目 录

5 NAT配置

通过NAT配置，实现了私网和公网地址的互相转换，解决IPv4地址短缺的问题，同时能够隐藏私网内部拓扑，提升网络的安全性。

5.1 NAT简介

5.2 原理描述

5.3 应用

5.1 NAT简介

定义

网络地址转换NAT（Network Address Translation）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。

目的

随着Internet的发展和网络应用的增多，IPv4地址枯竭已成为制约网络发展的瓶颈。尽管IPv6可以从根本上解决IPv4地址空间不足问题，但目前众多网络设备和网络应用大多是基于IPv4的，因此在IPv6广泛应用之前，一些过渡技术（如CIDR、私网地址等）的使用是解决这个问题最主要的技术手段。NAT主要用于实现内部网络（简称内网，使用私有IP地址）访问外部网络（简称外网，使用公有IP地址）的功能。当内网的主机要访问外网时，通过NAT技术可以将其私网地址转换为公网地址，可以实现多个私网用户共用一个公网地址来访问外部网络，这样既可保证网络互通，又节省了公网地址。私网地址的类型和分类请参见1.3.2 IPv4地址。

受益

作为减缓IP地址枯竭的一种过渡方案，NAT通过地址重用的方法来满足IP地址的需要，可以在一定程度上缓解IP地址空间枯竭的压力。NAT除了解决IP地址短缺的问题，还带来了两个好处：

- 有效避免来自外网的攻击，可以很大程度上提高网络安全性。
- 控制内网主机访问外网，同时也可以控制外网主机访问内网，解决了内网和外网不能互通的问题。

相关资料

视频：华为AR路由器NAT特性介绍

5.2 原理描述

5.2.1 NAT概述

NAT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，主要用于实现内部网络（私有IP地址）访问外部网络（公有IP地址）的功能。Basic NAT是实现一对一的IP地址转换，而NAPT可以实现多个私有IP地址映射到同一个公有IP地址上。

Basic NAT

Basic NAT方式属于一对一的地址转换，在这种方式下只转换IP地址，而不处理TCP/UDP协议的端口号，一个公网IP地址不能同时被多个私网用户使用。

图**5-1** Basic NAT示意图

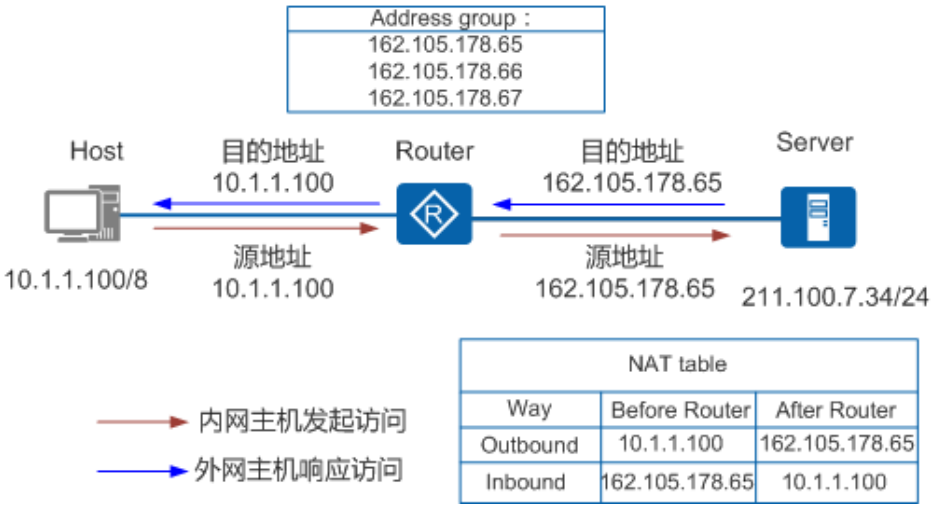


图5-1描述了Basic NAT的基本原理，实现过程如下：

1. Router收到内网侧Host发送的访问公网侧Server的报文，其源IP地址为10.1.1.100。
2. Router从地址池中选取一个空闲的公网IP地址，建立与内网侧报文源IP地址间的NAT转换表项（正反向），并依据查找正向NAT表项的结果将报文转换后向公网侧发送，其源IP地址是162.105.178.65，目的IP地址是211.100.7.34。
3. Router收到公网侧的回应报文后，根据其目的IP地址查找反向NAT表项，并依据查表结果将报文转换后向私网侧发送，其源IP地址是211.100.7.34，目的IP地址是10.1.1.100。

说明：

由于Basic NAT这种一对一的转换方式并未实现公网地址的复用，不能有效解决IP地址短缺的问题，因此在实际应用中并不常用。

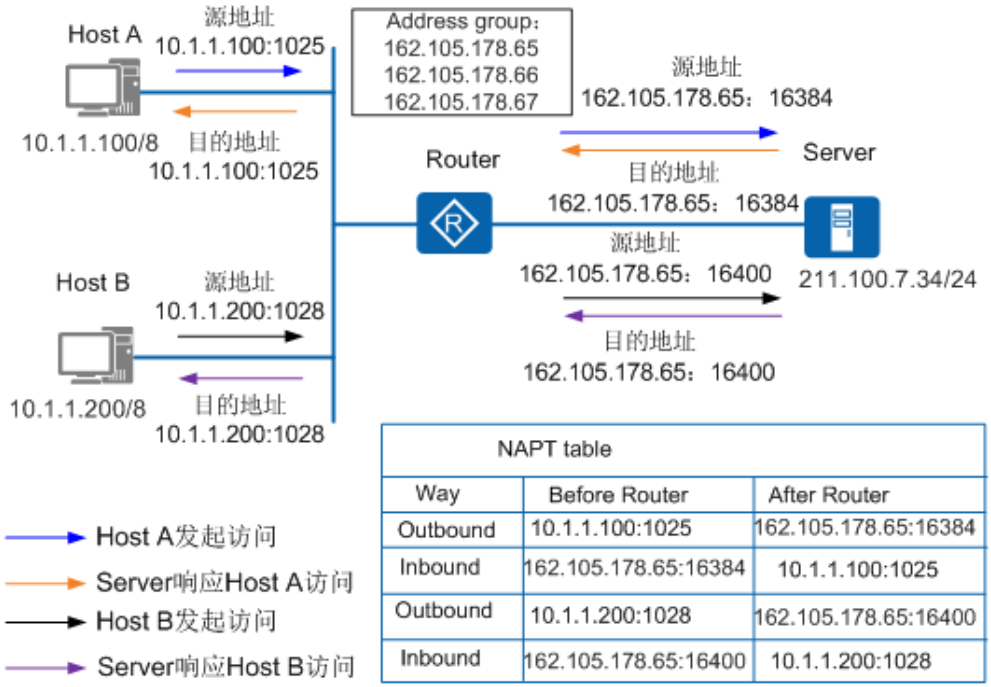
NAT设备拥有的公有IP地址数目要远少于内部网络的主机数目，这是因为所有内部主机并不会同时访问外部网络。公有IP地址数目的确定，应根据网络高峰期可能访问外部网络的内部主机数目的统计值来确定。

NAPT

除了一对一的NAT转换方式外，网络地址端口转换NAPT（Network Address Port Translation）可以实现并发的地址转换。它允许多个内部地址映射到同一个公有地址上，因此也可以称为“多对一地址转换”或地址复用。

NAPT方式属于多对一的地址转换，它通过使用“IP地址＋端口号”的形式进行转换，使多个私网用户可共用一个公网IP地址访问外网。

图**5-2** NAPT示意图



NAPT table

Way	Before Router	After Router
Outbound	10.1.1.100:1025	162.105.178.65:16384
Inbound	162.105.178.65:16384	10.1.1.100:1025
Outbound	10.1.1.200:1028	162.105.178.65:16400
Inbound	162.105.178.65:16400	10.1.1.200:1028

图5-2描述了NAPT的基本原理，实现过程如下：

1. Router收到内网侧Host发送的访问公网侧Server的报文。比如收到Host A报文的源地址是10.1.1.100，端口号1025。
2. Router从地址池中选取一对空闲的“公网IP地址＋端口号”，建立与内网侧报文“源IP地址＋源端口号”间的NAPT转换表项（正反向），并依据查找正向NAPT表项的结果将报文转换后向公网侧发送。比如Host A的报文经Router转换后的报文源地址为162.105.178.65，端口号16384。
3. Router收到公网侧的回应报文后，根据其“目的IP地址＋目的端口号”查找反向NAPT表项，并依据查表结果将报文转换后向私网侧发送。比如Server回应Host A的报文经Router转换后，目的地址为10.1.1.100，端口号1025。

5.2.2 NAT实现

Basic NAT和NAPT是私网IP地址通过NAT设备转换成公网IP地址的过程，分别实现一对一和多对一的地址转换功能。在现网环境下，NAT功能的实现还得依据Basic NAT和NAPT的原理，NAT实现主要包括：Easy IP、地址池NAT、NAT Server和静态NAT/NAPT。

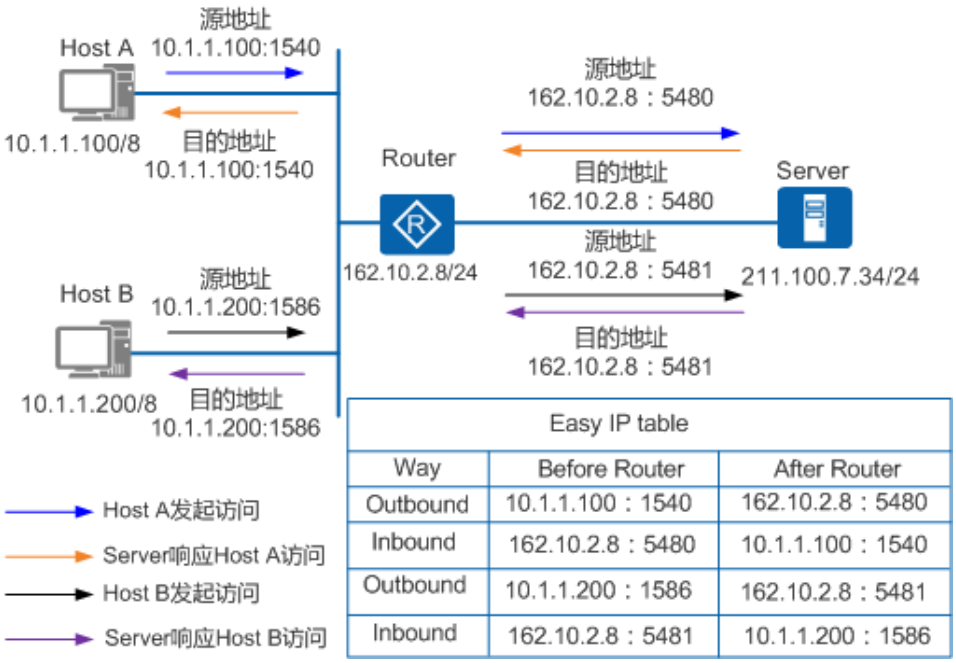
地址池NAT和Easy IP类似，此处只介绍Easy IP，关于地址池NAT相关内容请参见5.2.1 NAT概述中的NAPT。

Easy IP

Easy IP方式可以利用访问控制列表来控制哪些内部地址可以进行地址转换。

Easy IP方式特别适合小型局域网访问Internet的情况。这里的小型局域网主要指中小型网吧、小型办公室等环境，一般具有以下特点：内部主机较少、出接口通过拨号方式获得临时公网IP地址以供内部主机访问Internet。对于这种情况，可以使用Easy IP方式使局域网用户都通过这个IP地址接入Internet。

图**5-3** Easy IP示意图



Easy IP table		
Way	Before Router	After Router
Outbound	10.1.1.100：1540	162.10.2.8：5480
Inbound	162.10.2.8：5480	10.1.1.100：1540
Outbound	10.1.1.200：1586	162.10.2.8：5481
Inbound	162.10.2.8：5481	10.1.1.200：1586

如图5-3所示，Easy IP方式的处理过程如下：

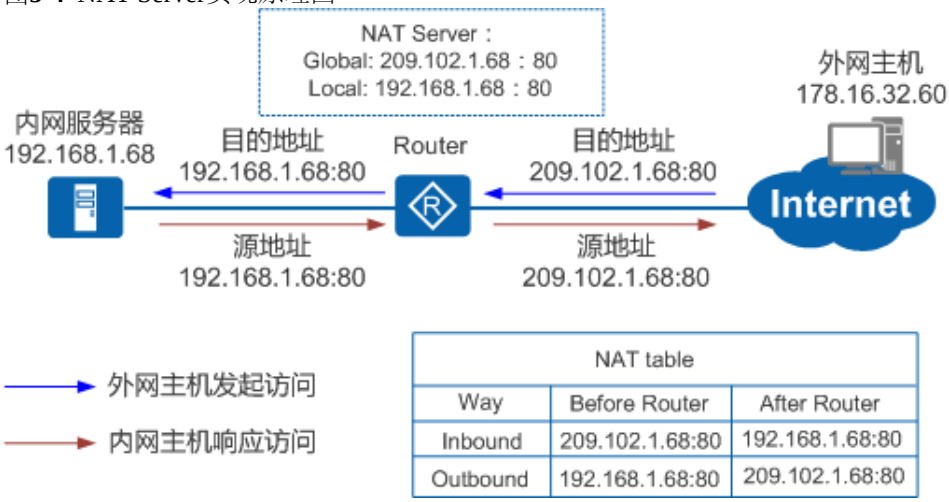
1. Router收到内网侧主机发送的访问公网侧服务器的报文。比如收到Host A报文的源地址是10.1.1.100，端口号1540。
2. Router利用公网侧接口的“公网IP地址＋端口号”，建立与内网侧报文“源IP地址＋源端口号”间的Easy IP转换表项（正反向），并依据查找正向Easy IP表项的结果将报文转换后向公网侧发送。比如Host A的报文经Router转换后的报文源地址为162.10.2.8，端口号5480。
3. Router收到公网侧的回应报文后，根据其“目的IP地址＋目的端口号”查找反向Easy IP表项，并依据查表结果将报文转换后向内网侧发送。比如Server回应Host A的报文经Router转换后，目的地址为10.1.1.100，端口号1540。

NAT Server

NAT具有“屏蔽”内部主机的作用，但有时内网需要向外网提供服务，比如提供WWW服务或者FTP服务。这种情况下需要内网的服务器不被“屏蔽”，外网用户可以随时访问内网服务器。

NAT Server可以很好地解决这个问题，当外网用户访问内网服务器时，它通过事先配置好的“公网IP地址+端口号”与“私网IP地址+端口号”间的映射关系，将服务器的“公网IP地址+端口号”根据映射关系替换成对应的“私网IP地址+端口号”。

图**5-4** NAT Server实现原理图



NAT table		
Way	Before Router	After Router
Inbound	209.102.1.68:80	192.168.1.68:80
Outbound	192.168.1.68:80	209.102.1.68:80

如图5-4所示，NAT Server的地址转换过程如下：

1. 在Router上配置NAT Server的转换表项。
2. Router收到公网用户发起的访问请求，设备根据该请求的“目的IP+端口号”查找NAT Server转换表项，找出对应的“私网IP+端口号”，然后用查找结果替换报文的“目的IP+端口号”。外网主机发送的报文，其目的地址是209.102.1.68，端口号80，经Router转换后目的地址转换为192.168.1.68，端口号80。
3. Router收到内网服务器的回应报文后，根据该回应报文的“源IP地址＋源端口号”查找NAT Server转换表项，找出对应的“公网IP+端口号”，然后用查找结果替换报文的“源IP地址＋源端口号”。内网服务器回应外网主机的报文，其源地址是192.168.1.68，端口号80，经Router转换后源地址转换为209.102.1.68，端口号80。

静态NAT/NAPT

静态NAT是指在进行NAT转换时，内部网络主机的IP同公网IP是一对一静态绑定的，静态NAT中的公网IP只会给唯一且固定的内网主机转换使用。

静态NAPT是指“内部网络主机的IP+协议号+端口号”同“公网IP+协议号+端口号”是一对一静态绑定的，静态NAPT中的公网IP可以为多个私网IP使用。

静态NAT/NAPT还支持将指定私网范围内的主机IP转换为指定的公网范围内的主机IP。当内部主机访问外部网络时，如果该主机地址在指定的内部主机地址范围内，会被转换为对应的公网地址；同样，当公网主机对内部主机进行访问时，如果该公网主机IP经过NAT转换后对应的私网IP地址在指定的内部主机地址范围内，也是可以直接访问到内部主机。

5.2.3 NAT ALG

NAT和NAPT只能对IP报文的头部地址和TCP/UDP头部的端口信息进行转换。对于一些特殊协议，例如FTP等，它们报文的数据部分可能包含IP地址信息或者端口信息，这些内容不能被NAT有效的转换。解决这些特殊协议的NAT转换问题的方法就是在NAT实现中使用应用层网关ALG（Application Level Gateway）功能。ALG是对特定的应用层协议进行转换，在对这些特定的应用层协议进行NAT转换过程中，通过NAT的状态信息来改变封装在IP报文数据部分中的特定数据，最终使应用层协议可以跨越不同范围运行。

例如，一个使用内部IP地址的FTP服务器可能在和外部网络主机建立会话的过程中需要将自己的IP地址发送给对方。而这个地址信息是放到IP报文的数据部分，NAT无法对它进行转换。当外部网络主机接收了这个私有地址并使用它，这时FTP服务器将表现为不可达。

目前支持ALG功能的协议包括：DNS、FTP、SIP、PPTP和RTSP。不同协议支持的NAT转换字段如表5-1所示。

表**5-1** 不同协议支持的NAT转换字段表

应用协议	做**NAT**变换的字段
DNS	响应报文中的IP和Port
FTP	• Port请求报文中载荷里的IP和Port • Passive响应报文中载荷里的IP和Port
SIP	• Request line • From • To • Contact • Via • O • Message body的C字段地址和M字段的端口 • record-router
PPTP	分PPTP Client在私网还是PPTP Server在私网两种场景： • PPTP Client在私网，PPTP Server在公网时，仅对Client-Call-ID进行端口替换 • PPTP Server在私网，PPTP Client在公网时，仅对Server-Call-ID进行端口替换
RTSP	setup/reply OK报文中的端口字段

