目 录

1 NAT

1.1 NAT简介

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

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

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

1.1.1 NAT工作机制

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

1. 基本概念

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

2. NAT的基本组网类型

(1) 传统 NAT

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

(2) 两次 NAT

报文入接口和出接口均为 NAT 接口。报文经过 NAT 设备时，先后进行两次 NAT 转换。对于内网访问外网的报文和外网访问内网的报文，均在入接口进行目的 IP 地址转换，在出接口进行源 IP 地址转换。这种方式常用于支持地址重叠的 VPN 间互访。

(3) 双向 NAT

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

(4) NAT hairpin

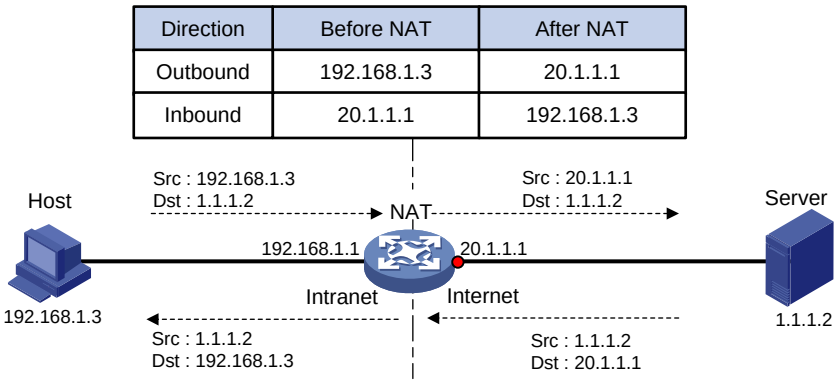
NAT hairpin 功能用于满足位于内网侧的用户之间或内网侧的用户与服务器之间通过 NAT 地址进行访问的需求。使能 NAT hairpin 的内网侧接口上会对报文同时进行源地址和目的地址的转换。它支持两种组网模式：

- P2P：位于内网侧的用户之间通过动态分配的 NAT 地址互访。
- C/S：位于内网侧的用户使用静态配置的 NAT 地址访问内网服务器。

3. 传统NAT的典型工作过程

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

图1-1 NAT 基本工作过程示意图



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

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

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

1.1.2 NAT转换控制

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

NAT 设备可以利用 ACL（Access Control List，访问控制列表）来对地址转换的使用范围进行控制，通过定义 ACL 规则，并将其与 NAT 配置相关联，实现只对匹配指定的 ACL permit 规则的报文才进行地址转换的目的。而且，NAT 仅使用规则中定义的源 IP 地址、源端口号、目的 IP 地址、目的端口号、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。

1.1.3 NAT实现方式

1. 静态方式

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

2. 动态方式

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

- NO-PAT 模式

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

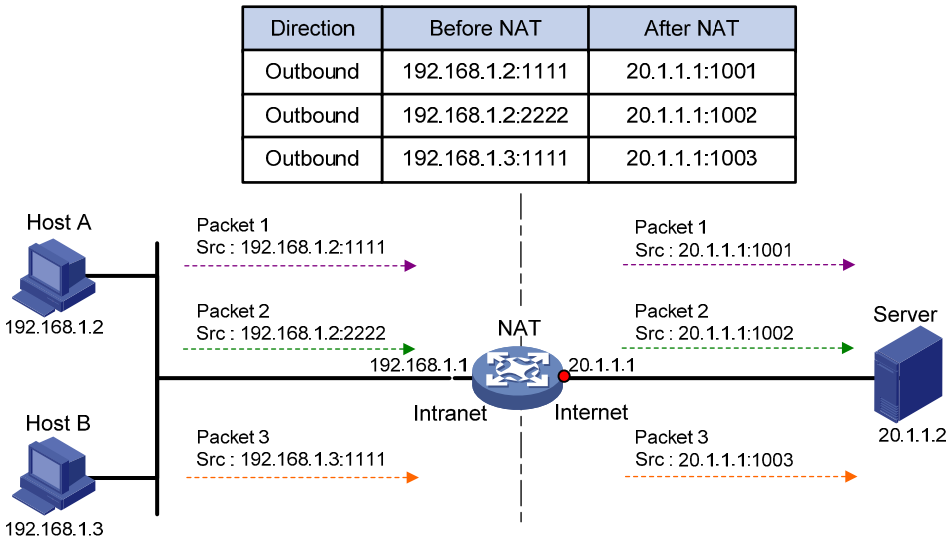
该模式下，NAT 设备只对报文的 IP 地址进行 NAT 转换，同时会建立一个 NO-PAT 表项用于记录 IP 地址映射关系，并可支持所有 IP 协议的报文。

- PAT 模式

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

图 1-2 描述了PAT的基本原理。

图1-2 PAT 基本原理示意图



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

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

- Endpoint-Independent Mapping（不关心对端地址和端口转换模式）：只要是来自相同源地址和源端口号的报文，不论其目的地址是否相同，通过 PAT 映射后，其源地址和源端口号都被转换为同一个外部地址和端口号，该映射关系会被记录下来并生成一个 EIM 表项；并且 NAT 设备允许所有外部网络的主机通过该转换后的地址和端口来访问这些内部网络的主机。这种模式可以很好的支持位于不同 NAT 网关之后的主机进行互访。
- Address and Port-Dependent Mapping（关心对端地址和端口转换模式）：对于来自相同源地址和源端口号的报文，相同的源地址和源端口号并不要求被转换为相同的外部地址和端口号，若其目的地址或目的端口号不同，通过 PAT 映射后，相同的源地址和源端口号通常会被转换成不同的外部地址和端口号。与 Endpoint-Independent Mapping 模式不同的是，NAT 设备只允许这些目的地址对应的外部网络的主机可以通过该转换后的地址和端口来访问这些内部网络的主机。这种模式安全性好，但由于同一个内网主机地址转换后的外部地址不唯一，因此不便于位于不同 NAT 网关之后的主机使用内网主机转换后的地址进行互访。

