# 目 录

# 1 NAT

## 1.1 NAT简介

NAT（Network Address Translation，网络地址转换）是将 IP 数据报文头中的 IP 地址转换为另一个 IP 地址的过程。在实际应用中，NAT 主要应用在连接两个网络的边缘设备上，用于实现允许内部网络用户访问外部公共网络以及允许外部公共网络访问部分内部网络资源（例如内部服务器）的目的。NAT 最初的设计目的是实现私有网络访问公共网络的功能，后扩展为实现任意两个网络间进行访问时的地址转换应用。

NAT可以让少量的外网网络IP地址代表较多的内部网络IP地址，这种地址转换能力具备以下优点：

- 私有网络内部的通信利用私网地址，如果私有网络需要与外部网络通信或访问外部资源，则可通过将大量的私网地址转换成少量的公网地址来实现，这在一定程度上缓解了 IPv4 地址空间日益枯竭的压力。
- 地址转换可以利用端口信息，通过同时转换公网地址与传输层端口号，使得多个私网用户可共用一个公网地址与外部网络通信，节省了公网地址。
- 通过静态映射，不同的内部服务器可以映射到同一个公网地址。外部用户可通过公网地址和端口访问不同的内部服务器，同时还隐藏了内部服务器的真实 IP 地址，从而防止外部对内部服务器乃至内部网络的攻击。
- 方便网络管理，例如私网服务器迁移时，无需过多配置的改变，仅仅通过调整内部服务器的映射表就可将这一变化体现出来。

### 1.1.1 NAT工作机制

配置了 NAT 功能的连接内部网络和外部网络的边缘设备，通常被称为 NAT 设备。当内部网络访问外部网络的报文经过 NAT 设备时，NAT 设备会用一个合法的公网地址替换原报文中的源 IP 地址，并对这种转换进行记录；之后，当报文从外网侧返回时，NAT 设备查找原有的记录，将报文的目的地址再替换回原来的私网地址，并转发给内网侧主机。这个过程，在私网侧或公网侧设备看来，与普通的网络访问并没有任何的区别。

#### 1. 基本概念

- NAT 接口：NAT 设备上应用了 NAT 相关配置的接口。
- NAT 规则：用于进行地址转换的 NAT 配置称为 NAT 规则。
- NAT 地址：用于进行地址转换的 IP 地址，与外部网络路由可达，可静态指定或动态分配。
- NAT 表项：NAT 设备上用于记录网络地址转换映射关系的表项。
- Easy IP 功能：NAT 转换时直接使用设备上接口的 IP 地址作为 NAT 地址。设备上接口的地址可通过 DHCP 或 PPPoE 等协议动态获取，因此对于支持 Easy IP 的 NAT 配置，不直接指定 NAT 地址，而是指定对应的接口或当前接口。

#### 2. NAT的基本组网类型

(1) 传统 NAT

报文经过 NAT 设备时，在 NAT 接口上仅进行一次源 IP 地址转换或一次目的 IP 地址转换。对于内网访问外网的报文，在出接口上进行源 IP 地址转换；对于外网访问内网的报文，在入接口上进行目的地址 IP 地址转换。

(2) 两次 NAT

报文入接口和出接口均为 NAT 接口。报文经过 NAT 设备时，先后进行两次 NAT 转换。对于内网访问外网的报文和外网访问内网的报文，均在入接口进行目的 IP 地址转换，在出接口进行源 IP 地址转换。