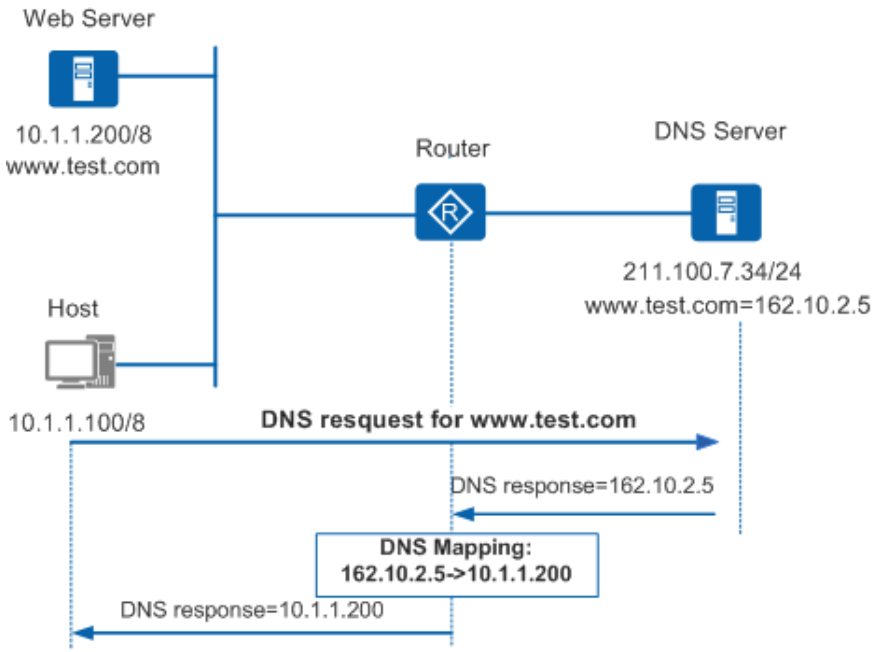
5.2.4 DNS Mapping

在某些应用中，私网用户希望通过域名访问位于同一私网的内部服务器，而DNS服务器却位于公网。由于通常DNS响应报文中携带的是内部服务器的公网IP地址，因此若NAT设备未将DNS Server解析的公网IP替换成内部服务器对应的私网IP，私网用户将无法通过域名访问到内部服务器。

这个问题可以使用DNS Mapping方式来解决，通过配置“域名—公网IP地址—公网端口—协议类型”映射表，建立内部服务器的域名与其公网信息间的对应关系。

图5-5描述了DNS Mapping的基本原理。

图**5-5** DNS Mapping示意图



如图5-5所示，私网用户Host希望通过域名方式访问Web Server，Router作为NAT服务器。当Router设备收到DNS响应报文后，先根据其中携带的域名查找DNS Mapping映射表，再根据“公网IP地址—公网端口—协议类型”查找Web Server，然后将DNS响应报文中的公网IP地址替换成Web Server的私网IP地址。这样，Host收到的DNS响应报文中就携带了Web Server的私网IP地址，从而可以通过域名来访问Web Server。

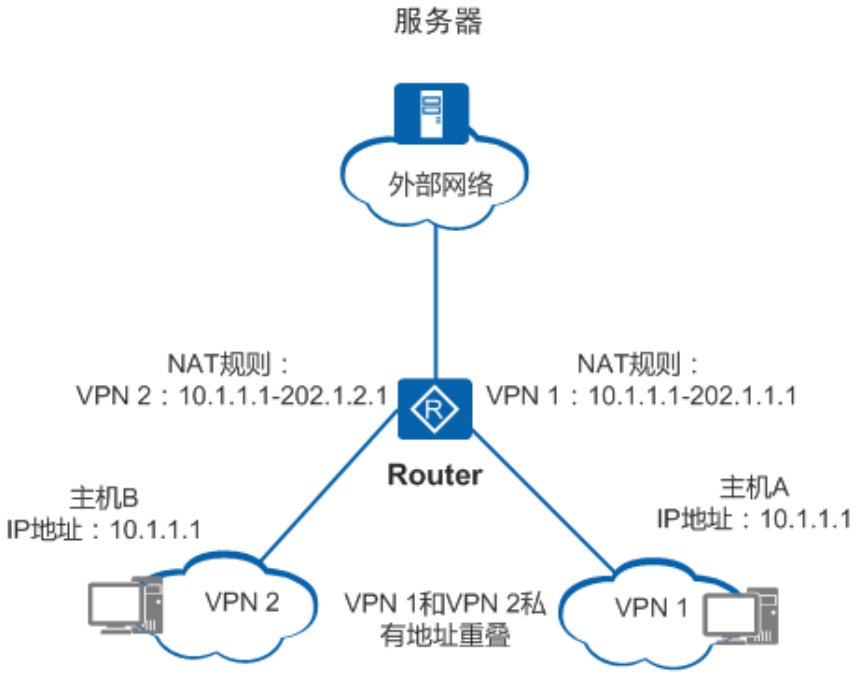
5.2.5 NAT关联VPN

NAT不仅可以使内部网络的用户访问外部网络，还允许内部网络中分属于不同VPN（Virtual Private Network）的用户通过同一个出口访问外部网络，解决内部网络中IP地址重叠的VPN同时访问外网主机的问题；NAT还支持VPN关联的NAT Server，允许外部网络中的主机访问内网中分属不同VPN的服务器，同时支持内网多个VPN地址重叠的场景。

VPN关联的源NAT

VPN关联的源NAT是指内部网络中分属于不同VPN的用户通过NAT技术访问外部网络，组网如图5-6所示。

图**5-6** VPN关联的源NAT



VPN关联的源NAT的实现方式如下：

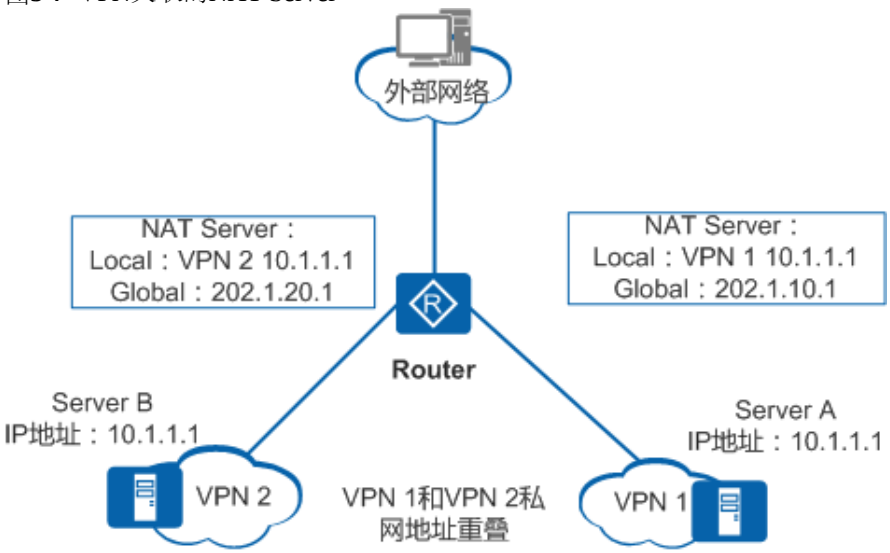
1. VPN 1内的主机A和VPN 2内的主机B地址重叠，都为私网地址10.1.1.1，都要同时访问外部网络的一个服务器。
2. Router在做源NAT时，将内部VPN作为一个NAT的匹配条件，将主机A发出报文的源IP转换为202.1.1.1，将主机B发出报文的源IP转换为202.1.2.1，同时在建立的NAT转换表中，记录用户的VPN信息。
3. 当外部网络服务器回应内部网络主机A和B的报文经过Router时，根据已建立的NAT映射表，NAT模块将发往主

机A报文的目的IP从202.1.1.1转换为10.1.1.1，然后再发往VPN 1的目的主机；将发往主机B报文的目的IP从202.1.2.1转换为10.1.1.1，然后再发往VPN 2的目的主机。

VPN关联的NAT Server

VPN关联的NAT Server是指外网主机通过NAT技术访问内网中分属不同VPN的服务器。

图**5-7** VPN关联的NAT Server



组网如图5-7所示，VPN 1内Server A和VPN 2内的Server B的地址都是10.1.1.1；使用202.1.10.1做为VPN 1内的Server A的外部地址，使用202.1.20.1做为VPN 2内的Server B的外部地址。这样，外部网络的用户使用202.1.10.1就可以访问到VPN 1提供的服务，使用202.1.20.1就可以访问VPN 2提供的服务。

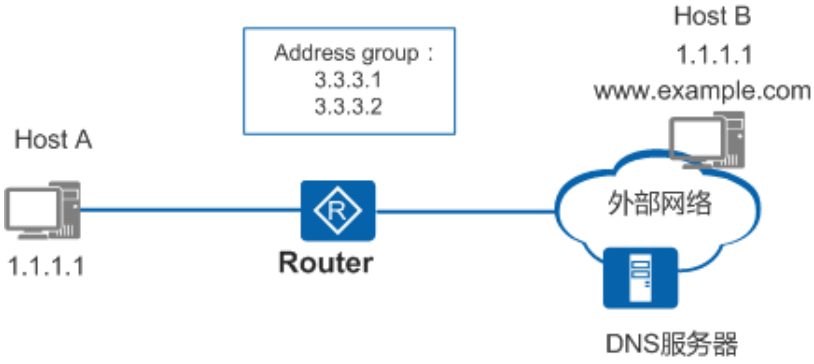
VPN关联的NAT Server的实现方式如下：

1. 外部网络的主机访问VPN 1内的Server A，报文目的IP是202.1.10.1；访问VPN 2内的Server B，报文目的IP是202.1.20.1。
2. Router在做NAT server时，根据报文的目的IP及VPN信息进行判断，将目的IP是202.1.10.1的报文的目的IP转换为10.1.1.1，然后发往VPN 1的目的Server A；将目的IP是202.1.20.1的报文的目的IP转换为10.1.1.1，然后发往VPN 2的目的Server B；同时在新建的NAT映射表中，记录下关联的VPN信息。
3. 当内部Server A和B回应外部网络主机的报文经过Router时，根据已建立的NAT映射表，NAT模块将从Server A发出的报文的源IP从10.1.1.1转换为202.1.10.1，再发往外部网络；将从Server B发出的报文的源IP从10.1.1.1转换为202.1.20.1，再发往外部网络。

5.2.6 两次NAT

两次NAT即Twice NAT，指源IP和目的IP同时转换，该技术应用于内部网络主机地址与外部网络上主机地址重叠的情况。

图**5-8** 两次NAT示意图

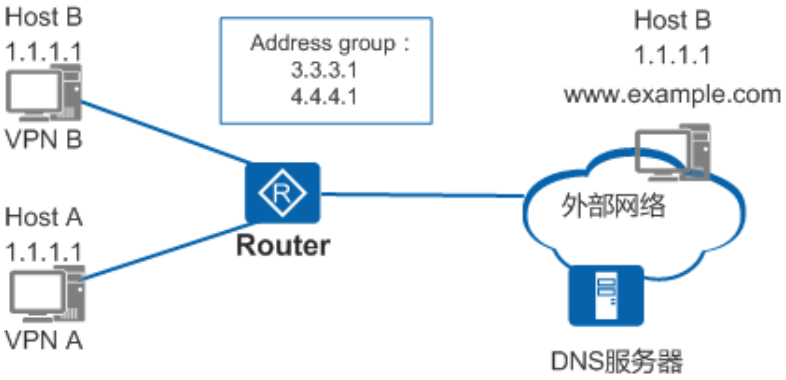


如图5-8所示，两次NAT转换的过程如下：

1. 内网Host A要访问地址重叠的外部网络Host B，Host A向位于外部网络的DNS服务器发送访问外网Host B的DNS请求，DNS服务器应答Host B的IP地址为1.1.1.1，DNS应答报文在经过Router时，进行DNS ALG，Router将DNS应答报文中的重叠地址1.1.1.1转换为唯一的临时地址3.3.3.1，然后再转发给Host A。
2. Host A访问Host B，目的IP为临时地址3.3.3.1，报文在经过Router时，Router检查到目的IP是临时地址，进行目的地址转换，将报文的目的IP转换为Host B的真实地址1.1.1.1，同时进行正常的NAT Outbound转换，将报文的源IP转换为源NAT地址池地址；Router将报文转发到Host B。

3. Host B回应Host A，目的IP为Host A的NAT Outbound地址池地址，源IP为Host B的地址1.1.1.1，报文在经过Router时，Router检查到源IP是重叠地址，进行源地址转换，将报文的源IP转换为对应的临时地址3.3.3.1，同时进行正常的目的地址转换，将报文的目的IP从源NAT地址池地址转换为Host A的内网地址1.1.1.1；Router将报文转发到Host A。

图**5-9** 内网多VPN情况下的两次NAT示意图



考虑到内网有多个VPN的场景，且内网多个VPN的地址一样的情况下，在Router上DNS ALG时，增加内网VPN信息作为重叠地址池到临时地址的映射关系匹配条件之一，如图5-9所示。内网多VPN情况下的两次NAT转换过程和两次NAT转换的过程类似，只是VPN A中的Host A转换为临时地址3.3.3.1，而VPN B中的Host B转换为临时地址4.4.4.1。

5.2.7 NAT过滤和映射方式

NAT过滤功能可以让NAT设备对外网发到内网的流量进行过滤；NAT映射功能可以让内部网络中的一组主机通过NAT映射表映射到一个外部IP地址，共享这一个IP地址，所有不同的信息流看起来好像来源于同一个IP地址。

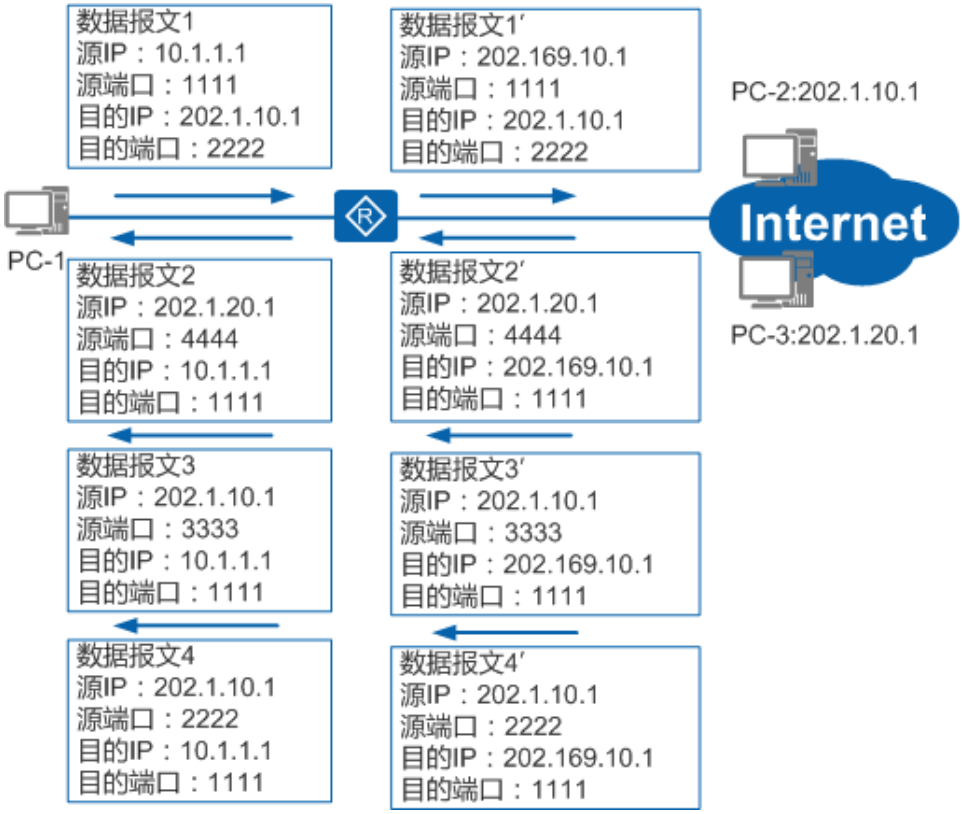
NAT过滤

NAT过滤是指NAT设备对外网发到内网的流量进行过滤，包括三种类型：

- 与外部地址无关的NAT过滤行为
- 与外部地址相关的NAT过滤行为
- 与外部地址和端口都相关的NAT过滤行为

应用场景如图5-10所示：

图**5-10** NAT过滤应用组网图



上图中，私网用户PC-1通过NAT设备与外网用户PC-2、PC-3进行通信。数据报文1代表私网主机PC-1访问公网PC-2，PC-1使用的端口号为1111，访问PC-2的端口2222；经过NAT设备时，源IP转换为202.169.10.1。

当私网主机向某公网主机发起访问后，公网主机发向私网主机的流量经过NAT设备时需要进行过滤。数据报文2’、数据报文3’和数据报文4’代表三种场景，分别对应上述三种NAT过滤类型：

- 数据报文2’代表公网主机PC-3（与报文1的目的地址不同）访问私网主机PC-1，目的端口号为1111，只有配置了外部地址无关的NAT过滤行为，才允许此报文通过，否则被NAT设备过滤掉。
- 数据报文3’代表公网服务器PC-2（与报文1的目的地址相同）访问私网主机PC-1，目的端口号为1111，源端口号为3333（与报文1的目的端口不同），只有配置了外部地址相关的NAT过滤行为或者配置了外部地址无关的NAT过滤行为，才允许此报文通过，否则被NAT设备过滤掉。
- 数据报文4’代表公网服务器PC-2（与报文1的目的地址相同）访问私网主机PC-1，目的端口号为1111，源端口号为2222（与报文1的目的端口相同），这属于外部地址和端口都相关的NAT过滤行为，是缺省的过滤行为，不配置或者配置任何类型的NAT过滤行为，都允许此报文通过，不会被过滤掉。

NAT映射

在Internet中使用NAT映射功能，所有不同的信息流看起来好像来源于同一个IP地址。因为NAT映射使得一组主机可以共享唯一的外部地址，当位于内部网络中的主机通过NAT设备向外部主机发起会话请求时，NAT设备就会查询NAT表，看是否有相关会话记录，如果有相关记录，就会将内部IP地址及端口同时进行转换，再转发出去；如果没有相关记录，进行IP地址和端口转换的同时，还会在NAT表增加一条该会话的记录。NAT映射是NAT设备对内网发到外网的流量进行映射，包括以下两种类型：

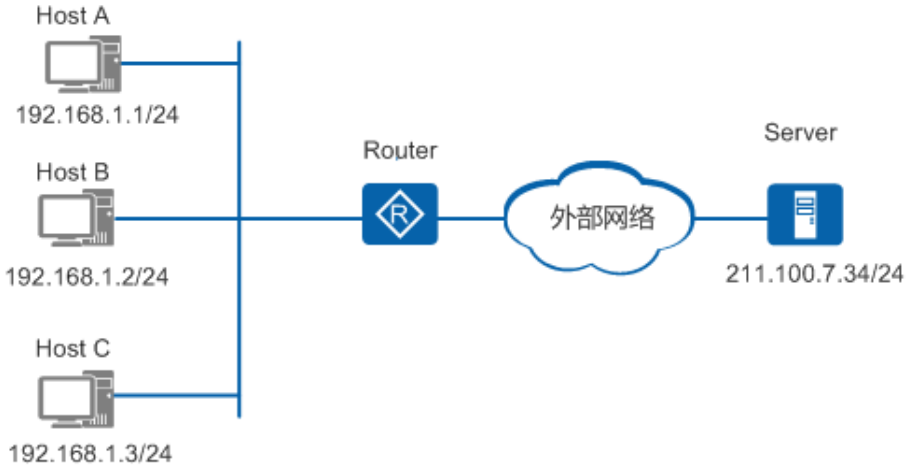
- 外部地址无关的映射：对相同的内部IP和端口重用相同的地址端口映射。
- 外部地址和端口相关的映射：对相同的内部IP地址和端口号访问相同的外部IP地址和端口号重用相同的端口映射（如果此映射条目还处在活动状态）。