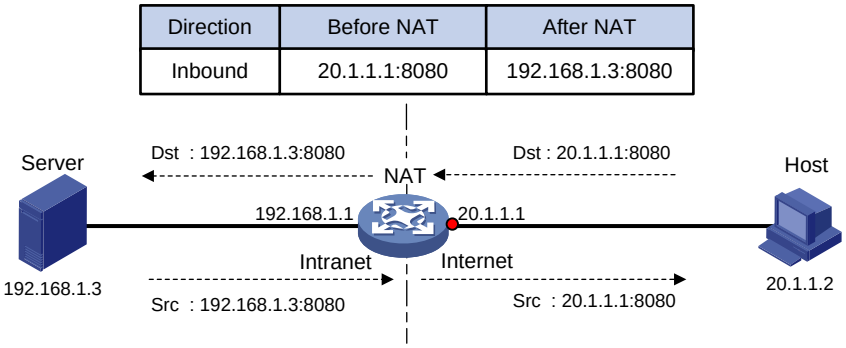
3. 内部服务器

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，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，NAT 内部服务器的配置就定义了 NAT 地址和端口与内网服务器地址和端口的映射关系。

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设备将报文的目的地址与接口上的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目

的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

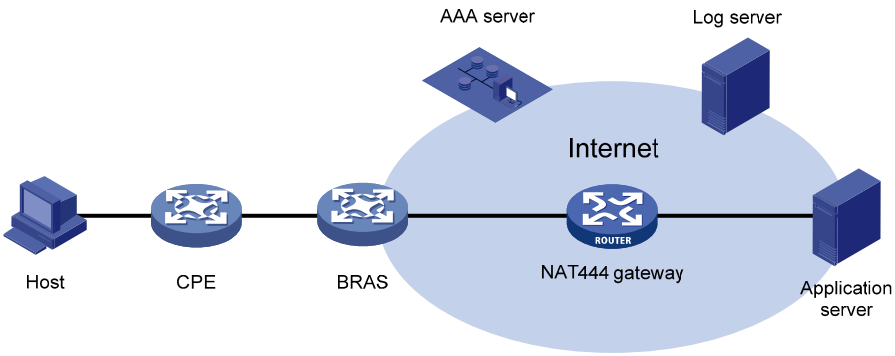


4. NAT444 端口块方式

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。

NAT444 解决方案的架构如 图 1-4 所示。

图1-4 NAT444 解决方案架构



- CPE：实现用户侧地址转换。
- BRAS：负责接入终端，并配合 AAA 完成用户认证、授权和计费。
- NAT444 网关：实现运营商级地址转换。
- AAA 服务器：负责用户认证、授权和计费等。
- 日志服务器：接受和记录用户访问信息，响应用户访问信息查询。

NAT444 网关设备进行的地址转换（以下称为“NAT444 地址转换”）是一种 PAT 方式的动态地址转换，但与普通 PAT 方式动态地址转换不同的是，NAT444 地址转换是基于端口块（即一个端口范围）的方式来复用公网 IP 地址的，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 之内的一个端口。

端口块的分配支持静态映射和动态映射两种方式。

(2) 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。

(3) 端口块动态映射

端口块动态映射融合了普通 NAT 动态地址转换和 NAT444 端口块静态映射的特点。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。

1.1.4 NAT表项

1. NAT会话表项

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

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

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

2. EIM表项

如果 NAT 设备上使能了 Endpoint-Independent Mapping 模式，则在 PAT 方式的动态地址转换过程中，会首先创建一个 NAT 会话表项，然后创建一个 EIM 表项用于记录地址和端口的转换关系（内网地址和端口<-->NAT 地址和端口），该表项有以下两个作用：

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

该表项在与其相关联的所有 NAT 会话表项老化后老化。

3. NO-PAT表项

在NO-PAT方式进行源地址的动态转换过程中，NAT设备首先创建一个NAT会话表项，然后建立一个NO-PAT表项用于记录该转换关系（内网地址<-->NAT地址）。除此之外，在NAT设备进行ALG处理时，也会触发创建NO-PAT表项。NAT ALG的相关介绍请参见“1.1.7 NAT支持ALG”。

NO-PAT 表项有以下两个作用：

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

该表项在与其相关联的所有 NAT 会话表项老化后老化。

4. NAT444 端口块表项

NAT444 端口块表项记录 1 个用户在 NAT444 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：

- 静态端口块表项在配置了 NAT444 端口块静态映射的相关命令时由系统自动创建，在删除相关配置时删除。
- 动态端口块表项在收到某私网 IP 地址的首次连接时创建，在该私网 IP 地址的所有连接都已关闭，表项中的所有端口都被回收时删除。

1.1.5 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。

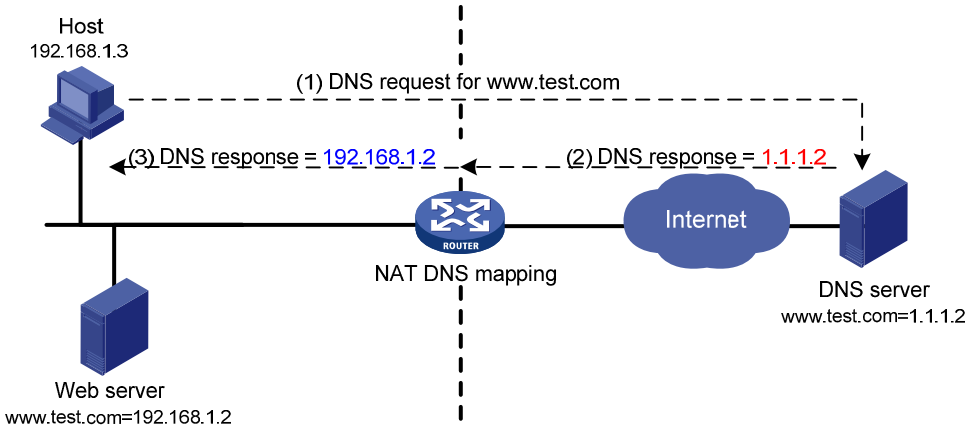
同时，NAT 内部服务器也支持多 VPN 实例，这给外部网络提供了访问 VPN 实例内服务器的机会。例如，VPN1 内提供 Web 服务的主机地址是 10.110.1.1，可以使用 202.110.10.20 作为 Web 服务器的外部地址，Internet 的用户使用 202.110.10.20 的地址就可以访问到 VPN1 提供的 Web 服务。

