H3C SR8800-F 路由器

NAT 命令参考

新华三技术有限公司
http://www.h3c.com

资料版本：6W102-20190108
产品版本：SR8800FS-CMW710-R7751P01 及以上版本

前 言

本命令参考主要介绍 NAT（Network Address Translation，网络地址转换）相关的配置命令。

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

1.1 NAT配置命令

1.1.1 address

address 命令用来添加一个地址成员。

undo address 命令用来删除一个地址成员。

【命令】

address *start-address end-address*

undo address *start-address end-address*

【缺省情况】

不存在地址成员。

【视图】

NAT 地址组视图

【缺省用户角色】

network-admin

【参数】

start-address end-address：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。*start-address* 和 *end-address* 之间的 IP 地址数量不能超过 256 个。

【使用指导】

一个 NAT 地址组/地址池是多个地址成员的集合。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成员中的某个地址。

多次执行本命令添加的地址成员不能互相重叠。

如果公网地址成员与 NAT 端口块静态映射中的公网地址成员重叠，请确保 NAT 端口块静态映射中的端口范围与 NAT 端口块动态映射中的端口范围不重叠。否则当用户上线时，如果设备为两个不同的用户分配了相同的公网 IP 地址和端口块，可能会导致无法为其中一个用户创建 NAT 会话。

【举例】

在 NAT 地址组 2 中添加地址成员。

```
<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

【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 1～65535。

【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

【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 1:
    Port range: 1-65535
    Failover group name: nat
    Address information:
      Start address         End address
      202.110.10.10         202.110.10.15

  Address group 2:
    Port range: 1-65535
    Failover group name: trans
    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
    Failover group name: nat
    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
    Failover group name: nat
    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
    Failover group name: nat
    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 1:
    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	地址组的编号
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
Failover group name	NAT地址组绑定的备份组的名称。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 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

【举例】

显示所有的 NAT 配置信息。（独立运行模式）

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

```
      202.110.10.10         202.110.10.15

  Address group 2:
    Port range: 1-65535
    Failover group name: group1
    Failover group name: trans
    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
    Failover group name: abc
    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
    Failover group name: trans
    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 outbound information:
  Totally 2 NAT outbound rules.
  Interface: GigabitEthernet1/0/2
    ACL: 2036         Address group: 1      Port-preserved: Y
    NO-PAT: N         Reversible: N
    Service card: ---
    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: 1      Port-preserved: N
    NO-PAT: Y         Reversible: Y
    VPN instance: vpn_nat
    Service card: ---
    Config status: Active

NAT internal server information:
  Totally 4 internal servers.
  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
    Service card  : Slot 2
    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
    Service card  : Slot 2
    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
    Service card  : Slot 2
    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
    Service card  : Slot 2
    Config status : Active

Static NAT mappings:
  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
    Failover group name: abc
    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
    Failover group name: group1
    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
    Service card : Slot 2
    Config status: Active

  Interface: GigabitEthernet1/0/6
    Service card : ---
    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
  Flow-begin               : Disabled
  Flow-end                 : Disabled
  Flow-active              : Disabled
  Port-block-assign        : Disabled
  Port-block-withdraw      : Disabled
  Port-alloc-fail          : Enabled
  Port-block-alloc-fail    : Disabled
  Port-usage               : Disabled
  Port-block-usage         : Enabled(40%)

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

  Interface: GigabitEthernet1/0/6
    Service card : Slot 2
    Config status: Active

NAT mapping behavior:
  Mapping mode : Connection-dependent

NAT ALG:
  DNS        : Disabled
  FTP        : Enabled
  H323       : Disabled
  ICMP-ERROR : Enabled
  ILS        : Disabled
  MGCP       : Disabled
  NBT        : Disabled
  PPTP       : Disabled
  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
    Failover group name: nat
    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
    Failover group name: group1
    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
    Service card    : ---
    Config status   : Active

  Interface: GigabitEthernet1/0/2
    port-block-group: 10
    Service card    : ---
```

```
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 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1-2 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1-14”
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1-8”
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1-13”
Static NAT mappings	静态地址转换的配置信息，详细字段解释请参见“表1-16”
NAT DNS mappings	NAT DNS mapping的配置信息，详细字段解释请参见“表1-3”
NAT logging	NAT日志功能的配置信息，详细字段解释请参见“表1-6”
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
Service card	显示提供NAT处理的业务板。如果接口下没有指定业务板，则显示为“---”
Config status	显示NAT hairpin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 hairpin 配置不生效的原因
Mapping mode	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的转换模式 • Connection-dependent：表示关心对端地址和端口的非共享转换模式
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	NAT端口块静态映射的配置信息，详细字段解释请参见“表1-9”

1.1.5 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

【举例】

显示 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1-3 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
Config status	显示DNS mapping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**

1.1.6 display nat eim

display nat eim 命令用来显示 NAT EIM 表项信息。

【命令】

独立运行模式：

display nat eim [**slot** *slot-number*] [**protocol** { **tcp** | **udp** }]

IRF 模式：

display nat eim [**chassis** *chassis-number* **slot** *slot-number*] [**protocol** { **tcp** | **udp** }]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

slot *slot-number*：显示指定单板上的 EIM 表项信息，*slot-number* 表示单板所在的槽位号。若不指定该参数，则表示显示所有单板上的 EIM 表项信息。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备的指定单板上的 EIM 表项信息，*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。若不指定该参数，则表示显示所有成员设备的所有单板上的 EIM 表项信息。（IRF 模式）

protocol：显示指定协议类型的 EIM 表项信息。

tcp：显示 TCP 协议类型的 EIM 表项信息。

udp：显示 UDP 协议类型的 EIM 表项信息。

【使用指导】

EIM 三元组表项是报文在进行 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】

显示指定 slot 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
DS-Lite tunnel peer: -
Local  VPN: vpn1
Global VPN: vpn2
Protocol: TCP(6)
Failover group name: group1