5.3 应用

5.3.1 私网主机访问公网

在许多小区、学校和企业的内网规划中，由于公网地址资源有限，内网用户实际使用的都是私网地址，在这种情况下，可以使用NAT技术来实现私网用户对公网的访问。如图5-11所示，通过在Router上配置Easy IP，可以实现私网主机访问公网服务器。

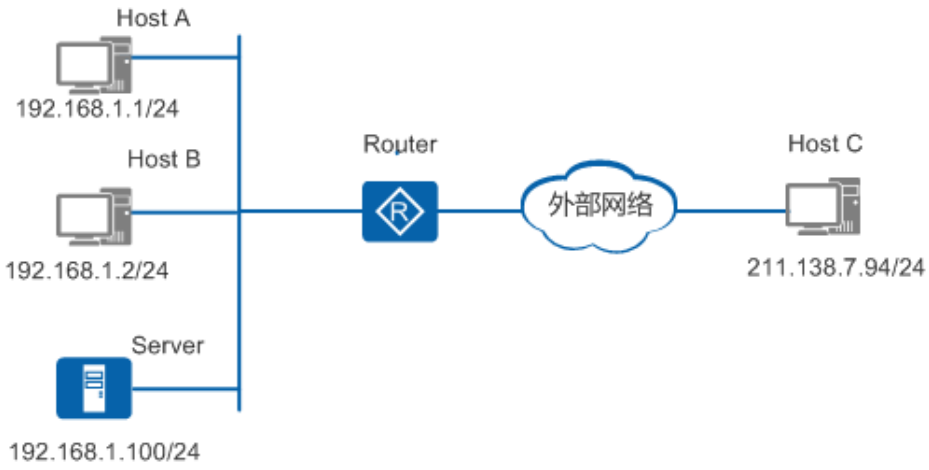
图**5-11** 私网主机访问公网服务器示意图



5.3.2 公网主机访问私网服务器

在某些场合，私网内部有一些服务器需要向公网提供服务，比如一些位于私网内的Web服务器、FTP服务器等，NAT可以支持这样的应用。如图5-12所示，通过配置NAT Server，即定义“公网IP地址＋端口号”与“私网IP地址＋端口号”间的映射关系，使位于公网的主机能够通过该映射关系访问到位于私网的服务器。

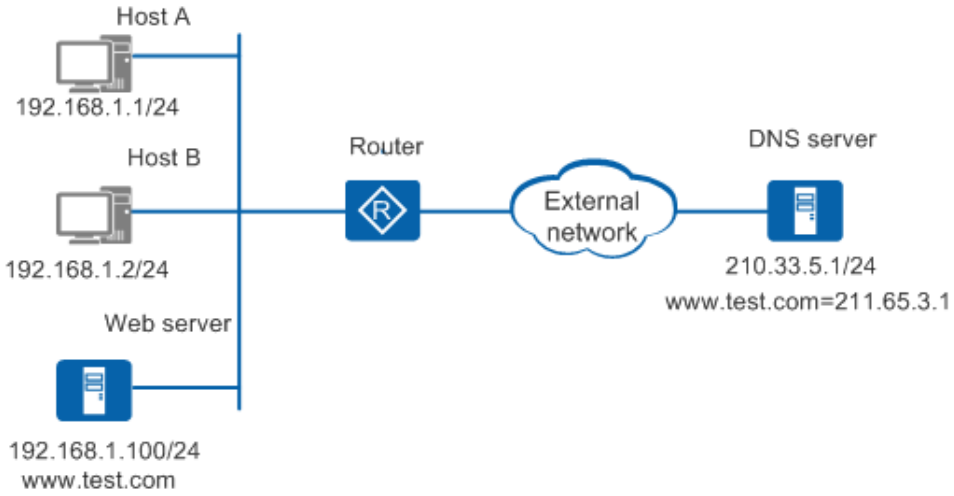
图**5-12** 公网主机访问私网服务器示意图



5.3.3 私网主机通过域名访问私网服务器

在某些场合，私网用户希望通过域名访问位于同一私网的内部服务器，而DNS服务器却位于公网，此时可通过DNS Mapping方式来实现。如图5-13所示，通过配置DNS Mapping映射表，即定义“域名—公网IP地址—公网端口—协议类型”间的映射关系，将DNS响应报文中携带的公网IP地址替换成内部服务器的私网IP地址，从而使私网用户可以通过域名来访问该服务器。

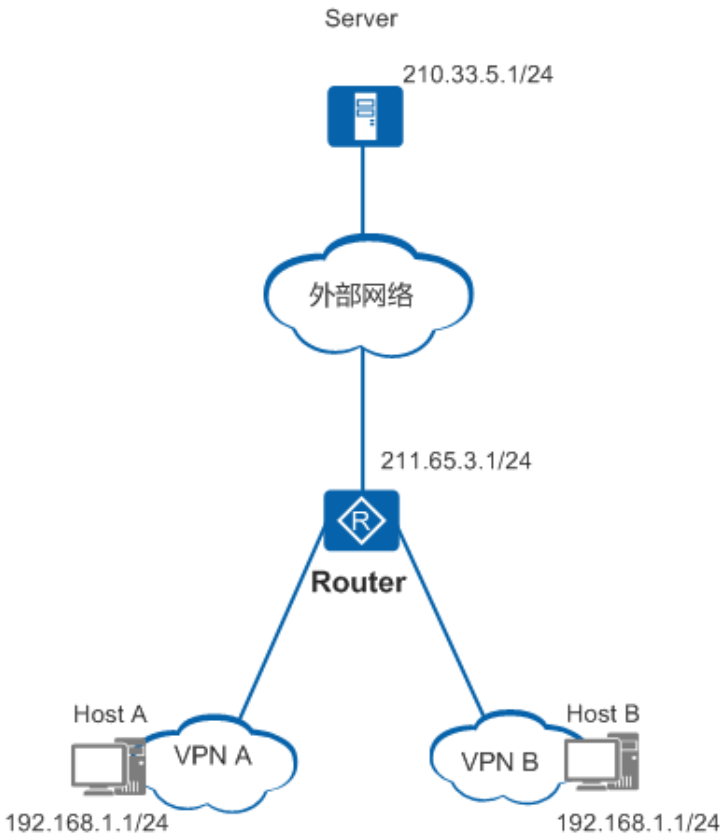
图**5-13** 私网主机通过域名访问私网服务器示意图



5.3.4 NAT多实例

当分属不同MPLS VPN的主机使用相同的私网地址，并通过同一个出口设备访问Internet时，NAT多实例可实现这些地址重叠的主机同时访问公网服务器。如图5-14所示，尽管HostA和HostB具有相同的私网地址，但由于其分属不同的VPN，通过使用NAT关联VPN技术，可以使NAT能够区分属于不同VPN的主机，允许二者同时访问公网服务器。

图**5-14** NAT多实例示意图



5.4 配置任务概览

用户可以根据实际应用场景选择对应的NAT特性完成配置任务，如表5-2所示。

表5-2 NAT配置任务概览

场景	描述	对应任务
内网主机使用内网IP地址访问外网主机	企业内的主机使用私网IP地址可以实现内网主机间的通信，但不能和外网通信。设备通过配置动态NAT功能可以把需要访问外网的私网IP地址替换为公网IP地址，并建立映射关系，待返回报文到达设备时再“反向”把公网IP地址替换回私网IP地址，然后转发给主机，实现内网用户和外网的通信。	5.6 配置动态地址转换
内网的重要主机的IP地址和端口号映射成固定外网IP地址和端口号与外网主机通信	动态NAT在转换地址时，做不到用固定的公网IP和端口号替换同一个私网IP和端口号。而一些重要主机需要对外通信时使用固定的公网IP地址和端口号，此时动态NAT无法满足要求。 静态NAT可以建立固定的一对一的公网IP地址和私网IP地址的映射，特定的私网IP地址只会被特定的公网IP地址替换。这样，就保证了重要主机使用固定的公网IP地址访问外网。	5.7 配置静态地址转换
外网用户访问内网服务器	NAT具有“屏蔽”内部主机的作用，但有时内网需要向外网提供服务，如提供WWW服务或FTP服务。这种情况下需要内网的服务器不被“屏蔽”，外网用户可以随时访问内网。 NAT Server可以很好地解决这个问题，当外网访问内网时，它通过事先配置好的“公网IP地址+端口号”与“私网IP地址+端口号”间的映射关系，将服务器的“公网IP地址+端口号”根据映射关系替换成对应的“私网IP地址+端口号”。	5.8 配置内部服务器

5.5 配置注意事项

介绍NAT配置注意事项

涉及网元

无需其他网元配合。

License支持

NAT是路由器的基本特性，无需获得License许可即可应用此功能。

特性依赖和限制

- 高端LAN板卡（8FE1GE、24GE、24ES2GP）缺省使能了路由转发功能，对收到的报文不会上送CPU，当IP报文在LAN板内路由转发时，VLANIF口不支持配置NAT业务。

5.6 配置动态地址转换

通过配置动态NAT，可以动态的建立内网IP和外网IP的映射表项，实现私网用户访问外网。

5.6.1 配置地址转换的ACL规则

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**acl [number]** *acl-number* **[match-order { auto | config }]**，使用编号创建一个ACL，并进入ACL视图。
3. 根据实际情况配置基本ACL规则或者高级ACL规则。详细请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR1600&AR2200&AR3200&AR3600系列企业路由器 配置指南-安全-ACL配置》中的“配置基本ACL”或“配置高级ACL”。

   说明:

   用于配置地址转换的ACL只能是2000～3999的基本ACL或高级ACL。

   a. 仅当ACL的rule配置为**permit**时，设备允许匹配该规则中指定的源IP地址使用地址池进行地址转换。
   b. 当ACL的rule没有配置为**permit**时，应用该ACL的NAT功能不生效，即不允许使用地址池进行地址转换，设备根据目的地址查找路由表转发报文。

5.6.2 配置出接口的地址关联

背景信息

NAT Outbound所用地址池是用来存放动态NAT使用到的IP地址的集合，在做动态NAT时会选择地址池中的某个地址用做地址转换。

如果用户想通过动态NAT访问外网时，可以根据自己公网IP的规划情况选择以下其中一种方式:

- 用户在配置了NAT设备出接口的IP和其他应用之后，还有空闲公网IP地址，可以选择带地址池的NAT Outbound。
- 用户在配置了NAT设备出接口的IP和其他应用之后，已没有其他可用公网IP地址，可以选择Easy IP方式，Easy IP可以借用NAT设备出接口的IP地址完成动态NAT。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 配置出接口的地址关联，用户根据实际情况选择其中一种配置方法。
   - 配置带地址池的NAT Outbound:
     a. 执行命令**nat address-group** *group-index start-address end-address*，配置公网地址池。
     b. 执行命令**interface** *interface-type interface-number* **[** *.subnumber* **]**，进入接口或子接口视图。

c. 执行命令**nat outbound** *acl-number* **address-group** *group-index* [**no-pat**]，配置带地址池的NAT Outbound。

- 配置不带地址池的Easy IP:

a. 执行命令**interface** *interface-type interface-number* [*.subnumber*]，进入接口或子接口视图。

b. 执行命令**nat outbound** *acl-number* [**interface** *interface-type interface-number* [*.subnumber*]] [**vrrp** *vrrpid*]，配置Easy IP。

5.6.3 （可选）使能NAT ALG功能

背景信息

一般情况下，NAT只能对IP报文头的IP地址和TCP/UDP头部的端口信息进行转换。对于一些特殊协议，例如DNS、FTP等，它们报文的数据部分可能包含IP地址或端口信息，这些内容不能被NAT有效的转换，从而无法正确完成通信。

使能ALG（Application Level Gateway）功能可以使NAT设备识别被封装在报文数据部分的IP地址或端口信息，并根据映射表项进行替换，实现报文正常穿越NAT。目前设备的ALG功能所支持的协议包括：DNS、FTP、SIP、PPTP和RTSP。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**nat alg** { **all** | *protocol-name* } **enable**，使能指定应用协议的NAT ALG功能。

   缺省情况下，NAT ALG处于未使能状态。
3. （可选）执行命令**port-mapping** { **dns** | **ftp** | **sip** | **rtsp** | **pptp** } **port** *port-number* **acl** *acl-number*，配置端口映射。

   当使能NAT ALG功能的应用协议采用非知名端口号，即非缺省定义的端口号时，需要执行命令**port-mapping**配置端口映射。

5.6.4 （可选）配置NAT设备上的SIP呼叫带宽限制功能

背景信息

针对SIP Server在公网侧，私网的SIP Phone和公网的SIP Phone互通的场景，如果NAT设备上的带宽不够，就会影响通话质量。我们可以在NAT设备上使能呼叫会话控制CAC（Call Admission Control）功能并配置总带宽，对SIP呼叫进行带宽限制，超过指定带宽的SIP呼叫将被拒绝，无法呼叫成功。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**nat sip cac enable bandwidth** { *bandwidth-value* | **percent** *value* **interface** *interface-type interface-number* [*.subnumber*] }，使能CAC功能并配置设备的总带宽值，对SIP呼叫进行带宽限制处理。

   缺省情况下，设备上配置的带宽限定值为0，不进行带宽限制处理。

5.6.5 （可选）配置NAT过滤方式和映射模式

背景信息

由于IPv4地址的短缺以及出于安全考虑等因素，在因特网中广泛采用了NAT技术。由于不同厂商实现的NAT功能不同，可能会导致使用STUN、TURN、ICE技术的应用软件无法穿越NAT，因为这些技术广泛依赖于SIP代理等软件。SIP属于多通道应用，在功能实现时需要创建多个数据通道链接。为了保障多个通道的链接，必须配置NAT映射模式和过滤方式，只允许符合映射关系、过滤条件的报文通过。

设备支持的NAT映射包含如下两种类型：

- 外部地址和端口无关的映射：对相同的内部IP地址和端口重用相同的地址端口映射。
- 外部地址和端口相关的映射：对相同的内部IP地址和端口号访问相同的外部IP地址和端口号重用相同的地址端口映射

（如果此映射项还处在活动状态）。

设备支持的NAT过滤方式包含如下三种类型：

- 与外部地址和端口无关的NAT过滤方式。
- 与外部地址相关，端口无关的NAT过滤方式。
- 与外部地址和端口都相关的NAT过滤方式。

说明：

使SIP代理等软件正常穿越NAT需要同时配置“外部地址和端口相关的映射”和“与外部地址和端口都相关的NAT过滤方式”。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**nat mapping-mode endpoint-independent** [*protocol-name* [**dest-port** *port-number*]]，配置NAT映射模式。

   缺省情况下，NAT映射模式为与外部地址和端口相关的映射。
3. 执行命令**nat filter-mode** { **endpoint-dependent** | **endpoint-independent** | **endpoint-and-port-dependent** }，配置NAT过滤方式。

   缺省情况下，NAT过滤方式为**endpoint-and-port-dependent**。

5.6.6 （可选）配置两次NAT

背景信息

内外网地址重叠的主机可以根据重叠地址池和临时地址池的映射关系，将重叠地址替换为临时地址同时做NAT，实现内外网的互访。

- 重叠地址池用来指定内网哪些IP允许和外网重叠，只有属于重叠地址池的地址才会做两次NAT。
- 临时地址池指定了用哪些临时IP地址来替换重叠地址池里的地址。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**nat overlap-address** *map-index overlappool-startaddress temppool-startaddress* **pool-length** *length* [**inside-vpn-instance** *inside-vpn-instance-name*]，配置两次NAT重叠地址池和临时地址池的映射关系。

   说明：

   - 重叠地址池和临时地址池的地址个数最大均为255。
   - 当配置中的VPN实例删除时，两次NAT的配置也同步删除。

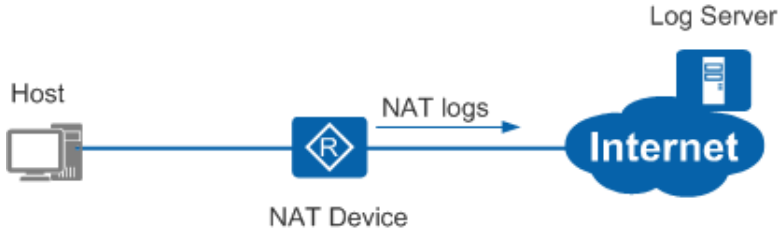
5.6.7 （可选）配置NAT日志输出

背景信息

NAT日志是设备在做NAT时生成的信息记录。该信息包括报文的源IP地址、源端口、目的IP地址、目的端口、转换后的源IP地址、转换后的源端口以及NAT的时间信息和用户执行的操作等。网络管理员可以通过查看NAT日志实时定位用户通过NAT访问网络的情况，增强了网络的安全性。

路由器支持将NAT日志输出至日志服务器，如图5-15所示：

图**5-15** NAT日志输出至指定服务器



操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**firewall log session enable**，使能防火墙日志功能。
3. 执行命令**firewall log session nat enable**，使能NAT类型的流日志功能。
4. （可选）执行命令**nat log-format elog**，将NAT日志设置为elog格式，输出日志为elog服务器规定的可以对接的格式。
5. 执行以下命令配置日志输出到信息中心日志主机或流日志主机：
   - 配置日志输出到信息中心日志主机
     a. 执行命令**info-center enable**，开启信息中心。
     b. 执行命令**info-center loghost** *ip-address* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | | { **vpn-instance** *vpn-instance-name* | **public-net** }] *，配置日志信息输出到日志主机所使用的通道。

     系统最多可配置8个日志主机，实现日志主机间相互备份的功能。

     说明：
     配置日志信息输出到日志主机，有详细的配置举例，请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR1600&AR2200&AR3200&AR3600系列企业路由器 配置指南-设备管理-信息中心配置》中的“配置向日志主机输出日志信息示例”。
   - 配置日志输出到流日志主机

     执行命令**firewall log binary-log host** *host-ip-address host-port* **source** *source-ip-address source-port* [**vpn-instance** *vpn-instance-name*]，配置流日志主机。

     缺省情况下，流日志主机未配置。

5.6.8 （可选）配置NAT地址映射表项有效时间

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**firewall-nat session** { { **dns** | **ftp** | **ftp-data** | **http** | **icmp** | **tcp** | **tcp-proxy** | **udp** | **sip** | **sip-media** | **rtsp** | **rtsp-media** | **pptp** | **pptp-data** } | { **tcp** | **udp** } **user-define** *port-number* } **aging-time** *time-value*，配置NAT表项老化时间。

