀信息的更新和重新绑定，进行前缀的释放。但也与分配地址存在一些差异。


- 前缀代理的消息交互中，没有使用到 Confirm 和 Decline 消息。
- 如果 DHCPv6 Client 移动到新的链路，需要确认前缀信息是否可用时，使用 Rebind 和 Reply 的消息交互机制进行重新确认。
- 各类消息里的 IA 类型是 IA\_PD，而不是 IA\_NA。

 前缀代理的消息交互参照请求\分配地址

#### 相关配置

##### ▾ 启用接口上的 DHCPv6 Server 功能

- 缺省情况下，接口上的 DHCPv6 Server 功能未启用。
- 使用 **ipv6 dhcp server** 命令可以启用或停用接口上的 DHCPv6 Server 功能。

 只能在三层接口上启用 DHCPv6 Server 功能。


##### ▾ DHCPv6 Server 前缀代理

- 缺省情况下，DHCPv6 Server 没有创建信息池和配置前缀信息。
- 使用 **ipv6 dhcp pool** 命令可以创建信息池。
- 使用 **prefix-delegation** 命令可为特定的 DHCPv6 Client 分配指定的前缀信息
- 使用 **prefix-delegation pool** 配置前缀信息池，后续所有的 DHCPv6 Client 请求的前缀信息都从该池中分配。

##### ▾ 启用接口上的 DHCPv6 Client 请求前缀功能

缺省情况下，接口上的 DHCPv6 Client 请求前缀功能未启用。

使用 **ipv6 dhcp client pd** 命令可以启用或停用接口上的 DHCPv6 Client 请求前缀功能。

 只能在三层接口上启用 DHCPv6 Client 请求前缀功能。

### 5.3.3 无状态服务

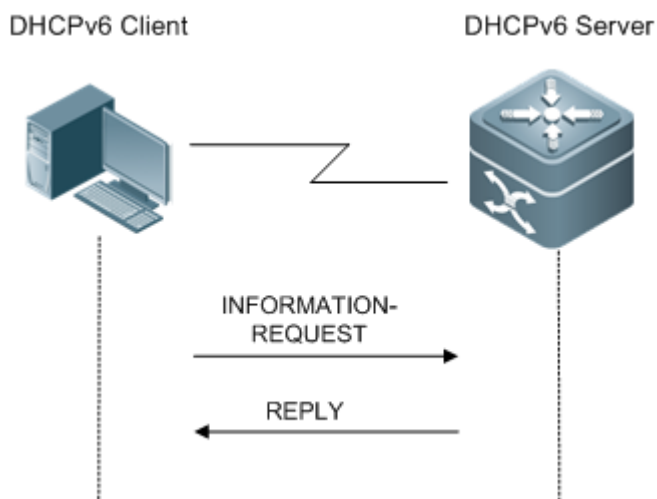
DHCPv6 Client 在只需要配置参数信息，而不需要地址或前缀信息时，通过 DHCPv6 无状态服务，可以获取相关的配置参数信息，解决了在无状态地址自动配置协议下无法获取参数的问题，如 DNS Server 地址。

#### 工作原理

网络中主机作为 DHCPv6 Client 与 DHCPv6 Server 通过消息交互完成配置参数的获取、更新等操作，

#### 无状态服务消息交互

图 5-12



- DHCPv6 Client 向 DHCPv6 Server 发送一个 Information-request 消息，即可请求无状态信息，该消息里通常没有包含特定 DHCPv6 Server 的 DUID。
- DHCPv6 Server 向 DHCPv6 Client 回复一个包含配置参数信息的 Reply 报文。

#### 相关配置

##### 启用接口上的 DHCPv6 Server 功能

- 缺省情况下，接口上的 DHCPv6 Server 功能未启用。
- 使用 `ipv6 dhcp server` 命令可以启用或停用接口上的 DHCPv6 Server 功能。



只能在三层接口上启用 DHCPv6 Server 功能。

##### DHCPv6 Server 的无状态服务

- 缺省情况下，DHCPv6 Server 没有创建信息池和配置参数信息。
- 使用 `ipv6 dhcp pool` 命令可以创建信息池。
- 使用 `dns-server` 命令可以添加 DNS Server 列表信息。

- 使用 **domain-name** 命令可以添加域名列表信息。
- 使用 **option52** 命令可以添加 CAPWAP AC 的 IPv6 地址信息。

#### 📌 DHCPv6 Client 的无状态服务

- 缺省情况下，接口上的 DHCPv6 Client 无状态服务未启用。
- 主机收到的 RA 通告里面设置了 O 标记，则会使 DHCPv6 Client 启动无状态服务。

### 5.3.4 中继服务

当 DHCPv6 Client 与 DHCPv6 Server 不在同一链路上时，DHCPv6 Client 可以通过 DHCPv6 Relay Agent 将相关的消息中继到 DHCPv6 Server，DHCPv6 Server 在处理后，也将响应消息通过 Relay Agent 中继到 DHCPv6 Client。

#### 工作原理

当 DHCPv6 Relay Agent 收到来自 DHCPv6 Client 消息时，会创建一个 Relay-forward 消息，该消息中包含了原始的 DHCPv6 Client 消息以及 Relay Agent 可能添加的一些选项信息。然后将 Relay-forward 发往指定的 DHCPv6 Server 或者特定的多播地址 FF05::1:3。

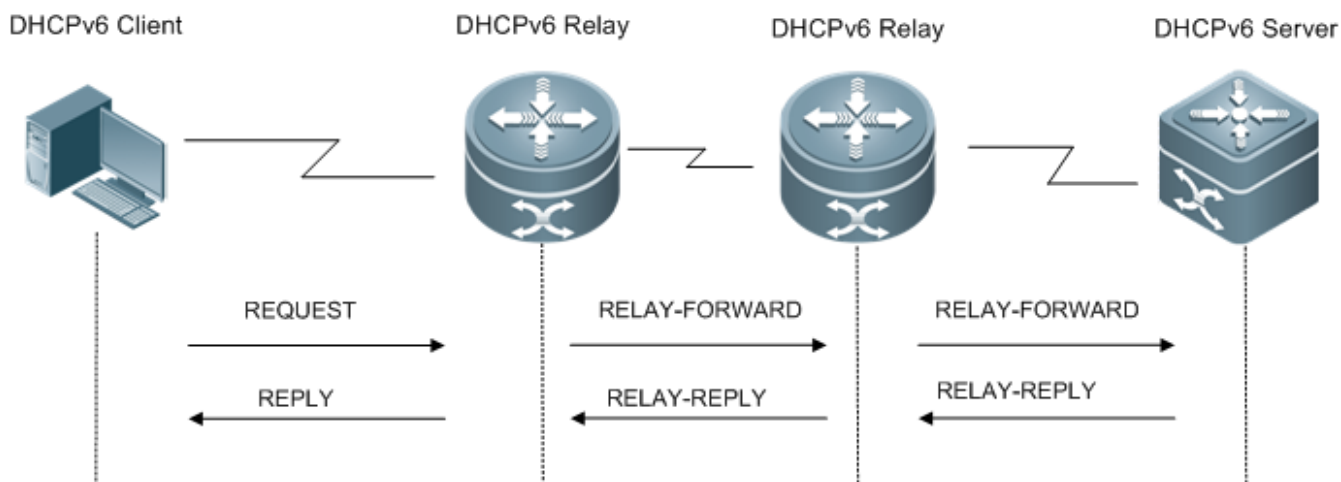
当 DHCPv6 Server 接收到 Relay-forward 消息后，将封装在 Relay-forward 消息里的原始 DHCPv6 Client 消息提取出来并进行处理。DHCPv6 Server 接着对该原始消息进行响应，并将响应消息封装 Relay-reply 消息，然后发送给 DHCPv6 Relay Agent。

当 DHCPv6 Relay Agent 收到 Relay-reply 消息时，将封装在 Relay-reply 消息中的原始 DHCPv6 Server 消息提取出来并转发给 DHCPv6 Client。

在 DHCPv6 Client 和 DHCPv6 Server 之间还允许有多级的 Relay Agent。

#### 📌 DHCPv6 Relay Agent

图 5-13



- DHCPv6 Relay Agent 在 DHCPv6 Client 和 DHCPv6 Server 之间进行报文的封装和解封装，解决 DHCPv6 Client 和 DHCPv6 Server 不在同一链路的问题。

### 5.3.5 中继源接口指定功能

当 DHCPv6 Server 无法通过上联口 IP 识别唯一的 DHCPv6 Relay 时，采用指定源接口的方式可区分不同的 DHCPv6 Relay 设备，确保报文转发正常。


#### 工作原理

源接口指定功能允许指定 IP 地址或者接口，DHCPv6 Relay 转发报文到 DHCPv6 Server 时，采用指定的信息填充到中继转发报文 Relay-forward 的源 IP 地址中，而其目的 IP 地址仍然为 DHCPv6 Server 的 IP 地址；DHCPv6 Server 收到 Relay-forward 报文后，将记录该报文的源 IP 地址，作为其应答报文 Relay-reply 的目的地址，即应答报文指向的是中继设备上的源接口指定功能配置的指定 IP 地址或者接口，从而实现绕过 DHCPv6 Relay 上联口的问题。





#### 相关配置

##### 📌 全局/接口配置模式下启用源接口指定功能

- 缺省情况下，未指定任何的源接口信息。
- 使用 **ipv6 dhcp relay source** 命令可以配置或删除全局上的源接口指定功能配置信息。
- 使用 **show ipv6 dhcp relay source** 可以查看相应的源接口指定功能配置信息。

 <sup>2</sup> 接口配置模式下，只能在三层接口上启用源接口指定功能。

## 5.4 配置详解

配置项	配置建议 & 相关命令	
配置 DHCPv6 Server	 必须配置。用于创建&配置信息池。	
	<b>ipv6 dhcp pool</b>	配置 DHCPv6 Server 的信息池。
	 可选配置。用于分配地址。	
	<b>iana-address prefix</b>	配置 DHCPv6 Server 上可分配的地址前缀。
	 可选配置。用于分配前缀。	
	<b>prefix-delegation</b>	配置 DHCPv6 Server 的静态绑定地址前缀信息。
	<b>prefix-delegation pool</b>	配置 DHCPv6 Server 通过本地前缀池分配前缀。
	<b>ipv6 local pool</b>	配置 IPv6 的本地前缀池。
	 可选配置。用于分配配置参数	
	<b>dns-server</b>	配置 DHCPv6 Server 的 DNS Server 列表信息。
	<b>domain-name</b>	配置 DHCPv6 Server 的 domain name 信息。
	<b>option52</b>	配置 DHCPv6 Server 的 CAPWAP AC 的 ipv6 地址信息。

	⚠ 必须配置。用于启用 DHCPv6 Server 服务。	
	ipv6 dhcp server	配置接口上启用 DHCPv6 Server 服务。
配置 DHCPv6 Relay	⚠ 必须配置。用于启用 DHCPv6 Relay 服务。	
	ipv6 dhcp relay destination	配置 DHCPv6 Relay Agent 功能。
	ipv6 dhcp relay source	配置 DHCPv6 Relay 的源接口指定功能
配置 DHCPv6 Client	⚠ 必须配置。用于请求地址信息或前缀信息。	
	ipv6 dhcp client ia	启用 DHCPv6 Client 并请求 IANA 地址信息。
	ipv6 dhcp client pd	启用 DHCPv6 Client 并请求地址前缀信息。
	⚠ 可选配置。使收到 RA 通告的主机通过 DHCPv6 Client 请求无状态服务。	
	ipv6 nd other-config-flag	在发送 RA 通告的设备上设置 RA 里的 O 标识，使收到 RA 通告的主机通过 DHCPv6 Client 请求无状态服务。

### 5.4.1 配置 DHCPv6 Server

#### 配置效果

- 上游设备能自动为下游设备分配 DHCPv6 地址、前缀及相关配置参数。

#### 注意事项

- 要提供 DHCPv6 Server 服务，必须指定 DHCPv6 Server 信息池。
- 配置的信息池的名字不能过长。
- 启用 DHCPv6 Server 服务时，必须指定一个信息池。
- 只支持 SVI ( Switch Virtual Interface )、ROUTED PORT、L3 AP 三层接口上配置。

#### 配置方法

##### 配置 DHCPv6 Server 信息池

- 必须配置。
- 若无特殊要求，应在每台需要提供 DHCPv6 Server 服务的设备上配置信息池。

##### 配置 DHCPv6 Server 上可分配的地址前缀

- 可选配置。

- 若要提供分配地址服务，应在每台需要提供 DHCPv6 Server 服务的设备上配置可分配的地址前缀。

#### 配置 DHCPv6 Server 的静态绑定地址前缀信息

- 可选配置。
- 若要提供静态绑定地址前缀代理服务，应在每台需要提供 DHCPv6 Server 服务的设备上配置静态绑定地址前缀信息。

#### 配置 DHCPv6 Server 通过本地前缀池分配前缀

- 可选配置。
- 若要提供前缀代理服务，应在每台需要提供 DHCPv6 Server 服务的设备上指定本地前缀池。

#### 配置 IPv6 的本地前缀池

- 可选配置。
- 若要提供通过前缀池的前缀代理服务，应在每台需要提供 DHCPv6 Server 服务的设备上配置本地前缀池。

#### 配置 DHCPv6 Server 的 DNS Server 列表信息

- 可选配置。
- 若要提供 DNS Server 信息，应在每台需要提供 DHCPv6 Server 服务的设备上配置 DNS Server 信息。

#### 配置 DHCPv6 Server 的 domain name 信息

- 可选配置。
- 若要提供 Domain name 信息，应在每台需要提供 DHCPv6 Server 服务的设备上配置 domain name 信息。

#### 配置 DHCPv6 Server 的 CAPWAP AC 的 ipv6 地址信息

- 可选配置。
- 若要提供 CAPWAP AC 信息，应在每台需要提供 DHCPv6 Server 服务的设备上配置 CAPWAP AC 信息。

#### 配置启用 DHCPv6 Server 服务

- 必须配置。
- 若无特殊要求，应在每台需要提供 DHCPv6 Server 服务的设备上的具体接口配置启用 DHCPv6 Server 服务。

## 检验方法

DHCPv6 Server 成功为 DHCPv6 Client 提供地址、前缀或配置参数信息。

- DHCPv6 Client 获取到所需的信息。
- DHCPv6 Server 本地成功创建绑定。

## 相关命令

## 配置 DHCPv6 Server 信息池

- 【命令格式】 **ipv6 dhcp pool** *poolname*
- 【参数说明】 *poolname*: 用户定义的 DHCPv6 池名字。
- 【命令模式】 全局模式
- 【使用指导】 使用 **ipv6 dhcp pool** 命令来创建一个 DHCPv6 Server 的配置信息池。配置该命令之后，将进入 DHCPv6 池配置模式，在这种模式下，管理员可以配置池的参数，例如前缀信息以及 DNS Server 信息等。
- DHCPv6 Server 的配置信息池创建之后，可以使用 **ipv6 dhcp server** 命令将该池与某个接口上的 DHCPv6 Server 关联起来。

## 配置 DHCPv6 Server 的 IA\_NA 地址前缀

- 【命令格式】 **iana-address prefix** *ipv6-prefix/prefix-length* [ **lifetime** { *valid-lifetime* | *preferred-lifetime* } ]
- 【参数说明】 *ipv6-prefix/prefix-length*: IPv6 地址前缀和前缀长度。
- lifetime**: 用来设置客户端可以使用分配到的地址的有效时间。如果该关键字配置，则 *valid-lifetime* 和 *preferred-lifetime* 都要配置。
- valid-lifetime*: 客户端可以有效使用该地址的时间。
- preferred-lifetime*: 地址仍然被优先分配给客户端的时间。
- 【命令模式】 接口模式
- 【使用指导】 **iana-address prefix** 命令为 DHCPv6 Server 配置了 IA\_NA 地址范围，可以从中分配 IA\_NA 地址给客户端。当 Server 收到客户端的 IA\_NA 地址请求时，将尝试从 IA\_NA 地址范围中选取一个可用的地址分配给客户端。当客户端不再使用该地址时，Server 将该地址标记可用以提供给其他客户端使用。

## 配置 DHCPv6 Server 的静态绑定地址前缀信息

- 【命令格式】 **prefix-delegation** *ipv6-prefix/prefix-length client-DUID* [ *lifetime* ]
- 【参数说明】 *ipv6-prefix/prefix-length*: IPv6 地址前缀和前缀长度。
- client-DUID*: 客户端的 DUID。
- lifetime*: 设定客户端可以使用这个前缀的时间间隔。
- 【命令模式】 DHCPv6 池配置模式
- 【使用指导】 管理员可以使用 **prefix-delegation** 命令为客户端的 IA\_PD 手动配置一个地址前缀信息列表，并为这些前缀配置有效时间。
- 参数 *client-DUID* 指定了哪个客户端将分配到该地址前缀，该地址前缀将分配给客户端中第一个 IA\_PD。
- DHCPv6 Server 收到客户端对地址前缀的 request 消息之后，先查找是否有对应的静态绑定，如果找到则直接返回该静态绑定；否则，Server 将尝试从另外的前缀信息源来分配地址前缀。

## 配置 DHCPv6 Server 通过本地前缀池分配前缀

- 【命令格式】 **prefix-delegation pool** *poolname* [ **lifetime** { *valid-lifetime* | *preferred-lifetime* } ]
- 【参数说明】 *poolname*: 用户定义的本地前缀池的名字。
- lifetime**: 用来设置客户端可以使用分配到的前缀的有效时间。如果该关键字配置，则 *valid-lifetime* 和 *preferred-lifetime* 都要配置。
- valid-lifetime*: 客户端可以有效使用该前缀的时间。
- preferred-lifetime*: 前缀仍然被优先分配给客户端的时间。
- 【命令模式】 DHCPv6 池配置模式



【使用指导】 **prefix-delegation pool** 命令为 DHCPv6 Server 配置了前缀池，可以从中分配前缀信息给客户端。使用 **ipv6 local pool** 命令来配置前缀池。

当 Server 收到客户端的前缀请求时，将尝试从前缀池中选取一个可用的前缀分配给客户端。当客户端不再使用该前缀时，Server 将该前缀返回前缀池以提供给其他客户端使用。

#### 配置 IPv6 本地前缀池

【命令格式】 **ipv6 local pool** *poolname prefix/prefix-length assigned-length*

【参数说明】 *poolname*：本地前缀池名字。  
*prefix/prefix-length*：前缀和前缀长度。  
*assigned-length*：分配给用户的前缀长度。

【命令模式】 全局模式

【使用指导】 使用 **ipv6 local pool** 创建本地前缀池，DHCPv6 Server 如果需要进行前缀代理，使用 **prefix-delegation pool** 指定本地前缀池，后续的前缀将从指定的本地前缀池中分配。

#### 配置 DHCPv6 Server 的 DNS Server 列表信息

【命令格式】 **dns-server** *ipv6-address*

【参数说明】 *ipv6-address*：DNS Server 的地址。

【命令模式】 DHCPv6 池配置模式

【使用指导】 可以多次使用 **dns-server** 命令来配置多个 DNS Server 地址。新配置的 DNS Server 地址不会覆盖旧的 DNS Server 地址。

#### 配置 DHCPv6 Server 的 domain name 信息

【命令格式】 **domain-name** *domain*

【参数说明】 *domain*：定义要分配给用户的 domain-name 名字。

【命令模式】 DHCPv6 池配置模式

【使用指导】 可以多次使用 **domain-name** 命令来创建多个 domain-name。新配置的 domain-name 不会覆盖旧的 domain-name。

#### 配置 DHCPv6 Server 的 option52 信息

【命令格式】 **option52** *ipv6-address*

【参数说明】 *ipv6-address*：指定 CAPWAP AC 的 ipv6 地址。

【命令模式】 DHCPv6 池配置模式

【使用指导】 可以多次使用 **option52** 命令来创建多个 CAPWAP AC 的 *ipv6-address*。新配置的 CAPWAP AC *ipv6-address* 不会覆盖旧的 *ipv6-address*。

#### 配置启用 DHCPv6 Server 服务

【命令格式】 **ipv6 dhcp server** *poolname* [**rapid-commit**] [**preference** *value*]

【参数说明】 *poolname*：用户定义的 DHCPv6 池名字。  
**rapid-commit**：允许使用 two-message 交互过程。  
**preference** *value*：配置 advertise 消息的优先级。取值范围<0-255>，默认值为 0。

【命令模式】 接口配置模式

【使用指导】 **ipv6 dhcp server** 命令在接口上启用 DHCPv6 服务。

**rapid-commit** 关键字允许在分配地址前缀以及其他配置信息时,和客户端进行 two-message 的交互过程。配置了该关键字后,如果客户端的 solicit 消息中包含 **rapid-commit** 选项,那么 DHCPv6 Server 将直接以 Reply 消息回复。

**preference** 如果配置为非 0 的值,那么 DHCPv6 Server 在发送 advertise 消息时会携带 preference 选项。preference 选项字段会影响客户端对 Server 的选取,如果 advertise 消息不包含该字段,则认为 preference 为 0,如果客户端收到 preference 值为 255,则立即向该 Server 发出 request 消息来获取配置信息。

DHCPv6 Client、Server 以及 Relay 功能是互斥的,一次只能有一种模式能够在接口上配置。

## 配置举例

### 配置 DHCPv6 Server

- 【配置方法】
- 配置一个名为“pool1”的信息池
  - 配置 DHCPv6 Server 的 IA\_NA 地址前缀
  - 配置 DHCPv6 Server 的静态绑定地址前缀信息。
  - 配置两个 DNS Server。
  - 配置域名。
  - 在接口启用 DHCPv6 Server 服务。

```
Ruijie# configure terminal
Ruijie(config)# ipv6 dhcp pool pool1
Ruijie(config-dhcp)# iana-address prefix 2008:50::/64 lifetime 2000 1000
Ruijie(config-dhcp)# prefix-delegation 2008:2::/64 0003000100d0f82233ac
Ruijie(config-dhcp)# dns-server 2008:1::1
Ruijie(config-dhcp)# dns-server 2008:1::2
Ruijie(config-dhcp)# domain-name example.com
Ruijie(config-dhcp)#exit
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# ipv6 dhcp server pool1
```

