

H3C S5130S-SI[LI]&S5120V2-SI[LI]&S5110V2-SI& S5000V3-EI&S5000E-X&S3100V3-SI 系列以太网交换机

三层技术-IP 业务命令参考

新华三技术有限公司
<http://www.h3c.com>

资料版本：6W103-20190822
产品版本：Release 612x 系列

Copyright © 2019 新华三技术有限公司及其许可者 版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

前言

本命令参考主要介绍 IP 业务相关特性的配置命令。

前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [资料意见反馈](#)

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定






格 式	意 义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用 加粗 字体表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[]	表示用“[]”括起来的部分在命令配置时是可选的。
{ x y ... }	表示从多个选项中仅选取一个。
[x y ...]	表示从多个选项选取一个或者不选。
{ x y ... } *	表示从多个选项中至少选取一个。
[x y ...] *	表示从多个选项选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1~n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格 式	意 义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[]	带方括号“[]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail: info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 ARP.....	1-1
1.1 ARP配置命令	1-1
1.1.1 arp check enable	1-1
1.1.2 arp check log enable	1-1
1.1.3 arp max-learning-num.....	1-2
1.1.4 arp max-learning-number	1-3
1.1.5 arp multiport	1-4
1.1.6 arp smooth.....	1-5
1.1.7 arp static.....	1-5
1.1.8 arp timer aging.....	1-6
1.1.9 display arp	1-7
1.1.10 display arp entry-limit	1-11
1.1.11 display arp <i>ip-address</i>	1-12
1.1.12 display arp openflow count.....	1-12
1.1.13 display arp timer aging	1-13
1.1.14 reset arp	1-13
2 免费ARP.....	2-1
2.1 免费ARP配置命令	2-1
2.1.1 arp ip-conflict log prompt	2-1
2.1.2 arp send-gratuitous-arp.....	2-1
2.1.3 gratuitous-arp mac-change retransmit.....	2-2
2.1.4 gratuitous-arp-learning enable	2-1
2.1.5 gratuitous-arp-sending enable	2-1
3 代理ARP.....	3-1
3.1 代理ARP配置命令	3-1
3.1.1 display local-proxy-arp	3-1
3.1.2 display proxy-arp	3-1
3.1.3 local-proxy-arp enable	3-2
3.1.4 proxy-arp enable	3-3
4 ARP Snooping	4-1
4.1 ARP Snooping配置命令	4-1
4.1.1 arp snooping enable.....	4-1

4.1.2 display arp snooping	4-1
4.1.3 reset arp snooping	4-2
5 ARP直连路由通告.....	5-1
5.1 ARP直连路由通告配置命令.....	5-1
5.1.1 arp route-direct advertise.....	5-1

1 ARP

1.1 ARP配置命令

1.1.1 arp check enable

arp check enable 命令用来开启动态 ARP 表项的检查功能。

undo arp check enable 命令用来关闭动态 ARP 表项的检查功能。

【命令】

```
arp check enable
undo arp check enable
```

【缺省情况】

动态 ARP 表项的检查功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

动态 ARP 表项检查功能可以控制设备上是否可以学习 ARP 报文中的发送端 MAC 地址为组播 MAC 的动态 ARP 表项。

开启 ARP 表项的检查功能后，设备上不能学习 ARP 报文中发送端 MAC 地址为组播 MAC 的动态 ARP 表项，也不能手工添加 MAC 地址为组播 MAC 的静态 ARP 表项。

关闭 ARP 表项的检查功能后，设备可以学习以太网源 MAC 地址为单播 MAC 且 ARP 报文中发送端 MAC 地址为组播 MAC 的动态 ARP 表项，也可以手工添加 MAC 地址为组播 MAC 的静态 ARP 表项。

【举例】

开启动态 ARP 表项的检查功能。

```
<Sysname> system-view
[Sysname] arp check enable
```

1.1.2 arp check log enable

arp check log enable 命令开启 ARP 日志信息功能。

undo arp check log enable 命令关闭 ARP 日志信息功能。

【命令】

```
arp check log enable
undo arp check log enable
```


【缺省情况】

设备 ARP 日志信息功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

ARP 日志可以方便管理员定位问题和解决问题，对处理 ARP 报文的信息进行的记录，包括设备未使能 ARP 代理功能时收到目的 IP 不是设备接口 IP 地址、VRRP 备份组的虚拟 IP 地址；收到的 ARP 报文中源地址和接收接口地址、VRRP 备份组中的虚拟 IP 地址冲突，且此报文不是 ARP 请求报文等。

设备生成的 ARP 日志信息会交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

为了防止设备输出过多的 ARP 日志信息而影响设备性能，除了审计或定位问题，一般情况下建议不要打开此功能。

【举例】

```
# 开启 ARP 日志信息功能。
<Sysname> system-view
[Sysname] arp check log enable
```

1.1.3 arp max-learning-num

arp max-learning-num 命令用来配置接口允许学习动态 ARP 表项的最大数目。

undo arp max-learning-num 命令用来恢复缺省情况。

【命令】

```
arp max-learning-num max-number [ alarm alarm-threshold ]
undo arp max-learning-num
```

【缺省情况】

各系列产品接口允许学习的动态 ARP 表项最大数目为：

- S5130S-SI、S5120V2-SI 系列交换机为 2048 个；
- S5130S-LI、S5120V2-LI、S3100V3-SI 系列交换机为 1024 个；
- S5110V2-SI、S5000V3-EI、S5000E-X 系列交换机为 128 个。

【视图】

二层以太网接口视图

二层聚合接口视图

VLAN 接口视图

【缺省用户角色】

network-admin

【参数】

max-number: 接口允许学习动态 ARP 表项的最大数目。各系列产品接口允许学习的动态 ARP 表项最大数目的取值范围为:

- S5130S-SI、S5120V2-SI 系列交换机为 0~2048 个;
- S5130S-LI、S5120V2-LI、S3100V3-SI 系列交换机为 0~1024 个;
- S5110V2-SI、S5000V3-EI、S5000E-X 系列交换机为 0~128 个。

alarm alarm-threshold: 设置动态 ARP 表项数量的告警阈值。**alarm-threshold** 的取值范围为 1~100, 单位为百分比。当接口学到的动态 ARP 表项数到达 ($max-number \times alarm-threshold/100$) 时, 设备会生成日志信息。如果未指定本参数, 设备不会生成日志信息。

【使用指导】

设备可以通过 ARP 协议自动生成动态 ARP 表项。为了防止部分接口下的用户占用过多的 ARP 资源, 可以通过设置接口学习动态 ARP 表项的最大数目来进行限制。当接口学习动态 ARP 表项的数目达到所设置的值时, 该接口将不再学习动态 ARP 表项。

当配置接口允许学习动态 ARP 表项的最大数目为 0 时, 表示禁止接口学习动态 ARP 表项。

【举例】

配置 VLAN 接口 40 上可以学习动态 ARP 表项的最大数目为 10。

```
<Sysname> system-view
[Sysname] interface vlan-interface 40
[Sysname-Vlan-interface40] arp max-learning-num 10
```

配置接口 GigabitEthernet1/0/1 上可以学习动态 ARP 表项的最大数目为 10。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp max-learning-num 10
```

配置二层聚合接口 1 上可以学习动态 ARP 表项的最大数目为 10。

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] arp max-learning-num 10
```

1.1.4 arp max-learning-number

arp max-learning-number 命令用来配置设备允许学习动态 ARP 表项的最大数目。

undo arp max-learning-number 命令用来恢复缺省情况。

【命令】

```
arp max-learning-number max-number slot slot-number
undo arp max-learning-number slot slot-number
```

【缺省情况】

各系列产品设备允许学习的动态 ARP 表项最大数目为:

- S5130S-SI、S5120V2-SI 系列交换机为 2048 个;
- S5130S-LI、S5120V2-LI、S3100V3-SI 系列交换机为 1024 个;
- S5110V2-SI、S5000V3-EI、S5000E-X 系列交换机为 128 个。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

max-number: 设备允许学习动态 ARP 表项的最大数目。各系列产品设备允许学习的动态 ARP 表项最大数目的取值范围为:

- S5130S-SI、S5120V2-SI 系列交换机为 0~2048 个;
- S5130S-LI、S5120V2-LI、S3100V3-SI 系列交换机为 0~1024 个;
- S5110V2-SI、S5000V3-EI、S5000E-X 系列交换机为 0~128 个。

slot slot-number: 设置指定成员设备上学习动态 ARP 表项的最大数目, *slot-number* 表示设备在 IRF 中的成员编号。

【使用指导】

设备可以通过 ARP 协议自动生成动态 ARP 表项。为了防止用户占用过多的 ARP 资源, 可以通过设置设备学习动态 ARP 表项的最大数目来进行限制。当设备学习动态 ARP 表项的数目达到所设置的值时, 该设备将不再学习动态 ARP 表项。

当配置设备允许学习动态 ARP 表项的最大数目为 0 时, 表示禁止该设备学习动态 ARP 表项。

【举例】

限制 Slot1 上学习的 ARP 表项的最大数目为 64。

```
<Sysname> system-view
[Sysname] arp max-learning-number 64 slot 1
```

1.1.5 arp multiport

arp multiport 命令用来配置多端口 ARP 表项。

undo arp 命令用来删除 ARP 表项。

【命令】

```
arp multiport ip-address mac-address vlan-id
undo arp ip-address
```

【缺省情况】

不存在多端口 ARP 表项。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ip-address: ARP 表项的 IP 地址部分。

mac-address: ARP 表项的 MAC 地址部分, 格式为 H-H-H。

vlan-id: 多端口 ARP 表项所属的 VLAN，取值范围为 1~4094。*vlan-id* 必须是用户已经创建好的 VLAN 的 ID。

【使用指导】

当多端口 ARP 表项所对应的 VLAN 或 VLAN 接口被删除时，该表项需删除。

用户需要先配置多端口单播 MAC 地址表项或组播 MAC 地址表项来指定所有的出接口，这两种 MAC 地址表项需要和多端口 ARP 表项有相同的 MAC 地址和 VLAN ID，且保证多端口 ARP 表项中 IP 地址与 VLAN 虚接口的 IP 地址属于同一网段，此时该多端口 ARP 表项才能正常指导转发。

【举例】

配置一条多端口 ARP 表项，IP 地址为 202.38.10.2，对应的 MAC 地址为 00e0-fc01-0000，此条 ARP 表项属于 VLAN 10。

```
<Sysname> system-view
[Sysname] arp multiport 202.38.10.2 00e0-fc01-0000 10
```

【相关命令】

- **display arp multiport**
- **reset arp multiport**

1.1.6 arp smooth

arp smooth 命令用来触发一次将 IRF 主设备的 ARP 表项同步到其他所有 IRF 从设备的操作。

【命令】

```
arp smooth
```

【视图】

用户视图

【缺省用户角色】

network-admin

【举例】

触发一次将 IRF 主设备的 ARP 表项同步到其他所有 IRF 从设备的操作。

```
<Sysname> arp smooth
```

1.1.7 arp static

arp static 命令用来配置静态 ARP 表项。

undo arp 命令用来删除 ARP 表项。

【命令】

```
arp static ip-address mac-address [ vlan-id interface-type  
interface-number ]  
undo arp ip-address
```

【缺省情况】

不存在静态 ARP 表项。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ip-address: ARP 表项的 IP 地址部分。

mac-address: ARP 表项的 MAC 地址部分，格式为 H-H-H。

vlan-id: 静态 ARP 表项所属的 VLAN，取值范围为 1~4094。

interface-type interface-number: 指定接口类型和接口编号。

【使用指导】

静态 ARP 表项通过手工配置和维护，不会被老化，不会被动态 ARP 表项覆盖，可以增加通信的安全性。

静态 ARP 表项分为短静态 ARP 表项和长静态 ARP 表项：

- 对于已经解析的短静态 ARP 表项，会由于外部事件，比如解析到的出接口状态 **down** 或者 *vlan-id* 所对应的 VLAN 和 VLAN 接口被删除等原因，恢复到未解析状态。
- 对于长静态 ARP 表项，根据设备的当前状态可能处于有效或无效两种状态。处于无效状态的原因可能是该 ARP 表项对应的 VLAN 接口状态 **down** 或出接口状态 **down**、该 ARP 表项中的 IP 地址与本地 IP 地址冲突或设备上没有与该 ARP 表项中的 IP 地址在同一网段的接口地址等原因。处于无效状态的长静态 ARP 表项不能指导报文转发。

指定 *vlan-id interface-type interface-number* 参数时，需要注意：

- *interface-type interface-number* 可以为以太网接口或聚合接口。
- *vlan-id* 所对应的 VLAN 和 VLAN 接口必须存在，接口 *interface-type interface-number* 必须属于此 VLAN。
- *vlan-id* 对应的 VLAN 接口的 IP 地址必须和 *ip-address* 属于同一网段。
- *vlan-id* 所对应的 VLAN 和 VLAN 接口被删除时，长静态 ARP 表项则会被删除。

【举例】

配置一条长静态 ARP 表项，IP 地址为 202.38.10.2，对应的 MAC 地址为 00e0-fc01-0000，此条 ARP 表项对应的出接口为属于 VLAN 10 的接口 GigabitEthernet1/0/1。

```
<Sysname> system-view
```

```
[Sysname] arp static 202.38.10.2 00e0-fc01-0000 10 gigabitethernet 1/0/1
```

【相关命令】

- **display arp**
- **reset arp**

1.1.8 arp timer aging

arp timer aging 命令用来配置动态 ARP 表项的老化时间。

undo arp timer aging 命令用来恢复缺省情况。

【命令】

```
arp timer aging { aging-minutes | second aging-seconds }  
undo arp timer aging
```

【缺省情况】

动态 ARP 表项的老化时间为 20 分钟。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

aging-minutes: 以分钟形式表示的动态 ARP 表项的老化时间，取值范围为 1~1440，单位为分钟。

second aging-seconds: 以秒形式表示的动态 ARP 表项的老化时间，取值范围为 5~86400，单位为秒。

【使用指导】

为适应网络的变化，ARP 表需要不断更新。ARP 表中的动态 ARP 表项并非永远有效，每一条记录都有一个生存周期，到达生存周期仍得不到刷新的记录将被从 ARP 表中删除，这个生存周期被称作老化时间。如果在到达老化时间前记录被刷新，则重新计算老化时间。

配置代理 ARP 功能后，应该减小动态 ARP 表项的老化时间，以尽快使无效动态 ARP 表项失效，减少发给设备而设备却不能转发的报文，以尽快删除无效的动态 ARP 表项。

【举例】

配置动态 ARP 表项的老化时间为 10 分钟。

```
<Sysname> system-view  
[Sysname] arp timer aging 10
```

配置动态 ARP 表项的老化时间为 200 秒。

```
<Sysname> system-view  
[Sysname] arp timer aging second 200
```

【相关命令】

- **display arp timer aging**

1.1.9 display arp

display arp 命令用来显示 ARP 表项。

【命令】

```
display arp [ [ all | dynamic | multiport | static ] [ slot slot-number ] | vlan  
vlan-id | interface interface-type interface-number ] [ count | verbose ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

all: 显示所有的 ARP 表项。

dynamic: 显示动态 ARP 表项。

multiport: 显示多端口 ARP 表项。

static: 显示静态 ARP 表项。

slot slot-number: 显示指定成员设备的 ARP 表项。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示主设备上的 ARP 表项。

vlan vlan-id: 显示指定 VLAN 的 ARP 表项，*vlan-id* 的取值范围为 1~4094。

interface interface-type interface-number: 显示指定接口的 ARP 表项。*interface-type interface-number* 用来指定接口类型和接口编号。如果未指定本参数，则显示所有接口的 ARP 表项。

count: 显示 ARP 表项的数目。

verbose: 显示 ARP 表项的详细信息。

【使用指导】

使用本命令可以查看静态、动态和多端口 ARP 表项的具体内容，包括 IP 地址、MAC 地址、VLAN ID、出接口、表项类型以及老化时间等信息。

【举例】

对于 Release 6126P09 版本：

显示所有 ARP 表项的信息。

```
<Sysname> display arp all
      Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport   I-Invalid
IP Address      MAC Address      VID      Interface/Link ID      Aging Type
1.1.1.1         02e0-f102-0023   1        GE1/0/1                N/A    S
1.1.1.2         00e0-fc00-0001  12        GE1/0/2                960    D
```

显示所有 ARP 表项的详细信息。

```
<Sysname> display arp all verbose
      Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport   I-Invalid
IP Address      : 1.1.1.1          VID : 1          Aging   : N/A
MAC Address     : 02e0-f102-0023   Type: S          Nickname: 0x0000
Interface/Link ID: GE1/0/1
VPN Instance    : [No Vrf]
VXLAN ID       : N/A
VSI Name       : N/A
VSI Interface  : N/A

IP Address      : 1.1.1.2          VID : 12         Aging   : 960 sec
MAC Address     : 0015-e944-adc5   Type: D          Nickname: 0x0000
Interface/Link ID: GE1/0/2
VPN Instance    : [No Vrf]
```

VXLAN ID : N/A
VSI Name : N/A
VSI Interface : N/A

显示所有 ARP 表项的数目。

```
<Sysname> display arp all count
Total number of entries : 4
```

表1-1 display arp 命令显示信息描述表(适用于 Release 6126P09 版本)

字段	描述
IP Address	ARP表项的IP地址
MAC Address	ARP表项的MAC地址
VID	(暂不支持VSI) ARP表项所属的VLAN ID或VSI Index (虚拟交换实例索引) (当表项类型为静态表项时, “N/A”表示未解析的短静态ARP表项; 如果ARP表项中的接口不属于某个VLAN或VSI, 也显示 “N/A”)
Interface/Link ID	ARP表项所对应的出接口或出链路标识符(当表项类型为静态表项时, “N/A”表示未解析的短静态ARP表项; 当表项类型为多端口表项时, “N/A”表示ARP表项不持有端口信息, 需要参考对应的多端口MAC地址)
Aging	ARP表项的老化时间, 对于静态ARP表项, 本字段取值为 “N/A”, 表示没有老化时间; 对于动态ARP表项, 取值包括: <ul style="list-style-type: none"> 具体老化时间值, 单位为秒 “N/A”表示老化时间不可知
Type	ARP表项类型: 动态, 用D表示; 静态, 用S表示; OpenFlow, 用O表示; Rule, 用R表示; 多端口, 用M表示; 无效, 用I表示
NickName	(暂不支持) ARP表项的NickName (长度为4的十六进制数字, 例如012a)
VPN Instance	(暂不支持) VPN实例名称, [No Vrf]表示未配置相应ARP的VPN实例
VXLAN ID	(暂不支持) ARP表项对应的VXLAN ID, 又称VNI (VXLAN网络标识符)。 “N/A”表示该表项不属于任何VXLAN
VSI Name	(暂不支持) ARP表项的VSI的名称, N/A表示该表项不属于VSI
VSI Interface	(暂不支持) 与VSI关联的VSI虚接口, 如果未指定VSI关联的VSI虚接口, 则显示 “N/A”
Total number of entries	ARP表项数目

对于 Release 6126P12 及以上版本:

显示所有 ARP 表项的信息。

```
<Sysname> display arp all
Type: S-Static D-Dynamic O-Openflow R-Rule M-Multiport I-Invalid
IP address      MAC address     VLAN/VSI      Interface/Link ID      Aging Type
1.1.1.1         02e0-f102-0023 1              GE1/0/1                --      S
1.1.1.2         00e0-fc00-0001 12             GE1/0/2                960     D
1.1.1.3         00e0-fe50-6503 12             Tunnel1                960     D
1.1.1.4         000d-88f7-9f7d 12             0x1                    960     D
```

显示所有 ARP 表项的详细信息。

```
<Sysname> display arp all verbose
```



```

IP address      : 1.1.1.1          MAC address    : 02e0-f102-0023
Type           : Static           Aging          : --
Interface      : GE1/0/1         VLAN           : 1
VPN instance   : --
Link ID        : --
VXLAN ID       : --
VSI name       : --
VSI interface  : --
Nickname       : 0x0000

```

```

IP address      : 1.1.1.2          MAC address    : 0015-e944-adc5
Type           : Static           Aging          : 960 sec
Interface      : GE1/0/2         VLAN           : 12
VPN instance   : --
Link ID        : --
VXLAN ID       : --
VSI name       : --
VSI interface  : --
Nickname       : 0x0000

```

```

IP address      : 1.1.1.3          MAC address    : 0013-1234-0001
Type           : Dynamic          Aging          : 960 sec
Interface      : Tunnell         VLAN           : 12
VPN instance   : --
Link ID        : --
VXLAN ID       : --
VSI name       : vpna
VSI interface  : Vsi1
Nickname       : 0x0000

```

```

IP address      : 1.1.1.4          MAC address    : 0012-1234-0002
Type           : Dynamic          Aging          : 960 sec
Interface      : --              VLAN           : 12
VPN instance   : --
Link ID        : 0x1
VXLAN ID       : --
VSI name       : vpna
VSI interface  : Vsi1
Nickname       : 0x0000

```

显示所有 ARP 表项的数目。

```

<Sysname> display arp all count
Total number of entries : 4

```

表1-2 display arp 命令显示信息描述表（适用于 Release 6126P12 及以上版本）

字段	描述
IP address	ARP表项的IP地址
MAC address	ARP表项的MAC地址

字段	描述
VLAN/VSI	（暂不支持VSI）ARP表项所属的VLAN ID或VSI Index（虚拟交换实例索引） （当表项类型为静态表项时，“--”表示未解析的短静态ARP表项；如果ARP表项中的接口不属于某个VLAN或VSI，也显示“--”）
Interface	ARP表项所对应的出接口（当表项类型为静态表项时，“--”表示未解析的短静态ARP表项；当表项类型为多端口表项时，“--”表示ARP表项不持有端口信息，需要参考对应的多端口MAC地址）
Link ID	出链路标识符，如果ARP表项不属于VSI，则显示为“--”
Aging	ARP表项的老化时间，对于静态ARP表项，本字段取值为“--”，表示没有老化时间；对于动态ARP表项，取值包括： <ul style="list-style-type: none"> • 具体老化时间值，单位为秒 • “--”表示老化时间不可知
Type	ARP表项类型：动态，用D表示；静态，用S表示；OpenFlow，用O表示；Rule，用R表示；多端口，用M表示；无效，用I表示
VPN instance	（暂不支持）VPN实例名称，“--”表示未配置相应ARP的VPN实例
VXLAN ID	（暂不支持）ARP表项对应的VXLAN ID，又称VNI（VXLAN网络标识符）。 “--”表示该表项不属于任何VXLAN
VSI name	（暂不支持）ARP表项的VSI的名称，“--”表示该表项不属于VSI
VSI interface	（暂不支持）与VSI关联的VSI虚接口，如果未指定VSI关联的VSI虚接口，则显示“--”
Nickname	（暂不支持）ARP表项的NickName（长度为4的十六进制数字，例如012a）
Total number of entries	ARP表项数目

【相关命令】

- `arp static`
- `reset arp`

1.1.10 display arp entry-limit

`display arp entry-limit` 命令用来显示设备支持 ARP 表项的最大数目。

【命令】

`display arp entry-limit`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

显示设备支持 ARP 表项的最大数目。

```
<Sysname> display arp entry-limit
ARP entries: 512
```

1.1.11 display arp ip-address

display arp ip-address 命令用来显示指定 IP 地址的 ARP 表项。

【命令】

```
display arp ip-address [ slot slot-number ] [ verbose ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

ip-address: 显示指定 IP 地址的 ARP 表项。

slot slot-number: 显示指定成员设备的 ARP 表项。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示主设备上的 ARP 表项。

verbose: 显示 ARP 表项的详细信息。

【使用指导】

用户可以通过本命令查看指定 IP 地址的 ARP 表项的具体内容,包括 IP 地址、MAC 地址、VLAN ID、出接口、表项类型以及老化时间等信息。

【举例】

显示 IP 地址为 20.1.1.1 的 ARP 表项的信息。(适用于 Release 6126P09 版本)

```
<Sysname> display arp 20.1.1.1
Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport   I-Invalid
IP Address      MAC Address      VID      Interface/Link ID      Aging Type
20.1.1.1        00e0-fc00-0001   N/A      N/A                    N/A      S
```

显示 IP 地址为 20.1.1.1 的 ARP 表项的信息。(适用于 Release 6126P12 及以上版本)

```
<Sysname> display arp 20.1.1.1
Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport   I-Invalid
IP address      MAC address      VLAN/VSI      Interface/Link ID      Aging Type
20.1.1.1        00e0-fc00-0001  --            --                    --        S
```

【相关命令】

- **arp static**
- **reset arp**

1.1.12 display arp openflow count

display arp openflow count 命令用来显示 OpenFlow 类型 ARP 表项个数。

【命令】

```
display arp openflow count [ slot slot-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot slot-number: 显示指定成员设备的 OpenFlow 类型 ARP 表项个数。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示主设备上的 OpenFlow 类型 ARP 表项个数。

【举例】

```
# 显示 OpenFlow 类型 ARP 表项个数。
<Sysname> display arp openflow count
Total number of OpenFlow ARP entries: 6
```

1.1.13 display arp timer aging

display arp timer aging 命令用来显示动态 ARP 表项的老化时间。

【命令】

display arp timer aging

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【使用指导】

不论通过 **arp timer aging** 命令配置的老化时间使用哪种时间单位，本命令显示的老化时间单位均为秒。

【举例】

```
# 显示动态 ARP 表项的老化时间。
<Sysname> display arp timer aging
Current ARP aging time is 1200 seconds
以上显示信息表示动态 ARP 表项的缺省老化时间为 1200 秒。
```

【相关命令】

- **arp timer aging**

1.1.14 reset arp

reset arp 命令用来清除 ARP 表项。

【命令】

```
reset arp { all | dynamic | interface interface-type interface-number |  
multiport | slot slot-number | static }
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

all: 表示清除所有的 ARP 表项。

dynamic: 表示清除动态 ARP 表项。

multiport: 表示清除多端口 ARP 表项。

static: 表示清除静态 ARP 表项。

slot *slot-number*: 表示清除指定成员设备的 ARP 表项。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则清除主设备上的 ARP 表项。

interface *interface-type interface-number*: 表示清除指定接口的 ARP 表项。*interface-type interface-number* 用来指定接口的类型和编号。如果未指定本参数，则清除所有接口的 ARP 表项。

【举例】

清除静态 ARP 表项。

```
<Sysname> reset arp static
```

【相关命令】

- **arp static**
- **display arp**

2 免费ARP

2.1 免费ARP配置命令

2.1.1 arp ip-conflict log prompt

arp ip-conflict log prompt 命令用来开启源 IP 地址冲突提示功能。

undo arp ip-conflict log prompt 命令用来关闭源 IP 地址冲突提示功能。

【命令】

```
arp ip-conflict log prompt
undo arp ip-conflict log prompt
```

【缺省情况】

源 IP 地址冲突提示功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

设备接收到其它设备发送的 ARP 报文后，如果发现报文中的源 IP 地址和自己的 IP 地址相同，该设备会根据当前源 IP 地址冲突提示功能的状态，进行如下处理：

- 如果源 IP 地址冲突提示功能处于关闭状态时，设备发送一个免费 ARP 报文确认是否冲突，如果收到对应的 ARP 应答后才提示存在 IP 地址冲突。
- 如果源 IP 地址冲突提示功能处于开启状态时，设备立刻提示存在 IP 地址冲突。

【举例】

在设备上开启源 IP 地址冲突提示功能。

```
<Sysname> system-view
[Sysname] arp ip-conflict log prompt
```

2.1.2 arp send-gratuitous-arp

arp send-gratuitous-arp 命令用来在接口上开启定时发送免费 ARP 功能。

undo arp send-gratuitous-arp 命令用来关闭定时发送免费 ARP 功能。

【命令】

```
arp send-gratuitous-arp [ interval interval ]
undo arp send-gratuitous-arp
```

【缺省情况】

定时发送免费 ARP 功能处于关闭状态。

【视图】

VLAN 接口视图

【缺省用户角色】

network-admin

【参数】

interval interval: 发送免费 ARP 报文的时间间隔，取值范围为 200~200000，单位为毫秒，缺省值为 2000。

【使用指导】

配置本命令后，只有当接口链路状态 up 并且配置 IP 地址后，此功能才真正生效。

只能为接口主 IP 地址和手工配置的从 IP 地址发送免费 ARP。主 IP 地址可以是手工配置或者通过其他方式获取的，但是从 IP 地址必须是手工配置的。

如果修改了免费 ARP 报文的发送时间间隔，则在下一个发送时间间隔才能生效。

如果同时在很多接口下开启本功能，或者每个接口有大量的从 IP 地址，或者两种情况共存的同时又配置很小的发送时间间隔，那么免费 ARP 报文的实际发送时间间隔可能会远远高于用户设定的时间间隔。

【举例】

在 VLAN 接口 2 上开启定时发送免费 ARP 功能，发送免费 ARP 报文的时间间隔为 300 毫秒。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp send-gratuitous-arp interval 300
```

2.1.3 gratuitous-arp mac-change retransmit

gratuitous-arp mac-change retransmit 命令用来配置当接口 MAC 地址变化时，重新发送免费 ARP 报文的次数和时间间隔。

undo gratuitous-arp mac-change retransmit 命令用来恢复缺省情况。

【命令】

```
gratuitous-arp mac-change retransmit times interval seconds
undo gratuitous-arp mac-change retransmit
```

【缺省情况】

当设备的接口 MAC 地址变化时，该接口只会发送一次免费 ARP 报文。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

times: 重发免费 ARP 报文的次数，取值范围为 1~10。

interval seconds: 重发免费 ARP 报文的时间间隔，*seconds* 取值范围为 1~10，单位为秒。

【使用指导】

当设备的 MAC 地址发生变化后,设备会通过免费 ARP 报文将修改后的 MAC 地址通告给其他设备。由于目前免费 ARP 报文没有重传机制,其他设备可能无法收到免费 ARP 报文。为了解决这个问题,用户可以配置当接口 MAC 地址变化时,该接口重新发送免费 ARP 报文的次数和时间间隔,保证其他设备可以收到该免费 ARP 报文。

执行本命令后,设备会按照指定的时间间隔重发免费 ARP 报文,直到到达配置的发送次数为止。

【举例】

配置当接口 MAC 地址变化时,该接口重新发送 3 次免费 ARP 报文,重新发送免费 ARP 报文时间间隔为 5 秒。

```
<Sysname> system-view  
[Sysname] gratuitous-arp mac-change retransmit 3 interval 5
```


2.1.4 gratuitous-arp-learning enable

gratuitous-arp-learning enable 命令用来开启免费 ARP 报文的学习功能。

undo gratuitous-arp-learning enable 命令用来关闭免费 ARP 报文学习功能。

【命令】

```
gratuitous-arp-learning enable
undo gratuitous-arp-learning enable
```

【缺省情况】

免费 ARP 报文的学习功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

开启免费 ARP 报文学习功能后，设备会根据收到的免费 ARP 报文中携带的信息对自身维护的 ARP 表进行修改（新建或者更新 ARP 表项）。

关闭免费 ARP 报文学习功能后，设备不会根据收到的免费 ARP 报文来新建 ARP 表项，但是会更新已存在的对应 ARP 表项。如果用户不希望通过免费 ARP 报文来新建 ARP 表项，可以关闭免费 ARP 报文学习功能，以节省 ARP 表项资源。

【举例】

```
# 开启免费 ARP 报文的学习功能。
<Sysname> system-view
[Sysname] gratuitous-arp-learning enable
```

2.1.5 gratuitous-arp-sending enable

gratuitous-arp-sending enable 命令用来开启设备收到非同一网段的 ARP 请求时发送免费 ARP 报文功能。

undo gratuitous-arp-sending enable 命令用来关闭设备收到非同一网段的 ARP 请求时发送免费 ARP 报文功能。

【命令】

```
gratuitous-arp-sending enable
undo gratuitous-arp-sending enable
```

【缺省情况】

设备收到非同一网段的 ARP 请求时发送免费 ARP 报文功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【举例】

关闭设备收到非同一网段的 ARP 请求时发送免费 ARP 报文功能。

```
<Sysname> system-view
```

```
[Sysname] undo gratuitous-arp-sending enable
```

3 代理ARP

3.1 代理ARP配置命令

3.1.1 display local-proxy-arp

display local-proxy-arp 命令用来显示本地代理 ARP 的状态。

【命令】

display local-proxy-arp [**interface** *interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface interface-type interface-number: 显示指定接口的本地代理 ARP 的状态。
interface-type interface-number 指定接口类型和接口编号。如果未指定本参数，则显示所有接口的本地代理 ARP 的状态。

【使用指导】

使用本命令可以查看本地代理 ARP 是处于开启（enabled）状态还是关闭（disabled）状态。

【举例】

显示 VLAN 接口 2 的本地代理 ARP 状态。

```
<Sysname> display local-proxy-arp interface vlan-interface 2
Interface Vlan-interface2
Local Proxy ARP status: enabled
```

【相关命令】

- **local-proxy-arp enable**

3.1.2 display proxy-arp

display proxy-arp 命令用来显示代理 ARP 的状态。

【命令】

display proxy-arp [**interface** *interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

interface *interface-type* *Interface-number*: 显示指定接口的代理 ARP 的状态。
interface-type interface-number 用来指定接口类型和接口编号。如果未指定本参数，则显示所有接口的代理 ARP 的状态。

【使用指导】

使用本命令可以查看代理 ARP 是处于开启（enabled）状态还是关闭（disabled）状态。

【举例】

显示 VLAN 接口 2 的代理 ARP 状态。

```
<Sysname> display proxy-arp interface vlan-interface 2
Interface Vlan-interface2
Proxy ARP status: disabled
```

【相关命令】

- **proxy-arp enable**

3.1.3 local-proxy-arp enable

local-proxy-arp enable 命令用来开启本地代理 ARP 功能。

undo local-proxy-arp enable 命令用来关闭本地代理 ARP 功能。

【命令】

```
local-proxy-arp enable [ ip-range start-ip-address to end-ip-address ]
undo local-proxy-arp enable
```

【缺省情况】

本地代理 ARP 功能处于关闭状态。

【视图】

VLAN 接口视图

【缺省用户角色】

network-admin

【参数】

ip-range *start-ip-address to end-ip-address*: 配置对指定 IP 地址范围进行本地代理 ARP。
start-ip-address 表示起始 IP 地址。*end-ip-address* 表示结束 IP 地址。
start-ip-address 必须小于等于 *end-ip-address*。

【使用指导】

如果 ARP 请求是从一个网络的主机发往同一网段却不在同一物理网络上的另一台主机，那么连接它们的具有代理 ARP 功能的设备就可以回答该请求，这个过程称作代理 ARP（Proxy ARP）。

代理 ARP 功能屏蔽了分离的物理网络这一事实，使用户使用起来，好像在同一个物理网络上。

代理 ARP 分为普通代理 ARP 和本地代理 ARP，二者的应用场景有所区别：

- 普通代理 ARP 的应用场景为：想要互通的主机分别连接到设备的不同三层接口上，且这些主机不在同一个广播域中。
- 本地代理 ARP 的应用场景为：想要互通的主机连接到设备的同一个三层接口上，且这些主机不在同一个广播域中。

需要注意的是，多次执行本命令配置不同的 IP 地址范围进行本地代理 ARP 时，最后一次执行的命令生效。

【举例】

在 VLAN 接口 2 上开启本地代理 ARP 功能。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] local-proxy-arp enable
```

在 VLAN 接口 2 上开启本地代理 ARP 功能，并指定进行 ARP 代理的 IP 地址范围。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] local-proxy-arp enable ip-range 1.1.1.1 to 1.1.1.20
```

【相关命令】

- **display local-proxy-arp**

3.1.4 proxy-arp enable

proxy-arp enable 命令用来开启代理 ARP 功能。

undo proxy-arp enable 命令用来关闭代理 ARP 功能。

【命令】

```
proxy-arp enable
undo proxy-arp enable
```

【缺省情况】

代理 ARP 功能处于关闭状态。

【视图】

VLAN 接口视图

【缺省用户角色】

network-admin

【使用指导】

如果 ARP 请求是从一个网络的主机发往同一网段却不在同一物理网络上的另一台主机，那么连接它们的具有代理 ARP 功能的设备就可以回答该请求，这个过程称作代理 ARP（Proxy ARP）。

代理 ARP 功能屏蔽了分离的物理网络这一事实，使用户使用起来，好像在同一个物理网络上。

代理 ARP 分为普通代理 ARP 和本地代理 ARP，二者的应用场景有所区别：

- 普通代理 ARP 的应用场景为：想要互通的主机分别连接到设备的不同三层接口上，且这些主机不在同一个广播域中。

- 本地代理 ARP 的应用场景为：想要互通的主机连接到设备的同一个三层接口上，且这些主机不在同一个广播域中。

【举例】

在 VLAN 接口 2 上开启代理 ARP。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] proxy-arp enable
```

【相关命令】

- **display proxy-arp**

4 ARP Snooping

4.1 ARP Snooping配置命令

4.1.1 arp snooping enable

arp snooping enable 命令用来开启 ARP Snooping 功能。

undo arp snooping enable 命令用来关闭 ARP Snooping 功能。

【命令】

```
arp snooping enable
undo arp snooping enable
```

【缺省情况】

ARP Snooping 功能处于关闭状态。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

【举例】

开启 VLAN 2 下的 ARP Snooping 功能。

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] arp snooping enable
```

4.1.2 display arp snooping

display arp snooping 命令用来显示 ARP Snooping 表项。

【命令】

```
display arp snooping [ vlan vlan-id ] [ slot slot-number ] [ count ]
display arp snooping ip ip-address [ slot slot-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

vlan *vlan-id*: 显示指定 VLAN 的 ARP Snooping 表项。*vlan-id* 的取值范围为 1~4094。

count: 显示当前 ARP Snooping 表项的计数。

ip ip-address: 显示指定 IP 地址的 ARP Snooping 表项。

slot slot-number: 显示指定成员设备上的所有 ARP Snooping 表项。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示主设备上的 ARP Snooping 表项。

【举例】

```
# 显示 VLAN 2 下的 ARP Snooping 表项。
<Sysname> display arp snooping vlan 2
IP Address    MAC Address    VLAN ID Interface  Aging    Status
3.3.3.3       0003-0003-0003 2           GE1/0/1    20       Valid
3.3.3.4       0004-0004-0004 2           GE1/0/2    5        Invalid

# 显示当前 ARP Snooping 表项的计数。
<Sysname> display arp snooping count
Total entries: 2
```

表4-1 display arp snooping 命令显示信息描述表

字段	描述
IP Address	ARP Snooping表项的IP地址
MAC Address	ARP Snooping表项的MAC地址
VLAN ID	ARP Snooping表项所属的VLAN ID
Interface	ARP Snooping表项所对应的入接口
Aging	ARP Snooping表项的老化时间，单位为分钟。当显示N/A时，表示当前成员设备不是创建ARP Snooping表项的端口所在的成员设备
Status	ARP Snooping表项的状态，分为以下三种： <ul style="list-style-type: none">Valid: 有效Invalid: 无效Collision: 冲突
Total entries	ARP Snooping表项数目

【相关命令】

- reset arp snooping**

4.1.3 reset arp snooping

reset arp snooping 命令用来清除 ARP Snooping 表项。

【命令】

```
reset arp snooping [ ip ip-address | vlan vlan-id ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

ip *ip-address*: 清除指定 IP 地址的 ARP Snooping 表项。

vlan *vlan-id*: 清除指定 VLAN 的 ARP Snooping 表项。*vlan-id* 的取值范围为 1~4094。

【使用指导】

如果未指定参数，则清除所有的 ARP Snooping 表项。

【举例】

清除 VLAN 2 下的 ARP Snooping 表项。

```
<Sysname> reset arp snooping vlan 2
```

【相关命令】

- **display arp snooping**

5 ARP直连路由通告

5.1 ARP直连路由通告配置命令

5.1.1 arp route-direct advertise

`arp route-direct advertise` 命令用来开启 ARP 直连路由通告功能。

`undo arp route-direct advertise` 命令用来关闭 ARP 直连路由通告功能。

【命令】

```
arp route-direct advertise
undo arp route-direct advertise
```

【缺省情况】

ARP 直连路由通告功能处于关闭状态。

【视图】

VLAN 接口视图

【缺省用户角色】

network-admin

【举例】

在 VLAN 接口 10 下开启 ARP 直连路由通告功能。

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] arp route-direct advertise
```

目 录

1 IP地址	1-1
1.1 IP地址配置命令	1-1
1.1.1 display ip interface	1-1
1.1.2 display ip interface brief	1-3
1.1.3 ip address	1-5
1.1.4 ip address unnumbered	1-6

1 IP地址

1.1 IP地址配置命令

1.1.1 display ip interface

display ip interface 命令用来显示三层接口与 IP 相关的配置和统计信息。

【命令】

display ip interface [*interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface-type interface-number: 显示指定接口的相关信息。如果未指定本参数，则显示所有三层接口的 IP 相关的配置和统计信息。

【使用指导】

display ip interface 命令用来查看三层接口与 IP 相关的配置和统计信息，包括接口上接收和发送的单播报文数、字节数和组播报文数，以及接口上收到的 TTL 无效报文数和 ICMP 报文数等。通过对显示信息中报文收发情况的分析，可以初步判断网络是否遭到攻击和攻击的可能来源。

【举例】

显示 VLAN 接口 10 与 IP 相关的配置和统计信息。

```
<Sysname> display ip interface vlan-interface 10
Vlan-interface10 current state: DOWN
Line protocol current state: DOWN
Internet Address is 1.1.1.1/8 Primary
Broadcast address: 1.255.255.255
The Maximum Transmit Unit: 1500 bytes
input packets : 0, bytes : 0, multicasts : 0
output packets : 0, bytes : 0, multicasts : 0
TTL invalid packet number:          0
ICMP packet input number:           0
  Echo reply:                       0
  Unreachable:                      0
  Source quench:                    0
  Routing redirect:                  0
  Echo request:                     0
  Router advert:                     0
  Router solicit:                    0
```

```

Time exceed:          0
IP header bad:        0
Timestamp request:    0
Timestamp reply:      0
Information request:  0
Information reply:     0
Netmask request:      0
Netmask reply:        0
Unknown type:         0

```

表1-1 display ip interface 命令显示信息描述表

字段	描述
current state	<p>接口当前的物理状态，可能的状态及含义如下：</p> <ul style="list-style-type: none"> • Administratively DOWN: 表示该接口已经通过 shutdown 命令被关闭，即管理状态为关闭 • DOWN: 该接口的管理状态为开启，但物理状态为关闭（可能因为未连接好或者线路故障） • UP: 该接口的管理状态和物理状态均为开启
Line protocol current state	<p>接口数据链路层协议状态，可能的状态及含义如下：</p> <ul style="list-style-type: none"> • DOWN: 表示接口的数据链路层协议状态为关闭 • UP: 表示接口的数据链路层协议状态为开启 • UP (spoofing): 该接口的协议状态为欺骗性开启，即虽然接口的链路层协议状态显示是开启的，但实际可能没有对应的链路，或者所对应的链路不是永久存在而是按需建立的
Internet Address	<p>接口的IP地址，IP地址后可携带如下参数：</p> <ul style="list-style-type: none"> • Primary: 表示手动配置的主 IP 地址 • Sub: 表示手动配置的从 IP 地址 • Unnumbered: 表示借用 IP 地址 • DHCP-Allocated: 表示 DHCP 动态分配 IP 地址 • BOOTP-Allocated: 表示 BOOTP 动态分配 IP 地址 • Mad: 表示 MAD IP 地址
Broadcast address	接口所在网段的广播地址
The Maximum Transmit Unit	接口的最大传输单元，单位为字节
input packets, bytes, multicasts output packets, bytes, multicasts	接口上接收和发送的所有报文数、字节数以及组播报文数（设备启动后就开始统计此信息）
TTL invalid packet number	接口上收到的TTL无效的报文个数（设备启动后就开始统计此信息）

字段	描述
ICMP packet input number:	接口上收到的ICMP报文的总数（设备启动后就开始统计此信息），包括如下报文：
Echo reply:	• Echo 应答报文
Unreachable:	• 不可达报文
Source quench:	• 源站抑制报文
Routing redirect:	• 路由重定向报文
Echo request:	• Echo 请求报文
Router advert:	• 路由器通告报文
Router solicit:	• 路由器请求报文
Time exceed:	• 超时报文
IP header bad:	• IP 报文头错误报文
Timestamp request:	• 时间戳请求报文
Timestamp reply:	• 时间戳响应报文
Information request:	• 信息请求报文
Information reply:	• 信息响应报文
Netmask request:	• 掩码请求报文
Netmask reply:	• 掩码响应报文
Unknown type:	• 未知类型报文

【相关命令】

- **display ip interface brief**
- **ip address**

1.1.2 display ip interface brief

display ip interface brief 命令用来显示三层接口与 IP 相关的简要信息。

【命令】

```
display ip interface [ interface-type [ interface-number ] ] brief
[ description ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface-type: 显示指定类型接口的 IP 基本配置信息。如果未指定本参数，则显示所有三层接口与 IP 相关的简要信息。

interface-number: 显示指定接口的 IP 基本配置信息。如果未指定本参数，则显示该类型所有三层接口的与 IP 相关的简要信息。

description: 显示接口完整的描述信息。如果未指定本参数，则最多可以显示 13 个字符，如果超过 13 个字符，那么则显示前 10 个字符和 “...”。

【使用指导】

display ip interface brief 命令用来查看三层接口与 IP 相关的简要信息，包括接口的物理和链路层协议状态、IP 地址、描述信息等。

【举例】

显示 VLAN 接口的基本配置信息。

```
<Sysname> display ip interface vlan-interface brief
*down: administratively down
(s): spoofing (l): loopback
Interface          Physical Protocol IP address      VPN instance Description
Vlan10             down      down      6.6.6.1        --          Link to Co...

<Sysname> display ip interface vlan-interface brief description
*down: administratively down
(s): spoofing (l): loopback
Interface          Physical Protocol IP address      VPN instance Description
Vlan10             down      down      6.6.6.1        --          Link to CoreR
                                                Outer
```

表1-2 display ip interface brief 命令显示信息描述表

字段	描述
*down: administratively down	接口处于管理down状态，即采用 shutdown 命令关闭了该接口
(s) : spoofing	接口的欺骗属性，即接口的链路层协议状态显示是up的，但实际可能没有对应的链路，或者所对应的链路不是永久存在而是按需建立的
Interface	接口的名称
Physical	接口的物理状态，可能的状态及含义如下： <ul style="list-style-type: none">• *down: 表示该接口已经通过 shutdown 命令被关闭，即管理状态为关闭• down: 该接口的管理状态为开启，但物理状态为关闭（可能因为未连接好或者线路故障）• up: 该接口的管理状态和物理状态均为开启
Protocol	接口的链路层协议状态，可能的状态及含义如下： <ul style="list-style-type: none">• down: 该接口的协议状态为关闭• down(l): 该接口的协议状态为 loopback down• up: 该接口的协议状态为开启• up(l): 该接口的协议状态为 loopback up• up(s): 该接口的协议状态为 spoofing up
IP address	接口的IP地址（如果未配置则显示 “--” ）
VPN instance	（暂不支持）接口所属的VPN实例名称，该属性列最多可以显示12个字符，如果超过12个字符，那么则显示前9个字符和 “...” 。（如果未配置则显示 “--” ）

字段	描述
Description	接口的描述信息，该属性列最多可以显示13个字符，如果超过13个字符，那么则显示前10个字符和“...”。（如果未配置则显示“--”）

【相关命令】

- **display ip interface**
- **ip address**

1.1.3 ip address

ip address 命令用来配置接口的 IP 地址。

undo ip address 命令用来删除接口的 IP 地址。

【命令】

ip address *ip-address* { *mask-length* | *mask* } [**sub**]

undo ip address *ip-address* { *mask-length* | *mask* } [**sub**]

【缺省情况】

未配置接口 IP 地址。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ip-address: 接口的 IP 地址，为点分十进制格式。

mask-length: 子网掩码长度，即掩码中连续“1”的个数，取值范围为 1~31，当接口为 LoopBack 接口时，取值范围为 1~32。

mask: 接口 IP 地址相应的子网掩码，为点分十进制格式。

sub: 表示该地址为接口的从 IP 地址。

【使用指导】

ip address 命令用来配置接口的 IP 地址。设备的每个接口可以配置多个 IP 地址，其中一个为主 IP 地址，其余为从 IP 地址。一般情况下，一个接口只需配置一个主 IP 地址，有时为了实现一个接口下的多个子网之间能够通信，需要在接口上配置从 IP 地址。

当配置主 IP 地址时，如果接口上已经有主 IP 地址，则新配置的地址将覆盖原有的主 IP 地址，成为新的主 IP 地址。

当接口被配置为通过 BOOTP 或 DHCP 动态获取或借用其他接口的 IP 地址后，不能再给该接口配置从 IP 地址。

undo ip address 命令中不指定任何参数表示删除该接口的所有 IP 地址。**undo ip address** *ip-address* { *mask* | *mask-length* } 表示删除主 IP 地址。**undo ip address** *ip-address* { *mask* | *mask-length* } **sub** 表示删除指定的从 IP 地址。

同一接口的主、从 IP 地址可以在同一网段，但不同接口之间的 IP 地址不可以在同一网段。

【举例】

指定 VLAN 接口 10 的主 IP 地址为 129.12.0.1，从 IP 地址为 202.38.160.1，子网掩码都为 255.255.255.0。

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ip address 129.12.0.1 255.255.255.0
[Sysname-Vlan-interface10] ip address 202.38.160.1 255.255.255.0 sub
```

【相关命令】

- **display ip interface**
- **display ip interface brief**

1.1.4 ip address unnumbered

ip address unnumbered 命令用来配置本接口借用指定接口的 IP 地址。

undo ip address unnumbered 命令用来恢复缺省情况。

【命令】

```
ip address unnumbered interface interface-type interface-number
undo ip address unnumbered
```

【缺省情况】

本接口未借用其它接口的 IP 地址。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

interface *interface-type interface-number*: 被借用接口的接口类型及接口编号。

【使用指导】

所谓“IP 地址借用”，是指一个接口上未配置 IP 地址，但为了使该接口能正常使用，就向同一设备上其它有 IP 地址的接口借用一个 IP 地址。

IP 地址借用的使用场景如下：

- 在 IP 地址资源比较匮乏的环境下，为了节约 IP 地址资源，可以配置某个接口借用其他接口的 IP 地址。
- 如果某个接口只是偶尔使用，可以配置该接口借用其他接口的 IP 地址，而不必让其一直占用一个单独的 IP 地址。

Loopback 接口的 IP 地址可被其它接口借用，但本身不能借用其它接口的地址。

一个接口的地址可以借给多个接口。如果被借用接口有多个手动配置的 IP 地址，则只有手动配置的主 IP 地址能被借用。

由于借用方接口本身没有 IP 地址，无法在此接口上启用动态路由协议。所以必须手动配置一条到对端网段的静态路由，才能实现设备间的连通。

【举例】

配置 VLAN 接口 10 借用 VLAN 接口 100 的 IP 地址。

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 10
```

```
[Sysname-Vlan-interface10] ip address unnumbered interface vlan-interface 100
```

目 录

1 DHCP	1-1
1.1 DHCP公共命令	1-1
1.1.1 dhcp client-detect	1-1
1.1.2 dhcp dscp	1-1
1.1.3 dhcp enable	1-2
1.1.4 dhcp log enable	1-3
1.1.5 dhcp select	1-3
1.2 DHCP服务器配置命令	1-4
1.2.1 address range	1-4
1.2.2 bims-server	1-5
1.2.3 bootfile-name	1-6
1.2.4 class ip-pool	1-7
1.2.5 class option-group	1-8
1.2.6 class range	1-9
1.2.7 default ip-pool	1-10
1.2.8 dhcp apply-policy	1-11
1.2.9 dhcp class	1-12
1.2.10 dhcp option-group	1-12
1.2.11 dhcp policy	1-13
1.2.12 dhcp server always-broadcast	1-14
1.2.13 dhcp server apply ip-pool	1-15
1.2.14 dhcp server bootp ignore	1-15
1.2.15 dhcp server bootp reply-rfc-1048	1-16
1.2.16 dhcp server database filename	1-17
1.2.17 dhcp server database update interval	1-18
1.2.18 dhcp server database update now	1-19
1.2.19 dhcp server database update stop	1-20
1.2.20 dhcp server forbidden-ip	1-20
1.2.21 dhcp server ip-pool	1-21
1.2.22 dhcp server ping packets	1-22
1.2.23 dhcp server ping timeout	1-23
1.2.24 dhcp server relay information enable	1-24
1.2.25 display dhcp server conflict	1-24

1.2.26 display dhcp server database	1-25
1.2.27 display dhcp server expired.....	1-26
1.2.28 display dhcp server free-ip	1-27
1.2.29 display dhcp server ip-in-use	1-28
1.2.30 display dhcp server pool	1-29
1.2.31 display dhcp server statistics	1-31
1.2.32 dns-list.....	1-33
1.2.33 domain-name.....	1-34
1.2.34 expired	1-35
1.2.35 forbidden-ip	1-36
1.2.36 gateway-list	1-36
1.2.37 if-match	1-37
1.2.38 ip-in-use threshold.....	1-40
1.2.39 nbns-list.....	1-41
1.2.40 netbios-type.....	1-42
1.2.41 network.....	1-43
1.2.42 next-server	1-44
1.2.43 option	1-44
1.2.44 reset dhcp server conflict	1-46
1.2.45 reset dhcp server expired	1-46
1.2.46 reset dhcp server ip-in-use.....	1-47
1.2.47 reset dhcp server statistics.....	1-47
1.2.48 static-bind	1-48
1.2.49 tftp-server domain-name.....	1-49
1.2.50 tftp-server ip-address	1-50
1.2.51 valid class	1-51
1.2.52 verify class	1-51
1.2.53 voice-config	1-52
1.3 DHCP中继配置命令	1-53
1.3.1 dhcp relay check mac-address	1-53
1.3.2 dhcp relay check mac-address aging-time.....	1-54
1.3.3 dhcp relay client-information record	1-54
1.3.4 dhcp relay client-information refresh	1-55
1.3.5 dhcp relay client-information refresh enable.....	1-56
1.3.6 dhcp relay dhcp-server timeout.....	1-57
1.3.7 dhcp relay gateway	1-58

1.3.8 dhcp relay information circuit-id.....	1-58
1.3.9 dhcp relay information enable.....	1-60
1.3.10 dhcp relay information remote-id	1-61
1.3.11 dhcp relay information strategy	1-62
1.3.12 dhcp relay master-server switch-delay	1-63
1.3.13 dhcp relay release ip.....	1-63
1.3.14 dhcp relay server-address algorithm.....	1-64
1.3.15 dhcp relay source-address	1-65
1.3.16 dhcp smart-relay enable	1-66
1.3.17 dhcp-server timeout.....	1-66
1.3.18 display dhcp relay check mac-address.....	1-67
1.3.19 display dhcp relay client-information.....	1-68
1.3.20 display dhcp relay information.....	1-69
1.3.21 display dhcp relay server-address.....	1-70
1.3.22 display dhcp relay statistics	1-71
1.3.23 gateway-list	1-73
1.3.24 master-server switch-delay	1-74
1.3.25 remote-server.....	1-74
1.3.26 remote-server algorithm	1-75
1.3.27 reset dhcp relay client-information	1-76
1.3.28 reset dhcp relay statistics.....	1-76
1.4 DHCP客户端配置命令	1-77
1.4.1 dhcp client dad enable	1-77
1.4.2 dhcp client dscp	1-78
1.4.3 dhcp client identifier	1-78
1.4.4 display dhcp client	1-79
1.4.5 ip address dhcp-alloc.....	1-81
1.5 DHCP Snooping配置命令.....	1-82
1.5.1 dhcp snooping binding database filename	1-82
1.5.2 dhcp snooping binding database update interval	1-84
1.5.3 dhcp snooping binding database update now.....	1-85
1.5.4 dhcp snooping binding record.....	1-85
1.5.5 dhcp snooping check mac-address.....	1-86
1.5.6 dhcp snooping check request-message.....	1-87
1.5.7 dhcp snooping deny	1-87
1.5.8 dhcp snooping disable	1-88

1.5.9 dhcp snooping enable.....	1-88
1.5.10 dhcp snooping enable vlan.....	1-89
1.5.11 dhcp snooping information circuit-id	1-90
1.5.12 dhcp snooping information enable	1-91
1.5.13 dhcp snooping information remote-id.....	1-92
1.5.14 dhcp snooping information strategy.....	1-93
1.5.15 dhcp snooping log enable	1-94
1.5.16 dhcp snooping max-learning-num	1-95
1.5.17 dhcp snooping rate-limit	1-96
1.5.18 dhcp snooping trust	1-96
1.5.19 dhcp snooping trust interface.....	1-97
1.5.20 display dhcp snooping binding	1-98
1.5.21 display dhcp snooping binding database	1-99
1.5.22 display dhcp snooping information	1-100
1.5.23 display dhcp snooping packet statistics.....	1-101
1.5.24 display dhcp snooping trust.....	1-102
1.5.25 reset dhcp snooping binding.....	1-103
1.5.26 reset dhcp snooping packet statistics	1-104
1.6 BOOTP客户端配置命令	1-104
1.6.1 display bootp client	1-104
1.6.2 ip address bootp-alloc.....	1-105

1 DHCP

1.1 DHCP公共命令

1.1.1 dhcp client-detect

dhcp client-detect 命令用来开启 DHCP 服务器或 DHCP 中继的用户下线探测功能。

undo dhcp client-detect 命令用来关闭 DHCP 服务器或 DHCP 中继的用户下线探测功能。

【命令】

```
dhcp client-detect
undo dhcp client-detect
```

【缺省情况】

DHCP 服务器或 DHCP 中继的用户下线探测功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

【使用指导】

DHCP 服务器开启该功能后，当设备上的 ARP 表项老化时，DHCP 服务器认为该表项对应的 DHCP 客户端已经下线，DHCP 服务器会删除对应的 IP 地址租约。

DHCP 中继开启该功能后，当设备上的 ARP 表项老化时，DHCP 中继认为该表项对应的 DHCP 客户端已经下线，DHCP 中继会删除对应的用户地址表项，并通过发 Release 报文通知 DHCP 服务器删除下线用户的 IP 地址租约。

【举例】

```
# 开启用户下线探测功能。
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp client-detect
```

1.1.2 dhcp dscp

dhcp dscp 命令用来配置 DHCP 服务器或 DHCP 中继发送 DHCP 报文的 DSCP 优先级。

undo dhcp dscp 命令用来恢复缺省情况。

【命令】

```
dhcp dscp dscp-value
undo dhcp dscp
```

【缺省情况】

DHCP 服务器或 DHCP 中继发送 DHCP 报文的 DSCP 优先级为 56。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

dscp-value: DHCP 报文的 DSCP 优先级，取值范围为 0~63。

【使用指导】

DSCP 优先级用来体现报文自身的优先等级，决定报文传输的优先程度。配置的 DSCP 优先级的取值越大，报文的优先级越高。

【举例】

```
# 配置 DHCP 服务器或 DHCP 中继发送的 DHCP 报文的 DSCP 优先级为 30。
<Sysname> system-view
[Sysname] dhcp dscp 30
```

1.1.3 dhcp enable

dhcp enable 命令用来开启 DHCP 服务。

undo dhcp enable 命令用来关闭 DHCP 服务。

【命令】

```
dhcp enable
undo dhcp enable
```

【缺省情况】

DHCP 服务处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

只有开启 DHCP 服务后，其它相关的 DHCP 配置才能生效。

配置 DHCP 服务器和 DHCP 中继时，都需要先开启 DHCP 服务。

【举例】

```
# 开启 DHCP 服务。
<Sysname> system-view
[Sysname] dhcp enable
```


1.1.4 dhcp log enable

dhcp log enable 命令用来开启 DHCP 服务器日志信息功能。

undo dhcp log enable 命令用来关闭 DHCP 服务器日志信息功能。

【命令】

```
dhcp log enable
undo dhcp log enable
```

【缺省情况】

DHCP 服务器日志信息功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

DHCP 服务器日志可以方便管理员定位问题和解决问题。设备生成 DHCP 日志信息会交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

比如大量 DHCP 客户端发生上下线操作时，DHCP 服务器会输出大量日志信息，这可能会降低设备性能，影响 DHCP 服务器分配 IP 地址的速度。为了避免该情况的发生，用户可以关闭 DHCP 服务器日志信息功能，使得 DHCP 服务器不再输出日志信息。

【举例】

开启 DHCP 服务器日志信息功能。

```
<Sysname> system-view
[Sysname] dhcp log enable
```

1.1.5 dhcp select

dhcp select 命令用来配置接口工作在 DHCP 服务器或 DHCP 中继模式。

undo dhcp select 命令用来取消接口工作在 DHCP 服务器或 DHCP 中继模式，即接口将丢弃 DHCP 客户端发来的 DHCP 报文。

【命令】

```
dhcp select { relay [ proxy ] | server }
undo dhcp select { relay | server }
```

【缺省情况】

接口工作在 DHCP 服务器模式，即当接口收到 DHCP 客户端发来的 DHCP 报文时，将从 DHCP 服务器的地址池中分配地址等参数。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

relay: 配置接口工作在 DHCP 中继模式。

proxy: 配置接口工作在 DHCP 代理模式。

server: 配置接口工作在 DHCP 服务器模式。

【使用指导】

接口从 DHCP 服务器模式切换到 DHCP 中继模式后，设备不会删除 IP 地址绑定信息，也不会删除相应的授权 ARP 表项。这些表项可能会与 DHCP 中继新生成的 ARP 表项冲突。因此，建议接口从 DHCP 服务器模式切换到 DHCP 中继模式之前，通过 **reset dhcp server ip-in-use** 命令清除已有的 IP 地址绑定信息。

当接口工作在 DHCP 代理模式时，如果收到 DHCP 客户端发来的 DHCP 报文，将报文转发给 DHCP 服务器，由 DHCP 服务器为 DHCP 客户端分配地址等参数；如果转发 DHCP 服务器发来的应答报文，把报文中的 DHCP 服务器地址修改为中继接口地址。

【举例】

配置 VLAN 接口 2 工作在 DHCP 中继模式。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] dhcp select relay
```

【相关命令】

- **dhcp relay server-address**
- **dhcp relay source-address**
- **dhcp smart-relay enable**
- **reset dhcp server ip-in-use**

1.2 DHCP服务器配置命令



说明

S5110V2-SI、S5000V3-EI 和 S5000E-X 系列交换机不支持本特性。

1.2.1 address range

address range 命令用来配置地址池动态分配的 IP 地址范围。

undo address range 命令用来恢复缺省情况。

【命令】

```
address range start-ip-address end-ip-address
undo address range
```

【缺省情况】

未配置动态分配的 IP 地址范围。

【视图】

DHCP 地址池视图

【缺省用户角色】

network-admin

【参数】

start-ip-address: 动态分配范围的起始 IP 地址。

end-ip-address: 动态分配范围的结束 IP 地址。

【使用指导】

如果未通过本命令配置地址池动态分配的 IP 地址范围，则地址池下 **network** 命令指定的网段地址都可以分配给 DHCP 客户端；如果通过本命令配置了地址池动态分配的 IP 地址范围，则只能从本命令指定的 IP 地址范围内选择地址分配给客户端。

配置 **address range** 命令后，不能再通过 **network secondary** 命令在地址池中配置从网段。多次执行本命令，最后一次执行的命令生效。

address range 命令指定的地址范围应该在 **network** 命令指定的网段范围内，网段范围外的地址将无法被分配。

【举例】

配置地址池 1 动态分配的地址范围为 192.168.8.1 到 192.168.8.150。

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 1
[Sysname-dhcp-pool-1] address range 192.168.8.1 192.168.8.150
```

【相关命令】

- **class**
- **dhcp class**
- **display dhcp server pool**
- **network**

1.2.2 bims-server

bims-server 命令用来配置 DHCP 地址池为 DHCP 客户端分配的 BIMS 服务器 IP 地址、端口及共享密钥信息。

undo bims-server 命令用来恢复缺省情况。

【命令】

```
bims-server ip ip-address [ port port-number ] sharekey { cipher | simple } string
undo bims-server
```

【缺省情况】

未配置 DHCP 地址池为 DHCP 客户端分配的 BIMS 服务器信息。

【视图】

DHCP 地址池视图

【缺省用户角色】

network-admin

【参数】

ip ip-address: 指定 BIMS 服务器的 IP 地址。

port port-number: 指定 BIMS 服务器的端口号。*port-number* 为端口号,取值范围为 1~65534。

cipher: 以密文形式设置密钥。

simple: 以明文形式设置密钥,该密钥将以密文方式存储。

string: 密钥字符串,区分大小写。明文密钥为 1~16 个字符的字符串,密文密钥为 1~53 个字符的字符串。DHCP 客户端获取到 BIMS 服务器的信息后,与 BIMS 服务器通信时,采用共享密钥对传递的消息进行加密,以保证消息传递的安全性。

【使用指导】

多次执行本命令,最后一次执行的命令生效。

【举例】

配置 DHCP 地址池 0 为 DHCP 客户端分配的 BIMS 服务器的 IP 地址为 1.1.1.1,端口号为 80,共享密钥为 aabbcc。

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bims-server ip 1.1.1.1 port 80 sharekey simple aabbcc
```

【相关命令】

- **display dhcp server pool**

1.2.3 bootfile-name

bootfile-name 命令用来配置 DHCP 客户端使用的启动文件名或远程启动文件的 HTTP 形式 URL。

undo bootfile-name 命令用来恢复缺省情况。

【命令】

```
bootfile-name { bootfile-name | url }
undo bootfile-name
```

【缺省情况】

未配置 DHCP 客户端使用的启动文件名或远程启动文件的 HTTP 形式 URL。

【视图】

DHCP 地址池视图

【缺省用户角色】

network-admin

【参数】

bootfile-name: 启动文件名, 为 1~63 个字符的字符串, 区分大小写。

url: 远程启动文件的 HTTP 形式 URL, 为 1~63 个字符的字符串, 区分大小写。

【使用指导】

多次执行本命令, 最后一次执行的命令生效。

当启动文件在 TFTP 服务器上, 使用 *bootfile-name* 参数指定 DHCP 客户端使用的启动文件名;

当启动文件在 HTTP 服务器上, 使用 *url* 参数指定远程启动文件的 HTTP 形式 URL。

【举例】

配置 DHCP 地址池 0 为 DHCP 客户端分配的启动文件名为 boot.cfg。

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bootfile-name boot.cfg
```

配置 DHCP 地址池 0 为 DHCP 客户端分配的启动文件的 HTTP URL 为 http://10.1.1.1/boot.cfg。

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bootfile-name http://10.1.1.1/boot.cfg
```

【相关命令】

- **display dhcp server pool**
- **next-server**
- **tftp-server domain-name**
- **tftp-server ip-address**

1.2.4 class ip-pool

class ip-pool 命令用来指定 DHCP 用户类关联的 DHCP 地址池。

undo class ip-pool 命令删除为指定 DHCP 用户类关联的 DHCP 地址池。

【命令】

```
class class-name ip-pool pool-name
undo class class-name ip-pool
```

【缺省情况】

未指定 DHCP 用户类关联的 DHCP 地址池。

【视图】

DHCP 策略视图

【缺省用户角色】

network-admin

【参数】

class-name: DHCP 用户类名称, 为 1~63 个字符的字符串, 不区分大小写。
pool-name: DHCP 地址池名称, 为 1~63 个字符的字符串, 不区分大小写。

【使用指导】

对于一个 DHCP 用户类, 在一个 DHCP 策略中只能关联一个 DHCP 地址池。
多次执行本命令为同一个 DHCP 用户类关联不同的 DHCP 地址池, 最后一次执行的命令生效。

【举例】

在 DHCP 策略 1 中, 配置 DHCP 用户类 test 关联 DHCP 地址池 pool1。

```
<Sysname> system-view
[Sysname] dhcp policy 1
[Sysname-dhcp-policy-1] class test ip-pool pool1
```

【相关命令】

- **default ip-pool**
- **dhcp policy**
- **dhcp server ip-pool**

1.2.5 class option-group

class option-group 命令用来配置 DHCP 地址池下 DHCP 用户类和 DHCP 选项组的关联。
undo class option-group 命令用来删除 DHCP 地址池下 DHCP 用户类和 DHCP 选项组的关联。

【命令】

```
class class-name option-group option-group-number
undo class class-name option-group
```

【缺省情况】

未配置 DHCP 地址池的 DHCP 用户类和 DHCP 选项组的关联。

【视图】

DHCP 地址池视图

【缺省用户角色】

network-admin

【参数】

class-name: DHCP 用户类名称, 为 1~63 个字符的字符串, 不区分大小写。
option-group-number: DHCP 选项组编号, 取值范围为 1~32768。

【使用指导】

DHCP 服务器应答 DHCP 客户端报文时, 首先根据配置顺序逐个匹配通过 **class option-group** 命令指定的 DHCP 用户类。如果匹配成功, 则将该用户类对应的选项组中的选项填充到应答报文中; 如果同时匹配多个 DHCP 用户类, 且各用户类对应的选项组中有相同编号的选项, 以最先匹配到 DHCP 用户类对应的选项组中的选项为准。

需要注意的是，对于一个 DHCP 用户类，在一个 DHCP 地址池中只能指定一个选项组。多次执行本命令为同一个 DHCP 用户类指定不同的选项组，最后一次执行的命令生效。

【举例】

在 DHCP 地址池 0 中，配置 DHCP 用户类 user 和 DHCP 选项组 1 的关联。

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] class user option-group 1
```

【相关命令】

- **dhcp option-group**

1.2.6 class range

class range 命令用来配置 DHCP 地址池为指定 DHCP 用户类动态分配的 IP 地址范围。

undo class range 命令用来删除为指定 DHCP 用户类动态分配的 IP 地址范围。

【命令】

```
class class-name range start-ip-address end-ip-address
undo class class-name range
```

【缺省情况】

未配置为指定 DHCP 用户类动态分配的 IP 地址范围。

【视图】

DHCP 地址池视图

【缺省用户角色】

network-admin

【参数】

class-name: DHCP 用户类名称，为 1~63 个字符的字符串，不区分大小写。如果指定的 DHCP 用户类不存在，则为该用户类指定的地址范围不能分配给任何 DHCP 客户端。

start-ip-address: 动态分配范围的起始 IP 地址。

end-ip-address: 动态分配范围的结束 IP 地址。

【使用指导】

DHCP 服务器从地址池中选择地址分配给客户端时，首先根据配置顺序逐个匹配通过 **class range** 命令指定的 DHCP 用户类。如果匹配成功，则从为该用户类指定的地址范围内选择地址分配给 DHCP 客户端；如果该用户类中没有可供分配的地址，则继续匹配下一个用户类；如果所有匹配上的用户类地址范围都没有可供分配的地址，则从公共地址范围中选择地址分配给客户端；如果不匹配任何 DHCP 用户类，则会从地址池动态分配的 IP 地址范围（通过 **address range** 命令配置）中选择地址分配给 DHCP 客户端；如果 **address range** 命令指定的地址范围内也没有空闲地址，或者未配置 **address range** 命令，则地址分配失败，即 DHCP 服务器无法为 DHCP 客户端分配地址。

通过本配置可以实现将一个地址池下的地址范围划分成多个地址段，分别分配给属于不同 DHCP 用户类的 DHCP 客户端。

配置 **class range** 命令后，不能再通过 **network secondary** 命令在地址池中配置从网段。

配置 **class range** 命令后，只能从 **class range** 命令或 **address range** 命令指定的地址范围内选择地址分配给客户端。

一个地址池中只能为一个 DHCP 用户类指定一个地址范围。多次执行本命令为同一个 DHCP 用户类指定不同的地址范围，最后一次执行的命令生效。

一个地址池中可以为多个不同的 DHCP 用户类指定地址范围。

class range 命令指定的地址范围应该在 **network** 命令指定的主网段范围内，主网段范围外的地址将无法被分配。

【举例】

在地址池 1 中配置为 DHCP 用户类 user 动态分配的地址范围为 192.168.8.1 到 192.168.8.150。

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 1
[Sysname-dhcp-pool-1] class user range 192.168.8.1 192.168.8.150
```

【相关命令】

- **address range**
- **dhcp class**
- **display dhcp server pool**

1.2.7 default ip-pool

default ip-pool 命令用来指定默认 DHCP 地址池。

undo default ip-pool 命令用来恢复缺省情况。

【命令】

```
default ip-pool pool-name
undo default ip-pool
```

【缺省情况】

未指定默认 DHCP 地址池。

【视图】

DHCP 策略视图

【缺省用户角色】

network-admin

【参数】

pool-name：默认 DHCP 地址池名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

若匹配 DHCP 策略中的所有 DHCP 用户类失败，当配置了默认 DHCP 地址池时，则从该地址池中分配 IP 地址和其他参数；当未配置默认 DHCP 地址池或默认 DHCP 地址池中不存在可供分配的地址信息时，IP 地址和其他参数分配失败。

在一个 DHCP 策略视图中，只能配置一个默认 DHCP 地址池。多次执行本命令，最后一次执行的命令生效。

【举例】

在 DHCP 策略 1 中指定默认 DHCP 地址池 pool1。

```
<Sysname> system-view
[Sysname] dhcp policy 1
[Sysname-dhcp-policy-1] default ip-pool pool1
```

【相关命令】

- **class ip-pool**
- **dhcp policy**

1.2.8 dhcp apply-policy

dhcp apply-policy 命令用来指定接口引用的 DHCP 策略。

undo dhcp apply-policy 命令用来恢复缺省情况。

【命令】

```
dhcp apply-policy policy-name
undo dhcp apply-policy
```

【缺省情况】

接口未引用 DHCP 策略。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

policy-name: DHCP 策略名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

在一个接口上只能引用一条 DHCP 策略。在同一个接口上多次执行本命令，最后一次执行的命令生效。

【举例】

指定 VLAN 接口 10 引用的 DHCP 策略 test。

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp apply-policy test
```

【相关命令】

- **dhcp policy**

1.2.9 dhcp class

dhcp class 命令用来创建 DHCP 用户类并进入 DHCP 用户类视图，如果指定的 DHCP 用户类已存在，则直接进入用户类视图。

undo dhcp class 命令用来删除指定的 DHCP 用户类。

【命令】

```
dhcp class class-name
undo dhcp class class-name
```

【缺省情况】

不存在 DHCP 用户类。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

class-name: DHCP 用户类的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

在 DHCP 用户类视图下，可以通过 **if-match** 命令配置 DHCP 用户类的匹配规则，根据匹配规则判断 DHCP 客户端属于的 DHCP 用户类，从而实现灵活的用户分类策略。

【举例】

创建名称为 test 的 DHCP 用户类，并进入 DHCP 用户类视图。

```
<Sysname> system-view
[Sysname] dhcp class test
[Sysname-dhcp-class-test]
```

【相关命令】

- **address range**
- **class ip-pool**
- **class option-group**
- **class range**
- **dhcp policy**
- **if-match**

1.2.10 dhcp option-group

dhcp option-group 命令用来创建 DHCP 选项组并进入 DHCP 选项组视图，如果指定的 DHCP 选项组已存在，则直接进入 DHCP 选项组视图。

undo dhcp option-group 命令用来删除指定的 DHCP 选项组。

【命令】

```
dhcp option-group option-group-number
```

undo dhcp option-group *option-group-number*

【缺省情况】

不存在 DHCP 选项组。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

option-group-number: DHCP 选项组编号，取值范围为 1~32768。

【举例】

创建 DHCP 选项组 1 并进入该选项组视图。

```
<Sysname> system-view
[Sysname] dhcp option-group 1
[Sysname-dhcp-option-group-1]
```

【相关命令】

- **class option-group**
- **option**

1.2.11 dhcp policy

dhcp policy 命令用来创建 DHCP 策略，并进入 DHCP 策略视图。如果指定的 DHCP 策略已存在，则直接进入 DHCP 策略视图。

undo dhcp policy 命令用来删除已创建的 DHCP 策略。

【命令】

```
dhcp policy policy-name
undo dhcp policy policy-name
```

【缺省情况】

不存在 DHCP 策略。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

policy-name: DHCP 策略名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

在 DHCP 策略视图下，可以通过 **class ip-pool** 命令指定 DHCP 用户类关联的 DHCP 地址池，使匹配该 DHCP 用户类的客户端可以从关联的地址池中获取到 IP 地址和其他参数。

需要注意的是，需要配置 **dhcp apply-policy** 命令在接口上引用 DHCP 策略后，DHCP 策略才能生效。

【举例】

创建 DHCP 策略 test，并进入该 DHCP 策略视图。

