H3C SecPath 防火墙产品

NAT 命令参考(V7)

新华三技术有限公司
http://www.h3c.com

资料版本：6W203-20191125
产品版本：

F100-C-EI/F100-C-G2/F100-S-G2/F100-M-G2/F100-C60-WiNet/F100-C80-WiNet/F1000-C8150/F1000-C8130/F1000-C8120/F100-C-A3/F100-C-A5/F100-C-A6	R9514
F100-A-G2/F100-A-EI/F100-E-G2/F100-E-EI/F100-A-SI/F1000-C-EI/F1000-C-G2/F1000-S-G2/F1000-A-G2/F1000-E-G2/F1000-C8180/F1000-C8170/F1000-C8160	R9323

前 言

本命令参考介绍了防火墙产品各软件特性的配置命令行，包括每条命令对应的视图、参数、缺省级别、用途描述和举例等。《NAT 命令参考》主要介绍 NAT 和 AFT 相关的命令。

前言部分包含如下内容：

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。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... }*	表示从多个选项中至少选取一个。
[x | y | ...]*	表示从多个选项中选取一个、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 NAT 命令

1.1 NAT配置命令

1.1.1 address

address 命令用来添加一个地址组成员。

undo address 命令用来删除一个地址组成员。

【命令】

address *start-address end-address*

undo address *start-address end-address*

【缺省情况】

不存在地址组成员。

【视图】

NAT 地址组视图

【缺省用户角色】

network-admin

context-admin

【参数】

start-address end-address：地址组成员的起始 IP 地址和结束 IP 地址。*end-address* 必须大于或等于 *start-address*，如果 *start-address* 和 *end-address* 相同，则表示只有一个地址。

【使用指导】

一个 NAT 地址组是多个地址组成员的集合。当需要对到达外部网络的数据报文进行地址转换时，报文的源地址将被转换为地址组成员中的某个地址。

一个地址组成员所包含的地址数目不能超过 65535。

各地址组成员的 IP 地址段不能互相重叠。

在多形态防火墙设备上，配置的所有地址组成员包含的地址总数不能少于安全引擎（或安全插卡）的数量。

【举例】

在 NAT 地址组 2 中添加两个地址组成员。

```
<Sysname> system-view
[Sysname] nat address-group 2
[Sysname-address-group-2] address 10.1.1.1 10.1.1.15
[Sysname-address-group-2] address 10.1.1.20 10.1.1.30
```

【相关命令】

- **nat address-group**

1.1.2 block-size

block-size 命令用来设置端口块大小。

undo block-size 命令用来恢复缺省情况。

【命令】

block-size *block-size*

undo block-size

【缺省情况】

一个端口块中包含 256 个端口。

【视图】

NAT 端口块组视图

【缺省用户角色】

network-admin

context-admin

【参数】

block-size：端口块大小，即一个端口块中所包含的端口数，取值范围为 1～*max_number*。其中 *max_number* 的取值范围为 1～65535。

【使用指导】

在一个端口块组中，需要根据私网 IP 地址个数，以及公网 IP 地址个数及其端口范围，确定一个合理的端口块大小值。端口块大小值不能超过公网地址的端口范围值。

【举例】

配置端口块组 1 的端口块大小为 1024。

```
<Sysname> system-view
[Sysname] nat port-block-group 1
[Sysname-port-block-group-1] block-size 1024
```

【相关命令】

- **nat port-block-group**

1.1.3 display nat address-group

display nat address-group 命令用来显示 NAT 地址组配置信息。

【命令】

display nat address-group [*group-id*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

group-id：地址组的编号，取值范围为 0～65535。如果不设置该值，则显示所有地址组。

【举例】

显示所有地址组的配置信息。

```
<Sysname> display nat address-group
NAT address group information:
  Totally 5 NAT address groups.
  Address group ID: 1    Address group name: a
    Port range: 1-65535
    Address information:
      Start address         End address
      202.110.10.10         202.110.10.15

  Address group ID: 2
    Port range: 1-65535
    Address information:
      Start address         End address
      202.110.10.20         202.110.10.25
      202.110.10.30         202.110.10.35

  Address group ID: 3
    Port range: 1024-65535
    Address information:
      Start address         End address
      202.110.10.40         202.110.10.50

  Address group ID: 4
    Port range: 10001-65535
    Port block size: 500
    Extended block number: 1
    Address information:
      Start address         End address
      202.110.10.60         202.110.10.65

  Address group ID: 6
    Port range: 1-65535
    Address information:
      Start address         End address
      ---                   ---
```

显示指定地址组的配置信息。

```
<Sysname> display nat address-group 1
  Address group ID: 1    Address group name: a
    Port range: 1-65535
```

```
Address information:
  Start address          End address
  202.110.10.10          202.110.10.15
```

表1-1 display nat address-group 命令显示信息描述表

字段	描述
NAT address group information	NAT地址组信息
Totally *n* NAT address groups	当前有*n*个地址组
Address group ID	地址组编号
Address group name	地址组名称。如果没有配置，则不显示该字段
Port range	地址的端口范围
Block size	端口块大小。如果未配置，则不显示
Extended block number	增量端口块数。如果未配置，则不显示
Address information	地址组成员信息
Start address	地址组成员的起始地址。如果未配置，则显示”---”
End address	地址组成员的结束地址。如果未配置，则显示”---”

【相关命令】

- **nat address-group**

1.1.4 display nat alg

display nat alg 用来显示所有协议类型的 NAT ALG 功能的开启状态。

【命令】

display nat alg

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【举例】

显示所有协议类型的 NAT ALG 功能的开启状态。

```
<Sysname> display nat alg
NAT ALG:
  DNS        : Enabled
  FTP        : Disabled
  H323       : Disabled
```

```
ICMP-ERROR : Disabled
ILS        : Disabled
MGCP       : Disabled
NBT        : Disabled
PPTP       : Disabled
RTSP       : Disabled
RSH        : Disabled
SCCP       : Disabled
SIP        : Disabled
SQLNET     : Disabled
TFTP       : Disabled
XDMCP      : Disabled
```

表1-2 display nat alg 命令显示信息描述表

字段	描述
Enabled	协议的NAT ALG功能处于开启状态
Disabled	协议的NAT ALG功能处于关闭状态

【相关命令】

- display nat all

1.1.5 display nat all

display nat all 命令用来显示所有的 NAT 配置信息。

【命令】

display nat all

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【举例】

显示所有的 NAT 配置信息。

```
<Sysname> display nat all
NAT address group information:
  Totally 5 NAT address groups.
  Address group 1:
    Port range: 1-65535
    Address information:
      Start address         End address
```

```
      202.110.10.10         202.110.10.15

  Address group 2:
    Port range: 1-65535
    Address information:
      Start address         End address
      202.110.10.20         202.110.10.25
      202.110.10.30         202.110.10.35

  Address group 3:
    Port range: 1024-65535
    Address information:
      Start address         End address
      202.110.10.40         202.110.10.50

  Address group 4:
    Port range: 10001-65535
    Port block size: 500
    Extended block number: 1
    Address information:
      Start address         End address
      202.110.10.60         202.110.10.65

  Address group 6:
    Port range: 1-65535
    Address information:
      Start address         End address
      ---                   ---

NAT server group information:
  Totally 3 NAT server groups.
  Group Number        Inside IP             Port        Weight
  1                   192.168.0.26          23          100
                      192.168.0.27          23          500
  2                   ---                   ---         ---
  3                   192.168.0.26          69          100

NAT inbound information:
  Totally 1 NAT inbound rules.
  Interface: GigabitEthernet1/0/1
    ACL: 2038
    Address group ID: 2
    Add route: Y         NO-PAT: Y         Reversible: N
    VPN instance: vpn_nat
    Rule name: abcdefg
    Priority: 1000
    Config status: Active
```

```
NAT outbound information:
  Totally 2 NAT outbound rules.
  Interface: GigabitEthernet1/0/2
    ACL: 2036
    Address group ID: 1
    Port-preserved: Y    NO-PAT: N         Reversible: N
    Rule name: cdefg
    Priority: 1001
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: address group, and ACL.

  Interface: GigabitEthernet1/0/2
    ACL: 2037
    Address group ID: 1
    Port-preserved: N    NO-PAT: Y         Reversible: Y
    VPN instance: vpn_nat
    Rule name: blue
    Priority: 1002
    Config status: Active

NAT internal server information:
  Totally 5 internal servers.
  Interface: GigabitEthernet1/0/1
    Global ACL    : 2000
    Local IP/port : 192.168.10.1/23
    Rule name     : cdefgab
    Priority      : 1000
    Config status : Active

  Interface: GigabitEthernet1/0/3
    Protocol: 6(TCP)
    Global IP/port: 50.1.1.1/23
    Local IP/port : 192.168.10.15/23
    ACL           : 2000
    Rule name     : green
    Config status : Active

  Interface: GigabitEthernet1/0/4
    Protocol: 6(TCP)
    Global IP/port: 50.1.1.1/23-30
    Local IP/port : 192.168.10.15-192.168.10.22/23
    Global VPN    : vpn1
    Local VPN     : vpn3
    Rule name     : blue
    Config status : Active

  Interface: GigabitEthernet1/0/4
```

```
    Protocol: 255(Reserved)
    Global IP/port: 50.1.1.100/---
    Local IP/port : 192.168.10.150/---
    Global VPN    : vpn2
    Local VPN     : vpn4
    ACL           : 3000
    Rule name     : white
    Config status : Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: local VPN, and ACL.

  Interface: GigabitEthernet1/0/5
    Protocol: 17(UDP)
    Global IP/port: 50.1.1.2/23
    Local IP/port : server group 1
                    192.168.0.26/23       (Connections: 10)
                    192.168.0.27/23       (Connections: 20)
    Global VPN    : vpn1
    Local VPN     : vpn3
    Rule name     : black
    Config status : Active

Static NAT mappings:
  Totally 2 inbound static NAT mappings.
  Net-to-net:
    Global IP    : 2.2.2.1 – 2.2.2.255
    Local IP     : 1.1.1.0
    Netmask      : 255.255.255.0
    Global VPN   : vpn2
    Local VPN    : vpn1
    ACL          : 2000
    Reversible   : Y
    Rule name     : pink
    Priority      : 1000
    Config status: Active

  IP-to-IP:
    Global IP    : 5.5.5.5
    Local IP     : 4.4.4.4
    Global VPN   : vpn3
    Local VPN    : vpn4
    ACL          : 2001
    Reversible   : Y
    Rule name    : yellow
    Priority     : 1000
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: local VPN, global VPN, and ACL.
```

```
  Totally 2 outbound static NAT mappings.
  Net-to-net:
    Local IP     : 1.1.1.1 - 1.1.1.255
    Global IP    : 2.2.2.0
    Netmask      : 255.255.255.0
    Local VPN    : vpn1
    Global VPN   : vpn2
    ACL          : 2000
    Reversible   : Y
    Rule name    : grey
    Priority     : 1000
    Config status: Active

  IP-to-IP:
    Local IP     : 4.4.4.4
    Global IP    : 5.5.5.5
    Local VPN    : vpn1
    Global VPN   : vpn2
    ACL:         : 2001
    Reversible   : Y
    Rule name    : orange
    Priority     : 10000
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.

Interfaces enabled with static NAT:
  Totally 2 interfaces enabled with static NAT.
  Interface: GigabitEthernet1/0/4
    Config status: Active

  Interface: GigabitEthernet1/0/6
    Config status: Active

NAT DNS mappings:
  Totally 2 NAT DNS mappings.
  Domain name  : www.server.com
  Global IP    : 6.6.6.6
  Global port  : 23
  Protocol     : TCP(6)
  Config status: Active

  Domain name  : www.service.com
  Global IP    : ---
  Global port  : 12
  Protocol     : TCP(6)
  Config status: Inactive
```

```
  Reasons for inactive status:
    The following items don't exist or aren't effective: interface IP address.

NAT logging:
  Log enable          : Enabled(ACL 2000)
  Flow-begin          : Disabled
  Flow-end            : Disabled
  Flow-active         : Enabled(10 minutes)
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
  Alarm               : Disabled

NAT hairpinning:
  Totally 2 interfaces enabled with NAT hairpinning.
  Interface: GigabitEthernet1/0/4
    Config status: Active

  Interface: GigabitEthernet1/0/6
    Config status: Active

NAT mapping behavior:
  Mapping mode : Endpoint-Independent
  ACL          : 2050
  Config status: Active

NAT ALG:
  DNS        : Enabled
  FTP        : Enabled
  H323       : Disabled
  ICMP-ERROR : Enabled
  ILS        : Disabled
  MGCP       : Disabled
  NBT        : Disabled
  PPTP       : Enabled
  RTSP       : Enabled
  RSH        : Disabled
  SCCP       : Disabled
  SIP        : Disabled
  SQLNET     : Disabled
  TFTP       : Disabled
  XDMCP      : Disabled

NAT port block group information:
  Totally 3 NAT port block groups.
  Port block group 1:
    Port range: 1-65535
    Block size: 256
    Local IP address information:
```

```
      Start address        End address          VPN instance
      172.16.1.1           172.16.1.254         ---
      192.168.1.1          192.168.1.254        vpna
      192.168.3.1          192.168.3.254        vpna
    Global IP pool information:
      Start address        End address
      201.1.1.1            201.1.1.10
      201.1.1.21           201.1.1.25

  Port block group 2:
    Port range: 10001-30000
    Block size: 500
    Local IP address information:
      Start address        End address          VPN instance
      10.1.1.1             10.1.10.255          vpnb
    Global IP pool information:
      Start address        End address
      202.10.10.101        202.10.10.120

  Port block group 3:
    Port range: 1-65535
    Block size: 256
    Local IP address information:
      Start address        End address          VPN instance
      ---                  ---                  ---
    Global IP pool information:
      Start address        End address
      ---                  ---

NAT outbound port block group information:
  Totally 2 outbound port block group items.
  Interface: GigabitEthernet1/0/2
    Port block group: 2
    Rule name: stone
    Config status   : Active

  Interface: GigabitEthernet1/0/2
    Port block group: 10
    Rule name: brown
    Config status   : Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: port block group.
```

上述显示信息是目前所有 NAT 配置信息的集合。由于部分 NAT 配置（**nat address-group**、**nat server-group**、**nat inbound**、**nat outbound**、**nat server**、**nat static**、**nat static net-to-net**、**nat static enable** 、**nat dns-map** 、**nat log** 、**nat port-block-group** 和 **nat outbound port-block-group**）有自己独立的显示命令，且此处显示信息的格式与各命令对应的显示信息的格式相同的，所以此处不对这些配置的显示字段的含义进行详细解释，如有需要，请参考各独立的显

示命令。下面的表格将给出相关显示命令的参见信息并仅解释 **nat hairpin enable**、**nat mapping-behavior** 和 **nat alg** 配置的显示字段的含义。

表1-3 display nat all 命令显示信息描述表

字段	描述
NAT address group information	NAT地址组的配置信息，详细字段解释请参见“表1-1”
NAT server group information	NAT内部服务器组的配置信息，详细字段解释请参见“表1-15”
NAT inbound information:	入方向动态地址转换的配置信息，详细字段解释请参见“表1-6”
NAT outbound information	出方向动态地址转换的配置信息，详细字段解释请参见“表1-9”
NAT internal server information	NAT内部服务器的配置信息，详细字段解释请参见“表1-14”
Static NAT mappings	静态地址转换的配置信息，详细字段解释请参见“表1-17”
NAT DNS mappings	NAT DNS mapping的配置信息，详细字段解释请参见“表1-4”
NAT logging	NAT日志功能的配置信息，详细字段解释请参见“表1-7”
NAT hairpinning	NAT hairpin功能
Totally *n* interfaces enabled NAT hairpinning	当前有*n*个接口开启NAT hairpin功能
Interface	开启NAT hairpin功能的接口
Rule name	NAT规则的名称
Priority	NAT规则的匹配优先级
Config status	显示NAT hairpin配置的状态 • Active：生效 • Inactive：不生效
NAT mapping behavior	PAT方式下的地址转换模式 • Endpoint-Independent：表示不关心对端地址和端口 • Address and Port-Dependent：表示关心对端地址和端口
ACL	引用的ACL编号或名称。如果未配置，则显示“---”
Config status	显示NAT mapping behavior配置的状态 • Active：生效 • Inactive：不生效
Reasons for inactive status	当Config status字段为Inactive时，显示NAT mapping behavior配置不生效的原因：The following items don't exist or aren't effective: ACL：引用的ACL不存在
NAT ALG	各协议的NAT ALG功能开启信息
NAT port block group information	NAT端口块组的配置信息，详细字段解释请参见“表1-12”
NAT outbound port block group information	NAT444端口块静态映射的配置信息，详细字段解释请参见“表1-10”

1.1.6 display nat dns-map

display nat dns-map 命令用来显示 NAT DNS mapping 配置信息。

【命令】

display nat dns-map

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【举例】

显示所有 NAT DNS mapping 的配置信息。

```
<Sysname> display nat dns-map
NAT DNS mapping information:
  Totally 2 NAT DNS mappings.
  Domain name   : www.server.com
  Global IP     : 6.6.6.6
  Global port   : 23
  Protocol      : TCP(6)
  Config status: Active

  Domain name   : www.service.com
  Global IP     : ---
  Global port   : 12
  Protocol      : TCP(6)
  Config status: Inactive
  Reasons for inactive status:
    The following items don't exist or aren't effective: interface IP address.
```

表1-4 display nat dns-map 命令显示信息描述表

字段	描述
NAT DNS mapping information	NAT DNS mapping配置信息
Totally *n* NAT DNS mappings	当前有*n*条DNS mapping配置
Domain name	DNS域名
Global IP	外网地址。如果配置使用的是Easy IP方式，则此处显示指定的接口的地址。“---”表示接口下未配置外网地址
Global port	外网端口号
Protocol	协议名称以及协议编号

字段	描述
Config status	显示DNS mapping配置的状态 • Active：生效 • Inactive：不生效
Reasons for inactive status	当Config status字段为Inactive时，显示DNS mapping配置不生效的原因：The following items don't exist or aren't effective: interface IP address：引用的接口未配置IP地址

【相关命令】

- **nat dns-map**

1.1.7 display nat eim

display nat eim 命令用来显示 NAT EIM 表项信息。

【命令】

display nat eim [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

slot *slot-number*：显示指定成员设备上的 EIM 表项信息，*slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数，则表示显示所有成员设备上的 EIM 表项信息。

【使用指导】

EIM 表项是报文在进行 Endpoint-Independent Mapping 方式的 PAT 转换时创建的，它记录了内网和外网的转换关系（内网地址和端口<-->NAT 地址和端口），该表项有以下两个作用：

- 保证后续来自相同源地址和源端口的新建连接与首次连接使用相同的转换关系。
- 允许外网主机向 NAT 地址和端口发起的新建连接根据 EIM 表项进行反向地址转换。

【举例】

显示 1 号成员设备上的 NAT EIM 表项信息。

```
<Sysname> display nat eim slot 1
Slot 1:
Local  IP/port: 192.168.100.100/1024
Global IP/port: 200.100.1.100/2048
Local  VPN: vpn1
Global VPN: vpn2
```

```
Protocol: TCP(6)

Local  IP/port: 192.168.100.200/2048
Global IP/port: 200.100.1.200/4096
Protocol: UDP(17)

Total entries found: 2
```

表1-5 display nat eim 命令显示信息描述表

字段	描述
Local IP/port	内网IP地址/端口号
Global IP/port	外网IP地址/端口号
Local VPN	内网地址所属的VPN实例名称。如果不属于任何VPN，则不显示该字段
Global VPN	外网地址所属的VPN实例名称。如果不属于任何VPN，则不显示该字段
Protocol	协议名称以及协议编号
Total entries found	当前查找到的EIM表项的个数

【相关命令】

- **nat mapping-behavior**
- **nat outbound**

1.1.8 display nat inbound

display nat inbound 命令用来显示 NAT 入方向动态地址转换的配置信息。

【命令】

display nat inbound

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【举例】

显示 NAT 入接口动态地址转换的配置信息。

```
<Sysname> display nat inbound
NAT inbound information:
  Totally 2 NAT inbound rules.
  Interface: GigabitEthernet1/0/2
    ACL: 2038
```

```
    Address group ID: 2            Address group name: b
    Add route: Y         NO-PAT: Y         Reversible: N
    VPN instance: vpn1
    Rule name: abcd
    Priority: 1000
    Config status: Active

Interface: GigabitEthernet1/0/3
    ACL: 2037
    Address group ID: 1            Address group name: a
    Add route: Y         NO-PAT: Y         Reversible: N
    VPN instance: vpn2
    Rule name: eif
    Priority: 1001
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: local VPN, and ACL.
```

表1-6 display nat inbound 命令显示信息描述表

字段	描述
NAT inbound information	NAT入方向动态地址转换的配置信息
Totally *n* NAT inbound rules	当前存在*n*条入入方向动态地址转换配置
Interface	入方向动态地址转换配置所在的接口
ACL	引用的ACL编号或名称
Address group ID	入方向动态地址转换使用的地址组编号
Address group name	入方向动态地址转换使用的地址组名称。如果没有配置，则不显示该字段
Add route	是否添加路由。若其值为“Y”，则表示有报文命中此项入接口动态地址转换配置时，设备会自动添加一条路由；否则，不添加
NO-PAT	是否使用NO-PAT方式进行地址转换。若其值为“Y”，则表示使用NO-PAT方式；若其值为“N”，则表示使用PAT方式
Reversible	是否允许反向地址转换。若其值为“Y”，则表示在某方向上发起的连接已成功建立地址转换表项的情况下，允许反方向发起的连接使用已建立的地址转换表项进行地址转换；否则，不允许
VPN instance	地址组所属的VPN实例名称。如果不属于任何VPN，则不显示该字段
Rule name	NAT规则的名称
Priority	NAT规则的匹配优先级
Config status	显示NAT配置的状态 • Active：生效 • Inactive：不生效
Reasons for inactive status	当Config status字段为Inactive时，显示NAT入方向动态地址转换的配置不生效的原因：The following items don't exist or aren't effective: local VPN, address group, and ACL：配置中地址组所属的VPN实例、地址组、ACL不存在或不生效

【相关命令】

- **nat inbound**

1.1.9 display nat log

display nat log 命令用来显示 NAT 日志功能的配置信息。

【命令】

display nat log

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【举例】

显示 NAT 日志功能的配置信息。

```
<Sysname> display nat log
NAT logging:
  Log enable          : Enabled(ACL 2000)
  Flow-begin          : Disabled
  Flow-end            : Disabled
  Flow-active         : Enabled(10 minutes)
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
  Alarm               : Disabled
```

表1-7 display nat log 命令显示信息描述表

字段	描述
NAT logging	NAT日志功能的配置信息
Log enable	NAT日志开关的开启情况。如果NAT日志开关处于开启状态，且指定了ACL，则同时显示指定的ACL编号或名称
Flow-begin	NAT会话新建日志开关的开启情况
Flow-end	NAT会话删除日志开关的开启情况
Flow-active	NAT活跃流日志开关的开启情况以及阈值信息。如果NAT活跃流日志开关处于开启状态，则同时显示配置的生成活跃流日志的时间间隔（单位为分）
Port-block-assign	端口块分配的NAT444用户日志开关的开启情况
Port-block-withdraw	端口块回收的NAT444用户日志开关的开启情况
Alarm	NAT444告警信息日志开关的开启情况

【相关命令】

- **nat log enable**
- **nat log flow-active**
- **nat log flow-begin**

1.1.10 display nat no-pat

display nat no-pat 命令用来显示 NAT NO-PAT 表项信息。

【命令】

display nat no-pat [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

slot *slot-number*：显示指定成员设备上的 NO-PAT 表项信息，*slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数，则表示显示所有成员设备上的 NO-PAT 表项信息。