- 【检验方法】
- 使用 **show ipv6 dhcp pool** 查看创建的信息池。

```
Ruijie# show ipv6 dhcp pool
DHCPv6 pool: pool1
Static bindings:
Binding for client 0003000100d0f82233ac
IA PD prefix: 2008:2::/64
preferred lifetime 3600, valid lifetime 3600
IANA address range: 2008:50::1/64 -> 2008:50::ffff:ffff:ffff:ffff/64
preferred lifetime 1000, valid lifetime 2000
DNS server: 2008:1::1
DNS server: 2008:1::2
Domain name: example.com
```

## 常见错误

---

- 指定了过长的 poolname。
- 配置的信息池数目超出系统限制 256 个。
- 在非 SVI ( Switch Virtual Interface )、ROUTED PORT、L3 AP 三层接口上配置。
- 配置 DHCPv6 Server 服务的接口数目超过系统限定值 256 个。
- 指定的 valid lifetime 值比 preferred lifetime 值小。
- 指定非法的 IA\_NA 地址。
- 配置的地址范围个数超过系统的限定值 20 个。
- 配置静态绑定地址前缀信息时，指定了过长的 DUID。
- 配置静态绑定地址前缀的数目超过系统的限定值 1024 个。
- 配置本地前缀池时，错误指定 valid lifetime 的时间大于 preferred lifetime。
- 配置的 DNS Server 个数超过系统限定值 10 个。
- 配置的 Domain Name 个数超过系统限定值 10 个。
- 配置的 option52 地址个数超过系统限定值 10 个。

## 5.4.2 配置 DHCPv6 Relay

### 配置效果

---

- 处于不同链路的 DHCPv6 Client 和 DHCPv6 Server 可以通过 Relay Agent 建立通信，进行地址分配、前缀代理、参数分配。

### 注意事项

---

- 需要指定目的地址，如果目的地址为多播地址（如 FF05::1:3），还需要指定出接口。

### 配置方法

---

#### 📄 配置 DHCPv6 Relay Agent 功能

- 必须配置。
- 若无特殊要求，应在每台需要提供 DHCPv6 Relay Agent 的设备上配置 DHCPv6 Relay 功能。

### 检验方法

---

DHCPv6 Client 和 DHCPv6 Server 通过 Relay Agent 进行报文交互。

- 检查接口状态是否为 DHCPv6 Relay 模式。
- 检查 DHCPv6 Relay Agent 是否可以正常收发报文。

## 相关命令

### 配置 DHCPv6 Relay Agent 功能

【命令格式】 **ipv6 dhcp relay destination** *ipv6-address* [*interface-type interface-number*]

【参数说明】 *ipv6-address*: 指定 Relay Agent 的目的端地址。  
*interface-type*: 指定到达目的端接口的类型（可选）。  
*interface-number*: 指定到达目的端接口的编号（可选）。

【命令模式】 接口配置

【使用指导】 开启 Dhcpv6 Relay 功能接口接收到的所有 DHCPv6 客户端报文都将被封装并朝指定接口（可选）发往配置好的目的地址（如果配置多个目的地址，则同时发多份。）

## 配置举例

### 配置 DHCPv6 Relay

【配置方法】 指定开启 Relay 服务的接口对于接收到的 DHCPv6 Client 报文通过指定接口（可选）转发至指定目的地址

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#interface vlan 1
Ruijie(config-if)#ipv6 dhcp relay destination 3001::2
Ruijie(config-if)#ipv6 dhcp relay destination ff02::1:2 vlan 2
```

【检验方法】 使用 **show ipv6 dhcp relay destination all** 查看配置的目的地址信息。

```
Interface:VLAN 1
Destination address(es)          Output Interface
3001::2
ff02::1:2                       VLAN 2
```

## 常见错误

- 在非 SVI（Switch Virtual Interface）、ROUTED PORT、L3 AP 三层接口上配置。

## 5.4.3 配置 DHCPv6 Client

### 配置效果

- 实现设备自动向服务器请求 IPv6 地址，或相关参数。

## 注意事项

---

- 只能在三层接口上配置。

## 配置方法

---

### ▾ 启用 DHCPv6 Client 并请求 IANA 地址信息。

- 必须配置。
- 若无特殊要求，应在每台需要通过 DHCPv6 请求地址的设备上启用 DHCPv6 Client 地址请求功能。

### ▾ 启用 DHCPv6 Client 并请求地址前缀信息。

- 必须配置。
- 若无特殊要求，应在每台需要通过 DHCPv6 请求前缀的设备上启用 DHCPv6 Client 前缀请求功能。

### ▾ 启用 DHCPv6 Client 无状态服务。

- 需要获取配置参数信息时，必须配置。

## 检验方法

---

检查接口是否使能 DHCPv6 Client 和接口上获取到的地址、前缀等信息。

## 相关命令

---

### ▾ 启用 DHCPv6 Client 请求地址功能

- 【命令格式】 **ipv6 dhcp client ia [ rapid-commit ]**
- 【参数说明】 **rapid-commit**：允许使用简化的交互过程。
- 【命令模式】 接口配置模式
- 【使用指导】 如果 DHCPv6 客户端模式还没有打开，该命令会在接口上启用 DHCPv6 客户端模式。  
**ipv6 dhcp client ia** 命令启用之后会向 DHCPv6 Server 发出 IANA 地址请求。  
**rapid-commit** 关键字允许客户端和服务端使用 two-message 交互过程，如果配置了该关键字，客户端发出的 solicit 消息中将包含 rapid-commit 选项。

### ▾ 启用 DHCPv6 Client 前缀请求

- 【命令格式】 **ipv6 dhcp client pd *prefix-name* [ rapid-commit ]**
- 【参数说明】 *prefix-name*：IPv6 通用前缀名。  
**rapid-commit**：允许使用简化的交互过程。
- 【命令模式】 接口配置模式

- 【使用指导】 如果 DHCPv6 客户端模式还没有打开，该命令会在接口上启用 DHCPv6 客户端模式。
- ipv6 dhcp client pd** 命令启用之后会向 DHCPv6 Server 发出前缀请求。得到前缀信息时，client 会将这个前缀信息保存在 IPv6 通用前缀池中，其他的命令以及应用程序就可以使用这个前缀。
- rapid-commit** 关键字允许客户端和服务端使用 two-message 交互过程，如果配置了该关键字，客户端发出的 solicit 消息中将包含 rapid-commit 选项。

## 配置无状态服务

- 【命令格式】 **ipv6 nd other-config-flag**
- 【参数说明】 -
- 【命令模式】 接口配置模式
- 【使用指导】 在发送 RA 通告的主机上设置 other-config-flag，则触发收到该 RA 通告的主机通过 DHCPv6 Client 获取无状态配置信息。

## 配置举例

### 启用 DHCPv6 Client 请求地址功能

- 【配置方法】
- 在接口上配置 DHCPv6 Client 地址请求功能。
- ```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# ipv6 dhcp client ia
```
- 【检验方法】
- 使用 **show ipv6 dhcp interface** 命令可以检查接口上是否启用 DHCPv6 Client。
- ```
Ruijie#show ipv6 dhcp interface GigabitEthernet 0/1
GigabitEthernet 0/1 is in client mode
Rapid-Commit: disable
```

### 启用 DHCPv6 Client 前缀请求

- 【配置方法】
- 在接口上配置 DHCPv6 Client 前缀请求功能。
- ```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# ipv6 dhcp client pd pd_name
```
- 【检验方法】
- 使用 **show ipv6 dhcp interface** 命令可以检查接口上是否启用 DHCPv6 Client。
- ```
Ruijie#show ipv6 dhcp interface GigabitEthernet 0/1
GigabitEthernet 0/1 is in client mode
Rapid-Commit: disable
```

### 启用 DHCPv6 Client 无状态请求

- 【配置方法】
- 在提供 RA 通告设备的接口上配置 other-config-flag。
- ```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# ipv6 nd other-config-flag
```

- 【检验方法】 ● 使用 **show ipv6 dhcp interface** 命令可以检查主机的某个接口是否获取到的配置参数信息。

```
Ruijie#show ipv6 dhcp interface GigabitEthernet 0/2
GigabitEthernet 0/2 is in client mode
DNS server: 2001::1
Rapid-Commit: disable
```

## 常见错误

- 在非三层接口上启用 DHCPv6 Client 地址请求。
- 在已启用 DHCPv6 Relay 或者 DHCPv6 Server 的接口上启用 DHCPv6 地址请求。
- 在非三层接口上启用 DHCPv6 Client 前缀请求。
- 在已启用 DHCPv6 Relay 或者 DHCPv6 Server 的接口上启用 DHCPv6 前缀请求。

## 5.4.4 配置源接口指定功能

### 配置效果

- 指定 DHCPv6 Relay 转发报文的源 IP 地址和 link address 字段。

### 注意事项

- 指定参数类型为接口时，该接口必须为三层口，且接口变更为非三层口后，将会删除对应的源接口指定配置信息。

### 配置方法

#### 配置源接口-源 IP 地址指定功能

- 可选配置。
- 若仅要求改变转发报文的源 IP 地址信息，可在相应的接口或者全局配置源接口-源 IP 地址指定功能。

#### 配置源接口-网关地址指定功能

- 可选配置。
- 若要求改变 DHCPv6 Client 获取到的网段信息，可在相应的接口或者全局配置源接口-网关地址指定功能。

### 检验方法

DHCPv6 Relay 的转发报文中相应字段根据指定配置信息正确填充。

- 抓包查看相应字段是否与源接口指定功能的配置信息一致。
- 检查 DHCPv6 Relay Agent 是否可以正常收发报文。

## 相关命令

### 配置源接口指定功能

- 【命令格式】 **ipv6 dhcp relay source {source-ip-address | gateway-address} {ipv6 address | interface-type interface-number}**
- 【参数说明】 **source-ip-address**：源接口-源 IP 地址指定类型，填充转发报文的源 IP 地址  
**gateway-address**：源接口-网关地址指定类型，填充转发报文的源 IP 地址和 link address 字段  
**ipv6-address**：源接口的指定参数类型，IPv6 地址  
**interface-type**：源接口的指定参数类型，指定接口的接口类型  
**interface-number**：源接口的指定参数类型，指定接口的接口编号
- 【命令模式】 全局/接口配置模式
- 【使用指导】 源接口指定功能会变更 DHCPv6 中继转发报文的源 IP 地址和 link address 字段；源接口指定功能的指定类型分为源 IP 地址指定和网关地址指定，前者变更转发报文的源 IP 地址，后者变更转发报文的源 IP 地址和 link address 字段。源接口指定功能允许配置于全局模式和接口模式，其中接口模式的源接口指定类型优先级大于全局模式的；而同一个模式下，新配置的源接口指定类型覆盖旧的指定类型。

## 配置举例

### 配置源接口指定功能

- 【配置方法】 配置接口 Interface VLAN 1 上开启源接口指定功能，指定类型为源接口-网关地址，指定参数类型为 IPv6 地址；全局模式上开启源接口指定功能，指定类型为源接口-源 IP 地址，指定参数类型为接口。

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface vlan 1
Ruijie(config-if)# ipv6 dhcp relay source gateway-address 1000::1
Ruijie(config-if)# exit
Ruijie(config)# ipv6 dhcp relay source source-ip-address loopback 0
Ruijie(config)#
```

- 【检验方法】 使用 **show ipv6 dhcp relay source** 查看设备当前源接口指定功能配置信息。

```
Ruijie#show ipv6 dhcp relay source
```

| Interface-Name | Source-Intf-Type | Source-Intf-Parameter |
|----------------|------------------|-----------------------|
| Global         | Source Address   | Loopback 0            |
| VLAN 1         | Gateway Address  | 1000::1               |

## 常见错误



在非 SVI ( Switch Virtual Interface )、ROUTED PORT、L3 AP 三层接口上配置

## 5.4.5 配置网关地址自动切换功能

### 配置效果

---

- Dhcpv6 relay 在 client 申请地址失败时，会变更转发报文中的 link address 字段。达到自动切换网段申请地址的目的

### 注意事项

---

- 只能在三层接口上配置

### 配置方法

---

#### 配置网关地址自动切换功能

- 可选配置。
- 若需要网关地址自动切换功能，需要在相应接口启用该功能。

### 检验方法

---

DHCPv6 Relay 的转发报文中相应字段在申请地址失败时会自动变更。

- 抓包查看在申请地址失败时，link address 字段会自动切换。
- 检查 DHCPv6 Relay Agent 是否可以正常收发报文。

### 相关命令

---

#### 配置源接口指定功能

【命令格式】 **ipv6 dhcp smart-relay**

【参数说明】 -

【命令模式】 接口配置模式

【使用指导】 网关地址自动切换功能能够在设备申请 ipv6 地址失败后，自动变更转发报文中的 link address 字段，达到切换网段申请地址的功能。

### 配置举例

---

#### 配置源接口指定功能

【配置方法】 配置接口 Interface VLAN 1 上开启源接口指定功能 ,指定类型为源接口-网关地址 ,指定参数类型为 IPv6 地址 ;

全局模式上开启源接口指定功能，指定类型为源接口-源 IP 地址，指定参数类型为接口。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface vlan 1
Ruijie(config-if)# ipv6 dhcp smart-relay
Ruijie(config-if)# exit
```

【检验方法】 使用 **show run** 查看网关地址自动切换功能的配置信息。


```
Ruijie#show run
interface VLAN 1
    ipv6 dhcp smart-relay
!
```

常见错误

在非 SVI ( Switch Virtual Interface )、ROUTED PORT、L3 AP 三层接口上配置

5.5 监视与维护

清除各类信息

 在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

| 作用                                   | 命令                                                                   |
|--------------------------------------|----------------------------------------------------------------------|
| 清除 DHCPv6 绑定信息。                      | <b>clear ipv6 dhcp binding</b> [ <i>ipv6-address</i> ]               |
| 清除 DHCPv6 服务器统计信息。                   | <b>clear ipv6 dhcp server statistics</b>                             |
| 清除 DHCPv6 Server 的冲突地址信息。            | <b>clear ipv6 dhcp conflict</b> { <i>ipv6-address</i>   * }          |
| 清除当前设备开启 DHCPv6 Relay 功能后各类报文收发情况统计。 | <b>clear ipv6 dhcp relay statistics</b>                              |
| 重新启动 DHCPv6 Client 功能。               | <b>clear ipv6 dhcp client</b> <i>interface-type interface-number</i> |

查看运行情况

| 作用                    | 命令                                                        |
|-----------------------|-----------------------------------------------------------|
| 查看设备的 DUID 信息。        | <b>show ipv6 dhcp</b>                                     |
| 查看 DHCPv6 服务器的地址绑定信息。 | <b>show ipv6 dhcp binding</b> [ <i>ipv6-address</i> ]     |
| 查看 DHCPv6 接口信息。       | <b>show ipv6 dhcp interface</b> [ <i>interface-name</i> ] |
| 查看 DHCPv6 池信息。        | <b>show ipv6 dhcp pool</b> [ <i>poolname</i> ]            |

|                                    |                                                                                          |
|------------------------------------|------------------------------------------------------------------------------------------|
| 查看 DHCPv6 的冲突地址信息。                 | <b>show ipv6 dhcp conflict</b>                                                           |
| 查看 DHCPv6 Server 的统计信息。            | <b>show ipv6 dhcp server statistics</b>                                                  |
| 查看 DHCPv6 Relay Agent 目的端地址信息。     | <b>show ipv6 dhcp relay destination { all   <i>interface-type interface-number</i> }</b> |
| 查看当前设备开启 DHCPv6 Relay 功能后各类报文收发情况。 | <b>show ipv6 dhcp relay statistics</b>                                                   |
| 查看 IPv6 本地前缀池信息。                   | <b>show ipv6 local pool [ <i>poolname</i> ]</b>                                          |
| 查看源接口指定功能的配置信息                     | <b>show ipv6 dhcp relay source</b>                                                       |

## 查看调试信息



输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

| 作用              | 命令                                |
|-----------------|-----------------------------------|
| 打开 DHCPv6 调试开关。 | <b>debug ipv6 dhcp [ detail ]</b> |

## 6 DNS

### 6.1 概述

DNS ( Domain Name System , 域名系统 ) , 因特网上作为域名和 IP 地址相互映射的一个分布式数据库 , 能够使用户更方便的访问互联网 , 而不用去记住能够被机器直接读取的 IP 数串。通过主机名 , 最终得到该主机名对应的 IP 地址的过程叫做域名解析 ( 或主机名解析 ) 。

 下文仅介绍 DNS 的相关内容。

#### 协议规范

- RFC1034 : DOMAIN NAMES - CONCEPTS AND FACILITIES
- RFC1035 : DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

### 6.2 典型应用

| 典型应用   | 场景描述                        |
|--------|-----------------------------|
| 静态域名解析 | 直接在本设备上根据预设的域名/IP 对应表进行域名解析 |
| 动态域名解析 | 从网络上的 DNS 服务器动态获取域名对应的地址    |

#### 6.2.1 静态域名解析

##### 应用场景

- 在设备上预设置域名和 IP 的对应表
- 设备上的一些应用 ( 比如 Ping , Telnet 等 ) 进行域名操作时 , 直接在设备上就能解析到预设的 IP , 无需连到网络上的服务器。

##### 功能部署

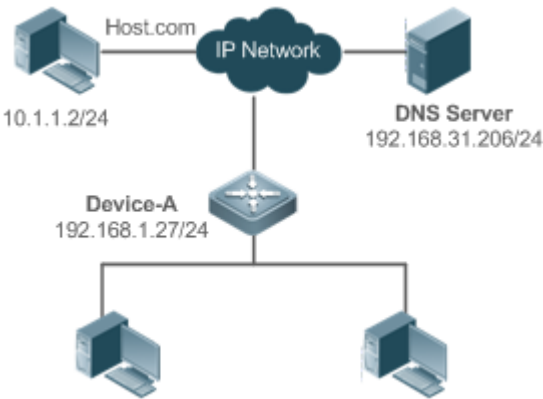
- 在设备上预设置域名和 IP 的对应关系

#### 6.2.2 动态域名解析

##### 应用场景

- “DNS Server” 部署在网络上，对外提供域名服务
- “host.com” 部署在网络上，使用域名(host.com)对外提供服务
- “Device-A”设备指定 “DNS Server” 作为 DNS 服务器，从 “DNS Server” 上获取到 “host.com”的地址

图 6-1 动态域名解析配置组网图



功能部属

- 将 DNS Server 部署为"Device-A"的 DNS 服务器

6.3 功能详解

基本概念

📌 DNS

DNS 由解析器和域名服务器组成。域名服务器是指保存有网络中所有主机的域名和 IP 地址的对应关系，并提供将域名和 IP 互转的服务器。DNS 的 TCP 和 UDP 端口号都是 53，通常使用 UDP。

功能特性

| 功能特性 | 作用                          |
|------|-----------------------------|
| 域名解析 | 根据域名从域名服务器或本地数据库获取对应的 IP 地址 |

6.3.1 域名解析

工作原理

📌 静态域名解析

静态域名解析，就是用户在设备上预先设置好域名和 IP 的对应关系，当用户使用某些应用(比如 Ping、Telnet 等等)进行域名操作时，系统从本设备上解析出域名对应的 IP，而不需要到网络上的 DNS 服务器获取域名对应的 IP。

### 📌 动态域名解析

动态域名解析，就是当用户使用某些应用进行域名操作时，系统 DNS 解析器查询外部的 DNS 服务器，获取到域名对应的 IP。

动态域名解析过程：

19. 用户应用(Ping、Telnet 等)向系统 DNS 解析器请求域名对应的 IP
20. 系统 DNS 解析器先查找动态缓存，如果动态缓存的域名未过期则返回给应用程序
21. 如果不存在未过期的域名，DNS 解析器向外部的 DNS 服务器发起域名转 IP 的请求
22. DNS 解析器接收到 DNS 服务器的应答，缓存并转发给应用程序

## 相关配置

### 📌 开启域名解析功能

- 缺省情况下，设备是开启域名解析功能。
- 通过 **ip domain-lookup** 命令开启域名解析功能。

### 📌 配置静态域名对应的 IP

- 缺省情况下，没有域名/IP 的静态配置。
- 通过 **ip host** 命令指定域名对应的 IPv4 地址
- 通过 **ipv6 host** 命令配置域名对应的 IPv6 地址

### 📌 配置域名服务器

- 缺省情况下，未配置域名服务器。
- 通过 **ip name-server** 命令配置域名服务器。

## 6.4 配置详解

| 配置项      | 配置建议 & 相关命令             |                 |
|----------|-------------------------|-----------------|
| 配置静态域名解析 | ⚠️ 可选配置                 |                 |
|          | <b>ip domain-lookup</b> | 开启域名解析功能        |
|          | <b>ip host</b>          | 配置域名对应的 IPv4 地址 |
|          | <b>ipv6 host</b>        | 配置域名对应的 IPv6 地址 |
| 配置动态域名解析 | ⚠️ 可选配置                 |                 |
|          | <b>ip domain-lookup</b> | 开启域名解析功能        |
|          | <b>ip name-server</b>   | 配置域名服务器         |

## 6.4.1 配置静态域名解析

### 配置效果

---

系统解析器从设备本地解析域名对应的 IP。

### 配置方法

---

#### 📌 开启域名解析功能

- 缺省已开启域名解析功能
- 如果关闭该功能，静态域名解析不生效。

#### 📌 配置静态域名对应的 IP 地址

- 必须配置，用户使用到的域名必须配置对应的 IP。

### 检验方法

---

- 通过 **show run** 查看配置信息。
- 通过 **show hosts** 当前的域名和 IP 对应关系

### 相关命令

---

#### 📌 配置域名对应的 IPv4 地址

- 【命令格式】 **ip host** *host-name ip-address*
- 【参数说明】 *host-name*：域名  
*ip-address*：对应的 IPv4 地址
- 【命令模式】 全局模式
- 【使用指导】 -

#### 📌 配置域名对应的 IPv6 地址

- 【命令格式】 **ipv6 host** *host-name ipv6-address*
- 【参数说明】 *host-name*：域名  
*ipv6-address*：对应的 IPv6 地址
- 【命令模式】 全局模式
- 【使用指导】 -

### 配置举例

---

## 配置静态域名解析

- 【配置方法】
- 在设备上静态配置域名 `www.test.com` 的 IP 地址为 `192.168.1.1`
  - 在设备上静态配置域名 `www.testv6.com` 的 IP 地址为 `2001::1`