Local  IP/port: 192.168.100.200/2048
Global IP/port: 200.100.1.200/4096
DS-Lite tunnel peer: -
Protocol: UDP(17)
Failover group name: group1

Total entries found: 2
```

显示指定 slot 上协议为 TCP 的 NAT EIM 表项信息。

```
<Sysname> display nat eim slot 1 protocol tcp
Slot 1:
Local  IP/port: 192.168.100.100/1024
Global IP/port: 200.100.1.100/2048
DS-Lite tunnel peer: -
Local  VPN: vpn1
Global VPN: vpn2
Protocol: TCP(6)
Failover group name: group1

Total entries found: 1
```

表1-4 display nat eim 命令显示信息描述表

字段	描述
DS-Lite tunnel peer	DS-Lite B4端隧道地址。会话不属于任何DS-Lite隧道时，本字段显示为“-”
Local VPN	内网地址所属的MPLS L3VPN的VPN实例名称。如果不属于任何VPN实例，则不显示该字段
Global VPN	外网地址所属的MPLS L3VPN的VPN实例名称。如果不属于任何VPN实例，则不显示该字段
Protocol	协议名称以及协议编号
Failover group name	备份组的名称。如果未绑定任何备份组，本字段显示为“-”
Total entries found	当前查找到的EIM表项的个数

【相关命令】

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

1.1.7 display nat eim statistics

display nat eim statistics 命令用来显示 NAT EIM 表项的统计信息。

【命令】

独立运行模式：

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

IRF 模式：

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

slot *slot-number*：显示指定单板上的 EIM 表项统计信息，*slot-number* 表示单板所在的槽位号。若不指定该参数，则表示显示所有单板上的 EIM 表项统计信息。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备的指定单板上的 EIM 表项统计信息，*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。若不指定该参数，则表示显示所有成员设备的所有单板上的 EIM 表项统计信息。（IRF 模式）

【使用指导】

通过本命令可以查看 NAT EIM 表项的统计信息，包括 EIM 表项的数量、传输层协议为 TCP 或 UDP 的 EIM 表项创建速率等信息。

【举例】

显示指定 slot 上 NAT EIM 的统计信息。

```
<Sysname> display nat eim statistics slot 2
EIM: Total EIM entries.
TCP: Total EIM entries for TCP.
UDP: Total EIM entries for UDP.
Rate: Creating rate of EIM entries.
TCP rate: Creating rate of EIM entries for TCP.
UDP rate: Creating rate of EIM entries for UDP.
Slot EIM       TCP       UDP       Rate          TCP rate      UDP rate
                                   (entries/s)   (entries/s)   (entries/s)
2    0         0         0         0             0             0
```

表1-5 display nat eim statistics 命令显示信息描述表

字段	描述
Total EIM entries	EIM表项个数
Total EIM entries for TCP	传输层协议为TCP的EIM表项个数
Total EIM entries for UDP	传输层协议为UDP的EIM表项个数

字段	描述
Creating rate of EIM entries	EIM表项的创建速率
Creating rate of EIM entries for TCP	传输层协议为TCP的EIM表项创建速率
Creating rate of EIM entries for UDP	传输层协议为UDP的EIM表项创建速率

【相关命令】

- **nat mapping-behavior**

1.1.8 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

【举例】

显示 NAT 日志功能的配置信息。

```
<Sysname> display nat log
NAT logging:
  Log enable               : Enabled
  Flow-begin               : Disabled
  Flow-end                 : Disabled
  Flow-active              : Disabled
  Port-block-assign        : Disabled
  Port-block-withdraw      : Disabled
  Port-alloc-fail          : Enabled
  Port-block-alloc-fail    : Disabled
  Port-usage               : Disabled
  Port-block-usage         : Enabled(40%)
```

表1-6 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 • Enabled：表示处于开启状态。如果指定了 ACL，则同时显示指定的 ACL 编号或名称

字段	描述
	• Disabled：表示处于关闭状态
Flow-begin	NAT会话新建日志功能开关 • Enabled：表示处于开启状态 • Disabled：表示处于关闭状态
Flow-end	NAT会话删除日志功能开关 • Enabled：表示处于开启状态 • Disabled：表示处于关闭状态
Flow-active	NAT活跃流日志功能开关 • Enabled：表示处于开启状态。该状态下，将同时显示配置的生成活跃流日志的时间间隔（单位为分） • Disabled：表示处于关闭状态
Port-block-assign	端口块分配的NAT444用户日志功能开关 • Enabled：表示处于开启状态 • Disabled：表示处于关闭状态
Port-block-withdraw	端口块回收的NAT444用户日志功能开关 • Enabled：表示处于开启状态 • Disabled：表示处于关闭状态
Port-alloc-fail	端口分配失败的日志功能开关 • Enabled：表示处于开启状态 • Disabled：表示处于关闭状态
Port-block-alloc-fail	端口块分配失败的日志功能开关 • Enabled：表示处于开启状态 • Disabled：表示处于关闭状态
Port-usage	端口块中端口使用率的日志功能开关 • Enabled：表示处于开启状态。该状态下，将同时显示配置的端口使用率的阈值（单位为百分比） • Disabled：表示处于关闭状态
Port-block-usage	端口块使用率的日志功能处于开启（Enabled）状态，同时显示配置的端口块使用率的阈值（单位为百分比），缺省值为90%

【相关命令】

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

1.1.9 display nat no-pat

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

【命令】

独立运行模式：

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

IRF 模式：

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

slot *slot-number*：显示指定单板上的 NO-PAT 表项信息，*slot-number* 表示单板所在的槽位号。若不指定该参数，则表示显示所有单板上的 NO-PAT 表项信息。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备的指定单板上的 NO-PAT 表项信息，*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。若不指定该参数，则表示显示所有成员设备的所有单板上的 NO-PAT 表项信息。（IRF 模式）

【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。

【举例】

显示指定 slot 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      : Outbound

Total entries found: 1
```