1.1.6 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设备的公网接口上配置内部服务器，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 1-5 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1-5 NAT DNS mapping 工作示意图



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。在配置了 NAT 的接口上，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。

1.1.7 NAT支持ALG

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

例如，FTP（File Transfer Protocol，文件传输协议）应用由 FTP 客户端与 FTP 服务器之间建立的数据连接和控制连接共同实现，而数据连接使用的地址和端口由控制连接协商报文中的载荷信息决定，这就需要 ALG 利用 NAT 的相关转换配置完成载荷信息的转换，以保证后续数据连接的正确建立。

1.2 NAT配置任务简介

若接口上同时存在普通 NAT 静态地址转换、普通 NAT 动态地址转换、NAT444 端口块静态映射、NAT444 端口块动态映射和内部服务器的配置，则在地址转换过程中，它们的优先级从高到低依次为：

(1) 内部服务器。

(2) 普通 NAT 静态地址转换。

(3) NAT444 端口块静态映射。

(4) NAT444 端口块动态映射和普通 NAT 动态地址转换，系统对二者不做区分，统一按照 ACL 编号由大到小的顺序匹配。

表1-1 NAT 配置任务简介

配置任务	说明	详细配置
配置静态地址转换	根据实际的组网需求，选择其中一种或多种转换方式 (1) 静态地址转换适用于：转换关系完全确定 (2) 动态地址转换	1.3
配置动态地址转换	• PAT 方式适用于大量内网用户通过少量 NAT 地址访问外网 • NO-PAT 方式，通常仅用于配合内部服务器或静态地址转换实现双向 NAT 应用	1.4
配置内部服务器	(3) 内部服务器：内网服务器向外网提供服务 (4) NAT444 地址转换	1.5
配置NAT444地址转换	• NAT444 端口块静态映射适用于：用户私网 IP 地址确定 • NAT444 端口块动态映射适用于：用户私网 IP 地址不确定	1.6
配置DNS mapping	可选	1.7
配置NAT hairpin	可选	1.8
配置NAT ALG功能	可选	1.9
配置NAT日志功能	可选	1.10

1.3 配置静态地址转换

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

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

1.3.1 配置准备

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

1.3.2 配置出方向一对一静态地址转换

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

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

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

表1-2 配置出方向一对一静态地址转换

操作	命令	说明
进入系统视图	**system-view**	-
配置出方向一对一静态地址转换映射	**nat static outbound** *local-ip* [**vpn-instance** *local-name*] *global-ip* [**vpn-instance** *global-name*] [**acl** *acl-number* [**reversible**]]	缺省情况下，不存在任何地址转换映射
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
开启接口上的NAT静态地址转换功能	**nat static enable**	缺省情况下，NAT静态地址转换功能处于关闭状态

1.3.3 配置出方向网段对网段静态地址转换

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

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

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

表1-3 配置出方向网段对网段静态地址转换

操作	命令	说明
进入系统视图	**system-view**	-
配置出方向网段对网段静态地址转换映射	**nat static outbound net-to-net** *local-start-address local-end-address* [**vpn-instance** *local-name*] **global** *global-network* { *mask-length* | *mask* } [**vpn-instance** *global-name*] [**acl** *acl-number* [**reversible**]]	缺省情况下，不存在任何地址转换映射

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

1.3.4 配置入方向一对一静态地址转换

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

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

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

表1-4 配置入方向一对一静态地址转换

操作	命令	说明
进入系统视图	**system-view**	-
配置入方向一对一静态地址转换映射	**nat static inbound** *global-ip* [**vpn-instance** *global-name*] *local-ip* [**vpn-instance** *local-name*] [**acl** *acl-number* [**reversible**]]	缺省情况下，不存在任何地址转换映射
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
开启接口上的NAT静态地址转换功能	**nat static enable**	缺省情况下，NAT静态地址转换功能处于关闭状态

1.3.5 配置入方向网段对网段静态地址转换

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

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

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

表1-5 配置入方向网段对网段静态地址转换

操作	命令	说明
进入系统视图	**system-view**	-
配置入方向网段对网段静态地址转换映射	**nat static inbound net-to-net** *global-start-address global-end-address* [**vpn-instance** *global-name*] **local** *local-network* { *mask-length* | *mask* } [**vpn-instance** *local-name*] [**acl** *acl-number* [**reversible**]]	缺省情况下，不存在任何地址转换映射
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
开启接口上的NAT静态地址转换功能	**nat static enable**	缺省情况下，NAT静态地址转换功能处于关闭状态

1.4 配置动态地址转换

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

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

1.4.1 配置限制和指导

在同时配置了多条动态地址转换的情况下：

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

1.4.2 配置准备

- 配置控制地址转换范围的 ACL。ACL 配置的相关介绍请参见“ACL 和 QoS 配置指导”中的“ACL”。需要注意的是，NAT 仅关注 ACL 规则中定义的源 IP 地址、源端口号、目的 IP 地址、目的端口号、传输层协议类型和 VPN 实例，不关注 ACL 规则中定义的其它元素。
- 确定是否直接使用接口的 IP 地址作为转换后的报文源地址。
- 配置根据实际网络情况，合理规划可用于地址转换的公网 IP 地址组。
- 确定地址转换过程中是否使用端口信息。
- 对于入方向动态地址转换，如果指定了 **add-route** 参数，则有报文命中该配置时，设备会自动添加路由表项：目的地址为本次地址转换使用的地址组中的地址，出接口为本配置所在接口，下一跳地址为报文的源地址；如果没有指定 **add-route** 参数，则用户需要在设备上手工添加路由。由于自动添加路由表项速度较慢，通常建议手工添加路由。