```
<Sysname> system-view
[Sysname] dhcp policy test
[Sysname-dhcp-policy-test]
```

【相关命令】

- **class ip-pool**
- **default ip-pool**
- **dhcp apply-policy**
- **dhcp class**

1.2.12 dhcp server always-broadcast

dhcp server always-broadcast 命令用来开启 DHCP 服务器的广播回应报文功能。

undo dhcp server always-broadcast 命令用来恢复缺省情况。

【命令】

```
dhcp server always-broadcast
undo dhcp server always-broadcast
```

【缺省情况】

DHCP 服务器的广播回应报文功能处于关闭状态。DHCP 服务器根据请求报文中的广播标志位来决定以广播还是单播的形式发送应答报文。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

开启 DHCP 服务器的广播回应报文功能后，DHCP 服务器忽略请求报文中的广播标志位，以广播的形式发送应答报文。

当已经存在 IP 地址的客户端发出请求报文（即报文中 **ciaddr** 字段不为 0）时，无论是否开启 DHCP 服务器的广播回应报文功能，DHCP 服务器都会以单播形式将回应报文发送给 DHCP 客户端（即目的地址为 **ciaddr**）。

当请求报文通过 DHCP 中继转发到 DHCP 服务器（即报文中 **giaddr** 字段不为 0）时，无论是否开启 DHCP 服务器的广播回应报文功能，DHCP 服务器都会以单播形式将回应报文发送给 DHCP 中继（即目的地址为 **giaddr**）。

【举例】

开启 DHCP 服务器的广播回应报文功能。

```
<Sysname> system-view
```

```
[Sysname] dhcp server always-broadcast
```

1.2.13 dhcp server apply ip-pool

dhcp server apply ip-pool 命令用来指定接口引用的地址池。

undo dhcp server apply ip-pool 命令用来恢复缺省情况。

【命令】

```
dhcp server apply ip-pool pool-name
```

```
undo dhcp server apply ip-pool
```

【缺省情况】

接口未引用地址池。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

pool-name: DHCP 地址池名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

如果接口上配置了本命令，则接口接收到 DHCP 请求后，将优先为客户端分配静态绑定的 IP 地址；如果不存在静态绑定的 IP 地址，则从引用的地址池中选择 IP 地址分配给客户端。引用的地址池中不存在可供分配的 IP 地址时，设备无法为客户端分配 IP 地址。

接口上配置了 **dhcp server apply ip-pool** 命令后，如果接口引用的地址池不存在，则无法为客户端动态分配 IP 地址。

多次执行本命令，最后一次执行的命令生效。

【举例】

配置 VLAN 接口 2 引用 DHCP 地址池 0。

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 2
```

```
[Sysname-Vlan-interface2] dhcp server apply ip-pool 0
```

【相关命令】

- **dhcp server ip-pool**

1.2.14 dhcp server bootp ignore

dhcp server bootp ignore 命令用来配置 DHCP 服务器忽略 BOOTP 请求。

undo dhcp server bootp ignore 命令用来恢复缺省情况。

【命令】

```
dhcp server bootp ignore
```

```
undo dhcp server bootp ignore
```

【缺省情况】

DHCP 服务器不会忽略 BOOTP 请求。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

BOOTP 客户端申请到的地址的租约是无限期的。在特殊的组网环境中，可能不希望出现无限期的地址租约。此时，可以通过配置 DHCP 服务器忽略 BOOTP 请求报文，避免分配无限期的地址租约。

【举例】

配置 DHCP 服务器忽略 BOOTP 请求。

```
<Sysname> system-view
[Sysname] dhcp server bootp ignore
```

1.2.15 dhcp server bootp reply-rfc-1048

dhcp server bootp reply-rfc-1048 命令用来开启 DHCP 服务器回应 RFC 1048 格式报文功能。

undo dhcp server bootp reply-rfc-1048 命令用来关闭 DHCP 服务器回应 RFC 1048 格式报文功能。

【命令】

```
dhcp server bootp reply-rfc-1048
undo dhcp server bootp reply-rfc-1048
```

【缺省情况】

DHCP 服务器回应 RFC 1048 格式报文功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

有些 BOOTP 客户端发送的请求报文中，vend 字段的格式不符合 RFC 1048 的要求。对于这种报文，DHCP 服务器的缺省处理方法是不解析 vend 字段内容，将报文中 vend 字段的内容拷贝到回复报文中的 vend 字段回应给 BOOTP 客户端。

开启 DHCP 服务器的回应 RFC 1048 格式报文功能后，对于这种格式不符合 RFC 1048 要求的报文，DHCP 服务器会将需要回应的选项以符合 RFC 1048 要求的格式，封装到回复报文的 vend 字段，并回应给 BOOTP 客户端。

需要注意的是，该功能只在客户端通过 BOOTP 报文申请静态绑定地址时有效。

【举例】

开启 DHCP 服务器的回应 RFC 1048 格式报文功能。

```
<Sysname> system-view  
[Sysname] dhcp server bootp reply-rfc-1048
```

1.2.16 dhcp server database filename

dhcp server database filename 命令用来指定存储 DHCP 服务器表项的文件名称。

undo dhcp server database filename 命令用来恢复缺省情况。

【命令】

```
dhcp server database filename { filename | url url [ username username  
[ password { cipher | simple } string ] ] }  
undo dhcp server database filename
```

【缺省情况】

未指定存储 DHCP 服务器表项的文件名称。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

filename: 目标文件名，该配置用于本地存储模式。文件名取值范围的详细介绍，请参见“基础配置指导”中的“文件系统管理”。

url url: 配置远程目标文件 URL，为 1~255 个字符的字符串，区分大小写，该配置用于远程文件系统模式。此参数中不能包含用户名和密码，和参数 **username** 和 **string** 配合使用。

username username: 配置远程目标文件 URL 时的用户名，为 1~32 个字符的字符串，区分大小写。如果未指定本参数，则表示登录远程目标文件 URL 时无需使用用户名。

cipher: 表示以密文方式设置用户密码。

simple: 表示以明文方式设置用户密码，该密码将以密文形式存储。

string: 密码字符串，区分大小写。明文密码为 1~32 个字符的字符串，密文密码为 1~73 个字符的字符串。如果未指定本参数，则表示登录远程目标文件 URL 时无需使用密码。

【使用指导】

存储 DHCP 服务器表项时，如果设备中还不存在对应名称的文件，则设备会自动创建该文件。

执行本命令后，会立即触发一次表项备份。之后，如果未配置 **dhcp server database update interval** 命令，若表项发生变化，默认在 300 秒之后刷新存储文件；若表项未发生变化，则不再刷新存储文件。如果配置了 **dhcp server database update interval** 命令，若表项发生变化，则到达刷新时间间隔后刷新存储文件；若表项未发生变化，则不再刷新存储文件。

参数 **filename** 不支持远程目标文件 URL，配置远程目标文件 URL 请使用 **url**、**username**、**string** 配合使用。

频繁擦写本地存储介质可能会影响存储介质寿命,建议使用远程文件系统模式存储 DHCP 服务器表项文件。

当进行远程存储时,支持 FTP 和 TFTP 协议:

- 当采用 FTP 或 TFTP 协议时,服务器地址支持 IPv4 形式或 IPv6 形式,并且支持 DNS 域名方式。服务器地址为 IPv6 地址形式时需使用方括号(“[”和“]”)引用。配置服务器地址为 DNS 域名格式时请勿使用方括号引用。
- 当采用 FTP 协议时,URL 采用“ftp://服务器地址[:端口号]/文件路径”的形式,如有用户名和密码请分别使用参数 *username* 和参数 *string* 进行配置,用户名和密码必须和服务器上的配置一致,如果服务器只对用户名进行认证,则不用输入密码。
- 当采用 TFTP 协议时,URL 采用“tftp://服务器地址[:端口号]/文件路径”的形式。

【举例】

配置存储 DHCP 服务器表项的文件名为 database.dhcp。

```
<Sysname> system-view
```

```
[Sysname] dhcp server database filename database.dhcp
```

配置远程存储 DHCP 服务器表项至 IP 地址为 10.1.1.1 的 FTP 服务器工作目录下,用户名为 1, 密码为 1, 文件名为 database.dhcp。

```
<Sysname> system-view
```

```
[Sysname] dhcp server database filename url ftp://10.1.1.1/database.dhcp username 1 password simple 1
```

【相关命令】

- **dhcp server database update interval**
- **dhcp server database update now**
- **dhcp server database update stop**

1.2.17 dhcp server database update interval

dhcp server database update interval 命令用来配置刷新 DHCP 服务器表项存储文件的延迟时间。

undo dhcp server database update interval 命令用来恢复缺省情况。

【命令】

```
dhcp server database update interval interval
```

```
undo dhcp server database update interval
```

【缺省情况】

若 DHCP 服务器表项不变化,则不刷新表项存储文件;若 DHCP 服务器表项发生变化,默认在 300 秒后刷新表项存储文件。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval: 刷新延迟时间，取值范围为 60~864000，单位为秒。

【使用指导】

执行本命令后，当服务器表项发生变化后，DHCP 服务器开始计时，当本命令配置的延迟时间到达后，DHCP 服务器会把这个时间段内表项所有的变化信息备份到固化文件中。

如果未通过 **dhcp server database filename** 命令指定存储表项的文件，则本命令的配置不会生效。

【举例】

若 DHCP 服务器表项发生变化，在 10 分钟后刷新表项存储文件。

```
<Sysname> system-view
[Sysname] dhcp server database update interval 600
```

【相关命令】

- **dhcp server database filename**
- **dhcp server database update now**
- **dhcp server database update stop**

1.2.18 dhcp server database update now

dhcp server database update now 命令用来将当前 DHCP 服务器表项保存到用户指定的文件中。

【命令】

```
dhcp server database update now
```

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

本命令只用来触发一次 DHCP 服务器表项的备份。

如果未通过 **dhcp server database filename** 命令指定存储表项的文件，则本命令的配置不会生效。

【举例】

将当前的 DHCP 服务器表项保存到文件中。

```
<Sysname> system-view
[Sysname] dhcp server database update now
```

【相关命令】

- **dhcp server database filename**
- **dhcp server database update interval**
- **dhcp server database update stop**

1.2.19 dhcp server database update stop

dhcp server database update stop 命令用来终止当前的 DHCP 服务器表项恢复操作。

【命令】

dhcp server database update stop

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

本命令只用来触发一次终止 DHCP 服务器表项的恢复操作。

本命令只用来停止设备重启后从固化文件中恢复表项信息的过程，不影响除此之外的其他运行过程。当中断恢复表项信息的过程后，如果 DHCP 服务器分配了未恢复表项中的地址信息，可能会导致局域网设备地址冲突情况发生。

从固化文件恢复表项的连接超时的最长时间为 60 分钟，可以通过本命令立刻终止远程恢复。DHCP 服务器从固化文件中恢复表项的过程中，DHCP 服务器不会学习新的表项。

【举例】

终止当前的 DHCP 服务器表项恢复操作。

```
<Sysname> system-view
[Sysname] dhcp server database update stop
```

【相关命令】

- **dhcp server database filename**
- **dhcp server database update interval**
- **dhcp server database update now**

1.2.20 dhcp server forbidden-ip

dhcp server forbidden-ip 命令用来配置全局不参与自动分配的 IP 地址。

undo dhcp server forbidden-ip 命令用来取消全局不参与自动分配的 IP 地址的配置。

【命令】

```
dhcp server forbidden-ip start-ip-address [ end-ip-address ]
undo dhcp server forbidden-ip start-ip-address [ end-ip-address ]
```

【缺省情况】

未配置全局不参与自动分配的 IP 地址。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

start-ip-address: 不参与自动分配的起始 IP 地址。

end-ip-address: 不参与自动分配的结束 IP 地址，不能小于 *start-ip-address*。如果未指定本参数，则表示只有一个不参与自动分配的 IP 地址，即 *start-ip-address*；否则，表示 *start-ip-address* 到 *end-ip-address* 之间的 IP 地址均不能参与自动分配。

【使用指导】

某些服务器占用的 IP 地址（如网关地址、FTP 服务器地址），不能分配给 DHCP 客户端。通过本命令可以避免这些地址参与自动分配。

如果通过 **dhcp server forbidden-ip** 命令将已经静态绑定的 IP 地址配置为不参与自动分配的地址，则该地址仍然可以分配给静态绑定的用户。

执行 **undo dhcp server forbidden-ip** 命令取消不参与自动分配 IP 地址的配置时，指定的地址/地址范围必须与执行 **dhcp server forbidden-ip** 命令时指定的地址/地址范围保持一致。如果配置不参与自动分配的 IP 地址为某一地址范围，则只能同时取消该地址范围内所有 IP 地址的配置，不能单独取消其中某个 IP 地址的配置。

多次执行 **dhcp server forbidden-ip** 命令，可以配置多个不参与自动分配的 IP 地址段。

【举例】

配置 10.110.1.1 到 10.110.1.63 之间的 IP 地址不参与地址自动分配。

```
<Sysname> system-view
```

```
[Sysname] dhcp server forbidden-ip 10.110.1.1 10.110.1.63
```

【相关命令】

- **forbidden-ip**
- **static-bind**

1.2.21 dhcp server ip-pool

dhcp server ip-pool 命令用来创建 DHCP 地址池并进入 DHCP 地址池视图。如果已经创建了 DHCP 地址池，则直接进入该地址池视图。

undo dhcp server ip-pool 命令用来删除指定的地址池。

【命令】

```
dhcp server ip-pool pool-name
```

```
undo dhcp server ip-pool pool-name
```

【缺省情况】

不存在 DHCP 地址池。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

pool-name: DHCP 地址池名称, 是地址池的唯一标识, 为 1~63 个字符的字符串, 不区分大小写。

【使用指导】

在 DHCP 地址池下, 可以配置为 DHCP 客户端分配的 IP 地址、网关地址等参数。

【举例】

```
# 创建名称为 pool1 的 DHCP 地址池。
<Sysname> system-view
[Sysname] dhcp server ip-pool pool1
[Sysname-dhcp-pool-pool1]
```

【相关命令】

- `class ip-pool`
- `dhcp server apply ip-pool`
- `display dhcp server pool`

1.2.22 dhcp server ping packets

`dhcp server ping packets` 命令用来配置 DHCP 服务器发送 ICMP 回显请求报文的最大数目。

`undo dhcp server ping packets` 命令用来恢复缺省情况。

【命令】

```
dhcp server ping packets number
undo dhcp server ping packets
```

【缺省情况】

DHCP 服务器发送 ICMP 回显请求报文的最大数目为 1。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

number: 发送 ICMP 回显请求报文的最大数目, 取值范围为 0~10。0 表示 DHCP 服务器将 IP 地址分配给 DHCP 客户端之前, 不会通过 ping 操作探测该地址是否冲突。

【使用指导】

为防止 IP 地址重复分配导致地址冲突, DHCP 服务器为客户端分配地址前, 需要先对该地址进行探测。

DHCP 服务器的地址探测是通过 ping 功能实现的, 通过检测是否能在指定时间内得到 ping 响应来判断是否存在地址冲突。DHCP 服务器发送目的地址为待分配地址的 ICMP 回显请求报文。如果在指定时间内收到 ICMP 回显响应报文, 则认为存在地址冲突。DHCP 服务器从地址池中选择新的 IP 地址, 并重复上述操作。如果在指定时间内未收到 ICMP 回显响应报文, 则继续发送 ICMP 回显请

求报文，直到发送的 ICMP 回显请求报文数目达到本命令配置的最大值。如果仍然未收到 ICMP 回显响应报文，则将地址分配给客户端，从而确保客户端获得的 IP 地址唯一。

【举例】

配置 DHCP 服务器最多发送 10 个 ICMP 回显请求报文。

```
<Sysname> system-view
[Sysname] dhcp server ping packets 10
```

【相关命令】

- `dhcp server ping timeout`
- `display dhcp server conflict`
- `reset dhcp server conflict`

1.2.23 dhcp server ping timeout

`dhcp server ping timeout` 命令用来配置 DHCP 服务器等待 ICMP 回显响应报文的超时时间。

`undo dhcp server ping timeout` 命令用来恢复缺省情况。

【命令】

```
dhcp server ping timeout milliseconds
undo dhcp server ping timeout
```

【缺省情况】

DHCP 服务器等待 ICMP 回显响应报文的超时时间为 500 毫秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

milliseconds: 等待 ICMP 回显响应报文的超时时间，取值范围是 0~10000，单位为毫秒。0 表示 DHCP 服务器将 IP 地址分配给 DHCP 客户端之前，不会通过 ping 操作探测该地址是否冲突。

【使用指导】

为防止 IP 地址重复分配导致地址冲突，DHCP 服务器为客户端分配地址前，需要先对该地址进行探测。

DHCP 服务器的地址探测是通过 ping 功能实现的，通过检测是否能在指定时间内得到 ping 响应来判断是否存在地址冲突。DHCP 服务器发送目的地址为待分配地址的 ICMP 回显请求报文。如果在本命令指定的时间内收到 ICMP 回显响应报文，则认为存在地址冲突。DHCP 服务器从地址池中选择新的 IP 地址，并重复上述操作。如果在指定时间内未收到 ICMP 回显响应报文，则继续发送 ICMP 回显请求报文，直到发送的回显请求报文数目达到最大值。如果仍然未收到 ICMP 回显响应报文，则将地址分配给客户端，从而确保客户端获取的 IP 地址唯一。

【举例】

配置 DHCP 服务器等待 ICMP 回显响应报文的超时时间为 1000 毫秒。

```
<Sysname> system-view
[Sysname] dhcp server ping timeout 1000
```

【相关命令】

- `dhcp server ping packets`
- `display dhcp server conflict`
- `reset dhcp server conflict`

1.2.24 dhcp server relay information enable

`dhcp server relay information enable` 命令用来配置 DHCP 服务器处理 Option 82。

`undo dhcp server relay information enable` 命令用来配置 DHCP 服务器忽略 Option 82。

【命令】

```
dhcp server relay information enable
undo dhcp server relay information enable
```

【缺省情况】

DHCP 服务器处理 Option 82。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

当 DHCP 服务器收到含有 Option 82 的报文时，如果 DHCP 服务器处理 Option 82，则将请求报文中的 Option 82 原样复制到应答报文中；如果 DHCP 服务器忽略 Option 82，则不会在应答报文中携带 Option 82。

【举例】

配置 DHCP 服务器忽略 Option 82。

```
<Sysname> system-view
[Sysname] undo dhcp server relay information enable
```

1.2.25 display dhcp server conflict

`display dhcp server conflict` 命令用来显示 DHCP 的地址冲突信息。

【命令】

```
display dhcp server conflict [ ip ip-address ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

ip ip-address: 显示指定 IP 地址的地址冲突信息。如果未指定本参数，则显示所有的地址冲突信息。

【使用指导】

DHCP 服务器在下列几种情况下会生成地址冲突信息：

- DHCP 服务器在为客户端分配 IP 地址前，通过 ping 操作检测到网络中已有主机使用该地址。
- DHCP 客户端向 DHCP 服务器发送 Decline 报文，报告 DHCP 服务器为其分配的地址存在冲突。
- DHCP 服务器检测到地址池内的可供分配的地址是设备自身的地址。

【举例】

显示所有的地址冲突信息。

```
<Sysname> display dhcp server conflict
IP address      Detect time
4.4.4.1         Apr 25 16:57:20 2007
4.4.4.2         Apr 25 17:00:10 2007
```

表1-1 display dhcp server conflict 命令显示信息描述表

字段	描述
IP address	发生冲突的IP地址
Detect time	检测到冲突的时间

【相关命令】

- **reset dhcp server conflict**

1.2.26 display dhcp server database

display dhcp server database 命令用来显示 DHCP 服务器的表项备份信息。

【命令】

display dhcp server database

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

显示 DHCP 服务器的表项备份信息。

```
<Sysname> display dhcp server database
File name      : database.dhcp
Username       :
```

```

Password          :
Update interval   :    600 seconds
Latest write time  :    Feb  8 16:09:53 2014
Status            :    Last write succeeded.

```

表1-2 display dhcp server database 命令显示信息描述表

字段	描述
File name	存储DHCP服务器表项的文件名称
Username	配置远程目标文件时的用户名
Password	配置远程目标文件时的密码，有配置时显示为"*****"
Update interval	定期刷新表项存储文件的刷新时间间隔，单位为秒
Latest write time	最近一次写文件的时间
Status	<p>写文件的状态，即写文件是否成功</p> <ul style="list-style-type: none"> Writing: 正在写文件 Last write succeeded.: 上一次写文件成功 Last write failed.: 上一次写文件失败

1.2.27 display dhcp server expired

display dhcp server expired 命令用来显示租约过期的地址绑定信息。

【命令】

```
display dhcp server expired [ ip ip-address | pool pool-name ]
```

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator

```

【参数】

ip *ip-address*: 显示指定 IP 地址的租约过期地址绑定信息。如果未指定本参数，则显示所有 IP 地址的租约过期地址绑定信息。

pool *pool-name*: 显示指定地址池中租约过期的地址绑定信息。*pool-name* 表示地址池名称，为 1~63 个字符的字符串，不区分大小写。如果未指定本参数，则显示所有地址池中的租约过期地址绑定信息。

【使用指导】

在 DHCP 地址池的可用地址分配完后，租约过期的地址将被分配给 DHCP 客户端。

【举例】

显示所有租约过期的地址绑定信息。

```
<Sysname> display dhcp server expired
```


IP address	Client-identifier/Hardware address	Lease expiration
4.4.4.6	3030-3066-2e65-3230-302e-3130-3234-2d45-7468-6572-6e65-7430-2f31	Apr 25 17:10:47 2007

表1-3 display dhcp server expired 命令显示信息描述表

字段	描述
IP address	租约过期的IP地址
Client-identifier/Hardware address	租约过期的客户端ID或MAC地址
Lease expiration	租约过期的时间

【相关命令】

- **reset dhcp server expired**

1.2.28 display dhcp server free-ip

display dhcp server free-ip 命令用来显示 DHCP 地址池的空闲地址信息，即尚未分配给 DHCP 客户端的 IP 地址信息。

【命令】

display dhcp server free-ip [*pool pool-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

pool pool-name: 显示指定地址池的空闲地址信息。*pool-name* 表示地址池名称，为 1~63 个字符的字符串，不区分大小写。如果未指定本参数，则显示所有地址池的空闲地址信息。

【举例】

显示所有 DHCP 地址池的空闲地址信息。

```
<Sysname> display dhcp server free-ip
Pool name: 1
Network: 10.0.0.0 mask 255.0.0.0
  IP ranges from 10.0.0.10 to 10.0.0.100
  IP ranges from 10.0.0.105 to 10.0.0.255
Secondary networks:
  10.1.0.0 mask 255.255.0.0
    IP ranges from 10.1.0.0 to 10.1.0.255
  10.2.0.0 mask 255.255.0.0
    IP Ranges from 10.2.0.0 to 10.2.0.255
```

```
Pool name: 2
```

Network: 20.1.1.0 mask 255.255.255.0

IP ranges from 20.1.1.0 to 20.1.1.255

表1-4 display dhcp server free-ip 命令显示信息描述表

字段	描述
Pool name	地址池的名称
Network	可分配的地址网段
IP ranges	可分配的地址范围
Secondary networks	可分配的从地址网段

【相关命令】

- **address range**
- **dhcp server ip-pool**
- **network**

1.2.29 display dhcp server ip-in-use

display dhcp server ip-in-use 命令用来显示 DHCP 地址绑定信息。

【命令】

display dhcp server ip-in-use [**ip** *ip-address* | **pool** *pool-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

ip *ip-address*: 显示指定 IP 地址的地址绑定信息。如果未指定本参数，则显示所有 IP 地址的地址绑定信息。

pool *pool-name*: 显示指定地址池的地址绑定信息。*pool-name* 表示地址池名称，为 1~63 个字符的字符串，不区分大小写。如果未指定本参数，则显示所有地址池的地址绑定信息。

【使用指导】

当 DHCP 服务器作为 DHCP 客户端的网关设备时，DHCP 服务器上记录的该 DHCP 客户端的地址绑定信息才会提供给其他安全特性使用。

需要注意的是，如果租约的截止时间超过 2100 年，则显示为 After 2100。

【举例】

显示所有 DHCP 地址绑定信息。

```
<Sysname> display dhcp server ip-in-use
```

IP address	Client identifier/ Hardware address	Lease expiration	Type
------------	--	------------------	------

10.1.1.1	4444-4444-4444	Not used	Static(F)
10.1.1.2	3030-3030-2e30-3030- 662e-3030-3033-2d45- 7468-6572-6e65-74	May 1 14:02:49 2015	Auto(C)
10.1.1.3	1111-1111-1111	After 2100	Static(C)

表1-5 display dhcp server ip-in-use 命令显示信息描述表

字段	描述
IP address	分配给DHCP客户端的IP地址
Client identifier/Hardware address	客户端ID或客户端的硬件地址
Lease expiration	租约到期时间，取值包括： <ul style="list-style-type: none"> 具体的时间值（如 May 1 14:02:49 2015）：表示租约在该时间到期 Not used：表示静态绑定的地址尚未分配给特定客户端 Unlimited：表示租约为无限长 After 2100：表示租约过期时间超过 2100 年
Type	地址绑定的类型，取值包括： <ul style="list-style-type: none"> Static(F)：表示尚未分配给客户端的静态绑定，即静态无效绑定 Static(O)：服务器从地址池选择静态绑定的 IP 地址，并发送 DHCP-OFFER 报文为客户端提供该 IP 地址后产生该类型的地址绑定信息，即静态临时绑定 Static(C)：表示已经分配给客户端的静态绑定，即静态正式绑定 Auto(O)：表示动态绑定的临时租约，即从地址池中动态选择 IP 地址，并发送 DHCP-OFFER 报文为客户端提供该 IP 地址后，产生的租约 Auto(C)：表示动态绑定的正式租约，即从地址池中动态选择 IP 地址，并发送 DHCP-ACK 报文成功将该 IP 地址分配给客户端后，产生的租约

【相关命令】

- `reset dhcp server ip-in-use`

1.2.30 display dhcp server pool

`display dhcp server pool` 命令用来显示 DHCP 地址池的信息。

【命令】

`display dhcp server pool [pool-name]`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

pool-name: 显示指定地址池的信息。*pool-name* 表示地址池名称, 为 1~63 个字符的字符串, 不区分大小写。如果未指定本参数, 则显示所有地址池的信息。

【举例】

显示所有 DHCP 地址池的信息。

```
<Sysname> display dhcp server pool
```

```
Pool name: 0
```

```
Network 20.1.1.0 mask 255.255.255.0
class a range 20.1.1.50 20.1.1.60
bootfile-name abc.cfg
dns-list 20.1.1.66 20.1.1.67 20.1.1.68
domain-name www.aabbcc.com
bims-server ip 192.168.0.51 sharekey cipher $c$3$K13OmQPi791YvQoF2Gs1E+65LOU=
option 2 ip-address 1.1.1.1
expired 1 2 3 0
```

```
Pool name: 1
```

```
Network 20.1.2.0 mask 255.255.255.0
secondary networks:
    20.1.3.0 mask 255.255.255.0
    20.1.4.0 mask 255.255.255.0
bims-server ip 192.168.0.51 port 50 sharekey cipher $c$3$K13OmQPi791YvQoF2Gs1E+65LOU=
forbidden-ip 20.1.1.22 20.1.1.36 20.1.1.37
forbidden-ip 20.1.1.22 20.1.1.23 20.1.1.24
gateway-list 20.1.1.1 20.1.1.2 20.1.1.4
nbns-list 20.1.1.5 20.1.1.6 20.1.1.7
netbios-type m-node
option 2 ip-address 1.1.1.1
expired 1 0 0 0
```

```
Pool name: 2
```

```
Network 20.1.3.0 mask 255.255.255.0
address range 20.1.3.1 to 20.1.3.15
class departmentA range 20.1.3.20 to 20.1.3.29
class departmentB range 20.1.3.30 to 20.1.3.40
next-server 20.1.3.33
tftp-server domain-name www.dian.org.cn
tftp-server ip-address 192.168.0.120
voice-config ncp-ip 20.1.3.2
voice-config as-ip 20.1.3.5
voice-config voice-vlan 3 enable
voice-config fail-over 20.1.3.6 123*
option 2 ip-address 20.1.3.10
expired 1 0 0 0
```

```
Pool name: 3
```

```
static bindings:
```

```

ip-address 10.10.1.2 mask 255.0.0.0
    hardware-address 00e0-00fc-0001 ethernet
ip-address 10.10.1.3 mask 255.0.0.0
    client-identifier aaaa-bbbb
expired unlimited

```

表1-6 display dhcp server pool 命令显示信息描述表

字段	描述
Pool name	地址池的名称
Network	可分配的地址网段
secondary networks	可分配的从地址网段
address range	可分配的地址范围
class <i>class-name</i> range	为指定DHCP用户类分配的地址范围
static bindings	静态绑定的IP地址、硬件地址或客户端ID
option	自定义的DHCP选项
expired	租约期限，其后数值的单位分别为天、小时、分钟和秒。例如， expired 1 2 3 4 表示租约期限为1天2小时3分钟4秒
bootfile-name	为DHCP客户端分配的启动文件名
dns-list	为DHCP客户端分配的DNS服务器地址
domain-name	为DHCP客户端分配的域名后缀
bims-server	为DHCP客户端分配的BIMS服务器信息
forbidden-ip	DHCP地址池中不参与自动分配的IP地址
gateway-list	为DHCP客户端分配的网关地址
nbns-list	为DHCP客户端分配的WINS服务器地址
netbios-type	为DHCP客户端分配的NetBIOS节点类型
next-server	为DHCP客户端分配的下一个提供服务的服务器IP地址
tftp-server domain-name	为DHCP客户端分配的TFTP服务器名
tftp-server ip-address	为DHCP客户端分配的TFTP服务器地址
voice-config ncp-ip	为DHCP客户端分配的网络呼叫处理器的地址
voice-config as-ip	为DHCP客户端分配的备用服务器的地址
voice-config voice-vlan	为DHCP客户端分配的语音VLAN
voice-config fail-over	为DHCP客户端分配的自动故障转移呼叫路由

1.2.31 display dhcp server statistics

display dhcp server statistics 命令用来显示 DHCP 服务器的统计信息。

【命令】

display dhcp server statistics [*pool pool-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

pool pool-name：显示指定地址池的统计信息。*pool-name* 表示地址池名称，为 1~63 个字符的字符串，不区分大小写。如果未指定本参数，则显示所有地址池的统计信息。

【举例】

显示 DHCP 服务器的统计信息。

```
<Sysname> display dhcp server statistics
Pool number:                        1
Pool utilization:                   0.39%
Bindings:
  Automatic:                        1
  Manual:                           0
  Expired:                          0
Conflict:                           1
Messages received:                  10
  DHCPDISCOVER:                     5
  DHCPREQUEST:                       3
  DHCPDECLINE:                       0
  DHCPRELEASE:                       2
  DHCPINFORM:                        0
  BOOTPREQUEST:                      0
Messages sent:                       6
  DHCPOFFER:                         3
  DHCPACK:                           3
  DHCPNAK:                           0
  BOOTPREPLY:                        0
Bad Messages:                       0
```

表1-7 display dhcp server statistics 命令显示信息描述表

字段	描述
Pool number	地址池的数目，显示指定地址池的统计信息时无此字段
Pool utilization	地址池利用率 <ul style="list-style-type: none">显示所有 DHCP 租约统计信息时，表示所有地址池的总体利用率显示指定地址池的租约统计信息时，表示该地址池的利用率
Bindings	各种状态的地址绑定数，包括：

字段	描述
	<ul style="list-style-type: none"> • Automatic: 动态分配的 IP 地址绑定数 • Manual: 手工绑定的 IP 地址绑定数 • Expired: 租约过期的 IP 地址绑定数
Conflict	冲突地址的总数，显示指定地址池的统计信息时无此字段
Messages received	DHCP服务器接收到DHCP客户端发送的报文数，包括： <ul style="list-style-type: none"> • DHCPDISCOVER • DHCPREQUEST • DHCPDECLINE • DHCPRELEASE • DHCPINFORM • BOOTPREREQUEST 显示指定地址池的统计信息时无此类字段
Messages sent	DHCP服务器发给DHCP客户端的报文数，包括： <ul style="list-style-type: none"> • DHCPOFFER • DHCPACK • DHCPNAK • BOOTPREPLY 显示指定地址池的统计信息时无此类字段
Bad Messages	错误信息数，显示指定地址池的统计信息时无此类字段

【相关命令】

- `reset dhcp server statistics`

1.2.32 dns-list

dns-list 命令用来配置 DHCP 地址池为 DHCP 客户端分配的 DNS 服务器地址。

undo dns-list 命令用来删除 DHCP 地址池为 DHCP 客户端分配的 DNS 服务器地址。

【命令】

dns-list *ip-address*&<1-8>

undo dns-list [*ip-address*&<1-8>]

【缺省情况】

未配置 DHCP 地址池为 DHCP 客户端分配的 DNS 服务器地址。

【视图】

DHCP 地址池视图

【缺省用户角色】

network-admin

【参数】

ip-address&<1-8>: DNS 服务器的 IP 地址。&<1-8>表示最多可以输入 8 个 IP 地址，每个 IP 地址之间用空格分隔。

【使用指导】

多次执行该命令，最后一次执行的命令生效。

执行 **undo dns-list** 命令时，如果未指定任何参数，则删除 DHCP 地址池中的所有 DNS 服务器地址。

【举例】

配置 DHCP 地址池 0 为 DHCP 客户端分配的 DNS 服务器地址为 10.1.1.254。

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] dns-list 10.1.1.254
```

【相关命令】

- **display dhcp server pool**

1.2.33 domain-name

domain-name 命令用来配置 DHCP 地址池为 DHCP 客户端分配的域名。

undo domain-name 命令用来恢复缺省情况。

【命令】

```
domain-name domain-name
undo domain-name
```

【缺省情况】

未配置 DHCP 地址池为 DHCP 客户端分配的域名。

【视图】

DHCP 地址池视图

【缺省用户角色】

network-admin

【参数】

domain-name: DHCP 客户端的域名，为 1~50 个字符的字符串，区分大小写。

【使用指导】

多次执行该命令，最后一次执行的命令生效。

【举例】

配置 DHCP 地址池 0 为 DHCP 客户端分配的域名为 company.com。

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] domain-name company.com
```


【相关命令】

- `display dhcp server pool`

1.2.34 expired

expired 命令用来配置 DHCP 地址池中分配的 IP 地址的租约有效期限。

undo expired 命令用来恢复缺省情况。

【命令】

```
expired { day day [ hour hour [ minute minute [ second second ] ] ] | unlimited }  
undo expired
```

【缺省情况】

DHCP 地址池中 IP 地址的租约有效期限为 1 天。

【视图】

DHCP 地址池视图

【缺省用户角色】

network-admin

【参数】

day day: 指定租约过期的天数, *day* 取值范围为 0~365。

hour hour: 指定租约过期的小时数, *hour* 取值范围为 0~23。如果未指定本参数, 则指定过期的小时数为 0。

minute minute: 指定租约过期的分钟数, *minute* 取值范围为 0~59。如果未指定本参数, 则指定过期的分钟数为 0。

second second: 指定租约过期的秒数, *second* 取值范围为 0~59。如果未指定本参数, 则指定过期的秒数为 0。

unlimited: 有效期限为无限长 (实际上系统限定约为 136 年)。

【使用指导】

DHCP 服务器从 DHCP 地址池中选择 IP 地址分配给 DHCP 客户端时, 会同时将该地址池中 IP 地址的租约有效期限通知给 DHCP 客户端。在租约有效期限到达之前, DHCP 客户端需要进行续约申请。如果续约成功, 则 DHCP 客户端可以继续使用该 IP 地址。否则, 租约有效期限到达后, DHCP 客户端不能再继续使用该 IP 地址, 并且 DHCP 服务器会将该地址添加到过期租约信息中。

【举例】

配置地址池 0 的 IP 地址租约有效期为 1 天 2 小时 3 分 4 秒。

```
<Sysname> system-view  
[Sysname] dhcp server ip-pool 0  
[Sysname-dhcp-pool-0] expired day 1 hour 2 minute 3 second 4
```

【相关命令】

- `display dhcp server expired`
- `display dhcp server pool`

- **reset dhcp server expired**

1.2.35 forbidden-ip

forbidden-ip 命令用来配置地址池中不参与自动分配的 IP 地址。

undo forbidden-ip 命令用来取消地址池中不参与自动分配的 IP 地址的配置。

【命令】

```
forbidden-ip ip-address&<1-8>
undo forbidden-ip [ ip-address&<1-8> ]
```

【缺省情况】

未配置地址池中不参与自动分配的 IP 地址。

【视图】

DHCP 地址池视图

【缺省用户角色】

network-admin

【参数】

ip-address&<1-8>: 地址池中不参与自动分配的 IP 地址。&<1-8>表示最多可以输入 8 个 IP 地址，每个 IP 地址之间用空格分隔。

【使用指导】

在 DHCP 地址池视图下通过 **forbidden-ip** 命令配置不参与自动分配的 IP 地址后，只有当前的地址池不能分配这些 IP 地址，其他地址池仍然可以分配这些 IP 地址。

多次执行 **forbidden-ip** 命令，可以配置多个不参与自动分配的 IP 地址。每个地址池最多能配置 4096 个地址。

执行 **undo forbidden-ip** 命令时，如果未指定任何参数，则删除所有不参与自动分配的 IP 地址。

【举例】

配置 DHCP 地址池 0 中不参与自动分配的 IP 地址为 192.168.1.3 和 192.168.1.10。

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] forbidden-ip 192.168.1.3 192.168.1.10
```

【相关命令】

- **dhcp server forbidden-ip**
- **display dhcp server pool**

1.2.36 gateway-list

gateway-list 命令用来配置 DHCP 服务器为 DHCP 客户端分配的网关地址。

undo gateway-list 命令用来删除 DHCP 服务器为 DHCP 客户端分配的网关地址。

【命令】

```
gateway-list ip-address&<1-64>
```

```
undo gateway-list [ ip-address&<1-64> ]
```

【缺省情况】

DHCP 地址池、DHCP 从网段下均未配置为 DHCP 客户端分配的网关地址。

【视图】

DHCP 地址池视图

DHCP 从网段视图

【缺省用户角色】

network-admin

【参数】

ip-address&<1-64>: 网关的 IP 地址。&<1-64>表示最多可以输入 64 个 IP 地址，每个 IP 地址之间用空格分隔。网关地址需要和 DHCP 客户端在同一个网段中。

【使用指导】

DHCP 地址池视图下执行 **gateway-list** 命令，配置的是为地址池中所有 DHCP 客户端分配的网关地址。如果用户需要为地址池下某个从网段的 DHCP 客户端分配其它的网关地址，可以在地址池的从网段视图下执行 **gateway-list** 命令。如果在地址池视图和从网段视图下都配置了网关地址，则优先将从网段视图下配置的网关地址分配给从网段的 DHCP 客户端。

执行 **undo gateway-list** 命令时，如果未指定任何参数，则删除所有配置的网关地址。

【举例】

配置 DHCP 地址池 0 为 DHCP 客户端分配的网关地址为 10.1.1.1。

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] gateway-list 10.1.1.1
```

【相关命令】

- **display dhcp server pool**

1.2.37 if-match

if-match 命令用来配置 DHCP 用户类的匹配规则。

undo if-match 命令用来删除 DHCP 用户类的匹配规则。

【命令】

```
if-match rule rule-number { hardware-address hardware-address mask
hardware-address-mask | option option-code [ ascii ascii-string [ offset
offset | partial ] | hex hex-string [ mask mask | offset offset length length |
partial ] ] | relay-agent gateway-address }
undo if-match rule rule-number
```

【缺省情况】

未配置 DHCP 用户类的匹配规则。

【视图】

DHCP 用户类视图

【缺省用户角色】

network-admin

【参数】

rule rule-number: 匹配规则编号，取值范围为 1~16。编号越小，匹配优先级越高。

hardware-address hardware-address: 指定匹配规则的硬件地址。*hardware-address* 表示客户端的硬件地址，为 4~39 个字符的字符串，字符串只能包含十六进制数和“-”，且形式为 H-H-H，除最后一个 H 表示 2 位或 4 位十六进制数外，其他均表示 4 位十六进制数。例如：*aabb-ccdd-ee* 为有效的硬件地址，*aabb-c-dddd* 和 *aabb-cc-dddd* 为无效的客户端硬件地址。

mask hardware-address-mask: 指定匹配规则的硬件地址掩码。长度需要与 *hardware-address* 保持一致。

option option-code: DHCP 选项的数值，取值范围为 1~254。*option-code* 用于指定匹配 DHCP 客户端时从 DHCP 报文中获取哪个选项。

ascii ascii-string: 指定用来匹配报文中指定选项的内容。*ascii-string* 为 1~128 个字符的 ASCII 字符串。

offset offset: 指定匹配 DHCP 客户端时获取选项内容的起始位置。*offset* 为选项内容偏移量，取值范围为 0~254，单位为字节。

partial: 指定部分匹配，即只要报文中的选项内容中包含指定的 *hex-string* 或 *ascii-string*，即认为匹配通过。

hex hex-string: 指定用来匹配报文中指定选项的内容。*hex-string* 为十六进制数，位数的取值范围为 2~256 之间的偶数。

mask mask: 指定与选项内容匹配时使用的掩码。*mask* 为十六进制掩码数，位数的取值范围为 2~256 之间的偶数。*mask* 的长度必须和 *hex-string* 长度相同。

length length: 指定匹配 DHCP 客户端时获取选项内容的长度。*length* 为选项内容的长度，取值范围为 1~128，单位为字节。指定的选项内容长度必须和 *hex-string* 长度相同。

relay-agent gateway-address: 指定匹配报文中的 *giaddr* 字段的内容。*gateway-address* 为 IP 地址，为点分十进制形式。

【使用指导】

DHCP 服务器通过将 DHCP 客户端发送的报文与本命令配置的规则匹配，来判断 DHCP 客户端属于的 DHCP 用户类。DHCP 用户类视图下通过多次执行 **if-match** 命令，可以配置多条匹配规则。只要任意一条规则匹配成功，就认为该 DHCP 客户端属于该用户类。

在同一用户类视图下配置匹配规则时：

- 多次执行相同 *rule-number* 的命令，如果规则类型（包括匹配 **option**、**relay-agent** 或 **hardware address**）相同，最后一次执行的命令生效；如果规则类型不同，则新的配置和已有配置会共存。建议不同类型的规则不要使用同一个 *rule-number*。
- 不同 *rule-number* 的匹配规则内容不能完全相同。

将报文与某一条 **if-match hardware-address** 命令配置的规则匹配的方式为：

- 匹配硬件地址类型，目前只支持以太类型的硬件地址（即 MAC 地址）匹配，非以太类型的硬件地址均会匹配失败。
- 如果报文中的客户端硬件地址与配置的客户端硬件地址及硬件地址掩码匹配，则认为匹配成功。否则，匹配失败。
- 匹配时报文中的客户端硬件地址长度与配置规则中的硬件地址长度一致时才进行匹配，否则直接认为不匹配。如匹配规则为 **if-match rule 1 hardware-address 0094-0000 mask ffff-0000**，需匹配硬件地址长度为 4 字节的用户；若报文中客户端硬件地址长度为 6 字节（比如 0094-0000-0010），则认为匹配失败。
- 匹配硬件地址时，可以配置不连续匹配的硬件地址，如匹配规则为 **if-match rule 1 hardware-address 0094-0000-1100 mask ffff-0000-ff00**，则匹配硬件地址为 0094-xxxx-11xx（x 代表变量）的报文。

将报文与某一条 **if-match option** 命令配置的规则匹配的方式为：

- 如果规则中只指定了 *option-code* 参数，则只要报文中包括该选项，就认为匹配成功。否则，匹配失败。
- 如果规则中只指定了 *option-code* 和 *hex-string/ascii-string* 参数，则报文中指定选项的值从第 1 位开始的部分与 *hex-string/ascii-string* 相同时，认为匹配成功。否则，匹配失败。
- 如果规则中指定了 *option-code*、*ascii-string* 和 *offset* 参数，则将指定选项的值的第 *offset*+1 位到最后一位的内容与 *ascii-string* 比较，二者相同时，认为匹配成功。否则，匹配失败。
- 如果规则中指定了 *option-code*、*hex-string*、*offset* 和 *length* 参数，则将指定选项值的第 *offset*+1 位到 *offset*+*length* 位的内容与 *hex-string* 比较，二者相同时，认为匹配成功。否则，匹配失败。
- 如果规则中指定了 *option-code*、*hex-string* 和 *mask* 参数，则将指定选项值的第 1 位到 *mask* 长度位的内容与 *mask* 进行与运算，将结果与 *hex-string* 与 *mask* 与运算的结果比较，二者相同时，认为匹配成功。否则，匹配失败。
- 如果规则中指定了 *option-code*、*hex-string/ascii-string* 和 **partial** 参数，则选项内容内包含了指定的 *hex-string/ascii-string*，就认为匹配成功。否则，匹配失败。例如匹配字段为 abc，那 xabc、xyzabca、xabcyz 和 abcxzy 均认为匹配通过。

将报文与某一条 **if-match relay-agent** 命令配置的规则匹配的方式是只要报文中的 **giaddr** 字段和指定的 *gateway-address* 一致时，认为匹配成功。否则，匹配失败。

【举例】

配置 DHCP 用户类 exam 的匹配规则，匹配规则编号 1，匹配硬件地址 0094-0000-0101，硬件掩码长度为 ffff-0000-0000。

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 1 hardware-address 0094-0000-0101 mask
ffff-0000-0000
```

配置 DHCP 用户类 exam 的匹配规则，匹配规则编号 2，报文中包含 Option 82。

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 2 option 82
```

配置 DHCP 用户类 **exam** 的匹配规则，匹配规则编号 3，报文中包含 Option 82，并且该选项的十六进制数第四个字节的最高位为 1。

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 3 option 82 hex 00000080 mask 00000080
```

配置 DHCP 用户类 **exam** 的匹配规则，匹配规则编号 4，报文中包含 Option 82，并且该选项的前三个字节为十六进制数 13ae92。

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 4 option 82 hex 13ae92 offset 0 length 3
```

配置 DHCP 用户类 **exam** 的匹配规则，匹配规则编号 5，报文中包含 Option 82，并且该选项内容中包含指定的十六进制数 13ae。

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 5 option 82 hex 13ae partial
```

配置 DHCP 用户类 **exam** 的匹配规则，匹配规则编号 6，报文中包含的 giaddr 字段值为 10.1.1.1。

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 6 relay-agent 10.1.1.1
```

【相关命令】

- **dhcp class**

1.2.38 ip-in-use threshold

ip-in-use threshold 命令用来设置地址池使用率告警门限阈值。

undo ip-in-use threshold 命令用来恢复缺省情况。

【命令】

```
ip-in-use threshold threshold-value
undo ip-in-use threshold
```

【缺省情况】

地址池使用率告警门限阈值为 100%。

【视图】

DHCP 地址池视图

【缺省用户角色】

network-admin

【参数】

threshold-value: 地址池使用率告警阈值，为百分比形式，取值范围为 1~100。比如若设置为 80，表示地址池使用率超过 80%时，系统会生成告警信息发送给信息中心。

【使用指导】

执行 **ip-in-use threshold** 命令设置地址池使用率告警阈值，在地址池中地址使用率超过阈值时，系统会生成告警信息提醒管理员进行地址池规划，避免因为地址池中地址资源耗尽，后续用户不能上线。

在同一个视图下多次执行本命令，最后一次执行的命令生效。

系统将告警信息发送给信息中心，通过设置信息中心的参数，最终决定日志信息的输出规则（即是否允许输出以及输出方向）。有关信息中心参数配置请参见“网络管理和监控配置指导”中的“信息中心”。

【举例】

配置地址池 p1 使用率告警门限阈值为 85%。

```
<Sysname> system-view
[Sysname] dhcp server ip-pool p1
[Sysname-dhcp-pool-p1] ip-in-use threshold 85
```

1.2.39 nbns-list

nbns-list 命令用来配置 DHCP 地址池为 DHCP 客户端分配的 WINS 服务器地址。

undo nbns-list 命令用来删除 DHCP 地址池为 DHCP 客户端分配的 WINS 服务器地址。

【命令】

```
nbns-list ip-address&<1-8>
undo nbns-list [ ip-address&<1-8> ]
```

【缺省情况】

未配置 DHCP 地址池为 DHCP 客户端分配的 WINS 服务器地址。

【视图】

DHCP 地址池视图

【缺省用户角色】

network-admin

【参数】

ip-address&<1-8>: WINS 服务器的 IP 地址。&<1-8>表示最多可以输入 8 个 IP 地址，每个 IP 地址之间用空格分隔。

【使用指导】

多次执行本命令，最后一次执行的命令生效。

执行 **undo nbns-list** 命令时，如果未指定任何参数，则删除 DHCP 地址池中的所有 WINS 服务器地址。

【举例】

配置 DHCP 地址池 0 为 DHCP 客户端分配 WINS 服务器地址为 10.1.1.1。

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] nbns-list 10.1.1.1
```


【相关命令】

- `display dhcp server pool`
- `netbios-type`

1.2.40 netbios-type

`netbios-type` 命令用来配置 DHCP 地址池为 DHCP 客户端分配的 NetBIOS 节点类型。

`undo netbios-type` 命令用来恢复缺省情况。

【命令】

```
netbios-type { b-node | h-node | m-node | p-node }  
undo netbios-type
```

【缺省情况】

未配置 DHCP 地址池为 DHCP 客户端分配的 NetBIOS 节点类型。

【视图】

DHCP 地址池视图

【缺省用户角色】

network-admin

【参数】

b-node: b 类节点，“b”代表广播（broadcast），此类节点采用广播方式获取主机名和 IP 地址之间的映射。源节点通过发送带有目的节点主机名的广播报文来获取目的节点的 IP 地址，目的节点收到广播报文后，就将自己的 IP 地址返回给源节点。

h-node: h 类节点，“h”代表混合（hybrid），是具备“端到端”通信机制的 b 类节点。此类节点首先发送单播报文与 WINS 服务器通信来获取映射关系，如果未获取到，再发送广播报文来获取映射关系。

m-node: m 类节点，“m”代表混合（mixed），是具有部分广播特性的 p 类节点。此类节点首先发送广播报文来获取映射关系，如果未获取到，则再发送单播报文与 WINS 服务器通信来获取映射关系。

p-node: p 类节点，“p”代表端到端（peer-to-peer），即此类节点采用发送单播报文与 WINS 服务器通信的方式获取映射关系。源节点给 WINS 服务器发送单播报文，WINS 服务器收到单播报文后，返回源节点请求的目的节点名所对应的 IP 地址。

【使用指导】

多次执行本命令，最后一次执行的命令生效。

【举例】

配置 DHCP 地址池 0 为 DHCP 客户端分配的 NetBIOS 节点类型为 p 类节点。

```
<Sysname> system-view  
[Sysname] dhcp server ip-pool 0  
[Sysname-dhcp-pool-0] netbios-type p-node
```

【相关命令】

- `display dhcp server pool`

- **nbns-list**

1.2.41 network

network 命令用来配置 DHCP 地址池动态分配的 IP 地址网段。

undo network 命令用来删除已经创建的用于动态分配的 IP 地址网段。

【命令】

```
network network-address [ mask-length | mask mask ] [ secondary ]
undo network network-address [ mask-length | mask mask ] [ secondary ]
```

【缺省情况】

未配置动态分配的 IP 地址网段，即没有可供分配的 IP 地址。

【视图】

DHCP 地址池视图

【缺省用户角色】

network-admin

【参数】

network-address: 用于动态分配的网段地址。未指定掩码长度和掩码时，表示采用自然掩码。

mask-length: IP 地址的网络掩码长度，取值范围为 1~30。

mask mask: IP 地址的网络掩码，*mask* 为点分十进制形式。

secondary: 指定配置的网段为从网段。如果未指定本参数，则表示配置的网段为主网段。主网段中的地址分配完之后，DHCP 服务器可以在从网段中选择地址分配给 DHCP 客户端。

【使用指导】

执行本命令时如果指定了 **secondary** 参数，则会进入从网段视图。用户可以在该视图下通过 **gateway-list** 命令配置为从网段的 DHCP 客户端分配的网关地址。

每个 DHCP 地址池中只能配置一个主网段，多次执行 **network** 命令配置主网段，最后一次执行的命令生效。

每个 DHCP 地址池中最多可以配置 32 个从网段。

一个 DHCP 地址池中各个主、从网段的网络号和掩码不能完全相同。

在地址池下配置了 **address range** 或 **class** 命令后，不能再在该地址池下配置从网段。

修改或删除 **network** 配置，会导致该地址池下现有的已分配地址被删除。

【举例】

配置 DHCP 地址池 0 动态分配的主地址网段为 192.168.8.0/24，从地址网段为 192.168.10.0/24。

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] network 192.168.8.0 mask 255.255.255.0
[Sysname-dhcp-pool-0] network 192.168.10.0 mask 255.255.255.0 secondary
[Sysname-dhcp-pool-0-secondary]
```

【相关命令】

- **display dhcp server pool**

- **gateway-list**

1.2.42 next-server

next-server 命令用来配置 DHCP 地址池为 DHCP 客户端分配的下一个提供服务的服务器 IP 地址。

undo next-server 命令用来恢复缺省情况。

【命令】

```
next-server ip-address
undo next-server
```

【缺省情况】

未配置 DHCP 地址池为 DHCP 客户端分配的下一个提供服务的服务器 IP 地址。

【视图】

DHCP 地址池视图

【缺省用户角色】

network-admin

【参数】

ip-address: 下一个提供服务的服务器 IP 地址。

【使用指导】

为 DHCP 客户端分配的下一个提供服务的服务器 IP 地址，是在 DHCP 客户端启动过程中，在获取到 IP 地址后，用于获取其他启动数据的服务器地址。例如，TFTP 服务器地址。

多次执行本命令，最后一次执行的命令生效。

【举例】

配置 DHCP 地址池 0 为 DHCP 客户端分配的下一个提供服务的服务器 IP 地址为 10.1.1.254。

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] next-server 10.1.1.254
```

【相关命令】

- **display dhcp server pool**

1.2.43 option

option 命令用来自定义 DHCP 选项。

undo option 命令用来删除自定义的 DHCP 选项。

【命令】

```
option code { ascii ascii-string | hex hex-string | ip-address
ip-address&<1-8> }
undo option code
```

【缺省情况】

未自定义 DHCP 选项。

【视图】

DHCP 地址池视图

DHCP 选项组视图

【缺省用户角色】

network-admin

【参数】

code: 选项的数值，取值范围为 2~254，不包括 50~54、56、58、59、61 和 82。

ascii *ascii-string*: 指定选项内容为配置的 ASCII 字符串。*ascii-string* 为 1~255 个字符的 ASCII 字符串，区分大小写。

hex *hex-string*: 指定选项内容为配置的十六进制数。*hex-string* 为十六进制数，位数的取值范围为 2~256 之间的偶数。

ip-address *ip-address*&<1-8>: 指定选项内容为配置的 IP 地址。&<1-8>表示最多可以输入 8 个 IP 地址，每个 IP 地址之间用空格分隔。

【使用指导】

通过执行本命令，可以配置编号为 *code* 的 DHCP 选项内容为指定的 ASCII 字符串、十六进制数或 IP 地址，即采用指定的内容来填充 DHCP 应答报文中编号为 *code* 的选项，以便将指定的选项内容分配给客户端。

本命令为 DHCP 服务器提供了灵活的选项配置方式，使得 DHCP 服务器可以为 DHCP 客户端提供更加丰富的选项内容。在以下情况下，可以使用本命令自定义 DHCP 选项：

- 随着 DHCP 的不断发展，新的 DHCP 选项会陆续出现。通过自定义 DHCP 选项，可以方便地添加新的 DHCP 选项。
- 有些选项的内容，RFC 中没有统一规定。厂商可以根据需要定义选项的内容，如 Option 43。通过自定义 DHCP 选项，可以为 DHCP 客户端提供厂商指定的信息。
- 设备上只提供了有限的选项配置命令（如 **gateway-list**、**dns-list** 命令），对于没有专门命令来配置的 DHCP 选项，可以通过 **option** 命令配置选项内容。例如，可以通过 **option 4 ip-address 1.1.1.1** 命令指定为 DHCP 客户端分配的时间服务器地址为 1.1.1.1。
- 扩展已有的 DHCP 选项。当前已提供的方式无法满足用户需求时（比如通过 **dns-list** 命令最多只能配置 8 个 DNS 服务器地址，如果用户需要配置的 DNS 服务器地址数目大于 8，则该命令无法满足需求），可以通过自定义 DHCP 选项的方式进行扩展。

有些 DHCP 选项既可以通过专门的命令来配置，也可以通过 **option** 命令来配置。例如，Option 6（DNS 服务器地址选项）既可以通过 **dns-list** 命令配置，也可以通过 **option 6** 命令配置。如果同时通过上述两种方式配置了这些选项，则在填充 DHCP 应答报文的选项时，优先选择专门命令的配置。如果未通过专门命令来配置，则采用 **option** 命令配置的内容填充选项。

DHCP 服务器在应答 DHCP 客户端报文时，如果 DHCP 选项组的选项编号和 DHCP 地址池选项编号相同且匹配用户类时，以 DHCP 选项组的选项为准。

多次执行本命令，并指定相同的选项数值 *code*，最后一次执行的命令生效。

【举例】

日志服务器选项的编号为 7。在 DHCP 地址池 0 中配置为 DHCP 客户端分配的日志服务器地址为 2.2.2.2。

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] option 7 ip-address 2.2.2.2
```

【相关命令】

- **display dhcp server pool**

1.2.44 reset dhcp server conflict

reset dhcp server conflict 命令用来清除 DHCP 的地址冲突信息。

【命令】

```
reset dhcp server conflict [ ip ip-address ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

ip ip-address: 清除指定 IP 地址的冲突信息。如果未指定本参数，则清除所有地址的冲突信息。

【使用指导】

出现冲突地址，一般是由于网络配置不合理，动态分配的地址和网络中静态配置的地址冲突而产生的。在合理调整网络配置，不再存在冲突的情况下，原来的冲突地址可能不再冲突，可以被重新分配。此时，通过本命令，清除检测到的冲突地址，则该地址可以被重新分配。

【举例】

```
# 清除全部地址冲突信息。
<Sysname> reset dhcp server conflict
```

【相关命令】

- **display dhcp server conflict**

1.2.45 reset dhcp server expired

reset dhcp server expired 命令用来清除租约过期的地址绑定信息。

【命令】

```
reset dhcp server expired [ ip ip-address | pool pool-name ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

ip ip-address: 清除指定 IP 地址的租约过期地址绑定信息。如果未指定本参数，则清除所有 IP 地址的租约过期地址绑定信息。

pool pool-name: 清除指定地址池中租约过期的地址绑定信息。*pool-name* 表示地址池名称，为 1~63 个字符的字符串，不区分大小写。如果未指定本参数，则清除所有地址池的租约过期地址绑定信息。

【举例】

清除所有租约过期的地址绑定信息。

```
<Sysname> reset dhcp server expired
```

【相关命令】

- **display dhcp server expired**

1.2.46 reset dhcp server ip-in-use

reset dhcp server ip-in-use 命令用来清除 DHCP 的正式绑定和临时绑定信息。

【命令】

```
reset dhcp server ip-in-use [ ip ip-address | pool pool-name ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

ip ip-address: 清除指定 IP 地址的正式绑定和临时绑定信息。如果未指定本参数，则清除所有 IP 地址的正式绑定和临时绑定信息。

pool pool-name: 清除指定地址池的正式绑定和临时绑定信息。*pool-name* 表示地址池名称，为 1~63 个字符的字符串，不区分大小写。如果未指定本参数，则清除所有地址池的正式绑定和临时绑定信息。

【使用指导】

清除静态正式绑定信息时，将使该绑定信息变为静态无效绑定。

【举例】

清除地址 10.110.1.1 的正式绑定和临时绑定信息。

```
<Sysname> reset dhcp server ip-in-use ip 10.110.1.1
```

【相关命令】

- **display dhcp server ip-in-use**

1.2.47 reset dhcp server statistics

reset dhcp server statistics 命令用来清除 DHCP 服务器的统计信息。

【命令】

```
reset dhcp server statistics
```

【视图】

用户视图

【缺省用户角色】

network-admin

【举例】

清除 DHCP 服务器的统计信息。

```
<Sysname> reset dhcp server statistics
```

【相关命令】

- `display dhcp server statistics`

1.2.48 static-bind

static-bind 命令用来在 DHCP 地址池中配置静态地址绑定，以便实现 DHCP 服务器为客户端 ID 或硬件地址为指定值的客户端分配固定的 IP 地址。

undo static-bind 命令用来删除 DHCP 地址池中的静态地址绑定。

【命令】

```
static-bind ip-address ip-address [ mask-length | mask mask ]  
{ client-identifier client-identifier | hardware-address hardware-address  
[ ethernet | token-ring ] }  
undo static-bind ip-address ip-address
```

【缺省情况】

未在 DHCP 地址池中配置静态地址绑定。

【视图】

DHCP 地址池视图

【缺省用户角色】

network-admin

【参数】

ip-address ip-address: 指定静态绑定的 IP 地址。未指定掩码长度和掩码时，表示采用自然掩码。

mask-length: 静态绑定 IP 地址的掩码长度，即掩码中连续“1”的个数，取值范围为 1~30。

mask mask: 指定静态绑定 IP 地址的掩码，*mask* 为点分十进制形式。

client-identifier client-identifier: 指定静态绑定的客户端 ID。
client-identifier 表示客户端 ID，为 4~254 个字符的字符串，字符串中只能包括十六进制数和“-”，且形式为 H-H-H...，除最后一个 H 表示 2 位或 4 位十六进制数外，其他均表示 4 位十六进制数。例如：aabb-cccc-dd 为有效的 ID，aabb-c-dddd 和 aabb-cc-dddd 为无效客户端 ID。

hardware-address *hardware-address* : 指定静态绑定的客户端硬件地址。
hardware-address 表示客户端硬件地址, 为 4~39 个字符的字符串, 字符串中只能包括十六进制数和“-”, 且形式为 H-H-H..., 除最后一个 H 表示 2 位或 4 位十六进制数外, 其他均表示 4 位十六进制数。例如: aabb-cccc-dd 为有效的客户端硬件地址, aabb-c-dddd 和 aabb-cc-dddd 为无效的客户端硬件地址。

ethernet: 指定客户端硬件地址类型为以太网, 缺省为以太网类型。

token-ring: 指定客户端硬件地址类型为令牌环网。

【使用指导】

静态绑定的 IP 地址不能是 DHCP 服务器的接口 IP 地址, 否则会导致 IP 地址冲突, 被绑定的客户端将无法获取到 IP 地址。

同一地址池下可以配置多个静态地址绑定。所有地址池下配置的静态地址绑定一共不能超过 8192 个。

同一地址只能绑定给一个客户端。不能通过重复执行本命令修改 IP 地址与客户端的绑定关系。如需修改 IP 地址与客户端的绑定关系, 请先通过 **undo static-bind** 命令删除静态地址绑定, 再执行 **static-bind** 命令。

【举例】

```
# 在 DHCP 地址池 0 中配置: 为客户端 ID 为 00aa-aabb 的客户端, 固定分配 IP 地址 10.1.1.1/24。
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0 client-identifier 00aa-aabb
```

【相关命令】

- **display dhcp server pool**

1.2.49 tftp-server domain-name

tftp-server domain-name 命令用来配置 DHCP 地址池为 DHCP 客户端分配的 TFTP 服务器域名。

undo tftp-server domain-name 命令用来恢复缺省情况。

【命令】

```
tftp-server domain-name domain-name
undo tftp-server domain-name
```

【缺省情况】

未配置 DHCP 地址池为 DHCP 客户端分配的 TFTP 服务器域名。

【视图】

DHCP 地址池视图

【缺省用户角色】

network-admin

【参数】

domain-name: TFTP 服务器域名，为 1~63 个字符的字符串，区分大小写。

【使用指导】

多次执行本命令，最后一次执行的命令生效。

【举例】

配置 DHCP 地址池 0 为 DHCP 客户端分配的 TFTP 服务器域名为 aaa。

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] tftp-server domain-name aaa
```

【相关命令】

- **display dhcp server pool**
- **tftp-server ip-address**

1.2.50 tftp-server ip-address

tftp-server ip-address 命令用来配置 DHCP 地址池为 DHCP 客户端分配的 TFTP 服务器地址。**undo tftp-server ip-address** 命令用来恢复缺省情况。

【命令】

```
tftp-server ip-address ip-address
undo tftp-server ip-address
```

【缺省情况】

未配置 DHCP 地址池为 DHCP 客户端分配的 TFTP 服务器地址。

【视图】

DHCP 地址池视图

【缺省用户角色】

network-admin

【参数】

ip-address: TFTP 服务器的 IP 地址。

【使用指导】

多次执行本命令，最后一次执行的命令生效。

【举例】

配置 DHCP 地址池 0 为 DHCP 客户端分配的 TFTP 服务器地址为 10.1.1.1。

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] tftp-server ip-address 10.1.1.1
```

【相关命令】

- **display dhcp server pool**
- **tftp-server domain-name**

1.2.51 valid class

valid class 命令用来配置 DHCP 白名单包括的用户类名。

undo valid class 命令用来删除 DHCP 白名单中包括的用户类名。

【命令】

```
valid class class-name<1-8>
undo valid class class-name<1-8>
```

【缺省情况】

未配置 DHCP 白名单包括的用户类。

【视图】

DHCP 地址池视图

【缺省用户角色】

network-admin

【参数】

class-name<1-8>: DHCP 白名单包括的用户类名列表。其中 *class-name* 为 DHCP 用户类名，为 1~63 个字符的字符串，不区分大小写。**<1-8>**代表最多可以输入 8 个用户类名，每个用户类名之间用空格分隔。

【使用指导】

在配置了 DHCP 地址池用户白名单功能后，DHCP 服务器才会检查用户是否属于白名单包括的用户类。

【举例】

在 DHCP 地址池 0 中配置 DHCP 白名单包括的用户类名为 test1 和 test2。

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] valid class test1 test2
```

【相关命令】

- **dhcp class**
- **verify class**

1.2.52 verify class

verify class 命令用来开启 DHCP 用户类白名单功能。

undo verify class 命令用来关闭 DHCP 用户类白名单功能。

【命令】

```
verify class
undo verify class
```

【缺省情况】

DHCP 用户类白名单功能处于关闭状态。

【视图】

DHCP 地址池视图

【缺省用户角色】

network-admin

【使用指导】

在开启了 DHCP 用户类白名单功能后，DHCP 服务器才会检查用户是否属于白名单包括的用户类。需要注意的是，DHCP 用户类白名单功能对获取静态绑定租约的客户端不生效。

【举例】

在 DHCP 地址池 0 中开启 DHCP 用户类白名单功能。

```
[Sysname] system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] verify class
```

【相关命令】

- **valid class**

1.2.53 voice-config

voice-config 命令用来配置 DHCP 地址池为 DHCP 客户端分配的 Option 184 内容。

undo voice-config 命令用来删除 DHCP 地址池为 DHCP 客户端分配的 Option 184 内容。

【命令】

```
voice-config { as-ip ip-address | fail-over ip-address dialer-string | ncp-ip ip-address | voice-vlan vlan-id { disable | enable } }
undo voice-config [ as-ip | fail-over | ncp-ip | voice-vlan ]
```

【缺省情况】

未配置 DHCP 地址池为 DHCP 客户端分配的 Option 184 内容。

【视图】

DHCP 地址池视图

【缺省用户角色】

network-admin

【参数】

as-ip ip-address: 指定备用服务器的 IP 地址。

fail-over ip-address dialer-string: 指定自动故障转移 IP 地址及呼叫字符串。
dialer-string 为 1~39 个字符的字符串，字符只能是数字 0~9 及 “*”。

ncp-ip ip-address: 指定网络呼叫处理器的 IP 地址。

voice-vlan vlan-id: 指定语音 VLAN 的 ID。vlan-id 取值范围为 2~4094。

- **disable**: 指定 VLAN 处于禁止状态，即 DHCP 客户端不会将所指定的 VLAN ID 作为语音 VLAN。
- **enable**: 指定 VLAN 处于开启状态，即 DHCP 客户端会将所指定的 VLAN ID 作为语音 VLAN。

【使用指导】

多次执行本命令，最后一次执行的命令生效。

【举例】

为 DHCP 地址池 0 指定 Option 184 的内容：网络呼叫处理器的 IP 地址为 10.1.1.1，备用服务器的 IP 地址为 10.2.2.2，语音 VLAN 的 ID 为 3，为开启状态，自动故障转移 IP 地址为 10.3.3.3，呼叫字符串为 99*。

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] voice-config ncp-ip 10.1.1.1
[Sysname-dhcp-pool-0] voice-config as-ip 10.2.2.2
[Sysname-dhcp-pool-0] voice-config voice-vlan 3 enable
[Sysname-dhcp-pool-0] voice-config fail-over 10.3.3.3 99*
```

【相关命令】

- **display dhcp server pool**

1.3 DHCP中继配置命令



说明

- S5110V2-SI 系列交换机不支持本特性。
- S5000V3-EI 和 S5000E-X 系列交换机仅 Release 6127 及以上版本支持 DHCP 中继配置命令。

1.3.1 dhcp relay check mac-address

dhcp relay check mac-address 命令用来开启 DHCP 中继的 MAC 地址检查功能。

undo dhcp relay check mac-address 命令用来关闭 DHCP 中继的 MAC 地址检查功能。

【命令】

```
dhcp relay check mac-address
undo dhcp relay check mac-address
```

【缺省情况】

DHCP 中继的 MAC 地址检查功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

【使用指导】

开启该功能后，DHCP 中继检查接收到的 DHCP 请求报文中的 chaddr 字段和数据帧的源 MAC 地址字段是否一致。如果一致，则认为该报文合法，将其转发给 DHCP 服务器；如果不一致，则丢弃该报文。

只有在接口上配置 **dhcp select relay** 后，DHCP 中继的 MAC 地址检查功能才会生效。

由于 DHCP 中继转发 DHCP 报文时会修改报文的源 MAC 地址，所以只能在靠近 DHCP 客户端的第一跳 DHCP 中继设备上开启 MAC 地址检查功能。

【举例】

开启 DHCP 中继的 MAC 地址检查功能。

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp relay check mac-address
```

【相关命令】

- **dhcp select relay**

1.3.2 dhcp relay check mac-address aging-time

dhcp relay check mac-address aging-time 命令用来配置 DHCP 中继的 MAC 地址检查表项的老化时间。

undo dhcp relay check mac-address aging-time 命令用来恢复缺省情况。

【命令】

```
dhcp relay check mac-address aging-time time
undo dhcp relay check mac-address aging-time
```

【缺省情况】

MAC 地址检查表项的老化时间为 30 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

如果未通过 **dhcp relay check mac-address** 命令开启 DHCP 中继的 MAC 地址检查功能，则本命令的配置不会生效。

【参数】

time: DHCP 中继的 MAC 地址检查表项的老化时间，取值范围为 30~600，单位为秒。

【举例】

配置 DHCP 中继的 MAC 地址检查表项的老化时间为 60 秒。

```
<Sysname> system-view
[Sysname] dhcp relay check mac-address aging-time 60
```

1.3.3 dhcp relay client-information record

dhcp relay client-information record 命令用来开启 DHCP 中继用户地址表项记录功能。

undo dhcp relay client-information record 命令用来关闭 DHCP 中继用户地址表项记录功能。

【命令】

```
dhcp relay client-information record
undo dhcp relay client-information record
```

【缺省情况】

DHCP 中继用户地址表项记录功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

当 DHCP 中继作为 DHCP 客户端的网关设备时，才会记录此 DHCP 客户端的地址表项。DHCP 中继用户地址表项记录了 DHCP 客户端的 IP 地址、MAC 地址和用户地址表项类型等信息。

关闭 DHCP 中继用户地址表项记录功能时，会删除 DHCP 中继上记录的全部地址表项。

【举例】

```
# 开启 DHCP 中继用户地址表项记录功能。
<Sysname> system-view
[Sysname] dhcp relay client-information record
```

【相关命令】

- **dhcp relay client-information refresh**
- **dhcp relay client-information refresh enable**

1.3.4 dhcp relay client-information refresh

dhcp relay client-information refresh 命令用来配置 DHCP 中继动态用户地址表项的定时刷新周期。

undo dhcp relay client-information refresh 命令用来恢复缺省情况。

【命令】

```
dhcp relay client-information refresh [ auto | interval interval ]
undo dhcp relay client-information refresh
```

【缺省情况】

定时刷新周期为 **auto**，即根据表项的数目自动计算刷新时间间隔。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

auto: 指定根据表项的数目自动计算刷新时间间隔。表项越多，刷新时间间隔越短，但最短时间间隔不会小于 50 毫秒。

interval interval: 刷新时间间隔，取值范围为 1~120，单位为秒。

【使用指导】

多次执行本命令，最后一次执行的命令生效。

【举例】

配置 DHCP 中继动态用户地址表项的刷新时间间隔为 100 秒。

```
<Sysname> system-view
```

```
[Sysname] dhcp relay client-information refresh interval 100
```

【相关命令】

- **dhcp relay client-information record**
- **dhcp relay client-information refresh enable**

1.3.5 dhcp relay client-information refresh enable

dhcp relay client-information refresh enable 命令用来开启 DHCP 中继动态用户地址表项定时刷新功能。

undo dhcp relay client-information refresh enable 命令用来关闭 DHCP 中继动态用户地址表项定时刷新功能。

【命令】

```
dhcp relay client-information refresh enable
```

```
undo dhcp relay client-information refresh enable
```

【缺省情况】

DHCP 中继动态用户地址表项定时刷新功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

DHCP 客户端释放动态获取的 IP 地址时，会向 DHCP 服务器单播发送 DHCP-RELEASE 报文，DHCP 中继不会处理该报文的内容。如果此时 DHCP 中继上记录了该 IP 地址与 MAC 地址的绑定关系，则会造成 DHCP 中继的用户地址表项无法实时刷新。为了解决这个问题，DHCP 中继支持动态用户地址表项的定时刷新功能。

DHCP 中继动态用户地址表项定时刷新功能开启时，DHCP 中继每隔指定时间采用客户端获取到的 IP 地址向 DHCP 服务器发送 DHCP-REQUEST 报文：

- 如果 DHCP 中继接收到 DHCP 服务器响应的 DHCP-ACK 报文或在指定时间内未接收到 DHCP 服务器的响应报文，则表明这个 IP 地址已经可以进行分配，DHCP 中继会删除动态用

户地址表中对应的表项，为了避免地址浪费，DHCP 中继收到 DHCP-ACK 报文后，会发送 DHCP-RELEASE 报文释放申请到的 IP 地址。

- 如果 DHCP 中继接收到 DHCP 服务器响应的 DHCP-NAK 报文，则表示该 IP 地址的绑定信息仍然存在，DHCP 中继不会删除该 IP 地址对应的表项。

需要注意的是，关闭 DHCP 中继动态用户地址表项定时刷新功能时，DHCP 中继上记录的用户地址表项不会自动老化。DHCP 客户端释放申请到的 IP 地址后，需要用户执行 **reset dhcp relay client-information** 命令删除 DHCP 中继上对应的用户地址表项。

【举例】

关闭 DHCP 中继动态用户地址表项定时刷新功能。

```
<Sysname> system-view
[Sysname] undo dhcp relay client-information refresh enable
```

【相关命令】

- **dhcp relay client-information record**
- **dhcp relay client-information refresh**
- **reset dhcp relay client-information**

1.3.6 dhcp relay dhcp-server timeout

dhcp relay dhcp-server timeout 命令用来配置 DHCP 服务器应答超时切换时间。

undo dhcp relay dhcp-server timeout 命令用来恢复缺省情况。

【命令】

```
dhcp relay dhcp-server timeout time
undo dhcp relay dhcp-server timeout
```

【缺省情况】

DHCP 服务器应答超时切换时间为 30 秒。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

time：超时切换时间，取值范围为 1～65535，单位为秒。

【使用指导】

多次执行本命令，最后一次执行的命令生效。

【举例】

在 VLAN 接口 2 上配置 DHCP 服务器应答超时切换时间为 60 秒。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] dhcp relay dhcp-server timeout 60
```

【相关命令】

- `dhcp relay server-address algorithm`

1.3.7 dhcp relay gateway

`dhcp relay gateway` 命令用来配置 DHCP 中继在 DHCP 报文中填充的中继地址。

`undo dhcp relay gateway` 命令用来恢复缺省情况。

【命令】

`dhcp relay gateway ip-address`

`undo dhcp relay gateway`

【缺省情况】

DHCP 中继在 DHCP 报文中填充的中继地址是接口下的主 IP 地址。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ip-address: 中继地址。该地址必须属于命令行所在的接口。

【使用指导】

在接口视图下配置此命令后，中继会使用此命令配置的地址作为中继地址。

多次执行本命令，最后一次执行的命令生效。

【举例】

在 VLAN 接口 2 上配置在 DHCP 报文中填充的中继地址为 10.1.1.1。

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 2
```

```
[Sysname-Vlan-interface2] dhcp relay gateway 10.1.1.1
```