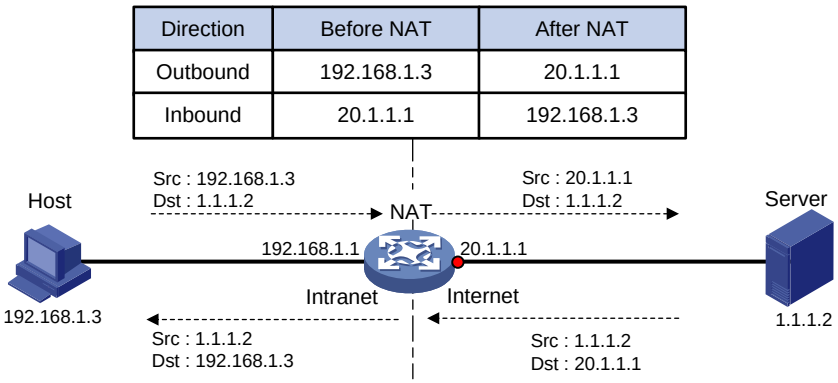
(3) 双向 NAT

报文经过 NAT 设备时，在 NAT 接口上同时进行一次源 IP 地址转换和一次目的 IP 地址转换。对于内网访问外网的报文，在出接口上同时进行源 IP 地址和目的 IP 地址的转换；对于外网访问内网的报文，同时在入接口上进行目的地址 IP 地址和源 IP 地址的转换。这种方式常用于支持内网用户主动访问与之地址重叠的外网资源。

### 3. 传统NAT的典型工作过程

如 图 1-1 所示，一台NAT设备连接内网和外网，连接外网的接口为NAT接口，当有报文经过NAT设备时，NAT的基本工作过程如下。

图1-1 NAT 基本工作过程示意图




(1) 当内网用户主机（192.168.1.3）向外网服务器（1.1.1.2）发送的 IP 报文通过 NAT 设备时，NAT 设备查看报文的 IP 头内容，发现该报文是发往外网的，则将其源 IP 地址字段的内网地址 192.168.1.3 转换成一个可路由的外网地址 20.1.1.1，并将该报文发送给外网服务器，同时在 NAT 设备上建立表项记录这一映射。

(2) 外网服务器给内网用户发送的应答报文到达 NAT 设备后，NAT 设备使用报文信息匹配建立的表项，然后查找匹配到的表项记录，用内网私有地址 192.168.1.3 替换初始的目的 IP 地址 20.1.1.1。

上述的 NAT 过程对终端（如图中的 Host 和 Server）来说是透明的。对外网服务器而言，它认为内网用户主机的 IP 地址就是 20.1.1.1，并不知道有 192.168.1.3 这个地址。因此，NAT“隐藏”了企业的私有网络。

### 1.1.2 NAT转换控制

在实际应用中，我们可能希望某些内部网络的主机可以访问外部网络，而某些主机不允许访问；或者希望某些外部网络的主机可以访问内部网络，而某些主机不允许访问。即 NAT 设备只对符合要求的报文进行地址转换。

NAT 设备可以利用 ACL（Access Control List，访问控制列表）来对地址转换的使用范围进行控制，通过定义 ACL 规则，并将其与 NAT 配置相关联，实现只对匹配指定的 ACL permit 规则的报文才进行地址转换的目的。而且，NAT 仅使用规则中定义的源 IP 地址、源端口号、目的 IP 地址、目的端口号和传输层协议类型这几个元素进行报文匹配，忽略其它元素。

### 1.1.3 NAT实现方式

#### 1. 静态方式

静态地址转换是指外部网络和内部网络之间的地址映射关系由配置确定，该方式适用于内部网络与外部网络之间存在固定访问需求的组网环境。静态地址转换支持双向互访：内网用户可以主动访问外网，外网用户也可以主动访问内网。

#### 2. 动态方式

动态地址转换是指内部网络和外部网络之间的地址映射关系在建立连接的时候动态产生。该方式通常适用于内部网络有大量用户需要访问外部网络的组网环境。动态地址转换存在两种转换模式：

- NO-PAT 模式

NO-PAT（Not Port Address Translation）模式下，一个外网地址同一时间只能分配给一个内网地址进行地址转换，不能同时被多个内网地址共用。当使用某外网地址的内网用户停止访问外网时，NAT 会将其占用的外网地址释放并分配给其他内网用户使用。