   缺省情况下，各协议的老化时间为：DNS（120秒）、ftp（120秒）、ftp-data（120秒）、HTTP（120秒）、icmp（20秒）、tcp（600秒）、tcp-proxy（10秒）、udp（120秒）、sip（1800秒）、sip-media（120秒）、rtsp（60秒）、rtsp-media（120秒）、pptp（600秒）、pptp-data（600秒）。TCP/UDP协议自定义端口下的会话表项缺省老化时间与对应协议一致。

5.6.9 （可选）使能NAT业务优先功能

前置任务

在使能NAT业务优先功能之前，需要完成以下任务：

- 配置静态地址映射

背景信息

在某些特殊场景，要求NAT业务的优先级高于路由业务，即要求先进行NAT地址转换，然后对转换后的地址查路由表，指导流量转发。例如：当私网设备允许公网设备通过固定IP地址访问时，先配置静态NAT，将私网设备的私网IP地址和指定的公网IP地址进行转换，然后再配置一条到该公网IP地址的静态路由，使公网发往私网的流量能通过NAT引流。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**nat inside priority enable**，使能NAT业务优先于路由业务功能。

   缺省情况下，系统默认为路由业务优先。

   说明：
   AR1600系列不支持此命令。

5.6.10 检查配置结果

操作步骤

- 执行命令**display nat address-group** [*group-index*] [**verbose**]，查看NAT地址池的配置信息。
- 执行命令**display nat outbound** [**acl** *acl-number* | **address-group** *group-index* | **interface** *interface-type interface-number* [*.subnumber*]]，查看NAT Outbound信息。
- 执行命令**display nat alg**，查看NAT ALG的配置信息。
- 执行命令**display nat overlap-address** { *map-index* | **all** | **inside-vpn-instance** *inside-vpn-instance-name* }，查看NAT双向地址转换的相关信息。
- 执行命令**display firewall-nat session aging-time**，查看NAT表项老化时间的相关信息。
- 执行命令**display nat sip cac bandwidth information** [**verbose**]，查看设备上的当前总带宽及被占用带宽。
- 执行命令**display nat filter-mode**，查看当前的NAT过滤方式。
- 执行命令**display nat mapping-mode**，查看NAT映射模式。
- 执行命令**display nat mapping table** { **all** | **number** }或者**display nat mapping table inside-address** *ip-address* **protocol** *protocol-name* **port** *port-number* [**vpn-instance** *vpn-instance-name*]，查看NAT映射表所有表项信息或个数。

5.7 配置静态地址转换

配置静态NAT以实现私网地址和公网地址的固定一对一映射。

5.7.1 配置静态地址映射

操作步骤

1. 配置静态地址映射分以下两种方式：

   方式一：在接口视图下配置静态映射：

   a. 执行命令**system-view**，进入系统视图。

   b. 执行命令**interface** *interface-type interface-number* [*.subnumber*]，进入接口或子接口视图。

   c. 用户根据实际情况选择下面的一条命令执行：

   - **nat static protocol** { **tcp** | **udp** } **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } *global-port* [*global-port2*] [**vrrp** *vrrpid*] **inside** *host-address* [*host-address2*] [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**acl** *acl-number*] [**global-to-inside** | **inside-to-global**] [**description** *description*]
   - **nat static** [**protocol** { *protocol-number* | **icmp** | **tcp** | **udp** }] **global** { *global-address* | **current-**

interface | **interface** *interface-type interface-number* [*.subnumber*] } [**vrrp** *vrrpid*] **inside** *host-address* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**acl** *acl-number*] [**global-to-inside** | **inside-to-global**] [**description** *description*]

- **nat static protocol** { **tcp** | **udp** } **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } *global-port global-port2* [**vrrp** *vrrpid*] **inside** *host-address host-port host-port2* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**acl** *acl-number*] [**description** *description*]

方式二：在系统视图下配置静态映射：

a. 执行命令**system-view**，进入系统视图。

b. 用户根据实际情况选择下面的一条命令执行：

- **nat static protocol** { **tcp** | **udp** } **global** *global-address global-port* [*global-port2*] **inside** *host-address* [*host-address2*] [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]
- **nat static protocol** { **tcp** | **udp** } **global interface loopback** *interface-number global-port* [*global-port2*] [**vpn-instance** *vpn-instance-name*] **inside** *host-address* [*host-address2*] [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]
- **nat static** [**protocol** { *protocol-number* | **icmp** | **tcp** | **udp** }] **global** { *global-address* | **interface loopback** *interface-number* } **inside** *host-address* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]
- **nat static protocol** { **tcp** | **udp** } **global** *global-address global-port global-port2* **inside** *host-address host-port host-port2* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]

c. 执行命令**interface** *interface-type interface-number* [*.subnumber*]，进入接口或子接口视图。

d. 执行命令**nat static enable**，在接口下使能nat static功能。

说明：

- 如果想实现Global侧VPN，建议在接口下配置静态NAT，设备会自动获取到接口关联的VPN，不需要手动配置Global侧VPN参数；在系统视图下配置静态NAT绑定Global侧VPN的场景可以通过配置Global侧出接口为Loopback接口，然后指定VPN的方式实现。
- 配置静态NAT时，其中的*global-address*和*host-address*必须保证和设备现有地址没有重复，包括设备接口地址，用户地址池地址，以避免冲突。
- 在设备上执行**undo nat static**命令，设备上的静态映射表项不会立刻消失，如果需要立刻清除静态NAT映射表项，请手动执行**reset nat session**命令来清除静态映射表项信息。
- 多个接口使用同一条nat static映射的情况下，建议使用第二种方法。
- 当配置借用接口地址的静态1：1 NAT（不指定端口号，接口地址对应一个私网地址）时，可能会造成在该接口地址上启用的其他业务无法正常使用，请谨慎选择，如果确定在该接口地址上启用其他应用，请在配置后面增加ACL排除启用应用的端口号。
- 指定的端口号global-port或host-port不能被其他应用程序所占用，否则，配置不生效。

5.7.2 （可选）使能NAT ALG功能

背景信息

一般情况下，NAT只能对IP报文头的IP地址和TCP/UDP头部的端口信息进行转换。对于一些特殊协议，例如DNS、FTP等，它们报文的数据部分可能包含IP地址或端口信息，这些内容不能被NAT有效的转换，从而无法正确完成通信。

使能ALG（Application Level Gateway）功能可以使NAT设备识别被封装在报文数据部分的IP地址或端口信息，并根据映射表项进行替换，实现报文正常穿越NAT。目前设备的ALG功能所支持的协议包括：DNS、FTP、SIP、PPTP和RTSP。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**nat alg** { **all** | *protocol-name* } **enable**，使能指定应用协议的NAT ALG功能。

   缺省情况下，NAT ALG处于未使能状态。
3. （可选）执行命令**port-mapping** { **dns** | **ftp** | **sip** | **rtsp** | **pptp** } **port** *port-number* **acl** *acl-number*，配置端口映射。

当使能NAT ALG功能的应用协议采用非知名端口号，即非缺省定义的端口号时，需要执行命令**port-mapping**配置端口映射。

5.7.3 （可选）配置NAT设备上的SIP呼叫带宽限制功能

背景信息

针对SIP Server在公网侧，私网的SIP Phone和公网的SIP Phone互通的场景，如果NAT设备上的带宽不够，就会影响通话质量。我们可以在NAT设备上使能呼叫会话控制CAC（Call Admission Control）功能并配置总带宽，对SIP呼叫进行带宽限制，超过指定带宽的SIP呼叫将被拒绝，无法呼叫成功。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**nat sip cac enable bandwidth** { *bandwidth-value* | **percent** *value* **interface** *interface-type interface-number* [*.subnumber*] }，使能CAC功能并配置设备的总带宽值，对SIP呼叫进行带宽限制处理。

   缺省情况下，设备上配置的带宽限定值为0，不进行带宽限制处理。

5.7.4 （可选）配置DNS Mapping

背景信息

企业内如果没有内网的DNS服务器，而且又有使用域名访问内网服务器的需求，这就要求企业内网用户必须使用外网的DNS服务器来实现域名访问。

内网用户可以通过NAT使用外网的DNS服务器访问外网的服务器，但如果内网用户通过外网的DNS服务器访问内网服务器时就会失败。因为来自外网的DNS解析结果是内网服务器对外宣称的IP地址，并非内网服务器真实的私网IP地址。

在配置静态地址转换时配置DNS Mapping，可以指明“域名—公网IP地址—公网端口—协议类型”映射表项。当DNS解析报文到达NAT设备时，NAT设备会根据DNS Mapping建立的映射表项查找静态地址表项，得到公网IP地址对应的私网IP地址，再用该私网地址替换DNS的解析结果转发给用户。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**nat dns-map** *domain-name* { *global-address* | **interface** *interface-type interface-number* [*.subnumber*] } *global-port protocol-name*，配置域名到外部IP地址、端口号、协议类型的映射。

   说明：

   配置了DNS Mapping后必须执行**nat alg dns enable**命令使能ALG DNS功能，才可以使DNS应答报文正常穿越NAT，否则内部主机无法使用域名访问内网服务器。

5.7.5 （可选）配置NAT过滤方式和映射模式

背景信息

由于IPv4地址的短缺以及出于安全考虑等因素，在因特网中广泛采用了NAT技术。由于不同厂商实现的NAT功能不同，可能会导致使用STUN、TURN、ICE技术的应用软件无法穿越NAT，因为这些技术广泛依赖于SIP代理等软件。SIP属于多通道应用，在功能实现时需要创建多个数据通道链接。为了保障多个通道的链接，必须配置NAT映射模式和过滤方式，只允许符合映射关系、过滤条件的报文通过。

设备支持的NAT映射包含如下两种类型：

- 外部地址和端口无关的映射：对相同的内部IP地址和端口重用相同的地址端口映射。
- 外部地址和端口相关的映射：对相同的内部IP地址和端口号访问相同的外部IP地址和端口号重用相同的地址端口映射（如果此映射项还处在活动状态）。

设备支持的NAT过滤方式包含如下三种类型：

- 与外部地址和端口无关的NAT过滤方式。
- 与外部地址相关，端口无关的NAT过滤方式。
- 与外部地址和端口都相关的NAT过滤方式。

说明：

使SIP代理等软件正常穿越NAT需要同时配置“外部地址和端口相关的映射”和“与外部地址和端口都相关的NAT过滤方式”。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**nat mapping-mode endpoint-independent** [*protocol-name* [**dest-port** *port-number*]]，配置NAT映射模式。

   缺省情况下，NAT映射模式为与外部地址和端口相关的映射。
3. 执行命令**nat filter-mode** { **endpoint-dependent** | **endpoint-independent** | **endpoint-and-port-dependent** }，配置NAT过滤方式。

   缺省情况下，NAT过滤方式为**endpoint-and-port-dependent**。

5.7.6 （可选）配置两次NAT

背景信息

内外网地址重叠的主机可以根据重叠地址池和临时地址池的映射关系，将重叠地址替换为临时地址同时做NAT，实现内外网的互访。

- 重叠地址池用来指定内网哪些IP允许和外网重叠，只有属于重叠地址池的地址才会做两次NAT。
- 临时地址池指定了用哪些临时IP地址来替换重叠地址池里的地址。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**nat overlap-address** *map-index overlappool-startaddress temppool-startaddress* **pool-length** *length* [**inside-vpn-instance** *inside-vpn-instance-name*]，配置两次NAT重叠地址池和临时地址池的映射关系。

   说明：

   - 重叠地址池和临时地址池的地址个数最大均为255。
   - 当配置中的VPN实例删除时，两次NAT的配置也同步删除。

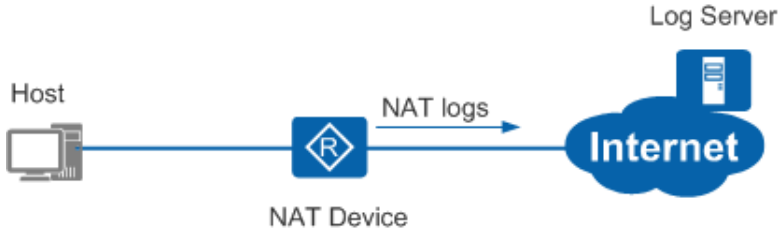
5.7.7 （可选）配置NAT日志输出

背景信息

NAT日志是设备在做NAT时生成的信息记录。该信息包括报文的源IP地址、源端口、目的IP地址、目的端口、转换后的源IP地址、转换后的源端口以及NAT的时间信息和用户执行的操作等。网络管理员可以通过查看NAT日志实时定位用户通过NAT访问网络的情况，增强了网络的安全性。

路由器支持将NAT日志输出至日志服务器，如图5-16所示：

图**5-16** NAT日志输出至指定服务器



操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**firewall log session enable**，使能防火墙日志功能。
3. 执行命令**firewall log session nat enable**，使能NAT类型的流日志功能。
4. （可选）执行命令**nat log-format elog**，将NAT日志设置为elog格式，输出日志为elog服务器规定的可以对接的格式。
5. 执行以下命令配置日志输出到信息中心日志主机或流日志主机：
   - 配置日志输出到信息中心日志主机
     a. 执行命令**info-center enable**，开启信息中心。
     b. 执行命令**info-center loghost** *ip-address* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | | { **vpn-instance** *vpn-instance-name* | **public-net** }] *，配置日志信息输出到日志主机所使用的通道。

     系统最多可配置8个日志主机，实现日志主机间相互备份的功能。

     说明：
     配置日志信息输出到日志主机，有详细的配置举例，请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR1600&AR2200&AR3200&AR3600系列企业路由器 配置指南-设备管理-信息中心配置》中的“配置向日志主机输出日志信息示例”。
   - 配置日志输出到流日志主机

     执行命令**firewall log binary-log host** *host-ip-address host-port* **source** *source-ip-address source-port* [**vpn-instance** *vpn-instance-name*]，配置流日志主机。

     缺省情况下，流日志主机未配置。

5.7.8 （可选）配置NAT地址映射表项有效时间

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**firewall-nat session** { { **dns** | **ftp** | **ftp-data** | **http** | **icmp** | **tcp** | **tcp-proxy** | **udp** | **sip** | **sip-media** | **rtsp** | **rtsp-media** | **pptp** | **pptp-data** } | { **tcp** | **udp** } **user-define** *port-number* } **aging-time** *time-value*，配置NAT表项老化时间。

   缺省情况下，各协议的老化时间为：DNS（120秒）、ftp（120秒）、ftp-data（120秒）、HTTP（120秒）、icmp（20秒）、tcp（600秒）、tcp-proxy（10秒）、udp（120秒）、sip（1800秒）、sip-media（120秒）、rtsp（60秒）、rtsp-media（120秒）、pptp（600秒）、pptp-data（600秒）。TCP/UDP协议自定义端口下的会话表项缺省老化时间与对应协议一致。

5.7.9 （可选）使能NAT业务优先功能

前置任务

在使能NAT业务优先功能之前，需要完成以下任务：

- 配置静态地址映射

背景信息

在某些特殊场景，要求NAT业务的优先级高于路由业务，即要求先进行NAT地址转换，然后对转换后的地址查路由表，指导流量转发。例如：当私网设备允许公网设备通过固定IP地址访问时，先配置静态NAT，将私网设备的私网IP地址和指定的公网IP地址进行转换，然后再配置一条到该公网IP地址的静态路由，使公网发往私网的流量能通过NAT引流。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**nat inside priority enable**，使能NAT业务优先于路由业务功能。

   缺省情况下，系统默认为路由业务优先。

   说明：
   AR1600系列不支持此命令。

5.7.10 检查配置结果

操作步骤

- 执行命令**display nat alg**，查看NAT ALG的配置信息。
- 执行命令**display nat dns-map** [*domain-name*]，查看DNS Mapping信息。
- 执行命令**display nat overlap-address** { *map-index* | **all** | **inside-vpn-instance** *inside-vpn-instance-name* }，查看NAT双向地址转换的相关信息。
- 执行命令**display firewall-nat session aging-time**，查看NAT表项老化时间的相关信息。
- 执行命令**display nat static** [**global** *global-address* | **inside** *host-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-name* [*.subnumber*] | **acl** *acl-number*]，查看NAT Static的配置信息。
- 执行命令**display nat sip cac bandwidth information** [**verbose**]，查看设备上的当前总带宽及被占用带宽。
- 执行命令**display nat filter-mode**，查看当前的NAT过滤方式。
- 执行命令**display nat mapping-mode**，查看NAT映射模式。
- 执行命令**display nat mapping table** { **all** | **number** }或者**display nat mapping table inside-address** *ip-address* **protocol** *protocol-name* **port** *port-number* [**vpn-instance** *vpn-instance-name*]，查看NAT映射表所有表项信息或个数。
- 执行命令**display nat static interface enable**，查看接口下静态NAT功能的使能情况。

5.8 配置内部服务器

通过配置内部服务器，可以使外网用户访问内网服务器。

5.8.1 配置内部服务器地址映射

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**interface** *interface-type interface-number* [*.subnumber*]，进入接口或子接口视图。
3. 根据实际情况，执行其中一条命令配置NAT Server：
   - **nat server protocol** { **tcp** | **udp** } **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } *global-port* [*global-port2*] [**vrrp** *vrrpid*] **inside** *host-address* [*host-address2*] [*host-port*] [**vpn-instance** *vpn-instance-name*] [**acl** *acl-number*] [**description** *description*]
   - **nat server** [**protocol** { *protocol-number* | **icmp** | **tcp** | **udp** }] **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } [**vrrp** *vrrpid*] **inside** *host-address* [**vpn-instance** *vpn-instance-name*] [**acl** *acl-number*] [**description** *description*]

说明：

- 配置NAT Server映射时，其中的*global-address*和*host-address*必须保证和设备现有地址没有重复，包括设备接口地址、用户地址池地址等，以避免冲突。
- 如果使用接口地址作为内网服务器地址，可以使用**current-interface**，也可以指定实际存在的**loopback**接口地址作为内网服务器地址。
- 在设备上执行**undo nat server**命令，设备上的映射表项不会立刻消失，需要手动执行**reset nat session**命令来清除表项信息。
- NAT Server和静态NAT的区别就是NAT Server对于内网主动访问外网的情况不做端口替换，仅作地址替换。
- 当配置借用接口地址的1：1 NAT Server（不指定端口号，接口地址对应一个私网地址）时，可能会造成在该接口地址上启用的其他业务无法正常使用，请谨慎选择，如果确定在该接口地址上启用其他应用，请在配置后面增加ACL排除启用应用的端口号。

5.8.2 （可选）使能NAT ALG功能

背景信息

一般情况下，NAT只能对IP报文头的IP地址和TCP/UDP头部的端口信息进行转换。对于一些特殊协议，例如DNS、FTP等，它们报文的数据部分可能包含IP地址或端口信息，这些内容不能被NAT有效的转换，从而无法正确完成通信。

使能ALG（Application Level Gateway）功能可以使NAT设备识别被封装在报文数据部分的IP地址或端口信息，并根据映射表项进行替换，实现报文正常穿越NAT。目前设备的ALG功能所支持的协议包括：DNS、FTP、SIP、PPTP和RTSP。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**nat alg** { **all** | *protocol-name* } **enable**，使能指定应用协议的NAT ALG功能。