1.4.3 配置出方向动态地址转换

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

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

表1-6 配置出方向动态地址转换

操作		命令	说明
进入系统视图		**system-view**	-
创建一个NAT地址组，并进入NAT地址组视图		**nat address-group** *group-number*	缺省情况下，不存在地址组
添加地址组成员		**address** *start-address end-address*	缺省情况下，不存在地址组成员 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
退回系统视图		**quit**	-
进入接口视图		**interface** *interface-type interface-number*	-
配置出方向动态地址转换	NO-PAT方式	**nat outbound** [*acl-number*] **address-group** *group-number* [**vpn-instance** *vpn-instance-name*] **no-pat** [**reversible**]	二者至少选其一 缺省情况下，不存在出方向动态地址转换配置 一个接口下可配置多个出方向的动态地址转换
	PAT方式	**nat outbound** [*acl-number*] [**address-group** *group-number*] [**vpn-instance** *vpn-instance-name*] [**port-preserved**]	
退回系统视图		**quit**	-
（可选）配置PAT方式地址转换的模式		**nat mapping-behavior endpoint-independent** [**acl** *acl-number*]	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

1.4.4 配置入方向动态地址转换

入方向动态地址转换功能通常与接口上的出方向动态地址转换（**nat outbound**）、内部服务器（**nat server**）或出方向静态地址转换（**nat static outbound**）配合，用于实现双向 NAT 应用，不建议单独使用。

入接口动态地址转换的具体过程如下：

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

需要注意的是，该方式下的地址转换不支持 Easy IP 功能。

表1-7 配置入方向动态地址转换

操作	命令	说明
进入系统视图	**system-view**	-
创建一个NAT地址组，并进入NAT地址组视图	**nat address-group** *group-number*	缺省情况下，不存在NAT地址组
添加地址组成员	**address** *start-address end-address*	缺省情况下，不存在地址组成员 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
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置入方向动态地址转换	**nat inbound** *acl-number* **address-group** *group-number* [**vpn-instance** *vpn-instance-name*] [**no-pat** [**reversible**] [**add-route**]]	缺省情况下，不存在入方向动态地址转换配置 一个接口下可配置多个入方向的动态地址转换

1.5 配置内部服务器

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。

内部服务器通常配置在外网侧接口上。

若内部服务器配置中引用了 **acl** 参数，则表示与指定的 ACL permit 规则匹配的报文才可以使用内部服务器的映射表进行地址转换。需要注意的是，NAT 仅关注 ACL 规则中定义的源 IP 地址、源端口号、目的 IP 地址、目的端口号、传输层协议类型和 VPN 实例，不关注 ACL 规则中定义的其它元素。

1.5.1 配置普通内部服务器

普通的内部服务器是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。

表1-8 配置普通内部服务器

操作		命令	说明
进入系统视图		**system-view**	-
进入接口视图		**interface** *interface-type interface-number*	-
配置普通内部服务器	外网地址单一，未使用外网端口或外网端口单一	**nat server protocol** *pro-type* **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } [*global-port*] [**vpn-instance** *global-name*] **inside** *local-address* [*local-port*] [**vpn-instance** *local-name*] [**acl** *acl-number*]	四者至少选其一 缺省情况下，不存在内部服务器 一个接口下可以配置多个普通内部服务器
	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-name*] **inside** { { *local-address* | *local-address1 local-address2* } *local-port* | *local-address local-port1 local-port2* } [**vpn-instance** *local-name*] [**acl** *acl-number*]	
	外网地址连续，未使用外网端口或外网端口单一	**nat server protocol** *pro-type* **global** *global-address1 global-address2* [*global-port*] [**vpn-instance** *global-name*] **inside** { *local-address* | *local-address1 local-address2* } [*local-port*] [**vpn-instance** *local-name*] [**acl** *acl-number*]	
	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-name*] **inside** *local-address local-port1 local-port2* [**vpn-instance** *local-name*] [**acl** *acl-number*]	

1.5.2 配置负载分担内部服务器

负载分担内部服务器是指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。

表1-9 配置负载分担内部服务器

操作	命令	说明
进入系统视图	**system-view**	-
配置内部服务器组，并进入服务器组视图	**nat server-group** *group-number*	缺省情况下，不存在内部服务器组
添加内部服务器组成员	**inside ip** *inside-ip* **port** *port-number* [**weight** *weight-value*]	缺省情况下，内部服务器组内没有内部服务器组成员 一个内部服务器组内可以添加多个组成员
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
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-name*] **inside server-group** *group-number* [**vpn-instance** *local-name*] [**acl** *acl-number*]	缺省情况下，不存在内部服务器 一个接口下可以配置多个负载分担内部服务器

1.6 配置NAT444地址转换

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。

NAT444 是出方向地址转换，通常配置在外网侧接口上。

1.6.1 配置NAT444 端口块静态映射

配置 NAT444 端口块静态映射需要创建一个端口块组，并在接口的出方向上应用该端口块组。端口块组中需要配置私网 IP 地址成员、公网 IP 地址成员、端口范围和端口块大小，系统会根据端口块组中的配置自动计算私网 IP 地址到公网 IP 地址、端口块的静态映射关系，创建静态端口块表项，并根据表项进行 NAT444 地址转换。

表1-10 配置 NAT444 端口块静态映射

操作	命令	说明
进入系统视图	**system-view**	-
创建一个NAT端口块组，并进入NAT端口块组视图	**nat port-block-group** *group-number*	缺省情况下，不存在NAT端口块组
添加私网地址成员	**local-ip-address** *start-address end-address*	缺省情况下，不存在私网地址成员 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
添加公网地址成员	**global-ip-pool** *start-address end-address*	缺省情况下，不存在公网地址成员 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
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
配置端口块大小	**block-size** *block-size*	缺省情况下，端口块大小为256
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置NAT444端口块静态映射	**nat outbound port-block-group** *group-number*	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