【相关命令】

- `gateway-list`

1.3.8 dhcp relay information circuit-id

`dhcp relay information circuit-id` 命令用来配置 Option 82 的 Circuit ID 子选项的填充模式和填充格式。

`undo dhcp relay information circuit-id` 命令用来恢复缺省情况。

【命令】

```
dhcp relay information circuit-id { bas | string circuit-id | { normal |  
verbose [ node-identifier { mac | sysname | user-defined node-identifier } ]  
[ interface ] } [ format { ascii | hex } ] }
```

```
undo dhcp relay information circuit-id
```


【缺省情况】

Option 82 的 Circuit ID 子选项的填充模式为 Normal，填充格式为 hex。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

bas: 表示支持使用工信部规范的格式填充 Circuit ID 子选项。填充内容包括接口信息、VLAN 信息。

string circuit-id: 指定以用户配置的字符串填充 Circuit ID 子选项。*circuit-id* 表示用户配置的用来填充 Circuit ID 子选项的内容，为 3~63 个字符的字符串，区分大小写。

normal: 指定以 Normal 模式填充 Circuit ID 子选项，填充内容为 VLAN ID 和端口号。

verbose: 指定以 Verbose 模式填充 Circuit ID 子选项。填充的内容为节点标识、接口信息和接口所在的 VLAN 编号。节点标识缺省以节点的 MAC 地址构成；接口信息缺省由以太网类型（取值固定为“eth”）、框号、槽号、子槽号和接口编号组成。

node-identifier { mac | sysname | user-defined node-identifier }: 指定接入节点标识。

- **mac**: 表示以节点的 MAC 地址作为节点标识。
- **sysname**: 表示以节点的设备名称作为节点标识。设备的系统名称可以通过系统视图下的 **sysname** 命令配置。不管配置了哪种填充格式，设备的系统名称始终采用 ASCII 码格式填充。
- **user-defined node-identifier**: 表示以指定的字符串作为节点标识，*node-identifier* 为 1~50 个字符的字符串，区分大小写。不管配置了哪种填充格式，指定的字符串始终采用 ASCII 码格式填充。

interface: 表示以接口名构成接口信息，始终采用 ASCII 码格式填充。

format: 指定 Circuit ID 子选项的填充格式。

ascii: 指定以 ASCII 码格式填充 Circuit ID 子选项，即将数值转换为对应的 ASCII 码填充到 Circuit ID 子选项。

hex: 指定以十六进制数值的格式填充 Circuit ID 子选项。

【使用指导】

以不同模式填充 Circuit ID 子选项时，填充格式有所不同：

- 以用户配置的字符串填充 Circuit ID 子选项时，填充格式固定为 ASCII 码格式；
- 以 Normal 和 Verbose 模式填充 Circuit ID 子选项时，填充格式由本命令的配置决定。

如果本命令中未指定填充格式，则对于 Normal 模式，VLAN ID 和端口号均以 hex 格式填充；对于 Verbose 模式，节点标识（MAC 地址、设备的系统名称或指定的字符串）、以太网类型、框号、槽号、子槽号、接口编号均以 ASCII 码格式填充，VLAN ID 以 hex 格式填充。

- 如果本命令中指定填充格式为 **ascii**，则所有内容均以 ASCII 码格式填充。
- 如果本命令中指定填充格式为 **hex**，则对于 Normal 模式，VLAN ID 和端口号均以 **hex** 格式填充；对于 Verbose 模式，设备的节点标识、以太网类型以 ASCII 码格式填充，其余内容均以 **hex** 格式填充。

- 如果以设备的系统名称（**sysname**）作为节点标识填充 DHCP 报文的 Option 82，则系统名称中不能包含空格；否则，DHCP 中继添加或替换 Option 82 失败。

多次执行本命令，最后一次执行的命令生效。

【举例】

配置以 Verbose 模式填充 Option 82 的 Circuit ID 子选项，节点标识为设备的系统名称，填充格式为 ASCII 码格式。

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp relay information enable
[Sysname-Vlan-interface10] dhcp relay information strategy replace
[Sysname-Vlan-interface10] dhcp relay information circuit-id verbose node-identifier
sysname format ascii
```

【相关命令】

- **dhcp relay information enable**
- **dhcp relay information strategy**
- **display dhcp relay information**

1.3.9 dhcp relay information enable

dhcp relay information enable 命令用来开启 DHCP 中继支持 Option 82 功能。

undo dhcp relay information enable 命令用来关闭 DHCP 中继支持 Option 82 功能。

【命令】

```
dhcp relay information enable
undo dhcp relay information enable
```

【缺省情况】

DHCP 中继支持 Option 82 功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

【使用指导】

开启 DHCP 中继支持 Option 82 功能后，DHCP 中继将向转发给 DHCP 服务器的请求报文中增加 Option 82 选项。选项内容由 **dhcp relay information circuit-id** 命令和 **dhcp relay information remote-id** 命令决定。如果 DHCP 中继收到的请求报文中已经包含 Option 82 选项，则按照 **dhcp relay information strategy** 命令配置的策略处理请求报文。

关闭 DHCP 中继支持 Option 82 功能后，DHCP 中继不会向转发给 DHCP 服务器的请求报文中增加 Option 82 选项，也不检查收到的请求报文中是否包含 Option 82 选项。

【举例】

开启 DHCP 中继支持 Option 82 功能。

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp relay information enable
```

【相关命令】

- `dhcp relay information circuit-id`
- `dhcp relay information remote-id`
- `dhcp relay information strategy`
- `display dhcp relay information`

1.3.10 dhcp relay information remote-id

`dhcp relay information remote-id` 命令用来配置 Option 82 的 Remote ID 子选项的填充模式和填充格式。

`undo dhcp relay information remote-id` 命令用来恢复缺省情况。

【命令】

```
dhcp relay information remote-id { normal [ format { ascii | hex } ] | string
remote-id | sysname }
undo dhcp relay information remote-id
```

【缺省情况】

Option 82 的 Remote ID 子选项的填充模式为 Normal、填充格式为 hex。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

normal: 指定以 Normal 模式填充 Remote ID 子选项，填充内容为接收报文接口的 MAC 地址。

format: 指定 Remote ID 子选项的填充格式。如果未配置本参数，则以 hex 格式填充。

ascii: 指定以 ASCII 码格式填充 Remote ID 子选项，即将数值转换为对应的 ASCII 码填充到 Remote ID 子选项。

hex: 指定以十六进制数值的格式填充 Remote ID 子选项。

string remote-id: 指定以用户配置的字符串填充 Remote ID 子选项。*remote-id* 表示用户配置的用来填充 Remote ID 子选项的内容，为 1~63 个字符的字符串，区分大小写。

sysname: 指定以设备的系统名称填充 Remote ID 子选项。设备的系统名称可以通过系统视图下的 `sysname` 命令配置。

【使用指导】

以用户配置的字符串（**string**）和设备的系统名称（**sysname**）填充 Remote ID 子选项时，填充内容固定为 ASCII 格式；以 Normal 模式填充 Remote ID 子选项时，填充内容的格式由本命令配置的填充格式决定。

多次执行本命令，最后一次执行的命令生效。

【举例】

配置采用字符串 device001 填充 Option 82 的 Remote ID 子选项。

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp relay information enable
[Sysname-Vlan-interface10] dhcp relay information strategy replace
[Sysname-Vlan-interface10] dhcp relay information remote-id string device001
```

【相关命令】

- **dhcp relay information enable**
- **dhcp relay information strategy**
- **display dhcp relay information**

1.3.11 dhcp relay information strategy

dhcp relay information strategy 命令用来配置 DHCP 中继对包含 Option 82 的请求报文的处理策略。

undo dhcp relay information strategy 命令用来恢复缺省情况。

【命令】

```
dhcp relay information strategy { drop | keep | replace }
undo dhcp relay information strategy
```

【缺省情况】

DHCP 中继对带有 Option 82 的请求报文的处理策略为 **replace**。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

drop: 如果报文中带有 Option 82，则丢弃该报文。

keep: 如果报文中带有 Option 82，则保持该报文中的 Option 82 不变并进行转发。

replace: 如果报文中带有 Option 82，则按照配置的填充内容和填充格式填充 Option 82，用该选项替换报文中原有的 Option 82，并进行转发。

【使用指导】

本命令仅对包含 Option 82 的请求报文有效。

如果开启了 DHCP 中继支持 Option 82 功能，则对于接收到的不包含 Option 82 的请求报文，DHCP 中继的处理方式始终为在请求报文中添加 Option 82，并转发给 DHCP 服务器。

DHCP 中继对包含 Option 82 请求报文的处理策略为 **replace** 时，需要配置 Option 82 的填充模式和填充格式；处理策略为 **keep** 或 **drop** 时，不需要配置 Option 82 选项的填充模式和填充格式。

【举例】

配置接收到的请求报文中带有 Option 82 时，DHCP 中继保持该报文中的 Option 82 不变并进行转发。

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp relay information enable
[Sysname-Vlan-interface10] dhcp relay information strategy keep
```

【相关命令】

- **dhcp relay information enable**
- **display dhcp relay information**

1.3.12 dhcp relay master-server switch-delay

dhcp relay master-server switch-delay 命令用来配置回切主用 DHCP 服务器并指定回切延迟时间。

undo dhcp relay master-server switch-delay 命令用来恢复缺省情况。

【命令】

```
dhcp relay master-server switch-delay delay-time
undo dhcp relay master-server switch-delay
```

【缺省情况】

DHCP 中继不回切到主用 DHCP 服务器。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

delay-time：延迟时间，取值范围为 1~65535，单位为分钟。

【使用指导】

多次执行本命令，最后一次执行的命令生效。

【举例】

在 VLAN 接口 2 上配置回切主用 DHCP 服务器并指定回切延迟时间为 3 分钟。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] dhcp relay master-server switch-delay 3
```

【相关命令】

- **dhcp relay server-address algorithm**

1.3.13 dhcp relay release ip

dhcp relay release ip 命令用来配置向 DHCP 服务器请求释放客户端申请到的 IP 地址。

【命令】

```
dhcp relay release ip ip-address
```

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ip-address: 请求释放的 DHCP 客户端 IP 地址。

【使用指导】

如果 DHCP 中继上存在客户端 IP 地址对应的动态用户地址表项，则配置通过 DHCP 中继释放该客户端 IP 地址后，DHCP 中继会主动向 DHCP 服务器发送 DHCP-RELEASE 报文。DHCP 服务器收到该报文后，将会释放指定 IP 地址的绑定信息。DHCP 中继也会删除该动态用户地址表项。

【举例】

向 DHCP 服务器请求释放客户端申请到的 IP 地址 1.1.1.1。

```
<Sysname> system-view
```

```
[Sysname] dhcp relay release ip 1.1.1.1
```

1.3.14 dhcp relay server-address algorithm

dhcp relay server-address algorithm 命令用来配置 DHCP 中继选择 DHCP 服务器方式。

undo dhcp relay server-address algorithm 命令用来恢复缺省情况。

【命令】

```
dhcp relay server-address algorithm { master-backup | polling }
```

```
undo dhcp relay server-address algorithm
```

【缺省情况】

DHCP 中继同时向所有 DHCP 服务器转发 DHCP 请求报文（**polling** 方式）。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

master-backup: 主备方式，即 DHCP 中继向主用 DHCP 服务器转发 DHCP 请求报文，当主用 DHCP 服务器不可用或没有空闲地址时，再按照服务器地址配置顺序依次向其他备用 DHCP 服务器发送 DHCP 请求报文。

polling: 全部方式，即 DHCP 中继同时向所有 DHCP 服务器转发 DHCP 请求报文。

【使用指导】

多次执行本命令，最后一次执行的命令生效。

【举例】

在 VLAN 接口 2 上配置 DHCP 中继使用主备方式选择 DHCP 服务器。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] dhcp relay server-address algorithm master-backup
```

【相关命令】

- `dhcp relay dhcp-server timeout`
- `dhcp relay master-server switch-delay`
- `dhcp relay server-address`
- `remote-server algorithm`

1.3.15 dhcp relay source-address

`dhcp relay source-address` 命令用来指定 DHCP 中继向 DHCP 服务器转发报文的源地址。

`undo dhcp relay source-address` 命令用来恢复缺省情况。

【命令】

```
dhcp relay source-address { ip-address | interface interface-type
interface-number }
undo dhcp relay source-address
```

【缺省情况】

DHCP 中继向 DHCP 服务器转发报文的源地址为向 DHCP 服务器转发报文出接口的地址。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ip-address: DHCP 中继向 DHCP 服务器转发报文的源地址。

interface *interface-type interface-number*: 指定该接口 IP 地址为发送到 DHCP 服务器的报文源地址。*interface-type interface-number* 表示接口类型和接口编号。

【使用指导】

在某些组网中，多个 DHCP 中继接口 IP 地址相同或者中继接口 IP 到服务器没有可达路由，用户需要配置本命令选择中继设备上的另一个接口（一般选择的是 Loopback 口）的 IP 地址填充到发送到 DHCP 服务器的 DHCP 请求报文中的源地址字段和 Giaddr 中。

当多个 DHCP 中继接口 IP 地址相同时，导致 DHCP 中继转发 DHCP 应答报文时无法根据目的 IP 地址找到唯一的出接口。配置本功能时需要先开启 DHCP 中继支持 Option 82 功能，DHCP 中继收到 DHCP 请求报文时在 Option 82 中的子选项 sub-option5 填充正确的子网网段，服务器可以根据中继填充的 sub-option5 来分配地址，之后 DHCP 中继处理 DHCP 应答报文时通过 MAC 地址表中的接口信息转发 DHCP 应答报文。

多次执行命令，最后一次执行的命令生效。

【举例】

在 VLAN 接口 2 上指定 DHCP 中继向 DHCP 服务器转发报文的源地址为 1.1.1.1

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] dhcp relay source-address 1.1.1.1
```

【相关命令】

- **dhcp select relay**

1.3.16 dhcp smart-relay enable

dhcp smart-relay enable 命令用来开启 DHCP 中继支持 smart-relay 功能。

undo dhcp smart-relay enable 命令用来关闭 DHCP 中继支持 smart-relay 功能。

【命令】

```
dhcp smart-relay enable
undo dhcp smart-relay enable
```

【缺省情况】

DHCP 中继支持 smart-relay 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

未开启 smart-relay 功能时, DHCP 中继只能使用中继接口的主 IP 地址填充请求报文的 giaddr 字段。
开启 smart-relay 功能后, 当 DHCP 中继转发 3 次 DHCP-DISCOVER 报文后, 若还未收到 DHCP 服务器的应答报文, 则 DHCP 中继可以使用除中继接口主地址外的其他 IP 地址来填充 giaddr 字段。

【举例】

开启 DHCP 中继支持 smart-relay 功能。

```
<Sysname> system-view
[Sysname] dhcp smart-relay enable
```

【相关命令】

- **dhcp select**
- **gateway-list**

1.3.17 dhcp-server timeout

dhcp-server timeout 命令用来配置 DHCP 服务器应答超时切换时间。

dhcp-server timeout 命令用来恢复缺省情况。

【命令】

```
dhcp-server timeout time
```


undo dhcp-server timeout

【缺省情况】

配置 DHCP 服务器应答超时切换时间为 30 秒。

【视图】

DHCP 地址池视图

【缺省用户角色】

network-admin

【参数】

time: 超时切换时间，取值范围为 1~65535，单位为秒。

【使用指导】

多次执行本命令，最后一次执行的命令生效。

【举例】

在中继地址池 0 中配置 DHCP 服务器应答超时切换时间为 60 秒。

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] dhcp-server timeout 60
```

【相关命令】

- **remote-server algorithm**

1.3.18 display dhcp relay check mac-address

display dhcp relay check mac-address 命令用来显示 DHCP 中继的 MAC 地址检查表项。

【命令】

display dhcp relay check mac-address

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

DHCP 中继的 MAC 地址检查表项。

```
<Sysname> display dhcp relay check mac-address
Source-MAC      Interface      Aging-time
23f3-1122-adf1   Vlan2          10
23f3-1122-2230   Vlan3          30
```

表1-8 display dhcp relay check mac-address 命令显示信息描述表

字段	描述
Source MAC	检测到攻击的源MAC地址
Interface	攻击来源的接口
Aging-time	DDOS攻击检测表项剩余时间，单位为秒

1.3.19 display dhcp relay client-information

display dhcp relay client-information 命令用来显示 DHCP 中继的用户地址表项信息。

【命令】

```
display dhcp relay client-information [ interface interface-type
interface-number | ip ip-address ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface *interface-type interface-number*: 显示指定接口上的用户地址表项信息。
interface-type interface-number 为接口类型和接口编号。如果未指定本参数，则显示所有接口上的用户地址表项信息。

ip *ip-address*: 显示指定 IP 地址的用户地址表项信息。如果未指定本参数，则显示所有 IP 地址的用户地址表项信息。

【使用指导】

只有执行 **dhcp relay client-information record** 命令后，DHCP 中继才会记录用户地址表项信息。

【举例】

显示所有 DHCP 中继的用户地址表项信息。

```
<Sysname> display dhcp relay client-information
Total number of client-information items: 2
Total number of dynamic items: 1
Total number of temporary items: 1
IP address      MAC address      Type      Interface      VPN name
10.1.1.5        00e0-0000-0000   Temporary Vlan2          N/A
```

表1-9 display dhcp relay client-information 命令显示信息描述表

字段	描述
Total number of	用户地址信息条目总数

字段	描述
client-information items	
Total number of dynamic items	动态用户地址条目总数
Total number of temporary items	临时用户地址条目总数
IP address	DHCP客户端的IP地址
MAC address	DHCP客户端的MAC地址
Type	用户地址表项类型的取值包括： <ul style="list-style-type: none"> • Dynamic: 动态用户地址表项, 接收到 DHCP 服务器对 DHCP 客户端 REQUEST 请求的 ACK 应答后, 创建的用户表项 • Temporary: 临时用户地址表项, 接收 DHCP 客户端的 REQUEST 请求, 但未收到 DHCP 服务器 ACK 应答时, 创建的用户表项
Interface	与DHCP客户端相连的三层接口。如果用户地址表项中未记录接口, 则显示为"N/A"
VPN name	(暂不支持) VPN实例名称, 如果表项不属于任何VPN, 则显示为"N/A"

【相关命令】

- `dhcp relay client-information record`
- `reset dhcp relay client-information`

1.3.20 display dhcp relay information

`display dhcp relay information` 命令用来显示 DHCP 中继上的 Option 82 配置信息。

【命令】

```
display dhcp relay information [ interface interface-type
interface-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface interface-type interface-number: 显示指定接口上的 Option 82 配置信息。
interface-type interface-number 为接口类型和接口编号。如果未指定本参数, 则显示所有接口上的 Option 82 配置信息。

【举例】

```
# 显示所有接口上的 Option 82 配置信息。
<Sysname> display dhcp relay information
Interface: Vlan-interface100
```

```

Status: Enable
Strategy: Replace
Circuit ID Pattern: Verbose
Remote ID Pattern: Sysname
Circuit ID format: Undefined
Remote ID format: ASCII
Node identifier: aabbcc
Interface: Vlan-interface200
Status: Enable
Strategy: Replace
Circuit ID Pattern: User Defined
Remote ID Pattern: User Defined
Circuit ID format: ASCII
Remote ID format: ASCII
User defined:
Circuit ID: vlan100
Remote ID: device001

```

表1-10 display dhcp relay information 命令显示信息描述表

字段	描述
Interface	接口名
Status	Option 82的状态，取值包括： <ul style="list-style-type: none"> Enable: 开启了 DHCP 中继支持 Option 82 功能 Disable: 未开启 DHCP 中继支持 Option 82 功能
Strategy	对包含Option 82的请求报文的处理策略，取值为Drop、Keep或Replace
Circuit ID Pattern	Circuit ID子选项的填充方式，取值为Verbose、Normal或User Defined
Remote ID Pattern	Remote ID子选项的填充方式，取值为Sysname、Normal或User Defined
Circuit ID format	Circuit ID子选项的填充格式，取值为ASCII、Hex或Undefined
Remote ID format	Remote ID子选项的填充格式，取值为ASCII、Hex或Undefined
Node identifier	接入节点的标识
User defined	用户自定义的子选项内容
Circuit ID	用户自定义的Circuit ID子选项的内容
Remote ID	用户自定义的Remote ID子选项的内容

1.3.21 display dhcp relay server-address

display dhcp relay server-address 命令用来显示接口上指定的 DHCP 服务器地址信息。

【命令】

```

display dhcp relay server-address [ interface interface-type
interface-number ]

```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface interface-type interface-number: 显示指定接口上的 DHCP 服务器地址信息。*interface-type interface-number* 为接口类型和接口编号。如果未指定本参数，则显示所有接口上的 DHCP 服务器地址信息。

【举例】

显示所有接口上指定的 DHCP 服务器地址信息。

```
<Sysname> display dhcp relay server-address
Interface name      Server IP address  Public/VRF name    Class name
Vlan2               2.2.2.2           Y/--              --
Vlan2               2.2.2.3           Y/--              abc
```

表1-11 display dhcp relay server-address 命令显示信息描述表

字段	描述
Interface name	接口名
Server IP address	DHCP服务器地址
Public/VRF name	(暂不支持) DHCP服务器所在位置，取值包括： <ul style="list-style-type: none">当配置了 dhcp relay server-address 命令时，显示为--/--当配置了 dhcp relay server-address public 命令时，显示为 Y/--当配置了 dhcp relay server-address vpn-instance vpn-instance-name 命令时，显示为--/VPN 实例名称
Class name	DHCP请求报文需要匹配的DHCP用户类，如果 dhcp relay server-address 命令中未配置 class 参数，显示为--

【相关命令】

- **dhcp relay server-address**

1.3.22 display dhcp relay statistics

display dhcp relay statistics 命令用来显示 DHCP 中继的相关报文统计信息。

【命令】

display dhcp relay statistics [interface interface-type interface-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface *interface-type interface-number*: 显示指定接口的 DHCP 中继相关报文统计信息。*interface-type interface-number* 为接口类型和接口编号。如果未指定本参数，则显示所有的 DHCP 中继相关报文统计信息。

【举例】

显示所有的 DHCP 中继相关报文统计信息。

```
<Sysname> display dhcp relay statistics
DHCP packets dropped:                0
DHCP packets received from clients:   0
    DHCPDISCOVER:                    0
    DHCPREQUEST:                     0
    DHCPINFORM:                      0
    DHCPRELEASE:                     0
    DHCPDECLINE:                     0
    BOOTPREREQUEST:                  0
DHCP packets received from servers:   0
    DHCPOFFER:                       0
    DHCPACK:                         0
    DHCPNAK:                         0
    BOOTPREPLY:                      0
DHCP packets relayed to servers:      0
    DHCPDISCOVER:                    0
    DHCPREQUEST:                     0
    DHCPINFORM:                      0
    DHCPRELEASE:                     0
    DHCPDECLINE:                     0
    BOOTPREREQUEST:                  0
DHCP packets relayed to clients:      0
    DHCPOFFER:                       0
    DHCPACK:                         0
    DHCPNAK:                         0
    BOOTPREPLY:                      0
DHCP packets sent to servers:         0
    DHCPDISCOVER:                    0
    DHCPREQUEST:                     0
    DHCPINFORM:                      0
    DHCPRELEASE:                     0
    DHCPDECLINE:                     0
    BOOTPREREQUEST:                  0
DHCP packets sent to clients:         0
    DHCPOFFER:                       0
    DHCPACK:                         0
    DHCPNAK:                         0
```

表1-12 display dhcp relay statistics 命令显示信息描述表

字段	描述
DHCP packets dropped	DHCP中继丢掉的报文数
DHCP packets received from clients	DHCP中继从客户端接收的DHCP报文数
DHCP packets received from servers	DHCP中继从服务器接收的DHCP报文数
DHCP packets relayed to servers	DHCP中继转发给服务器的报文数
DHCP packets relayed to clients	DHCP中继转发给客户端的报文数
DHCP packets sent to servers	DHCP中继主动发送给服务器的DHCP报文数, 用于实现动态用户地址表项的定时刷新
DHCP packets sent to clients	DHCP中继主动发送给客户端的DHCP报文数 (目前设备作为DHCP中继时, 不会主动发送DHCP报文给客户端)

【相关命令】

- `reset dhcp relay statistics`

1.3.23 gateway-list

gateway-list 命令用来指定匹配该地址池的 DHCP 客户端所在的网段的地址。

undo gateway-list 命令用来删除指定的匹配该地址池的 DHCP 客户端所在的网段的地址。

【命令】

```
gateway-list ip-address&<1-64>
undo gateway-list [ ip-address&<1-64> ]
```

【缺省情况】

未指定匹配该地址池的 DHCP 客户端所在的网段地址。

【视图】

DHCP 地址池视图

【缺省用户角色】

network-admin

【参数】

ip-address&<1-64>: 该地址池的 DHCP 客户端所在的网段的地址。&<1-64>表示最多可以输入 64 个 IP 地址, 每个 IP 地址之间用空格分隔。

【使用指导】

一台 DHCP 中继的一个接口下可能连接不同类型的用户, 当 DHCP 中继转发 DHCP 客户端请求报文给 DHCP 服务器时, 不能再以中继接口的 IP 地址作为选择地址池的依据。为了解决这个问题, 需要使用 **gateway-list** 命令指定某个类型用户所在的网段, 并将该地址添加到转发给 DHCP 服务器的报文字段中, 为 DHCP 服务器选择地址池提供依据。

【举例】

指定匹配该地址池 0 的 DHCP 客户端所在的网段的地址为 10.1.1.1。

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] gateway-list 10.1.1.1
```

【相关命令】

- **dhcp smart-relay enable**

1.3.24 master-server switch-delay

master-server switch-delay 命令用来配置回切主用 DHCP 服务器并指定回切延迟时间。

undo master-server switch-delay 命令用来恢复缺省情况。

【命令】

```
master-server switch-delay delay-time
undo master-server switch-delay
```

【缺省情况】

DHCP 中继不回切到主用 DHCP 服务器。

【视图】

DHCP 地址池视图

【缺省用户角色】

network-admin

【参数】

delay-time：延迟时间，取值范围为 1~65535，单位为分钟。

【使用指导】

多次执行本命令，最后一次执行的命令生效。

【举例】

在 DHCP 地址池 0 上，配置回切主用 DHCP 服务器并指定回切延迟时间为 3 分钟。

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] master-server switch-delay 3
```

【相关命令】

- **remote-server algorithm**

1.3.25 remote-server

remote-server 命令用来指定中继地址池对应的 DHCP 服务器地址。

undo remote-server 命令用来删除为中继地址池指定的 DHCP 服务器地址。

【命令】

```
remote-server ip-address<1-8>
```


undo remote-server [*ip-address*&<1-8>]

【缺省情况】

未指定中继地址池的 DHCP 服务器的地址。

【视图】

DHCP 地址池视图

【缺省用户角色】

network-admin

【参数】

ip-address&<1-8>: DHCP 服务器的 IP 地址。&<1-8>表示最多可以输入 8 个不同的 IP 地址，每个 IP 地址之间需要用空格分隔。

【使用指导】

多次执行本命令，最后一次执行的命令生效。

执行 **undo remote-server** 命令时，如果未指定任何参数，则删除所有配置 DHCP 服务器地址。

【举例】

配置 DHCP 地址池 0 为中继配置的服务器地址为 10.1.1.1。

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] remote-server 10.1.1.1
```

1.3.26 remote-server algorithm

remote-server algorithm 命令用来配置 DHCP 中继选择 DHCP 服务器方式。

undo remote-server algorithm 命令用来恢复缺省情况。

【命令】

```
remote-server algorithm { master-backup | polling }
undo remote-server algorithm
```

【缺省情况】

DHCP 中继同时向所有 DHCP 服务器转发 DHCP 请求报文（**polling** 方式）。

【视图】

DHCP 地址池视图

【缺省用户角色】

network-admin

【参数】

master-backup: 主备方式，即 DHCP 中继向主用 DHCP 服务器转发 DHCP 请求报文，当主用 DHCP 服务器不可用或没有空闲地址时，再按照服务器地址配置顺序依次向其他备用 DHCP 服务器发送 DHCP 请求报文。

polling: 全部方式，即 DHCP 中继同时向所有 DHCP 服务器转发 DHCP 请求报文。

【使用指导】

多次执行本命令，最后一次执行的命令生效。

【举例】

在中继地址池 0 内，配置 DHCP 中继使用主备方式选择 DHCP 服务器。

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] remote-server algorithm master-backup
```

【相关命令】

- **dhcp relay server-address algorithm**
- **dhcp-server timeout**
- **master-server switch-delay**
- **remote-server**

1.3.27 reset dhcp relay client-information

reset dhcp relay client-information 命令用来清除 DHCP 中继的用户地址表项信息。

【命令】

```
reset dhcp relay client-information [ interface interface-type
interface-number | ip ip-address ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface interface-type interface-number: 清除指定接口上的 DHCP 中继的用户地址表项信息。*interface-type interface-number* 为接口类型和接口编号。如果未指定本参数，则清除所有接口的 DHCP 中继的用户地址表项信息。

ip ip-address: 清除指定 IP 地址的用户地址表项信息。如果未指定本参数，则清除所有 IP 地址的 DHCP 中继的用户地址表项信息。

【举例】

清除所有 DHCP 中继的用户地址表项信息。

```
<Sysname> reset dhcp relay client-information
```

【相关命令】

- **display dhcp relay client-information**

1.3.28 reset dhcp relay statistics

reset dhcp relay statistics 命令用来清除 DHCP 中继的相关报文统计信息。

【命令】

```
reset dhcp relay statistics [ interface interface-type interface-number ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface interface-type interface-number: 清除指定接口的 DHCP 中继相关报文统计信息。*interface-type interface-number* 为接口类型和接口编号。如果未指定本参数，则清除所有的 DHCP 中继相关报文统计信息。

【举例】

清除所有的 DHCP 中继相关报文统计信息。

```
<Sysname> reset dhcp relay statistics
```

【相关命令】

- **display dhcp relay statistics**

1.4 DHCP客户端配置命令

1.4.1 dhcp client dad enable

dhcp client dad enable 命令用来开启地址冲突检查功能。

undo dhcp client dad enable 命令用来关闭地址冲突检查功能。

【命令】

```
dhcp client dad enable
```

```
undo dhcp client dad enable
```

【缺省情况】

地址冲突检查功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

DHCP 客户端通过发送和接收 ARP 报文，对 DHCP 服务器分配的 IP 地址进行地址冲突检测，如果攻击者仿冒地址拥有者进行 ARP 应答，就可以欺骗 DHCP 客户端，导致 DHCP 客户端无法正常使用分配到的 IP 地址。在网络中存在上述攻击者时，建议在客户端上关闭地址冲突检查功能。

【举例】

关闭地址冲突检查功能。

```
<Sysname> system-view
[Sysname] undo dhcp client dad enable
```

1.4.2 dhcp client dscp

dhcp client dscp 命令用来配置 DHCP 客户端发送 DHCP 报文的 DSCP 优先级。

undo dhcp client dscp 命令用来恢复缺省情况。

【命令】

```
dhcp client dscp dscp-value
undo dhcp client dscp
```

【缺省情况】

DHCP 客户端发送 DHCP 报文的 DSCP 优先级为 56。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

dscp-value: DHCP 请求报文的 DSCP 优先级，取值范围为 0~63。

【使用指导】

DSCP 优先级用来体现报文自身的优先等级，决定报文传输的优先程度。配置的 DSCP 优先级的取值越大，报文的优先级越高。

【举例】

配置 DHCP 客户端发送的 DHCP 报文的 DSCP 优先级为 30。

```
<Sysname> system-view
[Sysname] dhcp client dscp 30
```

1.4.3 dhcp client identifier

dhcp client identifier 命令用来配置接口使用指定的 DHCP 客户端 ID。

undo dhcp client identifier 命令用来恢复缺省情况。

【命令】

```
dhcp client identifier { ascii ascii-string | hex hex-string | mac
interface-type interface-number }
undo dhcp client identifier
```

【缺省情况】

根据本接口的 MAC 地址生成 DHCP 客户端 ID。如果本接口没有 MAC 地址，则获取设备第一个以太接口的 MAC 地址生成 DHCP 客户端 ID。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ascii *ascii-string*: 使用指定的 ASCII 字符串作为该接口的客户端 ID，为 1~63 个字符的字符串，区分大小写。

hex *hex-string*: 使用指定的十六进制数作为该接口的客户端 ID，为 4~64 个字符的字符串。

mac *interface-type interface-number*: 使用指定接口的 MAC 地址作为客户端 ID。
interface-type interface-number 表示接口类型和接口编号。

【使用指导】

DHCP 客户端 ID 用来填充 DHCP 报文 Option 61，作为识别 DHCP 客户端的唯一标识。DHCP 服务器可以根据客户端 ID 为特定的客户端分配特定的 IP 地址。用户可以通过以下三种方法指定 DHCP 客户端 ID：ASCII 字符串、十六进制数或使用指定接口的 MAC 地址作为 DHCP 客户端 ID，以上三种方式都需要由用户保证不同客户端的客户端 ID 不会相同。

【举例】

```
# 配置 VLAN 接口 10 使用的客户端 ID 为十六进制数 FFFFFFFF。
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp client identifier hex FFFFFFFF
```

【相关命令】

- **display dhcp client**

1.4.4 display dhcp client

display dhcp client 命令用来显示 DHCP 客户端的相关信息。

【命令】

display dhcp client [**verbose**] [**interface** *interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

verbose: 显示 DHCP 客户端的详细信息。如果未指定本参数，则显示 DHCP 客户端简要信息。

interface *interface-type interface-number*: 显示指定接口的 DHCP 客户端相关信息。
interface-type interface-number 为接口类型和接口编号。如果未指定本参数，则显示所有接口的 DHCP 客户端信息。

【举例】

```
# 显示所有接口的 DHCP 客户端简要信息。
```

```
<Sysname> display dhcp client
Vlan-interface10 DHCP client information:
  Current state: BOUND
  Allocated IP: 40.1.1.20 255.255.255.0
  Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
  DHCP server: 40.1.1.2
# 显示所有接口的 DHCP 客户端详细信息。
<Sysname> display dhcp client verbose
Vlan-interface10 DHCP client information:
  Current state: BOUND
  Allocated IP: 40.1.1.20 255.255.255.0
  Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
  Lease from May 21 19:00:29 2012    to    May 31 19:00:29 2012
  DHCP server: 40.1.1.2
  Transaction ID: 0x1c09322d
  Default router: 40.1.1.2
Classless static routes:
  Destination: 1.1.0.1, Mask: 255.0.0.0, NextHop: 192.168.40.16
  Destination: 10.198.122.63, Mask: 255.255.255.255, NextHop: 192.168.40.16
DNS servers: 44.1.1.11 44.1.1.12
Domain name: ddd.com
Boot servers: 200.200.200.200 1.1.1.1
ACS parameter:
  URL: http://192.168.1.1:7547/acs
  Username: bims
  Password: *****
Client ID type: acsii(type value=00)
Client ID value: 000c.29d3.8659-Vlan10
Client ID (with type) hex: 0030-3030-632e-3239-
                           6433-2e38-3635-392d-
                           4574-6830-2f30-2f32
T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.
```

表1-13 display dhcp client 命令显示信息描述表

字段	描述
XXXX DHCP client information	作为DHCP客户端的接口信息
Current state	DHCP客户端状态机的当前状态，取值包括： <ul style="list-style-type: none">• HALT：停止申请 IP 地址状态；• INIT：初始化状态；• SELECTING：发送 DHCP-DISCOVER 报文寻找 DHCP 服务器后，进入该状态，等待 DHCP 服务器的响应报文；• REQUESTING：发送 DHCP-REQUEST 报文请求 IP 地址后，进入该状态，等待 DHCP 服务器的响应报文；• BOUND：接收到 DHCP 服务器发送的 DHCP-ACK 报文，成功获取 IP 地址后，进入该状态；• RENEWING：T1 定时器超时后，进入该状态；

字段	描述
	<ul style="list-style-type: none"> REBOUNDING: T2 定时器超时后, 进入该状态。
Allocated IP	DHCP服务器为接口分配的IP地址
Allocated lease	租约时长
T1	DHCP客户端的一半左右租约时间 (以秒为单位)
T2	DHCP客户端的7/8租约时间 (以秒为单位)
Lease from....to....	租约起止时间
DHCP server	选择的DHCP服务器的地址
Transaction ID	DHCP客户端发起申请时生成的一个随机数, 用来唯一标识一次申请过程
Default router	为DHCP客户端指定的网关地址
Classless static routes	为DHCP客户端指定的无分类静态路由
Static routes	为DHCP客户端指定的有分类静态路由
DNS servers	为DHCP客户端指定的DNS服务器地址
Domain name	为DHCP客户端指定的域名后缀
Boot servers	为DHCP客户端指定的PXE引导服务器地址, 通过Option 43获取, 最多可以获取16个地址
ACS parameter	ACS参数
URL	ACS的URL地址
Username	登录ACS设备使用的用户名
Password	登录ACS设备使用的密码, 若存在密码, 则显示为“*****”; 若不存在密码, 则不显示此项;
Client ID type	DHCP客户端ID的类型, type value表示类型值。类型为ASCII时, type value为00; 为MAC address时, type value为01; 为Hex时, type value为配置的十六进制数的前两位
Client ID value	DHCP客户端ID的取值
Client ID (with type) hex	DHCP客户端ID的十六进制形式 (带类型值字段)
T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.	在多少时间后T1定时器 (即一半左右租约时间) 将到期

【相关命令】

- dhcp client identifier
- ip address dhcp-alloc

1.4.5 ip address dhcp-alloc

ip address dhcp-alloc 命令用来配置接口通过 DHCP 协议获取 IP 地址。

undo ip address dhcp-alloc 命令用来取消接口通过 DHCP 协议获取的 IP 地址。

【命令】

```
ip address dhcp-alloc
undo ip address dhcp-alloc
```

【缺省情况】

接口不通过 DHCP 协议获取 IP 地址。

【视图】

接口视图

【缺省用户角色】

network-admin

【使用指导】

取消接口通过 DHCP 协议获取 IP 地址时，DHCP 客户端会发送 DHCP-RELEASE 报文通知 DHCP 服务器释放租约。如果此时该接口处于 down 状态，则无法保证报文成功发送。

如果配置子接口通过 DHCP 协议获取 IP 地址，在其主接口上执行 **shutdown** 命令时，DHCP 客户端不会发送请求释放子接口 IP 地址租约的 DHCP-RELEASE 报文。

【举例】

在 VLAN 接口 10 上配置接口通过 DHCP 协议获取 IP 地址。

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ip address dhcp-alloc
```

【相关命令】

- **display dhcp client**

1.5 DHCP Snooping配置命令



说明

设备只有位于 DHCP 客户端与 DHCP 服务器之间，或 DHCP 客户端与 DHCP 中继之间时，DHCP Snooping 功能配置后才能正常工作；设备位于 DHCP 服务器与 DHCP 中继之间时，DHCP Snooping 功能配置后不能正常工作。

1.5.1 dhcp snooping binding database filename

dhcp snooping binding database filename 命令用来指定存储 DHCP Snooping 表项的文件名称。

undo dhcp snooping binding database filename 命令用来恢复缺省情况。

【命令】

```
dhcp snooping binding database filename { filename | url url [ username
username [ password { cipher | simple } string ] ] }
```


undo dhcp snooping binding database filename

【缺省情况】

未指定存储文件名称。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

filename: 目标文件名，该配置用于本地存储模式。文件名取值范围的详细介绍，请参见“基础配置指导”中的“文件系统管理”。

url url: 配置远程目标文件 URL，为 1~255 个字符的字符串，区分大小写，该配置用于远程文件系统模式。此参数中不能包含用户名和密码，和参数 **username** 和 **string** 配合使用。远程目标文件 URL 是否支持路径格式遵循远程服务器端规格。

username username: 配置登录远程目标文件 URL 时的用户名，为 1~32 个字符的字符串，区分大小写。如果未指定本参数，则表示登录远程目标文件 URL 时无需使用用户名。

cipher: 表示以密文方式设置用户密码。

simple: 表示以明文方式设置用户密码，该密码将以密文形式存储。

string: 密码字符串，区分大小写。明文密码为 1~32 个字符的字符串，密文密码为 1~73 个字符的字符串。如果未指定本参数，则表示登录远程目标文件 URL 时无需使用密码。

【使用指导】

存储 DHCP Snooping 表项时，如果设备中还不存在对应名称的文件，则设备会自动创建该文件。

执行本命令后，会立即触发一次表项备份。之后，如果未配置 **dhcp snooping binding database update interval** 命令，若表项发生变化，默认在 300 秒之后刷新存储文件；若表项未发生变化，则不再刷新存储文件。如果配置了 **dhcp snooping binding database update interval** 命令，若表项发生变化，则到达刷新时间间隔后刷新存储文件；若表项未发生变化，则不再刷新存储文件。

参数 **filename** 不支持远程目标文件 URL，配置远程目标文件 URL 请使用 **url**、**username**、**string** 配合使用。

频繁擦写本地存储介质可能会影响存储介质寿命，建议使用远程文件系统模式存储 DHCP Snooping 表项文件。

当进行远程存储时，支持 FTP 和 TFTP 协议：

- 当采用 FTP 或 TFTP 协议时，服务器地址支持 IPv4 形式或 IPv6 形式，并且支持 DNS 域名方式。服务器地址为 IPv6 地址形式时需使用方括号（“[”和“]”）引用。配置服务器地址为 DNS 域名格式时请勿使用方括号引用。
- 当采用 FTP 协议时，URL 采用“ftp://服务器地址[:端口号]/文件路径”的形式，如有用户名和密码请分别使用参数 **username** 和参数 **string** 进行配置，用户名和密码必须和服务器上的配置一致，如果服务器只对用户名进行认证，则不用输入密码。
- 当采用 TFTP 协议时，URL 采用“tftp://服务器地址[:端口号]/文件路径”的形式。

【举例】

配置存储 DHCP Snooping 表项的文件名为 database.dhcp。

```
<Sysname> system-view
```

```
[Sysname] dhcp snooping binding database filename database.dhcp
```

配置远程存储 DHCP Snooping 表项至 IP 地址为 1.1.1.1 的 ftp 服务器工作目录下,用户名为 1, 密码为 1, 文件名为 database.dhcp。

```
<Sysname> system-view
```

```
[Sysname] dhcp snooping binding database filename url ftp://10.1.1.1/database.dhcp username 1 password simple 1
```

配置远程存储 DHCP Snooping 表项至 IP 地址为 10.1.1.1 的 tftp 服务器工作目录下, 文件名为 database.dhcp。

```
<Sysname> system-view
```

```
[Sysname] dhcp snooping binding database filename tftp://10.1.1.1/database.dhcp
```

【相关命令】

- **dhcp snooping binding database update interval**

1.5.2 dhcp snooping binding database update interval

dhcp snooping binding database update interval 命令用来配置刷新 DHCP Snooping 表项存储文件的延迟时间。

undo dhcp snooping binding database update interval 命令用来恢复缺省情况。

【命令】

```
dhcp snooping binding database update interval interval
```

```
undo dhcp snooping binding database update interval
```

【缺省情况】

若 DHCP Snooping 表项不变化, 则不刷新存储文件; 若 DHCP Snooping 表项发生变化, 默认在 300 秒之后刷新存储文件。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval: 刷新延迟时间, 取值范围为 60~864000, 单位为秒。

【使用指导】

执行本命令后, 当 DHCP Snooping 表项发生变化后, DHCP Snooping 设备开始计时, 当本命令配置的延迟时间到达后, DHCP Snooping 会把这个时间段内表项所有的变化信息备份到固化文件中。

如果未通过 **dhcp snooping binding database filename** 命令指定存储表项的文件, 则本命令不会生效。

【举例】

若 DHCP Snooping 表项发生变化，在 600 秒后刷新表项存储文件。

```
<Sysname> system-view
[Sysname] dhcp snooping binding database update interval 600
```

【相关命令】

- **dhcp snooping binding database filename**

1.5.3 dhcp snooping binding database update now

dhcp snooping binding database update now 命令用来将当前的 DHCP Snooping 表项保存到用户指定的文件中。

【命令】

dhcp snooping binding database update now

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

本命令只用来触发一次 DHCP Snooping 表项的备份。

如果未通过 **dhcp snooping binding database filename** 命令指定存储表项的文件，则本命令不会生效。

【举例】

将当前的 DHCP Snooping 表项保存到文件中。

```
<Sysname> system-view
[Sysname] dhcp snooping binding database update now
```

【相关命令】

- **dhcp snooping binding database filename**

1.5.4 dhcp snooping binding record

dhcp snooping binding record 命令用来开启端口的 DHCP Snooping 表项记录功能。

undo dhcp snooping binding record 命令用来关闭端口的 DHCP Snooping 表项记录功能。

【命令】

dhcp snooping binding record
undo dhcp snooping binding record

【缺省情况】

端口 DHCP Snooping 表项记录功能处于关闭状态。

【视图】

二层以太网接口视图/二层聚合接口视图

VLAN 视图

【缺省用户角色】

network-admin

【使用指导】

用户可在 DHCP Snooping 设备直接与客户端连接的端口上开启 DHCP Snooping 表项记录功能。
在端口上开启 DHCP Snooping 表项记录功能后，设备将监听该端口上接收的报文，生成 DHCP Snooping 表项。

【举例】

开启端口 GigabitEthernet1/0/1 的 DHCP Snooping 表项记录功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping binding record
```

1.5.5 dhcp snooping check mac-address

dhcp snooping check mac-address 命令用来开启 DHCP Snooping 的 MAC 地址检查功能。

undo dhcp snooping check mac-address 命令用来关闭 DHCP Snooping 的 MAC 地址检查功能。

【命令】

```
dhcp snooping check mac-address
undo dhcp snooping check mac-address
```

【缺省情况】

DHCP Snooping 的 MAC 地址检查功能处于关闭状态。

【视图】

二层以太网接口视图/二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

开启该功能后，DHCP Snooping 检查接收到的 DHCP 请求报文中的 chaddr 字段和数据帧的源 MAC 地址字段是否一致。如果一致，则认为该报文合法，将其转发给 DHCP 服务器；如果不一致，则丢弃该报文。

【举例】

开启 DHCP Snooping 的 MAC 地址检查功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping check mac-address
```

1.5.6 dhcp snooping check request-message

dhcp snooping check request-message 命令用来开启 DHCP Snooping 的 DHCP 请求方向报文检查功能。

undo dhcp snooping check request-message 命令用来关闭 DHCP Snooping 的 DHCP 请求方向报文检查功能。

【命令】

dhcp snooping check request-message

undo dhcp snooping check request-message

【缺省情况】

DHCP Snooping 的 DHCP 请求方向报文检查功能处于关闭状态。

【视图】

二层以太网接口视图/二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

本功能用来检查 DHCP 续约报文、DHCP-DECLINE 和 DHCP-RELEASE 三种 DHCP 请求方向的报文，以防止非法客户端伪造这三种报文对 DHCP 服务器进行攻击。

如果开启了该功能，则 DHCP Snooping 设备接收到上述报文后，检查本地是否存在与接收报文匹配的 DHCP Snooping 表项。若存在，则接收报文信息与 DHCP Snooping 表项信息一致时，认为该报文为合法的请求方向报文，将其转发给 DHCP 服务器；不一致时，认为该报文为伪造的请求方向报文，将其丢弃。若不存在，则认为该报文合法，将其转发给 DHCP 服务器。

【举例】

开启 DHCP Snooping 的 DHCP 请求方向报文检查功能。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] dhcp snooping check request-message
```

1.5.7 dhcp snooping deny

dhcp snooping deny 命令用来在端口上开启 DHCP Snooping 报文阻断功能。

undo dhcp snooping deny 命令用来在端口上关闭 DHCP Snooping 报文阻断功能。

【命令】

dhcp snooping deny

undo dhcp snooping deny

【缺省情况】

端口上的 DHCP Snooping 报文阻断功能处于关闭状态。

【视图】

二层以太网接口视图/二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

在某些组网环境下，用户需要在 DHCP Snooping 设备的某一端口上丢弃该端口收到的所有 DHCP 请求方向报文，而又不影响其他端口正常接收 DHCP 报文。这时，用户可以在该端口上开启 DHCP Snooping 报文阻断功能。

【举例】

在端口 GigabitEthernet1/0/1 上开启 DHCP Snooping 报文阻断功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping deny
```

1.5.8 dhcp snooping disable

dhcp snooping disable 命令用来关闭接口的 DHCP Snooping 功能。

undo dhcp snooping disable 命令用来恢复缺省情况。

【命令】

```
dhcp snooping disable
undo dhcp snooping disable
```

【缺省情况】

若接口所在设备或 VLAN 上已经开启 DHCP Snooping 功能，则接口的 DHCP Snooping 功能处于开启状态；若接口所在设备或 VLAN 上未开启 DHCP Snooping 功能，则接口的 DHCP Snooping 功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

【使用指导】

当管理员在设备或 VLAN 中开启 DHCP Snooping 功能后，该设备或整个 VLAN 内的所有接口上都开启了 DHCP Snooping 功能。为了能灵活控制 DHCP Snooping 功能生效的接口范围，用户可以通过本功能关闭某个接口上的 DHCP Snooping 功能。

【举例】

关闭接口 GigabitEthernet1/0/1 上的 DHCP Snooping 功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping disable
```

1.5.9 dhcp snooping enable

dhcp snooping enable 命令用来全局开启 DHCP Snooping 功能。

undo dhcp snooping enable 命令用来全局关闭 DHCP Snooping 功能。

【命令】

```
dhcp snooping enable
undo dhcp snooping enable
```

【缺省情况】

全局的 DHCP Snooping 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

全局开启 DHCP Snooping 功能后，如果不信任端口接收到 DHCP 服务器发送的报文，将丢弃该报文，以保证客户端从合法的 DHCP 服务器获取 IP 地址。

在全局 DHCP Snooping 功能关闭后，所有端口都可转发 DHCP 服务器的响应报文。

【举例】

全局开启 DHCP Snooping 功能。

```
<Sysname> system-view
[Sysname] dhcp snooping enable
```

1.5.10 dhcp snooping enable vlan

dhcp snooping enable vlan 命令用来在指定 VLAN 内开启 DHCP Snooping 功能。

undo dhcp snooping enable vlan 命令用来在指定 VLAN 内关闭 DHCP Snooping 功能。

【命令】

```
dhcp snooping enable vlan vlan-id-list
undo dhcp snooping enable vlan vlan-id-list
```

【缺省情况】

所有 VLAN 内的 DHCP Snooping 功能均处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

vlan-id-list：VLAN 列表，表示方式为 *vlan-id-list* = { *vlan-id1* [**to** *vlan-id2*] }&<1-10>，*vlan-id* 取值范围为 1~4094，*vlan-id2* 的值要大于或等于 *vlan-id1* 的值，&<1-10>表示前面的参数最多可以重复输入 10 次。

【使用指导】

在指定 VLAN 内开启 DHCP Snooping 功能后，如果 VLAN 内的不信任端口接收到 DHCP 服务器发送的应答报文，该接口会丢弃该报文，以保证 DHCP 客户端从合法的 DHCP 服务器获取 IP 地址。

在指定 VLAN 内关闭 DHCP Snooping 功能后，该 VLAN 内所有接口都会转发 DHCP 服务器发送的应答报文。

【举例】

在 VLAN 5、VLAN 10 到 VLAN 20 和 VLAN 32 中开启 DHCP Snooping 功能。

```
<Sysname> system-view
[Sysname] dhcp snooping enable vlan 5 10 to 20 32
```

1.5.11 dhcp snooping information circuit-id

dhcp snooping information circuit-id 命令用来配置 Option 82 的 Circuit ID 子选项的填充模式和填充格式。

undo dhcp snooping information circuit-id 命令用来恢复缺省情况。

【命令】

```
dhcp snooping information circuit-id { [ vlan vlan-id ] string circuit-id |
{ normal | verbose [ node-identifier { mac | sysname | user-defined
node-identifier } ] } [ format { ascii | hex } ] }
undo dhcp snooping information circuit-id [ vlan vlan-id ]
```

【缺省情况】

Option 82 的 Circuit ID 子选项的填充模式为 Normal，填充格式为 hex。

【视图】

二层以太网接口视图/二层聚合接口视图/ONU 接口视图

【缺省用户角色】

network-admin

【参数】

vlan *vlan-id*: 为从指定 VLAN 内收到的 DHCP 报文填充 Circuit ID 子选项。如果未指定本参数，则表示为缺省 VLAN 内收到的 DHCP 报文填充 Circuit ID 子选项。

string *circuit-id*: 指定以用户配置的字符串填充 Circuit ID 子选项。*circuit-id* 表示用户配置的用来填充 Circuit ID 子选项的内容，为 3~63 个字符的字符串，区分大小写。

normal: 指定以 Normal 模式填充 Circuit ID 子选项，填充内容为 VLAN ID 和端口号。

verbose: 指定以 Verbose 模式填充 Circuit ID 子选项。填充的内容为节点标识、接口信息和接口所在的 VLAN 编号。节点标识缺省以节点的 MAC 地址构成；接口信息缺省由以太网类型（取值固定为“eth”）、框号、槽号、子槽号和接口编号组成。

node-identifier { mac | sysname | user-defined *node-identifier* }: 指定接入节点的标识。

- **mac**: 表示以节点的 MAC 地址作为节点标识。

- **sysname**: 表示以节点的设备名称作为节点标识。设备的系统名称可以通过系统视图下的 **sysname** 命令配置。不管配置了哪种填充格式,设备的系统名称始终采用 ASCII 码格式填充。
- **user-defined node-identifier**: 表示以指定的字符串作为节点标识, *node-identifier* 为 1~50 个字符的字符串, 区分大小写。不管配置了哪种填充格式, 指定的字符串始终采用 ASCII 码格式填充。

format: 指定 Circuit ID 子选项的填充格式。

ascii: 指定以 ASCII 码格式填充 Circuit ID 子选项, 即将数值转换为对应的 ASCII 码填充到 Circuit ID 子选项。

hex: 指定以十六进制数值的格式填充 Circuit ID 子选项。

【使用指导】

以用户配置的字符串填充 Circuit ID 子选项时, 填充格式固定为 ASCII 码格式。

以 Normal 和 Verbose 模式填充 Circuit ID 子选项时, 填充格式由本命令的配置决定。

- 如果本命令中未指定填充格式, 则对于 Normal 模式, VLAN ID 和端口号均以 hex 格式填充; 对于 Verbose 模式, 节点标识 (MAC 地址、设备的系统名称或指定的字符串)、以太网类型、框号、槽号、子槽号、接口编号均以 ASCII 码格式填充, VLAN ID 以 hex 格式填充。
- 如果本命令中指定填充格式为 **ascii**, 则所有内容均以 ASCII 码格式填充。
- 如果本命令中指定填充格式为 **hex**, 则对于 Normal 模式, VLAN ID 和端口号均以 hex 格式填充; 对于 Verbose 模式, 设备的节点标识、以太网类型以 ASCII 码格式填充, 其余内容均以 hex 格式填充。

如果以设备的系统名称 (**sysname**) 作为节点标识填充 DHCP 报文的 Option 82, 则系统名称中不能包含空格; 否则, DHCP Snooping 添加或替换 Option 82 失败

多次执行该命令, 最后一次执行的命令生效。

【举例】

配置以 Verbose 模式填充 Option 82 的 Circuit ID 子选项, 节点标识为设备的系统名称, 填充格式为 ASCII 码格式。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping information enable
[Sysname-GigabitEthernet1/0/1] dhcp snooping information strategy replace
[Sysname-GigabitEthernet1/0/1] dhcp snooping information circuit-id verbose node-identifier sysname format ascii
```

【相关命令】

- **dhcp snooping information enable**
- **dhcp snooping information strategy**
- **display dhcp snooping information**

1.5.12 dhcp snooping information enable

dhcp snooping information enable 命令用来开启 DHCP Snooping 支持 Option 82 功能。

undo dhcp snooping information enable 命令用来关闭 DHCP Snooping 支持 Option 82 功能。

【命令】

```
dhcp snooping information enable
undo dhcp snooping information enable
```

【缺省情况】

DHCP Snooping 支持 Option 82 功能处于关闭状态。

【视图】

二层以太网接口视图/二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

开启 DHCP Snooping 支持 Option 82 功能后，DHCP Snooping 将向转发给 DHCP 服务器的请求报文中增加 Option 82 选项。选项内容由 **dhcp snooping information circuit-id** 和 **dhcp snooping information remote-id** 决定。如果 DHCP Snooping 收到的请求报文中已经包含 Option 82 选项，则按照 **dhcp snooping information strategy** 配置的策略处理请求报文。

【举例】

```
# 开启 DHCP Snooping 支持 Option 82 功能。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping information enable
```

【相关命令】

- **dhcp snooping information circuit-id**
- **dhcp snooping information remote-id**
- **dhcp snooping information strategy**

1.5.13 dhcp snooping information remote-id

dhcp snooping information remote-id 命令用来配置 Option 82 的 Remote ID 子选项的填充模式和填充格式。

undo dhcp snooping information remote-id 命令用来恢复缺省情况。

【命令】

```
dhcp snooping information remote-id { normal [ format { ascii | hex } ] | [ vlan
vlan-id ] { string remote-id | sysname } }
undo dhcp snooping information remote-id [ vlan vlan-id ]
```

【缺省情况】

Option 82 的 Remote ID 子选项的填充模式为 Normal、填充格式为 hex。

【视图】

二层以太网接口视图/二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

vlan *vlan-id*: 为从指定 VLAN 内收到的 DHCP 报文填充 Remote ID 子选项。如果未指定本参数，则表示为缺省 VLAN 内收到的 DHCP 报文填充 Remote ID 子选项。

string *remote-id*: 指定以用户配置的字符串填充 Remote ID 子选项。*remote-id* 表示用户配置的用来填充 Remote ID 子选项的内容，为 1~63 个字符的字符串，区分大小写。

sysname: 指定以设备的系统名称填充 Remote ID 子选项。设备的系统名称可以通过系统视图下的 **sysname** 命令配置。

normal: 指定以 Normal 模式填充 Remote ID 子选项，填充内容为接收报文接口的 MAC 地址。

format: 指定 Remote ID 子选项的填充格式。如果未指定本参数，则以 hex 模式填充。

ascii: 指定以 ASCII 码格式填充 Remote ID 子选项，即将数值转换为对应的 ASCII 码填充到 Remote ID 子选项。

hex: 指定以十六进制数值的格式填充 Remote ID 子选项。

【使用指导】

以用户配置的字符串（**string**）和设备的系统名称（**sysname**）填充 Remote ID 子选项时，填充内容固定为 ASCII 格式；以 Normal 模式填充 Remote ID 子选项时，填充内容的格式由本命令配置的填充格式决定。

多次执行本命令，最后一次执行的命令生效。

【举例】

配置采用字符串 device001 填充 Option 82 的 Remote ID 子选项。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping information enable
[Sysname-GigabitEthernet1/0/1] dhcp snooping information strategy replace
[Sysname-GigabitEthernet1/0/1] dhcp snooping information remote-id string device001
```

【相关命令】

- **dhcp snooping information enable**
- **dhcp snooping information strategy**
- **display dhcp snooping information**

1.5.14 dhcp snooping information strategy

dhcp snooping information strategy 命令用来配置 DHCP Snooping 对包含 Option 82 的请求报文的处理策略。

undo dhcp snooping information strategy 命令用来恢复缺省情况。

【命令】

```
dhcp snooping information strategy { drop | keep | replace }
undo dhcp snooping information strategy
```

【缺省情况】

对带有 Option 82 的请求报文的处理策略为 **replace**。

【视图】

二层以太网接口视图/二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

drop: 如果报文中带有 Option 82，则丢弃该报文。

keep: 如果报文中带有 Option 82，则保持该报文中的 Option 82 不变并进行转发。

replace: 如果报文中带有 Option 82，则按照配置的填充格式填充 Option 82，用该选项替换报文中原有的 Option 82，并进行转发。

【使用指导】

本命令仅对包含 Option 82 的请求报文有效。

如果开启了 DHCP Snooping 支持 Option 82 功能，则对于接收到的不包含 Option 82 的请求报文，DHCP Snooping 的处理方式始终为在请求报文中添加 Option 82，并将报文转发给 DHCP 服务器。

DHCP Snooping 对包含 Option 82 请求报文的处理策略为 **replace** 时，需要配置 Option 82 的填充模式和填充格式；处理策略为 **keep** 或 **drop** 时，不需要配置 Option 82 选项的填充模式和填充格式。

【举例】

配置 DHCP Snooping 对带有 Option 82 的请求报文使用 **keep** 策略。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping information enable
[Sysname-GigabitEthernet1/0/1] dhcp snooping information strategy keep
```

【相关命令】

- **dhcp snooping information circuit-id**
- **dhcp snooping information remote-id**

1.5.15 dhcp snooping log enable

dhcp snooping log enable 命令用来开启 DHCP Snooping 日志信息功能。

undo dhcp snooping log enable 命令关闭 DHCP Snooping 日志信息功能。

【命令】

```
dhcp snooping log enable
undo dhcp snooping log enable
```

【缺省情况】

DHCP Snooping 日志信息功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

DHCP Snooping 日志可以方便管理员定位问题和解决问题。DHCP Snooping 设备生成 DHCP Snooping 日志信息会交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

当 DHCP Snooping 设备输出大量日志信息时，可能会降低设备性能。为了避免该情况的发生，用户可以关闭 DHCP Snooping 日志信息功能，使得 DHCP Snooping 设备不再输出日志信息。

【举例】

开启 DHCP Snooping 日志信息功能。

```
<Sysname> system-view
[Sysname] dhcp snooping log enable
```

1.5.16 dhcp snooping max-learning-num

dhcp snooping max-learning-num 命令用来配置接口动态学习 DHCP Snooping 表项的最大数目。

undo dhcp snooping max-learning-num 命令用来恢复缺省情况。

【命令】

```
dhcp snooping max-learning-num max-number
undo dhcp snooping max-learning-num
```

【缺省情况】

不限制接口动态学习 DHCP Snooping 表项的最大数目。

【视图】

二层以太网接口视图/二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

max-number：接口动态学习 DHCP Snooping 表项的最大数目，取值范围为 1～4294967295。

【使用指导】

接口动态学习的 DHCP Snooping 表项数达到最大数目后，不影响 DHCP Snooping 功能正常运行，但是接口不会继续学习新的 DHCP Snooping 表项。

【举例】

配置二层以太网接口 GigabitEthernet1/0/1 动态学习 DHCP Snooping 表项的最大数目为 10。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] dhcp snooping max-learning-num 10
```

1.5.17 dhcp snooping rate-limit

dhcp snooping rate-limit 命令用来开启 DHCP Snooping 的报文限速功能，即限制接口接收 DHCP 报文的速率。

undo dhcp snooping rate-limit 命令用来关闭 DHCP Snooping 的报文限速功能。

【命令】

```
dhcp snooping rate-limit rate
undo dhcp snooping rate-limit
```

【缺省情况】

DHCP Snooping 的报文限速功能处于关闭状态，即不限制接口接收 DHCP 报文的速率。

【视图】

二层以太网接口视图/二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

rate: 接口接收 DHCP 报文的最高速率，单位为 Kbps，取值范围为 64~512。

【使用指导】

只有开启 DHCP Snooping 功能后，本命令的配置才会生效。

如果接口接收到的 DHCP 报文速率超过了限制，则丢弃超过速率限制的 DHCP 报文。

如果二层以太网接口加入了聚合组，则该接口采用对应二层聚合接口下的 DHCP 报文限速配置。如果二层以太网接口离开聚合组，则该接口采用二层以太网接口下的 DHCP 报文限速配置。

设备支持的速率值是 8 的整数倍，当用户设置的速率值为 67 时，实际的生效值是 64 或 72。

【举例】

配置二层以太网接口 GigabitEthernet1/0/1 接收 DHCP 报文的最高速率为 64Kbps。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping rate-limit 64
```

1.5.18 dhcp snooping trust

dhcp snooping trust 命令用来配置端口为信任端口。

undo dhcp snooping trust 命令用来恢复端口为不信任端口。

【命令】

```
dhcp snooping trust
undo dhcp snooping trust
```

【缺省情况】

在开启 DHCP Snooping 功能后，设备上所有支持 DHCP Snooping 功能的端口均为不信任端口。

【视图】

二层以太网接口视图/二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

指向 DHCP 服务器方向的端口需要设置为信任端口，其他端口设置为不信任端口，从而保证 DHCP 客户端只能从合法的 DHCP 服务器获取 IP 地址，私自架设的伪 DHCP 服务器无法为 DHCP 客户端分配 IP 地址。

【举例】

配置二层以太网接口 GigabitEthernet1/0/1 为信任端口。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping trust
```

【相关命令】

- **display dhcp snooping trust**

1.5.19 dhcp snooping trust interface

dhcp snooping trust interface 命令用来配置指定端口为 VLAN 下 DHCP Snooping 功能的信任端口。

undo dhcp snooping trust interface 命令用来恢复端口为不信任端口。

【命令】

```
dhcp snooping trust interface interface-type interface-number
undo dhcp snooping trust interface interface-type interface-number
```

【缺省情况】

在 VLAN 内开启 DHCP Snooping 功能后，该 VLAN 内所有支持 DHCP Snooping 功能的接口均为不信任端口。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

【参数】

interface-type interface-number: 信任端口的类型和编号。

【使用指导】

在 VLAN 内连接 DHCP 服务器的接口需要设置为信任端口，其他接口设置为不信任端口，从而保证 DHCP 客户端只能从合法的 DHCP 服务器获取 IP 地址，私自架设的伪 DHCP 服务器无法为 DHCP 客户端分配 IP 地址。

在同一 VLAN 下多次执行本命令，可以为该 VLAN 下的 DHCP Snooping 功能指定多个信任端口。

为使配置生效，请保证将指定的信任端口加入到 VLAN 中。

【举例】

```
# 配置接口 GigabitEthernet1/0/1 为 VLAN 1 下 DHCP Snooping 功能的信任端口。
<Sysname> system-view
[Sysname] vlan 1
[Sysname-vlan 1] dhcp snooping trust interface gigabitethernet 1/0/1
```

【相关命令】

- **display dhcp snooping trust**

1.5.20 display dhcp snooping binding

display dhcp snooping binding 命令用来显示 DHCP Snooping 表项信息。

【命令】

```
display dhcp snooping binding [ ip ip-address [ vlan vlan-id ] ] [ verbose ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
```

【参数】

ip *ip-address*: 显示指定 IP 地址对应的 DHCP Snooping 表项信息。
vlan *vlan-id*: 显示指定 VLAN 内的 DHCP Snooping 表项信息。
verbose: 显示 DHCP Snooping 表项的详细信息。如果未指定本参数，则显示 DHCP Snooping 表项的概要信息。

【使用指导】

如果未指定 **ip** *ip-address* 和 **vlan** *vlan-id* 参数，则显示所有的 DHCP Snooping 表项信息。

【举例】

显示 DHCP Snooping 表项的概要信息。

```
<Sysname> display dhcp snooping binding
 2 DHCP snooping entries found
IP address      MAC address    Lease          VLAN   SVLAN Interface
=====
1.1.1.7         0000-0101-0107 16907533       2      3      GE1/0/1
1.1.1.11        0000-0101-010b 16907537       2      3      GE1/0/3
```

显示 DHCP Snooping 表项的详细信息。

```
<Sysname> display dhcp snooping binding verbose
IP address: 1.1.1.7
MAC address: 0000-0101-0107
Lease: 16907553 seconds
VLAN: 2
```



```
SVLAN: 3
Interface: GigabitEthernet1/0/1
Parameter request list: 03 06 21

IP address: 1.1.1.104
MAC address: 0000-0101-010b
Lease: 16907537 seconds
VLAN: 2
SVLAN: 3
Interface: GigabitEthernet1/0/3
Parameter request list: 37 0B 01 0F 03 06 2C 2E 2F 1F 21 F9 2B
```

表1-14 display dhcp snooping binding 命令显示信息描述表

字段	描述
DHCP snooping entries found	表项统计计数
IP address	DHCP服务器为DHCP客户端分配的IP地址
MAC address	DHCP客户端的MAC地址
Lease	绑定的租约剩余时间，单位为秒
VLAN	如果DHCP Snooping功能与QinQ功能同时使用，或接收到的DHCP报文带有两层VLAN Tag，则表示外层VLAN Tag；否则，表示与DHCP客户端连接的设备端口所属的VLAN（S5110V2-SI、S5000V3-EI和S5000E-X不支持QinQ功能）
SVLAN	如果DHCP Snooping功能与QinQ功能同时使用，或接收到的DHCP报文带有两层VLAN Tag，则表示内层VLAN Tag；否则，显示为“N/A”（S5110V2-SI、S5000V3-EI和S5000E-X不支持QinQ功能）
Interface	与DHCP客户端连接的设备端口
Parameter request list	DHCP客户端的请求参数，为十六进制字符串

【相关命令】

- **dhcp snooping enable**
- **reset dhcp snooping binding**

1.5.21 display dhcp snooping binding database

display dhcp snooping binding database 命令用来显示 DHCP Snooping 表项备份信息。

【命令】

display dhcp snooping binding database

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

显示 DHCP Snooping 表项备份信息。

```
<Sysname> display dhcp snooping binding database
File name           :   database.dhcp
Username            :
Password            :
Update interval     :   600 seconds
Latest write time   :   Feb 27 18:48:04 2012
Status              :   Last write succeeded.
```

表1-15 display dhcp snooping binding database 命令显示信息描述表

字段	描述
File name	存储DHCP Snooping表项的文件名称
Username	配置远程目标文件时的用户名
Password	配置远程目标文件时的密码，有配置时显示为"*****"
Update interval	定期刷新表项存储文件的刷新时间间隔，单位为秒
Latest write time	最近一次写文件的时间
Status	写文件的状态，即写文件是否成功 <ul style="list-style-type: none">Writing: 正在写文件Last write succeeded.: 写文件成功Last write failed.: 写文件失败

1.5.22 display dhcp snooping information

display dhcp snooping information 命令用来显示 DHCP Snooping 上 Option 82 的配置信息。

【命令】

```
display dhcp snooping information { all | interface interface-type
interface-number }
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
```

【参数】

all: 显示所有二层以太网接口对应的 Option 82 配置信息。

interface interface-type interface-number: 显示指定接口对应的 Option 82 配置信息。
interface-type interface-number 为接口类型和接口编号。

【举例】

```
# 显示所有接口对应的 Option 82 配置信息。
<Sysname> display dhcp snooping information all
Interface: Bridge-Aggregation1
  Status: Disable
  Strategy: Drop
  Circuit ID:
    Padding format: User Defined
    User defined: abcd
    Format: ASCII
  Remote ID:
    Padding format: Normal
    Format: ASCII
VLAN 10:
  Circuit ID: abcd
  Remote ID: company
```

表1-16 display dhcp snooping information 命令显示信息描述表

字段	描述
Interface	接口名
Status	Option 82的状态，取值为Enable或Disable
Strategy	对包含Option 82的请求报文的处理策略，取值为Drop、Keep或Replace
Circuit ID	Circuit ID子选项的内容
Padding format	Option 82的填充模式： <ul style="list-style-type: none">在填充 Circuit ID 子选项时，取值为 Normal、User Defined、Verbose(sysname)、Verbose(MAC)或 Verbose(user defined)在填充 Remote ID 子选项时，取值为 Normal、Sysname 或 User Defined
Node identifier	接入节点的标识
User defined	用户自定义的子选项内容
Format	Option 82子选项的填充格式 <ul style="list-style-type: none">在填充 Circuit ID 子选项时，取值为 ASCII、Default 或 Hex在填充 Remote ID 子选项时，取值为 ASCII 或 Hex
Remote ID	Remote ID子选项的内容
VLAN	为指定VLAN内收到的DHCP报文填充的Circuit ID子选项和Remote ID子选项内容

1.5.23 display dhcp snooping packet statistics

display dhcp snooping packet statistics 命令用来显示 DHCP Snooping 设备上的 DHCP 报文统计信息。

【命令】

display dhcp snooping packet statistics [slot *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot *slot-number*: 显示指定成员设备的 DHCP 报文统计信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示主设备上的 DHCP 报文统计信息。

【举例】

显示 DHCP Snooping 设备上的 DHCP 报文统计信息。

```
<Sysname> display dhcp snooping packet statistics
DHCP packets received           : 100
DHCP packets sent                : 200
Invalid DHCP packets dropped     : 0
```

表1-17 display dhcp snooping packet statistics 命令显示信息描述表

字段	描述
DHCP packets received	接收的DHCP报文数
DHCP packets sent	发送的DHCP报文数
Invalid DHCP packets dropped	丢弃的无效DHCP报文数

【相关命令】

- **reset dhcp snooping packet statistics**

1.5.24 display dhcp snooping trust

display dhcp snooping trust 命令用来显示信任端口信息。

【命令】

display dhcp snooping trust

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

显示信任端口信息。

```
<Sysname> display dhcp snooping trust
DHCP snooping is enabled.
Interface                               Trusted          VLAN
=====
GigabitEthernet1/0/1                   Trusted
GigabitEthernet1/0/2                   -                100
GigabitEthernet1/0/3                   -                100, 200
```

表1-18 display dhcp snooping trust 命令显示信息描述表

字段	描述
DHCP snooping is	DHCP Snooping功能的开启状态，取值包括： <ul style="list-style-type: none">enable: 开启 DHCP Snooping 功能disable: 未开启 DHCP Snooping 功能
Interface	接口名称
Trusted	在整个设备开启DHCP Snooping功能后配置的信任接口，则显示为“Trusted”，如果接口只在某些VLAN内开启DHCP Snooping功能后配置的信任接口，则显示为“-”
VLAN	配置该接口为信任端口的VLAN，如果接口是在整个设备开启DHCP Snooping功能后配置的信任接口，则此处显示为空

【相关命令】

- dhcp snooping trust
- dhcp snooping trust interface

1.5.25 reset dhcp snooping binding

reset dhcp snooping binding 命令用来清除 DHCP Snooping 表项。

【命令】

```
reset dhcp snooping binding { all | ip ip-address [ vlan vlan-id ] }
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

- all: 清除所有的 DHCP Snooping 表项。
- ip ip-address: 清除指定 IP 地址对应的 DHCP Snooping 表项。
- vlan vlan-id: 清除指定 VLAN 内的 DHCP Snooping 表项。如果未指定本参数，则清除缺省 VLAN 内的 DHCP Snooping 表项。

【举例】

清除所有的 DHCP Snooping 表项。

```
<Sysname> reset dhcp snooping binding all
```

【相关命令】

- **display dhcp snooping binding**

1.5.26 reset dhcp snooping packet statistics

reset dhcp snooping packet statistics 命令用来清除 DHCP Snooping 设备上的 DHCP 报文统计信息。

【命令】

```
reset dhcp snooping packet statistics [ slot slot-number ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

slot *slot-number*: 清除指定成员设备的 DHCP 报文统计信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则清除主设备上的 DHCP 报文统计信息。

【举例】

清除 DHCP Snooping 设备上的 DHCP 报文统计信息。

```
<Sysname> reset dhcp snooping packet statistics
```

【相关命令】

- **display dhcp snooping packet statistics**

1.6 BOOTP客户端配置命令

1.6.1 display bootp client

display bootp client 命令用来显示 BOOTP 客户端的相关信息。

【命令】

```
display bootp client [ interface interface-type interface-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

interface interface-type interface-number: 显示指定接口的 BOOTP 客户端相关信息。
interface-type interface-number 为接口类型和接口编号。如果未指定本参数，则显示所有接口上的 BOOTP 客户端的相关信息。

【举例】

