

# 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 .....	1-11
1.1.2 display ipv6 nd snooping count .....	1-12
1.1.6 display ipv6 neighbors .....	1-13
1.1.7 display ipv6 neighbors count .....	1-15
1.1.8 display ipv6 pathmtu .....	1-15
1.1.9 display ipv6 prefix .....	1-17
1.1.10 display ipv6 rawip .....	1-18
1.1.11 display ipv6 rawip verbose .....	1-19
1.1.12 display ipv6 statistics .....	1-23
1.1.13 display ipv6 tcp .....	1-27
1.1.14 display ipv6 tcp verbose .....	1-29
1.1.15 display ipv6 udp .....	1-34
1.1.16 display ipv6 udp verbose .....	1-35
1.1.17 ipv6 address .....	1-39
1.1.18 ipv6 address anycast .....	1-40
1.1.19 ipv6 address auto .....	1-41
1.1.20 ipv6 address auto link-local .....	1-41
1.1.21 ipv6 address eui-64 .....	1-42
1.1.22 ipv6 address link-local .....	1-43
1.1.23 ipv6 hop-limit .....	1-44
1.1.24 ipv6 hoplimit-expires enable .....	1-45
1.1.25 ipv6 icmpv6 error-interval .....	1-45
1.1.26 ipv6 icmpv6 multicast-echo-reply enable .....	1-46
1.1.27 ipv6 icmpv6 source .....	1-47
1.1.28 ipv6 mtu .....	1-47
1.1.29 ipv6 nd autoconfig managed-address-flag .....	1-48
1.1.30 ipv6 nd autoconfig other-flag .....	1-49

1.1.31 ipv6 nd dad attempts .....	1-49
1.1.32 ipv6 nd ns retrans-timer.....	1-50
1.1.33 ipv6 nd snooping enable global .....	1-51
1.1.34 ipv6 nd snooping enable link-local .....	1-52
1.1.35 ipv6 nd snooping glean source.....	1-52
1.1.36 ipv6 nd snooping max-learning-num.....	1-53
1.1.37 ipv6 nd nud reachable-time .....	1-53
1.1.38 ipv6 nd ra halt .....	1-54
1.1.39 ipv6 nd ra hop-limit unspecified.....	1-55
1.1.40 ipv6 nd ra interval.....	1-55
1.1.41 ipv6 nd ra no-advlinkmtu.....	1-56
1.1.42 ipv6 nd ra prefix .....	1-57
1.1.43 ipv6 nd ra router-lifetime .....	1-58
1.1.44 ipv6 nd router-preference.....	1-59
1.1.45 ipv6 neighbor .....	1-59
1.1.46 ipv6 neighbor link-local minimize .....	1-60
1.1.47 ipv6 neighbor stale-aging.....	1-61
1.1.48 ipv6 neighbors max-learning-num .....	1-62
1.1.49 ipv6 option drop enable .....	1-62
1.1.50 ipv6 pathmtu .....	1-63
1.1.51 ipv6 pathmtu age .....	1-64
1.1.52 ipv6 prefer temporary-address .....	1-64
1.1.53 ipv6 prefix .....	1-65
1.1.54 ipv6 redirects enable.....	1-66
1.1.55 ipv6 temporary-address.....	1-66
1.1.56 ipv6 unreachable enable .....	1-68
1.1.57 local-proxy-nd enable.....	1-68
1.1.58 proxy-nd enable.....	1-69
1.1.59 reset ipv6 nd snooping .....	1-69
1.1.60 reset ipv6 neighbors .....	1-70
1.1.61 reset ipv6 pathmtu.....	1-71
1.1.62 reset ipv6 statistics.....	1-71

# 1 IPv6 基础



说明

IPv6 功能中所指的“接口”为三层接口，包括 VLAN 接口、三层以太网接口等。三层以太网接口是指在以太网接口视图下通过 **port link-mode route** 命令切换为三层模式的以太网接口，有关以太网接口模式切换的操作，请参见“二层技术-以太网交换配置指导”中的“以太网接口配置”。

## 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。

*prefix-length*: 目的地址的前缀长度，取值范围为 0~128。

#### 【使用指导】

本命令可以用来查看 IPv6 FIB 信息，包括转发的目的地址、前缀长度、转发的下一跳地址、转发报文的出接口等内容。

需要注意的是：

- 如果不指定前缀长度，将显示与指定目的 IPv6 地址最长匹配的 IPv6 FIB 信息；如果指定前缀长度时，将显示与指定目的 IPv6 地址和前缀长度精确匹配的 IPv6 FIB 信息。
- 如果不指定任何参数，则显示公网所有的 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:Useable 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
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"> <li>• U: 表示路由可用</li> <li>• G: 表示网关路由</li> <li>• H: 表示主机路由</li> <li>• B: 表示黑洞路由</li> <li>• D: 表示动态路由</li> <li>• S: 表示静态路由</li> <li>• R: 表示迭代路由</li> <li>• F: 表示快速重路由</li> </ul>
Time stamp	IPv6 FIB表项的生成时间
Label	MPLS内层标签
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。

## 【使用指导】

本命令可以用来查看设备接收和发送的各类 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

字段	描述
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/发送的回显响应报文数
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
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。

## 【使用指导】

如果配置命令时指定了 **brief** 关键字，则显示接口的摘要信息，包括接口的物理状态、链路层协议状态以及 IPv6 地址信息；否则，将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。

需要注意的是：

- 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"> <li>• <b>Administratively DOWN</b>: 表示该 VLAN 接口已经通过 <b>shutdown</b> 命令被关闭，即管理状态为关闭</li> <li>• <b>DOWN</b>: 该 VLAN 接口的管理状态为开启，但物理状态为关闭，即该接口对应的 VLAN 内没有处于 <b>UP</b> 状态的端口（可能因为没有连接好或者线路故障）</li> <li>• <b>UP</b>: 该接口的管理状态和物理状态均为开启</li> </ul>
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"> <li>• <b>DOWN</b>: 该 VLAN 接口的协议状态为关闭</li> <li>• <b>UP</b>: 该 VLAN 接口的协议状态为开启</li> </ul>
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



