

H3C SecPath M9000 系列 多业务安全网关

NAT 配置指导(V7)

Copyright © 2021-2024 新华三技术有限公司及其许可者 版权所有，保留一切权利。

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

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

由于产品版本升级或其他原因，本手册内容有可能变更。**H3C** 保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，**H3C** 尽全力在本手册中提供准确的信息，但是 **H3C** 并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前言

本配置指导主要介绍 NAT（Network Address Translation，网络地址转换）的相关功能原理及配置。
前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [资料意见反馈](#)

读者对象

本手册主要适用于如下工程师：

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

本书约定

1. 命令行格式约定






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

2. 图形界面格式约定

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

3. 各类标志

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

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

4. 图标约定

本书使用的图标及其含义如下：

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

5. 示例约定

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

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

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail: info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 NAT 概述	1-1
1.1 NAT 配置限制和指导	1-1
1.2 NAT 基本概念	1-1
1.3 NAT 工作机制	1-2
1.4 NAT 转换控制	1-2
1.5 NAT 转换方式	1-3
1.5.1 静态 IP 地址转换	1-3
1.5.2 源 IP 地址转换	1-3
1.5.3 目的 IP 地址转换	1-5
1.6 NAT 表项	1-5
1.6.1 NAT 会话表项	1-5
1.6.2 EIM 表项	1-6
1.6.3 NO-PAT 表项	1-6
1.6.4 端口块表项	1-6
1.7 NAT 支持多 VPN 实例	1-6
1.8 NAT hairpin	1-7
1.9 NAT 支持 ALG	1-7
1.10 NAT DNS mapping	1-7
1.11 NAT 支持发送免费 ARP 报文	1-8
1.12 NAT444	1-8
1.12.1 NAT444 简介	1-8
1.12.2 NAT444 集中部署	1-8
1.13 地址重叠场景中的 NAT	1-9
1.13.1 地址重叠的两个 VPN 之间互访	1-9
1.13.2 内网用户主动访问与之地址重叠的外网服务器	1-9
1.14 NAT 在 DS-Lite 网络中的应用	1-10
2 配置全局 NAT	2-1
2.1 全局 NAT 简介	2-1
2.2 全局 NAT 与软件版本适配关系	2-1
2.3 vSystem 相关说明	2-1
2.4 全局 NAT 配置任务简介	2-1
2.5 配置全局 NAT 策略	2-2

2.5.1 功能简介	2-2
2.5.2 配置限制和指导	2-3
2.5.3 创建全局 NAT 策略	2-3
2.5.4 配置 NAT 类型的规则	2-3
2.5.5 配置 NAT64 类型的规则	2-5
2.5.6 配置 NAT66 类型的规则	2-8
2.5.7 移动 NAT 规则	2-9
2.5.8 禁用 NAT 规则	2-10
2.6 配置 NAT 地址组	2-11
2.7 配置 NAT ALG	2-12
2.8 配置 NAT DNS mapping 功能	2-12
2.9 配置 NAT 发送免费 ARP 报文功能	2-13
2.10 配置 NAT 支持 HA	2-13
2.10.1 功能简介	2-13
2.10.2 工作机制	2-13
2.10.3 配置主备模式下的 NAT	2-15
2.10.4 配置双主模式下的 NAT	2-17
2.11 特定条件下的 NAT 配置	2-20
2.11.1 开启反向报文的重定向功能	2-20
2.11.2 开启对 TCP SYN 和 SYN ACK 报文中时间戳的删除功能	2-21
2.12 配置 NAT 维护功能	2-21
2.12.1 配置 NAT 定时统计功能	2-21
2.12.2 配置全局 NAT 策略中 NAT 类型的 SNAT+DNAT 规则的源 IP 地址转换和目的 IP 转换先于安全策略匹配，以便与老版本兼容	2-22
2.12.3 开启新建 NAT 会话速率的统计功能	2-22
2.12.4 配置检测 NAT 地址组成员的可用性	2-23
2.12.5 开启 NAT 转换失败发送 ICMP 差错报文功能	2-23
2.13 配置 NAT 日志功能	2-24
2.13.1 配置 NAT 会话日志功能	2-24
2.13.2 配置 NAT444 用户日志功能	2-24
2.13.3 配置 NAT 告警信息日志功能	2-25
2.13.4 开启 NO-PAT 方式下 NAT 地址组中地址成员使用率的日志信息功能	2-26
2.14 全局 NAT 显示和维护	2-27
2.15 全局 NAT 典型配置举例	2-29
2.15.1 内网用户通过 NAT 地址访问外网配置举例（静态地址转换）	2-29
2.15.2 内网用户通过 NAT 地址访问外网配置举例（地址不重叠）	2-31

2.15.3 外网用户通过外网地址访问内网服务器配置举例	2-36
2.15.4 外网用户通过域名访问内网服务器配置举例（地址不重叠）	2-42
2.15.5 内网用户通过 NAT 地址互访配置举例	2-47
2.15.6 端口块动态映射配置举例	2-52
3 配置接口 NAT	3-1
3.1 vSystem 相关说明	3-1
3.2 接口 NAT 配置限制和指导	3-1
3.3 接口 NAT 配置任务简介	3-2
3.4 配置接口上的静态地址转换	3-3
3.4.1 配置限制和指导	3-3
3.4.2 配置准备	3-3
3.4.3 配置出方向一对一静态地址转换	3-3
3.4.4 配置出方向网段对网段静态地址转换	3-4
3.4.5 配置基于对象组的出方向静态地址转换	3-5
3.4.6 配置入方向一对一静态地址转换	3-6
3.4.7 配置入方向网段对网段静态地址转换	3-6
3.4.8 配置基于对象组的入方向静态地址转换	3-7
3.5 配置接口上的动态地址转换	3-8
3.5.1 配置限制和指导	3-8
3.5.2 配置准备	3-8
3.5.3 配置出方向动态地址转换	3-9
3.5.4 配置入方向动态地址转换	3-10
3.6 配置接口上的内部服务器	3-11
3.6.1 功能简介	3-11
3.6.2 配置限制和指导	3-12
3.6.3 配置普通内部服务器	3-12
3.6.4 配置负载分担内部服务器	3-13
3.6.5 配置基于 ACL 的内部服务器	3-14
3.6.6 配置基于对象组的内部服务器	3-14
3.7 配置接口上的 NAT444 地址转换	3-15
3.7.1 功能简介	3-15
3.7.2 配置限制和指导	3-15
3.7.3 配置 NAT444 端口块静态映射	3-15
3.7.4 配置 NAT444 端口块动态映射	3-16
3.7.5 配置 NAT444 端口块全局共享功能	3-17
3.8 配置接口上的 DS-Lite B4 地址转换	3-18

3.9 配置接口 NAT 策略.....	3-19
3.9.1 功能简介	3-19
3.9.2 配置限制和指导	3-19
3.9.3 创建 NAT 策略	3-19
3.9.4 配置 NAT 规则	3-19
3.9.5 移动 NAT 规则	3-21
3.9.6 禁用 NAT 规则	3-21
3.10 配置动态地址转换的备份组	3-22
3.10.1 功能简介	3-22
3.10.2 配置限制和指导	3-22
3.10.3 配置 NAT 地址组的备份组	3-22
3.10.4 配置 Easy IP 方式的地址转换使用的备份组	3-22
3.10.5 配置使用多备份组处理 Easy IP 方式地址转换的端口范围	3-23
3.11 配置 NAT hairpin 功能	3-24
3.12 配置 NAT ALG	3-24
3.13 配置 NAT DNS mapping 功能	3-25
3.14 配置 NAT 发送免费 ARP 报文功能	3-26
3.15 配置 NAT 业务引擎的负载分担功能	3-26
3.15.1 配置 NAT 业务引擎重新分担动态 NAT 功能	3-26
3.15.2 配置静态 NAT 的负载分担功能	3-27
3.15.3 配置 NAT 负载分担组	3-27
3.16 开启 NAT 动态端口块热备份功能	3-28
3.17 配置 NAT 支持 HA	3-28
3.17.1 功能简介	3-28
3.17.2 工作机制	3-28
3.17.3 配置主备模式下的 NAT	3-30
3.17.4 配置双主模式下的 NAT	3-32
3.18 配置 NAT 维护功能	3-34
3.18.1 配置 NAT 定时统计功能	3-34
3.18.2 开启新建 NAT 会话速率的统计功能	3-34
3.18.3 配置检测 NAT 地址组成员的可用性	3-34
3.18.4 开启 NAT 转换失败发送 ICMP 差错报文功能	3-35
3.19 配置 NAT 日志功能	3-36
3.19.1 配置 NAT 会话日志功能	3-36
3.19.2 配置 NAT444 用户日志功能	3-36
3.19.3 配置 NAT 告警信息日志功能	3-37

3.19.4 开启 NO-PAT 方式下 NAT 地址组中地址成员使用率的日志信息功能	3-38
3.20 配置 NAT 生成 OpenFlow 流表	3-38
3.21 特定条件下的 NAT 配置	3-39
3.21.1 开启反向报文的重定向功能	3-39
3.21.2 开启对 TCP SYN 和 SYN ACK 报文中时间戳的删除功能	3-39
3.21.3 开启主备链路切换后的 NAT 会话重建功能	3-40
3.21.4 主备链路切换导致出接口所属安全域变化后的 NAT 会话重建功能	3-40
3.22 接口 NAT 显示和维护	3-41
3.23 接口 NAT 典型配置举例	3-43
3.23.1 内网用户通过 NAT 地址访问外网配置举例（静态地址转换）	3-43
3.23.2 内网用户通过 NAT 地址访问外网配置举例（地址不重叠）	3-45
3.23.3 内网用户通过 NAT 地址访问外网配置举例（地址重叠）	3-49
3.23.4 外网用户通过外网地址访问内网服务器配置举例	3-53
3.23.5 外网用户通过域名访问内网服务器配置举例（地址不重叠）	3-57
3.23.6 外网用户通过域名访问内网服务器配置举例（地址重叠）	3-61
3.23.7 内网用户通过 NAT 地址访问内网服务器配置举例	3-66
3.23.8 内网用户通过 NAT 地址互访配置举例	3-70
3.23.9 地址重叠的两个 VPN 之间互访配置举例	3-74
3.23.10 负载分担内部服务器配置举例	3-78
3.23.11 NAT DNS mapping 配置举例	3-82
3.23.12 NAT444 端口块静态映射配置举例	3-87
3.23.13 NAT444 端口块动态映射配置举例	3-90
3.23.14 DS-Lite B4 端口块动态映射配置举例	3-93
3.23.15 HA 联动 VRRP 的主备组网中 NAT 功能典型配置举例	3-96
3.23.16 HA 联动 VRRP 的双主组网中 NAT 功能典型配置举例	3-96

1 NAT 概述

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。

1.1 NAT配置限制和指导

全局 NAT 的优先级高于接口 NAT。若同时存在全局 NAT 策略和接口 NAT 的配置，当流量与全局 NAT 策略中任意一条过滤规则匹配，那么接口 NAT 中的源地址转换和目的转换的配置均不生效。建议不要同时配置接口 NAT 和全局 NAT。

设备上经过 NAT 转换的报文不会再进行 AFT 转换。

使用 NAT 功能进行地址转换时，NAT 模块会发布公网 IP 地址的主机路由。如果公网 IP 地址是一段地址范围，则 NAT 模块会对公网 IP 地址范围划分网段，划分网段时使用的掩码长度为 8、16、24、26、28、30。例如，公网 IP 地址范围为 122.90.12.128~122.90.12.135，则 NAT 模块发布的主机路由的目的地址和掩码长度为 122.90.12.128/30 和 122.90.12.132/30。

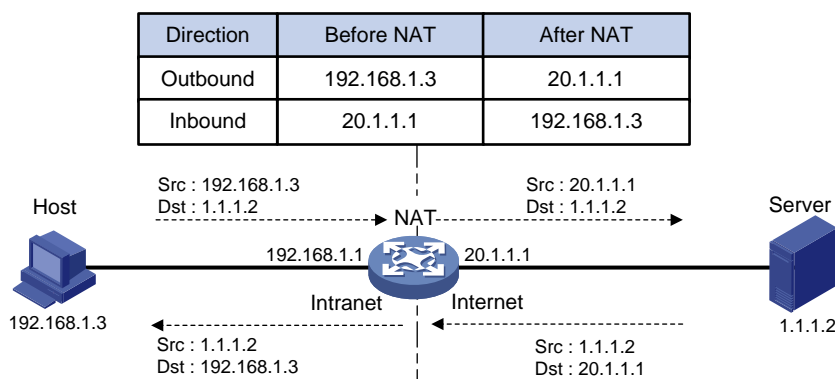
1.2 NAT基本概念

NAT 基本概念如下：

- NAT 设备：配置了 NAT 功能的连接内部网络和外部网络的边缘设备。
- 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 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。
- NAT 地址：用于进行地址转换的公网 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。关于 NAT 表项的详细介绍请参见“[1.6 NAT 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静态指定或通过 DHCP 等协议动态获取。
- 全局 NAT：NAT 规则的应用范围为全局。对于全局 NAT，所有经过 NAT 设备的流量都会进行匹配，并对匹配 NAT 规则的流量进行地址转换。
- 接口 NAT：NAT 规则的应用范围为接口。对于接口 NAT，只有经过应用 NAT 规则的接口的流量才会进行匹配，并对匹配 NAT 规则的流量进行地址转换。

1.3 NAT工作机制

图1-1 NAT 基本工作过程示意图



如图 1-1 所示，一台 NAT 设备连接内网和外网，当有报文经过 NAT 设备时，NAT 的基本工作过程如下：

- (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关系。
- (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，并不知道存在 192.168.1.3 这个地址。因此，NAT “隐藏”了企业的私有网络。

1.4 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、传输层协议类型和 VPN 实例这几个元素进行报文匹配，忽略其它元素。

1.5 NAT转换方式

1.5.1 静态 IP 地址转换

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。

1.5.2 源 IP 地址转换

源 IP 地址转换方式是一种动态地址转换方式，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。

源 IP 地址转换包括 NO-PAT 模式的地址转换、基于端口的 PAT 模式的地址转换和基于端口块的 PAT 模式的地址转换。

1. NO-PAT 模式

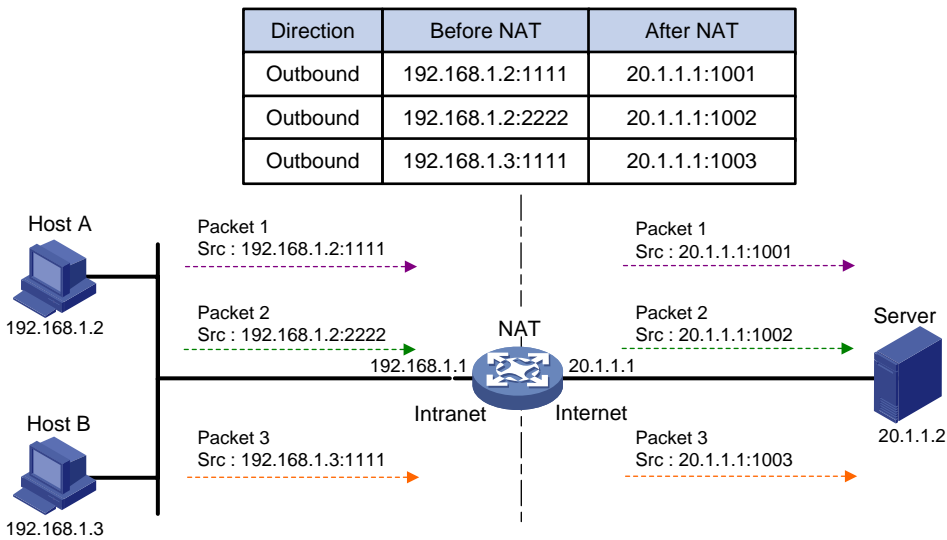
NO-PAT（Not Port Address Translation）模式下，一个外网地址同一时间只能分配给一个内网地址进行地址转换，不能同时被多个内网地址共用。当使用某外网地址的内网用户停止访问外网时，NAT 会将其占用的外网地址释放并分配给其他内网用户使用。

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。

2. 基于端口的 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 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 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。

3. 基于端口块的 PAT 模式

基于端口块的 PAT 模式是一种基于端口范围的 PAT 动态地址转换，即一个私网 IP 地址在一个时间段内独占一个公网 IP 地址的某个端口块。例如：假设私网 IP 地址 10.1.1.1 独占公网 IP 地址 202.1.1.1 的一个端口块 10001~10256，则该私网 IP 向公网发起的所有连接，源 IP 地址都将被转换为同一个公网 IP 地址 202.1.1.1，而源端口将被转换为端口块 10001~10256 之外的一个端口。

基于端口块的 PAT 模式包括端口块方式包括静态映射和动态映射两种，主要应用在 NAT444 或 DS-Lite 网络中。

- **端口块静态映射**

端口块静态映射是指，NAT 网关设备根据配置自动计算私网 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。当私网 IP 地址成员中的某个私网 IP 地址向公网发起新建连接时，根据私网 IP 地址匹配静态端口块表项，获取对应的公网 IP 地址和端口块，并从端口块中动态为其分配一个公网端口，对报文进行地址转换。

配置端口块静态映射时，需要创建一个端口块组，并在端口块组中配置私网 IP 地址成员、公网 IP 地址成员、端口范围和端口块大小。假设端口块组中每个公网 IP 地址的可用端口块数为 m （即端口范围除以端口块大小），则端口块静态映射的算法如下：按照从小到大的顺序对私网 IP 地址成员中的所有 IP 地址进行排列，最小的 m 个私网 IP 地址对应最小的公网 IP 地址及其端口块，端口块按照起始端口号从小到大的顺序分配；次小的 m 个私网 IP 地址对应次小的公网 IP 地址及其端口块，端口块的分配顺序相同；依次类推。

- **端口块动态映射**

当内网用户向公网发起连接时，首先根据动态地址转换中的 ACL 规则进行过滤，决定是否需要进行源地址转换。对于需要进行源地址转换的连接，当该连接为该用户的首次连接时，从所匹配的动态地址转换配置引用的 NAT 地址组中获取一个公网 IP 地址，从该公网 IP 地址中

动态分配一个端口块，创建动态端口块表项，然后从端口块表项中动态分配一个公网端口，进行地址转换。对该用户后续连接的转换，均从生成的动态端口块表项中分配公网端口。当该用户的所有连接都断开时，回收为其分配的端口块资源，删除相应的动态端口块表项。

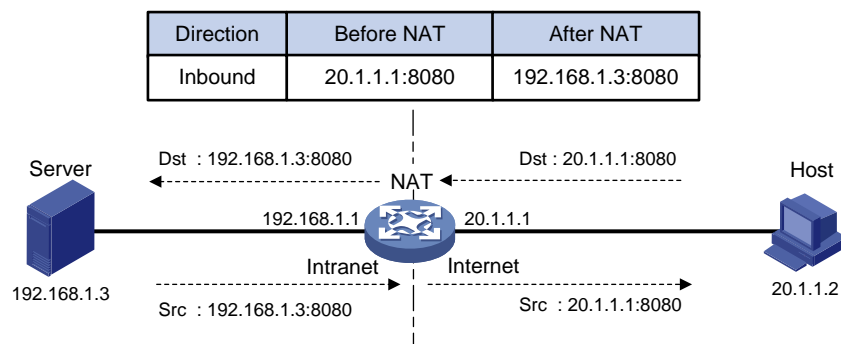
端口块动态映射支持增量端口块分配。当为某私网 IP 地址分配的端口块资源耗尽（端口块中的所有端口都被使用）时，如果该私网 IP 地址向公网发起新的连接，则无法再从端口块中获取端口，无法进行地址转换。此时，如果预先在相应的 NAT 地址组中配置了增量端口块数，则可以为该私网 IP 地址分配额外的端口块，进行地址转换。

1.5.3 目的 IP 地址转换

在实际应用中，内网中的服务器可能需要对外部网络提供一些服务，例如给外部网络提供 Web 服务，或是 FTP 服务。这种情况下，通过定义内部服务器对外提供服务使用的外部 IP 地址+端口与内部服务器在内网使用的地址+端口的映射关系，实现 NAT 设备允许外网用户通过指定的 NAT 地址和端口访问这些内部服务器。

如图 1-3 所示，外部网络用户访问内部网络服务器的数据报文经过 NAT 设备时，NAT 设备将报文的地址与接口上的 NAT 内部服务器配置进行匹配，并将匹配上的访问内部服务器的请求报文的源 IP 地址和端口号转换成内部服务器的私有 IP 地址和端口号。当内部服务器回应该报文时，NAT 设备再根据已有的地址映射关系将回应报文的源 IP 地址和端口号转换成外网 IP 地址和端口号。

图1-3 内部服务器基本原理示意图



1.6 NAT表项

1.6.1 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。
- 后续报文方向与首报文相反时，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”。

1.6.2 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）的 EIM 三元组表项，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。

1.6.3 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“[1.9 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。
- 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。

1.6.4 端口块表项

端口块表项记录 1 个用户在网关转换前的私网 IP 地址、转换后对应的公网 IP 地址及其端口块。端口块表项分为静态端口块表项和动态端口块表项。关于端口块表项的详细介绍，请参见“[1.5.2 3. 基于端口块的 PAT 模式](#)”。

1.7 NAT支持多VPN实例

支持多 VPN 实例的 NAT 允许 VPN 实例内的用户访问外部网络，同时允许分属于不同 VPN 实例的用户互访。例如，当某 VPN 实例内的用户经过 NAT 设备访问外部网络时，NAT 将内部网络主机的 IP 地址和端口替换为 NAT 地址和端口，同时还记录了用户的 VPN 实例信息（如 VPN 实例名称）。外部网络的回应报文到达 NAT 设备时，NAT 将外部网络地址和端口还原为内部网络主机的 IP 地址和端口，同时可得知该回应报文应该转发给哪一个 VPN 实例内的用户。另外，NAT 还可利用外部网络地址所携带的 VPN 实例信息，支持多个 VPN 实例之间的互访。

同时，NAT 内部服务器也支持多 VPN 实例，这给外部网络提供了访问 VPN 实例内服务器的机会。例如，VPN1 内提供 Web 服务的主机地址是 10.110.1.1，可以使用 202.110.10.20 作为 Web 服务器的外部地址，Internet 的用户使用 202.110.10.20 的地址就可以访问到 VPN1 提供的 Web 服务。目前，仅全局 NAT 支持多 VPN 实例。

1.8 NAT hairpin

NAT hairpin 功能用于满足位于内网侧的用户之间或内网侧的用户与服务器之间通过 NAT 地址进行访问的需求，通过对报文同时进行源地址和目的地址的转换来实现。它支持两种组网模式：

- P2P：位于内网侧的用户之间通过动态分配的 NAT 地址互访。内网各主机首先向外网服务器注册自己的内网地址信息，该地址信息为外网侧出方向地址转换的 NAT 地址，然后内网主机之间通过使用彼此向外网服务器注册的外网地址进行互访。
- C/S：位于内网侧的用户使用 NAT 地址访问内网服务器。

1.9 NAT支持ALG

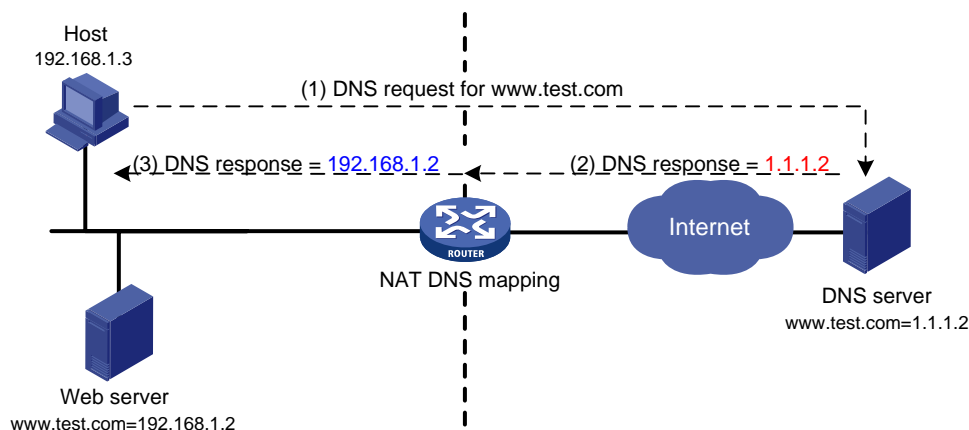
ALG（Application Level Gateway，应用层网关）主要完成对应用层报文的解析和处理。通常情况下，NAT 只对报文头中的 IP 地址和端口信息进行转换，不对应用层数据载荷中的字段进行分析和处理。然而对于一些应用层协议，它们的报文的数据载荷中可能包含 IP 地址或端口信息，这些载荷信息也必须进行有效的转换，否则可能导致功能不正常。

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。

1.10 NAT DNS mapping

一般情况下，DNS（Domain Name System，域名系统）服务器和访问私网服务器的用户都在公网，通过在 NAT 设备上配置内部服务器，可以将公网地址、端口等信息映射到私网内的服务器上，使得公网用户可以通过内部服务器的域名或公网地址来访问内部服务器。但是，如[图 1-4](#)所示，如果 DNS 服务器在公网，私网用户希望通过域名来访问私网的 Web 服务器，则会由于 DNS 服务器向私网用户发送的响应报文中包含的是私网服务器的公网地址，而导致收到响应报文的私网用户无法利用域名访问私网服务器。通过在设备上配置 DNS mapping 可以解决该问题。

图1-4 NAT DNS mapping 工作示意图



NAT DNS mapping 功能是指，通过配置“域名+公网 IP 地址+公网端口号+协议类型”的映射表，建立内部服务器域名与内部服务器公网信息的对应关系。NAT 设备检查接收到的 DNS 响应报文，根据报文中的域名查找用户配置的 DNS mapping 映射表，并根据表项内的“公网地址+公网端口+协议类型”信息查找内部服务器地址映射表中该信息对应的私网地址，替换 DNS 查询结果中的公网地址。这样，私网用户收到的 DNS 响应报文中就包含了要访问的内部服务器的私网地址，也就能够使用内部服务器域名访问同一私网内的内部服务器。

1.11 NAT支持发送免费ARP报文

NAT 模块会借助地址管理模块对公网 IPv4 地址资源进行管理，具体机制为：

- (1) NAT 模块将公网 IPv4 地址下发地址管理模块。
- (2) NAT 模块发送免费 ARP 报文通告下发到地址管理模块的公网 IPv4 地址与自身物理接口 MAC 地址的对应关系，以便局域网内其他设备的 ARP 表项或 MAC 地址表项保持最新。从而避免因 ARP 表项或 MAC 地址表项更新不及时引发的业务异常。

同时，NAT 模块会回应其他设备发送的免费 ARP。

关于免费 ARP 的详细介绍，请参见“三层技术-IP 业务配置指导”中的“ARP”。

1.12 NAT444

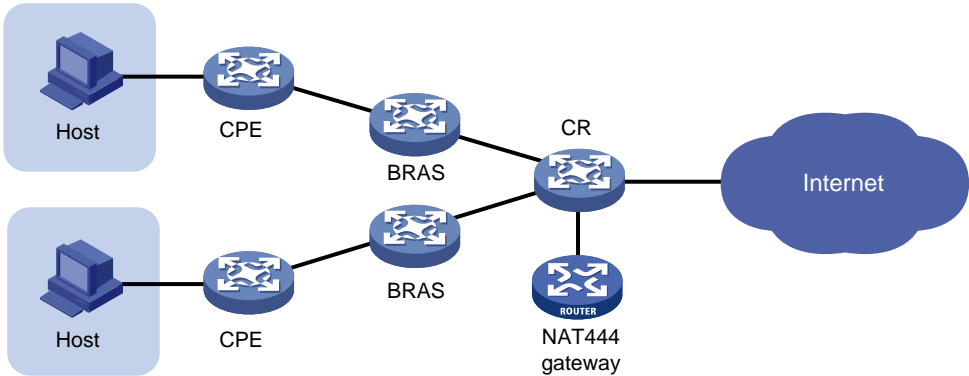
1.12.1 NAT444 简介

NAT444 是运营商网络部署 NAT 的整体解决方案，它基于 NAT444 网关，结合 AAA 服务器、日志服务器等配套系统，提供运营商级的 NAT，并支持用户溯源等功能。在众多 IPv4 向 IPv6 网络过渡的技术中，NAT444 仅需在运营商侧引入二次 NAT，对终端和应用服务器端的更改较小，并且 NAT444 通过端口块分配方式解决用户溯源等问题，因此成为了运营商的首选 IPv6 过渡方案。

1.12.2 NAT444 集中部署

通过在 CR 设备上安装处理 NAT 业务的 slot 或者旁挂 NAT444 设备来实现 NAT444。如[图 1-5](#)所示，用户访问外部网络时，CPE 设备上进行第一次 NAT 转换，然后在 BRAS 上完成 AAA 认证和私网地址的分配，认证通过后，用户发起访问外网的报文会在 NAT444 网关上进行 NAT444 转换（第二次 NAT 转换）。

图1-5 NAT444 集中部署组网图



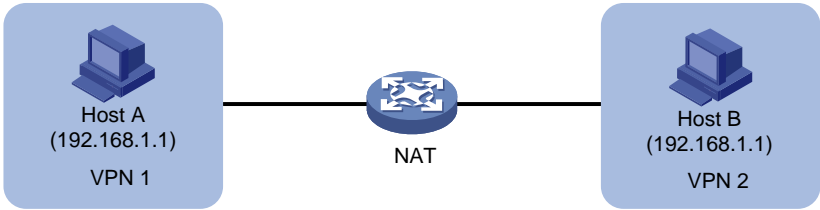
1.13 地址重叠场景中的NAT

1.13.1 地址重叠的两个VPN之间互访

分属不同VPN的内部网络主机使用了相同的地址空间，为了实现不同VPN中地址重叠的内网主机互访，需要配置静态NAT，对同一个方向的同一条流的数据报文同时进行源IP地址转换和目的IP地址转换。

如图1-6所示，VPN 1和VPN 2中的内网用户地址均为192.168.1.1。配置静态NAT，将VPN 1中Host A的地址在VPN 2中转换为172.16.1.1，将VPN 2中Host B的地址在VPN 1中转换为172.16.2.1。当静态NAT生效后，Host A使用172.16.2.1能够访问Host B，Host B使用172.16.1.1能够访问Host A。

图1-6 地址中叠的两个VPN之间互访



1.13.2 内网用户主动访问与之地址重叠的外网服务器

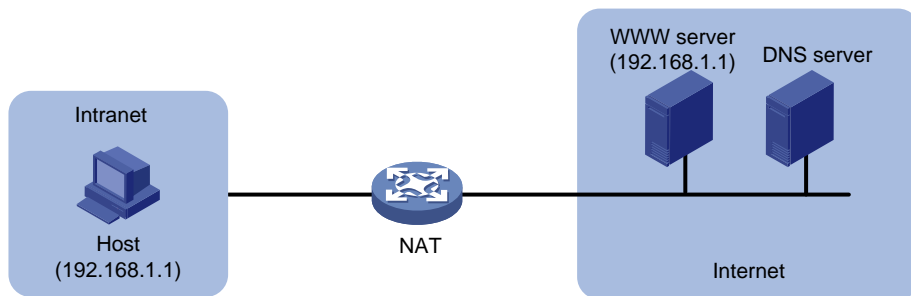
当内部网络主机使用外网注册地址或者合法的外网地址访问外部网络时，内网主机的IP地址和外网主机的IP地址可能会发生重叠。为了实现内网主机能够成功访问与之地址重叠的外部服务器，需要配置NAT ALG+动态NAT。

如图1-7所示，内网Host通过域名访问外网Web服务器，Host和Web服务器的IP地址均为192.168.1.1。

(1) 内网Host首先向外网的DNS服务器发起DNS查询请求。

- (2) DNS 服务器发送的 DNS 应答报文中，Web 服务器的域名对应的 IP 地址为 192.168.1.1。DNS 应答报文经过 NAT 设备时，进行 DNS 的 NAT ALG 处理，将 DNS 应答报文中域名对应的 IP 地址 192.168.1.1 转换为 10.1.1.1（该地址为临时分配的 NAT 地址）。NAT 设备将 ALG 处理后的 DNS 应答报文发送给内网 Host。
- (3) Host 访问 Web 服务器的报文中，源 IP 地址为 192.168.1.1，目的 IP 地址为 10.1.1.1。报文经过 NAT 设备时，NAT 设备根据动态 NAT 配置将源地址 192.168.1.1 转换为 20.1.1.1；NAT 设备检测到目的地址 10.1.1.1 为临时分配的 NAT 地址，根据步骤(2)中的转换关系，将 10.1.1.1 转换为 192.168.1.1。

图1-7 内网用户主动访问与之地址重叠的外网服务器

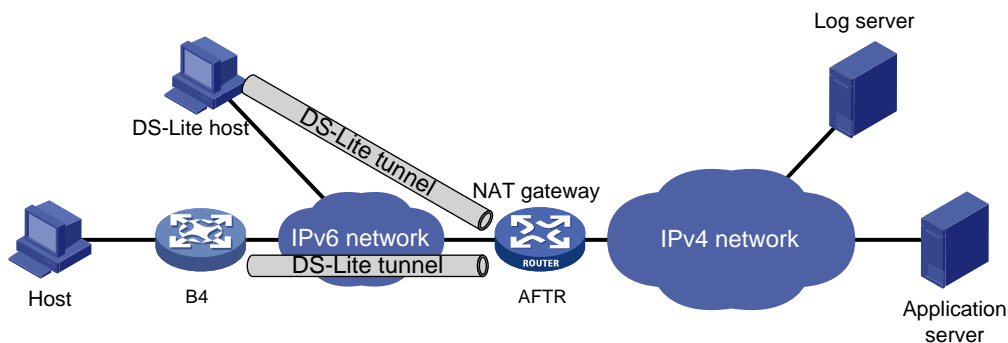


1.14 NAT在DS-Lite网络中的应用

DS-Lite（Dual Stack Lite，轻量级双协议栈）技术综合了 IPv4 over IPv6 隧道技术和 NAT 技术，利用隧道技术实现通过 IPv6 网络连接隔离的 IPv4 网络。

在 DS-Lite 网络中，B4 设备为用户网络的网关或者运行 DS-Lite 客户端软件的用户主机，AFTR 设备作为隧道端点设备和 NAT 网关负责执行隧道报文的封装、解封以及解封后的 IPv4 地址进行转换。有关 DS-Lite 隧道的详细介绍，请参见“VPN 配置指导”中的“隧道”。

图1-8 DS-Lite 网络组网图



在该组网环境下，AFTR 设备可基于 B4 的 IPv6 地址对 B4 分配端口块，DS-Lite 主机或所有以 B4 为网关的私网主机共用该 B4 的端口块访问 IPv4 网络。该方式支持对 DS-Lite 主机基于端口块的溯源。

目前，仅支持对 B4 进行动态映射方式的端口块分配。

2 配置全局 NAT

2.1 全局NAT简介

全局 NAT 适用于外部接口不固定的场景，当外部接口发生变化时，用户无需更改相关配置，降低了维护成本。

全局 NAT 通过在全局 NAT 策略中创建并执行 NAT 规则来实现地址转换。NAT 规则中包含报文的过滤条件和地址转换动作：

- 过滤条件用于匹配进行地址转换的报文。
- 地址转换动作包括源 NAT（SNAT）和目的 NAT（DNAT）。SNAT 转换报文的源 IP 地址，能够隐藏内网用户的 IP 地址；DNAT 转换报文的目的 IP 地址，通常用于内网服务器对外部网络用户提供服务的场景。在同一条 NAT 规则中组合使用 SNAT 和 DNAT，能够同时对报文进行源地址转换和目的地址转换。

全局 NAT 将 NAT 规则分为以下三类：

- SNAT 规则：一条 NAT 规则中的动作仅包括 SNAT。
- DNAT 规则：一条 NAT 规则中的动作仅包括 DNAT。
- SNAT+DNAT 规则：一条 NAT 规则中的动作包含 SNAT 和 DNAT。

2.2 全局NAT与软件版本适配关系

仅 Release 9X71P24 及以上版本支持全局 NAT 功能。

2.3 vSystem相关说明

非缺省 vSystem 不支持本特性的部分功能，具体包括：

- 开启 NAT 发送免费 ARP 报文功能
- 开启 NAT 端口负载分担功能
- 指定 HA 中主、从管理设备可以使用的 NAT 端口块范围
- 配置全局 NAT 策略中 NAT 类型的 SNAT+DNAT 规则的源 IP 地址转换和目的 IP 转换先于安全策略匹配，以便与老版本兼容



说明

非缺省 vSystem 对具体命令的支持情况，请见本特性的命令参考。有关 vSystem 的详细介绍请参见“虚拟化技术配置指导”中的“vSystem”。

2.4 全局NAT配置任务简介

- (1) [配置全局 NAT 策略](#)

- a. [创建全局 NAT 策略](#)
- b. [配置 NAT 类型的规则](#)
- c. [配置 NAT64 类型的规则](#)
- d. [配置 NAT66 类型的规则](#)
- e. [移动 NAT 规则](#)
- f. [禁用 NAT 规则](#)
- (2) (可选) [配置 NAT 地址组](#)
- (3) (可选) [配置 NAT ALG](#)
- (4) (可选) [配置 NAT DNS mapping 功能](#)
- (5) (可选) [配置 NAT 发送免费 ARP 报文功能](#)
- (6) (可选) 提高 NAT 业务的可靠性
 - o [配置 NAT 支持 HA](#)
- (7) (可选) [特定条件下的 NAT 配置](#)
 - o [开启反向报文的重定向功能](#)
 - o [开启对 TCP SYN 和 SYN ACK 报文中时间戳的删除功能](#)
- (8) (可选) [配置 NAT 维护功能](#)
 - o [配置 NAT 定时统计功能](#)
 - o [配置全局 NAT 策略中 NAT 类型的 SNAT+DNAT 规则的源 IP 地址转换和目的 IP 转换先于安全策略匹配，以便与老版本兼容](#)
 - o [开启新建 NAT 会话速率的统计功能](#)
 - o [配置检测 NAT 地址组成员的可用性](#)
 - o [开启 NAT 转换失败发送 ICMP 差错报文功能](#)
- (9) (可选) [配置 NAT 日志功能](#)
 - o [配置 NAT 会话日志功能](#)
 - o [配置 NAT444 用户日志功能](#)
 - o [配置 NAT 告警信息日志功能](#)
 - o [开启 NO-PAT 方式下 NAT 地址组中地址成员使用率的日志信息功能](#)

2.5 配置全局NAT策略

2.5.1 功能简介

全局 NAT 策略由 NAT 规则组成，NAT 规则由匹配条件和动作组成：

- 匹配条件：源地址、目的地址、服务类型、源安全域和目的安全域。每条 NAT 规则中可以根据需求配置不同的匹配条件，设备对匹配上的流量进行地址转换。匹配上的流量指的是能够匹配上某条 NAT 规则中所有匹配条件的流量。
- 动作：源地址转换和目的地址转换。

NAT 规则有如下三种类型：

- NAT 类型的地址转换，即 IPv4 和 IPv4 地址的相互转换。关于 NAT 功能和原理的详细介绍，请参见“NAT 配置指导”中的“NAT”。

- NAT64 类型的地址转换，即 IPv4 和 IPv6 地址的相互转换。关于 NAT64 功能和原理的详细介绍，请参见“NAT 配置指导”中的“AFT”。
- NAT66 类型的地址转换，即 IPv6 地址之间的相互转换，或者 NPTv6 方式的前缀转换。关于 NAT66 功能和原理的详细介绍，请参见“NAT 配置指导”中的“NAT66”。

2.5.2 配置限制和指导

若 NAT 规则未引用任何对象组或安全域，则该规则将匹配任意报文。

在全局 NAT 策略处于生效状态时，如果全局 NAT 策略中包含多条规则，则位置靠前的规则具有更高的匹配优先级。设备会按照规则的匹配优先级对报文进行匹配，一旦报文匹配上某条规则，匹配过程即结束。如果全局 NAT 策略未生效，则不会使用该策略中的规则进行报文匹配。可以通过 **display nat global-policy** 命令查看全局 NAT 策略的状态，显示信息中的“Config status”字段标识了全局 NAT 策略是否生效。

全局 NAT 策略下，最多可以创建 10000 条全局 NAT 规则。

配置内部服务器时，如果将 TCP 或 UDP 协议的端口号改为非知名端口号，则 NAT 设备不会进行 ALG 处理，导致用户无法使用内部服务器提供的服务。可通过如下两种方式解决上述问题：

- 修改内部服务器配置，使用 TCP 或 UDP 协议自身的知名端口号。
- 不修改内部服务器配置，使用 **port-mapping** 命令建立 TCP 或 UDP 协议与对应的内部服务器配置中的端口号的映射。关于 **port-mapping** 命令的详细介绍，请参见“安全配置指导”中的“ARP”。

2.5.3 创建全局 NAT 策略

- (1) 进入系统视图。

```
system-view
```

- (2) 创建全局 NAT 策略，并进入全局 NAT 策略视图。

```
nat global-policy
```

2.5.4 配置 NAT 类型的规则

1. 配置限制和指导

对于“DNAT 规则”或者“SNAT+DNAT 规则”，不能将目的安全域作为报文的过滤条件。对于使用静态地址转换方式的 SNAT 规则，该规则中引用的对象组中不能存在排除地址。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入全局 NAT 策略视图。

```
nat global-policy
```

- (3) 创建 NAT 类型的规则，并进入 NAT 规则视图。

```
rule name rule-name [ type nat ]
```

缺省情况下，不存在 NAT 规则。

- (4) (可选) 配置 NAT 规则的描述信息。

description *text*

缺省情况下, NAT 规则未配置任何描述信息。

- (5) 配置报文过滤条件。

- 配置 NAT 规则中用于匹配报文源 IP 地址的过滤条件。

source-ip { *ipv4-object-group-name* | **host** *ip-address* | **subnet** *subnet-ip-address mask-length* }

缺省情况下, NAT 规则中不存在用于匹配报文源 IP 地址的过滤条件。

- 配置 NAT 规则中用于匹配报文目的 IP 地址的过滤条件。

destination-ip { *ipv4-object-group-name* | **host** *ip-address* | **subnet** *subnet-ip-address mask-length* }

缺省情况下, NAT 规则中不存在用于匹配报文目的 IP 地址的过滤条件。

- 配置 NAT 规则中用于匹配报文携带的服务类型的过滤条件。

service *object-group-name*

缺省情况下, NAT 规则中不存在用于匹配报文携带的服务类型的过滤条件。

- 配置作为 NAT 规则过滤条件的源安全域。

source-zone *source-zone-name*

缺省情况下, NAT 规则中不存在源安全域过滤条件。

- 配置作为 NAT 规则过滤条件的目的安全域。

destination-zone *destination-zone-name*

缺省情况下, NAT 规则中不存在目的安全域过滤条件。

- 配置 NAT 规则中用于匹配报文所属 VPN 实例的过滤条件。

vrf *vrf-name*

缺省情况下, NAT 规则中不存在用于匹配报文所属 VPN 实例的过滤条件。

- (6) 配置 NAT 规则的动作。

- 配置 NAT 规则中源地址转换方式。

NO-PAT 方式:

action snat { **address-group** { *group-id* | **name** *group-name* } | **object-group** *ipv4-object-group-name* } **no-pat** [**reversible**] [**vrf** *vrf-name*]

PAT 方式:

action snat { **address-group** { *group-id* | **name** *group-name* } | **object-group** *ipv4-object-group-name* } [**port-preserved**] [**vrf** *vrf-name*]

Easy IP 方式:

action snat easy-ip [**port-preserved**] [**vrf** *vrf-name*]

静态地址转换方式:


```
action snat static { ip-address global-address | object-group
ipv4-object-group-name | subnet subnet-ip-address mask-length }
[ vrf vrf-name ]
```

NO-NAT 方式:

```
action snat no-nat
```

缺省情况下，未配置 NAT 规则中源地址的转换方式。

- 配置 NAT 规则的目的地址转换方式。

服务器映射方式:

```
action dnat { ip-address local-address | object-group
ipv4-object-group-name } [ local-port { local-port1 [ to
local-port2 ] }&<1-32> ]
```

NO-NAT 方式:

```
action dnat no-nat
```

缺省情况下，未配置 NAT 规则中目的地址的转换方式。

- (7) (可选) 开启 NAT 规则命中统计功能。

```
counting enable
```

缺省情况下，NAT 规则命中统计功能处于关闭状态。

- (8) 配置 PAT 方式地址转换的模式。

- a. 退回全局 NAT 策略视图。

```
quit
```

- b. 退回系统视图。

```
quit
```

- c. 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。

该配置只对 PAT 方式的出方向动态地址转换有效。

2.5.5 配置 NAT64 类型的规则

1. 功能简介

NAT64 类型的规则对应的功能为 AFT (Address Family Translation, 地址族转换), 有如下两种应用场景:

- IPv6 侧发起访问。在 IPv4 向 IPv6 过渡初期, 多数服务位于 IPv4 网络中, IPv6 网络用户访问 IPv4 网络中的服务时, 用户报文的源地址和目的地址的类型均为 IPv6, 需要将源地址和目的地址转换为 IPv4 地址。
- IPv4 侧发起访问。在 IPv4 向 IPv6 过渡后期, 多数服务位于 IPv6 网络中, IPv4 网络用户访问 IPv6 网络中的服务时, 用户报文的源地址和目的地址的类型均为 IPv4, 需要将源地址和目的地址转换为 IPv6 地址。

以上两种场景中, 既需进行源地址转换, 也需要进行目的地址转换。

2. 配置限制和指导

同一个 NAT64 规则中可以根据需求配置多个匹配条件，但后配置的匹配条件中的 IP 地址类型必须与先配置的匹配条件中的 IP 地址类型一致，例如先配置了 **source-ip host 192.168.1.1**，接下来配置了 **source-ip host 100::1**，那么 **source-ip host 100::1** 配置不生效。请根据实际应用场景规划配置。

使用前缀方式进行地址转换时，匹配条件中的 IPv6 地址前缀长度必须符合转换动作中 **General** 前缀、**IVI** 前缀或 **NAT64** 前缀对前缀长度的要求。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入全局 NAT 策略视图。

```
nat global-policy
```

- (3) 创建 NAT64 类型的规则，并进入 NAT 规则视图。

```
rule name rule-name type nat64
```

缺省情况下，不存在 NAT 规则。

- (4) （可选）配置 NAT 规则的描述信息。

```
description text
```

缺省情况下，NAT 规则未配置任何描述信息。

- (5) 配置报文过滤条件。

- 配置 NAT 规则中用于匹配报文源 IP 地址的过滤条件。

```
source-ip { { ipv4-object-group-name | ipv6-object-group-name } |  
host { ipv4-address | ipv6-address } | subnet { subnet-ipv4-address  
mask-length | subnet-ipv6-address prefix-length } }
```

缺省情况下，NAT 规则中不存在用于匹配报文源 IP 地址的过滤条件。

- 配置 NAT 规则中用于匹配报文目的 IP 地址的过滤条件。

```
destination-ip { { ipv4-object-group-name | ipv6-object-group-name }  
| host { ipv4-address | ipv6-address } | subnet { subnet-ipv4-address  
mask-length | subnet-ipv6-address prefix-length } }
```

- 配置 NAT 规则中用于匹配报文携带的服务类型的过滤条件。

```
service object-group-name
```

缺省情况下，NAT 规则中不存在用于匹配报文携带的服务类型的过滤条件。

- 配置作为 NAT 规则过滤条件的源安全域。

```
source-zone source-zone-name
```

缺省情况下，NAT 规则中不存在源安全域过滤条件。

- 配置 NAT 规则中用于匹配报文所属 VPN 实例的过滤条件。

```
vrf vrf-name
```

缺省情况下，NAT 规则中不存在用于匹配报文所属 VPN 实例的过滤条件。

- (6) 配置 NAT 规则的动作。

- 配置 NAT 规则中源地址转换方式。

NO-PAT 方式:

```
action snat object-group ipv4-object-group-name no-pat [ ipv4-vrrp  
virtual-router-id ] [ vrf vrf-name ]
```

```
action snat object-group ipv6-object-group-name no-pat [ vrf  
vrf-name ]
```

PAT 方式:

```
action snat object-group ipv4-object-group-name [ ipv4-vrrp  
virtual-router-id ] [ vrf vrf-name ]
```

```
action snat object-group ipv6-object-group-name [ vrf vrf-name ]
```

前缀转换方式:

```
action snat prefix { general { v4tov6 prefix-general  
general-prefix-length | v6tov4 } | ivi v6tov4 | nat64 v4tov6  
prefix-nat64 nat64-prefix-length } [ vrf vrf-name ]
```

静态地址转换方式:

```
action snat static ip-address global-ipv4-address [ ipv4-vrrp  
virtual-router-id ] [ vrf vrf-name ]
```

```
action snat static ip-address global-ipv6-address [ ipv6-vrrp  
virtual-router-id ] [ vrf vrf-name ]
```

- 配置 NAT 规则的目的地址转换方式。

静态地址转换方式:

```
action dnat static ip-address local-ipv4-address [ ipv6-vrrp  
virtual-router-id ] [ vrf vrf-name ]
```

```
action dnat static ip-address local-ipv6-address [ ipv4-vrrp  
virtual-router-id ] [ vrf vrf-name ]
```

服务器映射方式:

```
action dnat server ip-address local-ipv4-address [ local-port  
local-port ] [ vrf vrf-name ]
```

```
action dnat server ip-address local-ipv6-address [ local-port  
local-port ] [ ipv4-vrrp virtual-router-id ] [ vrf vrf-name ]
```

前缀方式:

```
action dnat prefix { general v6tov4 | nat64 v6tov4 } [ vrf vrf-name ]
```

```
action dnat prefix { general v4tov6 prefix-general prefix-length |  
ivi v4tov6 prefix-ivi } [ ipv4-vrrp virtual-router-id ] [ vrf  
vrf-name ]
```

- (7) (可选) 开启 NAT 规则命中统计功能。

counting enable

缺省情况下, NAT 规则命中统计功能处于关闭状态。

2.5.6 配置 NAT66 类型的规则

1. 功能简介

NAT66 是指 IPv6 地址之间的转换，包括动态方式、静态方式和 NPTv6 三种转换方式。IPv6 地址由网络前缀和接口 ID 两部分组成，NPTv6 方式的地址转换将网络前缀转换为新的网络前缀，同时 IPv6 地址接口 ID 部分会根据 RFC 6296 进行调整。具体算法请参考 RFC 6296。其他方式的地址转换是将 IPv6 地址转换为新的 IPv6 地址。在 IPv6 地址数量较多且对转换后的地址不敏感的情况下，建议采用 NPTv6 方式。

2. 配置限制和指导

对于“DNAT 规则”或者“SNAT+DNAT 规则”，不能将目的安全域作为报文的过滤条件。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入全局 NAT 策略视图。

```
nat global-policy
```

- (3) 创建 NAT66 类型的规则，并进入 NAT 规则视图。

```
rule name rule-name type nat66
```

缺省情况下，不存在 NAT 规则。

- (4) （可选）配置 NAT 规则的描述信息。

```
description text
```

缺省情况下，NAT 规则未配置任何描述信息。

- (5) 配置报文过滤条件。

- 配置 NAT 规则中用于匹配报文源 IP 地址的过滤条件。

```
source-ip { ipv6-object-group-name | host ipv6-address | subnet  
subnet-ipv6-address prefix-length }
```

缺省情况下，NAT 规则中不存在用于匹配报文源 IP 地址的过滤条件。

- 配置 NAT 规则中用于匹配报文目的 IP 地址的过滤条件。

```
destination-ip { ipv6-object-group-name | host ipv6-address | subnet  
subnet-ipv6-address prefix-length }
```