【使用指导】

NO-PAT 表项记录了动态分配的一对一地址映射关系，该表项有两个作用：

- 保证后续同方向的新连接使用与第一个连接相同的地址转换关系。
- 反方向的新连接可以使用 NO-PAT 表进行地址转换。

nat inbound 和 **nat outbound** 配置的 NO-PAT 方式在转换报文地址之后都需要创建 NO-PAT 表。这两种配置创建的 NO-PAT 表类型不同，不能互相使用，因此分成两类进行显示。

【举例】

显示 1 号成员设备的 NAT NO-PAT 表项。

```
<Sysname> display nat no-pat slot 1
Slot 1:
Global  IP: 200.100.1.100
Local   IP: 192.168.100.100
Global VPN: vpn2
Local  VPN: vpn1
Reversible: N
Type      : Inbound

Local   IP: 192.168.100.200
Global  IP: 200.100.1.200
```

```
Reversible: Y
Type      : Outbound

Total entries found: 2
```

表1-8 display nat no-pat 命令显示信息描述表

字段	描述
Local IP	内网IP地址
Global IP	外网IP地址
Local VPN	内网地址所属的VPN的实例名称。如果不属于任何VPN，则该行不显示
Global VPN	外网地址所属的VPN的实例名称。如果不属于任何VPN，则该行不显示
Reversible	是否允许反向地址转换。若其值为“Y”，则表示在某方向上发起的连接已成功建立地址转换表项的情况下，允许反方向发起的连接使用已建立的地址转换表项进行地址转换
Type	NO-PAT表项类型 • Inbound：入方向动态地址转换过程中创建的 NO-PAT 表项 • Outbound：出方向动态地址转换过程中创建的 NO-PAT 表项
Total entries found	当前查找到的NO-PAT表项的个数

【相关命令】

- **nat inbound**
- **nat outbound**

1.1.11 display nat outbound

display nat outbound 命令用来显示出方向动态地址转换的配置信息。

【命令】

display nat outbound

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【举例】

显示出方向动态地址转换的配置信息。

```
<Sysname> display nat outbound
NAT outbound information:
  Totally 2 NAT outbound rules.
```

```
Interface: GigabitEthernet1/0/1
  ACL: 2036
  Address group ID: 1            Address group name: a
  Port-preserved: Y    NO-PAT: N         Reversible: N
  Rule name: abefg
  Priority: 1000
  Config status: Active

Interface: GigabitEthernet1/0/2
  ACL: 2037
  Address group ID: 2            Address group name: b
  Port-preserved: N    NO-PAT: Y         Reversible: Y
  VPN instance: vpn_nat
  Rule name: cdefg
  Priority: 1001
  Config status: Inactive
  Reasons for inactive status:
    The following items don't exist or aren't effective: global VPN, and ACL.

Interface: GigabitEthernet1/0/1
  DS-Lite B4 ACL: 2100
  Address group ID: 2            Address group name: b
  Port-preserved: N    NO-PAT: N         Reversible: N
  Priority: 0
  Config status: Active
```

表1-9 display nat outbound 命令显示信息描述表

字段	描述
NAT outbound information	出方向动态地址转换的配置信息
Totally *n* NAT outbound rules	当前存在*n*条出方向动态地址转换
Interface	出方向动态地址转换配置所在的接口
ACL	引用的IPv4 ACL编号或名称。如果未配置，则显示“---”
DS-Lite B4 ACL	DS-Lite B4引用的IPv6 ACL编号或名称
Address group ID	出方向动态地址转换使用的地址组编号。如果未配置，则显示“---”
Address group name	出方向动态地址转换使用的地址组名称。如果未配置，则不显示该字段
Port-preserved	PAT方式下，是否尽量不转换端口
NO-PAT	是否使用NO-PAT方式进行转换。若其值为“N”，则表示使用PAT方式
Reversible	是否允许反向地址转换。若其值为“Y”，则表示在某方向上发起的连接已成功建立地址转换表项的情况下，允许反方向发起的连接使用已建立的地址转换表项进行地址转换
VPN instance	地址组所属的VPN实例名称。如果不属于任何VPN，则不显示该字段
Rule name	NAT规则的名称
Priority	NAT规则的匹配优先级

字段	描述
Config status	显示配置的状态 • Active：生效 • Inactive：不生效
Reasons for inactive status	当Config status字段为Inactive时，显示配置不生效的原因 • The following items don't exist or aren't effective: global VPN, interface IP address, address group, and ACL：配置中地址组所属的 VPN 实例、接口地址、地址组、ACL 不存在或不生效 • NAT address conflicts：NAT 地址冲突

【相关命令】

- **nat outbound**

1.1.12 display nat outbound port-block-group

display nat outbound port-block-group 命令用来显示 NAT444 端口块静态映射的配置信息。

【命令】

display nat outbound port-block-group

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【举例】

显示 NAT444 端口块静态映射的配置信息。

```
<Sysname> display nat outbound port-block-group
NAT outbound port block group information:
  Totally 2 outbound port block group items.
  Interface: GigabitEthernet1/0/2
    Port block group: 2
    VPN instance: vpna
    Rule name: abcdefg
    Config status   : Active

  Interface: GigabitEthernet1/0/2
    Port block group: 10
    VPN instance: vpna
    Rule name: abcfg
    Config status   : Inactive
```

```
Reasons for inactive status:
  The following items don't exist or aren't effective: port block group.
```

表1-10 display nat outbound port-block-group 命令显示信息描述表

字段	描述
NAT outbound port block group information	NAT444端口块静态映射的配置信息
Totally *n* outbound port block group items	当前存在*n*条NAT444端口块静态映射配置
Interface	NAT444端口块静态映射配置所在的接口
Port block group	端口块组编号
VPN instance	端口块组所属的VPN实例名称。如果该接口没有绑定任何VPN实例，则不显示该字段
Rule name	NAT规则的名称
Config status	显示配置的状态 • Active：生效 • Inactive：不生效
Reasons for inactive status	当Config status字段为Inactive时，显示配置不生效的原因：The following items don't exist or aren't effective: port block group：配置中端口块组不存在或不生效

【相关命令】

- **nat outbound port-block-group**

1.1.13 display nat port-block

display nat port-block 命令用来显示端口块表项。

【命令】

display nat port-block { **dynamic** [**ds-lite-b4**] | **static** } [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

dynamic：显示动态端口块表项。

ds-lite-b4：显示基于 DS-Lite B4 地址的端口块表项。

static：显示静态端口块表项。

slot *slot-number*：显示指定成员设备上的端口块表项信息，*slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数，则表示显示所有成员设备上的端口块表项信息。

【举例】

显示静态端口块表项。

```
<Sysname> display nat port-block static
Slot 0:
Local VPN     Local IP         Global IP        Port block   Connections
---           100.100.100.111  202.202.100.101  10001-10256  0
---           100.100.100.112  202.202.100.101  10257-10512  0
---           100.100.100.113  202.202.100.101  10513-10768  0
vpn012345678  100.100.100.113  202.202.100.101  10769-11024  0
901234567890
1234567
Total entries found: 4
```

显示动态端口块表项。

```
<Sysname> display nat port-block dynamic
Slot 0:
Local VPN     Local IP         Global IP        Port block   Connections
---           101.1.1.12       192.168.135.201  10001-11024  1
Total entries found: 1
```

显示基于 DS-Lite B4 地址的端口块表项。

```
<Sysname> display nat port-block dynamic ds-lite-b4
Slot 0:
Local VPN     DS-Lite B4 addr  Global IP        Port block   Connections
---           2000::2          192.168.135.201  10001-11024  1
Total entries found: 1
```

表1-11 display nat port-block 命令显示信息描述表

字段	描述
Local VPN	私网IP地址所属VPN，“---”表示不属于任何VPN
Local IP	私网IP地址
DS-Lite B4 addr	DS-Lite B4设备的IPv6地址
Global IP	公网IP地址
Port block	端口块（起始端口-结束端口）
Connections	当前使用本端口块中的端口建立的连接数

1.1.14 display nat port-block-group

display nat port-block-group 命令用来显示 NAT 端口块组配置信息。

【命令】

display nat port-block-group [*group-id*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

group-id：端口块组的编号，取值范围为 0～65535。如果不设置该值，则显示所有端口块组的配置信息。

【举例】

显示所有端口块组的配置信息。

```
<Sysname> display nat port-block-group
NAT port block group information:
  Totally 3 NAT port block groups.
  Port block group 1:
    Port range: 1-65535
    Block size: 256
    Local IP address information:
      Start address        End address          VPN instance
      172.16.1.1           172.16.1.254         ---
      192.168.1.1          192.168.1.254        vpna
      192.168.3.1          192.168.3.254        vpna
    Global IP pool information:
      Start address        End address
      201.1.1.1            201.1.1.10
      201.1.1.21           201.1.1.25

  Port block group 2:
    Port range: 10001-30000
    Block size: 500
    Local IP address information:
      Start address        End address          VPN instance
      10.1.1.1             10.1.10.255          vpnb
    Global IP pool information:
      Start address        End address
      202.10.10.101        202.10.10.120

  Port block group 3:
    Port range: 1-65535
    Block size: 256
    Local IP address information:
      Start address        End address          VPN instance
      ---                  ---                  ---
```

```
    Global IP pool information:
      Start address        End address
      ---                  ---
```

显示端口块组 1 的配置信息。

```
<Sysname> display nat port-block-group 1
  Port block group 1:
    Port range: 1-65535
    Block size: 256
    Local IP address information:
      Start address        End address          VPN instance
      172.16.1.1           172.16.1.254         ---
      192.168.1.1          192.168.1.254        vpna
      192.168.3.1          192.168.3.254        vpna
    Global IP pool information:
      Start address        End address
      201.1.1.1            201.1.1.10
      201.1.1.21           201.1.1.25
```

表1-12 display nat port-block-group 命令显示信息描述表

字段	描述
NAT port block group information	NAT端口块组信息
Totally *n* NAT port block groups	当前有*n*个端口块组
Port block group	端口块组的编号
Port range	公网地址的端口范围
Block size	端口块大小
Local IP address information	私网IP地址成员信息
Global IP pool information	公网IP地址成员信息
Start address	私网/公网IP地址成员的起始IP地址。如果未配置，则显示“---”
End address	私网/公网IP地址成员的成员结束IP地址。如果未配置，则显示“---”
VPN instance	私网IP地址成员所属的VPN。如果未配置，则显示“---”

【相关命令】

- **nat port-block-group**

1.1.15 display nat port-block-usage

display nat port-block-usage 命令用来显示动态 NAT444 地址组中端口块的使用率。

【命令】

display nat port-block-usage [**address-group** *group-id*] [**slot** *slot-number*]

【视图】

系统视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

address-group *group-id*：显示某一指定地址组的端口块使用率。*group-id* 表示地址组编号，取值范围为 0～65535。若不指定该参数，则显示所有地址组的端口块使用率。

slot *slot-number*：显示指定成员设备上动态 NAT444 地址组中端口块的使用率，*slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数，则显示所有成员设备上动态 NAT444 地址组中端口块的使用率。

【举例】

显示指定 slot 上动态 NAT444 地址组中端口块的使用率。

```
<Sysname> display nat port-block-usage slot 1
Slot 1:
Address group 0 on channel 0:
  Total port block entries :10
  Active port block entries:9
  Current port block usage :90%

Total NAT address groups found: 1
```

表1-13 display nat port-block-usage 命令显示信息描述表

字段	描述
Address group	地址组的编号
channel	FPGA（Field-Programmable Gate Array，现场可编程门阵列）编号
Total port block entries	地址组中端口块总数
Active port block entries	地址组中已分配端口块数
Current port block usage	地址组中当前端口块使用率
Total NAT address groups found	当前地址组的个数

1.1.16 display nat server

display nat server 命令用来显示 NAT 内部服务器的配置信息。

【命令】

display nat server

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【举例】

显示 NAT 内部服务器的信息。

```
<Sysname> display nat server
NAT internal server information:
  Totally 5 internal servers.
  Interface: GigabitEthernet1/0/1
    Global ACL    : 2000
    Local IP/port : 192.168.10.1/23
    Description   : aaa
    Rule name     : cdefgab
    Priority      : 1000
    Config status : Active

  Interface: GigabitEthernet1/0/3
    Protocol: 6(TCP)
    Global IP/port: 50.1.1.1/23
    Local IP/port : 192.168.10.15/23
    Description   : bbb
    Config status : Active

  Interface: GigabitEthernet1/0/4
    Protocol: 6(TCP)
    Global IP/port: 50.1.1.1/23-30
    Local IP/port : 192.168.10.15-192.168.10.22/23
    Global VPN    : vpn1
    Local VPN     : vpn3
    Rule name     : abcdef
    Config status : Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: local VPN.

  Interface: GigabitEthernet1/0/4
    Protocol: 255(Reserved)
    Global IP/port: 50.1.1.100/---
    Local IP/port : 192.168.10.150/---
    Global VPN    : vpn2
    Local VPN     : vpn4
    Rule name     : cdefg
    Config status : Active

  Interface: GigabitEthernet1/0/5
```

```
Protocol: 17(UDP)
Global IP/port: 50.1.1.2/23
Local IP/port : server group 1
                1.1.1.1/21            (Connections: 10)
                192.168.100.200/80    (Connections: 20)
Global VPN    : vpn1
Local VPN     : vpn10
Rule name     : white
Config status : Active
```

表1-14 display nat server 命令显示信息描述表

字段	描述
NAT internal server information	NAT内部服务器的配置信息
Totally *n* internal servers	当前存在*n*条内部服务器配置
Interface	内部服务器配置所在的接口
Protocol	内部服务器的协议编号以及协议名称
Global IP/port	内部服务器的外网地址/端口号 • Global IP 可以是单个地址，也可以是一个连续的地址段。如果使用 Easy IP 方式，则此处显示指定的接口的地址；如果接口下未配置地址，则 Global IP 显示为“---” • port 可以是单个端口，也可以是一个连续的端口段。如果指定的协议没有端口的概念，则 port 显示为“---”
Local IP/port	对于普通内部服务器，显示服务器的内网地址/端口号 • Local IP 可以是单个地址，也可以是一个连续的地址段 • port 可以是单个端口，也可以是一个连续的端口段。如果指定的协议没有端口的概念，则 port 显示为“---” 对于负载分担内部服务器，显示内部服务器组编号以及服务器组成员的IP地址、端口和连接数
Description	NAT内部服务器的描述信息
Global VPN	外网地址所属的VPN实例名称。如果不属于任何VPN，则不显示该字段
Local VPN	内网地址所属的VPN实例名称。 如果不属于任何VPN，则不显示该字段
ACL	引用的ACL编号或名称。如果未配置，则不显示该字段
Rule name	NAT规则的名称
Config status	显示配置的状态 • Active：生效 • Inactive：不生效

字段	描述
Reasons for inactive status	当Config status字段为Inactive时，显示配置不生效的原因 • The following items don't exist or aren't effective: local VPN, global VPN, interface IP address, server group, and ACL：配置中内网地址所属的 VPN 实例、外网地址所属的 VPN 实例、接口地址、服务器组、ACL 不存在或不生效 • Server configuration conflicts：NAT 内部服务器配置冲突 • NAT address conflicts：NAT 地址冲突

【相关命令】

- **nat server**

1.1.17 display nat server-group

display nat server-group 命令用来显示 NAT 内部服务器组的配置信息。

【命令】

display nat server-group [*group-id*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

group-id：NAT 内部服务器组的编号，取值范围为 0～65535。如果不指定该参数，则显示所有内部服务器组。

【举例】

显示所有 NAT 内部服务器组的配置信息。

```
<Sysname> display nat server-group
NAT server group information:
  Totally 3 NAT server groups.
  Group Number        Inside IP            Port        Weight
  1                   192.168.0.26         23          100
                      192.168.0.27         23          500
  2                   ---                  ---         ---
  3                   192.168.0.26         69          100
```

显示指定 NAT 内部服务器组的配置信息。

```
<Sysname> display nat server-group 1
  Group Number        Inside IP            Port        Weight
```

```
1                192.168.0.26          23          100
                 192.168.0.27          23          500
```

表1-15 display nat server-group 命令显示信息描述表

字段	描述
NAT server group information	NAT内部服务器组信息
Totally *n* NAT server groups	当前有*n*个内部服务器组
Group Number	内部服务器组的编号
Inside IP	内部服务器组成员在内网的IP地址。如果未配置，则显示“---”
Port	内部服务器组成员在内网的端口。如果未配置，则显示“---”
Weight	内部服务器组成员的权重值。如果未配置，则显示“---”

【相关命令】

- **nat server-group**

1.1.18 display nat session

display nat session 命令用来显示 NAT 会话表项，即经过 NAT 地址转换处理的会话。

【命令】

display nat session [[**responder**] { **source-ip** *source-ip* | **destination-ip** *destination-ip* } * [**vpn-instance** *vpn-instance-name*]] [**slot** *slot-number*] [**verbose**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

responder：表示以响应方的信息筛选显示 NAT 会话表项。若不指定该参数时，则以发起方的信息筛选显示 NAT 会话表项。

source-ip *source-ip*：显示指定源地址的 NAT 会话表项。*source-ip* 表示源地址，该地址必须是创建 NAT 会话表项的报文的源地址。

destination-ip *destination-ip*：显示指定目的地址的 NAT 会话表项。*destination-ip* 表示目的地址，该地址必须是创建 NAT 会话表项的报文的目的地址。

vpn-instance *vpn-instance-name*：显示指定目的 VPN 的 NAT 会话表项。*vpn-instance-name* 表示 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。该 VPN 必须是报文中携带的 VPN。如果不指定该参数，则显示目的 IP 不属于任何 VPN 的 NAT 会话表项。

slot *slot-number*：显示指定成员设备上的 NAT 会话表项，*slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数，则显示所有成员设备上的 NAT 会话表项。

verbose：显示 NAT 会话表项的详细信息。如果不配置则显示 NAT 会话表项的概要信息。

【使用指导】

如果不指定任何参数，则显示所有的 NAT 会话表项。

【举例】

显示 1 号成员设备上 NAT 会话表项的详细信息。

```
<Sysname> display nat session slot 1 verbose
Slot 1:
Initiator:
  Source      IP/port: 192.168.1.18/1877
  Destination IP/port: 192.168.1.55/22
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: SrcZone
Responder:
  Source      IP/port: 192.168.1.55/22
  Destination IP/port: 192.168.1.10/1877
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: DestZone
State: TCP_SYN_SENT
Application: SSH
Start time: 2011-07-29 19:12:36  TTL: 28s
Initiator->Responder:         1 packets         48 bytes
Responder->Initiator:         0 packets          0 bytes

Total sessions found: 1
```

表1-16 display nat session 命令显示信息描述表

字段	描述
Initiator	发起方的会话信息
Responder	响应方的会话信息
Source IP/port	源IP地址/端口号
Destination IP/port	目的IP地址/端口号
DS-Lite tunnel peer	DS-Lite隧道对端地址。会话不属于任何DS-Lite隧道时，本字段显示为“-”
VPN instance/VLAN ID/Inline ID	会话所属的VPN实例/二层转发时会话所属的VLAN ID/二层转发时会话所属的INLINE。如果未指定则显示“-/-/-”
Protocol	传输层协议类型，包括：DCCP、ICMP、Raw IP 、SCTP、TCP、UDP、UDP-Lite

字段	描述
Inbound interface	报文的入接口
Source security zone	源安全域，即入接口所属的安全域。若接口不属于任何安全域，则显示为“-”
State	会话状态
Application	应用层协议类型，取值包括：FTP、DNS等，OTHER表示未知协议类型，其对应的端口为非知名端口
Start time	会话创建时间
TTL	会话剩余存活时间，单位为秒
Initiator->Responder	发起方到响应方的报文数、报文字节数
Responder->Initiator	响应方到发起方的报文数、报文字节数
Total sessions found	当前查找到的会话表总数

【相关命令】

- **reset nat session**

1.1.19 display nat static

display nat static 命令用来显示 NAT 静态地址转换的配置信息。

【命令】

display nat static

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【举例】

显示 NAT 静态地址转换的配置信息。

```
<Sysname> display nat static
Static NAT mappings:
  Totally 2 inbound static NAT mappings.
  Net-to-net:
    Global IP    : 1.1.1.1 - 1.1.1.255
    Local IP     : 2.2.2.0
    Netmask      : 255.255.255.0
    Global VPN   : vpn2
    Local VPN    : vpn1
    ACL          : 2000
```

```
    Reversible   : Y
    Rule name    : adefg
    Priority     : 1000
    Config status: Active

  IP-to-IP:
    Global IP   : 5.5.5.5
    Local IP     : 4.4.4.4
    Global VPN   : vpn3
    Local VPN    : vpn4
    ACL          : 2001
    Reversible   : Y
    Rule name    : abefg
    Priority     : 1000
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: local VPN, global VPN, and ACL.

Totally 2 outbound static NAT mappings.
  Net-to-net:
    Local IP     : 1.1.1.1 - 1.1.1.255
    Global IP    : 2.2.2.0
    Netmask      : 255.255.255.0
    Local VPN    : vpn1
    Global VPN   : vpn2
    ACL          : 2000
    Reversible   : Y
    Rule name    : abcd
    Priority     : 1000
    Config status: Active

  IP-to-IP:
    Local IP     : 4.4.4.4
    Global IP    : 5.5.5.5
    Local VPN    : vpn4
    Global VPN   : vpn3
    ACL:         : 2000
    Reversible   : Y
    Rule name    : defg
    Priority     : 1000
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: local VPN, and global VPN.

Interfaces enabled with static NAT:
  Totally 2 interfaces enabled with static NAT.
  Interface: GigabitEthernet1/0/2
    Config status: Active
```

```
Interface: GigabitEthernet1/0/3
  Config status: Active
```

表1-17 display nat static 命令显示信息描述表

字段	描述
Static NAT mappings	静态地址转换的配置信息
Totally *n* inbound static NAT mappings	当前存在*n*条入方向静态地址转换的配置
Totally *n* outbound static NAT mappings	当前存在*n*条出方向静态地址转换的配置
Net-to-net	网段到网段的静态地址转换映射
IP-to-IP	IP到IP的静态地址转换映射
Local IP	内网IP地址或地址范围
Global IP	外网IP地址或地址范围
Netmask	IP地址掩码
Local VPN	内网地址所属的VPN实例名称。如果不属于任何VPN，则不显示该字段
Global VPN	外网地址所属的VPN实例名称。如果不属于任何VPN，则不显示该字段
ACL	引用的ACL编号或名称。如果未配置，则不显示该字段
Reversible	是否允许反向地址转换。若其值为“Y”，则表示在某方向上发起的连接已成功建立地址转换表项的情况下，允许反方向发起的连接使用已建立的地址转换表项进行地址转换 如果未配置，则不显示该字段
Interfaces enabled with static NAT	静态地址转换在接口下的开启情况
Totally *n* interfaces enabled with static NAT	当前有*n*个接口开启了静态地址转换
Interface	开启静态地址转换功能的接口
Rule name	NAT规则的名称
Priority	NAT规则的匹配优先级
Config status	显示配置的状态 • Active：生效 • Inactive：不生效
Reasons for inactive status	当Config status字段为Inactive时，显示配置不生效的原因 • The following items don't exist or aren't effective: local VPN, global VPN, and ACL：配置中内网地址所属的 VPN 实例、外网地址所属的 VPN 实例、ACL 不存在或不存在 • NAT address conflicts：NAT 地址冲突

【相关命令】

- **nat static**
- **nat static net-to-net**
- **nat static enable**

1.1.20 display nat statistics

display nat statistics 命令用来显示 NAT 统计信息。

【命令】

display nat statistics [**summary**] [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

summary：显示 NAT 统计信息的摘要信息。不指定该参数时，显示 NAT 统计信息的详细信息。

slot *slot-number*：显示指定成员设备上的 NAT 统计信息，*slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数，则显示所有成员设备上的 NAT 统计信息。