字段	描述
Global unicast address(es)	<p>接口上配置的全局单播地址</p> <p>可能的IPv6地址状态及含义如下：</p> <ul style="list-style-type: none"> <li>• <b>TENTATIVE</b>: 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</li> <li>• <b>DUPLICATE</b>: 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</li> <li>• <b>PREFERRED</b>: 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</li> <li>• <b>DEPRECATED</b>: 该状态表明地址有效，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需要被正常处理</li> </ul> <p>如果地址来源不为手工配置的全局单播地址，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"> <li>• <b>AUTOCFG</b>: 表示无状态自动配置的全局单播地址</li> <li>• <b>DHCP</b>: 表示 DHCPv6 服务器分配的全局单播地址</li> <li>• <b>EUI-64</b>: 表示手工配置的 EUI-64 格式全局单播地址</li> <li>• <b>RANDOM</b>: 表示自动生成的临时地址</li> </ul> <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局单播地址的有效生命期
preferred lifetime	接口上无状态自动配置的全局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 <b>ipv6 nd dad attempts</b> 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

字段	描述
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)
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

字段	描述
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 <b>shutdown</b> 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
Physical	接口的物理状态，可能的状态及含义如下： <ul style="list-style-type: none"> <li>• *down: 表示该接口已经通过 <b>shutdown</b> 命令被关闭，即管理状态为关闭</li> <li>• down: 该接口的管理状态为开启，但物理状态为关闭，即该接口对应的 VLAN 内没有处于 UP 状态的端口（可能因为没有连接好或者线路故障）</li> <li>• up: 该接口的管理状态和物理状态均为开启</li> </ul>
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"> <li>• down: 该接口的协议状态为关闭</li> <li>• up: 该接口的协议状态为开启</li> </ul>
IPv6 Address	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”

#### 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	前缀来源，包括： <ul style="list-style-type: none"><li>• STATIC: 手工配置前缀（命令 <b>ipv6 nd ra prefix</b>）</li><li>• 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</li><li>• ADDRESS: 由手工配置的地址产生的前缀</li></ul>
Age	老化时间（单位为秒），“-”表示前缀不会老化
Flag	前缀随RA报文公告时携带的标记，“-”表示没有标记 <ul style="list-style-type: none"><li>• 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</li><li>• 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</li></ul>
Lifetime	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 <ul style="list-style-type: none"><li>• Valid: 前缀的有效生命期</li><li>• Preferred: 前缀的首选生命期</li></ul>

## 【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。

## 【使用指导】

仅 Release 1122 及以上版本支持本命令。

## 【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: GE0/0/2
First VLAN ID: 1  Second VLAN ID: N/A
Status: VALID  Age: 57
```

表1 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
Status	ND Snooping表项的显示的状态, 选项如下: <ul style="list-style-type: none"> <li>• TENTATIVE: 临时非生效状态;</li> <li>• VALID: 生效状态;</li> <li>• 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;</li> <li>• 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;</li> </ul>
Age	ND Snooping表项的老化时间, 单位为秒

### 1.1.2 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。

## 【使用指导】

仅 Release 1122 及以上版本支持本命令。

## 【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2 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
Total number of entries on interface: <i>number</i>	接口下的ND Snooping表项个数

## 1.1.6 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。

**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* 的取值范围为 1~4094。

**verbose**: 显示邻居的详细信息。

## 【使用指导】

用户可以通过 **reset ipv6 neighbors** 命令清除指定的 IPv6 邻居信息。

## 【举例】

# 查看所有的邻居信息。

```
<Sysname> display ipv6 neighbors all
          Type: S-Static   D-Dynamic   O-Openflow   I-Invalid
IPv6 address          Link layer   VID Interface   State T Age
2::2                  0cda-415e-2332 N/A M-GE0/0/0     STALE D 572
FE80::EDA:41FF:FE5E:2332 0cda-415e-2332 N/A M-GE0/0/0     STALE D 562
```

# 查看所有邻居的详细信息。

```
<Sysname> display ipv6 neighbors all verbose
          Type: S-Static   D-Dynamic   O-Openflow   I-Invalid
IPv6 Address: 2::2
Link Layer  : 0cda-415e-2332      VID : N/A Interface: M-GE0/0/0
State       : STALE                Type: D Age      : 677
Vpn-instance: [No Vrf]

IPv6 Address: FE80::EDA:41FF:FE5E:2332
Link Layer  : 0cda-415e-2332      VID : N/A Interface: M-GE0/0/0
State       : STALE                Type: D Age      : 667
Vpn-instance: [No Vrf]
```

表1-6 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
Interface	与邻居相连的接口
State	邻居的状态，包括： <ul style="list-style-type: none"><li>• INCMP: 正在解析地址，邻居的链路层地址尚未确定</li><li>• REACH: 邻居可达</li><li>• 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</li><li>• DELAY: 未确定邻居是否可达，延迟一段时间发送邻居请求报文</li><li>• 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</li></ul>
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Openflow，I表示无效



字段	描述
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	VPN实例名称，[No Vrf]表示没有配置相应表项的VPN实例

### 【相关命令】

- **ipv6 neighbor**
- **reset ipv6 neighbors**

### 1.1.7 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。

**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* 的取值范围为 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
```

### 1.1.8 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。

## 【使用指导】

通过本命令可以查看 IPv6 的 PMTU 信息,包括动态创建的 PMTU 信息和静态配置的 PMTU 信息。

## 【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1-7 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**

### 1.1.9 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 业务命令参考/DHCPv6”中的命令 **ipv6 dhcp client pd**。

#### 【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1-8 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"><li>• <b>Static</b>: 表示静态 IPv6 前缀</li><li>• <b>Dynamic</b>: 表示动态 IPv6 前缀</li></ul>
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**

### 1.1.10 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。

### 【使用指导】

本命令可以用来查看 IPv6 RawIP 连接摘要信息，包括本端 IPv6 地址、对端 IPv6 地址、使用 IPv6 RawIP socket 的协议号等信息。

### 【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      1    0x0000000000000008
::              ::              58      1    0x0000000000000002
```

表1-9 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

字段	描述
Protocol	使用IPv6 RawIP socket的协议号
Slot	设备在IRF中的成员编号
PCB	协议控制块索引

### 1.1.11 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。

#### 【使用指导】

本命令可以用来查看 IPv6 RawIP 连接详细信息，包括 socket 的创建者、状态、选项、类型、使用的协议号等，以及 IPv6 RawIP 连接的源 IPv6 地址和目的 IPv6 地址等信息。

#### 【举例】

# 显示 IPv6 RawIP 连接详细信息。