操作	命令	说明
退回系统视图	**quit**	-
（可选）配置PAT方式出方向动态地址转换的模式	**nat mapping-behavior endpoint-independent** [**acl** *acl-number*]	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

1.6.2 配置NAT444 端口块动态映射

NAT444 端口块动态映射的配置方式与普通的 PAT 方式出方向动态地址转换的配置基本相同，只要在接口的出方向上配置 ACL 和 NAT 地址组的关联即可。所不同的是，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。

表1-11 配置 NAT444 端口块动态映射

操作	命令	说明
进入系统视图	**system-view**	-
创建一个NAT地址组，并进入NAT地址组视图	**nat address-group** *group-number*	缺省情况下，不存在地址组
添加地址组成员	**address** *start-address end-address*	缺省情况下，不存在地址组成员 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
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
配置端口块参数	**port-block block-size** *block-size* [**extended-block-number** *extended-block-number*]	缺省情况下，不存在端口块参数 该配置仅对PAT方式地址转换生效
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置PAT方式出方向动态地址转换	**nat outbound** [*acl-number*] [**address-group** *group-number*] [**vpn-instance** *vpn-instance-name*] [**port-preserved**]	缺省情况下，不存在PAT方式出方向动态地址转换配置 **port-preserved**参数对NAT444端口块动态映射无效
退回系统视图	**quit**	-
（可选）配置PAT方式地址转换的模式	**nat mapping-behavior endpoint-independent** [**acl** *acl-number*]	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

1.7 配置DNS mapping

通过配置 DNS mapping，可以在 DNS 服务器位于外网的情况下，实现内网用户可通过域名访问位于同一内网的内部服务器的功能。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。

NAT 设备对来自外网的 DNS 响应报文进行 DNS ALG 处理时，由于载荷中只包含域名和应用服务器的外网 IP 地址（不包含传输协议类型和端口号），当接口上存在多条 NAT 服务器配置且使用相同的外网地址而内网地址不同时，DNS ALG 仅使用 IP 地址来匹配内部服务器可能会得到错误的匹配结果。因此需要借助 DNS mapping 的配置，指定域名与应用服务器的外网 IP 地址、端口和协议的映射关系，由域名获取应用服务器的外网 IP 地址、端口和协议，进而（在当前 NAT 接口上）精确匹配内部服务器配置获取应用服务器的内网 IP 地址。

表1-12 配置 DNS mapping

操作	命令	说明
进入系统视图	**system-view**	-
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*	缺省情况下，不存在域名到内部服务器的映射 可配置多条域名到内部服务器的映射

1.8 配置NAT hairpin功能

通过在内网侧接口上使能 NAT hairpin 功能，可以实现内网用户使用 NAT 地址访问内网服务器或内网其它用户。NAT hairpin 功能需要与内部服务器（**nat server**）、出方向动态地址转换（**nat outbound**）或出方向静态地址转换（**nat static outbound**）配合工作，且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。

该功能在不同工作方式下的具体转换过程如下：

- C/S 方式：NAT 在内网接口上同时转换访问内网服务器的报文的源和目的 IP 地址，其中，目的 IP 地址转换通过匹配某外网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。
- P2P 方式：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。该方式下，外网侧的出方向地址转换必须配置为 PAT 转换方式，并使能 EIM 模式。

表1-13 配置 NAT hairpin 功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
使能NAT hairpin功能	**nat hairpin enable**	缺省情况下，NAT hairpin功能处于关闭状态

1.9 配置NAT ALG

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

表1-14 配置 NAT ALG 功能

操作	命令	说明
进入系统视图	**system-view**	-
开启指定或所有协议类型的NAT ALG功能	**nat alg** { **all** | **dns** | **ftp** | **h323** | **icmp-error** | **ils** | **mgcp** | **nbt** | **pptp** | **rsh** | **rtsp** | **sccp** | **sip** | **sqlnet** | **tftp** | **xdmcp** }	缺省情况下，所有协议类型的NAT ALG功能均处于开启状态

1.10 配置NAT日志功能

1.10.1 配置NAT会话日志功能

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

有三种情况可以触发设备生成 NAT 会话日志：

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

表1-15 配置 NAT 会话日志功能

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

1.10.2 配置NAT444 用户日志功能

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。

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”。

表1-16 配置 NAT444 用户日志功能

操作	命令	说明
进入系统视图	**system-view**	-
开启NAT日志功能	**nat log enable** [**acl** *acl-number*]	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
开启端口块分配的NAT444用户日志功能	**nat log port-block-assign**	二者至少选其一 缺省情况下，分配和回收端口块时，均不输出NAT444用户日志
开启端口块回收的NAT444用户日志功能	**nat log port-block-withdraw**	

1.10.3 配置NAT444 告警信息日志功能

在 NAT444 地址转换中，如果可为用户分配的公网 IP 地址、端口块或端口块中的端口都被占用，则该用户的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。为了监控公网 IP 地址和端口块资源的使用情况，可以对端口用满和资源用满两种情况记录告警信息日志。

- 端口用满告警：在私网 IP 地址对应的端口块中的所有端口都被占用的情况下，输出告警信息日志。对于端口块动态映射方式，如果配置了增量端口块分配，则当首次分配的端口块中的端口都被占用时，并不输出日志；只有当增量端口块中的端口也都被占用时，才会输出日志。
- 资源用满告警：在 NAT444 端口块动态映射中，如果所有资源（公网 IP 地址、端口块）都被占用，则输出日志。