- 配置 NAT 规则中用于匹配报文携带的服务类型的过滤条件。

```
service object-group-name
```

缺省情况下，NAT 规则中不存在用于匹配报文携带的服务类型的过滤条件。

- 配置作为 NAT 规则过滤条件的源安全域。

```
source-zone source-zone-name
```

缺省情况下，NAT 规则中不存在源安全域过滤条件。

- 配置作为 NAT 规则过滤条件的目的安全域。

```
destination-zone destination-zone-name
```

缺省情况下，NAT 规则中不存在目的安全域过滤条件。

- 配置 NAT 规则中用于匹配报文所属 VPN 实例的过滤条件。

vrf *vrf-name*

缺省情况下，NAT 规则中不存在用于匹配报文所属 VPN 实例的过滤条件。

(6) 配置 NAT 规则的动作。

- 配置 NAT 规则中源地址转换方式。

NO-PAT 方式：

```
action snat object-group ipv6-object-group-name no-pat [ vrf vrf-name ]
```

PAT 方式：

```
action snat object-group ipv6-object-group-name [ vrf vrf-name ]
```

静态地址转换方式：

```
action snat static ip-address global-ipv6-address [ ipv6-vrrp virtual-router-id ] [ vrf vrf-name ]
```

NPTv6 方式：

```
action snat nptv6 translated-ipv6-prefix nptv6-prefix-length [ vrf vrf-name ]
```

NO-NAT 方式：

```
action snat no-nat
```

- 配置 NAT 规则的目的地址转换方式。

服务器映射方式：

```
action dnat ip-address local-ipv6-address [ local-port local-port ] [ vrf vrf-name ]
```

NPTv6 方式：

```
action dnat nptv6 translated-ipv6-prefix nptv6-prefix-length [ vrf vrf-name ]
```

NO-NAT 方式：

```
action dnat no-nat
```

(7) （可选）开启 NAT 规则命中统计功能。

```
counting enable
```

缺省情况下，NAT 规则命中统计功能处于关闭状态。

2.5.7 移动 NAT 规则

1. 功能简介

NAT 规则的位置越靠前，则其具有更高的匹配优先级。对于需要调整 NAT 规则匹配顺序的场景，请使用本功能移动 NAT 规则的位置，从而灵活调整规则的匹配优先级顺序。

调整 NAT 规则的位置会修改规则的匹配优先级的值，优先级的值越小，则匹配优先级越高。具体机制为：

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

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

在全局 NAT 策略视图下，可通过执行 **display this** 命令查看 NAT 规则的匹配优先级顺序。匹配优先级顺序受规则创建顺序和规则中包含的转换动作类型的影响，具体如下：

- “DNAT 规则”和“SNAT+DNAT 规则”的匹配优先级高于所有“SNAT 规则”
- “DNAT 规则”和“SNAT+DNAT 规则”的匹配优先级顺序与创建顺序有关，先创建的规则拥有较高的匹配优先级。
- 当新建“DNAT 规则”或“SNAT+DNAT 规则”时，该规则位于所有已存在的“DNAT 规则”以及“SNAT+DNAT 规则”之后，即该规则的匹配优先级低于所有已存在的“DNAT 规则”以及“SNAT+DNAT 规则”。
- “SNAT 规则”的匹配优先级与创建顺序有关，先创建的规则拥有较高的匹配优先级。
- 当新建“SNAT 规则”时，该规则在所有已有的“SNAT 规则”之后，即该规则的匹配优先级低于所有已存在的“SNAT 规则”。

一旦设备匹配到了“DNAT 规则”或者“SNAT+DNAT 规则”，就不会再匹配“SNAT 规则”。用户可以通过移动 NAT 规则来调整匹配优先级顺序，但是需确保所有的“DNAT 规则”和“SNAT+DNAT 规则”位于“SNAT 规则”之前：

- 不允许将“DNAT 规则”或“SNAT+DNAT 规则”移动到“SNAT 规则”之后。
- 不允许将“SNAT 规则”移动到“DNAT 规则”或“SNAT+DNAT 规则”之前。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入全局 NAT 策略视图。

```
nat global-policy
```

- (3) 修改 NAT 规则的优先级顺序。

```
rule move rule-name1 [ type { nat | nat64 | nat66 } ] { after | before }
[ rule-name2 ] [ type { nat | nat64 | nat66 } ]
```

通过本命令只能调整已经存在的 NAT 规则的匹配优先级顺序。

调整 NAT 规则的匹配优先级顺序时，可以不指定规则类型。若指定了规则类型，建议指定准确的类型。

2.5.8 禁用 NAT 规则

1. 功能简介

配置本功能后，相应的 NAT 规则将不再生效，但是不会将此 NAT 规则删除。如果不再需要此 NAT 规则，需要执行 **undo rule name** 命令才能将其删除。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入全局 NAT 策略视图。

```
nat global-policy
```

- (3) 进入 NAT 规则视图。

```
rule name rule-name [ type { nat | nat64 | nat66 } ]
```

- (4) 禁用 NAT 规则中的地址转换映射。

```
disable
```

缺省情况下，NAT 规则中的地址转换映射处于开启状态。

2.6 配置NAT地址组

1. 功能简介

一个 NAT 地址组是多个地址成员的集合。在全局 NAT 中，NAT 类型的 SNAT 规则可以通过引用 NAT 地址组，将 NAT 地址组中的地址成员作为地址转换后的地址。

2. 配置步骤

- (1) 创建 NAT 地址组，并进入 NAT 地址组视图。

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

- (2) （可选）配置 NAT 地址组的描述信息。

```
description text
```

缺省情况下，未配置 NAT 地址组的描述信息。

- (3) 添加地址成员。下面两种方法互斥，请选择其中一项进行配置。

- 将 IP 地址段作为 NAT 地址组中的地址成员。

```
address start-address end-address
```

可通过多次执行本命令添加多个地址组成员。

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。

如果 IP 地址段的某些 IP 地址不能用于地址转换，可通过如下命令配置禁止用于地址转换的 IP 地址。

```
exclude-ip start-address end-address
```

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。

- 将接口的 IP 地址作为 NAT 地址组中的地址成员，即实现 Easy IP 功能。

```
address interface interface-type interface-number
```

缺省情况下，未指定接口地址作为地址成员。

在同一个 NAT 地址组中，通过本命令只能将一个接口的地址作为地址成员。

- (4) （可选）配置端口范围。

```
port-range start-port-number end-port-number
```

缺省情况下，端口范围为 1~65535。

该配置仅对 PAT 方式地址转换生效。

- (5) （可选）配置端口块参数。

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

缺省情况下，未配置 NAT 地址组的端口块参数。

该配置仅对 PAT 方式地址转换生效。

2.7 配置 NAT ALG

1. 配置限制和指导

对于全局 NAT，**nat alg** 命令仅对使用 NAT 类型规则的全局 NAT 策略生效。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启指定或所有协议类型的 NAT ALG 功能。

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

缺省情况下，DNS、FTP、ICMP 差错报文、PPTP、RTSP 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。

2.8 配置 NAT DNS mapping 功能

1. 功能简介

NAT DNS mapping 功能适用于 DNS 服务器在公网、私网用户希望通过域名来访问私网内部服务器的场景中，用于将 DNS 响应报文载荷中内部服务器域名对应的公网 IP 替换为私网 IP，从而让私网用户使用替换后的私网 IP 访问内部服务器。

DNS mapping 功能需要和服务器映射方式的地址转换配置配合使用：

- (1) DNS mapping 建立“内部服务器域名<-->外网 IP 地址+外网端口号+协议类型”的映射关系。
- (2) 服务器映射方式的地址转换配置中，用于匹配报文目的 IP 地址的过滤条件指定了内部服务器对外提供服务的公网 IP 地址，用于匹配报文携带的服务类型的过滤条件指定了内部服务器对外提供的服务类型以及端口号，转换动作指定了内部服务器公网 IP 地址转换后的私网 IP 地址。
- (3) NAT 设备收到 DNS 响应报文后，根据报文中的域名查找 DNS mapping 映射表，并根据表项内的“公网地址+公网端口+协议类型”信息查找服务器映射方式的地址转换配置中该信息对应的私网地址，替换 DNS 查询结果中的公网地址。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 DNS 协议类型的 NAT ALG 功能。

```
nat alg dns
```

缺省情况下，DNS 协议类型的 NAT ALG 功能处于开启状态。

- (3) 配置一条域名到内部服务器的映射。

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

可配置多条域名到内部服务器的映射。

2.9 配置NAT发送免费ARP报文功能

1. 功能简介

缺省情况下，NAT 模块会发送免费 ARP 报文，向同一局域网内所有节点通告 NAT 公网 IP 地址与 MAC 地址的对应关系，并且会回应同一局域网内其他节点发送的免费 ARP。当 NAT 公网地址较多时，发送免费 ARP 耗时较长，可能会导致 ARP 业务异常。这种情况下，为了保证 ARP 业务正常运行，可以暂时关闭此功能。关闭此功能后，NAT 不再发送免费 ARP 报文，仅回应同一局域网内其他节点发送的免费 ARP。

2. 配置限制和指导

关闭 NAT 发送免费 ARP 报文通告公网 IP 地址与 MAC 地址对应关系的功能后，当 NAT 公网地址或 NAT 公网地址对应的 VRRP 变更、接口 MAC 或虚 MAC 变更、等价出口的链路震荡等，NAT 模块不会主动发送免费 ARP，可能会导致同一局域网内其他节点不能及时更新 MAC 地址表项，从而引发业务异常。请谨慎使用。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 NAT 发送免费 ARP 报文功能。

```
nat gratuitous-arp enable
```

缺省情况下，NAT 发送免费 ARP 报文功能处于开启状态。

2.10 配置NAT支持HA

2.10.1 功能简介

在单台 NAT 设备的组网中，一旦发生单点故障，内网用户将无法与外网通信。采用 HA 可以很好的避免上述情况的发生。在 HA 组网中的两台设备均可承担 NAT 业务，并通过 HA 通道进行会话热备、会话关联表热备、NAT 端口块表项热备以及 NAT 配置的同步。当其中一台设备故障后流量自动切换到另一台正常工作的设备。

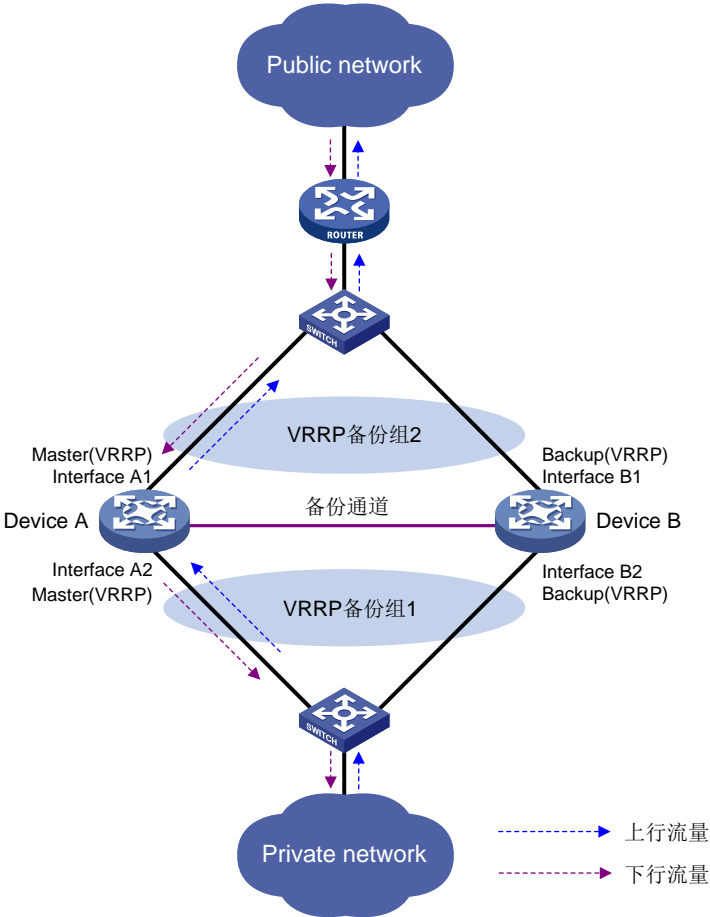
关于 HA 的详细介绍，请参见“高可靠性配置指导”中的“双机热备（RBM）”。

2.10.2 工作机制

HA 组网中的两台设备均可承担 NAT 业务，实际处理 NAT 业务的设备由 VRRP 备份组中的 Master 设备承担。下面以主备模式的 HA 为例，介绍该场景中当 Master 设备发生故障时如何保证 NAT 业务不中断。

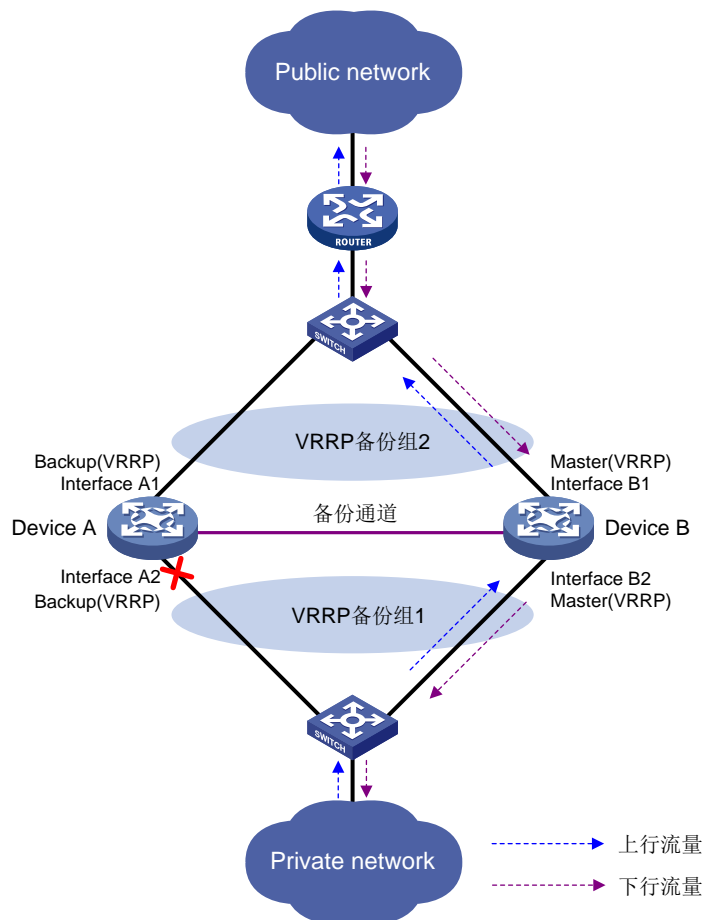
如图 2-1 所示，Device A 和 Device B 组成 HA（Device A 为 HA 的主管理设备，Device B 为 HA 的从管理设备），Device A 通过备份通道将会话表项、会话关联表项和端口块表项实时备份到 Device B。同时，Device A 和 Device B 的下行链路组成 VRRP 备份组 1，上行链路组成 VRRP 备份组 2，并将 VRRP 和 HA 关联。HA 根据链路状态或设备的转发能力选择 Device A 作为 Master 设备，正常情况下，由 Device A 进行地址转换。

图2-1 主备模式的 HA 组网



如图 2-2 所示，当 Device A 的接口 Interface A2 发生故障时，Device B 在 VRRP 备份组中的状态由 Backup 变为 Master，由于 Device B 上已经有相关的 NAT 配置信息和业务表项，因此可以保证链路切换后的 NAT 业务不中断。

图2-2 主备模式下的流量切换



2.10.3 配置主备模式下的 NAT

1. 功能简介

在主备模式的 HA 组网中，静态 IP 地址转换、源 IP 地址转换、目的 IP 地址转换的部分转换规则会将转换后的公网 IP 地址或内部服务器对外提供服务的公网 IP 地址下发到地址管理。然后，主、备设备均会向同一局域网内所有节点或本地链路范围内所有节点通告公网 IP 与自身物理接口 MAC 地址的对应关系。导致与 HA 直连的上行三层设备可能会将下行报文发送给 HA 中的 Backup 设备，从而影响业务的正常运行。

为了避免上述情况的发生，需要将地址转换方式与 VRRP 备份组绑定。执行绑定操作后，仅 Master 设备收到对转换后 IP 地址或内部服务器对外提供服务的公网 IP 地址的 ARP 请求或 NS 请求后，才会回应 ARP 响应报文或 NA 响应报文，响应报文中携带的 MAC 地址为此 VRRP 备份组的虚拟 MAC 地址。有关 HA 的详细介绍，请参见“高可靠性配置指导”中的“双机热备（RBM）”。

2. 配置限制和指导

请在 HA 的主管理设备的 NAT 规则视图下将地址转换方式与 VRRP 备份组绑定，该备份组的虚拟 IP 与转换后的 IP 地址或内部服务器对外提供服务的公网 IP 地址在同一网段。

3. 配置步骤（NAT 类型规则）

- (1) 进入系统视图。

```
system-view
```

- (2) 进入全局 NAT 策略视图。

```
nat global-policy
```

- (3) 进入 NAT 规则视图。

```
rule name rule-name [ type nat ]
```

- (4) 将地址转换方式与 VRRP 备份组绑定。请根据网络需求选择其中一项或多项进行配置。

- NO-PAT 方式源地址转换与 VRRP 绑定。

```
action snat address-group { group-id | name group-name } no-pat  
[ reversible ] vrrp virtual-router-id
```

- PAT 方式源地址转换与 VRRP 绑定。

```
action snat address-group { group-id | name group-name }  
[ port-preserved ] vrrp virtual-router-id
```

- 静态方式源地址转换与 VRRP 绑定。

```
action snat static { ip-address global-address | object-group  
object-group-name | subnet subnet-ip-address mask-length } vrrp  
virtual-router-id
```

- 服务器映射方式目的地址转换与 VRRP 绑定。

```
action dnat { ip-address local-address | object-group  
ipv4-object-group-name } [ local-port { local-port1 [ to  
local-port2 ] } <1-32> ] vrrp virtual-router-id
```

缺省情况下，地址转换方式未绑定任何 VRRP 备份组。

4. 配置步骤（NAT64 类型规则）

- (1) 进入系统视图。

```
system-view
```

- (2) 进入全局 NAT 策略视图。

```
nat global-policy
```

- (3) 进入 NAT 规则视图。

```
rule name rule-name type nat64
```

- (4) 将地址转换方式与 VRRP 备份组绑定。请根据网络需求选择其中一项或多项进行配置。

- NO-PAT 方式源地址转换与 VRRP 绑定。

```
action snat object-group ipv4-object-group-name no-pat [ ipv4-vrrp  
virtual-router-id ] [ vrf vrf-name ]
```

- PAT 方式源地址转换与 VRRP 绑定。

```
action snat object-group ipv4-object-group-name [ ipv4-vrrp  
virtual-router-id ] [ vrf vrf-name ]
```

- IPv6 到 IPv4 静态方式源地址转换与 VRRP 绑定。

```
action snat static ip-address global-ipv4-address [ ipv4-vrrp  
virtual-router-id ] [ vrf vrf-name ]
```

- IPv4 到 IPv6 静态方式源地址转换与 VRRP 绑定。

```
action snat static ip-address global-ipv6-address [ ipv6-vrrp  
virtual-router-id ] [ vrf vrf-name ]
```

- IPv6 到 IPv4 静态方式目的地址转换与 VRRP 绑定。

```
action dnat static ip-address local-ipv4-address [ ipv6-vrrp  
virtual-router-id ] [ vrf vrf-name ]
```

- IPv4 到 IPv6 静态方式目的地址转换与 VRRP 绑定。

```
action dnat static ip-address local-ipv6-address [ ipv4-vrrp  
virtual-router-id ] [ vrf vrf-name ]
```

- IPv4 到 IPv6 服务器映射方式目的地址转换与 VRRP 绑定。

```
action dnat server ip-address local-ipv6-address [ local-port  
local-port ] [ ipv4-vrrp virtual-router-id ] [ vrf vrf-name ]
```

- IPv4 到 IPv6 前缀方式目的地址转换与 VRRP 绑定。

```
action dnat prefix { general v4tov6 prefix-general prefix-length |  
ivi v4tov6 prefix-ivi } [ ipv4-vrrp virtual-router-id ] [ vrf  
vrf-name ]
```

缺省情况下，地址转换方式未绑定任何 VRRP 备份组。

5. 配置步骤（NAT66 类型规则）

- (1) 进入系统视图。

```
system-view
```

- (2) 进入全局 NAT 策略视图。

```
nat global-policy
```

- (3) 进入 NAT 规则视图。

```
rule name rule-name type nat66
```

- (4) 将静态方式源地址转换与 VRRP 备份组绑定。

```
action snat static ip-address global-ipv6-address [ ipv6-vrrp  
virtual-router-id ] [ vrf vrf-name ]
```

缺省情况下，静态方式源地址转换未绑定任何 VRRP 备份组。

2.10.4 配置双主模式下的 NAT

1. 功能简介

在双主模式的 HA 组网中，两台设备互为主备，仍然可能出现与 HA 直连的上行三层设备将下行报文发送给 HA 中的 Backup 设备，从而影响业务正常运行的情况。

为了避免上述情况的发生，需要将地址转换方式与 VRRP 备份组绑定。执行绑定操作后，仅 Master 设备收到对转换后 IP 地址或内部服务器对外提供服务的公网 IP 地址的 ARP 请求或 NS 请求后，才会回应 ARP 响应报文或 NA 响应报文，响应报文中携带的 MAC 地址为此 VRRP 备份组的虚拟 MAC 地址。有关 HA 的详细介绍，请参见“高可靠性配置指导”中的“双机热备（RBM）”。

2. 配置限制和指导

请根据不同的情况选择不同的配置方式：

- 双主模式的 HA 组网中，两台设备的 NAT 规则可以共用同一个 NAT 地址组时，需要注意的是，为了防止不同的 Master 设备将不同主机的流量转换为同一个地址和端口号，需要使用 PAT 方式的地址转换，并配置 `nat remote-backup port-alloc` 命令，使得不同的 Master 设备使用不同范围的端口资源。
- 除上述情况外，建议双主模式 HA 组网中的两台设备使用不同的公网 IP 进行地址转换，避免出现不同的 Master 设备对不同主机的流量进行地址转换后，地址转换的结果相同的情况。例如，当 HA 中的两台设备使用不同地址范围的 NAT 地址组时（通过 NAT 规则匹配用户流量，实现不同源 IP 地址范围的用户流量使用不同的 NAT 地址组进行地址转换），不同的内网用户设置不同的网关地址，使得正向地址转换的流量由不同的 Master 设备进行处理。请在 HA 的主管理设备上将使用不同的 NAT 地址组进行地址转换的地址转换方式与不同的 VRRP 备份组绑定，从而引导反向地址转换的流量使用不同的 Master 设备进行地址转换，实现 NAT 业务的负载分担。

请在 HA 的主管理设备的 NAT 规则视图下将地址转换方式与 VRRP 备份组绑定，该备份组的虚拟 IP 与转换后的 IP 地址或内部服务器对外提供服务的公网 IP 地址在同一网段。

3. 配置步骤（NAT 类型规则）

- (1) 进入系统视图。

```
system-view
```

- (2) 进入全局 NAT 策略视图。

```
nat global-policy
```

- (3) 进入 NAT 规则视图。

```
rule name rule-name [ type nat ]
```

- (4) 将地址转换方式与 VRRP 备份组绑定。请根据网络需求选择其中一项或多项进行配置。

- NO-PAT 方式源地址转换与 VRRP 绑定。

```
action snat address-group { group-id | name group-name } no-pat  
[ reversible ] vrrp virtual-router-id
```

- PAT 方式源地址转换与 VRRP 绑定。

```
action snat address-group { group-id | name group-name }  
[ port-preserved ] vrrp virtual-router-id
```

- 静态方式源地址转换与 VRRP 绑定。

```
action snat static { ip-address global-address | object-group  
object-group-name | subnet subnet-ip-address mask-length } vrrp  
virtual-router-id
```

- 服务器映射方式目的地址转换与 VRRP 绑定。

```
action dn timer { ip-address local-address | object-group  
ipv4-object-group-name } [ local-port { local-port1 [ to  
local-port2 ] } <1-32> ] vrrp virtual-router-id
```

缺省情况下，地址转换方式未绑定任何 VRRP 备份组。

- (5) （可选）指定 HA 中主、从管理设备可以使用的 NAT 端口块范围。

- a. 退回全局 NAT 策略视图。

quit

- b. 退回系统视图。

quit

- c. 指定 HA 中主、从管理设备可以使用的 NAT 端口块范围。

nat remote-backup port-alloc { primary | secondary }

缺省情况下，HA 中的主、从管理设备共用 NAT 端口资源。

参数	功能
primary	表示使用数值较小的一半端口
secondary	表示使用数值较大的一半端口

4. 配置步骤（NAT64 类型规则）

- (1) 进入系统视图。

system-view

- (2) 进入全局 NAT 策略视图。

nat global-policy

- (3) 进入 NAT 规则视图。

rule name rule-name type nat64

- (4) 将地址转换方式与 VRRP 备份组绑定。请根据网络需求选择其中一项或多项进行配置。

- o NO-PAT 方式源地址转换与 VRRP 绑定。

action snat object-group ipv4-object-group-name no-pat [ipv4-vrrp virtual-router-id] [vrf vrf-name]

- o PAT 方式源地址转换与 VRRP 绑定。

action snat object-group ipv4-object-group-name [ipv4-vrrp virtual-router-id] [vrf vrf-name]

- o IPv6 到 IPv4 静态方式源地址转换与 VRRP 绑定。

action snat static ip-address global-ipv4-address [ipv4-vrrp virtual-router-id] [vrf vrf-name]

- o IPv4 到 IPv6 静态方式源地址转换与 VRRP 绑定。

action snat static ip-address global-ipv6-address [ipv6-vrrp virtual-router-id] [vrf vrf-name]

- o IPv6 到 IPv4 静态方式目的地址转换与 VRRP 绑定。

action dnat static ip-address local-ipv4-address [ipv6-vrrp virtual-router-id] [vrf vrf-name]

- o IPv4 到 IPv6 静态方式目的地址转换与 VRRP 绑定。

action dnat static ip-address local-ipv6-address [ipv4-vrrp virtual-router-id] [vrf vrf-name]

- o IPv4 到 IPv6 服务器映射方式目的地址转换与 VRRP 绑定。

```
action dnat server ip-address local-ipv6-address [ local-port  
local-port ] [ ipv4-vrrp virtual-router-id ] [ vrf vrf-name ]
```

- IPv4 到 IPv6 前缀方式目的地址转换与 VRRP 绑定。

```
action dnat prefix { general v4tov6 prefix-general prefix-length |  
ivi v4tov6 prefix-ivi } [ ipv4-vrrp virtual-router-id ] [ vrf  
vrf-name ]
```

缺省情况下，地址转换方式未绑定任何 VRRP 备份组。

5. 配置步骤（NAT66 类型规则）

- (1) 进入系统视图。

```
system-view
```

- (2) 进入全局 NAT 策略视图。

```
nat global-policy
```

- (3) 进入 NAT 规则视图。

```
rule name rule-name type nat66
```

- (4) 将静态方式源地址转换与 VRRP 备份组绑定。

```
action snat static ip-address global-ipv6-address [ ipv6-vrrp  
virtual-router-id ] [ vrf vrf-name ]
```

缺省情况下，静态方式源地址转换未绑定任何 VRRP 备份组。

2.11 特定条件下的NAT配置

2.11.1 开启反向报文的重定向功能

1. 功能简介

在入方向动态地址转换功能与隧道功能配合使用的组网环境中，若多个隧道接口引用同一个 NAT 地址组，则设备会将来自不同隧道的报文的源 IP 地址转换为相同的 NAT 地址，并从设备的出接口转发出去。缺省情况下，设备出接口收到反向报文后，不会查询 NAT 会话表项，这将导致反向报文不能正确转发。为解决此问题，可在设备的出接口开启反向报文的重定向功能，使出接口收到反向报文后查询 NAT 会话表项，根据 NAT 会话表项记录的信息将反向报文的目的 IP 地址进行 NAT 地址转换，从而使反向报文通过接收正向报文的隧道发送出去。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 开启反向报文的重定向功能。

```
nat redirect reply-route enable
```

缺省情况下，反向报文的重定向功能处于关闭状态。

2.11.2 开启对 TCP SYN 和 SYN ACK 报文中时间戳的删除功能

1. 功能简介

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

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

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启对 TCP SYN 和 SYN ACK 报文中时间戳的删除功能。

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

缺省情况下，不对 TCP SYN 和 SYN ACK 报文中的时间戳进行删除。

多次执行本命令，可为不同 VPN 中的报文开启此功能。

2.12 配置 NAT 维护功能

2.12.1 配置 NAT 定时统计功能

1. 功能简介

开启 NAT 定时统计功能后，NAT 将按照一定的时间间隔对每个地址组中的会话数目和端口块分配冲突计数进行统计。

2. 配置限制和指导

使用本功能可能会占用较多的 CPU 资源，当 CPU 资源紧张时，可将其关闭。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 NAT 定时统计功能。

```
nat periodic-statistics enable
```

缺省情况下，NAT 定时统计功能处于关闭状态。

- (3) 配置 NAT 定时统计功能的时间间隔。

```
nat periodic-statistics interval interval
```

缺省情况下，NAT 定时统计功能的时间间隔为 300 秒。

如果将 NAT 定时统计功能的时间间隔调小，会占用较多的 CPU 资源。通常情况下，建议使用缺省值。

2.12.2 配置全局 NAT 策略中 NAT 类型的 SNAT+DNAT 规则的源 IP 地址转换和目的 IP 转换先于安全策略匹配，以便与老版本兼容

1. 功能简介

本功能用于解决如下场景中新老版本不兼容的问题。

设备进行软件版本升级前，当全局 NAT 策略中使用 SNAT+DNAT 规则时，设备先进行源 IP 和目的 IP 转换，然后使用转换后的源 IP 和目的 IP 匹配安全策略。

设备升级软件版本后，当全局 NAT 策略中使用 SNAT+DNAT 规则时，设备会先进行目的 IP 转换，然后使用转换前的源 IP 和转换后的目的 IP 匹配安全策略，最后进行源 IP 转换。这样会导致软件版本升级前后的处理方式不兼容。

为了解决上述问题，设备进行软件升级过程中，会自从生成并下发 **nat global-policy compatible-previous-version rule-type ipv4-snat-and-dnat translate-before-secp** 命令并保存此配置。

2. 配置限制和指导

本功能仅用于兼容老版本，不建议用户手工配置。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置全局 NAT 策略中 NAT 类型的 SNAT+DNAT 规则的源 IP 地址转换和目的 IP 转换先于安全策略匹配，以便与老版本兼容。

```
nat global-policy compatible-previous-version rule-type  
ipv4-snat-and-dnat translate-before-secp
```

缺省情况下，设备先进行全局 NAT 策略中 NAT 类型的 SNAT+DNAT 规则的目的 IP 转换，然后使用转换前的源地址和转换后的目的地址匹配安全策略，最后进行全局 NAT 策略中 NAT 类型的 SNAT+DNAT 规则的源 IP 转换。

2.12.3 开启新建 NAT 会话速率的统计功能

1. 功能简介

开启此功能后，设备会对新建 NAT 会话的速率进行统计，统计信息可以通过 **display nat statistics** 命令查看。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启新建 NAT 会话速率的统计功能。

```
nat session create-rate enable
```

缺省情况下，新建 NAT 会话速率的统计功能处于关闭状态。

2.12.4 配置检测 NAT 地址组成员的可用性

1. 功能简介

通过在地址组中引用 NQA 模板来实现检测 NAT 地址组中地址可用性的目的。关于 NQA 的详细介绍，请参见“网络管理和监控配置指导”中的“NQA”。

检测 NAT 地址组成员可用性的详细过程如下：

- (1) 引用 NQA 探测模板后，设备会周期性地向 NQA 模板中指定的目的地址依次发送探测报文，其中各探测报文的源 IP 地址是地址池中的 IP 地址。
- (2) 若设备在当前探测周期内没有收到 NQA 探测应答报文，则将该探测报文的源 IP 地址从地址池中排除，即在本探测周期内禁止该 IP 地址用于地址转换。
- (3) 下一个探测周期重复以上过程。被排除的 IP 地址也会重新进行可用性探测。

2. 配置限制和指导

一个 NAT 地址组视图下，可指定多个 NQA 探测模板。当指定多个 NQA 探测模板时，只要有一个 NQA 探测模板探测成功，则表示该地址可用于地址转换。

本功能仅对用于出方向地址转换的地址成员的可用性进行检测。不对通过 **exclude-ip** 命令配置的禁止用于地址转换的 IP 地址的可用性进行检测。

引用的 NQA 探测模板中，不能配置探测报文的源 IP 地址。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 NAT 地址组视图。

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

- (3) 指定 NAT 地址组中地址成员的检测方法。

```
probe template-name
```

缺省情况下，未指定 NAT 地址组中地址成员的检测方法。

指定的检测方法可以不存在，但要使检测功能生效，必须通过 **nqa template** 命令创建检测方法所使用的 NQA 模板。

2.12.5 开启 NAT 转换失败发送 ICMP 差错报文功能

1. 功能简介

缺省情况下，NAT 设备对 ICMP 报文的地址转换失败时，不会发送 ICMP 差错报文，从而导致使用 ICMP 协议报文的应用无法感知此事件。开启本功能后，NAT 设备对 ICMP 报文地址转换失败时，会发送 ICMP 差错报文，使用 ICMP 协议报文的应用根据收到的 ICMP 差错报文发现和定位问题。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启设备 NAT 对 ICMP 报文转换失败发送 ICMP 差错报文功能。

```
nat icmp-error reply
```

缺省情况下，NAT 设备对 ICMP 报文地址转换失败时，设备不发送 ICMP 差错报文。

2.13 配置 NAT 日志功能

2.13.1 配置 NAT 会话日志功能

1. 功能简介

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。NAT 活跃流日志仅支持通过 Flow 日志输出方式发送到日志主机，不支持以快速日志输出方式发送。关于通过 Flow 日志输出方式发送到日志主机的相关介绍，请参见“网络管理和监控配置指导”中的“Flow 日志”。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 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。

- (3) 开启 NAT 相关日志功能。请至少选择其中一项进行配置。

- 开启 NAT 新建会话的日志功能。

```
nat log flow-begin
```

- 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
```

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。

2.13.2 配置 NAT444 用户日志功能

1. 功能简介

NAT444 用户日志是为了满足互联网用户溯源的需要，在 NAT444 地址转换中，对每个用户的私网 IP 地址进行端口块分配或回收时，都会输出一条基于用户的日志，记录私网 IP 地址和端口块的映射关系。在进行用户溯源时，只需根据报文的公网 IP 地址和端口找到对应的端口块分配日志信息，即可确定私网 IP 地址。

有两种情况可以触发设备输出 NAT444 用户日志：

- 端口块分配：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输出日志。
- 端口块回收：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）时输出日志。

2. 配置准备

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

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 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。

ACL 参数对 NAT444 用户日志功能无效。

- (3) 开启端口块用户日志功能。请至少选择其中一项进行配置。

- 开启端口块分配的 NAT444 用户日志功能。

```
nat log port-block-assign
```

- 开启端口块回收的 NAT444 用户日志功能。

```
nat log port-block-withdraw
```

缺省情况下，分配和回收端口块时，均不输出 NAT444 用户日志。

2.13.3 配置 NAT 告警信息日志功能

1. 功能简介

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的资源无法对其进行地址转换，相应的报文将被丢弃。本命令用来在 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；在 NAT444 地址转换中，NAT 资源是指公网 IP、端口块和端口块中的端口。

NAT444 端口块动态映射方式中，当端口块分配失败时，系统会输出日志信息。

NAT444 端口块动态映射方式中，当端口块中的端口资源都用尽但还是无法满足用户的地址转换需求时，系统会输出日志信息。

2. 配置限制和指导

只有开启 NAT 日志功能（通过 `nat log enable` 命令）之后，NAT 告警信息日志功能才能生效。

3. 配置准备

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

4. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 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。

ACL 参数对 NAT 告警信息日志功能无效。

- (3) 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。

NAT 资源用尽时，系统会输出告警日志。

- (4) （可选）配置动态 NAT444 端口块使用率的阈值。

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

缺省情况下，动态 NAT444 的端口块使用率的阈值为 90%。

创建动态端口块表项时，若端口块的使用率大于阈值，系统会输出告警日志。

2.13.4 开启 NO-PAT 方式下 NAT 地址组中地址成员使用率的日志信息功能

1. 功能简介

创建 NO-PAT 表项时，若 NO-PAT 方式下 NAT 地址组中地址成员的使用率超过设定的百分比时，系统将会输出日志信息。

2. 配置限制和指导

只有开启 NAT 日志功能（通过 **nat log enable** 命令）之后，NAT 地址组中地址成员使用率的日志信息功能才能生效。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 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。

ACL 参数对 NO-PAT 方式下 NAT 地址组中地址成员使用率的日志信息功能无效。

- (3) 开启 NO-PAT 方式下 NAT 地址组中地址成员使用率的日志信息功能，并设置 NAT 地址组中地址成员使用率的阈值。

```
nat log no-pat ip-usage [ threshold value ]
```

缺省情况下，NAT 地址组中地址成员使用率的日志信息功能处于关闭状态。

2.14 全局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2-1 全局 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 [<i>group-id</i>]
显示NAT日志功能的配置信息	display nat log
显示NAT NO-PAT表项信息	(独立运行模式) display nat no-pat { <i>ipv4</i> <i>ipv6</i> } [<i>slot slot-number</i> [<i>cpu cpu-number</i>]] (IRF模式) display nat no-pat { <i>ipv4</i> <i>ipv6</i> } [<i>chassis chassis-number slot slot-number</i> [<i>cpu cpu-number</i>]]
显示NO-PAT方式下NAT地址组中地址成员的使用率	(独立运行模式) display nat no-pat ip-usage [<i>address-group</i> { <i>group-id</i> <i>name group-name</i> } <i>object-group object-group-name</i>] [<i>slot slot-number</i> [<i>cpu cpu-number</i>]] (IRF模式) display nat no-pat ip-usage [<i>address-group</i> { <i>group-id</i> <i>name group-name</i> } <i>object-group object-group-name</i>] [<i>chassis chassis-number slot slot-number</i> [<i>cpu cpu-number</i>]]
显示NAT定时统计功能的计数信息	(独立运行模式) display nat periodic-statistics { <i>address-group</i> [<i>group-id</i> <i>name group-name</i>] <i>ip global-ip</i> } [<i>slot slot-number</i> [<i>cpu cpu-number</i>]] (IRF模式) display nat periodic-statistics { <i>address-group</i> [<i>group-id</i> <i>name group-name</i>] <i>ip global-ip</i> } [<i>chassis chassis-number slot slot-number</i> [<i>cpu cpu-number</i>]]

操作	命令
显示NAT会话	<p>(独立运行模式)</p> <pre>display nat session [[responder] { source-ip source-ip destination-ip destination-ip } * [vpn-instance vpn -instance-name]] [slot slot-number [cpu cpu-number]] [verbose]</pre> <p>(IRF模式)</p> <pre>display nat session [[responder] { source-ip source-ip destination-ip destination-ip } * [vpn-instance vpn -instance-name]] [chassis chassis-number slot slot-number [cpu cpu-number]] [verbose]</pre>
显示NAT统计信息	<p>(独立运行模式)</p> <pre>display nat statistics [summary] [slot slot-number [cpu cpu-number]]</pre> <p>(IRF模式)</p> <pre>display nat statistics [summary] [chassis chassis-number slot slot-number [cpu cpu-number]]</pre>
显示端口块表项	<p>(独立运行模式)</p> <pre>display nat port-block dynamic [address-group { group-id name group-name }] [slot slot-number [cpu cpu-number]]</pre> <p>(IRF模式)</p> <pre>display nat port-block dynamic [address-group { group-id name group-name }] [chassis chassis-number slot slot-number [cpu cpu-number]]</pre>
显示动态NAT444地址组中端口块的使用率	<p>(独立运行模式)</p> <pre>display nat port-block-usage [address-group group-id] [slot slot-number [cpu cpu-number]]</pre> <p>(IRF模式)</p> <pre>display nat port-block-usage [address-group group-id] [chassis chassis-number slot slot-number [cpu cpu-number]]</pre>
显示NAT地址组中地址成员的检测信息	<pre>display nat probe address-group [group-id]</pre>
清除NAT转换计数信息	<pre>reset nat count statistics { all dynamic global-policy server static }</pre>
清除NAT定时统计功能的计数信息	<p>(独立运行模式)</p> <pre>reset nat periodic-statistics [slot slot-number [cpu cpu-number]]</pre> <p>(IRF模式)</p> <pre>reset nat periodic-statistics [chassis chassis-number slot slot-number [cpu cpu-number]]</pre>

操作	命令
删除NAT会话	(独立运行模式) reset nat session [slot slot-number [cpu cpu-number]] (IRF模式) reset nat session [chassis chassis-number slot slot-number [cpu cpu-number]]

2.15 全局NAT典型配置举例

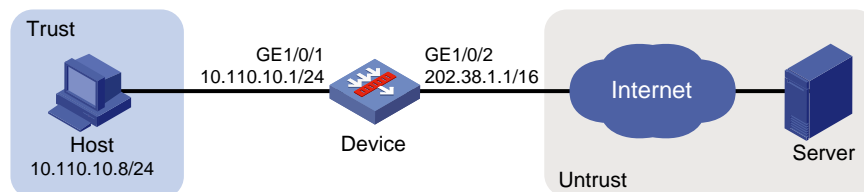
2.15.1 内网用户通过 NAT 地址访问外网配置举例（静态地址转换）

1. 组网需求

内部网络用户 10.110.10.8/24 使用外网地址 202.38.1.100 访问 Internet 中的地址为 201.20.1.1/24 的 Server。

2. 组网图

图2-3 内网用户通过 NAT 地址访问外网配置组网图（静态地址转换）



3. 配置步骤

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```

<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 10.110.10.1 24
[Device-GigabitEthernet1/0/1] quit
  
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 将接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```

[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 1/0/1
[Device-security-zone-Trust] quit
[Device] security-zone name untrust
[Device-security-zone-Untrust] import interface gigabitethernet 1/0/2
[Device-security-zone-Untrust] quit
  
```

(3) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达 Server 所在网络的下一跳 IP 地址为 202.38.1.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ip route-static 201.20.1.0 24 202.38.1.2
```

(4) 配置安全策略

配置名称为 trust-untrust 的安全策略，保证 Trust 安全域内的 Host 可以访问 Untrust 安全域中的 Server，具体配置步骤如下。

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-untrust
[Device-security-policy-ip-1-trust-untrust] source-zone trust
[Device-security-policy-ip-1-trust-untrust] destination-zone untrust
[Device-security-policy-ip-1-trust-untrust] source-ip-host 10.110.10.8
[Device-security-policy-ip-1-trust-untrust] destination-ip-host 201.20.1.1
[Device-security-policy-ip-1-trust-untrust] action pass
[Device-security-policy-ip-1-trust-untrust] quit
[Device-security-policy-ip] quit
```

(5) 配置 NAT 功能

配置内网 IP 地址 10.110.10.8 到外网地址 202.38.1.100 之间的一对一静态地址转换映射。

```
[Device] nat global-policy
[Device-nat-global-policy] rule name rule1
[Device-nat-global-policy-rule-rule1] source-ip host 10.110.10.8
[Device-nat-global-policy-rule-rule1] source-zone trust
[Device-nat-global-policy-rule-rule1] destination-zone untrust
[Device-nat-global-policy-rule-rule1] action snat static ip-address 202.38.1.100
```

4. 验证配置

以上配置完成后，内网主机可以访问外网服务器。通过查看如下显示信息，可以验证以上配置成功。

```
[Device] display nat global-policy
NAT global-policy information:
  Totally 1 NAT global-policy rules.
  Rule name: rule1
  Type                : nat
  SrcIP address       : 10.110.10.8
  Source-zone name    : Trust
  Destination-zone name : Untrust
  SNAT action:
```

```
Ipv4 address: 202.38.1.100
NAT counting : 0
Config status: Active
```

通过以下显示命令，可以看到 Host 访问某外网服务器时生成 NAT 会话信息。

```
[Device] display nat session verbose
Slot 1:
Initiator:
  Source      IP/port: 10.110.10.8/54765
  Destination IP/port: 201.20.1.1/23
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Trust
Responder:
  Source      IP/port: 201.20.1.1/23
  Destination IP/port: 202.38.1.100/54765
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Untrust
State: TCP_ESTABLISHED
Application: TELNET
Rule ID: -/-/-
Rule name:
Start time: 2017-05-19 10:57:47  TTL: 1195s
Initiator->Responder:          8 packets          375 bytes
Responder->Initiator:         10 packets          851 bytes

Total sessions found: 1
```

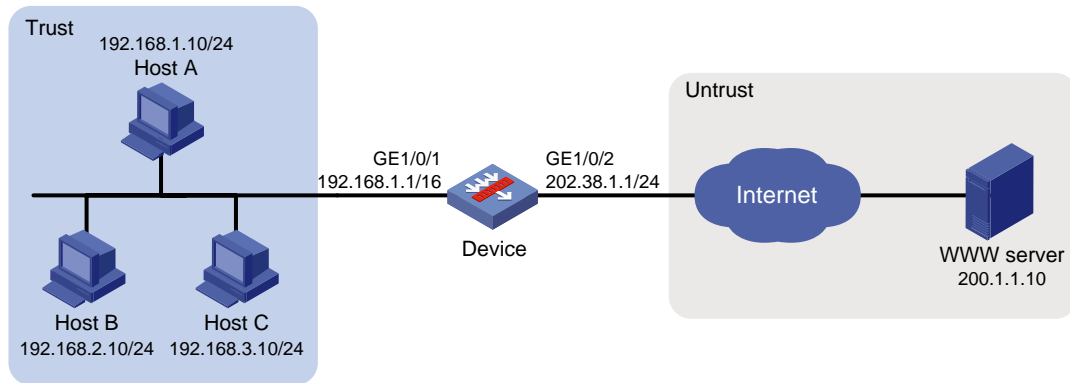
2.15.2 内网用户通过 NAT 地址访问外网配置举例（地址不重叠）

1. 组网需求

- 某公司内网使用的 IP 地址为 192.168.0.0/16。
- 该公司拥有 202.38.1.2 和 202.38.1.3 两个外网 IP 地址。
- 需要实现，内部网络中 192.168.1.0/24 网段的用户可以访问 Internet，其它网段的用户不能访问 Internet。使用的外网地址为 202.38.1.2 和 202.38.1.3。

2. 组网图

图2-4 内网用户通过 NAT 访问外网配置组网图（地址不重叠）



3. 配置步骤

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.1 16
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 将接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 1/0/1
[Device-security-zone-Trust] quit
[Device] security-zone name untrust
[Device-security-zone-Untrust] import interface gigabitethernet 1/0/2
[Device-security-zone-Untrust] quit
```

(3) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达 Server 所在网络的下一跳 IP 地址为 202.38.1.20，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ip route-static 200.1.1.0 24 202.38.1.20
```

(4) 配置安全策略

配置名称为 trust-untrust 的安全策略，保证 Trust 安全域内的 Host 可以访问 Untrust 安全域中的 Server，具体配置步骤如下。

```
[Device] security-policy ip
```

```
[Device-security-policy-ip] rule name trust-untrust
[Device-security-policy-ip-1-trust-untrust] source-zone trust
[Device-security-policy-ip-1-trust-untrust] destination-zone untrust
[Device-security-policy-ip-1-trust-untrust] source-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-1-trust-untrust] destination-ip-host 200.1.1.10
[Device-security-policy-ip-1-trust-untrust] action pass
[Device-security-policy-ip-1-trust-untrust] quit
[Device-security-policy-ip] quit
```

(5) 配置 NAT 功能

配置地址组 0，包含两个外网地址 202.38.1.2 和 202.38.1.3。

```
[Device] nat address-group 0
[Device-address-group-0] address 202.38.1.2 202.38.1.3
[Device-address-group-0] quit
```

配置地址对象组 obj1，仅允许对内部网络中 192.168.1.0/24 网段的用户报文进行地址转换。

```
[Device] object-group ip address obj1
[Device-obj-grp-ip-obj1] network subnet 192.168.1.0 24
[Device-obj-grp-ip-obj1] quit
```

配置全局 NAT 规则，允许使用地址组 0 中的地址对匹配的对象组 obj1 的报文进行源地址转换，并在转换过程中使用端口信息。

```
[Device] nat global-policy
[Device-nat-global-policy] rule name rule1
[Device-nat-global-policy-rule-rule1] source-ip obj1
[Device-nat-global-policy-rule-rule1] action snat address-group 0
```

4. 验证配置

以上配置完成后，Host A 能够访问 WWW server，Host B 和 Host C 无法访问 WWW server。通过查看如下显示信息，可以验证以上配置成功。

```
[Device] display nat all
NAT address group information:
  Totally 1 NAT address groups.
  Address group ID: 0
  Port range: 1-65535
  Address information:
    Start address      End address
    202.38.1.2         202.38.1.3
  Exclude address information:
    Start address      End address
    ---               ---
```

NAT global-policy information:

Totally 1 NAT global-policy rules.