```
Ruijie#configure terminal
Ruijie(config)# ip host www.test.com 192.168.1.1
Ruijie(config)# ipv6 host www.testv6.com 2001::1
Ruijie(config)# exit
```

- 【检验方法】 通过 **show hosts** 查看是否有所配置的静态域名表项

```
Ruijie#show hosts
Name servers are:

Host                type    Address          TTL(sec)
www.test.com        static  192.168.1.1     ---
www.testv6.com      static  2001::1         ---
```

## 6.4.2 配置动态域名解析

### 配置效果

系统解析器从 DNS 服务器解析域名对应的 IP

### 配置方法

#### 开启域名解析功能

- 缺省已开启域名解析功能
- 如果关闭该功能，动态域名解析不生效。

#### 配置 DNS 服务器

- 必须配置，使用动态域名解析必须配置外部的 DNS 服务器。

### 检验方法

- 通过 **show run** 查看配置信息

### 相关命令

#### 配置域名服务器

- 【命令格式】 **ip name-server [ oob ] { ip-address | ipv6-address }**
- 【参数说明】 *ip-address* : DNS 服务器的 IPv4 地址



*ipv6-address* : DNS 服务器的 IPv6 地址  
*oob* : DNS 服务器支持带外管理接口 ( interface of mgmt )

- 【命令模式】全局模式
- 【使用指导】-

配置举例

配置动态域名解析

【网络环境】

图 6-2



DEVICE : 从网络上的 DNS 服务器(192.168.10.1)解析域名

【配置方法】在设备上配置 DNS 服务器地址为 192.168.10.1

```
DEVICE#configure terminal
DEVICE(config)# ip name-server 192.168.10.1
DEVICE(config)# exit
```


【检验方法】通过 **show hosts** 查看是否配置指定 DNS 服务器

```
Ruijie(config)#show hosts
Name servers are:
192.168.10.1 static

Host          type      Address                               TTL(sec)
```

6.5 监视与维护

清除各类信息


 在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

| 作用          | 命令                                     |
|-------------|----------------------------------------|
| 清除动态主机名缓存表。 | <b>clear host</b> [ <i>host-name</i> ] |

查看运行情况

| 作用           | 命令                                     |
|--------------|----------------------------------------|
| 查看 DNS 的相关参数 | <b>show hosts</b> [ <i>host-name</i> ] |

查看调试信息

 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

| 作用     | 命令                  |
|--------|---------------------|
| 打开调试功能 | <b>debug ip dns</b> |

## 7 FTP-Server

### 7.1 概述

FTP Server 功能可以将一台设备配置为 FTP 服务器。这样可以通过 FTP 客户端与之连接，通过 FTP 协议往设备上传或下载文件。

用户可以利用 FTP Server 功能方便地获取设备中的文件，如 syslog 日志文件等；也可以通过 FTP 直接往设备的文件系统拷贝文件。

 下文仅介绍 FTP 的相关内容。

#### 协议规范

- RFC959 : FILE TRANSFER PROTOCOL (FTP)
- RFC3659 : Extensions to FTP
- RFC2228: FTP Security Extensions
- RFC2428: FTP Extensions for IPv6 and NATs
- RFC1635: How to Use Anonymous FTP

### 7.2 典型应用

| 典型应用          | 场景描述                   |
|---------------|------------------------|
| 局域网内提供 FTP 服务 | 在一个局域网内为同一个用户提供上传与下载服务 |

#### 7.2.1 局域网内提供 FTP 服务

##### 应用场景

在一个局域网内为同一个用户提供上传与下载服务

以下图为例，仅在局域网内开启 FTP-Server 服务

- G 开启 FTP Server 服务，S 二层透传功能
- User 发起 FTP 上传与下载请求

图 7-1



【注释】 G 为出口网关设备。  
S 为接入设备

## 功能部属

- G 启动 FTP Server
- S 当作二层交换机，起到二层透传的作用

## 7.3 功能详解

### 基本概念

#### FTP 协议

FTP ( File Transfer Protocol ) 是 IETF Network Working Group 所制定的一套标准协议，属于网络协议组的应用层，FTP 基于 TCP 传输控制协议(Transmission Control Protocol)实现文件传输。FTP 使用户能在两个联网的计算机之间传输文件，它是 Internet 传递文件最主要的方法。使用匿名 FTP，用户可以免费获取 Internet 丰富的资源。除此之外，FTP 还提供登录、目录查询、文件操作及其它会话控制等功能。FTP 协议在 TCP/IP 协议族中属于应用层协议，使用 TCP 端口 20 和 21 进行传输。端口 20 用于传输数据，端口 21 用于传输控制消息。FTP 协议基本操作在 RFC959 中进行了描述。

#### 用户授权

FTP Client 要连上 FTP Server，必须要有该 FTP 服务器授权的帐号，只有拥有一个用户标识和一个口令后才能登陆 FTP 服务器，享受 FTP 服务器提供的服务。设计考虑最大支持设定用户个数为 10 个，每个用户最大连接数为 2 个，服务器最大连接数为 10 个。

#### FTP 文件传输模式

FTP 有两种文件传输模式：

- 文本传输方式：也称为 ASCII 模式，用于传输文本格式的文件（比如后缀名为.txt、.bat 和.cfg 的文件），与 Binary 模式的区别是回车换行的处理，ASCII 模式将回车换行转换为本机的回车字符，比如 Unix 下是\n，Windows 下是\r\n，Mac 下是\r。假定用户正在拷贝的文件包含 ASCII 码文本，如果在远程机器上运行的不是 UNIX，当文件传输时 FTP 通常会自动地调整文件的内容以便于把文件解释成对端计算机存储文本文件的格式。
- 二进制传输模式：也称为 Binary 模式，用于传输程序文件（比如后缀名为.app、.bin 和.btm 的文件），可用来传送可执行文件，压缩文件，和图片文件，不对数据进行任何处理，比文本模式更快，可以传输所有 ASCII 值，保证不出错。

#### FTP 工作方式

FTP 的两种工作方式：

图 7-2

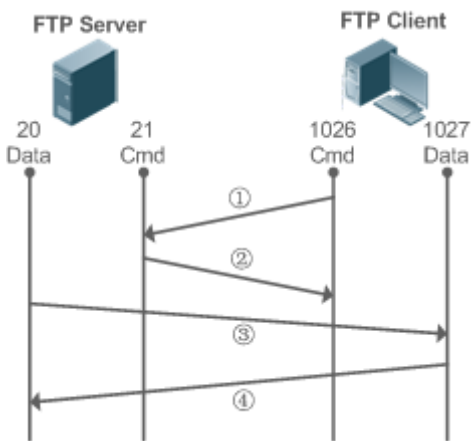
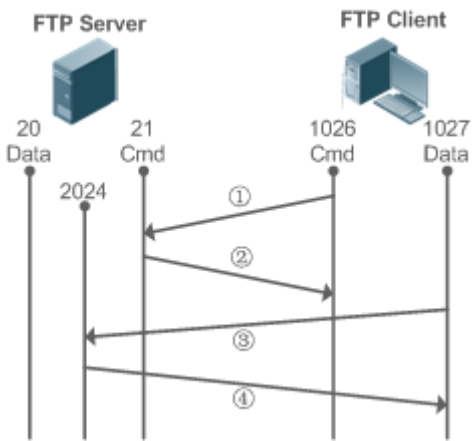


图 7-3



- PORT 模式见图 7-2：FTP 客户端首先通过端口(1026)和 FTP 服务器的端口(21)建立连接，通过这个通道发送命令，客户端需要接收数据的时候在这个通道上发送 PORT 命令。PORT 命令包含了客户端数据通道端口(1027)来接收数据。在传送数据的时候，服务器端通过自己的端口(20)连接至客户端的端口(1027)建立数据通道，实现数据收发；FTP Server 必须和客户端建立一个新的连接用来传送数据。
- PASV 模式见图 7-3：在建立控制通道的时候与 PORT 模式类似，但建立连接后发送的不是 Port 命令，而是 PASV 命令。FTP 服务器收到 PASV 命令后，随机打开一个高端端口( 2024 )并且通知客户端在该端口上传送数据，客户端用端口( 1027 )连接 FTP 服务器该端口，之后便可以在通道上进行数据收发，这个时候 FTP Server 不再需要建立一个新的和客户端之间的连接。

支持的 FTP 命令

当设备收到 FTP 连接请求时，FTP 服务器将要求客户端提供登录用户名和密码以进行身份认证。如果客户端通过身份认证，即可执行 FTP 客户端命令进行操作。目前的 FTP 服务器并没有支持所有的 FTP 命令，具体支持的 FTP 客户端命令如下：

|       |        |         |       |      |      |
|-------|--------|---------|-------|------|------|
| ascii | delete | mdelete | mput  | quit | send |
| bin   | dir    | mdir    | nlist | recv | size |

|       |     |       |         |        |        |
|-------|-----|-------|---------|--------|--------|
| bye   |     | mget  |         | rename | system |
| cd    | get | mkdir | passive |        | type   |
| cdup  |     | mls   | put     | rmdir  | user   |
| close | ls  |       | pwd     |        |        |

以上 FTP 客户端命令的用法请参考您所使用的 FTP 客户端软件的文档。另外不少 FTP 客户端工具（如 CuteFTP、FlashFXP 等）均提供了图形化的操作界面，使用此类工具可以无需再通过 FTP 命令进行操作。

## 功能特性

| 功能特性             | 作用                                     |
|------------------|----------------------------------------|
| 开启 FTP Server 服务 | 为 FTP-Client 提供上传、下载、显示文件、创建文件、删除文件等功能 |

### 7.3.1 开启 FTP Server 服务

#### 工作原理

基本工作原理如上一章所述，我司设备需要配置用户名、密码、顶层目录即可为用户提供 FTP 服务。

#### 相关配置

##### 全局使能 FTP Server

缺省情况下，全局不开启 FTP 服务器

使用 **ftp-server enable** 开启

必须在全局开启 FTP 服务器功能，否则无法使用

##### 配置用户名密码及顶层目录


缺省情况下，无用户授权及顶层目录

使用 **ftp-server username password**、**ftp-server topdir** 来设置授权与顶层目录

以上三项必须配置无配置无法启动 FTP 服务器功能

## 7.4 配置详解

| 配置项                | 配置建议&相关命令                                                                                              |               |
|--------------------|--------------------------------------------------------------------------------------------------------|---------------|
| 配置 FTP Server 基本功能 |  必须配置，用于启动 FTP 服务器。 |               |
|                    | <b>ftp-server enable</b>                                                                               | 启动 FTP 服务器功能  |
|                    | <b>ftp-server login timeout</b>                                                                        | 配置 FTP 登陆有效时长 |

|  |                                                                                        |                |
|--|----------------------------------------------------------------------------------------|----------------|
|  | ftp-server login times                                                                 | 配置 FTP 登陆有效次数  |
|  | ftp-server topdir                                                                      | 配置 FTP 服务器顶层目录 |
|  | ftp-server username password                                                           | 设置用户名，密码       |
|  |  可选配置 |                |
|  | ftp-server timeout                                                                     | 配置 FTP 会话的空闲时限 |

## 7.4.1 配置 FTP Server 基本功能

### 配置效果

- 建立 FTP Server，向 FTP Client 提供 FTP 服务

### 注意事项

- 需要配置用户名、密码及顶层访问目录
- 如果需要服务器在有限时间内关闭异常的会话，需要配置会话空闲时限

### 配置方法

#### 启动 FTP Server 功能

- 必须配置
- 若无特殊要求，应在每台路由器上启动 FTP Server 功能

#### 配置顶层目录

- 必须配置
- 若无特殊要求，应每台路由器上配置顶层目录为根目录

#### 配置登录用户名和密码

- 必须配置
- 注意用户名和密码的长度有限制

#### 配置会话空闲时限

- 可先配置
- 当 FTP 服务器某个用户在线时，如果该用户连接异常中断或用户非正常中断连接，FTP 服务器可能无法知道用户断开而将继续保持连接，导致与服务器的连接被长期占用使服务器无法响应其他用户的登录请求，因此可以配置该选项保证异常发生时在一定时间段内让其它用户可连接上

## 检验方法

利用 FTP 客户端与服务器进行连接

- 检查客户端是否能连接成功
- 检查客户端相关操作是否正常

## 相关命令

### 启动 FTP Server 功能

【命令格式】 **ftp-server enable**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 在正确配置服务器的顶层目录、登录用户名和密码之前客户端仍然无法访问 FTP 服务器，因此建议在首次启动服务之前先参考后面的章节完成服务器顶层目录、登录用户名与密码的配置

### 配置会话登陆有效次数

【命令格式】 **ftp-server login times times**

【参数说明】 *times*：有效次数（范围：1-10）

【命令模式】 全局模式

【使用指导】 会话的有效次数是指在一个 FTP 会话在登陆过程中，用户最多可以进行账号密码认证的次数。默认设置为 3 次，即在累计三次输入错误的用户名或密码时，会话被中止，从而允许其他用户上线。

### 配置会话登陆有效时长

【命令格式】 **ftp-server login timeout timeout**

【参数说明】 *timeout*：登陆有效时间（单位：分钟；范围：1-30）

【命令模式】 全局模式

【使用指导】 登陆有效时间是指用户建立链接后，每次认证用户账号和密码的最长在线时间。在该有效时间内用户若未再次进行用户密码认证将被中止会话，从而保证其他用户能够登陆。

### 配置服务器顶层目录

【命令格式】 **ftp-server topdir directory**

【参数说明】 *directory*：指定用户访问路径

【命令模式】 全局模式

【使用指导】 如可以指定服务器的顶层目录为“/syslog”目录，则 FTP 客户端登录后将仅能访问设备上“/syslog”目录下的文件和文件夹，客户端由于顶层目录的限制将无法退到“/syslog”目录的上级目录中



## 配置服务器登录用户名和密码

- 【命令格式】 **ftp-server username username password [type] password**
- 【参数说明】 *username* : 用户名  
*type* : 0 或 7, 0 代表密码未加密 (明文), 7 代表密码为加密过的密文  
*password* : 密码
- 【命令模式】 全局模式
- 【使用指导】 FTP 服务器不支持匿名用户, 因此需要配置用户名  
用户名最大长度为 64 个字符, 中间不允许有空格。用户名可以由英文字母、半角数字和半角符号组成  
密码必须为字母或数字, 密码前后可以有空格, 但将被忽略; 密码中间的空格作为密码的一部分。  
明文密码的最小长度为 1 个字符、最大长度为 25 个字符; 密文密码的最小长度为 4 个字符、最大长度为 52 个字符。  
用户名和密码必须一一配对, 最多仅能配置 10 个用户。

## 配置会话空闲时限

- 【命令格式】 **ftp-server timeout time**
- 【参数说明】 *time* : 空闲时限 (单位: 分钟; 范围: 1-3600)
- 【命令模式】 全局模式
- 【使用指导】 会话的空闲时间是指在一个 FTP 会话中从上次 FTP 操作完成后到下次 FTP 操作开始之间的时间。服务器在响应完一个 FTP Client 命令操作后 (如一个文件全部传输完毕后) 重新开始计算会话空闲时间; 在下一个 FTP Client 命令操作到来的时停止计算会话空闲时间。因此会话空闲时限的配置并不会对某些耗时的文件传输操作带来任何影响


## 查看服务器的状态信息

- 【命令格式】 **show ftp-server**
- 【参数说明】 -
- 【命令模式】 特权模式
- 【使用指导】 显示 FTP 服务器的相关状态信息

## 打开服务器的调试信息

- 【命令格式】 **debug ftp-server pro/err**
- 【参数说明】 -
- 【命令模式】 特权模式
- 【使用指导】 打开 FTP 服务器的过程/错误调试信息输出

## 配置举例

 以下配置举例, 仅介绍与 FTP Server 相关的配置。

## 在 IPv4 网络上建立 FTP Server 服务

- 【网络环境】 ● 能够建立从服务器传输到客户端的 TCP 连接。

- 【配置方法】
- 开启 FTP Server 服务
  - 配置顶层目录/syslog
  - 配置用户名为 user、密码为 password
  - 配置会话空闲时限为 5 分钟

```
Ruijie(config)#ftp-server username user
Ruijie(config)#ftp-server password password
Ruijie(config)#ftp-server timeout 5
Ruijie(config)#ftp-server topdir /
Ruijie(config)#ftp-server enable
```

【检验方法】 1.show ftp-server 查看

```
Ruijie#show ftp-server

ftp-server information
=====

enable : Y
topdir : tmp:/
timeout: 10min

username:aaaa          password:(PLAIN)bbbb          connect num[2]
    [0]trans-type:BINAR (ctrl)server IP:192.168.21.100[21]
                                client IP:192.168.21.26[3927]
    [1]trans-type:ASCII (ctrl)server IP:192.168.21.100[21]
                                client IP:192.168.21.26[3929]