表1-7 display nat no-pat 命令显示信息描述表

字段	描述
Local VPN	内网地址所属的MPLS L3VPN的实例名称。如果不属于任何VPN实例，则该行不显示
Global VPN	外网地址所属的MPLS L3VPN的实例名称。如果不属于任何VPN实例，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

字段	描述
	换表项进行地址转换；若其值为“N”，则表示不允许
Type	NO-PAT表项类型 • 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 outbound**

1.1.10 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

【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: 1      Port-preserved: Y
    NO-PAT: N         Reversible: N
    Service card: Slot 5
    Config status: Active

  Interface: GigabitEthernet1/0/2
    ACL: 2037         Address group: 2      Port-preserved: N
    NO-PAT: Y         Reversible: Y
    VPN instance: vpn_nat
    Service card: Slot 5
    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: 0      Port-preserved: N
    NO-PAT: N         Reversible: N
```

```
Service card: Slot 5
Config status: Active
```

表1-8 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	出方向动态地址转换使用的地址组。如果未配置，则显示“---”
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；若其值为“N”，则表示不允许
VPN instance	地址组所属的MPLS L3VPN的VPN实例名称。如果不属于任何VPN实例，则不显示该字段
Service card	显示提供NAT处理的业务板。如果接口下未指定业务板，则显示为“---”
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**

1.1.11 display nat outbound port-block-group

display nat outbound port-block-group 命令用来显示 NAT 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

【举例】

显示 NAT 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
    Config status   : Active

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

表1-9 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	NAT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NAT端口块静态映射配置
Interface	NAT端口块静态映射配置所在的接口
port-block-group	端口块组编号
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**

1.1.12 display nat port-block

display nat port-block 命令用来显示端口块表项。

【命令】

独立运行模式：

display nat port-block { dynamic [ds-lite-b4] | static } [ip *ipv4-source-address* **] [slot** *slot-number* **] [verbose]**

display nat port-block dynamic ds-lite-b4 [ipv6 *ipv6-source-address* **] [slot** *slot-number* **]] [verbose]**

IRF 模式：

display nat port-block { dynamic [ds-lite-b4] | static } [ip *ipv4-source-address* **] [chassis** *chassis-number* **slot** *slot-number* **] [verbose]**

display nat port-block { dynamic [ds-lite-b4] | static }[ipv6 *ipv6-source-address* **] [chassis** *chassis-number* **slot** *slot-number* **] [verbose]**

【视图】

任意视图

【缺省用户角色】

network-admin

network-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。

ip *ipv4-source-address*：显示指定 IPv4 源地址的端口块表项。*ipv4-source-address* 表示源地址，该地址必须是创建端口块表项的报文的源地址。

ipv6 *ipv6-source-address*：显示指定 IPv6 源地址的端口块表项。*ipv6-source-address* 表示源地址，该地址必须是创建端口块表项的报文的源地址。

slot *slot-number*：显示指定单板上的端口块表项信息，*slot-number* 表示单板所在的槽位号。若不指定该参数，则表示显示所有单板上的端口块表项信息。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备的指定单板上的端口块表项信息，*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。若不指定该参数，则表示显示所有成员设备的所有单板上的端口块表项信息。（IRF 模式）

verbose：显示单板上的端口块表项的详细信息。若不指定该参数，则显示端口块表项的概要信息。

【举例】

显示指定 slot 上的静态端口块表项。

```
<Sysname> display nat port-block static slot 1
Slot 1:
Local VPN     Local IP         Global IP        Port block   Connections  Extend
---           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            ---
vpn01         100.100.100.113  202.202.100.101  10769-11024  0            ---
Total mappings found: 4
```

显示指定 slot 上的动态端口块表项。

```
<Sysname> display nat port-block dynamic slot 1
```

```
Slot 1:
Local VPN     Local IP         Global IP        Port block   Connections  Extend
---           101.1.1.12       192.168.135.201  10001-11024  1            ---
Total mappings found: 1
```

显示指定 slot 上的基于 DS-Lite B4 地址的端口块表项。

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

显示指定 slot 上动态端口块表项的详细信息。

```
<Sysname> display nat port-block dynamic slot 1 verbose
Slot 1:
Dynamic port block entry
Local IP         : 200.1.24.219
Local vpn        : ---(0)
Global IP        : 202.2.1.8
Global vpn       : ---(0)
Port block       : 24774-26023
Connections      : 0
FailgroupID      : 16
PortLimit TCP    : N/A
PortLimit UDP    : N/A
PortLimit ICMP   : N/A
PortLimit total  : 100
PortUsed  TCP    : 0
PortUsed  UDP    : 0
PortUsed  ICMP   : 0
PortUsed  total  : 0
Extend port block: N

Dynamic port block entry
Local IP         : 200.1.40.231
Local vpn        : ---(0)
Global IP        : 202.2.1.10
Global vpn       : ---(0)
Port block       : 32274-33523
Connections      : 0
FailgroupID      : 16
PortLimit TCP    : N/A
PortLimit UDP    : N/A
PortLimit ICMP   : N/A
PortLimit total  : 100
PortUsed  TCP    : 0
PortUsed  UDP    : 0
PortUsed  ICMP   : 0
PortUsed  total  : 0
Extend port block: N
```