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

表1-17 配置 NAT444 告警信息日志功能

操作	命令	说明
进入系统视图	**system-view**	-
开启NAT日志功能	**nat log enable** [**acl** *acl-number*]	缺省情况下，NAT日志功能处于关闭状态 ACL参数对NAT444告警信息日志功能无效
开启NAT444告警信息的日志功能	**nat log alarm**	缺省情况下，NAT444告警信息日志功能处于关闭状态

1.11 NAT显示和维护

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

在用户视图下，执行 **reset** 命令可以清除 NAT 表项。

表1-18 NAT 显示和维护

操作	命令
显示所有的NAT配置信息	**display nat all**
显示NAT地址组的配置信息	**display nat address-group** [*group-number*]
显示NAT DNS mapping的配置信息	**display nat dns-map**
显示NAT EIM表项信息（独立运行模式）	**display nat eim** [**slot** *slot-number*]
显示NAT EIM表项信息（IRF模式）	**display nat eim** [**chassis** *chassis-number* **slot** *slot-number*]
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** [**slot** *slot-number*]
显示NAT NO-PAT表项信息（IRF模式）	**display nat no-pat** [**chassis** *chassis-number* **slot** *slot-number*]
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** [*group-number*]
显示NAT会话（独立运行模式）	**display nat session** [{ **source-ip** *source-ip* | **destination-ip** *destination-ip* } * [**vpn-instance** *vpn-name*]] [**slot** *slot-number*] [**verbose**]
显示NAT会话（IRF模式）	**display nat session** [{ **source-ip** *source-ip* | **destination-ip** *destination-ip* } * [**vpn-instance** *vpn-name*]] [**chassis** *chassis-number* **slot** *slot-number*] [**verbose**]
显示NAT静态地址转换的配置信息	**display nat static**

操作	命令
显示NAT统计信息（独立运行模式）	**display nat statistics** [**slot** *slot-number*]
显示NAT统计信息（IRF模式）	**display nat statistics** [**chassis** *chassis-number* **slot** *slot-number*]
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** [*group-number*]
显示端口块表项（独立运行模式）	**display nat port-block** { **dynamic** | **static** } [**slot** *slot-number*]
显示端口块表项（IRF模式）	**display nat port-block** { **dynamic** | **static** } [**chassis** *chassis-number* **slot** *slot-number*]
删除NAT会话	**reset nat session**

1.12 NAT典型配置举例

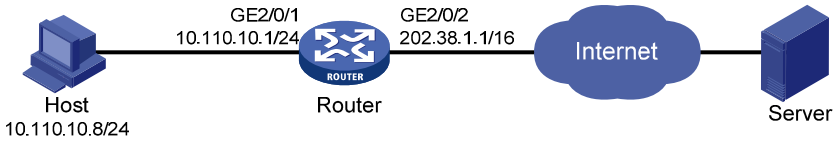
1.12.1 内网用户通过NAT地址访问外网（静态地址转换）

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1-6 静态地址转换典型配置组网图



3. 配置步骤

按照组网图配置各接口的 IP 地址，具体配置过程略。

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。

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

使配置的静态地址转换在接口 GigabitEthernet2/0/2 上生效。

```
[Router] interface gigabitethernet 2/0/2
[Router-GigabitEthernet2/0/2] nat static enable
[Router-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。

```
[Router] 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: GigabitEthernet2/0/2
    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。

```
[Router] display nat session verbose
Initiator:
  Source      IP/port: 10.110.10.8/42496
  Destination IP/port: 202.38.1.111/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet2/0/1
Responder:
  Source      IP/port: 202.38.1.111/42496
  Destination IP/port: 202.38.1.100/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet2/0/2
State: ICMP_REPLY
Application: INVALID
Start time: 2014-06-16 09:30:49  TTL: 27s
Initiator->Responder:            5 packets        420 bytes
Responder->Initiator:            5 packets        420 bytes

Total sessions found: 1
```

1.12.2 内网用户通过NAT地址访问外网（地址不重叠）

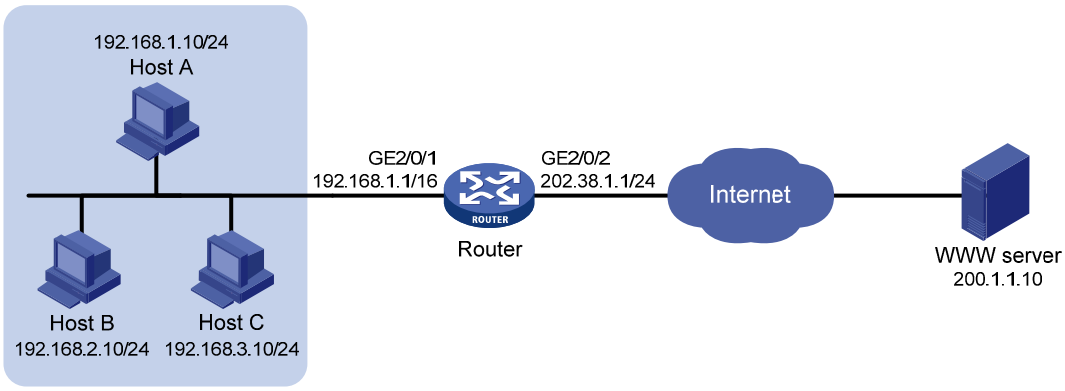
1. 组网需求

- 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1-7 内网用户通过 NAT 访问外网（地址不重叠）



3. 配置步骤

按照组网图配置各接口的 IP 地址，具体配置过程略。

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

```
<Router> system-view
[Router] nat address-group 0
[Router-nat-address-group-0] address 202.38.1.2 202.38.1.3
[Router-nat-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。

```
[Router] acl number 2000
[Router-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Router-acl-basic-2000] quit
```

在接口 GigabitEthernet2/0/2 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。

```
[Router] interface gigabitethernet 2/0/2
[Router-GigabitEthernet2/0/2] nat outbound 2000 address-group 0
[Router-GigabitEthernet2/0/2] 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。

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

NAT outbound information:
  Totallu 1 NAT outbound rules.
```

```
  Interface: GigabitEthernet2/0/2
    ACL: 2000         Address group: 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