username:a1            password:(PLAIN)bbbb          connect num[0]
username:a2            password:(PLAIN)bbbb          connect num[0]
username:a3            password:(PLAIN)bbbb          connect num[0]
username:a4            password:(PLAIN)bbbb          connect num[0]
username:a5            password:(PLAIN)bbbb          connect num[0]
username:a6            password:(PLAIN)bbbb          connect num[0]
username:a7            password:(PLAIN)bbbb          connect num[0]
username:a8            password:(PLAIN)bbbb          connect num[0]
username:a9            password:(PLAIN)bbbb          connect num[0]
```

## 常见错误

- 未配置用户名

- 未配置密码
- 未配置顶层目录

## 7.5 监视与维护

### 清除各类信息

---

-


### 查看运行情况

---

| 作用               | 命令              |
|------------------|-----------------|
| 查看 FTP Server 配置 | show ftp-server |

### 查看调试信息

---

 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

| 作用                       | 命令                          |
|--------------------------|-----------------------------|
| 打开 FTP Server 错误事件的调试开关。 | <b>debug ftp-server err</b> |
| 打开 FTP Server 消息事件的调试开关。 | <b>debug ftp-server pro</b> |

## 8 FTP Client


### 8.1 概述

FTP ( File Transfer Protocol , 文件传输协议 ) , 是 TCP/IP 的一种具体应用 , 通过在 FTP 客户端和服务器之间建立面向连接的 , 可靠的 TCP 连接 , 用户可以访问一个运行有 FTP 服务器程序的远程计算机。

FTP Client 为用户提供在设备上通过 FTP 协议与远程 FTP 服务器进行文件传输的功能。用户通过客户端向服务器发出命令 , 服务器响应命令并把执行结果返回客户端 , 通过这种命令交互 , 用户可以察看服务器目录下的文件 , 并把文件从远程计算机上拷到本地 , 或把本地的文件传送到远程计算机去。

FTP 主要是作用是 : 促进程序/数据文件的共享 ; 鼓励 ( 通过程序 ) 使用远程计算机 ; 使用户不必面对不同主机上不同文件系统的差异 ; 对数据进行高效可靠的传输。适用于远程安全的文件传输。

锐捷 FTP Client 并不像标准 FTP 客户端一样实现交互式命令 , 其控制连接相关的 open、user、pass 指令由 CLI 输入 copy 命令自动完成 , 在控制连接建立完成后 , 则进入文件传输过程 , 建立数据连接 , 实现文件的上传或下载。

 用于原来的设备支持 TFTP, 但是 TFTP 是用于小文件传输, FTP 协议支持大文件传输, 在设备上实现文件传输协议 FTP, 使设备可以同其它客户机或服务器进行文件传输。

#### 协议规范

- RFC959 : FILE TRANSFER PROTOCOL (FTP)

### 8.2 典型应用

| 典型应用               | 场景描述                                  |
|--------------------|---------------------------------------|
| 从本地上传一个文件到远程服务上    | 本地与远程的文件需要共享 , 如需要从本地上传一个文件到远程服务上     |
| 从远程服务器中下载一个文件到本地设备 | 本地与远程的文件需要共享 , 如需要从远程服务器中下载一个文件到本地设备。 |

#### 8.2.1 从本地上传一个文件到远程服务上

##### 应用场景

本地与远程的文件需要共享 , 如需要从本地上传一个文件到远程服务上。

以下图为例 , 仅在 Intranet 提供共享资源作用。

图 8-1



## 功能部属

- 在 Intranet 中只实现通信。
- FTP Client 打开 FTP Client 文件上传功能。
- FTP Server 打开 FTP Server 文件上传功能。

## 8.2.2 从远程服务器中下载一个文件到本地设备

### 应用场景

本地与远程的文件需要共享，如需要从远程服务器中下载一个文件到本地设备。

以下图为例，仅在 Intranet 提供共享资源作用。

图 8-2



## 功能部属

- 在 Intranet 中只实现通信。
- FTP Client 打开 FTP Client 文件下载功能。
- FTP Server 打开 FTP Server 文件下载功能。

## 8.3 功能详解

### 基本概念

#### 📌 FTP 文件上传

从 FTP Client 上把文件上传到 FTP Server 上。

#### 📌 FTP 文件下载

把 FTP Server 上的文件下载到 FTP Client 上。

### FTP 连接模式

FTP Client 与 FTP Server 的连接方式，有主动连接和被动连接之分。

### FTP 传输模式

FTP Client 与 FTP Server 的之间的传输数据的方式，FTP 的传输有两种方式：文本（ASCII）传输模式和二进制（BINARY）数据传输模式。

### FTP 传输指定源接口 IP

FTP Client 可以对与服务端进行通信的客户端源 IP 地址进行绑定。

## 功能特性

| 功能特性           | 作用                                    |
|----------------|---------------------------------------|
| FTP 文件上传       | 从 FTP Client 上把文件上传到 FTP Server 上     |
| FTP 文件下载       | 将 FTP Server 上的文件下载到 FTP Client 上     |
| FTP 连接模式       | FTP Client 与 FTP Server 的连接方式         |
| FTP 传输模式       | FTP Client 与 FTP Server 的之间的传输数据的方式   |
| FTP 传输指定源接口 IP | FTP Client 可以对与服务端进行通信的客户端源 IP 地址进行绑定 |
| FTP 校验文件大小     | FTP Client 下载文件时，可指定不进行文件大小校验         |

### 8.3.1 FTP 文件上传

FTP 具有文件上传的功能。进行 FTP 文件上传文件需要 FTP Client 与 FTP Server 两个设备同时打开，从 FTP Client 上把文件上传到 FTP Server 上。

### 8.3.2 FTP 文件下载

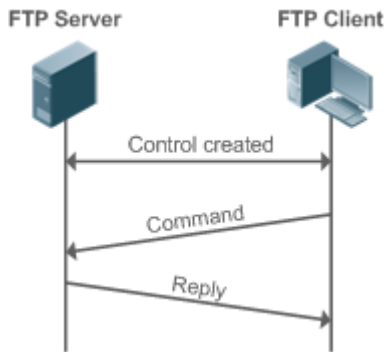
FTP 具有文件下载的功能。进行 FTP 文件下载文件需要 FTP Client 与 FTP Server 两个设备同时打开，把 FTP Server 上的文件下载到 FTP Client 上。

### 8.3.3 FTP 连接模式

FTP 协议要用到两个 TCP 连接，一个是控制链路（也称命令链路），用来在 FTP 客户端与服务器之间传递命令；另一个是数据链路，用来上传或下载数据。

1. 控制连接：对于一些比较简单的连接只需要建立控制连接，客户端向服务器发送命令，服务器接收到命令则进行命令响应，其过程如下：

图 8-3 控制连接



2. 控制连接与数据连接：当客户端发出的命令需要上传或下载数据时，这时不仅要建立控制连接还需要建立数据连接。

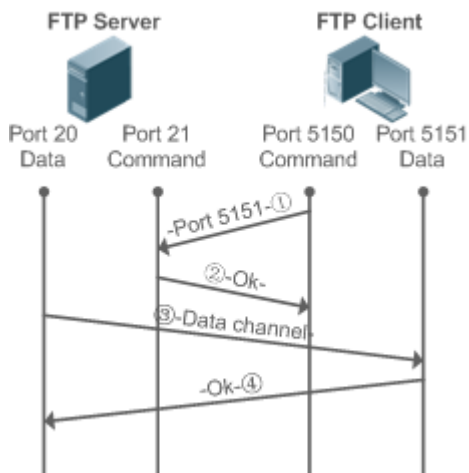
FTP 协议有两种数据连接方式：主动（PORT）方式和被动（PASV）方式。这两种工作模式主要区别在于数据连接建立方式不同，控制连接基本是一样的。

- 主动方式

该模式下 FTP server 在数据连接时是主动去连接 FTP client，所以被称为主动连接，其主要执行如下四个步骤：

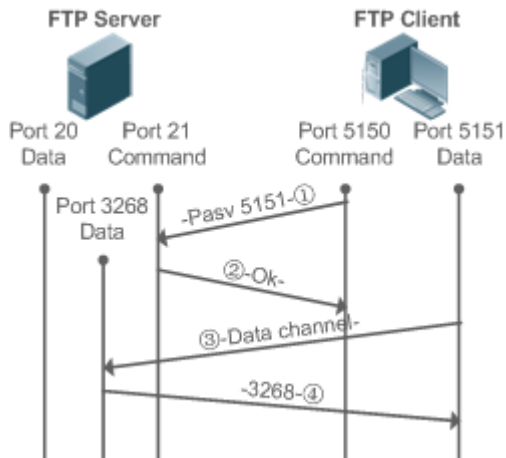
1. 客户端使用图例中的源端口 5150 与 server 端的 21 端口通信，请求建立连接，告诉服务器将用的端口是 5151。
2. server 收到后，发送应答信息，OK(ACK)，client and server 通过控制端口交换控制信令。
3. 服务器打开 20 端口作为数据发送的源端口，向客户端的 5151 端口发送。
4. 客户端应答，传输过程结束。

图 8-4 PORT（主动）模式



- 被动方式

图 8-5 PASV（被动）模式



该模式一般通过 `passive` 命令进行设置，由于 FTP server 在数据连接时是被动连接 FTP Client，所以称为被动连接，其主要执行如下四个步骤：

1. 被动模式下，客户端初始化控制信令连接，使用图例中 5150 源端口与服务器的 21 端口建立连接，并使用 `passive` 命令请求进入被动模式。
2. 服务器同意进入 PASV 模式，并随机选择一个大于 1024 的端口号，告知客户端。
3. 客户端接收到此信息后，使用图例中的 5151 端口与刚才服务器提供的 3268 端口进行数据通信，这里 5151 是源端口，3268 是目的端口。
4. 服务器收到信息，回传数据并发送应答 ACK (OK)。

当客户端和服务器建立数据连接后，就可以进行 FTP 最基本的上传和下载功能，并且在客户端可以对服务器进行一些相关文件操作。

**i** 用于传输命令和反馈信息的传输的控制连接始终存在，而数据连接只在需要的时候建立；PASV 和 PORT 模式的设置选择权仅在 FTP Client，由 FTP Client 发出命令建立不同的数据连接模式，我司 FTP Client 默认方式为被动模式

### 8.3.4 FTP 传输模式

FTP 的传输有两种方式：文本 (ASCII) 传输模式和二进制 (BINARY) 数据传输模式。我司产品 FTP Client 目前支持 ASCII 和 BINARY 两种传输模式，默认情况下为 BINARY 传输模式。

#### ● 文本模式

ASCII 模式和 BINARY 模式的区别是回车换行的处理，ASCII 模式将回车换行转换为本机的回车字符，比如 Unix 下是 `\n`，Windows 下是 `\r\n`，Mac 下是 `\r`。

#### ● 二进制模式

BINARY 模式可用来传送可执行文件，压缩文件和图片文件，不对数据进行任何处理。以 Unix 传送文本文件到 Windows 为例，使用 BINARY 模式时，不会对 Unix 下的换行符进行从 `\r` 到 `\r\n` 的转换，因此在 windows 上看这个文件是没有换行的，里面是一个个的黑方块。由于不进行回车换行的处理，因此 BINARY 模式比文本模式更快，可以传输所有 ASCII 值，保证不出错。





### 8.3.5 FTP 传输指定源接口 IP

FTP Client 可以对与服务端进行通信的客户端源 IP 地址进行绑定，这样可以用指定的源 IP 与 FTP Server 进行连接和传输文件。

### 8.3.6 FTP 传输不校验文件大小

FTP Client 可以配置为下载文件时，不校验文件大小。通过不对文件大小校验，可以从不支持应答文件大小的 ftp 服务器下载文件。

## 8.4 配置详解

| 配置项                | 配置建议 & 相关命令                                                                                                   |                                                    |
|--------------------|---------------------------------------------------------------------------------------------------------------|----------------------------------------------------|
| 配置 FTP Client 基本功能 |  必须配置。配置 FTP CLEINT 功能       |                                                    |
|                    | copy flash                                                                                                    | 文件上传                                               |
|                    | copy ftp                                                                                                      | 文件下载                                               |
| 配置 FTP Client 可选功能 |  可选配置。配置 FTP CLEINT 功能的工作模式 |                                                    |
|                    | ftp-client port                                                                                               | 设置 FTP 为主动连接模式                                     |
|                    | ftp-client ascii                                                                                              | 设置 FTP 为文本传输模式                                     |
|                    | ftp-client source                                                                                             | 配置进行 FTP 连接的客户端源 IP 地址                             |
|                    | default ftp-client                                                                                            | 恢复 FTP Client 为缺省配置，数据连接为被动方式，文件传输为二进制模式，清除源 IP 绑定 |
|                    | ftp-client disable-size-check                                                                                 | 配置下载文件时，不校验文件大小                                    |

#### 8.4.1 配置 FTP Client 基本功能

##### 配置效果

- 实现文件上传与下载。

##### 注意事项

- 文件上传与下载的格式。

##### 配置方法

## 文件上传

- 需要实现文件上传时，为必选配置。
- 在特权模式下的 copy 下的目的地址上配置 ftp 相关的 url。

## 文件下载。

- 需要实现文件下载时，为必选配置。
- 在特权模式下的 copy 下的源地址上配置 ftp 相关的 url。

## 检验方法

- 在 FTP Server 的目录中看所上传的文件是否存在。
- 在目的地址上查看下载的文件是否存在。

## 相关命令

### 文件上传

【命令格式】 **copy flash:[ local-directory/]/local-file ftp:**

**//username:password@dest-address[ /remote-directory ]/remote-file**

【参数说明】 *local-directory* : 指定设备目录，如果未指定，则表示当前工作目录。

*local-file* : 表示要操作的本地文件名


*username* : 指定访问 FTP Server 的用户名，最长不超过三十二个字节，不可包含 “:”、“/” 和空格等字符，不可省略。

*Password* : 指定访问 FTP Server 的密码，最长不超过三十二个字节，不可包含 “:”、“/” 和空格等字符，不可省略。

*dest-address* : 指定 FTP Server 的 IP 地址

*remote-directory* : 指定 Server 端的目录路径

*remote-file* : 指定要操作的 Server 端文件名

 如果包含 *local-directory* 字段，则必须保证设备中已创建了该目录，此下载命令不支持目录的自动创建。

【命令模式】 全局模式

【使用指导】 使用该命令从本地设备的 flash 上上传一个文件到 FTP SERVER 上去。

### 文件下载

【命令格式】 **copy ftp://username:password@dest-address[ /remote-directory ]/remote-file**

**flash:[ local-directory/]/local-file**

【参数说明】 *username* : 指定访问 FTP Server 的用户名，最长不超过三十二个字节，不可包含 “:”、“/” 和空格等字符，不可省略。

*password* : 指定访问 FTP Server 的密码，最长不超过三十二个字节，不可包含 “:”、“/” 和空格等字符，不可省略。


*dest-address* : 指定 FTP Server 的 IP 地址。

*remote-directory* : 指定 Server 端的目录路径。

*remote-file* : 指定要操作的 Server 端文件名。

*local-directory* : 指定设备目录, 如果未指定, 则表示当前工作目录。

*local-file* : 表示要操作的本地文件名。

 如果包含 *local-directory* 字段, 则必须保证设备中已创建了该目录, 此下载命令不支持目录的自动创建。

【命令模式】 全局模式

【使用指导】 使用该命令从 FTP SERVER 下载一个文件到本地设备的 flash 上去。

## 配置举例

 以下配置举例, 仅介绍与 FTP Client 上传下载相关的配置。

### 📁 上传文件示例

【配置方法】 将设备 home 目录中的 local-file 文件上传到用户名为 user, 密码为 pass, IP 地址为 192.168.23.69 的 FTP Server 的 root 目录下, 文件命名为 remote-file。

```
Ruijie# copy flash: home/local-file ftp://user:pass@192.168.23.69/root/remote-file
```

【检验方法】 在 FTP SERVER 上查看 remote-file 是否存在。

### 📁 下载文件示例

【配置方法】 从用户名为 user, 密码为 pass, IP 地址为 192.168.23.69 的 FTP Server 的 root 目录下载文件名为 remote-file 的文件到设备上的 home 目录中, 存储的文件名为 local-file

```
Ruijie# copy ftp://user:pass@192.168.23.69/root/remote-file flash: home/local-file
```

【检验方法】 在 flash 的 home 目录下查看 remote-file 是否存在。

## 常见配置错误

- 上传下载输入的格式错误。
- 用户名或密码错误。

## 8.4.2 配置 FTP Client 可选功能

### 配置效果

- 根据配置能让 FTP 工作在指定连接、传输模式及指定的 IP 地址下进行文件上传与下载。

## 注意事项

- FTP Client 在配置时如果需要指定的 vrf-name 进行配置时，首先必须先进行 vrf-name 的相关配置。

## 配置方法

### 设置 FTP 为主动连接方式。

- 可选配置。
- 配置 FTP 的连接模式。

### 设置 FTP 为文本传输模式。

- 可选配置。
- 配置 FTP 的传输模式。

### 设置进行 FTP 连接的客户端源 IP 地址。

- 可选配置。
- 配置进行 FTP 连接的客户端源 IP 地址。

### 恢复 FTP Client 为缺省配置。

- 可选配置。
- 恢复 FTP Client 为缺省配置。

## 检验方法

通过 **show run** 查看

## 相关命令

### 配置 FTP 为主动连接模式

【命令格式】 **ftp-client [ vrf vrf-name ] port**

【参数说明】 **vrf vrf-name**：指定 VRF。

【命令模式】 全局配置模式

【使用指导】 使用该命令可以将连接模式设置为主动方式，主动方式下，服务器主动去连接客户端。默认情况下 FTP 连接为被动（PASV）方式。

### 配置进行 FTP 连接的客户端源 IP 地址

【命令格式】 **ftp-client [ vrf vrfname ] source {ip-address | ipv6-address | interface}**

【参数说明】 **vrf vrf-name**：指定 VRF。

*ip-address* : 本地接口的 ipv4 地址。

*ipv6-address* : 本地接口的 ipv6 地址。

【命令模式】 全局配置模式

【使用指导】 使用该命令可以绑定客户端不同的接口 IP 地址，使客户端使用此 IP 地址连接服务器。默认情况下客户端不进行本地 IP 绑定，由路由进行选择。

## 📌 设置 FTP 为文本传输模式

【命令格式】 **ftp-client [ vrf vrf-name ] ascii**

【参数说明】 **vrf vrf-name** : 指定 VRF。

【命令模式】 全局配置模式

【使用指导】 使用该命令可以将文件传输方式设置为文本（ASCII）方式。默认情况下 FTP 传输模式为二进制（BINARY）方式。

## 📌 恢复 FTP Client 为缺省配置

【命令格式】 **default ftp-client [ vrf vrf-name ]**

【参数说明】 **vrf vrf-name** : 指定 VRF。

【命令模式】 全局配置模式

【使用指导】 恢复 FTP Client 为缺省配置，数据连接为被动方式，文件传输为二进制模式，清除源 IP 绑定。

## 📌 设置 FTP 不校验文件大小

【命令格式】 **ftp-client disable-size-check**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 配置下载文件时，不校验文件大小。默认校验文件大小。

## 配置举例

 以下配置举例，仅介绍与 FTP Client 可选择项相关的配置。

## 📌 可选项配置

- 【配置方法】
- 配置 FTP 连接模式为：port
  - 配置传输模式为：ASCII
  - 配置源 IP 为 192.168.23.167
  - 配置 vrf 123 的连接模式为：port
  - 配置 vrf 123 的传输模式为：ASCII

```
Ruijie# configure terminal
Ruijie(config)# ftp-client ascii
Ruijie(config)# ftp-client port
Ruijie(config)# ftp-client source 192.168.23.167
Ruijie(config)# ftp-client vrf 123 port
Ruijie(config)# ftp-client vrf 123 ascii
```

```
Ruijie(config)# end
```

【检验方法】 在设备上进行 **show run**，能看到以下信息

```
Ruijie# show run

!
ftp-client ascii
ftp-client port
ftp-client source 192.168.23.167
!
```

### 常见配置错误

- 源 IP 不是本地 IP。
- 配置 **ftp-client vrf** 之前，先要配置好 **vrf**。

## 8.5 监视与维护


### 清除各类信息

无

### 查看配置情况

| 作用                | 命令              |
|-------------------|-----------------|
| 查看 FTP Client 的配置 | <b>show run</b> |

### 查看调试信息

 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

| 作用                  | 命令                      |
|---------------------|-------------------------|
| 打开 FTP Client 调试开关。 | <b>debug ftp-client</b> |

## 9 TFTP-Server

### 9.1 概述

TFTP Server 功能可以将一台设备配置为 TFTP 服务器。这样可以通过 TFTP 客户端与之连接，通过 TFTP 协议往设备上传或下载文件。

用户可以利用 TFTP Server 功能方便地获取设备中的文件，如升级包文件等；也可以通过 TFTP Server 直接往设备的文件系统拷贝文件。

 下文仅介绍 TFTP Server 的相关内容。

#### 协议规范

- RFC1350: The TFTP Protocol (revision 2)
- RFC2347: TFTP Option Extension
- RFC2348: TFTP Blocksize Option
- RFC2349: TFTP Timeout Interval and Transfer Size Options

### 9.2 典型应用

| 典型应用                  | 场景描述                |
|-----------------------|---------------------|
| 局域网内提供 TFTP Server 服务 | 在一个局域网内为用户提供上传与下载服务 |

#### 9.2.1 局域网内提供 TFTP Server 服务

##### 应用场景

在一个局域网内为用户提供上传与下载服务

以下图为例

- G 开启 TFTP-server 服务
- User 发起 TFTP 上传与下载请求

图 9-1



【注释】 G 为运行 TFTP SERVER 的网络设备。

## 功能部属

---

- G 设备启动 TFTP Server
- User 通过 TFTP Client 上传或下载文件

## 9.3 功能详解

### 基本概念

---

#### 📌 TFTP 协议

TFTP ( Trivial File Transfer Protocol, 简单文件传输协议 ) 是 IETF Network Working Group 所制定的一套标准协议, 属于网络协议族的应用层, TFTP 基于 UDP ( User Datagram Protocol ) 传输控制协议, 提供不复杂、开销不大的文件传输服务。TFTP 不具备许多通常的 FTP 功能, 只能上传或下载文件, 不能列出目录, 不能认证, 没有安全机制。TFTP 使用超时重传确认的方式确保数据的传输, 具有三种传输模式: 8 位 ASCII 码形式的 netascii, 8 位源数据类型的 octet 和 mail 模式 ( 已不再支持 )。TFTP 使用的 UDP 端口号为 69。在 RFC1350 中对 TFTP 协议进行了描述。

#### 📌 TFTP 报文

在 TFTP 客户端发起读取或者写入文件请求, TFTP 服务端批准请求后, TFTP 就以固定大小 ( 512 字节 ) 的数据报文来传输数据。如果数据报文小于 512 字节, 则表明传输结束。

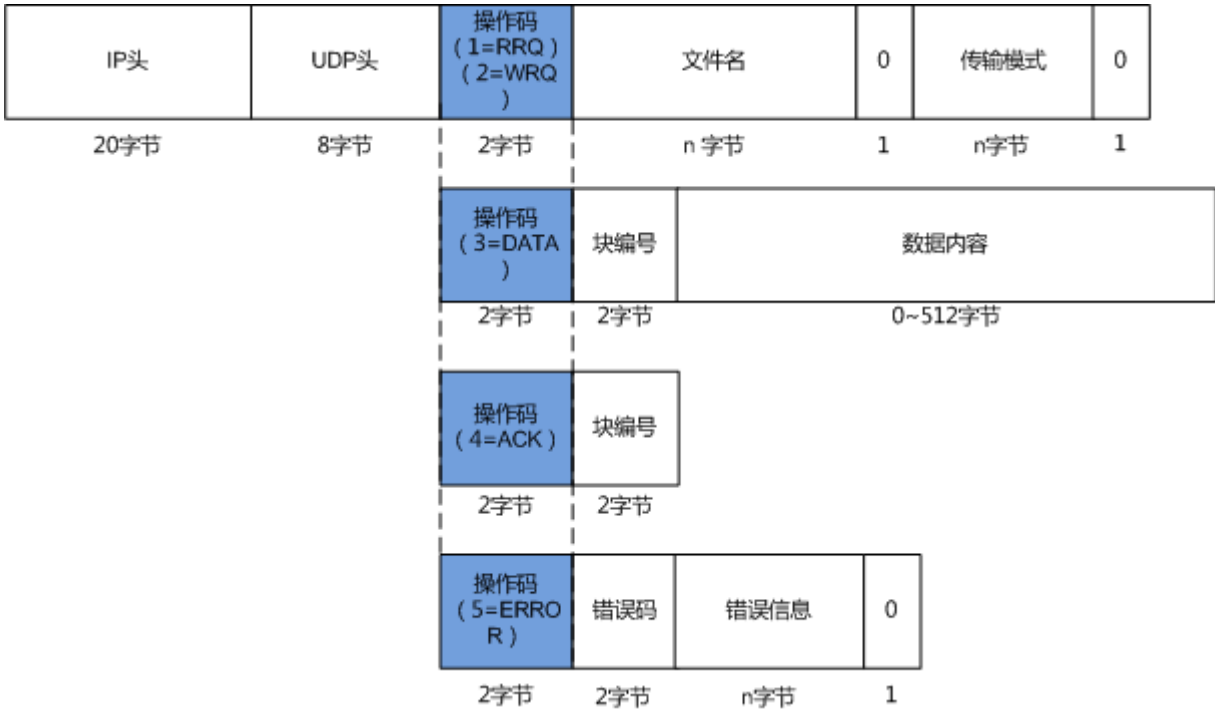
每个数据报文包含一块数据, 并且必须在收到对端的确认报文后才可以继续发送下一个数据报文。如果在规定时间内没有收到确认报文, 需要重传最后发送的一个数据报文。

TFTP 报文头部包含一个操作码 ( opcode ) 字段, 表明报文类型, 共有五类报文:

- 读请求报文 ( Read Request, RRQ )
- 写请求报文 ( Write Request, WRQ )
- 数据报文 ( Data, DATA )
- 确认报文 ( Acknowledgment, ACK )
- 错误报文 ( Error, ERROR )

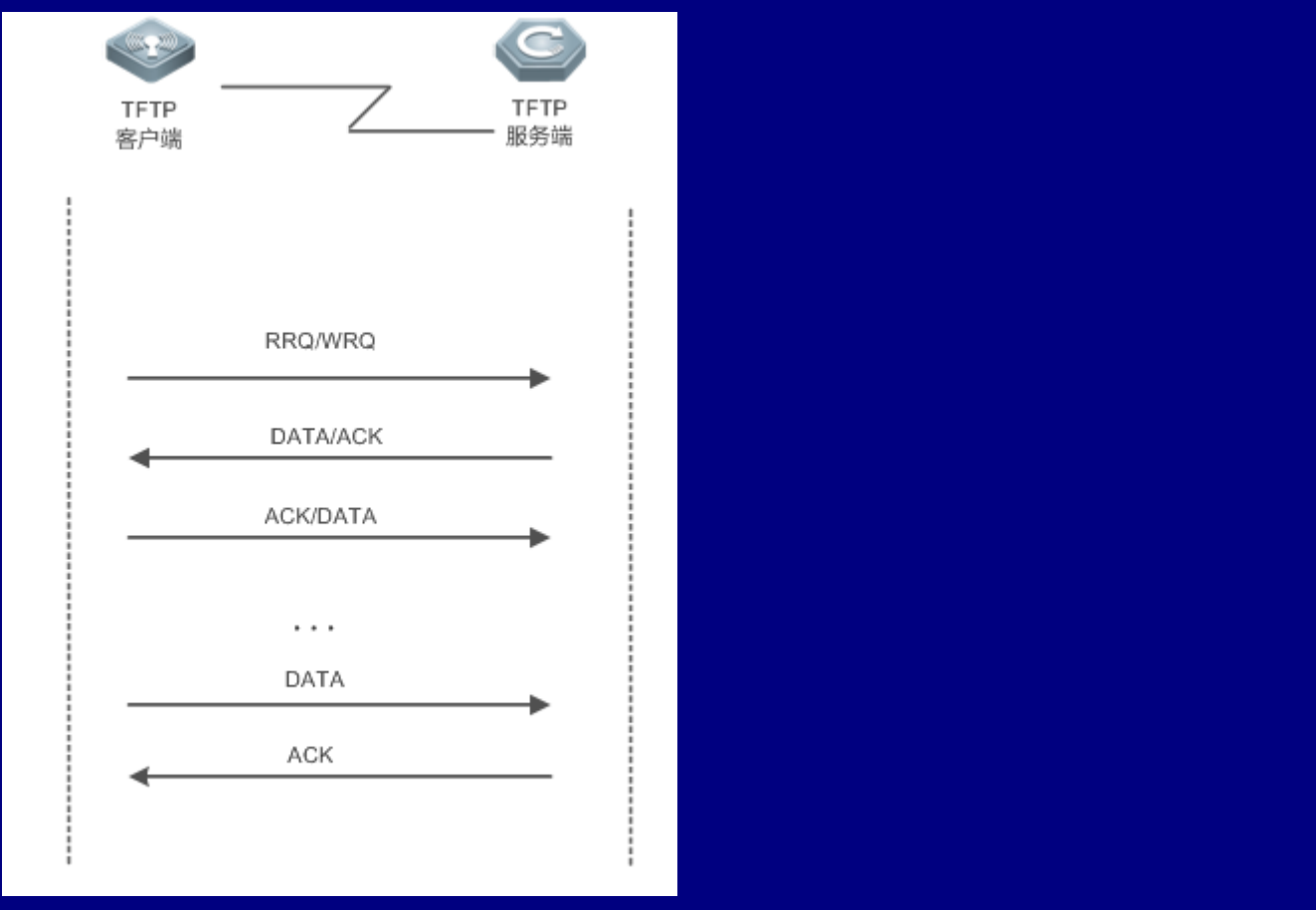
图 9-2





📄 TFTP 工作方式

图 9-3



- TFTP 客户端向 TFTP 服务端发起读请求（RRQ）或者写请求（WRQ）。
- TFTP 服务端收到读请求时，先判断读取条件是否满足（文件是否存在，是否有访问权限等），如果满足则发送数据报文（DATA）给 TFTP 客户端；TFTP 服务端收到写请求时，先判断写入条件是否满足（是否足够空间，是否有写入权限等），如果满足，则发送 ACK 报文给 TFTP 客户端。
- TFTP 客户端在准备下载文件时，收到 DATA 报文，则回复 ACK 报文；在准备上传文件时，收到 ACK 报文，则继续发送 DATA 报文。
- 重复发送确认的流程，直到最后一个长度小于 512 的 DATA 报文，表明传输的结束。
- 在传输过程中，如果遇到错误，则发送错误（ERROR）报文给对端。

功能特性

| 功能特性              | 作用                        |
|-------------------|---------------------------|
| 开启 TFTP-Server 服务 | 为 TFTP-Client 提供上传、下载文件功能 |

9.3.1 开启 TFTP-Server 服务

工作原理

基本工作原理如上一章所述，设备开启 TFTP server 服务后，配置顶层目录即可为用户提供 FTP 服务。

相关配置

使能 TFTP-Server

- 缺省情况下，不开启 TFTP Server
- 使用 **tftp-server enable** 开启
- 必须开启 TFTP 服务器功能，否则无法使用

配置顶层目录

- 缺省情况下，无配置顶层目录
- 使用 **tftp-server topdir** 来设置顶层目录
- 必须配置顶层目录，否则无法提供上传和下载

9.4 配置详解

| 配置项                 | 配置建议&相关命令                                                                                               |                 |
|---------------------|---------------------------------------------------------------------------------------------------------|-----------------|
| 配置 TFTP-SERVER 基本功能 |  必须配置，用于启动 TFTP 服务器。 |                 |
|                     | <b>tftp-server enable</b>                                                                               | 启动 TFTP 服务器功能   |
|                     | <b>tftp-server topdir</b>                                                                               | 配置 TFTP 服务器顶层目录 |

9.4.1 配置 TFTP-Server 基本功能

配置效果

- 建立 TFTP-Server，向 TFTP-Client 提供上传和下载服务

注意事项

- 需要配置顶层访问目录

配置方法

启动 TFTP-SERVER 功能

- 必须配置
- 若无特殊要求，应在每台设备上启动 TFTP-Server 功能

## 配置顶层目录

- 必须配置
- 若无特殊要求，应在每台设备上配置顶层目录为根目录

## 检验方法

利用 TFTP 客户端与服务器进行连接

- 检查客户端是否能连接成功
- 检查客户端下载和上传是否正常

## 相关命令

### 启动 TFTP-SERVER 功能

- 【命令格式】 **tftp-server enable**
- 【参数说明】 -
- 【命令模式】 全局模式
- 【使用指导】 在正确配置服务器的顶层目录之前客户端仍然无法访问 TFTP 服务器,因此建议在首次启动服务之前先参考后面的章节完成服务器顶层目录的配置

### 配置服务器顶层目录

- 【命令格式】 **tftp-server topdir *directory***
- 【参数说明】 *directory* : 指定用户访问路径
- 【命令模式】 全局模式
- 【使用指导】 如可以指定服务器的顶层目录为 “/dir” 目录,则 TFTP 客户端登录后将仅能访问设备上 “/dir” 目录下的文件和文件夹,客户端由于顶层目录的限制将无法退到 “/dir” 目录的上级目录中

### 打开服务器的调试信息

- 【命令格式】 **debug tftp-server**
- 【参数说明】 -
- 【命令模式】 特权模式
- 【使用指导】 打开 TFTP 服务器的过程/错误调试信息输出

## 配置举例

### 在 IPv4 网络上建立 TFTP-SERVER 服务

- 【配置方法】
- 开启 TFTP-SERVER 服务
  - 配置顶层目录/dir