```
<Sysname> display ipv6 rawip verbose
Total RawIP socket number: 1
Slot: 6
Creator: ping ipv6[320]
State: N/A
Options: N/A
Error: 0
Receiving buffer(cc/hiwat/lowat/state): 0 / 9216 / 1 / 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 vflag: INP_IPV6
Hop limit: 255 (minimum hop limit: 0)
Send VRF: 0xffff
Receive VRF: 0xffff

```

表1-10 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
Slot	设备在IRF中的成员编号
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"> <li>• NOFDREF：用户已经关闭</li> <li>• ISCONNECTED：连接已经建立</li> <li>• ISCONNECTING：正在建立连接</li> <li>• ISDISCONNECTING：正在断开连接</li> <li>• ASYNC：异步方式</li> <li>• ISDISCONNECTED：连接已经断开</li> <li>• PROTOREF：协议强关联</li> <li>• N/A：不处于上述状态</li> </ul>

字段	描述
Options	<p>socket的选项，有以下几种：</p> <ul style="list-style-type: none"> <li>• SO_DEBUG: 记录套接字的调试信息</li> <li>• SO_ACCEPTCONN: server 端监听连接请求</li> <li>• SO_REUSEADDR: 允许本地地址重复使用</li> <li>• SO_KEEPAVIVE: 协议需要查询空闲的连接</li> <li>• SO_DONTROUTE: 设置不查路由表，由于目的地址是直连网络的情况</li> <li>• SO_BROADCAST: 套接字支持广播报文</li> <li>• SO_LINGER: 套接字关闭但仍发送剩余数据</li> <li>• SO_OOBINLINE: 带外数据采用内联方式存储</li> <li>• SO_REUSEPORT: 允许本地端口重复使用</li> <li>• 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</li> <li>• SO_NOSIGPIPE: socket 不能发送数据导致返回失败时不创建 SIGPIPE</li> <li>• SO_TIMESTAMPNS: 和时戳选项功能类似，时间可以精确到纳秒</li> <li>• SO_KEEPAVIVETIME: 设置空闲探测时间，TCP 支持此选项</li> <li>• SO_FILTER: 设置报文过滤条件，OSI Socket 和 RawIP 支持此选项</li> <li>• N/A: 没有设置选项</li> </ul>
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 状态的取值有：</p> <ul style="list-style-type: none"> <li>• CANTSENDMORE: 不能发送数据到对端</li> <li>• CANTRCVMORE: 不能从对端接收数据</li> <li>• RCVATMARK: 接收标记</li> <li>• N/A: 不处于上述状态</li> </ul>
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"> <li>• CANTSENDMORE: 不能发送数据到对端</li> <li>• CANTRCVMORE: 不能从对端接收数据</li> <li>• RCVATMARK: 接收标记</li> <li>• N/A: 不处于上述状态</li> </ul>

字段	描述
Type	<p>使用的socket类型，类型的取值有：</p> <ul style="list-style-type: none"> <li>• 1: SOCK_STREAM, 流模式，提供可靠的字节流。TCP 协议使用此类型</li> <li>• 2: SOCK_DGRAM, 数据报模式的通信。UDP 协议使用此类型</li> <li>• 3: SOCK_RAW, RAW 模式的通信方式</li> <li>• N/A: 不是上述类型</li> </ul>
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
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"> <li>• INP_RECVOPTS: 接收传入的 IPv6 选项</li> <li>• INP_RECVRETOPTS: 接收回应的 IPv6 选项</li> <li>• INP_RECVDSTADDR: 接收目的 IPv6 地址</li> <li>• INP_HDRINCL: 用户提供整个 IPv6 头</li> <li>• INP_REUSEADDR: 重复使用地址</li> <li>• INP_REUSEPORT: 重复使用端口号</li> <li>• INP_ANONPORT: 用户未指定端口</li> <li>• INP_PROTOCOL_PACKET: 标识报文为协议报文</li> <li>• INP_RCVVLANID: 接收报文的 VLAN ID, 仅 UDP 和 RawIP 支持</li> <li>• IN6P_IPV6_V6ONLY: 仅支持 IPv6 协议栈</li> <li>• IN6P_PKTINFO: 接收报文的源地址和入接口</li> <li>• IN6P_HOPLIMIT: 接收报文 hoplimit</li> <li>• IN6P_HOPOPTS: 接收报文的逐跳扩展头信息</li> <li>• IN6P_DSTOPTS: 接收报文的扩展头信息</li> <li>• IN6P_RTHDR: 接收报文的由路由扩展头信息</li> <li>• IN6P_RTHDRDSTOPTS: 接收报文的由路由头前的目的扩展头信息</li> <li>• IN6P_TCLASS: 接收报文的优先级信息</li> <li>• IN6P_AUTOFLOWLABEL: 使用随机流标签</li> <li>• IN6P_RFC2292: 使用 RFC2292 API</li> <li>• IN6P_MTU: 感知路径 MTU 的变化, TCP 不支持</li> <li>• INP_RCVMACADDR: 接收报文的 MAC</li> <li>• INP_USEICMPSRC: 使用配置的 ICMPv6 地址作为源地址</li> <li>• INP_SYNCPCB: 阻塞等待 inpcb 同步</li> <li>• N/A: 不是上述标记</li> </ul>



字段	描述
Inpcb vflag	Internet协议控制块中的IP版本标记，标记的取值有： <ul style="list-style-type: none"> <li>• INP_IPV4: 运用与 IPv4 通信</li> <li>• INP_IPV6: 运用与 IPv6 通信</li> <li>• INP_IPV6PROTO: 运用 IPv6 协议创建的 inpcb</li> <li>• INP_TIMEWAIT: 处于等待状态</li> <li>• INP_ONESBCAST: 发送广播报文</li> <li>• INP_DROPPED: 协议丢弃标志</li> <li>• INP_SOCKETREF: socket 强关联</li> <li>• INP_DONTBLOCK: inpcb 同步时不能被阻塞</li> <li>• N/A: 不是上述标记</li> </ul>
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

### 1.1.12 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。

#### 【使用指导】

本命令可以用来查看设备接收和发送 IPv6 报文及 ICMPv6 报文的统计信息。

用户可以通过 **reset ipv6 statistics** 命令清除所有的 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
  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1-11 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> <ul style="list-style-type: none"> <li>Total:</li> <li>    Sent locally:</li> <li>    Forwarded:</li> <li>Raw packets:</li> <li>Discarded:</li> <li>Fragments:</li> <li>Fragments failed:</li> <li>Routing failed:</li> </ul>	<p>发送IPv6报文的统计信息，包括：</p> <ul style="list-style-type: none"> <li>• 本地发送报文和转发报文的总数</li> <li>• 本地发送报文数</li> <li>• 转发报文数</li> <li>• 使用 raw socket 发送的报文数</li> <li>• 丢弃报文数</li> <li>• 发送分片报文数</li> <li>• 分片报文发送失败的个数</li> <li>• 路由失败报文数</li> </ul>
<p>Received packets:</p> <ul style="list-style-type: none"> <li>Total:</li> <li>    Received locally:</li> <li>    Hop limit exceeded:</li> <li>    Fragments:</li> <li>    Reassembled:</li> <li>    Reassembly failures:</li> <li>    Reassembly timeout:</li> <li>    Format errors:</li> <li>    Option errors:</li> <li>    Protocol errors:</li> </ul>	<p>接收IPv6报文的统计信息，包括：</p> <ul style="list-style-type: none"> <li>• 接收报文总数</li> <li>• 本地接收报文数，即目的地是本机的报文数</li> <li>• 超出跳数范围的报文数</li> <li>• 接收的分片报文数</li> <li>• 重组报文数</li> <li>• 重组失败的报文数</li> <li>• 重组超时的报文数</li> <li>• 格式错误的报文数</li> <li>• 选项错误的报文数</li> <li>• 协议错误的报文数</li> </ul>
<p>ICMPv6 statistics:</p>	<p>ICMPv6报文的统计信息</p>

字段	描述
<p>Sent packets:</p> <p>  Total:</p> <p>    Unreached:</p> <p>    Too big:</p> <p>    Hop limit exceeded:</p> <p>    Reassembly timeouts:</p> <p>    Parameter problems:</p> <p>    Echo requests:</p> <p>    Echo replies:</p> <p>    Neighbor solicits:</p> <p>    Neighbor adverts:</p> <p>    Router solicits:</p> <p>    Router adverts:</p> <p>    Redirects:</p> <p>    Router Renumbering</p> <p>Sent failed:</p> <p>  Rate limitation:</p> <p>  Other errors:</p>	<p>发送ICMPv6报文的统计信息，包括：</p> <ul style="list-style-type: none"> <li>• 发送报文总数</li> <li>• 目的不可达报文数</li> <li>• 报文太长的报文数</li> <li>• 超出跳数限制的报文数</li> <li>• 分片重组超时报文数</li> <li>• 参数错误报文数</li> <li>• 回应请求报文数</li> <li>• 回应响应报文数</li> <li>• 邻居请求报文数</li> <li>• 邻居通告报文数</li> <li>• 路由器请求报文数</li> <li>• 路由器通告报文数</li> <li>• 重定向报文数</li> <li>• 本机发送失败的报文数</li> <li>• 因速率超过限制而未发送的报文数</li> <li>• 其他错误的报文数</li> </ul>

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"> <li>接收报文总数</li> </ul>
Checksum errors:	<ul style="list-style-type: none"> <li>校验和错误的报文数</li> </ul>
Too short:	<ul style="list-style-type: none"> <li>报文太短的报文数</li> </ul>
Bad codes:	<ul style="list-style-type: none"> <li>错误代码的报文数</li> </ul>
Unreachable:	<ul style="list-style-type: none"> <li>不可达报文数</li> </ul>
Too big:	<ul style="list-style-type: none"> <li>报文太长的报文数</li> </ul>
Hop limit exceeded:	<ul style="list-style-type: none"> <li>超出跳数限制的报文数</li> </ul>
Reassembly timeouts:	<ul style="list-style-type: none"> <li>分片重组超时的报文数</li> </ul>
Parameter problems:	<ul style="list-style-type: none"> <li>参数错误报文数</li> </ul>
Unknown error types:	<ul style="list-style-type: none"> <li>未知错误报文数</li> </ul>
Echo requests:	<ul style="list-style-type: none"> <li>回应请求报文数</li> </ul>
Echo replies:	<ul style="list-style-type: none"> <li>回应响应报文数</li> </ul>
Neighbor solicits:	<ul style="list-style-type: none"> <li>邻居请求报文数</li> </ul>
Neighbor adverts:	<ul style="list-style-type: none"> <li>邻居通告报文数</li> </ul>
Router solicits:	<ul style="list-style-type: none"> <li>路由器请求报文数</li> </ul>
Router adverts:	<ul style="list-style-type: none"> <li>路由器通告报文数</li> </ul>
Redirects:	<ul style="list-style-type: none"> <li>重定向报文数</li> </ul>
Router renumbering:	<ul style="list-style-type: none"> <li>路由器 IPv6 地址重新分配报文数</li> </ul>
Unknown info types:	<ul style="list-style-type: none"> <li>未知信息报文数</li> </ul>
Deliver failed:	<ul style="list-style-type: none"> <li>上送本机失败的报文数</li> </ul>
Bad length:	<ul style="list-style-type: none"> <li>长度错误的报文数</li> </ul>

### 【相关命令】

- **reset ipv6 statistics**

### 1.1.13 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。

### 【使用指导】

本命令可以用来查看 IPv6 TCP 连接摘要信息，包括本端 IPv6 地址及端口号、对端 IPv6 地址及端口号、TCP 连接的状态等信息。

### 【举例】

# 显示 IPv6 TCP 连接摘要信息。