Rule name: rule1

Type : nat

SrcIP object group : obj1

SNAT action:

Address group ID: 0

NO-PAT: N

Reversible: N

Port-preserved: N

NAT counting : 0

Config status: Active

NAT logging:

Log enable : Disabled

Flow-begin : Disabled

Flow-end : Disabled

Flow-active : Disabled

Port-block-assign : Disabled

Port-block-withdraw : Disabled

Alarm : Disabled

NO-PAT IP usage : Disabled

NAT mapping behavior:

Mapping mode : Address and Port-Dependent

ACL : ---

Config status: Active

NAT ALG:

DNS : Enabled

FTP : Enabled

H323 : Disabled

ICMP-ERROR : Enabled

ILS : Disabled

MGCP : Disabled

NBT : Disabled

PPTP : Enabled

```

RTSP      : Enabled
RSH       : Disabled
SCCP      : Disabled
SCTP      : Disabled
SIP       : Disabled
SQLNET    : Disabled
TFTP      : Disabled
XDMCP     : Disabled

Static NAT load balancing:      Disabled

NAT link-switch recreate-session: Disabled

NAT configuration-for-new-connection: Disabled

NAT global-policy compatible-previous-version rule-type ipv4-snat-and-dnat
translate-before-secp : Disabled

NAT gratuitous-arp: Enabled

```

通过以下显示命令，可以看到 Host A 访问 WWW server 时生成 NAT 会话信息。

```

[Device] display nat session verbose

Slot 1:

Initiator:

  Source      IP/port: 192.168.1.10/52082
  Destination IP/port: 200.1.1.10/80
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Trust

Responder:

  Source      IP/port: 200.1.1.10/80
  Destination IP/port: 202.38.1.2/1036
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Untrust

```

```

State: TCP_ESTABLISHED
Application: HTTP
Rule ID: -/-/-
Rule name:
Start time: 2017-05-19 16:16:59  TTL: 9995s
Initiator->Responder:          551 packets      32547 bytes
Responder->Initiator:          956 packets      1385514 bytes

Total sessions found: 1

```

2.15.3 外网用户通过外网地址访问内网服务器配置举例

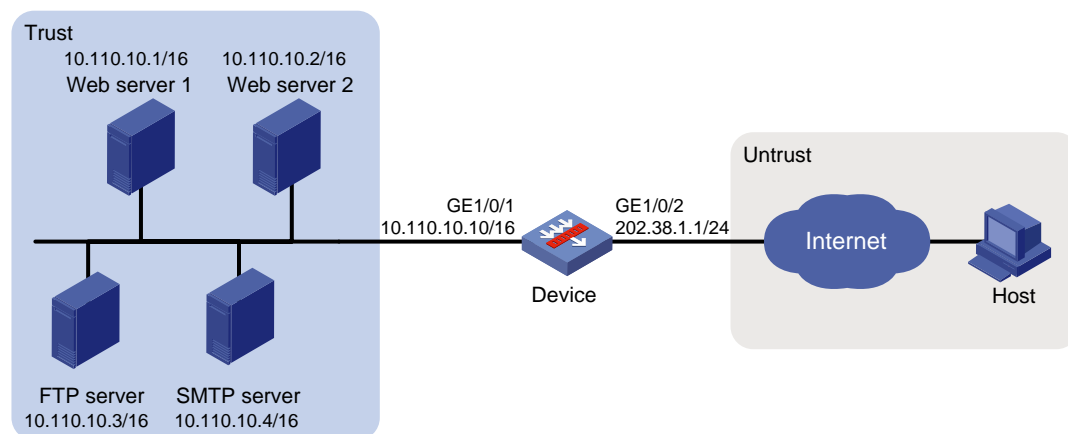
1. 组网需求

某公司内部对外提供 Web、FTP 和 SMTP 服务，而且提供两台 Web 服务器。公司内部网地址为 10.110.0.0/16。其中，内部 FTP 服务器地址为 10.110.10.3/16，内部 Web 服务器 1 的 IP 地址为 10.110.10.1/16，内部 Web 服务器 2 的 IP 地址为 10.110.10.2/16，内部 SMTP 服务器 IP 地址为 10.110.10.4/16。公司拥有 202.38.1.1 至 202.38.1.3 三个公网 IP 地址。要实现如下功能：

- 外部的主机可以访问内部的服务器。
- 选用 202.38.1.1 作为公司对外提供服务的 IP 地址，Web 服务器 2 对外采用 8080 端口。

2. 组网图

图2-5 外网用户通过外网地址访问内网服务器配置组网图



3. 配置步骤

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```

<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 10.110.10.10 16
[Device-GigabitEthernet1/0/1] quit

```


请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 将接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 1/0/1
[Device-security-zone-Trust] quit
[Device] security-zone name untrust
[Device-security-zone-Untrust] import interface gigabitethernet 1/0/2
[Device-security-zone-Untrust] quit
```

(3) 配置安全策略

配置名称为 untrust-trust 的安全策略，保证 Untrust 安全域中的 Host 可以访问 Trust 安全域中的 Server，具体配置步骤如下。

```
[Device] security-policy ip
[Device-security-policy-ip] rule name untrust-trust
[Device-security-policy-ip-1-untrust-trust] source-zone untrust
[Device-security-policy-ip-1-untrust-trust] destination-zone trust
[Device-security-policy-ip-1-untrust-trust] destination-ip-host 10.110.10.1
[Device-security-policy-ip-1-untrust-trust] destination-ip-host 10.110.10.2
[Device-security-policy-ip-1-untrust-trust] destination-ip-host 10.110.10.3
[Device-security-policy-ip-1-untrust-trust] destination-ip-host 10.110.10.4
[Device-security-policy-ip-1-untrust-trust] action pass
[Device-security-policy-ip-1-untrust-trust] quit
[Device-security-policy-ip] quit
```

(4) 配置 NAT 功能

配置服务对象组，提供 FTP、Web 和 SMTP 服务。

```
[Device] object-group service service1
[Device-obj-grp-service-service1] service tcp destination eq 21
[Device-obj-grp-service-service1] quit
[Device] object-group service service2
[Device-obj-grp-service-service2] service tcp destination eq 80
[Device-obj-grp-service-service2] quit
[Device] object-group service service3
[Device-obj-grp-service-service3] service tcp destination eq 8080
[Device-obj-grp-service-service3] quit
[Device] object-group service service4
[Device-obj-grp-service-service4] service tcp destination eq 25
[Device-obj-grp-service-service4] quit
```

配置全局 NAT 规则，允许外网主机访问内网服务器。

```

[Device] nat global-policy
[Device-nat-global-policy] rule name rule1
[Device-nat-global-policy-rule-rule1] destination-ip host 202.38.1.1
[Device-nat-global-policy-rule-rule1] source-zone untrust
[Device-nat-global-policy-rule-rule1] service service1
[Device-nat-global-policy-rule-rule1] action dnat ip-address 10.110.10.3 local-port 21
[Device-nat-global-policy-rule-rule1] quit
[Device-nat-global-policy] rule name rule2
[Device-nat-global-policy-rule-rule2] destination-ip host 202.38.1.1
[Device-nat-global-policy-rule-rule2] source-zone untrust
[Device-nat-global-policy-rule-rule2] service service2
[Device-nat-global-policy-rule-rule2] action dnat ip-address 10.110.10.1 local-port 80
[Device-nat-global-policy-rule-rule2] quit
[Device-nat-global-policy] rule name rule3
[Device-nat-global-policy-rule-rule3] destination-ip host 202.38.1.1
[Device-nat-global-policy-rule-rule3] source-zone untrust
[Device-nat-global-policy-rule-rule3] service service3
[Device-nat-global-policy-rule-rule3] action dnat ip-address 10.110.10.2 local-port 80
[Device-nat-global-policy-rule-rule3] quit
[Device-nat-global-policy] rule name rule4
[Device-nat-global-policy-rule-rule4] destination-ip host 202.38.1.1
[Device-nat-global-policy-rule-rule4] source-zone untrust
[Device-nat-global-policy-rule-rule4] service service4
[Device-nat-global-policy-rule-rule4] action dnat ip-address 10.110.10.4 local-port 25
[Device-nat-global-policy-rule-rule4] quit
[Device-nat-global-policy] quit

```

4. 验证配置

以上配置完成后，外网 Host 能够通过 NAT 地址访问各内网服务器。通过查看如下显示信息，可以验证以上配置成功。

```

[Device] display nat all
NAT global-policy information:
  Totally 4 NAT global-policy rules.
  Rule name: rule1
    Type                : nat
    DestIP address      : 202.38.1.1
    Source-zone name    : untrust
    Service object group : service1
  DNAT action:

```

```
IPv4 address: 10.110.10.3
Port: 21
NAT counting : 0
Config status: Active

Rule name: rule2
Type          : nat
DestIP address : 202.38.1.1
Source-zone name : untrust
Destination-zone name : trust
Service object group : service2
DNAT action:
IPv4 address: 10.110.10.1
Port: 80
NAT counting : 0
Config status: Active

Rule name: rule3
Type          : nat
DestIP address : 202.38.1.1
Source-zone name : untrust
Destination-zone name : trust
Service object group : service3
DNAT action:
IPv4 address: 10.110.10.2
Port: 80
NAT counting : 0
Config status: Active

Rule name: rule4
Type          : nat
DestIP address : 202.38.1.1
Source-zone name : untrust
Destination-zone name : trust
Service object group : service4
DNAT action:
IPv4 address: 10.110.10.4
Port: 25
```

NAT counting : 0
Config status: Active

NAT logging:

Log enable : Disabled
Flow-begin : Disabled
Flow-end : Disabled
Flow-active : Disabled
Port-block-assign : Disabled
Port-block-withdraw : Disabled
Alarm : Disabled
NO-PAT IP usage : Disabled

NAT mapping behavior:

Mapping mode : Address and Port-Dependent
ACL : ---
Config status: Active

NAT ALG:

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

Static NAT load balancing: Disabled

```
NAT link-switch recreate-session: Disabled
```

```
NAT configuration-for-new-connection: Disabled
```

```
NAT global-policy compatible-previous-version rule-type ipv4-snat-and-dnat  
translate-before-secp : Disabled
```

```
NAT gratuitous-arp: Enabled
```

通过以下显示命令，可以看到 Host 访问 FTP server 时生成 NAT 会话信息。

```
[Device] display nat session verbose
```

```
Slot 1:
```

```
Initiator:
```

```
Source      IP/port: 202.38.1.2/52802  
Destination IP/port: 202.38.1.1/21  
DS-Lite tunnel peer: -  
VPN instance/VLAN ID/Inline ID: -/-/-  
Protocol: TCP(6)  
Inbound interface: GigabitEthernet1/0/2  
Source security zone: Untrust
```

```
Responder:
```

```
Source      IP/port: 10.110.10.3/21  
Destination IP/port: 202.38.1.2/52802  
DS-Lite tunnel peer: -  
VPN instance/VLAN ID/Inline ID: -/-/-  
Protocol: TCP(6)  
Inbound interface: GigabitEthernet1/0/1  
Source security zone: Trust
```

```
State: TCP_ESTABLISHED
```

```
Application: FTP
```

```
Rule ID: -/-/-
```

```
Rule name:
```

```
Start time: 2017-05-21 11:13:39  TTL: 3597s
```

```
Initiator->Responder:          7 packets          313 bytes
```

```
Responder->Initiator:          6 packets          330 bytes
```

```
Total sessions found: 1
```

2.15.4 外网用户通过域名访问内网服务器配置举例（地址不重叠）

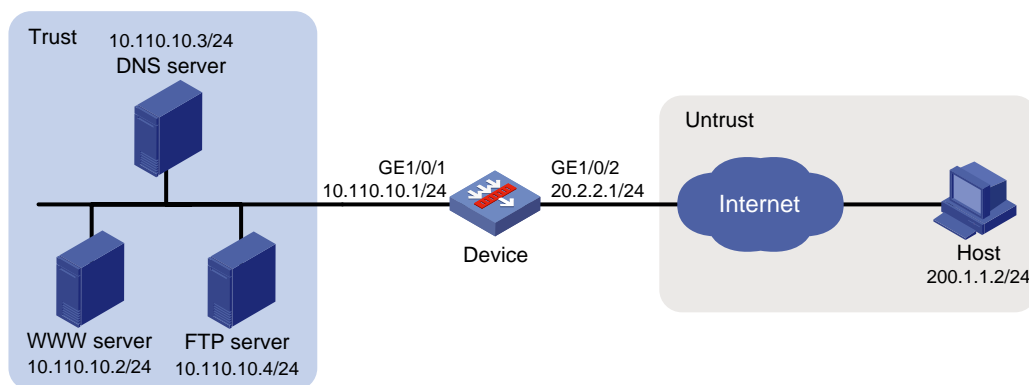
1. 组网需求

- 某公司内部对外提供 Web 服务，Web 服务器地址为 10.110.10.2/24。
- 该公司在内网有一台 DNS 服务器，IP 地址为 10.110.10.3/24，用于解析 Web 服务器的域名。
- 该公司拥有两个外网 IP 地址：202.38.1.2 和 202.38.1.3。

要实现，外网主机可以通过域名访问内网的 Web 服务器。

2. 组网图

图2-6 外网用户通过域名访问内网服务器配置组网图（地址不重叠）



3. 配置思路

- 外网主机通过域名访问 Web 服务器，首先需要通过访问内网 DNS 服务器获取 Web 服务器的 IP 地址，因此需要通过配置 NAT 内部服务器将 DNS 服务器的内网 IP 地址和 DNS 服务端口映射为一个外网地址和端口。
- DNS 服务器回应给外网主机的 DNS 报文载荷中携带了 Web 服务器的内网 IP 地址，因此需要将 DNS 报文载荷中的内网 IP 地址转换为一个外网 IP 地址。外网地址分配可以通过出方向动态地址转换功能实现，转换载荷信息可以通过 DNS ALG 功能实现。

4. 配置步骤

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 10.110.10.1 24
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 将接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 1/0/1
```

```
[Device-security-zone-Trust] quit
[Device] security-zone name untrust
[Device-security-zone-Untrust] import interface gigabitethernet 1/0/2
[Device-security-zone-Untrust] quit
```

(3) 配置安全策略

配置名称为 **untrust-trust** 的安全策略，保证 Untrust 安全域内的 Host 可以访问 Trust 安全域中的 Server，具体配置步骤如下。

```
[Device] security-policy ip
[Device-security-policy-ip] rule name untrust-trust
[Device-security-policy-ip-1-untrust-trust] source-zone untrust
[Device-security-policy-ip-1-untrust-trust] destination-zone trust
[Device-security-policy-ip-1-untrust-trust] destination-ip-host 10.110.10.2
[Device-security-policy-ip-1-untrust-trust] destination-ip-host 10.110.10.3
[Device-security-policy-ip-1-untrust-trust] destination-ip-host 10.110.10.4
[Device-security-policy-ip-1-untrust-trust] action pass
[Device-security-policy-ip-1-untrust-trust] quit
[Device-security-policy-ip] quit
```

(4) 配置 NAT 功能

开启 DNS 的 NAT ALG 功能。

```
[Device] nat alg dns
```

创建地址组。

```
[Device] nat address-group 1
[Device-address-group-1] address 202.38.1.3 202.38.1.3
[Device-address-group-1] quit
```

配置服务对象组 **service1**，提供 DNS 服务。

```
[Device] object-group service service1
[Device-obj-grp-service-service1] service tcp destination eq 53
[Device-obj-grp-service-service1] service udp destination eq 53
[Device-obj-grp-service-service1] quit
```

配置全局 NAT 规则，允许外网主机使用地址 202.38.1.2 访问内网 DNS 服务器。

```
[Device] nat global-policy
[Device-nat-global-policy] rule name rule1
[Device-nat-global-policy-rule-rule1] source-zone untrust
[Device-nat-global-policy-rule-rule1] destination-ip host 202.38.1.2
[Device-nat-global-policy-rule-rule1] service service1
[Device-nat-global-policy-rule-rule1] action dn timer ip-address 10.110.10.3 local-port 53
[Device-nat-global-policy-rule-rule1] quit
```

配置全局 NAT 规则，允许使用地址组 1 中的地址对 DNS 应答报文载荷中的内网地址进行转换，并在转换过程中不使用端口信息，以及允许反向地址转换。

```
[Device-nat-global-policy] rule name rule2
[Device-nat-global-policy-rule-rule2] source-ip host 10.110.10.2
[Device-nat-global-policy-rule-rule2] source-zone trust
[Device-nat-global-policy-rule-rule2] destination-zone untrust
[Device-nat-global-policy-rule-rule2] action snat address-group 1 no-pat reversible
[Device-nat-global-policy-rule-rule2] quit
[Device-nat-global-policy] quit
```

5. 验证配置

以上配置完成后，外网 Host 能够通过域名访问内网 Web server。通过查看如下显示信息，可以验证以上配置成功。

```
[Device] display nat all
NAT address group information:
  Totally 1 NAT address groups.
  Address group ID: 1
  Port range: 1-65535
  Address information:
    Start address      End address
    202.38.1.3         202.38.1.3

NAT global-policy information:
  Totally 2 NAT global-policy rules.
  Rule name: rule1
    Type                : nat
    DestIP address       : 202.38.1.2
    Source-zone name     : untrust
    Service object group : service1
  DNAT action:
    IPv4 address: 10.110.10.3
    Port: 53
    NAT counting : 0
    Config status: Active

  Rule name: rule2
    Type                : nat
    SrcIP address       : 10.110.10.2
    Source-zone name     : trust
```



```

    Destination-zone name : untrust

SNAT action:
    Address group ID: 1
    NO-PAT: Y
    Reversible: Y
    Port-preserved: N
    NAT counting : 0
    Config status: Active

NAT logging:
    Log enable          : Disabled
    Flow-begin          : Disabled
    Flow-end            : Disabled
    Flow-active         : Disabled
    Port-block-assign   : Disabled
    Port-block-withdraw : Disabled
    Alarm               : Disabled
    NO-PAT IP usage     : Disabled

NAT mapping behavior:
    Mapping mode : Address and Port-Dependent
    ACL          : ---
    Config status: Active

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

```

```
SQLNET      : Disabled
TFTP        : Disabled
XDMCP       : Disabled

Static NAT load balancing:      Disabled

NAT link-switch recreate-session: Disabled

NAT configuration-for-new-connection: Disabled

NAT global-policy compatible-previous-version rule-type ipv4-snat-and-dnat
translate-before-secp : Disabled

NAT gratuitous-arp: Enabled
```

通过以下显示命令，可以看到 Host 访问 Web server 时生成 NAT 会话信息。

```
[Device] display nat session verbose

Slot 1:

Initiator:

  Source      IP/port: 200.1.1.2/1694
  Destination IP/port: 202.38.1.3/8080
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Untrust

Responder:

  Source      IP/port: 10.110.10.2/8080
  Destination IP/port: 200.1.1.2/1694
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Trust

State: TCP_ESTABLISHED

Application: HTTP

Rule ID: -/-/-

Rule name:

Start time: 2017-06-15 14:53:29  TTL: 3597s
```

```
Initiator->Responder:          7 packets      308 bytes
Responder->Initiator:          5 packets      312 bytes

Total sessions found: 1
```

2.15.5 内网用户通过 NAT 地址互访配置举例

1. 组网需求

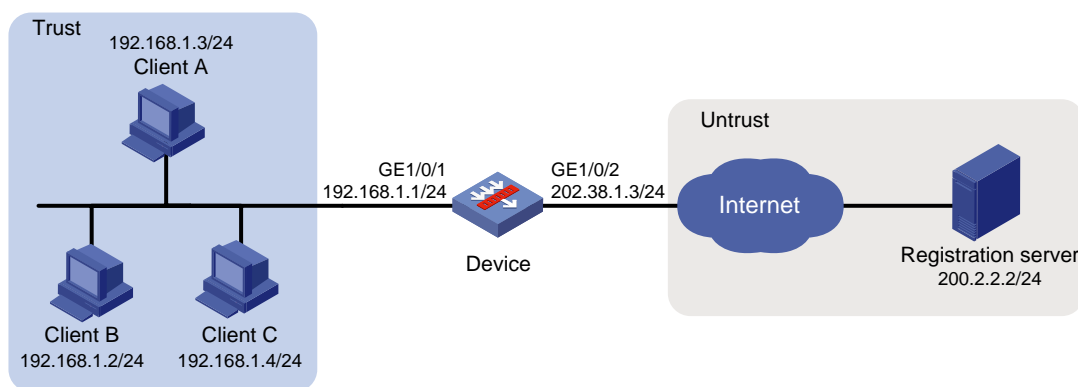
某 P2P 应用环境中，内网中的客户端首先需要向外网服务器进行注册，外网服务器会记录客户端的 IP 地址和端口号。如果内网的一个客户端要访问内网的另一个客户端，首先需要向服务器获取对方的 IP 地址和端口号。

需要实现如下功能：

- 内网客户端可以向外网中的服务器注册，且注册为一个相同的外网地址。
- 内网客户端能够通过从服务器获得的 IP 地址和端口进行互访。

2. 组网图

图2-7 内网用户通过 NAT 地址互访配置组网图



3. 配置思路

该需求为典型的 P2P 模式的 NAT hairpin 应用，具体配置思路如下。

- 内网中的客户端需要向外网中的服务器注册，因此需要进行源地址转换，可以配置出方向动态地址转换实现。
- 服务器记录客户端的 IP 地址和端口号，且该地址和端口号是 NAT 转换后的。由于服务器记录的客户端 IP 地址和端口号需要供任意源地址访问，因此客户端地址的转换关系必须不关心对端地址，这可以通过配置 EIM 模式的动态地址转换实现。

4. 配置步骤

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.1 24
```

```
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 将接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 1/0/1
[Device-security-zone-Trust] quit
[Device] security-zone name untrust
[Device-security-zone-Untrust] import interface gigabitethernet 1/0/2
[Device-security-zone-Untrust] quit
```

(3) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达 Server 所在网络的下一跳 IP 地址为 202.38.1.1，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ip route-static 200.2.2.0 24 202.38.1.1
```

(4) 配置安全策略

配置名称为 trust-untrust 的安全策略，保证 Trust 安全域内的 Host 可以访问 Untrust 安全域内的 Server，具体配置步骤如下。

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-untrust
[Device-security-policy-ip-1-trust-untrust] source-zone trust
[Device-security-policy-ip-1-trust-untrust] destination-zone untrust
[Device-security-policy-ip-1-trust-untrust] source-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-1-trust-untrust] destination-ip-host 200.2.2.2
[Device-security-policy-ip-1-trust-untrust] action pass
[Device-security-policy-ip-1-trust-untrust] quit
```

配置名称为 trust-trust 的安全策略，保证 Trust 安全域内的 Host 可以互访，具体配置步骤如下。

```
[Device-security-policy-ip] rule name trust-trust
[Device-security-policy-ip-2-trust-trust] source-zone trust
[Device-security-policy-ip-2-trust-trust] destination-zone trust
[Device-security-policy-ip-2-trust-trust] source-ip-host 202.38.1.3
[Device-security-policy-ip-2-trust-trust] destination-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-2-trust-trust] action pass
[Device-security-policy-ip-2-trust-trust] quit
[Device-security-policy-ip] quit
```

(5) 配置 NAT 功能

配置地址对象组 obj1，仅允许对 192.168.1.0/24 网段的用户报文进行地址转换。

```
[Device] object-group ip address obj1
[Device-obj-grp-ip-obj1] network subnet 192.168.1.0 24
[Device-obj-grp-ip-obj1] quit
```

配置全局 NAT 规则，通过 Easy IP 方式对内网访问外网的报文进行源地址转换，因为多个内部主机共用一个外网地址，因此需要配置为 PAT 方式，即转换过程中使用端口信息。

```
[Device] nat global-policy
[Device-nat-global-policy] rule name rule1
[Device-nat-global-policy-rule-rule1] source-zone trust
[Device-nat-global-policy-rule-rule1] destination-zone untrust
[Device-nat-global-policy-rule-rule1] source-ip obj1
[Device-nat-global-policy-rule-rule1] action snat easy-ip
[Device-nat-global-policy-rule-rule1] quit
[Device-nat-global-policy] quit
```

配置 ACL 2000，允许对内部网络中 192.168.1.0/24 网段的报文进行地址转换。

```
[Device] acl basic 2000
[Device-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Device-acl-ipv4-basic-2000] quit
```

配置 PAT 方式下的地址转换模式为 EIM，即只要是来自相同源地址和源端口号的且匹配 ACL 2000 的报文，不论其目的地址是否相同，通过 PAT 转换后，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。

```
[Device] nat mapping-behavior endpoint-independent acl 2000
```

5. 验证配置

以上配置完成后，Host A、Host B 和 Host C 分别向外网服务器注册之后，它们之间可以相互访问。通过查看如下显示信息，可以验证以上配置成功。

```
[Device] display nat all
NAT global-policy information:
  Totally 2 NAT global-policy rules.
  Rule name: rule1
    Type                : nat
    SrcIP object group   : obj1
    Source-zone name     : trust
    Destination-zone name : untrust
  SNAT action:
    Easy-IP
    Reversible: N
    Port-preserved: N
  NAT counting : 0
```

Config status: Active

NAT logging:

Log enable : Disabled
Flow-begin : Disabled
Flow-end : Disabled
Flow-active : Disabled
Port-block-assign : Disabled
Port-block-withdraw : Disabled
Alarm : Disabled
NO-PAT IP usage : Disabled

NAT mapping behavior:

Mapping mode : Endpoint-Independent

ACL : 2000

Config status: Active

NAT ALG:

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

Static NAT load balancing: Disabled

NAT link-switch recreate-session: Disabled

```
NAT configuration-for-new-connection: Disabled
```

```
NAT global-policy compatible-previous-version rule-type ipv4-snat-and-dnat  
translate-before-secp : Disabled
```

```
NAT gratuitous-arp: Enabled
```

通过以下显示命令，可以看到 Client A 访问 Client B 时生成 NAT 会话信息。

```
[Device] display nat session verbose
```

```
Slot 1:
```

```
Initiator:
```

```
Source      IP/port: 192.168.1.3/44929
```

```
Destination IP/port: 202.38.1.3/1
```

```
DS-Lite tunnel peer: -
```

```
VPN instance/VLAN ID/Inline ID: -/-/-
```

```
Protocol: UDP(17)
```

```
Inbound interface: GigabitEthernet1/0/1
```

```
Source security zone: Trust
```

```
Responder:
```

```
Source      IP/port: 192.168.1.2/69
```

```
Destination IP/port: 202.38.1.3/1024
```

```
DS-Lite tunnel peer: -
```

```
VPN instance/VLAN ID/Inline ID: -/-/-
```

```
Protocol: UDP(17)
```

```
Inbound interface: GigabitEthernet1/0/1
```

```
Source security zone: Trust
```

```
State: UDP_READY
```

```
Application: TFTP
```

```
Rule ID: -/-/-
```

```
Rule name:
```

```
Start time: 2012-08-15 15:53:36  TTL: 46s
```

```
Initiator->Responder:          1 packets          56 bytes
```

```
Responder->Initiator:          1 packets          72 bytes
```

```
Total sessions found: 1
```

2.15.6 端口块动态映射配置举例

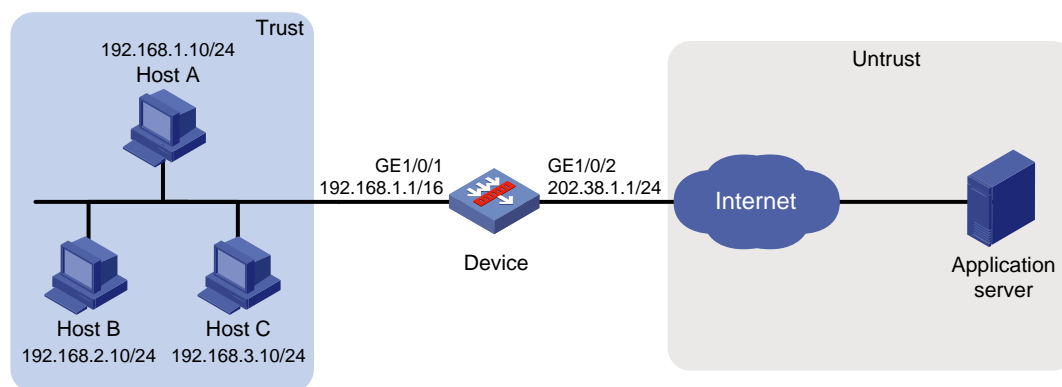
1. 组网需求

- 某公司内网使用的 IP 地址为 192.168.0.0/16。
- 该公司拥有 202.38.1.2 和 202.38.1.3 两个外网 IP 地址。

要实现，内部网络中的 192.168.1.0/24 网段的用户可以访问 Internet 中地址为 200.2.2.1 的 Server，其它网段的用户不能访问 Internet。基于 NAT444 端口块动态映射方式复用两个外网地址 202.38.1.2 和 202.38.1.3，外网地址的端口范围为 1024~65535，端口块大小为 300。当为某用户分配的端口块资源耗尽时，再为其增量分配 1 个端口块。

2. 组网图

图2-8 NAT444 端口块动态映射配置组网图



3. 配置步骤

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.1 16
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 将接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 1/0/1
[Device-security-zone-Trust] quit
[Device] security-zone name untrust
[Device-security-zone-Untrust] import interface gigabitethernet 1/0/2
[Device-security-zone-Untrust] quit
```

(3) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达 Server 所在网络的下一跳 IP 地址为 202.38.1.20，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ip route-static 200.2.2.1 32 202.38.1.20
```

(4) 配置安全策略

配置名称为 trust-untrust 的安全策略，保证 Trust 安全域内的 Host 可以访问 Untrust 安全域中的 Server，具体配置步骤如下。

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-untrust
[Device-security-policy-ip-1-trust-untrust] source-zone trust
[Device-security-policy-ip-1-trust-untrust] destination-zone untrust
[Device-security-policy-ip-1-trust-untrust] source-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-1-trust-untrust] destination-ip-host 200.2.2.1
[Device-security-policy-ip-1-trust-untrust] action pass
[Device-security-policy-ip-1-trust-untrust] quit
[Device-security-policy-ip] quit
```

(5) 配置 NAT 功能

配置地址组 0，包含两个外网地址 202.38.1.2 和 202.38.1.3，外网地址的端口范围为 1024～65535，端口块大小为 300，增量端口块数为 1。

```
[Device] nat address-group 0
[Device-address-group-0] address 202.38.1.2 202.38.1.3
[Device-address-group-0] port-range 1024 65535
[Device-address-group-0] port-block block-size 300 extended-block-number 1
[Device-address-group-0] quit
```

配置地址对象组 obj1，仅允许对内部网络中 192.168.1.0/24 网段的用户报文进行地址转换。

```
[Device] object-group ip address obj1
[Device-obj-grp-ip-obj1] network subnet 192.168.1.0 24
[Device-obj-grp-ip-obj1] quit
```

配置全局 NAT 规则，允许使用地址组 0 中的地址对匹配的对象组 obj1 的报文进行源地址转换，并在转换过程中使用端口信息。

```
[Device] nat global-policy
[Device-nat-global-policy] rule name rule1
[Device-nat-global-policy-rule-rule1] source-ip obj1
[Device-nat-global-policy-rule-rule1] action snat address-group 0
```

4. 验证配置

以上配置完成后，Host A 能够访问外网服务器，Host B 和 Host C 无法访问外网服务器。通过查看如下显示信息，可以验证以上配置成功。

```

[Device] display nat all
NAT address group information:
  Totally 1 NAT address groups.
  Address group ID: 0
    Port range: 1024-65535
    Port block size: 300
    Extended block number: 1
    Blade-load-sharing-group: Blade4fw-m90001
  Address information:
    Start address      End address
    202.38.1.2        202.38.1.3
  Exclude address information:
    Start address      End address

NAT global-policy information:
  Totally 1 NAT global-policy rules.
  Rule name: rule1
    SrcIP object group : obj1
  SNAT action:
    Address group ID: 0
    NO-PAT: N
    Reversible: N
    Port-preserved: N
    NAT counting : 0
    Config status: Active

NAT logging:
  Log enable          : Disabled
  Flow-begin          : Disabled
  Flow-end            : Disabled
  Flow-active         : Disabled
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
  Alarm               : Disabled
  NO-PAT IP usage     : Disabled

NAT mapping behavior:
  Mapping mode : Address and Port-Dependent

```

```
ACL          : ---
Config status: Active
```

NAT ALG:

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

Static NAT load balancing: Disabled

NAT link-switch recreate-session: Disabled

NAT configuration-for-new-connection: Disabled

NAT global-policy compatible-previous-version rule-type ipv4-snat-and-dnat
translate-before-secp : Disabled

NAT gratuitous-arp: Enabled

通过以下显示命令，可以看到 NAT 会话数、当前可分配的动态端口块总数和已分配的动态端口块个数。

```
[Device] display nat statistics
```

Slot 1:

```
Total session entries: 1
Session creation rate: 0
Total EIM entries: 0
```

```
Total inbound NO-PAT entries: 0
Total outbound NO-PAT entries: 0
Total static port block entries: 0
Total dynamic port block entries: 430
Active static port block entries: 0
Active dynamic port block entries: 1
```

通过以下显示命令，可以看到生成的动态端口块表项信息。

```
[Device] display nat port-block dynamic
```

```
Slot 1:
```

Local VPN	Local IP	Global IP	Port block	Connections	BackUp
---	192.168.1.10	202.38.1.2	45724-46023	1	No

```
Total mappings found: 1
```

3 配置接口 NAT

3.1 vSystem相关说明

非缺省 vSystem 不支持本特性的部分功能，具体包括：

- 配置动态地址转换的备份组
 - 配置 Easy IP 方式的地址转换使用的备份组
 - 配置使用多备份组处理 Easy IP 方式地址转换的端口范围
- 开启 NAT 发送免费 ARP 报文功能
- 配置 NAT 业务引擎的负载分担功能
- 开启 NAT 动态端口块热备份功能
- 指定 HA 中主、从管理设备可以使用的 NAT 端口块范围
- 配置 NAT 生成 OpenFlow 流表



说明

非缺省 vSystem 对具体命令的支持情况，请见本特性的命令参考。有关 vSystem 的详细介绍请参见“虚拟化技术配置指导”中的“vSystem”。

3.2 接口NAT配置限制和指导

接口 NAT 通用配置限制和指导如下：

- 如果 NAT 规则中使用了 ACL 进行报文过滤，则 NAT 只对匹配指定的 ACL permit 规则的报文才进行地址转换，匹配时仅关注 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、传输层协议类型和 VPN 实例，不关注 ACL 规则中定义的其他元素。
- 在双上行链路组网环境中，一个出接口配置了地址转换，另一个出接口没有配置地址转换，这种情况下，建议用户不要将两个出接口添加到同一个安全域，否则可能导致流量中断。关于“安全域”的相关介绍，请参见“安全配置指导”中的“安全域”。
- 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、内部服务器、NAT444 端口块静态映射、NAT444 端口块动态映射和 DS-Lite B4 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：
 - a. 内部服务器。
 - b. 普通 NAT 静态地址转换。
 - c. NAT444 端口块静态映射。
 - d. NAT444 端口块动态映射、普通 NAT 动态地址转换和 DS-Lite B4 地址转换。对于 NAT444 端口块动态映射和普通 NAT 动态地址转换，系统在处理 IPv4 报文时对二者不做区分，统一按照 ACL 编号由大到小的顺序匹配。DS-Lite B4 地址转换处理的是 IPv6 报文。

3.3 接口NAT配置任务简介

(1) 配置接口上的地址转换方式

- [配置接口上的静态地址转换](#)
- [配置接口上的动态地址转换](#)
- [配置接口上的内部服务器](#)
- [配置接口上的 NAT444 地址转换](#)
- [配置接口上的 DS-Lite B4 地址转换](#)
- [配置接口 NAT 策略](#)

NAT 策略可以控制多个接口的地址转换，灵活指定报文的过滤条件。

(2) (可选) [配置动态地址转换的备份组](#)

[需要使用](#) QoS 策略将流量重定向到本设备的备份组。关于备份组的详细介绍，请参见“虚拟化技术配置指导”中的“备份组”。

(3) (可选) [配置 NAT hairpin 功能](#)

(4) (可选) [配置 NAT ALG](#)

(5) (可选) [配置 NAT DNS mapping 功能](#)

(6) (可选) [配置 NAT 发送免费 ARP 报文功能](#)

(7) (可选) 提高 NAT 业务的可靠性

- [配置 NAT 业务引擎的负载分担功能](#)
- [开启 NAT 动态端口块热备份功能](#)
- [配置 NAT 支持 HA](#)

(8) (可选) [配置 NAT 维护功能](#)

- [配置 NAT 定时统计功能](#)
- [开启新建 NAT 会话速率的统计功能](#)
- [配置检测 NAT 地址组成员的可用性](#)
- [开启 NAT 转换失败发送 ICMP 差错报文功能](#)

(9) (可选) [配置 NAT 日志功能](#)

(10) (可选) [配置 NAT 生成 OpenFlow 流表](#)

(11) (可选) [特定条件下的 NAT 配置](#)

- [开启反向报文的重定向功能](#)
- [开启对 TCP SYN 和 SYN ACK 报文中时间戳的删除功能](#)
- [开启主备链路切换后的 NAT 会话重建功能](#)
- [主备链路切换导致出接口所属安全域变化后的 NAT 会话重建功能](#)

3.4 配置接口上的静态地址转换

3.4.1 配置限制和指导

入方向的静态地址转换建议与接口上的出方向动态地址转换（**nat outbound**）、内部服务器（**nat server**）或出方向静态地址转换（**nat static outbound**）配合使用，以实现“源 IP 地址转换 + 目的 IP 地址转换”。

3.4.2 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”。
- 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。

3.4.3 配置出方向一对一静态地址转换

1. 功能简介

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 IP 地址转换为 *local-ip*。

2. 配置限制和指导

多个出方向一对一静态地址转换引用不同的 ACL 规则时，可以将同一个私网地址转换为不同的公网地址。

出方向一对一静态地址转换的配置中不引用 ACL 规则时，该静态地址转换允许反方向发起的连接进行地址转换。否则，必须指定 **reversible** 参数才允许反向地址转换。

调整出方向一对一静态 NAT 规则的匹配优先级时，被移动的规则必须满足如下所有条件：

- 被移动的 NAT 规则均指定了规则名称。
- 被移动的 NAT 规则的 *global-ip* 相同或 *local-ip* 相同。符合此条件的两条 NAT 规则中，至少有一条 NAT 规则引用了 ACL。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置出方向一对一静态地址转换映射。

```
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 ] ] [ vrrp
```

```
virtual-router-id ] [ rule rule-name ] [ priority priority ] [ disable ]  
[ counting ] [ description text ]
```

- (3) (可选) 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
```

缺省情况下，出方向一对一静态 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。

- (4) 进入接口视图。

```
interface interface-type interface-number
```

- (5) 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。

3.4.4 配置出方向网段对网段静态地址转换

1. 功能简介

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，并将匹配的源 IP 地址转换为指定的内网网络地址之一。

2. 配置限制和指导

调整出方向网段到网段静态 NAT 规则的匹配优先级时，被移动的规则必须满足如下所有条件：

- 要移动的 NAT 规则均指定了规则名称。
- 要移动的 NAT 规则的外网网段相同或内网网段相同。符合此条件的两条 NAT 规则中，至少有一条 NAT 规则引用了 ACL。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 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  
[ 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 ] ] [ vrrp  
virtual-router-id ] [ rule rule-name ] [ priority priority ] [ disable ]  
[ counting ]
```

- (3) (可选) 调整出方向网段对网段静态 NAT 规则的匹配优先级。

```
nat static outbound net-to-net rule move nat-rule-name1 { after | before }  
nat-rule-name2
```


缺省情况下,出方向网段对网段静态 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。

- (4) 进入接口视图。

```
interface interface-type interface-number
```

- (5) 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。

3.4.5 配置基于对象组的出方向静态地址转换

1. 功能简介

基于对象组的出方向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 IPv4 地址对象组进行匹配,并将匹配的源 IP 地址转换为外网 IPv4 地址对象组中的地址。
- 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 IPv4 地址对象组进行匹配,并将匹配的源 IP 地址转换为内网 IPv4 地址对象组中的地址。

2. 配置限制和指导

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。

基于地址对象组的出方向静态地址转换引用的 IPv4 地址对象组满足如下条件时,配置才能生效:

- 引用的地址对象组中只能存在一个主机对象 (**host**) 或者一个子网对象 (**subnet**)。
- 引用的地址对象组的子网对象中不能包含排除地址。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置基于对象组的出方向静态地址转换映射。

```
nat static outbound object-group local-object-group-name  
[ vpn-instance local-vpn-instance-name ] object-group  
global-object-group-name [ vpn-instance global-vpn-instance-name ]  
[ acl { ipv4-acl-number | name ipv4-acl-name } [ reversible ] ] [ vrrp  
virtual-router-id ] [ disable ] [ counting ]
```

缺省情况下,不存在地址转换映射。

- (3) 进入接口视图。

```
interface interface-type interface-number
```

- (4) 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。

3.4.6 配置入方向一对一静态地址转换

1. 功能简介

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*。

2. 配置限制和指导

调整入方向一对一静态 NAT 规则的匹配优先级时，被移动的规则必须满足如下所有条件：

- 要移动的 NAT 规则均指定了规则名称。
- 要移动的 NAT 规则的 *global-ip* 相同或 *local-ip* 相同。符合此条件的两条 NAT 规则中，至少有一条 NAT 规则引用了 ACL。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置入方向一对一静态地址转换映射。

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

- (3) （可选）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
```

缺省情况下，入方向一对一静态 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。

- (4) 进入接口视图。

```
interface interface-type interface-number
```

- (5) 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。

3.4.7 配置入方向网段对网段静态地址转换

1. 功能简介

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。

2. 配置限制和指导

调整入方向网段到网段静态 NAT 规则的匹配优先级时，被移动的规则必须满足如下所有条件：

- 要移动的 NAT 规则均指定了规则名称。
- 要移动的 NAT 规则的外网网段相同或内网网段相同。符合此条件的两条 NAT 规则中，至少有一条 NAT 规则引用了 ACL。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 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
[ vpn-instance global-vpn-instance-name ] local local-network
{ mask-length | mask } [ vpn-instance local-vpn-instance-name ] [ acl
{ ipv4-acl-number | name ipv4-acl-name } [ reversible ] ] [ rule
rule-name ] [ priority priority ] [ disable ] [ counting ]
```

- (3) （可选）调整入方向网段对网段静态 NAT 规则的匹配优先级。

```
nat static inbound net-to-net rule move nat-rule-name1 { after | before }
nat-rule-name2
```

缺省情况下，入方向网段对网段静态 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。

- (4) 进入接口视图。

```
interface interface-type interface-number
```

- (5) 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。

3.4.8 配置基于对象组的入方向静态地址转换

1. 功能简介

基于对象组的入方向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 IPv4 地址对象组进行匹配，并将匹配的目的 IP 地址转换为指定的外网 IPv4 地址对象组中的地址。
- 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 IPv4 地址对象组进行匹配，并将匹配的源 IP 地址转换为指定的内网 IPv4 地址对象组中的地址。

2. 配置限制和指导

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。

基于地址对象组的入方向静态地址转换引用的 IPv4 地址对象组满足如下条件时，配置才能生效：

- 引用的地址对象组中只能存在一个主机对象（**host**）或者一个子网对象（**subnet**）。
- 引用的地址对象组的子网对象中不能包含排除地址。

如果接口上配置的基于地址对象组的入方向静态地址转换所引用的内网 IPv4 地址对象组中配置了主机对象，那么该主机对象的 IP 地址不能与该接口的 IP 地址处于同一网段。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置基于对象组的入方向静态地址转换映射。

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

缺省情况下，不存在地址转换映射。

- (3) 进入接口视图。

```
interface interface-type interface-number
```

- (4) 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。

3.5 配置接口上的动态地址转换

3.5.1 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。

对于多安全引擎设备，如果 NO-PAT 方式的地址转换需要进行 DNS ALG 处理，则配置的地址组成员个数应不少于处理安全业务的安全引擎数乘以内部服务器数的个数，从而保证每个处理 NAT 业务的安全引擎上都有足够的地址资源用于转换。有关安全引擎的详细介绍，请参见“虚拟化技术配置指导”中的“Context”。

3.5.2 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”。

- 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。

3.5.3 配置出方向动态地址转换

1. 功能简介

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。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建 NAT 地址组，并进入 NAT 地址组视图。

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

- (3) 添加地址组成员。

```
address start-address end-address
```

可通过多次执行本命令添加多个地址组成员。

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。

- (4) （可选）配置禁止用于地址转换的 IP 地址。

```
exclude-ip start-address end-address
```

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。

- (5) 退回系统视图。

```
quit
```

- (6) 进入接口视图。

```
interface interface-type interface-number
```

- (7) 配置出方向动态地址转换。请至少选择其中一项进行配置。

- NO-PAT 方式。

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

- PAT 方式。

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

一个接口下可配置多个出方向的动态地址转换。

参数	功能
address-group	不指定该参数时，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
no-pat reversible	在指定该参数，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

(8) (可选) 配置 PAT 方式地址转换的模式。

a. 退回系统视图。

quit

b. 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。

该配置只对 PAT 方式的出方向动态地址转换有效。

(9) (可选) 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
```

3.5.4 配置入方向动态地址转换

1. 配置限制和指导

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**)、内部服务器(**nat server**)或出方向静态地址转换(**nat static outbound**)配合，用于实现“源 IP 地址转换+目的 IP 地址转换”，不建议单独使用。

由于自动添加路由表项速度较慢，通常建议手工添加路由。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 NAT 地址组，并进入 NAT 地址组视图。

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

(3) 添加地址组成员。

```
address start-address end-address
```

可通过多次执行本命令添加多个地址组成员。

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。

(4) (可选) 配置禁止用于地址转换的 IP 地址。

```
exclude-ip start-address end-address
```

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。

(5) 退回系统视图。

quit

- (6) 进入接口视图。

```
interface interface-type interface-number
```

- (7) 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 } [ vpn-instance vpn-instance-name ]  
[ no-pat [ reversible ] [ add-route ] ] [ rule rule-name ] [ priority  
priority ] [ disable ] [ counting ] [ description text ]
```

一个接口下可配置多个入方向的动态地址转换。

参数	功能
no-pat reversible	指定该参数，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
add-route	<ul style="list-style-type: none">指定该参数，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没有指定该参数，则用户需要在设备上手工添加路由

- (8) （可选）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
```

3.6 配置接口上的内部服务器

3.6.1 功能简介

内部服务器通常配置在外网侧接口上。通过在 NAT 设备上配置内部服务器，建立一个或多个内网服务器内网地址和端口与外网地址和端口的映射关系，使外部网络用户能够通过配置的外网地址和端口来访问内网服务器。内部服务器可以位于一个普通的内网内，也可以位于一个 VPN 实例内。

内部服务器可以通过如下配置方式实现。

- 普通内部服务器：将内网服务器的地址和端口映射为外网地址和端口，允许外部网络中的主机通过配置的外网地址和端口访问位于内网的服务器。
- 负载分担内部服务器：在配置内部服务器时，将内部服务器的内网信息指定为一个内部服务器组，组内的多台主机可以共同对外提供某种服务。外网用户向内部服务器指定的外网地址发起应用请求时，NAT 设备可根据内网服务器的权重和当前连接数，选择其中一台内网服务器作为目的服务器，实现内网服务器负载分担。
- 基于 ACL 的内部服务器：普通内部服务器方式必须指定公网地址，基于 ACL 内部服务器不用指定具体的公网地址，而是指定公网地址的集合，即通过 ACL 规则匹配过滤的一部分公网地址。对于符合 ACL 规则的报文，它的目的地址统一转换成相同的内部服务器地址和端口，它是普通内部服务器的扩展。
- 基于对象组的内部服务器：基于对象组的内部服务器使用地址对象组和服务对象组作为报文匹配条件，对于符合匹配条件的报文，它的目的地址和端口统一转换成相同的内部服务器地址和端口。关于对象组的详细介绍，请参见“安全配置指导”中的“对象组”。

3.6.2 配置限制和指导

使用 RTP（Real-Time Transport Protocol，实时传输协议）传输音视频的场景中，在 RTP 会话期间，服务器和客户端作为会话的参与者会周期性发送 RTCP（Real-time Control Protocol，实时传输控制协议）报文。如果服务器位于私网，配置 **nat server** 命令时需要指定 **reversible** 参数，否则服务器发送到公网客户端的 RTCP 报文会被 NAT 设备丢弃，导致音视频传输业务出现异常。

在配置负载分担内部服务器时，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。在支持 NAT 内部服务器自动分配 NAT 规则名称的版本上执行配置回滚操作时，如果回滚配置文件中的 NAT 内部服务器不存在系统为其自动分配的 NAT 规则名称，会出现回滚失败的错误提示信息。比如，回滚配置文件中的配置为 **nat server global 112.1.1.1 inside 192.168.20.1**，回滚操作完成后的配置为 **nat server global 112.1.1.1 inside 192.168.20.1 rule 内部服务器规则_10**（内部服务器规则_10 为系统自动分配的 NAT 规则名称），系统会将此配置与回滚文件中的配置进行比较，比较后发现两者不一致，会提示用户回滚失败。这种情况下，相关的命令已下发成功，用户无需处理。

配置内部服务器时，如果将 TCP 或 UDP 协议的端口号改为非知名端口号，则 NAT 设备不会进行 ALG 处理，导致用户无法使用内部服务器提供的服务。可通过如下两种方式解决上述问题：

- 修改内部服务器配置，使用 TCP 或 UDP 协议自身的知名端口号。
- 不修改内部服务器配置，使用 **port-mapping** 命令建立 TCP 或 UDP 协议与对应的内部服务器配置中的端口号的映射。关于 **port-mapping** 命令的详细介绍，请参见“安全配置指导”中的“APR”。

3.6.3 配置普通内部服务器

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置普通内部服务器。请至少选择其中一项进行配置。

- 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 ] [ vrrp  
virtual-router-id ] [ rule rule-name ] [ disable ] [ counting ]  
[ description text ]
```

- 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-port1 local-port2 } [ vpn-instance
local-vpn-instance-name ] [ acl { ipv4-acl-number | name
ipv4-acl-name } ] [ vrrp virtual-router-id ] [ rule rule-name ]
[ disable ] [ counting ] [ description text ]

```

- 外网地址连续，未使用外网端口。

```

nat server protocol pro-type global global-address1 global-address2
[ 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 } ] [ vrrp virtual-router-id ] [ rule rule-name ]
[ disable ] [ counting ] [ description text ]

```

- 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-port1 local-port2 ] | [ local-address |
local-address1 local-address2 ] [ local-port ] } [ vpn-instance
local-vpn-instance-name ] [ acl { ipv4-acl-number | name
ipv4-acl-name } ] [ vrrp virtual-router-id ] [ rule rule-name ]
[ disable ] [ counting ] [ description text ]

```

一个接口下可以配置多个普通内部服务器。

3.6.4 配置负载分担内部服务器

- (1) 进入系统视图。

```
system-view
```

- (2) 创建内部服务器组，并进入服务器组视图。

```
nat server-group group-id
```

- (3) 添加内部服务器组成员。

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

一个内部服务器组内可以添加多个组成员。

- (4) 退回系统视图。

```
quit
```

- (5) 进入接口视图。

```
interface interface-type interface-number
```

- (6) 配置负载分担内部服务器。

```

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 } ] [ vrrp virtual-router-id ]  
[ rule rule-name ] [ disable ] [ counting ] [ description text ]
```

一个接口下可以配置多个负载分担内部服务器。

3.6.5 配置基于 ACL 的内部服务器

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置基于 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 ]  
[ vrrp virtual-router-id ] [ rule rule-name ] [ priority priority ]  
[ disable ] [ counting ] [ description text ]
```

一个接口下可以配置多个基于 ACL 的内部服务器。

- (4) （可选）调整基于 ACL 内部服务器 NAT 规则的匹配优先级。

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

3.6.6 配置基于对象组的内部服务器

1. 功能简介

基于对象组的内部服务器使用地址对象组和服务对象组作为报文匹配条件，对于符合匹配条件的报文，它的目的地址和端口统一转换成相同的内部服务器地址和端口。关于对象组的详细介绍，请参见“安全配置指导”中的“对象组”。

当存在多条基于对象组的 NAT 内部服务器规则时，报文会按照配置顺序与这些规则进行匹配，一旦匹配上某条规则便结束匹配过程。

2. 配置限制和指导

引用的服务对象组中，只有服务对象组的协议类型是 TCP 或 UDP 时，配置的内部服务器的内网端口号才会生效。

每个内部服务器最多可引用 5 个地址对象组和 1 个服务对象组。

3. 配置准备

创建 IPv4 地址对象组或服务对象组。其中，IPv4 地址对象组中不能存在排除的 IPv4 地址。

4. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置基于对象组的内部服务器。

```

nat server rule rule-name global destination-ip object-group-name<1-5>
[ service object-group-name ] inside local-address [ local-port ] [ vrrp
virtual-router-id ] [ disable ] [ counting ] [ description text ]

```

缺省情况下，不存在基于对象组的内部服务器。

- (4) 添加内部服务器引用的对象组。

```

nat server rule rule-name global { destination-ip
object-group-name<1-5> | service object-group-name }

```

只能向已经存在的基于对象组的 NAT 内部服务器规则中添加对象组。

3.7 配置接口上的NAT444地址转换

3.7.1 功能简介

NAT444 是出方向地址转换，通常配置在外网侧接口上。通过在 NAT444 网关设备上配置 NAT444 地址转换，可以实现基于端口块的公网 IP 地址复用，使一个私网 IP 地址在一个时间段内独占一个公网 IP 地址的某个端口块。

3.7.2 配置限制和指导

对于 NAT444 端口动态映射，必须在 NAT 地址组中配置端口块参数，以实现基于端口块的 NAT444 地址转换。

3.7.3 配置 NAT444 端口块静态映射

- (1) 进入系统视图。

```

system-view

```

- (2) 创建 NAT 端口块组，并进入 NAT 端口块组视图。

```

nat port-block-group group-id

```

- (3) 添加私网地址成员。

```

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

```

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

- (4) 添加公网地址成员。

```

global-ip-pool start-address end-address

```

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

- (5) 配置公网地址的端口范围。

```

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

```

缺省情况下，公网地址的端口范围为 1~65535。

- (6) 配置端口块大小。

```

block-size block-size

```

缺省情况下，端口块大小为 256。

- (7) 退回系统视图。

quit

- (8) 进入接口视图。

interface *interface-type interface-number*

- (9) 配置 NAT444 端口块静态映射。

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

缺省情况下，不存在 NAT444 端口块静态映射配置。

一个接口下可配置多条基于不同端口块组的 NAT444 端口块静态映射。

- (10) （可选）配置 PAT 方式出方向动态地址转换的模式。

- a. 退回系统视图。

quit

- b. 配置 PAT 方式出方向动态地址转换的模式。

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

缺省情况下，PAT 方式出方向动态地址转换的模式为 Address and Port-Dependent Mapping。

3.7.4 配置 NAT444 端口块动态映射

1. 配置限制和指导

向 NAT 地址组中添加地址成员时，可采用如下方式之一：

- 添加一个或多个 IP 地址段。
- 添加一个接口，即实现 Easy IP 功能的 NAT444 端口块动态映射。与实现 Easy IP 功能的出方向动态地址转换相比，该方式支持用户溯源。