   缺省情况下，NAT ALG处于未使能状态。
3. （可选）执行命令**port-mapping** { **dns** | **ftp** | **sip** | **rtsp** | **pptp** } **port** *port-number* **acl** *acl-number*，配置端口映射。

   当使能NAT ALG功能的应用协议采用非知名端口号，即非缺省定义的端口号时，需要执行命令**port-mapping**配置端口映射。

5.8.3 （可选）配置NAT设备上的SIP呼叫带宽限制功能

背景信息

针对SIP Server在公网侧，私网的SIP Phone和公网的SIP Phone互通的场景，如果NAT设备上的带宽不够，就会影响通话质量。我们可以在NAT设备上使能呼叫会话控制CAC（Call Admission Control）功能并配置总带宽，对SIP呼叫进行带宽限制，超过指定带宽的SIP呼叫将被拒绝，无法呼叫成功。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**nat sip cac enable bandwidth** { *bandwidth-value* | **percent** *value* **interface** *interface-type interface-number* [*.subnumber*] }，使能CAC功能并配置设备的总带宽值，对SIP呼叫进行带宽限制处理。

   缺省情况下，设备上配置的带宽限定值为0，不进行带宽限制处理。

5.8.4 （可选）配置DNS Mapping

背景信息

企业内如果没有内网的DNS服务器，而且又有使用域名访问内网服务器的需求，这就要求企业内网用户必须使用外网的DNS服务器来实现域名访问。

内网用户可以通过NAT使用外网的DNS服务器访问外网的服务器，但如果内网用户通过外网的DNS服务器访问内网服务器时

就会失败。因为来自外网的DNS解析结果是内网服务器对外宣称的IP地址，并非内网服务器真实的私网IP地址。

在配置静态地址转换时配置DNS Mapping，可以指明“域名—公网IP地址—公网端口—协议类型”映射表项。当DNS解析报文到达NAT设备时，NAT设备会根据DNS Mapping建立的映射表项查找静态地址表项，得到公网IP地址对应的私网IP地址，再用该私网地址替换DNS的解析结果转发给用户。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**nat dns-map** *domain-name* { *global-address* | **interface** *interface-type interface-number* [*.subnumber*] } *global-port protocol-name*，配置域名到外部IP地址、端口号、协议类型的映射。

   说明：

   配置了DNS Mapping后必须执行**nat alg dns enable**命令使能ALG DNS功能，才可以使DNS应答报文正常穿越NAT，否则内部主机无法使用域名访问内网服务器。

5.8.5 （可选）配置NAT过滤方式和映射模式

背景信息

由于IPv4地址的短缺以及出于安全考虑等因素，在因特网中广泛采用了NAT技术。由于不同厂商实现的NAT功能不同，可能会导致使用STUN、TURN、ICE技术的应用软件无法穿越NAT，因为这些技术广泛依赖于SIP代理等软件。SIP属于多通道应用，在功能实现时需要创建多个数据通道链接。为了保障多个通道的链接，必须配置NAT映射模式和过滤方式，只允许符合映射关系、过滤条件的报文通过。

设备支持的NAT映射包含如下两种类型：

- 外部地址和端口无关的映射：对相同的内部IP地址和端口重用相同的地址端口映射。
- 外部地址和端口相关的映射：对相同的内部IP地址和端口号访问相同的外部IP地址和端口号重用相同的地址端口映射（如果此映射项还处在活动状态）。

设备支持的NAT过滤方式包含如下三种类型：

- 与外部地址和端口无关的NAT过滤方式。
- 与外部地址相关，端口无关的NAT过滤方式。
- 与外部地址和端口都相关的NAT过滤方式。

说明：

使SIP代理等软件正常穿越NAT需要同时配置“外部地址和端口相关的映射”和“与外部地址和端口都相关的NAT过滤方式”。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**nat mapping-mode endpoint-independent** [*protocol-name* [**dest-port** *port-number*]]，配置NAT映射模式。

   缺省情况下，NAT映射模式为与外部地址和端口相关的映射。
3. 执行命令**nat filter-mode** { **endpoint-dependent** | **endpoint-independent** | **endpoint-and-port-dependent** }，配置NAT过滤方式。

   缺省情况下，NAT过滤方式为**endpoint-and-port-dependent**。

5.8.6 （可选）配置两次NAT

背景信息

内外网地址重叠的主机可以根据重叠地址池和临时地址池的映射关系，将重叠地址替换为临时地址同时做NAT，实现内外网的互访。

- 重叠地址池用来指定内网哪些IP允许和外网重叠，只有属于重叠地址池的地址才会做两次NAT。
- 临时地址池指定了用哪些临时IP地址来替换重叠地址池里的地址。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**nat overlap-address** *map-index overlappool-startaddress temppool-startaddress* **pool-length** *length* [**inside-vpn-instance** *inside-vpn-instance-name*]，配置两次NAT重叠地址池和临时地址池的映射关系。

   说明：
   - 重叠地址池和临时地址池的地址个数最大均为255。
   - 当配置中的VPN实例删除时，两次NAT的配置也同步删除。

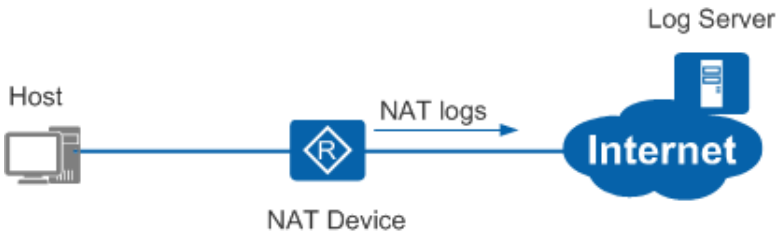
5.8.7 （可选）配置NAT日志输出

背景信息

NAT日志是设备在做NAT时生成的信息记录。该信息包括报文的源IP地址、源端口、目的IP地址、目的端口、转换后的源IP地址、转换后的源端口以及NAT的时间信息和用户执行的操作等。网络管理员可以通过查看NAT日志实时定位用户通过NAT访问网络的情况，增强了网络的安全性。

路由器支持将NAT日志输出至日志服务器，如图5-17所示：

图**5-17** NAT日志输出至指定服务器



操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**firewall log session enable**，使能防火墙日志功能。
3. 执行命令**firewall log session nat enable**，使能NAT类型的流日志功能。
4. （可选）执行命令**nat log-format elog**，将NAT日志设置为elog格式，输出日志为elog服务器规定的可以对接的格式。
5. 执行以下命令配置日志输出到信息中心日志主机或流日志主机：
   - 配置日志输出到信息中心日志主机
     a. 执行命令**info-center enable**，开启信息中心。
     b. 执行命令**info-center loghost** *ip-address* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | | { **vpn-instance** *vpn-instance-name* | **public-net** }] *，配置日志信息输出到日志主机所使用的通道。

        系统最多可配置8个日志主机，实现日志主机间相互备份的功能。

        说明：
        配置日志信息输出到日志主机，有详细的配置举例，请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR1600&AR2200&AR3200&AR3600系列企业路由器 配置指南-设备管理-信息中心配置》中的“配置向日志主机输出日志信息示例”。
   - 配置日志输出到流日志主机

     执行命令**firewall log binary-log host** *host-ip-address host-port* **source** *source-ip-address source-port* [**vpn-instance** *vpn-instance-name*]，配置流日志主机。

缺省情况下，流日志主机未配置。

5.8.8 （可选）配置NAT地址映射表项有效时间

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**firewall-nat session** { { **dns** | **ftp** | **ftp-data** | **http** | **icmp** | **tcp** | **tcp-proxy** | **udp** | **sip** | **sip-media** | **rtsp** | **rtsp-media** | **pptp** | **pptp-data** } | { **tcp** | **udp** } **user-define** *port-number* } **aging-time** *time-value*，配置NAT表项老化时间。

   缺省情况下，各协议的老化时间为：DNS（120秒）、ftp（120秒）、ftp-data（120秒）、HTTP（120秒）、icmp（20秒）、tcp（600秒）、tcp-proxy（10秒）、udp（120秒）、sip（1800秒）、sip-media（120秒）、rtsp（60秒）、rtsp-media（120秒）、pptp（600秒）、pptp-data（600秒）。TCP/UDP协议自定义端口下的会话表项缺省老化时间与对应协议一致。

5.8.9 （可选）使能NAT业务优先功能

前置任务

在使能NAT业务优先功能之前，需要完成以下任务：

- 配置静态地址映射

背景信息

在某些特殊场景，要求NAT业务的优先级高于路由业务，即要求先进行NAT地址转换，然后对转换后的地址查路由表，指导流量转发。例如：当私网设备允许公网设备通过固定IP地址访问时，先配置静态NAT，将私网设备的私网IP地址和指定的公网IP地址进行转换，然后再配置一条到该公网IP地址的静态路由，使公网发往私网的流量能通过NAT引流。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**nat inside priority enable**，使能NAT业务优先于路由业务功能。

   缺省情况下，系统默认为路由业务优先。

   说明：
   AR1600系列不支持此命令。

5.8.10 检查配置结果

操作步骤

- 执行命令**display nat server** [**global** *global-address* | **inside** *host-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-number* [*.subnumber*] | **acl** *acl-number*]，查看NAT Server的配置信息。
- 执行命令**display nat alg**，查看地址转换应用层网关ALG的配置信息。
- 执行命令**display nat dns-map** [*domain-name*]，查看DNS Mapping信息。
- 执行命令**display nat overlap-address** { *map-index* | **all** | **inside-vpn-instance** *inside-vpn-instance-name* }，查看NAT双向地址转换的相关信息。
- 执行命令**display firewall-nat session aging-time**，查看NAT表项老化时间的相关信息。
- 执行命令**display nat sip cac bandwidth information** [**verbose**]，查看设备上的当前总带宽及被占用带宽。
- 执行命令**display nat filter-mode**，查看当前的NAT过滤方式。

执行命令**display nat mapping-mode**，查看NAT映射模式。

- 执行命令**display nat mapping table** { **all** | **number** }或者**display nat mapping table inside-address** *ip-address* **protocol** *protocol-name* **port** *port-number* [**vpn-instance** *vpn-instance-name*]，查看NAT映射表所有表项信息或个数。

5.9 维护

维护NAT包括清除NAT映射表项和监控NAT映射表项。

5.9.1 清除NAT映射表项

背景信息

说明:
表项信息一旦清除则无法恢复，清除命令需慎用。

操作步骤

- 在确认需要清除NAT映射表项后，请在系统视图下执行命令**reset nat session** { **all** | **transit interface** *interface-type interface-number* [*.subnumber*] }。

5.9.2 监控NAT映射表项

操作步骤

- 执行命令**display nat session** { **all** [**verbose**] | **number** }、**display nat session protocol** { *protocol-name* | *protocol-number* } [**source** *source-address* [*source-port*]] [**destination** *destination-address* [*destination-port*]] [**verbose**]、**display nat session source** *source-address* [*source-port*] [**destination** *destination-address* [*destination-port*]] [**verbose**]或**display nat session destination** *destination-address* [*destination-port*] [**verbose**]，查看NAT的映射表项信息。

5.9.3 使能NAT模块定时器自愈功能

背景信息

如果NAT模块的定时器在运行过程中发生异常，会导致NAT业务失效，设备不可用。使能NAT模块定时器自愈功能后，可以自动检测NAT模块定时器的使用情况。当发现定时器出现异常时，通过复位设备消除定时器的异常，保证设备正常运行。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**set nat-session self-healing enable**，使能NAT模块定时器自愈功能。

   缺省情况下，设备的NAT模块定时器自愈功能处于未使能状态。

   说明:
   V200R009C00SPC302版本不支持此功能。

5.10 配置举例

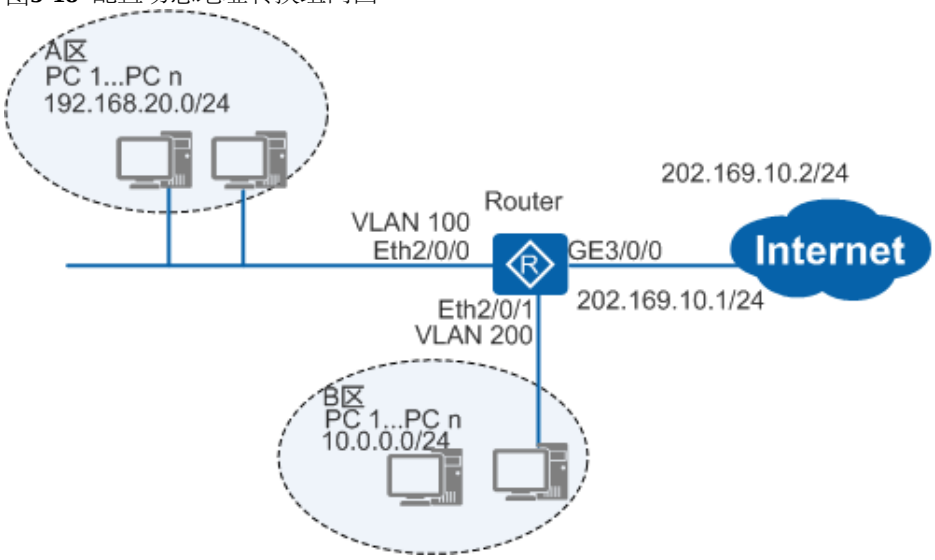
介绍在实际应用中使用NAT的各种举例。

5.10.1 配置动态地址转换示例

组网需求

如图5-18所示，某公司A区和B区的私网用户和互联网相连，路由器上接口GigabitEthernet3/0/0的公网地址为202.169.10.1/24，对端运营商侧地址为202.169.10.2/24。A区用户希望使用公网地址池中的地址（202.169.10.100～202.169.10.200）采用NAT方式替换A区内部的主机地址（网段为192.168.20.0/24），访问因特网。B区用户希望结合B区的公网IP地址比较少的情况，使用公网地址池（202.169.10.80～202.169.10.83）采用IP地址和端口的替换方式替换B区内部的主机地址（网段为10.0.0.0/24），访问因特网。

图**5-18** 配置动态地址转换组网图



配置思路

配置动态地址转换的思路如下:

1. 配置接口IP地址、缺省路由和在WAN侧接口下配置NAT Outbound，实现内部主机访问外网服务功能。

操作步骤

1. 在Router上配置接口IP地址

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan 100
[Router-vlan100] quit
[Router] interface vlanif 100
[Router-Vlanif100] ip address 192.168.20.1 24
[Router-Vlanif100] quit
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] port link-type access
[Router-Ethernet2/0/0] port default vlan 100
[Router-Ethernet2/0/0] quit
[Router] vlan 200
[Router-vlan200] quit
[Router] interface vlanif 200
[Router-Vlanif200] ip address 10.0.0.1 24
[Router-Vlanif200] quit
[Router] interface ethernet 2/0/1
[Router-Ethernet2/0/1] port link-type access
[Router-Ethernet2/0/1] port default vlan 200
[Router-Ethernet2/0/1] quit
[Router] interface gigabitethernet 3/0/0
[Router-GigabitEthernet3/0/0] ip address 202.169.10.1 24
[Router-GigabitEthernet3/0/0] quit
```

2. 在Router上配置缺省路由，指定下一跳地址为202.169.10.2

```
[Router] ip route-static 0.0.0.0 0.0.0.0 202.169.10.2
```

3. 在Router上配置NAT Outbound

```
[Router] nat address-group 1 202.169.10.100 202.169.10.200
[Router] nat address-group 2 202.169.10.80 202.169.10.83
[Router] acl 2000
[Router-acl-basic-2000] rule 5 permit source 192.168.20.0 0.0.0.255
[Router-acl-basic-2000] quit
```

```
[Router] acl 2001
[Router-acl-basic-2001] rule 5 permit source 10.0.0.0 0.0.0.255
[Router-acl-basic-2001] quit
[Router] interface gigabitethernet 3/0/0
[Router-GigabitEthernet3/0/0] nat outbound 2000 address-group 1 no-pat
[Router-GigabitEthernet3/0/0] nat outbound 2001 address-group 2
[Router-GigabitEthernet3/0/0] quit
```

说明:

如果需要在Router上执行**ping -a** *source-ip-address*命令通过指定发送ICMP ECHO-REQUEST报文的源IP地址来验证内网用户可以访问因特网，需要配置命令**ip soft-forward enhance enable**使能设备产生的控制报文的增强转发功能，这样，私网的源地址才能通过NAT转换为公网地址。缺省情况下，设备产生的控制报文的增强转发功能处于使能状态。如果之前已经执行命令**undo ip soft-forward enhance enable**去使能增强转发功能，需要重新在系统视图下执行命令**ip soft-forward enhance enable**。

4. 验证配置结果

在Router上执行命令**display nat outbound**，查看地址转换结果。

```
<Router> display nat outbound
 NAT Outbound Information:
 ----------------------------------------------------------------------
 Interface               Acl      Address-group/IP/Interface   Type
 ----------------------------------------------------------------------
 GigabitEthernet3/0/0     2000                     1          no-pat
 GigabitEthernet3/0/0     2001                     2           pat
 ----------------------------------------------------------------------
  Total : 2
```

在Router上执行命令**ping**，验证内网可以访问因特网。

```
<Router> ping -a 192.168.20.1 202.169.10.2
  PING 202.169.10.2: 56 data bytes, press CTRL_C to break
    Reply from 202.169.10.2: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 202.169.10.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 202.169.10.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 202.169.10.2: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 202.169.10.2: bytes=56 Sequence=5 ttl=255 time=1 ms
-- 202.169.10.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

```
<Router> ping -a 10.0.0.1 202.169.10.2
  PING 202.169.10.2: 56 data bytes, press CTRL_C to break
    Reply from 202.169.10.2: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 202.169.10.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 202.169.10.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 202.169.10.2: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 202.169.10.2: bytes=56 Sequence=5 ttl=255 time=1 ms
-- 202.169.10.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

配置文件

Router的配置文件

```
#
 sysname Router
#
vlan batch 100 200
#
acl number 2000
 rule 5 permit source 192.168.20.0 0.0.0.255
#
acl number 2001
 rule 5 permit source 10.0.0.0 0.0.0.255
#
 nat address-group 1 202.169.10.100 202.169.10.200
 nat address-group 2 202.169.10.80 202.169.10.83
```