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

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

```
[Router] display nat session verbose
Initiator:
  Source      IP/port: 192.168.1.10/52992
  Destination IP/port: 200.1.1.10/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet2/0/1
Responder:
  Source      IP/port: 200.1.1.10/4
  Destination IP/port: 202.38.1.3/0
  DS-Lite tunnel peer: -
```

```
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet2/0/2
State: ICMP_REPLY
Application: INVALID
Start time: 2014-06-15 14:53:29  TTL: 12s
Initiator->Responder:            1 packets         84 bytes
Responder->Initiator:            1 packets         84 bytes

Total sessions found: 1
```

1.12.3 内网用户通过NAT地址访问外网（地址重叠）

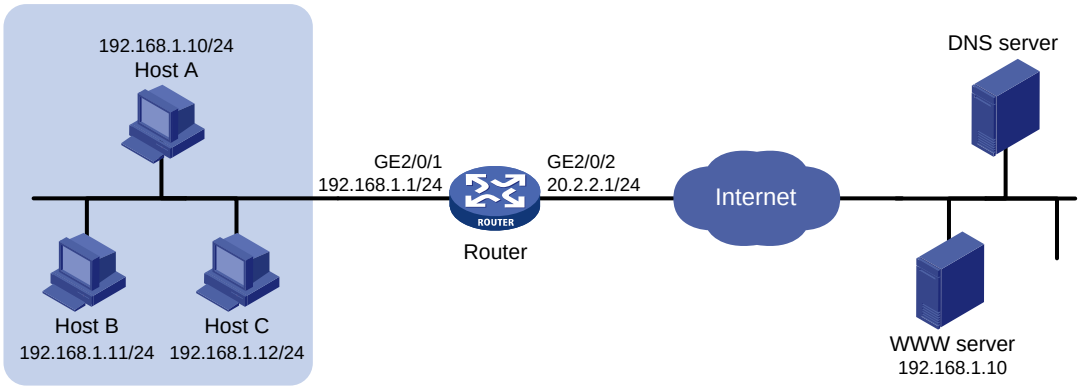
1. 组网需求

- 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。

需要实现，内网用户可以通过域名访问外网的 Web 服务器。

2. 组网图

图1-8 内网用户通过 NAT 访问外网（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的 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 GigabitEthernet2/0/2。

4. 配置步骤

按照组网图配置各接口的 IP 地址，具体配置过程略。

开启 DNS 的 NAT ALG 功能。

```
<Router> system-view
[Router] 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。

```
[Router] acl number 2000
[Router-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Router-acl-basic-2000] quit
```

创建地址组 1。

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

添加地址组成员 202.38.1.2。

```
[Router-nat-address-group-1] address 202.38.1.2 202.38.1.2
[Router-nat-address-group-1] quit
```

创建地址组 2。

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

添加地址组成员 202.38.1.3。

```
[Router-nat-address-group-2] address 202.38.1.3 202.38.1.3
[Router-nat-address-group-2] quit
```

在接口 GigabitEthernet2/0/2 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。

```
[Router] interface gigabitethernet 2/0/2
[Router-GigabitEthernet2/0/2] nat inbound 2000 address-group 1 no-pat reversible
```

在接口 GigabitEthernet2/0/2 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。

```
[Router-GigabitEthernet2/0/2] nat outbound 2000 address-group 2
[Router-GigabitEthernet2/0/2] 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 GigabitEthernet2/0/2，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）。

```
[Router] ip route-static 202.38.1.2 32 gigabitethernet 2/0/2 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。

```
[Router] display nat all
NAT address group information:
  Totally 2 NAT address groups.
  Address group 1:
    Port range: 1-65535
    Address information:
      Start address         End address
      202.38.1.2            202.38.1.2
```

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

NAT inbound information:
  Totally 1 NAT inbound rules.
  Interface: GigabitEthernet2/0/2
    ACL: 2000         Address group: 1      Add route: N
    NO-PAT: Y         Reversible: Y
    Config status: Active

NAT outbound information:
  Totally 1 NAT outbound rules.
  Interface: GigabitEthernet2/0/2
    ACL: 2000         Address group: 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

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

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

```
  SQLNET      : Enabled
  TFTP        : Enabled
  XDMCP       : 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。

```
[Router] display nat session verbose
Initiator:
  Source      IP/port: 192.168.1.10/1694
  Destination IP/port: 202.38.1.2/8080
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/1
Responder:
  Source      IP/port: 192.168.1.10/8080
  Destination IP/port: 202.38.1.3/1025
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/2
State: TCP_ESTABLISHED
Application: HTTP
Start time: 2014-06-15 14:53:29  TTL: 3597s
Initiator->Responder:            7 packets        308 bytes
Responder->Initiator:            5 packets        312 bytes

Total sessions found: 1
```

1.12.4 外网用户通过外网地址访问内网服务器

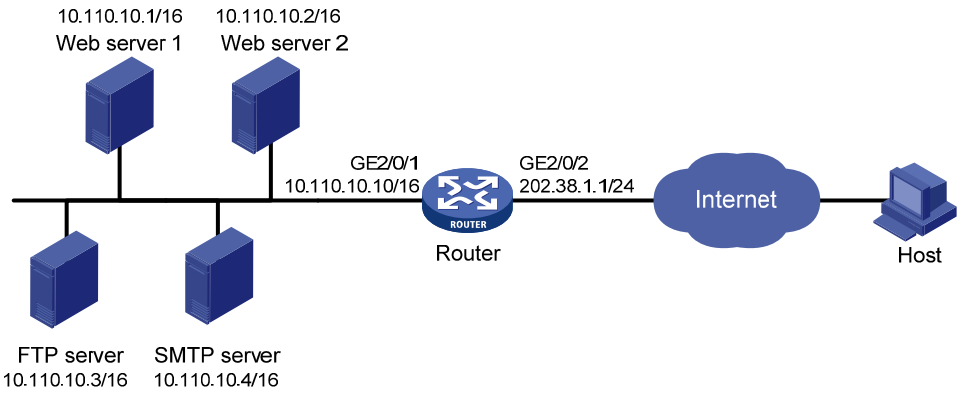
1. 组网需求

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1-9 外网用户通过外网地址访问内网服务器



3. 配置步骤

按照组网图配置各接口的 IP 地址，具体配置过程略。

进入接口 GigabitEthernet2/0/2。

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

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。

```
[Router-GigabitEthernet2/0/2] 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。