```
<Sysname> display ipv6 tcp
*: TCP MD5 Connection
  LAddr->port      FAddr->port      State           Slot PCB
*2001:2002:2003:2  3001:3002:3003:3 ESTABLISHED     1    0x00000000000000c387
004:2005:2006:20  004:3005:3006:30
07:2008->1200      07:3008->1200
2001::1->23         2001::5->1284    ESTABLISHED     1    0x0000000000000008
2003::1->25         2001::2->1283    LISTEN          1    0x0000000000000009
```

表1-12 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MD5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

字段	描述
State	<p>TCP连接状态，可能的状态如下：</p> <ul style="list-style-type: none"> <li>• CLOSED：服务器收到客户端的关闭连接请求回应后所处的状态</li> <li>• LISTEN：服务器在等待连接请求时所处的状态</li> <li>• SYN_SENT：客户端发出连接请求等待服务器回应时所处的状态</li> <li>• SYN_RCVD：服务器收到客户端连接请求时所处的状态</li> <li>• 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</li> <li>• CLOSE_WAIT：服务器收到客户端关闭连接请求时所处的状态</li> <li>• 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</li> <li>• 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</li> <li>• 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</li> <li>• FIN_WAIT_2：客户端收到服务器关闭连接回应后所处的状态</li> <li>• TIME_WAIT：客户端收到服务器的关闭连接请求后所处的状态</li> </ul>
Slot	设备在IRF中的成员编号
PCB	协议控制块索引

### 1.1.14 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。

## 【使用指导】

本命令可以用来查看 IPv6 TCP 连接详细信息，包括 socket 的创建者、状态、选项、类型、使用的协议号等，以及 IPv6 TCP 连接的源 IPv6 地址及端口号、目的 IPv6 地址及端口号、状态等信息。

## 【举例】