```
#
interface Vlanif100
 ip address 192.168.20.1 255.255.255.0
#
interface Vlanif200
 ip address 10.0.0.1 255.255.255.0
#
interface Ethernet2/0/0
 port link-type access
 port default vlan 100
#
interface Ethernet2/0/1
 port link-type access
 port default vlan 200
#
interface GigabitEthernet3/0/0
 ip address 202.169.10.1 255.255.255.0
 nat outbound 2000 address-group 1 no-pat
 nat outbound 2001 address-group 2
#
ip route-static 0.0.0.0 0.0.0.0 202.169.10.2
#
return
```

相关资料

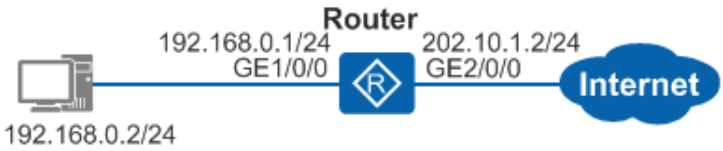
视频：配置NAT Outbound

5.10.2 配置静态一对一NAT示例

组网需求

如图5-19所示，路由器的出接口GE2/0/0的IP地址为202.10.1.2/24，LAN侧网关地址为192.168.0.1/24。对端运营商侧地址为202.10.1.1/24。该主机内网地址为192.168.0.2/24需要使用的固定地址为202.10.1.3/24。要求公司内部能够把私网地址转换为公网地址，连接到广域网。

图**5-19** 配置静态一对一NAT组网图



配置思路

采用如下思路配置静态一对一NAT：

1. 配置接口IP地址、缺省路由并且在WAN侧接口下配置NAT Static，实现内外网地址的一对一映射。

操作步骤

1. 在Router上配置接口IP地址

```
<Huawei> system-view
[Huawei] sysname Router
[Router] interface gigabitethernet 2/0/0
[Router-GigabitEthernet2/0/0] ip address 202.10.1.2 24
[Router-GigabitEthernet2/0/0] quit
[Router] interface gigabitethernet 1/0/0
[Router-GigabitEthernet1/0/0] ip address 192.168.0.1 24
[Router-GigabitEthernet1/0/0] quit
```

2. 在Router上配置缺省路由，指定下一跳地址为202.10.1.1

```
[Router] ip route-static 0.0.0.0 0.0.0.0 202.10.1.1
```

3. 在Router的上行接口GE2/0/0上配置一对一的NAT映射

```
[Router] interface gigabitethernet 2/0/0
[Router-GigabitEthernet2/0/0] nat static global 202.10.1.3 inside 192.168.0.2
```

```
[Router-GigabitEthernet2/0/0] quit
```

4. 验证配置结果

   在Router上执行**display nat static**命令查看地址池映射关系。

```
<Router> display nat static
  Static Nat Information:
  Interface  : GigabitEthernet2/0/0
    Global IP/Port     : 202.10.1.3/----
    Inside IP/Port     : 192.168.0.2/----
    Protocol : ----
    VPN instance-name  : ----
    Acl number         : ----
    Vrrp id            : ----
    Netmask  : 255.255.255.255
    Description : ----

  Total :    1
```

配置文件

Router的配置文件

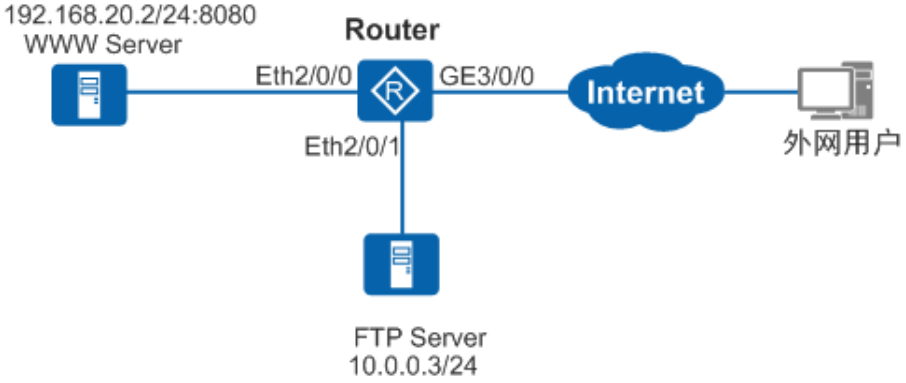
```
#
 sysname Router
#
interface GigabitEthernet1/0/0
 ip address 192.168.0.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 202.10.1.2 255.255.255.0
 nat static global 202.10.1.3 inside 192.168.0.2 netmask 255.255.255.255
#
 ip route-static 0.0.0.0 0.0.0.0 202.10.1.1
#
return
```

5.10.3 配置内部服务器示例

组网需求

如图5-20所示，某公司的网络中提供WWW Server和FTP Server供外部网络用户访问。其中WWW Server的内部IP地址为192.168.20.2/24，提供服务的端口为8080，对外公布的地址为202.169.10.5/24。FTP Server的内部IP地址为10.0.0.3/24，对外公布的地址为202.169.10.33/24，对端运营商侧地址为202.169.10.2/24。要求通过路由器的NAT功能把该公司的内部网络连接到因特网上。

图**5-20** 配置内部服务器组网图



配置思路

采用如下思路配置内部服务器：

1. 配置接口IP地址，并在接口Gigabitethernet 3/0/0上配置NAT Server，实现外部网络用户访问内网服务器功能。
2. 配置Router的缺省路由。
3. 使能FTP的NAT ALG功能，实现外部用户的FTP访问能正常穿越NAT。

操作步骤

1. 在Router上配置接口IP地址和NAT Server

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan 100
[Router-vlan100] quit
[Router] interface vlanif 100
[Router-Vlanif100] ip address 192.168.20.1 24
[Router-Vlanif100] quit
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] port link-type access
[Router-Ethernet2/0/0] port default vlan 100
[Router-Ethernet2/0/0] quit
[Router] vlan 200
[Router-vlan200] quit
[Router] interface vlanif 200
[Router-Vlanif200] ip address 10.0.0.1 24
[Router-Vlanif200] quit
[Router] interface ethernet 2/0/1
[Router-Ethernet2/0/1] port link-type access
[Router-Ethernet2/0/1] port default vlan 200
[Router-Ethernet2/0/1] quit
[Router] interface gigabitethernet 3/0/0
[Router-GigabitEthernet3/0/0] ip address 202.169.10.1 24
[Router-GigabitEthernet3/0/0] nat server protocol tcp global 202.169.10.5 www inside 192.168.20.2 8080

[Router-GigabitEthernet3/0/0] nat server protocol tcp global 202.169.10.33 ftp inside 10.0.0.3 ftp
[Router-GigabitEthernet3/0/0] quit
```

2. 在Router上配置缺省路由，下一跳地址为202.169.10.2

```
[Router] ip route-static 0.0.0.0 0.0.0.0 202.169.10.2
```

3. 在Router上使能FTP的NAT ALG功能

```
[Router] nat alg ftp enable
```

4. 验证配置结果

在Router上执行**display nat server**操作，结果如下。

```
<Router> display nat server
   Nat Server Information:
  Interface  : gigabitethernet 3/0/0
    Global IP/Port     : 202.169.10.5/80(www)
    Inside IP/Port     : 192.168.20.2/8080
    Protocol : 6(tcp)
    VPN instance-name  : ----
    Acl number         : ----
    Vrrp id            : ----
    Description        : ----

    Global IP/Port     : 202.169.10.33/21(ftp)
    Inside IP/Port     : 10.0.0.3/21(ftp)
    Protocol : 6(tcp)
    VPN instance-name  : ----
    Acl number         : ----
    Vrrp id            : ----
    Description        : ----

  Total :    2
```

在Router上执行**display nat alg**操作，结果如下。

```
<Router> display nat alg
NAT Application Level Gateway Information:
----------------------------------
  Application            Status
----------------------------------
  dns                    Disabled
  ftp                    Enabled
  rtsp                   Disabled
  sip                    Disabled
  pptp                   Disabled
```

```
--------------------------------
```

验证外网用户是否能正常访问公司的WWW Server和FTP Server（略）。

配置文件

Router的配置文件

```
#
 sysname Router
#
vlan batch 100 200
#
 nat alg ftp enable
#
interface Vlanif100
 ip address 192.168.20.1 255.255.255.0
#
interface Vlanif200
 ip address 10.0.0.1 255.255.255.0
#
interface Ethernet2/0/0
 port link-type access
 port default vlan 100
#
interface Ethernet2/0/1
 port link-type access
 port default vlan 200
#
interface gigabitethernet 3/0/0
 ip address 202.169.10.1 255.255.255.0
 nat server protocol tcp global 202.169.10.5 www inside 192.168.20.2 8080
 nat server protocol tcp global 202.169.10.33 ftp inside 10.0.0.3 ftp
#
ip route-static 0.0.0.0 0.0.0.0 202.169.10.2
#
return
```

相关资料

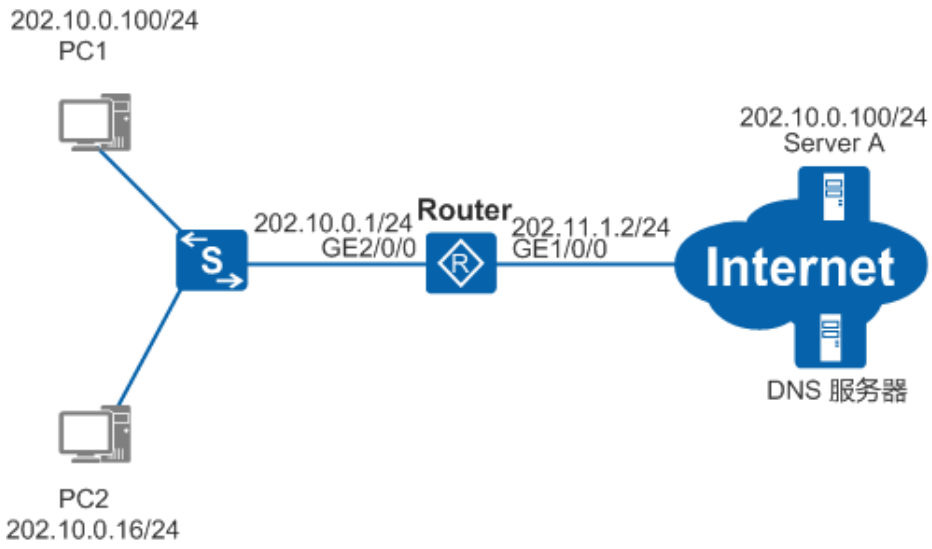
视频：配置NAT Server

5.10.4 配置两次NAT示例

组网需求

如图5-21所示，路由器出接口的地址为202.11.1.2/24，LAN侧网关地址为202.10.0.1/24，对端运营商地址为202.11.1.1/24。公司内网主机IP地址分配不合理，其内部网络主机PC1和公网的服务器Server A的地址重叠。这种情况下，内部网络主机PC2使用Server A的域名访问该服务器，但PC2根据DNS服务器解析的结果很可能访问同在内网的PC1。用户希望将保证报文的正确转发。

图**5-21** 配置两次NAT组网图



配置思路

采用如下思路配置两次NAT:

1. 配置接口IP地址。
2. 配置缺省路由。
3. 配置DNS ALG，实现DNS报文正常穿越NAT。
4. 配置重叠地址池到临时地址池的映射关系，将重叠地址转换为临时地址。
5. 配置NAT Outbound，实现内网用户访问外网服务功能。

操作步骤

1. 在Router上配置接口IP地址

```
<Huawei> system-view
[Huawei] sysname Router
[Router] interface gigabitethernet 1/0/0
[Router-GigabitEthernet1/0/0] ip address 202.11.1.2 24
[Router-GigabitEthernet1/0/0] quit
[Router] interface gigabitethernet 2/0/0
[Router-GigabitEthernet2/0/0] ip address 202.10.0.1 24
[Router-GigabitEthernet2/0/0] quit
```

2. 在Router上配置缺省路由，指定下一跳地址为202.11.1.1

```
[Router] ip route-static 0.0.0.0 0.0.0.0 202.11.1.1
```

3. 在Router上配置重叠地址池到临时地址池的映射关系

```
[Router] nat overlap-address 0 202.10.0.100 202.12.1.100 pool-length 254
```

4. 在Router上配置临时地址池到出接口GE1/0/0的静态路由

```
[Router] ip route-static 202.12.1.100 32 gigabitethernet 1/0/0 202.11.1.1
```

5. 在系统视图下配置DNS的NAT Alg功能

```
[Router] nat alg dns enable
```

6. 在Router的出接口GE1/0/0上配置NAT Outbound

   a. 配置ACL，并配置允许PC1通过的rule。

   ```
   [Router] acl 3180
   [Router-acl-adv-3180] rule 5 permit ip source 202.10.0.0 0.0.0.255
   [Router-acl-adv-3180] quit
   ```

   b. 配置NAT Outbound要使用的NAT地址池。

   ```
   [Router] nat address-group 1 202.11.1.100 202.11.1.200
   ```

   c. 在出接口GE1/0/0上配置常规NAT Outbound。

   ```
   [Router] interface gigabitethernet 1/0/0
   ```

```
[Router-GigabitEthernet1/0/0] nat outbound 3180 address-group 1
[Router-GigabitEthernet1/0/0] quit
```

7. 验证配置结果

在Router上执行**display nat overlap-address all**命令查看地址池映射关系。

```
<Router> display nat overlap-address all
Nat Overlap Address Pool To Temp Address Pool Map Information:
 ------------------------------------------------------------------------------
 Id  Overlap-Address  Temp-Address    Pool-Length       Inside-VPN-Instance-Name
 ------------------------------------------------------------------------------
 0   202.10.0.100     202.12.1.100    254
 ------------------------------------------------------------------------------
  Total : 1
```

在Router上执行**display nat outbound**命令查看NAT Outbound信息。

```
[Router] display nat outbound
 NAT Outbound Information:
 ----------------------------------------------------------------
 Interface              Acl      Address-group/IP/Interface      Type
 ----------------------------------------------------------------
 GigabitEthernet1/0/0    3180                 1                 pat
 ----------------------------------------------------------------
  Total : 1
```

配置文件

Router的配置文件

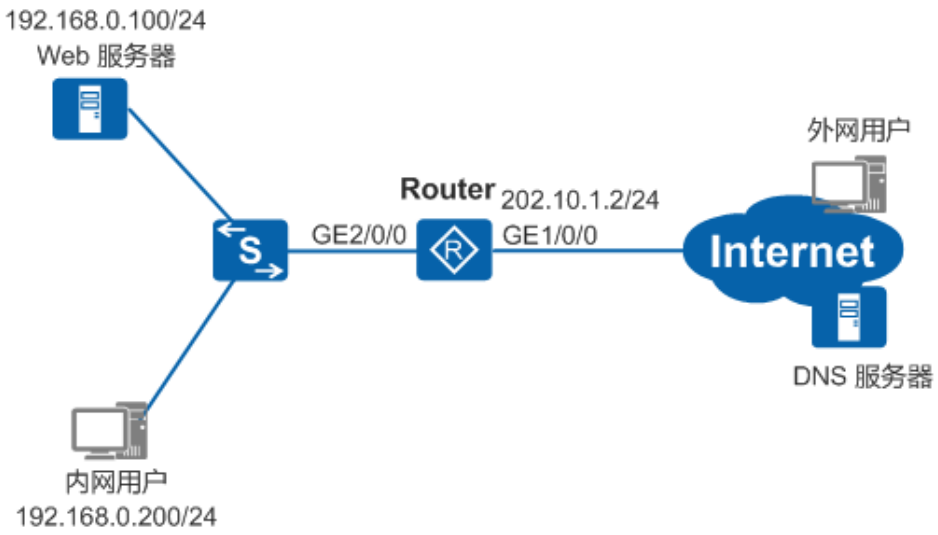
```
#
 sysname Router
#
acl number 3180
 rule 5 permit ip source 202.10.0.0 0.0.0.255
#
 nat alg dns enable
 #
 nat address-group 1 202.11.1.100 202.11.1.200
 #
 nat overlap-address 0 202.10.0.100 202.12.1.100 pool-length 254
#
interface GigabitEthernet2/0/0
 ip address 202.10.0.1 255.255.255.0
#
interface GigabitEthernet1/0/0
 ip address 202.11.1.2 255.255.255.0
 nat outbound 3180 address-group 1
#
ip route-static 0.0.0.0 0.0.0.0 202.11.1.1
ip route-static 202.12.1.100 255.255.255.255 GigabitEthernet1/0/0 202.11.1.1
#
return
```

5.10.5 配置NAT综合示例

组网需求

如图5-22所示，Web服务器的内部IP地址为192.168.0.100/24，采用8080端口提供Web服务。对外公布的公网IP地址为202.10.1.3/24，域名为www.TestNat.com。路由器的出接口GE1/0/0的IP地址为202.10.1.2/24，LAN侧网关地址为192.168.0.1。除此之外该公司没有其他公网IP地址。对端运营商侧地址为202.10.1.1/24。该公司要求通过公司内部的Web服务器对外网用户提供Web服务，同时公司的内网用户还可以访问外网，而且内网用户也可以通过外网的DNS服务器使用域名访问公司内部Web服务器。

图**5-22** 配置NAT综合示例组网图



配置思路

采用如下思路配置NAT综合示例：

- 配置接口IP地址。
- 配置缺省路由。
- 在WAN侧接口下配置Easy IP，实现内部主机访问外网服务功能。
- 在WAN侧接口下配置NAT Server，实现外部网络用户访问内网服务器功能。
- 在Router上配置DNS Mapping和DNS的NAT ALG功能，实现内网用户通过外网的DNS服务器用域名访问内网服务器。

操作步骤

1. 在Router上配置接口IP地址

```
<Huawei> system-view
[Huawei] sysname Router
[Router] interface gigabitethernet 1/0/0
[Router-GigabitEthernet1/0/0] ip address 202.10.1.2 24
[Router-GigabitEthernet1/0/0] quit
[Router] interface gigabitethernet 2/0/0
[Router-GigabitEthernet2/0/0] ip address 192.168.0.1 24
[Router-GigabitEthernet2/0/0] quit
```

2. 在Router上配置缺省路由，指定下一跳地址为202.10.1.1

```
[Router] ip route-static 0.0.0.0 0.0.0.0 202.10.1.1
```

3. 在Router的上行接口GE1/0/0上配置Easy IP方式的NAT Outbound

```
[Router] acl 2000
[Router-acl-basic-2000] rule 5 permit source 192.168.0.0 0.0.0.255
[Router-acl-basic-2000] quit
[Router] interface gigabitethernet 1/0/0
[Router-GigabitEthernet1/0/0] nat outbound 2000
[Router-GigabitEthernet1/0/0] quit
```

4. 在Router的上行接口GE1/0/0上配置NAT Server

```
[Router] interface gigabitethernet 1/0/0
[Router-GigabitEthernet1/0/0] nat server protocol tcp global 202.10.1.3 www inside 192.168.0.100 8080
[Router-GigabitEthernet1/0/0] quit
```

5. 在Router上配置DNS的NAT Alg功能和DNS Mapping

```
[Router] nat alg dns enable
[Router] nat dns-map www.TestNat.com 202.10.1.3 80 tcp
[Router] quit
```

6. 验证配置结果

   # 在Router上执行**display nat outbound**操作，结果如下。

```
<Router> display nat outbound
```

```
NAT Outbound Information:
-------------------------------------------------------------------------
Interface                    Acl      Address-group/IP/Interface      Type
GigabitEthernet1/0/0         2000                     202.10.1.2      easyip
-------------------------------------------------------------------------
 Total : 1
```