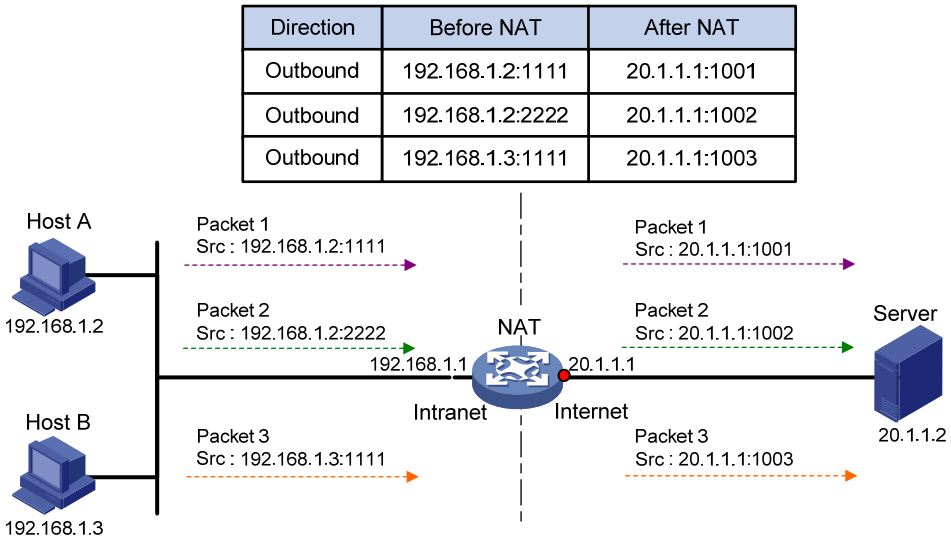
该模式下，NAT 设备只对报文的 IP 地址进行 NAT 转换，同时会建立一个 NO-PAT 表项用于记录 IP 地址映射关系，并可支持所有 IP 协议的报文。

- PAT 模式

PAT（Port Address Translation）模式下，一个 NAT 地址可以同时分配给多个内网地址共用。该模式下，NAT 设备需要对报文的 IP 地址和传输层端口同时进行转换，且只支持 TCP、UDP 和 ICMP（Internet Control Message Protocol，互联网控制消息协议）查询报文。

图 1-2 描述了PAT的基本原理。

图1-2 PAT 基本原理示意图




如 图 1-2 所示，三个带有内网地址的报文到达NAT设备，其中报文 1 和报文 2 来自同一个内网地址但有不同的源端口号，报文 1 和报文 3 来自不同的内网地址但具有相同的源端口号。通过PAT映射，三个报文的源IP地址都被转换为同一个外网地址，但每个报文都被赋予了不同的源端口号，因而仍保留了报文之间的区别。当各报文的回应报文到达时，NAT设备仍能够根据回应报文的目的IP地址和目的端口号来区别该报文应转发到的内部主机。

采用 PAT 方式可以更加充分地利用 IP 地址资源，实现更多内部网络主机对外部网络的同时访问。目前，PAT 支持两种不同的地址转换模式：

- Endpoint-Independent Mapping（不关心对端地址和端口转换模式）：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 设备允许所有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 网关之后的主机进行互访。
- Address and Port-Dependent Mapping（关心对端地址和端口转换模式）：对于来自相同源地址和源端口号的报文，相同的源地址和源端口号并不要求被转换为相同的外部地址和端口号，若其目的地址或目的端口号不同，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。与 Endpoint-Independent Mapping 模式不同的是，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。这种模式安全性好，但由于同一个内网主机地址转换后的外部地址不唯一，因此不便于位于不同 NAT 网关之后的主机使用内网主机转换后的地址进行互访。

## 1.1.4 NAT表项

### 1. NAT会话表项

NAT 设备处理一个连接的首报文时便确定了相应的地址转换关系，并同时创建会话表项，该会话表项中添加了 NAT 扩展信息（例如接口信息、转换方式）。会话表项中记录了首报文的地址转换信息。这类经过 NAT 处理的会话表项，也称为 NAT 会话表项。

当该连接的后续报文经过 NAT 设备时，将与 NAT 会话表项进行匹配，NAT 设备从匹配到的会话表项中得到首报文的转换方式，并根据首报文的转换方式对后续报文进行处理。后续报文方向与首报文相同时，源和目的的转换方式与首报文相同；方向相反时，转换方式与首报文相反。即，如果首报文转换了源地址，则后续报文需要转换目的地址；如果首报文转换了目的地址，则后续报文需要转换源地址。

NAT 会话表项的更新和老化由会话管理模块维护，关于会话管理的相关介绍请参见“安全配置指导”中的“会话管理”。

#### 2. EIM表项

如果 NAT 设备上开启了 Endpoint-Independent Mapping 模式，则在 PAT 方式的动态地址转换过程中，会首先创建一个 NAT 会话表项，然后创建一个 EIM 表项用于记录地址和端口的转换关系（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。