对于同一个 NAT 地址组，只能采用一种地址成员添加方式。

在 NAT 转换后的 IP 地址为设备外网侧接口的 IP 地址，且该地址是通过 DHCP 等协议动态获取的情况下，为了防止接口 IP 地址变化导致 NAT IP 地址信息不正确，请采用添加接口的方式。

2. 配置步骤

- (1) 进入系统视图。

system-view

- (2) （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 方式出方向动态地址转换的模式为 Address and Port-Dependent Mapping。

- (3) 创建 NAT 地址组，并进入 NAT 地址组视图。

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

- (4) 添加地址成员。下面两种方法互斥，请选择其中一项进行配置。

- 将 IP 地址段作为 NAT 地址组中的地址成员。

address *start-address end-address*

可通过多次执行本命令添加多个地址组成员。

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。

如果 IP 地址段的某些 IP 地址不能用于地址转换，可通过如下命令配置禁止用于地址转换的 IP 地址。

exclude-ip *start-address end-address*

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。

- 将接口的 IP 地址作为 NAT 地址组中的地址成员，即实现 Easy IP 功能。

address interface *interface-type interface-number*

缺省情况下，未指定接口地址作为地址成员。

在同一个 NAT 地址组中，通过本命令只能将一个接口的地址作为地址成员。

- (5) (可选) 配置端口范围。

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

缺省情况下，端口范围为 1~65535。

该配置仅对 PAT 方式地址转换生效。

- (6) 配置端口块参数。

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

缺省情况下，未配置 NAT 地址组的端口块参数。

该配置仅对 PAT 方式地址转换生效。

- (7) 退回系统视图。

quit

- (8) 进入接口视图。

interface *interface-type interface-number*

- (9) 配置 PAT 方式出方向动态地址转换。

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

port-preserved 参数对 NAT444 端口块动态映射无效。

3.7.5 配置 NAT444 端口块全局共享功能

1. 功能简介

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

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 NAT444 端口块全局共享功能。

```
nat port-block global-share enable
```

缺省情况下，端口块全局共享功能处于关闭状态。

3.8 配置接口上的DS-Lite B4地址转换

1. 功能简介

DS-Lite B4 地址转换配置在外网侧接口上，关联 IPv6 ACL 控制地址转换范围，目前仅支持端口块动态映射方式。

2. 配置准备

在配置接口上的 DS-Lite B4 地址转换之前，请确保 B4 设备和 AFTR 之间 IPv6 报文路由可达。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) （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 方式出方向动态地址转换的模式为 Address and Port-Dependent Mapping。

- (3) 创建 NAT 地址组，并进入 NAT 地址组视图。

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

- (4) 添加地址组成员。

```
address start-address end-address
```

可通过多次执行本命令添加多个地址组成员。

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。

- (5) （可选）配置禁止用于地址转换的 IP 地址。

```
exclude-ip start-address end-address
```

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。

- (6) 配置端口范围。

```
port-range start-port-number end-port-number
```

缺省情况下，端口范围为 1-65535。

该配置仅对 PAT 方式地址转换生效。

- (7) 配置端口块参数。

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

缺省情况下，未配置 NAT 地址组的端口块参数。

该配置仅对 PAT 方式地址转换生效。

- (8) 退回系统视图。

```
quit
```

- (9) 进入接口视图。

```
interface interface-type interface-number
```

- (10) 配置 DS-Lite B4 端口块映射。

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

3.9 配置接口NAT策略

3.9.1 功能简介

接口 NAT 策略根据报文的源 IP 地址、目的 IP 地址和携带的服务类型对多个接口出方向报文的地址转换进行控制。接口 NAT 策略中可以包含多条 NAT 规则，设备通过接口出方向上应用的 NAT 规则中引用的对象组识别出特定的报文，并根据预先设定的动作类型对其进行地址转换。

3.9.2 配置限制和指导

若 NAT 规则未引用任何对象组，则该规则将匹配任意报文。

NAT 策略目前仅支持动态地址转换，其优先级高于接口下的动态地址转换。

3.9.3 创建 NAT 策略

- (1) 进入系统视图。

```
system-view
```

- (2) 创建接口 NAT 策略，并进入接口 NAT 策略视图。

```
nat policy
```

缺省情况下，不存在接口 NAT 策略。

3.9.4 配置 NAT 规则

1. 配置限制和指导

当接口 NAT 策略中包含多条规则时，报文会按照配置顺序与这些规则进行匹配，一旦匹配上某条规则便结束匹配过程。NAT 规则的配置顺序可在接口 NAT 策略视图下通过 **display this** 命令查看，配置顺序与规则的创建顺序有关，先创建的规则处在配置顺序的优先位置。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口 NAT 策略视图。

```
nat policy
```

- (3) 创建 NAT 规则，并进入 NAT 规则视图。

rule name *rule-name*

缺省情况下，不存在 NAT 规则。

- (4) （可选）配置 NAT 规则的描述信息。

description *text*

缺省情况下，NAT 规则未配置任何描述信息。

- (5) 指定 NAT 规则的出接口。

outbound-interface *interface-type interface-name*

缺省情况下，未指定 NAT 规则的出接口。

- (6) 配置 NAT 规则引用的对象组。请至少选择其中一项进行配置。

- 配置 NAT 规则源地址对象组。

source-ip *ipv4-object-group-name*

源地址对象组用于匹配报文的源 IP 地址。

- 配置 NAT 规则引用目的地址对象组。

destination-ip *ipv4-object-group-name*

目的地址对象组用于匹配报文的目的 IP 地址。

- 配置 NAT 规则引用服务对象组。

service *object-group-name*

服务对象组用于匹配报文携带的服务类型。

缺省情况下，未配置 NAT 规则引用的对象组。

NAT 规则引用的对象组必须已经存在。

- (7) 配置 NAT 规则中的地址转换方式。请选择其中一项进行配置。

- 配置 NAT 规则中的地址转换方式为 Easy IP 方式。

action easy-ip

- 配置 NAT 规则中的地址转换方式为 NO-NAT 方式。

action no-nat

- 配置 NAT 规则中的地址转换方式为 NO-PAT 方式。

action address-group { *group-id* | **name** *group-name* } **no-pat**
[**reversible**]

- 配置 NAT 规则中的地址转换方式为 PAT 方式。

action address-group { *group-id* | **name** *group-name* } [**port-preserved**]

缺省情况下，未配置 NAT 规则中的地址转换方式。

- (8) （可选）开启 NAT 规则命中统计功能。

counting enable

缺省情况下，NAT 规则命中统计功能处于关闭状态。

- (9) 配置 PAT 方式地址转换的模式。

- 退回接口 NAT 策略视图。

quit

b. 退回系统视图。

```
quit
```

c. 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。

该配置只对 PAT 方式的出方向动态地址转换有效。

3.9.5 移动 NAT 规则

1. 功能简介

NAT 规则是按照配置先后顺序进行匹配的即先配置的 NAT 规则具有更高的匹配优先级。对于需要调整 NAT 规则匹配顺序的场景，请使用本功能移动 NAT 规则的位置，从而灵活调整 NAT 规则的匹配优先级顺序。

调整 NAT 规则的位置会修改规则的匹配优先级的值，优先级的值越小，则匹配优先级越高。具体机制为：

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

2. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 进入接口 NAT 策略视图。

```
nat policy
```

(3) 修改 NAT 规则的匹配优先级顺序。

```
rule move rule-name1 { after | before } [ rule-name2 ]
```

通过本命令只能调整已经存在的 NAT 规则的匹配优先级顺序。

3.9.6 禁用 NAT 规则

1. 配置限制和指导

配置本功能后，相应的 NAT 规则将不再生效，但是不会将此 NAT 规则删除。如果不再需要此 NAT 规则，需要执行 **undo rule name** 命令才能将其删除。

2. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 进入接口 NAT 策略视图。

```
nat policy
```

(3) 进入 NAT 规则视图。

rule name *rule-name*

- (4) 禁用 NAT 规则中的地址转换映射。

disable

缺省情况下，NAT 规则中的地址转换映射处于开启状态。

3.10 配置动态地址转换的备份组

3.10.1 功能简介

通过指定备份组，设备会将需要进行动态 NAT（包括动态地址转换和动态 NAT444）的流量引到指定的备份组通道进行处理，提高了 NAT 业务处理的性能。关于备份组的详细介绍，请参见“虚拟化技术配置指导”中的“备份组”。

3.10.2 配置限制和指导

如果设备上创建了手动备份组，则只能为 NAT 地址组指定手动备份组，不允许再指定自动备份组。

3.10.3 配置 NAT 地址组的备份组

1. 配置限制和指导

NAT 地址组中同时指定备份组和负载分担组(通过 **blade-load-sharing-group** 命令配置)时，备份组中的安全引擎必须是负载分担组中的安全引擎。

2. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 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。

- (3) 配置 NAT 地址组的备份组。

failover-group *group-name* [**channel** *channel-id*]

缺省情况下，没有为 NAT 地址组指定备份组。

3.10.4 配置 Easy IP 方式的地址转换使用的备份组

1. 配置限制和指导

每个接口上只能指定一个备份组处理 Easy IP 方式的地址转换。

如果在接口视图下配置了 **nat outbound easy-ip failover-group** 命令，并在系统视图下配置了 **nat outbound easy-ip port-range** 命令，那么后者的配置将失效。

2. 配置准备

配置 QoS 策略将流量重定向到备份组进行处理。需要保证 QoS 策略中流行为重定向的备份组必须与 Easy IP 方式地址转换使用的备份组保持一致；如果指定了 **channel** 参数，需要保证 QoS 策略中

流行为重定向的备份组引擎口与 Easy IP 方式地址转换使用的备份组引擎口保持一致。关于流量重定向的详细介绍，请参见“ACL 和 QoS 配置指导”中的“流量重定向”。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置 Easy IP 方式的地址转换使用的备份组。

```
nat outbound easy-ip failover-group group-name [ channel channel-id ]
```

缺省情况下，未配置 Easy IP 方式的地址转换使用的备份组。

3.10.5 配置使用多备份组处理 Easy IP 方式地址转换的端口范围

1. 功能简介

接口上使用 Easy IP 方式做出方向动态地址转换业务时，若使用了多备份组进行业务处理，可能会出现多个备份组使用同一接口地址进行转换后端口冲突的情况，为了避免该情况的发生，请为不同的备份组划分不同的端口范围。

通过将不同的端口掩码值和掩码位数组合与不同的备份组绑定，可以保证不同备份组占用不同的端口范围。对于端口范围的高位掩码值和掩码位数与端口号范围的转换关系如下：

- (1) 首先将端口范围的高位掩码值和掩码位数转换为对应的二进制，如高位掩码值为 2，掩码位数为 5，转换为二进制则表示为 00010；
- (2) 然后将 16 位二进制数的低位进行填充：
 - a. 全部填充为 0，即可得到端口范围的最小值；
 - b. 全部填充为 1，即可得到端口范围的最大值。
- (3) 将得到的二进制的最小值和最大值转换为十进制即可得到端口号范围。

例如高位掩码值为 2，掩码位数为 5，则对应的端口号范围二进制表示为 0001000000000000～0001011111111111，转换为十进制即 4096～6143。

2. 配置限制和指导

如果在接口视图下配置了 **nat outbound easy-ip failover-group** 命令，并在系统视图下配置了 **nat outbound easy-ip port-range** 命令，那么后者的配置将失效。

3. 配置准备

配置 QoS 策略将流量重定向到备份组进行处理。需要保证 QoS 策略中流行为重定向的备份组必须与 Easy IP 方式地址转换使用的备份组保持一致；如果指定了 channel 参数，需要保证 QoS 策略中流行为重定向的备份组引擎口与 Easy IP 方式地址转换使用的备份组引擎口保持一致。关于流量重定向的详细介绍，请参见“ACL 和 QoS 配置指导”中的“流量重定向”。

4. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 Easy IP 方式地址转换的备份组的端口范围。

```
nat outbound easy-ip port-range mask-value mask-length failover-group
group-name [ channel channel-id ]
```

缺省情况下，未配置 Easy IP 方式地址转换的备份组的端口范围。

3.11 配置NAT hairpin功能

1. 功能简介

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。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。

2. 配置限制和指导

NAT hairpin 功能需要与地址转换配合工作，支持如下两种不同的配合方式：

- NAT hairpin 功能与内部服务器（**nat server**）、出方向动态地址转换（**nat outbound**）配合工作。
- NAT hairpin 功能与内部服务器（**nat server**）、出方向静态地址转换（**nat static outbound**）配合工作。

NAT hairpin 与不同的地址转换配合工作时，这些配置所在的接口必须在同一个接口板，否则 NAT hairpin 功能无法正常工作。

当设备上安装了多块业务板时，NAT hairpin 功能不生效。

NAT hairpin 功能与地址转换配合工作时，地址转换相关命令中所指定的 VPN 实例需要保持一致。

NAT hairpin 功能与内部服务器配合工作时，仅支持与通过如下方式配置的内部服务器配合使用，并且使用如下方式配置内部服务器时，必须通过 **protocol** 参数指定协议类型，否则 NAT hairpin 功能不生效。

- [3.6.3 配置普通内部服务器](#)
- [3.6.4 配置负载分担内部服务器](#)

P2P 方式下，外网侧的出方向地址转换必须配置为 PAT 转换方式，并开启 EIM 模式。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 开启 NAT hairpin 功能。

```
nat hairpin enable
```

缺省情况下，NAT hairpin 功能处于关闭状态。

3.12 配置NAT ALG

1. 功能简介

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。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启指定或所有协议类型的 NAT ALG 功能。

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

缺省情况下，DNS、FTP、ICMP 差错报文、PPTP、RTSP 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。

3.13 配置 NAT DNS mapping 功能

1. 功能简介

NAT DNS mapping 功能适用于 DNS 服务器在公网、私网用户希望通过域名来访问私网内部服务器的场景中。在该场景中，NAT 设备对来自外网的 DNS 响应报文进行 DNS ALG 处理时，借助 DNS mapping 映射关系精确匹配内部服务器配置，进而获取内部服务器的内网 IP 地址。具体机制如下：

- (1) NAT 设备收到来自外网的 DNS 响应报文时，获取内部服务器域名和外网 IP 地址的对应关系。
- (2) NAT 设备根据域名和应用服务器外网 IP 地址的对应关系查找 NAT DNS mapping 映射表，获取“内部服务器域名<-->外网 IP 地址+外网端口号+协议类型”的映射关系。
- (3) NAT 设备根据“内部服务器域名<-->外网 IP 地址+外网端口号+协议类型”的映射关系匹配内部服务器配置，获取内部服务器的内网 IP 地址，并进行地址转换。
- (4) NAT 设备将地址转换后的 DNS 响应报文发送给内网用户。

2. 配置限制和指导

DNS mapping 功能需要和内部服务器配合使用，由 **nat server** 配置定义内部服务器对外提供服务的外网 IP 地址和端口号，由 DNS mapping 建立“内部服务器域名<-->外网 IP 地址+外网端口号+协议类型”的映射关系。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 DNS 协议类型的 NAT ALG 功能。

```
nat alg dns
```

缺省情况下，DNS 协议类型的 NAT ALG 功能处于开启状态。

- (3) 配置一条域名到内部服务器的映射。

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

可配置多条域名到内部服务器的映射。

3.14 配置NAT发送免费ARP报文功能

1. 功能简介

缺省情况下，NAT 模块会发送免费 ARP 报文，向同一局域网内所有节点通告 NAT 公网 IP 地址与 MAC 地址的对应关系。当 NAT 公网地址较多时，发送免费 ARP 耗时较长，可能会导致 ARP 业务异常。这种情况下，为了保证 ARP 业务正常运行，可以暂时关闭此功能。关闭此功能后，NAT 不再发送免费 ARP 报文，但会回应同一局域网内其他节点发送的免费 ARP。

2. 配置限制和指导

关闭 NAT 发送免费 ARP 报文通告公网 IP 地址与 MAC 地址对应关系的功能后，当 NAT 公网地址或 NAT 公网地址对应的 VRRP 变更、接口 MAC 或虚 MAC 变更、等价出口的链路震荡等，NAT 模块不会主动发送免费 ARP，可能会导致同一局域网内其他节点不能及时更新 MAC 地址表项，从而引发业务异常。请谨慎使用。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 NAT 发送免费 ARP 报文功能。

```
nat gratuitous-arp enable
```

缺省情况下，NAT 发送免费 ARP 报文功能处于开启状态。

3.15 配置NAT业务引擎的负载分担功能

3.15.1 配置 NAT 业务引擎重新分担动态 NAT 功能

1. 功能简介

本功能用于重新在多个处理 NAT 业务的安全引擎上进行动态 NAT（包括动态地址转换和 NAT 端口块动态映射）的负载分担。使用本功能后，设备会综合考虑当前所有的动态 NAT 配置（包括动态地址转换和 NAT 端口块动态映射的配置）或指定地址组的动态 NAT 配置，重新将动态 NAT 的处理分担到不同的 NAT 业务引擎上，以均衡各个 NAT 业务引擎上的负载。

2. 配置步骤

请在用户视图下执行本命令，重新在多个 NAT 业务引擎上进行动态 NAT 的负载分担。

```
reset nat dynamic-load-balance [ address-group group-id ]
```



注意

执行本命令后，会造成流量的暂时中断，请谨慎使用本命令。

3.15.2 配置静态 NAT 的负载分担功能

1. 功能简介

开启静态 NAT 的负载分担功能后，设备会将普通静态地址转换、内部服务器和 NAT444 端口块静态映射的处理分担到不同的处理 NAT 业务的安全引擎上，以均衡各个业务引擎上的负载。如果关闭本功能，则所有静态 NAT 都由主业务引擎来处理，可能会导致主业务引擎负载过重。

2. 配置限制和指导

开启或关闭本功能时，需要执行 **reset nat session** 和 **reset session table** 命令，以保证本功能正常运行。删除会话表项会造成业务中断，请谨慎使用本功能。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启静态 NAT 的负载分担功能。

```
nat static-load-balance enable
```

缺省情况下，静态 NAT 的负载分担功能处于关闭状态。

- (3) （可选）重新在多个 NAT 业务引擎上进行静态 NAT 的负载分担。

- a. 退回用户视图。

```
quit
```

- b. 重新在多个 NAT 业务引擎上进行静态 NAT 的负载分担。

```
reset nat static-load-balance
```



注意

执行本命令后，会造成流量的暂时中断，请谨慎使用本命令。

3.15.3 配置 NAT 负载分担组

1. 功能简介

通过配置 NAT 负载分担组，可以将 NAT 业务的处理分担到不同的业务引擎上，避免出现所有业务均由主业务引擎处理导致的主业务引擎负担过重的情况。

2. 配置静态 NAT 的负载分担组

- (1) 进入系统视图。

```
system-view
```

- (2) 配置静态 NAT 的负载分担组。

```
nat static blade-load-sharing-group group-name
```

缺省情况下，没有为静态 NAT 指定负载分担组。

3. 配置动态 NAT 的负载分担组

- (1) 进入系统视图。

```
system-view
```


- (2) 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。

- (3) 配置动态 NAT 的负载分担组。

```
blade-load-sharing-group group-name
```

缺省情况下，没有为 NAT 地址组指定负载分担组。

3.16 开启NAT动态端口块热备份功能

1. 功能简介

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

2. 配置限制和指导

RBM 组网环境下，开启 RBM 热备功能（执行 **hot-backup enable** 命令）后本功能才能生效。

IRF 组网环境下，开启会话业务热备份功能（执行 **session synchronization enable** 命令）后本功能才能生效。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 NAT 动态端口块热备份功能。

```
nat port-block synchronization enable
```

缺省情况下，NAT 动态端口块热备份功能处于关闭状态。

3.17 配置NAT支持HA

3.17.1 功能简介

在单台 NAT 设备的组网中，一旦发生单点故障，内网用户将无法与外网通信。采用 HA 方案可以很好的避免上述情况的发生。在该方案中部署两台设备组成 HA，这两台设备均可承担 NAT 业务，并通过 HA 通道进行会话热备、会话关联表热备、NAT 端口块表项热备以及 NAT 配置的同步。当其中一台设备故障后流量自动切换到另一台正常工作的设备。

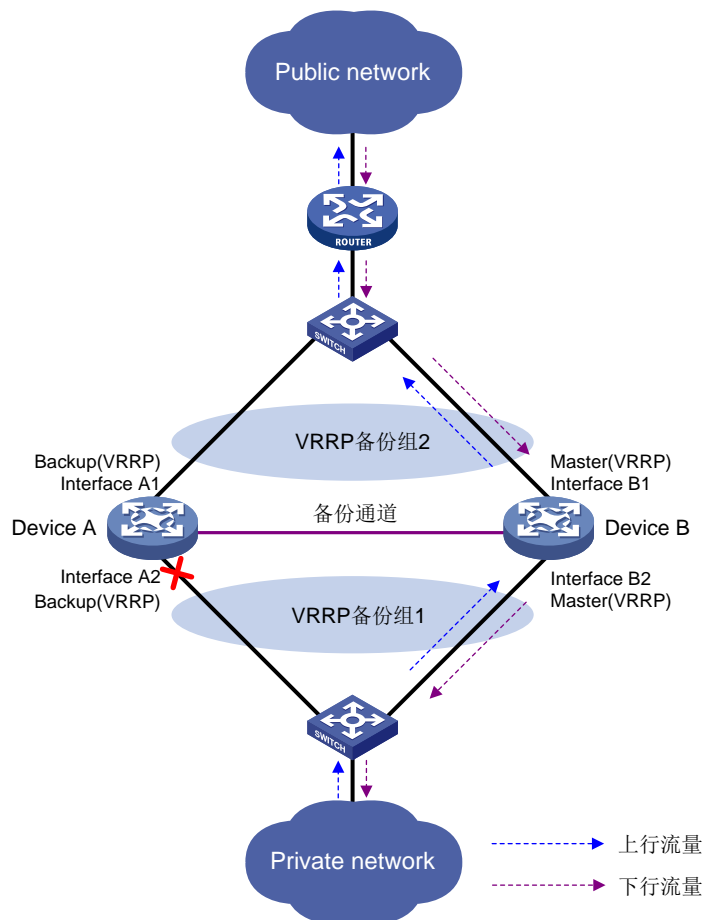
有关 HA 的详细介绍，请参见“高可靠性配置指导”中的“双机热备（RBM）”。

3.17.2 工作机制

HA 组网中的两台设备均可承担 NAT 业务，实际处理 NAT 业务的设备由 VRRP 备份组中的 Master 设备承担。下面以主备模式的 HA 为例，介绍该场景中当 Master 设备发生故障时如何保证 NAT 业务不中断。

如[图 3-1](#)所示，Device A 和 Device B 组成 HA（Device A 为 HA 中的主管理设备，Device B 为 HA 中的从管理设备），Device A 通过备份通道将会话表项、会话关联表项和端口块表项实时备份到 Device B。同时，Device A 和 Device B 的下行链路组成 VRRP 备份组 1，上行链路组成 VRRP 备

图3-2 主备模式下的流量切换



3.17.3 配置主备模式下的 NAT

1. 功能简介

在主备模式的 HA 组网中，静态 IP 地址转换、源 IP 地址转换、目的 IP 地址转换的部分转换配置会将转换后的公网 IP 地址或内部服务器对外提供服务的公网 IP 地址下发到地址管理。然后，主、备设备均会向同一局域网内所有节点通告公网 IP 与自身物理接口 MAC 地址的对应关系。导致与 HA 直连的上行三层设备可能会将下行报文发送给 HA 中的 Backup 设备，从而影响业务的正常运行。

为了避免上述情况的发生，需要将地址转换方式与 VRRP 备份组绑定。执行绑定操作后，仅 Master 设备收到对转换后 IP 地址或内部服务器对外提供服务的公网 IP 地址的 ARP 请求后，会回应 ARP 响应报文，响应报文中携带的 MAC 地址为此 VRRP 备份组的虚拟 MAC 地址，使得与 HA 直连的上行三层设备只会将下行报文发送给 HA 中的 Master 设备，保证业务的正常运行。

关于 HA 的详细介绍，请参见“高可靠性配置指导”中的“双机热备（RBM）”。

2. 配置限制和指导

请在 HA 的主管理设备的 NAT 地址组视图/NAT 端口组视图下配置 `vrrp` 命令。

3. 配置步骤

(1) 进入系统视图。

system-view

- (2) 将地址转换配置与 VRRP 备份组绑定。请根据网络需求选择步骤(3)~(8)中的一项或多项进行配置。
- (3) 将 NAT 地址组与 VRRP 备份组绑定。
 - a. 进入 NAT 地址组视图。

```
nat address-group group-id [ name group-name ]
```
 - b. 将 NAT 地址组与 VRRP 备份组绑定。

```
vrrp vrid virtual-router-id
```

缺省情况下, NAT 地址组未绑定任何 VRRP 备份组。
重复执行本命令, 最后一次执行的命令生效。
- (4) 将 NAT 端口块组与 VRRP 备份组绑定。
 - a. 进入 NAT 端口块组视图。

```
nat port-block-group group-id
```
 - b. 将 NAT 地址组与 VRRP 备份组绑定。

```
vrrp vrid virtual-router-id
```

缺省情况下, NAT 端口块组未绑定任何 VRRP 备份组。
重复执行本命令, 最后一次执行的命令生效。
- (5) 将出方向一对一静态地址转换映射与 VRRP 备份组绑定。
 - a. 进入接口视图。

```
interface interface-type interface-number
```
 - b. 将出方向一对一静态地址转换映射与 VRRP 备份组绑定。
请参见“[3.4.3 配置出方向一对一静态地址转换](#)”。
- (6) 将出方向网段到网段的静态地址转换映射 VRRP 备份组绑定。
 - a. 进入接口视图。

```
interface interface-type interface-number
```
 - b. 将出方向网段到网段的静态地址转换映射 VRRP 备份组绑定。
请参见“[3.4.4 配置出方向网段对网段静态地址转换](#)”。
- (7) 将基于对象组的出方向静态地址转换映射 VRRP 备份组绑定。
 - a. 进入接口视图。

```
interface interface-type interface-number
```
 - b. 将基于对象组的出方向静态地址转换映射 VRRP 备份组绑定。
请参见“[3.4.5 配置基于对象组的出方向静态地址转换](#)”。
- (8) 将 NAT 内部服务器与 VRRP 备份组绑定。
 - a. 进入接口视图。

```
interface interface-type interface-number
```
 - b. 将 NAT 内部服务器与 VRRP 备份组绑定。
请参见“[3.6.3 配置普通内部服务器](#)”、“[3.6.4 配置负载分担内部服务器](#)”、“[3.6.5 配置基于 ACL 的内部服务器](#)”和“[3.6.6 配置基于对象组的内部服务器](#)”。

3.17.4 配置双主模式下的 NAT

1. 功能简介

在双主模式的 HA 组网中，两台设备互为主备，仍然可能出现与 HA 直连的上行三层设备将下行报文发送给 HA 中的 Backup 设备，从而影响业务正常运行的情况。

为了避免上述情况的发生，需要将地址转换方式与 VRRP 备份组绑定。执行绑定操作后，仅 Master 设备收到对转换后 IP 地址或内部服务器对外提供服务的公网 IP 地址的 ARP 请求后，会回应 ARP 响应报文，响应报文中携带的 MAC 地址为此 VRRP 备份组的虚拟 MAC 地址。关于 HA 的详细介绍，请参见“高可靠性配置指导”中的“双机热备（RBM）”。

2. 配置限制和指导

请根据不同的情况选择不同的配置方式：

- 双主模式的 HA 组网中，两台设备可以共用同一个 NAT 地址组/NAT 端口块组，需要注意的是，为了防止不同的 Master 设备将不同主机的流量转换为同一个地址和端口号，需要使用 PAT 模式的地址转换，并配置 `nat remote-backup port-alloc` 命令，使得不同的 Master 设备使用不同范围的端口资源。
- 除上述情况外，建议双主模式 HA 组网中的两台设备使用不同的公网 IP 进行地址转换，避免出现不同的 Master 设备对不同主机的流量进行地址转换后，地址转换的结果相同的情况。例如，当 HA 中的两台设备使用不同地址范围的 NAT 地址组/NAT 端口块组时（通过 NAT 规则引用的 ACL 匹配用户流量，实现不同源 IP 地址范围的用户流量使用不同的 NAT 地址组/NAT 端口块组进行地址转换），不同的内网用户设置不同的网关地址，使得正向地址转换的流量由不同的 Master 设备进行处理。请在 HA 的主管理设备上将不同的 NAT 地址组或 NAT 端口块组与不同的 VRRP 备份组绑定，从而引导反向地址转换的流量使用不同的 Master 设备进行地址转换，实现 NAT 业务的负载分担。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 将地址转换配置与 VRRP 备份组绑定。请根据网络需求选择步骤(3)~(8)中的一项或多项进行配置。

- (3) 将 NAT 地址组与 VRRP 备份组绑定。

- a. 进入 NAT 地址组视图。

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

- b. 将 NAT 地址组与 VRRP 备份组绑定。

```
vrrp vrid virtual-router-id
```

缺省情况下，NAT 地址组未绑定任何 VRRP 备份组。

重复执行本命令，最后一次执行的命令生效。

- (4) 将 NAT 端口块组与 VRRP 备份组绑定。

- a. 进入 NAT 端口块组视图。

```
nat port-block-group group-id
```

- b. 将 NAT 端口块组与 VRRP 备份组绑定。

```
vrrp vrid virtual-router-id
```

缺省情况下，NAT 端口块组未绑定任何 VRRP 备份组。

重复执行本命令，最后一次执行的命令生效。

- (5) 将出方向一对一静态地址转换映射与 VRRP 备份组绑定。

- a. 进入接口视图。

```
interface interface-type interface-number
```

- b. 将出方向一对一静态地址转换映射与 VRRP 备份组绑定。

请参见“[3.4.3 配置出方向一对一静态地址转换](#)”。

- (6) 将出方向网段到网段的静态地址转换映射 VRRP 备份组绑定。

- a. 进入接口视图。

```
interface interface-type interface-number
```

- b. 将出方向网段到网段的静态地址转换映射 VRRP 备份组绑定。

请参见“[3.4.4 配置出方向网段对网段静态地址转换](#)”。

- (7) 将基于对象组的出方向静态地址转换映射 VRRP 备份组绑定。

- a. 进入接口视图。

```
interface interface-type interface-number
```

- b. 将基于对象组的出方向静态地址转换映射 VRRP 备份组绑定。

请参见“[3.4.5 配置基于对象组的出方向静态地址转换](#)”。

- (8) 将 NAT 内部服务器与 VRRP 备份组绑定。

- a. 进入接口视图。

```
interface interface-type interface-number
```

- b. 将 NAT 内部服务器与 VRRP 备份组绑定。

请参见“[3.6.3 配置普通内部服务器](#)”、“[3.6.4 配置负载分担内部服务器](#)”、“[3.6.5 配置基于 ACL 的内部服务器](#)”和“[3.6.6 配置基于对象组的内部服务器](#)”。

- (9) （可选）指定 HA 中主、从管理设备可以使用的 NAT 端口块范围。

- a. 退回系统视图。

```
quit
```

- b. 指定 HA 中主、从管理设备可以使用的 NAT 端口块范围。

```
nat remote-backup port-alloc { primary | secondary }
```

缺省情况下，HA 中的主、从管理设备共用 NAT 端口资源。

参数	功能
primary	表示使用数值较小的一半端口
secondary	表示使用数值较大的一半端口

3.18 配置NAT维护功能

3.18.1 配置 NAT 定时统计功能

1. 功能简介

开启 NAT 定时统计功能后，NAT 将按照一定的时间间隔对每个地址组中的会话数目和端口块分配冲突计数进行统计。

2. 配置限制和指导

使用本功能可能会占用较多的 CPU 资源，当 CPU 资源紧张时，可将其关闭。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 NAT 定时统计功能。

```
nat periodic-statistics enable
```

缺省情况下，NAT 定时统计功能处于关闭状态。

- (3) 配置 NAT 定时统计功能的时间间隔。

```
nat periodic-statistics interval interval
```

缺省情况下，NAT 定时统计功能的时间间隔为 300 秒。

如果将 NAT 定时统计功能的时间间隔调小，会占用较多的 CPU 资源。通常情况下，建议使用缺省值。

3.18.2 开启新建 NAT 会话速率的统计功能

1. 功能简介

开启此功能后，设备会对新建 NAT 会话的速率进行统计，统计信息可以通过 **display nat statistics** 命令查看。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启新建 NAT 会话速率的统计功能。

```
nat session create-rate enable
```

缺省情况下，新建 NAT 会话速率的统计功能处于关闭状态。

3.18.3 配置检测 NAT 地址组成员的可用性

1. 功能简介

通过在地址组中引用 NQA 模板来实现检测 NAT 地址组中地址可用性的目的。关于 NQA 的详细介绍，请参见“网络管理和监控配置指导”中的“NQA”。

检测 NAT 地址组成员可用性的详细过程如下：

- (1) 引用 NQA 探测模板后，设备会周期性地向 NQA 模板中指定的目的地址依次发送探测报文，其中各探测报文的源 IP 地址是地址池中的 IP 地址。
- (2) 若设备在当前探测周期内没有收到 NQA 探测应答报文，则将该探测报文的源 IP 地址从地址池中排除，即在本探测周期内禁止该 IP 地址用于地址转换。
- (3) 下一个探测周期重复以上过程。被排除的 IP 地址也会重新进行可用性探测。

2. 配置限制和指导

一个 NAT 地址组视图下，可指定多个 NQA 探测模板。当指定多个 NQA 探测模板时，只要有一个 NQA 探测模板探测成功，则表示该地址可用于地址转换。

本功能仅对用于出方向地址转换的地址成员的可用性进行检测。不对通过 **exclude-ip** 命令配置的禁止用于地址转换的 IP 地址的可用性进行检测。

引用的 NQA 探测模板中，不能配置探测报文的源 IP 地址。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 NAT 地址组视图。

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

- (3) 指定 NAT 地址组中地址成员的检测方法。

```
probe template-name
```

缺省情况下，未指定 NAT 地址组中地址成员的检测方法。

指定的检测方法可以不存在，但要使检测功能生效，必须通过 **nqa template** 命令创建检测方法所使用的 NQA 模板。

3.18.4 开启 NAT 转换失败发送 ICMP 差错报文功能

1. 功能简介

缺省情况下，NAT 设备对 ICMP 报文的地址转换失败时，不会发送 ICMP 差错报文，从而导致使用 ICMP 协议报文的应用无法感知此事件。开启本功能后，NAT 设备对 ICMP 报文地址转换失败时，会发送 ICMP 差错报文，使用 ICMP 协议报文的应用根据收到的 ICMP 差错报文发现和定位问题。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 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。

3.19 配置NAT日志功能

3.19.1 配置 NAT 会话日志功能

1. 功能简介

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。

2. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 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。

(3) 开启 NAT 相关日志功能。请至少选择其中一项进行配置。

- 开启 NAT 新建会话的日志功能。

```
nat log flow-begin
```

- 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
```

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。

3.19.2 配置 NAT444 用户日志功能

1. 功能简介

NAT444 用户日志是为了满足互联网用户溯源的需要，在 NAT444 地址转换中，对每个用户的私网 IP 地址进行端口块分配或回收时，都会输出一条基于用户的日志，记录私网 IP 地址和端口块的映射关系。在进行用户溯源时，只需根据报文的公网 IP 地址和端口找到对应的端口块分配日志信息，即可确定私网 IP 地址。

有两种情况可以触发设备输出 NAT444 用户日志：

- 端口块分配：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输出日志。

- 端口块回收：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）时输出日志。

2. 配置准备

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

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 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。

ACL 参数对 NAT444 用户日志功能无效。

- (3) 开启端口块用户日志功能。请至少选择其中一项进行配置。

- 开启端口块分配的 NAT444 用户日志功能。

```
nat log port-block-assign
```

- 开启端口块回收的 NAT444 用户日志功能。

```
nat log port-block-withdraw
```

缺省情况下，分配和回收端口块时，均不输出 NAT444 用户日志。

3.19.3 配置 NAT 告警信息日志功能

1. 功能简介

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的资源无法对其进行地址转换，相应的报文将被丢弃。本命令用来在 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；在 NAT444 地址转换中，NAT 资源是指公网 IP、端口块和端口块中的端口。

NAT444 端口块动态映射方式中，当端口块分配失败时，系统会输出日志信息。

NAT444 端口块动态映射方式中，当端口块中的端口资源都用尽但还是无法满足用户的地址转换需求时，系统会输出日志信息。

2. 配置限制和指导

只有开启 NAT 日志功能（通过 `nat log enable` 命令）之后，NAT 告警信息日志功能才能生效。

3. 配置准备

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

4. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 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。

ACL 参数对 NAT 告警信息日志功能无效。

- (3) 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。

NAT 资源用尽时，系统会输出告警日志。

- (4) （可选）配置动态 NAT444 端口块使用率的阈值。

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

缺省情况下，动态 NAT444 的端口块使用率的阈值为 90%。

创建动态端口块表项时，若端口块的使用率大于阈值，系统会输出告警日志。

3.19.4 开启 NO-PAT 方式下 NAT 地址组中地址成员使用率的日志信息功能

1. 功能简介

创建 NO-PAT 表项时，若 NO-PAT 方式下 NAT 地址组中地址成员的使用率超过设定的百分比时，系统将会输出日志信息。

2. 配置限制和指导

只有开启 NAT 日志功能（通过 `nat log enable` 命令）之后，NAT 地址组中地址成员使用率的日志信息功能才能生效。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 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。

ACL 参数对 NO-PAT 方式下 NAT 地址组中地址成员使用率的日志信息功能无效。

- (3) 开启 NO-PAT 方式下 NAT 地址组中地址成员使用率的日志信息功能，并设置 NAT 地址组中地址成员使用率的阈值。

```
nat log no-pat ip-usage [ threshold value ]
```

缺省情况下，NAT 地址组中地址成员使用率的日志信息功能处于关闭状态。

3.20 配置 NAT 生成 OpenFlow 流表

1. 功能简介

开启该功能后，新的 NAT 转换配置会生成 OpenFlow 流表，已经存在的 NAT 转换配置会补充生成 OpenFlow 流表。如果关闭此功能，则新的 NAT 转换配置不会再生成 OpenFlow 流表，已存在的 NAT 转换配置生成的 OpenFlow 流表会被删除，从而可能造成流量中断。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 NAT 生成 OpenFlow 流表的功能。

```
nat flow-redirect { all | dynamic | server | static | static-port-block }  
*
```

缺省情况下，NAT 生成 OpenFlow 流表的功能处于开启状态。

3.21 特定条件下的NAT配置

3.21.1 开启反向报文的重定向功能

1. 功能简介

在入方向动态地址转换功能与隧道功能配合使用的组网环境中，若多个隧道接口引用同一个 NAT 地址组，则设备会将来自不同隧道的报文的源 IP 地址转换为相同的 NAT 地址，并从设备的出接口转发出去。缺省情况下，设备出接口收到反向报文后，不会查询 NAT 会话表项，这将导致反向报文不能正确转发。为解决此问题，可在设备的出接口开启反向报文的重定向功能，使出接口收到反向报文后查询 NAT 会话表项，根据 NAT 会话表项记录的信息将反向报文的目的 IP 地址进行 NAT 地址转换，从而使反向报文通过接收正向报文的隧道发送出去。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 开启反向报文的重定向功能。

```
nat redirect reply-route enable
```

缺省情况下，反向报文的重定向功能处于关闭状态。

3.21.2 开启对 TCP SYN 和 SYN ACK 报文中时间戳的删除功能

1. 功能简介

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

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

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启对 TCP SYN 和 SYN ACK 报文中时间戳的删除功能。

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

缺省情况下，不对 TCP SYN 和 SYN ACK 报文中的时间戳进行删除。

多次执行本命令，可为不同 VPN 中的报文开启此功能。

3.21.3 开启主备链路切换后的 NAT 会话重建功能

1. 功能简介

广域网双出口组网环境中，分别在 NAT 设备的出接口（假设为 Interface A 和 Interface B）下配置出方向动态地址转换（引用不同的地址组），基于出接口所属安全域的不同情况，NAT 设备的处理机制有所不同：

- 如果两个出接口属于不同的安全域，当 Interface A 的链路发生故障切换到 Interface B 的链路时，NAT 设备会删除原来的会话表项，由流量触发重新建立 NAT 会话，保证用户访问外网的业务不受影响。
- 如果两个出接口属于相同的安全域，当 Interface A 的链路发生故障切换到 Interface B 的链路时，NAT 设备不会删除原来的会话表项，流量与原来的会话表项匹配，导致用户无法访问外网。为了避免该问题的发生，请开启本功能，保证用户业务的可用性。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启主备链路切换后的 NAT 会话重建功能。

```
nat link-switch recreate-session
```

缺省情况下，主备链路切换后的 NAT 会话重建功能处于关闭状态。

3.21.4 主备链路切换导致出接口所属安全域变化后的 NAT 会话重建功能

1. 功能简介

广域网双出口组网环境中，NAT 设备上的出方向动态地址转换（引用不同的地址组）分别在不同的出接口生效（假设为 Interface A 和 Interface B），基于出接口所属安全域的不同情况，NAT 设备的处理机制有所不同：

- 如果两个出接口属于不同的安全域，当 Interface A 的链路发生故障切换到 Interface B 的链路时，NAT 设备会删除原来的会话表项，由流量触发重新建立 NAT 会话表项。
- 如果两个出接口属于同一个安全域，当 Interface A 的链路发生故障切换到 Interface B 的链路时，NAT 设备不会删除原来的会话表项，流量与原来的会话表项匹配。若这种处理方式会导致用户无法访问外网，则请通过 **nat link-switch recreate-session** 命令开启主备链路切换后的 NAT 会话重建功能。若这种处理方式不会导致用户无法访问外网，则无需执行其他配置。

2. 配置限制和指导

主备链路切换导致出接口所属安全域变化后的 NAT 会话重建功能处于缺省开启状态，用户无法通过命令行对该功能的开启/关闭进行控制。

3.22 接口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。



说明

非缺省 vSystem 不支持部分显示和维护命令，具体情况请参见本特性的命令参考。

表3-1 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 [<i>group-id</i>]
显示NAT DNS mapping的配置信息	display nat dns-map
显示Easy IP方式动态地址转换的备份组的端口范围信息	display nat easy-ip failover-group port-range
显示NAT EIM表项信息	(独立运行模式) display nat eim [<i>slot slot-number</i> [<i>cpu cpu-number</i>]] (IRF模式) display nat eim [<i>chassis chassis-number slot slot-number</i> [<i>cpu cpu-number</i>]]
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	(独立运行模式) display nat no-pat { <i>ipv4</i> <i>ipv6</i> } [<i>slot slot-number</i> [<i>cpu cpu-number</i>]] (IRF模式) display nat no-pat { <i>ipv4</i> <i>ipv6</i> } [<i>chassis chassis-number slot slot-number</i> [<i>cpu cpu-number</i>]]
显示NO-PAT方式下NAT地址组中地址成员的使用率	(独立运行模式) display nat no-pat ip-usage [<i>address-group</i> { <i>group-id</i> <i>name group-name</i> } <i>object-group object-group-name</i>] [<i>slot slot-number</i> [<i>cpu cpu-number</i>]] (IRF模式) display nat no-pat ip-usage [<i>address-group</i> { <i>group-id</i> <i>name group-name</i> } <i>object-group object-group-name</i>] [<i>chassis chassis-number slot slot-number</i> [<i>cpu cpu-number</i>]]

操作	命令
显示NAT出接口动态地址转换关系的配置信息	display nat outbound
显示NAT定时统计功能的计数信息	（独立运行模式） display nat periodic-statistics { address-group [<i>group-id</i> name <i>group-name</i>] ip global-ip } [slot <i>slot-number</i> [cpu <i>cpu-number</i>]] （IRF模式） display nat periodic-statistics { address-group [<i>group-id</i> name <i>group-name</i>] ip global-ip } [chassis <i>chassis-number</i> slot <i>slot-number</i> [cpu <i>cpu-number</i>]]
显示接口NAT策略的配置信息	display nat policy
显示NAT内部服务器的配置信息	display nat server
显示NAT内部服务器组的配置信息	display nat server-group [<i>group-id</i>]
显示NAT会话	（独立运行模式） display nat session [[responder] { source-ip <i>source-ip</i> destination-ip <i>destination-ip</i> } * [vpn-instance <i>vpn-instance-name</i>]] [slot <i>slot-number</i> [cpu <i>cpu-number</i>]] [verbose] （IRF模式） display nat session [[responder] { source-ip <i>source-ip</i> destination-ip <i>destination-ip</i> } * [vpn-instance <i>vpn-instance-name</i>]] [chassis <i>chassis-number</i> slot <i>slot-number</i> [cpu <i>cpu-number</i>]] [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	（独立运行模式） display nat statistics [summary] [slot <i>slot-number</i> [cpu <i>cpu-number</i>]] （IRF模式） display nat statistics [summary] [chassis <i>chassis-number</i> slot <i>slot-number</i> [cpu <i>cpu-number</i>]]
显示NAT444端口块静态映射的配置信息	display nat outbound port-block-group
显示NAT端口块组配置信息	display nat port-block-group [<i>group-id</i>]

操作	命令
显示端口块表项	<p>(独立运行模式)</p> <pre>display nat port-block { dynamic [address-group { group-id name group-name }] [ds-lite-b4] static [port-block-group group-id] } [slot slot-number [cpu cpu-number]]</pre> <p>(IRF模式)</p> <pre>display nat port-block { dynamic [address-group { group-id name group-name }] [ds-lite-b4] static [port-block-group group-id] } [chassis chassis-number slot slot-number [cpu cpu-number]]</pre>
显示动态NAT444地址组中端口块的使用率	<p>(独立运行模式)</p> <pre>display nat port-block-usage [address-group group-id] [slot slot-number [cpu cpu-number]]</pre> <p>(IRF模式)</p> <pre>display nat port-block-usage [address-group group-id] [chassis chassis-number slot slot-number [cpu cpu-number]]</pre>
显示NAT地址组中地址成员的检测信息	<pre>display nat probe address-group [group-id]</pre>
清除NAT转换计数信息	<pre>reset nat count statistics { all dynamic policy server static static-port-block }</pre>
清除NAT定时统计功能的计数信息	<p>(独立运行模式)</p> <pre>reset nat periodic-statistics [slot slot-number [cpu cpu-number]]</pre> <p>(IRF模式)</p> <pre>reset nat periodic-statistics [chassis chassis-number slot slot-number [cpu cpu-number]]</pre>
删除NAT会话	<p>(独立运行模式)</p> <pre>reset nat session [slot slot-number [cpu cpu-number]]</pre> <p>(IRF模式)</p> <pre>reset nat session [chassis chassis-number slot slot-number [cpu cpu-number]]</pre>

3.23 接口NAT典型配置举例

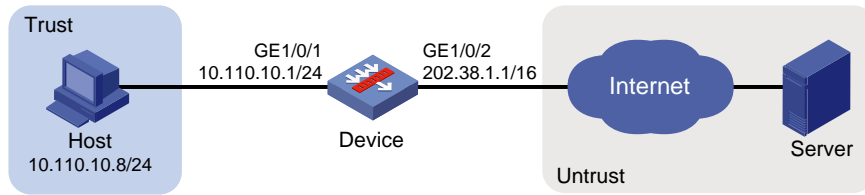
3.23.1 内网用户通过 NAT 地址访问外网配置举例（静态地址转换）

1. 组网需求

内部网络用户 10.110.10.8/24 使用外网地址 202.38.1.100 访问 Internet。

2. 组网图

图3-3 内网用户通过 NAT 地址访问外网配置组网图（静态地址转换）



3. 配置步骤

配置接口 IP 地址、路由、安全域及域间策略保证网络可达，具体配置步骤略。

配置内网 IP 地址 10.110.10.8 到外网地址 202.38.1.100 之间的一对一静态地址转换映射。

```
<Device> system-view
[Device] nat static outbound 10.110.10.8 202.38.1.100
```

使配置的静态地址转换在接口 GigabitEthernet1/0/2 上生效。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] nat static enable
[Device-GigabitEthernet1/0/2] quit
```

4. 验证配置

以上配置完成后，内网主机可以访问外网服务器。通过查看如下显示信息，可以验证以上配置成功。

```
[Device] display nat static
Static NAT mappings:
  Totally 1 outbound static NAT mappings.
  IP-to-IP:
    Local IP      : 10.110.10.8
    Global IP     : 202.38.1.100
    Config status: Active

Interfaces enabled with static NAT:
  Totally 1 interfaces enabled with static NAT.
  Interface: GigabitEthernet1/0/2
  Config status: Active
```

通过以下显示命令，可以看到 Host 访问某外网服务器时生成 NAT 会话信息。

```
[Device] display nat session verbose
Slot 1:
Initiator:
  Source      IP/port: 10.110.10.8/54765
  Destination IP/port: 202.38.1.2/23
```



```

DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/1
Source security zone: Trust
Responder:
Source      IP/port: 202.38.1.2/23
Destination IP/port: 202.38.1.100/54765
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/2
Source security zone: Untrust
State: TCP_ESTABLISHED
Application: TELNET
Rule ID: -/-/-
Rule name:
Start time: 2017-05-19 10:57:47  TTL: 1195s
Initiator->Responder:           8 packets      375 bytes
Responder->Initiator:          10 packets      851 bytes

Total sessions found: 1

```

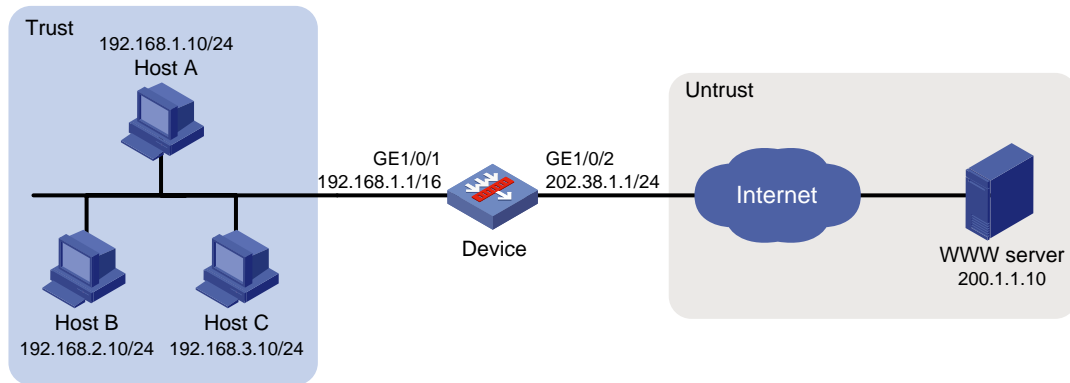
3.23.2 内网用户通过 NAT 地址访问外网配置举例（地址不重叠）

1. 组网需求

- 某公司内网使用的 IP 地址为 192.168.0.0/16。
- 该公司拥有 202.38.1.2 和 202.38.1.3 两个外网 IP 地址。
- 要实现，内部网络中 192.168.1.0/24 网段的用户可以访问 Internet，其它网段的用户不能访问 Internet。使用的外网地址为 202.38.1.2 和 202.38.1.3。

2. 组网图

图3-4 内网用户通过 NAT 访问外网配置组网图（地址不重叠）



3. 配置步骤

配置接口 IP 地址、路由、安全域及域间策略保证网络可达，具体配置步骤略。

配置地址组 0，包含两个外网地址 202.38.1.2 和 202.38.1.3。

```
<Device> system-view
[Device] nat address-group 0
[Device-address-group-0] address 202.38.1.2 202.38.1.3
[Device-address-group-0] quit
```

配置 ACL 2000，仅允许对内部网络中 192.168.1.0/24 网段的用户报文进行地址转换。

```
[Device] acl basic 2000
[Device-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Device-acl-ipv4-basic-2000] quit
```

在接口 GigabitEthernet1/0/2 上配置出方向动态地址转换，允许使用地址组 0 中的地址对匹配 ACL 2000 的报文进行源地址转换，并在转换过程中使用端口信息。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] nat outbound 2000 address-group 0
[Device-GigabitEthernet1/0/2] quit
```

4. 验证配置

以上配置完成后，Host A 能够访问 WWW server，Host B 和 Host C 无法访问 WWW server。通过查看如下显示信息，可以验证以上配置成功。

```
[Device] display nat all

NAT address group information:

  Totally 1 NAT address groups.