```
Ruijie(config)#tftp-server topdir /dir
```

```
Ruijie(config)#tftp-server enable
```

【检验方法】      ●    通过 **show run** 查看配置结果

```
Ruijie#show run
...
tftp-server enable
tftp-server topdir /dir
...
```

常见错误

- 未配置顶层目录

9.5    监视与维护


清除各类信息

-

查看运行情况

-

查看调试信息

 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

| 作用                | 命令                       |
|-------------------|--------------------------|
| 打开 TFTP 服务器的调试开关。 | <b>debug tftp-server</b> |

## 10 TUNNEL

### 10.1 概述

Tunnel 接口用于实现隧道功能，是系统虚拟的接口。Tunnel 接口并不特别指定传输协议或者负载协议，它提供的是一个用来实现标准的传输链路。每一个 Tunnel 接口代表一个传输链路。

Tunnel 功能实现包括下面三个主要组成部分：

- 负载协议：通过 Tunnel 传输的负载(网络数据)的封装协议。如 IPv4 和 IPv6 协议作为负载协议，对于 GRE 隧道，可以不是 IPv4 或者 IPv6 协议；
- 载体协议：用来二次封装并辨识待传输负载的协议。在本文描述的 TUNNEL 中，只有 GRE 隧道有载体协议，即 GRE 协议（也即封装协议）。其他类型的隧道都是 IPv4/IPv6 外面直接封装 IPv4/IPv6；
- 传输协议：实际传输经过载体协议二次封装后的负载的网络协议。锐捷产品使用最广泛应用的 IPv4 和 IPv6 协议作为传输协议。

实际上，如果两个私有同种协议网络需要通过异种公有网络实现互通讯，就可以采用 Tunnel 模式实现。


Tunnel 传输适用于以下情况：

- 允许运行非 IP 协议的本地网络之间通过一个单一网络（IP 网络）通讯，因为 Tunnel 支持多种不同的负载协议；允许那些对路由跳数有限制的协议可以在更广泛的范围内工作，因为 Tunnel 使用的是传输协议（IP）的路由工作；
- 允许通过单一的网络（IP 网络）连接间断子网；
- 允许在广域网上提供 VPN（Virtual Private Network，虚拟专用网络）功能。

由于 Tunnel 将负载封装后传输，这会带来处理上的复杂性，在某些情况下需要注意以下的变化。

- 由于 Tunnel 是逻辑链路，在路由的时候看起来只有一跳（hop），可实际上可能其路由花费不止一跳。在使用 Tunnel 的时候必须注意到 Tunnel 链路的路由与实际路由并不一致。
- 由于 Tunnel 传输将负载封装在传输协议中，在设置防火墙特别是访问控制链表(ACL)的时候，这一点需要考虑；同时必须注意到此时负载协议的传输带宽等(如 MTU)也比理论值更小。

---

 下文仅介绍 Tunnel 的相关内容。

---

### 协议规范

- RFC2784：Generic Routing Encapsulation (GRE)
- RFC2890：Key and Sequence Number Extensions to GRE
- RFC3056：Connection of IPv6 Domains via IPv4 Clouds
- RFC3068：An Anycast Prefix for 6to4 Relay Routers

- RFC3964 : Security Considerations for 6to4
- RFC4023 : Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)
- RFC4087 : IP Tunnel MIB
- RFC4213 : Basic Transition Mechanisms for IPv6 Hosts and Routers
- RFC4797 : Use of Provider Edge to Provider Edge (PE-PE) Generic Routing Encapsulation (GRE) or IP in BGP/MPLS IP Virtual Private Networks
- RFC5158 : 6to4 Reverse DNS Delegation Specification
- RFC5214 : Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
- RFC5332 : MPLS Multicast Encapsulations
- RFC5579 : Transmission of IPv4 Packets over Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) Interfaces
- RFC5845 : Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6
- RFC5969 : IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification
- RFC6245 : Generic Routing Encapsulation (GRE) Key Extension for Mobile IPv4
- RFC6343 : Advisory Guidelines for 6to4 Deployment
- RFC6372 : 6to4 Provider Managed Tunnels
- RFC6654 : Gateway-Initiated IPv6 Rapid Deployment on IPv4 Infrastructures (GI 6rd)
- draft-zhou-dhc-gre-option-00 DHCPv4 and DHCPv6 options for GRE
- draft-cai-softwire-6rd-mib-03 Definitions of Managed Objects for 6rd
- draft-howard-isp-ip6rdns-05 Reverse DNS in IPv6 for Internet Service Providers
- draft-tsou-softwire-6rd-multicast-02 IPv6 Multicast Using Native IPv4 Capabilities in a 6rd Deployment
- draft-templin-v6ops-isops-18 Operational Guidance for IPv6 Deployment in IPv4 Sites using ISATAP

## 10.2 典型应用

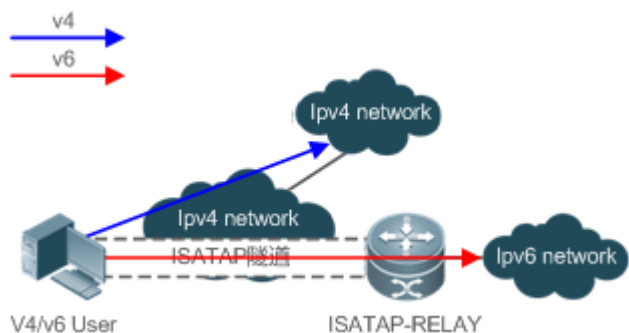
| 典型应用             | 场景描述              |
|------------------|-------------------|
| 访问园区网内部的 IPv6 站点 | 访问园区网内部的 IPv6 站点。 |
| 园区网接入 IPv6 骨干网   | 园区网接入 IPv6 骨干网。   |

### 10.2.1 访问园区网内部的 IPv6 站点

#### 应用场景

一些园区网有部署 IPv6 服务器，PC 需要能访问这些服务器。可以利用 ISATAP 自动隧道实现这种应用。

图 10-1



【注释】 ISATAP-RELAY 为支持 tunnel 的设备，园区网用户访问 IPv4 的服务器时，直接通过 IPv4 网络访问；访问 IPv6 的服务器时，需通过 ISATAP 隧道访问

## 功能部属

- V4/V6 用户通过 V4 地址访问 IPv4 网络。
- V4/V6 用户通过 ISATAP 隧道访问 IPv6 网络。
- ISATAP 隧道在 PC 和 ISATAP-RELAY 路由器建建立 ISATAP 隧道。

## 10.2.2 园区网接入 IPv6 骨干网

### 应用场景

将旧的园区网升级成支持 IPv6，或者新建一个支持 IPv6 的园区网。可以使用 6to4 自动隧道实现。

## 10.3 功能详解

### 基本概念

#### 隧道 MTU

- 隧道接口的 MTU (Maximum Transmission Unit, 最大传输单元) 一般低于普通接口，如普通的 IPv4 over IPv4 的隧道，假定在以太网上传输，那么除去 2 层 IP 头部，每个报文实际能传输的最大数据量是 1460 字节。所以隧道接口的 MTU 为 1480 字节，而不是标准以太网接口的 1500 字节。

#### 隧道路径 MTU



- 隧道接口实际上代表了一个虚拟的链路。以 IPv4 over IPv4 隧道为例。这个隧道接口的 MTU 实际上是隧道链路的 MTU，即隧道本端和对端之间的路径 MTU。当本端和对端之间的路由路径发生变化后，则路径 MTU 可能会发生变化，从而影响隧道接口的 MTU

#### 隧道嵌套层数

- 隧道可以嵌套。以 IPv4 over IPv4 隧道为例。可以将原始的 IPv4 报文再封装 2 层 IPv4 首部或者更多层次的 IPv4 首部以后再发送出去。需要隧道嵌套的场景一般不多见，主要是为了更安全的缘故。隧道嵌套后，可以传输的数据更少了。一个隧道接口的对端地址经过 FIB 选路后，如果出口是另一个隧道接口，则会发生隧道嵌套封装；如果选路后出口又是本隧道，那么会出现无穷嵌套（锐捷产品能检测出这种情况，并给出提示）。

### 功能特性

| 功能特性       | 作用                                     |
|------------|----------------------------------------|
| 隧道嵌套封装层数限制 | 根据实际需要调大隧道嵌套封装层数限制（很少使用）。              |
| 隧道数据有效性校验  | 对 GRE 隧道传输的数据增加校验和，用于检查数据传输过程中的是否发生错误。 |

## 10.4 配置详解

| 配置项          | 配置建议 & 相关命令                                                                                            |              |
|--------------|--------------------------------------------------------------------------------------------------------|--------------|
| 配置隧道接口基本功能   |  必须配置。用于建立隧道。       |              |
|              | <b>Interface tunnel</b>                                                                                | 新建一个隧道接口     |
|              | <b>tunnel source</b>                                                                                   | 设置隧道的本端地址    |
| 配置隧道模式       |  可选配置，用于设置隧道模式      |              |
|              | <b>tunnel mode</b>                                                                                     | 配置隧道封装模式     |
| 配置隧道对端地址     |  可选配置，用于设置隧道对端地址    |              |
|              | <b>tunnel destination</b>                                                                              | 配置隧道对端地址     |
| 配置隧道传输网络 TOS |  可选配置，用于设置传输网络的 TOS |              |
|              | <b>tunnel tos</b>                                                                                      | 配置隧道传输网络 TOS |
| 配置隧道传输网络 TTL |  可选配置，用于设置传输网络的 TTL |              |
|              | <b>tunnel ttl</b>                                                                                      | 配置传输网络的 TTL  |

### 10.4.1 配置隧道接口

#### 配置效果

- 新建一个隧道接口。

## 注意事项

---

无

## 配置方法

---

### 📄 新建隧道接口功能

- 在全局配置模式下，使用 **interface tunnel number** 新建隧道接口。
- 只有创建了隧道接口，才能使用隧道服务。

## 检验方法

---

- 使用 **show interfaces tunnel number** 观察是否成功配置。

## 相关命令

---

### 📄 配置隧道接口

- 【命令格式】 **interface tunnel number**
- 【参数说明】 *number*：隧道接口编号。
- 【命令模式】 全局模式
- 【使用指导】 -

### 📄 检查隧道配置

- 【命令格式】 **show interfaces tunnel number**
- 【参数说明】 *number*：隧道接口编号。
- 【命令模式】 全局模式
- 【使用指导】 -

## 配置举例

---

### 📄 新建一个隧道接口

- 【配置方法】
  - 新建一个隧道接口

```
Ruijie# configure terminal
Ruijie(config)# interface tunnel 1
Ruijie(config-if-Tunnel 1)# end
```

**【检验方法】**

- 检查隧道接口的配置

```
Ruijie# show interfaces tunnel 1
.....

Tunnel attributes:
.....

Tunnel protocol/transport is gre ip
```

## 常见错误

- 内存不足导致隧道接口创建失败。
- 硬件芯片资源不足导致隧道接口创建失败。

## 10.4.2 配置隧道封装模式

### 配置效果

- 需要使用非缺省封装模式的隧道时
- 在隧道接口模式下配置

### 注意事项

无

### 配置方法

#### 📌 设置隧道的封装模式

- 可选配置
- 交换机，无线产品的缺省封装模式是 tunnel mode ipv6ip。
- 路由器，网关产品缺省封装模式是 tunnel mode gre ip。
- 在隧道接口模式下，通过 tunnel mode 命令可以修改成其他模式。

### 检验方法

- 使用 **show interfaces tunnel number** 观察是否成功配置。

### 相关命令

## 配置隧道封装模式

【命令格式】 **tunnel mode { gre {ip | ipv6} | ipv6 | ipip | ipv6ip [ 6to4 | isatap ] }**

【参数说明】 每一种 mode 代表从此隧道接口发出的报文的封装格式

gre ip 表示，先经过一个 GRE 头部封装，再经过 IPv4 封装，然后在新的 IPv4 网络发送

gre ipv6 表示，先经过一个 GRE 头部封装，再经过 IPv6 封装，然后在新的 IPv6 网络发送

ipv6 表示，从此接口发出的报文直接经过 IPv6 封装后，在新的 IPv6 网络发送

ipip 表示，此接口只能承载 IPv4 报文，并且此报文再经过 IPv4 封装后，在新的 IPv4 网络发送

ipv6ip 表示，此接口只能承载 IPv6 报文，并且报文经过 IPv4 封装后，在新的 IPv4 网络中发送

上述隧道都是手工隧道，而 ipv6ip 6to4/isatap 是自动隧道，报文封装过程中，目标 IPv4 地址是通过目标 IPv6 地址映射而成。

【命令模式】 接口模式

【使用指导】 隧道的 2 端一般情况下需要配置相同的模式，否则不能正常工作。

## 配置举例

### 配置隧道的封装模式为 IPv4 over IPv4。

- 【配置方法】
- 配置隧道接口的封装模式为 IPv4 over IPv4。

```
Ruijie# configure terminal
Ruijie(config)# interface tunnel 1
Ruijie(config-if-Tunnel 1)# tunnel mode ipip
Ruijie(config)# end
```

- 【检验方法】
- 检查隧道接口的配置

```
Ruijie# show interfaces tunnel 1
.....
Tunnel attributes:
.....
Tunnel protocol/transport is ipv6ip
```

## 常见错误

- 相同 vrf 已经有一个 6to4 或者 isatap 隧道，继续配置这 2 种隧道。

## 10.4.3 配置隧道本端地址

### 配置效果

- 设置隧道的本端地址。

## 注意事项

- 隧道的本端地址必须同隧道的传输协议匹配。否则隧道口不会 UP(被禁用)。
- 当通过指定另外一个接口间接指定本端地址时，指的是 IPv4 主地址或者 IPv6 第一个全球公网地址。

## 配置方法

### 设置隧道的本端地址

- 必须配置
- 在隧道接口模式下使用 **tunnel source** 命令指定隧道的本端地址。

## 检验方法

- 通过 **show interfaces tunnel number** 命令可以观察隧道的本端地址

## 相关命令

### 配置隧道本端地址

- 【命令格式】 **tunnel source** { *ip-address* | *interface-name interface-number* }
- 【参数说明】 **ip-address**：可以是 IPv4 地址，也可以是 IPv6 地址。  
*Interface-name interface-number*：可以是各种 3 层接口。
- 【命令模式】 接口模式
- 【使用指导】 如果直接指定 IPv4 或者 IPv6 地址，则需要设置成设备自身的地址

## 配置举例

### 配置隧道的本端地址。

- 【配置方法】
- 配置隧道的本端地址为 1.1.1.1

```
Ruijie# configure terminal
Ruijie(config)# interface tunnel 1
Ruijie(config-if-Tunnel 1)# tunnel mode ipv6ip
Ruijie(config-if-Tunnel 1)# tunnel source 1.1.1.1
```

- 【检验方法】
- 检查隧道接口的配置。

```
Ruijie# show interfaces tunnel 1
.....
Tunnel attributes:
```

**【配置方法】**

- 配置隧道的本端地址为 1.1.1.1

```
Ruijie# configure terminal
Ruijie(config)# interface tunnel 1
Ruijie(config-if-Tunnel 1)# tunnel mode ipv6ip
Ruijie(config-if-Tunnel 1)# tunnel source 1.1.1.1
```

**【检验方法】**

- 检查隧道接口的配置。

```
Tunnel source 1.1.1.1, destination UNKNOWN, unroutable
Tunnel TOS/Traffic Class not set, Tunnel TTL 254
Tunnel config nested limit is 0, current nested number is 0
Tunnel protocol/transport ipv6ip
    Tunnel transport VPN is no set
.....
```

## 常见配置错误

---

无

## 10.4.4 配置隧道对端地址

### 配置效果

---

- 手工隧道，必须配置对端地址后，才能使用（接口才会 UP）。

### 注意事项

---

- 自动隧道不能配置对端地址。

### 配置方法

---

#### 📌 配置隧道对端地址

- 6to4, isatap 隧道不能配置，其他隧道必须配置
- 在接口模式下通过 **tunnel destination** 命令配置对端地址。

### 检验方法

---

- **show interfaces tunnel** 命令可以查看是否配置成功。

## 相关命令

### 配置对端地址

- 【命令格式】 **tunnel destination** { *ip-address* }
- 【参数说明】 *ip-address* : 可以是 ipv4 地址, 也可以是 IPv6 地址。
- 【命令模式】 接口模式
- 【使用指导】 手工隧道必须配置对端地址。  
配置的对端地址的协议族类型必须同传输协议一致, 否则隧道接口禁用 (不 UP)。

## 配置举例

### 配置隧道对端地址。

- 【配置方法】
  - 配置隧道对端地址为 2.2.2.2