该表项在与其相关联的所有 NAT 会话表项老化后老化。

#### 3. NO-PAT表项

在NO-PAT方式进行源地址的动态转换过程中，NAT设备首先创建一个NAT会话表项，然后建立一个NO-PAT表项用于记录该转换关系（内网地址<-->NAT地址）。除此之外，在NAT设备进行ALG处理时，也会触发创建NO-PAT表项。NAT ALG的相关介绍请参见“1.1.5 NAT支持ALG”。

NO-PAT 表项有以下两个作用：

- 保证后续来自相同源地址的新建连接与首次连接使用相同的转换关系。
- 配置了 **reversible** 参数的情况下，允许满足指定条件的主机向 NAT 地址发起的新建连接根据 NO-PAT 表项进行反向地址转换。

该表项在与其相关联的所有 NAT 会话表项老化后老化。

### 1.1.5 NAT支持ALG

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（File Transfer Protocol，文件传输协议）应用由 FTP 客户端与 FTP 服务器之间建立的数据连接和控制连接共同实现，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 的相关转换配置完成载荷信息的转换，以保证后续数据连接的正确建立。

## 1.2 NAT配置任务简介

若接口上同时存在普通 NAT 静态地址转换、普通 NAT 动态地址转换的配置，则在地址转换过程中，它们的优先级从高到低依次为：

(1) 普通 NAT 静态地址转换。

(2) 普通 NAT 动态地址转换。

表1-1 NAT 配置任务简介

| 配置任务 | 说明 | 详细配置 |
| --- | --- | --- |
| 配置静态地址转换 | 根据实际的组网需求，选择其中一种或两种转换方式<br>1. 静态地址转换适用于：转换关系完全确定<br>2. 动态地址转换 | 1.3 |
| 配置动态地址转换 | • PAT 方式适用于大量内网用户通过少量 NAT 地址访问外网<br>• NO-PAT 方式，通常仅用于配合内部服务器或静态地址转换实现双向 NAT 应用 | 1.4 |
| 调整NAT规则的匹配优先级 | 可选 | 1.5 |
| 配置NAT ALG功能 | 可选 | 1.6 |
| 配置NAT日志功能 | 可选 | 1.7 |
| 开启NAT转换失败发送ICMP差错报文功能 | 可选 | 1.8 |

## 1.3 配置静态地址转换

配置静态地址转换时，需要首先在系统视图下配置静态地址转换映射，然后在接口下使该转换映射生效。

静态地址转换映射支持两种方式：一对一静态转换映射、网段对网段静态转换映射。静态地址转换可以支持配置在接口的出方向（**nat static outbound**）或入方向（**nat static inbound**）上，入方向的静态地址转换通常用于与接口上的出方向动态地址转换（**nat outbound**）或出方向静态地址转换（**nat static outbound**）配合以实现双向 NAT，不建议单独配置。

### 1.3.1 配置准备

- 配置控制地址转换范围的 ACL。ACL 配置的相关介绍请参见“ACL 和 QoS 配置指导”中的“ACL”。需要注意的是，NAT 仅关注 ACL 规则中定义的源 IP 地址、源端口号、目的 IP 地址、目的端口号和传输层协议类型，不关注 ACL 规则中定义的其它元素。
- 对于入方向静态地址转换，需要手动添加路由：目的地址为静态地址转换配置中指定的 *local-ip* 或 *local-network*；下一跳为静态地址转换配置中指定的外网地址，或者报文出接口的实际下一跳地址。

### 1.3.2 配置出方向一对一静态地址转换

出方向一对一静态地址转换通常应用在外网侧接口上，用于实现一个内部私有网络地址到一个外部公有网络地址的转换，具体过程如下：

- 对于经过该接口发送的内网访问外网的报文，将其源 IP 地址与指定的内网 IP 地址 *local-ip* 进行匹配，并将匹配的源 IP 地址转换为 *global-ip*。
- 对于该接口接收到的外网访问内网的报文，将其目的 IP 地址与指定的外网 IP 地址 *global-ip* 进行匹配，并将匹配的目的 IP 地址转换为 *local-ip*。