```
# 显示 VLAN 接口 10 的 BOOTP 客户端相关信息。
<Sysname> display bootp client interface vlan-interface 10
Vlan-interface10 BOOTP client information:
  Allocated IP: 169.254.0.2 255.255.0.0
  Transaction ID: 0x3d8a7431
  MAC Address: 00e0-fc0a-c3ef
```

表1-19 display bootp client 命令显示信息描述表

字段	描述
XXXX BOOTP client information	作为BOOTP客户端的接口信息
Allocated IP	BOOTP服务器为BOOTP客户端分配的IP地址
Transaction ID	BOOTP报文中XID字段值，即BOOTP客户端发送BOOTP请求报文时选择的随机数，用来与BOOTP服务器的响应报文相匹配。如果响应报文的XID字段值与请求报文的XID字段值不相同，则BOOTP客户端丢弃该响应报文
MAC Address	BOOTP客户端的MAC地址

【相关命令】

- **ip address bootp-alloc**

1.6.2 ip address bootp-alloc

ip address bootp-alloc 命令用来配置接口通过 BOOTP 协议获取 IP 地址。
undo ip address bootp-alloc 命令用来取消接口通过 BOOTP 协议获取的 IP 地址。

【命令】

```
ip address bootp-alloc
undo ip address bootp-alloc
```

【缺省情况】

接口不通过 BOOTP 协议获取 IP 地址。

【视图】

接口视图

【缺省用户角色】

network-admin

【举例】

在 VLAN 接口 10 上配置接口通过 BOOTP 协议获取 IP 地址。

```
<Sysname> system-view  
[Sysname] interface vlan-interface 10  
[Sysname-Vlan-interface10] ip address bootp-alloc
```

【相关命令】

- **display bootp client**

目 录

1 域名解析.....	1-1
1.1 域名解析配置命令.....	1-1
1.1.1 display dns domain	1-1
1.1.2 display dns host	1-2
1.1.3 display dns server.....	1-3
1.1.4 display ipv6 dns server	1-4
1.1.5 dns domain	1-5
1.1.6 dns dscp.....	1-5
1.1.7 dns proxy enable	1-6
1.1.8 dns server.....	1-6
1.1.9 dns source-interface.....	1-7
1.1.10 dns spoofing	1-8
1.1.11 dns trust-interface	1-9
1.1.12 ip host	1-9
1.1.13 ipv6 dns dscp.....	1-10
1.1.14 ipv6 dns server.....	1-11
1.1.15 ipv6 dns spoofing.....	1-12
1.1.16 ipv6 host	1-12
1.1.17 reset dns host	1-13

1 域名解析

1.1 域名解析配置命令

1.1.1 display dns domain

display dns domain 命令用来显示域名后缀信息。

【命令】

display dns domain [dynamic]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

dynamic: 显示通过 DHCP 等协议动态获得的域名后缀信息。如果未指定本参数，则显示静态配置和动态获得的域名后缀信息。

【举例】

显示公网静态配置和动态获得的域名后缀信息。

<Sysname> display dns domain

Type:

D: Dynamic S: Static

No.	Type	Domain suffix
1	S	com
2	D	net

表1-1 display dns domain 命令显示信息描述表

字段	描述
No.	序号
Type	域名后缀类型: <ul style="list-style-type: none">S: 表示静态配置的域名后缀D: 表示通过 DHCP 等协议动态获得的域名后缀
Domain suffix	域名后缀

【相关命令】

- **dns domain**

1.1.2 display dns host

display dns host 命令用来显示域名解析信息。

【命令】

display dns host [ip | ipv6]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

ip: 显示 A 类查询的信息。A 类查询用来解析域名对应的 IPv4 地址。
ipv6: 显示 AAAA 类查询的信息。AAAA 类查询用来解析域名对应的 IPv6 地址。

【使用指导】

如果未指定 **ip** 和 **ipv6** 参数，则显示所有查询类型的域名解析信息。

【举例】

```
# 显示所有查询类型的域名解析信息。
<Sysname> display dns host
Type:
    D: Dynamic    S: Static

Total number: 3
No.  Host name      Type  TTL      Query type  IP addresses
1    sample.com      D     3132     A           192.168.10.1
                                           192.168.10.2
                                           192.168.10.3
2    zig.sample.com  S     -        A           192.168.1.1
3    sample.net      S     -        AAAA        FE80::4904:4448
```

表1-2 display dns host 命令显示信息描述表

字段	描述
No.	序号
Host name	查询名称
Type	域名解析信息的类型： <ul style="list-style-type: none">S：表示静态配置的域名解析信息，即通过 ip host 或 ipv6 host 命令配置的主机名及其对应的主机 IPv4/IPv6 地址D：表示通过动态域名解析获得的域名解析信息
TTL	域名解析信息的剩余有效时间，单位为秒 静态信息的TTL值显示为“-”
Query type	查询类型，取值包括A和AAAA

字段	描述
IP addresses	主机名对应的IP地址 <ul style="list-style-type: none"> 对于 A 类查询类型，为 IPv4 地址 对于 AAAA 类查询类型，为 IPv6 地址

【相关命令】

- `reset dns host`
- `ip host`
- `ipv6 host`

1.1.3 display dns server

`display dns server` 命令用来显示域名服务器的 IPv4 地址信息。

【命令】

`display dns server [dynamic]`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

dynamic: 显示通过 DHCP 等协议动态获得的域名服务器 IPv4 地址信息。如果未指定本参数，则显示静态配置和动态获得的域名服务器 IPv4 地址信息。

【举例】

显示公网的域名服务器 IPv4 地址信息。

```
<Sysname> display dns server
```

Type:

D: Dynamic S: Static

```
No. Type  IP address
1   S      202.114.0.124
2   S      169.254.65.125
```

表1-3 display dns server 命令显示信息描述表

字段	描述
No.	域名服务器的序号
Type	域名服务器类型 <ul style="list-style-type: none"> S 表示静态指定的域名服务器信息 D 表示通过 DHCP 等协议动态获得的域名服务器信息

字段	描述
IP address	域名服务器的IPv4地址

【相关命令】

- **dns server**

1.1.4 display ipv6 dns server

display ipv6 dns server 命令用来显示域名服务器的 IPv6 地址信息。

【命令】

display ipv6 dns server [dynamic]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

dynamic: 显示通过 DHCP 等协议动态获得的域名服务器 IPv6 地址信息。如果未指定本参数，则显示静态配置和动态获得的域名服务器 IPv6 地址信息。

【举例】

显示公网域名服务器的 IPv6 地址信息。

```
<Sysname> display ipv6 dns server
```

Type:

D: Dynamic S: Static

```
No. Type IPv6 address Outgoing Interface
1 S 2::2
```

表1-4 display ipv6 dns server 命令显示信息描述表

字段	描述
No.	域名服务器的序号
Type	域名服务器类型 <ul style="list-style-type: none"> • S 表示静态指定的域名服务器信息 • D 表示通过 DHCP 等协议动态获得的域名服务器信息
IPv6 address	域名服务器的IPv6地址
Outgoing Interface	出接口名

【相关命令】

- **ipv6 dns server**

1.1.5 dns domain

dns domain 命令用来添加域名后缀。

undo dns domain 命令用来删除指定的域名后缀。

【命令】

dns domain *domain-name*

undo dns domain *domain-name*

【缺省情况】

未配置域名后缀，即只根据用户输入的域名信息进行解析。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

domain-name：域名后缀，由“.”分隔的字符串组成（如 **aabbcc.com**），每个字符串的长度不超过 63 个字符，包括“.”在内的总长度不超过 253 个字符。不区分大小写，字符串中可以包含字母、数字、“-”、“_”或“.”。

【使用指导】

域名解析时，用户只需要输入域名的部分字段，系统会按照域名后缀配置的先后顺序，依次将输入的域名加上不同的域名后缀进行解析。

本命令配置的域名后缀同时用于 IPv4 域名解析和 IPv6 域名解析。

公网内最多可以配置 16 个域名后缀。

【举例】

为公网添加一个域名后缀 **com**。

```
<Sysname> system-view  
[Sysname] dns domain com
```

【相关命令】

- **display dns domain**

1.1.6 dns dscp

dns dscp 命令用来指定 DNS 客户端或 DNS proxy 发送 DNS 报文的 DSCP 优先级。

undo dns dscp 命令用来恢复缺省情况。

【命令】

dns dscp *dscp-value*

undo dns dscp

【缺省情况】

DNS 客户端或 DNS proxy 发送 DNS 报文的 DSCP 优先级为 0。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

dscp-value: DNS 报文的 DSCP 优先级，取值范围为 0~63。

【使用指导】

DSCP 优先级用来体现报文自身的优先等级，决定报文传输的优先程度。配置的 DSCP 优先级的取值越大，报文的优先级越高。

【举例】

配置发送的 DNS 报文的 DSCP 优先级为 30。

```
<Sysname> system-view
[Sysname] dns dscp 30
```

1.1.7 dns proxy enable

dns proxy enable 命令用来开启 DNS proxy 功能。

undo dns proxy enable 命令用来关闭 DNS proxy 功能。

【命令】

```
dns proxy enable
undo dns proxy enable
```

【缺省情况】

DNS proxy 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

本命令的配置同时用于 IPv4 域名解析和 IPv6 域名解析。

【举例】

开启 DNS proxy 功能。

```
<Sysname> system-view
[Sysname] dns proxy enable
```

1.1.8 dns server

dns server 命令用来配置域名服务器的 IPv4 地址。

undo dns server 命令用来删除域名服务器的 IPv4 地址。

【命令】

```
dns server ip-address  
undo dns server [ ip-address ]
```

【缺省情况】

未配置域名服务器的 IPv4 地址。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ip-address: 域名服务器的 IPv4 地址。

【使用指导】

在进行动态域名解析时，系统按照域名服务器 IPv4 地址配置的先后顺序，依次向各个域名服务器发送查询请求。

公网内最多可以配置 6 个域名服务器的 IPv4 地址。

执行 **undo dns server** 命令时如果未指定 *ip-address* 参数，则删除公网中的所有域名服务器 IPv4 地址。

【举例】

配置域名服务器的 IPv4 地址为 172.16.1.1。

```
<Sysname> system-view  
[Sysname] dns server 172.16.1.1
```

【相关命令】

- **display dns server**

1.1.9 dns source-interface

dns source-interface 命令用来指定 DNS 报文的源接口。

undo dns source-interface 命令用来恢复缺省情况。

【命令】

```
dns source-interface interface-type interface-number  
undo dns source-interface interface-type interface-number
```

【缺省情况】

设备根据 DNS server 的地址，通过路由表查找报文的出接口，并将该出接口的主 IP 地址作为发送到该服务器的 DNS 查询报文的源地址。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interface-type interface-number: 源接口的接口类型和接口编号。

【使用指导】

通过本命令指定 DNS 报文的源接口后，系统将选择指定接口的主 IPv4 地址或根据 RFC 3484 中定义的规则选择指定接口的某个 IPv6 地址，作为 DNS 查询报文的源地址。

本命令的配置同时用于 IPv4 域名解析和 IPv6 域名解析。

公网内只能配置 1 个源接口。多次执行本命令，最后一次执行的命令生效。

【举例】

指定公网 DNS 报文的源接口为 VLAN 接口 2。

```
<Sysname> system-view
[Sysname] dns source-interface vlan-interface 2
```

1.1.10 dns spoofing

dns spoofing 命令用来开启 DNS spoofing 功能，并指定应答的 IPv4 地址。

undo dns spoofing 命令关闭 DNS spoofing 功能。

【命令】

```
dns spoofing ip-address
undo dns spoofing ip-address
```

【缺省情况】

DNS spoofing 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ip-address: 用来欺骗性应答域名解析请求的 IPv4 地址。

【使用指导】

配置 DNS spoofing 前，需要先开启 DNS proxy 功能。

开启 DNS spoofing 功能后，如果设备上未配置域名服务器地址或不存在到达域名服务器的路由，则会利用配置的应答 IP 地址作为域名解析结果，欺骗性地应答 A 类域名解析请求。

公网内只能配置 1 个 DNS spoofing 应答的 IPv4 地址。多次执行本命令，最后一次执行的命令生效。

【举例】

开启公网的 DNS spoofing 功能，并指定应答的 IPv4 地址为 1.1.1.1。

```
<Sysname> system-view
[Sysname] dns proxy enable
```

```
[Sysname] dns spoofing 1.1.1.1
```

【相关命令】

- **dns proxy enable**

1.1.11 dns trust-interface

dns trust-interface 命令用来指定 DNS 信任接口。

undo dns trust-interface 命令用来删除指定的 DNS 信任接口。

【命令】

```
dns trust-interface interface-type interface-number
```

```
undo dns trust-interface [ interface-type interface-number ]
```

【缺省情况】

未指定任何接口为信任接口。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interface-type interface-number: DNS 信任接口的接口类型和接口编号。

【使用指导】

缺省情况下,任意接口通过 DHCP 等协议动态获得的域名后缀和域名服务器信息都将作为有效信息,用于域名解析。如果网络攻击者通过 DHCP 服务器为设备分配错误的域名后缀和域名服务器地址,则会导致设备域名解析失败,或解析到错误的结果。通过本配置指定信任接口后,域名解析时只采用信任接口动态获得的域名后缀和域名服务器信息,非信任接口获得的信息不能用于域名解析,从而在一定程度上避免这类攻击。

本命令同时用于 IPv4 域名解析和 IPv6 域名解析。

设备最多可以配置 128 个信任接口。

执行 **undo dns trust-interface** 命令时,如果未指定任何接口,则删除所有的 DNS 信任接口,恢复到缺省情况。

【举例】

指定 VLAN 接口 2 为 DNS 信任接口。

```
<Sysname> system-view
```

```
[Sysname] dns trust-interface vlan-interface 2
```

1.1.12 ip host

ip host 命令用来配置主机名及其对应的主机 IPv4 地址。

undo ip host 命令用来删除主机名及其对应的主机 IPv4 地址。

【命令】

```
ip host host-name ip-address  
undo ip host host-name ip-address
```

【缺省情况】

不存在主机名及 IPv4 地址的对应关系。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

host-name: 主机名，为 1~253 个字符的字符串，不区分大小写，字符串中可以包含字母、数字、“-”、“_”和“.”。

ip-address: 与主机名对应的 IPv4 地址。

【使用指导】

公网内最多可以配置 1024 个主机名和 IPv4 地址的对应关系。

在公网内，一个主机名只能对应一个 IPv4 地址。多次执行本命令，最后一次执行的命令生效。

ip、**-a**、**-c**、**-f**、**-h**、**-i**、**-m**、**-n**、**-p**、**-q**、**-r**、**-s**、**-t**、**-tos**、**-v** 和 **-vpn-instance** 已被系统用作 **ping** 命令的参数关键字，在配置主机名时，请避免使用相同的字符串作为主机名。**ping** 命令支持的参数形式，请参考“网络管理和监控”中的“**ping**”命令。

【举例】

```
# 配置公网内主机名 aaa 对应的 IPv4 地址为 10.110.0.1。
```

```
<Sysname> system-view  
[Sysname] ip host aaa 10.110.0.1
```

【相关命令】

- **display dns host**

1.1.13 ipv6 dns dscp

ipv6 dns dscp 命令用来指定 IPv6 DNS 客户端或 IPv6 DNS proxy 发出的 IPv6 DNS 报文的 DSCP 优先级。

undo ipv6 dns dscp 命令用来恢复缺省情况。

【命令】

```
ipv6 dns dscp dscp-value  
undo ipv6 dns dscp
```

【缺省情况】

IPv6 DNS 客户端或 IPv6 DNS proxy 发出的 IPv6 DNS 报文的 DSCP 优先级为 0。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

dscp-value: IPv6 DNS 报文的 DSCP 优先级，取值范围为 0~63。

【使用指导】

DSCP 优先级用来体现报文自身的优先等级，决定报文传输的优先程度。配置的 DSCP 优先级的取值越大，报文的优先级越高。

【举例】

配置发送的 IPv6 DNS 报文的 DSCP 优先级为 30。

```
<Sysname> system-view
[Sysname] ipv6 dns dscp 30
```

1.1.14 ipv6 dns server

ipv6 dns server 命令用来配置域名服务器的 IPv6 地址。

undo ipv6 dns server 命令用来删除域名服务器的 IPv6 地址。

【命令】

```
ipv6 dns server ipv6-address [ interface-type interface-number ]
undo ipv6 dns server [ ipv6-address [ interface-type interface-number ] ]
```

【缺省情况】

未配置域名服务器的 IPv6 地址。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv6-address: 域名服务器的 IPv6 地址。

interface-type interface-number: 指定报文的出接口的接口类型和接口编号。如果未指定本参数，则根据路由表查找报文的出接口。域名服务器的 IPv6 地址为链路本地地址时，必须指定本参数。域名服务器的 IPv6 地址为全球单播地址时，无法指定本参数。

【使用指导】

在进行动态域名解析时，系统按照域名服务器 IPv6 地址配置的先后顺序，依次向各个域名服务器发送查询请求。

公网内最多可以配置 6 个域名服务器的 IPv6 地址。

执行 **undo ipv6 dns server** 命令时如果未指定 *ipv6-address* 参数，则删除公网的所有域名服务器 IPv6 地址。

【举例】

```
# 配置公网内域名服务器的 IPv6 地址为 2002::1。  
<Sysname> system-view  
[Sysname] ipv6 dns server 2002::1
```

【相关命令】

- **display ipv6 dns server**

1.1.15 ipv6 dns spoofing

ipv6 dns spoofing 命令用来开启 DNS spoofing 功能，并指定应答的 IPv6 地址。

undo ipv6 dns spoofing 命令用来关闭 DNS spoofing 功能。

【命令】

```
ipv6 dns spoofing ipv6-address  
undo ipv6 dns spoofing ipv6-address
```

【缺省情况】

DNS spoofing 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv6-address：用来欺骗性应答域名解析请求的 IPv6 地址。

【使用指导】

本命令必须和 **dns proxy enable** 命令一起使用。

开启 DNS spoofing 功能后，如果设备上未配置域名服务器地址或不存在到达域名服务器的路由，则会利用配置的应答 IPv6 地址作为域名解析结果，欺骗性地应答 AAAA 类域名解析请求。

公网内只能配置 1 个 DNS spoofing 应答的 IPv6 地址。多次执行本命令，最后一次执行的命令生效。

【举例】

```
# 为公网开启 DNS spoofing 功能，并指定应答的 IPv6 地址为 2001::1。  
<Sysname> system-view  
[Sysname] dns proxy enable  
[Sysname] ipv6 dns spoofing 2001::1
```

【相关命令】

- **dns proxy enable**

1.1.16 ipv6 host

ipv6 host 命令用来配置主机名及其对应的主机 IPv6 地址。

undo ipv6 host 命令用来删除主机名及其对应的主机 IPv6 地址。

【命令】

```
ipv6 host host-name ipv6-address  
undo ipv6 host host-name ipv6-address
```

【缺省情况】

不存在主机名及 IPv6 地址的对应关系。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

host-name: 主机名，为 1~253 个字符的字符串，不区分大小写，字符串中可以包含字母、数字、“-”、“_”和“.”。

ipv6-address: 与主机名对应的 IPv6 地址。

【使用指导】

公网内最多可以配置 1024 个主机名和 IPv6 地址的对应关系。

在公网内，一个主机名只能对应一个 IPv6 地址。多次执行本命令，最后一次执行的命令生效。

-a、**-c**、**-i**、**-m**、**-q**、**-s**、**-t**、**-tc**、**-v** 和 **-vpn-instance** 已被系统用作 **ping ipv6** 命令的参数关键字，在配置主机名时，请避免使用相同的字符串作为主机名。**ping ipv6** 命令支持的参数形式，请参考“网络管理和监控”中的“**ping ipv6**”命令。

【举例】

```
# 配置公网内主机名 aaa 对应的 IPv6 地址为 2001::1。
```

```
<Sysname> system-view  
[Sysname] ipv6 host aaa 2001::1
```

【相关命令】

- **ip host**

1.1.17 reset dns host

reset dns host 命令用来清除动态域名解析缓存信息。

【命令】

```
reset dns host [ ip | ipv6 ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

ip: 清除 A 类查询的动态缓存信息。A 类查询用来解析域名对应的 IPv4 地址。

ipv6: 清除 AAAA 类查询的动态缓存信息。AAAA 类查询用来解析域名对应的 IPv6 地址。

【使用指导】

如果未指定 **ip** 和 **ipv6** 参数，则清除所有查询类型的动态域名解析缓存信息。

【举例】

清除公网所有查询类型的动态域名解析缓存信息。

```
<Sysname> reset dns host
```

【相关命令】

- **display dns host**

目 录

1 IP转发基础	1-1
1.1 IP转发基础配置命令	1-1
1.1.1 display fib	1-1
1.1.2 ip forwarding-table save	1-2

1 IP转发基础

1.1 IP转发基础配置命令

1.1.1 display fib

display fib 命令用来显示 FIB 表项的信息。

【命令】

display fib [*ip-address* [*mask* | *mask-length*]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

ip-address: 显示与指定目的 IP 地址匹配的 FIB 表项的信息。

mask: IP 地址掩码。

mask-length: IP 地址掩码长度，取值范围为 0~32。

【使用指导】

如果配置 *ip-address* 时不指定掩码和掩码长度，则显示与指定目的 IP 地址最长匹配的 FIB 表项的信息；如果配置 *ip-address* 时指定了掩码或掩码长度，则显示与指定目的 IP 地址和掩码精确匹配的 FIB 表项的信息。

【举例】

显示公网的所有 FIB 表项的信息。

```
<Sysname> display fib
```

```
Destination count: 5 FIB entry count: 5
```

```
Flag:
```

```
U:Usable    G:Gateway    H:Host    B:Blackhole    D:Dynamic    S:Static  
R:Relay      F:FRR
```

Destination/Mask	Nexthop	Flag	OutInterface/Token	Label
0.0.0.0/32	127.0.0.1	UH	InLoop0	Null
127.0.0.0/8	127.0.0.1	U	InLoop0	Null
127.0.0.0/32	127.0.0.1	UH	InLoop0	Null
127.0.0.1/32	127.0.0.1	UH	InLoop0	Null

显示目的地址为 10.2.1.1 的 FIB 表项的信息。

```
<Sysname> display fib 10.2.1.1
```

Destination count: 1 FIB entry count: 1

Flag:

U:Usable G:Gateway H:Host B:Blackhole D:Dynamic S:Static
R:Relay F:FRR

Destination/Mask	Nexthop	Flag	OutInterface/Token	Label
10.2.1.1/32	127.0.0.1	UH	InLoop0	Null

表1-1 display fib 命令显示信息描述表

字段	描述
Destination count	目的地址的个数
FIB entry count	FIB表项数目
Destination/Mask	目的地址/掩码长度
Nexthop	转发的下一跳地址
Flag	路由的标志： <ul style="list-style-type: none">• U：表示可用路由• G：表示网关路由• H：表示主机路由• B：表示黑洞路由• D：表示动态路由• S：表示静态路由• R：表示迭代路由• F：表示快速重路由
OutInterface/Token	转发接口/LSP索引号
Label	内层标签值

1.1.2 ip forwarding-table save

ip forwarding-table save 命令用来将当前的 IP 转发表项保存到用户指定的文件中。

【命令】

ip forwarding-table save filename *filename*

【视图】

任意视图

【缺省用户角色】

network-admin

【参数】

filename *filename*: 目标文件名，长度不超过 255 字节。文件名取值范围的详细介绍，请参见“基础配置指导”中的“文件系统管理”。

【使用指导】

执行本命令时，如果名称为 **filename** 的文件不存在，系统会先创建该文件，再保存；如果已存在，则会覆盖原文件的内容。

如果需要周期性地自动保存 IP 转发表，可以通过配置定时执行任务功能，采用循环执行方式，让设备在指定时间到达时，自动执行命令。关于配置定时执行任务功能的详细介绍，请参见“基础配置指导”中“设备管理”。

【举例】

将 IP 转发表保存到名为 **fib.txt** 的文件中。

```
<Sysname> ip forwarding-table save filename fib.txt
```

目 录

1 快速转发.....	1-1
1.1 快速转发配置命令.....	1-1
1.1.1 display ip fast-forwarding aging-time	1-1
1.1.2 display ip fast-forwarding cache	1-1
1.1.3 display ip fast-forwarding fragcache.....	1-2
1.1.4 ip fast-forwarding aging-time	1-3
1.1.5 ip fast-forwarding load-sharing.....	1-4
1.1.6 reset ip fast-forwarding cache.....	1-4

1 快速转发

1.1 快速转发配置命令

1.1.1 display ip fast-forwarding aging-time

display ip fast-forwarding aging-time 命令用来显示快速转发表项的老化时间。

【命令】

display ip fast-forwarding aging-time

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

显示快速转发表项的老化时间。

```
<Sysname> display ip fast-forwarding aging-time  
Aging time: 30s
```

表1-1 display ip fast-forwarding aging-time 命令显示信息描述表

字段	描述
Aging time	快转表项的老化时间

【相关命令】

- ip fast-forwarding aging-time**

1.1.2 display ip fast-forwarding cache

display ip fast-forwarding cache 命令用来显示快速转发表信息。

【命令】

display ip fast-forwarding cache [*ip-address*] [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

ip-address: 显示指定 IP 地址的快速转发表信息。如果不指定 *ip-address*，将显示所有快速转发表信息。

slot *slot-number*: 显示指定成员设备的快速转发表信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备的快速转发表信息。

【举例】

显示所有快速转发表的信息。

```
<Sysname> display ip fast-forwarding cache
Total number of fast-forwarding entries: 1
SIP          SPort  DIP          DPort  Pro  Input_If  Output_If  Flg
7.0.0.13     68     8.0.0.1      67     17   GE1/0/3   GE1/0/1    5
```

表1-2 display ip fast-forwarding cache 命令显示信息描述表

字段	描述
Total number of fast-forwarding entries	快速转发表项数目
SIP	源IP地址
SPort	源端口号
DIP	目的IP地址
DPort	目的端口号
Pro	协议号
Input_If	报文入接口类型和接口号（“N/A”表示接口存在但是该快速转发不涉及入接口，“-”表示接口不存在）
Output_If	报文出接口类型和接口号（“N/A”表示接口存在但是该快速转发不涉及出接口，“-”表示接口不存在）
Flg	内部标记，主要是标记分片等内部操作信息

【相关命令】

- **reset ip fast-forwarding cache**

1.1.3 display ip fast-forwarding fragcache

display ip fast-forwarding fragcache 命令用来显示分片报文快速转发表信息。

【命令】

```
display ip fast-forwarding fragcache [ ip-address ] [ slot slot-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

ip-address: 显示指定 IP 地址的分片报文快速转发表信息。如果不指定 *ip-address*，将显示所有分片报文快速转发表信息。

slot slot-number: 显示指定成员设备的分片报文快速转发表信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备的分片报文快速转发表信息。

【举例】

显示所有分片报文快速转发表信息。

```
<Sysname> display ip fast-forwarding fragcache
Total number of fragment fast-forwarding entries: 1
SIP          SPort DIP          DPort Pro Input_If  ID
7.0.0.13     68   8.0.0.1     67    17  GE1/0/3    2
```

表1-3 display ip fast-forwarding fragcache 命令显示信息描述表

字段	描述
Total number of fragment fast-forwarding entries	分片报文快速转发表项数目
SIP	源IP地址
SPort	源端口号
DIP	目的IP地址
DPort	目的端口号
Pro	协议号
Input_If	报文入接口类型和接口号（“N/A”表示接口存在但是该快速转发不涉及入接口，“-”表示接口不存在）
ID	分片IP报文ID

【相关命令】

- `reset ip fast-forwarding cache`

1.1.4 ip fast-forwarding aging-time

`ip fast-forwarding aging-time` 命令用来配置快速转发表项的老化时间。

`undo ip fast-forwarding aging-time` 命令用来恢复缺省情况。

【命令】

```
ip fast-forwarding aging-time aging-time
undo ip fast-forwarding aging-time
```

【缺省情况】

快速转发表项的老化时间为 30 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

aging-time: 快速转发表项的老化时间，取值范围为 10～300，单位为秒。

【举例】

```
# 配置快速转发表项的老化时间为 20 秒。
<Sysname> system-view
[Sysname] ip fast-forwarding aging-time 20
```

【相关命令】

- **display ip fast-forwarding aging-time**

1.1.5 ip fast-forwarding load-sharing

ip fast-forwarding load-sharing 命令用来开启快转负载分担功能。

undo ip fast-forwarding load-sharing 命令用来关闭快转负载分担功能。

【命令】

```
ip fast-forwarding load-sharing
undo ip fast-forwarding load-sharing
```

【缺省情况】

快转负载分担功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

开启快速转发负载分担功能后，当一条数据流从不同入接口上来进行转发时，不再根据入接口不同区分数据流，根据报文中的信息标识一条数据流。

关闭快速转发负载分担功能后，将会根据入接口的不同对已标识的数据流再次做出区分，即将入接口作为区分数据流的另一特征标识。

【举例】

```
# 开启快转负载分担功能。
<Sysname> system-view
[Sysname] ip fast-forwarding load-sharing
```

1.1.6 reset ip fast-forwarding cache

reset ip fast-forwarding cache 命令用来清除快速转发表中的信息。

【命令】

```
reset ip fast-forwarding cache [ slot slot-number ]
```


【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

slot *slot-number*: 清除指定成员设备的快速转发表信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则清除所有成员设备的快速转发表信息。

【举例】

清除快速转发表信息。

```
<Sysname> reset ip fast-forwarding cache
```

【相关命令】

- **display ip fast-forwarding cache**
- **display ip fast-forwarding fragcache**

目 录

1 IP性能优化	1-1
1.1 IP性能优化配置命令	1-1
1.1.1 display icmp statistics	1-1
1.1.2 display ip statistics	1-2
1.1.3 display rawip	1-4
1.1.4 display rawip verbose	1-5
1.1.5 display tcp	1-9
1.1.6 display tcp statistics	1-10
1.1.7 display tcp verbose	1-14
1.1.8 display udp	1-19
1.1.9 display udp statistics	1-20
1.1.10 display udp verbose	1-21
1.1.11 ip forward-broadcast	1-24
1.1.12 ip icmp error-interval	1-25
1.1.13 ip icmp source	1-26
1.1.14 ip mtu	1-27
1.1.15 ip reassemble local enable	1-28
1.1.16 ip redirects enable	1-28
1.1.17 ip ttl-expires enable	1-29
1.1.18 ip unreachable enable	1-30
1.1.19 reset ip statistics	1-30
1.1.20 reset tcp statistics	1-31
1.1.21 reset udp statistics	1-31
1.1.22 tcp mss	1-32
1.1.23 tcp path-mtu-discovery	1-33
1.1.24 tcp syn-cookie enable	1-33
1.1.25 tcp timer fin-timeout	1-34
1.1.26 tcp timer syn-timeout	1-35
1.1.27 tcp window	1-35

1 IP性能优化

1.1 IP性能优化配置命令

1.1.1 display icmp statistics

display icmp statistics 命令用来显示 ICMP 流量统计信息。

【命令】

display icmp statistics [*slot slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot slot-number: 显示指定成员设备的 ICMP 流量统计信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 ICMP 流量统计信息。

【使用指导】

display icmp statistics 命令用来显示设备接收和发送的各类 ICMP 流量的统计信息。

【举例】

显示 ICMP 流量统计信息。

```
<Sysname> display icmp statistics
  Input: bad formats      0                bad checksum      0
         echo            175              destination unreachable 0
         source quench    0                redirects          0
         echo replies     201              parameter problem   0
         timestamp        0                information requests 0
         mask requests    0                mask replies        0
         time exceeded    0                invalid type        0
         router advert    0                router solicit      0
         broadcast/multicast echo requests ignored 0
         broadcast/multicast timestamp requests ignored 0
  Output: echo            0                destination unreachable 0
         source quench    0                redirects          0
         echo replies     175              parameter problem   0
         timestamp        0                information replies 0
         mask requests    0                mask replies        0
         time exceeded    0                bad address         0
         packet error     1442              router advert       3
```

表1-1 display icmp statistics 命令显示信息描述表

字段	描述
bad formats	输入的格式错误报文数
bad checksum	输入的校验和错误报文数
echo	输入/输出的响应请求报文数
destination unreachable	输入/输出的目的不可达报文数
source quench	输入/输出的源站抑制报文数
redirects	输入/输出的重定向报文数
echo replies	输入/输出的响应应答报文数
parameter problem	输入/输出的参数错误报文数
timestamp	输入/输出的时间戳报文数
information requests	输入的信息请求报文数
mask requests	输入/输出的掩码请求报文数
mask replies	输入/输出的掩码应答报文数
invalid type	输入的非类型报文数
router advert	输入的路由器公告报文数
router solicit	输入的路由器请求报文数
broadcast/multicast echo requests ignored	输入的广播/组播响应请求丢弃报文数
broadcast/multicast timestamp requests ignored	输入的广播/组播时间戳请求丢弃报文数
information replies	输出的信息应答报文数
time exceeded	输入/输出的超时报文数
bad address	输出的目的地址非法报文数
packet error	输出的错误报文数
router advert	输入/输出的路由器公告报文数

1.1.2 display ip statistics

display ip statistics 命令用来显示 IP 报文统计信息。

【命令】

display ip statistics [slot slot-number]

【视图】

任意视图

【缺省用户角色】

network-admin

【参数】

slot slot-number: 显示指定成员设备的 IP 报文统计信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 IP 报文统计信息。

【使用指导】

display ip statistics 命令用来显示 IP 报文统计信息，包括接收报文、发送报文、分片、重组的统计信息。

【举例】

```
# 显示 IP 报文统计信息。
<Sysname> display ip statistics
  Input:      sum          7120          local          112
             bad protocol  0           bad format      0
             bad checksum  0           bad options     0
  Output: forwarding  0           local          27
             dropped      0           no route        2
             compress fails 0
  Fragment: input      0           output          0
             dropped      0
             fragmented  0           couldn't fragment 0
  Reassembling: sum    0           timeouts        0
```

表1-2 display ip statistics 命令显示信息描述表

字段	描述
Input:	接收报文的统计信息，包括： <ul style="list-style-type: none">• sum: 接收报文总数• local: 接收的目的地址是本地的报文数• bad protocol: 未知协议的报文数• bad format: 格式错误的报文数• bad checksum: 校验和错误的报文数• bad options: 选项错误的报文数

字段	描述
Output:	发送报文的统计信息，包括： <ul style="list-style-type: none"> • forwarding: 转发的报文数 • local: 本地发送报文数 • dropped: 发送时丢弃的报文数 • no route: 查不到路由的报文数 • compress fails: 压缩失败的报文数
Fragment:	分片报文的统计信息，包括： <ul style="list-style-type: none"> • input: 接收的分片报文数 • output: 发送的分片报文数 • dropped: 丢弃的分片报文数 • fragmented: 分片成功的报文数 • couldn't fragment: 分片失败的报文数
Reassembling:	重组报文的统计信息，包括： <ul style="list-style-type: none"> • sum: 重组的报文总数 • timeouts: 重组超时的分片报文数

【相关命令】

- **display ip interface** (三层技术-IP 业务命令参考/IP 地址)
- **reset ip statistics**

1.1.3 display rawip

display rawip 命令用来显示 RawIP 连接摘要信息。

【命令】

display rawip [*slot slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot slot-number: 显示指定成员设备的 RawIP 连接摘要信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 RawIP 连接摘要信息。

【使用指导】

display rawip 命令用来显示 RawIP 连接摘要信息，包括本端 IP 地址、对端 IP 地址、使用 RawIP socket 的协议号等信息。

【举例】

显示 RawIP 连接摘要信息。

```
<Sysname> display rawip
Local Addr      Foreign Addr    Protocol  Slot   PCB
0.0.0.0         0.0.0.0        1         1      0x0000000000000009
0.0.0.0         0.0.0.0        1         1      0x0000000000000008
```

表1-3 display rawip 命令显示信息描述表

字段	描述
Local Addr	本端IP地址
Foreign Addr	对端IP地址
Protocol	使用RawIP socket的协议号
PCB	协议控制块索引

1.1.4 display rawip verbose

display rawip verbose 命令用来显示 RawIP 连接详细信息。

【命令】

```
display rawip verbose [ slot slot-number [ pcb pcb-index ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

pcb pcb-index: 显示指定协议控制块索引的 RawIP 连接详细信息。*pcb-index* 表示协议控制块索引，取值为十六进制字符串 1~ffffffffffff。

slot slot-number: 显示指定成员设备的 RawIP 连接详细信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 RawIP 连接详细信息。

【使用指导】

display rawip verbose 命令用来显示 RawIP 连接详细信息，包括 socket 的创建者、状态、选项、类型、使用的协议号、以及 RawIP 连接的源 IP 地址和目的 IP 地址等信息。

【举例】

显示 RawIP 连接详细信息。

```
<Sysname> display rawip verbose
Total RawIP socket number: 1

Location: slot: 6 cpu: 0
Creator: ping[320]
```

State: N/A
Options: N/A
Error: 0
Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 9216 / 1 / 0 / N/A
Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
Type: 3
Protocol: 1
Connection info: src = 0.0.0.0, dst = 0.0.0.0
Inpcb flags: N/A
Inpcb extflag: INP_EXTRCVICMPERR INP_EXTFILTER
Inpcb vflag: INP_IPV4
TTL: 255(minimum TTL: 0)
Send VRF: 0xffff
Receive VRF: 0xffff

表1-4 display rawip verbose 命令显示信息描述表

字段	描述
Total RawIP socket number	RawIP socket总数
Creator	创建socket的任务名称，括号中为创建者的进程号
State	socket的状态，包括： <ul style="list-style-type: none">• NOFDREF：用户已经关闭• ISCONNECTED：连接已经建立• ISCONNECTING：正在建立连接• ISDISCONNECTING：正在断开连接• ASYNC：异步方式• ISDISCONNECTED：连接已经断开• PROTOREF：协议强关联• N/A：不处于上述状态

字段	描述
Options	<p>socket的选项，包括：</p> <ul style="list-style-type: none"> • SO_DEBUG：记录套接字的调试信息 • SO_ACCEPTCONN：server 端监听连接请求 • SO_REUSEADDR：允许本地地址重复使用 • SO_KEEPALIVE：协议需要查询空闲的连接 • SO_DONTROUTE：设置不查路由表（用于目的地址是直连网络的情况） • SO_BROADCAST：套接字支持广播报文 • SO_LINGER：套接字关闭但仍发送剩余数据 • SO_OOBINLINE：带外数据采用内联方式存储 • SO_REUSEPORT：允许本地端口重复使用 • SO_TIMESTAMP：记录入报文时间戳，只对非连接的协议有效，时间精确到毫秒 • SO_NOSIGPIPE：socket 不能发送数据导致返回失败时不创建 SIGPIPE • SO_FILTER：设置报文过滤条件，对接收报文有效 • SO_TIMESTAMPNS：和时间戳选项功能类似，时间可以精确到纳秒 • N/A：未设置选项
Error	影响socket连接的错误码
Receiving buffer (cc/hiwat/lowat/drop/state)	<p>接收缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间、丢包数和状态，包括：</p> <ul style="list-style-type: none"> • CANTSENDMORE：不能发送数据到对端 • CANTRCVMORE：不能从对端接收数据 • RCVATMARK：接收标记 • N/A：不处于上述状态
Sending buffer (cc/hiwat/lowat/state)	<p>发送缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间和状态，包括：</p> <ul style="list-style-type: none"> • CANTSENDMORE：不能发送数据到对端 • CANTRCVMORE：不能从对端接收数据 • RCVATMARK：接收标记 • N/A：不处于上述状态
Type	<p>使用的socket类型，包括：</p> <ul style="list-style-type: none"> • 1：SOCK_STREAM，流模式，提供可靠的字节流。TCP 协议使用此类型 • 2：SOCK_DGRAM，数据报模式的通信。UDP 协议使用此类型 • 3：SOCK_RAW，RAW 模式的通信方式 • N/A：不是上述类型
Protocol	使用socket的协议号
Connection info	连接信息，分别为源IP地址、目的IP地址

字段	描述
Inpcb flags	<p>Internet协议控制块中的标记，包括：</p> <ul style="list-style-type: none"> • INP_RECVOPTS: 接收传入的 IP 选项 • INP_RECVRETOPTS: 接收回应的 IP 选项 • INP_RECVDSTADDR: 接收目的 IP 地址 • INP_HDRINCL: 用户提供整个 IP 头 • INP_REUSEADDR: 重复使用地址 • INP_REUSEPORT: 重复使用端口号 • INP_ANONPORT: 用户未指定端口 • INP_RECVIF: 接收报文时记录报文的入接口 • INP_RECVTTL: 携带报文的 TTL，仅 UDP 和 RawIP 支持 • INP_DONTFRAG: 设置不可分片标志 • INP_ROUTER_ALERT: 接收携带路由器告警选项的报文，仅 RawIP 支持 • INP_PROTOCOL_PACKET: 标识报文为协议报文 • INP_RCVVLANID: 接收报文的 VLAN ID，仅 UDP 和 RawIP 支持 • INP_RCVMACADDR: 接收报文的 MAC • INP_RECVTOS: 携带报文的 TOS，仅 UDP 和 RawIP 支持 • INP_USEICMPSRC: 使用配置的 ICMP 地址作为源地址 • INP_SYNCPCB: 阻塞等待 inpcb 同步 • N/A: 不是上述标记
Inpcb extflag	<p>Internet协议控制块中的扩展标记，包括：</p> <ul style="list-style-type: none"> • INP_EXTRCVPVCIDX: 接收报文时记录报文的 PVC 索引 • INP_RCVPWID: 接收报文时记录报文的 PW ID • INP_EXTRCVICMPERR: 接收 ICMP 差错报文 • INP_EXTFILTER: 接收报文时对报文内容进行过滤 • N/A: 不是上述标记
Inpcb vflag	<p>Internet协议控制块中的IP版本标记，包括：</p> <ul style="list-style-type: none"> • INP_IPV4: 运用与 IPv4 通信 • INP_TIMEWAIT: 处于等待状态 • INP_ONESBCAST: 发送广播报文 • INP_DROPPED: 协议丢弃标志 • INP_SOCKREF: socket 强关联 • INP_DONTBLOCK: inpcb 同步时不能被阻塞 • N/A: 不是上述标记
TTL(minimum TTL)	Internet协议控制块中的生存周期，括号中为最小生存周期
Send VRF	（暂不支持）发送实例
Receive VRF	（暂不支持）接收实例

1.1.5 display tcp

display tcp 命令用来显示 TCP 连接摘要信息。

【命令】

display tcp [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot *slot-number*: 显示指定成员设备的 TCP 连接摘要信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 TCP 连接摘要信息。

【使用指导】

display tcp 命令用来显示 TCP 连接摘要信息，包括本端 IP 地址及端口号、对端 IP 地址及端口号、TCP 连接的状态等信息。

【举例】

显示 TCP 连接摘要信息。

```
<Sysname> display tcp
*: TCP connection with authentication
Local Addr:port      Foreign Addr:port    State      Slot  PCB
*0.0.0.0:21          0.0.0.0:0            LISTEN     1     0x0000000000000c387
192.168.20.200:23    192.168.20.14:1284   ESTABLISHED 1     0x0000000000000009
192.168.20.200:23    192.168.20.14:1283   ESTABLISHED 1     0x0000000000000002
```

表1-5 display tcp 命令显示信息描述表

字段	描述
*	如果某个连接前有此标识，则表示该TCP连接是采用加密算法认证的连接
Local Addr:port	本端IP地址及端口号
Foreign Addr:port	对端IP地址及端口号

字段	描述
State	<p>TCP连接状态，包括：</p> <ul style="list-style-type: none"> • CLOSED：服务器收到客户端的关闭连接请求回应后所处的状态 • LISTEN：服务器在等待连接请求时所处的状态 • SYN_SENT：客户端发出连接请求等待服务器回应时所处的状态 • SYN_RCVD：服务器收到客户端连接请求时所处的状态 • ESTABLISHED：服务器和客户端双方建立连接并能进行双向数据传递的状态 • CLOSE_WAIT：服务器收到客户端关闭连接请求时所处的状态 • FIN_WAIT_1：客户端发出关闭连接请求等待服务器回应时所处的状态 • CLOSING：连接双方在向对端发出关闭连接请求后等待对端回应过程中收到对端发出的关闭连接请求时所处的状态 • LAST_ACK：服务器向客户端发出关闭连接请求等待回应时所处的状态 • FIN_WAIT_2：客户端收到服务器关闭连接回应后所处的状态 • TIME_WAIT：客户端收到服务器的关闭连接请求后所处的状态
PCB	协议控制块索引

1.1.6 display tcp statistics

display tcp statistics 命令用来显示 TCP 连接的流量统计信息。

【命令】

display tcp statistics [slot slot-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot slot-number：显示指定成员设备的 TCP 连接流量统计信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 TCP 连接流量统计信息。

【使用指导】

display tcp statistics 命令用来显示 TCP 连接的流量统计信息，包括接收报文、发送报文以及 Syncache/syncookie 等相关统计信息。

【举例】

显示 TCP 连接的流量统计信息。

```
<Sysname> display tcp statistics
Received packets:
  Total: 4150
  packets in sequence: 1366 (134675 bytes)
```

window probe packets: 0, window update packets: 0
checksum error: 0, offset error: 0, short error: 0
packets dropped for lack of memory: 0
packets dropped due to PAWS: 0
duplicate packets: 12 (36 bytes), partially duplicate packets: 0 (0 bytes)
out-of-order packets: 0 (0 bytes)
packets with data after window: 0 (0 bytes)
packets after close: 0
ACK packets: 3531 (795048 bytes)
duplicate ACK packets: 33, ACK packets for unsent data: 0

Sent packets:

Total: 4058
urgent packets: 0
control packets: 50
window probe packets: 3, window update packets: 11
data packets: 3862 (795012 bytes), data packets retransmitted: 0 (0 bytes)
ACK-only packets: 150 (52 delayed)
unnecessary packet retransmissions: 0

Synccache/syncookie related statistics:

entries added to synccache: 12
synccache entries retransmitted: 0
duplicate SYN packets: 0
reply failures: 0
successfully build new socket: 12
bucket overflows: 0
zone failures: 0
synccache entries removed due to RST: 0
synccache entries removed due to timed out: 0
ACK checked by synccache or syncookie failures: 0
synccache entries aborted: 0
synccache entries removed due to bad ACK: 0
synccache entries removed due to ICMP unreachable: 0
SYN cookies sent: 0
SYN cookies received: 0

SACK related statistics:

SACK recoveries: 1
SACK retransmitted segments: 0 (0 bytes)
SACK blocks (options) received: 0
SACK blocks (options) sent: 0
SACK scoreboard overflows: 0

Other statistics:

retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
persist timeout: 0
keepalive timeout: 21, keepalive probe: 0

```
keepalive timeout, so connections disconnected: 0
fin_wait_2 timeout, so connections disconnected: 0
initiated connections: 29, accepted connections: 12, established connections:
23
closed connections: 50051 (dropped: 0, initiated dropped: 0)
bad connection attempt: 0
ignored RSTs in the window: 0
listen queue overflows: 0
RTT updates: 3518(attempt segment: 3537)
correct ACK header predictions: 0
correct data packet header predictions: 568
resends due to MTU discovery: 0
packets dropped due to MD5 authentication failure: 0
packets that passed MD5 authentication: 0
sent Keychain-encrypted packets: 0
packets that passed Keychain authentication: 0
packets dropped due to Keychain authentication failure: 0
```

表1-6 display tcp statistics 命令显示信息描述表

字段	描述
Received packets:	<div>收到报文的统计信息，包括：</div> <ul style="list-style-type: none">• Total: 接收的报文总数• packets in sequence: 按顺序到达的报文数，括号中为字节数• window probe packets: 接收的窗口探测报文数• window update packets: 接收的窗口更新报文数• checksum error: 接收的校验和错误报文数• offset error: 接收的偏移量错误报文数• short error: 接收的报文长度太短的报文数• packets dropped for lack of memory: 由于内存不足而被丢弃的报文数• packets dropped due to PAWS: 由于 PAWS（防止序号回绕）而被丢弃的报文数• duplicate packets: 接收的完全重复报文数，括号中为字节数• partially duplicate packets: 接收的部分重复报文数，括号中为字节数• out-of-order packets: 接收的顺序错乱的报文数，括号中为字节数• packets with data after window: 落在接收窗口外的报文数，括号中为字节数• packets after close: 在连接关闭后到达的报文数• ACK packets: 接收的 ACK 确认报文数，括号中为字节数• duplicate ACK packets: 接收的重复的 ACK 确认报文数• ACK packets for unsent data: 接收的确认未发送数据的 ACK 报文数

字段	描述
Sent packets:	<p>发送报文的统计信息，包括：</p> <ul style="list-style-type: none"> • Total: 发送的报文总数 • urgent packets: 发送的紧急数据报文数 • control packets: 发送的控制报文数，括号中为包含的重传数据报文数 • window probe packets: 发送的窗口探测报文数 • window update packets: 发送的窗口更新报文数 • data packets: 发送的数据报文数，括号中为字节数 • data packets retransmitted: 重发的数据报文数，括号中为字节数 • ACK-only packets: 发送的 ACK 报文数，括号中为延迟 ACK 报文数 • unnecessary packet retransmissions: 报文非必要重传次数
Syncache/syncookie related statistics:	<p>syncache/syncookie有关的统计，包括：</p> <ul style="list-style-type: none"> • entries added to syncache: 添加的 syncache 对象数 • syncache entries retransmitted: 重传的 syncache 对象数 • duplicate SYN packets: 重复的 SYN 报文数 • reply failures: 回复失败的报文数 • successfully build new socket: 创建子 socket 成功数 • bucket overflows: bucket 溢出次数 • zone failures: 内存分配失败次数 • syncache entries removed due to RST: 由于收到 RST（复位连接）报文段而删除的 syncache 对象个数 • syncache entries removed due to timed out: 定时器超时且重传次数超过限制时 syncache 对象删除数 • ACK checked by syncache or syncookie failures: 接收到 ACK 报文时查找 syncache 处理失败数 • syncache entries aborted: 创建子 socket 失败数 • syncache entries removed due to bad ACK: 由于 bad ACK 而删除的 syncache 对象数 • syncache entries removed due to ICMP unreachable: 由于接收到 ICMP 差错报文导致删除的 syncache 对象数 • SYN cookies sent: SYN cookie 发送数 • SYN cookies received: SYN cookie 接收数
SACK related statistics	<p>SACK有关的统计，包括：</p> <ul style="list-style-type: none"> • SACK recoveries: 通过 SACK 进行恢复的次数 • SACK retransmitted segments: 通过 SACK 进行重传的报文段个数，括号中为字节数 • SACK blocks (options) received: 接收到的带选择性 ACK 选项的报文数 • SACK blocks (options) sent: 发送的带选择性 ACK 选项的报文数 • SACK scoreboard overflows: 本地维护的对端缺失报文段记录队列溢出次数

字段	描述
Other statistics	<p>其他统计，包括：</p> <ul style="list-style-type: none"> • retransmitted timeout: 重传定时器超时次数 • connections dropped in retransmitted timeout: 重传次数超过限制而丢弃的连接数 • persist timeout: 持续定时器超时次数 • keepalive timeout: 存活定时器超时次数 • keepalive probe: 发送的存活探测报文数 • keepalive timeout, so connections disconnected: 存活定时器超时而中断的连接数 • fin_wait_2 timeout, so connections disconnected: Fin wait 2 定时器超时而中断的连接数 • initiated connections: 发起连接次数 • accepted connections: 接受连接次数 • established connections: 已建立连接数 • closed connections(dropped: 0, initiated dropped: 0): 已关闭连接数目，括号中为意外丢弃连接数（收到对端 SYN 之后）、主动连接失败数（收到对端 SYN 之前） • bad connection attempt: 接收到的错误连接报文数 • ignored RSTs in the window: 窗口中忽略的 RST 报文数 • listen queue overflows: 监听队列溢出次数 • RTT updates(attempt segment): RTT 更新次数，括号中为发送的报文数 • correct ACK header predictions: ACK 通过首部预测算法的次数 • correct data packet header predictions: 数据报文通过首部预测算法的次数 • resends due to MTU discovery: 由于 MTU 发现而重传的报文数 • packets dropped due to MD5 authentication failure: MD5 验证丢弃报文数 • packets that passed MD5 authentication: MD5 验证通过报文数 • sent Keychain-encrypted packets: Keychain 加密的发送报文数 • packets that passed Keychain authentication: Keychain 验证通过的接收报文数 • packets dropped due to Keychain authentication failure: Keychain 验证丢弃的接收报文数

【相关命令】

- **reset tcp statistics**

1.1.7 display tcp verbose

display tcp verbose 命令用来显示 TCP 连接详细信息。

【命令】

display tcp verbose [slot slot-number [pcb pcb-index]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

pcb *pcb-index*: 显示指定协议控制块索引的 TCP 连接详细信息。*pcb-index* 表示协议控制块索引，取值为十六进制字符串 1~ffffffffffffff。

slot *slot-number*: 显示指定成员设备的 TCP 连接详细信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 TCP 连接详细信息。

【使用指导】

display tcp verbose 命令用来显示 TCP 连接的详细信息，包括 socket 的创建者、状态、选项、类型、使用的协议号、以及 TCP 连接的源 IP 地址及端口号、目的 IP 地址及端口号、状态等信息。

【举例】

```
# 显示 TCP 连接详细信息。
<Sysname> display tcp verbose
TCP inpcb number: 1(tcpcb number: 1)

Location: slot: 6 cpu: 0
NSR standby: N/A
Creator: bgpd[199]
State: ISCONNECTED
Options: N/A
Error: 0
Receiving buffer(cc/hiwat/lowat/state): 0 / 65700 / 1 / N/A
Sending buffer(cc/hiwat/lowat/state): 0 / 65700 / 512 / N/A
Type: 1
Protocol: 6
Connection info: src = 192.168.20.200:179 , dst = 192.168.20.14:4181
Inpcb flags: N/A
Inpcb extflag: N/A
Inpcb vflag: INP_IPV4
TTL: 255(minimum TTL: 0)
Connection state: ESTABLISHED
TCP options: TF_REQ_SCALE TF_REQ_TSTMP TF_SACK_PERMIT TF_NSR
NSR state: READY(M)
Send VRF: 0x0
Receive VRF: 0x0
```

表1-7 display tcp verbose 命令显示信息描述表

字段	描述
TCP inpcb number	TCP类型internet协议控制块个数

字段	描述
tcpcb number	TCP控制块个数（处于TIME_WAIT状态的TCP则没有此计数）
Creator	创建socket的任务名称，括号中为创建者的进程号
State	<p>socket的状态，包括：</p> <ul style="list-style-type: none"> • NOFDREF：用户已经关闭 • ISCONNECTED：连接已经建立 • ISCONNECTING：正在建立连接 • ISDISCONNECTING：正在断开连接 • ASYNC：异步方式 • ISDISCONNECTED：连接已经断开 • PROTOREF：协议强关联 • N/A：不处于上述状态
Options	<p>socket的选项，包括：</p> <ul style="list-style-type: none"> • SO_DEBUG：记录套接字的调试信息 • SO_ACCEPTCONN：server 端监听连接请求 • SO_REUSEADDR：允许本地地址重复使用 • SO_KEEPALIVE：协议需要查询空闲的连接 • SO_DONTROUTE：设置不查路由表，由于目的地址是直连网络的情况 • SO_BROADCAST：套接字支持广播报文 • SO_LINGER：套接字关闭但仍发送剩余数据 • SO_OOBINLINE：带外数据采用内联方式存储 • SO_REUSEPORT：允许本地端口重复使用 • SO_TIMESTAMP：入报文记录时间戳，只对非连接的协议有效，时间精确到毫秒 • SO_NOSIGPIPE：socket 不能发送数据导致返回失败时不创建 SIGPIPE • SO_TIMESTAMPNS：和时间戳选项功能类似，时间可以精确到纳秒 • SO_KEEPALIVETIME：设置空闲探测时间 • N/A：未设置选项
Error	影响socket连接的错误码
Receiving buffer(cc/hiwat/lowat/state)	<p>接收缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间和状态，状态的取值包括：</p> <ul style="list-style-type: none"> • CANTSENDMORE：不能发送数据到对端 • CANTRCVMORE：不能从对端接收数据 • RCVATMARK：接收标记 • N/A：不处于上述状态

字段	描述
Sending buffer(cc/hiwat/lowat/state)	<p>发送缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间和状态，状态的取值包括：</p> <ul style="list-style-type: none"> • CANTSENDMORE：不能发送数据到对端 • CANTRCVMORE：不能从对端接收数据 • RCVATMARK：接收标记 • N/A：不处于上述状态
Type	<p>使用的socket类型，类型的取值包括：</p> <ul style="list-style-type: none"> • 1：SOCK_STREAM，流模式，提供可靠的字节流。TCP 协议使用此类型 • 2：SOCK_DGRAM，数据报模式的通信。UDP 协议使用此类型 • 3：SOCK_RAW，RAW 模式的通信方式 • N/A：不是上述类型
Protocol	使用socket的协议号
Connection info	连接信息，分别为源IP地址及端口号、目的IP地址及端口号
Inpcb flags	<p>Internet协议控制块中的标记，标记的取值包括：</p> <ul style="list-style-type: none"> • INP_RECVOPTS：接收传入的 IP 选项 • INP_RECVRETOPTS：接收回应的 IP 选项 • INP_RECVDSTADDR：接收目的 IP 地址 • INP_HDRINCL：用户提供整个 IP 头 • INP_REUSEADDR：重复使用地址 • INP_REUSEPORT：重复使用端口号 • INP_ANONPORT：用户未指定端口 • INP_RECVIF：接收报文时记录报文的入接口 • INP_RECVTTL：携带报文的 TTL，仅 UDP 和 RawIP 支持 • INP_DONTFRAG：设置不可分片标志 • INP_ROUTER_ALERT：接收携带路由器告警选项的报文，仅 RawIP 支持 • INP_PROTOCOL_PACKET：标识报文为协议报文 • INP_RCVVLANID：接收报文的 VLAN ID，仅 UDP 和 RawIP 支持 • INP_RCVMACADDR：接收报文的 MAC • INP_RECVTOS：携带报文的 TOS，仅 UDP 和 RawIP 支持 • INP_SYNCPCB：阻塞等待 inpcb 同步 • N/A：不是上述标记
Inpcb extflag	<p>Internet协议控制块中的扩展标记，标记的取值包括：</p> <ul style="list-style-type: none"> • INP_EXTRCVPVCIDX：接收报文时记录报文的 PVC 索引 • INP_RCVPWID：接收报文时记录报文的 PW ID • INP_EXTDONTDROP：接收报文时设置报文不要丢弃 • N/A：不是上述标记

字段	描述
Inpcb vflag	<p>Internet协议控制块中的IP版本标记，标记的取值包括：</p> <ul style="list-style-type: none"> • INP_IPV4: 运用与 IPv4 通信 • INP_TIMEWAIT: 处于等待状态 • INP_ONESBCAST: 发送广播报文 • INP_DROPPED: 协议丢弃标志 • INP_SOCKREF: socket 强关联 • INP_DONTBLOCK: inpcb 同步时不能被阻塞 • N/A: 不是上述标记
TTL	Internet协议控制块中的生存周期，括号中为最小生存周期
Connection state	<p>TCP连接状态，包括：</p> <ul style="list-style-type: none"> • CLOSED: 服务器收到客户端的关闭连接请求回应后所处的状态 • LISTEN: 服务器在等待连接请求时所处的状态 • SYN_SENT: 客户端发出连接请求等待服务器回应时所处的状态 • SYN_RCVD: 服务器收到客户端连接请求时所处的状态 • ESTABLISHED: 服务器和客户端双方建立连接并能进行双向数据传递的状态 • CLOSE_WAIT: 服务器收到客户端关闭连接请求时所处的状态 • FIN_WAIT_1: 客户端发出关闭连接请求等待服务器回应时所处的状态 • CLOSING: 连接双方在向对端发出关闭连接请求后等待对端回应过程中收到对端发出的关闭连接请求时所处的状态 • LAST_ACK: 服务器向客户端发出关闭连接请求等待回应时所处的状态 • FIN_WAIT_2: 客户端收到服务器关闭连接回应后所处的状态 • TIME_WAIT: 客户端收到服务器的关闭连接请求后所处的状态
TCP options	<p>TCP的选项类型，包括：</p> <ul style="list-style-type: none"> • TF_MD5SIG: 使能密钥 • TF_NODELAY: 关闭延时 ACK • TF_NOOPT: TCP 不使用选项 • TF_NOPUSH: 对写入的最后部分不进行 PUSH 操作 • TF_BINDFOREIGNADDR: 绑定对端 IP 地址 • TF_NSR: 使能 TCP NSR • TF_REQ_SCALE: 使能窗口缩放因子选项 • TF_REQ_TSTMP: 使能时间戳选项 • TF_SACK_PERMIT: 使能选择性 ACK 选项 • TF_ENHANCED_AUTH: 使能增强认证选项

字段	描述
NSR state	TCP连接NSR状态，可能的状态如下： <ul style="list-style-type: none"> • CLOSED：关闭（初始）状态 • CLOSING：连接待关闭状态 • ENABLED：使能备份功能状态 • OPEN：连接开始同步状态 • PENDING：连接判定状态 • READY：连接备份就绪状态 • SMOOTH：连接平滑状态 角色：M表示主连接、S表示备份连接
Send VRF	（暂不支持）发送实例
Receive VRF	（暂不支持）接收实例

1.1.8 display udp

display udp 命令用来显示 UDP 连接摘要信息。

【命令】

display udp [*slot slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot slot-number：显示指定成员设备的 UDP 连接摘要信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 UDP 连接摘要信息。

【使用指导】

display udp 命令用来显示 UDP 连接摘要信息，包括本端 IP 地址及端口号、对端 IP 地址及端口号等信息。

【举例】

显示 UDP 连接摘要信息。

```
<Sysname> display udp
Local Addr:port      Foreign Addr:port    Slot  PCB
0.0.0.0:69           0.0.0.0:0            1     0x0000000000000003
```

表1-8 display udp 命令显示信息描述表

字段	描述
Local Addr:port	本端IP地址及端口号

字段	描述
Foreign Addr:port	对端IP地址及端口号
PCB	协议控制块索引

1.1.9 display udp statistics

display udp statistics 命令用来显示 UDP 流量统计信息。

【命令】

display udp statistics [*slot slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot slot-number: 显示指定成员设备的 UDP 流量统计信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 UDP 流量统计信息。

【使用指导】

display udp statistics 命令用来显示 UDP 流量统计信息，包括接收和发送的各类 UDP 报文信息。

【举例】

显示 UDP 流量统计信息。

```
<Sysname> display udp statistics
Received packets:
  Total: 240
  checksum error: 0, no checksum: 0
  shorter than header: 0, data length larger than packet: 0
  no socket on port(unicast): 0
  no socket on port(broadcast/multicast): 240
  not delivered, input socket full: 0
Sent packets:
  Total: 0
```

表1-9 display udp statistics 命令显示信息描述表

字段	描述
Received packets:	<p>收到报文的信息，包括：</p> <ul style="list-style-type: none"> • Total: 接收的 UDP 报文总数 • checksum error: 校验和出错的报文数 • no checksum: 没有校验和的报文数 • shorter than header: 报文长度比报文头部短的报文数 • data length larger than packet: 报文数据长度超过报文长度的报文数 • no socket on port(unicast): 端口上无 socket 的单播报文数 • no socket on port(broadcast/multicast): 端口上无 socket 的广播和组播报文数 • not delivered, input socket full: 因为 socket 缓冲区已满而未向上层传送的报文数
Sent packets:	发送报文的信息，包括 Total ，表示发送的UDP报文总数

【相关命令】

- **reset udp statistics**

1.1.10 display udp verbose

display udp verbose 命令用来显示 UDP 连接详细信息。

【命令】

display udp verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

pcb *pcb-index*: 显示指定协议控制块索引的 UDP 连接详细信息。*pcb-index* 表示协议控制块索引，取值为十六进制字符串 1~ffffffffffffff。

slot *slot-number*: 显示指定成员设备的 UDP 连接详细信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 UDP 连接详细信息。

【使用指导】

display udp verbose 命令用来显示 UDP 连接的详细信息，包括 socket 的创建者、状态、选项、类型、使用的协议号、以及 UDP 连接的源 IP 地址及端口号、目的 IP 地址及端口号等信息。

【举例】

```
# 显示 UDP 连接详细信息。
<Sysname> display udp verbose
Total UDP socket number: 1

Location: slot: 6 cpu: 0
Creator: sock_test_mips[250]
State: N/A
Options: N/A
Error: 0
Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 41600 / 1 / 0 / N/A
Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
Type: 2
Protocol: 17
Connection info: src = 0.0.0.0:69, dst = 0.0.0.0:0
Inpcb flags: N/A
Inpcb extflag: N/A
Inpcb vflag: INP_IPV4
TTL: 255(minimum TTL: 0)
Send VRF: 0xffff
Receive VRF: 0xffff
```

表1-10 display udp verbose 命令显示信息描述表

字段	描述
Total UDP socket number	UDP socket总数
Creator	创建socket的任务名称，括号中为创建者的进程号
State	socket的状态，可能的状态如下： <ul style="list-style-type: none">• NOFDREF：用户已经关闭• ISCONNECTED：连接已经建立• ISCONNECTING：正在建立连接• ISDISCONNECTING：正在断开连接• ASYNC：异步方式• ISDISCONNECTED：连接已经断开• PROTOREF：协议强关联• N/A：不处于上述状态

字段	描述
Options	<p>socket的选项，有以下几种：</p> <ul style="list-style-type: none"> SO_DEBUG：记录套接字的调试信息 SO_ACCEPTCONN：server 端监听连接请求 SO_REUSEADDR：允许本地地址重复使用 SO_KEEPALIVE：协议需要查询空闲的连接 SO_DONTROUTE：设置不查路由表，由于目的地址是直连网络的情况 SO_BROADCAST：套接字支持广播报文 SO_LINGER：套接字关闭但仍发送剩余数据 SO_OOBINLINE：带外数据采用内联方式存储 SO_REUSEPORT：允许本地端口重复使用 SO_TIMESTAMP：入报文记录时间戳，只对非连接的协议有效，时间精确到毫秒 SO_NOSIGPIPE：socket 不能发送数据导致返回失败时不创建SIGPIPE SO_TIMESTAMPNS：和时戳选项功能类似，时间可以精确到纳秒 N/A：未设置选项
Error	影响socket连接的错误码
Receiving buffer(cc/hiwat/lowat/drop/state)	<p>接收缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间、丢包数和状态，状态的取值有：</p> <ul style="list-style-type: none"> CANTSENDMORE：不能发送数据到对端 CANTRCVMORE：不能从对端接收数据 RCVATMARK：接收标记 N/A：不处于上述状态
Sending buffer(cc/hiwat/lowat/state)	<p>发送缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间和状态，状态的取值有：</p> <ul style="list-style-type: none"> CANTSENDMORE：不能发送数据到对端 CANTRCVMORE：不能从对端接收数据 RCVATMARK：接收标记 N/A：不处于上述状态
Type	<p>使用的socket类型，类型的取值有：</p> <ul style="list-style-type: none"> 1：SOCK_STREAM，流模式，提供可靠的字节流。TCP 协议使用此类型 2：SOCK_DGRAM，数据报模式的通信。UDP 协议使用此类型 3：SOCK_RAW，RAW 模式的通信方式 N/A：不是上述类型
Protocol	使用socket的协议号
Connection info	连接信息，分别为源IP地址及端口号、目的IP地址及端口号

字段	描述
Inpcb flags	<p>Internet协议控制块中的标记，标记的取值有：</p> <ul style="list-style-type: none"> • INP_RECVOPTS: 接收传入的 IP 选项 • INP_RECVRETOPTS: 接收回应的 IP 选项 • INP_RECVDSTADDR: 接收目的 IP 地址 • INP_HDRINCL: 用户提供整个 IP 头 • INP_REUSEADDR: 重复使用地址 • INP_REUSEPORT: 重复使用端口号 • INP_ANONPORT: 用户未指定端口 • INP_RECVIF: 接收报文时记录报文的入接口 • INP_RECVTTL: 携带报文的 TTL，仅 UDP 和 RawIP 支持 • INP_DONTFRAG: 设置不可分片标志 • INP_ROUTER_ALERT: 接收携带路由器告警选项的报文，仅 RawIP 支持 • INP_PROTOCOL_PACKET: 标识报文为协议报文 • INP_RCVVLANID: 接收报文的 VLAN ID，仅 UDP 和 RawIP 支持 • INP_RCVMACADDR: 接收报文的 MAC • INP_RECVTOS: 携带报文的 TOS，仅 UDP 和 RawIP 支持 • INP_SYNCPCB: 阻塞等待 inpcb 同步 • N/A: 不是上述标记
Inpcb extflag	<p>Internet协议控制块中的扩展标记，标记的取值有：</p> <ul style="list-style-type: none"> • INP_EXTRCVPVCIDX: 接收报文时记录报文的 PVC 索引 • INP_RCVPWID: 接收报文时记录报文的 PW ID • N/A: 不是上述标记
Inpcb vflag	<p>Internet协议控制块中的IP版本标记，标记的取值有：</p> <ul style="list-style-type: none"> • INP_IPV4: 运用与 IPv4 通信 • INP_TIMEWAIT: 处于等待状态 • INP_ONESBCAST: 发送广播报文 • INP_DROPPED: 协议丢弃标志 • INP_SOCKREF: socket 强关联 • INP_DONTBLOCK: inpcb 同步时不能被阻塞 • N/A: 不是上述标记
TTL	Internet协议控制块中的生存周期，括号中为最小生存周期
Send VRF	（暂不支持）发送实例
Receive VRF	（暂不支持）接收实例

1.1.11 ip forward-broadcast

ip forward-broadcast 命令用来配置允许接口转发直连网段的定向广播报文。

undo ip forward-broadcast 命令用来禁止接口转发直连网段的定向广播报文。

【命令】

```
ip forward-broadcast [ acl acl-number ]
undo ip forward-broadcast
```

【缺省情况】

设备禁止转发直连网段的定向广播报文。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

acl acl-number: 对定向广播报文应用该 ACL 规则号对应的过滤条件，根据过滤结果决定是否转发该定向广播报文。*acl-number* 取值范围为 2000~3999，其中 2000 到 2999 是基本 ACL 规则，3000 到 3999 是高级 ACL 规则。

【使用指导】

定向广播报文是指发送给特定网络的广播报文。该报文的目的 IP 地址中网络号码字段为特定网络的网络号，主机号码字段为全 1。

在转发定向广播报文的情况下，如果在接口上配置了此命令，设备从其他接口接收到目的地址为此接口直连网段的定向广播报文时，会从此接口转发此类报文。

黑客可以利用定向广播报文来攻击网络系统，给网络的安全带来了很大的隐患。但在某些应用环境下，设备接口需要转发这类定向广播报文，例如：

- 开启 UDP Helper 功能，将广播报文转换为单播报文发送给指定的服务器。
- 开启 Wake on LAN（网络唤醒）功能，发送定向广播报文唤醒远程网络中的计算机。

在上述情况下，用户可以通过命令配置接口允许转发直连网段的定向广播报文。

【举例】

配置允许 VLAN 接口 2 转发面向直连网段的定向广播报文。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ip forward-broadcast
```

1.1.12 ip icmp error-interval

ip icmp error-interval 用来配置发送 ICMP 差错报文对应的令牌刷新周期和令牌桶容量。

undo ip icmp error-interval 用来恢复缺省情况

【命令】

```
ip icmp error-interval interval [ bucketsize ]
undo ip icmp error-interval
```

【缺省情况】

令牌刷新周期为 100 毫秒，令牌桶容量为 10。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval: 令牌刷新周期，取值范围 0~2147483647，单位为毫秒。取值为 0 时，表示不限制 ICMP 差错报文的发送。

bucket-size: 令牌桶中容纳的令牌数，取值范围 1~200。

【使用指导】

如果网络中短时间内发送的 ICMP 差错报文过多，将可能导致网络拥塞。为了避免这种情况，用户可以控制设备在指定时间内发送 ICMP 差错报文的数目，目前采用令牌桶算法来实现。

用户可以设置令牌桶的容量，即令牌桶中可以同时容纳的令牌数；同时可以设置令牌桶的刷新周期，即每隔多长时间发放一个令牌到令牌桶中，直到令牌桶中的令牌数达到配置的容量。一个令牌表示允许发送一个 ICMP 差错报文，每当发送一个 ICMP 差错报文，则令牌桶中减少一个令牌。如果连续发送的 ICMP 差错报文超过了令牌桶的容量，则后续的 ICMP 差错报文将不能被发送出去，直到按照所设置的刷新频率将新的令牌放入令牌桶中。

【举例】

配置设备发送 ICMP 差错报文对应的令牌刷新周期为 200 毫秒，令牌桶容量为 40。

```
<Sysname> system-view
[Sysname] ip icmp error-interval 200 40
```

1.1.13 ip icmp source

ip icmp source 命令用来指定 ICMP 报文源地址。

undo ip icmp source 命令用来删除指定的 ICMP 报文源地址。

【命令】

```
ip icmp source ip-address
undo ip icmp source
```

【缺省情况】

未指定 ICMP 报文源地址。设备使用出接口 IP 地址作为 ICMP 报文源地址。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ip-address: 表示设备发送 ICMP 报文时指定的源地址。

【使用指导】

在网络中 IP 地址配置较多的情况下，收到 ICMP 报文时，用户很难根据报文的源 IP 地址判断报文来自哪台设备。为了简化这一判断过程，可以配置 ICMP 报文指定源地址功能。用户配置特定地址（如环回口地址）为 ICMP 报文的源地址，可以简化判断。

设备发送 ICMP 差错报文（TTL 超时、端口不可达和参数错误等）和 ping echo request 报文时，都可以通过上述命令指定报文的源地址。

【举例】

配置设备发送 ICMP 报文时指定的源地址为 1.1.1.1。

```
<Sysname> system-view
[Sysname] ip icmp source 1.1.1.1
```

1.1.14 ip mtu

ip mtu 命令用来配置接口上发送 IPv4 报文的 MTU。

undo ip mtu 命令用来恢复缺省情况。

【命令】

```
ip mtu mtu-size
undo ip mtu
```

【缺省情况】

未配置接口上发送 IPv4 报文的 MTU。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

mtu-size：MTU 的大小，单位为字节，取值范围为 128～1500。

【使用指导】

当设备使用某个接口发送报文时，发现报文长度大于该接口的发送 IPv4 报文的 MTU 值，则进行下列处理：

- 如果报文不允许分片，则将报文丢弃；
- 如果报文允许分片，则将报文进行分片转发。

为了减轻转发设备在传输过程中的分片和重组数据包的压力，更高效的利用网络资源，请根据实际组网环境设置合适的接口发送 IPv4 报文的 MTU 值，以减少分片的发生。

如果当前接口同时支持 **mtu** 和 **ip mtu** 命令，则设备会以 **ip mtu** 命令配置的接口发送 IPv4 报文的 MTU 值对报文进行分片，不会再按照 **mtu** 命令配置的 MTU 值对报文进行分片。

【举例】

配置 VLAN 接口 100 上发送 IPv4 报文的 MTU 值为 1280 字节。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
```

```
[Sysname-Vlan-interface100] ip mtu 1280
```

1.1.15 ip reassemble local enable

ip reassemble local enable 命令用来开启 IP 分片报文本地重组功能。

undo ip reassemble local enable 命令用来关闭 IP 分片报文本地重组功能。

【命令】

```
ip reassemble local enable
undo ip reassemble local enable
```

【缺省情况】

IP 分片报文本地重组功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

多台设备组成的 IRF 环境下，当某成员设备收到目的为本 IRF 设备的 IP 分片报文时，需要把分片报文送到主设备进行重组，这样会导致报文重组性能较低的问题。当开启 IP 分片报文本地重组功能后，分片报文会在该成员设备上直接进行报文重组，这样就能提高分片报文的重组性能。开启 IP 分片报文本地重组功能后，如果分片报文是从设备上不同的成员设备进入的，会导致 IP 分片报文本地无法重组成功。

【举例】

开启 IP 分片报文本地重组功能。

```
<Sysname> system-view
[Sysname] ip reassemble local enable
```

1.1.16 ip redirects enable

ip redirects enable 命令用来开启设备的 ICMP 重定向报文的发送功能。

undo ip redirects enable 命令用来关闭设备的 ICMP 重定向报文的发送功能。

【命令】

```
ip redirects enable
undo ip redirects enable
```

【缺省情况】

ICMP 重定向报文发送功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

ICMP 重定向报文发送功能可以简化主机的管理，使具有很少选路信息的主机逐渐建立较完善的路由表，从而找到最佳路由。

主机启动时，它的路由表中可能只有一条到缺省网关的缺省路由。当满足一定的条件时，缺省网关会向源主机发送 ICMP 重定向报文，通知主机重新选择正确的下一跳进行后续报文的发送。