```
Ruijie# configure terminal
Ruijie(config)# interface tunnel 1
Ruijie(config-if-Tunnel 1)# tunnel mode ipv6ip
Ruijie(config-if-Tunnel 1)# tunnel destination 2.2.2.2
```

- 【检验方法】
  - 检查隧道接口的配置

```
Ruijie# show interfaces tunnel 1
.....
Tunnel attributes:
  Tunnel source: UNKNOWN, destination 2.2.2.2, unrouteable
  Tunnel TOS/Traffic Class not set, Tunnel TTL 254
  Tunnel config nested limit is 0, current nested number is 0
  Tunnel protocol/transport ipv6ip
.....
```

## 常见错误

- 为自动隧道配置对端地址。
- 和另一个隧道的对端地址相同。

## 10.4.5 配置隧道传输网络 TOS

## 配置效果

- 指定传输协议首部的 tos 或者 traffic class 字段。

## 注意事项

- 如果不指定，则拷贝承载协议对应的 tos 和 traffic class 字段。

## 配置方法

### 配置传输网络 TOS

- 可选配置
- 如果需要修订隧道数据在网络中的优先级
- 在接口模式下使用 tunnel tos 命令

## 检验方法

- 使用 **show interfaces tunnel** 命令查看是否成功设置。

## 相关命令

### 配置传输网络 TOS

【命令格式】 **tunnel tos number**

【参数说明】 *number* : 需要设置的 tos 的值。

【命令模式】 接口模式

【使用指导】 缺省情况下，如果隧道内层承载与外层封装都是 IPv4 协议，则缺省将内层 IPv4 头的 tos 字节拷贝到外层 IPv4 头。如果隧道内层承载与外层封装都是 IPv6 协议，则缺省将内层 IPv6 头的 traffic class8 比特拷贝到外层 IPv6 头。其他情况，外层 IPv4 tos / IPv6 traffic class,为 0。

## 配置举例

### 配置传输网络 TOS。

【配置方法】

- 配置传输网络 TOS

```
Ruijie# configure terminal
Ruijie(config)# interface tunnel 1
Ruijie(config-if-Tunnel 1)# tunnel mode ipv6ip
Ruijie(config-if-Tunnel 1)# tunnel tos 2
```

【检验方法】

- 检查隧道接口的配置



**【配置方法】**

- 配置传输网络 TOS

```
Ruijie# configure terminal
Ruijie(config)# interface tunnel 1
Ruijie(config-if-Tunnel 1)# tunnel mode ipv6ip
Ruijie(config-if-Tunnel 1)# tunnel tos 2
```

**【检验方法】**

- 检查隧道接口的配置

```
Ruijie# show interfaces tunnel 1
.....
Tunnel attributes:
  Tunnel source 1.1.1.1, destination UNKNOWN, unrouteable
  Tunnel TOS/Traffic Class 0x2, Tunnel TTL 254
  Tunnel config nested limit is 0, current nested number is 0
  Tunnel protocol/transport ipv6ip
  Tunnel transport VPN is VPN1
.....
```

## 常见错误

---

无

## 10.4.6 配置隧道传输网络 TTL

### 配置效果

---

- 指定隧道封装协议首部的 TTL 或者 hoplimit 的值。

### 注意事项

---

无

### 配置方法

---

#### 📌 配置传输网络 TTL

- 可选配置
- 缺省 254
- 如果需要将隧道链路的长度修改成特定值

- 使用 `tunnel ttl` 命令进行设置。

## 检验方法

---

- 使用 `show interfaces tunnel` 命令查看是否成功设置。

## 相关命令

---

### 配置传输网络 TTL

- 【命令格式】 `tunnel ttl hop-limit`
- 【参数说明】 `hop-limit`：传输网络的跳数限制。
- 【命令模式】 全局模式
- 【使用指导】 指的是传输网络最多可以经过的路由器数目，缺省是 254。需要修改成特定值，可以使用此命令。

## 配置举例

---

### 配置传输网络 TTL

- 【配置方法】
  - 配置传输网络 TTL。

```
Ruijie# configure terminal
Ruijie(config)# interface tunnel 1
Ruijie(config-if-Tunnel 1)# tunnel mode ipv6ip
Ruijie(config-if-Tunnel 1)# tunnel ttl 3
```

- 【检验方法】
  - 检查隧道接口的配置

```
Ruijie# show interfaces tunnel 1
.....
Tunnel attributes:
  Tunnel source 1.1.1.1, destination UNKNOWN, unrouteable
  Tunnel TOS/Traffic Class 0x2, Tunnel TTL 3
  Tunnel config nested limit is 0, current nested number is 0
  Tunnel protocol/transport ipv6ip
  Tunnel transport VPN is VPN1
```

## 常见错误

---

无

## 10.5 监视与维护

### 清除各类信息

---

无


### 查看运行情况

---

| 作用          | 命令                                          |
|-------------|---------------------------------------------|
| 查看隧道接口相关信息。 | <b>show interfaces tunnel <i>number</i></b> |

### 查看调试信息

---

 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

| 作用          | 命令                  |
|-------------|---------------------|
| 打开隧道接口的调试开关 | <b>debug tunnel</b> |

# 11 网络通信检测工具

## 11.1 概述

网络通信检测工具可以用于检查网络是否能够连通，用好网络通信监测工具可以很好地帮助我们分析判定网络故障。网络通信检测工具包括 PING（Packet Internet Groper，因特网包探索器）和 Traceroute（路由侦测）。PING 工具主要用于检测网络通与不通，以及网路的时延，时延值越大，则表示网络速度越慢。Traceroute 工具则可以帮助用户了解网络的物理与逻辑连接的拓扑情况以及数据传输的效率。在网络设备上，这两个工具所对应的命令为 ping 和 traceroute。

### 协议规范

- RFC792：Internet Control Message Protocol
- RFC4443：Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

## 11.2 典型应用

| 典型应用     | 场景描述                             |
|----------|----------------------------------|
| 端对端连通性检查 | 网络设备与目标主机都连接在 IP 网络上，都配置有 IP 地址。 |
| 主机路由检查   | 网络设备与目标主机都连接在 IP 网络上，都配置有 IP 地址。 |

### 11.2.1 端对端连通性检查

#### 应用场景

图 11-1 网络设备 A 与目标主机 B 都连接在 IP 网络上。

网络设备与目标主机都连接在 IP 网络上，端对端连通性检查就是判定 IP 报文能否在二者之间传输。目标主机可以是网络设备本身，这种情况一般用于检查设备自身网络接口和 TCP/IP 协议配置的正确性。



#### 功能部署

通过在网络设备上运行 Ping 功能。

## 11.2.2 主机路由检查

### 应用场景

图 11-2 网络设备 A 与目标主机 B 都连接在 IP 网络上。

网络设备与目标主机都连接在 IP 网络上，主机路由检查就是判定 IP 报文在二者之间传输，究竟需要经过多少网关（路由器）。目标主机通常不是网络设备本身，并且通常与网络设备不在同一个 IP 网段。



### 功能部属

通过在网络设备上运行 Traceroute 功能。

## 11.3 功能详解

### 功能特性

| 功能特性             | 作用                             |
|------------------|--------------------------------|
| Ping 连通性测试       | 检测指定 IPv4/v6 地址是否可达，并输出相关信息。   |
| Traceroute 连通性测试 | 显示 IPv4/v6 数据包从源地址到目的地址所经过的网关。 |

### 11.3.1 Ping 连通性测试

#### 工作原理

PING 工具向目标 IP 地址发送一个 ICMP 请求（ICMP Request）数据包，要求对方返回一个 ICMP 回声（ICMP Echo）数据包，来确定两台网络机器是否连接相通，时延是多少。

#### 相关配置

- 通过 ping 命令进行配置

## 11.3.2 Traceroute 连通性测试

### 工作原理

Traceroute 工具利用 ICMP 及 IP 报文头部的 TTL ( Time To Live ) 字段。首先，网络设备的 Traceroute 工具送出一个 TTL 是 1 的 ICMP Request 到目的主机，当路径上的第一个路由器收到这个报文时，它将 TTL 减 1。此时 TTL 变为 0 了，所以该路由器会将此报文丢弃，并送回一个 ICMP 超时 ( ICMP time exceeded ) 消息，Traceroute 工具收到这个消息后，便知道这个路由器存在于这个路径上，接着再送出另一个 TTL 是 2 的报文，发现第 2 个路由器。Traceroute 工具每次将送出的报文的 TTL 加 1 来发现另一个路由器，这个重复的动作一直持续到某个数据报文到达目的主机。当报文到达目的主机后，该主机不会送回 ICMP time exceeded 消息，而是送回 ICMP Echo，Traceroute 工具结束探测并显示从网络设备到目的主机的路径信息。

### 相关配置

- 通过 `traceroute` 命令进行配置

## 11.4 配置详解

| 配置项              | 配置建议 & 相关命令                                                                                                             |                   |
|------------------|-------------------------------------------------------------------------------------------------------------------------|-------------------|
| Ping 连通性测试       |  可选配置，用于检测 IPv4/v6 地址是否可达。           |                   |
|                  | <code>ping</code>                                                                                                       | 运行 Ping 功能。       |
| Traceroute 连通性测试 |  可选配置，显示 IPv4/v6 数据包从源地址到目的地址所经过的网关。 |                   |
|                  | <code>traceroute</code>                                                                                                 | 运行 Traceroute 功能。 |

### 11.4.1 Ping 连通性测试

#### 配置效果

在网络设备上采用 Ping 连通性测试，可以得知该网络设备和目的主机之间是否保持连通，报文是否可以在网络设备和目的主机之间传输。

#### 注意事项

执行 PING 操作的网络设备本身需要配置 IP 地址。

#### 配置方法

- 如果需要检测 IPv4 地址是否可达，可通过 `Ping IPv4` 命令。

- 如果需要检测 IPv6 地址是否可达，可通过 Ping IPv6 命令。

## 检验方法

输入 **ping** 命令，即可在 CLI 界面显示相关信息。

## 相关命令

### 📄 Ping IPv4

- 【命令格式】 **ping** [ **oob** | **vrf** *vrf-name* | **ip** ] { *address* } [ **length** *length* ] [ **ntimes** *times* ] [ **timeout** *seconds* ] [ **data** *data* ] [ **source** *source* ] [ **df-bit** ] [ **validate** ] [ **detail** ] [ **interval** *millisecond* ] }
- 【参数说明】 **oob**：设置使用带外通道。当指定 MGMT 口作为源接口时，必须设置该参数。  
*vrf-name*：VRF 名字。  
*address*：指定目的 IPv4 地址或域名。*length*：指定发送数据包数据填充段的长度，范围：36~18024，默认填充长度为 100。  
*times*：指定发送数据包的个数，范围：1~ 4294967295。  
*seconds*：指定超时的时间，范围：1~10（秒）。  
*data*：指定报文填充数据，格式为 1-255 长度的字符串，默认填充为 abcd。  
*source*：指定报文源 IPv4 地址或源接口。其中，环回接口地址（例如 127.0.0.1）不允许作为源地址。  
**df-bit**：设置 IP 的 DF 标识位，当 DF 位被设置为 1 时，表示不对数据包进行分段处理，默认 DF 位为 0。  
**validate**：设置是否校验响应报文。  
**detail**：设置回显是否显示详细信息，默认只显示 ‘!’ 和 ‘.’。  
*millisecond*：指定每个 ping 报文的间隔时间，范围：10~300000（毫秒），缺省间隔时间是 100 毫秒。
- 【命令模式】 在普通用户模式下，只能运行基本的 **ping** 功能；在特权用户模式下，还可以运行 **ping** 的扩展功能。  
在其他模式下，可以通过 do 命令执行 **ping** 的扩展功能，具体配置请参考 do 命令说明。
- 【使用指导】 运行 **ping** 功能，如果有应答，则显示出应答的相关信息，最后输出一个统计信息。在扩展 **ping** 中，可以指定发送数据包的个数、长度、超时的时间等等，和基本的 **ping** 功能一样，最后也输出一个统计信息。  
要使用域名功能，则要先配置域名服务器，具体配置请参考 DNS 配置部分。

### 📄 Ping IPv6

- 【命令格式】 **ping** [ **vrf** *vrf-name* | [ **oob** ] **ipv6** ] [ *address* [ **length** *length* ] [ **ntimes** *times* ] [ **timeout** *seconds* ] [ **data** *data* ] [ **source** *source* ] [ **detail** ] [ **interval** *millisecond* ] ] }
- 【参数说明】 **oob**：设置使用带外通道。当指定 MGMT 口作为源接口时，必须设置该参数。  
*vrf-name*：VRF 名字。  
*address*：指定目的 IPv6 地址或域名。  
*length*：指定发送数据包的长度，范围：16~18024，默认填充长度为 100。  
*times*：指定发送数据包的个数，范围：1~ 4294967295。  
*seconds*：指定超时的时间，范围：1~10（秒）。  
*data*：指定报文填充数据，格式为 1-255 长度的字符串。  
*source*：指定报文源 IPv6 地址或源接口。其中，环回接口地址（例如::1）不允许作为源地址。

**Detail**：设置回显是否显示详细信息，默认只显示 ‘!’ 和 ‘.’。

**millisecond**：指定每个 ping 报文的间隔时间，范围：10~300000（毫秒），缺省间隔时间是 100 毫秒

【命令模式】 在普通用户模式下，只能运行基本的 **ping ipv6** 功能；在特权用户模式下，还可以运行 **ping ipv6** 的扩展功能。在其他模式下，可以通过 **do** 命令执行 **ping** 的扩展功能，具体配置请参考 **do** 命令说明。

【使用指导】 运行 **ping ipv6** 功能，如果有应答，则显示出应答的相关信息，最后输出一个统计信息。在扩展 **ping ipv6** 中，可以指定发送数据包的个数、长度、超时的时间等等，和基本的 **ping ipv6** 功能一样，最后也输出一个统计信息。

要使用域名功能，则要先配置域名服务器，具体配置请参考 DNS 配置部分。

## 配置举例

### 运行普通 Ping 功能

【配置方法】 在特权模式下输入 Ping IPv4 地址 192.168.21.26

```
常规 ping
Ruijie# ping 192.168.21.26
Sending 5, 100-byte ICMP Echoes to 192.168.21.26, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

显示 detail 的 ping
Ruijie#ping 192.168.21.26 detail
Sending 5, 100-byte ICMP Echoes to 192.168.21.26, timeout is 2 seconds:
  < press Ctrl+C to break >
Reply from 192.168.21.26: bytes=100 time=4ms TTL=64
Reply from 192.168.21.26: bytes=100 time=3ms TTL=64
Reply from 192.168.21.26: bytes=100 time=1ms TTL=64
Reply from 192.168.21.26: bytes=100 time=1ms TTL=64
Reply from 192.168.21.26: bytes=100 time=1ms TTL=64

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms.
```

【检验方法】 缺省将 5 个数据段长度为 100Byte 的数据包发送到指定的 IP 地址，在指定的时间（缺省为 2 秒）内，显示相应的探测信息，最后输出一个统计信息。

### 运行扩展 Ping 功能

【配置方法】 在特权模式下输入 Ping IPv4 地址 192.168.21.26，并指定发送数据包的长度、个数、超时的时间等。

```
常规 ping
Ruijie# ping 192.168.21.26 length 1500 ntimes 100 data ffff source 192.168.21.99 timeout 3
Sending 100, 1500-byte ICMP Echoes to 192.168.21.26, timeout is 3 seconds:
  < press Ctrl+C to break >
!!
!!!!
```



```

Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms
显示 detail 的 ping
ping 192.168.21.26 length 1500 ntimes 20 data ffff source 192.168.21.99 timeout 3 detail
Sending 20, 1500-byte ICMP Echoes to 192.168.21.26, timeout is 3 seconds:
    < press Ctrl+C to break >
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=2ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=3ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64

Success rate is 100 percent (20/20), round-trip min/avg/max = 1/1/3 ms.

```

**【检验方法】** 将 20 个长度为 1500Byte 的数据包发送到指定的 IP 地址，在指定的时间（3 秒）内，如果有应答，显示相应的探测信息，最后输出一个统计信息。

## 运行普通 Ping IPv6 功能

**【配置方法】** 在特权模式下输入 Ping IPv6 地址 2001::1

```

常规 ping
Ruijie# ping ipv6 2001::1
Sending 5, 100-byte ICMP Echoes to 2001::1, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

显示 detail 的 ping

```

```
Ruijie#ping 2001::1 detail
Sending 5, 100-byte ICMP Echoes to 2001::1, timeout is 2 seconds:
< press Ctrl+C to break >
Reply from 2001::1: bytes=100 time=1ms
Reply from 2001::1: bytes=100 time=1ms
Reply from 2001::1: bytes=100 time=1ms
Reply from 2001::1: bytes=100 time=1ms
Reply from 2001::1: bytes=100 time=1ms

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

【检验方法】 缺省将 5 个数据段长度为 100Byte 的数据包发送到指定的 IP 地址，在指定的时间（缺省为 2 秒）内，显示相应的探测信息，最后输出一个统计信息。

## 运行扩展 Ping IPv6 功能

【配置方法】 在特权模式下输入 Ping IPv6 地址 2001::5，并指定发送数据包的长度、个数、超时的时间等。

```
常规 ping
Ruijie# ping ipv6 2001::5 length 1500 ntimes 100 data ffff source 2001::9 timeout 3
Sending 100, 1500-byte ICMP Echoes to 2001::5, timeout is 3 seconds:
< press Ctrl+C to break >
!!
!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms

显示 detail 的 ping
Ruijie#ping 2001::5 length 1500 ntimes 10 data ffff source 2001::9 timeout 3
Sending 10, 1500-byte ICMP Echoes to 2001::5, timeout is 3 seconds:
< press Ctrl+C to break >
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms

Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/1 ms.
```

【检验方法】 将 100 个长度为 1500Byte 的数据包发送到指定的 IPv6 地址，指定的时间（3 秒）内，显示相应的探测信息，最后输出一个统计信息。

## 11.4.2 Traceroute 连通性测试

### 配置效果

---

在网络设备上采用 Traceroute 连通性测试，可以得知该网络设备和目的主机之间的路由拓扑信息，报文从网络设备到目的主机经过了多少个网关。

### 注意事项

---

执行 Traceroute 操作的网络设备本身需要配置 IP 地址。

### 配置方法

---

- 如果需要跟踪 IPv4 数据包到达目的主机经过哪些网关，可通过配置 Traceroute IPv4 命令。
- 如果需要跟踪 IPv6 数据包到达目的主机经过哪些网关，可通过配置 Traceroute IPv6 命令。

### 检验方法

---

输入 **traceroute** 命令，即可在 CLI 界面显示相关信息。

### 相关命令

---

#### Traceroute IPv4

- 【命令格式】 **traceroute** [ **oob** | **vrf** *vrf-name* | **ip** ] { *address* } [ **probe** *number* ] [ **source** *source* ] [ **timeout** *seconds* ] [ **ttl** *minimum maximum* ] }
- 【参数说明】 **oob**：设置使用带外通道。当指定 MGMT 口作为源接口时，必须设置该参数。  
*vrf-name*：VRF 名字。  
*address*：指定目的 IPv4 地址或域名。  
*number*：指定发送的探测的数量，范围：1~255。  
*source*：指定报文源 IPv4 地址或源接口。其中，环回接口地址（例如 127.0.0.1）不允许作为源地址  
*seconds*：指定超时的时间，范围：1~10（秒）。  
*minimum maximum*：指定最小和最大 TTL 值，范围：1~255。
- 【命令模式】 在普通用户模式下，只能运行基本的 **traceroute** 功能；在特权用户模式下，还可以运行 **traceroute** 的扩展功能。
- 【使用指导】 **Traceroute** 命令主要用于检查网络的连通性，并在网络故障发生时，准确的定位故障发生的位置。要使用域名功能，则要先配置域名服务器，具体配置请参考 DNS 配置部分。

#### Traceroute IPv6

- 【命令格式】 **traceroute** [ **vrf** *vrf-name* | [ **oob** ] **ipv6** ] { *address* } [ **probe** *number* ] [ **timeout** *seconds* ] [ **ttl** *minimum*

```
maximum]]}
```

【参数说明】 **oob**：设置使用带外通道。当指定 MGMT 口作为源接口时，必须设置该参数。

**vrf-name**：VRF 名字。

**address**：指定目的 IPv6 地址或域名。

**number**：指定发送的探测的数量，范围：1~255。

**seconds**：指定超时时间，范围：1~10（秒）。

**minimum maximum**：指定最小和最大 TTL 值，范围：1~255。

【配置模式】 在普通用户模式下，只能运行基本的 **traceroute ipv6** 功能；在特权用户模式下，还可以运行 **traceroute ipv6** 的扩展功能。

【使用指导】 **Traceroute ipv6** 命令主要用于检查网络的连通性，并在网络故障发生时，准确的定位故障发生的位置。要使用域名功能，则要先配置域名服务器，具体配置请参考 DNS 配置部分。

## 配置举例

### 网络畅通的 Traceroute 举例

【配置方法】 在特权模式下，输入 Traceroute IPv6 地址 3002::1。

```
Ruijie#
Ruijie# traceroute ipv6 3004::1
< press Ctrl+C to break >
Tracing the route to 3004::1
 1      3000::1          0 msec  0 msec  0 msec
 2      3001::1          4 msec  4 msec  4 msec
 3      3002::1          8 msec  8 msec  4 msec
```