如果接口上配置的静态地址转换映射中指定了 **acl** 参数，则仅对符合指定 ACL permit 规则的报文进行地址转换。

表1-2 配置出方向一对一静态地址转换

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 配置出方向一对一静态地址转换映射 | **nat static outbound** *local-ip global-ip* [ **acl** { *ipv4-acl-number* \| **name** *ipv4-acl-name* } [ **reversible** ] ] [ **rule** *rule-name* ] [ **priority** *priority* ] [ **disable** ] | 缺省情况下，不存在地址转换映射 |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 开启接口上的NAT静态地址转换功能 | **nat static enable** | 缺省情况下，NAT静态地址转换功能处于关闭状态 |

### 1.3.3 配置出方向网段对网段静态地址转换

出方向网段对网段静态地址转换通常应用在外网侧接口上，用于实现一个内部私有网络到一个外部公有网络的地址转换，具体过程如下：

- 对于经过该接口发送的内网访问外网的报文，将其源 IP 地址与指定的内网网络地址进行匹配，并将匹配的源 IP 地址转换为指定外网网络地址之一。
- 对于该接口接收到的外网访问内网的报文，将其目的 IP 地址与指定的外网网络地址进行匹配，并将匹配的目的 IP 地址转换为指定的内网网络地址之一。

如果接口上配置的静态地址转换映射中指定了 **acl** 参数，则仅对符合指定 ACL permit 规则的报文进行地址转换。

表1-3 配置出方向网段对网段静态地址转换

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 配置出方向网段对网段静态地址转换映射 | **nat static outbound net-to-net** *local-start-address local-end-address* **global** *global-network* { *mask-length* \| *mask* } [ **acl** { *ipv4-acl-number* \| **name** *ipv4-acl-name* } [ **reversible** ] ] [ **rule** *rule-name* ] [ **priority** *priority* ] [ **disable** ] | 缺省情况下，不存在地址转换映射 |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 开启接口上的NAT静态地址转换功能 | **nat static enable** | 缺省情况下，NAT静态地址转换功能处于关闭状态 |

### 1.3.4 配置入方向一对一静态地址转换

入方向一对一静态地址转换用于实现一个内部私有网络地址与一个外部公有网络地址之间的转换，具体过程如下：

- 对于经过该接口发送的内网访问外网的报文，将其目的 IP 地址与指定的内网 IP 地址 *local-ip* 进行匹配，并将匹配的目的 IP 地址转换为 *global-ip*。
- 对于该接口接收到的外网访问内网的报文，将其源 IP 地址与指定的外网 IP 地址 *global-ip* 进行匹配，并将匹配的源 IP 地址转换为 *local-ip*。

如果接口上配置的静态地址转换映射中指定了 **acl** 参数，则仅对符合指定 ACL permit 规则的报文进行地址转换。

**表1-4 配置入方向一对一静态地址转换**

| 操作 | 命令 | 说明 |
|---|---|---|
| 进入系统视图 | **system-view** | - |
| 配置入方向一对一静态地址转换映射 | **nat static inbound** *global-ip local-ip* [ **acl** { *ipv4-acl-number* \| **name** *ipv4-acl-name* } [ **reversible** ] ] [ **rule** *rule-name* ] [ **priority** *priority* ] [ **disable** ] | 缺省情况下，不存在地址转换映射 |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 开启接口上的NAT静态地址转换功能 | **nat static enable** | 缺省情况下，NAT静态地址转换功能处于关闭状态 |

### 1.3.5 配置入方向网段对网段静态地址转换

入方向网段对网段静态地址转换用于实现一个内部私有网络与一个外部公有网络之间的地址转换，具体过程如下：

- 对于经过该接口发送的内网访问外网的报文，将其目的 IP 地址与指定的内网网络地址进行匹配，并将匹配的目的 IP 地址转换为指定的外网网络地址之一。
- 对于该接口接收到的外网访问内网的报文，将其源 IP 地址与指定的外网网络地址进行匹配，并将匹配的源 IP 地址转换为指定的内网网络地址之一。

如果接口上配置的静态地址转换映射中指定了 **acl** 参数，则仅对符合指定 ACL permit 规则的报文进行地址转换。

**表1-5 配置入方向网段对网段静态地址转换**

| 操作 | 命令 | 说明 |
|---|---|---|
| 进入系统视图 | **system-view** | - |
| 配置入方向网段对网段静态地址转换映射 | **nat static inbound net-to-net** *global-start-address global-end-address* **local** *local-network* { *mask-length* \| *mask* } [ **acl** { *ipv4-acl-number* \| **name** *ipv4-acl-name* } [ **reversible** ] ] [ **rule** *rule-name* ] [ **priority** *priority* ] [ **disable** ] | 缺省情况下，不存在地址转换映射 |