【举例】

显示所有 NAT 统计信息的详细信息。

```
<Sysname> display nat statistics
Slot 1:
  Total session entries: 100
  Session creation rate: 0
  Total EIM entries: 1
  Total inbound NO-PAT entries: 0
  Total outbound NO-PAT entries: 0
  Total static port block entries: 10
  Total dynamic port block entries: 15
  Active static port block entries: 0
  Active dynamic port block entries: 0
```

表1-18 display nat statistics 命令显示信息描述表

字段	描述
Total session entries	NAT会话表项个数
Session creation rate	NAT会话的新建速率
Total EIM entries	EIM表项个数

字段	描述
Total inbound NO-PAT entries	入方向的NO-PAT表项个数
Total outbound NO-PAT entries	出方向的NO-PAT表项个数
Total static port block entries	当前配置创建的静态端口块表项个数
Total dynamic port block entries	当前配置可创建的动态端口块表项个数，即可分配的动态端口块总数，包括已分配的端口块和尚未分配的端口块
Active static port block entries	当前正在使用的静态端口块表项个数
Active dynamic port block entries	当前已创建的动态端口块表项个数，即已分配的动态端口块个数

显示所有 NAT 统计信息的概要信息。

```
<Sysname> display nat statistics summary
EIM: Total EIM entries.
SPB: Total static port block entries.
DPB: Total dynamic port block entries.
ASPB: Active static port block entries.
ADPB: Active dynamic port block entries.
Slot Sessions  EIM       SPB       DPB       ASPB      ADPB
2    0         0         0         1572720   0         0
```

表1-19 display nat statistics summary 命令显示信息描述表

字段	描述
Slot	IRF中的成员编号
Sessions	NAT会话表项个数
EIM	EIM表项个数
SPB	当前配置创建的静态端口块表项个数
DPB	当前配置可创建的动态端口块表项个数，即可分配的动态端口块总数，包括已分配的端口块和尚未分配的端口块
ASPB	当前正在使用的静态端口块表项个数
ADPB	当前已创建的动态端口块表项个数，即已分配的动态端口块个数

1.1.21 global-ip-pool

global-ip-pool 命令用来添加一个公网地址成员。

undo global-ip-pool 命令用来删除一个公网地址成员。

【命令】

global-ip-pool *start-address end-address*

undo global-ip-pool *start-address*

【缺省情况】

不存在公网地址成员。

【视图】

NAT 端口块组视图

【缺省用户角色】

network-admin

context-admin

【参数】

start-address end-address：公网地址成员的起始 IP 地址和结束 IP 地址。*end-address* 必须大于或等于 *start-address*；如果 *start-address* 和 *end-address* 相同，则表示只有一个地址。

【使用指导】

在 NAT444 端口块静态映射中，端口基于公网地址成员的 IP 地址为私网地址成员的 IP 地址分配端口块。一个公网 IP 地址可对应的端口块个数，由端口块组配置的公网地址端口范围和端口块大小决定（端口范围除以端口块大小）。

一个端口块组内，可以配置多个公网地址成员，但各公网地址成员之间的 IP 地址不能重叠。

不同端口块组间的公网地址成员的 IP 地址可以重叠，但要保证在有地址重叠时端口范围不重叠。

【举例】

在端口块组 1 中添加一个公网地址成员，IP 地址从 202.10.1.1 到 202.10.1.10。

```
<Sysname> system-view
[Sysname] nat port-block-group 1
[Sysname-port-block-group-1] global-ip-pool 202.10.1.1 202.10.1.10
```

【相关命令】

- **nat port-block-group**

1.1.22 inside ip

inside ip 命令用来添加一个内部服务器组成员。

undo inside ip 命令用来删除一个内部服务器组成员。

【命令】

inside ip *inside-ip* **port** *port-number* [**weight** *weight-value*]

undo inside ip *inside-ip* **port** *port-number*

【缺省情况】

内部服务器组内没有内部服务器组成员。

【视图】

内部服务器组视图

【缺省用户角色】

network-admin

context-admin

【参数】

inside-ip：内部服务器组成员的 IP 地址。

port *port-number*：内部服务器组成员提供服务的端口号，取值范围为 1～65535（FTP 数据端口号 20 除外）。

weight *weight-value*：内部服务器组成员的权重。*weight-value* 表示权值，取值范围为 1～1000，缺省值为 100。

【使用指导】

内部服务器组成员按照权重比例对外提供服务，权重值越大的内部服务器组成员对外提供服务的比重越大。

【举例】

为内部服务器组 1 添加一个内部服务器组成员，其 IP 地址为 10.1.1.2，服务端口号为 30。

```
<Sysname> system-view
[Sysname] nat server-group 1
[Sysname-nat-server-group-1] inside ip 10.1.1.2 port 30
```

【相关命令】

- **nat server-group**

1.1.23 local-ip-address

local-ip-address 命令用来添加一个私网地址成员。

undo local-ip-address 命令用来删除一个私网地址成员。

【命令】

local-ip-address *start-address end-address* [**vpn-instance** *vpn-instance-name*]

undo local-ip-address *start-address end-address* [**vpn-instance** *vpn-instance-name*]

【缺省情况】

不存在私网地址成员。

【视图】

NAT 端口块组视图

【缺省用户角色】

network-admin

context-admin

【参数】

start-address end-address：私网地址成员的起始 IP 地址和结束 IP 地址。*end-address* 必须大于或等于 *start-address*；如果 *start-address* 和 *end-address* 相同，则表示只有一个地址。

vpn-instance *vpn-instance-name*：私网地址成员所属的 VPN。*vpn-instance-name* 表示 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示私网地址成员不属于任何一个 VPN。

【使用指导】

私网地址成员的 IP 地址作为端口块的使用者，基于端口块组配置的公网地址成员的 IP 地址为其分配端口块。在一个端口块组内，一个私网 IP 地址只分配一个端口块。

一个端口块组内，可以配置多个私网地址成员，但各私网地址成员之间的 IP 地址不能重叠。

不同端口块组间的私网地址成员的 IP 地址可以重叠。

如果一个端口块组中的私网地址总数超过可分配的端口块总数（端口范围除以端口块大小），则在进行 NAT444 端口块静态映射时，超出部分的私网地址将无法分配到端口块。

【举例】

在端口块组 1 中添加一个私网地址成员，IP 地址从 172.16.1.1 到 172.16.1.255，所属 VPN 为 vpn1。

```
<Sysname> system-view
[Sysname] nat port-block-group 1
[Sysname-port-block-group-1] local-ip-address 172.16.1.1 172.16.1.255 vpn-instance vpn1
```

【相关命令】

- **nat port-block-group**

1.1.24 nat address-group

nat address-group 命令用来创建地址组，并进入地址组视图。如果指定的地址组已经存在，则直接进入地址组视图。

undo nat address-group 命令用来删除指定的地址组。

【命令】

nat address-group *group-id* [**name** *group-name*]

undo nat address-group *group-id*

【缺省情况】

不存在地址组。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

group-id：地址组编号，取值范围为 0～65535。

name *group-name*：地址组的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

一个地址组是多个地址组成员的集合，各个地址组成员通过 **address** 命令配置。当需要对数据报文进行动态地址转换时，其源地址将被转换为地址组成员中的某个地址。

【举例】

创建一个地址组，编号为 1，名称为 abc。

```
<Sysname> system-view
[Sysname] nat address-group 1 name abc
```

【相关命令】

- **address**
- **display nat address-group**
- **display nat all**
- **nat inbound**
- **nat outbound**

1.1.25 nat alg

nat alg 命令用来开启指定或所有协议类型的 NAT ALG 功能。

undo nat alg 命令用来关闭指定或所有协议类型的 NAT ALG 功能。

【命令】

nat alg { **all** | **dns** | **ftp** | **h323** | **icmp-error** | **ils** | **mgcp** | **nbt** | **pptp** | **rsh** | **rtsp** | **sccp** | **sip** | **sqlnet** | **tftp** | **xdmcp** }

undo nat alg { **all** | **dns** | **ftp** | **h323** | **icmp-error** | **ils** | **mgcp** | **nbt** | **pptp** | **rsh** | **rtsp** | **sccp** | **sip** | **sqlnet** | **tftp** | **xdmcp** }

【缺省情况】

DNS、FTP、ICMP 差错报文、RTSP、PPTP 协议类型的 NAT ALG 功能处于开启状态，其他协议类型的 NAT ALG 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

all：所有可指定的协议的 ALG 功能。

dns：表示 DNS 协议的 ALG 功能。

ftp：表示 FTP 协议的 ALG 功能。

h323：表示 H323 协议的 ALG 功能。

icmp-error：表示 ICMP 差错控制报文的 ALG 功能。

ils：表示 ILS（Internet Locator Service，互联网定位服务）协议的 ALG 功能。

mgcp：表示 MGCP（Media Gateway Control Protocol，媒体网关控制协议）协议的 ALG 功能。

nbt：表示 NBT（NetBIOS over TCP/IP，基于 TCP/IP 的网络基本输入输出系统）协议的 ALG 功能。

pptp：表示 PPTP（Point-to-Point Tunneling Protocol，点到点隧道协议）协议的 ALG 功能。

rsh：表示 RSH（Remote Shell，远程外壳）协议的 ALG 功能。

rtsp：表示 RTSP（Real Time Streaming Protocol，实时流协议）协议的 ALG 功能。

sccp：表示 SCCP（Skinny Client Control Protocol，瘦小客户端控制协议）协议的 ALG 功能。

sip：表示 SIP（Session Initiation Protocol，会话初始协议）协议的 ALG 功能。

sqlnet：表示 SQLNET 协议的 ALG 功能。

tftp：表示 TFTP 协议的 ALG 功能。

xdmcp：表示 XDMCP（X Display Manager Control Protocol，X 显示监控）协议的 ALG 功能。

【使用指导】

ALG（Application Level Gateway，应用层网关）主要完成对应用层报文的解析和处理。通常情况下，NAT 只对报文头中的 IP 地址和端口信息进行转换，不对应用层数据载荷中的字段进行分析和处理。然而对于一些应用层协议，它们的报文的数据载荷中可能包含 IP 地址或端口信息，这些载荷信息也必须进行有效的转换，否则可能导致功能不正常。

例如，FTP 应用由数据连接和控制连接共同完成，而数据连接使用的地址和端口由控制连接协商报文中的载荷信息决定，这就需要 ALG 利用 NAT 的相关转换配置来完成载荷信息的转换，以保证后续数据连接的正确建立。

【举例】

开启 FTP 协议的 ALG 功能。

```
<Sysname> system-view
[Sysname] nat alg ftp
```

【相关命令】

- **display nat all**

1.1.26 nat dns-map

nat dns-map 命令用来配置一条域名到内部服务器的映射。

undo nat dns-map 命令用来删除一条域名到内部服务器的映射。

【命令】

nat dns-map domain *domain-name* **protocol** *pro-type* { **interface** *interface-type interface-number* | **ip** *global-ip* } **port** *global-port*

undo nat dns-map domain *domain-name*

【缺省情况】

不存在域名到内部服务器的映射。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

domain *domain-name*：指定内部服务器的合法域名。*domain-name* 表示内部服务器的域名，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“.”。

protocol *pro-type*：指定内部服务器的协议类型。*pro-type* 表示具体的协议类型，取值为 **tcp** 或 **udp**。

interface *interface-type interface-number*：表示使用指定接口的地址作为内部服务器的外网地址。*interface-type interface-number* 表示接口类型和接口编号。

ip *global-ip*：指定内部服务器提供给外部网络访问的 IP 地址。*global-ip* 表示外网 IP 地址。

port *global-port*：指定内部服务器提供给外部网络访问的服务端口号，可输入的形式如下：

- 数字：取值范围为 1～65535。
- 协议名称：为 1～15 个字符的字符串，例如 **ftp**、**telnet** 等。

【使用指导】

NAT 的 DNS mapping 功能需要和内部服务器配合使用，主要应用于 DNS 服务器在外网，应用服务器在内网（在 NAT 设备上有对应的 **nat server** 配置），内网用户需要通过域名访问内网应用服务器的场景。NAT 设备对来自外网的 DNS 响应报文进行 DNS ALG 处理时，由于载荷中只包含域名和应用服务器的外网 IP 地址（不包含传输协议类型和端口号），当接口上存在多条 NAT 服务器配置且使用相同的外网地址而内网地址不同时，DNS ALG 仅使用 IP 地址来匹配内部服务器可能会得到错误的匹配结果。因此需要借助 DNS mapping 的配置，指定域名与应用服务器的外网 IP 地址、端口和协议的映射关系，由域名获取应用服务器的外网 IP 地址、端口和协议，进而（在当前 NAT 接口上）精确匹配内部服务器配置获取应用服务器的内网 IP 地址。

设备可支持配置多条域名到内部服务器的映射。

【举例】

某公司内部对外提供 Web 服务，内部服务器的域名为 www.server.com，对外的 IP 地址为 202.112.0.1，服务端口号为 12345。配置一条域名到内部服务器的映射，使得公司内部用户可以通过域名访问内部 Web 服务器。

```
<Sysname> system-view
[Sysname] nat dns-map domain www.server.com protocol tcp ip 202.112.0.1 port 12345
```

【相关命令】

- **display nat all**
- **display nat dns-map**
- **nat server**

1.1.27 nat hairpin enable

nat hairpin enable 命令用来开启 NAT hairpin 功能。

undo nat hairpin enable 用来关闭 NAT hairpin 功能。

【命令】

nat hairpin enable

undo nat hairpin enable

【缺省情况】

NAT hairpin 功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

NAT hairpin 功能用于满足位于内网侧的用户之间或用户与服务器之间通过 NAT 地址进行访问的需求，需要与内部服务器（**nat server**）、出方向动态地址转换（**nat outbound**）或出方向静态地址转换（**nat static outbound**）配合工作。开启 NAT hairpin 的内网侧接口上会对报文同时进行源地址和目的地址的转换。

【举例】

在 GigabitEthernet1/0/1 接口下开启 NAT hairpin 功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat hairpin enable
```

【相关命令】

- **display nat all**

1.1.28 nat icmp-error reply

nat icmp-error reply 命令用来开启 NAT 转换失败时发送 ICMP 差错报文功能。

undo nat icmp-error reply 命令用来恢复缺省情况。

【命令】

nat icmp-error reply

undo nat icmp-error reply

【缺省情况】

NAT 转换失败不发送 ICMP 差错报文。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

缺省情况下，设备在 NAT 转换失败时，不发送 ICMP 差错报文，既可以减少网络上的无用报文，节约带宽，还可以避免将防火墙 IP 地址暴露在公网侧。

使用 traceroute 功能时，需要用到 ICMP 差错报文，需要开启发送 ICMP 差错报文的功能。

【举例】

开启设备在 NAT 转换失败时，发送 ICMP 差错报文功能。

```
<Sysname> system-view
[Sysname] nat icmp-error reply
```

1.1.29 nat inbound

nat inbound 命令用来配置入方向动态地址转换。

undo nat inbound 命令用来删除指定的入方向动态地址转换。

【命令】

nat inbound { *ipv4-acl-number* | **name** *ipv4-acl-name* } **address-group** { *group-id* | **name** *group-name* } [**vpn-instance** *vpn-instance-name*] [**no-pat** [**reversible**] [**add-route**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**description** *text*]

undo nat inbound { *ipv4-acl-number* | **name** *ipv4-acl-name* }

【缺省情况】

不存在入方向动态地址转换配置。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv4-acl-number：ACL 的编号，取值范围为 2000～3999。

name *ipv4-acl-name*：ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 all。

address-group：指定地址转换使用的地址组。

group-id：地址组的编号，取值范围为 0～65535。

group-name：地址组的名称，为 1～63 个字符的字符串，不区分大小写。

vpn-instance *vpn-instance-name*：指定地址组中的地址所属的 VPN。*vpn-instance-name* 表示 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示地址组中的地址不属于任何一个 VPN。

no-pat：表示使用 NO-PAT 方式进行转换，即转换时不使用报文的端口信息。如果未指定本参数，则表示使用 PAT 方式进行转换，即转换时使用报文的端口信息。PAT 方式仅支持 TCP、UDP 和 ICMP 查询报文，由于 ICMP 报文没有端口的概念，我们将 ICMP ID 作为 ICMP 报文的源端口。

reversible：表示允许反向地址转换。即，在外网用户主动向内网发起连接并成功触发建立地址转换表项的情况下，允许内网向该外网用户发起的连接使用已建立的地址转换表项进行目的地址转换。

add-route：为转换后的地址添加路由表，其目的地址是转换后的地址，出接口为进行地址转换的接口，下一跳为该报文转换前的源地址。

rule *rule-name*：NAT 规则的名称，取值范围为 1～63 个字符的字符串，不区分大小写，不能包括“\”、“/”、“:”、“*”、“?”、“<”、“>”、“|”、“”、和“@”。如果不指定该参数，则表示该规则无名称。

priority *priority*：NAT 规则的匹配优先级，取值范围为 0～2147483647，数值越小，优先级越高。如果不指定该参数，那么相应的 NAT 规则在同类 NAT 规则中，其匹配优先级最低。

disable：表示禁用该地址转换映射。如果不指定该参数，则地址转换映射处于启用状态。

description *text*：配置入方向动态地址转换的描述信息，*text* 为 1～63 个字符的字符串，不区分大小写。

【使用指导】

从配置了入方向地址转换的接口接收到的符合 ACL permit 规则的报文，会使用地址组 *group-id* 中的地址进行源地址转换。

入方向地址转换有两种转换方式：

- PAT 方式：对于从外网到内网的报文，如果符合 ACL，则使用地址组中的地址进行源地址转换，同时转换源端口（IP1/port1 转换为 IP2/port2）。
- NO-PAT 方式：对于从外网到内网的报文，如果符合 ACL，则使用地址组中的地址进行源地址转换，不转换源端口（IP1 转换为 IP2）；如果用户配置了 **reversible**，则允许内网通过 IP2 主动访问外网，对于此类访问报文，需要进行 ACL 反向匹配（提取报文的源地址/端口和目的地址/端口，并将目的地址转换为 IP1，然后将源地址/端口和目的地址/端口互换去匹配 ACL），只有反向匹配 ACL 的报文才能进行转换（将目的地址 IP2 转换为 IP1），否则不予转换。

nat inbound 命令通常与 **nat outbound**、**nat server** 或 **nat static** 配合使用，用于支持在外网侧口上对报文同时进行源和目的转换，即双向 NAT。

指定入方向和出方向动态地址转换引用的地址组时，需要注意：

- 一个地址组被 **nat inbound** 配置引用后，就不能再被 **nat outbound** 配置引用。
- 一个地址组被 PAT 方式的 **nat inbound** 配置引用后，不能再被 NO-PAT 方式的 **nat inbound** 配置引用，反之亦然。

add-route 参数不能应用在内网与外网地址重叠的组网场景中。在其他组网场景中：

- 如果指定了 **add-route** 参数，则有报文命中该配置时，设备会自动添加路由表项：目的地址为本次地址转换使用的地址组中的地址，出接口为本配置所在接口，下一跳地址为报文的源地址；
- 如果没有指定 **add-route** 参数，则用户需要在设备上手工添加路由。由于自动添加路由表项速度较慢，通常建议手工添加路由。

在一个接口下，一个 ACL 只能被一个 **nat inbound** 引用。

一个接口下可同时配置多条入方向地址转换。

在 VPN 组网中，配置入方向动态地址转换时需要指定 **vpn-instance** 参数，且 VPN 实例的名称必须与该接口关联的 VPN 实例一致。

对于入方向动态地址转换，当 NAT 规则的匹配优先级相同时，设备将按照 ACL 名称或 ACL 编号进行匹配，且 ACL 名称的优先级高于 ACL 编号的优先级，具体规则如下：

- 对于 ACL 名称，设备将根据名称的字符序对 NAT 规则进行排序，在字符序中的位置越靠前，相应的 NAT 规则的匹配优先级越高。
- 对于 ACL 编号，编号越大，优先级越高，设备将优先进行匹配。

【举例】

配置 ACL 2001，允许对 VPN 实例 vpn10 内 10.110.10.0/24 网段的主机进行地址转换。

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit vpn-instance vpn10 source 10.110.10.0 0.0.0.255
[Sysname-acl-ipv4-basic-2001] rule deny
[Sysname-acl-ipv4-basic-2001] quit
```

配置 VPN 实例 vpn10。

```
[Sysname] ip vpn-instance vpn10
[Sysname-vpn-instance-vpn10] route-distinguisher 100:001
[Sysname-vpn-instance-vpn10] vpn-target 100:1 export-extcommunity
[Sysname-vpn-instance-vpn10] vpn-target 100:1 import-extcommunity
[Sysname-vpn-instance-vpn10] quit
```

配置地址组 1，并添加地址组成员：202.110.10.10、202.110.10.11、202.110.10.12。

```
[Sysname] nat address-group 1
[Sysname-address-group-1] address 202.110.10.10 202.110.10.12
[Sysname-address-group-1] quit
```

在接口 GigabitEthernet1/0/1 上配置入方向动态地址转换，使用地址组 1 中的地址进行地址转换，在转换的时候不使用 TCP/UDP 的端口信息，且需要添加路由。同时指定该入方向动态 NAT 规则的名称为 abc，匹配优先级为 0。

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat inbound 2001 address-group 1 vpn-instance vpn10 no-pat
add-route rule abc priority 0
```

【相关命令】

- **display nat all**
- **display nat inbound**
- **display nat no-pat**

1.1.30 nat inbound rule move

nat inbound rule move 命令用来调整入方向动态 NAT 规则的匹配优先级。

【命令】

nat inbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

nat-rule-name1：要移动的 NAT 规则的名称。

after：将 *nat-rule-name1* 移动到 *nat-rule-name2* 后面，*nat-rule-name2* 的匹配优先级的值不变，*nat-rule-name1* 的匹配优先级的值=*nat-rule-name2* 的匹配优先级的值＋1。

before：将 *nat-rule-name1* 移动到 *nat-rule-name2* 前面，*nat-rule-name2* 的匹配优先级的值不变，*nat-rule-name1* 的匹配优先级的值=*nat-rule-name2* 的匹配优先级的值－1。

nat-rule-name2：要移动的 NAT 规则的名称。

【使用指导】

本命令仅对指定了 NAT 规则名称的入方向动态 NAT 生效。

对于被移动到前面的 NAT 规则，设备将会优先进行匹配。

【举例】

将入方向动态 NAT 规则 abc 移动到入方向动态 NAT 规则 def 的前面。

```
<Sysname> nat inbound rule move abc before def
```

【相关命令】

- **nat inbound**

1.1.31 nat log alarm

nat log alarm 命令用来开启 NAT 告警信息日志功能。

undo nat log alarm 命令用来关闭 NAT 告警信息日志功能。

【命令】

nat log alarm

undo nat log alarm

【缺省情况】

NAT 告警信息日志功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

对于 NAT444 告警日志，在配置 NAT 告警信息日志功能前，必须先配置将用户定制日志发送到日志主机的功能，否则无法产生 NAT444 告警信息日志。详细配置请参见“网络管理和监控配置指导”中的“信息中心”。

【举例】

开启 NAT 告警信息日志功能。