从上面的结果可以清楚地看到，从源地址要访问 IP 地址为 3002::1 的主机，网络数据包都经过了哪些网关（1 - 3），同时给出了到达该网关所花费的时间。

### 网络中某些网关不通的 Traceroute 举例

【配置方法】 在特权模式下，输入 Traceroute IPv4 地址 202.108.37.42。

```

Ruijie# traceroute 202.108.37.42
< press Ctrl+C to break >
Tracing the route to 202.108.37.42
 1  192.168.12.1      0 msec  0 msec  0 msec
 2  192.168.9.2       0 msec  4 msec  4 msec
 3  192.168.110.1    16 msec 12 msec 16 msec
 4  * * *
 5  61.154.8.129     12 msec 28 msec 12 msec
 6  61.154.8.17      8 msec 12 msec 16 msec
 7  61.154.8.250     12 msec 12 msec 12 msec
 8  218.85.157.222   12 msec 12 msec 12 msec
 9  218.85.157.130   16 msec 16 msec 16 msec
10  218.85.157.77    16 msec 48 msec 16 msec
11  202.97.40.65     76 msec 24 msec 24 msec
12  202.97.37.65     32 msec 24 msec 24 msec
13  202.97.38.162    52 msec 52 msec 224 msec
14  202.96.12.38     84 msec 52 msec 52 msec
15  202.106.192.226  88 msec 52 msec 52 msec
16  202.106.192.174  52 msec 52 msec 88 msec
17  210.74.176.158  100 msec 52 msec 84 msec
18  202.108.37.42    48 msec 48 msec 52 msec

```

从上面的结果可以清楚地看到，从源地址要访问 IP 地址为 202.108.37.42 的主机，网络数据包都经过了哪些网关（1 - 17），并且网关 4 出现了故障。

## 网络畅通的 Traceroute ipv6 举例

【配置方法】 在特权模式下，输入 Traceroute IPv6 地址 3004::1。

```

Ruijie# traceroute ipv6 3004::1
< press Ctrl+C to break >
Tracing the route to 3004::1
 1  3000::1          0 msec  0 msec  0 msec
 2  3001::1          4 msec  4 msec  4 msec
 3  3002::1          8 msec  8 msec  4 msec
 4  3004::1          4 msec 28 msec 12 msec

```

从上面的结果可以清楚地看到，从源地址要访问 IP 地址为 3004::1 的主机，网络数据包都经过了哪些网关（1 - 4），同时给出了到达该网关所花费的时间。

## 网络中某些网关不通的 Traceroute IPv6 举例

【配置方法】 在特权模式下，输入 Traceroute IPv6 地址 3004::1。

```
Ruijie# traceroute ipv6 3004::1
< press Ctrl+C to break >
Tracing the route to 3004::1
 1      3000::1          0 msec  0 msec  0 msec
 2      3001::1          4 msec  4 msec  4 msec
 3      3002::1          8 msec  8 msec  4 msec
 4      * * *
 5      3004::1          4 msec  28 msec  12 msec
```

从上面的结果可以清楚地看到，从源地址要访问 IP 地址为 3004::1 的主机，网络数据包都经过了哪些网关（1 - 5），并且网关 4 出现了故障。

## 12 TCP

### 12.1 概述

TCP 协议为应用层提供了一个可靠的、有连接的基于 IP 的传输层协议。

应用层向 TCP 层发送用于网间传输的、用 8 位字节表示的数据流，然后 TCP 把数据流分割成适当长度的报文段，最大分段大小 (MSS) 通常受该计算机连接的网路的数据链路层的最大传送单元 (MTU) 限制。之后 TCP 把报文传给 IP 层，由它来通过网络将报文传送给接收端实体的 TCP 层。

TCP 为了保证不发生丢包，就给每个字节一个序号，同时序号也保证了传送到接收端实体的包的按序接收。然后接收端实体对已成功收到的字节发回一个相应的确认 (ACK)；如果发送端实体在合理的往返时延 (RTT) 内未收到确认，那么对应的数据 (假设丢失了) 将会被重传。

- 在数据正确性与合法性上，TCP 用一个校验和函数来检验数据是否有错误，在发送和接收时都要计算校验和。  
同时可以使用 MD5 认证对数据进行校验。
- 在保证可靠性上，采用超时重传和捎带确认机制。
- 在流量控制上，采用滑动窗口协议，协议中规定，对于窗口内未经确认的分组需要重传。

#### 协议规范

- RFC 793 : Transmission Control Protocol
- RFC 1122 : Requirements for Internet Hosts -- Communication Layers
- RFC 1191 : Path MTU Discovery
- RFC 1213 : Management Information Base for Network Management of TCP/IP-based internets:MIB-II
- RFC 2385 : Protection of BGP Sessions via the TCP MD5 Signature Option
- RFC 4022 : Management Information Base for the Transmission Control Protocol (TCP)

### 12.2 典型应用

| 典型应用       | 场景描述                                                         |
|------------|--------------------------------------------------------------|
| TCP 性能优化   | TCP 传输路径上某一段链路的 MTU 比较小，为了避免 TCP 报文分片，可以开启 TCP 的路径 MTU 发现功能。 |
| TCP 连接异常检测 | TCP 探测对端是否还在正常工作。                                            |

## 12.2.1 TCP 性能优化

### 应用场景

以下图为例，A 和 D 建立 TCP 连接，A 和 B 之间链路的 MTU 是 1500 字节，B 和 C 之间链路的 MTU 是 1300 字节，C 和 D 之间链路的 MTU 是 1500 字节，为了使 TCP 传输性能达到最优，需要避免 TCP 报文在设备 B 和设备 C 上分片。

图 12-1



【注释】 A、B、C 和 D 为路由器。

### 功能部署

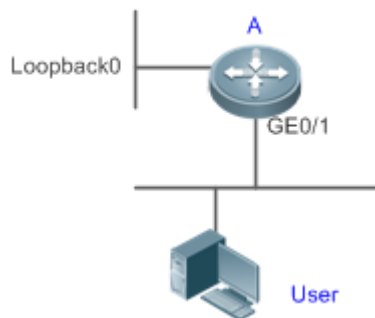
- 在 A 和 D 上开启 TCP 的路径 MTU 发现功能。

## 12.2.2 TCP 连接异常检测

### 应用场景

以下图为例，用户远程登录到设备 A，用户异常关机，如果设备 A 等待 TCP 重传超时，会导致用户的 TCP 连接残留比较长的一段时间，可以利用 TCP 保活功能快速检测出用户的 TCP 连接异常。

图 12-2



【注释】 A 是路由器。

### 功能部署

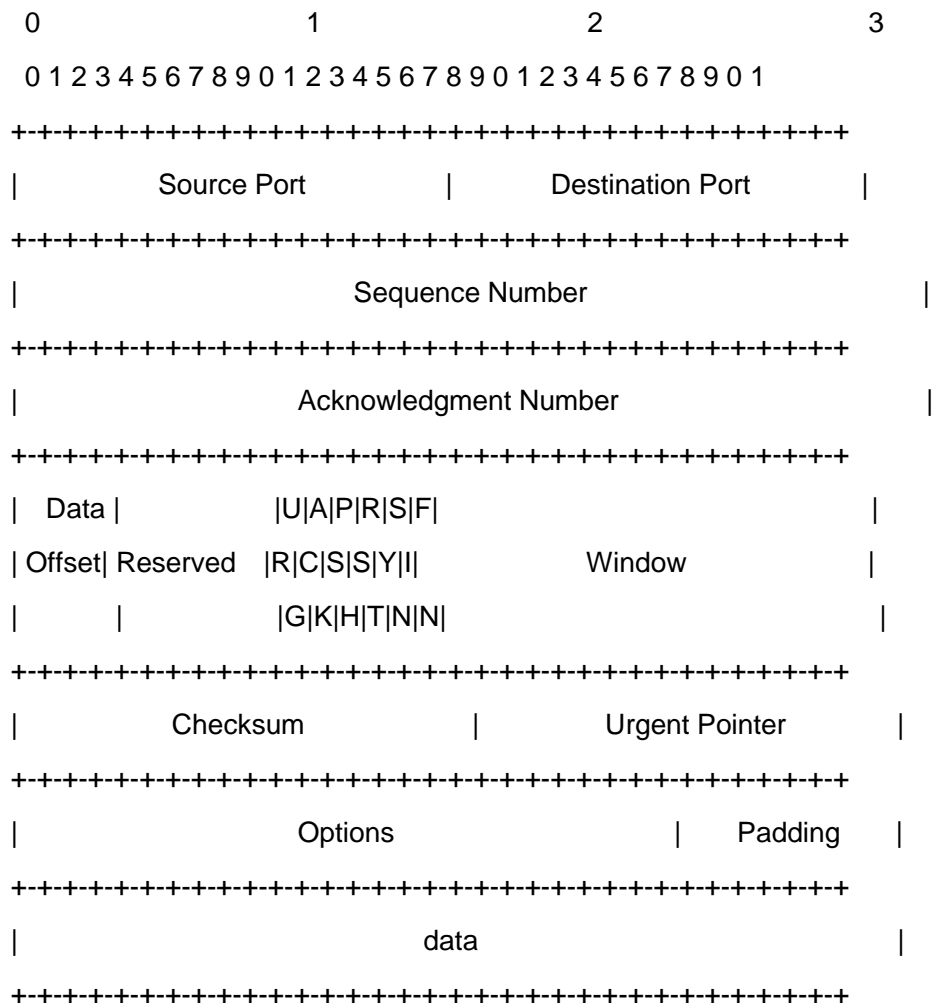


- 在设备 A 上开启 TCP 保活功能。

## 12.3 功能详解

### 基本概念

#### ✚ TCP 首部格式



- Source Port 是源端口，16 位。
- Destination Port 是目的端口，16 位。
- Sequence Number 是序列号，32 位。
- Acknowledgment Number 是确认序列号，32 位。
- Data Offset 是数据偏移，4 位，该字段的值是 TCP 首部（包括选项）长度除以 4。

- 标志位：6 位，URG 表示 Urgent Pointer 字段有意义，ACK 表示 Acknowledgment Number 字段有意义，PSH 表示 Push 功能，RST 表示复位 TCP 连接，SYN 表示 SYN 报文（在建立 TCP 连接的时候使用），FIN 表示发送方没有数据需要发送了（在关闭 TCP 连接的时候使用）。
- Window 表示接收缓冲区的空闲空间，16 位，用来告诉 TCP 连接对端自己能够接收的最大数据长度。
- Checksum 是校验和，16 位。
- Urgent Pointers 是紧急指针，16 位，只有 URG 标志位被设置时该字段才有意义，表示紧急数据相对序列号（Sequence Number 字段的值）的偏移。

### 📌 TCP 三次握手

- TCP 三次握手的过程如下：
  - (1) 客户端发送 SYN 报文给服务器端。
  - (2) 服务器端收到 SYN 报文，回应一个 SYN ACK 报文。
  - (3) 客户端收到服务器端的 SYN 报文，回应一个 ACK 报文。
- 三次握手完成，TCP 客户端和服务端成功地建立连接，可以开始传输数据了。

### 功能特性

| 功能特性                  | 作用                                                |
|-----------------------|---------------------------------------------------|
| 配置 SYN 超时             | 配置 TCP 发送 SYN 报文或者 SYN ACK 报文后等待应答报文的超时           |
| 配置窗口大小                | 配置窗口大小                                            |
| 配置端口不可达时是否发送 reset 报文 | 配置在收到端口不可达的 TCP 报文时是否发送 reset 报文                  |
| 配置 MSS                | 配置 TCP 连接的 MSS                                    |
| 路径 MTU 发现功能           | 探测 TCP 传输路径上的最小 MTU，根据最小 MTU 调整发送的 TCP 报文的大小，避免分片 |
| TCP 保活功能              | 探测 TCP 连接对端是否还在正常工作                               |

## 12.3.1 配置 SYN 超时

### 工作原理

建立 TCP 连接需要经过三次握手：发起方先发送 SYN 报文，响应方回应 SYN+ACK 报文，然后发起方再回应 ACK。

- 在发起方发送 SYN 报文后，如果响应方一直不回应 SYN+ACK 报文，发起方会不断的重传 SYN 报文直到超过一定的重传次数或超时时间。
- 在发起方发送 SYN 报文后，响应方回应 SYN+ACK 报文，但发起方不再回复 ACK，响应方也会一直重传直到超过一定的重传次数或超时时间。（SYN 报文攻击会出现这种情况。）

## 相关配置

### 设置 TCP SYN 超时时间

- TCP SYN 超时时间的缺省值是 20 秒。
- 用户可以在全局配置模式下使用 “**ip tcp synwait-time seconds**” 命令设置 SYN 超时时间，取值范围是 5 到 300，单位是秒。
- 如果网络中存在 SYN 攻击，减少 SYN 超时时间可以防止一些资源消耗，但对连续的 SYN 攻击达不到效果。在设备主动与外界请求建立连接时，减少 SYN 超时时间可以减少用户等待时间，如 telnet。如果网络比较差也可以适当增加超时时间。

**i** 11.0 版本废弃了 10.x 版本的配置命令 “ip tcp syntime-out” 被废弃，但兼容 10.x 版本，如果执行了 10.x 版本的配置命令，将自动转换成 11.0 版本的配置命令。

**i** 10.x 版本该命令只对 IPv4 TCP 生效，从 11.0 版本开始该命令对 IPv4 TCP 和 IPv6 TCP 都生效。

## 12.3.2 配置窗口大小

### 工作原理

TCP 的接收缓冲区用来缓存从对端接收到的数据，这些数据后续会被应用程序读取。一般情况下，TCP 的窗口值反映接收缓冲区的空闲空间的大小。对于带宽比较大、有大量数据的连接，增大窗口可以显著提高 TCP 传输性能。

## 相关配置

### 设置窗口大小

- 用户可以在全局配置模式下使用 “**ip tcp window-size size**” 命令设置窗口大小，单位是字节，取值范围是 128 到 (65535<<14)，缺省值是 65535。如果窗口大于 65535 字节，自动开启窗口扩大功能。
- 实际通告给对端的窗口大小是从配置的窗口大小和接收缓冲区的剩余空间取较小值。

**i** 10.x 版本只对 IPv4 TCP 生效，从 11.0 版本开始对 IPv4 TCP 和 IPv6 TCP 都生效。

## 12.3.3 配置端口不可达时是否发送 reset 报文

### 工作原理

TCP 协议在分发 TCP 报文给应用程序时，如果找不到该报文所属的 TCP 连接会主动回复一个 reset 报文以终止对端的 TCP 连接。攻击者可能利用大量的端口不可达的 TCP 报文对设备进行攻击。

## 相关配置

### 配置端口不可达时是否发送 reset 报文

收到端口不可达的 TCP 报文时，默认发送 reset 报文。

用户可以在全局配置模式下使用 “no ip tcp send-reset” 命令禁止发送 reset 报文。

如果允许发送 reset 报文，攻击者可能利用大量的端口不可达的 TCP 报文对设备进行攻击。

- i 11.0 版本废弃了 10.x 版本的配置命令 “ip tcp not-send-rst”，并且兼容 10.x 版本，如果执行了 10.x 版本的配置命令，将自动转换成 11.0 版本的配置命令。
- i 10.x 版本只对 IPv4 TCP 生效，从 11.0 版本开始对 IPv4 TCP 和 IPv6 TCP 都生效。

## 12.3.4 配置 MSS

### 工作原理

最大分段大小 (Maximum Segment Size, MSS)，指一个 TCP 报文的数据载荷的最大长度，不包括 TCP 选项。

在 TCP 建立连接的三次握手中需要进行 MSS 协商，连接的双方都在 SYN 报文中增加 MSS 选项，其选项值表示本端最大能接收的段大小，即对端最大能发送的段大小。连接的双方取本端发送的 MSS 值和接收对端的 MSS 值的较小者作为本连接最大传输段大小。

发送 SYN 报文时 MSS 选项值的计算方法如下：

- IPv4 TCP：MSS = 对端 IP 地址对应的出口的 IP MTU - 20 字节 IP 首部 - 20 字节 TCP 首部。
- IPv6 TCP：MSS = 对端 IPv6 地址对应的路径 MTU - 40 字节 IPv6 首部 - 20 字节 TCP 首部。

- i 10.x 版本只对 IPv4 TCP 生效，从 11.0 版本开始对 IPv4 TCP 和 IPv6 TCP 都生效。
- i 实际生效的 MSS 是从根据 MTU 计算得到的 MSS 和用户配置的 MSS 取较小值。
- i 如果该连接支持某些选项，那么 MSS 还要减去选项 4 字节对齐后的长度值。如 MD5 选项要减去 20 字节，MD5 选项长度 18 字节，对齐后 20 字节。

## 相关配置

### 设置 MSS

- 用户可以在全局配置模式下使用 “ip tcp mss max-segment-size” 命令设置 TCP 连接的 MSS，单位是字节，取值范围是 68 到 10000，默认使用根据 MTU 计算得到的 MSS。如果用户配置了 MSS，实际生效的 MSS 是从根据 MTU 计算得到的 MSS 和用户配置的 MSS 取较小值。
- MSS 太小会降低传输性能，增加 MSS 可以提高传输性能，但不是越大越好，选择 MSS 值可以参考接口的 MTU，如果 MSS 大于接口的 MTU，TCP 报文需要分片重组，会降低传输性能。

## 12.3.5 路径 MTU 发现功能

### 工作原理

RFC1191 规定的 TCP 连接的路径 MTU 发现功能，用来发现 TCP 报文传输路径的最小 MTU，避免分片重组，可以提高网络带宽的利用率。IPv4 TCP 路径 MTU 发现的过程如下：


- (1) TCP 源端将发送的 TCP 报文的外层 IP 首部设置不可分片标志位。
- (2) 如果 TCP 路径上某路由器的出口 MTU 值小于该 IP 报文长度，则会丢弃报文，并向 TCP 源端发送 ICMP 差错报文，报文中会携带该出口 MTU 值。
- (3) TCP 源端通过解析该 ICMP 差错报文，可知 TCP 路径上当前最小的 MTU 值，即路径 MTU。
- (4) 后续 TCP 源端发送数据段的长度不超过 MSS， $MSS = \text{路径 MTU} - \text{IP 头部长度} - \text{TCP 头部长度}$ 。

### 相关配置

#### 📌 启用路径 MTU 发现功能

TCP 缺省关闭路径 MTU 发现功能。

用户可以在全局配置模式下使用 “**ip tcp path-mtu-discovery**” 命令开启路径 MTU 发现功能。

 10.x 版本对 IPv4 TCP 和 IPv6 TCP 都生效。从 11.0 版本开始只对 IPv4 TCP 生效，IPv6 TCP 总是开启路径 MTU 发现功能，并且不能关闭。

## 12.3.6 TCP 保活功能

### 工作原理

如果 TCP 希望知道对端是否还在正常工作，可以开启保活功能。当 TCP 对端在一段时间内（称为空闲时间）没有发送过报文给本端，本端开始发送保活报文，连续发送若干次，如果没有收到一个应答报文，就认为对端异常，关闭 TCP 连接。

### 相关配置

#### 📌 启用保活功能

- TCP 缺省关闭保活功能。
- 用户可以在全局配置模式下使用 “**ip tcp keepalive [interval num1] [times num2] [idle-period num3]**” 命令开启保活功能。interval 是时间间隔，默认值是 75 秒；times 是发送保活报文的最大次数，默认值是 6 次；idle-period 是空闲时间，默认值是 15 分钟。

 10.x 版本只对 IPv4 TCP 生效，从 11.0 版本开始对 IPv4 TCP 和 IPv6 TCP 都生效。

- i** 10.x 版本提供全局配置模式的配置命令“**service tcp-keepalives-in**”用来开启 TCP 服务器端的保活功能，11.0 版本废弃该命令，该命令隐藏，如果用户执行该命令，将转换成新的配置命令保存。
- i** 10.x 版本提供全局配置模式的配置命令“**service tcp-keepalives-out**”用来开启 TCP 客户端的保活功能，11.0 版本废弃该命令，该命令隐藏，如果用户执行该命令，将转换成新的配置命令保存。
- i** 该命令不再区分服务器端和客户端，对所有的 TCP 连接都生效。

## 12.4 配置详解

| 配置项        | 配置建议 & 相关命令                                                                                                 |                                  |
|------------|-------------------------------------------------------------------------------------------------------------|----------------------------------|
| TCP 性能优化   |  可选配置，用于优化 TCP 连接的性能。      |                                  |
|            | <b>ip tcp synwait-time</b>                                                                                  | 配置建立 TCP 连接的超时时间。                |
|            | <b>ip tcp window-size</b>                                                                                   | 配置 TCP 窗口大小。                     |
|            | <b>ip tcp send-reset</b>                                                                                    | 配置收到端口不可达的 TCP 报文时是否发送 reset 报文。 |
|            | <b>ip tcp mss</b>                                                                                           | 配置 TCP 连接的 MSS。                  |
|            | <b>ip tcp path-mtu-discovery</b>                                                                            | 开启路径 MTU 发现功能。                   |
| TCP 连接异常检测 |  可选配置，用于检测 TCP 对端是否正常工作。 |                                  |
|            | <b>ip tcp keepalive</b>                                                                                     | 开启 TCP 保活功能。                     |

### 12.4.1 TCP 性能优化

#### 配置效果

- TCP 连接的传输性能达到最优，避免分片。

#### 注意事项

-

#### 配置方法

##### 配置 SYN 超时

- 可选配置。
- 在 TCP 连接的两端配置。

### 配置 TCP 窗口大小

- 可选配置。
- 在 TCP 连接的两端配置。

### 配置端口不可达时是否发送 reset 报文

- 可选配置。
- 在 TCP 连接的两端配置。

### 配置 MSS

- 可选配置。
- 在 TCP 连接的两端配置。

### 配置 TCP 的路径 MTU 发现功能

- 可选配置。
- 在 TCP 连接的两端配置。

## 检验方法

---

-

## 相关命令

---

### 配置 SYN 超时

【命令格式】 **ip tcp synwait-time** *seconds*

【参数说明】 *seconds* : SYN 报文超时时间。单位为秒，取值范围是 5 到 300，缺省值是 20。

【命令模式】 全局模式

【使用指导】 如果网络中存在 SYN 攻击，减少 SYN 超时时间可以防止一些资源消耗，但对连续的 SYN 攻击达不到效果。在设备主动与外界请求建立连接时，减少 SYN 超时时间可以减少用户等待时间，如 telnet。如果网络比较差也可以适当增加超时时间。