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 开启接口上的NAT静态地址转换功能 | **nat static enable** | 缺省情况下，NAT静态地址转换功能处于关闭状态 |

## 1.4 配置动态地址转换

通过在接口上配置 ACL 和地址组（或接口地址）的关联即可实现动态地址转换。

- 直接使用接口的 IP 地址作为转换后的地址，即实现 Easy IP 功能。
- 选择使用地址组中的地址作为转换后的地址，根据地址转换过程中是否转换端口信息可将动态地址转换分为 NO-PAT 和 PAT 两种方式。

### 1.4.1 配置限制和指导

在同时配置了多条动态地址转换的情况下：

- 指定了 ACL 参数的动态地址转换配置的优先级高于未指定 ACL 参数的动态地址转换配置；
- 对于指定了 ACL 参数的动态地址转换配置，其优先级由 ACL 编号的大小决定，编号越大，优先级越高。

### 1.4.2 配置准备

- 配置控制地址转换范围的 ACL。ACL 配置的相关介绍请参见“ACL 和 QoS 配置指导”中的“ACL”。需要注意的是，NAT 仅关注 ACL 规则中定义的源 IP 地址、源端口号、目的 IP 地址、目的端口号和传输层协议类型，不关注 ACL 规则中定义的其它元素。
- 确定是否直接使用接口的 IP 地址作为转换后的报文源地址。
- 配置根据实际网络情况，合理规划可用于地址转换的公网 IP 地址组。
- 确定地址转换过程中是否使用端口信息。
- 对于入方向动态地址转换，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。

### 1.4.3 配置出方向动态地址转换

出方向动态地址转换通常应用在外网侧接口上，用于实现一个内部私有网络地址到一个外部公有网络地址的转换，具体过程如下：

- 对于经过该接口发送的内网访问外网的报文，将与指定 ACL permit 规则匹配的报文源 IP 地址转换为地址组中的地址。
- 在指定了 **no-pat reversible** 参数，并且已经存在 NO-PAT 表项的情况下，对于经过该接口收到的外网访问内网的首报文，将其目的 IP 地址与 NO-PAT 表项进行匹配，并将目的 IP 地址转换为匹配的 NO-PAT 表项中记录的内网地址。

表1-6 配置出方向动态地址转换

| 操作 | | 命令 | 说明 |
|---|---|---|---|
| 进入系统视图 | | **system-view** | - |
| 创建NAT地址组，并进入NAT地址组视图 | | **nat address-group** *group-id* [ **name** *group-name* ] | 缺省情况下，不存在地址组 |
| 添加地址组成员 | | **address** *start-address end-address* | 缺省情况下，不存在地址组成员<br>可通过多次执行本命令添加多个地址组成员<br>当前地址组成员的IP地址段不能与该地址组中或者其它地址组中已有的地址成员组成员重叠 |
| 退回系统视图 | | **quit** | - |
| 进入接口视图 | | **interface** *interface-type interface-number* | - |
| 配置出方向动态地址转换 | NO-PAT方式 | **nat outbound** [ *ipv4-acl-number* \| **name** *ipv4-acl-name* ] **address-group** { *group-id* \| **name** *group-name* } **no-pat** [ **reversible** ] [ **rule** *rule-name* ] [ **priority** *priority* ] [ **disable** ] [ **description** *text* ] | 二者至少选其一<br>缺省情况下，不存在出方向动态地址转换配置<br>一个接口下可配置多个出方向的动态地址转换 |
| | PAT方式 | **nat outbound** [ *ipv4-acl-number* \| **name** *ipv4-acl-name* ] [ **address-group** { *group-id* \| **name** *group-name* } ] [ **port-preserved** ] [ **rule** *rule-name* ] [ **priority** *priority* ] [ **disable** ] [ **description** *text* ] | |
| 退回系统视图 | | **quit** | - |
| （可选）配置PAT方式地址转换的模式 | | **nat mapping-behavior endpoint-independent** [ **acl** { *ipv4-acl-number* \| **name** *ipv4-acl-name* } ] | 缺省情况下，PAT方式地址转换的模式为Address and Port-Dependent Mapping<br>该配置只对PAT方式的出方向动态地址转换有效 |