```
<Sysname> system-view
[Sysname] nat log alarm
```

【相关命令】

- **display nat all**
- **display nat log**
- **nat log enable**

1.1.32 nat log enable

nat log enable 命令用来开启 NAT 日志功能。

undo nat log enable 用来关闭 NAT 日志功能。

【命令】

nat log enable [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }]

undo nat log enable

【缺省情况】

NAT 日志功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

acl：指定 ACL 的编号或名称。

ipv4-acl-number：ACL 的编号，取值范围为 2000～3999。

name *ipv4-acl-name*：ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 all。

【使用指导】

必须开启 NAT 日志功能，NAT 会话日志功能（包括 NAT 新建会话、NAT 删除会话和 NAT 活跃流的日志功能）、NAT444 用户日志功能（包括 NAT444 端口块分配和 NAT444 端口块回收的日志功能）和 NAT 告警信息日志功能才能生效。

acl 参数只对 NAT 会话日志功能有效，对其他 NAT 日志功能无效。如果指定了 ACL，则只有符合 ACL permit 规则的数据流才有可能触发输出 NAT 会话日志；如果没有指定 ACL，则表示对所有被 NAT 处理过的数据流都有可能触发输出 NAT 会话日志。

【举例】

开启 NAT 日志功能。

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

【相关命令】

- **display nat all**
- **display nat log**
- **nat log alarm**
- **nat log flow-active**
- **nat log flow-begin**
- **nat log flow-end**
- **nat log port-block-assign**

- **nat log port-block-withdraw**

1.1.33 nat log flow-active

nat log flow-active 命令用来开启 NAT 活跃流日志功能，并设置生成活跃流日志的时间间隔。

undo nat log flow-active 命令用来关闭 NAT 活跃流的日志功能。

【命令】

nat log flow-active *time-value*

undo nat log flow-active

【缺省情况】

NAT 活跃流的日志功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

time-value：表示触发输出 NAT 活跃流日志的时间间隔，取值范围为 10～120，单位为分钟。

【使用指导】

对于一些长时间没有断开的 NAT 会话（即活跃流），如果需要定期记录其连接情况，则可以通过活跃流日志功能来实现。

开启 NAT 活跃流日志功能后，对于 NAT 活跃流，每经过指定的时间间隔，设备就会记录一次 NAT 日志。

只有开启 NAT 日志功能之后，活跃流日志功能才能生效。

【举例】

开启 NAT 活跃流日志功能，并设置输出 NAT 活跃流日志的时间间隔为 10 分钟。

```
<Sysname> system-view
[Sysname] nat log flow-active 10
```

【相关命令】

- **display nat all**
- **display nat log**
- **nat log enable**

1.1.34 nat log flow-begin

nat log flow-begin 命令用来开启 NAT 新建会话的日志功能，即新建 NAT 会话时，输出 NAT 日志。

undo nat log flow-begin 命令用来关闭 NAT 新建会话的日志功能。

【命令】

nat log flow-begin

undo nat log flow-begin

【缺省情况】

NAT 新建会话的日志功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

只有开启 NAT 日志功能之后，NAT 新建会话的日志功能才能生效。

【举例】

开启 NAT 新建会话的日志功能。

```
<Sysname> system-view
[Sysname] nat log flow-begin
```

【相关命令】

- **display nat all**
- **display nat log**
- **nat log enable**

1.1.35 nat log flow-end

nat log flow-end 命令用来开启 NAT 删除会话的日志功能。

undo nat log flow-end 命令用来关闭 NAT 删除会话的日志功能。

【命令】

nat log flow-end

undo nat log flow-end

【缺省情况】

NAT 删除会话的日志功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

只有开启 NAT 日志功能之后，NAT 删除会话的日志功能才能生效。

【举例】

开启 NAT 删除会话的日志功能。

```
<Sysname> system-view
[Sysname] nat log flow-end
```

【相关命令】

- **display nat all**
- **display nat log**
- **nat log enable**

1.1.36 nat log port-block usage threshold

nat log port-block usage threshold 命令用来配置动态 NAT444 端口块使用率的阈值。

undo nat log port-block usage threshold 命令用来恢复缺省情况。

【命令】

nat log port-block usage threshold *threshold-value*

undo nat log port-block usage threshold

【缺省情况】

动态 NAT444 的端口块使用率的阈值为 90%。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

threshold-value：端口使用率的阈值，为百分比数值，取值范围为 40～100。

【使用指导】

创建动态端口块表项时，若端口块的使用率大于阈值，系统会输出告警日志。

【举例】

配置动态 NAT444 端口块使用率的阈值为 60%。

```
<Sysname> system-view
[Sysname] nat log port-block usage threshold 60
```

1.1.37 nat log port-block-assign

nat log port-block-assign 命令用来开启端口块分配的 NAT444 用户日志功能。

undo nat log port-block-assign 命令用来关闭端口块分配的 NAT444 用户日志功能。

【命令】

nat log port-block-assign

undo nat log port-block-assign

【缺省情况】

端口块分配的 NAT444 用户日志功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

端口块静态映射方式下，在某私网 IP 地址的第一个新建连接通过端口块进行地址转换时，如果开启了端口块分配的 NAT444 用户日志功能，则会输出日志。

端口块动态映射方式下，在为某私网 IP 地址分配端口块或增量端口块时，如果开启了端口块分配的 NAT444 用户日志功能，则会输出日志。

只有开启 NAT 日志功能之后，端口块分配的 NAT444 用户日志功能才能生效。

【举例】

开启端口块分配的 NAT444 用户日志功能。

```
<Sysname> system-view
[Sysname] nat log port-block-assign
```

【相关命令】

- **display nat all**
- **display nat log**
- **nat log enable**

1.1.38 nat log port-block-withdraw

nat log port-block-withdraw 命令用来开启端口块回收的 NAT444 用户日志功能。

undo nat log port-block-withdraw 命令用来关闭端口块回收的 NAT444 用户日志功能。

【命令】

nat log port-block-withdraw

undo nat log port-block-withdraw

【缺省情况】

端口块回收的 NAT444 用户日志功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

端口块静态映射方式下，在某私网 IP 地址的最后一个连接拆除时，如果开启了端口块回收的 NAT444 用户日志功能，则会输出日志。

端口块动态映射方式下，在释放端口块资源（并删除端口块表项）时，如果开启了端口块回收的 NAT444 用户日志功能，则会输出日志。

只有开启 NAT 日志功能之后，端口块回收的 NAT444 用户日志功能才能生效。

【举例】

开启端口块回收的 NAT444 用户日志功能。

```
<Sysname> system-view
[Sysname] nat log port-block-withdraw
```

【相关命令】

- **display nat all**
- **display nat log**
- **nat log enable**

1.1.39 nat mapping-behavior

nat mapping-behavior 命令用来配置 PAT 方式出方向动态地址转换的模式。

undo nat mapping-behavior 命令用来恢复缺省情况。

【命令】

nat mapping-behavior endpoint-independent [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }]

undo nat mapping-behavior endpoint-independent

【缺省情况】

PAT 出方向动态方式地址转换的模式为 Address and Port-Dependent Mapping。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

acl：指定 ACL 的编号或名称，用于控制需要遵守指定地址转换模式的报文范围。

ipv4-acl-number：ACL 的编号，取值范围为 2000～3999。

name *ipv4-acl-name*：ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 all。

【使用指导】

PAT 方式出方向动态地址转换支持两种模式：

- Endpoint-Independent Mapping（不关心对端地址和端口的转换模式）：只要是来自相同源地址和源端口号的报文，不论其目的地址是否相同，通过 PAT 映射后，其源地址和源端口号都被转换为同一个外部地址和端口号，该映射关系会被记录下来并生成一个 EIM 表项；并且 NAT 网关设备允许外部网络的主机通过该转换后的地址和端口来访问这些内部网络的主机。这种模式可以很好的支持位于不同 NAT 网关之后的主机间进行互访。

- Address and Port-Dependent Mapping（关心对端地址和端口的转换模式）：对于来自相同源地址和源端口号的报文，若其目的地址和目的端口号不同，由于相同的源地址和源端口号不要求被转换为相同的外部地址和端口号，所以通过 PAT 映射后，相同的源地址和源端口号通常会被转换成不同的外部地址和端口号。并且 NAT 网关设备只允许这些目的地址对应的外部网络的主机才可以通过该转换后的地址和端口来访问这些内部网络的主机。这种模式安全性好，但是不便于位于不同 NAT 网关之后的主机间进行互访。

该配置只对出方向动态地址转换的 PAT 方式起作用。入方向动态地址转换的 PAT 方式的转换模式始终为 Address and Port-Dependent Mapping。

如果配置了 **acl** 参数，则表示只有符合 ACL permit 规则的报文才采用 Endpoint-Independent Mapping 模式进行地址转换；如果没有配置 **acl** 参数，则表示所有的报文都采用 Endpoint-Independent Mapping 模式进行地址转换。

【举例】

对所有报文都以 Endpoint-Independent Mapping 模式进行地址转换。

```
<Sysname> system-view
[Sysname] nat mapping-behavior endpoint-independent
```

仅对 FTP 和 HTTP 报文才以 Endpoint-Independent Mapping 模式进行地址转换，其它报文采用 Address and Port-Dependent Mapping 模式进行地址转换。

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule permit tcp destination-port eq 80
[Sysname-acl-ipv4-adv-3000] rule permit tcp destination-port eq 21
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] nat mapping-behavior endpoint-independent acl 3000
```

【相关命令】

- **nat outbound**
- **display nat eim**

1.1.40 nat outbound

nat outbound 命令用来配置出方向动态地址转换。

undo nat outbound 命令用来删除指定的出方向动态地址转换。

【缺省情况】

不存在动态地址转换配置。

【命令】

- NO-PAT 方式

nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*] **address-group** { *group-id* | **name** *group-name* } [**vpn-instance** *vpn-instance-name*] **no-pat** [**reversible**] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**description** *text*]

undo nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*]

- PAT 方式

nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*] [**address-group** { *group-id* | **name** *group-name* }] [**vpn-instance** *vpn-instance-name*] [**port-preserved**] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**description** *text*]

undo nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*]

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv4-acl-number：ACL 的编号，取值范围为 2000～3999。

name *ipv4-acl-name*：ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 all。

address-group：指定地址转换使用的地址组。如果不指定该参数，则直接使用该接口的 IP 地址作为转换后的地址，即实现 Easy IP 功能。

group-id：地址组的编号，取值范围为 0～65535。

group-name：地址组的名称，为 1～63 个字符的字符串，不区分大小写。

vpn-instance *vpn-instance-name*：指定地址组中的地址所属的 VPN。*vpn-instance-name* 表示 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示地址组中的地址不属于任何一个 VPN。

no-pat：表示使用 NO-PAT 方式进行转换，即转换时不使用报文的端口信息；如果未指定本参数，则表示使用 PAT 方式进行转换，即转换时使用报文的端口信息。PAT 方式仅支持 TCP、UDP 和 ICMP 查询报文，由于 ICMP 报文没有端口的概念，我们将 ICMP ID 作为 ICMP 报文的源端口。

reversible：表示允许反向地址转换。即，在内网用户主动向外网发起连接并成功触发建立地址转换表项的情况下，允许外网向该内网用户发起的连接使用已建立的地址转换表项进行目的地址转换。

port-preserved：PAT 方式分配端口时尽量不转换端口。

rule *rule-name*：NAT 规则的名称，取值范围为 1～63 个字符的字符串，不区分大小写，不能包括“\”、“/”、“:”、“*”、“?”、“<”、“>”、“|”、“””、和“@”。如果不指定该参数，则表示该规则无名称。

priority *priority*：NAT 规则的匹配优先级，取值范围为 0～2147483647，数值越小，优先级越高。如果不指定该参数，那么相应的 NAT 规则在同类 NAT 规则中，其匹配优先级最低。

disable：表示禁用该地址转换映射。如果不指定该参数，则地址转换映射处于启用状态。

description *text*：配置出方向动态地址转换的描述信息，*text* 为 1～63 个字符的字符串，不区分大小写。

【使用指导】

一般情况下，出方向动态地址转换配置在和外部网络连接的接口上。动态地址转换有两种转换方式：

- PAT 方式：对于从内网到外网的报文，如果符合 ACL permit 规则，则使用地址组中的地址或该接口的地址（Easy IP 方式）进行源地址转换，同时转换源端口（IP1/port1 转换为 IP2/port2）；如果同时配置了 PAT 方式下的地址转换模式为 EIM（Endpoint-Independent Mapping），则

外网可以通过 IP2/port2 主动访问内网，NAT 设备根据 EIM 表项转换目的地址和端口（IP2/port2 转换为 IP1/port1）。

- NO-PAT 方式：对于从内网到外网的报文，如果符合 ACL permit 规则，则使用地址组中的地址进行源地址转换，不转换源端口（IP1 转换为 IP2）；如果同时配置了 **reversible**，则允许外网通过 IP2 主动访问内网，对于此类报文，需要进行 ACL 反向匹配（提取报文的源地址/端口和目的地址/端口，并将目的地址转换为 IP1，然后将源地址/端口和目的地址/端口互换去匹配 ACL），只有反向匹配 ACL 的报文才能进行转换（将目的地址 IP2 转换为 IP1），否则不予转换。NAT444 端口块动态映射不支持该方式。

一个接口下可同时配置多条出方向地址转换。

指定出方向和入方向动态地址转换引用的地址组时，需要注意：

- 一个地址组被 **nat outbound** 配置引用后，不能再被 **nat inbound** 引用。
- 一个地址组被 PAT 方式的 **nat outbound** 配置引用后，不能再被 NO-PAT 方式的 **nat outbound** 配置引用，反之亦然。
- 如果 PAT 方式的 **nat outbound** 所引用的地址组中配置了端口块参数，则将对匹配的报文进行 NAT444 端口块动态映射。**port-preserved** 参数对 NAT444 端口块动态映射无效。

指定出方向动态地址转换引用的 ACL 时，需要注意：

- 在一个接口下，一个 ACL 只能被一个 **nat outbound** 引用。
- 配置多条出方向动态地址转换时，只有一个 **nat outbound** 可以不引用 ACL。
- 不指定 ACL 编号或名称的情况下，不对转换对象进行限制。
- 对于同一接口下的出方向动态地址转换配置，指定了 ACL 的配置的优先级高于未指定 ACL 的配置的优先级；对于指定了 ACL 的出方向动态地址转换配置，其生效优先级由 ACL 编号的大小决定，编号越大，优先级越高。

在 VPN 组网中，配置出方向动态地址转换时需要指定 **vpn-instance** 参数，且 VPN 实例的名称必须与该接口关联的 VPN 实例一致。

对于引用了 ACL 的出方向动态地址转换，当 NAT 规则的匹配优先级相同时，设备将按照 ACL 名称或 ACL 编号进行匹配，且 ACL 名称的优先级高于 ACL 编号的优先级，具体规则如下：

- 对于 ACL 名称，设备将根据名称的字符序对 NAT 规则进行排序，在字符序中的位置越靠前，相应的 NAT 规则的匹配优先级越高。
- 对于 ACL 编号，编号越大，优先级越高，设备将优先进行匹配。

【举例】

配置 ACL 2001，允许对 10.110.10.0/24 网段的主机报文进行地址转换。

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.110.10.0 0.0.0.255
[Sysname-acl-ipv4-basic-2001] rule deny
[Sysname-acl-ipv4-basic-2001] quit
```

配置地址组 1，并添加地址组成员：202.110.10.10、202.110.10.11、202.110.10.12。

```
[Sysname] nat address-group 1
[Sysname-address-group-1] address 202.110.10.10 202.110.10.12
[Sysname-address-group-1] quit
```

在接口 GigabitEthernet1/0/1 上配置出方向动态地址转换，允许对匹配 ACL 2001 的报文使用地址组 1 中的地址进行地址转换，且在转换的时候使用 TCP/UDP 的端口信息。

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat outbound 2001 address-group 1
[Sysname-GigabitEthernet1/0/1] quit
```

如果在接口 GigabitEthernet1/0/1 上不使用 TCP/UDP 的端口信息进行地址转换，可以使用如下配置。

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat outbound 2001 address-group 1 no-pat
[Sysname-GigabitEthernet1/0/1] quit
```

如果直接使用接口 GigabitEthernet1/0/1 接口的 IP 地址进行地址转换，可以使用如下的配置。

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet 1/0/1] nat outbound 2001
[Sysname-GigabitEthernet 1/0/1] quit
```

内网 10.110.10.0/24 网段的主机使用地址组 1 中的地址作为转换后的地址访问外部网络。如果要在内网用户向外网主动发起访问之后，允许外网用户主动向 10.110.10.0/24 网段的主机发起访问，并利用已建立的地址转换表项进行反向地址转换，可以使用如下配置。

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat outbound 2001 address-group 1 no-pat reversible
```

【相关命令】

- **display nat eim**
- **display nat outbound**
- **nat mapping-behavior**

1.1.41 nat outbound ds-lite-b4

nat outbound ds-lite-b4 命令用来配置 DS-Lite B4 端口块映射。

undo nat outbound ds-lite-b4 命令用来删除指定的 DS-Lite B4 端口块映射。

【命令】

nat outbound ds-lite-b4 { *ipv6-acl-number* | **name** *ipv6-acl-name* } **address-group** *group-id*

undo nat outbound ds-lite-b4 { *ipv6-acl-number* | **name** *ipv6-acl-name* }

【缺省情况】

不存在 DS-Lite B4 端口块映射。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv6-acl-number：用于匹配 B4 设备 IPv6 地址的 IPv6 ACL 编号，取值范围为 2000～2999。

name *ipv6-acl-name*：用于匹配 B4 设备 IPv6 地址的 IPv6 ACL 名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 all。

address-group *group-id*：指定地址转换使用的地址组。*group-id* 为地址组的编号，取值范围为 0～65535。目前仅支持端口块动态映射方式的地址组，因此指定的 NAT 地址组中必须配置端口块参数，否则配置不生效。

【使用指导】

在使用 DS-Lite 隧道技术实现通过 IPv6 网络连接 IPv4 网络的组网环境下，DS-Lite B4 端口块映射配置在 NAT444 网关设备连接外部网络的接口上，通常用于在 NAT444 网关设备已知 B4 设备或 DS-Lite 主机的 IPv6 地址的情况下为 DS-Lite 用户提供 NAT 地址转换。

【举例】

配置 IPv6 ACL 2100，允许对 2000::/64 网段的主机报文进行地址转换。

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2100
[Sysname-acl-ipv6-basic-2100] rule permit source 2000::/64
[Sysname-acl-ipv6-basic-2100] quit
```

配置地址组 1，并添加地址组成员：202.110.10.10～202.110.10.12。

```
[Sysname] nat address-group 1
[Sysname-nat-address-group-1] address 202.110.10.10 202.110.10.12
```

配置地址组 1 的端口块参数，端口块大小为 256。

```
[Sysname-nat-address-group-1] port-block block-size 256
[Sysname-nat-address-group-1] quit
```

在接口 GigabitEthernet1/0/1 上配置 DS-Lite B4 端口块映射，允许对匹配 IPv6 ACL 2100 的报文使用地址组 1 中的地址进行地址转换。

```
[Sysname] interface ethernet 1/1
[Sysname-GigabitEthernet1/0/1] nat outbound ds-lite-b4 2100 address-group 1
```

【相关命令】

- **display nat outbound**

1.1.42 nat outbound port-block-group

nat outbound port-block-group 命令用来配置 NAT444 端口块静态映射。

undo nat outbound port-block-group 命令用来删除指定的 NAT444 端口块静态映射配置。

【命令】

nat outbound port-block-group *group-id* [**rule** *rule-name*]

undo nat outbound port-block-group *group-id*

【缺省情况】

不存在 NAT444 端口块静态映射配置。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

group-id：端口块组的编号，取值范围为 0～65535。

rule *rule-name*：NAT 规则的名称，取值范围为 1～63 个字符的字符串，不区分大小写，不能包括“\”、“/”、“:”、“*”、“?”、“<”、“>”、“|”、“”” 和 “@”。如果不指定该参数，则表示该规则无名称。

【使用指导】

该配置在接口下引用指定的端口块组，根据端口块组内的配置数据，按照固定的算法为每个私网 IP 地址分配一个静态端口块并创建静态端口块表项。当某私网 IP 地址向公网发起连接时，通过该私网 IP 地址查找静态端口块表项，使用表项中记录的公网 IP 地址进行地址转换，并从对应的端口块中动态分配一个端口进行 TCP/UDP 端口转换。

一个接口下可以配置多条基于不同端口块组的 NAT444 端口块静态映射。

IRF 组网环境下，还需要通过命令 **ip fast-forwarding load-sharing** 配置负载分担，否则会导致端口分配冲突。

【举例】

在接口 GigabitEthernet1/0/1 的出方向上配置基于端口组 1 的 NAT444 端口块静态映射。同时指定该 NAT444 端口块静态映射规则的名称为 abc。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat outbound port-block-group 1 rule abc
```

【相关命令】

- **display nat all**
- **display nat outbound port-block-group**
- **display nat port-block**
- **nat port-block-group**

1.1.43 nat outbound rule move

nat outbound rule move 命令用来调整出方向动态 NAT 规则的匹配优先级。

【命令】

nat outbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

nat-rule-name1：要移动的 NAT 规则的名称。

after：将 *nat-rule-name1* 移动到 *nat-rule-name2* 后面，*nat-rule-name2* 的匹配优先级的值不变，*nat-rule-name1* 的匹配优先级的值=*nat-rule-name2* 的匹配优先级的值＋1。

before：将 *nat-rule-name1* 移动到 *nat-rule-name2* 前面，*nat-rule-name2* 的匹配优先级的值不变，*nat-rule-name1* 的匹配优先级的值=*nat-rule-name2* 的匹配优先级的值－1。

nat-rule-name2：要移动的 NAT 规则的名称。

【使用指导】

本命令仅对指定了 NAT 规则名称的出方向动态 NAT 生效。

对于被移动到前面的 NAT 规则，设备将会优先进行匹配。

【举例】

将出方向动态 NAT 规则 abc 移动到出方向动态 NAT 规则 def 的前面。

```
<Sysname> nat outbound rule move abc before def
```

【相关命令】

- **nat outbound**

1.1.44 nat port-block global-share enable

nat port-block global-share enable 命令用来开启端口块全局共享功能。

undo nat port-block global-share enable 命令用来关闭端口块全局共享功能。

【命令】

nat port-block global-share enable

undo nat port-block global-share enable

【缺省情况】

端口块全局共享功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

在已配置 NAT444 端口块动态映射的情况下，当同一个源 IP 地址的报文从不同出接口进行 NAT 地址转换时，可能会分配到不同的端口块。如果需要使同一个源 IP 地址分配到相同的端口块，请开启端口块全局共享功能。

【举例】

开启端口块全局共享功能。

```
<Sysname> system-view
[Sysname] nat port-block global-share enable
```

【相关命令】

- **port-block**

1.1.45 nat port-block synchronization enable

nat port-block synchronization enable 命令用来开启 NAT444 业务热备份功能。

undo nat port-block synchronization enable 命令用来关闭 NAT444 业务热备份功能。

【命令】

nat port-block synchronization enable

undo nat port-block synchronization enable

【缺省情况】

NAT444 业务热备份功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

在业务热备份环境中，通过开启 NAT444 业务热备份功能，可以实现主备切换后动态 NAT444 端口块表项一致。

【举例】

开启 NAT444 业务热备份功能。

```
<Sysname> system-view
[Sysname] nat port-block synchronization enable
```

1.1.46 nat port-block-group

nat port-block-group 命令用来创建 NAT 端口块组，并进入 NAT 端口块组视图。如果指定的 NAT 端口块组已经存在，则直接进入 NAT 端口块组视图。

undo nat port-block-group 命令用来删除指定的 NAT 端口块组。

【命令】

nat port-block-group *group-id*

undo nat port-block-group *group-id*

【缺省情况】

不存在 NAT 端口块组。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

group-id：NAT 端口块组的编号，取值范围为 0～65535。

【使用指导】

创建的 NAT 端口块组用于配置 NAT444 端口块静态映射。一个端口块组中包含如下内容：

- 一个或多个私网地址成员，通过 **local-ip-address** 命令配置。
- 一个或多个公网地址成员，通过 **global-ip-pool** 命令配置。
- 公网地址的端口范围，通过 **port-range** 命令配置。
- 端口块大小，通过 **block-size** 命令配置。

在进行 NAT444 端口块静态映射时，系统根据相应端口块组的配置计算出私网 IP 地址到公网 IP 地址、端口块的静态映射关系，并创建静态端口块表项。

【举例】

创建一个 NAT 端口块组，编号为 1。