```
# 显示 IPv6 TCP 连接详细信息。
<Sysname> display ipv6 tcp verbose
TCP inpcb number: 1(tcpcb number: 1)

Slot: 6
Creator: telnetd_mips[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->23 , dst = 2001::2->4181
Inpcb flags: N/A
Inpcb vflag: INP_IPV6
Hop limit: 255 (minimum hop limit: 0)
Connection state: ESTABLISHED
Send VRF: 0x0
Receive VRF: 0x0
```

表1-13 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）
Slot	设备在IRF中的成员编号
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"> <li>• NOFDREF：用户已经关闭</li> <li>• ISCONNECTED：连接已经建立</li> <li>• ISCONNECTING：正在建立连接</li> <li>• ISDISCONNECTING：正在断开连接</li> <li>• ASYNC：异步方式</li> <li>• ISDISCONNECTED：连接已经断开</li> <li>• PROTOREF：协议强关联</li> <li>• N/A：不处于上述状态</li> </ul>
Options	<p>socket的选项，有以下几种：</p> <ul style="list-style-type: none"> <li>• SO_DEBUG：记录套接字的调试信息</li> <li>• SO_ACCEPTCONN：server 端监听连接请求</li> <li>• SO_REUSEADDR：允许本地地址重复使用</li> <li>• SO_KEEPALIVE：协议需要查询空闲的连接</li> <li>• SO_DONTROUTE：设置不查路由表，由于目的地址是直连网络的情况</li> <li>• SO_BROADCAST：套接字支持广播报文</li> <li>• SO_LINGER：套接字关闭但仍发送剩余数据</li> <li>• SO_OOBINLINE：带外数据采用内联方式存储</li> <li>• SO_REUSEPORT：允许本地端口重复使用</li> <li>• SO_NOSIGPIPE：socket 不能发送数据导致返回失败时不创建 SIGPIPE</li> <li>• SO_TIMESTAMPNS：和时戳选项功能类似，时间可以精确到纳秒</li> <li>• N/A：没有设置选项</li> </ul>
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、状态 状态的取值有：</p> <ul style="list-style-type: none"> <li>• CANTSENDMORE：不能发送数据到对端</li> <li>• CANTRCVMORE：不能从对端接收数据</li> <li>• RCVATMARK：接收标记</li> <li>• N/A：不处于上述状态</li> </ul>

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"> <li>• CANTSENDMORE：不能发送数据到对端</li> <li>• CANTRCVMORE：不能从对端接收数据</li> <li>• RCVATMARK：接收标记</li> <li>• N/A：不处于上述状态</li> </ul>
Type	<p>使用的socket类型，类型的取值有：</p> <ul style="list-style-type: none"> <li>• 1：SOCK_STREAM，流模式，提供可靠的字节流。TCP 协议使用此类型</li> <li>• 2：SOCK_DGRAM，数据报模式的通信。UDP 协议使用此类型</li> <li>• 3：SOCK_RAW，RAW 模式的通信方式</li> <li>• N/A：不是上述类型</li> </ul>
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"> <li>• INP_RECVOPTS: 接收传入的 IPv6 选项</li> <li>• INP_RECVRETOPTS: 接收回应的 IPv6 选项</li> <li>• INP_RECVDSTADDR: 接收目的 IPv6 地址</li> <li>• INP_HDRINCL: 用户提供整个 IPv6 头</li> <li>• INP_REUSEADDR: 重复使用地址</li> <li>• INP_REUSEPORT: 重复使用端口号</li> <li>• INP_ANONPORT: 用户未指定端口</li> <li>• INP_PROTOCOL_PACKET: 标识报文为协议报文</li> <li>• INP_RCVVLANID: 接收报文的 VLAN ID, 仅 UDP 和 RawIP 支持</li> <li>• IN6P_IPV6_V6ONLY: 仅支持 IPv6 协议栈</li> <li>• IN6P_PKTINFO: 接收报文的源地址和入接口</li> <li>• IN6P_HOPLIMIT: 接收报文 hoplimit</li> <li>• IN6P_HOPOPTS: 接收报文的逐跳扩展头信息</li> <li>• IN6P_DSTOPTS: 接收报文的的目的扩展头信息</li> <li>• IN6P_RTHDR: 接收报文的路由扩展头信息</li> <li>• IN6P_RTHDRDSTOPTS: 接收报文的路由头前的目的扩展头信息</li> <li>• IN6P_TCLASS: 接收报文的优先级信息</li> <li>• IN6P_AUTOFLOWLABEL: 使用随机流标签</li> <li>• IN6P_RFC2292: 使用 RFC2292 API</li> <li>• IN6P_MTU: 感知路径 MTU 的变化, TCP 不支持</li> <li>• INP_RCVMACADDR: 接收报文的 MAC</li> <li>• INP_SYNCPCB: 阻塞等待 inpcb 同步</li> <li>• N/A: 不是上述标记</li> </ul>
Inpcb vflag	<p>Internet协议控制块中的IP版本标记：</p> <ul style="list-style-type: none"> <li>• INP_IPV4: 运用与 IPv4 通信</li> <li>• INP_IPV6: 运用与 IPv6 通信</li> <li>• INP_IPV6PROTO: 运用 IPv6 协议创建的 inpcb</li> <li>• INP_TIMEWAIT: 处于等待状态</li> <li>• INP_ONESBCAST: 发送广播报文</li> <li>• INP_DROPPED: 协议丢弃标志</li> <li>• INP_SOCKETREF: socket 强关联</li> <li>• INP_DONTBLOCK: inpcb 同步时不能被阻塞</li> <li>• N/A: 不是上述标记</li> </ul>

字段	描述
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"> <li>• CLOSED：服务器收到客户端的关闭连接请求回应后所处的状态</li> <li>• LISTEN：服务器在等待连接请求时所处的状态</li> <li>• SYN_SENT：客户端发出连接请求等待服务器回应时所处的状态</li> <li>• SYN_RCVD：服务器收到客户端连接请求时所处的状态</li> <li>• 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</li> <li>• CLOSE_WAIT：服务器收到客户端关闭连接请求时所处的状态</li> <li>• 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</li> <li>• 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</li> <li>• 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</li> <li>• FIN_WAIT_2：客户端收到服务器关闭连接回应后所处的状态</li> <li>• TIME_WAIT：客户端收到服务器的关闭连接请求后所处的状态</li> </ul>
Send VRF	发送实例
Receive VRF	接收实例

### 1.1.15 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。

### 【使用指导】

本命令可以用来查看 IPv6 UDP 连接摘要信息，包括本端 IPv6 地址及端口号、对端 IPv6 地址及端口号等信息。

### 【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     0x000000000000c387
004:2005:2006:20 004:3005:3006:30
07:2008->1200    07:3008->1200
2001::1->23      2001::5->1284    1     0x0000000000000008
2003::1->25      2001::2->1283    1     0x0000000000000009
```