在Router上执行**display nat server**操作，结果如下。

```
<Router> display nat server
  Nat Server Information:
  Interface  : GigabitEthernet 1/0/0
    Global IP/Port     : 202.10.1.3/80(www)
    Inside IP/Port     : 192.168.0.100/8080
    Protocol : 6(tcp)
    VPN instance-name  : ----
    Acl number         : ----
    Vrrp id            : ----
    Description : ----
  Total :    1
```

在Router上执行**display nat alg**操作，结果如下。

```
<Router> display nat alg
NAT Application Level Gateway Information:
----------------------------------
  Application            Status
----------------------------------
  dns                    Enabled
  ftp                    Disabled
  rtsp                   Disabled
  sip                    Disabled
  pptp                   Disabled
----------------------------------
```

配置文件

Router的配置文件

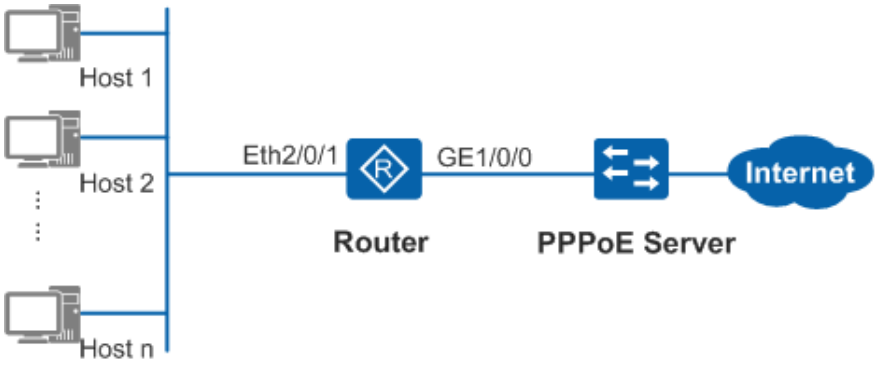
```
#
 sysname Router
#
acl number 2000
 rule 5 permit source 192.168.0.0 0.0.0.255
#
 nat alg dns enable
 #
 nat dns-map www.testnat.com 202.10.1.3 80 tcp
#
interface GigabitEthernet2/0/0
 ip address 192.168.0.1 255.255.255.0
#
interface GigabitEthernet1/0/0
 ip address 202.10.1.2 255.255.255.0
 nat server protocol tcp global 202.10.1.3 www inside 192.168.0.100 8080
 nat outbound 2000
#
 ip route-static 0.0.0.0 0.0.0.0 202.10.1.1
#
return
```

5.10.6 配置PPPoE拨号通过Easy IP访问外网示例

组网需求

如图5-23所示，路由器作为PPPoE客户端由服务器分配IP地址。其中，路由器的Eth2/0/1地址为192.168.0.1/24，PPPoE服务器的IP地址为178.18.1.1/16。企业内的主机通过路由器连接网络。路由器采用PPPoE拨号方式从PPPoE服务器动态获取公网IP地址。用户希望企业网内的主机可以访问外网。

图**5-23** 配置PPPoE拨号通过Easy IP访问外网组网图



配置思路

采用如下的思路配置PPPoE拨号通过Easy IP访问外网：

通过创建拨号口并配置拨号口相关参数、建立PPPoE会话、配置Router的静态路由和在设备的拨号口上配置Easy IP，实现配置PPPoE拨号通过Easy IP访问外网的目标。

操作步骤

1. 配置PPPoE服务器端

   PPPoE服务器端需要配置认证方式、IP地址获取方式或设置为PPPoE客户端分配的IP地址或地址池。不同设备作为PPPoE服务器的配置过程也不同，请参考具体设备的相关资料。Router作为PPPoE服务器的配置请参见配置设备作为PPPoE Server示例。

2. 配置拨号口

```
<Huawei> system-view
[Huawei] sysname Router
[Router] dialer-rule
[Router-dialer-rule] dialer-rule 1 ip permit
[Router-dialer-rule] quit
[Router] interface dialer 1
[Router-Dialer1] dialer user user2
[Router-Dialer1] dialer-group 1
[Router-Dialer1] dialer bundle 1
[Router-Dialer1] dialer timer idle 300
INFO:  The configuration will become effective after link reset.
[Router-Dialer1] dialer queue-length 8
[Router-Dialer1] ppp chap user user1@system
[Router-Dialer1] ppp chap password cipher huawei123
[Router-Dialer1] ip address ppp-negotiate
[Router-Dialer1] quit
```

3. 建立PPPoE会话

```
[Router] interface gigabitethernet 1/0/0
[Router-GigabitEthernet1/0/0] pppoe-client dial-bundle-number 1 on-demand
[Router-GigabitEthernet1/0/0] quit
```

4. 配置路由器的静态路由

```
[Router] ip route-static 0.0.0.0 0 dialer 1
```

5. 在拨号口上配置Easy IP方式的NAT Outbound

```
[Router] acl 2000
[Router-acl-basic-2000] rule 5 permit source 192.168.0.0 0.0.0.255
[Router-acl-basic-2000] quit
[Router] interface dialer 1
[Router-Dialer1] nat outbound 2000
[Router-Dialer1] quit
```

6. 验证配置结果

   # 执行命令**display pppoe-client session summary**查看PPPoE会话的状态和配置信息。根据显示信息判断会话状态是否正常（状态为up表示正常）、配置是否正确（是否和之前的数据规划和组网一致）。

```
<Router> display pppoe-client session summary
PPPoE Client Session:
ID    Bundle  Dialer  Intf            Client-MAC    Server-MAC    State
1     1       1       GE1/0/0         00e0fc030201  00e0fc030206  PPPUP
```

待拨号成功后，在Router上执行**display nat outbound**操作，结果如下。

```
<Router> display nat outbound
NAT Outbound Information:
--------------------------------------------------------------------------
Interface                       Acl      Address-group/IP/Interface      Type
--------------------------------------------------------------------------
Dialer1                        2000                       178.18.1.2       easyip
--------------------------------------------------------------------------
 Total : 1
```

配置文件

Router的配置文件

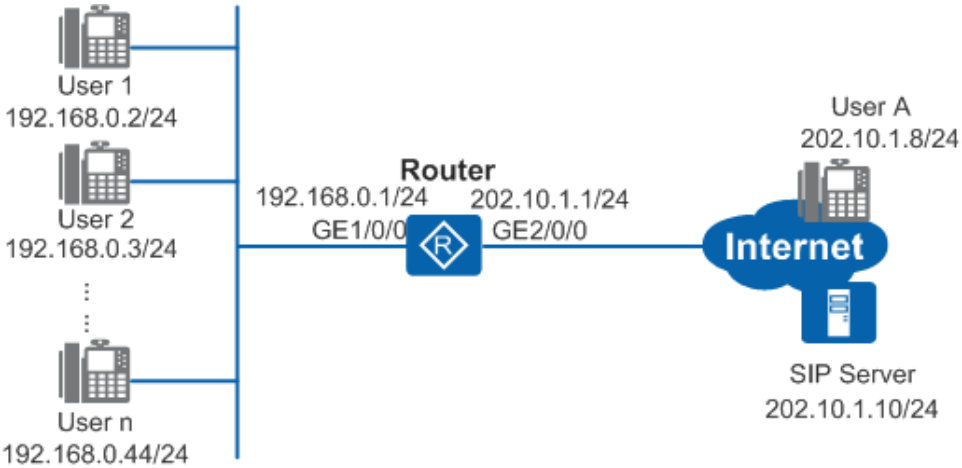
```
#
 sysname Router
#
acl number 2000
 rule 5 permit source 192.168.0.0 0.0.0.255
#
dialer-rule
 dialer-rule 1 ip permit
#
interface Dialer1
 link-protocol ppp
 ppp chap user user1@system
 ppp chap password cipher %^%#R=>NT8A-8KmWU38WOZq(s%MsRSg>3,}19b%K.%!S%^%#
 ip address ppp-negotiate
 dialer user user2
 dialer bundle 1
 dialer queue-length 8
 dialer timer idle 300
 dialer-group 1
 nat outbound 2000
#
interface GigabitEthernet1/0/0
 pppoe-client dial-bundle-number 1 on-demand
#
 ip route-static 0.0.0.0 0.0.0.0 Dialer1
#
return
```

5.10.7 配置NAT设备上的SIP呼叫带宽限制示例

组网需求

如图5-24所示，Router作为NAT网关连接企业内部和Internet，企业内部有多台SIP Phone用户，都经常和Internet上的SIP Phone用户User A通信，比如企业内部多个用户和Internet上的SIP Phone召开电话会议。SIP Phone上的语音配置和Router上的NAT配置都已经完成，企业内部的用户可以呼叫Internet上的SIP Phone用户。由于NAT设备上的带宽有限，要求在NAT设备上对SIP呼叫进行带宽限制，超过指定带宽限制的SIP呼叫将无法成功。

图**5-24** 配置NAT设备上的SIP呼叫带宽限制组网图



配置思路

采用如下思路配置NAT设备上的SIP呼叫带宽限制：

使能CAC功能并配置设备的总带宽值，对呼叫进行带宽限制处理。

操作步骤

1. 在Router上使能CAC功能并配置设备的总带宽值为2000Kbps

```
<Huawei> system-view
[Huawei] sysname Router
[Router] nat sip cac enable bandwidth 2000
[Router] quit
```

2. 验证配置结果

在Router上执行**display nat sip cac bandwidth information verbose**命令查看当前配置的总带宽及被占用带宽的详细信息。

```
<Router> display nat sip cac bandwidth information verbose
------------------------------------------------------------------------------
Total Bandwidth(Kbps)       Used Bandwidth(Kbps)
  2000                        1900
------------------------------------------------------------------------------
Src-IP          Src-Port Dest-IP         Dest-Port Protocol Used Bandwidth(Kbps)
192.168.0.2     50       202.10.1.10     5060      udp         600
192.168.0.3     50       202.10.1.10     5060      udp         700
192.168.0.4     50       202.10.1.10     5060      udp         600
------------------------------------------------------------------------------
```

企业内部的User 1、User 2、User 3可以同时和Internet上的User A召开电话会议（带宽未超过2000Kbps）。如果接入电话会议的用户总带宽超过2000Kbps，则呼叫失败。

配置文件

Router的配置文件

```
#
 sysname Router
#
nat sip cac enable bandwidth 2000
#
return
```

5.11 常见配置错误

介绍常见配置错误的案例，避免在配置阶段引入故障。

5.11.1 NAT Outbound故障现象：内网用户无法访问公网

故障现象

本类故障的常见原因包括：

- 未在访问公网的出接口上正确配置NAT Outbound。
- NAT Outbound引用的ACL配置错误。

操作步骤

1. 检查设备的接口是否有报文进入

在设备上执行**display interface** *interface-type interface-number*命令，查看显示信息的**Input**字段值。

- 如果**Input**字段值为0，表示设备没有报文进入，请排查接口的配置，保证接口能接收报文。
- 如果**Input**字段值不为0，请执行步骤2。

说明:

设备支持GE、FE、Eth-Trunk及子接口等多种接口。如果使用的是Eth-Trunk子接口，使用**display interface eth-trunk** [*trunk-id* [*.subnumber*]] 命令查看接口是否有报文进入。

2. 检查NAT Outbound绑定的ACL规则，是否允许NAT业务报文通过

在设备上执行命令**display nat outbound**，查看出接口上是否正确配置了NAT Outbound。

```
[Huawei]display nat outbound
 NAT Outbound Information:
 --------------------------------------------------------------------------
 Interface                       Acl      Address-group/IP/Interface      Type
 --------------------------------------------------------------------------
 GigabitEthernet0/0/0          2000                                  1    no-pat
 --------------------------------------------------------------------------
  Total : 1
```

由显示信息可知NAT出接口GigabitEthernet0/0/0上NAT Outbound关联的ACL号为2000。

然后查看ACL 2000的规则配置是否正确。如果ACL 2000未配置正确的IP地址、端口号或协议类型，将导致报文无法正常出入网络。

使用命令**display acl 2000**查看当前ACL 2000关联的NAT Outbound配置。

```
[Huawei] display acl 2000
Basic ACL2000, 1 rule
Acl's step is 5
rule 5 permit source 192.168.1.100 0
```

根据ACL规则可以看出，源地址为192.168.1.100的报文才能够匹配该ACL规则，进行NAT业务。

- 如果ACL匹配规则配置错误，请重新进行配置。
- 如果ACL匹配规则配置正确，故障仍然存在，请执行步骤3。

3. 检查地址池配置是否正确

在设备上执行命令**display nat address-group**，查看出接口上NAT Outbound所绑定的地址池是否正确。

```
[Huawei] display nat address-group 1
NAT Address-Group Information:
--------------------------------------
Index   Start-address      End-address
--------------------------------------
1       10.0.0.100         10.0.0.110
--------------------------------------
Total : 1
```

针对Easy IP方式，需要在设备上执行命令**display nat outbound**，查看NAT出接口上配置的Easy IP信息。

```
[Huawei] display nat outbound
 NAT Outbound Information:
 --------------------------------------------------------------------------
 Interface                       Acl      Address-group/IP/Interface      Type
 --------------------------------------------------------------------------
 GigabitEthernet0/0/1          2000                        30.30.30.1    easyip
 --------------------------------------------------------------------------
  Total : 1
```

由上述信息可以看到出接口GigabitEthernet0/0/1配置的是Easy IP方式，并且绑定的地址池是接口上发布的地址30.30.30.1。如果NAT不通，需要确认:

- 绑定的IP地址是否是接口的IP地址，如果是则需要确认接口地址的有效性

5.11.2 NAT Server故障现象：外网主机无法访问内网服务器

故障现象

本类故障的常见原因主要包括:

- NAT Server配在错误的接口上（比如，配置在出接口上，或其他不相关的接口上），正确应该配置在外网主机访问内网的入接口上。
- NAT Server配置错误（比如，配置的内部Server对应的公网、私网IP地址不对，私网端口和内部服务器打开的端口不

一样）。

操作步骤

1. 检查内网NAT Server上的应用服务正常

   当从外网无法访问NAT Server所提供的服务时，先确认内网服务器上相应的服务（例如HTTP Server，FTP Server等）是否打开。可以从内网其他主机上尝试访问内网服务器，以确保相应服务正在运行。

   - 如果内网NAT Server上的应用服务未正常运行，请打开相应服务。
   - 如果内网NAT Server上的应用服务正常运行，故障仍然存在，请执行步骤2。

2. 检查NAT Server配置是否正确

   在设备上执行命令**display nat server**，查看NAT Server是否配置在正确的NAT接口上，是否配置了正确的协议、端口和地址信息。

   ```
   [Huawei] display nat server
     Nat Server Information:
     Interface  : GigabitEthernet 2/0/0
       Global IP/Port     : 202.10.1.3/80 (www)
       Inside IP/Port     : 192.168.0.100/8080
       Protocol : 6(tcp)
       VPN instance-name  : ----
       Acl number         : ----
       Vrrp id            : ----
       Description : ----
     Total :    1
   ```

   特别需要注意的是，被映射的内网地址和端口是否正确。某些服务传送报文数据时，会使用到多个端口（有些端口是随机产生的），例如FTP和TFTP，因此为这些服务配置NAT Server时，应该把对端口的限制放开，使得内部服务器可以正常提供服务。

   - 如果NAT Server配置错误，请重新进行正确配置。
   - 如果NAT Server配置正确，故障仍然存在，请执行步骤3。

3. 检查外网主机和NAT Server外网接口之间的连接及配置

   检查NAT Server外网接口上的IP地址以及为NAT Server配置的外网IP地址是否正确。例如，是否和其他该网段的地址发生冲突。从外网主机上ping NAT Server的外网接口地址，确保外网主机到NAT Server之间的连通性。

   - 如果外网主机和NAT Server外网接口之间的连通性存在问题，请检查并确保连通性正常。
   - 如果外网主机和NAT Server外网接口之间的连通性正常，故障仍然存在，请执行步骤4。

4. 检查内网NAT Server的网关或路由配置

   检查内网服务器上是否配置了正确的路由或者网关，使得发向外网的报文可以正确的送到NAT网关。

   - 如果NAT Server的网关或路由配置有问题，请重新进行正确配置。
   - 如果NAT Server的网关或路由配置正常，故障仍然存在，请联系技术支持人员。

5.11.3 两次NAT故障现象：内网重叠主机无法访问外网服务器

故障现象

本类故障的常见原因包括：

- 内网访问公网对应的出接口上配置NAT Outbound错误。
- 未使能DNS协议的NAT ALG。
- 配置的DNS Mapping错误（比如，对应的公网地址和外网服务器IP地址不同）。
- 没有配置从内网临时地址到NAT公网出接口的路由。

操作步骤

1. 检查配置的NAT Outbound是否正确

在设备上执行命令**display nat outbound**，查看NAT出接口上是否配置了NAT Outbound。

```
[Huawei]display  nat outbound
 NAT Outbound Information:
 ----------------------------------------------------------------------------
 Interface                       Acl      Address-group/IP/Interface      Type
 ----------------------------------------------------------------------------
 GigabitEthernet0/0/1          3180                                  1       pat
 ----------------------------------------------------------------------------
  Total : 1
```

由上可知NAT Outbound关联的ACL号为3180，地址池索引为1。查看NAT Outbound引用的地址池是否正确，地址池的配置需要注意：避免外网目的地址和地址池中的地址重复。通过执行命令**display nat address-group**查看地址池配置信息。

```
[Huawei]display nat address-group 1
NAT Address-Group Information:
--------------------------------------
Index   Start-address      End-address
--------------------------------------
1       202.10.10.10     202.10.10.100
--------------------------------------
Total : 1
```

最后再查看NAT Outbound关联的ACL规则是否正确，ACL规则常见问题有：没有配置合适的地址、协议、端口等，导致内网报文无法送出或外网报文无法进入。

执行命令**display acl 3180**查看当前NAT Outbound关联的ACL配置。

```
[Huawei]display acl 3180
Advanced ACL 3180, 1 rule
Acl's step is 5
rule 5 permit tcp source 1.1.1.1 0
```

说明：

ACL规则一般配置比较严格，只根据具体的组网需求开放特定的地址段、协议或端口。当某种协议的报文无法通过NAT网关时，先检查ACL中是否配置了允许该类报文通过的规则。

- 如果NAT Outbound配置错误，请修改对应配置。
- 如果NAT Outbound配置正确，故障仍然存在，请执行步骤2。

2. 检查DNS Mapping配置是否正确

在设备上执行命令**display nat dns-map**，查看DNS Map是否配置在正确的NAT出接口上，是否配置了正确的协议、端口和地址信息。

```
[Huawei]display nat dns-map
  NAT DNS mapping information:
  Domain-name : test1
  Global IP   : 10.1.1.1
  Global port : 2012
  Protocol    : tcp

  Total : 1
```