```
Total mappings found: 2
```

表1-10 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实例，“---”表示不属于任何VPN实例
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
Extend	是否为增量端口块： • Ext：表示是增量端口块 • ---：表示非增量端口块
Total mappings found	当前查找到的端口块表项的个数

表1-11 display nat port-block verbose 命令详细显示信息描述表

字段	描述
Local IP	私网IP地址
Local vpn	私网IP地址所属VPN实例，“---(0)”表示不属于任何VPN实例
Global IP	公网IP地址
Global vpn	公网IP地址所属VPN实例，“---(0)”表示不属于任何VPN实例
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
FailgroupID	端口块表项所属的备份组
PortLimit TCP	最多可分配给TCP协议的端口数量
PortLimit UDP	最多可分配给UDP协议的端口数量
PortLimit ICMP	最多可分配给ICMP协议的端口数量
PortLimit total	最多可分配的端口数量
PortUsed TCP	TCP报文分配的端口数
PortUsed UDP	UDP报文分配的端口数
PortUsed ICMP	ICMP报文分配的端口数
PortUsed total	分配的端口总数
Extend port block	是否为增量端口块： • Y：表示是增量端口块

字段	描述
	• N：表示非增量端口块
Total mappings found	当前查找到的端口块表项的个数

1.1.13 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

【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
    Failover group name: nat
    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
    Failover group name: trans
    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
    Failover group name: nat
    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
    Failover group name: nat
    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
Failover group name	NAT端口块组绑定的备份组的名称。如果未配置，则不显示
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“---”

字段	描述
VPN instance	私网IP地址成员所属的VPN实例。如果未配置，则显示“---”

【相关命令】

- **nat port-block-group**

1.1.14 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

【举例】

显示 NAT 内部服务器的信息。

```
<Sysname> display nat server
NAT internal server information:
  Totally 4 internal servers.
  Interface: GigabitEthernet1/0/3
    Protocol: 6(TCP)
    Global IP/port: 50.1.1.1/23
    Local IP/port : 192.168.10.15/23
    Service card  : ---
    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
    Service card  : ---
    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
  Service card  : Slot 5
  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
  Service card  : Slot 5
  Config status : Active
```

表1-13 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
Global VPN	外网地址所属的MPLS L3VPN的VPN实例名称。如果不属于任何VPN实例，则不显示该字段
Local VPN	内网地址所属的MPLS L3VPN的VPN实例名称。 如果不属于任何VPN实例，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
Service card	显示提供NAT处理的业务板。如果接口下未指定业务板，则显示为“---”
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**

1.1.15 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

【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1-14 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**

1.1.16 display nat session

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

【命令】

独立运行模式：

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

IRF 模式：

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

source-ip *source-ip*：显示指定源地址的会话。*source-ip* 表示源地址，该地址必须是创建会话的报文的源地址。

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

vpn-instance *vpn-instance-name*：显示指定目的 VPN 实例的会话。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。该 VPN 实例必须是报文中携带的 VPN 实例。如果不指定该参数，则显示目的 IP 不属于任何 VPN 实例的会话。

slot *slot-number*：显示指定单板上的 NAT 会话，*slot-number* 表示单板所在的槽位号。若不指定该参数，则显示所有单板上的 NAT 会话（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备的指定单板上的 NAT 会话，*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。若不指定该参数，则显示所有成员设备的所有单板上的 NAT 会话。（IRF 模式）

brief：显示 NAT 会话的简要信息。

verbose：显示 NAT 会话的详细信息。若不指定该参数，则显示会话的概要信息。

【使用指导】

如果不指定任何参数，则显示所有的 NAT 会话的详细信息。

【举例】

显示指定 slot 上 NAT 会话的详细信息。

```
<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/VLL ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
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/VLL ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
State: TCP_SYN_SENT
Application: SSH
Role: Standby
Failover group ID: 1
Start time: 2017-10-18 11:22:45
Initiator->Responder:         1 packets         48 bytes
Responder->Initiator:         0 packets          0 bytes

Total sessions found: 1
```

显示指定 slot 上 NAT 会话的简要信息。

```
<Sysname> display nat session slot 1 brief
Slot 1:
Protocol   Source IP/port      Destination IP/port    Global IP/port
TCP        10.2.1.58/2477      20.1.1.2/1025          30.2.4.9/226
Total sessions found: 1
```

表1-15 display nat session 命令显示信息描述表

字段	描述
Source IP/port	源IP地址/端口号

字段	描述
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/VLL ID	会话所属的MPLS L3VPN/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
Inbound interface	报文的入接口
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
Role	slot在备份组中的角色： • Master：备份组的主节点 • Standby：备份组的备节点
Failover group ID	备份组ID，当备份组中的主节点处理业务时，备节点上创建了会话，此时显示为“-”
Start time	会话创建时间
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	当前查找到的会话的总数
Source IP/port	发起方的源IP地址/端口号
Destination IP/port	发起方的目的IP地址/端口号
Global IP/port	公网IP地址/端口号

【相关命令】

- **reset nat session**

1.1.17 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

【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 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
    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
    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
    Service card : Slot 5
    Config status: Active

  Interface: GigabitEthernet1/0/3
    Service card : ---
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: local VPN, global VPN, and ACL.
```

表1-16 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* 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

字段	描述
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MPLS L3VPN的VPN实例名称。如果不属于任何VPN实例，则不显示该字段
Global VPN	外网地址所属的MPLS L3VPN的VPN实例名称。如果不属于任何VPN实例，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
Service card	显示提供NAT服务的业务板。如果接口下未指定业务板，则显示为“---”
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**

1.1.18 display nat statistics

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

【命令】

独立运行模式：

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

IRF 模式：

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-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*：显示指定单板上的 NAT 统计信息，*slot-number* 表示单板所在的槽位号。若不指定该参数，则显示所有单板上的 NAT 统计信息。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备的指定单板上的 NAT 统计信息，*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。若不指定该参数，则显示所有成员设备的所有单板上的 NAT 统计信息。（IRF 模式）

【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
  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1-17 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
Total EIM entries	EIM表项个数
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1-18 display nat statistics summary 命令显示信息描述表