满足下列条件时，设备会发送 ICMP 重定向报文：

- 接收和转发数据报文的接口是同一接口；
- 被选择的路由本身没有被 ICMP 重定向报文创建或修改过；
- 被选择的路由不是设备的默认路由；
- 数据报文中没有源路由选项。

【举例】

开启设备的 ICMP 重定向报文发送功能。

```
<Sysname> system-view
[Sysname] ip redirects enable
```

1.1.17 ip ttl-expires enable

ip ttl-expires enable 命令用来开启设备的 ICMP 超时报文的发送功能。

undo ip ttl-expires enable 命令用来关闭设备的 ICMP 超时报文的发送功能。

【命令】

```
ip ttl-expires enable
undo ip ttl-expires enable
```

【缺省情况】

ICMP 超时报文发送功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

ICMP 超时报文发送功能是在设备收到 IP 数据报文后，如果发生超时差错，则将报文丢弃并给源端发送 ICMP 超时差错报文。

设备在满足下列条件时会发送 ICMP 超时报文：

- 设备收到 IP 数据报文后，如果报文的目的地不是本地且报文的 TTL 字段是 1，则发送“TTL 超时”ICMP 差错报文；
- 设备收到目的地址为本地的 IP 数据报文的第一个分片后，启动定时器，如果所有分片报文到达之前定时器超时，则会发送“重组超时”ICMP 差错报文。

需要注意的是，关闭 ICMP 超时报文发送功能后，设备不会再发送“TTL 超时”ICMP 差错报文，但“重组超时”ICMP 差错报文仍会正常发送。

【举例】

开启设备的 ICMP 超时报文发送功能。

```
<Sysname> system-view
[Sysname] ip ttl-expires enable
```

1.1.18 ip unreachable enable

ip unreachable enable 命令用来开启设备的 ICMP 目的不可达报文的发送功能。

undo ip unreachable enable 命令用来关闭设备的 ICMP 目的不可达报文的发送功能。

【命令】

```
ip unreachable enable
undo ip unreachable enable
```

【缺省情况】

ICMP 目的不可达报文发送功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

ICMP 目的不可达报文发送功能是在设备收到 IP 数据报文后，如果发生目的不可达的差错，则将报文丢弃并给源端发送 ICMP 目的不可达差错报文。

设备在满足下列条件时会发送目的不可达报文：

- 设备在转发报文时，如果在路由表中未找到对应的转发路由，且路由表中没有缺省路由，则给源端发送“网络不可达” ICMP 差错报文；
- 设备收到目的地址为本地的数据报文时，如果设备不支持数据报文采用的传输层协议，则给源端发送“协议不可达” ICMP 差错报文；
- 设备收到目的地址为本地、传输层协议为 UDP 的数据报文时，如果报文的端口号与正在使用的进程不匹配，则给源端发送“端口不可达” ICMP 差错报文；
- 源端如果采用“严格的源路由选择”发送报文，当中间设备发现源路由所指定的下一个设备不在其直接连接的网络上，则给源端发送“源站路由失败”的 ICMP 差错报文；
- 设备在转发报文时，如果转发接口的 MTU 小于报文的长度，但报文被设置了不可分片，则给源端发送“需要进行分片但设置了不分片比特” ICMP 差错报文。

【举例】

开启设备的 ICMP 目的不可达报文发送功能。

```
<Sysname> system-view
[Sysname] ip unreachable enable
```

1.1.19 reset ip statistics

reset ip statistics 命令用来清除 IP 报文统计信息。

【命令】

```
reset ip statistics [ slot slot-number ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

slot slot-number: 清除指定成员设备的 IP 报文统计信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则清除所有成员设备上的 IP 报文统计信息。

【使用指导】

在某些情况下，需要统计一定时间内接口的 IP 报文统计信息，这时必须在统计开始前清除原有的统计信息，重新进行统计。

【举例】

```
# 清除 IP 报文统计信息。  
<Sysname> reset ip statistics
```

【相关命令】

- **display ip interface**（三层技术-IP 业务命令参考/IP 地址）
- **display ip statistics**

1.1.20 reset tcp statistics

reset tcp statistics 命令用来清除 TCP 连接的流量统计信息。

【命令】

```
reset tcp statistics
```

【视图】

用户视图

【缺省用户角色】

network-admin

【举例】

```
# 清除 TCP 连接的流量统计信息。  
<Sysname> reset tcp statistics
```

【相关命令】

- **display tcp statistics**

1.1.21 reset udp statistics

reset udp statistics 命令用来清除 UDP 流量统计信息。

【命令】

```
reset udp statistics
```

【视图】

用户视图

【缺省用户角色】

network-admin

【举例】

清除 UDP 流量统计信息。

```
<Sysname> reset udp statistics
```

【相关命令】

- `display udp statistics`

1.1.22 tcp mss

`tcp mss` 命令用来配置接口的 TCP 最大报文段长度。

`undo tcp mss` 命令用来恢复缺省情况。

【命令】

```
tcp mss value
```

```
undo tcp mss
```

【缺省情况】

未配置接口的 TCP 最大报文段长度。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

value: TCP 最大报文段长度，取值范围为 128~1460，单位为字节。

【使用指导】

TCP 最大报文段长度（Max Segment Size, MSS）表示 TCP 连接的对端发往本端的最大 TCP 报文段的长度，目前作为 TCP 连接建立时的一个选项来协商：当一个 TCP 连接建立时，连接的双方要将 MSS 作为 TCP 报文的一个选项通告给对端，对端会记录下这个 MSS 值，后续在发送 TCP 报文时，会限制 TCP 报文的大小不超过该 MSS 值。当对端发送的 TCP 报文的长度小于本端的 TCP 最大报文段长度时，TCP 报文不需要分段；否则，对端需要对 TCP 报文按照最大报文段长度进行分段处理后再发给本端。

该配置仅对新建的 TCP 连接生效，对于配置前已建立的 TCP 连接不生效。

该配置仅对 IP 报文生效。

【举例】

配置 VLAN 接口 100 上 TCP 最大报文段长度为 300 字节。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] tcp mss 300
```

1.1.23 tcp path-mtu-discovery

tcp path-mtu-discovery 命令用来开启 TCP 连接的 Path MTU 探测功能。

undo tcp path-mtu-discovery 命令用来关闭 TCP 连接的 Path MTU 探测功能。

【命令】

```
tcp path-mtu-discovery [ aging age-time | no-aging ]
undo tcp path-mtu-discovery
```

【缺省情况】

TCP 连接的 Path MTU 探测功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

aging age-time: Path MTU 的老化时间, *age-time* 的取值范围为 10~30, 单位为分钟, 缺省值为 10。

no-aging: Path MTU 不老化。

【使用指导】

开启 TCP 连接的 Path MTU 探测功能后, 新建的 TCP 连接均会携带 Path MTU 探测属性, 可以通过探测机制确定 Path MTU, 按照数据路径上的最小 MTU 组织 TCP 分段长度, 最大限度利用网络资源, 避免 IP 分片的发生。

关闭 TCP 连接的 Path MTU 探测功能后, 系统将停止所有正在运行的 Path MTU 定时器, 此后创建的 TCP 连接均无 Path MTU 探测功能, 但是对于此前已经建立的 TCP 连接, 其 Path MTU 探测功能不会被关闭。

【举例】

开启 TCP 连接的 Path MTU 探测功能, Path MTU 的老化时间为 20 分钟。

```
<Sysname> system-view
[Sysname] tcp path-mtu-discovery aging 20
```

1.1.24 tcp syn-cookie enable

tcp syn-cookie enable 命令用来开启 SYN Cookie 功能, 防止设备受到 SYN Flood 攻击。

undo tcp syn-cookie enable 命令用来关闭 SYN Cookie 功能。

【命令】

```
tcp syn-cookie enable
undo tcp syn-cookie enable
```

【缺省情况】

SYN Cookie 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

一般情况下，TCP 连接的建立需要经过三次握手，一些恶意的攻击者利用 TCP 连接的建立过程进行 SYN Flood 攻击：攻击者向服务器发送大量请求建立 TCP 连接的 SYN 报文，而不回应服务器的 SYN ACK 报文，导致服务器上建立了大量的 TCP 半连接。从而，达到耗费服务器资源，使服务器无法处理正常业务的目的。

SYN Cookie 功能用来防止 SYN Flood 攻击。当服务器收到 TCP 连接请求时，不建立 TCP 半连接，而直接向发起者回复 SYN ACK 报文。服务器接收到发起者回应的 ACK 报文后，才建立连接。通过这种方式，可以避免在服务器上建立大量的 TCP 半连接，防止服务器受到 SYN Flood 攻击。

【举例】

```
# 开启 SYN Cookie 功能。
<Sysname> system-view
[Sysname] tcp syn-cookie enable
```

1.1.25 tcp timer fin-timeout

tcp timer fin-timeout 命令用来配置 TCP 的 finwait 定时器超时时间。

undo tcp timer fin-timeout 命令用来恢复缺省情况。

【命令】

```
tcp timer fin-timeout time-value
undo tcp timer fin-timeout
```

【缺省情况】

TCP finwait 定时器的超时时间为 675 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

time-value：TCP finwait 定时器的超时时间，取值范围为 76～3600，单位为秒。

【使用指导】

当 TCP 的连接状态为 FIN_WAIT_2 时，启动 finwait 定时器，如果在定时器超时前未收到报文，则 TCP 连接终止；如果收到 FIN 报文，则 TCP 连接状态变为 TIME_WAIT 状态；如果收到非 FIN 报文，则从收到的最后一个非 FIN 报文开始重新计时，在超时后中止连接。

【举例】

配置 TCP finwait 定时器的超时时间为 800 秒。

```
<Sysname> system-view
[Sysname] tcp timer fin-timeout 800
```

1.1.26 tcp timer syn-timeout

tcp timer syn-timeout 命令用来配置 TCP 的 synwait 定时器超时时间。

undo tcp timer syn-timeout 命令用来恢复缺省情况。

【命令】

```
tcp timer syn-timeout time-value
undo tcp timer syn-timeout
```

【缺省情况】

TCP synwait 定时器的超时时间为 75 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

time-value：TCP synwait 定时器的超时时间，取值范围为 2~600，单位为秒。

【使用指导】

当发送 SYN 报文时，TCP 启动 synwait 定时器和重传 SYN 报文定时器，当 synwait 定时器超时且 SYN 报文重传未达到最大次数时，如果设备未收到回应报文，则 TCP 连接建立不成功；当 synwait 定时器未超时但是 SYN 报文重传达到最大次数时，如果设备未收到回应报文，则 TCP 连接建立不成功。

【举例】

配置 TCP synwait 定时器的超时时间为 80 秒。

```
<Sysname> system-view
[Sysname] tcp timer syn-timeout 80
```

1.1.27 tcp window

tcp window 命令用来设置 TCP 连接的收发缓冲区大小。

undo tcp window 命令用来恢复缺省情况。

【命令】

```
tcp window window-size  
undo tcp window
```

【缺省情况】

TCP 连接的收发缓冲区大小为 63KB。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

window-size: TCP 连接的收发缓冲区大小，取值范围为 1~64，单位为 KB（千字节）。

【举例】

设置 TCP 连接的收发缓冲区大小为 3KB。

```
<Sysname> system-view  
[Sysname] tcp window 3
```

目 录

1 UDP Helper.....	1-1
1.1 UDP Helper配置命令.....	1-1
1.1.1 display udp-helper interface	1-1
1.1.2 reset udp-helper statistics.....	1-2
1.1.3 udp-helper broadcast-map.....	1-2
1.1.4 udp-helper enable.....	1-3
1.1.5 udp-helper port.....	1-4
1.1.6 udp-helper server	1-4

1 UDP Helper



说明

S5110V2-SI、S5000V3-EI 和 S5000E-X 系列交换机不支持本特性。

1.1 UDP Helper配置命令

1.1.1 display udp-helper interface

display udp-helper interface 命令用来显示指定接口下广播转单播中继转发的相关信息。

【命令】

display udp-helper interface *interface-type* *interface-number*

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface-type interface-number: 接口类型和接口编号。

【使用指导】

通过本命令可以查看指定接口配置的广播转单播中继转发的目的服务器信息以及广播转单播中继转发处理的报文数目。

【举例】

显示 VLAN 接口 100 的 UDP 中继转发相关信息。

```
<Sysname> display udp-helper interface vlan-interface 100
```

Interface	Server VPN instance	Server address	Packets sent
Vlan-interface100	N/A	192.1.1.2	0
Vlan-interface100	N/A	192.1.1.2	0

表1-1 display udp-helper interface 命令显示信息描述表

字段	描述
Interface	接口名
Server VPN instance	（暂不支持）中继转发目的服务器所在的VPN实例名
Server address	中继转发目的服务器地址
Packets sent	广播转单播UDP Helper 处理的报文数目

【相关命令】

- `reset udp-helper statistics`
- `udp-helper server`

1.1.2 reset udp-helper statistics

`reset udp-helper statistics` 命令用来清除广播转单播中继转发的报文统计数目。

【命令】

`reset udp-helper statistics`

【视图】

用户视图

【缺省用户角色】

network-admin

【举例】

清除广播转单播中继转发的报文统计数目。

<Sysname> `reset udp-helper statistics`

【相关命令】

- `display udp-helper interface`

1.1.3 udp-helper broadcast-map

`udp-helper broadcast-map` 命令用来配置广播转组播中继转发。

`undo udp-helper broadcast-map` 命令用来取消广播转组播中继转发。

【命令】

`udp-helper broadcast-map` *multicast-address* [**acl** *acl-number*]

`undo udp-helper broadcast-map` *multicast-address*

【缺省情况】

未配置广播转组播中继转发。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

multicast-address: 组播地址。中继处理 UDP 广播报文时，将其目的 IP 地址从广播地址修改为指定的组播地址。

acl acl-number: ACL 的编号。通过指定 ACL 来实现对接口入方向的报文进行过滤，符合条件的才会按照配置的组播中继进行转发。支持基本 ACL（2000～2999）与高级 ACL（3000～3999）。如果未指定本参数，则不通过指定 ACL 来实现对接口入方向的报文进行过滤。

【使用指导】

请在接收广播报文的入接口上配置广播转组播中继转发。

一个接口上最多可以配置的广播中继个数为 20 个（包括广播转单播和广播转组播）。

【举例】

在 VLAN 接口 100 上配置广播转组播中继转发的组播地址为 225.0.0.1。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] udp-helper broadcast-map 225.0.0.1
```

1.1.4 udp-helper enable

udp-helper enable 命令用来开启 UDP Helper 功能。

undo udp-helper enable 命令用来关闭 UDP Helper 功能。

【命令】

```
udp-helper enable
undo udp-helper enable
```

【缺省情况】

UDP Helper 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

开启 UDP Helper 功能后，只有当全局配置了需要中继转发的 UDP 端口号，并且接口下配置了 UDP Helper 相关配置时，UDP Helper 功能才会生效。

【举例】

开启 UDP Helper 功能。

```
<Sysname> system-view
[Sysname] udp-helper enable
```

【相关命令】

- **udp-helper port**
- **udp-helper server**
- **udp-helper broadcast-map**

1.1.5 udp-helper port

udp-helper port 命令用来配置需要中继转发的报文的目的 UDP 端口。

undo udp-helper port 命令用来取消已配置的需要中继转发的报文的目的 UDP 端口。

【命令】

```
udp-helper port { port-number | dns | netbios-ds | netbios-ns | tacacs | tftp  
| time }  
undo udp-helper port { port-number | dns | netbios-ds | netbios-ns | tacacs  
| tftp | time }
```

【缺省情况】

未配置需要中继转发的报文的目的 UDP 端口。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

port-number: 需要中继转发的报文的目的 UDP 端口号，取值范围为 1~65535（不支持 67 和 68）。

dns: 对 DNS 报文进行中继转发，对应的 UDP 端口号为 53。

netbios-ds: 对 NetBIOS 数据服务报文进行中继转发，对应的 UDP 端口号为 138。

netbios-ns: 对 NetBIOS 名字服务报文进行中继转发，对应的 UDP 端口号为 137。

tacacs: 对终端访问控制器访问控制系统报文进行中继转发，对应的 UDP 端口号为 49。

tftp: 对简单文件传输协议报文进行中继转发，对应的 UDP 端口号为 69。

time: 对时间服务报文进行中继转发，对应的 UDP 端口号为 37。

【使用指导】

需要中继转发的报文的目的 UDP 端口有两种配置方法：指定端口号配置和指定参数配置。例如：

udp-helper port 53 和 **udp-helper port dns** 的效果是一样的。

设备上最多可以配置 256 个需要中继转发的报文的目的 UDP 端口。

【举例】

配置需要中继转发的报文的目的 UDP 端口号为 100。

```
<Sysname> system-view  
[Sysname] udp-helper port 100
```

1.1.6 udp-helper server

udp-helper server 命令用来配置广播转单播中继转发的目的服务器。

undo udp-helper server 命令用来删除已配置的广播转单播中继转发的目的服务器。

【命令】

```
udp-helper server ip-address
```

undo udp-helper server [*ip-address*]

【缺省情况】

未配置广播转单播中继转发的目的服务器。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ip-address: 目的服务器的 IP 地址，为点分十进制形式。

【使用指导】

请在接收广播报文的入接口上配置中继转发的目的服务器。一个接口上最多可以配置的广播中继个数为 20 个（包括广播转单播和广播转组播）。

配置 **undo udp-helper server** 命令时如果不指定 IP 地址，将会删除该接口下配置的所有广播转单播中继转发的目的服务器。

【举例】

在 VLAN 接口 100 上配置广播转单播中继转发的目的服务器地址为 192.1.1.2。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] udp-helper server 192.1.1.2
```

【相关命令】

- **display udp-helper interface**

目 录

1 IPv6 基础	1-1
1.1 IPv6 基础配置命令	1-1
1.1.1 display ipv6 fib	1-1
1.1.2 display ipv6 icmp statistics	1-2
1.1.3 display ipv6 interface	1-4
1.1.4 display ipv6 interface prefix	1-9
1.1.5 display ipv6 nd snooping	1-10
1.1.6 display ipv6 nd snooping count	1-12
1.1.7 display ipv6 neighbors	1-13
1.1.8 display ipv6 neighbors count	1-14
1.1.9 display ipv6 neighbors entry-limit	1-15
1.1.10 display ipv6 pathmtu	1-16
1.1.11 display ipv6 prefix	1-17
1.1.12 display ipv6 rawip	1-18
1.1.13 display ipv6 rawip verbose	1-19
1.1.14 display ipv6 statistics	1-23
1.1.15 display ipv6 tcp	1-27
1.1.16 display ipv6 tcp verbose	1-29
1.1.17 display ipv6 udp	1-34
1.1.18 display ipv6 udp verbose	1-35
1.1.19 ipv6 address	1-40
1.1.20 ipv6 address anycast	1-41
1.1.21 ipv6 address auto	1-42
1.1.22 ipv6 address auto link-local	1-42
1.1.23 ipv6 address eui-64	1-43
1.1.24 ipv6 address link-local	1-44
1.1.25 ipv6 address <i>prefix-number</i>	1-45
1.1.26 ipv6 hop-limit	1-46
1.1.27 ipv6 hoplimit-expires enable	1-47
1.1.28 ipv6 icmpv6 error-interval	1-47
1.1.29 ipv6 icmpv6 multicast-echo-reply enable	1-48
1.1.30 ipv6 icmpv6 source	1-49
1.1.31 ipv6 mtu	1-50

1.1.32 ipv6 nd autoconfig managed-address-flag	1-50
1.1.33 ipv6 nd autoconfig other-flag.....	1-51
1.1.34 ipv6 nd dad attempts	1-52
1.1.35 ipv6 nd ns retrans-timer.....	1-52
1.1.36 ipv6 nd nud reachable-time	1-53
1.1.37 ipv6 nd ra halt	1-54
1.1.38 ipv6 nd ra hop-limit unspecified	1-54
1.1.39 ipv6 nd ra interval.....	1-55
1.1.40 ipv6 nd ra no-advlinkmtu.....	1-56
1.1.41 ipv6 nd ra prefix.....	1-56
1.1.42 ipv6 nd ra prefix default	1-58
1.1.43 ipv6 nd ra router-lifetime	1-59
1.1.44 ipv6 nd router-preference.....	1-59
1.1.45 ipv6 nd snooping dad retrans-timer	1-60
1.1.46 ipv6 nd snooping enable global	1-61
1.1.47 ipv6 nd snooping enable link-local	1-61
1.1.48 ipv6 nd snooping glean source.....	1-62
1.1.49 ipv6 nd snooping lifetime	1-63
1.1.50 ipv6 nd snooping max-learning-num.....	1-63
1.1.51 ipv6 nd snooping uplink	1-64
1.1.52 ipv6 neighbor	1-65
1.1.53 ipv6 neighbor link-local minimize	1-66
1.1.54 ipv6 neighbor stale-aging.....	1-66
1.1.55 ipv6 neighbors max-learning-num	1-67
1.1.56 ipv6 pathmtu	1-68
1.1.57 ipv6 pathmtu age	1-69
1.1.58 ipv6 prefer temporary-address	1-69
1.1.59 ipv6 prefix	1-70
1.1.60 ipv6 reassemble local enable.....	1-71
1.1.61 ipv6 redirects enable.....	1-72
1.1.62 ipv6 temporary-address.....	1-72
1.1.63 ipv6 unreachable enable	1-73
1.1.64 local-proxy-nd enable.....	1-74
1.1.65 proxy-nd enable.....	1-75
1.1.66 reset ipv6 nd snooping	1-75
1.1.67 reset ipv6 neighbors	1-76

1.1.68 reset ipv6 pathmtu.....	1-77
1.1.69 reset ipv6 statistics.....	1-77

1 IPv6 基础

1.1 IPv6基础配置命令

1.1.1 display ipv6 fib

`display ipv6 fib` 命令用来显示 IPv6 FIB 信息。

【命令】

`display ipv6 fib [ipv6-address [prefix-length]]`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

ipv6-address: 显示目的地址为指定 IPv6 地址的 IPv6 FIB 信息。如果不指定目的地址，则显示所有的 IPv6 FIB 信息。
prefix-length: 目的地址的前缀长度，取值范围为 0~128。如果不指定前缀长度，则显示与指定目的 IPv6 地址最长匹配的 IPv6 FIB 信息

【举例】

```
# 显示公网所有的 IPv6 FIB 信息。
<Sysname> display ipv6 fib

Destination count: 1 FIB entry count: 1

Flag:
  U:Usable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay    F:FRR

Destination: ::1                               Prefix length: 128
Nexthop      : ::1                               Flags: UH
Time stamp   : 0x1                               Label: Null
Interface    : InLoop0                           Token: Invalid
```

表1-1 display ipv6 fib 命令显示信息描述表

字段	描述
Destination count	目的地址的个数
FIB entry count	IPv6 FIB表项数目

字段	描述
Destination	转发的目的地址
Prefix length	转发的目的地址的前缀长度
Nexthop	向目的地址转发报文的下一跳地址
Flags	路由的标志： <ul style="list-style-type: none"> • U：表示路由可用 • G：表示网关路由 • H：表示主机路由 • B：表示黑洞路由 • D：表示动态路由 • S：表示静态路由 • R：表示迭代路由 • F：表示快速重路由
Time stamp	IPv6 FIB表项的生成时间
Label	MPLS内层标签，公网的IPv6 FIB信息中显示为Null
Interface	转发报文的出接口
Token	LSP索引号

1.1.2 display ipv6 icmp statistics

display ipv6 icmp statistics 命令用来显示 ICMPv6 流量统计信息。

【命令】

display ipv6 icmp statistics [*slot slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot slot-number: 显示指定成员设备的 ICMPv6 流量统计信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 ICMPv6 流量统计信息。

【举例】

显示 ICMPv6 流量统计信息。

```
<Sysname> display ipv6 icmp statistics
```

```

Input: bad code          0          too short          0
      checksum error     0          bad length        0
      path MTU changed    0          destination unreachable 0
      too big            0          parameter problem    0
      echo request        0          echo reply           0
      neighbor solicit    0          neighbor advertisement 0
      router solicit      0          router advertisement  0
      redirect            0          router renumbering    0
output: parameter problem 0          echo request          0
      echo reply          0          unreachable no route  0
      unreachable admin   0          unreachable beyond scope 0
      unreachable address 0          unreachable no port    0
      too big            0          time exceed transit    0
      time exceed reassembly 0        redirect              0
      ratelimited         0          other errors           0

```

表1-2 display ipv6 icmp statistics 命令显示信息描述表

字段	描述
bad code	接收的代码错误的报文数
too short	接收的长度过小的报文数
checksum error	接收的校验和错误的报文数
bad length	接收的长度错误的报文数
path MTU changed	接收的路径MTU改变报文数
destination unreachable	接收的目标不可达报文数
too big	接收/发送的数据包超长报文数
parameter problem	接收/发送的参数错误报文数
echo request	接收/发送的回显请求报文数
echo reply	接收/发送的回应响应报文数
neighbor solicit	接收的邻居请求报文数
neighbor advertisement	接收的邻居通告报文数
router solicit	接收的路由请求报文数
router advertisement	接收的路由通告报文数
redirect	接收/发送的重定向报文数
router renumbering	接收的路由器重计数报文数

字段	描述
unreachable no route	发送的路由不可达报文数
unreachable admin	发送的与目标的通信被管理策略禁止的报文数
unreachable beyondscope	发送的源地址超出范围的报文数
unreachable address	发送的地址不可达报文数
unreachable no port	发送的端口不可达报文数
time exceed transit	发送的传输超时报文数
time exceed reassembly	发送的重组超时报文数
ratelimited	因速率超过限制而未发送的报文数
other errors	发送的其他的错误报文数

1.1.3 display ipv6 interface

display ipv6 interface 命令用来显示接口的 IPv6 信息。

【命令】

display ipv6 interface [*interface-type* [*interface-number*]] [**brief**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface-type: 显示指定类型接口的 IPv6 信息。

interface-number: 显示指定接口的 IPv6 信息。

brief: 显示接口摘要信息，包括接口的物理状态、链路层协议状态以及 IPv6 地址信息。如果不指定该参数，则显示接口的详细信息，包括接口上和 IPv6 相关的配置以及运行信息，以及 IPv6 报文统计信息

【使用指导】

如果不指定接口类型和接口编号，则显示所有接口的 IPv6 信息；

如果只指定接口类型，不指定接口编号，则显示所有指定类型接口的 IPv6 信息；

如果同时指定接口类型和接口编号，则显示指定接口的 IPv6 信息。

【举例】

查看 VLAN 接口 2 上的 IPv6 信息。

```

<Sysname> display ipv6 interface vlan-interface 2
Vlan-interface2 current state: UP
Line protocol current state: UP
IPv6 is enabled, link-local address is FE80::1234:56FF:FE65:4322 [TENTATIVE]
Global unicast address(es):
  10::1234:56FF:FE65:4322, subnet is 10::/64 [TENTATIVE] [AUTOCFG]
    [valid lifetime 4641s/preferred lifetime 4637s]
  20::1234:56ff:fe65:4322, subnet is 20::/64 [TENTATIVE] [EUI-64]
  30::1, subnet is 30::/64 [TENTATIVE] [ANYCAST]
  40::2, subnet is 40::/64 [TENTATIVE] [DHCP]
  50::3, subnet is 50::/64 [TENTATIVE]
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF00:1
  FF02::1:FF65:4322
MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND retransmit interval is 1000 milliseconds
Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
InReceives:                0
InTooShorts:                0
InTruncatedPkts:           0
InHopLimitExceeds:         0
InBadHeaders:               0
InBadOptions:               0
ReasmReqds:                 0
ReasmOKs:                   0
InFragDrops:                0
InFragTimeouts:             0
OutFragFails:               0
InUnknownProtos:           0
InDelivers:                 0
OutRequests:                0
OutForwDatagrams:           0
InNoRoutes:                 0
InTooBigErrors:             0
OutFragOKs:                  0
OutFragCreates:             0
InMcastPkts:                0
InMcastNotMembers:         0
OutMcastPkts:               0
InAddrErrors:               0
InDiscards:                  0
OutDiscards:                 0

```

表1-3 display ipv6 interface 命令显示信息描述表

字段	描述
Vlan-interface2 current state	<p>接口的物理状态，可能的状态及含义如下：</p> <ul style="list-style-type: none"> • Administratively DOWN: 表示该接口已经通过 shutdown 命令被关闭，即管理状态为关闭 • DOWN: 该接口的管理状态为开启，但物理状态为关闭（可能因为没有连接好或者线路故障） • UP: 该接口的管理状态和物理状态均为开启
Line protocol current state	<p>接口的链路层协议状态，可能的状态及含义如下：</p> <ul style="list-style-type: none"> • DOWN: 该接口的协议状态为关闭 • UP: 该接口的协议状态为开启
IPv6 is enabled	接口的IPv6转发功能状态（为某接口配置任一IPv6地址后系统将自动使能该接口的IPv6功能，此例中处于使能状态）
link-local address	接口上配置的链路本地地址
Global unicast address(es)	<p>接口上配置的全球单播地址</p> <p>可能的IPv6地址状态及含义如下：</p> <ul style="list-style-type: none"> • TENTATIVE: 该状态为地址初始化状态，此时该地址可能正在进行 DAD 检测或准备进行 DAD 检测，处于该状态的地址不能作为报文的源地址或者目的地址 • DUPLICATE: 该状态表明地址 DAD 检测已经结束，由于该地址在链路上不唯一，因此不能使用 • PREFERRED: 该状态表明地址处于首选生命期以内。该状态的地址可以作为报文的源地址或者目的地址。为该状态时，不显示地址的状态标识 • DEPRECATED: 该状态表明地址超过首选生命期，但是在有效生命期以内。该状态地址有效，但不应作为新建连接报文的源地址，目的地址是该地址的报文还可以被正常处理 <p>如果地址来源不为手工配置的全球单播地址，则会标记地址来源。可能的地址来源及含义如下：</p> <ul style="list-style-type: none"> • AUTOCFG: 表示无状态自动配置的全球单播地址 • DHCP: 表示 DHCPv6 服务器分配的全球单播地址 • EUI-64: 表示手工配置的 EUI-64 格式全球单播地址 • RANDOM: 表示自动生成的临时地址 <p>如果地址为手工配置的任播地址，则会标记ANYCAST</p>
valid lifetime	接口上无状态自动配置的全球单播地址的有效生命期

字段	描述
preferred lifetime	接口上无状态自动配置的全球单播地址的首选生命期
Joined group address(es)	接口加入的组播组地址
MTU	接口的最大传输单元
ND DAD is enabled, number of DAD attempts	<p>重复地址检测功能是否使能（该例中使能）</p> <p>若处于使能状态则同时显示重复地址检测时发送邻居请求消息的次数（可通过ipv6 nd dad attempts命令进行配置）</p> <p>若处于关闭状态则显示“ND DAD is disabled”（可通过配置重复地址检测时发送邻居请求消息的次数为0关闭该功能）</p>
ND reachable time	保持邻居可达的时间
ND retransmit interval	邻居请求消息重传时间间隔
Hosts use stateless autoconfig for addresses	主机采用无状态自动配置的方式获取IPv6地址
InReceives	接口接收到的所有IPv6报文，包括各种错误的报文
InTooShorts	接口接收到的太短的IPv6报文，譬如报文长度不足40字节
InTruncatedPkts	接口接收到的IPv6报文，其实际长度小于报文内容中所指出的报文长度
InHopLimitExceeds	接口接收到的IPv6报文，其跳数超出限制
InBadHeaders	接口接收到的IPv6报文，其基本报文头错误
InBadOptions	接口接收到的IPv6报文，其扩展报文头错误
ReasmReqds	接口接收到的IPv6分片报文
ReasmOKs	接口接收到的IPv6分片，被组装好的报文，这里指的不是分片个数，是组装好的报文数
InFragDrops	接口接收到的IPv6分片报文，该分片报文由于错误被丢弃
InFragTimeouts	接口接收到的IPv6分片报文，该分片停留在系统缓冲中时间超过指定时间，被丢弃
OutFragFails	出接口上分片失败的报文
InUnknownProtos	接口接收到的IPv6报文，其协议类型不能被识别或不能被支持
InDelivers	接口接收到的IPv6报文，该报文被上送到IPv6的用户协议处（如ICMPv6、TCP、UDP等）

字段	描述
OutRequests	IPv6本地出报文，即各IPv6的用户协议层要求IPv6发送出去的报文
OutForwDatagrams	出接口上被转发的报文
InNoRoutes	接口接收到的IPv6报文，找不到匹配的路由被丢弃
InTooBigErrors	接口接收到的IPv6报文，转发时，由于超过链路MTU被丢弃
OutFragOKs	出接口上分片成功的报文
OutFragCreates	出接口上成功分片后的分片报文，指分片数
InMcastPkts	接口接收到的IPv6组播报文
InMcastNotMembers	接口接收到的IPv6组播报文，但该接口却没有加入对应组播组，报文被丢弃
OutMcastPkts	接口发送的IPv6组播报文
InAddrErrors	接口接收到的IPv6报文，其目的地址不合法，报文被丢弃
InDiscards	接口接收到的IPv6报文，由于资源问题被丢弃的报文，而不是由于报文内容等被丢弃的报文
OutDiscards	接口需要发送的报文，由于资源问题被丢弃的报文，而不是由于报文内容等被丢弃的报文

查看所有接口的 IPv6 摘要信息。

```
<Sysname> display ipv6 interface brief
*down: administratively down
(s): spoofing
Interface          Physical Protocol IPv6 Address
Vlan-interface1    down      down    Unassigned
Vlan-interface2    up        up      2001::1
Vlan-interface100  up        up      Unassigned
```

表1-4 display ipv6 interface brief 命令显示信息描述表

字段	描述
*down: administratively down	接口处于管理down状态，即采用shutdown命令关闭了该接口
(s): spoofing	接口的欺骗属性，即接口的链路协议状态显示是up的，但实际可能没有对应的链路，或者所对应的链路不是永久存在而是按需建立的
Interface	接口的名称

字段	描述
Physical	<p>接口的物理状态，可能的状态及含义如下：</p> <ul style="list-style-type: none"> • *down: 表示该接口已经通过 shutdown 命令被关闭，即管理状态为关闭 • down: 该接口的管理状态为开启，但物理状态为关闭（可能因为没有连接好或者线路故障） • up: 该接口的管理状态和物理状态均为开启
Protocol	<p>接口的链路层协议状态，可能的状态及含义如下：</p> <ul style="list-style-type: none"> • down: 该接口的协议状态为关闭 • up: 该接口的协议状态为开启
IPv6 Address	<p>接口的IPv6地址，接口上有全球单播地址时，显示地址最小的全球单播地址，没有全球单播地址则显示链路本地地址，没有链路本地地址则显示“Unassigned”</p>

1.1.4 display ipv6 interface prefix

display ipv6 interface prefix 命令用来显示接口的 IPv6 前缀信息。

【命令】

display ipv6 interface *interface-type* *interface-number* **prefix**

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface-type interface-number: 指定接口类型和接口编号。

【举例】

查看 VLAN 接口 10 的 IPv6 前缀信息。

```
<Sysname> display ipv6 interface Vlan-interface 10 prefix
Prefix: 1001::/65                                Origin: ADDRESS
Age:      -                                       Flag:    AL
Lifetime(Valid/Preferred): 2592000/604800

Prefix: 2001::/64                                Origin: STATIC
Age:      -                                       Flag:    L
Lifetime(Valid/Preferred): 3000/2000
```



```

Prefix: 3001::/64                                Origin: RA
Age:      600                                    Flag:   A
Lifetime(Valid/Preferred): -

```

表1-5 display ipv6 interface prefix 命令显示信息描述表

字段	描述
Prefix	IPv6地址前缀
Origin	<p>前缀来源，包括：</p> <ul style="list-style-type: none"> • STATIC: 手工配置前缀（命令 ipv6 nd ra prefix） • RA: 使能无状态地址自动配置功能后根据 RA 报文生成的前缀 • ADDRESS: 由手工配置的地址产生的前缀
Age	老化时间（单位为秒），“-”表示前缀不会老化
Flag	<p>前缀随RA报文公告时携带的标记，“-”表示没有标记</p> <ul style="list-style-type: none"> • L: 表示前缀是直接可达的。没有此标记，则表示前缀不是该链路上直连可达的 • A: 表示前缀用于无状态自动配置。没有此标记，则表示前缀不用于无状态自动配置 • N: 表示前缀不在 RA 消息中发布。没有此标记，则表示指定前缀在 RA 消息中发布
Lifetime	<p>前缀随RA报文公告时携带的生存时间（单位为秒），“-”表示前缀不需要公告</p> <ul style="list-style-type: none"> • Valid: 前缀的有效生命期 • Preferred: 前缀的首选生命期

【相关命令】

- **ipv6 nd ra prefix**

1.1.5 display ipv6 nd snooping

display ipv6 nd snooping 命令用来显示 ND Snooping 表项信息。

【命令】

```

display ipv6 nd snooping [ [ vlan vlan-id | interface interface-type
interface-number ] [ global | link-local ] | ipv6-address ] [ verbose ]

```

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator

```

【参数】

vlan *vlan-id*: 显示指定 VLAN 内的 ND Snooping 表项。*vlan-id* 表示 VLAN ID，取值范围为 1~4094。

interface *interface-type interface-number*: 显示指定接口的 ND Snooping 表项。*interface-type interface-number* 表示接口类型和接口编号

ipv6-address : 显示指定 IPv6 地址的 ND Snooping 表项。

global: 显示表项地址类型为全局单播地址的 ND Snooping 表项。

link-local: 显示表项地址类型为链路本地地址的 ND Snooping 表项。

verbose: 显示 ND Snooping 表项的详细信息。不指定该参数时显示 ND Snooping 表项的摘要信息。

【举例】

显示 VLAN 1 的 ND Snooping 表项信息。

```
<Sysname> display ipv6 nd snooping vlan 1
```

IPv6 address	MAC address	VID	Interface	Status	Age
1::2	0000-1234-0c01	1	GE1/0/2	VALID	57

显示 VLAN 1 的 ND Snooping 表项信息的详细信息。

```
<Sysname> display ipv6 nd snooping vlan 1 verbose
```

IPv6 address: 1::2
MAC address: 0000-1234-0c01
Interface: GE1/0/2
First VLAN ID: 1 Second VLAN ID: N/A
Status: VALID Age: 57

表1-6 display ipv6 nd snooping 命令显示信息描述表

字段	描述
IPv6 address	ND Snooping表项的IPv6地址
MAC address	ND Snooping表项的MAC地址
VID	ND Snooping表项所属VLAN的编号
First VLAN ID	ND Snooping表项所属外层VLAN的编号
Second VLAN ID	ND Snooping表项所属内层VLAN的编号，当不存在内层VLAN信息时，则显示N/A。 外层VLAN和内层VLAN的描述，请参见“二层技术-以太网交换配置指导”中的“QinQ”
Interface	ND Snooping表项所对应的入端口

字段	描述
Status	ND Snooping表项的显示的状态，选项如下： <ul style="list-style-type: none"> • TENTATIVE：临时非生效状态； • VALID：生效状态； • TESTING_TPLT：从信任端口收到对应源地址的报文，或者表项到达老化，触发向该表项所在端口进行探测； • TESTING_VP：从其他非信任端口收到对应源地址的报文，触发向该表项所在接口进行探测；
Age	ND Snooping表项的VALID状态的超时时间，即表项的老化时间（单位为秒），其他状态的超时时间显示“#”

1.1.6 display ipv6 nd snooping count

display ipv6 nd snooping count 命令用来显示 ND Snooping 表项个数。

【命令】

display ipv6 nd snooping count [**interface** *interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface interface-type interface-number：显示指定接口的 ND Snooping 表项个数。
interface-type interface-number 表示接口类型和接口编号。

【举例】

显示设备上的 ND Snooping 表项个数。

```
<Sysname> display ipv6 nd snooping count
Total number of entries: 5
```

显示接口 GigabitEthernet1/0/1 的 ND Snooping 表项个数。

```
<Sysname> display ipv6 nd snooping count interface gigabitethernet 1/0/1
Total number of entries on interface: 2
```

表1-7 display ipv6 nd snooping count 命令显示信息描述表

字段	描述
Total number of entries	设备的ND Snooping表项个数

字段	描述
Total number of entries on interface: <i>number</i>	接口下的ND Snooping表项个数

1.1.7 display ipv6 neighbors

display ipv6 neighbors 命令用来显示邻居信息。

【命令】

```
display ipv6 neighbors { { ipv6-address | all | dynamic | static } [ slot
slot-number ] | interface interface-type interface-number | vlan vlan-id }
[ verbose ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

ipv6-address: 显示指定 IPv6 地址的邻居信息。

all: 显示所有邻居的信息，包括公网和所有私网下动态获取的和静态配置的邻居信息。

dynamic: 显示所有动态获取的邻居信息。

static: 显示所有静态配置的邻居信息。

slot slot-number: 显示指定成员设备的邻居信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的邻居信息。

interface interface-type interface-number: 显示指定接口的邻居信息。*interface-type interface-number* 为接口类型和接口编号。

vlan vlan-id: 显示指定 VLAN 的邻居信息。*vlan-id* 表示 VLAN ID，取值范围为 1~4094。

verbose: 显示邻居的详细信息。

【举例】

查看所有的邻居信息。

```
<Sysname> display ipv6 neighbors all
Type: S-Static    D-Dynamic    O-Openflow    R-Rule    I-Invalid
IPv6 address      Link layer    VID          Interface/Link ID  State T  Age
1::2              6864-6839-0202 1          GE1/0/1          STALE D  136
FE80::6A64:68FF:FE39:202 6864-6839-0202 1          GE1/0/1          STALE D  126
```

查看所有邻居的详细信息。

```
<Sysname> display ipv6 neighbors all verbose
Type: S-Static    D-Dynamic    O-Openflow    R-Rule    I-Invalid
IPv6 Address: 1::2
```

```

Link Layer : 6864-6839-0202      VID : 1      Interface: GE1/0/1
State      : STALE                Type: D      Age      : 290
Vpn-instance: [No Vrf]
Nickname   : 0x0
IPv6 Address: FE80::6A64:68FF:FE39:202
Link Layer : 6864-6839-0202      VID : 1      Interface: GE1/0/1
State      : STALE                Type: D      Age      : 280
Vpn-instance: [No Vrf]
Nickname   : 0x0

```

表1-8 display ipv6 neighbors 命令显示信息描述表

字段	描述
IPv6 Address	邻居的IPv6地址
Link Layer	邻居的链路层地址（MAC地址）
VID	与邻居相连的接口所属的VLAN，N/A表示VLAN索引无效
Interface/Link ID	与邻居相连的接口。N/A表示无法获取接口名
State	邻居的状态，包括： <ul style="list-style-type: none"> • INCMP: 正在解析地址，邻居的链路层地址尚未确定 • REACH: 邻居可达 • STALE: 未确定邻居是否可达，设备不会再验证邻居的可达性，除非有数据发送给该邻居 • DELAY: 未确定邻居是否可达，延迟一段时间发送邻居请求报文 • PROBE: 未确定邻居是否可达，发送邻居请求报文来验证邻居的可达性
Type	邻居信息的类型，S表示静态配置，D表示动态获取，O表示从OpenFlow特性获取，R表示从Portal等特性获取，I表示无效
Age	静态项显示“-”，动态项显示上次可达以来经过的时间（单位为秒），如果始终不可达则显示“#”（只适用于动态项）
Vpn-instance	（暂不支持）VPN实例名称，[No Vrf]表示没有配置相应表项的VPN实例
Nickname	邻居表项的Nickname（长度为4的十六进制数字，例如0x012a）

【相关命令】

- **ipv6 neighbor**
- **reset ipv6 neighbors**

1.1.8 display ipv6 neighbors count

display ipv6 neighbors count 命令用来显示邻居表项的个数。

【命令】

```
display ipv6 neighbors { { all | dynamic | static } [ slot slot-number ] |  
interface interface-type interface-number | vlan vlan-id } count
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

all: 显示所有邻居表项的总个数，包括动态获取的和静态配置的邻居信息。

dynamic: 显示所有动态获取的邻居表项的总个数。

static: 显示所有静态配置的邻居表项的总个数。

slot slot-number: 显示指定成员设备的邻居表项的总个数。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的邻居表项的总个数。

interface interface-type interface-number: 显示指定接口的邻居表项的总个数。*interface-type interface-number* 为接口类型和接口编号。

vlan vlan-id: 显示指定 VLAN 的邻居表项的总个数。*vlan-id* 表示 VLAN ID，取值范围为 1～4094。

【举例】

显示动态获取的邻居表项的总个数。

```
<Sysname> display ipv6 neighbors dynamic count  
Total number of dynamic entries: 2
```

1.1.9 display ipv6 neighbors entry-limit

display ipv6 neighbors entry-limit 命令用来显示设备支持 ND 表项的最大数目。

【命令】

```
display ipv6 neighbors entry-limit
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

显示 ND 表项最大数目。

```
<Sysname> display ipv6 neighbors entry-limit  
ND entries: 128
```

1.1.10 display ipv6 pathmtu

display ipv6 pathmtu 命令用来显示 IPv6 的 PMTU 信息。

【命令】

display ipv6 pathmtu { *ipv6-address* | { **all** | **dynamic** | **static** } [**count**] }

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

ipv6-address: 显示到达指定 IPv6 地址的 PMTU 信息。

all: 显示所有公网的 PMTU 信息。

dynamic: 显示所有动态 PMTU 信息。

static: 显示所有静态 PMTU 信息。

count: 显示 PMTU 表项数目。

【举例】

显示所有 PMTU 信息。

```
<Sysname> display ipv6 pathmtu all
IPv6 destination address      PathMTU    Age      Type
1:2::3:2                     1800       -        Static
1:2::4:2                     1400       10       Dynamic
1:2::5:2                     1280       10       Dynamic
```

显示所有 PMTU 表项数目。

```
<Sysname> display ipv6 pathmtu all count
Total number of entries: 3
```

表1-9 display ipv6 pathmtu 命令显示信息描述表

字段	描述
IPv6 destination address	IPv6目的地址
PathMTU	对应IPv6地址的PMTU值
Age	PMTU老化时间（单位为分钟），如果是静态表项则显示为“-”
Type	PMTU类型，Dynamic表示动态协商的PMTU，Static表示静态配置的PMTU
Total number of entries	PMTU表项数目

【相关命令】

- **ipv6 pathmtu**

- `reset ipv6 pathmtu`

1.1.11 display ipv6 prefix

`display ipv6 prefix` 命令用来显示 IPv6 前缀信息，包括静态和动态前缀。

【命令】

`display ipv6 prefix [prefix-number]`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

prefix-number: 显示指定的 IPv6 前缀信息。*prefix-number* 表示 IPv6 前缀编号，取值范围为 1~1024。如果不指定本参数，则显示所有 IPv6 前缀的信息。

【使用指导】

静态 IPv6 前缀指的是通过 `ipv6 prefix` 命令创建的前缀。
动态 IPv6 前缀指的是设备作为 DHCPv6 客户端获取到前缀后，自动创建的指定编号的 IPv6 前缀。
详细介绍请参见“三层技术-IP 业务配置指导/DHCPv6 客户端”。

【举例】

```
# 显示所有 IPv6 前缀的信息。
<Sysname> display ipv6 prefix
Number Prefix                                     Type
1       1::/16                                     Static
2       11:77::/32                                 Dynamic

# 显示 IPv6 前缀编号 1 的信息。
<Sysname> display ipv6 prefix 1
Number: 1
Type   : Dynamic
Prefix: ABCD:77D8::/32
Preferred lifetime 90 sec, valid lifetime 120 sec
```

表1-10 display ipv6 prefix 命令显示信息描述表

字段	描述
Number	前缀编号
Type	前缀的类型，取值包括： <ul style="list-style-type: none">• Static: 表示静态 IPv6 前缀• Dynamic: 表示动态 IPv6 前缀
Prefix	前缀及其长度。“Not-available”表示目前尚未获取到前缀

字段	描述
Preferred lifetime 90 sec	首选生命期，单位为秒。如果是静态IPv6前缀，则不显示
valid lifetime 120 sec	有效生命期，单位为秒。如果是静态IPv6前缀，则不显示

【相关命令】

- `ipv6 prefix`

1.1.12 display ipv6 rawip

`display ipv6 rawip` 命令用来显示 IPv6 RawIP 连接摘要信息。

【命令】

`display ipv6 rawip [slot slot-number]`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot slot-number: 显示指定成员设备的 IPv6 RawIP 连接摘要信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 IPv6 RawIP 连接摘要信息。

【举例】

显示 IPv6 RawIP 连接摘要信息。

```
<Sysname> display ipv6 rawip
Local Addr      Foreign Addr    Protocol Slot  PCB
2001:2002:2003:2 3001:3002:3003:3 58      1    0x0000000000000009
004:2005:2006:20 004:3005:3006:30
07:2008         07:3008
2002::100       2002::138      58      2    0x0000000000000008
::              ::              58      5    0x0000000000000002
```

表1-11 display ipv6 rawip 命令显示信息描述表

字段	描述
Local Addr	本端IPv6地址
Foreign Addr	对端IPv6地址
Protocol	使用IPv6 RawIP socket的协议号
PCB	协议控制块索引

1.1.13 display ipv6 rawip verbose

display ipv6 rawip verbose 命令用来显示 IPv6 RawIP 连接详细信息。

【命令】

display ipv6 rawip verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

pcb *pcb-index*: 显示指定协议控制块索引的 IPv6 RawIP 连接详细信息。*pcb-index* 表示协议控制块索引，取值范围为 1~16。

slot *slot-number*: 显示指定成员设备的 IPv6 RawIP 连接详细信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 IPv6 RawIP 连接详细信息。

【举例】

```
# 显示 Ipv6 RawIP 连接详细信息。
<Sysname> display ipv6 rawip verbose
Total RawIP socket number: 1

Location: slot: 6
Creator: ping ipv6[320]
State: N/A
Options: N/A
Error: 0
Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 9216 / 1 / 0 / N/A
Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
Type: 3
Protocol: 58
Connection info: src = ::, dst = ::
Inpcb flags: N/A
Inpcb extflag: INP_EXTRCVICMPERR INP_EXTFILTER
Inpcb vflag: INP_IPV6
Hop limit: 255 (minimum hop limit: 0)
Send VRF: 0xffff
Receive VRF: 0xffff
```

表1-12 display ipv6 rawip verbose 命令显示信息描述表

字段	描述
Total RawIP socket number	IPv6 RawIP socket总数
Creator	创建socket的任务名称，括号中为创建者的进程号

字段	描述
State	<p>socket的状态，可能的状态如下：</p> <ul style="list-style-type: none"> • NOFDREF：用户已经关闭 • ISCONNECTED：连接已经建立 • ISCONNECTING：正在建立连接 • ISDISCONNECTING：正在断开连接 • ASYNC：异步方式 • ISDISCONNECTED：连接已经断开 • PROTOREF：协议强关联 • N/A：不处于上述状态
Options	<p>socket的选项，有以下几种：</p> <ul style="list-style-type: none"> • SO_DEBUG：记录套接字的调试信息 • SO_ACCEPTCONN：server 端监听连接请求 • SO_REUSEADDR：允许本地地址重复使用 • SO_KEEPALIVE：协议需要查询空闲的连接 • SO_DONTROUTE：设置不查路由表，由于目的地址是直连网络的情况 • SO_BROADCAST：套接字支持广播报文 • SO_LINGER：套接字关闭但仍发送剩余数据 • SO_OOBINLINE：带外数据采用内联方式存储 • SO_REUSEPORT：允许本地端口重复使用 • SO_TIMESTAMP：记录入报文时间戳，只对非连接的协议有效，时间精确到毫秒 • SO_NOSIGPIPE：socket 不能发送数据导致返回失败时不创建 SIGPIPE • SO_TIMESTAMPNS：和时戳选项功能类似，时间可以精确到纳秒 • SO_KEEPALIVETIME：设置空闲探测时间，TCP 支持此选项 • SO_FILTER：设置报文过滤条件，OSI Socket 和 RawIP 支持此选项 • N/A：没有设置选项
Error	影响socket连接的错误码

字段	描述
Receiving buffer (cc/hiwat/lowat/drop/state)	<p>接收缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间、丢包数和状态</p> <p>状态的取值有：</p> <ul style="list-style-type: none"> • CANTSENDMORE：不能发送数据到对端 • CANTRCVMORE：不能从对端接收数据 • RCVATMARK：接收标记 • N/A：不处于上述状态
Sending buffer (cc/hiwat/lowat/state)	<p>发送缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间和状态</p> <p>状态的取值有：</p> <ul style="list-style-type: none"> • CANTSENDMORE：不能发送数据到对端 • CANTRCVMORE：不能从对端接收数据 • RCVATMARK：接收标记 • N/A：不处于上述状态
Type	<p>使用的socket类型，类型的取值有：</p> <ul style="list-style-type: none"> • 1: SOCK_STREAM，流模式，提供可靠的字节流。TCP 协议使用此类型 • 2: SOCK_DGRAM，数据报模式的通信。UDP 协议使用此类型 • 3: SOCK_RAW，RAW 模式的通信方式 • N/A：不是上述类型
Protocol	使用IPv6 RawIP socket的协议号，58表示ICMP协议
Connection info	连接信息，分别为源IPv6地址、目的IPv6地址

字段	描述
Inpcb flags	<p>Internet协议控制块中的标记，标记的取值有：</p> <ul style="list-style-type: none"> • INP_RECVOPTS: 接收传入的 IPv6 选项 • INP_RECVRETOPTS: 接收回应的 IPv6 选项 • INP_RECVDSTADDR: 接收目的 IPv6 地址 • INP_HDRINCL: 用户提供整个 IPv6 头 • INP_REUSEADDR: 重复使用地址 • INP_REUSEPORT: 重复使用端口号 • INP_ANONPORT: 用户未指定端口 • INP_PROTOCOL_PACKET: 标识报文为协议报文 • INP_RCVVLANID: 接收报文的 VLAN ID，仅 UDP 和 RawIP 支持 • IN6P_IPV6_V6ONLY: 仅支持 IPv6 协议栈 • IN6P_PKTINFO: 接收报文的源地址和入接口 • IN6P_HOPLIMIT: 接收报文 hoplimit • IN6P_HOPOPTS: 接收报文的逐跳扩展头信息 • IN6P_DSTOPTS: 接收报文的目的扩展头信息 • IN6P_RTHDR: 接收报文的路由扩展头信息 • IN6P_RTHDRDSTOPTS: 接收报文的路由头前的目的扩展头信息 • IN6P_TCLASS: 接收报文的优先级信息 • IN6P_AUTOFLOWLABEL: 使用随机流标签 • IN6P_RFC2292: 使用 RFC2292 API • IN6P_MTU: 感知路径 MTU 的变化，TCP 不支持 • INP_RCVMACADDR: 接收报文的 MAC • INP_USEICMPSRC: 使用配置的 ICMPv6 地址作为源地址 • INP_SYNCPCB: 阻塞等待 inpcb 同步 • N/A: 不是上述标记
Inpcb extflag	<p>Internet协议控制块中的扩展标记，标记的取值有：</p> <ul style="list-style-type: none"> • INP_EXTRCVPVCIDX: 接收报文时记录报文的 PVC 索引 • INP_RCVPWID: 接收报文时记录报文的 PW ID • INP_EXTRCVICMPERR: 接收 ICMP 差错报文 • INP_EXTFILTER: 接收报文时对报文内容进行过滤 • N/A: 不是上述标记

字段	描述
Inpcb vflag	<p>Internet协议控制块中的IP版本标记，标记的取值有：</p> <ul style="list-style-type: none"> • INP_IPV4: 运用与 IPv4 通信 • INP_IPV6: 运用与 IPv6 通信 • INP_IPV6PROTO: 运用 IPv6 协议创建的 inpcb • INP_TIMEWAIT: 处于等待状态 • INP_ONESBCAST: 发送广播报文 • INP_DROPPED: 协议丢弃标志 • INP_SOCKREF: socket 强关联 • INP_DONTBLOCK: inpcb 同步时不能被阻塞 • N/A: 不是上述标记
Hop limit(minimum hop limit)	Internet协议控制块中的跳数限制，括号中为最小跳数限制
Send VRF	发送实例
Receive VRF	接收实例

1.1.14 display ipv6 statistics

display ipv6 statistics 命令用来显示 IPv6 报文及 ICMPv6 报文的统计信息。

【命令】

display ipv6 statistics [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot *slot-number*: 显示指定成员设备的 IPv6 报文及 ICMPv6 报文统计信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 IPv6 报文及 ICMPv6 报文统计信息。

【举例】

查看 IPv6 报文及 ICMPv6 报文的统计信息。

```
<Sysname> display ipv6 statistics
IPv6 statistics:
```

```
Sent packets:
```

```

Total:      0
  Sent locally:      0          Forwarded:      0
  Raw packets:      0          Discarded:      0
  Fragments:        0          Fragments failed: 0
  Routing failed:    0

Received packets:
Total:      0
  Received locally:  0          Hop limit exceeded: 0
  Fragments:        0          Reassembled:      0
  Reassembly failures: 0        Reassembly timeout: 0
  Format errors:     0          Option errors:   0
  Protocol errors:   0

ICMPv6 statistics:

Sent packets:
Total:      0
  Unreachable:      0          Too big:      0
  Hop limit exceeded: 0        Reassembly timeouts: 0
  Parameter problems: 0
  Echo requests:    0          Echo replies:  0
  Neighbor solicits: 0          Neighbor adverts: 0
  Router solicits:  0          Router adverts: 0
  Redirects:        0          Router renumbering: 0
Send failed:
  Rate limitation:   0          Other errors:   0

Received packets:
Total:      0
  Checksum errors:   0          Too short:     0
  Bad codes:         0
  Unreachable:      0          Too big:      0
  Hop limit exceeded: 0        Reassembly timeouts: 0
  Parameter problems: 0        Unknown error types: 0
  Echo requests:    0          Echo replies:  0
  Neighbor solicits: 0          Neighbor adverts: 0
  Router solicits:  0          Router adverts: 0
  Redirects:        0          Router renumbering: 0
  Unknown info types: 0
Deliver failed:
  Bad length:        0

```

表1-13 display ipv6 statistics 命令显示信息描述表

字段	描述
IPv6 statistics:	IPv6报文统计信息

字段	描述
<p>Sent packets:</p> <p>Total:</p> <p>Sent locally:</p> <p>Forwarded:</p> <p>Raw packets:</p> <p>Discarded:</p> <p>Fragments:</p> <p>Fragments failed:</p> <p>Routing failed:</p>	<p>发送IPv6报文的统计信息，包括：</p> <ul style="list-style-type: none"> • 本地发送报文和转发报文的总数 • 本地发送报文数 • 转发报文数 • 使用 raw socket 发送的报文数 • 丢弃报文数 • 发送分片报文数 • 分片报文发送失败的个数 • 路由失败报文数
<p>Received packets:</p> <p>Total:</p> <p>Received locally:</p> <p>Hop limit exceeded:</p> <p>Fragments:</p> <p>Reassembled:</p> <p>Reassembly failures:</p> <p>Reassembly timeout:</p> <p>Format errors:</p> <p>Option errors:</p> <p>Protocol errors:</p>	<p>接收IPv6报文的统计信息，包括：</p> <ul style="list-style-type: none"> • 接收报文总数 • 本地接收报文数，即目的地是本机的报文数 • 超出跳数范围的报文数 • 接收的分片报文数 • 重组报文数 • 重组失败的报文数 • 重组超时的报文数 • 格式错误的报文数 • 选项错误的报文数 • 协议错误的报文数
ICMPv6 statistics:	ICMPv6报文的统计信息

字段	描述
Sent packets:	发送ICMPv6报文的统计信息，包括：
Total:	<ul style="list-style-type: none"> • 发送报文总数
Unreachable:	<ul style="list-style-type: none"> • 目的不可达报文数
Too big:	<ul style="list-style-type: none"> • 报文太长的报文数
Hop limit exceeded:	<ul style="list-style-type: none"> • 超出跳数限制的报文数
Reassembly timeouts:	<ul style="list-style-type: none"> • 分片重组超时报文数
Parameter problems:	<ul style="list-style-type: none"> • 参数错误报文数
Echo requests:	<ul style="list-style-type: none"> • 回应请求报文数
Echo replies:	<ul style="list-style-type: none"> • 回应响应报文数
Neighbor solicits:	<ul style="list-style-type: none"> • 邻居请求报文数
Neighbor adverts:	<ul style="list-style-type: none"> • 邻居通告报文数
Router solicits:	<ul style="list-style-type: none"> • 路由器请求报文数
Router adverts:	<ul style="list-style-type: none"> • 路由器通告报文数
Redirects:	<ul style="list-style-type: none"> • 重定向报文数
Router renumbering	<ul style="list-style-type: none"> • 路由器重编号报文数
Sent failed:	<ul style="list-style-type: none"> • 本机发送失败的报文数
Rate limitation:	<ul style="list-style-type: none"> • 因速率超过限制而未发送的报文数
Other errors:	<ul style="list-style-type: none"> • 其他错误的报文数

字段	描述
Received packets:	接收ICMPv6报文的统计信息，包括：
Total:	<ul style="list-style-type: none"> 接收报文总数
Checksum errors:	<ul style="list-style-type: none"> 校验和错误的报文数
Too short:	<ul style="list-style-type: none"> 报文太短的报文数
Bad codes:	<ul style="list-style-type: none"> 错误代码的报文数
Unreachable:	<ul style="list-style-type: none"> 不可达报文数
Too big:	<ul style="list-style-type: none"> 报文太长的报文数
Hop limit exceeded:	<ul style="list-style-type: none"> 超出跳数限制的报文数
Reassembly timeouts:	<ul style="list-style-type: none"> 分片重组超时的报文数
Parameter problems:	<ul style="list-style-type: none"> 参数错误报文数
Unknown error types:	<ul style="list-style-type: none"> 未知错误报文数
Echo requests:	<ul style="list-style-type: none"> 回应请求报文数
Echo replies:	<ul style="list-style-type: none"> 回应响应报文数
Neighbor solicits:	<ul style="list-style-type: none"> 邻居请求报文数
Neighbor adverts:	<ul style="list-style-type: none"> 邻居通告报文数
Router solicits:	<ul style="list-style-type: none"> 路由器请求报文数
Router adverts:	<ul style="list-style-type: none"> 路由器通告报文数
Redirects:	<ul style="list-style-type: none"> 重定向报文数
Router renumbering:	<ul style="list-style-type: none"> 路由器重编号报文数
Unknown info types:	<ul style="list-style-type: none"> 未知信息报文数
Deliver failed:	<ul style="list-style-type: none"> 上送本机失败的报文数
Bad length:	<ul style="list-style-type: none"> 长度错误的报文数

【相关命令】

- `reset ipv6 statistics`

1.1.15 display ipv6 tcp

`display ipv6 tcp` 命令用来显示 IPv6 TCP 连接摘要信息。

【命令】

`display ipv6 tcp [slot slot-number]`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot slot-number: 显示指定成员设备的 IPv6 TCP 连接摘要信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 IPv6 TCP 连接摘要信息。

【举例】

```
# 显示 IPv6 TCP 连接摘要信息。
<Sysname> display ipv6 tcp
*: TCP connection with authentication
LAddr->port      FAddr->port      State      Slot   PCB
*2001:2002:2003:2 3001:3002:3003:3 ESTABLISHED 1      0x000000000000c387
004:2005:2006:20 004:3005:3006:30
07:2008->1200    07:3008->1200
2001::1->23      2001::5->1284    ESTABLISHED 2      0x0000000000000008
2003::1->25      2001::2->1283    LISTEN      3      0x0000000000000009
```

表1-14 display ipv6 tcp 命令显示信息描述表

字段	描述
*	如果某个连接前有此标识，则表示该TCP连接是采用加密算法认证的连接
LAddr->port	本端IPv6地址及端口号
FAddr->port	对端IPv6地址及端口号
State	TCP连接状态，可能的状态如下： <ul style="list-style-type: none">• CLOSED：服务器收到客户端的关闭连接请求回应后所处的状态• LISTEN：服务器在等待连接请求时所处的状态• SYN_SENT：客户端发出连接请求等待服务器回应时所处的状态• SYN_RCVD：服务器收到客户端连接请求时所处的状态• ESTABLISHED：服务器和客户端双方建立连接并能进行双向数据传递的状态• CLOSE_WAIT：服务器收到客户端关闭连接请求时所处的状态• FIN_WAIT_1：客户端发出关闭连接请求等待服务器回应时所处的状态• CLOSING：连接双方在向对端发出关闭连接请求后等待对端回应过程中收到对端发出的关闭连接请求时所处的状态• LAST_ACK：服务器向客户端发出关闭连接请求等待回应时所处的状态• FIN_WAIT_2：客户端收到服务器关闭连接回应后所处的状态• TIME_WAIT：客户端收到服务器的关闭连接请求后所处的状态
PCB	协议控制块索引

1.1.16 display ipv6 tcp verbose

display ipv6 tcp verbose 命令用来显示 IPv6 TCP 连接详细信息。

【命令】

display ipv6 tcp verbose [*slot slot-number* [*pcb pcb-index*]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

pcb pcb-index: 显示指定协议控制块索引的 IPv6 TCP 连接详细信息。*pcb-index* 表示协议控制块索引，取值范围为 1~16。

slot slot-number: 显示指定成员设备的 IPv6 TCP 连接详细信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 IPv6 TCP 连接详细信息。

【举例】

显示 IPv6 TCP 连接详细信息。

```
<Sysname> display ipv6 tcp verbose
TCP inpcb number: 1(tcpcb number: 1)

Location: Slot: 6
NSR standby: N/A
Creator: bgpd[199]
State: ISCONNECTED
Options: N/A
Error: 0
Receiving buffer(cc/hiwat/lowat/state): 0 / 65536 / 1 / N/A
Sending buffer(cc/hiwat/lowat/state): 0 / 65536 / 512 / N/A
Type: 1
Protocol: 6
Connection info: src = 2001::1->179 , dst = 2001::2->4181
Inpcb flags: N/A
Inpcb extflag: N/A
Inpcb vflag: INP_IPV6
Hop limit: 255 (minimum hop limit: 0)
Connection state: ESTABLISHED
TCP options: TF_REQ_SCALE TF_REQ_TSTMP TF_SACK_PERMIT TF_NSR
NSR state: READY(M)
Send VRF: 0x0
Receive VRF: 0x0
```

表1-15 display ipv6 tcp verbose 命令显示信息描述表

字段	描述
TCP inpcb number	IPv6 TCP类型Internet协议控制块个数
tcpcb number	IPv6 TCP控制块个数（处于TIME_WAIT状态的TCP则不列入计数）
Creator	创建socket的任务名称，括号中为创建者的进程号
State	<p>socket的状态，可能的状态如下：</p> <ul style="list-style-type: none"> • NOFDREF：用户已经关闭 • ISCONNECTED：连接已经建立 • ISCONNECTING：正在建立连接 • ISDISCONNECTING：正在断开连接 • ASYNC：异步方式 • ISDISCONNECTED：连接已经断开 • PROTOREF：协议强关联 • N/A：不处于上述状态
Options	<p>socket的选项，有以下几种：</p> <ul style="list-style-type: none"> • SO_DEBUG：记录套接字的调试信息 • SO_ACCEPTCONN：server 端监听连接请求 • SO_REUSEADDR：允许本地地址重复使用 • SO_KEEPALIVE：协议需要查询空闲的连接 • SO_DONTROUTE：设置不查路由表，由于目的地址是直连网络的情况 • SO_BROADCAST：套接字支持广播报文 • SO_LINGER：套接字关闭但仍发送剩余数据 • SO_OOBINLINE：带外数据采用内联方式存储 • SO_REUSEPORT：允许本地端口重复使用 • SO_NOSIGPIPE：socket 不能发送数据导致返回失败时不创建 SIGPIPE • SO_TIMESTAMPNS：和时戳选项功能类似，时间可以精确到纳秒 • SO_KEEPALIVETIME：设置空闲探测时间，TCP 支持此选项 • SO_FILTER：设置报文过滤条件，OSI Socket 和 RawIP 支持此选项 • N/A：没有设置选项
Error	影响socket连接的错误码

字段	描述
Receiving buffer(cc/hiwat/lowat/state)	<p>接收缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间、状态</p> <p>状态的取值有：</p> <ul style="list-style-type: none"> • CANTSENDMORE：不能发送数据到对端 • CANTRCVMORE：不能从对端接收数据 • RCVATMARK：接收标记 • N/A：不处于上述状态
Sending buffer(cc/hiwat/lowat/state)	<p>发送缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间、状态</p> <p>状态的取值有：</p> <ul style="list-style-type: none"> • CANTSENDMORE：不能发送数据到对端 • CANTRCVMORE：不能从对端接收数据 • RCVATMARK：接收标记 • N/A：不处于上述状态
Type	<p>使用的socket类型，类型的取值有：</p> <ul style="list-style-type: none"> • 1: SOCK_STREAM，流模式，提供可靠的字节流。TCP 协议使用此类型 • 2: SOCK_DGRAM，数据报模式的通信。UDP 协议使用此类型 • 3: SOCK_RAW，RAW 模式的通信方式 • N/A：不是上述类型
Protocol	使用TCP socket的协议号，6表示运用TCP协议
Connection info	连接信息，分别为源IPv6地址及端口号、目的IPv6地址及端口号

字段	描述
Inpcb flags	<p>Internet协议控制块中的标记，标记的取值有：</p> <ul style="list-style-type: none"> • INP_RECVOPTS: 接收传入的 IPv6 选项 • INP_RECVRETOPTS: 接收回应的 IPv6 选项 • INP_RECVDSTADDR: 接收目的 IPv6 地址 • INP_HDRINCL: 用户提供整个 IPv6 头 • INP_REUSEADDR: 重复使用地址 • INP_REUSEPORT: 重复使用端口号 • INP_ANONPORT: 用户未指定端口 • INP_PROTOCOL_PACKET: 标识报文为协议报文 • INP_RCVVLANID: 接收报文的 VLAN ID，仅 UDP 和 RawIP 支持 • IN6P_IPV6_V6ONLY: 仅支持 IPv6 协议栈 • IN6P_PKTINFO: 接收报文的源地址和入接口 • IN6P_HOPLIMIT: 接收报文 hoplimit • IN6P_HOPOPTS: 接收报文的逐跳扩展头信息 • IN6P_DSTOPTS: 接收报文的目的扩展头信息 • IN6P_RTHDR: 接收报文的路由扩展头信息 • IN6P_RTHDRDSTOPTS: 接收报文的路由头前的目的扩展头信息 • IN6P_TCLASS: 接收报文的优先级信息 • IN6P_AUTOFLOWLABEL: 使用随机流标签 • IN6P_RFC2292: 使用 RFC2292 API • IN6P_MTU: 感知路径 MTU 的变化，TCP 不支持 • INP_RCVMACADDR: 接收报文的 MAC • INP_SYNCPCB: 阻塞等待 inpcb 同步 • N/A: 不是上述标记
Inpcb extflag	<p>Internet协议控制块中的扩展标记，标记的取值有：</p> <ul style="list-style-type: none"> • INP_EXTRCVPVCIDX: 接收报文时记录报文的 PVC 索引 • INP_RCVPWID: 接收报文时记录报文的 PW ID • INP_EXTDONTDROP: 接收报文时设置报文不要丢弃 • INP_EXLISTEN: 监听 socket • N/A: 不是上述标记

字段	描述
Inpcb vflag	<p>Internet协议控制块中的IP版本标记:</p> <ul style="list-style-type: none"> • INP_IPV4: 运用与 IPv4 通信 • INP_IPV6: 运用与 IPv6 通信 • INP_IPV6PROTO: 运用 IPv6 协议创建的 inpcb • INP_TIMEWAIT: 处于等待状态 • INP_ONESBCAST: 发送广播报文 • INP_DROPPED: 协议丢弃标志 • INP_SOCKREF: socket 强关联 • INP_DONTBLOCK: inpcb 同步时不能被阻塞 • N/A: 不是上述标记
Hop limit(minimum hop limit)	Internet协议控制块中的跳数限制, 括号中为最小跳数限制
Connection state	<p>TCP连接状态, 可能的状态如下:</p> <ul style="list-style-type: none"> • CLOSED: 服务器收到客户端的关闭连接请求回应后所处的状态 • LISTEN: 服务器在等待连接请求时所处的状态 • SYN_SENT: 客户端发出连接请求等待服务器回应时所处的状态 • SYN_RCVD: 服务器收到客户端连接请求时所处的状态 • ESTABLISHED: 服务器和客户端双方建立连接并能进行双向数据传递的状态 • CLOSE_WAIT: 服务器收到客户端关闭连接请求时所处的状态 • FIN_WAIT_1: 客户端发出关闭连接请求等待服务器回应时所处的状态 • CLOSING: 连接双方在向对端发出关闭连接请求后等待对端回应过程中收到对端发出的关闭连接请求时所处的状态 • LAST_ACK: 服务器向客户端发出关闭连接请求等待回应时所处的状态 • FIN_WAIT_2: 客户端收到服务器关闭连接回应后所处的状态 • TIME_WAIT: 客户端收到服务器的关闭连接请求后所处的状态

字段	描述
TCP options	<p>TCP的选项类型，有以下几种：</p> <ul style="list-style-type: none"> • TF_MD5SIG：使能密钥 • TF_NODELAY：关闭延时 ACK • TF_NOOPT：TCP 不使用选项 • TF_NOPUSH：对写入的最后部分不进行 PUSH 操作 • TF_BINDFOREIGNADDR：绑定对端 IP 地址 • TF_NSR：使能 TCP NSR • TF_REQ_SCALE：使能窗口缩放因子选项 • TF_REQ_TSTMP：使能事件戳选项 • TF_SACK_PERMIT：使能选择性 ACK 选项 • TF_ENHANCED_AUTH：使能增强认证选项
NSR state	<p>TCP连接NSR状态，可能的状态如下：</p> <ul style="list-style-type: none"> • CLOSED：关闭（初始）状态 • CLOSING：连接待关闭状态 • ENABLED：使能备份功能状态 • OPEN：连接开始同步状态 • PENDING：连接判定状态 • READY：连接备份就绪状态 • SMOOTH：连接平滑状态 <p>角色：M表示主连接、S表示备份连接</p>
Send VRF	发送实例
Receive VRF	接收实例

1.1.17 display ipv6 udp

display ipv6 udp 命令用来显示 IPv6 UDP 连接摘要信息。

【命令】

display ipv6 udp [slot slot-number]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

slot slot-number: 显示指定成员设备的 IPv6 UDP 连接摘要信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 IPv6 UDP 连接摘要信息。

【举例】

显示 IPv6 UDP 连接摘要信息。

```
<Sysname> display ipv6 udp
LAddr->port      FAddr->port      Slot  PCB
2001:2002:2003:2 3001:3002:3003:3 1      0x0000000000000c387
004:2005:2006:20 004:3005:3006:30
07:2008->1200    07:3008->1200
2001::1->23      2001::5->1284    2      0x0000000000000008
2003::1->25      2001::2->1283    3      0x0000000000000009
```

表1-16 display ipv6 udp 命令显示信息描述表

字段	描述
LAddr->port	本端IPv6地址及端口号
FAddr->port	对端IPv6地址及端口号
PCB	协议控制块索引

1.1.18 display ipv6 udp verbose

display ipv6 udp verbose 命令用来显示 IPv6 UDP 连接详细信息。

【命令】

```
display ipv6 udp verbose [ slot slot-number [ pcb pcb-index ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

pcb pcb-index: 显示指定协议控制块索引的 IPv6 UDP 连接详细信息。*pcb-index* 表示协议控制块索引，取值范围为 1~16。

slot slot-number: 显示指定成员设备的 IPv6 UDP 连接详细信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 IPv6 UDP 连接详细信息。

【举例】

显示 IPv6 UDP 连接详细信息。