表1-14 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
Slot	设备在IRF中的成员编号
PCB	协议控制块索引

### 1.1.16 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。

## 【使用指导】

本命令可以用来查看 IPv6 UDP 连接详细信息，包括 socket 的创建者、状态、选项、类型、使用的协议号等，以及 IPv6 UDP 连接的源 IPv6 地址及端口号、目的 IPv6 地址及端口号等信息。

## 【举例】

# 显示 IPv6 UDP 连接详细信息。

```
<Sysname> display ipv6 udp verbose
Total UDP socket number: 1

Slot: 6
Creator: sock_test_mips[250]
State: N/A
Options: N/A
Error: 0
Receiving buffer(cc/hiwat/lowat/state): 0 / 41600 / 1 / 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 vflag: INP_IPV6
Hop limit: 255 (minimum hop limit: 0)
Send VRF: 0xffff
Receive VRF: 0xffff
```

表1-15 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
Slot	设备在IRF中的成员编号
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"><li>• NOFDREF：用户已经关闭</li><li>• ISCONNECTED：连接已经建立</li><li>• ISCONNECTING：正在建立连接</li><li>• ISDISCONNECTING：正在断开连接</li><li>• ASYNC：异步方式</li><li>• ISDISCONNECTED：连接已经断开</li><li>• PROTOREF：协议强关联</li><li>• N/A：不处于上述状态</li></ul>

字段	描述
Options	<p>socket的选项，有以下几种：</p> <ul style="list-style-type: none"> <li>• SO_DEBUG：记录套接字的调试信息</li> <li>• SO_ACCEPTCONN：server 端监听连接请求</li> <li>• SO_REUSEADDR：允许本地地址重复使用</li> <li>• SO_KEEPAIVE：协议需要查询空闲的连接</li> <li>• SO_DONTROUTE：设置不查路由表，由于目的地址是直连网络的情况</li> <li>• SO_BROADCAST：套接字支持广播报文</li> <li>• SO_LINGER：套接字关闭但仍发送剩余数据</li> <li>• SO_OOBINLINE：带外数据采用内联方式存储</li> <li>• SO_REUSEPORT：允许本地端口重复使用</li> <li>• 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</li> <li>• SO_NOSIGPIPE：socket 不能发送数据导致返回失败时不创建 SIGPIPE</li> <li>• SO_TIMESTAMPNS：和时戳选项功能类似，时间可以精确到纳秒</li> <li>• SO_KEEPAIVETIME：设置空闲探测时间，TCP 支持此选项</li> <li>• SO_FILTER：设置报文过滤条件，OSI Socket 和 RawIP 支持此选项</li> <li>• N/A：没有设置选项</li> </ul>
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、状态 状态的取值有：</p> <ul style="list-style-type: none"> <li>• CANTSENDMORE：不能发送数据到对端</li> <li>• CANTRCVMORE：不能从对端接收数据</li> <li>• RCVATMARK：接收标记</li> <li>• N/A：不处于上述状态</li> </ul>
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 状态的取值有：</p> <ul style="list-style-type: none"> <li>• CANTSENDMORE：不能发送数据到对端</li> <li>• CANTRCVMORE：不能从对端接收数据</li> <li>• RCVATMARK：接收标记</li> <li>• N/A：不处于上述状态</li> </ul>