```
<Sysname>system-view
[Sysname]nat port-block-group 1
[Sysname-port-block-group-1]
```

【相关命令】

- **block-size**
- **display nat all**
- **display nat port-block-group**
- **global-ip-pool**
- **local-ip-address**
- **nat outbound port-block-group**
- **port-range**

1.1.47 nat port-load-balance enable

nat port-load-balance enable 命令用来开启 NAT 端口负载分担功能。

undo nat port-load-balance enable 命令用来关闭 NAT 端口负载分担功能。

【命令】

nat port-load-balance enable slot *slot-number*

undo nat port-load-balance enable slot *slot-number*

【缺省情况】

NAT 端口负载分担功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

slot *slot-number*：指定使用数值较小的一半端口的成员设备，*slot-number* 表示设备在 IRF 中的成员编号。

【使用指导】

在双机热备的负载分担场景下，开启 NAT 端口负载分担功能后，两台设备各获得一半端口块资源，使相同私网 IP 地址在不同的成员设备上独占一定的端口资源，避免端口分配冲突。

在双机热备的主备备份场景下或者设备工作于独立运行模式下时，不需要配置此命令。

【举例】

开启 NAT 端口负载分担功能，并指定 1 号成员设备使用数值较小的一半端口。

```
<Sysname> system
[Sysname] nat port-load-balance enable slot 1
```

【相关命令】

- **nat port-block synchronization enable**

1.1.48 nat redirect reply-route

nat redirect reply-route enable 命令用来开启反向报文的重定向功能。

undo nat redirect reply-route enable 命令用来关闭反向报文的重定向功能。

【命令】

nat redirect reply-route enable

undo nat redirect reply-route enable

【缺省情况】

反向报文的重定向功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

通过在设备的出接口开启反向报文的重定向功能，使出接口收到反向报文后查询 NAT 会话表项，根据 NAT 会话表项记录的信息将反向报文的目的 IP 地址进行 NAT 地址转换，从而使反向报文通过接收正向报文的隧道发送出去。

【举例】

开启接口 GigabitEthernet1/0/2 上的反向报文的重定向功能。

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

```
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] nat redirect reply-route enable
```

1.1.49 nat server

nat server 命令用来配置 NAT 内部服务器，即定义内部服务器的外网地址和端口与内网地址和端口的映射表项。

undo nat server 命令用来删除指定的内部服务器配置。

【命令】

(1) 普通内部服务器

- 外网地址单一，未使用外网端口或外网端口单一

nat server [**protocol** *pro-type*] **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } [*global-port*] [**vpn-instance** *global-vpn-instance-name*] **inside** *local-address* [*local-port*] [**vpn-instance** *local-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**reversible**] [**rule** *rule-name*] [**disable**] [**description** *text*]

undo nat server [**protocol** *pro-type*] **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } [*global-port*] [**vpn-instance** *global-vpn-instance-name*]

- 外网地址单一，外网端口连续

nat server protocol *pro-type* **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } *global-port1 global-port2* [**vpn-instance** *global-vpn-instance-name*] **inside** { { *local-address* | *local-address1 local-address2* } *local-port* | *local-address local-port*1 *local-port*2 } [**vpn-instance** *local-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**rule** *rule-name*] [**disable**] [**description** *text*]

undo nat server protocol *pro-type* **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } *global-port1 global-port2* [**vpn-instance** *global-vpn-instance-name*]

- 外网地址连续，未使用外网端口或外网端口单一

nat server protocol *pro-type* **global** *global-address1 global-address2* [*global-port*] [**vpn-instance** *global-vpn-instance-name*] **inside** { *local-address* | *local-address1 local-address2* } [*local-port*] [**vpn-instance** *local-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**rule** *rule-name*] [**disable**] [**description** *text*]

undo nat server protocol *pro-type* **global** *global-address1 global-address2* [*global-port*] [**vpn-instance** *global-vpn-instance-name*]

- 外网地址连续，外网端口单一

nat server protocol *pro-type* **global** *global-address1 global-address2 global-port* [**vpn-instance** *global-vpn-instance-name*] **inside** *local-address local-port*1 *local-port*2 [**vpn-instance** *local-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**rule** *rule-name*] [**disable**] [**description** *text*]

undo nat server protocol *pro-type* **global** *global-address1 global-address2 global-port* [**vpn-instance** *global-vpn-instance-name*]

(2) 负载均衡内部服务器

nat server protocol *pro-type* **global** { { *global-address* | **current-interface** | **interface** *interface-type interface-number* } { *global-port* | *global-port1 global-port2* } | *global-address1 global-address2 global-port* } [**vpn-instance** *global-vpn-instance-name*] **inside server-group** *group-id* [**vpn-instance** *local-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**rule** *rule-name*] [**disable**] [**description** *text*]

undo nat server protocol *pro-type* **global** { { *global-address* | **current-interface** | **interface** *interface-type interface-number* } { *global-port* | *global-port1 global-port2* } | *global-address1 global-address2 global-port* } [**vpn-instance** *global-vpn-instance-name*]

(3) 基于 ACL 的内部服务器

nat server global { *ipv4-acl-number* | **name** *ipv4-acl-name* } **inside** *local-address* [*local-port*] [**vpn-instance** *local-vpn-instance-name*] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**description** *text*]

undo nat server global { *ipv4-acl-number* | **name** *ipv4-acl-name* }

【缺省情况】

不存在内部服务器。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

protocol *pro-type*：指定协议类型。只有当协议类型是 TCP、UDP 协议时，配置的内部服务器才能带端口参数。如果不指定协议类型，则表示对所有协议类型的报文都生效。*pro-type* 可输入以下形式：

- 数字：取值范围为 1～255。
- 协议名称：取值包括 **icmp**、**tcp** 和 **udp**。

global-address：内部服务器向外提供服务时对外公布的外网 IP 地址。

global-address1、*global-address2*：外网 IP 地址范围，所包含的地址数目不能超过 10000。*global-address1* 表示起始地址，*global-address2* 表示结束地址。*global-address2* 必须大于 *global-address1*。

global：指定 ACL 的编号或名称。只有与指定的 ACL permit 规则匹配的报文才可以进行目的地址转换。

ipv4-acl-number：ACL 的编号，取值范围为 2000～3999。

name *ipv4-acl*-name：ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 all。

current-interface：使用当前接口的地址作为内部服务器的外网地址，即实现 Easy IP 方式的内部服务器。

interface *interface-type interface-number*：表示使用指定接口的地址作为内部服务器的外网地址，即实现 Easy IP 方式的内部服务器。*interface-type interface-number* 表示接口类型和接口编号。目前只支持 Loopback 接口。

global-port1、*global-port2*：外网端口范围，和内部主机的 IP 地址范围构成一一对应的关系。*global-port1* 表示起始端口，*global-port2* 表示结束端口。*global-port2* 必须大于 *global-port1*，且端口范围中的端口数目不能大于 10000。外网端口可输入以下形式：

- 数字：取值范围为 1～65535。起始端口和结束端口均支持此形式。
- 协议名称：为 1～15 个字符的字符串，例如 **http**、**telnet** 等。仅起始端口支持该形式。

local-address1、*local-address2*：定义一组连续的内网 IP 地址范围，和外网端口范围构成一一对应的关系。*local-address1* 表示起始地址，*local-address2* 表示结束地址。*local-address2* 必须大于 *local-address1*。该地址范围的数量必须和 *global-port1*、*global-port2* 定义的端口数量相同。

local-port：内部服务器的内网端口号，可输入以下形式：

- 数字：取值范围为 1～65535（FTP 数据端口号 20 除外）。
- 协议名称：为 1～15 个字符的字符串，例如 **http**、**telnet** 等。

global-port：外网端口号，缺省值以及取值范围的要求和 *local-port* 的规定一致。

local-address：服务器的内网 IP 地址。

vpn-instance *global-vpn-instance-name*：对外公布的外网地址所属的 VPN。*global-vpn-instance-name* 表示 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示对外公布的外网地址不属于任何一个 VPN。

vpn-instance *local-vpn-instance-name*：内部服务器所属的 VPN。*local-vpn-instance-name* 表示 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示内部服务器不属于任何一个 VPN。

server-group *group-id*：服务器在内网所属的服务器组。若指定了该参数，则表示要配置一个负载分担内部服务器。*group-id* 表示内部服务器组的编号，取值范围为 0～65535。

acl：指定 ACL 的编号或名称。若指定了该参数，则表示与指定的 ACL permit 规则匹配的报文才可以使用内部服务器的映射表进行地址转换。

ipv4-acl-number：ACL 的编号，取值范围为 2000～3999。

name *ipv4-acl-name*：ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 all。

reversible：表示支持私网侧内部服务器主动访问外网。内部服务器主动访问外网时，将私网地址转换为内部服务器向外提供服务的外网 IP 地址。

rule *rule-name*：NAT 规则的名称，取值范围为 1～63 个字符的字符串，不区分大小写，不能包括“\”、“/”、“:”、“*”、“?”、“<”、“>”、“|”、“”” 和 “@”。如果不指定该参数，则表示该规则无名称。

priority *priority*：NAT 规则的匹配优先级，取值范围为 0～2147483647，数值越小，优先级越高。如果不指定该参数，那么相应的 NAT 规则在同类 NAT 规则中，其匹配优先级最低。

disable：表示禁用该地址转换映射。如果不指定该参数，则地址转换映射处于启用状态。

description *text*：配置 NAT 内部服务器的描述信息，*text* 为 1～63 个字符的字符串，不区分大小写。

【使用指导】

通过该配置可以利用 NAT 设备将一些内部网络的服务器提供给外部网络使用，例如内部的 Web 服务器、FTP 服务器、Telnet 服务器、POP3 服务器、DNS 服务器等。这些内部服务器可以位于普通的内网内，也可以位于 VPN 实例内。

NAT 内部服务器通常配置在 NAT 设备的外网侧接口上。外网用户可以通过 *global-address* 定义的外网地址和 *global-port* 定义的外网端口来访问内网地址和内网端口分别为 *local-address* 和 *local-port* 的内部服务器。当 *pro-type* 不是 TCP（协议号为 6）或 UDP（协议号为 17）时，用户只能设置内部 IP 地址与外部 IP 地址的一一对应的关系，无法设置端口号之间的映射。

NAT 内部服务器支持以下几种内网和外网的地址、端口映射关系。

表1-20 NAT 内部服务器的地址与端口映射关系

外网	内网
一个外网地址	一个内网地址
一个外网地址、一个端口号	一个内网地址、一个内网端口号
一个外网地址，N个连续的外网端口号	一个内网地址，一个内网端口
	N个连续的内网地址，一个内网端口号
	一个内网地址，N个连续的内网端口号
N个连续的外网地址	一个内网地址
	N个连续的内网地址
N个连续的外网地址连续，一个外网端口号	一个内网地址，一个内网端口号
	N个连续的内网地址，一个内网端口号
	一个内网地址，N个连续的内网端口号
一个外网地址，一个外网端口号	一个内部服务器组
一个外网地址，N个连续的外网端口号	
N个连续的外网地址，一个外网端口号	
外网地址（通过ACL进行匹配）	一个内网地址
	一个内网地址、一个内网端口号

一个接口下允许配置的 **nat server** 命令个数与设备的型号有关。对于同一个接口下配置的 NAT 服务器，其协议类型、外网地址和外网端口号的组合必须是唯一的，否则认为是配置冲突。本规则同样适用于 Easy IP 方式的 NAT 服务器。每个 **nat server** 命令下可以配置的 NAT 内部服务器数目为 *global-port2* 与 *global-port1* 的差值，即配置多少个外网端口就对应多少个 NAT 内部服务器。

设备支持引用接口地址作为 NAT 内部服务器的外网地址（Easy IP 方式）。如果配置关键字 **current-interface**，表示外网地址使用的是当前接口的当前主地址；如果指定具体的接口，则只能指定 Loopback 接口，外网地址使用的是配置的 Loopback 接口的当前主地址。

由于 Easy IP 方式的 NAT 内部服务器使用了当前接口或其它接口的 IP 地址作为它的外网地址，因此强烈建议在配置了 Easy IP 方式的 NAT 内部服务器之后，其它 NAT 内部服务器不要再配置该接口的 IP 地址作为它的外网地址，反之亦然。

对于 Easy IP 方式的 NAT 服务器，如果其引用的接口的 IP 地址发生改变，导致跟现有的其它非 Easy IP 方式的 NAT 服务器冲突，则 Easy IP 方式的 NAT 服务器配置失效；如果接口地址又修改为不冲突的 IP，或者之前与之冲突的 NAT 服务器被删除，则 Easy IP 方式的 NAT 配置重新生效。

在 VPN 组网中，配置 NAT 内部服务器时需要指定 **vpn-instance** 参数，且 VPN 实例的名称必须与该接口关联的 VPN 实例一致。

在配置负载均衡内部服务器时，若配置一个外网地址，N 个连续的外网端口号对应一个内部服务器组，或 N 个连续的外网地址，一个外网端口号对应一个内部服务器组，则内部服务器组的成员个数不能小于 N，即同一用户不能通过不同的外网地址或外网端口号访问相同内网服务器的同一服务。

对于基于 ACL 的内部服务器，当 NAT 规则的匹配优先级相同时，设备将按照 ACL 名称或 ACL 编号进行匹配，且 ACL 名称的优先级高于 ACL 编号的优先级，具体规则如下：

- 对于 ACL 名称，设备将根据名称的字符序对 NAT 规则进行排序，在字符序中的位置越靠前，相应的 NAT 规则的匹配优先级越高。
- 对于 ACL 编号，编号越大，优先级越高，设备将优先进行匹配。

【举例】

在接口 GigabitEthernet1/0/1 上配置 NAT 内部服务器，指定局域网内部的 Web 服务器的 IP 地址是 10.110.10.10，希望外部通过 http://202.110.10.10:8080 可以访问 Web 服务器。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat server protocol tcp global 202.110.10.10 8080 inside 10.110.10.10 http
[Sysname-GigabitEthernet1/0/1] quit
```

在接口 GigabitEthernet1/0/1 上配置 NAT 内部服务器，指定 VPN vrf10 内部的 FTP 服务器的 IP 地址是 10.110.10.11，希望外部通过 ftp://202.110.10.10 可以访问 FTP 服务器。

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat server protocol tcp global 202.110.10.10 21 inside 10.110.10.11 vpn-instance vrf10
[Sysname-GigabitEthernet1/0/1] quit
```

在接口 GigabitEthernet1/0/1 上配置 NAT 内部服务器，指定一个 VPN vrf10 内部的主机 10.110.10.12，希望外部网络的主机可以利用 ping 202.110.10.11 命令 ping 通它。

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat server protocol icmp global 202.110.10.11 inside 10.110.10.12 vpn-instance vrf10
[Sysname-GigabitEthernet1/0/1] quit
```

在接口 GigabitEthernet1/0/1 上配置 NAT 内部服务器，指定一个外部地址 202.110.10.10，从端口 1001～1100 分别映射 VPN vrf10 内主机 10.110.10.1～10.110.10.100 的 telnet 服务。202.110.10.10:1001 访问 10.110.10.1，202.110.10:1002 访问 10.110.10.2，依此类推。

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat server protocol tcp global 202.110.10.10 1001 1100 inside 10.110.10.1 10.110.10.100 telnet vpn-instance vrf10
```

正确的服务器地址为 10.0.0.172，用户配置的错误地址为 192.168.0.0/24 网段的地址，在接口 GigabitEthernet1/0/1 上配置基于 ACL 的内部服务器对这部分用户的配置错误进行纠正。

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 5 permit ip destination 192.168.0.0 0.0.0.255
```

```
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat server global 3000 inside 10.0.0.172
```

【相关命令】

- **display nat all**
- **display nat server**
- **nat server-group**

1.1.50 nat server rule move

nat server rule move 命令用来调整基于 ACL 内部服务器 NAT 规则的匹配优先级。

【命令】

nat server rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

nat-rule-name1：要移动的 NAT 规则的名称。

after：将 *nat-rule-name1* 移动到 *nat-rule-name2* 后面，*nat-rule-name2* 的匹配优先级的值不变，*nat-rule-name1* 的匹配优先级的值=*nat-rule-name2* 的匹配优先级的值＋1。

before：将 *nat-rule-name1* 移动到 *nat-rule-name2* 前面，*nat-rule-name2* 的匹配优先级的值不变，*nat-rule-name1* 的匹配优先级的值=*nat-rule-name2* 的匹配优先级的值－1。

nat-rule-name2：要移动的 NAT 规则的名称。

【使用指导】

本命令仅对指定了 NAT 规则名称的基于 ACL 内部服务器 NAT 生效。

对于被移动到前面的 NAT 规则，设备将会优先进行匹配。

【举例】

将基于 ACL 内部服务器 NAT 规则 abc 移动到基于 ACL 内部服务器 NAT 规则 def 的前面。

```
<Sysname> nat server rule move abc before def
```

【相关命令】

- **nat server**

1.1.51 nat server-group

nat server-group 命令用来创建内部服务器组，并进入内部服务器组视图。如果指定的内部服务器组已经存在，则直接进入内部服务器组视图。

undo nat server-group 命令用来删除指定的内部服务器组。

【命令】

nat server-group *group-id*

undo nat server-group *group-id*

【缺省情况】

不存在内部服务器组。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

group-id：服务器组编号，取值范围为 0～65535。

【使用指导】

一个内部服务器组中可以包括多个内部服务器组成员（通过 **inside ip** 命令配置）。

【举例】

配置一个内部服务器组，编号为 1。

```
<Sysname> system-view
[Sysname] nat server-group 1
```

【相关命令】

- **display nat all**
- **display nat server-group**
- **inside ip**
- **nat server**

1.1.52 nat session create-rate enable

nat session create-rate enable 命令用来开启 NAT 会话新建速率的统计功能。

undo nat session create-rate enable 命令用来关闭 NAT 会话新建速率的统计功能。

【命令】

nat session create-rate enable

undo nat session create-rate enable

【缺省情况】

NAT 会话新建速率的统计功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

开启 NAT 会话新建速率的统计功能后，设备会对 NAT 会话的新建速率进行统计，统计信息可以通过 **display nat statistics** 命令查看。

【举例】

开启 NAT 会话新建速率的统计功能。

```
<Sysname> system-view
[Sysname] nat session create-rate enable
```

【相关命令】

- **display nat statistics**

1.1.53 nat static enable

nat static enable 命令用来开启接口上的 NAT 静态地址转换功能。

undo nat static enable 命令用来关闭接口上的 NAT 静态地址转换功能。

【命令】

nat static enable

undo nat static enable

【缺省情况】

NAT 静态地址转换功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

接口下开启 NAT 静态地址转换功能后，所有已配置的静态地址转换映射都会在该接口上生效。

【举例】

配置内网 IP 地址 192.168.1.1 到外网 IP 地址 2.2.2.2 的出方向一对一静态地址转换，并且在接口 GigabitEthernet1/0/1 上开启静态地址转换功能。

```
<Sysname> system-view
[Sysname] nat static outbound 192.168.1.1 2.2.2.2
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat static enable
```

【相关命令】

- **display nat all**
- **display nat static**
- **nat static**

- **nat static net-to-net**

1.1.54 nat static inbound

nat static inbound 命令用来配置入方向一对一静态地址转换映射。

undo nat static inbound 命令用来删除指定的入方向一对一静态地址转换映射。

【命令】

nat static inbound *global-ip* [**vpn-instance** *global-vpn-instance-name*] *local-ip* [**vpn-instance** *local-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**]

undo nat static inbound *global-ip* [**vpn-instance** *global-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }]

【缺省情况】

不存在地址转换映射。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

global-ip：外网 IP 地址。

vpn-instance *global-vpn-instance-name*：外网 IP 地址所属的 VPN。*global-vpn-instance-name* 表示 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示外网 IP 地址不属于任何一个 VPN。

local-ip：内网 IP 地址。

vpn-instance *local-vpn-instance-name*：内网 IP 地址所属的 VPN。*local-vpn-instance-name* 表示 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示内网 IP 地址不属于任何一个 VPN。

acl：指定 ACL 的编号或名称，本参数用于控制指定访问范围的报文可以使用 NAT 规则进行地址转换。

ipv4-acl-number：ACL 的编号，取值范围为 3000～3999。

name *ipv4-acl-name*：ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 all。

reversible：表示从内网主动访问外网的报文必须通过 ACL 反向匹配，才能使用该配置进行目的地址转换。

rule *rule-name*：NAT 规则的名称，取值范围为 1～63 个字符的字符串，不区分大小写，不能包括“\\”、“/”、“:”、“*”、“?”、“\”、“<”、“>”、“|”、“”” 和 “@”。如果不指定该参数，则表示该规则无名称。

priority *priority*：NAT 规则的匹配优先级，取值范围为 0～2147483647，数值越小，优先级越高。如果不指定该参数，那么相应的 NAT 规则在同类 NAT 规则中，其匹配优先级最低。

disable：表示禁用该地址转换映射。如果不指定该参数，则地址转换映射处于启用状态。

【使用指导】

对于从外网到内网的报文，将其源地址 *global-ip* 转换为 *local-ip*；对于从内网到外网的报文，将其目的地址 *local-ip* 转换为 *global-ip*。

指定引用的 ACL 时，需要注意：

- 如果没有指定 ACL，则所有从外网到内网的报文都可以使用该配置进行源地址转换；所有从内网到外网的报文都可以使用该配置进行目的地址转换。
- 如果仅指定了 ACL，没有指定 ACL 反向匹配（即没有配置 **reversible**），对于从外网到内网的报文，只有报文符合 ACL permit 规则，才能使用该配置进行源地址转换；对于从内网主动访问外网的报文，不能使用该配置进行目的地址转换。
- 如果既指定了 ACL，又指定了 ACL 反向匹配（即配置了 **reversible**），对于外网到内网的报文，只有报文符合 ACL permit 规则，才能使用该配置进行源地址转换；对于从内网主动访问外网的报文，需要进行 ACL 反向匹配（提取报文的源地址/端口和目的地址/端口，并根据配置转换目的地址，然后将源地址/端口和目的地址/端口互换去匹配 ACL），只有反向匹配 ACL 的报文才能使用该配置进行转换，否则不予转换。

如果接口下既配置了 NAT 动态地址转换，又配置了 NAT 静态地址转换，则优先使用静态地址转换。

设备可支持配置多条入方向静态地址转换映射（包括 **nat static inbound** 和 **nat static inbound net-to-net**）。

在 VPN 组网中，配置入方向静态地址转换时需要指定 **vpn-instance** 参数，且 VPN 实例的名称必须与该接口关联的 VPN 实例一致。

对于引用了 ACL 的入方向一对一静态地址转换映射，当 NAT 规则的匹配优先级相同时，设备将按照 ACL 名称或 ACL 编号进行匹配，且 ACL 名称的优先级高于 ACL 编号的优先级，具体规则如下：

- 对于 ACL 名称，设备将根据名称的字符序对 NAT 规则进行排序，在字符序中的位置越靠前，相应的 NAT 规则的匹配优先级越高。
- 对于 ACL 编号，编号越大，优先级越高，设备将优先进行匹配。

【举例】

配置外网 IP 地址 2.2.2.2 到内网 IP 地址 192.168.1.1 的入方向静态地址转换。

```
<Sysname> system-view
[Sysname] nat static inbound 2.2.2.2 192.168.1.1
```