字段	描述
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

1.1.19 failover-group

failover-group 命令用来配置 NAT 地址组或 NAT 端口块组与备份组绑定。

undo failover-group 命令用来恢复缺省情况。

【命令】

failover-group *group-name* [**user-group** *user-group-name*]

undo failover-group

【缺省情况】

NAT 地址组或 NAT 端口块组未绑定任何备份组。

【视图】

NAT 地址组视图

NAT 端口块组视图

【缺省用户角色】

network-admin

【参数】

group-name：备份组的名称，为 1～63 个字符的字符串，区分大小写。绑定的备份组可以不存在，但要使配置生效，必须通过 **failover group** 命令创建备份组。

user-group *user-group-name*：指定与备份组绑定的用户组的名称，为 1～32 个字符的字符串，不区分大小写。

【使用指导】

使用 CGN 单板提供 NAT 功能的环境中，对于动态地址转换或 NAT 端口块地址转换，需要将 NAT 地址组与节点为 CGN 单板的备份组绑定。

NAT 地址组或 NAT 端口块组与备份组绑定后，不能通过 **nat service** 命令来指定处理 NAT 业务的 slot。

在 NAT 控制与转发分离的组网环境中，DP 设备上需要将 NAT 地址组与备份组绑定，并指定用户组（指定的用户组可以不存在，但要使配置生效，必须通过 **user-group** 命令创建用户组）。当 PPPoE 或 IPoE 用户上线成功后，DP 设备通过用户的用户组将用户流量引到该用户组绑定的备份组，在备份组的主节点上进行地址转换。关于备份组的详细介绍，请参见“可靠性配置指导”中的“备份组”；关于用户组的详细介绍，请参见“BRAS 业务配置指导”中的“AAA”。

【举例】

将 NAT 地址组与名称为 nat-failover 的备份组绑定。

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

将 NAT 端口块组与名称为 nat-failover 的备份组绑定。

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

【相关命令】

- **failover group**（可靠性命令参考/备份组）
- **nat service**
- **user-group**（BRAS 业务命令参考/AAA）

1.1.20 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

【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 NAT 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，一次添加的公网地址成员的数量不能超过 255 个，且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。

如果公网地址成员与 NAT 端口块静态映射中的公网地址成员重叠，请确保 NAT 端口块静态映射中的端口范围与 NAT 端口块动态映射中的端口范围不重叠。否则当用户上线时，如果设备为两个不同的用户分配了相同的公网 IP 地址和端口块，可能会导致无法为其中一个用户创建 NAT 会话。

【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**

1.1.21 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

【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。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**

1.1.22 local-ip-address

local-ip-address 命令用来添加私网地址成员。

undo local-ip-address 命令用来删除私网地址成员。

【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

【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 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 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 实例。

【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。

同一个端口块组内，可配置多个私网地址成员：

- 属于同一 VPN 实例的各私网地址成员之间的 IP 地址不能重叠。
- 不属于任何 VPN 实例的私网地址成员之间的 IP 地址不能重叠。

不同端口块组内，执行本命令且指定相同的 VPN 实例时，配置的私网地址成员的 IP 地址不要重叠，否则可能导致无法正确处理 NAT 业务。

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 NAT 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 实例为 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**

1.1.23 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*

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

【参数】

group-id：地址组编号，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。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。

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

【相关命令】

- **address**

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

1.1.24 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】

FTP 协议、ICMP 差错控制报文和 RTSP 协议的 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

【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**

1.1.25 nat centralized-backup enable

nat centralized-backup enable 命令用来开启集中式备份分布式 CGN 功能。

undo nat centralized-backup enable 命令用来关闭集中式备份分布式 CGN 功能。

【命令】

nat centralized-backup enable

undo nat centralized-backup enable

【缺省情况】

集中式备份分布式 CGN 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

在集中式备份分布式 CGN 组网环境中，开启本功能后，当 BRAS 设备的 CGN 业务板故障时，已上线的用户不会下线。

【举例】

开启集中式备份分布式 CGN 功能。

```
<Sysname> system-view
[Sysname] nat centralized-backup enable
```

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

【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 extended-port-block report-radius enable

nat extended-port-block report-radius enable 命令用来开启 NAT 设备将用户私网 IP 与扩展端口块的映射关系上报给 RADIUS 服务器的功能。

undo nat extended-port-block report-radius enable 命令用来恢复缺省情况。

【命令】

nat extended-port-block report-radius enable

undo nat extended-port-block report-radius enable

【缺省情况】

NAT 设备将用户私网 IP 与扩展端口块的映射关系上报给 RADIUS 服务器的功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

network-operator

【使用指导】

在 NAT 与 BRAS 联动的场景中，用户通过 RADIUS 认证并分配得到私网地址之后，设备会为其预先分配公网 IP 和端口块，并创建地址映射关系，然后通过 RADIUS 报文将上线用户获得的私网 IP 地址及其对应的公网 IP 和端口块等信息上报给 RADIUS 服务器。RADIUS 服务器获得用户的地址映射关系后，将这些信息记录到在线用户信息中，以提供用户溯源服务。之后，如果用户向公网发起的连接使用了增量端口块，设备并不会将私网 IP 地址及其对应的公网 IP 和扩展端口块等信息上报给 RADIUS 服务器，导致无法对使用增量端口块的用户进行溯源。开启本功能可以避免上述问题的产生。

当存在 PPPoE 或 IPoE 在线用户时，无法改变本功能的开启或关闭状态。

【举例】

开启 NAT 设备将用户私网 IP 与增量端口块的映射关系上报给 RADIUS 服务器的功能。

```
<Sysname> system-view
[Sysname] nat address-group 2
[Sysname-address-group-2] port-block block-size 256 extended-block-number 1
[Sysname-address-group-2] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat outbound 2001 address-group 2
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] nat extended-port-block report-radius enable
```

【相关命令】

- **port-block block-size**

1.1.28 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

【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**

1.1.29 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

【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 NAT444 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 flow-active**
- **nat log flow-begin**
- **nat log flow-end**
- **nat log port-alloc-fail**
- **nat log port-block-alloc-fail**
- **nat log port-block-assign**
- **nat log port-block-withdraw**

1.1.30 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

【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（通过 **nat log enable** 命令）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**