### 配置 TCP 窗口大小

【命令格式】 **ip tcp window-size** *size*

【参数说明】 *size* : 单位是字节，取值范围是 128 到(65535 << 14)，缺省值是 65535。

【命令模式】 全局模式

【使用指导】 -

### 配置端口不可达时是否发送 reset 报文

【命令格式】 **ip tcp send-reset**

【参数说明】 -

- 【命令模式】 全局模式
- 【使用指导】 收到端口不可达的 TCP 报文时，默认发送 reset 报文。

## 配置 MSS

- 【命令格式】 **ip tcp mss max-segment-size**
- 【参数说明】 **max-segment-size**：MSS 的上限值。单位为字节，取值范围是 68 到 10000，默认使用根据 MTU 计算得到的 MSS。
- 【命令模式】 全局模式
- 【使用指导】 **ip tcp mss** 的作用就是限制即将建立的 TCP 连接的 MSS 的最大值。任何新建立的连接协商的 MSS 值不能超过配置的值。如果要减小连接的最大 MSS 值，可以配置该命令，一般情况下不需要配置。

## 配置路径 MTU 发现功能

- 【命令格式】 **ip tcp path-mtu-discovery [ age-timer minutes | age-timer infinite ]**
- 【参数说明】 **age-timer minutes**：TCP 在发现路径 MTU 后，重新进行探测的时间间隔。单位是分钟，取值范围是 10 到 30。缺省值是 10。
- age-timer infinite**：TCP 在发现路径 MTU 后，不重新探测。
- 【命令模式】 全局模式
- 【使用指导】 TCP 的路径 MTU 发现功能是按 RFC1191 实现的，这个功能可以提高网络带宽的利用率。当用户使用 TCP 来批量传输大块数据时，该功能可以使传输性能得到明显提升。
- 按 RFC1191 的描述，TCP 在发现路径 MTU 后，隔一段时间可以使用更大的 MSS 来探测新的路径 MTU。这个时间间隔就是使用参数 **age-timer** 来指定。当设备发现的路径 MTU 比 TCP 连接两端协商出来的 MSS 小时，设备就会按上述配置时间间隔，去尝试发现更大的路径 MTU。直到路径 MTU 达到 MSS 的值，或者用户停止这个定时器，这个探测过程才会停止。停止这个定时器，使用 **age-timer infinite** 参数。

## 配置举例

### 开启 TCP 的路径 MTU 发现功能。

- 【配置方法】 在设备上开启 TCP 的路径 MTU 发现功能，重新探测的时间间隔取缺省值。

```
Ruijie# configure terminal
Ruijie(config)# ip tcp path-mtu-discovery
Ruijie(config)# end
```

- 【检验方法】 用户可以执行命令 **show tcp pmtu** 查看 IPv4 TCP 连接的路径 MTU。

```
Ruijie# show tcp pmtu
```

| Number | Local Address      | Foreign Address       | PMTU |
|--------|--------------------|-----------------------|------|
| 1      | 192.168.195.212.23 | 192.168.195.112.13560 | 1440 |

用户可以执行命令 **show ipv6 tcp pmtu** 查看 IPv6 TCP 连接的路径 MTU。

```
Ruijie# show ipv6 tcp pmtu
```



【配置方法】 在设备上开启 TCP 的路径 MTU 发现功能，重新探测的时间间隔取缺省值。

```
Ruijie# configure terminal
Ruijie(config)# ip tcp path-mtu-discovery
Ruijie(config)# end
```

【检验方法】 用户可以执行命令 **show tcp pmtu** 查看 IPv4 TCP 连接的路径 MTU。

| Number | Local Address | Foreign Address | PMTU |
|--------|---------------|-----------------|------|
| 1      | 1000::1:23    | 1000::2:13560   | 1440 |

## 常见错误

-

## 12.4.2 TCP 连接异常检测

### 配置效果

- TCP 探测对端是否还在正常工作。

### 注意事项

-

### 配置方法

#### 📌 开启保活功能

- 可选配置。

### 检验方法

-

### 相关命令

#### 📌 开启保活功能

【命令格式】 **ip tcp keepalive [interval num1] [times num2] [idle-period num3]**

【参数说明】 **interval num1**：发送保活报文的时间间隔，单位是秒，取值范围是 1 到 120，缺省值是 75 秒。

**times num2**：发送保活报文的最大次数，取值范围是 1 到 10，缺省值是 6。

**idle-period num3** :空闲时间,即对端没有向本端发送过报文的时间长度,单位是秒,取值范围是 60 到 1800 ,缺省值是 15 分钟。

【命令模式】 全局模式

【使用指导】 如果 TCP 希望知道对端是否还在正常工作,可以开启保活功能,默认关闭。

假设用户开启保活功能,时间间隔,次数和空闲时间都使用缺省值,TCP 在 15 分钟内没有收到过对端发送的报文,开始发送保活报文,每隔 75 秒发送一次,连续发送 6 次,如果没有收到对方发送的任何 TCP 报文,就认为 TCP 连接无效,自动释放 TCP 连接。

## 配置举例

### 📌 开启 TCP 保活功能。

【配置方法】 在设备上开启 TCP 保活功能,空闲时间是 3 分钟,发送保活报文的时间间隔是 60 秒,如果连续发送 4 次保活报文,没有收到对方发送的任何 TCP 报文,就认为 TCP 连接无效。

```
Ruijie# configure terminal
Ruijie(config)# ip tcp keepalive interval 60 times 4 idle-period 180
Ruijie(config)# end
```

【检验方法】 用户远程登录到设备,然后用户异常关机,在设备上执行 show tcp connect 观察用户的 IPv4 TCP 连接被删除的时间。

## 常见错误

## 12.5 监视与维护

### 清除各类信息

### 查看运行情况

| 作用                     | 命令                                                                                            |
|------------------------|-----------------------------------------------------------------------------------------------|
| 显示 IPv4 TCP 连接的基本信息    | <b>show tcp connect</b> [local-ip a.b.c.d] [local-port num] [peer-ip a.b.c.d] [peer-port num] |
| 显示 IPv4 TCP 连接的统计信息    | <b>show tcp connect statistics</b>                                                            |
| 显示 IPv4 TCP 路径 MTU 的信息 | <b>show tcp pmtu</b> [local-ip a.b.c.d] [local-port num] [peer-ip a.b.c.d] [peer-port num]    |

|                        |                                                                                                              |
|------------------------|--------------------------------------------------------------------------------------------------------------|
| 显示 IPv4 TCP 端口使用情况     | <b>show tcp port</b> [num]                                                                                   |
| 显示 IPv4 TCP 参数信息       | <b>show tcp parameter</b>                                                                                    |
| 显示 IPv4 TCP 统计信息       | <b>show tcp statistics</b>                                                                                   |
| 显示 IPv6 TCP 连接的基本信息    | <b>show ipv6 tcp connect</b> [local-ipv6 X:X:X:X::X] [local-port num] [peer-ipv6 X:X:X:X::X] [peer-port num] |
| 显示 IPv6 TCP 连接的统计信息    | <b>show ipv6 tcp connect statistics</b>                                                                      |
| 显示 IPv6 TCP 路径 MTU 的信息 | <b>show ipv6 tcp pmtu</b> [local-ipv6 X:X:X:X::X] [local-port num] [peer-ipv6 X:X:X:X::X] [peer-port num]    |
| 显示 IPv6 TCP 端口使用情况     | <b>show ipv6 tcp port</b> [num]                                                                              |

## 查看调试信息



输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

| 作用                  | 命令                                                                                                                                                        |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 查看 IPv4 TCP 报文的调试信息 | <b>debug ip tcp packet</b> [ in   out] [local-ip a.b.c.d] [peer-ip a.b.c.d] [global   vrf vrf-name] [local-port num] [peer-port num] [deeply]             |
| 查看 IPv4 TCP 连接的调试信息 | <b>debug ip tcp transactions</b> [local-ip a.b.c.d] [peer-ip a.b.c.d] [local-port num] [peer-port num]                                                    |
| 查看 IPv6 TCP 报文的调试信息 | <b>debug ipv6 tcp packet</b> [ in   out] [local-ipv6 X:X:X:X::X] [peer-ipv6 X:X:X:X::X] [global   vrf vrf-name] [local-port num] [peer-port num] [deeply] |
| 查看 IPv6 TCP 连接的调试信息 | <b>debug ipv6 tcp transactions</b> [local-ipv6 X:X:X:X::X] [peer-ipv6 X:X:X:X::X] [local-port num] [peer-port num]                                        |

# 13 软件 IPv4/v6 快转

## 13.1 概述

在不支持硬件转发的产品上，由软件转发 IPv4/v6 报文，为了使软件转发性能达到最优，我司实现了软件 IPv4/v6 快转。

快转主要维护两张表：转发表和邻接表。转发表用来存放路由；邻接表用来存放下一跳的链路层信息，相当于 ARP 表和 IPv6 邻居表。

快转可以主动解析下一跳，还可以实现流量负载均衡。

 下文仅介绍软件 IPv4/v6 的相关内容。

### 协议规范

## 13.2 典型应用

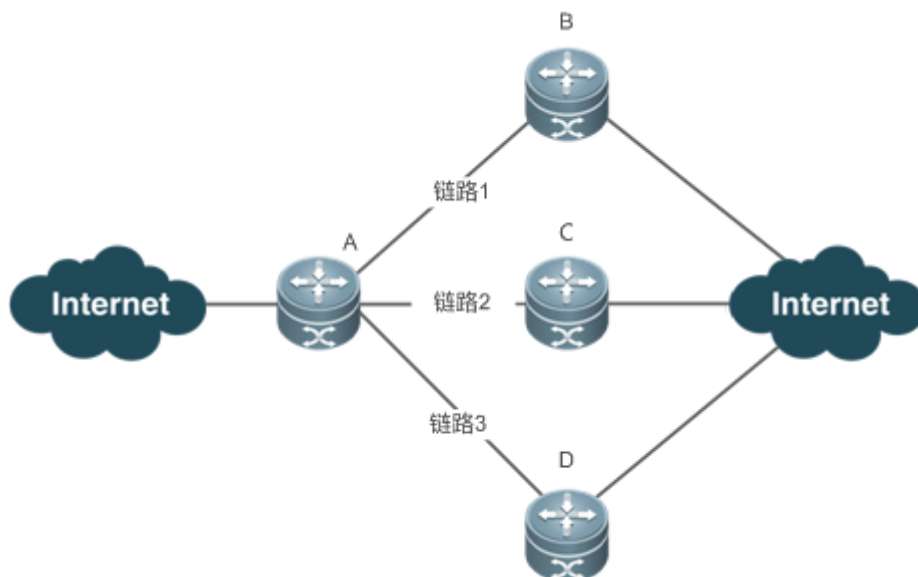
| 典型应用   | 场景描述                                       |
|--------|--------------------------------------------|
| 流量负载均衡 | 在网络路由中，当路由前缀关联到多个下一跳时，快转可以在多个下一跳中实现流量负载均衡。 |

### 13.2.1 流量负载均衡

#### 应用场景

以下图为例，路由器 A 上，对于某条路由前缀关联 3 个下一跳，即链路 1、链路 2 和链路 3。缺省情况下，快转使用目的 IP 地址进行负载均衡，还可以根据源 IP 地址和目的 IP 地址进行负载均衡。

图 13-1



【注释】 A 为运行软件快转的路由器。  
B、C、D 可以为其它转发设备。

## 功能部署

- 路由器 A 上运行软件快转。

## 13.3 功能详解

### 基本概念

IPv4/v6 快转主要涉及以下基本概念：

#### 📌 路由表

IPv4/v6 路由表中存储着指向特定网络地址的路径，同时含有网络周边的拓扑信息。在报文转发的过程中 IPv4/v6 快转根据路由表选择报文的传输路径。

#### 📌 邻接节点

邻接节点包含了被路由报文的输出接口信息。例如下一跳列表、下一个处理部件、链路层输出封装等信息。当报文与该邻接节点匹配时，直接对报文进行封装，而后调用该节点的发送函数即可实现转发。为了便于检索和更新，邻接节点构成的表一般组织成哈希表的形式；为了支持路由负载均衡，邻接节点的下一条列表信息被组织为负载均衡表的形式；邻接节点中也可以不包含下一跳信息，也可以包含下一个处理部件的索引号（例如其它线卡，多业务卡）。

#### 📌 主动解析

快转支持主动解析下一跳。对于以太网接口上的下一跳，如果不知道 MAC 地址，快转将主动解析下一跳。IPv4 快转请求 ARP 模块解析下一跳；

IPv6 快转请求 ND 模块解析下一跳。

📌 报文转发路径

报文的路由转发是根据报文的 IPv4/v6 地址，所以如果指定了报文源 IPv4/v6 地址和目的 IPv4/v6 地址，则该报文的转发路径将是确定的。

13.3.1 快转负载均衡策略

快转负载均衡就是利用多个网络设备通道均衡分担流量。

工作原理

快转支持报文的负载均衡处理，目前实现两种基于 IP 地址的负载均衡策略。在快转模型中，当路由前缀关联到多个下一跳时，即多径路由，该路由将关联到一个负载均衡表，并依路由权重实现负载均衡。当 IPv4/v6 报文依最长前缀匹配到该均衡表时，快转根据报文的 IPv4/v6 地址进行散列，选中其中的一条路径转发报文。

IPv4/v6 快转支持两种负载均衡模式，分别是根据报文的目的 IP 地址进行均衡、根据报文的源 IP 和目的 IP 地址进行均衡。

相关配置


📌 配置 IPv4 源 IP 地址 + 目的 IP 地址负载均衡算法

- 缺省根据 IPv4 报文的目的 IP 地址进行均衡。
- 可以根据 **ip ref load-sharing original** 配置该负载均衡算法。
- 配置后根据 IPv4 报文的目的 IP 地址和源 IP 地址进行均衡。

📌 配置 IPv6 源 IP 地址 + 目的 IP 地址负载均衡算法

- 缺省根据 IPv6 报文的目的地址进行均衡。
- 根据 **ipv6 ref load-sharing original** 配置该负载均衡算法。
- 配置后根据 IPv6 报文的目的 IP 地址和源 IP 地址进行均衡。

13.4 配置详解

| 配置项                        | 配置建议&相关命令                                                                                 |                                  |
|----------------------------|-------------------------------------------------------------------------------------------|----------------------------------|
| <a href="#">配置快转负载均衡策略</a> |  可选配置。 |                                  |
|                            | <b>ip ref load-sharing original</b>                                                       | 启动 IPv4 源 IP 地址 + 目的 IP 地址负载均衡算法 |
|                            | <b>ipv6 ref load-sharing original</b>                                                     | 启动 Ipv6 源 IP 地址 + 目的 IP 地址负载均衡算法 |

### 13.4.1 配置快转负载均衡策略

#### 配置效果

---

路由快转支持的两种选路策略如下：

- 按 IPv4/v6 报文的目的 IPv4/v6 地址进行均衡，对报文的目标地址进行散列，权重大的路径被选中的机率大。缺省采用此策略。
- 按 IPv4/v6 报文的目的 IPv4/v6 地址和源 IPv4/v6 地址进行均衡，对报文的目的 IPv4/v6 地址和源 IPv4/v6 地址进行散列，权重大的路径被选中的机率大。

#### 注意事项

---

-

#### 配置方法

---

- 可选配置。
- 在 IPv4/v6 环境下，如果需要根据源 IP 地址+目的 IP 地址进行流量均衡，可采用此配置。
- 在连接多条链路的路由设备上配置。

#### 检验方法

---

使用 show ip ref adjacency statistic 命令可以查看 IPv4 快转的负载均衡策略；

使用 show ipv6 ref adjacency statistic 命令可以查看 IPv6 快转的负载均衡策略。

#### 相关命令

---

##### 配置 IPv4 源 IP 地址 + 目的 IP 地址负载均衡算法

【命令格式】 ip ref load-sharing original

【参数说明】 -

【命令模式】 全局模式

【使用指导】

##### 配置 IPv6 源 IP 地址 + 目的 IP 地址负载均衡算法

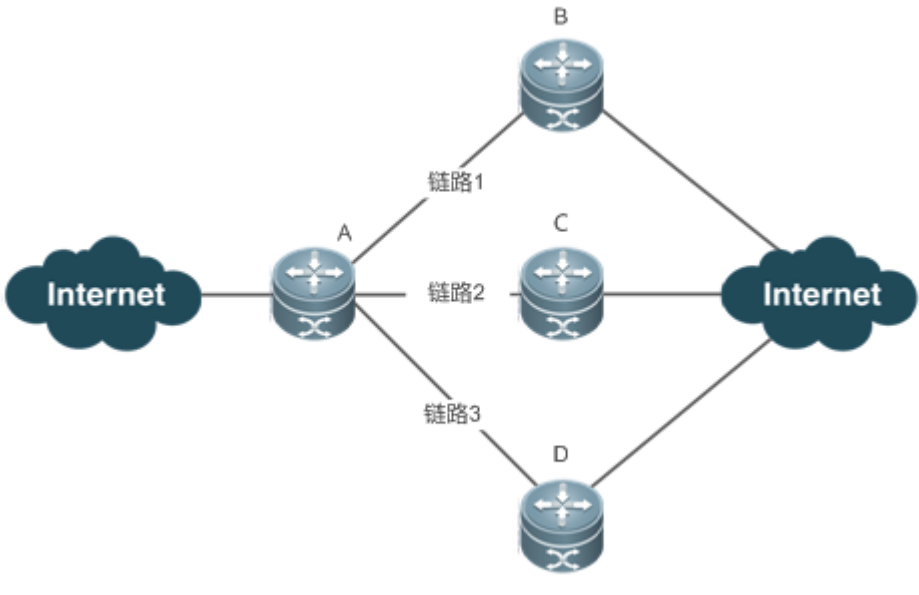
【命令格式】 ipv6 ref load-sharing original

- 【参数说明】 -
- 【命令模式】 全局模式

配置举例

配置基于 IPv4 源 IP 地址 + 目的 IP 地址负载均衡

- 【网络环境】
- 图 13-2



在路由器 A 上，对于某条路由前缀关联 3 个下一跳，即链路 1、链路 2 和链路 3。

- 【配置方法】 在路由器 A 上配置 IPv4 源 IP 地址 + 目的 IP 地址负载均衡

A

```
A#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
A(config)#ip ref load-sharing original
```

- 【检验方法】

```
A #show ip ref adjacency statistics
adjacency balance table statistic:
  source-dest-address load-sharing
  balance: 0

adjacency node table statistic:
  total   : 3
  local   : 1
  glean   : 0
  forward : 0
  discard : 0
  mcast   : 1
  punt    : 1
  bcast   : 0
```



## 常见配置错误

-

## 13.5 监视与维护

### 统计快转报文信息

快转报文统计信息即快转所处理的报文统计信息，包括了转发的报文数目，以及各种原因丢弃的报文数目等。快转提供配置信息查看和清除当前的统计信息，以供判断报文的转发行为是否和预期相同。

| 命令                                      | 作用                  |
|-----------------------------------------|---------------------|
| <b>show ip ref packet statistics</b>    | 显示 IPv4 快转当前的报文统计信息 |
| <b>clear ip ref packet statistics</b>   | 清除 IPv4 快转当前的报文统计信息 |
| <b>show ipv6 ref packet statistics</b>  | 显示 IPv6 快转当前的报文统计信息 |
| <b>clear ipv6 ref packet statistics</b> | 清除 IPv6 快转当前的报文统计信息 |

### 查看邻接信息

用户可以通过以下命令来查看当前的邻接信息：

| 命令                                                                                                                                               | 作用                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| <b>show ip ref adjacency</b> [glean   local   ip-address   {interface interface_type interface_number}] <b>discard</b>   <b>statistics</b> ]     | 可以指定显示 IPv4 快转的集合邻接、本地邻接、指定 IP 对应邻接、指定接口关联邻接及所有邻接节点相关信息。     |
| <b>show ipv6 ref adjacency</b> [glean   local   ipv6-address   (interface interface_type interface_number)] <b>discard</b>   <b>statistics</b> ] | 可以指定显示 IPv6 快转的集合邻接、本地邻接、指定 IPv6 地址对应邻接、指定接口关联邻接及所有邻接节点相关信息。 |

### 查看主动解析信息

用户可以通过以下命令来查看需要主动解析的下一跳：

| 命令                                | 作用                  |
|-----------------------------------|---------------------|
| <b>show ip ref resolve-list</b>   | 查看 IPv4 快转主动解析的下一跳。 |
| <b>show ipv6 ref resolve-list</b> | 查看 IPv6 快转主动解析的下一跳。 |

### 查看报文转发路径信息

报文的路由转发是根据报文的 IPv4/v6 地址，所以如果指定了报文源 IPv4/v6 地址和目的 IPv4/v6 地址，则该报文的转发路径将是确定的。执行下面的命令，并指定报文的源 IPv4/v6 地址与目的 IPv4/v6 地址，将会显示该报文的实际转发路径，比如报文丢弃、提交 CPU 或转发，进一步还可以知道从哪个接口转发等等。

| 命令                                                                                       | 作用                                         |
|------------------------------------------------------------------------------------------|--------------------------------------------|
| <b>show ip ref exact-route</b> [oob  vrf vrf_name]<br>source-ipaddressdest_ipaddress     | 显示某特定报文的实际转发路径。oob 表示带外，即管理口所属的管理网络。       |
| <b>show ipv6 ref exact-route</b> [oob  vrf<br>vrf-name ]src-ipv6-addressdst-ipv6-address | 显示某特定 IPv6 报文的实际转发路径。oob 表示带外，即管理口所属的管理网络。 |

## 查看快转表路由信息

通过下面的命令可以查看快转表的路由信息：

| 命令                                                                                        | 作用                                                            |
|-------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| <b>show ip ref route</b> [oob   vrfvrf_name] [default   {ip mask}<br>statistics]          | 显示当前 IPv4 快转表中的路由信息，参数 default 表示显示缺省路由。oob 表示带外，即管理口所属的管理网络。 |
| <b>show ipv6 ref route</b> [oob   vrf vrf-name ] [ default   statistics  <br>prefix/len ] | 显示当前 IPv6 快转表中的路由信息，参数 default 表示显示缺省路由。oob 表示带外，即管理口所属的管理网络。 |