【相关命令】

- **display nat all**
- **display nat static**
- **nat static enable**

1.1.55 nat static inbound net-to-net

nat static inbound net-to-net 命令用来配置入方向网段到网段的静态地址转换映射。

undo nat static inbound net-to-net 命令用来删除指定的入方向网段到网段的静态地址转换映射。

【命令】

nat static inbound net-to-net *global-start-address global-end-address* [**vpn-instance** *global-vpn-instance-name*] **local** *local-network* { *mask-length* | *mask* } [**vpn-instance** *local-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**]

undo nat static inbound net-to-net *global-start-address global-end-address* [**vpn-instance** *global-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }]

【缺省情况】

不存在地址转换映射。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

global-start-address global-end-address：外网地址范围，所包含的地址数目不能超过 255。*global-start-address* 表示起始地址，*global-end-address* 表示结束地址。*global-end-address* 必须大于或等于 *global-start-address*，如果二者相同，则表示只有一个地址。

vpn-instance *global-vpn-instance-name*：外网 IP 地址所属的 VPN。*global-vpn-instance-name* 表示 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示外网 IP 地址不属于任何一个 VPN。

local-network：内网网段地址。

mask-length：内网网络地址的掩码长度，取值范围为 8～31。

mask：内网网络地址掩码。

vpn-instance *local-vpn-instance-name*：内网 IP 地址所属的 VPN。*local-vpn-instance-name* 表示 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示内网 IP 地址不属于任何一个 VPN。

acl：指定 ACL 的编号或名称，本参数用于控制指定访问范围的报文可以使用 NAT 规则进行地址转换。

ipv4-acl-number：ACL 的编号，取值范围为 3000～3999。

name *ipv4-acl-name*：ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 all。

reversible：表示从内网主动访问外网的报文必须通过 ACL 反向匹配，才能使用该配置进行目的地址转换。

rule *rule-name*：NAT 规则的名称，取值范围为 1～63 个字符的字符串，不区分大小写，不能包括“\”、“/”、“:”、“*”、“?”、“<”、“>”、“|”、“”” 和 “@”。如果不指定该参数，则表示该规则无名称。

priority *priority*：NAT 规则的匹配优先级，取值范围为 0～2147483647，数值越小，优先级越高。如果不指定该参数，那么相应的 NAT 规则在同类 NAT 规则中，其匹配优先级最低。

disable：表示禁用该地址转换映射。如果不指定该参数，则地址转换映射处于启用状态。

【使用指导】

外网网段通过起始地址和结束地址来指定，内网网段通过内网地址和掩码来指定。

对于从外网到内网的报文，使用其源地址匹配外网地址，将源地址转换为内网地址；对于从内网到外网的报文，使用其目的地址匹配内网地址，将目的地址转换为外网地址。

外网结束地址不能大于外网起始地址和内网掩码所决定的网段中的最大 IP 地址。比如：内网地址配置为 2.2.2.0，掩码为 255.255.255.0，外网起始地址为 1.1.1.100，则外网结束地址不应该大于 1.1.1.0/24 网段中可用的最大 IP 地址，即 1.1.1.255。

指定引用的 ACL 时，需要注意：

- 如果没有指定 ACL，则所有从外网到内网的报文都可以使用该配置进行源地址转换；所有从内网到外网的报文都可以使用该配置进行目的地址转换。
- 如果仅指定了 ACL，没有指定 ACL 反向匹配（即没有配置 **reversible**），对于从外网到内网的报文，只有报文符合 ACL permit 规则，才能使用该配置进行源地址转换；对于从内网到外网的报文，不能使用该配置进行目的地址转换。
- 如果既指定了 ACL，又指定了 ACL 反向匹配（即配置了 **reversible**），对于外网到内网的报文，只有报文符合 ACL permit 规则，才能使用该配置进行源地址转换；对于从内网到外网的报文，需要进行 ACL 反向匹配（提取报文的源地址/端口和目的地址/端口，并根据配置转换目的地址，然后将源地址/端口和目的地址/端口互换去匹配 ACL），只有反向匹配 ACL 的报文才能使用该配置进行转换，否则不予转换。

如果接口下既配置了 NAT 动态地址转换，又配置了 NAT 静态地址转换，则优先使用静态地址转换。

设备支持配置多条入方向静态地址转换映射（包括 **nat static inbound** 和 **nat static inbound net-to-net**）。

在 VPN 组网中，配置入方向静态地址转换时需要指定 **vpn-instance** 参数，且 VPN 实例的名称必须与该接口关联的 VPN 实例一致。

对于引用了 ACL 的入方向网段到网段的静态地址转换映射，当 NAT 规则的匹配优先级相同时，设备将按照 ACL 名称或 ACL 编号进行匹配，且 ACL 名称的优先级高于 ACL 编号的优先级，具体规则如下：

- 对于 ACL 名称，设备将根据名称的字符序对 NAT 规则进行排序，在字符序中的位置越靠前，相应的 NAT 规则的匹配优先级越高。
- 对于 ACL 编号，编号越大，优先级越高，设备将优先进行匹配。

【举例】

配置外网网段 202.100.1.0/24 到内网网段 192.168.1.0/24 的入方向静态地址转换。

```
<Sysname> system-view
[Sysname] nat static inbound net-to-net 202.100.1.1 202.100.1.255 local 192.168.1.0 24
```

【相关命令】

- **display nat all**
- **display nat static**
- **nat static enable**

1.1.56 nat static inbound object-group

nat static inbound object-group 命令用来配置基于对象组的入方向静态地址转换映射。

undo nat static inbound object-group 命令用来删除指定的基于对象组的入方向静态地址转换映射。

【命令】

nat static inbound object-group *global-object-group-name* [**vpn-instance** *global-vpn-instance-name*] **object-group** *local-object-group-name* [**vpn-instance** *local-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**disable**]

undo nat static inbound object-group *global-object-group-name* [**vpn-instance** *global-vpn-instance-name*]

【缺省情况】

不存在地址转换映射。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

object-group *global-object-group-name*：外网 IPv4 地址对象组。*global-object-group-name* 表示 IPv4 地址对象组的名称，为 1～31 个字符的字符串，不区分大小写。

vpn-instance *global-vpn-instance-name*：外网 IP 地址所属的 VPN。*global-vpn-instance-name* 表示 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示外网 IP 地址不属于任何一个 VPN。

object-group *local-object-group-name*：内网 IPv4 地址对象组。*local-object-group-name* 表示 IPv4 地址对象组的名称，为 1～31 个字符的字符串，不区分大小写。

vpn-instance *local-vpn-instance-name*：内网 IP 地址所属的 VPN。*local-vpn-instance-name* 表示 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示内网 IP 地址不属于任何一个 VPN。

acl：指定 ACL 的编号或名称，本参数用于控制指定访问范围的报文可以使用 NAT 规则进行地址转换。

ipv4-acl-number：ACL 的编号，取值范围为 3000～3999。

name *ipv4-acl-name*：ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 all。

reversible：表示从内网主动访问外网的报文必须通过 ACL 反向匹配，才能使用该配置进行目的地址转换。

disable：表示禁用该地址转换映射。如果不指定该参数，则地址转换映射处于启用状态。

【使用指导】

外网地址通过外网 IPv4 地址对象组来指定，内网地址通过内网 IPv4 地址对象组来指定。

对于从外网到内网的报文，使用其源地址匹配外网地址，将源地址转换为内网地址；对于从内网到外网的报文，使用其目的地址匹配内网地址，将目的地址转换为外网地址。

指定引用的 object-group 时，需要注意：

- 内网 IPv4 地址对象组和外网 IPv4 地址对象组内只能存在一个 IPv4 地址对象。
- 内网 IPv4 地址对象组内地址数应不小于外网 IPv4 地址对象组。
- 内网 IPv4 地址对象组的地址对象不能是地址范围。

指定引用的 ACL 时，需要注意：

- 如果没有指定 ACL，则所有从外网到内网的报文都可以使用该配置进行源地址转换；所有从内网到外网的报文都可以使用该配置进行目的地址转换。
- 如果仅指定了 ACL，没有指定 ACL 反向匹配（即没有配置 **reversible**），对于从外网到内网的报文，只有报文符合 ACL permit 规则，才能使用该配置进行源地址转换；对于从内网主动访问外网的报文，不能使用该配置进行目的地址转换。
- 如果既指定了 ACL，又指定了 ACL 反向匹配（即配置了 **reversible**），对于外网到内网的报文，只有报文符合 ACL permit 规则，才能使用该配置进行源地址转换；对于从内网主动访问外网的报文，需要进行 ACL 反向匹配（提取报文的源地址/端口和目的地址/端口，并根据配置转换目的地址，然后将源地址/端口和目的地址/端口互换去匹配 ACL），只有反向匹配 ACL 的报文才能使用该配置进行转换，否则不予转换。

如果接口下既配置了 NAT 动态地址转换，又配置了 NAT 静态地址转换，则优先使用静态地址转换。

设备可支持配置多条入方向静态地址转换映射（包括 **nat static inbound**、**nat static inbound net-to-net** 和 **nat static inbound object-group**）。

在 VPN 组网中，配置入方向静态地址转换时需要指定 **vpn-instance** 参数，且 VPN 实例的名称必须与该接口关联的 VPN 实例一致。

基于地址对象组的入方向静态地址转换引用的 IPv4 地址对象组中，只能存在一个主机对象（**host**）或者一个子网对象（**subnet**），否则引用不生效。

【举例】

配置外网 IP 地址 2.2.2.2 到内网 IP 地址 192.168.1.1 基于对象组的入方向静态地址转换。

```
<Sysname> system-view
[Sysname] object-group ip address global
[Sysname-obj-grp-ip-global] network host address 2.2.2.2
[Sysname-obj-grp-ip-global] quit
[Sysname] object-group ip address local
[Sysname-obj-grp-ip-local] network host address 192.168.1.1
[Sysname-obj-grp-ip-local] quit
[Sysname] nat static inbound object-group global object-group local
```

【相关命令】

- **display nat all**
- **display nat static**
- **nat static enable**

1.1.57 nat static inbound rule move

nat static inbound rule move 命令用来调整入方向一对一静态 NAT 规则的匹配优先级。

【命令】

nat static inbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

nat-rule-name1：要移动的 NAT 规则的名称。

after：将 *nat-rule-name1* 移动到 *nat-rule-name2* 后面，*nat-rule-name2* 的匹配优先级的值不变，*nat-rule-name1* 的匹配优先级的值=*nat-rule-name2* 的匹配优先级的值＋1。

before：将 *nat-rule-name1* 移动到 *nat-rule-name2* 前面，*nat-rule-name2* 的匹配优先级的值不变，*nat-rule-name1* 的匹配优先级的值=*nat-rule-name2* 的匹配优先级的值－1。

nat-rule-name2：要移动的 NAT 规则的名称。

【使用指导】

本命令仅对指定了 NAT 规则名称的入方向一对一静态 NAT 生效。

对于被移动到前面的 NAT 规则，设备将会优先进行匹配。

【举例】

将入方向一对一静态 NAT 规则 abc 移动到入方向一对一静态 NAT 规则 def 的前面。

```
<Sysname> nat static inbound rule move abc before def
```

【相关命令】

- **nat static inbound**

1.1.58 nat static outbound

nat static outbound 命令用来配置出方向一对一静态地址转换映射。

undo nat static outbound 命令用来删除出方向一对一静态地址转换映射。

【命令】

nat static outbound *local-ip* [**vpn-instance** *local-vpn-instance-name*] *global-ip* [**vpn-instance** *global-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**]

undo nat static outbound *local-ip* [**vpn-instance** *local-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }]

【缺省情况】

不存在任何地址转换映射。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

local-ip：内网 IP 地址。

vpn-instance *local-vpn-instance-name*：内网 IP 地址所属的 VPN。*local-vpn-instance-name* 表示 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示内网 IP 地址不属于任何一个 VPN。

global-ip：外网 IP 地址。

vpn-instance *global-vpn-instance-name*：外网 IP 地址所属的 VPN。*global-vpn-instance-name* 表示 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示外网 IP 地址不属于任何一个 VPN。

acl：指定 ACL 的编号或名称，本参数用于控制指定访问范围的报文可以使用 NAT 规则进行地址转换。

ipv4-acl-number：ACL 的编号，取值范围为 3000～3999。

name *ipv4-acl-name*：ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 all。

reversible：表示从外网主动访问内网的报文必须通过 ACL 反向匹配，才能使用该配置进行目的地址转换。

rule *rule-name*：NAT 规则的名称，取值范围为 1～63 个字符的字符串，不区分大小写，不能包括“\”、“/”、“:”、“*”、“?”、“<”、“>”、“|”、“”” 和 “@”。如果不指定该参数，则表示该规则无名称。

priority *priority*：NAT 规则的匹配优先级，取值范围为 0～2147483647，数值越小，优先级越高。如果不指定该参数，那么相应的 NAT 规则在同类 NAT 规则中，其匹配优先级最低。

disable：表示禁用该地址转换映射。如果不指定该参数，则地址转换映射处于启用状态。

【使用指导】

对于从内网到外网的报文，将其源地址 *local-ip* 转换为 *global-ip*；对于从外网到内网的报文，将其目的地址 *global-ip* 转换为 *local-ip*。

指定引用的 ACL 时，需要注意：

- 如果没有指定 ACL，则所有从内网到外网的报文都可以使用该配置进行源地址转换；所有从外网到内网的报文都可以使用该配置进行目的地址转换。
- 如果仅指定了 ACL，没有指定 ACL 反向匹配（即没有配置 **reversible**），对于从内网到外网的报文，只有报文符合 ACL permit 规则，才能使用该配置进行源地址转换；对于从外网主动访问内网的报文，不能使用该配置进行目的地址转换。
- 如果既指定了 ACL，又指定了 ACL 反向匹配（即配置了 **reversible**），对于从内网到外网的报文，只有报文符合 ACL permit 规则，才能使用该配置进行源地址转换；对于从外网主动访问内网的报文，需要进行 ACL 反向匹配（提取报文的源地址/端口和目的地址/端口，并根据配

置转换目的地址，然后将源地址/端口和目的地址/端口互换去匹配 ACL），只有反向匹配 ACL 的报文才能使用该配置进行转换，否则不予转换。

如果接口下既配置了 NAT 动态地址转换，又配置了 NAT 静态地址转换，则优先使用静态地址转换。

设备可支持配置多条出方向静态地址转换映射（包括 **nat static outbound** 和 **nat static outbound net-to-net**）。

在 VPN 组网中，配置出方向静态地址转换时需要指定 **vpn-instance** 参数，且 VPN 实例的名称必须与该接口关联的 VPN 实例一致。

对于引用了 ACL 的出方向一对一静态地址转换映射，当 NAT 规则的匹配优先级相同时，设备将按照 ACL 名称或 ACL 编号进行匹配，且 ACL 名称的优先级高于 ACL 编号的优先级，具体规则如下：

- 对于 ACL 名称，设备将根据名称的字符序对 NAT 规则进行排序，在字符序中的位置越靠前，相应的 NAT 规则的匹配优先级越高。
- 对于 ACL 编号，编号越大，优先级越高，设备将优先进行匹配。

【举例】

配置内网 IP 地址 192.168.1.1 到外网 IP 地址 2.2.2.2 的出方向静态地址转换映射。

```
<Sysname> system-view
[Sysname] nat static outbound 192.168.1.1 2.2.2.2
```

配置出方向静态地址转换映射，允许内网用户 192.168.1.1 访问外网网段 3.3.3.0/24 时，使用外网 IP 地址 2.2.2.2。

```
<Sysname> system-view
[Sysname] acl advanced 3001
[Sysname-acl-ipv4-adv-3001] rule permit ip destination 3.3.3.0 0.0.0.255
[Sysname-acl-ipv4-adv-3001] quit
[Sysname] nat static outbound 192.168.1.1 2.2.2.2 acl 3001
```

【相关命令】

- **display nat all**
- **display nat static**
- **nat static enable**

1.1.59 nat static outbound net-to-net

nat static outbound net-to-net 命令用来配置出方向网段到网段的静态地址转换映射。

undo nat static outbound net-to-net 命令用来删除出方向网段到网段的静态地址转换映射。

【命令】

nat static outbound net-to-net *local-start-address local-end-address* [**vpn-instance** *local-vpn-instance-name*] **global** *global-network* { *mask-length* | *mask* } [**vpn-instance** *global-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**]

undo nat static outbound net-to-net *local-start-address local-end-address* [**vpn-instance** *local-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }

【缺省情况】

不存在任何地址转换映射。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

local-start-address *local-end-address*：内网地址范围，所包含的地址数目不能超过 255。*local-start-address* 表示起始地址，*local-end-address* 表示结束地址。*local-end-address* 必须大于或等于 *local-start-address*，如果二者相同，则表示只有一个地址。

vpn-instance *local-vpn-instance-name*：内网 IP 地址所属的 VPN。*local-vpn-instance-name* 表示 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示内网 IP 地址不属于任何一个 VPN。

global-network：外网网段地址。

mask-length：外网网络地址的掩码长度，取值范围为 8～31。

mask：外网网络地址掩码。

vpn-instance *global-vpn-instance-name*：外网 IP 地址所属的 VPN。*global-vpn-instance-name* 表示 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示外网 IP 地址不属于任何一个 VPN。

acl：指定 ACL 的编号或名称，本参数用于控制指定访问范围的报文可以使用 NAT 规则进行地址转换。

ipv4-acl-number：ACL 的编号，取值范围为 3000～3999。

name *ipv4-acl-name*：ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 all。

reversible：表示从外网主动访问内网的报文必须通过 ACL 反向匹配，才能使用该配置进行目的地址转换。

rule *rule-name*：NAT 规则的名称，取值范围为 1～63 个字符的字符串，不区分大小写，不能包括“\”、“/”、“:”、“*”、“?”、“<”、“>”、“|”、“”” 和 “@”。如果不指定该参数，则表示该规则无名称。

priority *priority*：NAT 规则的匹配优先级，取值范围为 0～2147483647，数值越小，优先级越高。如果不指定该参数，那么相应的 NAT 规则在同类 NAT 规则中，其匹配优先级最低。

disable：表示禁用该地址转换映射。如果不指定该参数，则地址转换映射处于启用状态。

【使用指导】

内网网段通过起始地址和结束地址来指定，外网网段通过外网地址和掩码来指定。

对于从内网到外网的报文，使用其源地址匹配内网地址，将源地址转换为外网地址；对于从外网到内网的报文，使用其目的地址匹配外网地址，将目的地址转换为内网地址。

内网结束地址不能大于内网起始地址和外网掩码所决定的网段中的最大 IP 地址。比如：外网地址配置为 2.2.2.0，掩码为 255.255.255.0，内网起始地址为 1.1.1.100，则内网结束地址不应该大于 1.1.1.0/24 网段中可用的最大 IP 地址，即 1.1.1.255。

指定引用的 ACL 时，需要注意：

- 如果没有指定 ACL，则所有从内网到外网的报文都可以使用该配置进行源地址转换；所有从外网到内网的报文都可以使用该配置进行目的地址转换。
- 如果仅指定了 ACL，没有指定 ACL 反向匹配（即没有配置 **reversible**），对于从内网到外网的报文，只有报文符合 ACL permit 规则，才能使用该配置进行源地址转换；对于从外网主动访问内网的报文，不能使用该配置进行目的地址转换。
- 如果既指定了 ACL，又指定了 ACL 反向匹配（即配置了 **reversible**），对于从内网到外网的报文，只有报文符合 ACL permit 规则，才能使用该配置进行源地址转换；对于从外网主动访问内网的报文，需要进行 ACL 反向匹配（提取报文的源地址/端口和目的地址/端口，并根据配置转换目的地址，然后将源地址/端口和目的地址/端口互换去匹配 ACL），只有反向匹配 ACL 的报文才能使用该配置进行转换，否则不予转换。

如果接口下既配置了 NAT 动态地址转换，又配置了 NAT 静态地址转换，则优先使用静态地址转换。

设备可支持配置多条出方向静态地址转换映射（包括 **nat static outbound** 和 **nat static outbound net-to-net**）。

在 VPN 组网中，配置出方向静态地址转换时需要指定 **vpn-instance** 参数，且 VPN 实例的名称必须与该接口关联的 VPN 实例一致。

对于引用了 ACL 的出方向网段到网段的静态地址转换映射，当 NAT 规则的匹配优先级相同时，设备将按照 ACL 名称或 ACL 编号进行匹配，且 ACL 名称的优先级高于 ACL 编号的优先级，具体规则如下：

- 对于 ACL 名称，设备将根据名称的字符序对 NAT 规则进行排序，在字符序中的位置越靠前，相应的 NAT 规则的匹配优先级越高。
- 对于 ACL 编号，编号越大，优先级越高，设备将优先进行匹配。

【举例】

配置内网网段 192.168.1.0/24 到外网网段 2.2.2.0/24 的出方向静态地址转换映射。

```
<Sysname> system-view
[Sysname] nat static outbound net-to-net 192.168.1.1 192.168.1.255 global 2.2.2.0 24
```

配置出方向网段到网段的静态地址转换映射，允许内网 192.168.1.0/24 网段的用户访问外网网段 3.3.3.0/24 时，使用外网网段 2.2.2.0/24 中的地址。

```
<Sysname> system-view
[Sysname] acl advanced 3001
[Sysname-acl-ipv4-adv-3001] rule permit ip destination 3.3.3.0 0.0.0.255
[Sysname-acl-ipv4-adv-3001] quit
[Sysname] nat static outbound net-to-net 192.168.1.1 192.168.1.255 global 2.2.2.0 24 acl 3001
```

【相关命令】

- **display nat all**
- **display nat static**
- **nat static enable**

1.1.60 nat static outbound object-group

nat static outbound object-group 命令用来配置基于对象组的出方向静态地址转换映射。

undo nat static outbound object-group 命令用来删除指定基于对象组的出方向静态地址转换映射。

【命令】

nat static outbound object-group *local-object-group-name* [**vpn-instance** *local-vpn-instance-name*] **object-group** *global-object-group-name* [**vpn-instance** *global-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**disable**]

undo nat static outbound object-group *local-object-group-name* [**vpn-instance** *local-vpn-instance-name*]

【缺省情况】

不存在地址转换映射。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

object-group *local-object-group-name*：内网 IPv4 地址对象组。*local-object-group-name* 表示 IPv4 地址对象组的名称，为 1～31 个字符的字符串，不区分大小写。

vpn-instance *local-vpn-instance-name*：内网 IP 地址所属的 VPN。*local-vpn-instance-name* 表示 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示内网 IP 地址不属于任何一个 VPN。

object-group *global-object-group-name*：外网 IPv4 地址对象组。*global-object-group-name* 表示 IPv4 地址对象组的名称，为 1～31 个字符的字符串，不区分大小写。

vpn-instance *global-vpn-instance-name*：外网 IP 地址所属的 VPN。*global-vpn-instance-name* 表示 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示外网 IP 地址不属于任何一个 VPN。

acl：指定 ACL 的编号或名称，本参数用于控制指定访问范围的报文可以使用 NAT 规则进行地址转换。

ipv4-acl-number：ACL 的编号，取值范围为 3000～3999。

name *ipv4-acl-name*：ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 all。

reversible：表示从外网主动访问内网的报文必须通过 ACL 反向匹配，才能使用该配置进行目的地址转换。

disable：表示禁用该地址转换映射。如果不指定该参数，则地址转换映射处于启用状态。

【使用指导】

内网地址通过内网 IPv4 地址对象组来指定，外网地址通过外网 IPv4 地址对象组来指定。

对于从内网到外网的报文，使用其源地址匹配内网地址，将源地址转换为外网地址；对于从外网到内网的报文，使用其目的地址匹配外网地址，将目的地址转换为内网地址。

指定引用的 object-group 时，需要注意：

- 内网 IPv4 地址对象组和外网 IPv4 地址对象组内只能存在一个 IPv4 地址对象。
- 内网 IPv4 地址对象组内地址数应不大于外网 IPv4 地址对象组。
- 外网 IPv4 地址对象组的地址对象不能是地址范围。