1.1.31 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

【使用指导】

只有开启 NAT 日志功能（通过 **nat log enable** 命令）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**

1.1.32 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

【使用指导】

只有开启 NAT 日志功能（通过 **nat log enable** 命令）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**

1.1.33 nat log port-alloc-fail

nat log port-alloc-fail 命令用来开启 NAT 端口分配失败的日志功能。

undo nat log port-alloc-fail 命令用来关闭 NAT 端口分配失败的日志功能。

【命令】

nat log port-alloc-fail

undo nat log port-alloc-fail

【缺省情况】

NAT 端口分配失败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

【使用指导】

开启本功能后，当动态方式的 NAT 地址转换发生端口分配失败的情况时，系统会输出端口分配失败的日志。通常，端口块中所有的端口资源都被占用时会导致端口分配失败。

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

【举例】

开启 NAT 端口分配失败的日志功能。

```
<Sysname> system-view
[Sysname] nat log port-alloc-fail
```

【相关命令】

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

1.1.34 nat log port-block port-usage threshold

nat log port-block port-usage threshold 命令用来开启 NAT 端口块中端口使用率的日志信息功能，并设置 NAT 端口使用率的阈值。

undo nat log port-block port-usage threshold 命令用来关闭 NAT 端口块中端口使用率的日志信息功能。

【命令】

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

undo nat log port-block port-usage threshold

【缺省情况】

NAT 端口块中端口使用率的日志信息功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

value：告警阈值，取值范围为 40～100，单位为百分比。

【使用指导】

开启本功能后，当端口块中端口数的使用率超过设定的百分比时，系统将会输出日志信息。

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

【举例】

开启 NAT 端口块中端口使用率的日志信息功能，并设置 NAT 端口使用率的阈值为 90%。

```
<Sysname> system-view
[Sysname] nat log port-block port-usage threshold 90
```

【相关命令】

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

1.1.35 nat log port-block usage threshold

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

undo nat log port-block usage threshold 命令恢复缺省情况。

【命令】

nat log port-block usage threshold *value*

undo nat log port-block usage threshold

【缺省情况】

NAT 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

【参数】

value：端口使用率的阈值，取值范围为 40～100，单位为百分比。

【使用指导】

当端口块的使用率超过设定的百分比时，系统将会输出日志信息。

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

【举例】

配置 NAT 端口块的使用率告警阈值为 80%。

```
<Sysname> system-view
[Sysname] nat log port-block usage threshold 80
```

【相关命令】

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

1.1.36 nat log port-block-alloc-fail

nat log port-block-alloc-fail 命令用来开启 NAT 端口块分配失败的日志功能。

undo nat log port-block-alloc-fail 命令用来关闭 NAT 端口块分配失败的日志功能。

【命令】

nat log port-block-alloc-fail

undo nat log port-block-alloc-fail

【缺省情况】

NAT 端口块分配失败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

【使用指导】

开启本功能后，当 NAT 端口块地址转换发生端口块分配失败的情况时，系统会输出端口块分配失败的日志。

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

【举例】

开启 NAT 端口块分配失败的日志功能。

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

【相关命令】

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

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

【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（通过 **nat log enable** 命令）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

【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（通过**nat log enable**命令）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 endpoint-independent

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

undo nat mapping-behavior endpoint-independent命令用来恢复缺省情况。

【命令】

nat mapping-behavior endpoint-independent { tcp [tcp-5-tuple] | udp [udp-5-tuple] } *

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Connection-Dependent Mapping。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

tcp：表示配置设备为传输层协议类型为TCP的报文在PAT方式出方向地址转换创建EIM表项。

udp：表示配置设备为传输层协议类型为UDP的报文在PAT方式出方向地址转换创建EIM表项。

tcp-5-tuple：表示配置设备为传输层协议类型为 TCP 的报文在 PAT 方式出方向地址转换中创建五元组（源地址、源端口号、协议类型、目的地址、目的端口号）类型的会话表项。如果不指定该参数，则表示仅创建 EIM 表项。

udp-5-tuple：表示配置设备为传输层协议类型为 UDP 的报文在 PAT 方式出方向地址转换中创建五元组（源地址、源端口号、协议类型、目的地址、目的端口号）类型的会话表项。如果不指定该参数，则表示仅创建 EIM 表项。

【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。
- Connection-Dependent Mapping（关心对端地址和端口的非共享转换模式）：来自同一源地址和源端口号并且去往特定目的地址和端口号的报文，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。同一源地址和源端口号并且去往不同目的地址和端口号的报文，通过 PAT 映射后，其源地址和源端口号被转换为不同的外部地址和端口号。与 Endpoint-Independent Mapping 模式不同的是，这种模式安全性好，即 NAT 设备只允许这些目的地址对应的外部网络的主机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。

存在 **nat server**、**nat static outbound**、**nat static outbound net-to-net** 中任意一种或几种配置的情况下，无法配置 **nat mapping-behavior endpoint-independent tcp** 和 **nat mapping-behavior endpoint-independent udp** 命令。

配置本命令后，对于 ICMP 报文，始终会创建 EIM 表项和五元组类型的会话表项。

【举例】

对 TCP 报文以 Endpoint-Independent Mapping 模式进行地址转换，且仅创建 EIM 表项。

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

【相关命令】

- **display nat eim**
- **display nat eim statistics**
- **nat outbound**
- **nat server**
- **nat static outbound**
- **nat static outbound net-to-net**

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* [**vpn-instance** *vpn-instance-name*] **no-pat** [**reversible**]

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*] [**vpn-instance** *vpn-instance-name*] [**port-preserved**]

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

【视图】

接口视图

【缺省用户角色】

network-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 *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。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。

vpn-instance *vpn-instance-name*：指定地址组中的地址所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 中的 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 实例。

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。**port-preserved** 参数对 NAT444 端口块动态映射无效。