### 1.4.4 配置入方向动态地址转换

入方向动态地址转换功能通常与接口上的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，用于实现双向 NAT 应用，不建议单独使用。

入接口动态地址转换的具体过程如下：

- 对于该接口接收到的外网访问内网的首报文，将与指定的 ACL permit 规则匹配的报文的源 IP 地址转换为地址组中的地址。
- 在指定了 **no-pat reversible** 参数，并且已经存在 NO-PAT 表项的情况下，对于经过该接口发送的内网访问外网的首报文，将其目的 IP 地址与 NO-PAT 表项进行匹配，并将目的 IP 地址转换为匹配的 NO-PAT 表项中记录的外网地址。

需要注意的是，该方式下的地址转换不支持 Easy IP 功能。

表1-7 配置入方向动态地址转换

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 创建NAT地址组，并进入NAT地址组视图 | **nat address-group** *group-id* [ **name** *group-name* ] | 缺省情况下，不存在NAT地址组 |
| 添加地址组成员 | **address** *start-address end-address* | 缺省情况下，不存在地址组成员<br>可通过多次执行本命令添加多个地址组成员<br>当前地址组成员的IP地址段不能与该地址组中或者其它地址组中已有的地址组成员重叠 |
| 退回系统视图 | **quit** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 配置入方向动态地址转换 | **nat inbound** { *ipv4-acl-number* \| **name** *ipv4-acl-name* } **address-group** { *group-id* \| **name** *group-name* } [ **no-pat** [ **reversible** ] [ **add-route** ] ] [ **rule** *rule-name* ] [ **priority** *priority* ] [ **disable** ] [ **description** *text* ] | 缺省情况下，不存在入方向动态地址转换配置<br>一个接口下可配置多个入方向的动态地址转换 |

# 1.5 调整NAT规则的匹配优先级

## 1.5.1 功能简介

NAT 规则的位置决定了匹配的优先级，位置越靠前的 NAT 规则，其匹配优先级越高。本功能通过调整 NAT 规则的位置，可以改变同一类 NAT 规则的匹配顺序。

## 1.5.2 配置限制和指导

用户调整 NAT 规则的匹配顺序后，NAT 规则的匹配优先级的值也会发生变化，具体规则为：将 *nat-rule-name1* 移动到 *nat-rule-name2* 后面/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* 的匹配优先级的值－1。

## 1.5.3 配置准备

在调整 NAT 规则的匹配优先级前，需要为 NAT 规则指定规则名称，否则无法使用本功能。

## 1.5.4 调整出方向动态NAT规则的匹配优先级

表1-8 调整出方向动态 NAT 规则的匹配优先级

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 调整出方向动态NAT规则的匹配优先级 | **nat outbound rule move** *nat-rule-name1* { **after** \| **before** } *nat-rule-name2* | - |

### 1.5.5 调整入方向动态NAT规则的匹配优先级

表1-9 调整入方向动态 NAT 规则的匹配优先级

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 调整入方向动态NAT规则的匹配优先级 | **nat inbound rule move** *nat-rule-name1* { **after** \| **before** } *nat-rule-name2* | - |

### 1.5.6 调整入方向一对一静态NAT规则的匹配优先级

表1-10 调整入方向一对一静态 NAT 规则的匹配优先级

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 调整入方向一对一静态NAT规则的匹配优先级 | **nat static inbound rule move** *nat-rule-name1* { **after** \| **before** } *nat-rule-name2* | - |

### 1.5.7 调整出方向一对一静态NAT规则的匹配优先级

表1-11 调整出方向一对一静态 NAT 规则的匹配优先级

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 调整出方向一对一静态NAT规则的匹配优先级 | **nat static outbound rule move** *nat-rule-name1* { **after** \| **before** } *nat-rule-name2* | - |

## 1.6 配置NAT ALG

通过开启指定应用协议类型的 ALG 功能，实现对应用层报文数据载荷字段的分析和 NAT 处理。

表1-12 配置 NAT ALG 功能

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 开启指定或所有协议类型的NAT ALG功能 | **nat alg** { **all** \| **dns** \| **ftp** \| **icmp-error** \| **ils** \| **mgcp** \| **nbt** \| **pptp** \| **rsh** \| **rtsp** \| **sccp** \| **sqlnet** \| **tftp** \| **xdmcp** } | 缺省情况下，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 |