- 如果DNS Mapping配置错误，请在系统视图下执行命令**nat dns-map**，配置正确的DNS Mapping，再尝试访问主机。
- 如果DNS Mapping配置正确，故障仍然存在，请执行步骤3。

3. 检查是否使能了DNS协议的NAT ALG功能

在设备上执行命令**display nat alg**，查看DNS的NAT ALG是否使能。

```
[Huawei]display nat alg
NAT Application Level Gateway Information:
---------------------------------
  Application           Status
---------------------------------
  dns                   Disabled
  ftp                   Disabled
  rtsp                  Enabled
  sip                   Disabled
  pptp                  Disabled
---------------------------------
```

- 如果DNS的NAT ALG未使能，请使用**nat alg**使能NAT ALG。
- 如果DNS的NAT ALG已使能，故障仍然存在，请执行步骤4。

4. 检查配置的重叠地址池到临时地址池的映射是否正确

   在设备上执行命令**display nat overlap-address**，查看所有已配置的重叠地址池到临时地址池的映射。

```
[Huawei]display nat overlap-address all
Nat Overlap Address Pool To Temp Address Pool Map Information:
 ------------------------------------------------------------------------------
 Id  Overlap-Address  Temp-Address  Pool-Length  Inside-VPN-Instance-Name
 ------------------------------------------------------------------------------
 1   1.1.1.1          20.20.20.20     34
------------------------------------------------------------------------------
  Total : 1
```

   说明：

   临时地址池是设备上空闲可用的IP地址，不能和接口地址、VRRP地址、NAT类型地址存在冲突。 Inside-VPN-Instance-Name表示和主机连接的内网接口所在的VPN实例名。

   - 如果映射关系不正确，请重新进行正确配置。
   - 如果映射关系正确，故障仍然存在，请执行步骤5。

5. 检查是否配置临时地址池到NAT出接口的路由

   在设备上执行命令**display ip routing-table**，查看公网上的所有路由。

```
[Huawei]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 2        Routes : 2

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

    10.0.0.0/8     Static   60   0           D   10.164.50.1     Ethernet1/0/0
    10.10.10.10/32 Direct   64   0           D   127.0.0.1       Vlanif3
```

   说明：

   若主机连接的内网接口所在的VPN实例名不为空，则查询路由使用**display ip routing-table vpn-instance** *vpn-name*。

   - 如果没有正确的路由表项，请检查并重新配置路由。
   - 如果路由表项正确，故障仍然存在，请联系技术支持人员。

5.12 FAQ

介绍NAT的常见问题。

5.12.1 NAT是否支持VPN多实例

NAT支持VPN多实例。

5.12.2 如何查看NAT的流表信息

执行**display nat session all**命令查看NAT的流表信息。

5.12.3 如何手动强制老化NAT的流表

执行**reset nat session all**命令强制老化NAT的流表。

5.12.4 NAT Server的global地址可以是NAT Outbound地址池中的地址吗

可以。

5.12.5 如何使能NAT日志使能并设置日志采集时间

NAT日志是设备在做NAT时生成的信息记录。

配置举例

配置NAT日志的输出时间间隔为200秒。

```
<Huawei> system-view
[Huawei] firewall log all enable
[Huawei] info-center enable
[Huawei] firewall log defend log-interval 200
```

5.12.6 如何设置流表老化时间

firewall-nat session aging-time命令用来配置各种会话表项的老化时间。

配置举例

配置FTP会话的流表老化时间为60秒。

```
<Huawei> system-view
[Huawei] firewall-nat session ftp aging-time 60
```

5.12.7 内网用户通过域名无法访问内网服务器

客户的设备请求域名时可能携带主机名，也可能不携带主机名（根据客户实际情况）。在这两种情况下，配置需要解析的域名时，需要分情况处理。例如，客户需要访问的域名为www.hbjs.gov.cn：

- 若客户设备发送的DNS请求携带主机名，即客户设备对域名www.hbjs.gov.cn进行请求时，需要使用命令**nat dns-map** *www.hbjs.gov.cn global-address global-port* { **tcp** | **udp** }，进行配置。
- 若客户设备发送的DNS请求不携带主机名，即客户设备对域名hbjs.gov.cn进行请求时，需要使用命令**nat dns-map** *hbjs.gov.cn global-address global-port* { **tcp** | **udp** }，进行配置。

说明：

如果您对您的设备在进行DNS请求时是否携带主机名并不了解，我们建议您配置全部两条命令。

5.12.8 私网用户和私网服务器在同一个VLAN下，在VLANIF接口下配置nat server映射服务器公网地址，用户以公网地址访问服务器失败

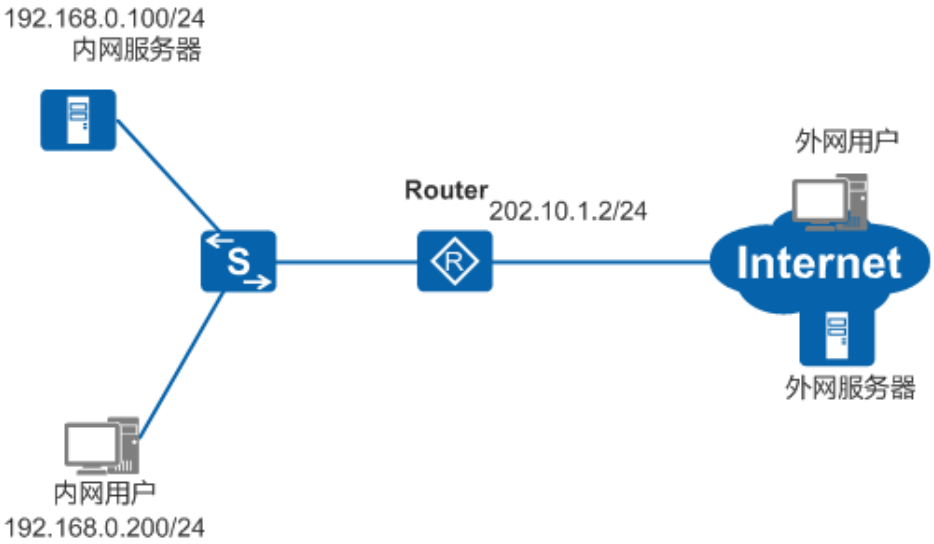
私网用户和私网服务器属于同一个VLANIF接口并且在同一个子卡下，当在VLANIF接口下配置**nat server**映射服务器公网地址时，服务器回应用户的报文无法上送CPU处理进行NAT转换，导致用户和服务器之间的连接建立失败。这种情况下可以在VLANIF接口下同时配置**nat outbound**，服务器回应报文就会经过路由器并进行NAT转换，路由器将回应报文转发给私网用户，私网用户和私网服务器之间的连接才可以成功建立。

5.12.9 NAT Server和NAT Static的区别是什么

配置NAT Server和NAT Static的区别就是：NAT Server对于内网主动访问外网的情况不做端口替换，仅作地址替换；NAT Static对于内网主动访问外网的情况会同时替换地址和端口号。

如图5-25所示，企业希望内网用户可以正常访问外网服务器，外网用户可以正常访问内网服务器。如果在Router上同时配置了NAT Server和Easy IP功能，由于NAT Server对于内网主动访问外网的情况不做端口替换，仅作地址替换，可能会存在流表建立失败的情况，建议用户在这种情况可将NAT Server配置改为NAT Static。

图**5-25** 配置NAT综合示例组网图



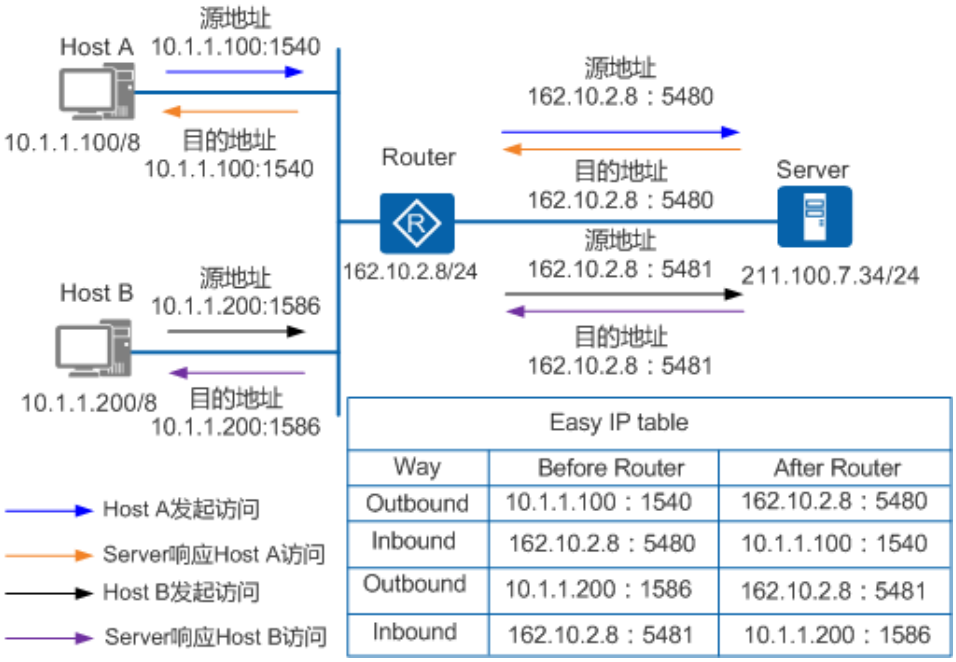
5.12.10 设备作为SIP Server，出口处配置NAT Server后，外网话机注册失败

SIP Server在内网的场景下，用户在出口处配置NAT server，在内网入口配置MTU值。由于发送报文正常情况下是强制不分片的，所以在配置MTU值后，报文强制分片，设备会响应ICMP ERROR报文，外网话机注册失败。这种情况下需要在内网入口取消MTU配置或者通过命令**ip soft-forward enhance enable**使能设备的IP增强转发功能，从而实现正常的NAT转换，使外网话机可以正常注册。

5.12.11 NAT功能中Easy IP方式跟地址池方式的区别

采用Easy IP方式进行NAT映射时，接口的IP地址作为映射后的公网地址，如图5-26所示。

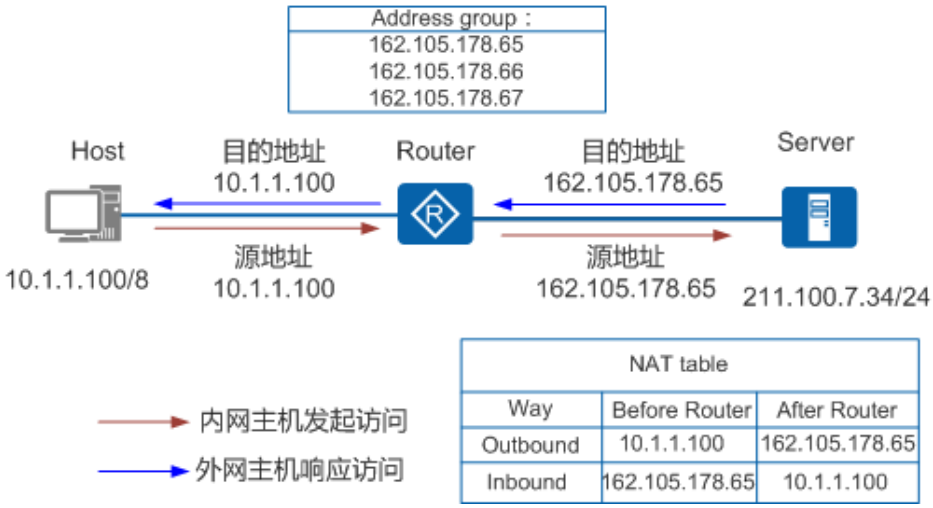
图**5-26** Easy IP方式NAT映射组网图



Easy IP table		
Way	Before Router	After Router
Outbound	10.1.1.100：1540	162.10.2.8：5480
Inbound	162.10.2.8：5480	10.1.1.100：1540
Outbound	10.1.1.200：1586	162.10.2.8：5481
Inbound	162.10.2.8：5481	10.1.1.200：1586

采用地址池方式进行NAT映射时，需要配置公网地址池，私网地址映射的公网地址会从公网地址池中选择，如图5-27所示。

图**5-27** 地址池方式NAT映射组网图



用户通过NAT功能访问公网时，可以根据公网IP的规划情况选择以下其中一种方式：

- 用户在配置了NAT设备出接口的IP和其他应用之后，还有空闲公网IP地址，可以选择地址池方式的NAT映射。
- 用户在配置了NAT设备出接口的IP和其他应用之后，已没有其他可用公网IP地址，可以选择Easy IP方式的NAT映射。

5.12.12 设备支持NAT功能的接口包括哪些

设备支持NAT功能的接口包括：

- 物理接口：

  三层Ethernet接口、三层GigabitEthernet接口、G.SHDSL接口、ADSL接口、VDSL接口、PON接口、Serial接口、POS接口、Async接口、ATM接口、BRI接口和Cellular接口。

- 逻辑接口：

  Dialer接口、Tunnel接口、三层Eth-Trunk接口、VE接口、VLANIF接口、VT接口、IP-Trunk接口、Mp-group接口、MFR接口和IMA-Group接口。

- 子接口：

  以太子接口、Eth-Trunk子接口、ATM子接口、Serial子接口、MFR子接口、IMA-Group子接口、PON子接口和POS子接口。

5.12.13 设备作为出口网关配置NAT后，带源地址（私网地址）无法ping通公网地址

在设备上配置NAT Outbound实现私网地址到公网地址的转换后，执行命令**ping -a** *source-ip-address host*（源地址为私网地址）前，需要先执行命令**ip soft-forward enhance enable**使能设备的IP增强转发功能，这样，设备发送报文时会将私网的源地址转换为公网地址。

5.12.14 配置NAT地址池后，发往该地址池中IP地址的报文被丢弃，应如何避免

接口下配置NAT地址池后，会自动生成一条32位UNR本机路由，其优先级为64。发往该地址的过路报文经过路由器时，会命中该32位本机路由送至设备协议栈。但由于设备缺少该IP地址的协议栈，路由器无法转发该报文，则会将报文丢弃。

可以使用命令**ip route-static**配置一条静态路由。静态路由优先级缺省值为60，高于自动产生的UNR路由，可以防止发往该地址池中IP地址的报文被意外丢弃。

例如，配置使用NAT地址池方式对10.110.10.0/24网段的主机进行多对一的地址转换，NAT地址池中地址为1.1.1.1。

```
<Huawei> system-view
[Huawei] acl number 2001
[Huawei-acl-basic-2001] rule permit source 10.110.10.0 0.0.0.255
[Huawei-acl-basic-2001] quit
[Huawei] nat address-group 1 1.1.1.1 1.1.1.1
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] nat outbound 2001 address-group 1
[Huawei-GigabitEthernet0/0/1] quit
```

配置完成后查看路由列表。列表中新增一条优先级为64的UNR路由。

```
[Huawei] display ip routing-table
Route Flags:Route Flags: R - relay, D - download to fib
```

```
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 5        Routes : 5

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        1.1.1.1/32  Unr     64   0           D   127.0.0.1       InLoopBack0
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

通过命令行**ip route-static**配置一条目的地址为1.1.1.1的静态路由。配置完成后查看路由表。

```
[Huawei] ip route-static 1.1.1.1 32 192.168.200.100
[Huawei] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 6       Routes : 6

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        1.1.1.1/32  Static  60   0          RD   192.168.200.100 GigabitEthernet0/0/0
        1.1.1.1/32  Unr     64   0           D   127.0.0.1       InLoopBack0
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

如路由表中所示，新增一条目的地址为1.1.1.1的静态路由，此后到该地址的报文都会根据此路由转发。

5.12.15 配置DNS Mapping后，CPU占用率高应如何解决

配置DNS Mapping之后，发出的报文会经过CPU处理后转发。报文数量大时，会造成CPU占用率高。

CPU持续占用率高并影响使用时，建议删除DNS Mapping配置并关闭DNS ALG功能以阻止报文上送CPU，从而降低CPU占用率。同时在内网侧接口下增加相应的NAT Server配置，在保护设备的同时满足用户的使用需求。

内网用户通过域名访问内网服务器时，发送域名请求到DNS Server，DNS Server将此域名对应的公网IP地址封装在回应报文中。在配置了DNS Mapping和ALG功能的情况下，路由器向内网用户转发DNS回应报文时，会将其中封装的公网IP地址转换为内网IP地址。但删除DNS Mapping和ALG配置后，路由器无法进行此项IP地址转换。在内网侧接口下增加NAT Server配置，可以使公网IP地址转换为内网服务器地址，满足内网用户访问内网服务器的需求。

具体配置步骤如下。

1. 在NAT设备上执行命令**undo nat alg enable**关闭DNS ALG功能，并执行命令**undo nat dns-map**删除DNS Mapping配置。
2. 在内网侧的接口下使用命令**nat server**增加相应的NAT Server配置，在内网用户访问内网服务器时，将服务器公网地址转换为内网地址。

如下所示，首先关闭DNS ALG功能并删除DNS Mapping配置。

```
<Huawei> system view
[Huawei] undo nat dns-map www.bz2z.com 220.180.111.161 80 tcp
[Huawei] undo nat dns-map bz2z.com 220.180.111.161 80 tcp
```

假设公网端口为GE0/0/0，内网端口为GE0/0/1。查看公网端口配置。

```
[Huawei] interface gigabitethernet 0/0/0
[Huawei-GigabitEthernet0/0/0] display this
#
interface GigabitEthernet0/0/0
 ip address 202.100.1.10 255.255.255.0
 nat server protocol tcp global current-interface 80 inside 192.168.1.100 80
 nat outbound 3001
[Huawei-GigabitEthernet0/0/0] quit
```

在内网入接口配置NAT Server，并将公网口NAT Server配置中关键字**current-interface**修改为指定的公网接口。

```
[Huawei-GigabitEthernet0/0/1] nat server protocol tcp global interface gigabitethernet 0/0/0 80 inside 192.168.1.100
80
```

此时CPU占用率下降，内网用户也可以正常访问内网服务器。

5.13 参考信息

本特性的参考资料清单如下:

文档	描述
RFC 1631	The IP Network Address Translator (NAT)
RFC 2663	IP Network Address Translator (NAT) Terminology and Considerations
RFC 2709	Security Model with Tunnel-mode IPsec for NAT Domains
RFC 2993	Architectural Implications of NAT
RFC 3022	Traditional IP Network Address Translator (Traditional NAT)
RFC 3235	Network Address Translator (NAT)-Friendly Application Design Guidelines
RFC 3519	Mobile IP Traversal of Network Address Translation (NAT) Devices
RFC 3715	IPsec-Network Address Translation (NAT) Compatibility Requirements
RFC 3947	Negotiation of NAT-Traversal in the IKE
RFC 4008	Definitions of Managed Objects for Network Address Translators (NAT)
RFC 4787	Network Address Translation (NAT) Behavioral Requirements for Unicast UDP