```
<Sysname> display ipv6 udp verbose
```

```
Total UDP socket number: 1

Location: slot: 6
Creator: sock_test_mips[250]
State: N/A
Options: N/A
Error: 0
Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 41600 / 1 / 0 / N/A
Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
Type: 2
Protocol: 17
Connection info: src = ::->69, dst = ::->0
Inpcb flags: N/A
Inpcb extflag: N/A
Inpcb vflag: INP_IPV6
Hop limit: 255 (minimum hop limit: 0)
Send VRF: 0xffff
Receive VRF: 0xffff
```

表1-17 display ipv6 udp verbose 命令显示信息描述表

字段	描述
Total UDP socket number	IPv6 UDP socket总数
Creator	创建socket的任务名称，括号中为创建者的进程号
State	<div>socket的状态，可能的状态如下：</div> <ul style="list-style-type: none">• NOFDREF：用户已经关闭• ISCONNECTED：连接已经建立• ISCONNECTING：正在建立连接• ISDISCONNECTING：正在断开连接• ASYNC：异步方式• ISDISCONNECTED：连接已经断开• PROTOREF：协议强关联• N/A：不处于上述状态

字段	描述
Options	<p>socket的选项，有以下几种：</p> <ul style="list-style-type: none"> • SO_DEBUG: 记录套接字的调试信息 • SO_ACCEPTCONN: server 端监听连接请求 • SO_REUSEADDR: 允许本地地址重复使用 • SO_KEEPALIVE: 协议需要查询空闲的连接 • SO_DONTROUTE: 设置不查路由表，由于目的地址是直连网络的情况 • SO_BROADCAST: 套接字支持广播报文 • SO_LINGER: 套接字关闭但仍发送剩余数据 • SO_OOBINLINE: 带外数据采用内联方式存储 • SO_REUSEPORT: 允许本地端口重复使用 • SO_TIMESTAMP: 入报文记录时间戳，只对非连接的协议有效，时间精确到毫秒 • SO_NOSIGPIPE: socket 不能发送数据导致返回失败时不创建SIGPIPE • SO_TIMESTAMPNS: 和时戳选项功能类似，时间可以精确到纳秒 • SO_KEEPALIVETIME: 设置空闲探测时间，TCP 支持此选项 • SO_FILTER: 设置报文过滤条件，OSI Socket 和 RawIP 支持此选项 • SO_USCBINDEX: 获取接收报文里的 UserProfile 索引 • N/A: 没有设置选项
Error	影响socket连接的错误码
Receiving buffer(cc/hiwat/lowat/drop/state)	<p>接收缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间、丢包数和状态</p> <p>状态的取值有：</p> <ul style="list-style-type: none"> • CANTSENDMORE: 不能发送数据到对端 • CANTRCVMORE: 不能从对端接收数据 • RCVATMARK: 接收标记 • N/A: 不处于上述状态

字段	描述
Sending buffer(cc/hiwat/lowat/state)	<p>发送缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间、状态</p> <p>状态的取值有：</p> <ul style="list-style-type: none"> • CANTSENDMORE：不能发送数据到对端 • CANTRCVMORE：不能从对端接收数据 • RCVATMARK：接收标记 • N/A：不处于上述状态
Type	<p>使用的socket类型，类型的取值有：</p> <ul style="list-style-type: none"> • 1: SOCK_STREAM，流模式，提供可靠的字节流。TCP 协议使用此类型 • 2: SOCK_DGRAM，数据报模式的通信。UDP 协议使用此类型 • 3: SOCK_RAW，RAW 模式的通信方式 • N/A：不是上述类型
Protocol	使用UDP socket的协议号，17表示运用UDP协议
Connection info	连接信息，分别为源IPv6地址及端口号、目的IPv6地址及端口号

字段	描述
Inpcb flags	<p>Internet协议控制块中的标记，标记的取值有：</p> <ul style="list-style-type: none"> • INP_RECVOPTS: 接收传入的 IPv6 选项 • INP_RECVRETOPTS: 接收回应的 IPv6 选项 • INP_RECVDSTADDR: 接收目的 IPv6 地址 • INP_HDRINCL: 用户提供整个 IPv6 头 • INP_REUSEADDR: 重复使用地址 • INP_REUSEPORT: 重复使用端口号 • INP_ANONPORT: 用户未指定端口 • INP_PROTOCOL_PACKET: 标识报文为协议报文 • INP_RCVVLANID: 接收报文的 VLAN ID，仅 UDP 和 RawIP 支持 • IN6P_IPV6_V6ONLY: 仅支持 IPv6 协议栈 • IN6P_PKTINFO: 接收报文的源地址和入接口 • IN6P_HOPLIMIT: 接收报文 hoplimit • IN6P_HOPOPTS: 接收报文的逐跳扩展头信息 • IN6P_DSTOPTS: 接收报文的目的扩展头信息 • IN6P_RTHDR: 接收报文的路由扩展头信息 • IN6P_RTHDRDSTOPTS: 接收报文的路由头前的目的扩展头信息 • IN6P_TCLASS: 接收报文的优先级信息 • IN6P_AUTOFLOWLABEL: 使用随机流标签 • IN6P_RFC2292: 使用 RFC2292 API • IN6P_MTU: 感知路径 MTU 的变化，TCP 不支持 • INP_RCVMACADDR: 接收报文的 MAC • INP_SYNCPCB: 阻塞等待 inpcb 同步 • N/A: 不是上述标记
Inpcb extflag	<p>Internet协议控制块中的扩展标记，标记的取值有：</p> <ul style="list-style-type: none"> • INP_EXTRCVPVCIDX: 接收报文时记录报文的 PVC 索引 • INP_RCVPWID: 接收报文时记录报文的 PW ID • N/A: 不是上述标记

字段	描述
Inpcb vflag	<p>Internet协议控制块中的IP版本标记，标记的取值有：</p> <ul style="list-style-type: none"> • INP_IPV4: 运用与 IPv4 通信 • INP_IPV6: 运用与 IPv6 通信 • INP_IPV6PROTO: 运用 IPv6 协议创建的 inpcb • INP_TIMEWAIT: 处于等待状态 • INP_ONESBCAST: 发送广播报文 • INP_DROPPED: 协议丢弃标志 • INP_SOCKREF: socket 强关联 • INP_DONTBLOCK: inpcb 同步时不能被阻塞 • N/A: 不是上述标记
Hop limit(minimum hop limit)	Internet协议控制块中的跳数限制，括号中为最小跳数限制
Send VRF	发送实例
Receive VRF	接收实例

1.1.19 ipv6 address

ipv6 address 命令用来手工配置接口的 IPv6 全球单播地址。

undo ipv6 address 命令用来删除接口的 IPv6 地址。

【命令】

```

ipv6 address { ipv6-address prefix-length | ipv6-address/prefix-length }
undo ipv6 address [ ipv6-address prefix-length | ipv6-address/prefix-length ]

```

【缺省情况】

接口上未配置 IPv6 全球单播地址。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6-address: IPv6 地址。

prefix-length: 前缀长度，取值范围为 1~128。

【使用指导】

IPv6 全球单播地址等同于 IPv4 公网地址，提供给网络服务提供商。这种类型的地址允许路由前缀的聚合，从而限制了全球路由表项的数量。

undo ipv6 address 命令不带参数则删除该接口的所有 IPv6 地址。

【举例】

指定 VLAN 接口 100 的 IPv6 全球单播地址为 2001::1，前缀长度为 64。

方法一：

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1/64
```

方法二：

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1 64
```

1.1.20 ipv6 address anycast

ipv6 address anycast 命令用来给接口配置 IPv6 任播地址。

undo ipv6 address anycast 命令用来删除接口上已配置的 IPv6 任播地址。

【命令】

```
ipv6 address { ipv6-address prefix-length | ipv6-address/prefix-length }
anycast
undo ipv6 address { ipv6-address prefix-length | ipv6-address/prefix-length }
anycast
```

【缺省情况】

接口上未配置 IPv6 任播地址。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6-address：指定 IPv6 任播地址。

prefix-length：前缀长度，取值范围为 1~128。

【举例】

指定 VLAN 接口 100 的 IPv6 任播地址为 2001::1，前缀长度为 64。

方法一：

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1/64 anycast
```

方法二：


```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1 64 anycast
```

1.1.21 ipv6 address auto

ipv6 address auto 命令用来开启无状态地址自动配置功能，使接口通过无状态自动配置方式生成全球单播地址。

undo ipv6 address auto 命令用来关闭无状态地址自动配置功能。

【命令】

```
ipv6 address auto
undo ipv6 address auto
```

【缺省情况】

无状态地址自动配置功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

【使用指导】

通过无状态自动配置方式生成全球单播地址时，会自动生成链路本地地址，生成的全球单播地址和链路本地地址可以通过执行 **undo ipv6 address auto** 命令或 **undo ipv6 address** 命令删除。

【举例】

配置 VLAN 接口 100 通过无状态自动配置方式生成全球单播地址。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address auto
```

1.1.22 ipv6 address auto link-local

ipv6 address auto link-local 命令用来配置系统自动为接口生成链路本地地址。

undo ipv6 address auto link-local 命令用来恢复缺省情况。

【命令】

```
ipv6 address auto link-local
undo ipv6 address auto link-local
```

【缺省情况】

接口上没有链路本地地址。当接口配置了 IPv6 全球单播地址后，会自动生成链路本地地址。

【视图】

接口视图

【缺省用户角色】

network-admin

【使用指导】

链路本地地址用于邻居发现协议和无状态自动配置中链路本地上节点之间的通信。使用链路本地地址作为源或目的地址的数据报文不会被转发到其他链路上。

接口配置了 IPv6 全球单播地址后，所自动生成的链路本地地址与采用 **ipv6 address auto link-local** 命令生成的链路本地地址相同。

undo ipv6 address auto link-local 命令只能删除使用 **ipv6 address auto link-local** 命令生成的链路本地地址。即如果此时接口已配置了 IPv6 全球单播地址，则接口仍有链路本地地址；如果此时接口未配置 IPv6 全球单播地址，则接口没有链路本地地址。

配置链路本地地址时，手工指定方式的优先级高于自动生成方式。即如果先采用自动生成方式，之后手工指定，则手工指定的地址会覆盖自动生成的地址；如果先手工指定，之后采用自动生成的方式，则自动配置不生效，接口的链路本地地址仍是手工指定的。此时，如果删除手工指定的地址，则自动生成的链路本地地址会生效。关于手工指定方式的介绍请参见命令 **ipv6 address link-local**。

【举例】

配置 VLAN 接口 100 自动生成链路本地地址。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address auto link-local
```

【相关命令】

- **ipv6 address link-local**

1.1.23 ipv6 address eui-64

ipv6 address eui-64 命令用来为接口配置 EUI-64 格式的 global 单播地址。

undo ipv6 address eui-64 命令用来删除接口上指定的 EUI-64 格式的 global 单播地址。

【命令】

```
ipv6 address { ipv6-address prefix-length | ipv6-address/prefix-length }
eui-64

undo ipv6 address [ ipv6-address prefix-length | ipv6-address/prefix-length ]
eui-64
```

【缺省情况】

接口上未配置 EUI-64 格式的 global 单播地址。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6-address/prefix-length: IPv6 地址/前缀长度，共同指定采用 EUI-64 格式形成的 IPv6 地址的前缀。前缀长度 *prefix-length* 的取值范围为 1~64。

【使用指导】

EUI-64 格式的地址由指定的地址前缀和自动产生的接口标识符生成，最终生成的地址可以通过 **display ipv6 interface** 命令查看。

在配置 EUI-64 地址时前缀长度取值不能大于 64。

【举例】

配置 VLAN 接口 100 采用 EUI-64 格式形成 IPv6 地址，其地址前缀与 2001::1/64 的前缀相同，接口标识符由设备的 MAC 地址生成。

方法一：

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1/64 eui-64
```

方法二：

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1 64 eui-64
```

【相关命令】

- **display ipv6 interface**

1.1.24 ipv6 address link-local

ipv6 address link-local 命令用来手动指定接口的链路本地地址。

undo ipv6 address link-local 命令用来恢复缺省情况。

【命令】

```
ipv6 address ipv6-address link-local
undo ipv6 address ipv6-address link-local
```

【缺省情况】

未指定接口的链路本地地址。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6-address: IPv6 链路本地地址，地址前面 10 位必须为 1111111010（二进制标识），即地址最前面的一组十六进制数为 FE80~FEBF。

【使用指导】

配置链路本地地址时，手工指定方式的优先级高于自动生成方式。即如果先采用自动生成方式，之后手工指定，则手工指定的地址会覆盖自动生成的地址；如果先手工指定，之后采用自动生成的方式，则自动配置不生效，接口的链路本地地址仍是手工指定的。此时，如果删除手工指定的地址，则自动生成的链路本地地址会生效。关于自动生成方式的介绍请参见命令 **ipv6 address auto link-local**。

【举例】

配置 VLAN 接口 100 的链路本地地址。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address fe80::1 link-local
```

【相关命令】

- **ipv6 address auto link-local**

1.1.25 ipv6 address prefix-number

ipv6 address prefix-number 命令用来引用前缀生成接口上的 IPv6 地址，并将此前缀分配给终端设备。

undo ipv6 address prefix-number 命令用来恢复缺省情况。

【命令】

```
ipv6 address prefix-number sub-prefix/prefix-length
undo ipv6 address prefix-number
```

【缺省情况】

接口上未引用前缀，也不会向终端设备分配该前缀。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

prefix-number: 表示 IPv6 前缀编号，取值范围为 1~1024。引用的 IPv6 前缀可以是手工静态配置，也可以是通过 DHCPv6 动态获取。

sub-prefix: 表示 IPv6 地址的子前缀位和主机位。

prefix-length: 表示地址的前缀长度，取值范围为 1~128。

【使用指导】

配置该命令后，接口的 IPv6 地址由指定编号的前缀、子前缀位和主机位构成。

一个接口上只能有一个引用前缀生成的地址，且不能通过重复执行本命令修改引用前缀生成的地址。如需修改引用前缀生成的地址，请先通过 **undo ipv6 address prefix-number** 命令取消引用前缀生成接口上的 IPv6 地址，再执行 **ipv6 address prefix-number** 命令。

【举例】

静态配置编号为 1 的 IPv6 前缀为 AAAA::/16，在接口上使用编号为 1 的前缀生成 IPv6 地址为 AAAA:CCCC:DDDD::10/32，并将编号为 1 的 IPv6 前缀分配给终端设备。

```
<Sysname> system-view
[Sysname] ipv6 prefix 1 AAAA::/16
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 1 BBBB:CCCC:DDDD::10/32
```

在 VLAN 接口 10 上配置动态获取 IPv6 前缀的编号为 2。在 VLAN 接口 100 上使用编号为 2 的前缀生成 IPv6 地址为 AAAA:CCCC:DDDD::10/32，并将编号为 2 的 IPv6 前缀分配给终端设备。

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ipv6 dhcp client pd 2 rapid-commit option-group 1
[Sysname-Vlan-interface10] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2 BBBB:CCCC:DDDD::10/32
```

【相关命令】

- **ipv6 prefix**
- **ipv6 dhcp client pd**（三层技术-IP 业务命令参考/DHCPv6）

1.1.26 ipv6 hop-limit

ipv6 hop-limit 命令用来配置设备的跳数限制。

undo ipv6 hop-limit 命令用来恢复缺省情况。

【命令】

```
ipv6 hop-limit value
undo ipv6 hop-limit
```

【缺省情况】

设备的跳数限制为 64 跳。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

value：跳数值，取值范围为 1～255。

【使用指导】

设备的跳数限制有以下两个作用：

- 决定了设备发送的 IPv6 数据报文的跳数，即 IPv6 数据报文的 Hop Limit 字段的值。
- 设备发送的 RA 消息中将携带此处配置的跳数限制值。收到该 RA 消息之后，主机在发送 IPv6 报文时，将使用该跳数值填充 IPv6 报文头中的 Hop Limit 字段。配置命令 **ipv6 nd ra hop-limit unspecified** 可以配置 RA 消息中不指定跳数限制。

【举例】

```
# 配置设备的跳数限制为 100 跳。
<Sysname> system-view
[Sysname] ipv6 hop-limit 100
```

【相关命令】

- `ipv6 nd ra hop-limit unspecified`

1.1.27 ipv6 hoplimit-expires enable

`ipv6 hoplimit-expires enable` 命令用来开启设备的 ICMPv6 超时报文的发送功能。

`undo ipv6 hoplimit-expires enable` 命令用来关闭设备的 ICMPv6 超时报文的发送功能。

【命令】

```
ipv6 hoplimit-expires enable
undo ipv6 hoplimit-expires enable
```

【缺省情况】

ICMPv6 超时报文发送功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

ICMPv6 超时报文发送功能是在设备收到 IPv6 数据报文后，如果发生超时（Hop-limit 超时或者重组超时）差错，则将报文丢弃并给源端发送 ICMPv6 超时差错报文。

如果接收到大量需要发送 ICMPv6 差错报文的恶意攻击报文，设备会因为处理大量该类报文而导致性能降低。为了避免该现象发生，可以关闭设备的 ICMPv6 超时报文发送功能，从而减少网络流量、防止遭到恶意攻击。

关闭 ICMPv6 超时报文发送功能后，设备不会再发送“Hop-Limit 超时”ICMPv6 差错报文，但“重组超时”ICMPv6 差错报文仍会正常发送。

【举例】

```
# 关闭设备的 ICMPv6 超时报文发送功能。
<Sysname> system-view
[Sysname] undo ipv6 hoplimit-expires enable
```

1.1.28 ipv6 icmpv6 error-interval

`ipv6 icmpv6 error-interval` 命令用来配置发送 ICMPv6 差错报文对应的令牌桶容量和令牌刷新周期。

`undo ipv6 icmpv6 error-interval` 命令用来恢复缺省情况。

【命令】

```
ipv6 icmpv6 error-interval interval [ bucketsize ]
```

```
undo ipv6 icmpv6 error-interval
```

【缺省情况】

令牌桶容量为 10，令牌刷新周期为 100 毫秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval: 令牌刷新周期, 取值范围 0~2147483647, 单位为毫秒。取值为 0 时, 表示不限制 ICMPv6 差错报文的发送。

bucketsize: 令牌桶中容纳的令牌数, 取值范围 1~200。

【使用指导】

如果网络中短时间内发送的 ICMPv6 差错报文过多, 将可能导致网络拥塞。为了避免这种情况, 用户可以控制在指定时间内发送 ICMPv6 差错报文的最大个数, 目前采用令牌桶算法来实现。

用户可以设置令牌桶的容量, 即令牌桶中可以同时容纳的令牌数; 同时可以设置令牌桶的刷新周期, 即每隔多长时间发放一个令牌到令牌桶中, 直到令牌桶中的令牌数达到配置的容量。一个令牌表示允许发送一个 ICMPv6 差错报文, 每当发送一个 ICMPv6 差错报文, 则令牌桶中减少一个令牌。如果连续发送的 ICMPv6 差错报文超过了令牌桶的容量, 则后续的 ICMPv6 差错报文将不能被发送出去, 直到按照所设置的刷新频率将新的令牌放入令牌桶中。

【举例】

配置设备发送 ICMPv6 差错报文对应的令牌桶容量为 40, 令牌刷新时间为 200 毫秒。

```
<Sysname> system-view  
[Sysname] ipv6 icmpv6 error-interval 200 40
```

1.1.29 ipv6 icmpv6 multicast-echo-reply enable

ipv6 icmpv6 multicast-echo-reply enable 命令用来配置允许设备回复组播形式的 Echo request 报文。

undo ipv6 icmpv6 multicast-echo-reply enable 命令用来恢复缺省情况。

【命令】

```
ipv6 icmpv6 multicast-echo-reply enable  
undo ipv6 icmpv6 multicast-echo-reply enable
```

【缺省情况】

不允许设备回复组播形式的 Echo request 报文。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

如果主机 B 允许回复组播形式的 Echo request 报文，则主机 A 可以构造目的地址为组播地址、源地址为主机 B 的 Echo request 报文，使该组播组中的所有的主机都向主机 B 发送 Echo reply 报文，从而达到攻击主机 B 的目的。因此，为了避免主机利用设备达到攻击的目的，缺省情况下，不允许设备回复组播形式的 Echo request 报文。

但在某些应用场景下，可能需要使用组播形式的 Echo request 报文来获取信息，此时可以配置允许设备回复组播形式的 Echo request 报文。

【举例】

配置允许设备回复组播形式的 Echo request 报文。

```
<Sysname> system-view
[Sysname] ipv6 icmpv6 multicast-echo-reply enable
```

1.1.30 ipv6 icmpv6 source

ipv6 icmpv6 source 命令用来开启 ICMPv6 报文指定源地址功能。

undo ipv6 icmpv6 source 命令用来关闭 ICMPv6 报文指定源地址功能。

【命令】

```
ipv6 icmpv6 source ipv6-address
undo ipv6 icmpv6 source
```

【缺省情况】

ICMPv6 报文指定源地址功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv6-address：表示设备发送 ICMPv6 报文时指定的源地址。

【使用指导】

在网络中 IPv6 地址配置较多的情况下，收到 ICMPv6 报文时，用户很难根据报文的源 IPv6 地址判断报文来自哪台设备。为了简化这一判断过程，可以配置 ICMPv6 报文指定源地址功能。用可配置特定地址（如环回口地址）为 ICMPv6 报文的源地址，可以简化判断。

设备发送 ICMPv6 差错报文（TTL 超时、报文过大、端口不可达和参数错误等）和 ping echo request 报文时，都可以通过上述命令指定报文的源地址。

【举例】

配置设备发送 ICMPv6 报文时指定的源地址为 1::1。

```
<Sysname> system-view
[Sysname] ipv6 icmpv6 source 1::1
```


1.1.31 ipv6 mtu

ipv6 mtu 命令用来配置接口上发送 IPv6 报文的 MTU。

undo ipv6 mtu 命令用来恢复缺省情况。

【命令】

```
ipv6 mtu size
undo ipv6 mtu
```

【缺省情况】

未配置接口上发送 IPv6 报文的 MTU。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

size: 接口的 MTU 值，单位为字节。取值范围为 1280～1500。

【使用指导】

当设备发送报文时，如果发现报文长度比发送该报文的接口的 MTU 值大，则会将其丢弃。如果设备是作为中间设备转发该报文，同时会将接口的 MTU 值通过 ICMPv6 报文的“Packet Too Big”消息发给源端主机，源端主机以该值重新发送 IPv6 报文。为减少报文被丢弃带来的额外流量开销，需要根据实际组网环境设置合适的接口 MTU 值。

【举例】

配置 VLAN 接口 100 上发送 IPv6 报文的 MTU 为 1280 字节。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 mtu 1280
```

1.1.32 ipv6 nd autoconfig managed-address-flag

ipv6 nd autoconfig managed-address-flag 命令用来配置被管理地址的配置标志位为 1，即主机通过有状态自动配置（例如 DHCPv6 服务器）获取 IPv6 地址。

undo ipv6 nd autoconfig managed-address-flag 命令用来恢复缺省情况。

【命令】

```
ipv6 nd autoconfig managed-address-flag
undo ipv6 nd autoconfig managed-address-flag
```

【缺省情况】

被管理地址的配置标志位为 0，即主机通过无状态自动配置获取 IPv6 地址。

【视图】

接口视图

【缺省用户角色】

network-admin

【使用指导】

被管理地址配置标志位（M flag）用于确定主机是否采用有状态自动配置获取 IPv6 地址。

如果设置该标志位为 1，主机将通过有状态自动配置（例如 DHCPv6 服务器）来获取 IPv6 地址；否则，将通过无状态自动配置获取 IPv6 地址，即根据自己的链路层地址及路由器发布的前缀信息生成 IPv6 地址。

【举例】

配置主机通过有状态自动配置获取 IPv6 地址。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd autoconfig managed-address-flag
```

1.1.33 ipv6 nd autoconfig other-flag

ipv6 nd autoconfig other-flag 命令用来配置其他信息配置标志位为 1，即主机通过有状态自动配置（例如 DHCPv6 服务器）获取除 IPv6 地址外的其他信息。

undo ipv6 nd autoconfig other-flag 命令用来恢复该缺省情况。

【命令】

```
ipv6 nd autoconfig other-flag
undo ipv6 nd autoconfig other-flag
```

【缺省情况】

其他信息配置标志位为 0，即主机通过无状态自动配置获取其他信息。

【视图】

接口视图

【缺省用户角色】

network-admin

【使用指导】

其他信息配置标志位（O flag）用于确定主机是否采用有状态自动配置获取除 IPv6 地址外的其他信息。

如果设置该标志位为 1，主机将通过有状态自动配置（例如 DHCPv6 服务器）来获取除 IPv6 地址外的其他信息；否则，将通过无状态自动配置获取其他信息。

【举例】

配置主机通过无状态自动配置来获取除 IPv6 地址外的其他信息。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo ipv6 nd autoconfig other-flag
```

1.1.34 ipv6 nd dad attempts

ipv6 nd dad attempts 命令用来配置进行重复地址检测时发送邻居请求消息的次数。

undo ipv6 nd dad attempts 命令用来恢复缺省情况。

【命令】

```
ipv6 nd dad attempts interval
undo ipv6 nd dad attempts
```

【缺省情况】

进行重复地址检测时发送邻居请求消息的次数为 1。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

interval: 进行重复地址检测时发送邻居请求消息的次数，取值范围为 0~600。当配置为 0 时，表示禁止重复地址检测。

【使用指导】

接口获得 IPv6 地址后，将发送邻居请求消息进行重复地址检测，如果在指定的时间内（通过 **ipv6 nd ns retrans-timer** 命令配置）没有收到响应，则继续发送邻居请求消息，当发送的次数达到使用 **ipv6 nd dad attempts** 命令所设置的次数后，仍未收到响应，则认为该地址可用。

【举例】

配置 VLAN 接口 100 进行重复地址检测时发送邻居请求消息的次数为 20 次。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd dad attempts 20
```

【相关命令】

- **display ipv6 interface**
- **ipv6 nd ns retrans-timer**

1.1.35 ipv6 nd ns retrans-timer

ipv6 nd ns retrans-timer 命令用来配置邻居请求消息的重传时间间隔。

undo ipv6 nd ns retrans-timer 命令用来恢复缺省情况。

【命令】

```
ipv6 nd ns retrans-timer value
undo ipv6 nd ns retrans-timer
```

【缺省情况】

接口发送 NS 消息的时间间隔为 1000 毫秒；接口发布的 RA 消息中 Retrans Timer 字段的值为 0，即不对主机进行指定。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

value: NS 消息重传时间间隔，取值范围为 1000~4294967295，单位为毫秒。

【使用指导】

设备发送 NS 消息后，如果未在指定的邻居请求消息重传时间间隔内收到响应，则会重新发送 NS 消息。

本命令配置的时间间隔既用于本接口发送 NS 消息的时间间隔，同时也作为本接口发布的 RA 消息中 Retrans Timer 字段的值。

【举例】

配置 VLAN 接口 100 发送 NS 消息的时间间隔为 10000 毫秒。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ns retrans-timer 10000
```

【相关命令】

- **display ipv6 interface**

1.1.36 ipv6 nd nud reachable-time

ipv6 nd nud reachable-time 命令用来配置接口保持邻居可达状态的时间。

undo ipv6 nd nud reachable-time 命令用来恢复缺省情况。

【命令】

```
ipv6 nd nud reachable-time time
undo ipv6 nd nud reachable-time
```

【缺省情况】

接口保持邻居可达状态的时间为 30000 毫秒；接口发布的 RA 消息中 Reachable Timer 字段的值为 0，即不对主机进行指定。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

time: 保持邻居可达状态的时间，取值范围为 1~3600000，单位为毫秒。

【使用指导】

当通过邻居可达性检测确认邻居可达后，在所设置的接口保持邻居可达状态的时间内，设备认为邻居可达；超过设置的时间后，如果需要向邻居发送报文，会重新确认邻居是否可达。

本命令配置的时间既用于本接口保持邻居可达状态的时间，同时也作为本接口发布的 RA 消息中 Reachable Timer 字段的值。

【举例】

```
# 配置 VLAN 接口 100 上保持邻居可达状态的时间为 10000 毫秒。
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd nud reachable-time 10000
```

【相关命令】

- **display ipv6 interface**

1.1.37 ipv6 nd ra halt

ipv6 nd ra halt 命令用来抑制 RA 消息的发布。

undo ipv6 nd ra halt 命令用来取消对 RA 消息发布的抑制。

【命令】

```
ipv6 nd ra halt
undo ipv6 nd ra halt
```

【缺省情况】

抑制发布 RA 消息。

【视图】

接口视图

【缺省用户角色】

network-admin

【举例】

```
# 取消对 VLAN 接口 100 发布 RA 消息的抑制。
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo ipv6 nd ra halt
```

1.1.38 ipv6 nd ra hop-limit unspecified

ipv6 nd ra hop-limit unspecified 命令用来配置 RA 消息中不指定跳数限制。

undo ipv6 nd ra hop-limit unspecified 命令用来恢复缺省情况。

【命令】

```
ipv6 nd ra hop-limit unspecified
undo ipv6 nd ra hop-limit unspecified
```

【缺省情况】

RA 消息中发布本设备的跳数限制。本设备的跳数限制默认为 64 跳。

【视图】

接口视图

【缺省用户角色】

network-admin

【使用指导】

本设备的跳数限制默认为 64 跳，可以通过命令 **ipv6 hop-limit** 进行配置。

【举例】

```
# 配置 VLAN 接口 100 上 RA 消息中不指定跳数限制。
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra hop-limit unspecified
```

【相关命令】

- **ipv6 hop-limit**

1.1.39 ipv6 nd ra interval

ipv6 nd ra interval 命令用来配置 RA 消息发布的最大时间间隔和最小时间间隔。

undo ipv6 nd ra interval 命令用来恢复缺省情况。

【命令】

```
ipv6 nd ra interval max-interval min-interval
undo ipv6 nd ra interval
```

【缺省情况】

RA 消息发布的最大时间间隔为 600 秒，最小时间间隔为 200 秒。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

max-interval: 指定 RA 消息发布的最大时间间隔，取值范围是 4~1800，单位为秒。

min-interval: 指定 RA 消息发布的最小时间间隔，取值范围是 3~ (*max-interval* * 3/4)，单位为秒。

【使用指导】

RA 消息周期性发布时，设备在最大时间间隔与最小时间间隔之间随机选取一个值作为周期性发布 RA 消息的时间间隔。

RA 消息发布的最大实际间隔应该小于或等于 RA 消息中路由器的生存时间。

【举例】

配置设备周期性发布 RA 消息的最大时间间隔为 1000 秒，最小时间间隔为 700 秒。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra interval 1000 700
```

【相关命令】

- **ipv6 nd ra router-lifetime**

1.1.40 ipv6 nd ra no-advlinkmtu

ipv6 nd ra no-advlinkmtu 命令用来配置 RA 消息中不携带 MTU 选项。

undo ipv6 nd ra no-advlinkmtu 命令用来恢复缺省情况。

【命令】

```
ipv6 nd ra no-advlinkmtu
undo ipv6 nd ra no-advlinkmtu
```

【缺省情况】

RA 消息中携带 MTU 选项。

【视图】

接口视图

【缺省用户角色】

network-admin

【使用指导】

RA 消息中携带的 MTU 选项可以用来发布链路的 MTU，用于确保同一链路路上的所有节点采用相同的 MTU 值。

【举例】

配置 VLAN 接口 100 上 RA 消息中不携带 MTU 选项。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra no-advlinkmtu
```

1.1.41 ipv6 nd ra prefix

ipv6 nd ra prefix 命令用来配置 RA 消息中的前缀信息。

undo ipv6 nd ra prefix 命令用来恢复缺省情况。

【命令】

```
ipv6 nd ra prefix { ipv6-prefix prefix-length | ipv6-prefix/prefix-length }  
[ valid-lifetime preferred-lifetime [ no-autoconfig | off-link ] * |  
no-advertise ]  
undo ipv6 nd ra prefix { ipv6-prefix | ipv6-prefix/prefix-length }
```

【缺省情况】

未配置 RA 消息中的前缀信息，此时将使用发送 RA 消息的接口 IPv6 地址作为 RA 中的前缀信息，其手工配置地址的有效生命期是 2592000 秒（30 天），首选生命期是 604800（7 天）；其他自动分配地址（如 DHCPv6 分配地址）的有效生命期和首选生命期与地址本身的生命期相同。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6-prefix: IPv6 地址前缀。

prefix-length: 前缀长度。

valid-lifetime: 前缀的有效存活时间，即有效生命期。取值范围为 0~4294967295，单位为秒，缺省值为 2592000 秒（30 天）。

preferred-lifetime: 前缀用于无状态地址配置的优选项的存活时间，即首选生命期。取值范围为 0~4294967295，单位为秒。*preferred-lifetime* 的值要小于等于 *valid-lifetime* 的值，缺省值为 604800 秒（7 天）。

no-autoconfig: 指定前缀不用于无状态地址配置。如果不选择该参数，则指定前缀用于无状态地址配置。

off-link: 指定前缀不是该链路上直连可达的。如果不选择该参数，则表示指定前缀是直连可达的。

no-advertise: 指定前缀不在 RA 消息中发布。如果不选择该参数，则表示指定前缀在 RA 消息中发布。

【使用指导】

如果使用本命令配置的前缀和 IPv6 地址生成的前缀相同，则优先使用本命令配置的前缀信息进行 RA 消息发布。

在同一链路上的主机收到设备发布的 RA 消息中后，可以根据 RA 消息中的前缀信息进行无状态自动配置等操作。

配置 RA 消息中的前缀信息时，如果不指定任何参数，在使用 **ipv6 nd ra prefix default** 命令的情况下，采用 **default** 配置参数，否则采用缺省情况下的参数值，即有效生命期是 2592000 秒（30 天），首选生命期是 604800（7 天），配置的前缀可以用于无状态地址配置、在 RA 消息中发布，并且是直连可达的。

【举例】

配置 VLAN 接口 100 上 RA 消息中的前缀信息。

方法一：

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra prefix 2001:10::100/64 100 10
```

方法二：

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra prefix 2001:10::100 64 100 10
```

1.1.42 ipv6 nd ra prefix default

ipv6 nd ra prefix default 命令用来配置通过 RA 消息发布的前缀使用的缺省参数。

undo ipv6 nd ra prefix default 命令用来恢复缺省情况。

【命令】

```
ipv6 nd ra prefix default [ valid-lifetime preferred-lifetime
[ no-autoconfig | off-link ] * | no-advertise ]
undo ipv6 nd ra prefix default
```

【缺省情况】

未配置通过 RA 消息发布的前缀使用的缺省参数。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

valid-lifetime：前缀的有效存活时间，即有效生命期。取值范围为 0~4294967295，单位为秒，缺省值为 2592000 秒（30 天）。

preferred-lifetime：前缀用于无状态地址配置的优选项的存活时间，即首选生命期。取值范围为 0~4294967295，单位为秒。**preferred-lifetime** 的值要小于等于 **valid-lifetime** 的值，缺省值为 604800（7 天）。

no-autoconfig：前缀不用于无状态地址配置。如果不选择该参数，则表示前缀用于无状态地址配置。

off-link：前缀不是该链路上直连可达的。如果不选择该参数，则表示前缀是直连可达的。

no-advertise：前缀不在 RA 消息中发布。如果不选择该参数，则表示前缀在 RA 消息中发布。

【使用指导】

对于使用 **ipv6 nd ra prefix { ipv6-prefix prefix-length | ipv6-prefix/prefix-length }** 命令配置的前缀，本命令的所有配置生效；对于由发布 RA 消息的接口的 IPv6 地址生成的前缀，本命令的配置中只有 **no-advertise** 配置生效。

通过本命令配置缺省参数后，在配置 **ipv6 nd ra prefix { ipv6-prefix prefix-length | ipv6-prefix/prefix-length }** 命令时，如果指定了 **valid-lifetime**、

preferred-lifetime、*no-autoconfig*、*off-link*、*no-advertise* 等参数，则使用指定的参数，如果没有指定这些参数，则使用本命令配置的缺省参数。

【举例】

配置 VLAN 接口 100 上 RA 消息中的缺省前缀信息。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra prefix default 100 10
```

1.1.43 ipv6 nd ra router-lifetime

ipv6 nd ra router-lifetime 命令用来配置 RA 消息中路由器的生存时间。

undo ipv6 nd ra router-lifetime 命令用来恢复缺省情况。

【命令】

```
ipv6 nd ra router-lifetime time
undo ipv6 nd ra router-lifetime
```

【缺省情况】

RA 消息中路由器的生存时间为 1800 秒。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

time：RA 消息中路由器的生存时间，取值范围为 0~9000，单位为秒。当配置为 0 时，表示本设备不作为默认路由器。

【使用指导】

RA 消息中路由器的生存时间用于设置发布 RA 消息的路由器作为主机的默认路由器的时间。主机根据接收到的 RA 消息中的路由器生存时间参数值，就可以确定是否将发布该 RA 消息的路由器作为默认路由器。发布 RA 消息中路由器生存时间为 0 的路由器不能作为默认路由器。

RA 消息中路由器的生存时间应该大于或等于 RA 消息的发布时间间隔。

【举例】

配置 VLAN 接口 100 上 RA 消息中路由器的生存时间为 1000 秒。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra router-lifetime 1000
```

【相关命令】

- **ipv6 nd ra interval**

1.1.44 ipv6 nd router-preference

ipv6 nd router-preference 命令用来配置接口下发送的 RA 消息中的路由器优先级。

undo ipv6 nd router-preference 命令用来恢复缺省情况。

【命令】

```
ipv6 nd router-preference { high | low | medium }  
undo ipv6 nd router-preference
```

【缺省情况】

设备发送的 RA 消息中的路由器优先级为 **medium**。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

high: 设置发布 RA 的路由器为高优先级。

low: 设置发布 RA 的路由器为低优先级。

medium: 设置发布 RA 的路由器为中优先级。

【使用指导】

主机根据接收到的 RA 消息中的路由器优先级，可以选择优先级最高的路由器作为默认网关。

在路由器的优先级相同的情况下，遵循“先来先用”的原则，优先选择先接收到的 RA 消息对应的发送路由器作为默认网关。

【举例】

配置 VLAN 接口 100 下发送的 RA 消息中的路由优先级为 **high**。

```
<Sysname> system-view  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] ipv6 nd router-preference high
```

1.1.45 ipv6 nd snooping dad retrans-timer

ipv6 nd snooping dad retrans-timer 命令用来配置发送两次 DAD NS 报文进行探测的时间间隔。

undo ipv6 nd snooping dad retrans-timer 命令用来恢复缺省情况。

【命令】

```
ipv6 nd snooping dad retrans-timer interval  
undo ipv6 nd snooping dad retrans-timer
```

【缺省情况】

发送两次 DAD NS 报文进行探测的时间间隔为 250 毫秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval: 发送两次 DAD NS 报文的时间间隔，取值范围为 100～500，单位为毫秒。

【使用指导】

ND Snooping 在表项建立、迁移和老化过程中，都会发送 DAD NS 报文进行探测。设备在第一次 DAD NS 报文发出后，如果一定时间内未收到应答报文，同时为了防止报文被丢弃，增加可靠性，会再次发送报文。用户可以根据网络实际情况调整两次报文发送的时间间隔。

如果 ND Snooping 表项的 INVALID 状态超时时间大于本命令配置的发送间隔，则会发送两次 DAD NS 报文。如果 INVALID 状态超时时间小于本命令配置的发送间隔，则只发送一次 DAD NS 报文。

【举例】

配置发送两次 DAD NS 报文进行探测的时间间隔为 200 毫秒。

```
<Sysname> system-view
[Sysname] ipv6 nd snooping dad retrans-timer 200
```

1.1.46 ipv6 nd snooping enable global

ipv6 nd snooping enable global 命令用来开启学习表项地址类型为全局单播地址的 ND Snooping 表项的功能。

undo ipv6 nd snooping enable global 命令用来关闭学习表项地址类型为全局单播地址的 ND Snooping 表项的功能。

【命令】

```
ipv6 nd snooping enable global
undo ipv6 nd snooping enable global
```

【缺省情况】

学习表项地址类型为全局单播地址的 ND Snooping 表项的功能处于关闭状态。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

【举例】

开启 VLAN2 内接口学习表项地址类型为全局单播地址的 ND Snooping 表项的功能。

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] ipv6 nd snooping enable global
```

1.1.47 ipv6 nd snooping enable link-local

ipv6 nd snooping enable link-local 命令用来开启学习表项地址类型为链路本地地址的 ND Snooping 表项的功能。

undo ipv6 nd snooping enable link-local 命令用来关闭学习表项地址类型为链路本地地址的 ND Snooping 表项的功能。

【命令】

```
ipv6 nd snooping enable link-local
undo ipv6 nd snooping enable link-local
```

【缺省情况】

学习表项地址类型为链路本地地址的 ND Snooping 表项的功能处于关闭状态。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

【举例】

```
# 开启 VLAN 2 内接口学习表项地址类型为链路本地地址的 ND Snooping 表项的功能。
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] ipv6 nd snooping enable link-local
```

1.1.48 ipv6 nd snooping glean source

ipv6 nd snooping glean source 命令用来开启通过 IPv6 数据报文学习 ND Snooping 表项的功能。

undo ipv6 nd snooping glean source 命令用来关闭通过 IPv6 数据报文学习 ND Snooping 表项的功能。

【命令】

```
ipv6 nd snooping glean source
undo ipv6 nd snooping glean source
```

【缺省情况】

通过 IPv6 数据报文学习 ND Snooping 表项的功能处于关闭状态。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

【使用指导】

当用户需要通过侦听 IPv6 数据报文来生成 ND Snooping 表项时，必须配置本命令。

至少配置了 **ipv6 nd snooping enable global** 和 **ipv6 nd snooping enable link-local** 这两条命令其中之一后，本功能才能生效。

本命令开启后，VLAN 内 ND 非信任端口必须开启 IPv6 Source Guard 功能，否则会导致该端口的报文不能正常转发。

【举例】

开启 VLAN 2 内的接口通过 IPv6 数据报文学习 ND Snooping 表项的功能。

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] ipv6 nd snooping glean source
```

1.1.49 ipv6 nd snooping lifetime

ipv6 nd snooping lifetime 命令用来配置 ND Snooping 表项的超时时间。

undo ipv6 nd snooping lifetime 命令用来恢复缺省情况。

【命令】

```
ipv6 nd snooping lifetime { invalid invalid-lifetime | valid valid-lifetime }
undo ipv6 nd snooping lifetime { invalid | valid }
```

【缺省情况】

ND Snooping 表项的 INVALID 状态（TENTATIVE、TESTING_TPLT 和 TESTING_VP 状态）的超时时间为 500 毫秒，VALID 状态的超时时间为 300 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

invalid *invalid-lifetime*：ND Snooping 表项的 INVALID 状态（TENTATIVE、TESTING_TPLT 和 TESTING_VP 状态）的超时时间，取值范围为 250~1000，单位为毫秒。

valid *valid-lifetime*：ND Snooping 表项的 VALID 状态的超时时间，即表项的老化时间，取值范围为 60~900，单位为秒。

【举例】

配置表项的 VALID 状态的超时时间为 250 秒。

```
<Sysname> system-view
[Sysname] ipv6 nd snooping lifetime valid 250
```

1.1.50 ipv6 nd snooping max-learning-num

ipv6 nd snooping max-learning-num 命令用来配置接口下学习 ND Snooping 表项的最大个数。

undo ipv6 nd snooping max-learning-num 命令用来恢复缺省情况。

【命令】

```
ipv6 nd snooping max-learning-num max-number
undo ipv6 nd snooping max-learning-num
```

【缺省情况】

接口下学习 ND Snooping 表项的最大个数为 1024。

【视图】

二层以太网接口视图
二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

max-number: 接口下学习 ND Snooping 表项的最大个数，取值范围为 1~1024。

【举例】

```
# 配置接口 GigabitEthernet1/0/1 学习 ND Snooping 表项的最大个数为 64。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd snooping max-learning-num 64
```

1.1.51 ipv6 nd snooping uplink

ipv6 nd snooping uplink 命令用来配置接口为 ND Snooping 上行接口，该接口禁止学习 ND Snooping 表项。

undo ipv6 nd snooping uplink 命令用来恢复缺省情况。

【命令】

```
ipv6 nd snooping uplink
undo ipv6 nd snooping uplink
```

【缺省情况】

接口不是 ND Snooping 的上行接口，在开启 ND Snooping 功能后，允许学习 ND Snooping 表项。

【视图】

二层以太网接口视图
二层聚合接口视图

【缺省用户角色】

network-admin

【举例】

```
# 配置二层以太网接口 GigabitEthernet1/0/1 为上行口，禁止接口学习 ND Snooping 表项。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd snooping uplink
# 配置二层聚合接口 Bridge-Aggregation1 为上行口，禁止接口学习 ND Snooping 表项。
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] ipv6 nd snooping uplink
```

1.1.52 ipv6 neighbor

ipv6 neighbor 命令用来配置静态邻居表项。

undo ipv6 neighbor 命令用来删除邻居表项。

【命令】

```
ipv6 neighbor ipv6-address mac-address { vlan-id port-type port-number |  
interface interface-type interface-number }  
undo ipv6 neighbor ipv6-address interface-type interface-number
```

【缺省情况】

不存在静态邻居表项。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv6-address: 静态邻居表项中的 IPv6 地址。

mac-address: 静态邻居表项中的链路层地址（48 位，格式为 H-H-H）。

vlan-id: 静态邻居表项所对应的 VLAN ID，取值范围为 1~4094。

port-type port-number: 静态邻居表项所对应的二层端口类型和端口号。

interface interface-type interface-number: 静态邻居表项所对应的三层接口类型和接口号。

【使用指导】

邻居表项保存的是设备在链路范围内的邻居信息，设备邻居表项可以通过邻居请求消息 NS 及邻居通告消息 NA 来动态创建，也可以通过手工配置来静态创建。

设备根据邻居节点的 IPv6 地址和与此邻居节点相连的三层接口号来唯一标识一个静态邻居表项。

目前，静态邻居表项有两种配置方式：

- 配置本节点的三层接口相连的邻居节点的 IPv6 地址和链路层地址；
- 配置本节点 VLAN 中的二层端口相连的邻居节点的 IPv6 地址和链路层地址。

对于 VLAN 接口，可以采用上述两种方式来配置静态邻居表项：

- 采用第一种方式配置静态邻居表项后，该邻居表项处于 INCMP 状态。设备解析该 VLAN 下的二层端口信息后，该邻居表项才会进入 REACH 状态。
- 采用第二种方式配置静态邻居表项，需要保证 *port-type port-number* 指定的二层端口属于 *vlan-id* 指定的 VLAN，且该 VLAN 已经创建了 VLAN 接口。在配置后，设备会将 VLAN 所对应的 VLAN 接口与 IPv6 地址相对应来唯一标识一个静态邻居表项，并且该表项处于 REACH 状态。

执行 **undo ipv6 neighbor** 命令既可以删除静态邻居表项，也可以删除动态邻居表项。

在删除 VLAN 接口对应的邻居表项时，只需要指定 VLAN 对应的 VLAN 接口即可。

【举例】

配置 VLAN 接口 1 对应的静态邻居表项。

```
<Sysname> system-view
[Sysname] ipv6 neighbor 2000::1 fe-e0-89 interface Vlan-interface 1
```

【相关命令】

- **display ipv6 neighbors**
- **reset ipv6 neighbors**

1.1.53 ipv6 neighbor link-local minimize

ipv6 neighbor link-local minimize 命令用来配置链路本地 ND 表项资源占用最小化。

undo ipv6 neighbor link-local minimize 命令用来恢复缺省情况。

【命令】

```
ipv6 neighbor link-local minimize
undo ipv6 neighbor link-local minimize
```

【缺省情况】

所有 ND 表项均会下发硬件表项。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

本功能可以对链路本地 ND 表项（该 ND 表项的 IPv6 地址为链路本地地址）占用的资源进行优化。配置本功能后，新学习的、未被引用的链路本地 ND 表项（该 ND 表项的链路本地地址不是某条路由的下一跳）不下发硬件表项，以节省资源。

本功能只对后续新学习的 ND 表项生效，已经存在的 ND 表项不受影响。

【举例】

配置链路本地 ND 表项资源占用最小化。

```
<Sysname> system-view
[Sysname] ipv6 neighbor link-local minimize
```

1.1.54 ipv6 neighbor stale-aging

ipv6 neighbor stale-aging 命令用来配置 STALE 状态 ND 表项的老化时间。

undo ipv6 neighbor stale-aging 命令用来恢复缺省情况。

【命令】

```
ipv6 neighbor stale-aging aging-time
undo ipv6 neighbor stale-aging
```

【缺省情况】

STALE 状态 ND 表项的老化时间为 240 分钟。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

aging-time: STALE 状态 ND 表项的老化时间，取值范围为 1~1440，单位为分钟。

【使用指导】

为适应网络的变化，ND 表需要不断更新。ND 表中的 STALE 状态 ND 表项并非永远有效，每一条记录都有一个老化时间。到达老化时间的 STALE 状态 ND 表项将迁移到 DELAY 状态。5 秒钟后 DELAY 状态超时，ND 表项将迁移到 PROBE 状态，并发送 3 次 NS 报文进行可达性探测。若邻居已经下线，则收不到回应的 NA 报文，此时会将该 ND 表项删除。

【举例】

配置 STALE 状态 ND 表项的老化时间为 120 分钟。

```
<Sysname> system-view
[Sysname] ipv6 neighbor stale-aging 120
```

1.1.55 ipv6 neighbors max-learning-num

ipv6 neighbors max-learning-num 命令用来配置接口上允许学习的动态邻居表项的最大个数。

undo ipv6 neighbors max-learning-num 命令用来恢复缺省情况。

【命令】

```
ipv6 neighbors max-learning-num max-number
undo ipv6 neighbors max-learning-num
```

【缺省情况】

各系列产品接口上允许学习的动态邻居表项的最大个数为：

- S5130S-SI 系列交换机、S5120V2-SI 系列交换机为 512。
- S5130S-LI 系列交换机、S5120V2-LI 系列交换机和 S3100V3-SI 系列交换机为 256。
- S5110V2-SI 系列交换机为 128。
- S5000V3-EI 系列交换机、S5000E-X 系列交换机为 64。

【视图】

二层接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

max-number: 接口上允许学习的动态邻居表项的最大个数。取值范围为:

- S5130S-SI 系列交换机、S5120V2-SI 系列交换机为 1~512。
- S5130S-LI 系列交换机、S5120V2-LI 系列交换机和 S3100V3-SI 系列交换机为 1~256。
- S5110V2-SI 系列交换机为 1~128。
- S5000V3-EI 系列交换机、S5000E-X 系列交换机为 1~64。

【使用指导】

设备可以通过 NS 消息和 NA 消息来动态获取邻居节点的链路层地址，并将其加入到邻居表中。为了防止部分接口下的用户占用过多的资源，可以通过设置接口学习动态邻居表项的最大数目来进行限制。当接口学习到的动态邻居表项的个数达到所设置的最大值时，该接口将不再学习动态邻居表项。

【举例】

配置 VLAN 接口 100 上允许动态学习的邻居的最大个数为 10 个。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 neighbors max-learning-num 10
```

1.1.56 ipv6 pathmtu

ipv6 pathmtu 命令用来配置 IPv6 地址对应的静态 PMTU。

undo ipv6 pathmtu 命令用来删除指定 IPv6 地址的 PMTU 配置。

【命令】

```
ipv6 pathmtu ipv6-address value
undo ipv6 pathmtu ipv6-address
```

【缺省情况】

未配置 IPv6 地址对应的静态 PMTU 值。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv6-address: 指定的 IPv6 地址。

value: 指定 IPv6 地址对应的 PMTU 值，取值范围为 1280~10240，单位为字节。

【使用指导】

用户可以为指定的目的 IPv6 地址配置静态的 PMTU 值。当源端主机从接口发送报文时，将比较该接口的 MTU 与指定目的 IPv6 地址的静态 PMTU，如果报文长度大于二者中的最小值，则采用此最小值对报文进行分片。

【举例】

```
# 配置指定 IPv6 地址对应的静态 PMTU 值。
<Sysname> system-view
[Sysname] ipv6 pathmtu fe80::12 1300
```

【相关命令】

- **display ipv6 pathmtu**
- **reset ipv6 pathmtu**

1.1.57 ipv6 pathmtu age

ipv6 pathmtu age 命令用来配置动态 PMTU 的老化时间。
undo ipv6 pathmtu age 命令用来恢复缺省情况。

【命令】

```
ipv6 pathmtu age age-time
undo ipv6 pathmtu age
```

【缺省情况】

动态 PMTU 的老化时间为 10 分钟。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

age-time: PMTU 老化时间，取值范围为 10~100，单位为分钟。

【使用指导】

动态确定源端主机到目的端主机的 PMTU 后，源端主机将使用这个 MTU 值发送后续报文到目的端主机。当 PMTU 老化时间超时后：

- 删除动态 PMTU；
- 源端主机会通过 PMTU 机制重新确定发送报文的 MTU 值。

该配置对静态 PMTU 不起作用。

【举例】

```
# 配置动态 PMTU 的老化时间为 40 分钟。
<Sysname> system-view
[Sysname] ipv6 pathmtu age 40
```

【相关命令】

- **display ipv6 pathmtu**

1.1.58 ipv6 prefer temporary-address

ipv6 prefer temporary-address 命令用来开启优先选择临时地址作为报文的源地址功能。

undo ipv6 prefer temporary-address 命令用来关闭优先选择临时地址作为报文的源地址功能。

【命令】

```
ipv6 prefer temporary-address
undo ipv6 prefer temporary-address
```

【缺省情况】

优先选择临时地址作为报文的源地址功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

在配置了优先选择临时地址功能前提下发送报文，系统将优先选择临时地址作为报文的源地址。如果生成的临时地址因为 DAD 冲突不可用，就采用公共地址作为报文的源地址。

【举例】

开启优先选择临时地址作为报文的源地址功能。

```
<Sysname> system-view
[Sysname] ipv6 prefer temporary-address
```

【相关命令】

- **ipv6 address auto**
- **ipv6 nd ra prefix**
- **ipv6 temporary-address**

1.1.59 ipv6 prefix

ipv6 prefix 命令用来手工配置静态 IPv6 前缀。

undo ipv6 prefix 命令用来删除指定的静态 IPv6 前缀。

【命令】

```
ipv6 prefix prefix-number ipv6-prefix/prefix-length
undo ipv6 prefix prefix-number
```

【缺省情况】

未配置静态 IPv6 前缀。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

prefix-number: 前缀编号, 取值范围为 1~1024。

ipv6-prefix/prefix-length: 前缀和前缀长度。*prefix-length* 的取值范围为 1~128。

【使用指导】

不能通过重复执行本命令修改已经创建的静态 IPv6 前缀。如需修改静态 IPv6 前缀, 请先通过 **undo ipv6 prefix** 命令删除静态 IPv6 前缀, 再执行 **ipv6 prefix** 命令。

不允许手工修改和删除从 DHCPv6 服务器获取的动态 IPv6 前缀。

手工配置的静态 IPv6 前缀与动态生成的 IPv6 前缀编号允许相同, 静态 IPv6 前缀优先。

【举例】

创建 IPv6 静态前缀编号为 1, 前缀为 2001:0410::/32。

```
<Sysname> system-view
[Sysname] ipv6 prefix 1 2001:0410::/32
```

【相关命令】

- **display ipv6 prefix**

1.1.60 ipv6 reassemble local enable

ipv6 reassemble local enable 命令用来开启 IPv6 分片报文本地重组功能。

undo ipv6 reassemble local enable 命令用来关闭 IPv6 分片报文本地重组功能。

【命令】

```
ipv6 reassemble local enable
undo ipv6 reassemble local enable
```

【缺省情况】

IPv6 分片报文本地重组功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

多台设备组成的 IRF 环境下, 当某成员设备收到目的为本 IRF 设备的 IPv6 分片报文时, 需要把分片报文送到主设备进行重组, 这样会导致报文重组性能较低的问题。当开启 IPv6 分片报文本地重组功能后, 分片报文会在该成员设备上直接进行报文重组, 这样就能提高分片报文的重组性能。开启 IPv6 分片报文本地重组功能后, 如果分片报文是从设备上不同的成员设备进入的, 会导致 IPv6 分片报文本地无法重组成功。

【举例】

开启 IPv6 分片报文本地重组功能。

```
<Sysname> system-view
[Sysname] ipv6 reassemble local enable
```

1.1.61 ipv6 redirects enable

ipv6 redirects enable 命令用来开启设备的 ICMPv6 重定向报文的发送功能。

undo ipv6 redirects enable 命令用来关闭设备的 ICMPv6 重定向报文的发送功能。

【命令】

```
ipv6 redirects enable
undo ipv6 redirects enable
```

【缺省情况】

ICMPv6 重定向报文发送功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

主机启动时，它的路由表中可能只有一条到缺省网关的缺省路由。当满足一定的条件时，作为缺省网关的设备会向源主机发送 ICMPv6 重定向报文，通知主机重新选择正确的下一跳进行后续报文的发送。

ICMPv6 重定向报文发送功能可以简化主机的管理，使具有很少选路信息的主机逐渐建立较完善的路由表，从而找到最佳路由。但是由于重定向功能会在主机的路由表中增加主机路由，当增加的主机路由很多时，会降低主机性能。因此默认情况下设备的 ICMPv6 重定向报文发送功能是关闭的。

【举例】

开启设备的 ICMPv6 重定向报文发送功能。

```
<Sysname> system-view
[Sysname] ipv6 redirects enable
```

1.1.62 ipv6 temporary-address

ipv6 temporary-address 命令用来配置系统生成临时地址。

undo ipv6 temporary-address 命令用来恢复缺省情况。

【命令】

```
ipv6 temporary-address [ valid-lifetime preferred-lifetime ]
undo ipv6 temporary-address
```

【缺省情况】

系统不生成临时地址。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

valid-lifetime: 临时地址的有效生命期, 取值范围为 600~4294967295, 单位为秒, 缺省值为 604800 (7 天)。

preferred-lifetime: 临时地址的首选生命期, 取值范围为 600~4294967295, 单位为秒, 缺省值为 86400 (1 天)。*preferred-lifetime* 的值要小于等于 *valid-lifetime* 的值。

【使用指导】

配置本功能时需要打开地址无状态自动配置功能。

在配置了无状态自动配置 IPv6 地址功能后, 接口会根据接收到的 RA 报文中携带的地址前缀信息和接口 ID, 自动生成 IPv6 全球单播地址。如果接口是 IEEE 802 类型的接口 (例如, 以太网接口、VLAN 接口), 其接口 ID 是由 MAC 地址根据一定的规则生成, 此接口 ID 具有全球唯一性。对于不同的前缀, 接口 ID 部分始终不变, 攻击者通过接口 ID 可以很方便的识别出通信流量是由哪台设备产生的, 并分析其规律, 会造成一定的安全隐患。

如果在地址无状态自动配置时, 自动生成接口 ID 不断变化的 IPv6 地址, 就可以加大攻击的难度, 从而保护网络。为此, 设备提供了临时地址功能, 使得系统可以生成临时地址。

配置该功能后, 通过地址无状态自动配置, IEEE 802 类型的接口可以同时生成两类地址:

- 公共地址: 地址前缀采用 RA 报文携带的前缀, 接口 ID 由 MAC 地址产生。接口 ID 始终不变。
- 临时地址: 地址前缀采用 RA 报文携带的前缀, 接口 ID 由系统根据 MD5 算法计算产生。接口 ID 不断变化。

当临时地址的有效生命期过期后, 这个临时地址将被删除, 同时, 系统会通过 MD5 算法重新生成一个接口 ID 不同的临时地址。所以, 该接口发送报文的源地址的接口 ID 总是在不停变化。

配置的临时地址的有效生命期要大于或等于首选生命期。

临时地址的首选生命期是如下两个值之中的较小者:

- RA 前缀中的首选生命期
- 配置的临时地址首选生命期减去 DESYNC_FACTOR (DESYNC_FACTOR 是一个 0~600 秒的随机值)。

临时地址的有效生命期是如下两个值之中的较小者:

- RA 前缀中的有效生命期。
- 配置的临时地址有效生命期。

【举例】

配置系统生成临时地址。

```
<Sysname> system-view
[Sysname] ipv6 temporary-address
```

【相关命令】

- **ipv6 address auto**
- **ipv6 nd ra prefix**
- **ipv6 prefer temporary-address**

1.1.63 ipv6 unreachable enable

ipv6 unreachable enable 命令用来开启设备的 ICMPv6 目的不可达报文的发送功能。

undo ipv6 unreachableables enable 命令用来关闭设备的 ICMPv6 目的不可达报文的发送功能。

【命令】

```
ipv6 unreachableables enable
undo ipv6 unreachableables enable
```

【缺省情况】

ICMPv6 目的不可达报文发送功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

ICMPv6 目的不可达报文发送功能是在设备收到 IPv6 数据报文后，如果发生目的不可达的差错，则将报文丢弃并给源端发送 ICMPv6 目的不可达差错报文。

由于 ICMPv6 目的不可达报文传递给用户进程的信息为不可达信息，如果有用户恶意攻击，可能会影响终端用户的正常使用。为了避免上述现象发生，可以关闭设备的 ICMPv6 目的不可达报文发送功能，从而减少网络流量、防止遭到恶意攻击。

【举例】

开启设备的 ICMPv6 目的不可达报文发送功能。

```
<Sysname> system-view
[Sysname] ipv6 unreachableables enable
```

1.1.64 local-proxy-nd enable

local-proxy-nd enable 命令用来开启本地 ND Proxy 功能。

undo local-proxy-nd enable 命令用来关闭本地 ND Proxy 功能。

【命令】

```
local-proxy-nd enable
undo local-proxy-nd enable
```

【缺省情况】

本地 ND Proxy 功能处于关闭状态。

【视图】

VLAN 接口视图

【缺省用户角色】

network-admin

【举例】

在 VLAN 接口 100 上开启本地 ND Proxy 功能。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
```

```
[Sysname-Vlan-interface100] local-proxy-nd enable
```

【相关命令】

- **proxy-nd enable**

1.1.65 proxy-nd enable

proxy-nd enable 命令用来开启 ND Proxy 功能。

undo proxy-nd enable 命令用来关闭 ND Proxy 功能。

【命令】

```
proxy-nd enable
undo proxy-nd enable
```

【缺省情况】

ND Proxy 功能处于关闭状态。

【视图】

VLAN 接口视图

【缺省用户角色】

network-admin

【举例】

在 VLAN 接口 100 上开启 ND Proxy 功能。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] proxy-nd enable
```

【相关命令】

- **local-proxy-nd enable**

1.1.66 reset ipv6 nd snooping

reset ipv6 nd snooping 命令用来清除设备的 ND Snooping 表项。

【命令】

```
reset ipv6 nd snooping [ [ vlan vlan-id ] [ global | link-local ] | vlan vlan-id
ipv6-address ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

vlan *vlan-id*: 清除指定 VLAN 内的 ND Snooping 表项。*vlan-id* 表示 VLAN ID，取值范围为 1~4094。

global: 清除表项地址类型为全局单播地址的 ND Snooping 表项。

link-local: 清除表项地址类型为链路本地地址的 ND Snooping 表项。

vlan vlan-id ipv6-address: 清除指定 VLAN 内的指定 IPv6 地址的 ND Snooping 表项。
vlan-id 表示 VLAN ID, 取值范围为 1~4094。

【举例】

清除设备上的 ND Snooping 表项。

```
<Sysname> reset ipv6 nd snooping
```

1.1.67 reset ipv6 neighbors

reset ipv6 neighbors 命令用来清除 IPv6 邻居信息。

【命令】

```
reset ipv6 neighbors { all | dynamic | interface interface-type  
interface-number | slot slot-number | static }
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

all: 清除所有接口上的静态与动态邻居信息。

dynamic: 清除所有接口上的动态邻居信息。

interface interface-type interface-number: 清除指定接口上的动态邻居信息。
interface-type interface-number 为接口类型和接口编号

slot slot-number: 清除指定成员设备的动态邻居信息。slot-number 表示设备在 IRF 中的成员编号。如果未指定本参数, 则清除所有成员设备上的动态邻居信息。

static: 清除所有接口上的静态邻居信息。

【举例】

清除所有接口上的所有邻居信息。

```
<Sysname> reset ipv6 neighbors all
```

```
This will delete all the entries. Continue? [Y/N]:Y
```

清除所有接口上的动态邻居信息。

```
<Sysname> reset ipv6 neighbors dynamic
```

```
This will delete all the dynamic entries. Continue? [Y/N]:Y
```

清除接口 GigabitEthernet1/0/1 上的所有邻居信息。

```
<Sysname> reset ipv6 neighbors interface gigabitethernet 1/0/1
```

```
This will delete all the dynamic entries by the interface you specified. Continue? [Y/N]:Y
```

【相关命令】

- **display ipv6 neighbors**
- **ipv6 neighbor**

1.1.68 reset ipv6 pathmtu

reset ipv6 pathmtu 命令用来清除 PMTU 信息。

【命令】

```
reset ipv6 pathmtu { all | dynamic | static }
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

all: 清空所有的 PMTU 信息。

dynamic: 清空所有动态创建的 PMTU 信息。

static: 清空所有的静态 PMTU 信息。

【举例】

清除所有 PMTU 信息。

```
<Sysname> reset ipv6 pathmtu all
```

【相关命令】

- **display ipv6 pathmtu**

1.1.69 reset ipv6 statistics

reset ipv6 statistics 命令用来清除 IPv6 报文及 ICMPv6 报文的统计信息。

【命令】

```
reset ipv6 statistics [ slot slot-number ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

slot slot-number: 清除指定成员设备的 IPv6 报文及 ICMPv6 报文统计信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则清除所有成员设备上的 IPv6 报文及 ICMPv6 报文统计信息。

【举例】

清除 IPv6 报文及 ICMPv6 报文的统计信息。

```
<Sysname> reset ipv6 statistics
```

【相关命令】

- **display ipv6 statistics**

目 录

1 DHCPv6	1-1
1.1 DHCPv6 公共命令	1-1
1.1.1 display ipv6 dhcp duid	1-1
1.1.2 ipv6 dhcp advertise pd-route	1-1
1.1.3 ipv6 dhcp dscp	1-2
1.1.4 ipv6 dhcp log enable	1-3
1.1.5 ipv6 dhcp select	1-3
1.2 DHCPv6 服务器配置命令	1-4
1.2.1 address range	1-4
1.2.2 address-alloc-mode eui-64	1-5
1.2.3 class pool	1-6
1.2.4 default pool	1-7
1.2.5 display ipv6 dhcp option-group	1-8
1.2.6 display ipv6 dhcp pool	1-10
1.2.7 display ipv6 dhcp prefix-pool	1-12
1.2.8 display ipv6 dhcp server	1-14
1.2.9 display ipv6 dhcp server conflict	1-15
1.2.10 display ipv6 dhcp server database	1-16
1.2.11 display ipv6 dhcp server expired	1-16
1.2.12 display ipv6 dhcp server ip-in-use	1-17
1.2.13 display ipv6 dhcp server pd-in-use	1-19
1.2.14 display ipv6 dhcp server statistics	1-21
1.2.15 dns-server	1-23
1.2.16 domain-name	1-24
1.2.17 if-match	1-24
1.2.18 ipv6 dhcp apply-policy	1-27
1.2.19 ipv6 dhcp class	1-27
1.2.20 ipv6 dhcp option-group	1-28
1.2.21 ipv6 dhcp policy	1-29
1.2.22 ipv6 dhcp pool	1-30
1.2.23 ipv6 dhcp prefix-pool	1-30
1.2.24 ipv6 dhcp server	1-32
1.2.25 ipv6 dhcp server apply pool	1-33

1.2.26	ipv6 dhcp server database filename	1-34
1.2.27	ipv6 dhcp server database update interval	1-35
1.2.28	ipv6 dhcp server database update now	1-36
1.2.29	ipv6 dhcp server database update stop	1-37
1.2.30	ipv6 dhcp server forbidden-address	1-37
1.2.31	ipv6 dhcp server forbidden-prefix	1-38
1.2.32	network	1-39
1.2.33	option	1-41
1.2.34	option-group	1-42
1.2.35	prefix-pool	1-43
1.2.36	reset ipv6 dhcp server conflict	1-44
1.2.37	reset ipv6 dhcp server expired	1-45
1.2.38	reset ipv6 dhcp server ip-in-use	1-45
1.2.39	reset ipv6 dhcp server pd-in-use	1-46
1.2.40	reset ipv6 dhcp server statistics	1-47
1.2.41	sip-server	1-47
1.2.42	static-bind	1-48
1.2.43	temporary address range	1-49
1.3	DHCPv6 中继配置命令	1-51
1.3.1	display ipv6 dhcp relay server-address	1-51
1.3.2	display ipv6 dhcp relay statistics	1-52
1.3.3	gateway-list	1-54
1.3.4	ipv6 dhcp relay gateway	1-55
1.3.5	ipv6 dhcp relay interface-id	1-55
1.3.6	ipv6 dhcp relay server-address	1-56
1.3.7	ipv6 dhcp relay source-address	1-57
1.3.8	remote-server	1-58
1.3.9	reset ipv6 dhcp relay statistics	1-59
1.4	DHCPv6 客户端配置命令	1-60
1.4.1	display ipv6 dhcp client	1-60
1.4.2	display ipv6 dhcp client statistics	1-62
1.4.3	ipv6 address dhcp-alloc	1-63
1.4.4	ipv6 dhcp client dscp	1-64
1.4.5	ipv6 dhcp client duid	1-65
1.4.6	ipv6 dhcp client pd	1-66
1.4.7	ipv6 dhcp client stateful	1-67

1.4.8 ipv6 dhcp client stateless enable.....	1-68
1.4.9 reset ipv6 dhcp client statistics.....	1-68
1.5 DHCPv6 Snooping配置命令.....	1-69
1.5.1 display ipv6 dhcp snooping binding.....	1-69
1.5.2 display ipv6 dhcp snooping binding database	1-70
1.5.3 display ipv6 dhcp snooping packet statistics	1-71
1.5.4 display ipv6 dhcp snooping pd binding	1-72
1.5.5 display ipv6 dhcp snooping trust	1-73
1.5.6 ipv6 dhcp snooping binding database filename	1-74
1.5.7 ipv6 dhcp snooping binding database update interval	1-75
1.5.8 ipv6 dhcp snooping binding database update now	1-76
1.5.9 ipv6 dhcp snooping binding record	1-77
1.5.10 ipv6 dhcp snooping check request-message	1-77
1.5.11 ipv6 dhcp snooping deny	1-78
1.5.12 ipv6 dhcp snooping enable.....	1-79
1.5.13 ipv6 dhcp snooping log enable.....	1-79
1.5.14 ipv6 dhcp snooping option interface-id enable	1-80
1.5.15 ipv6 dhcp snooping option interface-id string.....	1-81
1.5.16 ipv6 dhcp snooping option remote-id enable	1-81
1.5.17 ipv6 dhcp snooping option remote-id string.....	1-82
1.5.18 ipv6 dhcp snooping pd binding record.....	1-83
1.5.19 ipv6 dhcp snooping rate-limit	1-84
1.5.20 ipv6 dhcp snooping trust.....	1-84
1.5.21 reset ipv6 dhcp snooping binding.....	1-85
1.5.22 reset ipv6 dhcp snooping packet statistics	1-86
1.5.23 reset ipv6 dhcp snooping pd binding	1-86

1 DHCPv6

1.1 DHCPv6公共命令

1.1.1 display ipv6 dhcp duid

display ipv6 dhcp duid 命令用来显示本设备的 DUID。

【命令】

display ipv6 dhcp duid

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【使用指导】

DUID（DHCP Unique Identifier，DHCP 唯一标识符）是一台 DHCPv6 设备（包括客户端、服务器和中继）的唯一标识。在 DHCPv6 报文交互过程中，DHCPv6 客户端、服务器和中继通过在报文中添加 DUID 来标识自己。

只有在设备上开启 DHCPv6 进程，配置本命令才会有显示信息。

【举例】

```
# 显示本设备的 DUID。  
<Sysname> display ipv6 dhcp duid  
The DUID of this device: 0003000100e0fc005552.
```

1.1.2 ipv6 dhcp advertise pd-route

ipv6 dhcp advertise pd-route 命令用来开启 DHCPv6 服务器或 DHCPv6 中继发布前缀路由功能。

undo ipv6 dhcp advertise pd-route 命令用来关闭 DHCPv6 服务器或 DHCPv6 中继发布前缀路由功能。

【命令】

ipv6 dhcp advertise pd-route
undo ipv6 dhcp advertise pd-route

【缺省情况】

DHCPv6 服务器或 DHCPv6 中继发布前缀路由功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

DHCPv6 客户端获取到 IPv6 前缀后，通过该 IPv6 前缀给下行网络内的主机分配 IPv6 地址。此时，DHCPv6 客户端与网络内的主机不在同一网段，会导致主机无法与外界通信。为了解决这个问题，需要在 DHCPv6 服务器或 DHCPv6 中继上开启发布前缀路由功能。需要注意的是：

- DHCPv6 服务器和 DHCPv6 客户端在同一个链路范围内，需要在 DHCPv6 服务器上开启发布前缀路由功能；
- DHCPv6 服务器和 DHCPv6 客户端不在同一个链路范围内，需要在和 DHCPv6 客户端处于同一个链路范围内的 DHCPv6 中继上开启发布前缀路由功能。

开启 DHCPv6 中继发布前缀路由功能前，需要先开启 DHCPv6 中继用户表项记录功能。

【举例】

开启 DHCPv6 服务器发布前缀路由功能。

```
<Sysname> system-view  
[Sysname] ipv6 dhcp advertise pd-route
```

1.1.3 ipv6 dhcp dscp

ipv6 dhcp dscp 命令用来配置 DHCPv6 服务器或 DHCPv6 中继发送 DHCPv6 报文的 DSCP 优先级。

undo ipv6 dhcp dscp 命令用来恢复缺省情况。

【命令】

```
ipv6 dhcp dscp dscp-value  
undo ipv6 dhcp dscp
```

【缺省情况】

DHCPv6 服务器或 DHCPv6 中继发送 DHCPv6 报文的 DSCP 优先级为 56。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

dscp-value：IPv6 DHCP 报文的 DSCP 优先级，取值范围为 0～63。

【使用指导】

DSCP 优先级用来体现报文自身的优先等级，决定报文传输的优先程度。配置的 DSCP 优先级的取值越大，报文的优先级越高。

【举例】

配置 DHCPv6 服务器或 DHCPv6 中继发送的 DHCPv6 报文的 DSCP 优先级为 30。

```
<Sysname> system-view
```

```
[Sysname] ipv6 dhcp dscp 30
```

1.1.4 ipv6 dhcp log enable

ipv6 dhcp log enable 命令用来开启 DHCPv6 服务器日志信息功能。

undo ipv6 dhcp log enable 命令用来关闭 DHCPv6 服务器日志信息功能。

【命令】

```
ipv6 dhcp log enable
undo ipv6 dhcp log enable
```

【缺省情况】

DHCPv6 服务器日志信息功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

DHCPv6 服务器日志可以方便管理员定位问题和解决问题。设备生成 DHCPv6 日志信息会交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

比如大量 DHCPv6 客户端发生上下线操作时，DHCPv6 服务器需要输出大量日志信息，这可能会降低设备性能，影响 DHCPv6 服务器分配 IPv6 前缀或 IPv6 地址的速度。为了避免该情况的发生，用户可以关闭 DHCPv6 服务器日志信息功能，使得 DHCPv6 服务器不再输出日志信息。

【举例】

开启 DHCPv6 服务器日志信息功能。

```
<Sysname> system-view
[Sysname] ipv6 dhcp log enable
```

1.1.5 ipv6 dhcp select

ipv6 dhcp select 命令用来配置接口工作在 DHCPv6 服务器或 DHCPv6 中继模式。

undo ipv6 dhcp select 命令用来恢复缺省情况。

【命令】

```
ipv6 dhcp select { relay | server }
undo ipv6 dhcp select
```

【缺省情况】

接口未工作在 DHCPv6 服务器模式，也未工作在 DHCPv6 中继模式，接口接收到 DHCPv6 客户端发来的 DHCPv6 报文后，丢弃该报文。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

relay: 配置接口工作在 DHCPv6 中继模式。

server: 配置接口工作在 DHCPv6 服务器模式。

【使用指导】

当接口从 DHCPv6 服务器模式切换到 DHCPv6 中继模式时，设备不会删除 IPv6 地址/前缀绑定信息。建议接口从 DHCPv6 服务器模式切换到 DHCPv6 中继模式时，通过 **reset ipv6 dhcp server ip-in-use** 命令和 **reset ipv6 dhcp server pd-in-use** 命令清除已有的 IPv6 地址/前缀绑定信息。

建议不要在一个接口上同时配置 DHCPv6 客户端和 DHCPv6 中继/服务器功能。

【举例】

配置 VLAN 接口 10 工作在 DHCPv6 服务器模式。

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ipv6 dhcp select server
```

配置 VLAN 接口 20 工作在 DHCPv6 中继模式。

```
<Sysname> system-view
[Sysname] interface vlan-interface 20
[Sysname-Vlan-interface20] ipv6 dhcp select relay
```

【相关命令】

- **display ipv6 dhcp relay server-address**
- **display ipv6 dhcp server**

1.2 DHCPv6服务器配置命令



说明

S5110V2-SI 和 S5000V3-EI 系列交换机不支持本特性。

1.2.1 address range

address range 命令用来配置地址池中动态分配的 IPv6 非临时地址范围。

undo address range 命令用来恢复缺省情况。

【命令】