【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，一个接口下可同时配置多条出方向地址转换。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。NAT 端口块动态映射不支持该方式。

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 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范围和端口块参数，则将对匹配的报文进行 NAT 端口块动态映射。

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。
- NAT 端口块动态映射环境下，在同一接口下新增出方向动态转换的配置时，如果已经有流量与已存在配置中的 ACL 规则匹配，那么新增配置中的 ACL 规则不要与已存在配置中的 ACL 规则有重叠。

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。

【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

【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 2000～3999。

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。

【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。

通过在 NAT 网关设备上配置 DS-Lite B4 地址转换，可以实现基于端口块的公网 IP 地址复用，使一个 DS-Lite B4 IPv6 地址在一个时间段内独占一个公网 IP 地址的某个端口块。

【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 gigabitethernet 1/0/1
[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 easy-ip failover-group

nat outbound easy-ip failover-group 命令用来为 Easy IP 方式的动态地址转换指定备份组。

undo nat outbound easy-ip failover-group 命令用来恢复缺省情况。

【命令】

nat outbound easy-ip failover-group *group-name*

undo nat outbound easy-ip failover-group

【缺省情况】

没有为 Easy IP 方式的动态地址转换指定备份组。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

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

【使用指导】

配置该命令后，设备会将需要进行动态地址转换的流量引到指定的备份组进行处理。

如果设备上创建了手动备份组，则只能指定手动备份组，不允许再指定自动备份组。

本命令与 **nat service** 命令互斥，不能同时配置。

【举例】

在接口 GigabitEthernet1/0/1 上为出方向动态地址转换指定名字为 nat-failover 的备份组。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat outbound easy-ip failover-group nat-failover
```

【相关命令】

- **display nat outbound**
- **nat service**

1.1.43 nat outbound port-block-group

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

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

【命令】

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

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

【缺省情况】

不存在 NAT 端口块静态映射配置。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

group-id：端口块组的编号，取值范围为 0～65535。

【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 NAT 端口块静态映射。

【举例】

在接口 GigabitEthernet1/0/1 的出方向上配置基于端口组 1 的 NAT 端口块静态映射。

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

【相关命令】

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

1.1.44 nat port-block flow-trigger enable

nat port-block flow-trigger enable 命令用来开启流量触发分配端口块功能。

undo nat port-block flow-trigger enable 命令用来关闭流量触发分配端口块功能。

【命令】

nat port-block flow-trigger enable

undo nat port-block flow-trigger enable

【缺省情况】

流量触发分配端口块功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

此命令只用于集中式备份分布式 CGN 组网环境中。当 BRAS 设备的 CGN 业务板故障时，只有在集中式部署 CGN 的设备上开启此功能，设备才能为用户分配地址和端口块资源。

【举例】

开启流量触发分配端口块功能。

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

1.1.45 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

【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 NAT 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 NAT 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**

1.1.46 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**]

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* }]

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* }]

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* }]

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* }]

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*]

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

【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：指定服务器向外提供服务的外网信息。

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 256。*global-address1* 表示起始地址，*global-address2* 表示结束地址。*global-address2* 必须大于 *global-address1*。

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：使用当前接口的主用 IP 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主用 IP 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 256。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。

inside：指定服务器的内网信息。

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 实例。*global-vpn-instance-name* 表示 MPLS L3VPN 的 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 实例。

vpn-instance *local-vpn-instance-name*：内部服务器所属的 VPN 实例。*local-vpn-instance-name* 表示 MPLS L3VPN 的 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 实例。

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。

【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 MPLS 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1-19 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

外网	内网
	• 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。

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。

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。

【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 MPLS VPN 实例 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 实例 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 MPLS VPN 实例 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**

1.1.47 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

【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**

1.1.48 nat service

nat service 命令用来指定处理 NAT 业务的 slot。

undo nat service 命令用来恢复缺省情况。

【命令】

独立运行模式：

nat service slot *slot-number*

undo nat service slot

IRF 模式：

nat service chassis *chassis-number* **slot** *slot-number*

undo nat service chassis

【缺省情况】

未指定处理 NAT 业务的 slot。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

slot *slot-number*：指定单板所在的槽位号。*slot-number* 表示单板所在的槽位号。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：指定单板。*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。（IRF 模式）

【使用指导】

对于支持本命令的设备，必须在配置了 NAT 业务的接口上指定提供 NAT 处理的 slot。否则接口的 NAT 功能不生效。

一个接口上的 NAT 业务只能由一个 slot 处理，该 slot 可以是设备上的任意可提供 NAT 处理的 slot。通常，如果接口所在的 slot 具有 NAT 处理能力，那么建议将接口所在 slot 指定为处理 NAT 业务的 slot。

多个接口引用了同一个地址组或外网地址时，这些接口必须指定同一个 slot 进行 NAT 处理。否则，可能会出现配置成功但实际不生效的情况，并且在配置恢复（由设备重启、软件升级等原因导致）时可能会造成配置丢失。

在接口上，不能通过重复执行本命令来修改接口上指定处理 NAT 业务的 slot。如需修改，请先通过 **undo nat service** 命令取消指定的 slot，再执行 **nat service** 命令。

接口上配置本命令后，该接口的动态地址转换（包括出方向动态地址转换、Easy IP 方式的动态地址转换和 NAT 端口块动态映射）和 NAT 端口块静态映射中，不能将地址组/端口块组与备份组绑定。

【举例】

指定 slot 5 作为提供 NAT 业务处理的 slot。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat service slot 5
```

【相关命令】

- **failover-group**

1.1.49 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

【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**

1.1.50 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**]] [**failover-group** *group-name*]

undo nat static outbound *local-ip* [**vpn-instance** *local-vpn-instance-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