指定引用的 ACL 时，需要注意：

- 如果没有指定 ACL，则所有从内网到外网的报文都可以使用该配置进行源地址转换；所有从外网到内网的报文都可以使用该配置进行目的地址转换。
- 如果仅指定了 ACL，没有指定 ACL 反向匹配（即没有配置 **reversible**），对于从内网到外网的报文，只有报文符合 ACL permit 规则，才能使用该配置进行源地址转换；对于从外网主动访问内网的报文，不能使用该配置进行目的地址转换。
- 如果既指定了 ACL，又指定了 ACL 反向匹配（即配置了 **reversible**），对于从内网到外网的报文，只有报文符合 ACL permit 规则，才能使用该配置进行源地址转换；对于从外网主动访问内网的报文，需要进行 ACL 反向匹配（提取报文的源地址/端口和目的地址/端口，并根据配置转换目的地址，然后将源地址/端口和目的地址/端口互换去匹配 ACL），只有反向匹配 ACL 的报文才能使用该配置进行转换，否则不予转换。

如果接口下既配置了 NAT 动态地址转换，又配置了 NAT 静态地址转换，则优先使用静态地址转换。

设备可支持配置多条出方向静态地址转换映射（包括 **nat static outbound**、**nat static outbound net-to-net** 和 **nat static outbound object-group**）。

在 VPN 组网中，配置出方向静态地址转换时需要指定 **vpn-instance** 参数，且 VPN 实例的名称必须与该接口关联的 VPN 实例一致。

基于地址对象组的出方向静态地址转换引用的 IPv4 地址对象组中，只能存在一个主机对象（**host**）或者一个子网对象（**subnet**），否则引用不生效。

【举例】

配置基于对象组的出方向静态地址转换映射，允许内网用户 192.168.1.1 访问外网网段 3.3.3.0/24 时，使用外网 IP 地址 2.2.2.2。

```
<Sysname> system-view
[Sysname] object-group ip address global
[Sysname-obj-grp-ip-global] network host address 2.2.2.2
[Sysname-obj-grp-ip-global] quit
[Sysname] object-group ip address local
[Sysname-obj-grp-ip-local] network host address 192.168.1.1
[Sysname-obj-grp-ip-local] quit
[Sysname] nat static outbound object-group local object-group global
```

【相关命令】

- **display nat all**
- **display nat static**

1.1.61 nat static outbound rule move

nat static outbound rule move 命令用来调整出方向一对一静态 NAT 规则的匹配优先级。

【命令】

nat static outbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

nat-rule-name1：要移动的 NAT 规则的名称。

after：将 *nat-rule-name1* 移动到 *nat-rule-name2* 后面，*nat-rule-name2* 的匹配优先级的值不变，*nat-rule-name1* 的匹配优先级的值=*nat-rule-name2* 的匹配优先级的值＋1。

before：将 *nat-rule-name1* 移动到 *nat-rule-name2* 前面，*nat-rule-name2* 的匹配优先级的值不变，*nat-rule-name1* 的匹配优先级的值=*nat-rule-name2* 的匹配优先级的值－1。

nat-rule-name2：要移动的 NAT 规则的名称。

【使用指导】

本命令仅对指定了 NAT 规则名称的出方向一对一静态 NAT 生效。

对于被移动到前面的 NAT 规则，设备将会优先进行匹配。

【举例】

将出方向一对一静态 NAT 规则 abc 移动到出方向一对一 NAT 规则 def 的前面。

```
<Sysname> nat static outbound rule move abc before def
```

【相关命令】

- **nat static outbound**

1.1.62 nat timestamp delete

nat timestamp delete 命令用来开启对 TCP SYN 和 SYN ACK 报文中时间戳的删除功能。

undo nat timestamp delete 命令用来恢复缺省情况。

【命令】

nat timestamp delete [**vpn-instance** *vpn-instance-name*]

undo nat timestamp delete [**vpn-instance** *vpn-instance-name*]

【缺省情况】

不对 TCP SYN 和 SYN ACK 报文中的时间戳进行删除处理。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

vpn-instance *vpn-instance-name*：表示 TCP SYN 和 SYN ACK 报文所属的 VPN。*vpn-instance-name* 表示 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。若未指定本参数，则表示 TCP SYN 和 SYN ACK 报文属于公网。

【使用指导】

开启本功能后，未指定 VPN 参数时，系统会把动态地址转换后的公网上 TCP SYN 和 SYN ACK 报文中的时间戳删除；指定 VPN 参数时，系统会把动态地址转换后的指定 VPN 中 TCP SYN 和 SYN ACK 报文中的时间戳删除。

在 PAT 方式的动态地址转换（即接口上配置了 **nat inbound** 或 **nat outbound** 命令）组网环境中，若服务器上同时开启了 tcp_timestams 和 tcp_tw_recycle 功能，则 Client 与 Server 之间可能会出现无法建立 TCP 连接的现象。

为了解决以上问题，可在服务器上关闭 tcp_tw_recycle 功能或在设备上开启对 TCP SYN 和 SYN ACK 报文中时间戳的删除功能。

多次执行本命令，可为不同 VPN 中的报文开启此功能。

【举例】

开启对公网上 TCP SYN 和 SYN ACK 报文中时间戳的删除功能。

```
<Sysname> system-view
[Sysname] nat timestamp delete
```

开启对名称为 aa 的 VPN 中 TCP SYN 和 SYN ACK 报文中时间戳的删除功能。

```
<Sysname> system-view
[Sysname] nat timestamp delete vpn-instance aa
```

【相关命令】

- **nat outbound**
- **nat inbound**

1.1.63 port-block

port-block 命令用来配置 NAT 地址组的端口块参数。

undo port-block 命令用来恢复缺省情况。

【命令】

port-block block-size *block-size* [**extended-block-number** *extended-block-number*]

undo port-block

【缺省情况】

未配置 NAT 地址组的端口块参数。

【视图】

NAT 地址组视图

【缺省用户角色】

network-admin

context-admin

【参数】

block-size *block-size*：端口块大小，即一个端口块中所包含的端口数，取值范围为 1～65535。同一 NAT 地址组内，该参数的值不能超过 **port-range** 参数的值。

extended-block-number *extended-block-number*：增量端口块数，取值范围为 1～5。当分配端口块中的端口资源耗尽（所有端口都被使用）时，如果对应的私网 IP 地址向公网发起新的连接，则无法从分配端口块中获取端口。此时，如果分配端口块的公网 IP 地址所属的 NAT 地址组中配置了增量端口块数，则可以为对应的私网 IP 地址进行增量端口块分配。一个私网 IP 地址最多可同时占有 1＋*extended-block-number* 个端口块。

【使用指导】

端口块动态映射方式下，配置出方向地址转换所引用的 NAT 地址组中必须配置端口块参数。当某私网 IP 地址首次向公网发起连接时，从所匹配的 NAT 地址组中获取一个公网 IP 地址，从获取的公网 IP 地址中分配一个动态端口块并创建动态端口块表项（该私网 IP 地址后续向公网发起连接时，通过私网 IP 地址查找动态端口块表项），使用公网 IP 地址进行 IP 地址转换，并从端口块中动态分配一个端口进行 TCP/UDP 端口转换。

【举例】

配置 NAT 地址组 2 的端口块参数，端口块大小为 256，增量端口块数为 1。

```
<Sysname> system-view
[Sysname] nat address-group 2
[Sysname-address-group-2] port-block block-size 256 extended-block-number 1
```

【相关命令】

- **nat address-group**

1.1.64 port-range

port-range 命令用来配置公网 IP 地址的端口范围。

undo port-range 命令用来恢复缺省情况。

【命令】

port-range *start-port-number end-port-number*

undo port-range

【缺省情况】

公网 IP 地址的端口范围为 1～65535。

【视图】

NAT 地址组视图/NAT 端口块组视图

【缺省用户角色】

network-admin

context-admin

【参数】

start-port-number end-port-number：公网 IP 地址端口的起始端口号和结束端口号。*end-port-number* 必须大于或等于 *start-port-number*。

【使用指导】

在 NAT 地址组（或 NAT 端口块组）视图下配置端口范围后，该 NAT 地址组（或 NAT 端口块组）内的所有公网 IP 地址可用于地址转换的端口都必须位于所指定的端口范围之内。

在 NAT 端口块组内配置端口范围时，端口范围不能小于端口块大小。在 NAT 地址组内配置端口范围时，如果地址组配置了端口块参数，则端口范围也不能小于端口块大小。

【举例】

配置 NAT 地址组 1 的公网 IP 地址端口范围为 1024～65535。

```
<Sysname> system-view
[Sysname] nat address-group 1
[Sysname-address-group-1] port-range 1024 65535
```

配置 NAT 端口块组 1 的公网 IP 地址端口范围为 30001～65535。

```
<Sysname> system-view
[Sysname] nat port-block-group 1
[Sysname-port-block-group-1] port-range 30001 65535
```

【相关命令】

- **nat address-group**
- **nat port-block-group**

1.1.65 reset nat session

reset nat session 命令用来删除 NAT 会话表项。

【命令】

reset nat session [**slot** *slot-number*]

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

slot *slot-number*：删除指定成员设备上的 NAT 会话表项，*slot-number* 表示设备在 IRF 中的成员编号。如果不指定该参数，则表示删除所有成员设备上的 NAT 会话表项。

【使用指导】

NAT 会话表项被删除之后，与其相关的 NAT EIM 表和 NO-PAT 表也会同时删除。

【举例】

删除 2 号成员设备的 NAT 会话表项。

```
<Sysname> reset nat session slot 2
```

【相关命令】

- **display nat session**

目 录

1 AFT 命令

设备各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
F1000-E-G2/F1000-A-G2/F1000-S-G2/F1000-C-G2	AFT	支持
F100-E-G2/F100-A-G2/F100-M-G2/F100-S-G2/F100-C-G2		• F100-E-G2/F100-A-G2：支持 • F100-M-G2/F100-S-G2/F100-C-G2：不支持
F1000-C-EI/F100-E-EI/F100-A-EI/F100-C-EI/F100-A-SI		• F1000-C-EI/F100-E-EI/F100-A-EI/F100-A-SI：支持 • F100-C-EI：不支持
F100-C-HI/F100-S-HI/F100-A-HI/F1000-C-HI		• F100-A-HI/F1000-C-HI：支持 • F100-C-HI/F100-S-HI：不支持
F1000-C8180/F1000-C8170/F1000-C8160/F1000-C8150/F1000-C8130/F1000-C8120		• F1000-C8180/F1000-C8170/F1000-C8160：支持 • F1000-C8150/F1000-C8130/F1000-C8120：不支持
F100-C80-WiNet/F100-C60-WiNet		不支持

1.1 AFT配置命令

1.1.1 address

address 命令用来添加一个地址组成员。

undo address 命令用来删除一个地址组成员。

【命令】

address *start-address end-address*

undo address *start-address end-address*

【缺省情况】

地址组内不存在地址组成员。

【视图】

AFT 地址组视图

【缺省用户角色】

network-admin

context-admin

【参数】

start-address end-address：地址组成员的起始 IP 地址和结束 IP 地址。*end-address* 必须大于或等于 *start-address*，如果 *start-address* 和 *end-address* 相同，则表示只有一个地址。

【使用指导】

一个地址组是多个地址组成员的集合。当需要对从 IPv6 网络到达 IPv4 网络的数据报文进行源地址转换时，IPv6 报文的源地址将被转换为地址组成员中的某个 IPv4 地址。

一个地址组成员所包含的地址数目不能超过 256。

各地址组成员的 IP 地址段不能相互重叠。

【举例】

在地址组 2 下添加两个地址组成员。

```
<Sysname> system-view
[Sysname] aft address-group 2
[Sysname-aft-address-group-2] address 10.1.1.1 10.1.1.15
[Sysname-aft-address-group-2] address 10.1.1.20 10.1.1.30
```

【相关命令】

- **aft address-group**

1.1.2 aft address-group

aft address-group 命令用来创建一个地址组，并进入地址组视图。如果指定的地址组已经存在，则直接进入地址组视图。

undo aft address-group 命令用来删除指定的地址组。

【命令】

aft address-group *group-id*

undo aft address-group *group-id*

【缺省情况】

不存在 AFT 地址组。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

group-id：地址组的编号，取值范围为 0～65535。

【使用指导】

一个地址组是多个地址组成员的集合，各个地址组成员通过 **address** 命令配置。地址组用于动态地址转换。当需要对从 IPv6 网络到达 IPv4 网络的数据报文进行源地址转换时，IPv6 报文的源地址将被转换为地址组成员中的某个 IPv4 地址。

【举例】

创建编号为 1 的 AFT 地址组，并进入 AFT 地址组视图。

```
<Sysname> system-view
[Sysname] aft address-group 1
[Sysname-aft-address-group-1]
```

【相关命令】

- **address**
- **aft v6tov4 source**
- **display aft address-group**
- **display aft configuration**

1.1.3 aft enable

aft enable 命令用来开启接口的 AFT 功能。

undo aft enable 命令用来关闭接口的 AFT 功能。

【命令】

aft enable

undo aft enable

【缺省情况】

接口的 AFT 功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

所有参与 IPv4 网络与 IPv6 网络通信的接口均需开启 AFT 功能。

【举例】

开启接口的 AFT 功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] aft enable
```

【相关命令】

- **display aft configuration**

1.1.4 aft log enable

aft log enable 命令用来开启 AFT 日志功能。

undo aft log enable 命令用来关闭 AFT 日志功能。

【命令】

aft log enable

undo aft log enable

【缺省情况】

AFT 日志功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

为了满足网络管理员安全审计的需要，可以开启 AFT 日志功能，以便对 AFT 连接（AFT 连接是指报文经过设备时，源或目的地址进行过 AFT 转换的连接）信息进行记录。

在以下情况下会触发记录 AFT 日志：

- AFT 端口块新建
- AFT 端口块删除
- AFT 流创建，即 AFT 会话创建时输出日志，需要同时配置 **aft log flow-begin** 命令。
- AFT 流删除，即 AFT 会话释放时输出日志，需要同时配置 **aft log flow-end** 命令。

生成的日志信息将被发送到设备的信息中心，通过设置信息中心的参数，决定日志信息的输出规则（即是否允许输出以及输出方向）。有关信息中心参数的配置请参见“网络管理和监控配置指导”中的“信息中心”。

【举例】

开启 AFT 日志功能。

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

【相关命令】

- **aft log flow-begin**
- **aft log flow-end**
- **display aft configuration**

1.1.5 aft log flow-begin

aft log flow-begin 命令用来开启 AFT 新建流的日志功能。

undo aft log flow-begin 命令用来关闭 AFT 新建流的日志功能。

【命令】

aft log flow-begin

undo aft log flow-begin

【缺省情况】

AFT 新建流的日志功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

开启 AFT 新建流的日志功能后，新建 AFT 会话时，会输出 AFT 日志。

只有开启 AFT 日志功能（**aft log enable** 命令）之后，本命令才能生效。

【举例】

开启 AFT 新建流的日志功能。

```
<Sysname> system-view
[Sysname] aft log flow-begin
```

【相关命令】

- **aft log enable**
- **aft log flow-end**
- **display aft configuration**

1.1.6 aft log flow-end

aft log flow-end 命令用来开启 AFT 删除流的日志功能。

undo aft log flow-end 命令用来关闭 AFT 删除流的日志功能。

【命令】

aft log flow-end

undo aft log flow-end

【缺省情况】

AFT 删除流的日志功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

开启 AFT 删除流的日志功能后，释放 AFT 会话时，会输出 AFT 日志。

只有开启 AFT 日志功能（**aft log enable** 命令）之后，本命令才能生效。

【举例】

开启 AFT 删除流的日志功能。

```
<Sysname> system-view
[Sysname] aft log flow-end
```

【相关命令】

- **aft log enable**
- **aft log flow-begin**
- **display aft configuration**

1.1.7 aft prefix-general

aft prefix-general 命令用来配置 General 前缀。

undo aft prefix-general 命令用来删除指定的 General 前缀。

【命令】

aft prefix-general *prefix-general prefix-length*

undo aft prefix-general *prefix-general prefix-length*

【缺省情况】

不存在 General 前缀。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

prefix-general：General 前缀。

prefix-length：前缀长度，取值为 32、40、48、56、64 或 96。

【使用指导】

General 前缀是长度为 32、40、48、56、64 或 96 位的 IPv6 地址前缀，用来将 IPv6 地址和 IPv4 地址互相转换。General 前缀既可以用于转换源地址，也可以用于转换目的地址。

General 前缀不能与设备上的接口地址同网段，并且，General 前缀、NAT64 前缀和 IVI 前缀三者不能相同。

【举例】

配置 General 前缀为 2000:db8e::，前缀长度为 32。

```
<Sysname> system-view
[Sysname] aft prefix-general 2000:db8e:: 32
```

【相关命令】

- **display aft configuration**

1.1.8 aft prefix-ivi

aft prefix-ivi 命令用来配置 IVI 前缀。

undo aft prefix-ivi 命令用来删除指定的 IVI 前缀。

【命令】

aft prefix-ivi *prefix-ivi*

undo aft prefix-ivi *prefix-ivi*

【缺省情况】

不存在 IVI 前缀。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

prefix-ivi：IVI 前缀，前缀取值固定为 32。

【使用指导】

IVI 前缀长度固定为 32 位，该前缀用于检查 IPv6 地址是否符合 IVI 格式，对符合 IVI 前缀格式的 IPv6 地址，取出内嵌的 IPv4 地址进行 AFT 转换。同时，IVI 前缀还可以添加在 IPv4 地址前面组成 IPv6 地址以进行 AFT 转换。

IVI 前缀、NAT64 前缀和 General 前缀三者不能相同。

【举例】

配置 IVI 前缀为 3000:db8e::。

```
<Sysname> system-view
[Sysname] aft prefix-ivi 3000:db8e::
```

【相关命令】

- **display aft configuration**

1.1.9 aft prefix-nat64

aft prefix-nat64 命令用来配置 NAT64 前缀。

undo aft prefix-nat64 命令用来删除指定的 NAT64 前缀。

【命令】

aft prefix-nat64 *prefix-nat64 prefix-length*

undo aft prefix-nat64 *prefix-nat64 prefix-length*

【缺省情况】

不存在 NAT64 前缀。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

prefix-nat64：NAT64 前缀。

prefix-length：前缀长度，取值为 32、40、48、56、64 或 96。

【使用指导】

NAT64 前缀是长度为 32、40、48、56、64 或 96 位的 IPv6 地址前缀，用来将 IPv4 主机的 IPv4 地址转换为 IPv6 地址，以便 IPv4 主机与 IPv6 主机通信。

NAT64 前缀不能与设备上的接口地址同网段，并且，NAT64 前缀、IVI 前缀和 General 前缀三者不能相同。

【举例】

配置 NAT64 前缀为 2000:db8e::，前缀长度为 32。

```
<Sysname> system-view
[Sysname] aft prefix-nat64 2000:db8e:: 32
```

【相关命令】

- **display aft configuration**

1.1.10 aft turn-off tos

aft turn-off tos 命令用来配置 IPv6 报文转换为 IPv4 报文后，IPv4 报文中的 ToS 字段值为 0。

undo aft turn-off tos 命令用来恢复缺省情况。

【命令】

aft turn-off tos

undo aft turn-off tos

【缺省情况】

IPv6 报文转换为 IPv4 报文后，IPv4 报文中的 ToS 字段与转换前的 IPv6 报文的 Traffic Class 字段值相同。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【举例】

配置 IPv6 报文转换为 IPv4 报文后，IPv4 报文中的 ToS 字段值为 0。

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

```
[Sysname] aft turn-off tos
```

1.1.11 aft turn-off traffic-class

aft turn-off traffic-class 命令用来配置 IPv4 报文转换为 IPv6 报文后，IPv6 报文中的 Traffic Class 字段值为 0。

undo aft turn-off traffic-class 命令用来恢复缺省情况。

【命令】

aft turn-off traffic-class

undo aft turn-off traffic-class

【缺省情况】

IPv4 报文转换为 IPv6 报文后，IPv6 报文中的 Traffic Class 字段与转换前的 IPv4 报文的 ToS 字段值相同。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【举例】

配置 IPv4 报文转换为 IPv6 报文后，IPv6 报文中的 Traffic Class 字段值为 0。

```
<Sysname> system-view
[Sysname] aft turn-off traffic-class
```

1.1.12 aft v4tov6 destination

aft v4tov6 destination 命令用来配置从 IPv4 到 IPv6 的目的地址转换策略。

undo aft v4tov6 destination 命令用来删除从 IPv4 到 IPv6 的目的地址转换策略。

【命令】

aft v4tov6 destination acl { **name** *ipv4-acl-name* **prefix-ivi** *prefix-ivi* [**vpn-instance** *ipv6-vpn-instance-name*] | **number** *ipv4-acl-number* { **prefix-general** *prefix-general prefix-length* | **prefix-ivi** *prefix-ivi* [**vpn-instance** *ipv6-vpn-instance-name*] } }

undo aft v4tov6 destination acl { **name** *ipv4-acl-name* | **number** *ipv4-acl-number* }

【缺省情况】

不存在从 IPv4 到 IPv6 的目的地址转换策略。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

acl：指定用来匹配 IPv4 报文的 IPv4 ACL。对于 IPv4 网络到 IPv6 网络的报文，如果 IPv4 报文匹配该 IPv4 ACL，则根据本命令转换目的 IPv4 地址。

name *ipv4-acl-name*：IPv4 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头，为避免混淆，ACL 的名称不允许使用英文单词 all。

number *ipv4-acl-number*：IPv4 ACL 的编号，取值范围为 2000～3999。

prefix-general *prefix-general prefix-length*：配置 General 前缀。对于 IPv4 网络到 IPv6 网络的报文，如果匹配该 IPv4 ACL，则根据 General 前缀将目的 IPv4 地址转换为 IPv6 地址。

prefix-ivi *prefix-ivi*：配置 IVI 前缀。对于 IPv4 网络到 IPv6 网络的报文，如果匹配该 IPv4 ACL，则根据 IVI 前缀将目的 IPv4 地址转换为 IVI 格式的 IPv6 地址。

vpn-instance *ipv6-vpn-instance-name*：指定 IPv6 地址所属 VPN 实例。*ipv6-vpn-instance-name* 表示 IPv6 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果不指定本参数，则表示该 IPv6 地址属于公网。

【使用指导】

不同的 IPv4 到 IPv6 目的地址转换策略引用的 ACL 不能相同。

引用 IVI 前缀或 General 前缀之前，需要先进行 IVI 前缀或 General 前缀的配置，转换策略才能生效。

【举例】

配置动态地址转换策略，将匹配 ACL 2000 的 IPv4 报文目的地址使用 IVI 前缀 3000:db8e::转换为 IPv6 地址。

```
<Sysname> system-view
[Sysname] aft prefix-ivi 3000:db8e::
[Sysname] aft v4tov6 destination acl number 2000 prefix-ivi 3000:db8e::
```

配置动态地址转换策略，将匹配 ACL 2000 的 IPv4 报文目的地址使用 General 前缀 2000:db8e::/32 转换为 IPv6 地址。