  Address group ID: 0

  Port range: 1-65535

  Address information:

    Start address      End address
```

```

202.38.1.2          202.38.1.3

Exclude address information:

Start address      End address
---              ---

NAT outbound information:

Totally 1 NAT outbound rules.

Interface: GigabitEthernet1/0/2

ACL: 2000

Address group ID: 0

Port-preserved: N   NO-PAT: N       Reversible: N

Config status: Active

NAT logging:

Log enable         : Disabled
Flow-begin         : Disabled
Flow-end           : Disabled
Flow-active        : Disabled
Port-block-assign  : Disabled
Port-block-withdraw : Disabled
Alarm              : Disabled
NO-PAT IP usage    : Disabled

NAT mapping behavior:

Mapping mode : Address and Port-Dependent
ACL          : ---
Config status: Active

NAT ALG:

DNS           : Enabled
FTP           : Enabled
H323          : Disabled
ICMP-ERROR    : Enabled
ILS           : Disabled
MGCP          : Disabled
NBT           : Disabled
PPTP          : Enabled
RTSP          : Enabled

```

```

RSH      : Disabled
SCCP     : Disabled
SCTP     : Disabled
SIP      : Disabled
SQLNET   : Disabled
TFTP     : Disabled
XDMCP    : Disabled

Static NAT load balancing:      Disabled

NAT link-switch recreate-session: Disabled

NAT configuration-for-new-connection: Disabled

NAT global-policy compatible-previous-version rule-type ipv4-snat-and-dnat
translate-before-secp : Disabled

NAT gratuitous-arp: Enabled

```

通过以下显示命令，可以看到 Host A 访问 WWW server 时生成 NAT 会话信息。

```

[Device] display nat session verbose
Slot 1:
Initiator:
  Source      IP/port: 192.168.1.10/52082
  Destination IP/port: 200.1.1.10/80
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Trust
Responder:
  Source      IP/port: 200.1.1.10/80
  Destination IP/port: 202.38.1.2/1036
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Untrust
State: TCP_ESTABLISHED

```

```

Application: HTTP
Rule ID: -/-/-
Rule name:
Start time: 2017-05-19 16:16:59   TTL: 9995s
Initiator->Responder:           551 packets      32547 bytes
Responder->Initiator:           956 packets      1385514 bytes
Total sessions found: 1

```

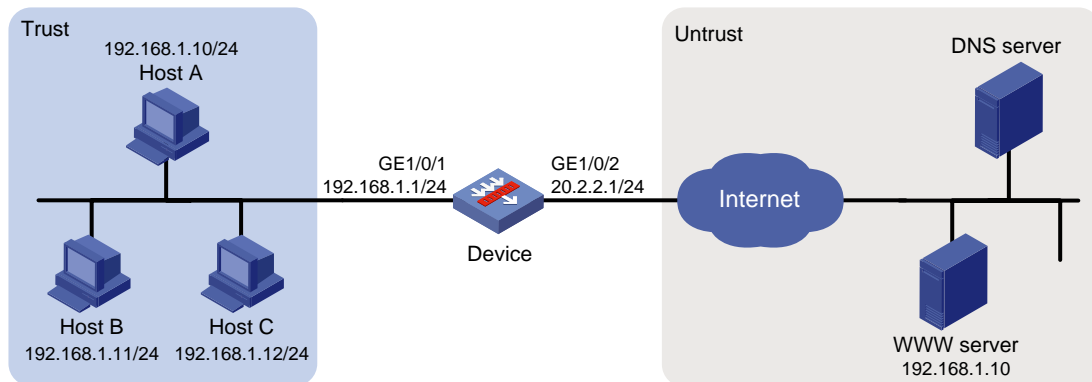
3.23.3 内网用户通过 NAT 地址访问外网配置举例（地址重叠）

1. 组网需求

- 某公司内网网段地址为 192.168.1.0/24，该网段与要访问的外网 Web 服务器所在网段地址重叠。
- 该公司拥有 202.38.1.2 和 202.38.1.3 两个外网 IP 地址。
- 要实现，内网用户可以通过域名访问外网的 Web 服务器。

2. 组网图

图3-5 内网用户通过 NAT 访问外网配置组网图（地址重叠）



3. 配置思路

这是一个典型的双向 NAT 应用，具体配置思路如下。

- 内网主机通过域名访问外网 Web 服务器时，首先需要向外网的 DNS 服务器发起 DNS 查询请求。由于外网 DNS 服务器回复给内网主机的 DNS 应答报文载荷中的携带的 Web 服务器地址与内网主机地址重叠，因此 NAT 设备需要将载荷中的 Web 服务器地址转换为动态分配的一个 NAT 地址。动态地址分配可以通过入方向动态地址转换实现，载荷中的地址转换需要通过 DNS ALG 功能实现。
- 内网主机得到外网 Web 服务器的 IP 地址之后（该地址为临时分配的 NAT 地址），通过该地址访问外网 Web 服务器。由于内网主机的地址与外网 Web 服务器的真实地址重叠，因此也需要为其动态分配一个 NAT 地址，可以通过出方向动态地址转换实现。

- 外网 Web 服务器对应的 NAT 地址在 NAT 设备上没有路由，因此需要手工添加静态路由，使得目的地址为外网服务器 NAT 地址的报文出接口为 GigabitEthernet1/0/2。

4. 配置步骤

配置接口 IP 地址、路由、安全域及域间策略保证网络可达，具体配置步骤略。

开启 DNS 的 NAT ALG 功能。

```
<Device> system-view
```

```
[Device] nat alg dns
```

配置 ACL 2000，仅允许对 192.168.1.0/24 网段的用户报文进行地址转换。

```
[Device] acl basic 2000
```

```
[Device-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255
```

```
[Device-acl-ipv4-basic-2000] quit
```

创建地址组 1。

```
[Device] nat address-group 1
```

添加地址组成员 202.38.1.2。

```
[Device-address-group-1] address 202.38.1.2 202.38.1.2
```

```
[Device-address-group-1] quit
```

创建地址组 2。

```
[Device] nat address-group 2
```

添加地址组成员 202.38.1.3。

```
[Device-address-group-2] address 202.38.1.3 202.38.1.3
```

```
[Device-address-group-2] quit
```

在接口 GigabitEthernet1/0/2 上配置入方向动态地址转换，允许使用地址组 1 中的地址对 DNS 应答报文载荷中的外网地址进行转换，并在转换过程中不使用端口信息，以及允许反向地址转换。

```
[Device] interface gigabitethernet 1/0/2
```

```
[Device-GigabitEthernet1/0/2] nat inbound 2000 address-group 1 no-pat reversible
```

在接口 GigabitEthernet1/0/2 上配置出方向动态地址转换，允许使用地址组 2 中的地址对内网访问外网的报文进行源地址转换，并在转换过程中使用端口信息。

```
[Device-GigabitEthernet1/0/2] nat outbound 2000 address-group 2
```

```
[Device-GigabitEthernet1/0/2] quit
```

配置静态路由，目的地址为外网服务器 NAT 地址 202.38.1.2，出接口为 GigabitEthernet1/0/2，下一跳地址为 20.2.2.2（20.2.2.2 为本例中的直连下一跳地址，实际使用中请以具体组网情况为准）。

```
[Device] ip route-static 202.38.1.2 32 gigabitethernet 1/0/2 20.2.2.2
```

5. 验证配置

以上配置完成后，Host A 能够通过域名访问 Web server。通过查看如下显示信息，可以验证以上配置成功。

```
[Device] display nat all
```

```
NAT address group information:
```

```
Totally 2 NAT address groups.
```

```

Address group ID: 1
  Port range: 1-65535
  Address information:
    Start address      End address
    202.38.1.2         202.38.1.2
  Exclude address information:
    Start address      End address
    ---               ---

Address group ID: 2
  Port range: 1-65535
  Address information:
    Start address      End address
    202.38.1.3         202.38.1.3
  Exclude address information:
    Start address      End address
    ---               ---

NAT inbound information:
  Totally 1 NAT inbound rules.
  Interface: GigabitEthernet1/0/2
  ACL: 2000
  Address group ID: 1
  Add route: N        NO-PAT: Y    Reversible: Y
  Config status: Active

NAT outbound information:
  Totally 1 NAT outbound rules.
  Interface: GigabitEthernet1/0/2
  ACL: 2000
  Address group ID: 2
  Port-preserved: N    NO-PAT: N    Reversible: N
  Config status: Active

NAT logging:
  Log enable          : Disabled
  Flow-begin          : Disabled
  Flow-end            : Disabled

```

```

Flow-active           : Disabled
Port-block-assign     : Disabled
Port-block-withdraw   : Disabled
Alarm                 : Disabled
NO-PAT IP usage       : Disabled

NAT mapping behavior:

Mapping mode : Address and Port-Dependent
ACL          : ---
Config status: Active

NAT ALG:

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

Static NAT load balancing:      Disabled

NAT link-switch recreate-session: Disabled

NAT configuration-for-new-connection: Disabled

NAT global-policy compatible-previous-version rule-type ipv4-snat-and-dnat
translate-before-secp : Disabled

```



```
NAT gratuitous-arp: Enabled
```

通过以下显示命令，可以看到 Host A 访问 WWW server 时生成 NAT 会话信息。

```
[Device] display nat session verbose

Slot 1:

Initiator:

  Source      IP/port: 192.168.1.10/51716
  Destination IP/port: 202.38.1.2/80
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Trust

Responder:

  Source      IP/port: 202.38.1.2/80
  Destination IP/port: 202.38.1.3/1059
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Untrust

State: TCP_ESTABLISHED
Application: HTTP
Rule ID: -/-/-
Rule name:

Start time: 2017-05-21 15:36:29  TTL: 1197s

Initiator->Responder:          125 packets          6304 bytes
Responder->Initiator:          223 packets          325718 bytes

Total sessions found: 1
```

3.23.4 外网用户通过外网地址访问内网服务器配置举例

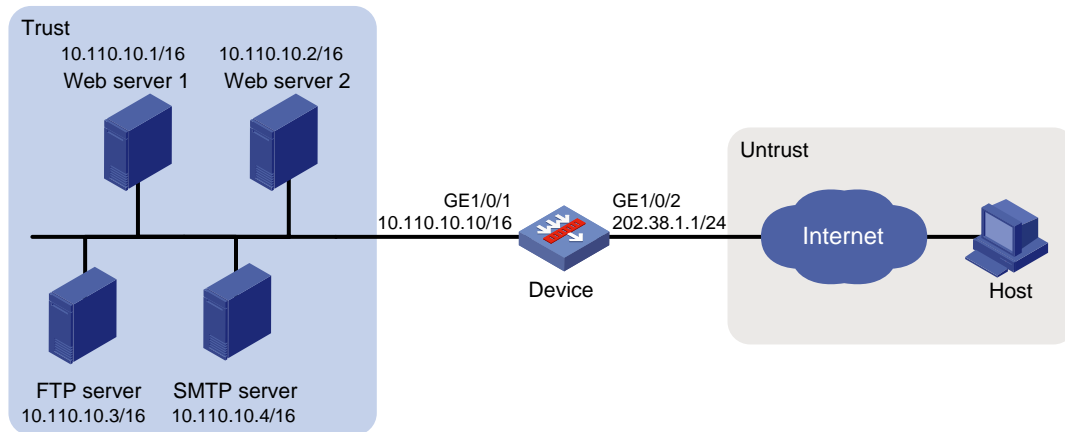
1. 组网需求

某公司内部对外提供 Web、FTP 和 SMTP 服务，而且提供两台 Web 服务器。公司内部网址为 10.110.0.0/16。其中，内部 FTP 服务器地址为 10.110.10.3/16，内部 Web 服务器 1 的 IP 地址为 10.110.10.1/16，内部 Web 服务器 2 的 IP 地址为 10.110.10.2/16，内部 SMTP 服务器 IP 地址为 10.110.10.4/16。公司拥有 202.38.1.1 至 202.38.1.3 三个公网 IP 地址。需要实现如下功能：

- 外部的主机可以访问内部的服务器。
- 选用 202.38.1.1 作为公司对外提供服务的 IP 地址，Web 服务器 2 对外采用 8080 端口。

2. 组网图

图3-6 外网用户通过外网地址访问内网服务器配置组网图



3. 配置步骤

配置接口 IP 地址、路由、安全域及域间策略保证网络可达，具体配置步骤略。

进入接口 GigabitEthernet1/0/2。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/2
```

配置内部 FTP 服务器，允许外网主机使用地址 202.38.1.1、端口号 21 访问内网 FTP 服务器。

```
[Device-GigabitEthernet1/0/2] nat server protocol tcp global 202.38.1.1 21 inside
10.110.10.3 ftp
```

配置内部 Web 服务器 1，允许外网主机使用地址 202.38.1.1、端口号 80 访问内网 Web 服务器 1。

```
[Device-GigabitEthernet1/0/2] nat server protocol tcp global 202.38.1.1 80 inside
10.110.10.1 http
```

配置内部 Web 服务器 2，允许外网主机使用地址 202.38.1.1、端口号 8080 访问内网 Web 服务器 2。

```
[Device-GigabitEthernet1/0/2] nat server protocol tcp global 202.38.1.1 8080 inside
10.110.10.2 http
```

配置内部 SMTP 服务器，允许外网主机使用地址 202.38.1.1 以及 SMTP 协议定义的端口访问内网 SMTP 服务器。

```
[Device-GigabitEthernet1/0/2] nat server protocol tcp global 202.38.1.1 smtp inside
10.110.10.4 smtp
[Device-GigabitEthernet1/0/2] quit
```

4. 验证配置

以上配置完成后，外网 Host 能够通过 NAT 地址访问各内网服务器。通过查看如下显示信息，可以验证以上配置成功。

```
[Device] display nat all

NAT internal server information:
```

Totally 4 internal servers.

Interface: GigabitEthernet1/0/2

Protocol: 6(TCP)

Global IP/port: 202.38.1.1/21

Local IP/port : 10.110.10.3/21

Rule name : ServerRule_1

NAT counting : 0

Config status : Active

Interface: GigabitEthernet1/0/2

Protocol: 6(TCP)

Global IP/port: 202.38.1.1/25

Local IP/port : 10.110.10.4/25

Rule name : ServerRule_4

NAT counting : 0

Config status : Active

Interface: GigabitEthernet1/0/2

Protocol: 6(TCP)

Global IP/port: 202.38.1.1/80

Local IP/port : 10.110.10.1/80

Rule name : ServerRule_2

NAT counting : 0

Config status : Active

Interface: GigabitEthernet1/0/2

Protocol: 6(TCP)

Global IP/port: 202.38.1.1/8080

Local IP/port : 10.110.10.2/80

Rule name : ServerRule_3

NAT counting : 0

Config status : Active

NAT logging:

Log enable : Disabled

Flow-begin : Disabled

Flow-end : Disabled

Flow-active : Disabled

```

Port-block-assign      : Disabled
Port-block-withdraw    : Disabled
Alarm                  : Disabled
NO-PAT IP usage        : Disabled

NAT mapping behavior:

Mapping mode : Address and Port-Dependent
ACL          : ---
Config status: Active

NAT ALG:

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

Static NAT load balancing:      Disabled

NAT link-switch recreate-session: Disabled

NAT configuration-for-new-connection: Disabled

NAT global-policy compatible-previous-version rule-type ipv4-snat-and-dnat
translate-before-secp : Disabled

NAT gratuitous-arp: Enabled

```

通过以下显示命令，可以看到 Host 访问 FTP server 时生成 NAT 会话信息。

```
[Device] display nat session verbose
Slot 1:
Initiator:
    Source      IP/port: 202.38.1.2/52802
    Destination IP/port: 202.38.1.1/21
    DS-Lite tunnel peer: -
    VPN instance/VLAN ID/Inline ID: -/-/-
    Protocol: TCP(6)
    Inbound interface: GigabitEthernet1/0/2
    Source security zone: Untrust
Responder:
    Source      IP/port: 10.110.10.3/21
    Destination IP/port: 202.38.1.2/52802
    DS-Lite tunnel peer: -
    VPN instance/VLAN ID/Inline ID: -/-/-
    Protocol: TCP(6)
    Inbound interface: GigabitEthernet1/0/1
    Source security zone: Trust
State: TCP_ESTABLISHED
Application: FTP
Rule ID: -/-/-
Rule name:
Start time: 2017-05-21 11:13:39  TTL: 3597s
Initiator->Responder:          7 packets          313 bytes
Responder->Initiator:          6 packets          330 bytes

Total sessions found: 1
```

3.23.5 外网用户通过域名访问内网服务器配置举例（地址不重叠）

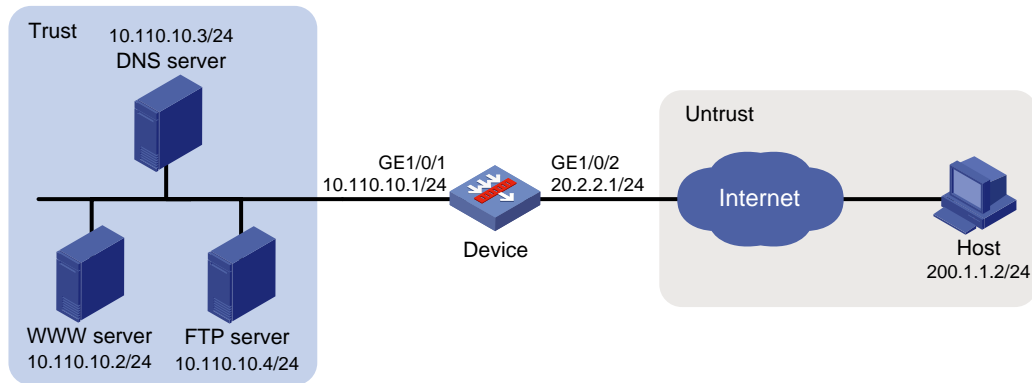
1. 组网需求

- 某公司内部对外提供 Web 服务，Web 服务器地址为 10.110.10.2/24。
- 该公司在内网有一台 DNS 服务器，IP 地址为 10.110.10.3/24，用于解析 Web 服务器的域名。
- 该公司拥有两个外网 IP 地址：202.38.1.2 和 202.38.1.3。

需要实现，外网主机可以通过域名访问内网的 Web 服务器。

2. 组网图

图3-7 外网用户通过域名访问内网服务器配置组网图（地址不重叠）



3. 配置思路

- 外网主机通过域名访问 Web 服务器，首先需要通过访问内网 DNS 服务器获取 Web 服务器的 IP 地址，因此需要通过配置 NAT 内部服务器将 DNS 服务器的内网 IP 地址和 DNS 服务端口映射为一个外网地址和端口。
- DNS 服务器回应给外网主机的 DNS 报文载荷中携带了 Web 服务器的内网 IP 地址，因此需要将 DNS 报文载荷中的内网 IP 地址转换为一个外网 IP 地址。外网地址分配可以通过出方向动态地址转换功能实现，转换载荷信息可以通过 DNS ALG 功能实现。

4. 配置步骤

配置接口 IP 地址、路由、安全域及域间策略保证网络可达，具体配置步骤略。

开启 DNS 协议的 ALG 功能。

```
<Device> system-view
```

```
[Device] nat alg dns
```

配置 ACL 2000，允许对内部网络中 10.110.10.2 的报文进行地址转换。

```
[Device] acl basic 2000
```

```
[Device-acl-ipv4-basic-2000] rule permit source 10.110.10.2 0
```

```
[Device-acl-ipv4-basic-2000] quit
```

创建地址组 1。

```
[Device] nat address-group 1
```

添加地址组成员 202.38.1.3。

```
[Device-address-group-1] address 202.38.1.3 202.38.1.3
```

```
[Device-address-group-1] quit
```

在接口 GigabitEthernet1/0/2 上配置 NAT 内部服务器，允许外网主机使用地址 202.38.1.2 访问内网 DNS 服务器。

```
[Device] interface gigabitethernet 1/0/2
```

```
[Device-GigabitEthernet1/0/2] nat server protocol udp global 202.38.1.2 inside 10.110.10.3 dns
```

在接口 GigabitEthernet1/0/2 上配置出方向动态地址转换，允许使用地址组 1 中的地址对 DNS 应答报文载荷中的内网地址进行转换，并在转换过程中不使用端口信息，以及允许反向地址转换。

```
[Device-GigabitEthernet1/0/2] nat outbound 2000 address-group 1 no-pat reversible
[Device-GigabitEthernet1/0/2] quit
```

5. 验证配置

以上配置完成后，外网 Host 能够通过域名访问内网 Web server。通过查看如下显示信息，可以验证以上配置成功。

```
[Device] display nat all
NAT address group information:
  Totally 1 NAT address groups.
  Address group ID: 1
  Port range: 1-65535
  Address information:
    Start address      End address
    202.38.1.3         202.38.1.3
  Exclude address information:
    Start address      End address
    ---               ---

NAT outbound information:
  Totally 1 NAT outbound rules.
  Interface: GigabitEthernet1/0/2
  ACL: 2000
  Address group ID: 1
  Port-preserved: N    NO-PAT: Y    Reversible: Y
  Config status: Active

NAT internal server information:
  Totally 1 internal servers.
  Interface: GigabitEthernet1/0/2
  Protocol: 17(UDP)
  Global IP/port: 202.38.1.2/53
  Local IP/port : 10.110.10.3/53
  Rule name      : ServerRule_1
  NAT counting   : 0
  Config status  : Active

NAT logging:
```

Log enable : Disabled
Flow-begin : Disabled
Flow-end : Disabled
Flow-active : Disabled
Port-block-assign : Disabled
Port-block-withdraw : Disabled
Alarm : Disabled
NO-PAT IP usage : Disabled

NAT mapping behavior:

Mapping mode : Address and Port-Dependent
ACL : ---
Config status: Active

NAT ALG:

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

Static NAT load balancing: Disabled

NAT link-switch recreate-session: Disabled

NAT configuration-for-new-connection: Disabled


```
NAT global-policy compatible-previous-version rule-type ipv4-snat-and-dnat
translate-before-secp : Disabled
```

```
NAT gratuitous-arp: Enabled
```

通过以下显示命令，可以看到 Host 访问 Web server 时生成 NAT 会话信息。

```
[Device] display nat session verbose
Slot 1:
Initiator:
    Source      IP/port: 200.1.1.2/1694
    Destination IP/port: 202.38.1.3/8080
    DS-Lite tunnel peer: -
    VPN instance/VLAN ID/Inline ID: -/-/-
    Protocol: TCP(6)
    Inbound interface: GigabitEthernet1/0/2
    Source security zone: Untrust
Responder:
    Source      IP/port: 10.110.10.2/8080
    Destination IP/port: 200.1.1.2/1694
    DS-Lite tunnel peer: -
    VPN instance/VLAN ID/Inline ID: -/-/-
    Protocol: TCP(6)
    Inbound interface: GigabitEthernet1/0/1
    Source security zone: Trust
State: TCP_ESTABLISHED
Application: HTTP
Rule ID: -/-/-
Rule name:
Start time: 2017-06-15 14:53:29  TTL: 3597s
Initiator->Responder:          7 packets          308 bytes
Responder->Initiator:          5 packets          312 bytes

Total sessions found: 1
```

3.23.6 外网用户通过域名访问内网服务器配置举例（地址重叠）

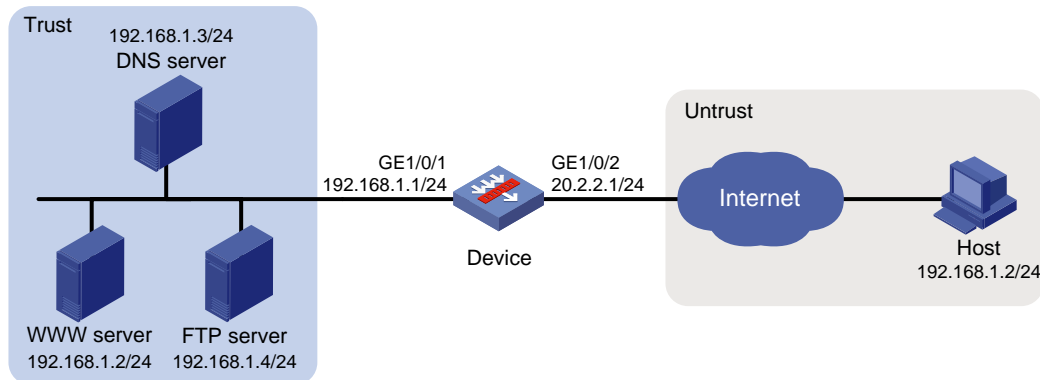
1. 组网需求

- 某公司内网使用的 IP 地址为 192.168.1.0/24。
- 该公司内部对外提供 Web 服务，Web 服务器地址为 192.168.1.2/24。
- 该公司在内网有一台 DNS 服务器，IP 地址为 192.168.1.3/24，用于解析 Web 服务器的域名。

- 该公司拥有三个外网 IP 地址：202.38.1.2、202.38.1.3 和 202.38.1.4。
需要实现，外网主机可以通过域名访问与其地址重叠的内网 Web 服务器。

2. 组网图

图3-8 外网用户通过域名访问内网服务器配置组网图（地址重叠）



3. 配置思路

这是一个典型的双向 NAT 应用，具体配置思路如下。

- 外网主机通过域名访问 Web 服务器，首先需要访问内部的 DNS 服务器获取 Web 服务器的 IP 地址，因此需要通过配置 NAT 内部服务器将 DNS 服务器的内网 IP 地址和 DNS 服务端口映射为一个外网地址和端口。
- DNS 服务器回应给外网主机的 DNS 报文载荷中携带了 Web 服务器的内网 IP 地址，该地址与外网主机地址重叠，因此在出方向上需要为内网 Web 服务器动态分配一个 NAT 地址，并将载荷中的地址转换为该地址。NAT 地址分配可以通过出方向动态地址转换功能实现，转换载荷信息可以通过 DNS ALG 功能实现。
- 外网主机得到内网 Web 服务器的 IP 地址之后（该地址为 NAT 地址），使用该地址访问内网 Web 服务器，因为外网主机的地址与内网 Web 服务器的真实地址重叠，因此在入方向上也需要为外网主机动态分配一个 NAT 地址，可以通过入方向动态地址转换实现。
- NAT 设备上没有目的地址为外网主机对应 NAT 地址的路由，因此需要手工添加静态路由，使得目的地址为外网主机 NAT 地址的报文的出接口为 GigabitEthernet1/0/2。

4. 配置步骤

配置接口 IP 地址、路由、安全域及域间策略保证网络可达，具体配置步骤略。

开启 DNS 协议的 ALG 功能。

```
<Device> system-view
[Device] nat alg dns
```

配置 ACL 2000，允许对内部网络中 192.168.1.0/24 网段的报文进行地址转换。

```
[Device] acl basic 2000
[Device-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Device-acl-ipv4-basic-2000] quit
```

创建地址组 1。

```
[Device] nat address-group 1
```

添加地址组成员 202.38.1.2。

```
[Device-address-group-1] address 202.38.1.2 202.38.1.2
```

```
[Device-address-group-1] quit
```

创建地址组 2。

```
[Device] nat address-group 2
```

添加地址组成员 202.38.1.3。

```
[Device-address-group-2] address 202.38.1.3 202.38.1.3
```

```
[Device-address-group-2] quit
```

在接口 GigabitEthernet1/0/2 上配置 NAT 内部服务器，允许外网主机使用地址 202.38.1.4 访问内网 DNS 服务器。

```
[Device] interface gigabitethernet 1/0/2
```

```
[Device-GigabitEthernet1/0/2] nat server protocol udp global 202.38.1.4 inside 192.168.1.3  
dns
```

在接口 GigabitEthernet1/0/2 上配置出方向动态地址转换，允许使用地址组 1 中的地址对 DNS 应答报文载荷中的内网地址进行转换，并在转换过程中不使用端口信息，以及允许反向地址转换。

```
[Device-GigabitEthernet1/0/2] nat outbound 2000 address-group 1 no-pat reversible
```

在接口 GigabitEthernet1/0/2 上配置入方向动态地址转换，允许使用地址组 2 中的地址对外网访问内网的报文进行源地址转换，并在转换过程中使用端口信息。

```
[Device-GigabitEthernet1/0/2] nat inbound 2000 address-group 2
```

```
[Device-GigabitEthernet1/0/2] quit
```

配置到达 202.38.1.3 地址的静态路由，出接口为 GigabitEthernet1/0/2，下一跳地址为 20.2.2.2（20.2.2.2 为本例中的直连下一跳地址，实际使用中请以具体组网情况为准）。

```
[Device] ip route-static 202.38.1.3 32 gigabitethernet 1/0/2 20.2.2.2
```

5. 验证配置

以上配置完成后，外网 Host 能够通过域名访问内网相同 IP 地址的 Web server。通过查看如下显示信息，可以验证以上配置成功。

```
[Device] display nat all
```

NAT address group information:

Totally 2 NAT address groups.

Address group ID: 1

Port range: 1-65535

Address information:

Start address	End address
202.38.1.2	202.38.1.2

Exclude address information:

Start address	End address
---	---

```

Address group ID: 2
  Port range: 1-65535
  Address information:
    Start address      End address
    202.38.1.3         202.38.1.3
  Exclude address information:
    Start address      End address
    ---               ---

NAT inbound information:
  Totally 1 NAT inbound rules.
  Interface: GigabitEthernet1/0/2
  ACL: 2000
  Address group ID: 2
  Add route: N        NO-PAT: N        Reversible: N
  Config status: Active

NAT outbound information:
  Totally 1 NAT outbound rules.
  Interface: GigabitEthernet1/0/2
  ACL: 2000
  Address group ID: 1
  Port-preserved: N   NO-PAT: Y        Reversible: Y
  Config status: Active

NAT internal server information:
  Totally 1 internal servers.
  Interface: GigabitEthernet1/0/2
  Protocol: 17(UDP)
  Global IP/port: 202.38.1.4/53
  Local IP/port : 200.1.1.3/53
  Rule name      : ServerRule_1
  NAT counting   : 0
  Config status  : Active

NAT logging:
  Log enable      : Disabled
  Flow-begin      : Disabled

```

Flow-end : Disabled
Flow-active : Disabled
Port-block-assign : Disabled
Port-block-withdraw : Disabled
Alarm : Disabled
NO-PAT IP usage : Disabled

NAT mapping behavior:

Mapping mode : Address and Port-Dependent
ACL : ---
Config status: Active

NAT ALG:

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

Static NAT load balancing: Disabled

NAT link-switch recreate-session: Disabled

NAT configuration-for-new-connection: Disabled

NAT global-policy compatible-previous-version rule-type ipv4-snat-and-dnat
translate-before-secp : Disabled

```
NAT gratuitous-arp: Enabled
```

通过以下显示命令，可以看到 Host 访问 Web server 时生成 NAT 会话信息。

```
[Device] display nat session verbose

Slot 1:

Initiator:

    Source      IP/port: 192.168.1.2/1694
    Destination IP/port: 202.38.1.2/8080
    DS-Lite tunnel peer: -
    VPN instance/VLAN ID/Inline ID: -/-/-
    Protocol: TCP(6)
    Inbound interface: GigabitEthernet1/0/2
    Source security zone: Untrust

Responder:

    Source      IP/port: 192.168.1.2/8080
    Destination IP/port: 202.38.1.3/1025
    DS-Lite tunnel peer: -
    VPN instance/VLAN ID/Inline ID: -/-/-
    Protocol: TCP(6)
    Inbound interface: GigabitEthernet1/0/1
    Source security zone: Trust

State: TCP_ESTABLISHED
Application: HTTP
Rule ID: -/-/-
Rule name:

Start time: 2017-06-15 14:53:29  TTL: 3597s

Initiator->Responder:          7 packets          308 bytes
Responder->Initiator:          5 packets          312 bytes

Total sessions found: 1
```

3.23.7 内网用户通过 NAT 地址访问内网服务器配置举例

1. 组网需求

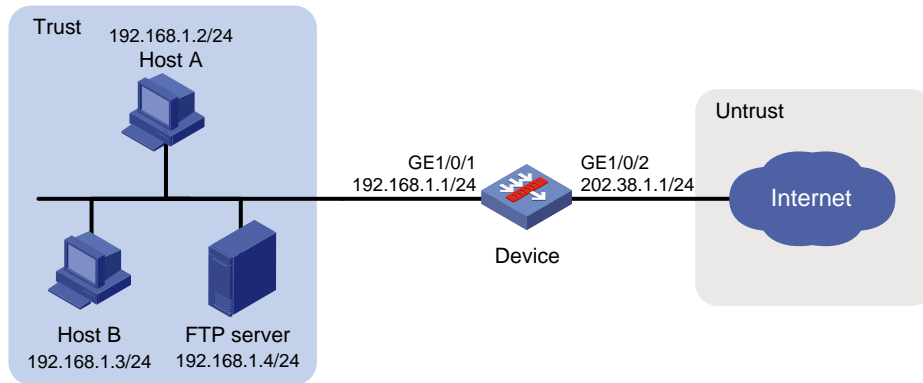
- 某公司内部网络中有一台 FTP 服务器，地址为 192.168.1.4/24。
- 该公司拥有两个外网 IP 地址：202.38.1.1 和 202.38.1.2。

需要实现如下功能：

- 外网主机可以通过 202.38.1.2 访问内网中的 FTP 服务器。
- 内网主机也可以通过 202.38.1.2 访问内网中的 FTP 服务器。

2. 组网图

图3-9 内网用户通过 NAT 地址访问内网服务器配置组网图



3. 配置思路

该需求为典型的 C-S 模式的 NAT hairpin 应用，具体配置思路如下。

- 为使外网主机可以通过外网地址访问内网 FTP 服务器，需要在外网侧接口配置 NAT 内部服务器。
- 为使内网主机通过外网地址访问内网 FTP 服务器，需要在内网侧接口开启 NAT hairpin 功能。其中，目的 IP 地址转换通过匹配外网侧接口上的内部服务器配置来完成，源地址转换通过匹配内部服务器配置所在接口上的出方向动态地址转换或出方向静态地址转换来完成，本例中采用出方向动态地址转换配置。

4. 配置步骤

配置接口 IP 地址、路由、安全域及域间策略保证网络可达，具体配置步骤略。

配置 ACL 2000，允许对内部网络中 192.168.1.0/24 网段的报文进行地址转换。

```
<Device> system-view
[Device] acl basic 2000
[Device-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Device-acl-ipv4-basic-2000] quit
```

在接口 GigabitEthernet1/0/2 上配置 NAT 内部服务器，允许外网主机使用地址 202.38.1.2 访问内网 FTP 服务器，同时使得内网主机访问内网 FTP 服务器的报文可以进行目的地址转换。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] nat server protocol tcp global 202.38.1.2 inside 192.168.1.4 ftp
```

在接口 GigabitEthernet1/0/2 上配置 Easy IP 方式的出方向动态地址转换，使得内网主机访问内网 FTP 服务器的报文可以使用接口 GigabitEthernet1/0/2 的 IP 地址进行源地址转换。

```
[Device-GigabitEthernet1/0/2] nat outbound 2000
[Device-GigabitEthernet1/0/2] quit
```

在接口 GigabitEthernet1/0/1 上开启 NAT hairpin 功能。

```
[Device] interface gigabitethernet 1/0/1
```

```
[Device-GigabitEthernet1/0/1] nat hairpin enable
[Device-GigabitEthernet1/0/1] quit
```

5. 验证配置

以上配置完成后，内网主机和外网主机均能够通过外网地址访问内网 FTP Server。通过查看如下显示信息，可以验证以上配置成功。

```
[Device] display nat all
NAT outbound information:

  Totally 1 NAT outbound rules.
  Interface: GigabitEthernet1/0/2
    ACL: 2000
    Address group ID: ---
    Port-preserved: N    NO-PAT: N    Reversible: N
    Config status: Active

NAT internal server information:

  Totally 1 internal servers.
  Interface: GigabitEthernet1/0/2
    Protocol: 6(TCP)
    Global IP/port: 202.38.1.2/21
    Local IP/port : 192.168.1.4/21
    Rule name      : ServerRule_1
    NAT counting   : 0
    Config status  : Active

NAT logging:

  Log enable           : Disabled
  Flow-begin           : Disabled
  Flow-end             : Disabled
  Flow-active          : Disabled
  Port-block-assign    : Disabled
  Port-block-withdraw  : Disabled
  Alarm                : Disabled
  NO-PAT IP usage      : Disabled

NAT hairpinning:

  Totally 1 interfaces enabled with NAT hairpinning.
  Interface: GigabitEthernet1/0/1
    Config status: Active
```


NAT mapping behavior:

Mapping mode : Address and Port-Dependent

ACL : ---

Config status: Active

NAT ALG:

DNS : Enabled

FTP : Enabled

H323 : Disabled

ICMP-ERROR : Enabled

ILS : Disabled

MGCP : Disabled

NBT : Disabled

PPTP : Enabled

RTSP : Enabled

RSH : Disabled

SCCP : Disabled

SCTP : Disabled

SIP : Disabled

SQLNET : Disabled

TFTP : Disabled

XDMCP : Disabled

Static NAT load balancing: Disabled

NAT link-switch recreate-session: Disabled

NAT configuration-for-new-connection: Disabled

NAT global-policy compatible-previous-version rule-type ipv4-snat-and-dnat
translate-before-secp : Disabled

NAT gratuitous-arp: Enabled

通过以下显示命令，可以看到 Host A 访问 FTP server 时生成 NAT 会话信息。

[Device] **display nat session verbose**

Slot 1:

Initiator:

```

Source      IP/port: 192.168.1.2/1694
Destination IP/port: 202.38.1.2/21
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/1
Source security zone: Trust
Responder:
Source      IP/port: 192.168.1.4/21
Destination IP/port: 202.38.1.1/1025
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/1
Source security zone: Trust
State: TCP_ESTABLISHED
Application: FTP
Rule ID: -/-/-
Rule name:
Start time: 2017-06-15 14:53:29  TTL: 3597s
Initiator->Responder:          7 packets          308 bytes
Responder->Initiator:          5 packets          312 bytes

Total sessions found: 1

```

3.23.8 内网用户通过 NAT 地址互访配置举例

1. 组网需求

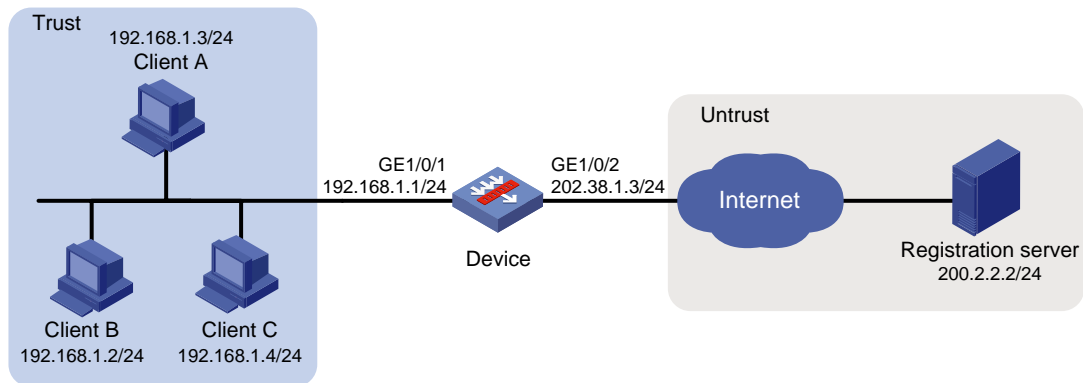
某 P2P 应用环境中，内网中的客户端首先需要向外网服务器进行注册，外网服务器会记录客户端的 IP 地址和端口号。如果内网的一个客户端要访问内网的另一个客户端，首先需要向服务器获取对方的 IP 地址和端口号。

需要实现如下功能：

- 内网客户端可以向外网中的服务器注册，且注册为一个相同的外网地址。
- 内网客户端能够通过从服务器获得的 IP 地址和端口进行互访。

2. 组网图

图3-10 内网用户通过 NAT 地址互访配置组网图



3. 配置思路

该需求为典型的 P2P 模式的 NAT hairpin 应用，具体配置思路如下。

- 内网中的客户端需要向外网中的服务器注册，因此需要进行源地址转换，可以通过在外网侧接口配置出方向动态地址转换实现。
- 服务器记录客户端的 IP 地址和端口号，且该地址和端口号是 NAT 转换后的。由于服务器记录的客户端 IP 地址和端口号需要供任意源地址访问，因此客户端地址的转换关系必须不关心对端地址，这可以通过配置 EIM 模式的动态地址转换实现。
- 内部主机通过外网地址进行互访，需要在内网侧接口开启 NAT hairpin 功能。

4. 配置步骤

配置接口 IP 地址、路由、安全域及域间策略保证网络可达，具体配置步骤略。

配置 ACL 2000，允许对内部网络中 192.168.1.0/24 网段的报文进行地址转换。

```
<Device> system-view
[Device] acl basic 2000
[Device-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Device-acl-ipv4-basic-2000] quit
```

在外网侧接口 GigabitEthernet1/0/2 上配置 Easy IP 方式的出方向动态地址转换，允许使用接口 GigabitEthernet1/0/2 的 IP 地址对内网访问外网的报文进行源地址转换，因为多个内部主机共用一个外网地址，因此需要配置为 PAT 方式，即转换过程中使用端口信息。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] nat outbound 2000
[Device-GigabitEthernet1/0/2] quit
```

配置 PAT 方式下的地址转换模式为 EIM，即只要是来自相同源地址和源端口号的且匹配 ACL 2000 的报文，不论其目的地址是否相同，通过 PAT 转换后，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。

```
[Device] nat mapping-behavior endpoint-independent acl 2000
```

在内网侧接口 GigabitEthernet1/0/1 上开启 NAT hairpin 功能。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] nat hairpin enable
[Device-GigabitEthernet1/0/1] quit
```

5. 验证配置

以上配置完成后，Host A、Host B 和 Host C 分别向外网服务器注册之后，它们之间可以相互访问。通过查看如下显示信息，可以验证以上配置成功。

```
[Device] display nat all
NAT outbound information:

  Totally 1 NAT outbound rules.
  Interface: GigabitEthernet1/0/2
  ACL: 2000
  Address group ID: ---
  Port-preserved: N      NO-PAT: N      Reversible: N
  Config status: Active

NAT logging:

  Log enable           : Disabled
  Flow-begin           : Disabled
  Flow-end             : Disabled
  Flow-active          : Disabled
  Port-block-assign    : Disabled
  Port-block-withdraw  : Disabled
  Alarm                : Disabled
  NO-PAT IP usage      : Disabled

NAT hairpinning:

  Totally 1 interfaces enabled with NAT hairpinning.
  Interface: GigabitEthernet1/0/1
  Config status: Active

NAT mapping behavior:

  Mapping mode : Endpoint-Independent
  ACL          : 2000
  Config status: Active

NAT ALG:

  DNS      : Enabled
  FTP      : Enabled
```

```
H323      : Disabled
ICMP-ERROR : Enabled
ILS       : Disabled
MGCP      : Disabled
NBT       : Disabled
PPTP      : Enabled
RTSP      : Enabled
RSH       : Disabled
SCCP      : Disabled
SCTP      : Disabled
SIP       : Disabled
SQLNET    : Disabled
TFTP      : Disabled
XDMCP     : Disabled
```

```
Static NAT load balancing:      Disabled
```

```
NAT link-switch recreate-session: Disabled
```

```
NAT configuration-for-new-connection: Disabled
```

```
NAT global-policy compatible-previous-version rule-type ipv4-snat-and-dnat
translate-before-secp : Disabled
```

```
NAT gratuitous-arp: Enabled
```

通过以下显示命令，可以看到 Client A 访问 Client B 时生成 NAT 会话信息。

```
[Device] display nat session verbose
```

```
Slot 1:
```

```
Initiator:
```

```
Source      IP/port: 192.168.1.3/44929
```

```
Destination IP/port: 202.38.1.3/1
```

```
DS-Lite tunnel peer: -
```

```
VPN instance/VLAN ID/Inline ID: -/-/-
```

```
Protocol: UDP(17)
```

```
Inbound interface: GigabitEthernet1/0/1
```

```
Source security zone: Trust
```

```
Responder:
```

```
Source      IP/port: 192.168.1.2/69
```

```

Destination IP/port: 202.38.1.3/1024
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: UDP(17)
Inbound interface: GigabitEthernet1/0/1
Source security zone: Trust
State: UDP_READY
Application: TFTP
Rule ID: -/-/-
Rule name:
Start time: 2012-08-15 15:53:36  TTL: 46s
Initiator->Responder:          1 packets          56 bytes
Responder->Initiator:          1 packets          72 bytes

Total sessions found: 1

```

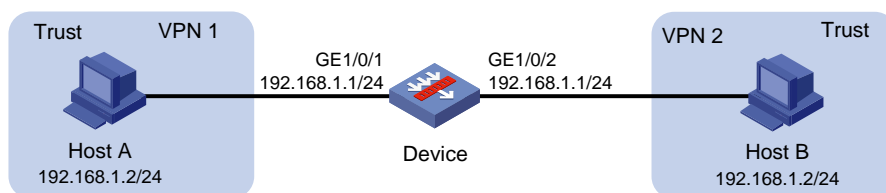
3.23.9 地址重叠的两个 VPN 之间互访配置举例

1. 组网需求

某公司两个部门由于需要业务隔离而分属不同的 VPN 实例，且两个部门内部使用了相同的子网地址空间。现在要求这两个部门的主机 Host A 和 Host B 之间能够通过 NAT 地址互相访问。

2. 组网图

图3-11 地址重叠的两个 VPN 之间互访配置组网图



3. 配置思路

这是一个典型的两次 NAT 应用：两个 VPN 之间主机交互的报文的源 IP 地址和目的 IP 地址都需要转换，即需要在连接两个 VPN 的接口上先后进行两次 NAT，这可以通过在 NAT 设备的两侧接口上分别配置静态地址转换实现。

为实现 VPN 之间互访，配置域间策略时，需要配置允许 VPN 实例报文通过，放行 VPN 实例间的流量。

4. 配置步骤

配置接口 IP 地址、路由、安全域及域间策略，在域间策略中配置允许 VPN 实例报文通过，以保证网络可达，具体配置步骤略。

配置 VPN 1 内的 IP 地址 192.168.1.2 到 VPN 2 内的 IP 地址 172.16.1.2 之间的静态地址转换映射。

```
<Device> system-view
```

```
[Device] nat static outbound 192.168.1.2 vpn-instance vpn1 172.16.1.2 vpn-instance vpn2
```

配置VPN 2内的IP地址192.168.1.2到VPN 1内的IP地址172.16.2.2之间的静态地址转换映射。

```
[Device] nat static outbound 192.168.1.2 vpn-instance vpn2 172.16.2.2 vpn-instance vpn1
```

在接口 GigabitEthernet1/0/2 上配置静态地址转换。

```
[Device] interface gigabitethernet 1/0/2
```

```
[Device-GigabitEthernet1/0/2] nat static enable
```

```
[Device-GigabitEthernet1/0/2] quit
```

在接口 GigabitEthernet1/0/1 上配置静态地址转换。

```
[Device] interface gigabitethernet 1/0/1
```

```
[Device-GigabitEthernet1/0/1] nat static enable
```

```
[Device-GigabitEthernet1/0/1] quit
```

5. 验证配置

以上配置完成后，Host A 和 Host B 可以互通，且 Host A 的对外地址为 172.16.1.2，Host B 的对外地址为 172.16.2.2。通过查看如下显示信息，可以验证以上配置成功。

```
[Device] display nat all
```

Static NAT mappings:

Totally 2 outbound static NAT mappings.

IP-to-IP:

Local IP : 192.168.1.2

Global IP : 172.16.1.2

Local VPN : vpn1

Global VPN : vpn2

Config status: Active

IP-to-IP:

Local IP : 192.168.1.2

Global IP : 172.16.2.2

Local VPN : vpn2

Global VPN : vpn1

Config status: Active

Interfaces enabled with static NAT:

Totally 2 interfaces enabled with static NAT.

Interface: GigabitEthernet1/0/1

Config status: Active

Interface: GigabitEthernet1/0/2

Config status: Active

NAT logging:

Log enable : Disabled
Flow-begin : Disabled
Flow-end : Disabled
Flow-active : Disabled
Port-block-assign : Disabled
Port-block-withdraw : Disabled
Alarm : Disabled
NO-PAT IP usage : Disabled

NAT mapping behavior:

Mapping mode : Address and Port-Dependent
ACL : ---
Config status: Active

NAT ALG:

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

Static NAT load balancing: Disabled

NAT link-switch recreate-session: Disabled


```
NAT configuration-for-new-connection: Disabled
```

```
NAT global-policy compatible-previous-version rule-type ipv4-snat-and-dnat  
translate-before-secp : Disabled
```

```
NAT gratuitous-arp: Enabled
```

通过以下显示命令，可以看到 Host A 访问 Host B 时生成 NAT 会话信息。

```
[Device] display nat session verbose
```

```
Slot 1:
```

```
Initiator:
```

```
Source      IP/port: 192.168.1.2/42496  
Destination IP/port: 172.16.2.2/2048  
DS-Lite tunnel peer: -  
VPN instance/VLAN ID/Inline ID: vpn1/-/-  
Protocol: ICMP(1)  
Inbound interface: GigabitEthernet1/0/1  
Source security zone: Trust
```

```
Responder:
```

```
Source      IP/port: 192.168.1.2/42496  
Destination IP/port: 172.16.1.2/0  
DS-Lite tunnel peer: -  
VPN instance/VLAN ID/Inline ID: vpn2/-/-  
Protocol: ICMP(1)  
Inbound interface: GigabitEthernet1/0/2  
Source security zone: Trust
```

```
State: ICMP_REPLY
```

```
Application: INVALID
```

```
Rule ID: -/-/-
```

```
Rule name:
```

```
Start time: 2012-08-16 09:30:49  TTL: 27s
```

```
Initiator->Responder:          5 packets          420 bytes
```

```
Responder->Initiator:          5 packets          420 bytes
```

```
Total sessions found: 1
```

3.23.10 负载分担内部服务器配置举例

1. 组网需求

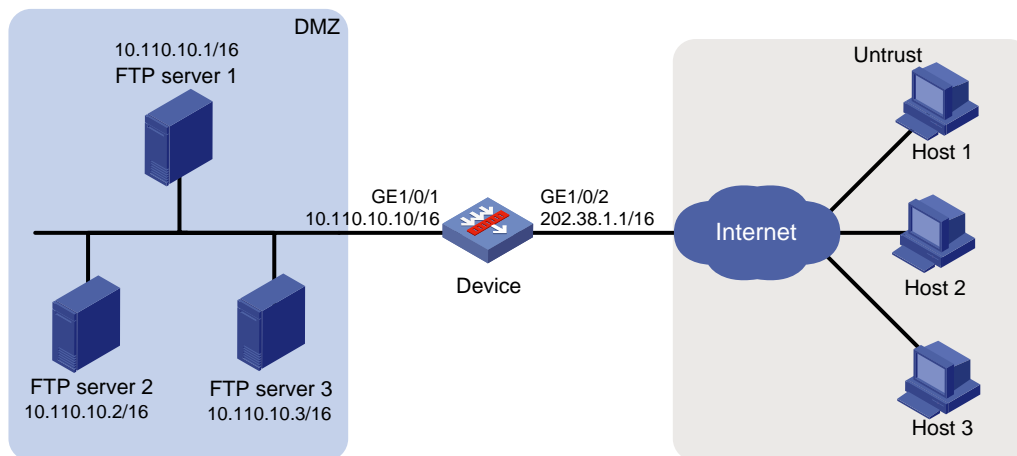
某公司内部拥有 3 台 FTP 服务器对外提供 FTP 服务。

需要实现如下功能：

- 使用 IP 地址为 202.38.1.1 作为公司对外提供服务的 IP 地址。
- 3 台 FTP 服务器可以同时对外提供服务，并进行负载分担。

2. 组网图

图3-12 负载分担内部服务器配置组网图



3. 配置步骤

配置接口 IP 地址、路由、安全域及域间策略保证网络可达，具体配置步骤略。

配置内部服务器组 0 及其成员 10.110.10.1、10.110.10.2 和 10.110.10.3。

```
<Device> system-view
[Device] nat server-group 0
[Device-nat-server-group-0] inside ip 10.110.10.1 port 21
[Device-nat-server-group-0] inside ip 10.110.10.2 port 21
[Device-nat-server-group-0] inside ip 10.110.10.3 port 21
[Device-nat-server-group-0] quit
```

在接口 GigabitEthernet1/0/2 上配置负载分担内部服务器，引用内部服务器组 0，该组内的主机共同对外提供 FTP 服务。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] nat server protocol tcp global 202.38.1.1 ftp inside
server-group 0
[Device-GigabitEthernet1/0/2] quit
```

4. 验证配置

以上配置完成后，外网主机可以访问内网 FTP 服务器组。通过查看如下显示信息，可以验证以上配置成功。

[Device] **display nat all**

NAT server group information:

Totally 1 NAT server groups.