【参数】

local-ip：内网 IP 地址。

vpn-instance *local-vpn-instance-name*：内网 IP 地址所属的 VPN 实例。*local-vpn-instance-name* 表示 MPLS L3VPN 的 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 实例。

global-ip：外网 IP 地址。

vpn-instance *global-vpn-instance-name*：外网 IP 地址所属的 VPN 实例。*global-vpn-instance-name* 表示 MPLS L3VPN 的 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 实例。

acl：指定 ACL 的编号或名称，本参数用于控制内网主机可以访问的目的地址。

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。

failover-group *group-name*：指定该地址转换映射绑定的备份组。*group-name* 表示备份组的名称，为 1～63 个字符的字符串，区分大小写。有关备份组的详细介绍，请参见“可靠性配置指导”中的“备份组”。

【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。

使用 CGN 单板处理 NAT 业务的环境中，需要将出方向一对一静态地址转换映射与节点为 CGN 单板的备份组绑定，否则会导致反向报文地址转换失败。

【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**

1.1.51 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**]] [**failover-group** *group-name*]

undo nat static outbound net-to-net *local-start-address local-end-address* [**vpn-instance** *local-vpn-instance-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

【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实例。*local-vpn-instance-name* 表示MPLS L3VPN的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实例。

global-network：外网网段地址。

vpn-instance *global-vpn-instance-name*：外网IP地址所属的VPN实例。*global-vpn-instance-name* 表示MPLS L3VPN的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实例。

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。

acl：指定ACL的编号或名称，本参数用于控制内网主机可以访问的目的地址。

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。

failover-group *group-name*：指定该地址转换映射绑定的备份组。*group-name* 表示备份组的名称，为 1～63 个字符的字符串，区分大小写。有关备份组的详细介绍，请参见“可靠性配置指导”中的“备份组”。

【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。

使用 CGN 单板处理 NAT 业务的环境中，需要将出方向网段到网段的静态地址转换映射与节点为 CGN 单板的备份组绑定，否则会导致反向报文地址转换失败。

【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**

1.1.52 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/地址池的端口块参数。

【视图】

NAT 地址组视图

【缺省用户角色】

network-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**

1.1.53 port-limit

port-limit 命令用来限制分配给协议的端口数量。

undo port-limit 命令用来取消分配给协议的端口数量的限制。

【命令】

port-limit { **icmp** | **tcp** | **total** | **udp** } *number*

undo port-limit { **icmp** | **tcp** | **total** | **udp** }

【缺省情况】

不对分配给协议的端口数量做限制。

【视图】

NAT 地址组视图

NAT 端口块组视图

【缺省用户角色】

network-admin

【参数】

icmp：限制分配给 ICMP 协议的端口数量。

tcp：限制分配给 TCP 协议的端口数量。

total：限制分配给所有协议的端口数量。

udp：限制分配给 UDP 协议的端口数量。

number：指定最多分配给协议的端口数量，取值范围为 0～65535。

【举例】

配置地址组 1 最多可分配给 TCP 协议的端口数量为 10。

```
<Sysname> system-view
[Sysname] nat address-group 1
[Sysname-address-group-1] port-limit tcp 10
```

配置端口块组 1 最多可分配给 TCP 协议的端口数量为 10。

```
<Sysname> system-view
[Sysname] nat port-block-group 1
[Sysname-port-block-group-1] port-limit tcp 10
```

【相关命令】

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

1.1.54 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

【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*。建议将 *start-port-number* 配置为大于或等于 1024 的数值，避免出现应用协议识别错误的问题。

【使用指导】

在 NAT 地址组/NAT 端口块组视图下配置端口范围后，该 NAT 地址组/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/地址池配置了端口块参数，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**

1.1.55 reset nat eim

reset nat eim 命令用来删除 NAT EIM 表项信息。

【命令】

独立运行模式：

reset nat eim [**protocol** { **tcp** | **udp** }] [**slot** *slot-number*]

IRF 模式：

reset nat eim [**protocol** { **tcp** | **udp** }] [**chassis** *chassis-number* **slot** *slot-number*]

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

protocol：删除指定协议类型的 EIM 表项信息。如果未指定本参数，则表示删除所有协议类型的 EIM 表项信息。

tcp：删除 TCP 协议类型的 EIM 表项信息。

udp：删除 UDP 协议类型的 EIM 表项信息。

slot *slot-number*：删除指定单板上的 EIM 表项信息，*slot-number* 表示单板所在的槽位号。若不指定该参数，则表示删除所有单板上的 EIM 表项信息。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：删除指定单板上的 EIM 表项信息，*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。若不指定该参数，则表示删除所有单板上的 EIM 表项信息。（IRF 模式）

【举例】

删除指定 slot 上的 NAT EIM 表项信息。

```
<Sysname> reset nat eim slot 1
```

【相关命令】

- **display nat eim**
- **display nat eim statistics**
- **nat mapping-behavior**

1.1.56 reset nat session

reset nat session 命令用来删除 NAT 会话。

【命令】

独立运行模式：

reset nat session [**protocol** { **tcp** | **udp** }] [**slot** *slot-number*]

IRF 模式：

reset nat session [**protocol** { **tcp** | **udp** }] [**chassis** *chassis-number* **slot** *slot-number*]

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

protocol：删除指定协议类型的 NAT 会话。如果未指定本参数，则表示删除所有协议类型的 NAT 会话。

tcp：删除 TCP 协议类型的 NAT 会话。

udp：删除 UDP 协议类型的 NAT 会话。

slot *slot-number*：删除指定单板上的 NAT 会话，*slot-number* 表示单板所在的槽位号。如果不指定该参数，则表示删除所有单板上的 NAT 会话。（独立运行模式）。

chassis *chassis-number* **slot** *slot-number*：删除指定成员设备上指定单板的 NAT 会话，*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。如果不指定该参数，则表示删除所有成员设备的所有单板上的 NAT 会话。（IRF 模式）

【使用指导】

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

【举例】

删除指定 slot 上的 NAT 会话。

```
<Sysname> reset nat session slot 1
```

【相关命令】

- **display nat session**