```
<Sysname> system-view
[Sysname] aft v4tov6 destination acl number 2000 prefix-general 2000:db8e:: 32
```

【相关命令】

- **display aft configuration**

1.1.13 aft v4tov6 source

aft v4tov6 source 命令用来配置从 IPv4 到 IPv6 的源地址转换策略。

undo aft v4tov6 source 命令用来删除从 IPv4 到 IPv6 的源地址转换策略。

【命令】

静态方式：

aft v4tov6 source *ipv4-address* [**vpn-instance** *ipv4-vpn-instance-name*] *ipv6-address* [**vpn-instance** *ipv6-vpn-instance-name*]

undo aft v4tov6 source *ipv4-address* [**vpn-instance** *ipv4-vpn-instance-name*]

动态方式：

aft v4tov6 source acl { **name** *ipv4-acl-name* **prefix-nat64** *prefix-nat64 prefix-length* [**vpn-instance** *ipv6-vpn-instance-name*] | **number** *ipv4-acl-number* { **prefix-general** *prefix-general prefix-length* | **prefix-nat64** *prefix-nat64 prefix-length* [**vpn-instance** *ipv6-vpn-instance-name*] } }

undo aft v4tov6 source acl { **name** *ipv4-acl-name* | **number** *ipv4-acl-number* }

【缺省情况】

不存在从 IPv4 到 IPv6 的源地址转换策略。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv4-address：指定源 IPv4 地址。

vpn-instance *ipv4-vpn-instance-name*：指定该 IPv4 地址所属 VPN 实例。*ipv4-vpn-instance-name* 表示 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果不指定本参数，则表示该 IPv4 地址属于公网。

ipv6-address：指定转换后的源 IPv6 地址。

vpn-instance *ipv6-vpn-instance-name*：指定该 IPv6 地址所属 VPN 实例。*ipv6-vpn-instance-name* 表示 IPv6 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果不指定本参数，则表示该 IPv6 地址属于公网。

acl：指定用来匹配 IPv4 报文的 IPv4 ACL。对于从 IPv4 网络到 IPv6 网络的报文，如果 IPv4 报文匹配该 IPv4 ACL，则根据本命令转换源 IPv4 地址。

name *ipv4-acl-name*：IPv4 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头，为避免混淆，ACL 的名称不允许使用英文单词 all。

number *ipv4-acl-number*：IPv4 ACL 的编号，取值范围为 2000～3999。

prefix-general *prefix-general prefix-length*：配置 General 前缀，对于匹配 IPv4 ACL 的报文，根据此 General 前缀，将源 IPv4 地址转换为 IPv6 地址。*prefix-general* 为 General 前缀。*prefix-length* 为前缀长度，取值为 32、40、48、56、64 或 96 位。

prefix-nat64 *prefix-nat64 prefix-length*：配置 NAT64 前缀，对于匹配 IPv4 ACL 的报文，根据此 NAT64 前缀，将源 IPv4 地址转换为 IPv6 地址。*prefix-nat64* 为 NAT64 前缀。*prefix-length* 为前缀长度，取值为 32、40、48、56、64 或 96 位。

【使用指导】

不同的 IPv4 到 IPv6 源地址转换策略指定的 IPv4 地址、IPv6 地址以及 ACL 不能相同。

引用 NAT64 前缀或 General 前缀之前，需要先进行 NAT64 前缀或 General 前缀的配置，转换策略才能生效。

静态方式中指定的 IPv6 地址不能与设备上的接口地址同网段。

【举例】

配置静态源地址转换策略，将源 IPv4 地址 2.2.2.123 转换为源 IPv6 地址 3001::5。

```
<Sysname> system-view
[Sysname] aft v4tov6 source 2.2.2.123 3001::5
```

配置动态地址转换策略，将匹配 ACL 2000 的 IPv4 报文源地址使用 NAT64 前缀 2000::/32 转换为 IPv6 地址。

```
<Sysname> system-view
[Sysname] aft prefix-nat64 2000:: 32
[Sysname] aft v4tov6 source acl number 2000 prefix-nat64 2000:: 32
```

配置动态地址转换策略，将匹配 ACL 2000 的 IPv4 报文源地址使用 General 前缀 3000::/32 转换为 IPv6 地址。

```
<Sysname> system-view
[Sysname] aft v4tov6 source acl number 2000 prefix-general 3000:: 32
```

【相关命令】

- **display aft configuration**

1.1.14 aft v6server

aft v6server 命令用来配置 IPv6 侧服务器对应的 IPv4 地址及端口号。

undo aft v6server 命令用来删除 IPv6 侧服务器对应的 IPv4 地址及端口号。

【命令】

aft v6server protocol *protocol-type ipv4-destination-address ipv4-port-number* [**vpn-instance** *ipv4-vpn-instance-name*] *ipv6-destination-address ipv6-port-number* [**vpn-instance** *ipv6-vpn-instance-name*]

undo aft v6server protocol *protocol-type ipv4-destination-address ipv4-port-number* [**vpn-instance** *ipv4-vpn-instance-name*]

【缺省情况】

不存在 IPv6 侧服务器对应的 IPv4 地址及端口号。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

protocol *protocol-type*：指定支持的协议类型。*protocol-type* 取值及含义如下：

- **tcp**：表示 TCP 协议。
- **udp**：表示 UDP 协议。

ipv4-destination-address：IPv6 地址映射的 IPv4 地址。

ipv4-port-number：IPv4 端口号，取值范围为 1～65535。

vpn-instance *ipv4-vpn-instance-name*：指定该 IPv4 地址所属 VPN 实例。*ipv4-vpn-instance-name* 表示 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果不指定本参数，则表示该 IPv4 地址属于公网。

ipv6-destination-address：需要映射的 IPv6 目的地址。

ipv6-port-number：IPv6 端口号，取值范围为 1～65535。

vpn-instance *ipv6-vpn-instance-name*：指定该 IPv6 地址所属 VPN 实例。*ipv6-vpn-instance-name* 表示 IPv6 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果不指定本参数，则表示该 IPv6 地址属于公网。

【使用指导】

不同的 IPv6 侧服务器配置的 IPv4 协议、地址、端口和 VPN 信息不能完全相同。

【举例】

配置 IPv6 服务器 3001::5 对应 IPv4 地址 2.2.2.123 及端口号 1720，指定支持的协议为 TCP。

```
<Sysname> system-view
[Sysname] aft v6server protocol tcp 2.2.2.123 1720 3001::5 1720
```

【相关命令】

- **display aft configuration**

1.1.15 aft v6tov4 source

aft v6tov4 source 命令用来配置从 IPv6 到 IPv4 的源地址转换策略。

undo aft v6tov4 source 命令用来删除从 IPv6 到 IPv4 的源地址转换策略。

【命令】

静态方式：

aft v6tov4 source *ipv6-address* [**vpn-instance** *ipv6-vpn-instance-name*] *ipv4-address* [**vpn-instance** *ipv4-vpn-instance-name*]

undo aft v6tov4 source *ipv6-address* [**vpn-instance** *ipv6-vpn-instance-name*]

动态方式：

aft v6tov4 source { **acl ipv6** { **name** *ipv6-acl-name* | **number** *ipv6-acl-number* } | **prefix-nat64** *prefix-nat64 prefix-length* [**vpn-instance** *ipv6-vpn-instance-name*] } { **address-group** *group-id* [**no-pat** | **port-block-size** *blocksize*] | **interface** *interface-type interface-number* } [**vpn-instance** *ipv4-vpn-instance-name*]

undo aft v6tov4 source { **acl ipv6** { **name** *ipv6-acl-name* | **number** *ipv6-acl-number* } | **prefix-nat64** *prefix-nat64 prefix-length* [**vpn-instance** *ipv6-vpn-instance-name*] }

【缺省情况】

不存在从 IPv6 到 IPv4 的源地址转换策略。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv6-address：指定源 IPv6 地址。

vpn-instance *ipv6-vpn-instance-name*：指定该 IPv6 地址所属的 VPN 实例。*ipv6-vpn-instance-name* 表示 IPv6 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果不指定本参数，则表示该 IPv6 地址属于公网。

ipv4-address：指定转换后的源 IPv4 地址。

vpn-instance *ipv4-vpn-instance-name*：指定该 IPv4 地址所属的 VPN 实例。*ipv4-vpn-instance-name* 表示 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果不指定本参数，则表示该 IPv4 地址属于公网。

acl ipv6：指定用来匹配 IPv6 报文的 IPv6 ACL。对于 IPv6 网络到 IPv4 网络的报文，如果 IPv6 报文匹配该 IPv6 ACL，则根据本命令转换源 IPv6 地址。

name *ipv6-acl-name*：IPv6 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头，为避免混淆，IPv6 ACL 的名称不允许使用英文单词 all。

number *ipv6-acl-number*：IPv6 ACL 的编号，取值范围为 2000～3999。

prefix-nat64 *prefix-nat64 prefix-length*：指定用来匹配 IPv6 报文目的地址的 NAT64 前缀。对于从 IPv6 网络到 IPv4 网络的报文，如果目的 IPv6 地址符合配置的 NAT64 前缀格式，则根据本命令转换源 IPv6 地址。*prefix-nat64* 为 NAT64 前缀。*prefix-length* 为前缀长度，取值为 32、40、48、56、64 或 96。

address-group *group-id*：指定将源 IPv6 地址转换为该地址组中的 IPv4 地址。*group-id* 为 AFT 地址组的编号，取值范围为 0～65535。

no-pat：指定该地址转换策略不进行端口转换。如果不指定该参数，则表示进行端口转换。

port-block-size *blocksize*：端口块大小，取值范围为 100～64512。如果不指定该参数，则表示 PAT 方式进行端口转换时不做端口块限制。

interface *interface-type interface-number*：指定将源 IPv6 地址转换为该接口的主 IPv4 地址。*interface-type interface-number* 表示接口类型和接口编号。如果指定该参数，则表示接口将一定采用 PAT 方式进行端口转换，不做端口块限制。

【使用指导】

如果指定了 **port-block-size** *blocksize* 参数，则进行 PAT 转换时，可用的端口范围为 1024～65535。该端口范围被划分成多个端口块，每个端口块的大小由 **port-block-size** *blocksize* 参数决定。例如，*blocksize* 为 1000 时，第一个端口块的端口号范围为 1024～2023，第二个端口块的端口号范围为 2024～3023，以此类推。

引用 NAT64 前缀之前，需要先进行 NAT64 前缀的配置，转换策略才能生效。

不同 IPv6 到 IPv4 源地址转换策略中指定的 IPv6 地址、IPv4 地址、地址组、ACL、NAT64 前缀均不能相同。

【举例】

配置静态地址转换策略，将源 IPv6 地址 3001::5 转换为源 IPv4 地址 2.2.2.123。

```
<Sysname> system-view
[Sysname] aft v6tov4 source 3001::5 2.2.2.123
```

配置动态地址转换策略，将匹配 ACL 2000 的 IPv6 报文源地址转换为地址组 0 中的地址，并指定 PAT 方式进行端口转换时的端口块大小为 100。

```
<Sysname> system-view
[Sysname] aft v6tov4 source acl ipv6 number 2000 address-group 0 port-block-size 100
```

【相关命令】

- **display aft configuration**
- **display aft port-block**

1.1.16 display aft address-group

display aft address-group 命令用来显示地址组信息。

【命令】

display aft address-group [*group-id*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

group-id：地址组的编号，取值范围为 0～65535。如果不指定本参数，则显示所有地址组的信息。

【举例】

显示所有地址组的信息。

```
<Sysname> display aft address-group
  There are 3 AFT address groups.
  Group number            Start address         End address
  1                       202.110.10.10         202.110.10.15
  2                       202.110.10.20         202.110.10.25
                          202.110.10.30         202.110.10.35
  6                       ---                   ---
```

显示指定地址组的信息。

```
<Sysname> display aft address-group 1
  Group number             Start address         End address
  1                        202.110.10.10         202.110.10.15
```

表1-1 display aft address-group 命令显示信息描述表

字段	描述
There are *n* AFT address groups	当前有*n*个AFT地址组
Group number	地址组编号

字段	描述
Start address	地址组成员的起始地址。如果未配置，则显示为“---”
End address	地址组成员的结束地址。如果未配置，则显示为“---”

1.1.17 display aft address-mapping

display aft address-mapping 命令用来显示 AFT 地址映射信息。

【命令】

display aft address-mapping [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

slot *slot-number*：显示指定成员设备上的 AFT 地址映射表项信息，*slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数，则显示所有成员设备上的 AFT 地址映射表项信息。

【举例】

显示 AFT 地址映射表的信息。

```
<Sysname> display aft address-mapping
Slot 0:
IPv6: Source IP/port: 2000:0:FF01:101:100::8/1024
      Destination IP/port: 5000::1717:1714/1025
      VPN instance/VLAN ID/Inline ID: -/-/-
      Protocol: TCP(6)
IPv4: Source IP/port: 1.1.1.1/1031
      Destination IP/port: 23.23.23.20/1025
      VPN instance/VLAN ID/Inline ID: -/-/-
      Protocol: TCP(6)

Total address mappings found: 1
```

表1-2 display aft address-group 命令显示信息描述表

字段	描述
Slot 0	指定成员设备上的AFT地址映射信息
IPv4	IPv4地址信息
IPv6	IPv6地址信息

字段	描述
Source IP/port	源IP地址/端口号
Destination IP/port	目的IP地址/端口号
VPN instance/VLAN ID/Inline ID	会话所属的VPN实例/二层转发时会话所属的VLAN ID/二层转发时会话所属的INLINE。如果未指定则显示“-/-/-”
Protocol	协议类型，包括：DCCP、ICMP、ICMPv6、Raw IP 、SCTP、TCP、UDP、UDP-Lite

1.1.18 display aft configuration

display aft configuration 命令用来显示 AFT 配置信息。

【命令】

display aft configuration

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【举例】

显示 AFT 的配置信息。

```
<Sysname> display aft configuration
aft address-group 1
  address 202.110.10.10 202.110.10.15
  address 101.1.1.100 101.1.1.200

aft prefix-ivi 2013::
aft prefix-ivi 1111::

aft v6tov4 source 1::1 1.1.1.1
aft v6tov4 source 1::2 1.1.1.2

interface GigabitEthernet1/0/1
  aft enable
```

1.1.19 display aft no-pat

display aft no-pat 命令用来显示 AFT NO-PAT 表项信息。

【命令】

display aft no-pat [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

slot *slot-number*：显示指定成员设备上的 AFT NO-PAT 表项信息，*slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数，则显示所有成员设备上的 AFT NO-PAT 表项信息。

【使用指导】

NO-PAT 是指 IPv6 地址与 IPv4 地址存在一一对应的转换关系，不存在端口转换关系。

【举例】

显示 AFT NO-PAT 表项信息。

```
<Sysname> display aft no-pat
Slot 0:
IPv6 address: 3006::0002
IPv4 address: 200.100.1.100
IPv4 VPN    : vpn2
IPv6 VPN    : vpn1

IPv6 address: 4016::1102
IPv4 address: 202.120.12.110
IPv4 VPN    : vpn2
IPv6 VPN    : vpn1

Total entries found: 2
```

表1-3 display aft no-pat 命令显示信息描述表

字段	描述
Slot 0	指定成员设备上的AFT NO-PAT表项信息
IPv6 address	转换前的IPv6地址
IPv4 address	转换后的IPv4地址
IPv4 VPN	转换后的IPv4地址所属VPN实例。如果不属于任何VPN，则该行不显示
IPv6 VPN	转换前的IPv6地址所属VPN实例。如果不属于任何VPN，则该行不显示
Total entries found	AFT NO-PAT表项的总数

1.1.20 display aft port-block

display aft port-block 命令用来显示端口块映射表项信息。

【命令】

display aft port-block [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

slot *slot-number*：显示指定成员设备上的 AFT 端口块映射表项信息，*slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数，则显示所有成员设备上的 AFT 端口块映射表项信息。

【举例】

显示端口块映射表项信息。

```
<Sysname> display aft port-block
Slot 0:
IPv6 address: 3006::0002
IPv4 address: 200.100.1.100
Port block  : [1024 – 1123]
IPv4 VPN    : vpn2
IPv6 VPN    : vpn1

IPv6 address: 4016::1102
IPv4 address: 202.120.12.110
Port block  : [1024 – 1200]
IPv4 VPN    : vpn2
IPv6 VPN    : vpn1

Total entries found: 2
```

表1-4 display aft port-block 命令显示信息描述表

字段	描述
Slot 0	指定成员设备的AFT端口映射表项信息
IPv6 address	转换前的IPv6地址
IPv4 address	转换后的IPv4地址
Port block	转换后的IPv4端口范围
IPv4 VPN	转换后的IPv4地址所属VPN实例。如果不属于任何VPN，则该行不显示
IPv6 VPN	转换前的IPv6地址所属VPN实例。如果不属于任何VPN，则该行不显示
Total entries found	AFT端口映射表项的总数

1.1.21 display aft session

display aft session 命令用来显示 AFT 会话（即进行过 AFT 地址转换的会话）的信息。

【命令】

display aft session ipv4 [{ **source-ip** *source-ip-address* | **destination-ip** *destination-ip-address* } * [**vpn-instance** *ipv4-vpn-instance-name*]] [**slot** *slot-number*] [**verbose**]

display aft session ipv6 [{ **source-ip** *source-ipv6-address* | **destination-ip** *destination-ipv6-address* } * [**vpn-instance** *ipv6-vpn-instance-name*]] [**slot** *slot-number*] [**verbose**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

ipv4：显示 AFT 创建的 IPv4 会话信息。

source-ip *source-ip-address*：显示指定源地址的会话。*source-ip-address* 表示源 IPv4 地址，该地址必须是创建会话的报文的源地址。

destination-ip *destination-ip-address*：显示指定目的地址的会话。*destination-ip-address* 表示目的 IPv4 地址，该地址必须是创建会话的报文的目的地址。

vpn-instance *ipv4-vpn-instance-name*：显示指定 VPN 的会话。*ipv4-vpn-instance-name* 表示 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果不指定该参数，则显示属于公网的 IPv4 会话信息。

ipv6：显示 AFT 创建的 IPv6 会话信息。

source-ip *source-ipv6-address*：显示指定源地址的会话。*source-ipv6-addrsss* 表示源 IPv6 地址，该地址必须是创建会话的报文的源地址。

destination-ip *destination-ipv6-address*：显示指定目的地址的会话。*destination-ipv6-address* 表示目的 IPv6 地址，该地址必须是创建会话的报文的目的地址。

vpn-instance *ipv6-vpn-instance-name*：显示指定 VPN 的会话。*ipv6-vpn-instance-name* 表示 IPv6 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果不指定该参数，则显示属于公网的 IPv6 会话信息。

slot *slot-number*：显示指定成员设备上的 AFT 会话信息，*slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数，则显示所有成员设备上的 AFT 会话信息。

verbose：显示 AFT 会话的详细信息。不指定此参数时，显示会话的概要信息。

【使用指导】

如果不指定任何参数，则显示所有 AFT 会话的信息。

【举例】

显示 AFT 会话的详细信息。

```
<Sysname> display aft session ipv4 slot 0 verbose
Slot 0:
Initiator:
  Source IP/port: 192.168.1.18/1877
  Destination IP/port: 102.128.1.55/22
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
Responder:
  Source IP/port: 102.128.1.55/22
  Destination IP/port: 192.168.1.18/1877
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
App: SSH   State: TCP_SYN_SENT
Start time: 2011-07-29 19:12:36  TTL: 28s
Initiator->Responder:         1 packets         48 bytes
Responder->Initiator:         0 packets          0 bytes

Total sessions found: 1
```

表1-5 display aft session 命令显示信息描述表

字段	描述
Slot 0	显示指定成员设备的AFT会话信息
Initiator	发起方的会话信息
Source IP/port	源IP地址/端口号
Destination IP/port	目的IP地址/端口号
VPN instance/VLAN ID/Inline ID	会话所属的VPN实例/二层转发时会话所属的VLAN ID/二层转发时会话所属的INLINE。如果未指定则显示“-/-/-”
Protocol	协议类型，包括：DCCP、ICMP、ICMPv6、Raw IP 、SCTP、TCP、UDP、UDP-Lite
Inbound interface	入接口
Responder	响应方的会话信息
App	应用层协议类型，包括：FTP、DNS等，unknown表示非知名端口并且也未使用用户自定义的协议类型
State	会话状态
Start time	会话创建时间
TTL	会话剩余存活时间，单位为秒
Initiator->Responder	发起方到响应方的报文数、报文字节数

字段	描述
Responder->Initiator	响应方到发起方的报文数、报文字节数
Total sessions found	AFT会话总数

【相关命令】

- **reset aft session**

1.1.22 display aft statistics

display aft statistics 显示 AFT 统计信息。

【命令】

display aft statistics [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

slot *slot-number*：显示指定成员设备上的 AFT 统计信息，*slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数，则显示所有成员设备上的 AFT 统计信息。

【使用指导】

如果不指定任何参数，则显示所有 AFT 统计信息。

【举例】

显示所有 AFT 统计信息。

```
<Sysname> display aft statistics
Total NO-PAT entries found: 0
Total port-block entries found: 0
Dropped packets: 0
  Configuration sequence changed: 0
  Failed to transfer payload: 0
  Failed to transfer packet header: 0
  Packet examination failed before packet sending: 0
  Failed to translate destination address: 0
  The translated destination address is invalid: 0
  Failed to translate source address: 0
  Failed to transfer FSBUF to MBUF: 0
  Session ext-info is null: 0
  Peer session is null: 0
```

```
Failed to get translation information from session: 0
Failed to create session: 0
Failed to fragment the MBUF: 0
Failed to create fast forwarding table: 0
Failed to formalize session: 0
Other reasons: 0
```

表1-6 display aft statistics 命令显示信息描述表

字段	描述
Total NO-PAT entries found	AFT创建的NO-PAT表项个数
Total port-block entries found	AFT创建的端口块映射表项个数
Dropped packets	AFT丢弃的报文个数
Configuration sequence changed	配置序列变更丢包
Failed to transfer payload	ALG处理失败丢包
Failed to transfer packet header	报文头转换失败丢包
Packet examination failed before packet sending	报文发送前检查失败丢包
Failed to translate destination address	目的地址转换失败丢包
The translated destination address is invalid	转换后的目的地址非法丢包
Failed to translate source address	源地址转换失败丢包
Failed to transfer FSBUF to MBUF	数据从FSBUF结构转换为MBUF结构失败丢包
Session ext-info is null	未找到会话扩展信息丢包
Peer session is null	未找到对端会话丢包
Failed to get translation information from session	由会话获取转换信息失败丢包
Failed to create session	创建会话失败丢包
Failed to fragment the MBUF	分片失败丢包
Failed to create fast forwarding table	创建快转表失败丢包
Failed to formalize session	会话正式化失败丢包
Other reasons	其他原因丢包

【相关命令】

- **reset aft statistics**

1.1.23 reset aft session

reset aft session 命令用来删除 AFT 会话。

【命令】

reset aft session [**slot** *slot-number*]

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

slot *slot-number*：删除指定成员设备上的 AFT 会话，*slot-number* 表示设备在 IRF 中的成员编号。如果不指定该参数，则表示删除所有成员设备上的 AFT 会话。

【使用指导】

执行本命令删除 AFT 会话后，该会话对应的 AFT NO-PAT 表项和端口块映射表信息也会同时被删除。

【举例】

删除所有 AFT 会话。

```
<Sysname> reset aft session
```

删除 2 号成员设备上的 AFT 会话。

```
<Sysname> reset aft session slot 2
```

【相关命令】

- **display aft session**

1.1.24 reset aft statistics

reset aft statistics 命令用来清除 AFT 统计信息。

【命令】

reset aft statistics [**slot** *slot-number*]

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

slot *slot-number*：删除指定成员设备上的 AFT 统计信息，*slot-number* 表示设备在 IRF 中的成员编号。如果不指定该参数，则表示删除所有成员设备上的 AFT 统计信息。

【使用指导】

AFT 统计信息包括 AFT 丢弃的报文个数，NO-PAT 表项个数和端口块映射表项个数。该命令仅会清除 AFT 丢弃的报文个数统计。

【举例】

清除 AFT 统计信息。

```
<Sysname> reset aft statistics
```

清除 2 号成员设备上的 AFT 统计信息。

```
<Sysname> reset aft statistics slot 2
```

【相关命令】

- **display aft statistics**