字段	描述
Type	<p>使用的socket类型，类型的取值有：</p> <ul style="list-style-type: none"> <li>• 1: SOCK_STREAM, 流模式，提供可靠的字节流。TCP 协议使用此类型</li> <li>• 2: SOCK_DGRAM, 数据报模式的通信。UDP 协议使用此类型</li> <li>• 3: SOCK_RAW, RAW 模式的通信方式</li> <li>• N/A: 不是上述类型</li> </ul>
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
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"> <li>• INP_RECVOPTS: 接收传入的 IPv6 选项</li> <li>• INP_RECVRETOPTS: 接收回应的 IPv6 选项</li> <li>• INP_RECVDSTADDR: 接收目的 IPv6 地址</li> <li>• INP_HDRINCL: 用户提供整个 IPv6 头</li> <li>• INP_REUSEADDR: 重复使用地址</li> <li>• INP_REUSEPORT: 重复使用端口号</li> <li>• INP_ANONPORT: 用户未指定端口</li> <li>• INP_PROTOCOL_PACKET: 标识报文为协议报文</li> <li>• INP_RCVVLANID: 接收报文的 VLAN ID, 仅 UDP 和 RawIP 支持</li> <li>• IN6P_IPV6_V6ONLY: 仅支持 IPv6 协议栈</li> <li>• IN6P_PKTINFO: 接收报文的源地址和入接口</li> <li>• IN6P_HOPLIMIT: 接收报文 hoplimit</li> <li>• IN6P_HOPOPTS: 接收报文的逐跳扩展头信息</li> <li>• IN6P_DSTOPTS: 接收报文的扩展头信息</li> <li>• IN6P_RTHDR: 接收报文的路由扩展头信息</li> <li>• IN6P_RTHDRDSTOPTS: 接收报文的路由头前的扩展头信息</li> <li>• IN6P_TCLASS: 接收报文的优先级信息</li> <li>• IN6P_AUTOFLOWLABEL: 使用随机流标签</li> <li>• IN6P_RFC2292: 使用 RFC2292 API</li> <li>• IN6P_MTU: 感知路径 MTU 的变化, TCP 不支持</li> <li>• INP_RCVMACADDR: 接收报文的 MAC</li> <li>• INP_SYNCPCB: 阻塞等待 inpcb 同步</li> <li>• N/A: 不是上述标记</li> </ul>



字段	描述
Inpcb vflag	Internet协议控制块中的IP版本标记，标记的取值有： <ul style="list-style-type: none"> <li>• INP_IPV4: 运用与 IPv4 通信</li> <li>• INP_IPV6: 运用与 IPv6 通信</li> <li>• INP_IPV6PROTO: 运用 IPv6 协议创建的 inpcb</li> <li>• INP_TIMEWAIT: 处于等待状态</li> <li>• INP_ONESBCAST: 发送广播报文</li> <li>• INP_DROPPED: 协议丢弃标志</li> <li>• INP_SOCKREF: socket 强关联</li> <li>• INP_DONTBLOCK: inpcb 同步时不能被阻塞</li> <li>• N/A: 不是上述标记</li> </ul>
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

### 1.1.17 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】

接口上没有配置 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。

需要注意的是，**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
```

## 1.1.18 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】

接口上没有配置 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
```

### 1.1.19 ipv6 address auto

**ipv6 address auto** 命令用来使能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
```

### 1.1.20 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** 命令用来删除接口自动生成的链路本地地址。

#### 【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。

需要注意的是：

- 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；如果此时接口没有配置任何 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**

### 1.1.21 ipv6 address eui-64

**ipv6 address eui-64** 命令用来给接口配置 EUI-64 格式的全球单播地址。

**undo ipv6 address eui-64** 命令用来删除接口上已配置的 EUI-64 格式的全球单播地址。

## 【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】

接口上没有配置 EUI-64 格式的全球单播地址。

## 【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。

需要注意的是，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**

### 1.1.22 ipv6 address link-local

**ipv6 address link-local** 命令用来手动配置指定接口的链路本地地址。

**undo ipv6 address link-local** 命令用来删除接口上手动配置的链路本地地址。

## 【命令】

```
ipv6 address ipv6-address link-local
undo ipv6 address ipv6-address link-local
```

## 【缺省情况】

接口上没有手动配置的链路本地地址。

## 【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**

### 1.1.23 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。
- 如果用户配置了在 RA 消息中发布本设备的跳数限制（配置命令 **undo ipv6 nd hop-limit unspecified**），则设备发送的 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。

•

#### 【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 hop-limit unspecified**

### 1.1.24 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。

需要注意的是，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
```

### 1.1.25 ipv6 icmpv6 error-interval

**ipv6 icmpv6 error-interval** 命令用来配置指定时间内发送 ICMPv6 差错报文的最大个数。

**undo ipv6 icmpv6 error-interval** 命令用来恢复缺省情况。

#### 【命令】

```
ipv6 icmpv6 error-interval milliseconds [ bucketsize ]
undo ipv6 icmpv6 error-interval
```

#### 【缺省情况】

令牌桶容量为 10，令牌桶的刷新周期为 100 毫秒，即每一个刷新周期内最多可以发送 10 个 ICMPv6 差错报文。

#### 【视图】

系统视图

### 【缺省用户角色】

network-admin

### 【参数】

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

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

### 【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，即每隔多长时间将令牌桶内的令牌个数刷新为所配置的容量。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】

# 配置设备每 200 毫秒最多发送 40 个 ICMPv6 差错报文。

```
<Sysname> system-view  
[Sysname] ipv6 icmpv6 error-interval 200 40
```

## 1.1.26 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** 命令用来配置不允许设备回复组播形式的 Echo request 报文。

### 【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
```

### 1.1.27 ipv6 icmpv6 source

**ipv6 icmpv6 source** 命令用来配置 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
```

### 1.1.28 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 mtu-size
undo ipv6 mtu
```

### 【缺省情况】

没有配置接口 MTU。

### 【视图】

接口视图

### 【缺省用户角色】

network-admin

### 【参数】

**mtu-size**: 接口 MTU 的大小, 单位为字节。对于 Release 1118P02 版本, 取值范围为 1280~1500; 对于 Release 1122 及以上版本, 取值范围为 1280~9216。

### 【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, 同时会将转发接口的 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
```

## 1.1.29 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
```

### 1.1.30 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
```

### 1.1.31 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 value**

## 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】

**value:** 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**

## 1.1.32 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**

## 1.1.33 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

### 【使用指导】

仅 Release 1122 及以上版本支持本命令。

### 【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
```

### 1.1.34 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

#### 【使用指导】

仅 Release 1122 及以上版本支持本命令。

#### 【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
```

### 1.1.35 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 内非信任口必须开启 IPv6 Source Guard 功能，否则会导致该口的报文不能正常转发。

仅 Release 1122 及以上版本支持本命令。

### 【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
```

## 1.1.36 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】

接口下允许 ND Snooping 学习表项的最大个数为 8192。

### 【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 1~8192。

### 【使用指导】

仅 Release 1122 及以上版本支持本命令。

### 【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
```