```
address range start-ipv6-address end-ipv6-address [ preferred-lifetime
preferred-lifetime valid-lifetime valid-lifetime ]
undo address range
```

【缺省情况】

未配置地址池中动态分配的 IPv6 非临时地址范围，通过 **network** 命令指定的网段内的单播地址都可以作为非临时地址分配给客户端。

【视图】

DHCPv6 地址池视图

【缺省用户角色】

network-admin

【参数】

start-ipv6-address: 动态分配的起始 IPv6 非临时地址。

end-ipv6-address: 动态分配的结束 IPv6 非临时地址。

preferred-lifetime preferred-lifetime: 指定地址池中分配的 IPv6 非临时地址的首选生命周期。*preferred-lifetime* 为非临时地址的首选生命周期，取值范围为 60~4294967295，单位为秒，缺省值为 604800（7 天）。

valid-lifetime valid-lifetime: 指定地址池中分配的 IPv6 非临时地址的有效生命周期。*valid-lifetime* 为非临时地址的有效生命周期，取值范围为 60~4294967295，单位为秒，缺省值为 2592000（30 天）。*valid-lifetime* 必须大于或等于 *preferred-lifetime*。

【使用指导】

如果未在地址池下通过 **address range** 命令配置动态分配的 IPv6 非临时地址范围，则 **network** 命令指定的网段内的单播地址都可以分配给 DHCPv6 客户端。如果配置了 **address range** 命令，则只会从该地址范围内分配 IPv6 非临时地址，即使该范围内的地址分配完毕，也不会从 **network** 命令指定的地址范围内分配 IPv6 非临时地址。

一个地址池下只能配置一个 IPv6 非临时地址范围，多次执行本命令，最后一次执行的命令生效。

address range 命令配置动态分配的 IPv6 非临时地址范围必须在 **network** 命令指定的网段内，否则无法分配。

【举例】

配置地址池 1 动态分配的 IPv6 非临时地址范围为 3ffe:501:ffff:100::10 到 3ffe:501:ffff:100::31。

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] network 3ffe:501:ffff:100::/64
[Sysname-dhcp6-pool-1] address range 3ffe:501:ffff:100::10 3ffe:501:ffff:100::31
```

【相关命令】

- **display ipv6 dhcp pool**
- **network**
- **temporary address range**

1.2.2 address-alloc-mode eui-64

address-alloc-mode eui-64 命令用来配置 DHCPv6 地址池按照 EUI-64 方式分配 IPv6 地址。

undo address-alloc-mode eui-64 命令用来恢复缺省情况。

【命令】

```
address-alloc-mode eui-64
undo address-alloc-mode eui-64
```

【缺省情况】

DHCPv6 地址池不按照 EUI-64 方式分配 IPv6 地址。

【视图】

DHCPv6 地址池视图

【缺省用户角色】

network-admin

【使用指导】

配置本功能后，之前已经分配的 IPv6 地址租约不受影响。

只有在动态分配的 IPv6 地址网段的前缀长度不超过 64 的 DHCPv6 地址池中配置本功能才生效。

因为 DHCPv6 服务器只能从 DHCP 请求报文的链路层报文头中获取到客户端的 MAC 地址信息，所以在 DHCPv6 客户端通过 DHCPv6 中继向 DHCPv6 服务器获取地址的网络环境中，无法配置本功能。

【举例】

配置 DHCPv6 地址池 pool1 按照 EUI-64 方式分配 IPv6 地址。

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool pool1
[Sysname-dhcp6-pool-pool1] address-alloc-mode eui-64
```

1.2.3 class pool

class pool 命令用来指定 DHCPv6 用户类关联的 DHCPv6 地址池。

undo class pool 命令用来恢复缺省情况。

【命令】

```
class class-name pool pool-name
undo class class-name pool
```

【缺省情况】

未指定 DHCPv6 用户类关联的 DHCPv6 地址池。

【视图】

DHCPv6 策略视图

【缺省用户角色】

network-admin

【参数】

class-name: DHCPv6 用户类名称，为 1~63 个字符的字符串，不区分大小写。

pool-name: DHCPv6 地址池名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

对于一个 DHCPv6 用户类，在一个 DHCPv6 策略中只能关联一个 DHCPv6 地址池。
多次执行本命令为同一个 DHCPv6 用户类关联不同的 DHCPv6 地址池，最后一次执行的命令生效。

【举例】

在 DHCPv6 策略 1 中，配置 DHCPv6 用户类 test 关联 DHCPv6 地址池 pool1。

```
<Sysname> system-view
[Sysname] ipv6 dhcp policy 1
[Sysname-dhcp6-policy-1] class test pool pool1
```

【相关命令】

- **default pool**
- **ipv6 dhcp policy**
- **ipv6 dhcp pool**

1.2.4 default pool

default pool 命令用来指定默认 DHCPv6 地址池。

undo default pool 命令用来恢复缺省情况。

【命令】

```
default pool pool-name
undo default pool
```

【缺省情况】

未指定默认 DHCPv6 地址池。

【视图】

DHCPv6 策略视图

【缺省用户角色】

network-admin

【参数】

pool-name：默认 DHCPv6 地址池名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

若匹配 DHCPv6 策略中的所有 DHCPv6 用户类失败，当配置了默认 DHCPv6 地址池时，则从该地址池中分配 IPv6 地址和其他参数；当未配置默认 DHCPv6 地址池或默认 DHCPv6 地址池中不存在可供分配的地址信息时，IPv6 地址和其他参数分配失败。

在一个 DHCPv6 策略视图中，只能配置一个默认 DHCPv6 地址池。多次执行本命令，最后一次执行的命令生效。

【举例】

在 DHCPv6 策略 1 中指定默认 DHCPv6 地址池 pool1。

```
<Sysname> system-view
[Sysname] ipv6 dhcp policy 1
```

```
[Sysname-dhcp6-policy-1] default pool pool1
```

【相关命令】

- `class pool`
- `ipv6 dhcp policy`

1.2.5 display ipv6 dhcp option-group

`display ipv6 dhcp option-group` 命令用来显示 DHCPv6 选项组信息。

【命令】

```
display ipv6 dhcp option-group [ option-group-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

option-group-number：显示指定 DHCPv6 选项组的信息。*option-group-number* 为 DHCPv6 选项组编号，取值范围为 1~100。如果未指定本参数，则显示所有 DHCPv6 选项组的信息，包括静态和动态 DHCPv6 选项组。

【使用指导】

静态 DHCPv6 选项组指的是通过 `ipv6 dhcp option-group` 命令创建的选项组。

动态 DHCPv6 选项组指的是设备作为 DHCPv6 客户端获取到 DHCPv6 选项后，自动创建的选项组。
不允许手工修改或删除动态 DHCPv6 选项组。

【举例】

显示所有 DHCPv6 选项组的信息。

```
<Sysname> display ipv6 dhcp option-group
DHCPv6 option group: 1
  DNS server addresses:
    Type: Static
    Interface: N/A
    1::1
  DNS server addresses:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: Vlan-interface10
    1::1
  Domain name:
    Type: Static
    Interface: N/A
    aaa.com
  Domain name:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: Vlan-interface10
```

```

aaa.com
Options:
  Code: 23
    Type: Dynamic (DHCPv6 prefix allocation)
    Interface: Vlan-interface10
    Length: 2 bytes
    Hex: ABCD
DHCPv6 option group: 20
  DNS server addresses:
    Type: Static
    Interface: N/A
    1::1
  DNS server addresses:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: Vlan-interface10
    1::1
  Domain name:
    Type: Static
    Interface: N/A
    aaa.com
  Domain name:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: Vlan-interface10
    aaa.com
Options:
  Code: 23
    Type: Dynamic (DHCPv6 prefix allocation)
    Interface: Vlan-interface10
    Length: 2 bytes
    Hex: ABCD

```

表1-1 display ipv6 dhcp option-group 命令显示信息描述表

字段	描述
DHCPv6 option group	DHCPv6选项组编号
Type	DHCPv6选项的类型，取值包括： <ul style="list-style-type: none"> • Static: 表示静态 DHCPv6 选项 • Dynamic (DHCPv6 address allocation): 表示动态地址申请得到的 DHCPv6 选项 • Dynamic (DHCPv6 prefix allocation): 表示动态前缀申请得到的 DHCPv6 选项 • Dynamic (DHCPv6 address and prefix allocation): 表示同时申请地址、前缀时得到的 DHCPv6 选项
Interface	接口名
DNS server addresses	DNS服务器地址
Domain name	域名后缀

字段	描述
SIP server addresses	SIP服务器地址
SIP server domain names	SIP服务器域名
Options	自定义选项
Code	自定义选项编码
Length	自定义选项长度，单位为字节
Hex	自定义选项内容，以十六进制数表示

【相关命令】

- `ipv6 dhcp option-group`

1.2.6 display ipv6 dhcp pool

`display ipv6 dhcp pool` 命令用来显示 DHCPv6 地址池的信息。

【命令】

`display ipv6 dhcp pool [pool-name]`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

pool-name：显示指定 DHCPv6 地址池的信息。*pool-name* 表示 DHCPv6 地址池名称，为 1～63 个字符的字符串，不区分大小写。如果未指定本参数，则显示所有 DHCPv6 地址池的信息。

【举例】

显示指定 DHCPv6 地址池的信息。

```
<Sysname> display ipv6 dhcp pool 1
DHCPv6 pool: 1
  Network: 3FFE:501:FFFF:100::/64
  Preferred lifetime 604800, valid lifetime 2592000
  Prefix pool: 1
    Preferred lifetime 24000, valid lifetime 36000
  Addresses:
    Range: from 3FFE:501:FFFF:100::1
           to 3FFE:501:FFFF:100::99
    Preferred lifetime 70480, valid lifetime 200000
    Total address number: 153
    Available: 153
    In-use: 0
  Temporary addresses:
```

```

Range: from 3FFE:501:FFFF:100::200
      to 3FFE:501:FFFF:100::210
Preferred lifetime 60480, valid lifetime 259200
Total address number: 17
Available: 17
In-use: 0
Static bindings:
  DUID: 0003000100e0fc000001
  IAID: 0000003f
  Prefix: 3FFE:501:FFFF:200::/64
    Preferred lifetime 604800, valid lifetime 2592000
  DUID: 0003000100e0fc00c0ff1
  IAID: 00000001
  Address: 3FFE:501:FFFF:2001::1/64
    Preferred lifetime 604800, valid lifetime 2592000
DNS server addresses:
  2::2
Domain name:
  aaa.com
SIP server addresses:
  5::1
SIP server domain names:
  bbb.com

```

显示指定 DHCPv6 地址池的信息，地址池引用了未生效前缀。

```

<Sysname> display ipv6 dhcp pool 1
DHCPv6 pool: 1
  Network: Not-available
  Preferred lifetime 604800, valid lifetime 2592000

```

#显示指定 DHCPv6 地址池的信息，此时设备配置恢复后地址池引用的前缀未生效。

```

<Sysname> display ipv6 dhcp pool 1
DHCPv6 pool: 1
  Network: 1::/64(Zombie)
  Preferred lifetime 604800, valid lifetime 2592000

```

表1-2 display ipv6 dhcp pool 命令详细显示信息描述表

字段	描述
DHCPv6 pool	DHCPv6地址池名称
Network	DHCPv6地址池中用于动态分配的IPv6地址网段。如果引用了未生效的前缀，则显示为Not-available；如果配置恢复后（如主备倒换）对应引用的前缀未生效，处于僵死状态，则显示为(Zombie)
Prefix pool	地址池引用的前缀池索引
Preferred lifetime	租约首选生命期，单位为秒
valid lifetime	租约有效生命期，单位为秒
Addresses	用于动态分配的IPv6非临时地址信息

字段	描述
Range	用于动态分配的IPv6地址范围
Total address number	可供分配的地址总数
Available	空闲的地址总数
In-use	已分配的地址总数
Temporary addresses	用于动态分配的IPv6临时地址信息
Static bindings	静态绑定的IPv6地址或前缀信息
DUID	静态绑定的客户端DUID
IAID	静态绑定的客户端IAID，未配置则显示为Not configured
Prefix	静态绑定的IPv6前缀
Address	静态绑定的IPv6地址
DNS server addresses	为客户端分配的DNS服务器地址
Domain name	为客户端分配的域名
SIP server addresses	为客户端分配的SIP服务器地址
SIP server domain names	为客户端分配的SIP服务器域名

1.2.7 display ipv6 dhcp prefix-pool

display ipv6 dhcp prefix-pool 命令用来显示前缀池的信息。

【命令】

display ipv6 dhcp prefix-pool [*prefix-pool-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

prefix-pool-number：显示指定前缀池的详细信息。*prefix-pool-number* 为前缀池索引，取值范围 1~128。如果未指定该参数，则显示所有前缀池的简要信息。

【举例】

显示所有前缀池的简要信息。

```
<Sysname> display ipv6 dhcp prefix-pool
Prefix-pool Prefix Available In-use Static
1 5::/64 64 0 0
```

显示所有前缀池的简要信息，引用的是未生效前缀。

```
<Sysname> display ipv6 dhcp prefix-pool
```

```
Prefix-pool Prefix Available In-use Static
2 Not-available 0 0 0
```

#显示所有前缀池的简要信息，此时设备配置恢复后前缀池引用的前缀未生效。

```
<Sysname> display ipv6 dhcp prefix-pool
```

```
Prefix-pool Prefix Available In-use Static
11 21::/112(Zombie) 0 64 0
```

显示前缀池 1 的详细信息。

```
<Sysname> display ipv6 dhcp prefix-pool 1
```

```
Prefix: 5::/64
```

```
Assigned length: 70
```

```
Total prefix number: 64
```

```
Available: 64
```

```
In-use: 0
```

```
Static: 0
```

显示前缀池 1 引用未生效前缀的详细信息。

```
<Sysname> display ipv6 dhcp prefix-pool 1
```

```
Prefix: Not-available
```

```
Assigned length: 70
```

```
Total prefix number: 0
```

```
Available: 0
```

```
In-use: 0
```

```
Static: 0
```

显示前缀池 1 引用生效前缀进程重启配置恢复后引用前缀未激活的详细信息。

```
<Sysname> display ipv6 dhcp prefix-pool 1
```

```
Prefix: 5::/64(Zombie)
```

```
Assigned length: 70
```

```
Total prefix number: 10
```

```
Available: 0
```

```
In-use: 10
```

```
Static: 0
```

表1-3 display ipv6 dhcp prefix-pool 命令显示信息描述表

字段	描述
Prefix-pool	前缀池索引
Prefix	前缀池中配置的前缀。如果引用了未生效的前缀，则显示为 Not-available ；如果配置恢复后（如主备倒换）对应引用的前缀未生效，处于僵死状态，则显示为 (Zombie)
Available	空闲的前缀数量
In-use	已分配的前缀数量
Static	静态绑定的前缀数量
Assigned length	分配的前缀长度
Total prefix number	可供分配的前缀数量

1.2.8 display ipv6 dhcp server

display ipv6 dhcp server 命令用来显示接口上的 DHCPv6 服务器信息。

【命令】

display ipv6 dhcp server [**interface** *interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface interface-type interface-number: 显示指定接口的 DHCPv6 服务器信息。
其中, *interface-type interface-number* 为接口类型和接口编号。如果未指定该参数, 则显示所有接口的 DHCPv6 服务器信息。

【举例】

显示所有接口的 DHCPv6 服务器相关信息。

```
<Sysname> display ipv6 dhcp server
Interface                Pool
Vlan-interface2          1
Vlan-interface3          global
```

显示 VLAN 接口 2 的 DHCPv6 服务器相关信息。

```
<Sysname> display ipv6 dhcp server interface vlan-interface 2
Using pool: 1
Preference value: 0
Allow-hint: Enabled
Rapid-commit: Disabled
```

表1-4 display ipv6 dhcp server 命令显示信息描述表

字段	描述
Interface	工作在DHCPv6服务器模式的接口
Pool	接口引用的地址池, 如果显示为global, 则表示接口上未引用某个地址池, 分配地址、前缀和其他网络参数时全局动态选择地址池
Using pool	接口引用的地址池, 如果显示为global, 则表示接口上未引用某个地址池, 分配地址、前缀和其他网络参数时全局动态选择地址池
Preference value	服务器优先级, 取值为0~255, 该值越大, 表示服务器的优先级越高
Allow-hint	是否支持优先为客户端分配其期望的地址和前缀: <ul style="list-style-type: none">• Enabled: 表示支持优先为客户端分配其期望的地址和前缀• Disabled: 表示忽略客户端期望的地址和前缀
Rapid-commit	是否支持地址和前缀快速分配功能: <ul style="list-style-type: none">• Enabled: 表示配置了地址和前缀快速分配功能

字段	描述
	<ul style="list-style-type: none"> Disabled: 表示未配置地址和前缀快速分配功能

1.2.9 display ipv6 dhcp server conflict

display ipv6 dhcp server conflict 命令用来显示 DHCPv6 的地址冲突信息。

【命令】

display ipv6 dhcp server conflict [**address** *ipv6-address*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

address *ipv6-address*: 显示指定 IPv6 地址的地址冲突信息。如果未指定本参数，则显示所有 IPv6 地址的地址冲突信息。

【使用指导】

DHCPv6 服务器在下列几种情况下会产生地址冲突信息：

- DHCPv6 客户端向 DHCPv6 服务器发送 Decline 报文，通知 DHCPv6 服务器为其分配的地址存在冲突。
- DHCPv6 服务器检测到地址池内的可供分配的地址是设备自身的地址。

【举例】

显示所有的地址冲突信息。

```
<Sysname> display ipv6 dhcp server conflict
IPv6 address          Detect time
2001::1               Apr 25 16:57:20 2007
1::1:2               Apr 25 17:00:10 2007
```

表1-5 display ipv6 dhcp server conflict 命令显示信息描述表

字段	描述
IPv6 address	发生冲突的IPv6地址
Detect time	检测到冲突的时间

【相关命令】

- reset ipv6 dhcp server conflict**

1.2.10 display ipv6 dhcp server database

display ipv6 dhcp server database 命令用来显示 DHCPv6 服务器的表项备份信息。

【命令】

display ipv6 dhcp server database

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

显示 DHCPv6 服务器表项备份信息。

```
<Sysname> display ipv6 dhcp server database
File name           : database.dhcp
Username            :
Password            :
Update interval     : 600 seconds
Latest write time    : Feb  8 16:02:23 2014
Status              : Last write succeeded.
```

表1-6 display ipv6 dhcp server database 命令显示信息描述表

字段	描述
File name	存储DHCPv6服务器表项的文件名称
Username	配置远程目标文件时的用户名
Password	配置远程目标文件时的密码，有配置时显示为“*****”
Update interval	定期刷新表项存储文件的刷新时间间隔，单位为秒
Latest write time	最近一次写文件的时间
Status	写文件时的状态 <ul style="list-style-type: none">Writing: 正在写文件Last write succeeded.: 上一次写文件成功Last write failed.: 上一次写文件失败

1.2.11 display ipv6 dhcp server expired

display ipv6 dhcp server expired 命令用来显示租约过期的 DHCPv6 地址绑定信息。

【命令】

display ipv6 dhcp server expired [**address** *ipv6-address* | **pool** *pool-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

address *ipv6-address*: 显示指定 IPv6 地址的租约过期地址绑定信息。如果未指定本参数，则显示所有 IPv6 地址的租约过期地址绑定信息。

pool *pool-name*: 显示指定地址池中租约过期的地址绑定信息。*pool-name* 表示地址池名称，为 1~63 个字符的字符串，不区分大小写。如果未指定本参数，则显示所有地址池中租约过期的地址绑定信息。

【使用指导】

在 DHCPv6 地址池的可用地址分配完后，租约过期的地址将被分配给 DHCPv6 客户端。

【举例】

显示所有 DHCPv6 地址池中租约过期的地址绑定信息。

```
<Sysname> display ipv6 dhcp server expired
```

IPv6 address	DUID	Lease expiration
2001:3eff:fe80:4caa:	3030-3066-2e65-3230-302e-	Apr 25 17:10:47 2007
37ee:7::1	3130-3234-2d45-7468-6572-	
	6e65-7430-2f31	

表1-7 display dhcp server expired 命令显示信息描述表

字段	描述
IPv6 address	租约过期的IPv6地址
DUID	租约过期的客户端的DUID
Lease expiration	租约过期的时间

【相关命令】

- **reset ipv6 dhcp server expired**

1.2.12 display ipv6 dhcp server ip-in-use

display ipv6 dhcp server ip-in-use 命令用来显示 DHCPv6 地址绑定信息。

【命令】

display ipv6 dhcp server ip-in-use [**address** *ipv6-address* | **pool** *pool-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

address *ipv6-address*: 显示指定 IPv6 地址的地址绑定信息。如果未指定本参数，则显示所有 IPv6 地址的地址绑定信息。

pool *pool-name*: 显示指定 DHCPv6 地址池的地址绑定信息。*pool-name* 表示 DHCPv6 地址池名称，为 1~63 个字符的字符串，不区分大小写。如果未指定本参数，则显示所有地址池中地址绑定信息。

【举例】

显示所有的 DHCPv6 地址绑定信息。

```
<Sysname> display ipv6 dhcp server ip-in-use
Pool: 1
  IPv6 address      Type      Lease expiration
  2:1::1            Auto(O)   Jul 10 19:45:01 2008
Pool: 2
  IPv6 address      Type      Lease expiration
  1:1::2            Static(F) Not available
Pool: 3
  IPv6 address      Type      Lease expiration
  1:2::1F1          Static(O) Oct  9 09:23:31 2008
Pool: 4
  IPv6 address      Type      Lease expiration
  1:2::2            Auto(Z)   Oct  11 09:23:31 2008
```

显示指定 DHCPv6 地址池的地址绑定信息。

```
<Sysname> display ipv6 dhcp server ip-in-use pool 1
Pool: 1
  IPv6 address      Type      Lease expiration
  2:1::1            Auto(O)   Jul 10 22:22:22 2008
  3:1::2            Static(C) Jan  1 11:11:11 2008
```

显示指定 IPv6 地址的地址绑定信息。

```
<Sysname> display ipv6 dhcp server ip-in-use address 2:1::3
Pool: 1
Client: FE80::C800:CFF0:FE18:0
Type: Auto(O)
DUID: 00030001CA000C180000
IAID: 0x00030001
  IPv6 address: 2:1::3
  Preferred lifetime 400, valid lifetime 500
  Expires at Jul 10 09:45:01 2008 (288 seconds left)
```

表1-8 display ipv6 dhcp server ip-in-use 命令显示信息描述表

字段	描述
Pool	地址绑定信息所属的地址池
IPv6 address	已分配的IPv6地址
Type	IPv6地址绑定的类型，取值包括： <ul style="list-style-type: none">Static(F): 表示尚未分配给客户端的静态绑定（Free），即静态

字段	描述
	无效绑定 <ul style="list-style-type: none"> • Static(O): 设备上配置静态绑定的地址后, 如果收到对应客户端发送的 Solicit 消息, 则产生该类型的绑定信息, 即静态临时绑定 (Offered) • Static(C): 表示已经分配给客户端的静态绑定 (Committed), 即静态正式绑定 • Auto(O): 表示接收到客户端发送的 Solicit 消息后, 产生的动态临时绑定 (Offered) • Auto(C): 表示接收到客户端发送的 Request 消息, 或支持地址快速分配功能的服务器收到客户端发送的包含 Rapid Commit 选项的 Solicit 消息后, 产生的动态正式绑定 (Committed) • Auto(Z): 表示已成功分配的租约表项在配置恢复后 (如主备倒换), 由于所在地址池引用的前缀不生效产生的僵死绑定 (Zombie)
Lease-expiration	IPv6地址的租约过期时间。如果租约过期时间在2100年以后, 则显示为 Expires after 2100 ; 对于静态无效绑定, 显示为 Not available
Client	DHCPv6客户端的IPv6地址。对于静态无效绑定, 该字段显示为空
DUID	客户端的DUID
IAID	客户端的IAID。对于静态无效绑定且未配置IAID, 该字段显示为N/A
Preferred lifetime	IPv6地址的首选生命期, 单位为秒
valid lifetime	IPv6地址的有效生命期, 单位为秒
Expires at	IPv6地址的租约过期时间。如果租约过期时间在2100年以后, 则显示为 Expires after 2100

【相关命令】

- **reset ipv6 dhcp server ip-in-use**

1.2.13 display ipv6 dhcp server pd-in-use

display ipv6 dhcp server pd-in-use 命令用来显示 DHCPv6 前缀绑定信息。

【命令】

```
display ipv6 dhcp server pd-in-use [ pool pool-name | prefix
prefix/prefix-len ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

pool *pool-name*: 显示指定 DHCPv6 地址池的前缀绑定信息。*pool-name* 表示 DHCPv6 地址池名称，为 1~63 个字符的字符串，不区分大小写。如果未指定本参数，则显示所有 DHCPv6 地址池的前缀绑定信息。

prefix *prefix/prefix-len*: 显示指定前缀的前缀绑定信息。*prefix/prefix-len* 为 IPv6 前缀/前缀长度，*prefix-len* 取值范围为 1~128。如果未指定本参数，则显示所有前缀的前缀绑定信息。

【举例】

显示所有的 DHCPv6 前缀绑定信息。

```
<Sysname> display ipv6 dhcp server pd-in-use
Pool: 1
  IPv6 prefix          Type      Lease expiration
  2:1::/24             Auto(O)   Jul 10 19:45:01 2008
Pool: 2
  IPv6 prefix          Type      Lease expiration
  1:1::/64             Static(F) Not available
Pool: 3
  IPv6 prefix          Type      Lease expiration
  1:2::/64             Static(O) Oct  9 09:23:31 2008
Pool: 4
  IPv6 prefix          Type      Lease expiration
  12::/80              Auto(Z)   Oct 17 09:34:59 2008
```

显示指定 DHCPv6 地址池的前缀绑定信息。

```
<Sysname> display ipv6 dhcp server pd-in-use pool 1
Pool: 1
  IPv6 prefix          Type      Lease expiration
  2:1::/24             Auto(O)   Jul 10 22:22:22 2008
  3:1::/64             Static(C) Jan  1 11:11:11 2008
```

显示指定前缀的前缀绑定信息。

```
<Sysname> display ipv6 dhcp server pd-in-use prefix 2:1::3/24
Pool: 1
Client: FE80::C800:CFF:FE18:0
Type: Auto(O)
DUID: 00030001CA000C180000
IAID: 0x00030001
  IPv6 prefix: 2:1::/24
  Preferred lifetime 400, valid lifetime 500
  Expires at Jul 10 09:45:01 2008 (288 seconds left)
```

表1-9 display ipv6 dhcp server pd-in-use 命令显示信息描述表

字段	描述
IPv6 prefix	已分配的IPv6前缀
Type	前缀绑定的类型，取值包括： <ul style="list-style-type: none">Static(F): 表示尚未分配给客户端的静态绑定前缀（Free），即

字段	描述
	静态无效绑定 <ul style="list-style-type: none"> • Static(O): 表示静态临时绑定。设备上配置静态绑定的前缀后，如果收到对应客户端发送的 Solicit 消息，则产生该类型的绑定信息，即静态临时绑定 (Offered) • Static(C): 表示已经分配给客户端的静态绑定，即静态正式绑定 (Committed) • Auto(O): 表示接收到客户端发送的 Solicit 消息后，产生的动态临时绑定 (Offered) • Auto(C): 表示接收到客户端发送的 Request 消息，或支持前缀快速分配功能的服务器收到客户端发送的包含 Rapid Commit 选项的 Solicit 消息后，产生的动态正式绑定 (Committed) • Auto(Z): 表示已成功分配的前缀表项在配置恢复（如主备倒换）后，由于所在前缀池引用的前缀不生效产生的僵死绑定 (Zombie)
Pool	前缀绑定所属的地址池
Lease-expiration	前缀的租约过期时间。如果租约过期时间在2100年以后，则显示为 Expires after 2100 ；对于静态无效绑定，显示为 Not available
Client	DHCPv6客户端的IPv6地址。对于静态无效绑定，该字段显示为空
DUID	客户端的DUID
IAID	客户端的IAID。对于静态无效绑定且未配置IAID，该字段显示为N/A
Preferred lifetime	前缀的首选生命期，单位为秒
valid lifetime	前缀的有效生命期，单位为秒
Expires at	前缀的租约过期时间。如果租约过期时间在2100年以后，则显示为 Expires after 2100

【相关命令】

- `reset ipv6 dhcp server pd-in-use`

1.2.14 display ipv6 dhcp server statistics

`display ipv6 dhcp server statistics` 命令用来显示 DHCPv6 服务器的报文统计信息。

【命令】

`display ipv6 dhcp server statistics [pool pool-name]`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

pool pool-name: 显示指定地址池的信息。*pool-name* 表示地址池名称，为 1~63 个字符的字符串，不区分大小写。如果未指定本参数，则显示所有地址池的信息。

【举例】

```
# 显示 DHCPv6 服务器的报文统计信息。
<Sysname> display ipv6 dhcp server statistics
Bindings:
    Ip-in-use           : 1
    Pd-in-use           : 0
    Expired              : 0
Conflict               : 0
Packets received       : 1
    Solicit              : 1
    Request              : 0
    Confirm              : 0
    Renew                : 0
    Rebind               : 0
    Release              : 0
    Decline              : 0
    Information-request  : 0
    Relay-forward        : 0
Packets dropped         : 0
Packets sent           : 0
    Advertise            : 0
    Reconfigure          : 0
    Reply                : 0
    Relay-reply          : 0
```

表1-10 display ipv6 dhcp server statistics 命令显示信息描述表

字段	描述
Bindings	各种状态的地址绑定数，包括： <ul style="list-style-type: none">Ip-in-use: 地址绑定信息总数Pd-in-use: 前缀绑定信息的总数Expired: 租约过期的地址绑定信息的总数
Conflict	冲突地址的总数，显示指定地址池的统计信息时无此字段
Packets received	接收报文的数目，报文类型如下： <ul style="list-style-type: none">SolicitRequestConfirmRenewRebindReleaseDeclineInformation-request

字段	描述
	<ul style="list-style-type: none"> Relay-forward 显示指定地址池的统计信息时无此类字段
Packets dropped	丢弃报文的数目，显示指定地址池的统计信息时无此字段
Packets sent	发送报文的数目，报文类型如下： <ul style="list-style-type: none"> Advertise Reconfigure Reply Relay-reply 显示指定地址池的统计信息时无此类字段

【相关命令】

- `reset ipv6 dhcp server statistics`

1.2.15 dns-server

dns-server 命令用来配置为客户端分配的 DNS 服务器地址。

undo dns-server 命令用来删除指定的 DNS 服务器地址。

【命令】

dns-server *ipv6-address*

undo dns-server *ipv6-address*

【缺省情况】

未指定为客户端分配的 DNS 服务器地址。

【视图】

DHCPv6 地址池视图

DHCPv6 选项组视图

【缺省用户角色】

network-admin

【参数】

ipv6-address: DNS 服务器的 IPv6 地址。

【使用指导】

可以通过多次执行本命令配置多个 DNS 服务器地址。一个地址池下最多可以配置 8 个 DNS 服务器地址，且配置的先后顺序决定了 DNS 服务器的优先级，先配置的 DNS 服务器优先级大于后配置的 DNS 服务器。

【举例】

配置 DHCPv6 地址池 1 为客户端分配的 DNS 服务器地址为 2:2::3。

```
<Sysname> system-view
```

```
[Sysname] ipv6 dhcp pool 1
```

```
[Sysname-dhcp6-pool-1] dns-server 2:2::3
```

【相关命令】

- **display ipv6 dhcp pool**

1.2.16 domain-name

domain-name 命令用来配置为客户端分配的域名。

undo domain-name 命令用来恢复缺省情况。

【命令】

```
domain-name domain-name
```

```
undo domain-name
```

【缺省情况】

未指定为客户端分配的域名。

【视图】

DHCPv6 地址池视图

DHCPv6 选项组视图

【缺省用户角色】

network-admin

【参数】

domain-name: 域名，为 1~50 个字符的字符串，区分大小写。

【使用指导】

一个地址池下只能配置一个域名。多次执行本命令，最后一次执行的命令生效。

【举例】

配置 DHCPv6 地址池 1 为客户端分配的域名为 **aaa.com**。

```
<Sysname> system-view
```

```
[Sysname] ipv6 dhcp pool 1
```

```
[Sysname-dhcp6-pool-1] domain-name aaa.com
```

【相关命令】

- **display ipv6 dhcp pool**

1.2.17 if-match

if-match 命令用来配置 DHCPv6 用户类的匹配规则。

undo if-match 命令用来恢复缺省情况。

【命令】

```
if-match rule rule-number { option option-code [ ascii ascii-string [ offset offset | partial ] | hex hex-string [ mask mask | offset offset length length | partial ] ] | relay-agent gateway-ipv6-address }
```

```
undo if-match rule rule-number
```

【缺省情况】

未配置 DHCPv6 用户类的匹配规则。

【视图】

DHCPv6 用户类视图

【缺省用户角色】

network-admin

【参数】

rule *rule-number*: 匹配规则编号，取值范围为 1~16。编号越小，匹配优先级越高。

option *option-code*: DHCPv6 选项的数值，取值范围为 1~65535。*option-code* 用于指定匹配 DHCPv6 客户端时从 DHCPv6 报文中获取哪个选项。

ascii *ascii-string*: 指定用来匹配报文中指定选项的内容。*ascii-string* 为 1~128 个字符的 ASCII 字符串。

offset *offset*: 指定匹配 DHCPv6 客户端时获取选项内容的起始位置。*offset* 为选项内容偏移量，取值范围为 0~65534，单位为字节。如果未指定本参数，则表示从选项值第一字节开始匹配整个选项的内容。

partial: 指定部分匹配，即只要报文中的选项内容中包含指定的 *hex-string* 或 *ascii-string*，即认为匹配通过。

hex *hex-string*: 指定用来匹配报文中指定选项的内容。*hex-string* 为十六进制数，位数的取值范围为 2~256 之间的偶数。

mask *mask*: 指定与选项内容匹配时使用的掩码。*mask* 为十六进制掩码数，位数的取值范围为 2~256 之间的偶数。*mask* 的长度必须和 *hex-string* 长度相同。

length *length*: 指定匹配 DHCPv6 客户端时获取选项内容的长度。*length* 为选项内容的长度，取值范围为 1~128，单位为字节。*length* 长度必须和 *hex-string* 长度相同。

relay-agent *gateway-ipv6-address*: 指定匹配报文中的 *link-address* 字段的内容。*gateway-ipv6-address* 为 IPv6 地址。

【使用指导】

DHCPv6 服务器通过将 DHCPv6 客户端发送的报文与本命令配置的规则匹配，来判断 DHCPv6 客户端属于的 DHCPv6 用户类。DHCPv6 用户类视图下通过多次执行 **if-match** 命令，可以配置多条不同类(**option** 或 **relay-agent**)的匹配规则。只要任意一条规则匹配成功，就认为该 DHCPv6 客户端属于该用户类。

在同一用户类视图下配置匹配规则时：

- 在同一用户类视图下，多次配置相同 *rule-number* 的命令，如果规则类型（包括匹配 **option** 和 **relay-agent**）相同，最后一次执行的命令生效；如果规则类型不同，则新的配置和已有配置会共存。建议不同类型的规则不要使用同一个 *rule-number*。
- 在同一用户类视图下，不同 *rule-number* 的匹配规则内容不能完全相同。

将报文与某一条 **if-match option** 命令配置的规则匹配的方式为：

- 如果规则中只指定了 *option-code* 参数，则只要报文中包含该选项，就认为匹配成功。否则，匹配失败。

- 如果规则中只指定了 *option-code* 和 *hex-string/ascii-string* 参数，则报文中指定选项的值从第 1 位开始的部分与 *hex-string/ascii-string* 相同时，认为匹配成功。否则，匹配失败。
- 如果规则中指定了 *option-code*、*ascii-string* 和 *offset* 参数，则将指定选项的值的第 *offset*+1 位到最后一位的内容与 *ascii-string* 比较，二者相同时，认为匹配成功。否则，匹配失败。
- 如果规则中指定了 *option-code*、*hex-string* 和 *mask* 参数，则将指定选项值的第 1 位到 *mask* 长度位的内容与 *mask* 进行与运算，将结果与 *hex-string* 与 *mask* 与运算的结果比较，二者相同时，认为匹配成功。否则，匹配失败。
- 如果规则中指定了 *option-code*、*hex-string*、*offset* 和 *length* 参数，则将指定选项值的第 *offset*+1 位到 *offset*+*length* 位的内容与 *hex-string* 比较，二者相同时，认为匹配成功。否则，匹配失败。
- 如果规则中指定了 *option-code*、*hex-string/ascii-string* 和 **partial** 参数，则选项内容内包含了指定的 *hex-string/ascii-string*，就认为匹配成功。否则，匹配失败。例如匹配字段为 *abc*，那 *xabc*、*xyzabca*、*xabcyz* 和 *abcxyz* 均认为匹配通过。

将报文与某一条 **if-match relay-agent** 命令配置的规则匹配的方式是只要报文中的 *link-address* 字段和指定的 *gateway-ipv6-address* 一致时，认为匹配成功。否则，匹配失败。

【举例】

配置 DHCPv6 用户类 **exam** 的匹配规则，匹配规则编号 1，报文中包含 Option 16。

```
<Sysname> system-view
[Sysname] ipv6 dhcp class exam
[Sysname-dhcp6-class-exam] if-match rule 1 option 16
```

配置 DHCPv6 用户类 **exam** 的匹配规则，匹配规则编号 2，报文中包含 Option 16，并且该选项的十六进制数第四个字节最高位为 1。

```
<Sysname> system-view
[Sysname] ipv6 dhcp class exam
[Sysname-dhcp6-class-exam] if-match rule 2 option 16 hex 00000080 mask 00000080
```

配置 DHCPv6 用户类 **exam** 的匹配规则，匹配规则编号 3，报文中包含 Option 16，并且该选项的前三个字节为十六进制数 **13ae92**。

```
<Sysname> system-view
[Sysname] ipv6 dhcp class exam
[Sysname-dhcp6-class-exam] if-match rule 3 option 16 hex 13ae92 offset 0 length 3
```

配置 DHCPv6 用户类 **exam** 的匹配规则，匹配规则编号 4，报文中包含 Option 16，并且该选项内容中包含指定的十六进制数 **13ae**。

```
<Sysname> system-view
[Sysname] ipv6 dhcp class exam
[Sysname-dhcp6-class-exam] if-match rule 4 option 16 hex 13ae partial
```

配置 DHCPv6 用户类 **exam** 的匹配规则，匹配规则编号 5，报文中包含的 *link-address* 字段值为 **2001::1**。

```
<Sysname> system-view
[Sysname] ipv6 dhcp class exam
[Sysname-dhcp6-class-exam] if-match rule 5 relay-agent 2001::1
```

【相关命令】

- **ipv6 dhcp class**

1.2.18 ipv6 dhcp apply-policy

ipv6 dhcp apply-policy 命令用来指定接口引用的 DHCPv6 策略。

undo ipv6 dhcp apply-policy 命令用来恢复缺省情况。

【命令】

ipv6 dhcp apply-policy *policy-name*

undo ipv6 dhcp apply-policy

【缺省情况】

接口未引用 DHCPv6 策略。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

policy-name: DHCPv6 策略名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

在一个接口上只能引用一条 DHCPv6 策略。在一个接口上多次执行本命令，最后一次执行的命令生效。

【举例】

指定 VLAN 接口 2 引用 DHCPv6 策略 test。

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 2
```

```
[Sysname-Vlan-interface2] ipv6 dhcp apply-policy test
```

【相关命令】

- **ipv6 dhcp class**

1.2.19 ipv6 dhcp class

ipv6 dhcp class 命令用来创建 DHCPv6 用户类并进入 DHCPv6 用户类视图，如果已经创建了 DHCPv6 用户类，则直接进入该用户类视图。

undo ipv6 dhcp class 命令用来删除指定的 DHCPv6 用户类。

【命令】

ipv6 dhcp class *class-name*

undo ipv6 dhcp class *class-name*

【缺省情况】

不存在 DHCPv6 用户类。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

class-name: DHCPv6 用户类名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

在 DHCPv6 用户类视图下，可以通过 **if-match** 命令配置 DHCPv6 用户类的匹配规则，根据匹配规则判断 DHCPv6 客户端属于的 DHCPv6 用户类，从而实现灵活的用户分配策略。

【举例】

创建名称为 test 的 DHCPv6 用户类，并进入 DHCPv6 用户类视图。

```
<Sysname> system-view
[Sysname] ipv6 dhcp class test
[Sysname-dhcp6-class-test]
```

【相关命令】

- **class pool**
- **ipv6 dhcp policy**
- **if-match**

1.2.20 ipv6 dhcp option-group

ipv6 dhcp option-group 命令用来手工创建静态 DHCPv6 选项组，并进入 DHCPv6 选项组视图。

undo ipv6 dhcp option-group 命令用来删除指定的静态 DHCPv6 选项组。

【命令】

```
ipv6 dhcp option-group option-group-number
undo ipv6 dhcp option-group option-group-number
```

【缺省情况】

设备上不存在 DHCPv6 选项组。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

option-group-number: 选项组编号，取值范围为 1~100。

【使用指导】

手工配置的静态 DHCPv6 选项组与动态生成的 DHCPv6 选项组编号允许相同，静态选项组信息优先。

【举例】

创建静态 DHCPv6 选项组 1，并进入 DHCPv6 选项组视图。

```
<Sysname> system-view
[Sysname] ipv6 dhcp option-group 1
[Sysname-dhcp6-option-group1]
```

【相关命令】

- **display ipv6 dhcp option-group**

1.2.21 ipv6 dhcp policy

ipv6 dhcp policy 命令用来创建 DHCPv6 策略，并进入 DHCPv6 策略视图。如果已经存在 DHCPv6 策略，则直接进入该策略视图。

undo ipv6 dhcp policy 命令用来删除已创建的 DHCPv6 策略。

【命令】

```
ipv6 dhcp policy policy-name
undo ipv6 dhcp policy policy-name
```

【缺省情况】

不存在 DHCPv6 策略。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

policy-name: DHCPv6 策略名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

在 DHCPv6 策略视图下，可以通过 **class pool** 命令指定 DHCPv6 用户类关联的 DHCPv6 地址池，使匹配该 DHCPv6 用户类的客户端可以从关联的地址池中获取到 IPv6 地址、前缀和其他参数。

需要注意的是，需要配置 **ipv6 dhcp apply-policy** 命令在接口上引用 DHCPv6 策略后，DHCPv6 策略才能生效。

【举例】

创建 DHCPv6 策略 test，并进入该 DHCPv6 策略视图。

```
<Sysname> system-view
[Sysname] ipv6 dhcp policy test
[Sysname-dhcp6-policy-test]
```

【相关命令】

- `class pool`
- `default pool`
- `ipv6 dhcp apply-policy`
- `ipv6 dhcp class`

1.2.22 ipv6 dhcp pool

`ipv6 dhcp pool` 命令用来创建 DHCPv6 地址池，并进入 DHCPv6 地址池视图。如果指定的地址池已存在，则直接进入地址池视图。

`undo ipv6 dhcp pool` 命令用来删除指定的 DHCPv6 地址池。

【命令】

```
ipv6 dhcp pool pool-name  
undo ipv6 dhcp pool pool-name
```

【缺省情况】

设备上不存在 DHCPv6 地址池。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

pool-name: DHCPv6 地址池名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

在 DHCPv6 地址池下，可以配置为 DHCPv6 客户端分配的 IPv6 地址、前缀等参数。

需要注意的是，删除 DHCPv6 地址池时，该地址池中已经分配的地址绑定信息和前缀绑定信息也将被删除。

【举例】

创建名称为 pool1 的 DHCPv6 地址池，并进入 DHCPv6 地址池视图。

```
<Sysname> system-view  
[Sysname] ipv6 dhcp pool pool1  
[Sysname-dhcp6-pool-pool1]
```

【相关命令】

- `class pool`
- `display ipv6 dhcp pool`
- `ipv6 dhcp server apply pool`

1.2.23 ipv6 dhcp prefix-pool

`ipv6 dhcp prefix-pool` 命令用来创建前缀池，并指定包含的前缀和分配的前缀长度。

undo ipv6 dhcp prefix-pool 命令用来删除指定的前缀池。

【命令】

```
ipv6 dhcp prefix-pool prefix-pool-number prefix { prefix-number |  
prefix/prefix-len } assign-len assign-len  
undo ipv6 dhcp prefix-pool prefix-pool-number
```

【缺省情况】

设备上不存在 DHCPv6 前缀池。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

prefix-pool-number: 前缀池索引, 取值范围为 1~128。

prefix { prefix-number | prefix/prefix-len }: 引用前缀编号或指定前缀池包含的前缀。引用的 IPv6 前缀编号, 取值范围为 1~1024。prefix/prefix-len 为 IPv6 前缀/前缀长度, 其中, prefix-len 取值范围为 1~128。

assign-len assign-len: 指定分配的前缀长度。assign-len 取值范围为 1~128, assign-len 必须大于或等于 prefix-len, 且与 prefix-len 之差小于或等于 16。

【使用指导】

所有前缀池包含的前缀范围之间不能重叠, 即前缀范围不能相交也不能相互包含。

不能通过重复执行本命令修改前缀池。如需修改前缀池, 请先通过 **undo ipv6 dhcp prefix-pool** 命令删除前缀池, 再执行 **ipv6 dhcp prefix-pool** 命令。

删除前缀池, 会清除从该前缀池中分配的所有前缀绑定信息。

如果设备上不存在本命令引用的 IPv6 前缀编号, 则本命令暂时不会生效。设备上创建引用的 IPv6 前缀编号后, 本命令才生效。

引用的相同 IPv6 前缀编号的前缀发生变化时, 前缀池包含的前缀范围也会随之发生变化。

【举例】

配置 IPv6 前缀编号为 3, 前缀为 88:99::/32, 配置前缀池 2 引用 IPv6 前缀编号 3, 分配的前缀长度为 42, 即前缀池 2 可以分配 88:99::/42~88:99:FFC0::/42 范围内的 1024 个前缀。

```
<Sysname> system-view
```

```
[Sysname] ipv6 prefix 3 88:99::/32
```

```
[Sysname] ipv6 dhcp prefix-pool 2 prefix 3 assign-len 42
```

配置前缀池 1, 包含的前缀为 2001:0410::/32, 分配的前缀长度为 42, 即前缀池 1 包含 2001:0410::/42~2001:0410:FFC0::/42 范围内的 1024 个前缀。

```
<Sysname> system-view
```

```
[Sysname] ipv6 dhcp prefix-pool 1 prefix 2001:0410::/32 assign-len 42
```

【相关命令】

- **display ipv6 dhcp prefix-pool**

- `prefix-pool`

1.2.24 ipv6 dhcp server

`ipv6 dhcp server` 命令用来配置全局查找地址池，并指定全局查找 DHCPv6 地址池时地址或前缀分配策略。

`undo ipv6 dhcp server` 命令用来恢复缺省情况。

【命令】

```
ipv6 dhcp server { allow-hint | preference preference-value | rapid-commit }  
*  
  
undo ipv6 dhcp server
```

【缺省情况】

接口全局查找 DHCPv6 地址池时，不支持期望地址/前缀分配和地址/前缀快速分配功能，服务器优先级的值为 0。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

allow-hint: 指定服务器支持期望地址/前缀分配功能。如果未指定本参数，则表示不支持期望地址/前缀分配功能。

preference preference-value: 指定发送的 Advertise 消息中的服务器优先级。
preference-value 为服务器优先级，取值范围为 0~255，缺省值为 0。该值越大，表示服务器的优先级越高，DHCPv6 客户端选择该服务器分配的地址或前缀的可能性越大。

rapid-commit: 指定服务器支持交互两个报文的地址/前缀快速分配功能。如果未指定本参数，则表示服务器不支持地址/前缀快速分配功能。

【使用指导】

如果执行本命令时，指定了 **allow-hint** 参数，则服务器优先为客户端分配它期望的地址或前缀。如果客户端期望的地址或前缀不在接口可分配的地址池中，或者已经分配给其他客户端，则服务器忽略客户端的期望地址或前缀，并为客户端分配其他空闲地址或前缀。如果未指定 **allow-hint** 参数，则服务器忽略客户端期望的地址或前缀，从地址池中选择地址或前缀分配给客户端。

需要注意的是，如果在同一个接口上同时执行了 `ipv6 dhcp server` 命令和 `ipv6 dhcp server apply pool` 命令，则以 `ipv6 dhcp server apply pool` 命令的配置为准。

【举例】

配置接口 Vlan-interface2 全局查找地址池，服务器支持期望地址/前缀分配和地址/前缀快速分配功能，优先级设置为最高，即 255。

```
<Sysname> system-view  
[Sysname] interface vlan-interface 2  
[Sysname-Vlan-interface2] ipv6 dhcp server allow-hint preference 255 rapid-commit
```

【相关命令】

- `display ipv6 dhcp server`
- `ipv6 dhcp select`

1.2.25 ipv6 dhcp server apply pool

`ipv6 dhcp server apply pool` 命令用来指定接口引用的 DHCPv6 地址池，并指定地址和前缀分配策略。

`undo ipv6 dhcp server apply pool` 命令用来恢复缺省情况。

【命令】

```
ipv6 dhcp server apply pool pool-name [ allow-hint | preference
preference-value | rapid-commit ] *
undo ipv6 dhcp server apply pool
```

【缺省情况】

接口未引用地址池。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

pool-name: DHCPv6 地址池名称，为 1~63 个字符的字符串，不区分大小写。

allow-hint: 指定服务器支持期望地址/前缀分配功能。如果未指定本参数，则表示不支持期望地址/前缀分配功能。

preference preference-value: 指定发送的 Advertise 消息中的服务器优先级。
preference-value 为服务器优先级，取值范围为 0~255，缺省值为 0。该值越大，表示服务器的优先级越高，DHCPv6 客户端选择该服务器分配的地址或前缀的可能性越大。

rapid-commit: 指定服务器支持交互两个报文的地址/前缀快速分配功能。如果未指定本参数，则表示服务器不支持地址/前缀快速分配功能。

【使用指导】

如果接口上引用了地址池，则从该接口接收到客户端发送的 DHCPv6 请求后，将从引用的地址池中选择 IPv6 地址或前缀，分配给客户端；否则，服务器将根据接口的地址或 DHCPv6 中继的地址选择匹配的 DHCPv6 地址池，并从该地址池中选择 IPv6 地址或前缀分配给客户端。

如果执行本命令时，指定了 **allow-hint** 参数，则服务器优先为客户端分配它期望的地址或前缀。如果客户端期望的地址或前缀不在接口可分配的地址池中，或者已经分配给其他客户端，则服务器忽略客户端的期望地址或前缀，并为客户端分配其他空闲地址或前缀。如果未指定 **allow-hint** 参数，则服务器忽略客户端期望的地址或前缀，从地址池中选择地址或前缀分配给客户端。

一个接口上最多只能引用一个地址池，多次执行本命令，最后一次执行的命令生效。

接口可以引用并不存在的地址池，但是，此时该接口无法为客户端分配 IPv6 地址、前缀等信息。只有创建该地址池后，才能为客户端分配 IPv6 地址、前缀等信息。

【举例】

配置 VLAN 接口 2 引用已存在的地址池 1，服务器支持期望地址/前缀分配和地址/前缀快速分配功能，优先级设置为最高，即 255。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 dhcp server apply pool 1 allow-hint preference 255
rapid-commit
```

【相关命令】

- **display ipv6 dhcp server**
- **ipv6 dhcp pool**
- **ipv6 dhcp select**

1.2.26 ipv6 dhcp server database filename

ipv6 dhcp server database filename 命令用来指定存储 DHCPv6 服务器表项的文件名称。

undo ipv6 dhcp server database filename 命令用来恢复缺省情况。

【命令】

```
ipv6 dhcp server database filename { filename | url url [ username username
[ password { cipher | simple } string ] ] }
undo ipv6 dhcp server database filename
```

【缺省情况】

未指定存储文件名称。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

filename: 目标文件名，该配置用于本地存储模式。文件名取值范围的详细介绍，请参见“基础配置指导”中的“文件系统管理”。

url url: 配置远程目标文件 URL，为 1~255 个字符的字符串，区分大小写，该配置用于远程文件系统模式。此参数中不能包含用户名和密码，和参数 **username** 和 **string** 配合使用。

username username: 配置远程目标文件 URL 时的用户名，为 1~32 个字符的字符串，区分大小写。如果未指定本参数，则表示登录远程目标文件 URL 时无需使用用户名。

cipher: 表示以密文方式设置用户密码。

simple: 表示以明文方式设置用户密码，该密码将以密文形式存储。

string: 密码字符串，区分大小写。明文密码为 1~32 个字符的字符串，密文密码为 1~73 个字符的字符串。如果未指定本参数，则表示登录远程目标文件 URL 时无需使用密码。

【使用指导】

存储 DHCPv6 服务器表项时，如果设备中还不存在对应名称的文件，则设备会自动创建该文件。

执行本命令后，会立即触发一次表项备份。之后，如果未配置 **ipv6 dhcp server database update interval** 命令，若表项发生变化，默认在 300 秒之后刷新存储文件；若表项未发生变化，则不再刷新存储文件。如果配置了 **ipv6 dhcp server database update interval** 命令，若表项发生变化，则到达刷新时间间隔后刷新存储文件；若表项未发生变化，则不再刷新存储文件。参数 *filename* 不支持远程目标文件 URL，配置远程目标文件 URL 请使用 *url*、*username*、*string* 配合使用。

频繁擦写本地存储介质可能会影响存储介质寿命，建议使用远程文件系统模式存储 DHCPv6 服务器表项文件。

当进行远程存储时，支持 FTP 和 TFTP 协议：

- 当采用 FTP 或 TFTP 协议时，服务器地址支持 IPv4 形式或 IPv6 形式，并且支持 DNS 域名方式。服务器地址为 IPv6 地址形式时需使用方括号（“[”和“]”）引用。配置服务器地址为 DNS 域名格式时请勿使用方括号引用。
- 当采用 FTP 协议时，URL 采用 “*ftp://服务器地址[:端口号]/文件路径*” 的形式，如有用户名和密码请分别使用参数 *username* 和参数 *string* 进行配置，用户名和密码必须和服务器的配置一致，如果服务器只对用户名进行认证，则不用输入密码。
- 当采用 TFTP 协议时，URL 采用 “*tftp://服务器地址[:端口号]/文件路径*” 的形式。

【举例】

配置存储 DHCPv6 服务器表项的文件名为 *database.dhcp*。

```
<Sysname> system-view
```

```
[Sysname] ipv6 dhcp server database filename database.dhcp
```

配置远程存储 DHCPv6 服务器表项至 IPv6 地址为 10::1 的 FTP 服务器工作目录下,用户名为 1，密码为 1，文件名为 *database.dhcp*。

```
<Sysname> system-view
```

```
[Sysname] ipv6 dhcp server database filename url ftp://[10::1]/database.dhcp username 1  
password simple 1
```

【相关命令】

- **ipv6 dhcp server database update interval**
- **ipv6 dhcp server database update now**
- **ipv6 dhcp server database update stop**

1.2.27 ipv6 dhcp server database update interval

ipv6 dhcp server database update interval 命令用来配置刷新 DHCPv6 服务器表项存储文件的延迟时间。

undo ipv6 dhcp server database update interval 命令用来恢复缺省情况。

【命令】

```
ipv6 dhcp server database update interval interval
```

```
undo ipv6 dhcp server database interval
```

【缺省情况】

若 DHCPv6 服务器表项不变化，则不刷新表项存储文件；若 DHCPv6 服务器表项发生变化，默认在 300 秒后刷新表项存储文件。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval: 刷新延迟时间，取值范围为 60～864000，单位为秒。

【使用指导】

执行本命令后，当服务器表项发生变化后，DHCPv6 服务器开始计时，当本命令配置的延迟时间到达后，DHCPv6 服务器会把这个时间段内表项所有的变化信息备份到固化文件中。

如果未通过 **ipv6 dhcp server database filename** 命令指定存储表项的文件，则本命令的配置不会生效。

【举例】

若 DHCPv6 服务器表项发生变化，在 600 秒后刷新表项存储文件。

```
<Sysname> system-view
```

```
[Sysname] ipv6 dhcp server database update interval 600
```

【相关命令】

- **ipv6 dhcp server database filename**
- **ipv6 dhcp server database update now**
- **ipv6 dhcp server database update stop**

1.2.28 ipv6 dhcp server database update now

ipv6 dhcp server database update now 命令用来将当前 DHCPv6 服务器表项保存到用户指定的文件中。

【命令】

```
ipv6 dhcp server database update now
```

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

本命令只用来触发一次 DHCPv6 服务器表项的备份。

如果未通过 **ipv6 dhcp server database filename** 命令指定存储表项的文件，则本命令的配置不会生效。

【举例】

将当前的 DHCPv6 服务器表项保存到文件中。

```
<Sysname> system-view
```

```
[Sysname] ipv6 dhcp server database update now
```

【相关命令】

- `ipv6 dhcp server database filename`
- `ipv6 dhcp server database update interval`
- `ipv6 dhcp server database update stop`

1.2.29 ipv6 dhcp server database update stop

`ipv6 dhcp server database update stop` 命令用来终止当前的 DHCPv6 服务器表项恢复操作。

【命令】

`ipv6 dhcp server database update stop`

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

本命令只用来触发一次终止 DHCPv6 服务器表项的恢复操作。

本命令只用来停止设备重启后从固化文件中恢复表项信息的过程，不影响除此之外的其他运行过程。当中断恢复表项信息的过程后，如果 DHCP 服务器分配了未恢复表项中的地址信息，可能会导致局域网设备地址冲突情况发生。

从固化文件恢复表项的连接超时间隔为 60 分钟，可以通过本命令立刻终止远程恢复。DHCPv6 服务器从固化文件中恢复表项的过程中，DHCPv6 服务器不会学习新的表项。

【举例】

终止当前的 DHCPv6 服务器表项恢复操作。

```
<Sysname> system-view
[Sysname] ipv6 dhcp server database update stop
```

【相关命令】

- `ipv6 dhcp server database filename`
- `ipv6 dhcp server database update interval`
- `ipv6 dhcp server database update now`

1.2.30 ipv6 dhcp server forbidden-address

`ipv6 dhcp server forbidden-address` 命令用来配置不参与自动分配的 IPv6 地址。

`undo ipv6 dhcp server forbidden-address` 命令用来取消不参与自动分配的 IPv6 地址的配置。

【命令】

`ipv6 dhcp server forbidden-address start-ipv6-address [end-ipv6-address]`

```
undo ipv6 dhcp server forbidden-address start-ipv6-address  
[ end-ipv6-address ]
```

【缺省情况】

除 DHCPv6 服务器接口的 IPv6 地址外，DHCPv6 地址池中的所有 IPv6 地址都参与自动分配。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

start-ipv6-address: 不参与自动分配的起始 IPv6 地址。

end-ipv6-address: 不参与自动分配的结束 IPv6 地址，不能小于 *start-ipv6-address*。如果未指定该参数，则表示只有一个不参与自动分配的 IPv6 地址，即 *start-ipv6-address*；否则，表示 *start-ipv6-address* 到 *end-ipv6-address* 之间的 IPv6 地址均不能参与自动分配。

【使用指导】

某些服务器占用的 IPv6 地址（如网关地址、FTP 服务器地址），不能分配给 DHCPv6 客户端。通过本命令可以避免这些地址参与自动分配。

如果通过 **ipv6 dhcp server forbidden-address** 将已经静态绑定的 IPv6 地址配置为不参与自动分配的地址，则该地址仍然可以分配给静态绑定的用户。

执行 **undo ipv6 dhcp server forbidden-address** 命令取消不参与自动分配 IPv6 地址的配置时，指定的地址/地址范围必须与执行 **ipv6 dhcp server forbidden-address** 命令时指定的地址/地址范围保持一致。如果配置不参与自动分配的 IPv6 地址为某一地址范围，则只能同时取消该地址范围内所有 IPv6 地址的配置，不能单独取消其中某个 IPv6 地址的配置。

多次执行 **ipv6 dhcp server forbidden-address** 命令，可以配置多个不参与自动分配的 IPv6 地址范围。

【举例】

配置 2001:10:110::1 到 2001:10:110::20 之间的 IPv6 地址不参与地址自动分配。

```
<Sysname> system-view
```

```
[Sysname] ipv6 dhcp server forbidden-address 2001:10:110::1 2001:10:110::20
```

【相关命令】

- **ipv6 dhcp server forbidden-prefix**
- **static-bind**

1.2.31 ipv6 dhcp server forbidden-prefix

ipv6 dhcp server forbidden-prefix 命令用来配置不参与自动分配的 IPv6 前缀。

undo ipv6 dhcp server forbidden-prefix 命令用来取消不参与自动分配的 IPv6 前缀的配置。

【命令】

```
ipv6      dhcp      server      forbidden-prefix      start-prefix/prefix-len  
[ end-prefix/prefix-len ]  
undo      ipv6      dhcp      server      forbidden-prefix      start-prefix/prefix-len  
[ end-prefix/prefix-len ]
```

【缺省情况】

DHCPv6 前缀池中的所有 IPv6 前缀都参与自动分配。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

start-prefix/prefix-len: 不参与自动分配的起始 IPv6 前缀。*prefix-len* 为前缀长度，取值范围为 1~128。

end-prefix/prefix-len: 不参与自动分配的结束 IPv6 前缀。*prefix-len* 为前缀长度，取值范围为 1~128。*end-prefix* 的取值不能小于 *start-prefix*。如果未指定该参数，则表示只有一个不参与自动分配的 IPv6 前缀，即 *start-prefix/prefix-len*；否则，表示 *start-prefix/prefix-len* 到 *end-prefix/prefix-len* 之间的前缀均不能参与自动分配。

【使用指导】

如果通过 **ipv6 dhcp server forbidden-prefix** 将已经静态绑定的 IPv6 前缀配置为不参与自动分配的前缀，则该前缀仍然可以分配给静态绑定的用户。

执行 **undo ipv6 dhcp server forbidden-prefix** 命令取消不参与自动分配 IPv6 前缀的配置时，指定的前缀/前缀范围必须与执行 **ipv6 dhcp server forbidden-prefix** 命令时指定的前缀/前缀范围保持一致。如果配置不参与自动分配的 IPv6 前缀为某一前缀范围，则只能同时取消该前缀范围内所有 IPv6 前缀的配置，不能单独取消其中某个 IPv6 前缀的配置。

多次执行 **ipv6 dhcp server forbidden-prefix** 命令，可以配置多个不参与自动分配的 IPv6 前缀段。

【举例】

配置 2001:3e11::/32 到 2001:3eff::/32 之间的 IPv6 前缀不参与前缀自动分配。

```
<Sysname> system-view
```

```
[Sysname] ipv6 dhcp server forbidden-prefix 2001:3e11::/32 2001:3eff::/32
```

【相关命令】

- **ipv6 dhcp server forbidden-address**
- **static-bind**

1.2.32 network

network 命令用来配置 DHCPv6 地址池动态分配的 IPv6 地址网段。

undo network 命令用来恢复缺省情况。

【命令】

```
network      {      prefix/prefix-length      |      prefix      prefix-number  
[ sub-prefix/sub-prefix-length ] } [ preferred-lifetime preferred-lifetime  
valid-lifetime valid-lifetime ]  
undo network
```

【缺省情况】

未配置动态分配的 IPv6 地址网段，即没有可供分配的 IPv6 地址。

【视图】

DHCPv6 地址池视图

【缺省用户角色】

network-admin

【参数】

prefix/prefix-length: 用于动态分配的 IPv6 地址网段。*prefix/prefix-length* 为地址网段的前缀和前缀长度，*prefix-length* 的取值范围为 1~128。

prefix *prefix-number*: 引用前缀作为动态分配的 IPv6 地址网段。*prefix-number* 为前缀编号，取值范围为 1~1024。

sub-prefix/sub-prefix-length: IPv6 子前缀及子前缀长度。*sub-prefix-length* 的取值范围为 1~128。IPv6 子前缀及子前缀长度用来进一步划分引用的 IPv6 前缀。如果被引用的前缀长度大于子前缀长度 *sub-prefix-length*，则使用被引用的前缀长度作为动态分配地址网段的前缀长度。如果不配置此参数，则使用前缀编号对应的前缀作为动态分配的 IPv6 地址网段。

preferred-lifetime *preferred-lifetime*: 指定地址池中分配的地址和前缀的首选生命期。*preferred-lifetime* 为地址和前缀的首选生命期，取值范围为 60~4294967295，单位为秒，缺省值为 604800（7 天）。

valid-lifetime *valid-lifetime*: 指定地址池中分配的地址和前缀的有效生命期。*valid-lifetime* 为地址和前缀的有效生命期，取值范围为 60~4294967295，单位为秒，缺省值为 2592000（30 天）。*valid-lifetime* 必须大于或等于 *preferred-lifetime*。

【使用指导】

每个 DHCPv6 地址池只能配置一个网段，多次执行 **network** 命令，最后一次执行的命令生效。

修改或删除 **network** 命令的配置，会导致该地址池下现有的已分配地址被删除。

如果配置 **network prefix** 命令之前设备上不存在前缀编号为 *prefix-number* 的 IPv6 前缀，则 **network prefix** 命令暂时不会生效。设备上创建前缀编号为 *prefix-number* 的 IPv6 前缀后，配置的 **network prefix** 命令才会生效。

地址池通过 **network** 命令配置的 *prefix/prefix-length* 或通过前缀编号和 *sub-prefix/sub-prefix-length* 得出自身可分配的 IPv6 地址网段。不同地址池分配的 IPv6 地址网段不能完全相同。

如果 **network prefix** 命令引用的前缀发生改变，则 **network prefix** 命令生成的地址网段也会随之发生改变。已经动态分配的前缀和地址绑定信息都会被自动清除。

【举例】

配置 DHCPv6 地址池 1 动态分配的地址网段为 3ffe:501:ffff:100::/64。

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] network 3ffe:501:ffff:100::/64
```

配置 IPv6 前缀编号为 3，IPv6 前缀为 88:99::/32。配置 DHCPv6 地址池 1 动态分配的 IPv6 地址网段时，指定引用 IPv6 前缀编号 3，则 DHCPv6 地址池 1 可分配的地址网段为引用的 IPv6 前缀对应的网段，即 88:99::/32。

```
<Sysname> system-view
[Sysname] ipv6 prefix 3 88:99::/32
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] network prefix 3
```

配置 IPv6 前缀编号为 3，IPv6 前缀为 88:99::/32。配置 DHCPv6 地址池 1 动态分配的 IPv6 地址网段时，指定引用 IPv6 前缀编号 3，并指定子前缀及子前缀长度为 3ffe:501:ffff:100::/64，则 DHCPv6 地址池 1 可分配的地址网段为 88:99:ffff:100::/64，即前 32 位由 IPv6 前缀编号 3 决定，33 位~64 位由子前缀及子前缀长度决定，且动态分配地址网段的前缀长度为子前缀长度 64。

```
<Sysname> system-view
[Sysname] ipv6 prefix 3 88:99::/32
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] network prefix 3 3ffe:501:ffff:100::/64
```

【相关命令】

- **address range**
- **display ipv6 dhcp pool**
- **temporary address range**

1.2.33 option

option 命令用来配置 DHCPv6 地址池的 DHCPv6 自定义选项。

undo option 命令用来删除 DHCPv6 地址池的 DHCPv6 自定义选项。

【命令】

```
option code hex hex-string
undo option code
```

【缺省情况】

未配置 DHCPv6 地址池的 DHCPv6 自定义选项。

【视图】

DHCPv6 地址池视图

DHCPv6 选项组视图

【缺省用户角色】

network-admin

【参数】

code: 选项的数值, 取值范围为 21~65535, 不包括 25~26, 37~40, 43~48。

hex hex-string: 指定选项内容为配置的十六进制数。*hex-string* 为偶数位的十六进制数, 位数的取值范围为 2~256。

【使用指导】

通过执行本命令, 可以配置编号为 *code* 的 DHCPv6 选项内容为指定的十六进制数, 即采用指定的内容来填充 DHCPv6 应答报文中编号为 *code* 的选项, 以便将指定的选项内容分配给客户端。

本命令为 DHCPv6 服务器提供了灵活的选项配置方式, 使得 DHCPv6 服务器可以为 DHCPv6 客户端提供更加丰富的选项内容。在以下情况下, 可以使用本命令配置 DHCPv6 自定义选项:

- 随着 DHCPv6 的不断发展, 新的 DHCPv6 选项会陆续出现。通过配置 DHCPv6 自定义选项, 可以方便地添加新的 DHCPv6 选项。
- 有些选项的内容, RFC 中没有统一规定。厂商可以根据需要定义选项的内容, 如 Option 43。通过配置 DHCPv6 自定义选项, 可以为 DHCPv6 客户端提供厂商指定的信息。
- 设备上只提供了有限的选项配置命令 (如 **dns-server** 命令), 对于没有专门命令来配置的 DHCPv6 选项, 可以通过 **option** 命令配置选项内容。例如, 可以通过 **option 31 hex 00c80000000000000000000000000001** 命令指定为 DHCPv6 客户端分配的 NTP 服务器地址为 200::1。

有些 DHCPv6 选项既可以通过专门的命令来配置, 也可以通过 **option** 命令来配置。例如, Option 23 (DNS 服务器地址选项) 既可以通过 **dns-server** 命令配置, 也可以通过 **option 23** 命令配置。如果同时通过上述两种方式配置了这些选项, 则在填充 DHCPv6 应答报文的选项时, 优先选择专门命令的配置。如果未通过专门命令来配置, 则采用 **option** 命令配置的内容填充选项。

多次执行本命令, 并指定相同的选项数值 *code*, 最后一次执行的命令生效。

【举例】

DNS 服务器地址选项的编号为 23。在 DHCPv6 地址池 1 中配置为 DHCPv6 客户端分配的 DNS 服务器地址为 2001:f3e0::1。

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] option 23 hex 2001f3e0000000000000000000000001
```

【相关命令】

- **display ipv6 dhcp pool**
- **dns-server**
- **domain-name**
- **sip-server**

1.2.34 option-group

option-group 命令用来配置 DHCPv6 地址池引用选项组。

undo option-group 命令用来恢复缺省情况。

【命令】

option-group *option-group-number*

undo option-group

【缺省情况】

DHCPv6 地址池未引用选项组。

【视图】

DHCPv6 地址池视图

【缺省用户角色】

network-admin

【参数】

option-group-number: DHCPv6 选项组编号，取值范围为 1~100。

【举例】

配置 DHCPv6 地址池 1 引用选项组 1。

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] option-group 1
```

【相关命令】

- **display ipv6 dhcp pool**
- **ipv6 dhcp option-group**

1.2.35 prefix-pool

prefix-pool 命令用来配置地址池引用前缀池，以便从前缀池中动态选择前缀分配给客户端。

undo prefix-pool 命令用来取消地址池引用前缀池。

【命令】

```
prefix-pool prefix-pool-number [ preferred-lifetime preferred-lifetime
valid-lifetime valid-lifetime ]
undo prefix-pool prefix-pool-number
```

【缺省情况】

未配置地址池引用的前缀池。

【视图】

DHCPv6 地址池视图

【缺省用户角色】

network-admin

【参数】

prefix-pool-number: 前缀池索引，取值范围 1~128。

preferred-lifetime *preferred-lifetime*: 指定分配前缀的首选生命期。
preferred-lifetime 为前缀的首选生命期，取值范围为 60~4294967295，单位为秒，缺省值为 604800（7 天）。

valid-lifetime *valid-lifetime*: 指定分配前缀的有效生命期。*valid-lifetime* 为前缀的有效生命期, 取值范围为 60~4294967295, 单位为秒, 缺省值为 2592000 (30 天)。*valid-lifetime* 必须大于或等于 *preferred-lifetime*。

【使用指导】

一个地址池最多只能引用一个前缀池。

地址池可以引用并不存在的前缀池, 但是, 此时设备无法从该地址池中动态选择前缀分配给客户端。只有创建该前缀池后, 才能支持前缀的动态分配。

不能通过重复执行本命令的方式修改地址池引用的前缀池、前缀的首选生命期和有效生命期。如需修改地址池引用的前缀池、前缀的首选生命期和有效生命期, 请先通过 **undo prefix-pool** 命令删除引用的前缀池, 再执行 **prefix-pool** 命令。

【举例】

在地址池 1 中引用前缀池 1, 首选生命期和有效生命期为缺省值。

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] prefix-pool 1
```

在地址池 2 中引用前缀池 2, 并设置首选生命期为 1 天, 有效生命期为 3 天。

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 2
[Sysname-dhcp6-pool-2] prefix-pool 2 preferred-lifetime 86400 valid-lifetime 259200
```

【相关命令】

- **display ipv6 dhcp pool**
- **ipv6 dhcp prefix-pool**

1.2.36 reset ipv6 dhcp server conflict

reset ipv6 dhcp server conflict 命令用来清除 DHCPv6 地址冲突信息。

【命令】

```
reset ipv6 dhcp server conflict [ address ipv6-address ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

address *ipv6-address*: 清除指定 IPv6 地址的地址冲突信息。如果未指定本参数, 则清除所有 IPv6 地址的地址冲突信息。

【使用指导】

如果网络配置不合理, 则动态分配的地址和网络中静态配置的地址可能会发生冲突。在合理调整网络配置, 不再存在冲突的情况下, 原来发生冲突的地址可以重新分配给客户端。此时, 通过本命令清除检测到的冲突地址, 则该地址可以被重新分配。

【举例】

清除全部地址冲突信息。

```
<Sysname> reset ipv6 dhcp server conflict
```

【相关命令】

- `display ipv6 dhcp server conflict`

1.2.37 reset ipv6 dhcp server expired

`reset ipv6 dhcp server expired` 命令用来清除租约过期的 DHCPv6 地址绑定信息。

【命令】

```
reset ipv6 dhcp server expired [ address ipv6-address | pool pool-name ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

address *ipv6-address*: 清除指定 IPv6 地址的租约过期地址绑定信息。如果未指定本参数，则清除所有 IPv6 地址的租约过期地址绑定信息。

pool *pool-name*: 清除指定地址池中租约过期的 DHCPv6 地址绑定信息。*pool-name* 表示 DHCPv6 地址池名称，为 1~63 个字符的字符串，不区分大小写。如果未指定本参数，则清除所有地址池中租约过期的 DHCPv6 地址绑定信息。

【举例】

清除地址 2001:f3e0::1 的租约过期地址绑定信息。

```
<Sysname> reset ipv6 dhcp server expired address 2001:f3e0::1
```

【相关命令】

- `display ipv6 dhcp server expired`

1.2.38 reset ipv6 dhcp server ip-in-use

`reset ipv6 dhcp server ip-in-use` 命令用来清除 DHCPv6 的正式地址绑定和临时地址绑定信息。

【命令】

```
reset ipv6 dhcp server ip-in-use [ address ipv6-address | pool pool-name ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

address ipv6-address: 清除指定 IPv6 地址的正式地址绑定和临时地址绑定信息。如果未指定本参数，则清除所有 IPv6 地址的正式地址绑定和临时地址绑定信息。

pool pool-name: 清除指定 DHCPv6 地址池的正式地址绑定和临时地址绑定信息。*pool-name* 表示 DHCPv6 地址池名称，为 1~63 个字符的字符串，不区分大小写。如果未指定本参数，则清除所有地址池中的正式地址绑定和临时地址绑定信息。

【使用指导】

执行本命令后，静态临时地址绑定和静态正式地址绑定信息将变为静态无效地址绑定。

【举例】

清除所有的 DHCPv6 正式地址绑定和临时地址绑定信息。

```
<Sysname> reset ipv6 dhcp server ip-in-use
```

清除地址池 1 的 DHCPv6 正式地址绑定和临时地址绑定信息。

```
<Sysname> reset ipv6 dhcp server ip-in-use pool 1
```

清除 IPv6 地址 2001:0:0:1::1 的 DHCPv6 正式地址绑定和临时地址绑定信息。

```
<Sysname> reset ipv6 dhcp server ip-in-use address 2001:0:0:1::1
```

【相关命令】

- **display ipv6 dhcp server ip-in-use**

1.2.39 reset ipv6 dhcp server pd-in-use

reset ipv6 dhcp server pd-in-use 命令用来清除 DHCPv6 正式前缀绑定和临时前缀绑定信息。

【命令】