Group Number	Inside IP	Port	Weight
0	10.110.10.1	21	100
	10.110.10.2	21	100
	10.110.10.3	21	100

NAT internal server information:

Totally 1 internal servers.

Interface: GigabitEthernet1/0/2

Protocol: 6(TCP)

Global IP/port: 202.38.1.1/21

Local IP/port : server group 0

10.110.10.1/21 (Connections: 1)

10.110.10.2/21 (Connections: 1)

10.110.10.3/21 (Connections: 1)

Rule name : ServerRule_1

NAT counting : 0

Config status : Active

NAT logging:

Log enable : Disabled

Flow-begin : Disabled

Flow-end : Disabled

Flow-active : Disabled

Port-block-assign : Disabled

Port-block-withdraw : Disabled

Alarm : Disabled

NO-PAT IP usage : Disabled

NAT mapping behavior:

Mapping mode : Address and Port-Dependent

ACL : ---

Config status: Active

NAT ALG:

DNS : Enabled

```
FTP          : Enabled
H323         : Disabled
ICMP-ERROR   : Enabled
ILS          : Disabled
MGCP         : Disabled
NBT          : Disabled
PPTP        : Enabled
RTSP         : Enabled
RSH          : Disabled
SCCP         : Disabled
SCTP         : Disabled
SIP          : Disabled
SQLNET       : Disabled
TFTP         : Disabled
XDMCP        : Disabled
```

```
Static NAT load balancing:      Disabled
```

```
NAT link-switch recreate-session: Disabled
```

```
NAT configuration-for-new-connection: Disabled
```

```
NAT global-policy compatible-previous-version rule-type ipv4-snat-and-dnat
translate-before-secp : Disabled
```

```
NAT gratuitous-arp: Enabled
```

通过以下显示命令，可以看到外网主机访问内网 FTP server 时生成 NAT 会话信息。

```
[Device] display nat session verbose
```

```
Slot 1:
```

```
Initiator:
```

```
Source      IP/port: 202.38.1.27/5760
Destination IP/port: 202.38.1.1/21
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/2
Source security zone: Untrust
```

```
Responder:
```

```

Source      IP/port: 10.110.10.3/21
Destination IP/port: 202.38.1.27/5760
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/1
Source security zone: DMZ
State: TCP_ESTABLISHED
Application: FTP
Rule ID: -/-/-
Rule name:
Start time: 2017-05-19 16:10:27  TTL: 3598s
Initiator->Responder:          15 packets      702 bytes
Responder->Initiator:          16 packets      891 bytes

Initiator:
Source      IP/port: 202.38.1.26/30018
Destination IP/port: 202.38.1.1/21
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/2
Source security zone: Untrust
Responder:
Source      IP/port: 10.110.10.2/21
Destination IP/port: 202.38.1.26/30018
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/1
Source security zone: DMZ
State: TCP_ESTABLISHED
Application: FTP
Start time: 2017-05-19 16:09:58  TTL: 3576s
Initiator->Responder:          15 packets      702 bytes
Responder->Initiator:          16 packets      891 bytes

Initiator:

```

```

Source      IP/port: 202.38.1.25/35652
Destination IP/port: 202.38.1.1/21
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/2
Source security zone: Untrust
Responder:
Source      IP/port: 10.110.10.1/21
Destination IP/port: 202.38.1.25/35652
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/1
Source security zone: DMZ
State: TCP_ESTABLISHED
Application: FTP
Start time: 2017-05-19 16:09:46  TTL: 3579s
Initiator->Responder:          15 packets      702 bytes
Responder->Initiator:          16 packets      891 bytes

Total sessions found: 3

```

3.23.11 NAT DNS mapping 配置举例

1. 组网需求

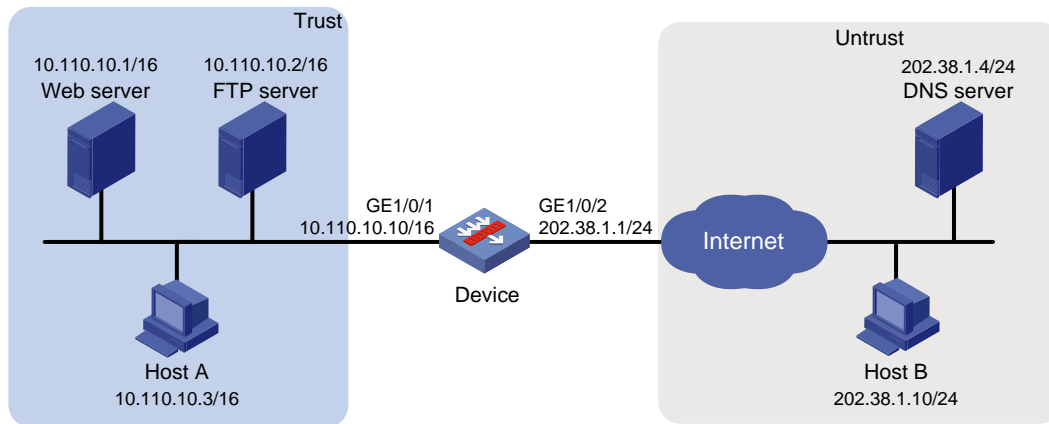
某公司内部对外提供 Web 和 FTP 服务。公司内部网址为 10.110.0.0/16。其中，Web 服务器地址为 10.110.10.1/16，FTP 服务器地址为 10.110.10.2/16。公司具有 202.38.1.1 至 202.38.1.3 三个公网 IP 地址。另外公司在外网有一台 DNS 服务器，IP 地址为 202.38.1.4。

需要实现如下功能：

- 选用 202.38.1.2 作为公司对外提供服务的 IP 地址。
- 外网用户可以通过域名或 IP 地址访问内部服务器。
- 内网用户可以通过域名访问内部服务器。

2. 组网图

图3-13 NAT DNS mapping 配置组网图



3. 配置思路

- 内网服务器对外提供服务，需要配置 NAT 内部服务器将各服务器的内网 IP 地址和端口映射为一个外网地址和端口。
- 内网主机通过域名访问内网服务器时，首先需要通过出接口地址转换分配的外网地址访问外网的 DNS 服务器，并获取内网服务器的内网 IP 地址。由于 DNS 服务器向内网主机发送的响应报文中包含的是内网服务器的外网地址，因此 NAT 设备需要将 DNS 报文载荷内的外网地址转换为内网地址，这可以通过查找 DNS mapping 映射表配合 DNS ALG 功能实现。DNS mapping 映射表用于实现根据“域名+外网 IP 地址+外网端口号+协议类型”查找到对应的“内网 IP+内网端口号”。

4. 配置步骤

配置接口 IP 地址、路由、安全域及域间策略保证网络可达，具体配置步骤略。

开启 DNS 的 NAT ALG 功能。

```
<Device> system-view
```

```
[Device] nat alg dns
```

进入接口 GigabitEthernet1/0/2。

```
[Device] interface gigabitethernet 1/0/2
```

配置 NAT 内部 Web 服务器，允许外网主机使用地址 202.38.1.2 访问内网 Web 服务器。

```
[Device-GigabitEthernet1/0/2] nat server protocol tcp global 202.38.1.2 inside 10.110.10.1 http
```

配置 NAT 内部 FTP 服务器，允许外网主机使用地址 202.38.1.2 访问内网 FTP 服务器。

```
[Device-GigabitEthernet1/0/2] nat server protocol tcp global 202.38.1.2 inside 10.110.10.2 ftp
```

在接口 GigabitEthernet1/0/2 上配置 Easy IP 方式的出方向动态地址转换。

```
[Device-GigabitEthernet1/0/2] nat outbound
```

```
[Device-GigabitEthernet1/0/2] quit
```

配置两条 DNS mapping 表项：Web 服务器的域名 `www.example.com` 对应 IP 地址 `202.38.1.2`；FTP 服务器的域名 `ftp.example.com` 对应 IP 地址 `202.38.1.2`。

```
[Device] nat dns-map domain www.example.com protocol tcp ip 202.38.1.2 port https
[Device] nat dns-map domain ftp.example.com protocol tcp ip 202.38.1.2 port ftp
```

5. 验证配置

以上配置完成后，内网主机和外网主机均可以通过域名访问内网服务器。通过查看如下显示信息，可以验证以上配置成功。

```
[Device] display nat all
NAT outbound information:

Totally 1 NAT outbound rules.
Interface: GigabitEthernet1/0/2
ACL: ---
Address group ID: ---
Port-preserved: N      NO-PAT: N      Reversible: N
Config status: Active

NAT internal server information:

Totally 2 internal servers.
Interface: GigabitEthernet1/0/2
Protocol: 6(TCP)
Global IP/port: 202.38.1.2/21
Local IP/port : 10.110.10.2/21
Rule name      : ServerRule_2
NAT counting   : 0
Config status  : Active

Interface: GigabitEthernet1/0/2
Protocol: 6(TCP)
Global IP/port: 202.38.1.2/80
Local IP/port : 10.110.10.1/80
Rule name      : ServerRule_1
NAT counting   : 0
Config status  : Active

NAT DNS mapping information:

Totally 2 NAT DNS mappings.
Domain name: ftp.example.com
Global IP   : 202.38.1.2
```


Global port: 21

Protocol : TCP(6)

Config status: Active

Domain name: www.example.com

Global IP : 202.38.1.2

Global port: 443

Protocol : TCP(6)

Config status: Active

NAT logging:

Log enable : Disabled
Flow-begin : Disabled
Flow-end : Disabled
Flow-active : Disabled
Port-block-assign : Disabled
Port-block-withdraw : Disabled
Alarm : Disabled
NO-PAT IP usage : Disabled

NAT mapping behavior:

Mapping mode : Address and Port-Dependent
ACL : ---

Config status: Active

NAT ALG:

DNS : Enabled
FTP : Enabled
H323 : Disabled
ICMP-ERROR : Enabled
ILS : Disabled
MGCP : Disabled
NBT : Disabled
PPTP : Enabled
RTSP : Enabled
RSH : Disabled
SCCP : Disabled
SCTP : Disabled

```
SIP          : Disabled
SQLNET       : Disabled
TFTP        : Disabled
XDMCP       : Disabled

Static NAT load balancing:      Disabled

NAT link-switch recreate-session: Disabled

NAT configuration-for-new-connection: Disabled

NAT global-policy compatible-previous-version rule-type ipv4-snat-and-dnat
translate-before-secp : Disabled

NAT gratuitous-arp: Enabled
```

通过以下显示命令，可以看到外网主机访问内网 Web Server 时生成 NAT 会话信息。

```
[Device] display nat session verbose

Slot 1:

Initiator:

  Source      IP/port: 202.38.1.10/63593
  Destination IP/port: 202.38.1.2/80
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Untrust

Responder:

  Source      IP/port: 10.110.10.1/80
  Destination IP/port: 202.38.1.10/63593
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Trust

State: TCP_ESTABLISHED
Application: HTTP
Rule ID: -/-/-
Rule name:
```

```

Start time: 2017-05-21 15:09:11  TTL: 11s
Initiator->Responder:                5 packets      1145 bytes
Responder->Initiator:                3 packets      1664 bytes

Total sessions found: 1

```

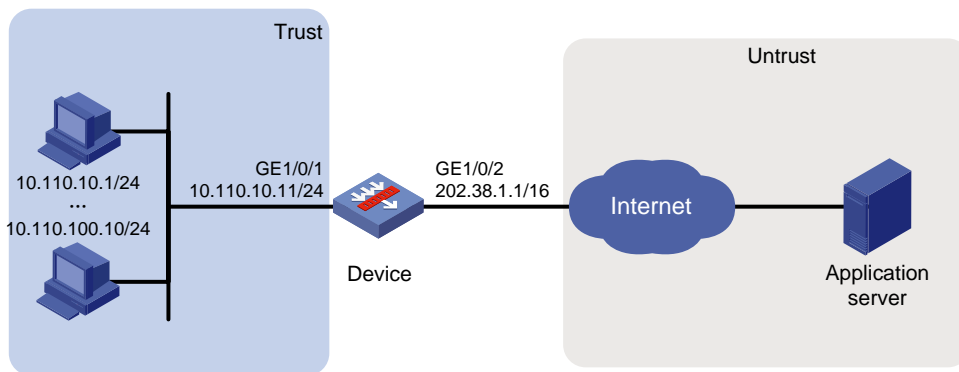
3.23.12 NAT444 端口块静态映射配置举例

1. 组网需求

内部网络用户 10.110.10.1~10.110.10.10 使用外网地址 202.38.1.100 访问 Internet。内网用户地址基于 NAT444 端口块静态映射方式复用外网地址 202.38.1.100，外网地址的端口范围为 10001~15000，端口块大小为 500。

2. 组网图

图3-14 NAT444 端口块静态映射配置组网图



3. 配置步骤

配置接口 IP 地址、路由、安全域及域间策略保证网络可达，具体配置步骤略。

创建 NAT 端口块组 1。

```

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

```

添加私网地址成员 10.110.10.1~10.110.10.10。

```

[Device-port-block-group-1] local-ip-address 10.110.10.1 10.110.10.10

```

添加公网地址成员为 202.38.1.100。

```

[Device-port-block-group-1] global-ip-pool 202.38.1.100 202.38.1.100

```

配置端口块大小为 500，公网地址的端口范围为 10001~15000。

```

[Device-port-block-group-1] block-size 500
[Device-port-block-group-1] port-range 10001 15000
[Device-port-block-group-1] quit

```

在接口 GigabitEthernet1/0/2 上配置 NAT444 端口块静态映射，引用端口块组 1。

```

[Device] interface gigabitethernet 1/0/2

```

```
[Device-GigabitEthernet1/0/2] nat outbound port-block-group 1
[Device-GigabitEthernet1/0/2] quit
```

4. 验证配置

以上配置完成后，内网主机可以访问外网服务器。通过查看如下显示信息，可以验证以上配置成功。

```
[Device] display nat all
NAT logging:
  Log enable           : Disabled
  Flow-begin           : Disabled
  Flow-end             : Disabled
  Flow-active          : Disabled
  Port-block-assign    : Disabled
  Port-block-withdraw  : Disabled
  Alarm                : Disabled
  NO-PAT IP usage      : Disabled

NAT mapping behavior:
  Mapping mode : Address and Port-Dependent
  ACL          : ---
  Config status: Active

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

NAT port block group information:

Totally 1 NAT port block groups.

Port block group 1:

Port range: 10001-15000

Block size: 500

Local IP address information:

Start address	End address	VPN instance
10.110.10.1	10.110.10.10	---

Global IP pool information:

Start address	End address
202.38.1.100	202.38.1.100

NAT outbound port block group information:

Totally 1 outbound port block group items.

Interface: GigabitEthernet1/0/2

port-block-group: 1

Config status : Active

Static NAT load balancing: Disabled

NAT link-switch recreate-session: Disabled

NAT configuration-for-new-connection: Disabled

NAT global-policy compatible-previous-version rule-type ipv4-snat-and-dnat
translate-before-secp : Disabled

NAT gratuitous-arp: Enabled

通过以下显示命令，可以看到系统生成的静态端口块表项信息。

[Device] **display nat port-block static**

Slot 1:

Local VPN	Local IP	Global IP	Port block	Connections	BackUp
---	10.110.10.7	202.38.1.100	13001-13500	1	No
---	10.110.10.5	202.38.1.100	12001-12500	1	No
---	10.110.10.9	202.38.1.100	14001-14500	1	No
---	10.110.10.3	202.38.1.100	11001-11500	1	No
---	10.110.10.2	202.38.1.100	10501-11000	1	No

---	10.110.10.4	202.38.1.100	11501-12000	1	No
---	10.110.10.6	202.38.1.100	12501-13000	1	No
---	10.110.10.1	202.38.1.100	10001-10500	1	No
---	10.110.10.10	202.38.1.100	14501-15000	1	No
---	10.110.10.8	202.38.1.100	13501-14000	1	No
Total mappings found: 10					

3.23.13 NAT444 端口块动态映射配置举例

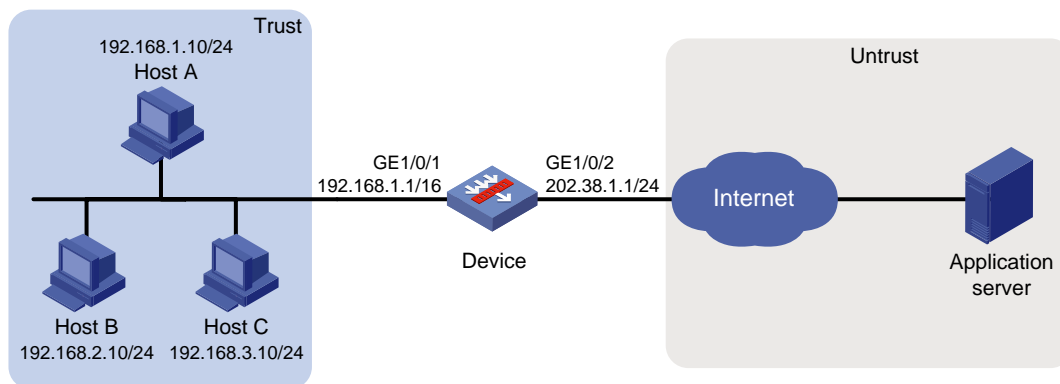
1. 组网需求

- 某公司内网使用的 IP 地址为 192.168.0.0/16。
- 该公司拥有 202.38.1.2 和 202.38.1.3 两个外网 IP 地址。

要实现，内部网络中的 192.168.1.0/24 网段的用户可以访问 Internet，其它网段的用户不能访问 Internet。基于 NAT444 端口块动态映射方式复用两个外网地址 202.38.1.2 和 202.38.1.3，外网地址的端口范围为 1024~65535，端口块大小为 300。当为某用户分配的端口块资源耗尽时，再为其增量分配 1 个端口块。

2. 组网图

图3-15 NAT444 端口块动态映射配置组网图



3. 配置步骤

配置接口 IP 地址、路由、安全域及域间策略保证网络可达，具体配置步骤略。

配置地址组 0，包含两个外网地址 202.38.1.2 和 202.38.1.3，外网地址的端口范围为 1024~65535，端口块大小为 300，增量端口块数为 1。

```
<Device> system-view
[Device] nat address-group 0
[Device-address-group-0] address 202.38.1.2 202.38.1.3
[Device-address-group-0] port-range 1024 65535
[Device-address-group-0] port-block block-size 300 extended-block-number 1
[Device-address-group-0] quit
```

配置 ACL 2000，仅允许对内部网络中 192.168.1.0/24 网段的用户报文进行地址转换。

```
[Device] acl basic 2000
[Device-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Device-acl-ipv4-basic-2000] quit
```

在接口 GigabitEthernet1/0/2 上配置出方向动态地址转换, 允许使用地址组 0 中的地址对匹配 ACL 2000 的报文进行源地址转换, 并在转换过程中使用端口信息。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] nat outbound 2000 address-group 0
[Device-GigabitEthernet1/0/2] quit
```

4. 验证配置

以上配置完成后, Host A 能够访问外网服务器, Host B 和 Host C 无法访问外网服务器。通过查看如下显示信息, 可以验证以上配置成功。

```
[Device] display nat all
NAT address group information:
  Totally 1 NAT address groups.
  Address group ID: 0
    Port range: 1024-65535
    Port block size: 300
    Extended block number: 1
  Address information:
    Start address      End address
    202.38.1.2         202.38.1.3
  Exclude address information:
    Start address      End address
    ---               ---

NAT outbound information:
  Totally 1 NAT outbound rules.
  Interface: GigabitEthernet1/0/2
    ACL: 2000
    Address group ID: 0
    Port-preserved: N   NO-PAT: N   Reversible: N
    Config status: Active

NAT logging:
  Log enable           : Disabled
  Flow-begin           : Disabled
  Flow-end             : Disabled
  Flow-active          : Disabled
```

```

Port-block-assign      : Disabled
Port-block-withdraw    : Disabled
Alarm                  : Disabled
NO-PAT IP usage        : Disabled

NAT mapping behavior:

Mapping mode : Address and Port-Dependent
ACL          : ---
Config status: Active

NAT ALG:

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

Static NAT load balancing:      Disabled

NAT link-switch recreate-session: Disabled

NAT configuration-for-new-connection: Disabled

NAT global-policy compatible-previous-version rule-type ipv4-snat-and-dnat
translate-before-secp : Disabled

NAT gratuitous-arp: Enabled

```


通过以下显示命令，可以看到 NAT 会话数、当前可分配的动态端口块总数和已分配的动态端口块个数。

```
[Device] display nat statistics

Total session entries: 1
Session creation rate: 0
Total EIM entries: 0
Total inbound NO-PAT entries: 0
Total outbound NO-PAT entries: 0
Total static port block entries: 0
Total dynamic port block entries: 430
Active static port block entries: 0
Active dynamic port block entries: 1
```

通过以下显示命令，可以看到生成的动态端口块表项信息。

```
[Device] display nat port-block dynamic

Slot 1:

Local VPN  Local IP          Global IP          Port block  Connections  BackUp
---          192.168.1.10      202.38.1.2        65224-65523  1            No
Total mappings found: 1
```

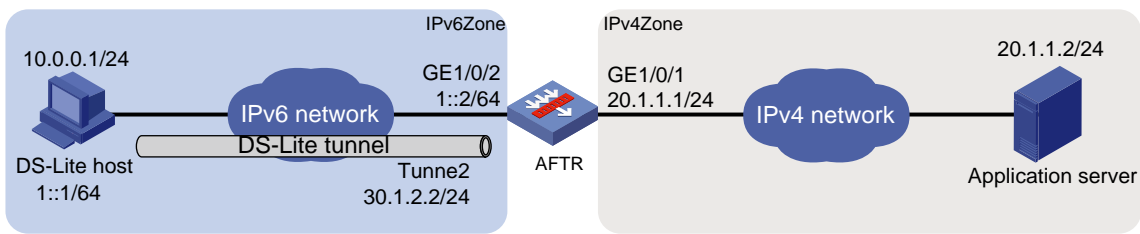
3.23.14 DS-Lite B4 端口块动态映射配置举例

1. 组网需求

支持 DS-Lite 协议的私网 IPv4 主机（即：DS-Lite host）和公网 IPv4 network 通过 IPv6 网络相连。通过在 DS-Lite host 和 AFTR 之间建立 DS-Lite 隧道，并在 AFTR 连接 IPv4 network 接口上配置 NAT，为 DS-Lite host 动态分配端口块，实现 IPv4 私网穿越 IPv6 网络访问 IPv4 公网。

2. 组网图

图3-16 DS-Lite 隧道配置组网图



3. 配置注意事项

需要将创建的 DS-Lite 隧道接口加入到安全域，并放行域间流量。（本例即将 Tunnel 2 加入安全域 IPv6Zone，同时放行 IPv6Zone 域到 IPv4Zone 域间的相关流量。）

4. 配置步骤

(1) 配置 AFTR 端

创建安全域 IPv6Zone 和 IPv4Zone，按照组网图将接口分别加入到对应的安全域中，配置域间策略保证网络可达，具体配置步骤略。

配置接口 GigabitEthernet1/0/1 的地址。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 20.1.1.1 24
[Device-GigabitEthernet1/0/1] quit
```

配置接口 GigabitEthernet1/0/2（隧道的实际物理接口）的地址。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] ipv6 address 1::2 64
[Device-GigabitEthernet1/0/2] quit
```

创建模式为 AFTR 端 DS-Lite 隧道的接口 Tunnel2。

```
[Device] interface tunnel 2 mode ds-lite-aftr
```

配置 Tunnel2 接口的 IP 地址。

```
[Device-Tunnel2] ip address 30.1.2.2 255.255.255.0
```

配置 Tunnel2 接口的源接口为 GigabitEthernet1/0/2。

```
[Device-Tunnel2] source gigabitethernet 1/0/2
[Device-Tunnel2] quit
```

将 Tunnel2 接口加入到安全域 IPv6Zone。

```
[Device] security-zone name IPv6Zone
[Device-security-zone-IPv6Zone] import interface Tunnel 2
[Device-security-zone-IPv6Zone] quit
```

在接口 GigabitEthernet1/0/1 上开启 DS-Lite 隧道功能。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ds-lite enable
[Device-GigabitEthernet1/0/1] quit
```

配置 NAT 地址组 0，包含两个外网地址 20.1.1.11 和 20.1.1.12，外网地址的端口范围为 1024～65535，端口块大小为 300。

```
[Device] nat address-group 0
[Device-address-group-0] address 20.1.1.11 20.1.1.12
[Device-address-group-0] port-range 1024 65535
[Device-address-group-0] port-block block-size 300
[Device-address-group-0] quit
```

配置 IPv6 ACL 2100，仅允许对 1::/64 网段的 IPv6 源地址进行地址转换。

```
[Device] acl ipv6 basic 2100
[Device-acl-ipv6-basic-2100] rule permit source 1::/64
[Device-acl-ipv6-basic-2100] quit
```

在接口 GigabitEthernet1/0/1 上配置出方向动态地址转换,允许使用地址组 0 中的地址对匹配 IPv6 ACL 2100 的 DS-Lite B4 报文进行源地址转换,并在转换过程中使用端口信息。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] nat outbound ds-lite-b4 2100 address-group 0
[Device-GigabitEthernet1/0/1] quit
```

(2) 配置 DS-Lite host

配置 DS-Lite host 的 IPv4 地址为 10.0.0.1, IPv6 地址为 1::1/64, 并配置 DS-Lite tunnel 路由。(具体配置过程略)

5. 验证配置

完成上述配置后,在 AFTR 上执行 **display interface tunnel** 命令,可以看出 Tunnel 接口处于 up 状态。(具体显示信息略)

从 DS-Lite host 上可以 ping 通 IPv4 Application server。

```
C:\> ping 20.1.1.2

Pinging 20.1.1.2 with 32 bytes of data:
Reply from 20.1.1.2: bytes=32 time=51ms TTL=255
Reply from 20.1.1.2: bytes=32 time=44ms TTL=255
Reply from 20.1.1.2: bytes=32 time=1ms TTL=255
Reply from 20.1.1.2: bytes=32 time=1ms TTL=255

Ping statistics for 20.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 51ms, Average = 24ms
```

通过以下显示命令,可以看到出方向动态地址转换的配置信息。

```
[Device] display nat outbound

NAT outbound information:

  Totally 1 NAT outbound rules.

  Interface: GigabitEthernet1/0/1

    DS-Lite B4 ACL: 2100

    Address group ID: 0

    Port-preserved: N    NO-PAT: N    Reversible: N

    Config status: Active
```

通过以下显示命令,可以看到 NAT 会话数、当前可分配的动态端口块总数和已分配的动态端口块个数。

```
[Device] display nat statistics

Total session entries: 1

Session creation rate: 0

Total EIM entries: 0

Total inbound NO-PAT entries: 0
```

```
Total outbound NO-PAT entries: 0
Total static port block entries: 0
Total dynamic port block entries: 430
Active static port block entries: 0
Active dynamic port block entries: 1
```

通过以下显示命令，可以看到生成的 DS-Lite B4 动态端口块表项。

```
[Device] display nat port-block dynamic ds-lite-b4

Slot 1:
Local VPN  DS-Lite B4 addr      Global IP      Port block  Connections  BackUp
---          1::1                20.1.1.11     65224-65523  1             No
Total mappings found: 1
```

3.23.15 HA 联动 VRRP 的主备组网中 NAT 功能典型配置举例

关于此典型配置举例的具体内容，请参见“高可靠性配置指导”中的“双机热备（RBM）”。

3.23.16 HA 联动 VRRP 的双主组网中 NAT 功能典型配置举例

关于此典型配置举例的具体内容，请参见“高可靠性配置指导”中的“双机热备（RBM）”。

目 录

1 AFT	1-1
1.1 AFT 简介	1-1
1.2 AFT 转换方式	1-1
1.2.1 静态转换	1-1
1.2.2 动态转换	1-2
1.2.3 前缀转换	1-2
1.2.4 IPv6 内部服务器	1-4
1.2.5 IPv4 内部服务器	1-4
1.2.6 静态端口块方式	1-4
1.3 AFT 报文转换过程	1-4
1.3.1 IPv6 侧发起访问	1-5
1.3.2 IPv4 侧发起访问	1-6
1.4 AFT 支持 ALG	1-6
1.5 AFT 配置限制和指导	1-7
1.6 vSystem 相关说明	1-7
1.7 AFT 配置任务简介	1-7
1.8 开启 AFT 功能	1-8
1.9 配置 IPv6 到 IPv4 的目的地址转换策略	1-8
1.9.1 功能简介	1-8
1.9.2 配置 IPv4 内部服务器	1-8
1.9.3 配置 IPv4 到 IPv6 源地址静态转换策略	1-9
1.9.4 General 前缀	1-9
1.9.5 配置 NAT64 前缀	1-9
1.10 配置 IPv6 到 IPv4 的源地址转换策略	1-10
1.10.1 功能简介	1-10
1.10.2 配置 IPv6 到 IPv4 源地址静态转换策略	1-10
1.10.3 配置 General 前缀	1-10
1.10.4 配置 IVI 前缀	1-10
1.10.5 配置 IPv6 到 IPv4 的源地址动态转换策略	1-11
1.10.6 配置 IPv6 到 IPv4 端口块方式的静态 AFT 源地址转换策略	1-11
1.11 配置 IPv4 到 IPv6 目的地址转换策略	1-13
1.11.1 功能简介	1-13
1.11.2 配置限制和指导	1-13

1.11.3 配置 IPv6 内部服务器	1-13
1.11.4 配置 IPv6 到 IPv4 的源地址静态转换策略	1-13
1.11.5 配置引用 IVI 前缀或 General 前缀的 IPv4 到 IPv6 目的地址转换策略	1-13
1.12 配置 IPv4 到 IPv6 源地址转换策略	1-14
1.12.1 功能简介	1-14
1.12.2 配置限制和指导	1-14
1.12.3 配置 IPv4 到 IPv6 的源地址静态转换策略	1-14
1.12.4 配置引用 NAT64 前缀或 General 前缀的 IPv4 到 IPv6 源地址转换策略	1-15
1.12.5 配置 NAT64 前缀	1-15
1.13 配置 AFT 转换后 IPv4 报文的 ToS 字段值	1-15
1.14 配置 AFT 转换后 IPv6 报文的 Traffic Class 字段值	1-16
1.15 配置 AFT ALG	1-16
1.16 配置 AFT 的高可靠性	1-16
1.16.1 功能简介	1-16
1.16.2 配置 IRF 双机热备场景下的 AFT 端口负载分担功能	1-17
1.16.3 配置 HA+VRRP 场景中 AFT 与 VRRP 备份组绑定	1-18
1.16.4 开启 AFT 动态端口块热备份功能	1-19
1.17 开启 AFT 日志功能	1-19
1.17.1 配置 AFT 连接的日志功能	1-19
1.17.2 配置 AFT 告警信息日志功能	1-20
1.18 关闭 AFT 生成 OpenFlow 流表功能	1-21
1.19 AFT 显示和维护	1-21
1.20 AFT 典型配置举例	1-23
1.20.1 IPv6 网络访问 IPv4 Internet 配置举例	1-23
1.20.2 IPv4 Internet 访问 IPv6 网络内部服务器配置举例	1-27
1.20.3 IPv4 网络和 IPv6 网络互访配置举例	1-31
1.20.4 IPv4 网络访问 IPv6 Internet 中的服务器配置举例	1-35
1.20.5 IPv6 Internet 访问 IPv4 网络配置举例	1-39

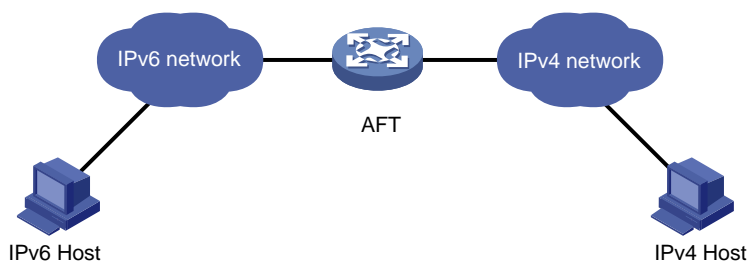
1 AFT

1.1 AFT简介

AFT（Address Family Translation，地址族转换）提供了 IPv4 和 IPv6 地址之间的相互转换功能。在 IPv4 网络完全过渡到 IPv6 网络之前，两个网络之间直接的通信可以通过 AFT 来实现。例如，使用 AFT 可以使 IPv4 网络中的主机直接访问 IPv6 网络中的 FTP 服务器。

如图 1-1 所示，AFT 作用于 IPv4 和 IPv6 网络边缘设备上，所有的地址转换过程都在该设备上实现，对 IPv4 和 IPv6 网络内的用户来说是透明的，即用户不必改变目前网络中主机的配置就可实现 IPv6 网络与 IPv4 网络的通信。

图1-1 AFT 应用场景



1.2 AFT转换方式

AFT 的地址转换分为静态转换、动态转换、前缀转换及 IPv6 内部服务器方式。

1.2.1 静态转换

静态转换方式是指采用手工配置的 IPv6 地址与 IPv4 地址的一一对应关系来实现 IPv6 地址与 IPv4 地址的转换。静态转换方式包括 IPv4 到 IPv6 源地址静态转换策略和 IPv6 到 IPv4 源地址静态转换策略。

IPv4 到 IPv6 源地址静态转换策略可用于如下地址转换场景：

- 对于从 IPv4 侧发起的访问，当报文的源 IPv4 地址匹配 IPv4 到 IPv6 源地址静态转换策略中的 IPv4 地址时，AFT 将报文的源 IPv4 地址转换为 IPv6 地址。
- 对于从 IPv6 侧发起的访问，当报文的目的 IPv6 地址匹配 IPv4 到 IPv6 源地址静态转换策略中的 IPv6 地址时，AFT 将报文的目的 IPv6 地址转换为 IPv4 地址。

IPv6 到 IPv4 源地址静态转换策略可用于如下地址转换场景：

- 对于从 IPv6 侧发起的访问，当报文的源 IPv6 地址匹配 IPv6 到 IPv4 源地址静态转换策略中的 IPv6 地址时，AFT 将报文的源 IPv6 地址转换为 IPv4 地址。
- 对于从 IPv4 侧发起的访问，当报文的目的 IPv4 地址匹配 IPv6 到 IPv4 源地址静态转换策略中的 IPv4 地址时，AFT 将报文的目的 IPv4 地址转换为 IPv6 地址。

1.2.2 动态转换

动态转换方式是指动态地创建 IPv6 地址与 IPv4 地址的对应关系来实现 IPv6 地址与 IPv4 地址的转换。和静态转换方式不同，动态转换方式中 IPv6 和 IPv4 地址之间不存在固定的一一对应关系。

将 IPv6 报文的源 IPv6 地址转换为 IPv4 地址时，动态转换方式分为 NO-PAT 和 PAT 两种模式。

1. NO-PAT 模式

NO-PAT（Not Port Address Translation，非端口地址转换）模式下，一个 IPv4 地址同一时间只能对应一个 IPv6 地址进行转换，不能同时被多个 IPv6 地址共用。当使用某 IPv4 地址的 IPv6 网络用户停止访问 IPv4 网络时，AFT 会将其占用的 IPv4 地址释放并分配给其他 IPv6 网络用户使用。

该模式下，AFT 设备只对报文的 IP 地址进行 AFT 转换，同时会建立一个 NO-PAT 表项用于记录 IPv6 地址和 IPv4 地址的映射关系，并不涉及端口转换，可支持所有 IP 协议的报文。

2. PAT 模式

PAT（Port Address Translation，端口地址转换）模式下，一个 IPv4 地址可以同时被多个 IPv6 地址共用。该模式下，AFT 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 ICMPv6（Internet Control Message Protocol for IPv6，IPv6 互联网控制消息协议）查询报文。

PAT 模式的动态转换策略支持对端口块大小进行限制，从而达到限制转换和溯源的目的。可划分的端口号范围为 1024~65535，剩余不足划分的部分则不会进行分配。IPv6 主机首次发起连接时，为该地址分配一个用于转换的 IPv4 地址，以及该 IPv4 地址的一个端口块。后续从该 IPv6 主机发起的连接都使用这个 IPv4 地址和端口块里面的端口进行转换，直到端口块里面的端口用尽。

1.2.3 前缀转换

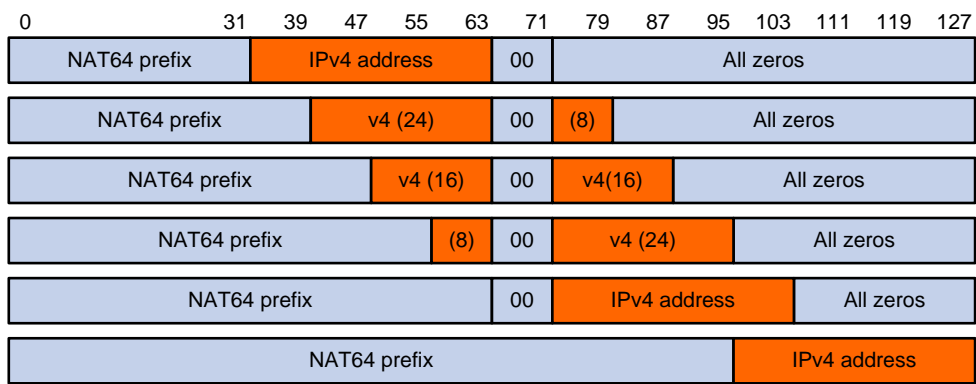
前缀转换包括 NAT64 前缀转换、IVI 前缀转换和 General 前缀转换。

1. NAT64 前缀转换

NAT64 前缀是长度为 32、40、48、56、64 或 96 位的 IPv6 地址前缀，用来构造 IPv4 节点在 IPv6 网络中的地址，以便 IPv4 主机与 IPv6 主机通信。网络中并不存在带有 NAT64 前缀的 IPv6 地址的主机。

如[图 1-2](#)所示，NAT64 前缀长度不同时，地址转换方法有所不同。其中，NAT64 前缀长度为 32、64 和 96 位时，IPv4 地址作为一个整体添加到 IPv6 地址中；NAT64 前缀长度为 40、48 和 56 位时，IPv4 地址被拆分成两部分，分别添加到 64~71 位的前后。64~71 位为保留位，必须设置为 0。

图1-2 对应 IPv4 地址带有 NAT64 前缀的 IPv6 地址格式



AFT 构造 IPv4 节点在 IPv6 网络中的地址示例如表 1-1 所示。

表1-1 IPv4 地址带有 NAT64 前缀的 IPv6 地址示例

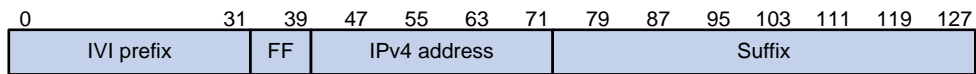
IPv6 前缀	IPv4 地址	嵌入 IPv4 地址的 IPv6 地址
2001:db8::/32	192.0.2.33	2001:db8:c000:221::
2001:db8:100::/40	192.0.2.33	2001:db8:1c0:2:21::
2001:db8:122::/48	192.0.2.33	2001:db8:122:c000:2:2100::
2001:db8:122:300::/56	192.0.2.33	2001:db8:122:3c0:0:221::
2001:db8:122:344::/64	192.0.2.33	2001:db8:122:344:c0:2:2100::
2001:db8:122:344::/96	192.0.2.33	2001:db8:122:344::192.0.2.33

IPv4 侧发起访问时，AFT 利用 NAT64 前缀将报文的源 IPv4 地址转换为 IPv6 地址；IPv6 侧发起访问时，AFT 利用 NAT64 前缀将报文的目的 IPv6 地址转换为 IPv4 地址。

2. IVI 前缀转换

IVI 前缀是长度为 32 位的 IPv6 地址前缀。IVI 地址是 IPv6 主机实际使用的 IPv6 地址，这个 IPv6 地址中内嵌了一个 IPv4 地址，可以用于与 IPv4 主机通信。由 IVI 前缀构成的 IVI 地址格式如图 1-3 所示。

图1-3 IVI 地址格式

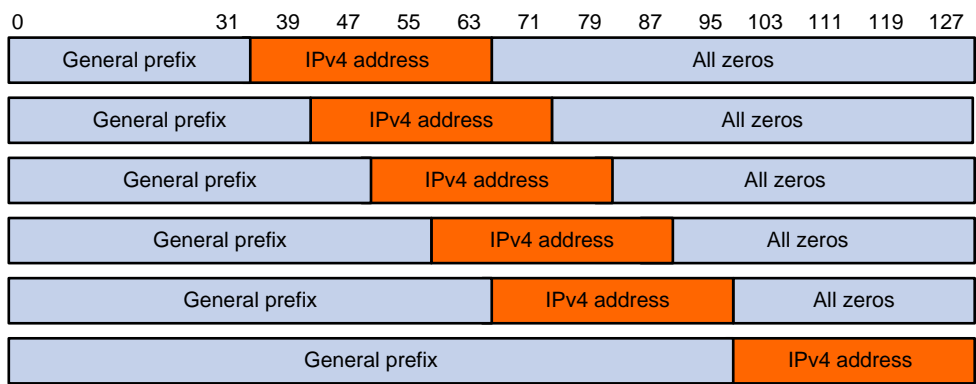


从 IPv6 侧发起访问时，AFT 可以使用 IVI 前缀将报文的源 IPv6 地址转换为 IPv4 地址。

3. General 前缀

General 前缀与 NAT64 前缀类似，都是长度为 32、40、48、56、64 或 96 位的 IPv6 地址前缀，用来构造 IPv4 节点在 IPv6 网络中的地址。如图 1-4 所示，General 前缀与 NAT64 前缀的区别在于，General 前缀没有 64 到 71 位的 8 位保留位，IPv4 地址作为一个整体添加到 IPv6 地址中。

图1-4 对应 IPv4 地址带有 General 前缀的 IPv6 地址格式



从 IPv6 侧发起访问时，AFT 利用 General 前缀将报文的源/目的 IPv6 地址转换为 IPv4 地址。需要注意的是，General 前缀与 NAT64 前缀都不能与设备上的接口地址同网段。

1.2.4 IPv6 内部服务器

IPv6 内部服务器是指向 IPv4 网络主机提供服务的 IPv6 网络中的服务器。通过配置 IPv6 内部服务器，可以将 IPv6 服务器的地址和端口映射到 IPv4 网络，IPv4 网络中的主机通过访问映射后的 IPv4 地址和端口就可以访问 IPv6 网络中的服务器。

1.2.5 IPv4 内部服务器

在 IPv4 向 IPv6 过渡前期，多数服务仍然位于 IPv4 网络中，IPv6 用户访问 IPv4 侧服务器时，通过配置 IPv4 内部服务器，可以将 IPv4 服务器的地址和端口映射到 IPv6 网络，IPv6 网络中的主机通过映射后的 IPv6 地址和端口就可以访问 IPv4 网络中的服务器。

1.2.6 静态端口块方式

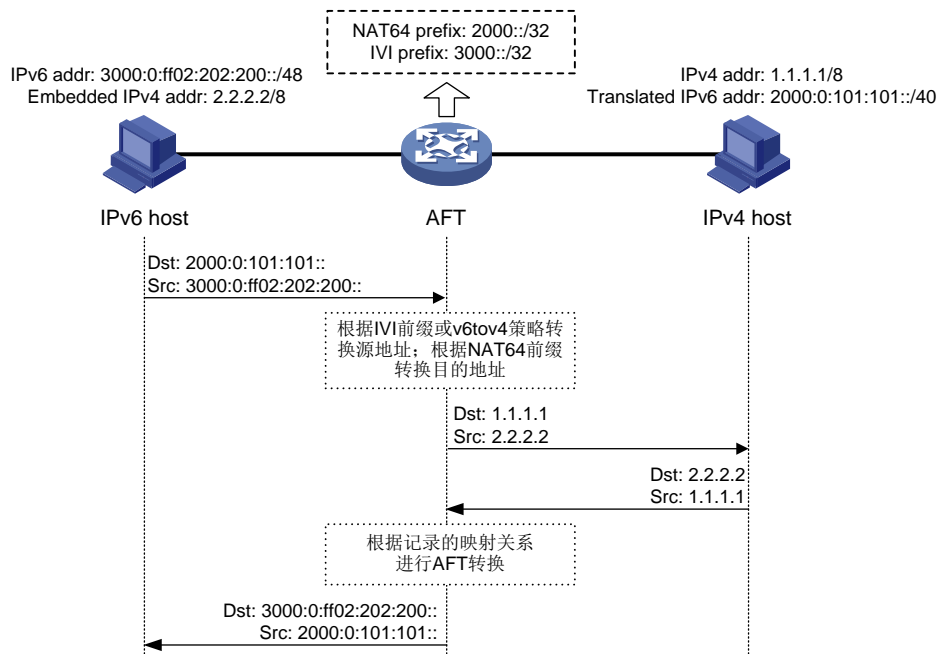
端口块静态映射是指，AFT 设备根据配置自动计算 IPv6 地址与 IPv4 地址、端口块的静态映射关系，并创建静态端口块映射表项。当 IPv6 侧发起连接时，设备通过报文的源 IPv6 地址匹配的 IPv6 前缀查找静态端口块映射表项，使用表项中记录的 IPv4 地址进行地址转换，并从对应的端口块中分配一个端口进行 TCP/UDP 端口转换。

1.3 AFT 报文转换过程

IPv6 侧发起访问和 IPv4 侧发起访问的报文转换过程有所不同，下面将分别介绍。

1.3.1 IPv6 侧发起访问

图1-5 IPv6 侧发起访问的 AFT 报文转换过程

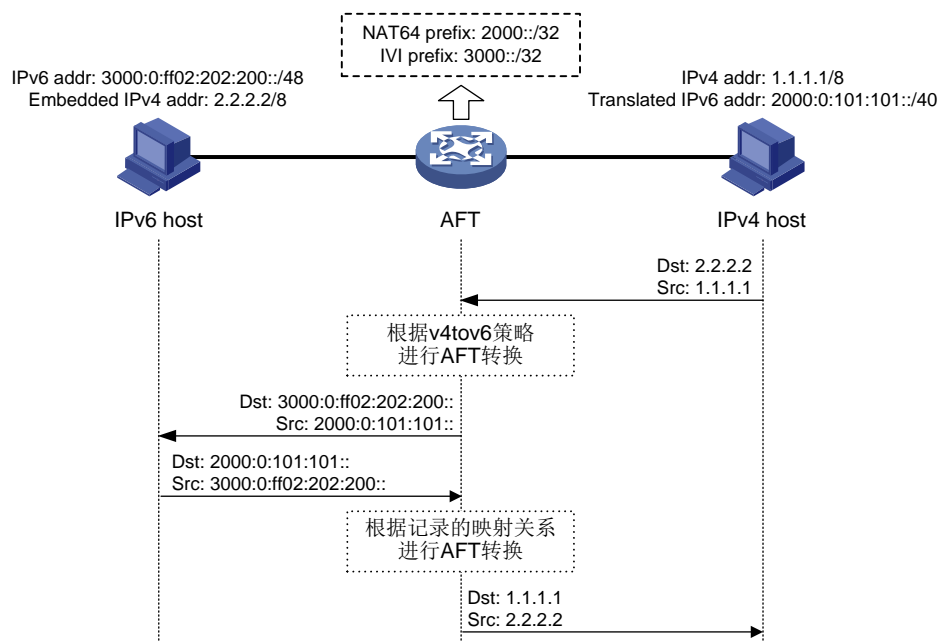


如图 1-5 所示，IPv6 侧发起访问时 AFT 设备对报文的转换过程为：

- (1) 判断是否需要 AFT 转换：AFT 设备接收到 IPv6 网络主机（IPv6 host）发送给 IPv4 网络主机（IPv4 host）的报文后，判断该报文是否要转发到 IPv4 网络。如果报文的目的 IPv6 地址能够匹配到 IPv6 目的地址转换策略，则该报文需要转发到 IPv4 网络，需要进行 AFT 转换；如果未匹配到任何一种转换策略，则表示该报文不需要进行 AFT 转换。
- (2) 转换报文目的地址：根据 IPv6 目的地址转换策略将报文目的 IPv6 地址转换为 IPv4 地址。
- (3) 根据目的地址预查路由：根据转换后的 IPv4 目的地址查找路由表，确定报文的出接口。如果查找失败，则丢弃报文。需要注意的是，预查路由时不会查找策略路由。
- (4) 转换报文源地址：根据 IPv6 源地址转换策略将报文源 IPv6 地址转换为 IPv4 地址。如果未匹配到任何一种转换策略，则报文将被丢弃。
- (5) 转发报文并记录映射关系：报文的源 IPv6 地址和目的 IPv6 地址都转换为 IPv4 地址后，设备按照正常的转发流程将报文转发到 IPv4 网络中的主机。同时，将 IPv6 地址与 IPv4 地址的映射关系保存在设备中。
- (6) 根据记录的映射关系转发应答报文：IPv4 网络主机发送给 IPv6 网络主机的应答报文到达 AFT 设备后，设备将根据已保存的映射关系进行相反的转换，从而将报文发送给 IPv6 网络主机。