# 1.7 配置NAT日志功能

## 1.7.1 配置NAT会话日志功能

NAT 会话日志是为了满足网络管理员安全审计的需要，对 NAT 会话（报文经过设备时，源或目的信息被 NAT 进行过转换的连接）信息进行的记录，包括 IP 地址及端口的转换信息、用户的访问信息以及用户的网络流量信息。

有三种情况可以触发设备生成 NAT 会话日志：

- 新建 NAT 会话。
- 删除 NAT 会话。新增高优先级的配置、删除配置、报文匹配规则变更、NAT 会话老化以及执行删除 NAT 会话的命令时，都可能导致 NAT 会话被删除。
- 存在 NAT 活跃流。NAT 活跃流是指在一定时间内存在的 NAT 会话。当设置的生成活跃流日志的时间间隔到达时，当前存在的 NAT 会话信息就被记录并生成日志。

表1-13 配置 NAT 会话日志功能

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 开启NAT日志功能 | **nat log enable** [ **acl** { *ipv4-acl-number* \| **name** *ipv4-acl-name* } ] | 缺省情况下，NAT日志功能处于关闭状态 |
| 开启NAT新建会话的日志功能 | **nat log flow-begin** | 三者至少选其一<br>缺省情况下，创建、删除NAT会话或存在NAT活跃流时，均不生成NAT日志 |
| 开启NAT删除会话的日志功能 | **nat log flow-end** | |
| 开启NAT活跃流的日志功能，并设置生成活跃流日志的时间间隔 | **nat log flow-active** *time-value* | |

## 1.7.2 配置NAT告警信息日志功能

在 NAT 地址转换中，如果可为用户分配的 NAT 资源用尽，后续连接由于没有可用资源无法进行地址转换，相应的报文将被丢弃。NAT 告警信息日志功能用来在 NAT 资源用尽时输出告警日志。在 NO-PAT 动态映射中，NAT 资源是指公网 IP 地址；在 EIM 模式的 PAT 动态映射中，NAT 资源是指公网 IP 地址和端口。

表1-14 配置 NAT 告警信息日志功能

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 开启NAT日志功能 | **nat log enable** [ **acl** { *ipv4-acl-number* \| **name** *ipv4-acl-name* } ] | 缺省情况下，NAT日志功能处于关闭状态<br>ACL参数对NAT告警信息日志功能无效 |
| 开启NAT告警信息的日志功能 | **nat log alarm** | 缺省情况下，NAT告警信息日志功能处于关闭状态 |

## 1.8 开启NAT转换失败发送ICMP差错报文功能

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，还可以避免将设备 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。

表1-15 开启 NAT 转换失败发送 ICMP 差错报文功能

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 开启设备NAT转换失败发送ICMP差错报文功能 | **nat icmp-error reply** | 缺省情况下，NAT转换失败时，设备不发送ICMP差错报文 |

## 1.9 NAT显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示 NAT 配置后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **reset** 命令可以清除 NAT 表项。

表1-16 NAT 显示和维护

| 操作 | 命令 |
| --- | --- |
| 显示NAT ALG功能的开启状态 | **display nat alg** |
| 显示所有的NAT配置信息 | **display nat all** |
| 显示NAT地址组的配置信息 | **display nat address-group** [ *group-id* ] |
| 显示NAT EIM表项信息 | **display nat eim** |
| 显示NAT入接口动态地址转换关系的配置信息 | **display nat inbound** |
| 显示NAT日志功能的配置信息 | **display nat log** |
| 显示NAT NO-PAT表项信息 | **display nat no-pat** |
| 显示NAT出接口动态地址转换关系的配置信息 | **display nat outbound** |

| 操作 | 命令 |
| --- | --- |
| 显示NAT会话表项 | **display nat session** [ [ **responder** ] { **source-ip** *source-ip* \| **destination-ip** *destination-ip* } * ] [ **verbose** ] |
| 显示NAT静态地址转换的配置信息 | **display nat static** |
| 显示NAT统计信息 | **display nat statistics** [ **summary** ] |
| 删除NAT会话表项 | **reset nat session** |