```
reset ipv6 dhcp server pd-in-use [ pool pool-name | prefix  
prefix/prefix-len ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

pool pool-name: 清除指定 DHCPv6 地址池的前缀绑定信息。*pool-name* 表示 DHCPv6 地址池名称，为 1~63 个字符的字符串，不区分大小写。如果未指定本参数，则清除所有 DHCPv6 地址池的前缀绑定信息。

prefix prefix/prefix-len: 清除指定前缀的前缀绑定信息。*prefix/prefix-len* 为 IPv6 前缀/前缀长度，*prefix-len* 取值范围为 1~128。如果未指定本参数，则清除所有前缀的前缀绑定信息。

【使用指导】

执行本命令后，静态临时前缀绑定和静态正式前缀绑定信息将变为静态无效前缀绑定。

【举例】

```
# 清除所有的 DHCPv6 前缀绑定信息。
<Sysname> reset ipv6 dhcp server pd-in-use
# 清除 DHCPv6 地址池 1 的正式前缀绑定和临时前缀绑定信息。
<Sysname> reset ipv6 dhcp server pd-in-use pool 1
# 清除 IPv6 前缀 2001:0:0:1::/64 的前缀绑定信息。
<Sysname> reset ipv6 dhcp server pd-in-use prefix 2001:0:0:1::/64
```

【相关命令】

- **display ipv6 dhcp server pd-in-use**

1.2.40 reset ipv6 dhcp server statistics

reset ipv6 dhcp server statistics 命令用来清除 DHCPv6 服务器的报文统计信息。

【命令】

```
reset ipv6 dhcp server statistics
```

【视图】

用户视图

【缺省用户角色】

network-admin

【举例】

```
# 清除 DHCPv6 服务器的报文统计信息。
<Sysname> reset ipv6 dhcp server statistics
```

【相关命令】

- **display ipv6 dhcp server statistics**

1.2.41 sip-server

sip-server 命令用来配置为客户端分配的 SIP 服务器地址或域名。

undo sip-server 命令用来删除为客户端分配的 SIP 服务器地址或域名。

【命令】

```
sip-server { address ipv6-address | domain-name domain-name }
undo sip-server { address ipv6-address | domain-name domain-name }
```

【缺省情况】

未指定为客户端分配的 SIP 服务器地址和域名。

【视图】

DHCPv6 地址池视图

DHCPv6 选项组视图

【缺省用户角色】

network-admin

【参数】

address *ipv6-address*: 指定 SIP 服务器的 IPv6 地址。

domain-name *domain-name*: 指定 SIP 服务器的域名, *domain-name* 为 1~50 个字符的字符串, 不区分大小写。

【使用指导】

同一地址池下最多可以配置 8 个 SIP 服务器地址和 8 个 SIP 服务器域名。配置的先后顺序决定了 SIP 服务器地址或域名的优先级, 即先配置的地址或域名优先级高于后配置的地址或域名。

【举例】

配置 DHCPv6 地址池 1 为客户端分配的 SIP 服务器地址为 2:2::4。

```
<Sysname> system-view
```

```
[Sysname] ipv6 dhcp pool 1
```

```
[Sysname-dhcp6-pool-1] sip-server address 2:2::4
```

配置 DHCPv6 地址池 1 为客户端分配的 SIP 服务器域名为 bbb.com。

```
[Sysname-dhcp6-pool-1] sip-server domain-name bbb.com
```

【相关命令】

- **display ipv6 dhcp pool**

1.2.42 static-bind

static-bind 命令用来配置静态绑定的 IPv6 地址或前缀, 以便实现 DHCPv6 服务器为特定的客户端分配固定的 IPv6 地址或前缀。

undo static-bind 命令用来删除静态绑定的 IPv6 地址或前缀。

【命令】

```
static-bind { address ipv6-address/addr-prefix-length | prefix prefix/prefix-len } duid duid [ iaid iaid ] [ preferred-lifetime preferred-lifetime valid-lifetime valid-lifetime ]
```

```
undo static-bind { address ipv6-address/addr-prefix-length | prefix prefix/prefix-len }
```

【缺省情况】

未配置静态绑定的 IPv6 地址和前缀。

【视图】

DHCPv6 地址池视图

【缺省用户角色】

network-admin

【参数】

address *ipv6-address/addr-prefix-length*: 指定静态绑定的 IPv6 地址及地址前缀长度。
addr-prefix-length 的取值范围为 1~128。

prefix *prefix/prefix-len*: 指定静态绑定的前缀及前缀长度。*prefix-len* 的取值范围为 1~128。

duid *duid*: 指定静态绑定的客户端 DUID 字符串。*duid* 取值为偶数位的十六进制数，且位数的取值范围为 2~256。

iaid *iaid*: 指定静态绑定的客户端 IAID。*iaid* 取值范围为 0~FFFFFFFF 的十六进制数。未指定该参数，则表示不需要匹配客户端的 IAID。

preferred-lifetime *preferred-lifetime*: 指定静态绑定的地址或前缀的首选生命期。
preferred-lifetime 为地址或前缀的首选生命期，取值范围为 60~4294967295，单位为秒，缺省值为 604800（7 天）。

valid-lifetime *valid-lifetime*: 指定静态绑定的地址或前缀的有效生命期。
valid-lifetime 为地址或前缀的有效生命期，取值范围为 60~4294967295，单位为秒，缺省值为 2592000（30 天）。*valid-lifetime* 必须大于或等于 *preferred-lifetime*。

【使用指导】

多次执行 **static-bind** 命令，可以配置多个静态绑定的 IPv6 地址和前缀。

同一 IPv6 地址或者前缀只能绑定给一个客户端。不能通过重复执行本命令修改 IPv6 地址或者前缀与客户端的绑定关系。如需修改 IPv6 地址或者前缀与客户端的绑定关系，请先通过 **undo static-bind** 命令删除绑定关系，再执行 **static-bind** 命令。

【举例】

在地址池 1 中配置静态绑定地址：将地址 2001:0410::1/35 固定分配给 DUID 为 0003000100e0fc005552、IAID 为 A1A1A1A1 的客户端。

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] static-bind address 2001:0410::1/35 duid 0003000100e0fc005552 iaid
A1A1A1A1
```

在地址池 1 中配置静态绑定前缀：将前缀 2001:0410::/35 固定分配给 DUID 为 00030001CA0006A400、IAID 为 A1A1A1A1 的客户端。

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] static-bind prefix 2001:0410::/35 duid 00030001CA0006A400 iaid
A1A1A1A1
```

【相关命令】

- **display ipv6 dhcp pool**

1.2.43 temporary address range

temporary address range 命令用来配置地址池中动态分配的 IPv6 临时地址范围。

undo temporary address range 命令用来恢复缺省情况。

【命令】

```
temporary address range start-ipv6-address end-ipv6-address  
[ preferred-lifetime preferred-lifetime valid-lifetime valid-lifetime ]  
undo temporary address range
```

【缺省情况】

未配置地址池动态分配的 IPv6 临时地址范围，不能分配 IPv6 临时地址。

【视图】

DHCPv6 地址池视图

【缺省用户角色】

network-admin

【参数】

start-ipv6-address：动态分配范围的起始 IPv6 临时地址。

end-ipv6-address：动态分配范围的结束 IPv6 临时地址。

preferred-lifetime *preferred-lifetime*：指定地址池分配的临时地址的首选生命期。
preferred-lifetime 为临时地址的首选生命期，取值范围为 60~4294967295，单位为秒，缺省值为 604800（7 天）。

valid-lifetime *valid-lifetime*：指定地址池分配的临时地址的有效生命期。
valid-lifetime 为临时地址的有效生命期，取值范围为 60~4294967295，单位为秒，缺省值为 2592000（30 天）。*valid-lifetime* 必须大于或等于 *preferred-lifetime*。

【使用指导】

不配置 **temporary address range** 命令时，地址池不会从 **network** 或者 **address range** 命令配置的地址范围内分配临时地址。即此时不支持临时地址分配。

一个地址池最多只能配置一个 IPv6 临时地址范围，多次执行本命令，最后一次执行的命令生效。

【举例】

配置 DHCPv6 地址池 1 动态分配的 IPv6 临时地址范围为 3ffe:501:ffff:100::50 到 3ffe:501:ffff:100::60。

```
<Sysname> system-view  
[Sysname] ipv6 dhcp pool 1  
[Sysname-dhcp6-pool-1] network 3ffe:501:ffff:100::/64  
[Sysname-dhcp6-pool-1] temporary address range 3ffe:501:ffff:100::50 3ffe:501:ffff:100::60
```

【相关命令】

- **address range**
- **display ipv6 dhcp pool**
- **network**

1.3 DHCPv6中继配置命令

1.3.1 display ipv6 dhcp relay server-address

display ipv6 dhcp relay server-address 命令用来显示 DHCPv6 中继上指定的 DHCPv6 服务器地址信息。

【命令】

```
display ipv6 dhcp relay server-address [ interface interface-type
interface-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface *interface-type interface-number*: 显示指定接口上指定的 DHCPv6 服务器地址信息。其中, *interface-type interface-number* 为接口类型和接口编号。如果未指定本参数, 则显示所有接口上指定的 DHCPv6 服务器地址信息。

【举例】

显示 DHCPv6 中继上指定的所有 DHCPv6 服务器地址信息。

```
<Sysname> display ipv6 dhcp relay server-address
Interface: Vlan-interface2
  Server address      Outgoing Interface      Public/VRF name
  2::3                --/--
  3::4                Vlan-interface4        Y/--
  4::5                --/1

Interface: Vlan-interface3
  Server address      Outgoing Interface      Public/VRF name
  2::3                --/--
  3::4                Vlan-interface4        Y/--
  4::5                --/1
```

显示 VLAN 接口 2 上指定的 DHCPv6 服务器地址信息。

```
<Sysname> display ipv6 dhcp relay server-address interface vlan-interface 2
Interface: Vlan-interface2
  Server address      Outgoing Interface      Public/VRF name
  2::3                --/--
  3::4                Vlan-interface4        Y/--
  4::5                --/1
```

表1-11 display ipv6 dhcp relay server-address 命令显示信息描述表

字段	描述
Interface	接口名
Server address	接口上指定的DHCPv6服务器地址
Outgoing Interface	DHCPv6报文的出接口，若未指定出接口，则表明报文将通过路由自动查找出接口
PublicVRF name	（暂不支持）指定的DHCPv6服务器所在位置，取值包括： <ul style="list-style-type: none">当配置了 ipv6 dhcp relay server-address 命令时，显示为--/--当配置了 ipv6 dhcp relay server-address public 命令时，显示为 Y/--当配置了 ipv6 dhcp relay server-address vpn-instance vpn-instance-name 命令时，显示为--/VPN 实例名称

【相关命令】

- **ipv6 dhcp relay server-address**
- **ipv6 dhcp select**

1.3.2 display ipv6 dhcp relay statistics

display ipv6 dhcp relay statistics 命令用来显示 DHCPv6 中继的相关报文统计信息。

【命令】

display ipv6 dhcp relay statistics [**interface** *interface-type* *interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface *interface-type* *interface-number*: 显示指定接口上 DHCPv6 中继的相关报文统计信息。其中，*interface-type* *interface-number* 为接口类型和接口编号。如果未指定本参数，则显示所有接口上 DHCPv6 中继的相关报文统计信息。

【举例】

显示 DHCPv6 中继的相关报文统计信息。

```
<Sysname> display ipv6 dhcp relay statistics
Packets dropped           : 4
Packets received          : 14
    Solicit                : 0
    Request                : 0
    Confirm                : 0
```

```

Renew                : 0
Rebind               : 0
Release              : 0
Decline              : 0
Information-request  : 7
Relay-forward        : 0
Relay-reply          : 7
Packets sent         : 14
Advertise            : 0
Reconfigure          : 0
Reply                : 7
Relay-forward        : 7
Relay-reply          : 0

```

显示 VLAN 接口 2 上 DHCPv6 中继的相关报文统计信息。

```

<Sysname> display ipv6 dhcp relay statistics interface vlan-interface 2
Packets dropped      : 4
Packets received     : 16
  Solicit            : 0
  Request            : 0
  Confirm            : 0
  Renew              : 0
  Rebind             : 0
  Release            : 0
  Decline            : 0
  Information-request : 8
  Relay-forward      : 0
  Relay-reply        : 8
Packets sent         : 16
  Advertise          : 0
  Reconfigure        : 0
  Reply              : 8
  Relay-forward      : 8
  Relay-reply        : 0

```

表1-12 display ipv6 dhcp relay statistics 命令显示信息描述表

字段	描述
Packets dropped	丢弃的报文总数
Packets received	接收到的报文总数
Solicit	接收到的Solicit报文数目
Request	接收到的Request报文数目
Confirm	接收到的Confirm报文数目
Renew	接收到的Renew报文数目
Rebind	接收到的Rebind报文数目
Release	接收到的Release报文数目

字段	描述
Decline	接收到的Decline报文数目
Information-request	接收到的Information-request报文数目
Relay-forward	接收到的Relay-forward报文数目
Relay-reply	接收到的Relay-reply报文数目
Packets sent	发送的报文总数
Advertise	发送的Advertise报文数目
Reconfigure	发送的Reconfigure报文数目
Reply	发送的Reply报文数目
Relay-forward	发送的Relay-forward报文数目
Relay-reply	发送的Relay-reply报文数目

【相关命令】

- `reset ipv6 dhcp relay statistics`

1.3.3 gateway-list

gateway-list 命令用来指定匹配该地址池的 DHCPv6 客户端所在的网段的地址。

undo gateway-list 命令用来删除指定的匹配该地址池的 DHCPv6 客户端所在的网段的地址。

【命令】

```
gateway-list ipv6-address&<1-8>
undo gateway-list [ ipv6-address&<1-8> ]
```

【缺省情况】

未指定匹配该地址池的 DHCPv6 客户端所在的网段的地址。

【视图】

DHCPv6 地址池视图

【缺省用户角色】

network-admin

【参数】

ipv6-address&<1-8>: 匹配该地址池的 DHCPv6 客户端所在的网段 IPv6 地址。&<1-8>表示最多可以输入 8 个 IPv6 地址，每个 IPv6 地址之间用空格分隔。

【使用指导】

一台 DHCPv6 中继的一个接口下可能连接不同类型的用户，当 DHCPv6 中继转发 DHCPv6 客户端请求报文给 DHCPv6 服务器时，不能再以中继接口的 IPv6 地址作为选择地址池的依据。为了解决这个问题，需要使用 **gateway-list** 命令指定某个类型用户所在的网段，并将该地址添加到转发给 DHCPv6 服务器的报文的 Link-address 字段中，为 DHCPv6 服务器选择地址池提供依据。

【举例】

```
# 指定匹配该地址池 p1 的 DHCPv6 客户端所在的网段的地址为 10::1。
<Sysname> system-view
[Sysname] ipv6 dhcp pool p1
[Sysname-dhcp6-pool-p1] gateway-list 10::1
```

1.3.4 ipv6 dhcp relay gateway

ipv6 dhcp relay gateway 命令用来配置 DHCPv6 中继为 DHCPv6 客户端分配的网关地址。
undo ipv6 dhcp relay gateway 命令用来恢复缺省情况。

【命令】

```
ipv6 dhcp relay gateway ipv6-address
undo ipv6 dhcp relay gateway
```

【缺省情况】

分配接口下第一个 IPv6 地址作为 DHCPv6 客户端的网关地址。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6-address: 指定作为客户端网关的 IPv6 地址。该 IPv6 地址必须属于命令行所在的接口。

【使用指导】

在接口视图下配置此命令后，中继会使用此命令配置的地址作为客户端的网关地址。
多次执行本命令，最后一次执行的命令生效。

【举例】

```
# 在 VLAN 接口 2 上配置为 DHCPv6 客户端分配的网关地址为 10::1。
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 dhcp relay gateway 10::1
```

【相关命令】

- **gateway-list**

1.3.5 ipv6 dhcp relay interface-id

ipv6 dhcp relay interface-id 命令用来配置 DHCPv6 中继支持的 interface-id 选项填充模式。
undo ipv6 dhcp relay interface-id 命令用来恢复缺省情况。

【命令】

```
ipv6 dhcp relay interface-id { bas | interface }
```

undo ipv6 dhcp relay interface-id

【缺省情况】

interface-id 选项的填充模式为接口索引信息。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

bas：表示配置 interface-id 选项填充模式为 BAS 模式。

interface：表示配置 interface-id 选项填充模式为接口名模式。填充内容为 ASCII 码格式的接口名和接口所在 VLAN 的编号。

【使用指导】

执行 **ipv6 dhcp relay interface-id** 命令之前，如果未配置 DHCPv6 中继模式，本命令不生效。

【举例】

在 VLAN 接口 10 下配置 DHCPv6 中继支持的 interface-id 选项填充模式为 BAS 模式。

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ipv6 dhcp relay interface-id bas
```

在 VLAN 接口 10 下配置 DHCPv6 中继支持的 interface-id 选项填充模式为接口名模式。

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ipv6 dhcp relay interface-id interface
```

1.3.6 ipv6 dhcp relay server-address

ipv6 dhcp relay server-address 命令用来在 DHCPv6 中继上指定 DHCPv6 服务器的地址。

undo ipv6 dhcp relay server-address 命令用来删除 DHCPv6 中继上指定的 DHCPv6 服务器地址。

【命令】

```
ipv6 dhcp relay server-address ipv6-address [ interface interface-type interface-number ]
```

```
undo ipv6 dhcp relay server-address [ ipv6-address [ interface interface-type interface-number ] ]
```

【缺省情况】

未在 DHCPv6 中继上指定 DHCPv6 服务器地址。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6-address: DHCPv6 服务器的 IPv6 地址。如果 DHCPv6 服务器的 IPv6 地址是组播地址或者链路本地地址，则必须指定报文的出接口。

interface interface-type interface-number: 指定报文的出接口。其中，**interface-type interface-number** 为接口类型和接口编号。如果指定了本参数，则通过指定的接口将 DHCPv6 客户端发送的请求报文转发给 DHCPv6 服务器；如果未指定本参数，则根据路由查找报文的出接口。

【使用指导】

工作在 DHCPv6 中继模式的接口接收到 DHCPv6 客户端发来的报文后，将其封装在 Relay-forward 报文中，并发送给指定的 DHCPv6 服务器，由 DHCPv6 服务器为客户端分配地址和网络配置参数。

通过多次执行 **ipv6 dhcp relay server-address** 命令可以指定多个 DHCPv6 服务器，一个接口下最多可以指定 8 个 DHCPv6 服务器。DHCPv6 中继从接口接收到 DHCPv6 客户端发送的报文后，将其转发给该接口上指定的所有 DHCPv6 服务器。

如果指定的 DHCPv6 服务器地址为链路本地地址或组播地址，则必须指定出接口，否则报文可能会无法到达服务器。

执行 **undo ipv6 dhcp relay server-address** 命令时，如果指定了 **ipv6-address** 参数，则删除指定的 DHCPv6 服务器地址；如果未指定任何参数，则删除接口上的所有 DHCPv6 服务器地址。

建议不要在一个接口上同时配置 DHCPv6 客户端和 DHCPv6 中继功能。

【举例】

配置 VLAN 接口 2 工作在 DHCPv6 中继模式，并指定 DHCPv6 服务器地址为 2001:1::3。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 dhcp select relay
[Sysname-Vlan-interface2] ipv6 dhcp relay server-address 2001:1::3
```

【相关命令】

- **display ipv6 dhcp relay server-address**
- **ipv6 dhcp select**

1.3.7 ipv6 dhcp relay source-address

ipv6 dhcp relay source-address 命令用来指定 DHCPv6 中继向 DHCPv6 服务器转发报文的源地址。

undo ipv6 dhcp relay source-address 命令用来恢复缺省情况。

【命令】

```
ipv6 dhcp relay source-address { ipv6-address | interface interface-type
interface-number }
undo ipv6 dhcp relay source-address
```


【缺省情况】

DHCPv6 中继自动选择向 DHCPv6 服务器转发报文出接口的一个全球单播地址作为 DHCPv6 中继向 DHCPv6 服务器转发报文的源地址。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6-address: 指定该 IPv6 地址为发送到 DHCPv6 服务器的报文源地址。

interface *interface-type interface-number*: 指定该接口 IPv6 地址为发送到 DHCPv6 服务器的报文源地址。*interface-type interface-number* 表示接口类型和接口编号。

【使用指导】

在某些组网中，DHCPv6 中继接口到 DHCPv6 服务器没有可达路由，用户需要配置本命令选择 DHCPv6 中继设备上的另一个接口（一般选择的是 Loopback 口）的 IPv6 地址填充到转发给 DHCPv6 服务器的 DHCPv6 请求报文中的源地址字段。

当使用 **interface interface-type interface-number** 参数指定 DHCPv6 服务器的报文源地址时，如果该接口不存在 IPv6 全球单播地址，则恢复缺省情况。

多次执行命令，最后一次执行的命令生效。

【举例】

在 VLAN 接口 2 上指定 DHCPv6 中继向 DHCPv6 服务器转发报文的源地址为 10::1

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 dhcp relay source-address 10::1
```

1.3.8 remote-server

remote-server 命令指定中继地址池对应的 DHCPv6 服务器地址。

undo remote-server 命令用来删除为中继地址池指定的 DHCPv6 服务器地址。

【命令】

```
remote-server ipv6-address [ interface interface-type interface-number ]
undo remote-server [ ipv6-address [ interface interface-type interface-number ] ]
```

【缺省情况】

未指定中继地址池的 DHCPv6 服务器的地址。

【视图】

DHCPv6 地址池视图

【缺省用户角色】

network-admin

【参数】

ipv6-address: DHCPv6 服务器的 IPv6 地址。

interface *interface-type interface-number*: 指定 DHCPv6 中继将报文转发给 DHCPv6 服务器的出接口, *interface-type interface-number* 表示接口类型和接口编号。如果未指定本参数, 则 DHCPv6 中继根据路由表查找报文出接口。

【使用指导】

在一个地址池中, 最多可以通过配置 **remote-server** 命令来指定 8 个 DHCPv6 服务器的地址。

执行 **undo remote-server** 命令时, 如果未指定任何参数, 则删除所有配置的 DHCPv6 服务器地址。

当配置的目的地址是链路本地地址时, 必须指定 DHCPv6 中继将报文转发给 DHCPv6 服务器的出接口。

【举例】

配置 DHCPv6 地址池 0 为中继配置的服务器地址为 10::1。

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 0
[Sysname-dhcp6-pool-0] remote-server 10::1
```

1.3.9 reset ipv6 dhcp relay statistics

reset ipv6 dhcp relay statistics 命令用来清除 DHCPv6 中继的相关报文统计信息。

【命令】

```
reset ipv6 dhcp relay statistics [ interface interface-type
interface-number ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface *interface-type interface-number*: 清除指定接口上的 DHCPv6 中继相关报文统计信息。其中, *interface-type interface-number* 为接口类型和接口编号。如果未指定本参数, 则清除所有接口上的 DHCPv6 中继相关报文统计信息。

【举例】

清除 DHCPv6 中继的相关报文统计信息。

```
<Sysname> reset ipv6 dhcp relay statistics
```

【相关命令】

- **display ipv6 dhcp relay statistics**

1.4 DHCPv6客户端配置命令

1.4.1 display ipv6 dhcp client

display ipv6 dhcp client 命令用来显示 DHCPv6 客户端的信息。

【命令】

display ipv6 dhcp client [**interface** *interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface interface-type interface-number: 显示指定接口的 DHCPv6 客户端信息。
其中, *interface-type interface-number* 为接口类型和接口编号。如果未指定本参数, 则显示所有 DHCPv6 客户端的信息。

【举例】

显示 VLAN 接口 2 上的 DHCPv6 客户端信息。

```
<Sysname> display ipv6 dhcp client interface vlan-interface 2
Vlan-interface2:
  Type: Stateful client requesting address and prefix
  State: OPEN
  Client DUID: 0003000100e002000000
  Preferred server:
    Reachable via address: FE80::2E0:1FF:FE00:18
    Server DUID: 0003000100e001000000
  IA_NA: IAID 0x00000642, T1 50 sec, T2 80 sec
    Address: 1:1::2/128
      Preferred lifetime 100 sec, valid lifetime 200 sec
      Will expire on Feb 4 2014 at 15:37:20(288 seconds left)
  IA_PD: IAID 0x00000642, T1 50 sec, T2 80 sec
    Prefix: 12:34::/48
      Preferred lifetime 100 sec, valid lifetime 200 sec
      Will expire on Mar 27 2014 at 08:13:24 (199 seconds left)
  DNS server addresses:
    2:2::3
  Domain name:
    aaa.com
  SIP server addresses:
    2:2::4
  SIP server domain names:
    bbb.com
  Options:
```

Code: 88

Length: 3 bytes

Hex: AABBC

表1-13 display ipv6 dhcp client 命令显示信息描述表

字段	描述
Type	DHCPv6客户端类型，取值包括： <ul style="list-style-type: none">Stateful client requesting address: 表示获取 IPv6 地址的 DHCPv6 客户端Stateful client requesting prefix: 表示获取 IPv6 前缀的 DHCPv6 客户端Stateful client requesting address and prefix: 表示同时获取 IPv6 地址和 IPv6 前缀的 DHCPv6 客户端Stateless client: 表示无状态 DHCPv6 客户端
State	客户端的当前状态，取值包括： <ul style="list-style-type: none">IDLE: 闲置状态SOLICIT: 正在定位服务器REQUEST: 正在申请租约OPEN: 申请成功RENEW: 正在申请更新租约（租约 T1 时间之后，T2 时间之前）REBIND: 正在申请更新租约（租约 T2 时间之后，过期之前）RELEASE: 正在申请释放租约DECLINE: 检测到地址冲突，正在申请禁用该地址INFO-REQUESTING: 正在无状态获取配置信息
Client DUID	客户端的DUID
Preferred server	DHCPv6客户端选用的DHCPv6服务器的信息
Reachable via address	可达地址，服务器或中继的链路本地地址
Server DUID	服务器的DUID
IA_NA	申请到的IA_NA信息
IA_PD	申请到的IA_PD信息
IAID	IA标识符
T1	租约的T1生命期，单位为秒
T2	租约的T2生命期，单位为秒
Address	申请到的地址，只有客户端类型为Stateful client requesting address时，显示该信息
Prefix	申请到的前缀，只有客户端类型为Stateful client requesting prefix时，显示该信息
Preferred lifetime	租约的首选生命期，单位为秒
valid lifetime	租约的有效生命期，单位为秒
Will expire on Feb 4 2014 at 15:37:20(288 seconds left)	将在2014年2月4日15点37分20秒过期（还有288秒）。如果租约过期时间在2100年以后，则显示为Will expire after 2100
DNS server addresses	申请到的DNS服务器地址

字段	描述
Domain name	申请到的域名后缀
SIP server addresses	申请到的SIP服务器地址
SIP server domain names	申请到的SIP服务器域名
Options	申请到的自定义选项
Code	自定义选项编码
Length	自定义选项长度，单位为字节
Hex	自定义选项内容，以十六进制数表示

【相关命令】

- `ipv6 address dhcp-alloc`
- `ipv6 dhcp client duid`
- `ipv6 dhcp client pd`

1.4.2 display ipv6 dhcp client statistics

`display ipv6 dhcp client statistics` 命令用来显示 DHCPv6 客户端的统计信息。

【命令】

```
display ipv6 dhcp client statistics [ interface interface-type
interface-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface interface-type interface-number: 显示指定接口上 DHCPv6 客户端的统计信息。其中，*interface-type interface-number* 为接口类型和接口编号。如果未指定本参数，则显示所有 DHCPv6 客户端的统计信息。

【举例】

显示 VLAN 接口 2 上 DHCPv6 客户端的统计信息。

```
<Sysname> display ipv6 dhcp client statistics interface vlan-interface 2
Interface                : Vlan-interface2
Packets received         : 1
    Reply                 : 1
    Advertise              : 0
    Reconfigure            : 0
    Invalid                : 0
```

```

Packets sent          : 5
    Solicit           : 0
    Request           : 0
    Renew             : 0
    Rebind            : 0
    Information-request : 5
    Release           : 0
    Decline           : 0

```

表1-14 display ipv6 dhcp client statistics 命令显示信息描述表

字段	描述
Interface	DHCPv6客户端所在的接口
Packets received	收到的报文数目
Reply	收到Reply报文的数目
Advertise	收到Advertise报文的数目
Reconfigure	收到Reconfigure报文的数目
Invalid	无效报文的数目
Packets sent	已发送报文的数目
Solicit	已发送Solicit报文的数目
Request	已发送Request报文的数目
Renew	已发送Renew报文的数目
Rebind	已发送Rebind报文的数目
Information-request	已发送Information-request报文的数目
Release	已发送Release报文的数目
Decline	已发送Decline报文的数目

【相关命令】

- **reset ipv6 dhcp client statistics**

1.4.3 ipv6 address dhcp-alloc

ipv6 address dhcp-alloc 命令用来配置接口作为 DHCPv6 客户端，通过 DHCPv6 方式获取 IPv6 地址和其他网络配置参数。

undo ipv6 address dhcp-alloc 命令用来取消接口作为 DHCPv6 客户端，并删除通过 DHCPv6 获取到的 IPv6 地址和其他网络配置参数。

【命令】

```

ipv6 address dhcp-alloc [ option-group option-group-number | rapid-commit ]
*
undo ipv6 address dhcp-alloc

```

【缺省情况】

接口不会作为 DHCPv6 客户端获取 IPv6 地址和其他网络配置参数。

【视图】

VLAN 接口视图

【缺省用户角色】

network-admin

【参数】

option-group *option-group-number*: 指定 DHCPv6 选项组编号。*option-group-number* 表示 DHCPv6 选项组编号，取值范围为 1~100。如果指定了本参数，则 DHCPv6 客户端获取到 DHCPv6 选项后，将自动创建指定编号的 DHCPv6 选项组，并将获取到的 DHCPv6 选项保存在该 DHCPv6 选项组中。如果未指定本参数，则不会自动创建 DHCPv6 选项组。

rapid-commit: 配置客户端支持地址快速分配功能。如果未指定该参数，表示该客户端不支持地址快速分配功能。

【举例】

配置 VLAN 接口 10 作为 DHCPv6 客户端，通过 DHCPv6 方式获取 IPv6 地址和其他网络配置参数，指定客户端支持地址快速分配功能，并指定获取到网络配置参数时，创建 DHCPv6 选项组 1，并将获取的参数保存在该选项组中。

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ipv6 address dhcp-alloc rapid-commit option-group 1
```

【相关命令】

- **display ipv6 dhcp client**

1.4.4 ipv6 dhcp client dscp

ipv6 dhcp client dscp 命令用来配置 DHCPv6 客户端发送的 DHCPv6 报文的 DSCP 优先级。

undo ipv6 dhcp client dscp 命令用来恢复缺省情况。

【命令】

```
ipv6 dhcp client dscp dscp-value
undo ipv6 dhcp client dscp
```

【缺省情况】

DHCPv6 报文的 DSCP 优先级为 56。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

dscp-value: DHCPv6 报文的 DSCP 优先级，取值范围为 0~63。

【使用指导】

DSCP 携带在 DHCPv6 报文中的 Traffic class 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。配置的 DSCP 优先级的取值越大，报文的优先级越高。

【举例】

配置 DHCPv6 客户端发送的 DHCPv6 报文的 DSCP 优先级为 30。

```
<Sysname> system-view
[Sysname] ipv6 dhcp client dscp 30
```

1.4.5 ipv6 dhcp client duid

ipv6 dhcp client duid 命令用来配置接口使用指定的 DHCPv6 客户端 DUID。

undo ipv6 dhcp client duid 命令用来恢复缺省情况。

【命令】

```
ipv6 dhcp client duid { ascii ascii-string | hex hex-string | mac
interface-type interface-number }
undo ipv6 dhcp client duid
```

【缺省情况】

根据设备的桥 MAC 地址生成 DHCPv6 客户端 DUID。

【视图】

VLAN 接口视图

【缺省用户角色】

network-admin

【参数】

ascii *ascii-string*: 使用指定的 ASCII 字符串作为该接口的 DHCPv6 客户端 DUID，为 1～130 个字符的字符串，区分大小写。

hex *hex-string*: 使用指定的十六进制数作为该接口的 DHCPv6 客户端 DUID，为 2～260 个字符的字符串。

mac *interface-type interface-number*: 使用指定接口的 MAC 地址作为该接口的 DHCPv6 客户端 DUID，*interface-type interface-number* 表示接口类型和接口编号。

【使用指导】

DHCPv6 客户端 DUID 用来填充 DHCPv6 报文的 Option 1，作为识别 DHCPv6 客户端的唯一标识。

DHCPv6 服务器可以根据 DHCPv6 客户端 DUID 为特定的 DHCPv6 客户端分配特定的 IPv6 地址。用户需保证不同 DHCPv6 客户端的 DUID 不会相同。

【举例】

配置 VLAN 接口 10 使用的 DHCPv6 客户端 DUID 为十六进制数 FFFFFFFF。

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ipv6 dhcp client duid hex ffffffff
```


【相关命令】

- `display ipv6 dhcp client`

1.4.6 ipv6 dhcp client pd

`ipv6 dhcp client pd` 命令用来配置接口作为 DHCPv6 客户端，通过 DHCPv6 方式获取 IPv6 前缀和其他网络配置参数。

`undo ipv6 dhcp client pd` 命令用来取消接口作为 DHCPv6 客户端，并删除通过 DHCPv6 获取到的 IPv6 前缀和其他网络配置参数。

【命令】

```
ipv6 dhcp client pd prefix-number [ option-group option-group-number |  
rapid-commit ]*  
undo ipv6 dhcp client pd
```

【缺省情况】

接口不会作为 DHCPv6 客户端，通过 DHCPv6 方式获取 IPv6 前缀和其他网络配置参数。

【视图】

VLAN 接口视图

【缺省用户角色】

network-admin

【参数】

prefix-number: IPv6 前缀编号，取值范围为 1~1024。DHCPv6 客户端获取到 IPv6 前缀后，将动态创建指定编号的 IPv6 前缀，该前缀编号对应的 IPv6 前缀为 DHCPv6 客户端获取到的前缀。

rapid-commit: 指定客户端支持前缀快速分配功能。未指定该参数时，表示不支持前缀快速分配功能。

option-group option-group-number: 指定 DHCPv6 选项组编号。*option-group-number* 表示 DHCPv6 选项组编号，取值范围为 1~100。如果指定了本参数，则 DHCPv6 客户端获取到 DHCPv6 选项后，将自动创建指定编号的 DHCPv6 选项组，并将获取到的 DHCPv6 选项保存在该 DHCPv6 选项组中。如果未指定本参数，则不会自动创建 DHCPv6 选项组。

【举例】

配置 VLAN 接口 10 作为 DHCPv6 客户端，通过 DHCPv6 方式获取 IPv6 前缀和其他网络配置参数；指定获取到 IPv6 前缀后，创建编号为 1 的 IPv6 前缀；配置客户端支持前缀快速分配功能，并指定获取到网络配置参数时，创建 DHCPv6 选项组 1，并将获取的参数保存在该选项组中。

```
<Sysname> system-view  
[Sysname] interface vlan-interface 10  
[Sysname-Vlan-interface10] ipv6 dhcp client pd 1 rapid-commit option-group 1
```

【相关命令】

- `display ipv6 dhcp client`

1.4.7 ipv6 dhcp client stateful

ipv6 dhcp client stateful 命令用来配置接口作为 DHCPv6 客户端，通过 DHCPv6 方式同时获取 IPv6 地址、IPv6 前缀和网络配置参数。

undo ipv6 dhcp client stateful 命令用来取消接口作为 DHCPv6 客户端，通过 DHCPv6 方式同时获取 IPv6 地址、IPv6 前缀和网络配置参数。

【命令】

```
ipv6 dhcp client stateful prefix prefix-number [ option-group  
option-group-number | rapid-commit ] *  
undo ipv6 dhcp client stateful
```

【缺省情况】

接口不会作为 DHCPv6 客户端同时获取 IPv6 地址、IPv6 前缀和网络配置参数。

【视图】

VLAN 接口视图

【缺省用户角色】

network-admin

【参数】

prefix *prefix-number*: IPv6 前缀编号，取值范围为 1~1024。DHCPv6 客户端获取到 IPv6 前缀后，将动态创建指定编号的 IPv6 前缀，该前缀编号对应的 IPv6 前缀为 DHCPv6 客户端获取到的前缀。

rapid-commit: 指定客户端支持前缀快速分配功能。未指定该参数时，表示不支持前缀快速分配功能。

option-group *option-group-number*: 指定 DHCPv6 选项组编号。*option-group-number* 表示 DHCPv6 选项组编号，取值范围为 1~100。如果指定了本参数，则 DHCPv6 客户端获取到 DHCPv6 选项后，将自动创建指定编号的 DHCPv6 选项组，并将获取到的 DHCPv6 选项保存在该 DHCPv6 选项组中。如果未指定本参数，则不会自动创建 DHCPv6 选项组。

【使用指导】

ipv6 dhcp client stateful 命令优先于 **ipv6 address dhcp-alloc** 和 **ipv6 dhcp client pd** 命令：

- 接口上同时配置以上三个命令时，接口上只会生效 **ipv6 dhcp client stateful** 命令运行状态机去同时申请 IPv6 地址和前缀。
- 接口上同时存在以上三个命令时，如果执行 **undo ipv6 dhcp client stateful** 命令，则会生效接口上另外两条命令，分别去申请 IPv6 地址和 IPv6 前缀。

【举例】

配置 VLAN 接口 10 作为 DHCPv6 客户端，通过 DHCPv6 方式获取 IPv6 地址、IPv6 前缀和其他网络配置参数；指定获取到 IPv6 前缀后，创建编号为 1 的 IPv6 前缀；指定客户端支持快速分配功能，并指定获取到网络配置参数时，创建 DHCPv6 选项组 1，并将获取的参数保存在该选项组中。

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 10
```

```
[Sysname-Vlan-interface10] ipv6 dhcp client stateful prefix 1 rapid-commit option-group 1
```

【相关命令】

- `ipv6 address dhcp-alloc`
- `ipv6 dhcp client pd`

1.4.8 ipv6 dhcp client stateless enable

`ipv6 dhcp client stateless enable` 命令用来开启 DHCPv6 客户端无状态配置功能。

`undo ipv6 dhcp client stateless enable` 命令用来关闭 DHCPv6 客户端无状态配置功能。

【命令】

```
ipv6 dhcp client stateless enable
undo ipv6 dhcp client stateless enable
```

【缺省情况】

DHCPv6 客户端无状态配置功能处于关闭状态。

【视图】

VLAN 接口视图

【缺省用户角色】

network-admin

【使用指导】

接口开启无状态配置功能后发送 `information request` 报文申请配置信息。

【举例】

在 VLAN 接口 2 上开启 DHCPv6 客户端无状态配置功能。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 dhcp client stateless enable
```

1.4.9 reset ipv6 dhcp client statistics

`reset ipv6 dhcp client statistics` 命令用来清除 DHCPv6 客户端的统计信息。

【命令】

```
reset ipv6 dhcp client statistics [ interface interface-type
interface-number ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface interface-type interface-number: 清除指定接口上 DHCPv6 客户端的统计信息。其中, *interface-type interface-number* 为接口类型和接口编号。如果未指定本参数, 则清除所有 DHCPv6 客户端的统计信息。

【举例】

清除所有 DHCPv6 客户端的统计信息。

```
<Sysname> reset ipv6 dhcp client statistics
```

【相关命令】

- **display ipv6 dhcp client statistics**

1.5 DHCPv6 Snooping配置命令



说明

设备只有位于 DHCPv6 客户端与 DHCPv6 服务器之间, 或 DHCPv6 客户端与 DHCPv6 中继之间时, DHCPv6 Snooping 功能配置后才能正常工作; 设备位于 DHCPv6 服务器与 DHCPv6 中继之间时, DHCPv6 Snooping 功能配置后不能正常工作。

1.5.1 display ipv6 dhcp snooping binding

display ipv6 dhcp snooping binding 命令用来显示 DHCPv6 Snooping 地址表项信息。

【命令】

```
display ipv6 dhcp snooping binding [ address ipv6-address [ vlan vlan-id ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

address ipv6-address: 显示指定 IPv6 地址对应的 DHCPv6 Snooping 地址表项。如果未指定本参数, 则显示所有 IPv6 地址对应的 DHCPv6 Snooping 地址表项。

vlan vlan-id: 显示指定 VLAN 对应的 DHCPv6 Snooping 地址表项。如果未指定本参数, 则显示所有 VLAN 内的 DHCPv6 Snooping 地址表项。

【举例】

显示所有 DHCPv6 Snooping 地址表项信息。

```
<Sysname> display ipv6 dhcp snooping binding
```

```
1 DHCPv6 snooping entries found.
```

IPv6 address	MAC address	Lease	VLAN	SVLAN	Interface
--------------	-------------	-------	------	-------	-----------

=====

表1-15 display ipv6 dhcp snooping binding 命令显示信息描述表

字段	描述
IPv6 Address	DHCPv6客户端获取到的IPv6地址
MAC Address	DHCPv6客户端的MAC地址
Lease	IPv6地址租约剩余时间，单位为秒
VLAN	如果DHCPv6 Snooping功能与QinQ功能同时使用，或接收到的DHCPv6报文带有两层VLAN Tag，则表示第一层VLAN Tag；否则，表示与DHCP客户端连接的设备端口所属的VLAN（S5110V2-SI和S5000V3-EI不支持QinQ功能）
SVLAN	如果DHCPv6 Snooping功能与QinQ功能同时使用，或接收到的DHCPv6报文带有两层VLAN Tag，则表示第二层VLAN Tag；否则，显示为“N/A”（S5110V2-SI和S5000V3-EI不支持QinQ功能）
Interface	连接DHCPv6客户端的端口

【相关命令】

- `ipv6 dhcp snooping binding record`
- `reset ipv6 dhcp snooping binding`

1.5.2 display ipv6 dhcp snooping binding database

`display ipv6 dhcp snooping binding database` 命令用来显示 DHCPv6 Snooping 表项备份信息。

【命令】

`display ipv6 dhcp snooping binding database`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

显示 DHCPv6 Snooping 表项备份信息。

```
<Sysname> display ipv6 dhcp snooping binding database
File name           : database.dhcp
Username            :
Password            :
Update interval     : 600 seconds
Latest write time    : Feb 27 18:48:04 2012
Status              : Last write succeeded.
```

表1-16 display ipv6 dhcp snooping binding database 命令显示信息描述表

字段	描述
File name	存储DHCPv6 Snooping表项的文件名称
Username	配置远程目标文件时的用户名
Password	配置远程目标文件时的密码，有配置时显示为“*****”
Update interval	定期刷新表项存储文件的刷新时间间隔，单位：秒
Latest write time	最近一次写文件的时间
Status	写文件的状态，即写文件是否成功 <ul style="list-style-type: none"> Writing: 正在写文件 Last write succeeded: 写文件成功 Last write failed: 写文件失败

1.5.3 display ipv6 dhcp snooping packet statistics

display ipv6 dhcp snooping packet statistics 命令用来显示 DHCPv6 Snooping 设备上的 DHCPv6 报文统计信息。

【命令】

display ipv6 dhcp snooping packet statistics [slot slot-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot slot-number: 显示指定成员设备的 DHCPv6 报文统计信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示主设备上的 DHCPv6 报文统计信息。

【举例】

显示 DHCPv6 Snooping 设备上的 DHCPv6 报文统计信息。

```
<Sysname> display ipv6 dhcp snooping packet statistics
DHCPv6 packets received      : 100
DHCPv6 packets sent          : 200
Invalid DHCPv6 packets dropped : 0
```

表1-17 display ipv6 dhcp snooping packet statistics 命令显示信息描述表

字段	描述
DHCPv6 packets received	接收的DHCPv6报文数
DHCPv6 packets sent	发送的DHCPv6报文数

字段	描述
Invalid DHCPv6 packets dropped	丢弃的无效DHCPv6报文数

【相关命令】

- `reset ipv6 dhcp snooping packet statistics`

1.5.4 display ipv6 dhcp snooping pd binding

`display ipv6 dhcp snooping pd binding` 命令用来显示 DHCPv6 Snooping 前缀表项信息。

【命令】

```
display ipv6 dhcp snooping pd binding [ prefix prefix/prefix-length [ vlan
vlan-id ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

prefix *prefix/prefix-length*: 显示指定 IPv6 前缀/前缀长度的 DHCPv6 Snooping 前缀表项信息。*prefix/prefix-length* 表示 IPv6 地址前缀和前缀长度。*prefix-length* 的取值范围为 1~128。

vlan *vlan-id*: 显示指定 VLAN 内的 DHCPv6 Snooping 前缀表项信息，*vlan-id* 的取值范围为 1~4094。

【使用指导】

只有在 DHCP Snooping 设备端口上开启 DHCPv6 Snooping 前缀表项记录功能后，执行本命令才能查看到 DHCPv6 Snooping 前缀表项记录信息。

如果未指定任何参数，则显示所有的 DHCPv6 Snooping 前缀表项。

【举例】

显示 DHCPv6 Snooping 前缀表项信息。

```
<Sysname> display ipv6 dhcp snooping pd binding
1 DHCPv6 snooping PD entries found.
IPv6 prefix      Lease      VLAN SVLAN Interface
=====
1:2::/64         54         2    N/A    GigabitEthernet1/0/1
```

图1-1 display ipv6 dhcp snooping pd binding 命令显示信息描述表

字段	描述
DHCPv6 snooping PD entries found.	DHCPv6前缀表项统计计数

字段	描述
IPv6 prefix	DHCPv6客户端获取到的IPv6前缀
Lease	绑定的租约剩余时间，单位为秒
VLAN	如果DHCPv6 Snooping功能与QinQ功能同时使用，或接收到的DHCPv6报文带有两层VLAN Tag，则表示第一层VLAN Tag；否则，表示与DHCP客户端连接的设备端口所属的VLAN
SVLAN	如果DHCPv6 Snooping功能与QinQ功能同时使用，或接收到的DHCPv6报文带有两层VLAN Tag，则表示第二层VLAN Tag；否则，显示为“N/A”
Interface	连接DHCPv6客户端的端口

【相关命令】

- `ipv6 dhcp snooping pd binding record`
- `reset ipv6 dhcp snooping pd binding`

1.5.5 display ipv6 dhcp snooping trust

`display ipv6 dhcp snooping trust` 命令用来显示信任端口信息。

【命令】

`display ipv6 dhcp snooping trust`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

```
# 显示 DHCPv6 Snooping 信任端口信息。
<Sysname> display ipv6 dhcp snooping trust
DHCPv6 snooping is enabled.
Interface                               Trusted
=====
GigabitEthernet1/0/1                   Trusted

VSI(Trust tunnel)                       Trusted
=====

Interface                               SrvID      Trusted
=====
```

图1-2 display ipv6 dhcp snooping trust 命令显示信息描述表

字段	描述
Interface	接口名称

字段	描述
VSI(Trust tunnel)	(暂不支持)信任接口的VSI(信任隧道)名称,在VSI视图下配置 ipv6 dhcp snooping trust tunnel 命令后,该项信息会显示
SrvID	(暂不支持)信任接口的以太网服务实例编号
Trusted	开启DHCP Snooping功能后配置的信任接口,则显示为“Trusted”

【相关命令】

- **ipv6 dhcp snooping trust**

1.5.6 ipv6 dhcp snooping binding database filename

ipv6 dhcp snooping binding database filename 命令用来指定存储 DHCPv6 Snooping 表项的文件名称。

undo ipv6 dhcp snooping binding database filename 命令用来恢复缺省情况。

【命令】

ipv6 dhcp snooping binding database filename { *filename* | **url** *url* [**username** *username* [**password** { **cipher** | **simple** } *string*]] }

undo ipv6 dhcp snooping binding database filename

【缺省情况】

未指定存储文件名称。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

filename: 目标文件名,该配置用于本地存储模式。文件名取值范围的详细介绍,请参见“基础配置指导”中的“文件系统管理”。

url url: 配置远程目标文件 URL,为 1~255 个字符的字符串,区分大小写,该配置用于远程文件系统模式。此参数中不能包含用户名和密码,和参数 *username* 和 *string* 配合使用。远程目标文件 URL 是否支持路径格式遵循远程服务器端规格。

username username: 配置远程目标文件 URL 时的用户名,为 1~32 个字符的字符串,区分大小写。如果未指定本参数,则表示登录远程目标文件 URL 时无需使用用户名。

cipher: 表示以密文方式设置用户密码。

simple: 表示以明文方式设置用户密码,该密码将以密文形式存储。

string: 密码字符串,区分大小写。明文密码为 1~32 个字符的字符串,密文密码为 1~73 个字符的字符串。如果未指定本参数,则表示登录远程目标文件 URL 无需使用密码。

【使用指导】

- 存储 DHCPv6 Snooping 表项时，如果设备中还不存在对应名称的文件，则设备会自动创建该文件。
- 执行本命令后，会立即触发一次表项备份。之后，如果未配置 **ipv6 dhcp snooping binding database update interval** 命令，若表项发生变化，默认在 300 秒之后刷新存储文件；若表项未发生变化，则不再刷新存储文件。如果配置了 **ipv6 dhcp snooping binding database update interval** 命令，若表项发生变化，则到达刷新时间间隔后刷新存储文件；若表项未发生变化，则不再刷新存储文件。
- 参数 *filename* 不支持远程目标文件 URL，配置远程目标文件 URL 请使用 *url*、*username*、*string* 配合使用。
- 频繁擦写本地存储介质可能会影响存储介质寿命，建议使用远程文件系统模式存储 DHCPv6 Snooping 表项文件。

当进行远程存储时，支持 FTP 和 TFTP 协议：

- 当采用 FTP 或 TFTP 协议时，服务器地址支持 IPv4 形式或 IPv6 形式，并且支持 DNS 域名方式。服务器地址为 IPv6 地址形式时需使用方括号（“[”和“]”）引用。配置服务器地址为 DNS 域名格式时请勿使用方括号引用。
- 当采用 FTP 协议时，URL 采用 “ftp://[服务器地址][:端口号]/文件路径” 的形式，如有用户名和密码请分别使用参数 *username* 和参数 *string* 进行配置，其中用户名和密码必须和服务器上的配置一致，如果服务器只对用户名进行认证，则不用输入密码。
- 当采用 TFTP 协议时，URL 采用 “tftp://服务器地址[:端口号]/文件路径” 的形式。

【举例】

配置存储 DHCPv6 Snooping 表项的文件名称为 database.dhcp。

```
<Sysname> system-view
```

```
[Sysname] ipv6 dhcp snooping binding database filename database.dhcp
```

配置远程存储 DHCPv6 Snooping 表项至 IP 地址为 1::1 的 ftp 服务器工作目录下，用户名为 1，密码为 1，文件名为 database.dhcp。

```
<Sysname> system-view
```

```
[Sysname] ipv6 dhcp snooping binding database filename url ftp://[1::1]/database.dhcp  
username 1 password simple 1
```

配置远程存储 DHCP Snooping 表项至 IP 地址为 2::1 的 tftp 服务器工作目录下，文件名为 database.dhcp。

```
<Sysname> system-view
```

```
[Sysname] ipv6 dhcp snooping binding database filename url tftp://[2::1]/database.dhcp
```

【相关命令】

- **ipv6 dhcp snooping binding database update interval**

1.5.7 ipv6 dhcp snooping binding database update interval

ipv6 dhcp snooping binding database update interval 命令用来配置刷新 DHCPv6 Snooping 表项存储文件的延迟时间。

undo ipv6 dhcp snooping binding database update interval 命令用来恢复缺省情况。

【命令】

```
ipv6 dhcp snooping binding database update interval interval
undo ipv6 dhcp snooping binding database update interval
```

【缺省情况】

若 DHCPv6 Snooping 表项不变化，则不刷新存储文件；若 DHCPv6 Snooping 表项发生变化，默认在 300 秒之后刷新存储文件。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval：刷新延迟时间，取值范围为 60-864000，单位为秒。

【使用指导】

执行本命令后，当 DHCPv6 Snooping 表项发生变化后，DHCPv6 Snooping 设备开始计时，当本命令配置的延迟时间到达后，DHCPv6 Snooping 设备会把这个时间段内表项所有的变化信息备份到固化文件中。

如果未通过 **ipv6 dhcp snooping binding database filename** 命令指定存储表项的文件，则本命令的配置不会生效。

【举例】

若 DHCPv6 Snooping 表项发生变化，在 600 秒后刷新表项存储文件。

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping binding database update interval 600
```

【相关命令】

- **ipv6 dhcp snooping binding database filename**

1.5.8 ipv6 dhcp snooping binding database update now

ipv6 dhcp snooping binding database update now 命令用来将当前的 DHCPv6 Snooping 表项保存到用户指定的文件中。

【命令】

```
ipv6 dhcp snooping binding database update now
```

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

本命令只用来触发一次 DHCPv6 Snooping 表项的备份。

如果未通过 **ipv6 dhcp snooping binding database filename** 命令指定存储表项的文件，则本命令的配置不会生效。

【举例】

将当前的 DHCPv6 Snooping 表项保存到文件中。

```
<Sysname> system-view
```

```
[Sysname] ipv6 dhcp snooping binding database update now
```

【相关命令】

- **ipv6 dhcp snooping binding database filename**

1.5.9 ipv6 dhcp snooping binding record

ipv6 dhcp snooping binding record 命令用来开启端口的 DHCPv6 Snooping 地址表项记录功能。

undo ipv6 dhcp snooping binding record 命令用来关闭端口的 DHCPv6 Snooping 地址表项记录功能。

【命令】

```
ipv6 dhcp snooping binding record
```

```
undo ipv6 dhcp snooping binding record
```

【缺省情况】

端口的 DHCPv6 Snooping 地址表项记录功能处于关闭状态。

【视图】

二层以太网接口视图/二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

用户可在 DHCPv6 Snooping 设备直接与客户端连接的端口上开启 DHCPv6 Snooping 表项记录功能。

在端口上开启端口的 DHCPv6 Snooping 地址表项记录功能后，可以在端口上监听 DHCPv6 报文，生成 DHCPv6 Snooping 地址表项。

【举例】

开启端口 GigabitEthernet1/0/1 的 DHCPv6 Snooping 地址表项记录功能。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping binding record
```

1.5.10 ipv6 dhcp snooping check request-message

ipv6 dhcp snooping check request-message 命令用来开启 DHCPv6 Snooping 的 DHCPv6 请求方向报文检查功能。

undo ipv6 dhcp snooping check request-message 命令用来关闭 DHCPv6 Snooping 的 DHCPv6 请求方向报文检查功能。

【命令】

```
ipv6 dhcp snooping check request-message
undo ipv6 dhcp snooping check request-message
```

【缺省情况】

DHCPv6 Snooping 的 DHCPv6 请求方向报文检查功能处于关闭状态。

【视图】

二层以太网接口视图/二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

本功能用来检查 DHCPv6-Renew、DHCPv6-Denied 和 DHCPv6-Release 三种 DHCPv6 请求方向的报文，以防止非法客户端伪造这三种报文对 DHCPv6 服务器进行攻击。

如果开启了该功能，则 DHCPv6 Snooping 设备接收到上述报文后，检查本地是否存在与接收报文匹配的 DHCPv6 Snooping 表项。若存在，则接收报文信息与 DHCPv6 Snooping 表项信息一致时，认为该报文为合法的请求方向报文，将其转发给 DHCPv6 服务器；不一致时，认为该报文为伪造的请求方向报文，将其丢弃。若不存在，则认为该报文合法，将其转发给 DHCPv6 服务器。

【举例】

开启 DHCPv6 Snooping 的 DHCPv6 请求方向报文检查功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping check request-message
```

1.5.11 ipv6 dhcp snooping deny

ipv6 dhcp snooping deny 命令用来在端口上开启 DHCPv6 Snooping 报文阻断功能。

undo ipv6 dhcp snooping deny 命令用来在端口上关闭 DHCPv6 Snooping 报文阻断功能。

【命令】

```
ipv6 dhcp snooping deny
undo ipv6 dhcp snooping deny
```

【缺省情况】

端口上的 DHCPv6 Snooping 报文阻断功能处于关闭状态。

【视图】

二层以太网接口视图/二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

在某些组网环境下，用户需要在 DHCPv6 Snooping 设备的某一端口上丢弃该端口收到的所有 DHCPv6 请求方向报文，而又不影响其他端口正常接收 DHCPv6 报文。这时，用户可以在该端口上开启 DHCPv6 Snooping 报文阻断功能。

【举例】

在端口 GigabitEthernet1/0/1 上开启 DHCPv6 Snooping 报文阻断功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping deny
```

1.5.12 ipv6 dhcp snooping enable

ipv6 dhcp snooping enable 命令用来开启 DHCPv6 Snooping 功能。

undo ipv6 dhcp snooping enable 命令用来关闭 DHCPv6 Snooping 功能。

【命令】

```
ipv6 dhcp snooping enable
undo ipv6 dhcp snooping enable
```

【缺省情况】

DHCPv6 Snooping 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

开启 DHCPv6 Snooping 功能后，如果不信任端口接收到 DHCPv6 服务器发送的报文，将丢弃该报文，以保证客户端从合法的 DHCPv6 服务器获取 IPv6 地址。

在 DHCPv6 Snooping 功能关闭后，所有端口都可转发 DHCPv6 服务器的响应报文。

【举例】

开启 DHCPv6 Snooping 功能。

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping enable
```

1.5.13 ipv6 dhcp snooping log enable

ipv6 dhcp snooping log enable 命令用来开启 DHCPv6 Snooping 日志信息功能。

undo ipv6 dhcp snooping log enable 命令用来关闭 DHCPv6 Snooping 日志信息功能。

【命令】

```
ipv6 dhcp snooping log enable
undo ipv6 dhcp snooping log enable
```

【缺省情况】

DHCPv6 Snooping 日志信息功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

DHCPv6 Snooping 日志可以方便管理员定位问题和解决问题。DHCPv6 Snooping 设备生成 DHCPv6 Snooping 日志信息会交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

当 DHCPv6 Snooping 设备输出大量日志信息时，可能会降低设备性能。为了避免该情况的发生，用户可以关闭 DHCPv6 Snooping 日志信息功能，使得 DHCPv6 Snooping 设备不再输出日志信息。

【举例】

```
# 开启 DHCPv6 Snooping 日志信息功能。  
<Sysname> system-view  
[Sysname] ipv6 dhcp snooping log enable
```

1.5.14 ipv6 dhcp snooping option interface-id enable

ipv6 dhcp snooping option interface-id enable 命令用来开启 DHCPv6 Snooping 支持 Option 18 功能。

undo ipv6 dhcp snooping option interface-id enable 命令用来关闭 DHCPv6 Snooping 支持 Option 18 功能。

【命令】

```
ipv6 dhcp snooping option interface-id enable  
undo ipv6 dhcp snooping option interface-id enable
```

【缺省情况】

DHCPv6 Snooping 支持 Option 18 功能处于关闭状态。

【视图】

二层以太网接口视图/二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

只有在系统视图下全局开启 DHCPv6 Snooping 功能，该配置才会生效。

【举例】

```
# 开启 DHCPv6 Snooping 支持 Option 18 功能。  
<Sysname> system-view  
[Sysname] ipv6 dhcp snooping enable
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option interface-id enable
```

【相关命令】

- **ipv6 dhcp snooping enable**
- **ipv6 dhcp snooping option interface-id string**

1.5.15 ipv6 dhcp snooping option interface-id string

ipv6 dhcp snooping option interface-id string 命令用来配置 Option 18 选项中的 DUID。

undo ipv6 dhcp snooping option interface-id string 命令用来恢复缺省情况。

【命令】

```
ipv6 dhcp snooping option interface-id [ vlan vlan-id ] string interface-id
undo ipv6 dhcp snooping option interface-id [ vlan vlan-id ] string
```

【缺省情况】

Option 18 选项中的 DUID 为当前 DHCPv6 Snooping 设备的 DUID。

【视图】

二层以太网端口视图/二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

vlan vlan-id: 为从指定 VLAN 内收到的 DHCPv6 报文填充 Option 18 选项中的 DUID。如果未指定本参数，则为从缺省 VLAN 内收到的 DHCPv6 报文填充 Option 18 选项中的 DUID。

interface-id: 用户自定义的 Option 18 选项中的 DUID，为 1~128 个字符的字符串。

【举例】

配置 Option 18 选项中的 DUID 为 company001。

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option interface-id enable
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option interface-id string company001
```

【相关命令】

- **ipv6 dhcp snooping enable**
- **ipv6 dhcp snooping option interface-id enable**

1.5.16 ipv6 dhcp snooping option remote-id enable

ipv6 dhcp snooping option remote-id enable 命令用来开启 DHCPv6 Snooping 支持 Option 37 功能。

undo ipv6 dhcp snooping option remote-id enable 命令用来关闭 DHCPv6 Snooping 支持 Option 37 功能。

【命令】

```
ipv6 dhcp snooping option remote-id enable
undo ipv6 dhcp snooping option remote-id enable
```

【缺省情况】

DHCPv6 Snooping 支持 Option 37 功能处于关闭状态。

【视图】

二层以太网接口视图/二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

只有在系统视图下全局开启 DHCPv6 Snooping 功能，该配置才会生效。

【举例】

```
# 开启 DHCPv6 Snooping 支持 Option 37 功能。
<Sysname> system-view
[Sysname] ipv6 dhcp snooping enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option remote-id enable
```

【相关命令】

- **ipv6 dhcp snooping enable**
- **ipv6 dhcp snooping option remote-id string**

1.5.17 ipv6 dhcp snooping option remote-id string

ipv6 dhcp snooping option remote-id string 命令用来配置 Option 37 选项中的 DUID。

undo ipv6 dhcp snooping option remote-id string 命令用来恢复缺省情况。

【命令】

```
ipv6 dhcp snooping option remote-id [ vlan vlan-id ] string remote-id
undo ipv6 dhcp snooping option remote-id [ vlan vlan-id ] string
```

【缺省情况】

Option 37 选项中的 DUID 为当前 DHCPv6 Snooping 设备的 DUID。

【视图】

二层以太网端口视图/二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

vlan vlan-id: 为从指定 VLAN 内收到的 DHCPv6 报文填充 Option 37 选项中的 DUID。如果未指定本参数，则为从缺省 VLAN 内收到的 DHCPv6 报文填充 Option 37 选项中的 DUID。

remote-id: 用户自定义的 Option 37 选项中的 DUID，为 1~128 个字符的字符串。

【举例】

配置 Option 37 选项中的 DUID 为 device001。

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option remote-id enable
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option remote-id string device001
```

【相关命令】

- **ipv6 dhcp snooping enable**
- **ipv6 dhcp snooping option remote-id enable**

1.5.18 ipv6 dhcp snooping pd binding record

ipv6 dhcp snooping pd binding record 命令用来开启端口的 DHCPv6 Snooping 前缀表项记录功能。

undo ipv6 dhcp snooping pd binding record 命令用来关闭端口的 DHCPv6 Snooping 前缀表项记录功能。

【命令】

```
ipv6 dhcp snooping pd binding record
undo ipv6 dhcp snooping pd binding record
```

【缺省情况】

端口的 DHCPv6 Snooping 前缀表项记录功能处于关闭状态。

【视图】

二层以太网接口视图/二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

用户可在 DHCPv6 Snooping 设备直接与客户端连接的端口上开启 DHCPv6 Snooping 前缀表项记录功能。设备将监听该端口上接收的报文并解析报文前缀信息，生成 DHCPv6 Snooping 前缀表项，IPv6 Source Guard 可通过 DHCPv6 Snooping 前缀表项生成动态绑定表项，对接口收到的报文进行过滤控制。

【举例】

开启端口 GigabitEthernet1/0/1 的 DHCPv6 Snooping 前缀表项记录功能。

```
<Sysname> system-view
[Sysname]interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping pd binding record
```

【相关命令】

- **display ipv6 dhcp snooping pd binding**

1.5.19 ipv6 dhcp snooping rate-limit

ipv6 dhcp snooping rate-limit 命令用来开启 DHCPv6 Snooping 的报文限速功能，即限制接口接收 DHCPv6 报文的速率。

undo ipv6 dhcp snooping rate-limit 命令用来关闭 DHCPv6 Snooping 的报文限速功能。

【命令】

```
ipv6 dhcp snooping rate-limit rate
```

```
undo ipv6 dhcp snooping rate-limit
```

【缺省情况】

DHCPv6 Snooping 的报文限速功能处于关闭状态，即不限制接口接收 DHCPv6 报文的速率。

【视图】

二层以太网接口视图/二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

rate: 接口接收 DHCPv6 报文的最高速率，单位为 Kbps，取值范围为 64~512。

【使用指导】

只有开启 DHCPv6 Snooping 功能后，本命令的配置才会生效。

如果接口接收到的 DHCPv6 报文速率超过了限制，则丢弃超过速率限制的 DHCPv6 报文。

如果二层以太网接口加入了聚合组，则该接口采用对应二层聚合接口下的 DHCPv6 报文限速配置。

如果二层以太网接口离开聚合组，则该接口采用二层以太网接口下的 DHCPv6 报文限速配置。

芯片支持的速率值是 8 的整数倍，当用户设置的速率值为 67 时，实际的生效值是 64 或 72。

【举例】

开启 DHCPv6 Snooping 的报文限速功能，即限制接口 GigabitEthernet1/0/1 接收 DHCPv6 报文速率为 64Kbps。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping rate-limit 64
```

1.5.20 ipv6 dhcp snooping trust

ipv6 dhcp snooping trust 命令用来配置端口为信任端口。

undo ipv6 dhcp snooping trust 命令用来恢复端口为不信任端口。

【命令】

```
ipv6 dhcp snooping trust
```

```
undo ipv6 dhcp snooping trust
```

【缺省情况】

在开启 DHCPv6 Snooping 功能后，设备上所有支持 DHCPv6 snooping 功能的端口均为不信任端口。

【视图】

二层以太网接口视图/二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

指向 DHCPv6 服务器方向的端口需要设置为信任端口，其他端口设置为不信任端口，从而保证 DHCPv6 客户端只能从合法的 DHCPv6 服务器获取 IPv6 地址，私自架设的伪 DHCPv6 服务器无法为 DHCPv6 客户端分配 IPv6 地址。

【举例】

```
# 配置以太网端口 GigabitEthernet1/0/1 为信任端口。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping trust
```

【相关命令】

- **display ipv6 dhcp snooping trust**

1.5.21 reset ipv6 dhcp snooping binding

reset ipv6 dhcp snooping binding 命令用来清除 DHCPv6 Snooping 地址表项。

【命令】

```
reset ipv6 dhcp snooping binding { all | address ipv6-address [ vlan
vlan-id ] }
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

address ipv6-address: 清除指定 IPv6 地址对应的 DHCPv6 Snooping 地址表项。

vlan vlan-id: 清除指定 VLAN 对应的 DHCPv6 Snooping 地址表项。如果未指定本参数，则清除缺省 VLAN 对应的 DHCPv6 Snooping 地址表项。

all: 清除所有 DHCPv6 Snooping 地址表项。

【举例】

```
# 清除所有的 DHCPv6 Snooping 地址表项。
<Sysname> reset ipv6 dhcp snooping binding all
```

【相关命令】

- `display ipv6 dhcp snooping binding`

1.5.22 reset ipv6 dhcp snooping packet statistics

`reset ipv6 dhcp snooping packet statistics` 命令用来清除 DHCPv6 Snooping 设备上的 DHCPv6 报文统计信息。

【命令】

`reset ipv6 dhcp snooping packet statistics [slot slot-number]`

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

slot slot-number: 清除指定成员设备的 DHCPv6 报文统计信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则清除主设备上的 DHCPv6 报文统计信息。

【举例】

清除 DHCPv6 Snooping 设备上的 DHCPv6 报文统计信息。

```
<Sysname> reset ipv6 dhcp snooping packet statistics
```

【相关命令】

- `display ipv6 dhcp snooping packet statistics`

1.5.23 reset ipv6 dhcp snooping pd binding

`reset ipv6 dhcp snooping pd binding` 命令用来清除 DHCPv6 Snooping 前缀表项信息。

【命令】

`reset ipv6 dhcp snooping pd binding { all | prefix prefix/prefix-length [vlan vlan-id] }`

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

all: 清除所有 DHCPv6 Snooping 前缀表项信息。

prefix prefix/prefix-length: 清除指定 IPv6 前缀对应的 DHCPv6 Snooping 前缀表项信息。*prefix/prefix-length* 表示 IPv6 地址网段的前缀与前缀长度，*prefix-length* 的取值范围为 1~128。

vlan *vlan-id*: 清除指定 VLAN 内的 DHCPv6 Snooping 前缀表项信息, *vlan-id* 的取值范围为 1~4094。

【使用指导】

如果未指定任何参数, 则删除所有 DHCPv6 Snooping 前缀表项信息。

【举例】

清除指定前缀为 1:2::/64 的 DHCPv6 Snooping 前缀表项信息。

```
<Sysname> reset ipv6 dhcp snooping pd binding prefix 1:2::/64
```

【相关命令】

- **display ipv6 dhcp snooping pd binding**

目 录

1 IPv6 快速转发	1-1
1.1 IPv6 快速转发配置命令	1-1
1.1.1 display ipv6 fast-forwarding aging-time	1-1
1.1.2 display ipv6 fast-forwarding cache	1-1
1.1.3 ipv6 fast-forwarding aging-time	1-3
1.1.4 ipv6 fast-forwarding load-sharing	1-3
1.1.5 reset ipv6 fast-forwarding cache	1-4

1 IPv6 快速转发

1.1 IPv6快速转发配置命令

1.1.1 display ipv6 fast-forwarding aging-time

display ipv6 fast-forwarding aging-time 命令用来显示 IPv6 快速转发表项的老化时间。

【命令】

display ipv6 fast-forwarding aging-time

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

显示 IPv6 快速转发表项的老化时间。

```
<Sysname> display ipv6 fast-forwarding aging-time  
Aging time: 30s
```

表1-1 display ipv6 fast-forwarding aging-time 命令显示信息描述表

字段	描述
Aging time	IPv6快转表项的老化时间，单位为秒

【相关命令】

- **ipv6 fast-forwarding aging-time**

1.1.2 display ipv6 fast-forwarding cache

display ipv6 fast-forwarding cache 命令用来显示 IPv6 快速转发表信息。

【命令】

display ipv6 fast-forwarding cache [*ipv6-address*] [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

ipv6-address: 显示指定 IPv6 地址的 IPv6 快速转发表信息。如果不指定 *ipv6-address*，将显示所有 IPv6 地址的 IPv6 快速转发表信息。

slot slot-number: 显示指定成员设备的 IPv6 快速转发表信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 IPv6 快速转发表信息。

【举例】

显示 IPv6 快转表信息。

```
<Sysname> display ipv6 fast-forwarding cache
Total number of IPv6 fast-forwarding items: 2
Src IP: 123::2                               Src Port: 1036
Dst IP: 123::1                               Dst Port: 32768
Protocol: 58
VPN instance: N/A
Input interface: Vlan2
Output interface: InLoop0

Src IP: 123::1                               Src Port: 1036
Dst IP: 123::2                               Dst Port: 33024
Protocol: 58
VPN instance: N/A
Input interface: InLoop0
Output interface: Vlan2
```

表1-2 display ipv6 fast-forwarding cache 命令显示信息描述表

字段	描述
Total number of IPv6 fast-forwarding items	IPv6快速转发表项数目
Src IP	源IPv6地址
Src port	源端口号
Dst IP	目的IPv6地址
Dst Port	目的端口号
Protocol	协议号
VPN instance	VPN实例名称，（“N/A”表示该表项属于公网）
Input interface	报文入接口类型和接口号（“N/A”表示接口存在但是该快速转发不涉及入接口，“-”表示接口不存在）
Output interface	报文出接口类型和接口号（“N/A”表示接口存在但是该快速转发不涉及出接口，“-”表示接口不存在）

【相关命令】

- `reset ipv6 fast-forwarding cache`

1.1.3 ipv6 fast-forwarding aging-time

ipv6 fast-forwarding aging-time 命令用来配置 IPv6 快速转发表项的老化时间。

undo ipv6 fast-forwarding aging-time 命令用来恢复缺省情况。

【命令】

ipv6 fast-forwarding aging-time *aging-time*

undo ipv6 fast-forwarding aging-time

【缺省情况】

IPv6 快速转发表项的老化时间为 30 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

aging-time: IPv6 快速转发表项的老化时间，取值范围为 10~300，单位为秒。

【举例】

配置 IPv6 快速转发表项的老化时间为 20 秒。

```
<Sysname> system-view
```

```
[Sysname] ipv6 fast-forwarding aging-time 20
```

【相关命令】

- **display ipv6 fast-forwarding aging-time**

1.1.4 ipv6 fast-forwarding load-sharing

ipv6 fast-forwarding load-sharing 命令用来开启 IPv6 快转负载分担功能。

undo ipv6 fast-forwarding load-sharing 命令用来关闭 IPv6 快转负载分担功能。

【命令】

ipv6 fast-forwarding load-sharing

undo ipv6 fast-forwarding load-sharing

【缺省情况】

IPv6 快转负载分担功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

开启 IPv6 快速转发负载分担功能后，当一条数据流从不同入接口上来进行转发时，不再根据入接口不同区分数据流，根据报文中的信息标识一条数据流。

关闭 IPv6 快速转发负载分担功能后，将会根据入接口的不同对已标识的数据流再次做出区分，即将入接口作为区分数据流的另一特征标识。

【举例】

开启 IPv6 快转负载分担功能。

```
<Sysname> system-view  
[Sysname] ipv6 fast-forwarding load-sharing
```

1.1.5 reset ipv6 fast-forwarding cache

reset ipv6 fast-forwarding cache 命令用来清除 IPv6 快速转发表信息。

【命令】

```
reset ipv6 fast-forwarding cache [ slot slot-number ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

slot *slot-number*: 清除指定成员设备的 IPv6 快速转发表信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则清除所有成员设备的 IPv6 快速转发表信息。

【举例】

清除 IPv6 快速转发表信息。

```
<Sysname> reset ipv6 fast-forwarding cache
```

【相关命令】

- **display ipv6 fast-forwarding cache**

目 录

1 HTTP重定向	1-1
1.1 HTTP重定向配置命令	1-1
1.1.1 http-redirect https-port	1-1
1.1.2 http-redirect ssl-server-policy	1-1

1 HTTP重定向

1.1 HTTP重定向配置命令

1.1.1 http-redirect https-port

http-redirect https-port 命令用来配置对 HTTPS 报文进行重定向的内部侦听端口号。

undo http-redirect https-port 命令用来恢复缺省情况。

【命令】

http-redirect https-port *port-number*

undo http-redirect https-port

【缺省情况】

对于 Release 6126P20 及之前版本，未配置对 HTTPS 报文进行重定向的内部侦听端口号。对于 Release 6127 及以上版本，对 HTTPS 报文进行重定向的内部侦听端口号为 6654。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

port-number: 对 HTTPS 报文进行重定向的内部侦听端口号，取值范围为 1~65535。

【使用指导】

在配置侦听端口号时，需确保该端口号没有被其他服务占用。可通过 **display tcp** 命令查看已被占用的 TCP 端口号。

对 HTTPS 报文进行重定向的内部侦听端口号不能与知名协议使用的端口号配置一致，否则会发生冲突导致服务不能正常使用。

多次执行本命令，最后一次执行的命令生效。

【举例】

配置对 HTTPS 报文进行重定向的内部侦听端口号为 8888。

```
<Sysname> system-view
```

```
[Sysname] http-redirect https-port 8888
```

1.1.2 http-redirect ssl-server-policy

http-redirect ssl-server-policy 命令用来指定 HTTPS 重定向服务关联的 SSL 服务器端策略。

undo http-redirect ssl-server-policy 命令用来恢复缺省情况。

【命令】

```
http-redirect ssl-server-policy policy-name  
undo http-redirect ssl-server-policy
```

【缺省情况】

HTTPS 重定向服务未与 SSL 服务器端策略关联，HTTPS 重定向服务使用自签名证书。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

policy-name: SSL 服务器端策略名，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

如果关联的 SSL 服务器端策略不存在，则无法完成 HTTPS 报文的重定向。允许用户先关联一个不存在的 SSL 服务器端策略，再对该策略进行相关配置。关于 SSL 的详细描述，请参见“安全配置指导”中的“SSL”。

修改 SSL 服务器端策略会立即生效。

如果多次执行该命令，则最后一次关联的 SSL 服务器端策略生效。

【举例】

指定 HTTPS 重定向服务关联的 SSL 服务器端策略为 policy1。

```
<Sysname> system-view  
[Sysname] http-redirect ssl-server-policy policy1
```

【相关命令】

- **ssl server-policy**（安全命令参考/SSL）