1.3.2 IPv4 侧发起访问

图1-6 IPv4 侧发起访问的 AFT 报文转换过程



如图 1-6 所示，IPv4 侧发起访问时 AFT 设备对报文的转换过程为：

- (1) 判断是否需要 AFT 转换：AFT 设备接收到 IPv4 网络主机（IPv4 host）发送给 IPv6 网络主机（IPv6 host）的报文后，判断该报文是否要转发到 IPv6 网络。如果报文的目的 IPv4 地址能够匹配到 IPv4 目的地址转换策略，则该报文需要转发到 IPv6 网络，需要进行 AFT 转换。如果未匹配到任何一种转换策略，则表示该报文不需要进行 AFT 地址转换。
- (2) 转换报文目的地址：根据 IPv4 目的地址转换策略将报文目的 IPv4 地址转换为 IPv6 地址。
- (3) 根据目的地址预查路由：根据转换后的 IPv6 目的地址查找路由表，确定报文的出接口。如果查找失败，则丢弃报文。需要注意的是，预查路由时不会查找策略路由。
- (4) 转换报文源地址：根据 IPv4 源地址转换策略将报文源 IPv4 地址转换为 IPv6 地址。如果未匹配到任何一种转换策略，则报文将被丢弃。
- (5) 转发报文并记录映射关系：报文的源 IPv4 地址和目的 IPv4 地址都转换为 IPv6 地址后，设备按照正常的转发流程将报文转发到 IPv6 网络中的主机。同时，将 IPv4 地址与 IPv6 地址的映射关系保存在设备中。
- (6) 根据记录的映射关系转发应答报文：IPv6 网络主机发送给 IPv4 网络主机的应答报文到达 AFT 设备后，设备将根据已保存的映射关系进行相反的转换，从而将报文发送给 IPv4 网络主机。

1.4 AFT 支持 ALG

AFT 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。然而对于一些特殊协议，它们的报文的数据载荷中可能包含 IP 地址或端口信息。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报文中的载荷信息决定。这

些载荷信息也必须进行有效的转换，否则可能导致功能问题。ALG（Application Level Gateway，应用层网关）主要完成对应用层报文的处理，利用 ALG 可以完成载荷信息的转换。

1.5 AFT配置限制和指导

设备上经过 AFT 转换的报文不会再进行 NAT 转换。

1.6 vSystem相关说明

非缺省 vSystem 不支持本特性的部分功能，具体包括：

- 开启 AFT 端口负载分担功能
- 指定 HA 中主、从管理设备可以使用的 AFT 端口块范围
- 开启 AFT 动态端口块热备份功能
- 关闭 AFT 生成 OpenFlow 流表功能



说明

非缺省 vSystem 不支持本特性的部分命令，具体情况请见本文相关描述。有关 vSystem 的详细介绍请参见“虚拟化技术配置指导”中的“vSystem”。

1.7 AFT配置任务简介

AFT 配置任务如下：

(1) [开启 AFT 功能](#)

(2) 配置 IPv6 侧发起的会话的转换配置

可通过使用本文中的配置任务实现 IPv6 侧发起的会话的转换，或者使用全局 NAT 策略实现 IPv6 侧发起的会话的转换。关于使用全局 NAT 策略实现此功能的详细介绍，请参见“三层技术-IP 业务配置指导”中的“NAT”。

- [配置 IPv6 到 IPv4 的目的地址转换策略](#)
- [配置 IPv6 到 IPv4 的源地址转换策略](#)
- （可选）[配置 AFT 转换后 IPv4 报文的 ToS 字段值](#)

(3) 配置 IPv4 侧发起的会话的转换配置

可通过使用本文中的配置任务实现 IPv4 侧发起的会话的转换，或者使用全局 NAT 策略实现 IPv6 侧发起的会话的转换。关于使用全局 NAT 策略实现此功能的详细介绍，请参见“三层技术-IP 业务配置指导”中的“NAT”。

- [配置 IPv4 到 IPv6 目的地址转换策略](#)
- [配置 IPv4 到 IPv6 源地址转换策略](#)
- （可选）[配置 AFT 转换后 IPv6 报文的 Traffic Class 字段值](#)

(4) （可选）[配置 AFT ALG](#)

(5) （可选）[配置 AFT 的高可靠性](#)

- [配置 IRF 双机热备场景下的 AFT 端口负载分担功能](#)

- [配置 HA+VRRP 场景中 AFT 与 VRRP 备份组绑定](#)
- [开启 AFT 动态端口块热备份功能](#)
- (6) (可选) [开启 AFT 日志功能](#)
 - [配置 AFT 连接的日志功能](#)
 - [配置 AFT 告警信息日志功能](#)
- (7) (可选) [关闭 AFT 生成 OpenFlow 流表](#)

1.8 开启AFT功能

1. 配置限制和指导

只有在连接 IPv4 网络和 IPv6 网络的接口上都开启 AFT 功能后，才能实现 IPv4 报文和 IPv6 报文之间的相互转换。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 开启 AFT 功能。

```
aft enable
```

缺省情况下，AFT 功能处于关闭状态。

1.9 配置IPv6到IPv4的目的地址转换策略

1.9.1 功能简介

IPv6 目的地址转换策略匹配的优先级从高到低为：

- (1) IPv4 内部服务器
- (2) IPv4 到 IPv6 的源地址静态转换策略。
- (3) General 前缀。
- (4) NAT64 前缀。

2. 配置限制和指导

此功能需要保证安全策略放行 IPv6 网络侧安全域到 Local 安全域的报文。

1.9.2 配置 IPv4 内部服务器

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 IPv4 侧服务器对应的 IPv6 地址及端口。

```
aft v4server protocol protocol-type ipv6-destination-address  
ipv6-port-number [ vpn-instance ipv6-vpn-instance-name ]
```

```
ipv4-destination-address ipv4-port-number [ vpn-instance  
ipv4-vpn-instance-name ] [ vrrp virtual-router-id ]
```

缺省情况下，未配置 IPv4 侧服务器对应的 IPv6 地址及端口号。

1.9.3 配置 IPv4 到 IPv6 源地址静态转换策略

1. 配置限制和指导

IPv4 到 IPv6 源地址静态转换策略手工建立了 IPv4 地址与 IPv6 地址的一一对应关系，可用于如下地址转换场景：

- 对于从 IPv4 侧发起的访问，当报文的源 IPv4 地址匹配 IPv4 到 IPv6 源地址静态转换策略中的 IPv4 地址时，AFT 将报文的源 IPv4 地址转换为 IPv6 地址。
- 对于从 IPv6 侧发起的访问，当报文的目的 IPv6 地址匹配 IPv4 到 IPv6 源地址静态转换策略中的 IPv6 地址时，AFT 将报文的目的 IPv6 地址转换为 IPv4 地址。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 IPv4 到 IPv6 源地址静态转换策略。

```
aft v4tov6 source ipv4-address [ vpn-instance ipv4-vpn-instance-name ]  
ipv6-address [ vpn-instance ipv6-vpn-instance-name ] [ vrrp  
virtual-router-id ]
```

缺省情况下，未配置 IPv4 到 IPv6 源地址静态转换策略。

1.9.4 General 前缀

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 General 前缀。

```
aft prefix-general prefix-general prefix-length
```

缺省情况下，未配置 General 前缀。

1.9.5 配置 NAT64 前缀

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 NAT64 前缀。

```
aft prefix-nat64 prefix-nat64 prefix-length
```

缺省情况下，未配置 NAT64 前缀。

1.10 配置IPv6到IPv4的源地址转换策略

1.10.1 功能简介

IPv6 源地址转换策略匹配的优先级从高到低为：

- (1) IPv6 到 IPv4 的源地址静态转换策略。
- (2) General 前缀。
- (3) IVI 前缀。
- (4) IPv6 到 IPv4 端口块方式的静态 AFT 源地址转换策略。
- (5) IPv6 到 IPv4 的源地址动态转换策略。

2. 配置限制和指导

此功能需要保证安全策略放行 Local 安全域到 IPv4 网络侧安全域的报文。

1.10.2 配置 IPv6 到 IPv4 源地址静态转换策略

1. 配置限制和指导

IPv6 到 IPv4 源地址静态转换策略手工建立了 IPv6 地址与 IPv4 地址的一一对应关系，可用于如下地址转换场景：

- 对于从 IPv6 侧发起的访问，当报文的源 IPv6 地址匹配 IPv6 到 IPv4 源地址静态转换策略中的 IPv6 地址时，AFT 将报文的源 IPv6 地址转换为 IPv4 地址。
- 对于从 IPv4 侧发起的访问，当报文的目的 IPv4 地址匹配 IPv6 到 IPv4 源地址静态转换策略中的 IPv4 地址时，AFT 将报文的目的 IPv4 地址转换为 IPv6 地址。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 IPv6 到 IPv4 源地址静态转换策略。

```
aft v6tov4 source ipv6-address [ vpn-instance ipv6-vpn-instance-name ]  
ipv4-address [ vpn-instance ipv4-vpn-instance-name ] [ vrrp  
virtual-router-id ]
```

1.10.3 配置 General 前缀

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 General 前缀。

```
aft prefix-general prefix-general prefix-length
```

1.10.4 配置 IVI 前缀

- (1) 进入系统视图。

```
system-view
```


- (2) 配置IVI前缀。

```
aft prefix-ivi prefix-ivi
```

1.10.5 配置 IPv6 到 IPv4 的源地址动态转换策略

1. 功能简介

IPv6 到 IPv4 源地址动态转换方式是指动态地创建 IPv6 地址与 IPv4 地址的对应关系来实现 IPv6 地址与 IPv4 地址的转换。在 PAT 模式的 IPv6 到 IPv4 源地址动态转换方式中，一个 IPv4 地址可以同时被多个 IPv6 地址共用。该模式下，AFT 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 ICMPv6（Internet Control Message Protocol for IPv6，IPv6 互联网控制消息协议）查询报文。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) （可选）配置 AFT 地址组。

- a. 创建一个 AFT 地址组，并进入 AFT 地址组视图。

```
aft address-group group-id
```

在配置 IPv6 到 IPv4 源地址动态转换策略前，根据实际情况选配。

- b. 添加地址组成员。

```
address start-address end-address
```

可通过多次执行本命令添加多个地址组成员。

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成员的 IP 地址段重叠。

- c. 退回系统视图。

```
quit
```

- (3) 配置 IPv6 到 IPv4 源地址动态转换策略。

```
aft v6tov4 source { acl ipv6 { name ipv6-acl-name | number  
ipv6-acl-number } | prefix-nat64 prefix-nat64 prefix-length  
[ vpn-instance ipv6-vpn-instance-name ] } { address-group group-id  
[ no-pat | port-block-size blocksize [ extended-block-number  
extended-block-number ] [ port-range start-port-number  
end-port-number ] ] | interface interface-type interface-number }  
[ vpn-instance ipv4-vpn-instance-name ]
```

1.10.6 配置 IPv6 到 IPv4 端口块方式的静态 AFT 源地址转换策略

1. 功能简介

配置 IPv6 到 IPv4 端口块方式的静态 AFT 源地址转换策略时，需要创建一个 AFT 端口块组，一个 AFT 端口块组包含如下内容：

- 地址组成员，包含转换前的 IPv6 地址和转换后的 IPv4 地址。
- IPv4 地址的端口范围。

- 端口块大小。

设备将根据 AFT 端口块组内的配置数据，按照固定的算法生成内网 IPv6 地址前缀与外网 IPv4 地址和端口块的映射关系。AFT 端口块组中可分配的端口块总数=端口范围÷端口块大小，假设可分配的端口块总数为 n 个，转换后的 IPv4 地址有 m 个，则可映射的 IPv6 地址前缀总数= $n \times m$ ，超出此数目的 IPv6 地址前缀将无法转换。例如，转换后的 IPv4 地址为 X1 和 Y1，可分配的端口块总数为 n。设备取 n 个转换前的 IPv6 地址前缀，映射同一个 IPv4 地址，并依次映射第一个到第 n 个端口块，生成的映射关系如下所示：

- IPv6 地址前缀 x1<-->IPv4 地址 X1+端口块 1
- IPv6 地址前缀 x2<-->IPv4 地址 X1+端口块 2
-
- IPv6 地址前缀 xn<-->IPv4 地址 X1+端口块 n
- IPv6 地址前缀 y1<-->IPv4 地址 Y1+端口块 1
- IPv6 地址前缀 y2<-->IPv4 地址 Y1+端口块 2
-
- IPv6 地址前缀 yn<-->IPv4 地址 Y1+端口块 n。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建 AFT 端口块组，并进入 AFT 端口块组视图。

```
aft port-block-group block-group-id
```

- (3) 向 AFT 端口块组中添加源地址转换前的 IPv6 地址成员。

```
ipv6-prefix ipv6-start-prefix ipv6-end-prefix prefix-length  
[ vpn-instance vpn-name ]
```

缺省情况下，AFT 端口块组中不存在源地址转换前的 IPv6 地址成员。

- (4) 向 AFT 端口块组中添加源地址转换后的 IPv4 地址成员。

```
ip-address start-address end-address [ vpn-instance vpn-name ]
```

缺省情况下，AFT 端口块组中不存在源地址转换后的 IPv4 地址成员。

- (5) 配置 AFT 进行端口块分配的端口范围。

```
port-range start-port-number end-port-number
```

缺省情况下，AFT 进行端口块分配的端口范围为 1~65535。

- (6) 设置 AFT 端口块大小。

```
block-size block-size-value
```

缺省情况下，一个端口块中包含 256 个端口。

- (7) 退回系统视图。

```
quit
```

- (8) 配置从 IPv6 到 IPv4 端口块方式的静态 AFT 源地址转换策略。

```
aft v6tov4 source port-block-group group-id
```

缺省情况下，未配置从 IPv6 到 IPv4 端口块方式的静态 AFT 源地址转换策略。

1.11 配置IPv4到IPv6目的地址转换策略

1.11.1 功能简介

IPv4 目的地址转换策略的匹配优先级从高到低为：

- (1) IPv6 内部服务器。
- (2) IPv6 到 IPv4 的源地址静态转换策略。
- (3) 引用 IVI 前缀或 General 前缀的 IPv4 到 IPv6 目的地址转换策略。

1.11.2 配置限制和指导

此功能需要保证安全策略放行 IPv4 网络侧安全域到 Local 安全域的报文。

1.11.3 配置 IPv6 内部服务器

- (1) 进入系统视图。

system-view

- (2) 配置 IPv6 侧服务器对应的 IPv4 地址及端口。

```
aft v6server protocol protocol-type ipv4-destination-address  
ipv4-port-number [ vpn-instance ipv4-vpn-instance-name ]  
ipv6-destination-address ipv6-port-number [ vpn-instance  
ipv6-vpn-instance-name ] [ vrrp virtual-router-id ]
```

1.11.4 配置 IPv6 到 IPv4 的源地址静态转换策略

1. 配置限制和指导

IPv6 到 IPv4 源地址静态转换策略手工建立了 IPv6 地址与 IPv4 地址的一一对应关系，可用于如下地址转换场景：

- 对于从 IPv6 侧发起的访问，当报文的源 IPv6 地址匹配 IPv6 到 IPv4 源地址静态转换策略中的 IPv6 地址时，AFT 将报文的源 IPv6 地址转换为 IPv4 地址。
- 对于从 IPv4 侧发起的访问，当报文的目的 IPv4 地址匹配 IPv6 到 IPv4 源地址静态转换策略中的 IPv4 地址时，AFT 将报文的目的 IPv4 地址转换为 IPv6 地址。

2. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 配置 IPv6 到 IPv4 源地址静态转换策略。

```
aft v6tov4 source ipv6-address [ vpn-instance ipv6-vpn-instance-name ]  
ipv4-address [ vpn-instance ipv4-vpn-instance-name ] [ vrrp  
virtual-router-id ]
```

1.11.5 配置引用 IVI 前缀或 General 前缀的 IPv4 到 IPv6 目的地址转换策略

- (1) 进入系统视图。

system-view

- (2) 配置 IVI 前缀或 General 前缀。请选择其中一项进行配置。

- 配置 IVI 前缀。

aft prefix-ivi *prefix-ivi*

- 配置 General 前缀。

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

- (3) 配置引用 IVI 前缀或 General 前缀的 IPv4 到 IPv6 目的地址转换策略。

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

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

1.12 配置IPv4到IPv6源地址转换策略

1.12.1 功能简介

IPv4 源地址转换策略的匹配优先级从高到低为：

- (1) IPv4 到 IPv6 的源地址静态转换策略。
- (2) 引用 NAT64 前缀或 General 前缀的 IPv4 到 IPv6 源地址转换策略。
- (3) NAT64 前缀。

1.12.2 配置限制和指导

此功能需要保证安全策略放行 Local 安全域到 IPv6 网络侧安全域的报文。

1.12.3 配置 IPv4 到 IPv6 的源地址静态转换策略

1. 配置限制和指导

IPv4 到 IPv6 源地址静态转换策略手工建立了 IPv4 地址与 IPv6 地址的一一对应关系，可用于如下地址转换场景：

- 对于从 IPv4 侧发起的访问，当报文的源 IPv4 地址匹配 IPv4 到 IPv6 源地址静态转换策略中的 IPv4 地址时，AFT 将报文的源 IPv4 地址转换为 IPv6 地址。
- 对于从 IPv6 侧发起的访问，当报文的目的 IPv6 地址匹配 IPv4 到 IPv6 源地址静态转换策略中的 IPv6 地址时，AFT 将报文的目的 IPv6 地址转换为 IPv4 地址。

2. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 配置 IPv4 到 IPv6 源地址静态转换策略。

```
aft v4tov6 source ipv4-address [ vpn-instance ipv4-vpn-instance-name ]
ipv6-address [ vpn-instance ipv6-vpn-instance-name ] [ vrrp
virtual-router-id ]
```

1.12.4 配置引用 NAT64 前缀或 General 前缀的 IPv4 到 IPv6 源地址转换策略

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 NAT64 前缀或 General 前缀。请选择其中一项进行配置。

- 配置 NAT64 前缀。

```
aft prefix-nat64 prefix-nat64 prefix-length
```

- 配置 General 前缀。

```
aft prefix-general prefix-general prefix-length
```

- (3) 配置引用 NAT64 前缀或 General 前缀的 IPv4 到 IPv6 源地址转换策略。

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

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

1.12.5 配置 NAT64 前缀

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 NAT64 前缀。

```
aft prefix-nat64 prefix-nat64 prefix-length
```

1.13 配置 AFT 转换后 IPv4 报文的 ToS 字段值

1. 功能简介

用户可以设置在进行 AFT 转换后，IPv4 报文中 ToS 字段的取值：

- 为 0：表示将转换后报文的服务优先级降为最低。
- 与转换前对应的 ToS 字段取值相同：表示保持原有的服务优先级。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 IPv6 报文转换为 IPv4 报文后，IPv4 报文的 ToS 字段值为 0。

```
aft turn-off tos
```

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

1.14 配置AFT转换后IPv6报文的Traffic Class字段值

1. 功能简介

用户可以设置在 AFT 转换后，IPv6 报文中 Traffic Class 字段的取值：

- 为 0：表示将转换后报文的服务优先级降为最低。
- 与转换前对应的 Traffic Class 字段取值相同：表示保持原有的服务优先级。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 IPv4 报文转换为 IPv6 报文后，IPv6 报文的 Traffic Class 字段值为 0。

```
aft turn-off traffic-class
```

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

1.15 配置AFT ALG

1. 配置限制和指导

在 IRF 组网环境中，物理接口上配置的 AFT 业务不支持 ALG 功能。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启指定或所有协议类型的 AFT ALG 功能。

```
aft alg { all | dns | ftp | h323 | http | icmp-error | rtsp | sip }
```

缺省情况下，DNS 协议、FTP 协议、H323 协议、HTTP 协议、ICMP 差错控制报文、RTSP 协议、SIP 协议的 AFT ALG 功能均处于开启状态。

1.16 配置AFT的高可靠性

1.16.1 功能简介

网络中仅部署一台 AFT 设备时，一旦该设备发生故障，内网用户将无法与外网通信。采用双机热备方案可以很好的避免上述情况的发生。在 IRF 双机热备和 HA 高可靠性方案中，主备部署或双主部署的两台设备均可承担 AFT 业务；两台设备间进行会话热备、会话关联表热备、AFT 端口块表项热备以及 AFT 配置的同步。当其中一台设备故障后流量自动切换到另一台正常工作的设备。

关于 IRF 的详细介绍，请参见“虚拟化技术配置指导”中的“IRF”。

关于 HA 的详细介绍，请参见“高可靠性配置指导”中的“双机热备（RBM）”。

1.16.2 配置 IRF 双机热备场景下的 AFT 端口负载分担功能

1. 硬件适配关系

本功能的支持情况与设备型号有关，请以设备的实际情况为准。

设备型号	业务板类型	说明
M9006 M9010 M9014	Blade IV 防火墙业务板	不支持
	Blade V 防火墙业务板	不支持
	NAT 业务板	不支持
M9010-GM	加密业务板	不支持
M9016-V	Blade V 防火墙业务板	不支持
M9008-S M9012-S	Blade IV 防火墙业务板	不支持
	入侵防御业务板	支持
	视频网关业务板	支持
M9008-S-V	Blade IV 防火墙业务板	不支持
M9000-AI-E4 M9000-AI-E8 M9000-AI-E16	Blade V 防火墙业务板	支持
M9000-AK001	Blade V 防火墙业务板	支持
M9000-X06 M9000-X06-B M9000-X06-B-G M9000-X06-G M9000-X10	Blade VI 防火墙业务板	不支持
M9000-AI-X06 M9000-AI-X10	Blade VI 防火墙业务板	不支持

2. 配置限制和指导

AFT 支持双主模式的 IRF 双机热备和主备模式的 IRF 双机热备。两种热备场景中需要的 AFT 配置不同，差异如下：

- 在双主模式的 IRF 双机热备场景下，当两台 IRF 成员设备共用 AFT 地址组中的地址时，可能会出现两台设备上不同的 IPv6 地址+端口号的地址转换结果相同的情况。为了避免上述情况的发生，需要在 IRF 设备上开启 AFT 端口负载分担功能。开启本功能后，两台设备各获得一半端口资源，从而保证两台设备上不同流量的地址转换结果不同。
- 在主备模式的 IRF 双机热备场景下，分别完成 IRF 双机热备配置以及 AFT 的基本配置即可，不需要额外的 AFT 配置来配合。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 AFT 端口负载分担功能。

```
aft port-load-balance enable slot slot-number
```

(IRF 模式)

```
aft port-load-balance enable chassis chassis-number
```

缺省情况下，AFT 端口负载分担功能处于关闭状态。

1.16.3 配置 HA+VRRP 场景中 AFT 与 VRRP 备份组绑定

1. 功能简介

在 HA+VRRP 的高可靠性组网中，当 VRRP 的虚拟 IP 地址与 AFT 地址组或 AFT 端口块组中公网地址成员处于同一网段时，为了避免出现响应 AFT 地址组或 AFT 端口块组中地址成员的 ARP 请求出错的情况，需要将 AFT 地址组或 AFT 端口块组与 VRRP 备份组绑定，由 VRRP 备份组中的 Master 设备对 AFT 地址组或 AFT 端口块组中地址成员的 ARP 请求进行响应。关于 VRRP 的详细介绍，请参见“高可靠性配置指导”中的“高可靠性”。

2. 配置限制和指导

在双主模式的 HA 组网中，不建议用户使用 AFT 端口块组进行地址转换。否则，其中一台设备故障，由另外一台设备承担其业务时，可能会出现 AFT 业务异常的情况。

3. 配置步骤（双主模式）

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 AFT 地址组视图。

```
aft address-group group-id
```

- (3) 将 AFT 地址组与 VRRP 备份组绑定。

```
vrrp vrid virtual-router-id
```

缺省情况下，AFT 地址组未绑定任何 VRRP 备份组。

- (4) 退回系统视图。

```
quit
```

- (5) 指定 HA 中主、从管理设备可以使用的 AFT 端口块范围。

```
aft remote-backup port-alloc { primary / secondary }
```

缺省情况下，HA 中的主、从管理设备共用 AFT 端口资源。

当两台设备共用 AFT 地址组中的地址时，需要在主管理设备上配置本命令。

4. 配置步骤（主备模式）

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 AFT 地址组视图或 AFT 端口块组视图。

- 进入 AFT 地址组视图。

```
aft address-group group-id
```

- 进入 AFT 端口块组视图。

```
aft port-block-group block-group-id
```

- (3) 将 AFT 地址组或者 AFT 端口块组与 VRRP 备份组绑定。

```
vrrp vrid virtual-router-id
```

缺省情况下，AFT 地址组或者 AFT 端口块组未绑定任何 VRRP 备份组。

请在远端备份组主管理设备上配置本命令。

1.16.4 开启 AFT 动态端口块热备份功能

1. 功能简介

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

2. 配置限制和指导

HA 组网环境下，开启 HA 热备业务表项功能（执行 **hot-backup enable** 命令）后本功能才能生效。

IRF 组网环境下，开启会话业务热备份功能（执行 **session synchronization enable** 命令）后本功能才能生效。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 AFT 动态端口块热备份功能。

```
aft port-block synchronization enable
```

缺省情况下，AFT 动态端口块热备份功能处于开启状态。

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

1.17 开启 AFT 日志功能

1.17.1 配置 AFT 连接的日志功能

1. 功能简介

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

- AFT 端口块新建。
- AFT 端口块删除。
- AFT 端口块分配。
- AFT 端口块回收。

- AFT 端口块耗尽。
- AFT 流创建，即 AFT 会话创建时输出日志。
- AFT 流删除，即 AFT 会话释放时输出日志。

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

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 AFT 连接的日志功能。

```
aft log enable
```

缺省情况下，AFT 连接的日志功能处于关闭状态。

配置本命令后，将记录 AFT 端口块新建和 AFT 端口块删除的日志信息。

- (3) （可选）开启 AFT 端口块日志功能。

```
aft log port-block { alarm | assign | withdraw }
```

缺省情况下，AFT 端口块日志功能处于关闭状态。

如需记录 AFT 端口块分配、回收以及 AFT 端口块耗尽时的日志信息，则需要配置本命令。只有配置 **aft log enable** 命令之后，本命令才能生效。

- (4) （可选）开启 AFT 流创建或流删除的日志功能。

- 开启 AFT 流创建的日志功能。

```
aft log flow-begin
```

缺省情况下，AFT 新建流的日志功能处于关闭状态。

如需记录 AFT 会话创建时的日志信息，则需要配置本命令。只有配置 **aft log enable** 命令之后，本命令才能生效。

- 开启 AFT 流删除的日志功能。

```
aft log flow-end
```

缺省情况下，AFT 删除流的日志功能处于关闭状态。

如需记录 AFT 会话释放时的日志信息，则需要配置本命令。只有配置 **aft log enable** 命令之后，本命令才能生效。

1.17.2 配置 AFT 告警信息日志功能

1. 功能简介

端口块方式的 IPv6 到 IPv4 源地址动态转换策略中，如果可为用户分配的 AFT 资源用尽，后续连接由于没有可用的资源无法对其进行地址转换，相应的报文将被丢弃。本命令用来在 AFT 资源用尽时输出告警日志。AFT 资源是指 IPv4 地址和端口块。当端口块的使用率大于设置的阈值时，系统会输出告警日志。

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

2. 配置限制和指导

只有开启 AFT 连接的日志功能（通过 **aft log enable** 命令）之后，AFT 告警信息日志功能才能生效。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 AFT 连接的日志功能。

```
aft log enable
```

缺省情况下，AFT 连接的日志功能处于关闭状态。

- (3) 配置 AFT 端口块使用率的阈值。

```
aft log port-block usage threshold threshold-value
```

缺省情况下，AFT 端口块使用率的阈值为 90%。

1.18 关闭AFT生成OpenFlow流表功能

1. 功能简介

对于多安全引擎设备，为保证同一条流的正向报文和反向报文由同一个引擎处理，AFT 模块会在接口板下发 OpenFlow 流表来匹配和处理报文。有关安全引擎的详细介绍，请参见“虚拟化技术配置指导”中的“Context”。

开启该功能后，系统会为新的 AFT 转换配置以及已经存在的 AFT 转换配置生成 OpenFlow 流表。关闭该功能后，系统不再为新的 AFT 转换配置生成 OpenFlow 流表，并删除已存在的 AFT 转换配置生成的 OpenFlow 流表，可能会造成流量中断。

2. 配置限制和指导

使用 IPv6 到 IPv4 的源地址动态转换策略时，建议关闭前缀转换和静态转换生成 AFT 流表功能，否则可能会导致转换策略不生效。

HA 组网下，不允许开启 AFT 前缀转换生成 OpenFlow 流表的功能。关于 HA 组网的详细介绍，请参见“高可靠性配置指导”中的“双机热备（RBM）”。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 关闭 AFT 生成 OpenFlow 流表的功能。

```
aft flow-redirect { all | dynamic | prefix | static | v6server } disable
```

缺省情况下，AFT 前缀转换生成 OpenFlow 流表的功能处于关闭状态，动态 AFT、静态 AFT 和 IPv6 内部服务器生成 OpenFlow 流表的功能处于开启状态。

1.19 AFT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 AFT 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** 命令可以删除 AFT 会话或统计信息。

表1-2 AFT 显示和维护

操作	命令
显示AFT配置信息	display aft configuration
显示地址组信息	display aft address-group [<i>group-id</i>]
显示AFT地址映射信息	（独立运行模式） display aft address-mapping [<i>slot</i> <i>slot-number</i> [<i>cpu</i> <i>cpu-number</i>]] （IRF模式） display aft address-mapping [<i>chassis</i> <i>chassis-number</i> <i>slot</i> <i>slot-number</i> [<i>cpu</i> <i>cpu-number</i>]]
显示AFT NO-PAT表项信息	（独立运行模式） display aft no-pat [<i>slot</i> <i>slot-number</i> [<i>cpu</i> <i>cpu-number</i>]] （IRF模式） display aft no-pat [<i>chassis</i> <i>chassis-number</i> <i>slot</i> <i>slot-number</i> [<i>cpu</i> <i>cpu-number</i>]]
显示AFT端口块映射表项信息	（独立运行模式） display aft port-block { <i>dynamic</i> <i>static</i> } [<i>slot</i> <i>slot-number</i> [<i>cpu</i> <i>cpu-number</i>]] （IRF模式） display aft port-block { <i>dynamic</i> <i>static</i> } [<i>chassis</i> <i>chassis-number</i> <i>slot</i> <i>slot-number</i> [<i>cpu</i> <i>cpu-number</i>]]
显示AFT会话	（独立运行模式） display aft session ipv4 [{ <i>source-ip</i> <i>source-ip-address</i> <i>destination-ip</i> <i>destination-ip-address</i> } * [<i>vpn-instance</i> <i>ipv4-vpn-instance-name</i>]] [<i>slot</i> <i>slot-number</i> [<i>cpu</i> <i>cpu-number</i>]] [<i>verbose</i>] display aft session ipv6 [{ <i>source-ip</i> <i>source-ipv6-address</i> <i>destination-ip</i> <i>destination-ipv6-address</i> } * [<i>vpn-instance</i> <i>ipv6-vpn-instance-name</i>]] [<i>slot</i> <i>slot-number</i> [<i>cpu</i> <i>cpu-number</i>]] [<i>verbose</i>] （IRF模式） display aft session ipv4 [{ <i>source-ip</i> <i>source-ip-address</i> <i>destination-ip</i> <i>destination-ip-address</i> } * [<i>vpn-instance</i> <i>ipv4-vpn-instance-name</i>]] [<i>chassis</i> <i>chassis-number</i> <i>slot</i> <i>slot-number</i> [<i>cpu</i> <i>cpu-number</i>]] [<i>verbose</i>] display aft session ipv6 [{ <i>source-ip</i> <i>source-ipv6-address</i> <i>destination-ip</i> <i>destination-ipv6-address</i> } * [<i>vpn-instance</i> <i>ipv6-vpn-instance-name</i>]] [<i>chassis</i> <i>chassis-number</i> <i>slot</i> <i>slot-number</i> [<i>cpu</i> <i>cpu-number</i>]] [<i>verbose</i>]

操作	命令
显示AFT统计信息	(独立运行模式) display aft statistics [slot <i>slot-number</i>] [cpu <i>cpu-number</i>]] (IRF模式) display aft statistics [chassis <i>chassis-number</i> slot <i>slot-number</i> [cpu <i>cpu-number</i>]]
删除AFT会话	(独立运行模式) reset aft session [slot <i>slot-number</i> [cpu <i>cpu-number</i>]] (IRF模式) reset aft session [chassis <i>chassis-number</i> slot <i>slot-number</i> [cpu <i>cpu-number</i>]]
删除AFT统计信息	(独立运行模式) reset aft statistics [slot <i>slot-number</i> [cpu <i>cpu-number</i>]] (IRF模式) reset aft statistics [chassis <i>chassis-number</i> slot <i>slot-number</i> [cpu <i>cpu-number</i>]]

1.20 AFT典型配置举例

1.20.1 IPv6 网络访问 IPv4 Internet 配置举例

1. 组网需求

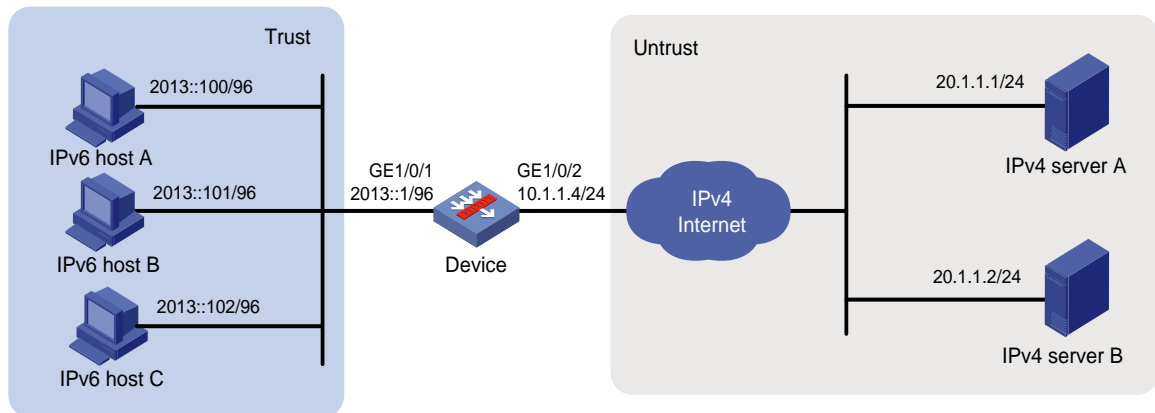
某公司将网络升级到了 IPv6，但是仍然希望内网 2013::/96 网段的用户可以访问 IPv4 Internet，其它网段的用户不能访问 IPv4 Internet。该公司访问 IPv4 Internet 使用的 IPv4 地址为 10.1.1.1、10.1.1.2 和 10.1.1.3。

为满足上述需求，本例中实现方式如下：

- 使用 NAT64 前缀与 IPv4 网络中的主机地址组合成为 IPv6 地址，此 IPv6 地址将与 IPv4 Internet 内的主机建立相应的映射关系，IPv6 网络中的主机访问该 IPv6 地址即可实现对 IPv4 Internet 的访问。报文到达 Device 后，设备将根据 NAT64 前缀将该目的 IPv6 地址转换为对应的 IPv4 地址。
- 使用 IPv6 到 IPv4 源地址动态转换策略将 IPv6 网络到 IPv4 网络报文的源地址转换为 IPv4 地址 10.1.1.1、10.1.1.2 或 10.1.1.3。

2. 组网图

图1-7 IPv6 网络访问 IPv4 Internet 配置组网图



3. 配置步骤

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ipv6 address 2013::1 96
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 将接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 1/0/1
[Device-security-zone-Trust] quit
[Device] security-zone name untrust
[Device-security-zone-Untrust] import interface gigabitethernet 1/0/2
[Device-security-zone-Untrust] quit
```

(3) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达 Server 所在网络的下一跳 IP 地址为 10.1.1.100，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ip route-static 20.1.1.0 24 10.1.1.100
```

(4) 配置安全策略

配置名称为 **aflocalin** 的安全策略，使 Device 能对 Host 访问 Server 的报文进行 AFT 转换，具体配置步骤如下。

```
[Device] security-policy ipv6
```

```
[Device-security-policy-ipv6] rule name aftlocalin
[Device-security-policy-ipv6-1-aftlocalin] source-zone trust
[Device-security-policy-ipv6-1-aftlocalin] destination-zone local
[Device-security-policy-ipv6-1-aftlocalin] source-ip-subnet 2013:: 96
[Device-security-policy-ipv6-1-aftlocalin] destination-ip-host 2012::20.1.1.1
[Device-security-policy-ipv6-1-aftlocalin] destination-ip-host 2012::20.1.1.2
[Device-security-policy-ipv6-1-aftlocalin] action pass
[Device-security-policy-ipv6-1-aftlocalin] quit
[Device-security-policy-ipv6] quit
```

配置名称为 **aftlocalout** 的安全策略，允许将 AFT 转换后的报文转发至 Server，具体配置步骤如下。

```
[Device] security-policy ip
[Device-security-policy-ip] rule name aftlocalout
[Device-security-policy-ip-1-aftlocalout] source-zone local
[Device-security-policy-ip-1-aftlocalout] destination-zone untrust
[Device-security-policy-ip-1-aftlocalout] source-ip-host 10.1.1.1
[Device-security-policy-ip-1-aftlocalout] source-ip-host 10.1.1.2
[Device-security-policy-ip-1-aftlocalout] source-ip-host 10.1.1.3
[Device-security-policy-ip-1-aftlocalout] destination-ip-host 20.1.1.1
[Device-security-policy-ip-1-aftlocalout] destination-ip-host 20.1.1.2
[Device-security-policy-ip-1-aftlocalout] action pass
[Device-security-policy-ip-1-aftlocalout] quit
[Device-security-policy-ip] quit
```

(5) 配置 AFT 功能

配置地址组 0 包含三个 IPv4 地址 10.1.1.1、10.1.1.2 和 10.1.1.3。

```
[Device] aft address-group 0
[Device-aft-address-group-0] address 10.1.1.1 10.1.1.3
[Device-aft-address-group-0] quit
```

配置 IPv6 ACL 2000，该 ACL 用来匹配源 IPv6 地址属于 2013::/96 网段的报文。

```
[Device] acl ipv6 basic 2000
[Device-acl-ipv6-basic-2000] rule permit source 2013:: 96
[Device-acl-ipv6-basic-2000] rule deny
[Device-acl-ipv6-basic-2000] quit
```

配置 IPv6 到 IPv4 的源地址动态转换策略，将匹配 ACL 2000 的 IPv6 报文源地址转换为地址组 0 中的地址，即将 2013::/96 网段内主机所发送报文的源 IPv6 地址转换为 IPv4 地址 10.1.1.1、10.1.1.2 或 10.1.1.3。

```
[Device] aft v6tov4 source acl ipv6 number 2000 address-group 0
```

配置 NAT64 前缀为 2012::/96，报文的目的地地址根据该 NAT64 前缀转换为 IPv4 地址。

```
[Device] aft prefix-nat64 2012:: 96
```

在设备 IPv6 侧和 IPv4 侧接口开启 AFT 功能。

```
[Device] interface gigabitethernet 1/0/1
```

```
[Device-GigabitEthernet1/0/1] aft enable
```

```
[Device-GigabitEthernet1/0/1] quit
```

```
[Device] interface gigabitethernet 1/0/2
```

```
[Device-GigabitEthernet1/0/2] aft enable
```

```
[Device-GigabitEthernet1/0/2] quit
```

4. 验证配置

以上配置完成后，检查 IPv6 Host 与 IPv4 Server 的连通性。以 IPv6 host A ping IPv4 server A 为例：

```
D:\>ping 2012::20.1.1.1
```

```
Pinging 2012::20.1.1.1 with 32 bytes of data:
```

```
Reply from 2012::20.1.1.1: time=3ms
```

```
Reply from 2012::20.1.1.1: time=3ms
```

```
Reply from 2012::20.1.1.1: time=3ms
```

```
Reply from 2012::20.1.1.1: time=3ms
```

通过查看 AFT 会话，可以看到创建了一个 IPv6 会话和 IPv4 会话，分别对应转换前和转换后的报文。

```
[Device] display aft session ipv6 verbose
```

```
Initiator:
```

```
Source      IP/port: 2013::100/0
```

```
Destination IP/port: 2012::1401:0101/32768
```

```
VPN instance/VLAN ID/Inline ID: -/-/-
```

```
Protocol: IPV6-ICMP(58)
```

```
Inbound interface: GigabitEthernet1/0/1
```

```
Source security zone: Trust
```

```
Responder:
```

```
Source      IP/port: 2012::1401:0101/0
```

```
Destination IP/port: 2013::100/33024
```

```
VPN instance/VLAN ID/Inline ID: -/-/-
```

```
Protocol: IPV6-ICMP(58)
```

```
Inbound interface: GigabitEthernet1/0/2
```

```
Source security zone: Local
```

```
State: ICMPV6_REPLY
```

```
Application: ICMP
```

```
Rule ID: -/-/-
```

```
Rule name:
```



```

Start time: 2014-03-13 08:52:59  TTL: 23s

Initiator->Responder:          4 packets          320 bytes
Responder->Initiator:          4 packets          320 bytes

Total sessions found: 1

[Device] display aft session ipv4 verbose
Initiator:
  Source      IP/port: 10.1.1.1/1025
  Destination IP/port: 20.1.1.1/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Local
Responder:
  Source      IP/port: 20.1.1.1/1025
  Destination IP/port: 10.1.1.1/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Untrust
State: ICMP_REPLY
Application: ICMP
Rule ID: 0
Rule name: aftlocalout
Start time: 2014-03-13 08:52:59  TTL: 27s

Initiator->Responder:          4 packets          240 bytes
Responder->Initiator:          4 packets          240 bytes

Total sessions found: 1

```

1.20.2 IPv4 Internet 访问 IPv6 网络内部服务器配置举例

1. 组网需求

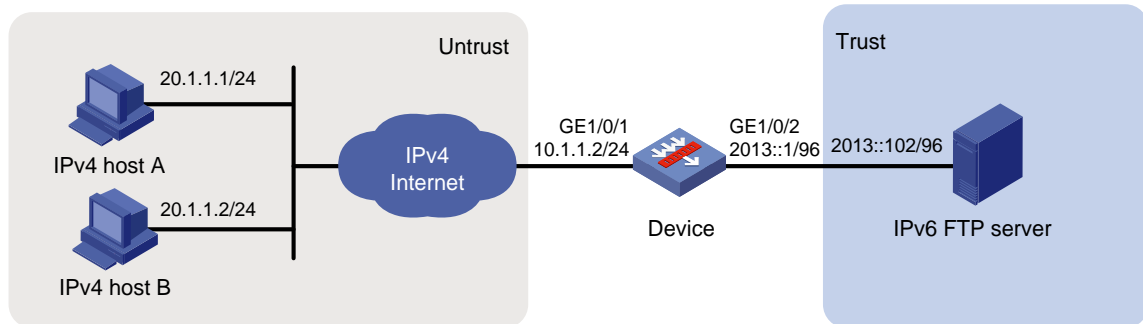
某公司将网络升级到了 IPv6，此时 Internet 仍然是 IPv4 网络。该公司希望内部的 FTP 服务器能够继续为 IPv4 Internet 的用户提供服务。该公司拥有的 IPv4 地址为 10.1.1.1。

为满足上述要求，本例实现方式如下：

- 使用 IPv6 侧服务器配置将 IPv6 内部服务器的地址及端口映射为 IPv4 地址及端口，Device 收到来自 IPv4 Internet 的报文后，根据该配置策略将报文 IPv4 目的地址转换为 IPv6 地址；
- 使用 NAT64 前缀将报文源 IPv4 地址转换为 IPv6 地址。

2. 组网图

图1-8 IPv4 Internet 访问 IPv6 网络内部服务器配置组网图



3. 配置步骤

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 10.1.1.2 24
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 将接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 1/0/2
[Device-security-zone-Trust] quit
[Device] security-zone name untrust
[Device-security-zone-Untrust] import interface gigabitethernet 1/0/1
[Device-security-zone-Untrust] quit
```

(3) 配置安全策略

配置名称为 **aftlocalin** 的安全策略，使 Device 能对 Host 访问 Server 的报文进行 AFT 转换，具体配置步骤如下。

```
[Device] security-policy ip
[Device-security-policy-ip] rule name aftlocalin
[Device-security-policy-ip-1-aftlocalin] source-zone untrust
[Device-security-policy-ip-1-aftlocalin] destination-zone local
[Device-security-policy-ip-1-aftlocalin] destination-ip-host 10.1.1.1
[Device-security-policy-ip-1-aftlocalin] action pass
```

```
[Device-security-policy-ip-1-aftlocalin] quit
[Device-security-policy-ip] quit
```

配置名称为 **aftlocalout** 的安全策略，允许将 AFT 转换后的报文转发至 Server，具体配置步骤如下。

```
[Device] security-policy ipv6
[Device-security-policy-ipv6] rule name aftlocalout
[Device-security-policy-ipv6-1-aftlocalout] source-zone local
[Device-security-policy-ipv6-1-aftlocalout] destination-zone trust
[Device-security-policy-ipv6-1-aftlocalout] source-ip-subnet 2012:: 96
[Device-security-policy-ipv6-1-aftlocalout] destination-ip-host 2013::102
[Device-security-policy-ipv6-1-aftlocalout] action pass
[Device-security-policy-ipv6-1-aftlocalout] quit
[Device-security-policy-ipv6] quit
```

(4) 配置 AFT 功能

配置 IPv6 侧服务器对应的 IPv4 地址及端口号。IPv4 网络内用户通过访问该 IPv4 地址及端口即可访问 IPv6 服务器。

```
[Device] aft v6server protocol tcp 10.1.1.1 21 2013::102 21
```

报文的源地址将根据配置的 NAT64 前缀转换为 IPv6 地址。

```
[Device] aft prefix-nat64 2012:: 96
```

在设备 IPv4 侧和 IPv6 侧接口开启 AFT。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] aft enable
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] aft enable
[Device-GigabitEthernet1/0/2] quit
```

4. 验证配置

以上配置完成后，IPv4 Host 可以通过 FTP 协议访问 IPv6 FTP Server。

通过查看 AFT 会话，可以看到创建了一个 IPv4 会话和 IPv6 会话，分别对应转换前和转换后的报文。

```
[Device] display aft session ipv4 verbose
Initiator:
  Source      IP/port: 20.1.1.1/11025
  Destination IP/port: 10.1.1.1/21
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
```

```

Source security zone: Untrust
Responder:
  Source      IP/port: 10.1.1.1/21
  Destination IP/port: 20.1.1.1/11025
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Local
State: TCP_ESTABLISHED
Application: FTP
Rule ID: -/-/-
Rule name:
Start time: 2014-03-13 09:07:30  TTL: 3577s
Initiator->Responder:          3 packets          124 bytes
Responder->Initiator:          2 packets          108 bytes

Total sessions found: 1

[Device] display aft session ipv6 verbose
Initiator:
  Source      IP/port: 2012::1401:0101/1029
  Destination IP/port: 2013::102/21
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Local
Responder:
  Source      IP/port: 2013::102/21
  Destination IP/port: 2012::1401:0101/1029
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Trust
State: TCP_ESTABLISHED
Application: FTP
Rule ID: 0
Rule name: aftlocalout

```

```

Start time: 2014-03-13 09:07:30   TTL: 3582s

Initiator->Responder:                3 packets        184 bytes
Responder->Initiator:                2 packets        148 bytes

Total sessions found: 1

```

1.20.3 IPv4 网络和 IPv6 网络互访配置举例

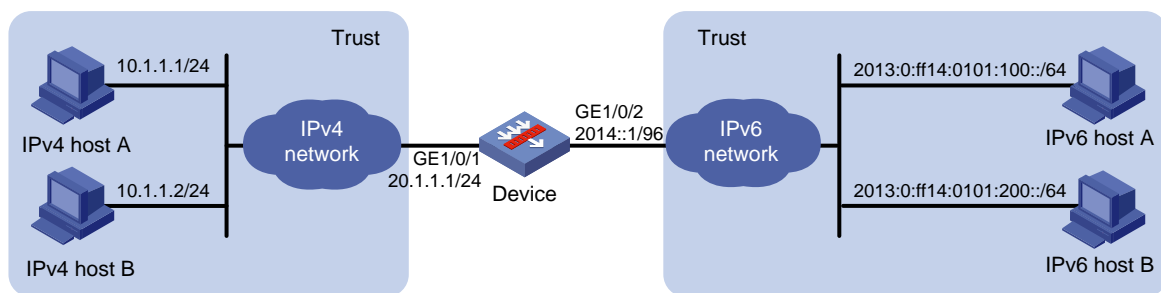
1. 组网需求

某公司内部同时部署了 IPv4 网络和 IPv6 网络，并且希望 IPv4 网络和 IPv6 网络能够互相访问。为满足上述需求，本例中使用如下方式实现：

- 为 IPv6 网络分配一个 IVI 前缀和 IPv4 网段，IPv6 网络中所有 IPv6 主机的地址均配置为由 IVI 前缀和 IPv4 网段中地址组合而成的 IPv6 地址。
- 为 IPv4 网络分配一个 NAT64 前缀，IPv4 网络主动访问 IPv6 网络时，IPv4 源地址使用 NAT64 前缀转换为 IPv6 地址；IPv6 网络主动访问 IPv4 网络时，目的地址使用 NAT64 前缀和 IPv4 地址组合成的 IPv6 地址。

2. 组网图

图1-9 IPv4 网络和 IPv6 网络互访配置组网图



3. 配置步骤

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```

<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 20.1.1.1 24
[Device-GigabitEthernet1/0/1] quit

```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 将接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```

[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 1/0/1
[Device-security-zone-Trust] import interface gigabitethernet 1/0/2

```

```
[Device-security-zone-Trust] quit
```

(3) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达 IPv6 Host 所在网络的下一跳 IPv6 地址为 2014::100，到达 IPv4 Host 所在网络的下一跳 IP 地址为 20.1.1.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ipv6 route-static 2013:: 32 2014::100
```

```
[Device] ip route-static 10.1.1.0 24 20.1.1.2
```

(4) 配置安全策略

a. 配置安全策略放行 IPv4 Host 访问 IPv6 Host 的流量。

配置名称为 **aftlocalin4** 的安全策略，使 Device 能对 IPv4 Host 访问 IPv6 Host 的报文进行 AFT 转换，具体配置步骤如下。

```
[Device] security-policy ip
[Device-security-policy-ip] rule name aftlocalin4
[Device-security-policy-ip-1-aftlocalin4] source-zone trust
[Device-security-policy-ip-1-aftlocalin4] destination-zone local
[Device-security-policy-ip-1-aftlocalin4] source-ip-subnet 10.1.1.0 24
[Device-security-policy-ip-1-aftlocalin4] destination-ip-subnet 20.1.1.0 24
[Device-security-policy-ip-1-aftlocalin4] action pass
[Device-security-policy-ip-1-aftlocalin4] quit
[Device-security-policy-ip] quit
```

配置名称为 **aftlocalout6** 的安全策略，允许将 AFT 转换后的报文转发至 IPv6 Host，具体配置步骤如下。

```
[Device] security-policy ipv6
[Device-security-policy-ipv6] rule name aftlocalout6
[Device-security-policy-ipv6-1-aftlocalout6] source-zone local
[Device-security-policy-ipv6-1-aftlocalout6] destination-zone trust
[Device-security-policy-ipv6-1-aftlocalout6] source-ip-subnet 2012:: 96
[Device-security-policy-ipv6-1-aftlocalout6] destination-ip-subnet 2013:: 32
[Device-security-policy-ipv6-1-aftlocalout6] action pass
[Device-security-policy-ipv6-1-local-ipv6] quit
```

b. 配置安全策略放行 IPv6 Host 访问 IPv4 Host 的流量。

配置名称为 **aftlocalin6** 的安全策略，使 Device 能对 IPv6 Host 访问 IPv4 Host 的报文进行 AFT 转换，具体配置步骤如下。

```
[Device-security-policy-ipv6] rule name aftlocalin6
[Device-security-policy-ipv6-2-aftlocalin6] source-zone trust
[Device-security-policy-ipv6-2-aftlocalin6] destination-zone local
[Device-security-policy-ipv6-2-aftlocalin6] source-ip-subnet 2013:: 32
```

```
[Device-security-policy-ipv6-2-aftlocalin6] destination-ip-subnet 2012:: 96
[Device-security-policy-ipv6-2-aftlocalin6] action pass
[Device-security-policy-ipv6-2-aftlocalin6] quit
[Device-security-policy-ipv6] quit
```

配置名称为 **aftlocalout4** 的安全策略，允许将 AFT 转换后的报文转发至 IPv4 Host，具体配置步骤如下。