## 1.1.37 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 value  
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】**

*value*: 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**

### 1.1.38 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
```

## 1.1.39 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**

## 1.1.40 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-value min-interval-value
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-value*: 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-value*: 指定 RA 消息发布的最小时间间隔，取值范围是 3~(*max-interval-value* \* 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。

需要注意的是，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**

#### 1.1.41 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
```

### 1.1.42 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** 命令用来取消 RA 消息中前缀信息的配置。

## 【命令】

```
ipv6 nd ra prefix { ipv6-prefix prefix-length | ipv6-prefix/prefix-length } valid-lifetime
preferred-lifetime [ no-autoconfig | off-link ] *
undo ipv6 nd ra prefix { ipv6-prefix | ipv6-prefix/prefix-length }
```

## 【缺省情况】

没有配置 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。

*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。

**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。

## 【使用指导】

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。

### 【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
```

### 1.1.43 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 value**

**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】

**value:** 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。

需要注意的是，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 neighbor

**ipv6 neighbor** 命令用来配置静态邻居表项。

**undo ipv6 neighbor** 命令用来删除静态邻居表项。

#### 【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】

设备上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】

将邻居节点的 IPv6 地址解析为链路层地址，可以通过邻居请求消息 NS 及邻居通告消息 NA 来动态实现，也可以通过手工配置静态邻居表项来实现。

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对应的邻居节点的 IPv6 地址、链路层地址；
- 配置本节点 VLAN 中的端口对应的邻居节点的 IPv6 地址、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。设备解析到 VLAN 对应的二层端口信息后，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 VLAN 所对应的 VLAN 接口已经存在，且 *port-type port-number* 指定的二层端口属于 *vlan-id* 指定的 VLAN。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。

在删除 VLAN 接口对应的静态邻居表项时，只需要指定 VLAN 对应的 VLAN 接口即可。

## 【举例】

# 配置接口 Vlan-interface1 对应的静态邻居表项。

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

```
[Sysname] ipv6 neighbor 1::1 1-1-1 interface Vlan-interface 1
```

## 【相关命令】

- **display ipv6 neighbors**
- **reset ipv6 neighbors**

### 1.1.46 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。缺省情况下，所有 ND 表项均会下发硬件表项。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
```

## 1.1.47 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。

用户可以根据网络实际情况调整老化时间。

#### 【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
```

### 1.1.48 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** *number*

**undo ipv6 neighbors max-learning-num**

#### 【缺省情况】

接口上允许学习的动态邻居表项的最大个数为 4096。

#### 【视图】

二层接口视图/二层聚合接口视图/三层接口视图/三层聚合接口视图

#### 【缺省用户角色】

network-admin

#### 【参数】

*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 1~4096。

#### 【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
```

### 1.1.49 ipv6 option drop enable

**ipv6 option drop enable** 命令用来开启设备对于带有扩展头的 IPv6 报文的丢弃功能。

**undo ipv6 option drop enable** 命令用来关闭设备对于带有扩展头的 IPv6 报文的丢弃功能。

#### 【命令】

**ipv6 option drop enable**

**undo ipv6 option drop enable**



### 【缺省情况】

设备对于带有扩展头的 IPv6 报文的丢弃功能处于关闭状态。

### 【视图】

系统视图

### 【缺省用户角色】

network-admin

### 【使用指导】

配置本功能后：

- 如果接收到带有逐跳扩展报文头的 IPv6 报文，设备将直接丢弃。
- 如果接收到携带一层其它扩展报文头的 IPv6 报文，设备将正常转发。
- 如果接收到携带两层或两层以上其它扩展报文头的 IPv6 报文，设备将直接丢弃。

### 【举例】

# 开启设备对于带有扩展头的 IPv6 报文的丢弃功能。

```
<Sysname> system-view  
[Sysname] ipv6 option drop enable
```

## 1.1.50 ipv6 pathmtu

**ipv6 pathmtu** 命令用来配置指定 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】

没有配置静态 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**

### 1.1.51 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，源端主机会通过 PMTU 机制重新确定发送报文的 MTU 值。

需要注意的是，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**

### 1.1.52 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** 命令用来恢复缺省情况。

#### 【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**

## 1.1.53 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】

设备上不存在任何静态 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】

- 不允许通过重复执行 **ipv6 prefix** 命令来修改已经创建的静态 IPv6 前缀。
- 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**

### 1.1.54 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
```

### 1.1.55 ipv6 temporary-address

**ipv6 temporary-address** 命令用来配置系统生成临时地址。

**undo ipv6 temporary-address** 命令用来取消系统生成临时地址功能，同时会删除已经存在的临时地址。

## 【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 秒 (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 秒 (1 天)。*preferred-lifetime* 的值要小于等于 *valid-lifetime* 的值。

## 【使用指导】

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。

需要注意的是:

- 配置本功能时需要打开地址无状态自动配置功能。
- 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和 (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和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**

### 1.1.56 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 unreachable 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 unreachable enable  
undo ipv6 unreachable 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 unreachable enable
```

### 1.1.57 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** 命令用来恢复缺省情况。

#### 【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/三层以太网接口视图

### 【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**

## 1.1.58 proxy-nd enable

**proxy-nd enable** 命令用来开启 ND Proxy 功能。

**undo proxy-nd enable** 命令用来恢复缺省情况。

### 【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/三层以太网接口视图

### 【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**

## 1.1.59 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。

### 【使用指导】

仅 Release 1122 及以上版本支持本命令。

### 【举例】

```
# 清除设备上的 ND Snooping 表项。
<Sysname> reset ipv6 nd snooping
```

## 1.1.60 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。

**static**: 清除所有接口上的静态邻居信息。

### 【使用指导】

当前的 IPv6 邻居信息可以通过 **display ipv6 neighbors** 命令查看。

### 【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
```

#### 【相关命令】

- **display ipv6 neighbors**
- **ipv6 neighbor**

### 1.1.61 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**

### 1.1.62 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。

### 【使用指导】

当前的 IPv6 报文及 ICMPv6 报文的统计信息可以通过 **display ipv6 statistics** 命令查看。

### 【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**