```
[Device] security-policy ip
[Device-security-policy-ip] rule 2 name aftlocalout4
[Device-security-policy-ip-2-aftlocalout4] source-zone local
[Device-security-policy-ip-2-aftlocalout4] destination-zone trust
[Device-security-policy-ip-2-aftlocalout4] source-ip-subnet 20.1.1.0 24
[Device-security-policy-ip-2-aftlocalout4] destination-ip-subnet 10.1.1.0 24
[Device-security-policy-ip-2-aftlocalout4] action pass
[Device-security-policy-ip-2-aftlocalout4] quit
[Device-security-policy-ip] quit
```

(5) 配置 AFT 功能

配置 ACL 2000 用来过滤需要访问 IPv6 网络的用户，同时匹配该 ACL 2000 的报文的目的地址将会根据配置的 IVI 前缀转换为 IPv6 地址。此处所有 IPv4 网络用户均需要访问 IPv6 网络。

```
[Device] acl basic 2000
[Device-acl-ipv4-basic-2000] rule permit
[Device-acl-ipv4-basic-2000] quit
```

配置 NAT64 前缀，用于进行 IPv4 到 IPv6 的源地址转换和 IPv6 到 IPv4 的目的地址转换。

```
[Device] aft prefix-nat64 2012:: 96
```

配置 IVI 前缀，用于进行 IPv6 到 IPv4 源地址转换，且在 IPv4 到 IPv6 动态目的地址转换策略中引用该前缀。

```
[Device] aft prefix-ivi 2013::
```

配置 IPv4 到 IPv6 动态目的地址转换策略，IPv4 到 IPv6 报文的目的 IPv4 地址转换为 IPv6 地址。

```
[Device] aft v4tov6 destination acl number 2000 prefix-ivi 2013::
```

在设备 IPv4 侧和 IPv6 侧接口开启 AFT。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] aft enable
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] aft enable
[Device-GigabitEthernet1/0/2] quit
```

4. 验证配置

以上配置完成后, IPv4 host 与 IPv6 host 可以互通。以 IPv6 host A ping IPv4 host A 为例:

```
D:\>ping 2012::a01:0101

Pinging 2012::a01:0101 with 32 bytes of data:

Reply from 2012::a01:0101: time=3ms
Reply from 2012::a01:0101: time=3ms
Reply from 2012::a01:0101: time=3ms
Reply from 2012::a01:0101: time=3ms
```

通过查看 AFT 会话, 可以看到创建了一个 IPv6 会话和 IPv4 会话, 分别对应转换前和转换后的报文。显示内容如下:

```
[Device] display aft session ipv6 verbose

Initiator:

  Source      IP/port: 2013:0:FF14:0101:0100::/0
  Destination IP/port: 2012::0a01:0101/32768
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: IPV6-ICMP(58)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Trust

Responder:

  Source      IP/port: 2012::0a01:0101/0
  Destination IP/port: 2013:0:FF14:0101:0100::/33024
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: IPV6-ICMP(58)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Local

State: ICMPV6_REPLY
Application: ICMP
Rule ID: -/-/-
Rule name:

Start time: 2014-03-13 08:52:59  TTL: 23s

Initiator->Responder:          4 packets          320 bytes
Responder->Initiator:          4 packets          320 bytes

Total sessions found: 1

[Device] display aft session ipv4 verbose

Initiator:

  Source      IP/port: 20.1.1.1/1025
```



```

Destination IP/port: 10.1.1.1/2048
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: ICMP(1)
Inbound interface: GigabitEthernet1/0/2
Source security zone: Local
Responder:
Source      IP/port: 10.1.1.1/1025
Destination IP/port: 20.1.1.1/0
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: ICMP(1)
Inbound interface: GigabitEthernet1/0/1
Source security zone: Trust
State: ICMP_REPLY
Application: ICMP
Rule ID: 2
Rule name: aftlocalout4
Start time: 2014-03-13 08:52:59  TTL: 27s
Initiator->Responder:          4 packets          240 bytes
Responder->Initiator:          4 packets          240 bytes

Total sessions found: 1

```

1.20.4 IPv4 网络访问 IPv6 Internet 中的服务器配置举例

1. 组网需求

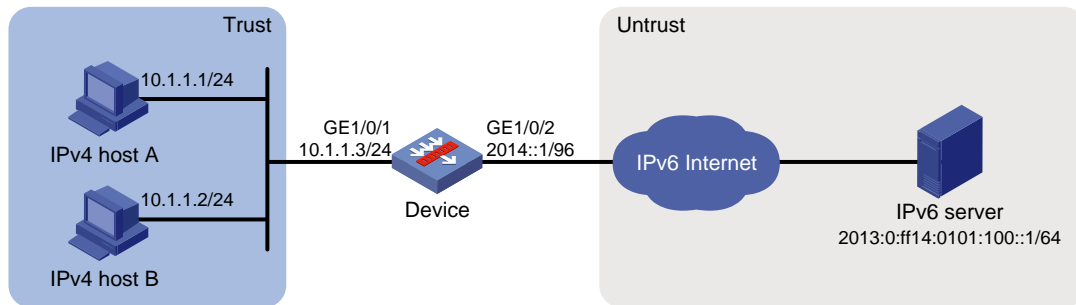
Internet 已经升级到了 IPv6，但是某公司内部网络仍然是 IPv4 网络。而该公司内部网络的 10.1.1.0/24 网段的用户仍需要访问 IPv6 Internet 中的服务器，其他用户不能访问。

为满足上述要求，本例中使用如下方式实现：

- 使用 IPv4 到 IPv6 源地址动态地址转换策略，将 IPv4 报文的源地址转换为 IPv6 地址。
- 通过 IPv6 到 IPv4 的源地址静态转换策略为 IPv6 Internet 上服务器的 IPv6 地址指定一个对应的 IPv4 地址，Device 收到发往该 IPv4 地址的报文时将其转换为对应的 IPv6 地址。

2. 组网图

图1-10 IPv4 网络访问 IPv6 Internet 中的服务器配置组网图



3. 配置步骤

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 10.1.1.3 24
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 将接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 1/0/1
[Device-security-zone-Trust] quit
[Device] security-zone name untrust
[Device-security-zone-Untrust] import interface gigabitethernet 1/0/2
[Device-security-zone-Untrust] quit
```

(3) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达 Server 所在网络的下一跳 IPv6 地址为 2014::100，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ipv6 route-static 2013:0:ff14:0101:100:: 64 2014::100
```

(4) 配置安全策略

配置名称为 aftlocalin 的安全策略，使 Device 能对 Host 访问 Server 的报文进行 AFT 转换，具体配置步骤如下。

```
[Device] security-policy ip
[Device-security-policy-ip] rule name aftlocalin
[Device-security-policy-ip-1-aftlocalin] source-zone trust
```

```
[Device-security-policy-ip-1-aftlocalin] destination-zone local
[Device-security-policy-ip-1-aftlocalin] source-ip-subnet 10.1.1.0 24
[Device-security-policy-ip-1-aftlocalin] destination-ip-host 20.1.1.1
[Device-security-policy-ip-1-aftlocalin] action pass
[Device-security-policy-ip-1-aftlocalin] quit
[Device-security-policy-ip] quit
```

配置名称为 **aftlocalout** 的安全策略，允许将 AFT 转换后的报文转发至 Server，具体配置步骤如下。

```
[Device] security-policy ipv6
[Device-security-policy-ipv6] rule name aftlocalout
[Device-security-policy-ipv6-1-aftlocalout] source-zone local
[Device-security-policy-ipv6-1-aftlocalout] destination-zone untrust
[Device-security-policy-ipv6-1-aftlocalout] source-ip-subnet 2012:: 96
[Device-security-policy-ipv6-1-aftlocalout] destination-ip-host
2013:0:ff14:0101:100::1
[Device-security-policy-ipv6-1-aftlocalout] action pass
[Device-security-policy-ipv6-1-aftlocalout] quit
[Device-security-policy-ipv6] quit
```

(5) 配置 AFT 功能

配置 ACL 2000，仅允许 IPv4 网络中 10.1.1.0/24 网段的用户可以访问 IPv6 Internet。

```
[Device] acl basic 2000
[Device-acl-ipv4-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[Device-acl-ipv4-basic-2000] rule deny
[Device-acl-ipv4-basic-2000] quit
```

配置 NAT64 前缀，此前缀将在 IPv4 到 IPv6 源地址动态转换策略中被调用，将报文的源地址转换为 IPv6 地址。

```
[Device] aft prefix-nat64 2012:: 96
```

配置 IPv4 到 IPv6 源地址动态转换策略，将匹配 ACL 2000 报文的源地址根据 NAT64 前缀转换为 IPv6 地址。

```
[Device] aft v4tov6 source acl number 2000 prefix-nat64 2012:: 96
```

配置 IPv6 到 IPv4 的源地址静态转换策略，用于将报文的目的地址转换为 IPv6 地址。

```
[Device] aft v6tov4 source 2013:0:ff14:0101:100::1 20.1.1.1
```

在设备 IPv4 侧和 IPv6 侧接口开启 AFT。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] aft enable
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] aft enable
[Device-GigabitEthernet1/0/2] quit
```

4. 验证配置

以上配置完成后, 检查 IPv4 host 与 IPv6 server 的连通性。以 IPv4 host A ping IPv6 server 为例:

```
D:\>ping 20.1.1.1

Pinging 20.1.1.1 with 32 bytes of data:

Reply from 20.1.1.1: bytes=32 time=14ms TTL=63
Reply from 20.1.1.1: bytes=32 time=1ms TTL=63
Reply from 20.1.1.1: bytes=32 time=1ms TTL=63
Reply from 20.1.1.1: bytes=32 time=1ms TTL=63
```

通过查看 AFT 会话, 可以看到创建了一个 IPv4 会话和 IPv6 会话, 分别对应转换前和转换后的报文。

```
[Device] display aft session ipv4 verbose

Initiator:

  Source      IP/port: 10.1.1.1/1025
  Destination IP/port: 20.1.1.1/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Trust

Responder:

  Source      IP/port: 20.1.1.1/1025
  Destination IP/port: 10.1.1.1/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Local

State: ICMP_REPLY
Application: ICMP
Rule ID: -/-/-
Rule name:

Start time: 2014-03-13 08:52:59  TTL: 27s

Initiator->Responder:          4 packets          240 bytes
Responder->Initiator:          4 packets          240 bytes

Total sessions found: 1

[Device] display aft session ipv6 verbose
```

```

Initiator:
    Source      IP/port: 2012::0A01:0101/0
    Destination IP/port: 2013:0:FF14:0101:0100::/32768
    VPN instance/VLAN ID/Inline ID: -/-/-
    Protocol: IPV6-ICMP(58)
    Inbound interface: GigabitEthernet1/0/1
    Source security zone: Local
Responder:
    Source      IP/port: 2013:0:FF14:0101:0100::/0
    Destination IP/port: 2012::0A01:0101/33024
    VPN instance/VLAN ID/Inline ID: -/-/-
    Protocol: IPV6-ICMP(58)
    Inbound interface: GigabitEthernet1/0/2
    Source security zone: Untrust
State: ICMPV6_REPLY
Application: ICMP
Rule ID: 0
Rule name: aftlocalout
Start time: 2014-03-13 08:52:59  TTL: 23s
Initiator->Responder:          4 packets          320 bytes
Responder->Initiator:          4 packets          320 bytes

Total sessions found: 1

```

1.20.5 IPv6 Internet 访问 IPv4 网络配置举例

1. 组网需求

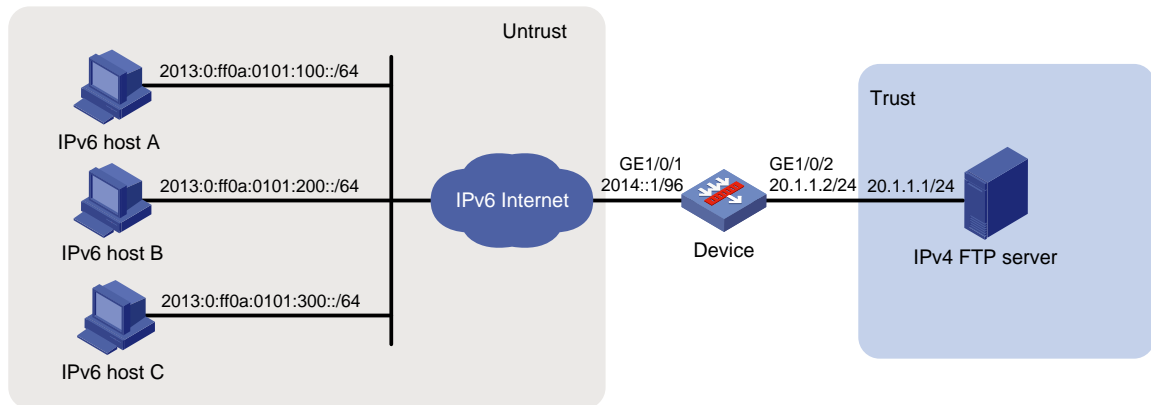
Internet 已经升级到了 IPv6, 但是某公司内部网络仍然是 IPv4 网络。而该公司仍希望为 IPv6 Internet 内的用户提供 FTP 服务。该公司访问 IPv6 Internet 使用的 IPv6 地址为 2012::1。

为满足上述要求, 实现方式如下:

- 通过 IPv4 到 IPv6 源地址静态转换策略, 为 IPv4 网络中的 FTP 服务器地址指定一个对应的 IPv6 地址, IPv6 Internet 中的主机通过访问该 IPv6 地址可以访问 IPv4 网络中的 FTP 服务器。Device 收到发往该 IPv6 地址的报文时将其目的地址转换为对应的 IPv4 地址。
- 通过 IPv6 到 IPv4 源地址动态转换策略, 将 IPv6 Internet 发送过来的 IPv6 报文源地址转换为 IPv4 地址 30.1.1.1 和 30.1.1.2。

2. 组网图

图1-11 IPv6 Internet 访问 IPv4 网络配置组网图



3. 配置步骤

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ipv6 address 2014::1 96
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 将接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 1/0/2
[Device-security-zone-Trust] quit
[Device] security-zone name untrust
[Device-security-zone-Untrust] import interface gigabitethernet 1/0/1
[Device-security-zone-Untrust] quit
```

(3) 配置安全策略

配置名称为 **aftlocalin** 的安全策略，使 Device 能对 Host 访问 Server 的报文进行 AFT 转换，具体配置步骤如下。

```
[Device] security-policy ipv6
[Device-security-policy-ipv6] rule name aftlocalin
[Device-security-policy-ipv6-1-aftlocalin] source-zone untrust
[Device-security-policy-ipv6-1-aftlocalin] destination-zone local
[Device-security-policy-ipv6-1-aftlocalin] destination-ip-host 2012::1
[Device-security-policy-ipv6-1-aftlocalin] action pass
[Device-security-policy-ipv6-1-aftlocalin] quit
```

```
[Device-security-policy-ipv6] quit
```

配置名称为 **aftlocalout** 的安全策略，允许将 AFT 转换后的报文转发至 Server，具体配置步骤如下。

```
[Device] security-policy ip
```

```
[Device-security-policy-ip] rule name aftlocalout
```

```
[Device-security-policy-ip-1-aftlocalout] source-zone local
```

```
[Device-security-policy-ip-1-aftlocalout] destination-zone trust
```

```
[Device-security-policy-ip-1-aftlocalout] source-ip-host 30.1.1.1
```

```
[Device-security-policy-ip-1-aftlocalout] source-ip-host 30.1.1.2
```

```
[Device-security-policy-ip-1-aftlocalout] destination-ip-host 20.1.1.1
```

```
[Device-security-policy-ip-1-aftlocalout] action pass
```

```
[Device-security-policy-ip-1-aftlocalout] quit
```

```
[Device-security-policy-ip] quit
```

(4) 配置 AFT 功能

配置 IPv4 到 IPv6 源地址静态转换策略，手动指定 IPv4 与 IPv6 地址一一对应的转换关系，此策略可将报文的目的地址转换为对应的 IPv4 地址。

```
[Device] aft v4tov6 source 20.1.1.1 2012::1
```

配置地址组 0 包含 2 个 IPv4 地址：30.1.1.1 和 30.1.1.2。

```
[Device] aft address-group 0
```

```
[Device-aft-address-group-0] address 30.1.1.1 30.1.1.2
```

```
[Device-aft-address-group-0] quit
```

配置 IPv6 ACL 2000，匹配 IPv6 网络到 IPv4 网络的报文。此处允许所有 IPv6 网络内主机访问 IPv4 FTP Server。

```
[Device] acl ipv6 basic 2000
```

```
[Device-acl-ipv6-basic-2000] rule permit
```

```
[Device-acl-ipv6-basic-2000] quit
```

配置 IPv6 到 IPv4 的源地址动态转换策略，将匹配 ACL 2000 的 IPv6 报文源地址转换为地址组 0 中的 IPv4 地址 30.1.1.1 或 30.1.1.2。

```
[Device] aft v6tov4 source acl ipv6 number 2000 address-group 0
```

在设备 IPv6 侧和 IPv4 侧接口 GigabitEthernet1/0/1 开启 AFT。

```
[Device] interface gigabitethernet 1/0/1
```

```
[Device-GigabitEthernet1/0/1] aft enable
```

```
[Device-GigabitEthernet1/0/1] quit
```

```
[Device] interface gigabitethernet 1/0/2
```

```
[Device-GigabitEthernet1/0/2] aft enable
```

```
[Device-GigabitEthernet1/0/2] quit
```

4. 验证配置

以上配置完成后，检查 IPv6 host 与 IPv4 FTP server 的连通性。以 IPv6 host A ping IPv4 FTP server 为例：

```
D:\>ping 2012::1

Pinging 2012::1 with 32 bytes of data:
Reply from 2012::1: time=3ms
Reply from 2012::1: time=3ms
Reply from 2012::1: time=3ms
Reply from 2012::1: time=3ms
```

通过查看 AFT 会话，可以看到创建了一个 IPv6 会话和 IPv4 会话，分别对应转换前和转换后的报文。

```
[Device] display aft session ipv6 verbose
Initiator:
  Source      IP/port: 2013:0:FF0A:0101:0100::/1029
  Destination IP/port: 2012::1/21
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: IPV6-ICMP(58)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Untrust
Responder:
  Source      IP/port: 2012::1/21
  Destination IP/port: 2013:0:FF0A:0101:0100::/1029
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: IPV6-ICMP(58)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Local
State: ICMPV6_REPLY
Application: ICMP
Rule ID: -/-/-
Rule name:
Start time: 2014-03-13 09:07:30  TTL: 3582s
Initiator->Responder:          3 packets          184 bytes
Responder->Initiator:          2 packets          148 bytes

Total sessions found: 1

[Device] display aft session ipv4 verbose
Initiator:
```



```
Source      IP/port: 30.1.1.1/11025
Destination IP/port: 20.1.1.1/21
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: ICMP(1)
Inbound interface: GigabitEthernet1/0/1
Source security zone: Local
Responder:
Source      IP/port: 20.1.1.1/21
Destination IP/port: 30.1.1.1/11025
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: ICMP(1)
Inbound interface: GigabitEthernet1/0/2
Source security zone: Trust
State: ICMP_REPLY
Application: ICMP
Rule ID: 0
Rule name: aftlocalout
Start time: 2014-03-13 09:07:30  TTL: 3577s
Initiator->Responder:      3 packets      124 bytes
Responder->Initiator:      2 packets      108 bytes

Total sessions found: 1
```

目 录

1 NAT66.....	1-1
1.1 NAT66 简介	1-1
1.1.1 IPv6 源地址转换的前缀映射	1-1
1.1.2 IPv6 目的地址转换的前缀映射	1-1
1.2 NAT66 支持 ALG	1-1
1.3 vSystem 相关说明	1-2
1.4 配置 IPv6 源地址转换的前缀映射关系	1-2
1.5 配置 IPv6 目的地址转换的前缀映射关系	1-2
1.6 NAT66 显示和维护	1-3
1.7 NAT66 典型配置举例	1-3
1.7.1 IPv6 内网用户通过转换后的地址前缀访问外网配置举例	1-3
1.7.2 IPv6 外网用户通过转换后的地址前缀访问内网服务器配置举例	1-5
1.8 NAT66 典型配置举例	1-7
1.8.1 IPv6 内网用户通过转换后的地址前缀访问外网配置举例（单个内部网络和外部网络）	1-7
1.8.2 IPv6 内网用户通过转换后的地址前缀访问外网配置举例（多宿主）	1-10
1.8.3 IPv6 外网用户通过转换后的地址前缀访问内网服务器配置举例	1-15

1 NAT66

1.1 NAT66简介

NPTv6（IPv6-to-IPv6 Network Prefix Translation，IPv6-to-IPv6 网络前缀转换）是基于 IPv6 网络的地址转换技术，用于将 IPv6 报文中的 IPv6 地址前缀转换为另一个 IPv6 地址前缀。我们将这种地址转换方式称为 NAT66。支持 NAT66 功能的设备称为 NAT66 设备，可提供 NAT66 源地址转换功能和目的地址转换功能。

1.1.1 IPv6 源地址转换的前缀映射

NAT66 源地址转换功能主要应用在如下场景中：

- 单个内部网络和外部网络。使用 NAT66 设备连接单个内部网络和公网，内部网络中的主机使用仅支持在本地范围内路由的 IPv6 地址前缀。当内部网络中的主机访问外部网络时，报文中的源 IPv6 地址前缀将被 NAT66 设备转换为全球单播 IPv6 地址前缀。
- 冗余和负载分担。一个 IPv6 网络去往另外一个 IPv6 网络的边缘位置存在多个 NAT66 设备，通过 NAT66 设备去往另一个 IPv6 网络的路径形成了等价路由，流量可以在这些 NAT66 设备上进行负载分担。这种情况下，可以在这些 NAT66 设备上配置相同的源地址转换规则，使得任意一台 NAT66 设备都可以处理不同站点间的 IPv6 流量。
- 多宿主。在多宿主的网络环境中，NAT66 设备连接一个内部网络，同时连接到不同的外部网络。可以在 NAT66 设备的各个外网侧接口上配置地址转换，将同一个内网地址转换成不同的外网地址，实现同一个内部地址到多个外部地址的映射。

1.1.2 IPv6 目的地址转换的前缀映射

NAT66 目的地址转换功能用于内网中的服务器对外部网络提供服务的场景中，例如给外部网络提供 Web 服务，或是 FTP 服务。通过在 NAT66 设备外网侧接口上配置内部服务器地址和外网地址的映射关系，外部网络用户能够通过指定的外网地址来访问内网服务器。

1.2 NAT66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，NAT66 只对报文头中的 IPv6 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 IPv6 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。

目前，NAT66 支持对 FTP 报文和 ICMP 差错报文进行 ALG 处理。

1.3 vSystem相关说明

vSystem 支持本特性的所有功能。有关 vSystem 的详细介绍请参见“虚拟化技术配置指导”中的“vSystem”。

1.4 配置IPv6源地址转换的前缀映射关系

1. 配置限制和指导

在同一个接口下，一个内网地址前缀和一个外网地址前缀必须是一对一的唯一映射关系。

不同接口下，不同的内网地址前缀不能映射到同一个外网地址前缀。

使用不进行端口转换的源地址转换方式时，需要保证转换前后的源 IPv6 地址前缀长度一致。

转换后的源 IPv6 地址前缀不能与 NAT66 设备的外网地址前缀以及目的外网地址前缀相同。

可以使用全局 NAT 策略实现 IPv6 源地址的前缀映射。关于全局 NAT 策略实现 IPv6 源地址前缀映射的详细介绍，请参见“三层技术-IP 业务配置指导”中的“配置 NAT”。

不支持对 AH 和 ESP 协议的报文进行 NAT66 源地址转换。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置 IPv6 源地址转换的前缀映射关系。

```
nat66 prefix source original-ipv6-prefix prefix-length [ vpn-instance  
original-vpn-instance-name ] translated-ipv6-prefix prefix-length  
[ vpn-instance translated-vpn-instance-name ] [ pat ]
```

缺省情况下，未配置 IPv6 源地址转换前缀映射关系。

1.5 配置IPv6目的地址转换的前缀映射关系

1. 配置限制和指导

在同一个接口下，一个内网地址前缀和一个外网地址前缀必须是一对一的唯一映射关系。

不同接口下，同一个外网地址前缀不能映射为不同的内网地址前缀。

内部服务器向外提供服务时对外公布的外网 IPv6 地址前缀不能与 NAT66 设备的外网地址前缀以及访问内部服务器的外网主机地址前缀相同。

可以使用全局 NAT 策略实现 IPv6 目的地址的前缀映射。关于全局 NAT 策略实现 IPv6 目的地址前缀映射的详细介绍，请参见“三层技术-IP 业务配置指导”中的“配置 NAT”。

不支持对 AH 和 ESP 协议的报文进行 NAT66 目的地址转换。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置 IPv6 目的地址转换的前缀映射关系。

```
nat66 prefix destination [ protocol pro-type ] original-ipv6-prefix  
prefix-length [ global-port ] [ vpn-instance  
original-vpn-instance-name ] translated-ipv6-prefix prefix-length  
[ local-port ] [ vpn-instance translated-vpn-instance-name ]
```

缺省情况下，未配置 IPv6 目的地址转换的前缀映射关系。

1.6 NAT66显示和维护

表1-1 NAT66 显示和维护

操作	命令
显示所有的NAT66配置信息	display nat66 all
显示NAT66会话，即经过NAT66地址转换处理的会话	(独立运行模式) display nat66 session [slot slot-number [cpu cpu-number]] [verbose] (IRF模式) display nat66 session [chassis chassis-number slot slot-number [cpu cpu-number]] [verbose]
显示NAT66统计信息	(独立运行模式) display nat66 statistics [summary] [slot slot-number [cpu cpu-number]] (IRF模式) display nat66 statistics [summary] [chassis chassis-number slot slot-number [cpu cpu-number]]
删除NAT66会话	(独立运行模式) reset nat66 session [slot slot-number [cpu cpu-number]] (IRF模式) reset nat66 session [chassis chassis-number slot slot-number [cpu cpu-number]]

1.7 NAT66典型配置举例

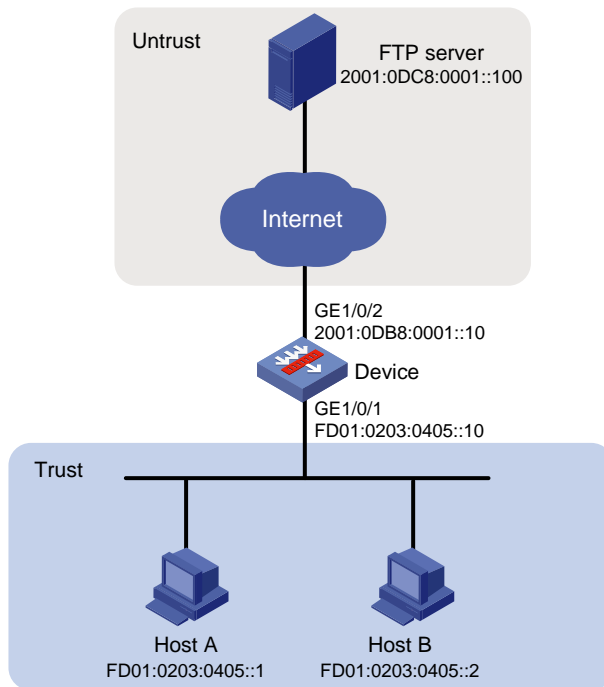
1.7.1 IPv6 内网用户通过转换后的地址前缀访问外网配置举例

1. 组网需求

某公司为了隐藏内部网络，为用户分配的 IPv6 地址的前缀为 FD01:0203:0405::/48，使用该地址前缀的 IPv6 地址为唯一本地地址，不可在互联网上路由。为了使内网网络用户能够访问互联网上的 FTP 服务器，将内网用户使用的 IPv6 地址前缀转换为 2001:0DF8:0001::/48。

2. 组网图

图1-1 IPv6 内网用户通过转换后的地址前缀访问外网配置组网图



3. 配置步骤

配置接口 IPv6 地址、路由、安全域及安全策略保证网络可达，具体配置步骤略。

配置 IPv6 源地址转换的前缀映射关系，将 IPv6 地址前缀 FD01:0203:0405::/48 转换为 2001:0DF8:0001::/48。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] nat66 prefix source fd01:0203:0405:: 48 2001:0df8:0001:: 48
[Device-GigabitEthernet1/0/2] quit
```

4. 验证配置

以上配置完成后，内网主机能够访问 FTP server。通过查看如下显示信息，可以验证以上配置成功。

```
[Device] display nat66 all
NAT66 source information:
  Totally 1 source rules.
  Interface(outbound): GigabitEthernet1/0/2
  Original prefix/prefix-length: FD01:203:405::/48
  Translated prefix/prefix-length: 2001:DF8:1::/48
```

通过以下显示命令，可以看到内部主机访问外部 FTP server 时生成 NAT66 会话信息。

```
<Device> display nat66 session verbose
```

```

Slot 1:

Initiator:

  Source      IP/port: FD01:203:405::1/56002
  Destination IP/port: 2001:DC8:1::100/21
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Trust

Responder:

  Source      IP/port: 2001:DC8:1::100/21
  Destination IP/port: 2001:DF8:1:D50F::1/56002
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Untrust

State: TCP_ESTABLISHED
Application: FTP
Rule ID: 1
Rule name: 1
Start time: 2018-12-06 14:48:31  TTL: 3597s

Initiator->Responder:      0 packets      0 bytes
Responder->Initiator:      0 packets      0 bytes

Total sessions found: 1

```

1.7.2 IPv6 外网用户通过转换后的地址前缀访问内网服务器配置举例

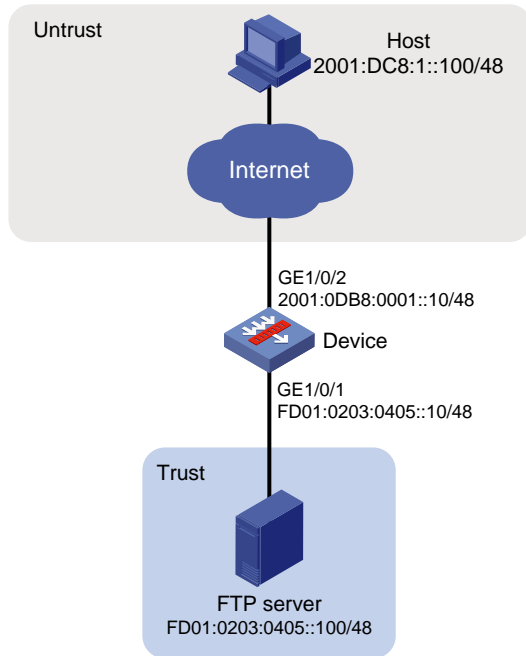
1. 组网需求

某公司内部对外提供 FTP 服务。公司内部使用的 IPv6 地址前缀为 FD01:0203:0405::/48。其中，内部 FTP 服务器地址为 FD01:0203:0405::100/48。要实现如下功能：

- 外部的主机可以访问内部的 FTP 服务器。
- 使用 2001:AB01:0001::1 作为公司对外提供服务的 IPv6 地址。

2. 组网图

图1-2 IPv6 外网用户通过转换后的地址前缀访问内网服务器配置组网图



3. 配置步骤

配置接口 IPv6 地址、路由、安全域及安全策略保证网络可达，具体配置步骤略。

配置 IPv6 目的地址转换的前缀映射关系，将 IPv6 地址前缀 2001:AB01:0001::1/128 转换为 FD01:0203:0405::100/128。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] nat66 prefix destination 2001:ab01:1::1 128 fd01:203:405::100 128
[Device-GigabitEthernet1/0/2] quit
```

4. 验证配置

以上配置完成后，外部主机能够访问 FTP server。通过查看如下显示信息，可以验证以上配置成功。

```
[Device] display nat66 all
NAT66 destination information:
  Totally 1 destination rules.
  Interface(inbound): GigabitEthernet1/0/2
  Original prefix/prefix-length: 2001:AB01:1::1/128
  Translated prefix/prefix-length: FD01:203:405::100/128
```

通过以下显示命令，可以看到外部主机访问内部 FTP server 时生成 NAT 会话信息。

```
[Device] display nat66 session verbose
Slot 1:
```



```

Initiator:
    Source      IP/port: 2001:DC8:1::100/9025
    Destination IP/port: 2001:AB01:1::1/21
    VPN instance/VLAN ID/Inline ID: -/-/-
    Protocol: TCP(6)
    Inbound interface: GigabitEthernet1/0/2
    Source security zone: Untrust
Responder:
    Source      IP/port: FD01:203:405::100/21
    Destination IP/port: 2001:DC8:1::100/9025
    VPN instance/VLAN ID/Inline ID: -/-/-
    Protocol: TCP(6)
    Inbound interface: GigabitEthernet1/0/1
    Source security zone: Trust
State: TCP_ESTABLISHED
Application: FTP
Rule ID: 1
Rule name: 1
Start time: 2018-12-06 14:56:03  TTL: 3579s
Initiator->Responder:      0 packets      0 bytes
Responder->Initiator:      0 packets      0 bytes

Total sessions found: 1

```

1.8 NAT66典型配置举例

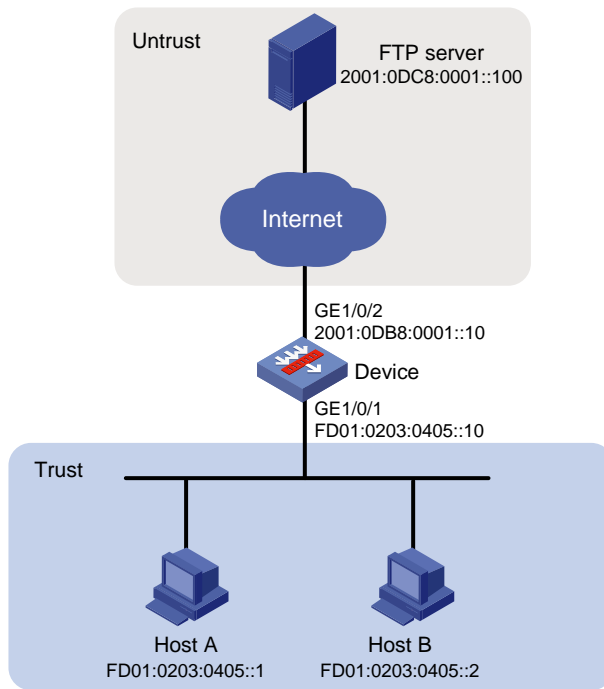
1.8.1 IPv6 内网用户通过转换后的地址前缀访问外网配置举例（单个内部网络和外部网络）

1. 组网需求

某公司为了隐藏内部网络，为用户分配的 IPv6 地址的前缀为 FD01:0203:0405::/48，使用该地址前缀的 IPv6 地址为唯一本地地址，不可在互联网上路由。为了使内网网络用户能够访问互联网上的 FTP 服务器，将内网用户使用的 IPv6 地址前缀转换为 2001:0DF8:0001::/48。

2. 组网图

图1-3 IPv6 内网用户通过转换后的地址前缀访问外网配置组网图（单个内部网络和外部网络）



3. 配置步骤

(1) 配置接口 IPv6 地址

根据组网图中规划的信息，配置各接口的 IPv6 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ipv6 address FD01:0203:0405::10 48
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达 FTP 服务器所在网络的下一跳 IP 地址为 2001:0DB8:0001::11，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ipv6 route-static 2001:0DC8:0001::100 48 2001:0DB8:0001::11
```

(3) 将接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 1/0/1
[Device-security-zone-Trust] quit
[Device] security-zone name untrust
```

```
[Device-security-zone-Untrust] import interface gigabitethernet 1/0/2
[Device-security-zone-Untrust] quit
```

(4) 配置安全策略

配置名称为 trust-untrust 的安全策略，保证 Trust 安全域内的 Host A 和 Host B 可以访问 Internet 中的 FTP Server，具体配置步骤如下。

```
[Device] security-policy ipv6
[Device-security-policy-ipv6] rule 1 name trust-untrust
[Device-security-policy-ipv6-1-trust-untrust] source-zone trust
[Device-security-policy-ipv6-1-trust-untrust] destination-zone untrust
[Device-security-policy-ipv6-1-trust-untrust] source-ip-host FD01:0203:0405::1
[Device-security-policy-ipv6-1-trust-untrust] source-ip-host FD01:0203:0405::2
[Device-security-policy-ipv6-1-trust-untrust] destination-ip-host
2001:0DC8:0001::100
[Device-security-policy-ipv6-1-trust-untrust] action pass
[Device-security-policy-ipv6-1-trust-untrust] quit
[Device-security-policy-ipv6] quit
```

(5) 配置 NAT66 前缀转换功能

配置 IPv6 源地址转换的前缀映射关系，将 IPv6 地址前缀 FD01:0203:0405::/48 转换为 2001:0DF8:0001::/48。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] nat66 prefix source fd01:0203:0405:: 48 2001:0df8:0001::
48
[Device-GigabitEthernet1/0/2] quit
```

4. 验证配置

以上配置完成后，内网主机能够访问 FTP server。通过查看如下显示信息，可以验证以上配置成功。

```
[Device] display nat66 all
NAT66 source information:
  Totally 1 source rules.
  Interface(outbound): GigabitEthernet1/0/2
  Original prefix/prefix-length: FD01:203:405::/48
  Translated prefix/prefix-length: 2001:DF8:1::/48
```

通过以下显示命令，可以看到内部主机访问外部 FTP server 时生成 NAT66 会话信息。

```
<Device> display nat66 session verbose
Slot 1:
Initiator:
  Source      IP/port: FD01:203:405::1/56002
  Destination IP/port: 2001:DC8:1::100/21
```

```

VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/1
Source security zone: Trust
Responder:
Source      IP/port: 2001:DC8:1::100/21
Destination IP/port: 2001:DF8:1:D50F::1/56002
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/2
Source security zone: Untrust
State: TCP_ESTABLISHED
Application: FTP
Rule ID: 1
Rule name: 1
Start time: 2018-12-06 14:48:31  TTL: 3597s
Initiator->Responder:          0 packets          0 bytes
Responder->Initiator:          0 packets          0 bytes

Total sessions found: 1

```

1.8.2 IPv6 内网用户通过转换后的地址前缀访问外网配置举例（多宿主）

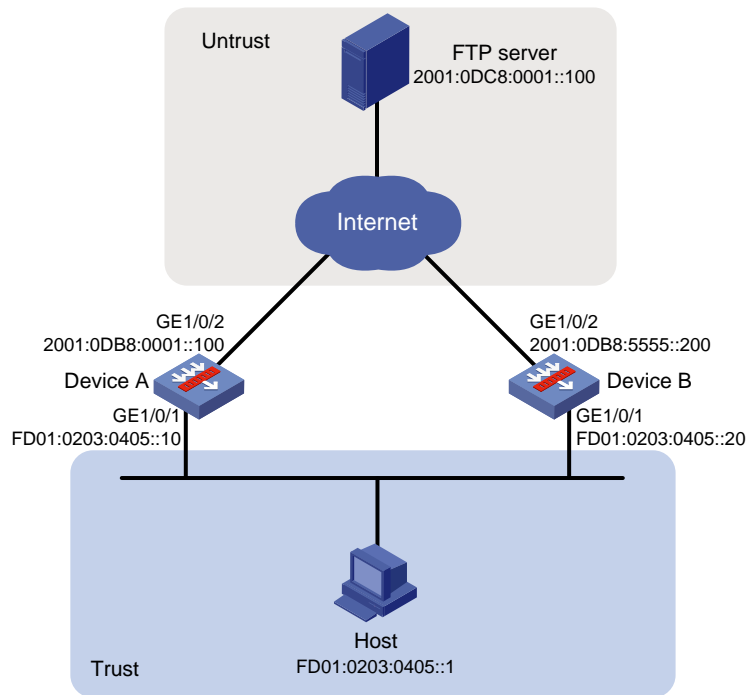
1. 组网需求

某公司为了隐藏内部网络，为用户分配的 IPv6 地址的前缀为 FD01:0203:0405::/48，使用该地址前缀的 IPv6 地址为唯一本地地址，不可在互联网上路由。

两台 NAT66 设备连接同一个内部网络，同时连接到不同的外部网络。分别在两台 NAT66 设备的外网侧接口上配置地址转换，将同一个内网地址转换成不同的外网地址，实现同一个内部地址到多个外部地址的映射。

2. 组网图

图1-4 IPv6 内网用户通过转换后的地址前缀访问外网配置组网图（多宿主）



3. 配置 Device A

(1) 配置接口 IPv6 地址

根据组网图中规划的信息，配置各接口的 IPv6 地址，具体配置步骤如下。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ipv6 address FD01:0203:0405::10 48
[DeviceA-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达 FTP 服务器所在网络的下一跳 IP 地址为 2001:0DB8:0001::11，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[DeviceA] ipv6 route-static 2001:0DC8:0001::100 48 2001:0DB8:0001::11
```

(3) 将接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[DeviceA] security-zone name trust
[DeviceA-security-zone-Trust] import interface gigabitethernet 1/0/1
[DeviceA-security-zone-Trust] quit
[DeviceA] security-zone name untrust
```

```
[DeviceA-security-zone-Untrust] import interface gigabitethernet 1/0/2
[DeviceA-security-zone-Untrust] quit
```

(4) 配置安全策略

配置名称为 trust-untrust 的安全策略，保证 Trust 安全域内的 Host 可以访问 Internet 中的 FTP Server，具体配置步骤如下。

```
[DeviceA] security-policy ipv6
[DeviceA-security-policy-ipv6] rule name trust-untrust
[DeviceA-security-policy-ipv6-1-trust-untrust] source-zone trust
[DeviceA-security-policy-ipv6-1-trust-untrust] destination-zone untrust
[DeviceA-security-policy-ipv6-1-trust-untrust] source-ip-host FD01:0203:0405::1
[DeviceA-security-policy-ipv6-1-trust-untrust] destination-ip-host
2001:0DC8:0001::100
[DeviceA-security-policy-ipv6-1-trust-untrust] action pass
[DeviceA-security-policy-ipv6-1-trust-untrust] quit
[DeviceA-security-policy-ipv6] quit
```

(5) 配置 NAT66 前缀转换功能

配置 IPv6 源地址转换的前缀映射关系，将 IPv6 地址前缀 FD01:0203:0405::/48 转换为 2001:0DF8:0001::/48。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] nat66 prefix source fd01:0203:0405:: 48 2001:0df8:0001::
48
[DeviceA-GigabitEthernet1/0/2] quit
```

4. 配置 Device B

(1) 配置接口 IPv6 地址

根据组网图中规划的信息，配置各接口的 IPv6 地址，具体配置步骤如下。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ipv6 address FD01:0203:0405::20 48
[DeviceB-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达 FTP 服务器所在网络的下一跳 IP 地址为 2001:0DB8:5555::11，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[DeviceB] ipv6 route-static 2001:0DC8:0001::100 48 2001:0DB8:5555::11
```

(3) 将接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[DeviceB] security-zone name trust
```

```
[DeviceB-security-zone-Trust] import interface gigabitethernet 1/0/1
[DeviceB-security-zone-Trust] quit
[DeviceB] security-zone name untrust
[DeviceB-security-zone-Untrust] import interface gigabitethernet 1/0/2
[DeviceB-security-zone-Untrust] quit
```

(4) 配置安全策略

配置名称为 trust-untrust 的安全策略，保证 Trust 安全域内的 Host 可以访问 Internet 中的 FTP Server，具体配置步骤如下。

```
[DeviceB] security-policy ipv6
[DeviceB-security-policy-ipv6] rule name trust-untrust
[DeviceB-security-policy-ipv6-1-trust-untrust] source-zone trust
[DeviceB-security-policy-ipv6-1-trust-untrust] destination-zone untrust
[DeviceB-security-policy-ipv6-1-trust-untrust] source-ip-host FD01:0203:0405::1
[DeviceB-security-policy-ipv6-1-trust-untrust] destination-ip-host
2001:0DC8:0001::100
[DeviceB-security-policy-ipv6-1-trust-untrust] action pass
[DeviceB-security-policy-ipv6-1-trust-untrust] quit
[DeviceB-security-policy-ipv6] quit
```

(5) 配置 NAT66 前缀转换功能

配置 IPv6 源地址转换的前缀映射关系，将 IPv6 地址前缀 FD01:0203:0405::/48 转换为 2001:0DE8:0001::/48。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] nat66 prefix source fd01:0203:0405:: 48 2001:0de8:0001::
48
[DeviceB-GigabitEthernet1/0/2] quit
```

5. 验证配置

以上配置完成后，内网主机能够通过 Device A 或 Device B 访问 FTP server。对于内网主机经由不同的 NAT66 设备到达 FTP 服务器的报文，映射后的结果不同。同时，从 FTP 服务器经由不同的 NAT66 设备到达内网主机的报文，均会被 NAT66 设备映射为相同的 IPv6 地址，该地址即为内网主机的唯一本地地址。

在 Device A 上通过查看如下显示信息，可以验证以上配置成功。

```
[DeviceA] display nat66 all
NAT66 source information:
  Totally 1 source rules.
  Interface(outbound): GigabitEthernet1/0/2
  Original prefix/prefix-length: FD01:203:405::/48
  Translated prefix/prefix-length: 2001:DF8:1::/48
```

在 Device B 上通过查看如下显示信息，可以验证以上配置成功。

```
[DeviceB] display nat66 all
```

NAT66 source information:

Totally 1 source rules.

Interface(outbound): GigabitEthernet1/0/2

Original prefix/prefix-length: FD01:203:405::/48

Translated prefix/prefix-length: 2001:DE8:1::/48

在 Device A 上查看内部主机访问外部 FTP server 时生成 NAT66 会话信息。

[DeviceA] **display nat66 session verbose**

Slot 1:

Initiator:

Source IP/port: FD01:203:405::1/35990

Destination IP/port: 2001:DC8:1::100/21

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: TCP(6)

Inbound interface: GigabitEthernet1/0/1

Source security zone: Trust

Responder:

Source IP/port: 2001:DC8:1::100/21

Destination IP/port: 2001:DF8:1:D50F::1/35990

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: TCP(6)

Inbound interface: GigabitEthernet1/0/2

Source security zone: Trust

State: TCP_ESTABLISHED

Application: FTP

Rule ID: 0

Rule name: aaa

Start time: 2021-10-31 14:47:44 TTL: 3584s

Initiator->Responder: 0 packets 0 bytes

Responder->Initiator: 0 packets 0 bytes

Total sessions found: 1

在 Device B 上查看内部主机访问外部 FTP server 时生成 NAT66 会话信息。

[DeviceB] **display nat66 session verbose**

Slot 1:

Initiator:

Source IP/port: FD01:203:405::1/35992

Destination IP/port: 2001:DC8:1::100/21

VPN instance/VLAN ID/Inline ID: -/-/-


```

Protocol: TCP(6)

Inbound interface: GigabitEthernet1/0/1

Source security zone: Trust

Responder:

Source      IP/port: 2001:DC8:1::100/21

Destination IP/port: 2001:DE8:1:D51F::1/35992

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: TCP(6)

Inbound interface: GigabitEthernet1/0/2

Source security zone: Trust

State: TCP_ESTABLISHED

Application: FTP

Rule ID: 0

Rule name: aaa

Start time: 2021-10-31 14:50:03  TTL: 3594s

Initiator->Responder:          0 packets          0 bytes
Responder->Initiator:          0 packets          0 bytes

Total sessions found: 1

```

1.8.3 IPv6 外网用户通过转换后的地址前缀访问内网服务器配置举例

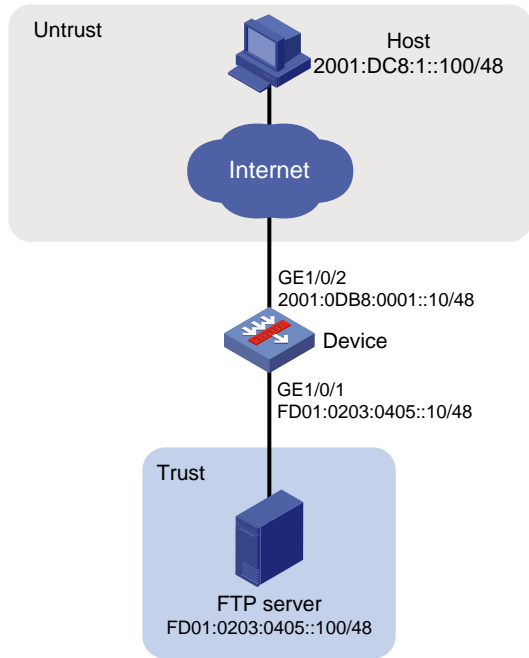
1. 组网需求

某公司内部对外提供 FTP 服务。公司内部使用的 IPv6 地址前缀为 FD01:0203:0405::/48。其中，内部 FTP 服务器地址为 FD01:0203:0405::100/48。要实现如下功能：

- 外部的主机可以访问内部的 FTP 服务器。
- 使用 2001:AB01:0001::1 作为公司对外提供服务的 IPv6 地址。

2. 组网图

图1-5 IPv6 外网用户通过转换后的地址前缀访问内网服务器配置组网图



3. 配置步骤

(1) 配置接口 IPv6 地址

根据组网图中规划的信息，配置各接口的 IPv6 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ipv6 address FD01:0203:0405::10 48
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 将接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 1/0/1
[Device-security-zone-Trust] quit
[Device] security-zone name untrust
[Device-security-zone-Untrust] import interface gigabitethernet 1/0/2
[Device-security-zone-Untrust] quit
```

(3) 配置安全策略

配置名称为 untrust-trust 的安全策略，保证 Internet 中的主机可以访问 Trust 安全域内的 FTP Server，具体配置步骤如下。

```
[Device] security-policy ipv6
```

```
[Device-security-policy-ipv6] rule 1 name untrust-trust
[Device-security-policy-ipv6-1-untrust-trust] source-zone untrust
[Device-security-policy-ipv6-1-untrust-trust] destination-zone trust
[Device-security-policy-ipv6-1-untrust-trust] destination-ip-host
FD01:0203:0405::100
[Device-security-policy-ipv6-1-untrust-trust] action pass
[Device-security-policy-ipv6-1-untrust-trust] quit
[Device-security-policy-ipv6] quit
```

(4) 配置 NAT66 前缀转换功能

配置 IPv6 目的地址转换的前缀映射关系，将 IPv6 地址前缀 2001:AB01:0001::1/128 转换为 FD01:0203:0405::100/128。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] nat66 prefix destination 2001:ab01:1::1 128
fd01:203:405::100 128
[Device-GigabitEthernet1/0/2] quit
```

4. 验证配置

以上配置完成后，外部主机能够访问 FTP server。通过查看如下显示信息，可以验证以上配置成功。

```
[Device] display nat66 all
NAT66 destination information:
  Totally 1 destination rules.
  Interface(inbound): GigabitEthernet1/0/2
  Original prefix/prefix-length: 2001:AB01:1::1/128
  Translated prefix/prefix-length: FD01:203:405::100/128
```

通过以下显示命令，可以看到外部主机访问内部 FTP server 时生成 NAT 会话信息。

```
[Device] display nat66 session verbose
Slot 1:
Initiator:
  Source      IP/port: 2001:DC8:1::100/9025
  Destination IP/port: 2001:AB01:1::1/21
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Untrust
Responder:
  Source      IP/port: FD01:203:405::100/21
  Destination IP/port: 2001:DC8:1::100/9025
  VPN instance/VLAN ID/Inline ID: -/-/-
```

```
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/1
Source security zone: Trust
State: TCP_ESTABLISHED
Application: FTP
Rule ID: 1
Rule name: 1
Start time: 2018-12-06 14:56:03  TTL: 3579s
Initiator->Responder:          0 packets          0 bytes
Responder->Initiator:          0 packets          0 bytes

Total sessions found: 1
```