```
[Router-GigabitEthernet2/0/2] 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。

```
[Router-GigabitEthernet2/0/2] 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。

```
[Router-GigabitEthernet2/0/2] nat server protocol tcp global 202.38.1.1 smtp inside
10.110.10.4 smtp
[Router-GigabitEthernet2/0/2] 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。

```
[Router] display nat all
NAT internal server information:
  Totally 4 internal servers.
  Interface: GigabitEthernet2/0/2
    Protocol: 6(TCP)
    Global IP/port: 202.38.1.1/21
    Local IP/port : 10.110.10.3/21
```

```
    Config status : Active

  Interface: GigabitEthernet2/0/2
    Protocol: 6(TCP)
    Global IP/port: 202.38.1.1/25
    Local IP/port : 10.110.10.4/25
    Config status : Active

  Interface: GigabitEthernet2/0/2
    Protocol: 6(TCP)
    Global IP/port: 202.38.1.1/80
    Local IP/port : 10.110.10.1/80
    Config status : Active

  Interface: GigabitEthernet2/0/2
    Protocol: 6(TCP)
    Global IP/port: 202.38.1.1/8080
    Local IP/port : 10.110.10.2/80
    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

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

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

```
  TFTP        : Enabled
  XDMCP       : 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。

```
[Router] display nat session verbose
Initiator:
  Source      IP/port: 202.38.1.10/1694
  Destination IP/port: 202.38.1.1/21
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/1
Responder:
  Source      IP/port: 10.110.10.3/21
  Destination IP/port: 202.38.1.10/1694
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/2
State: TCP_ESTABLISHED
Application: FTP
Start time: 2014-06-15 14:53:29  TTL: 3597s
Initiator->Responder:            7 packets        308 bytes
Responder->Initiator:            5 packets        312 bytes

Total sessions found: 1
```

1.12.5 外网用户通过域名访问内网服务器（地址不重叠）

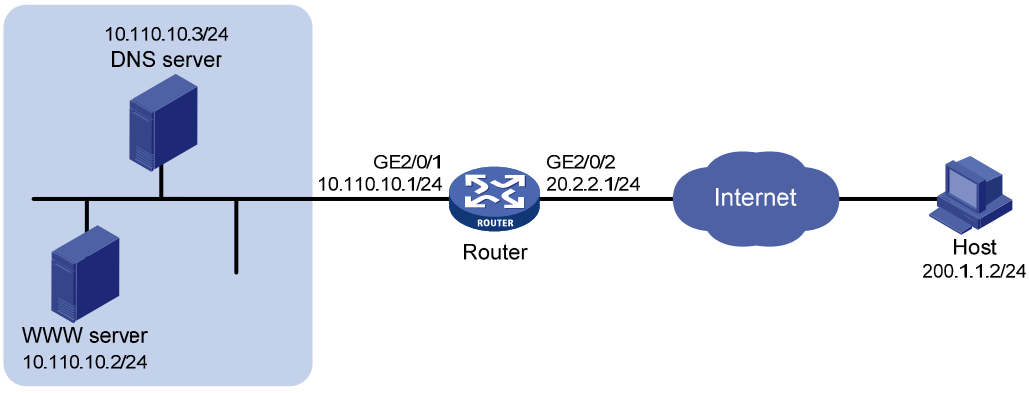
1. 组网需求

- 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1-10 外网用户通过域名访问内网服务器（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

按照组网图配置各接口的 IP 地址，具体配置过程略。

开启 DNS 协议的 ALG 功能。

```
<Router> system-view
[Router] 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。

```
[Router] acl number 2000
[Router-acl-basic-2000] rule permit source 10.110.10.2 0
[Router-acl-basic-2000] quit
```

创建地址组 1。

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

添加地址组成员 202.38.1.3。

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

在接口 GigabitEthernet2/0/2 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。

```
[Router] interface gigabitethernet 2/0/2
[Router-GigabitEthernet2/0/2] nat server protocol udp global 202.38.1.2 inside 10.110.10.3
domain
```

在接口 GigabitEthernet2/0/2 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。

```
[Router-GigabitEthernet2/0/2] nat outbound 2000 address-group 1 no-pat reversible
[Router-GigabitEthernet2/0/2] 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。

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

```
NAT outbound information:
  Totally 1 NAT outbound rules.
  Interface: GigabitEthernet2/0/2
    ACL: 2000         Address group: 1      Port-preserved: N
    NO-PAT: Y         Reversible: Y
    Config status: Active

NAT internal server information:
  Totally 1 internal servers.
  Interface: GigabitEthernet2/0/2
    Protocol: 17(UDP)
    Global IP/port: 202.38.1.2/53
    Local IP/port : 10.110.10.3/53
    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

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

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

```
[Router] display nat session verbose
Initiator:
```

```
  Source      IP/port: 202.1.1.2/1694
  Destination IP/port: 202.38.1.3/8080
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/1
Responder:
  Source      IP/port: 10.110.10.2/8080
  Destination IP/port: 202.1.1.2/1694
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/2
State: TCP_ESTABLISHED
Application: HTTP
Start time: 2014-06-15 14:53:29  TTL: 3597s
Initiator->Responder:            7 packets        308 bytes
Responder->Initiator:            5 packets        312 bytes

Total sessions found: 1
```

1.12.6 外网用户通过域名访问内网服务器（地址重叠）

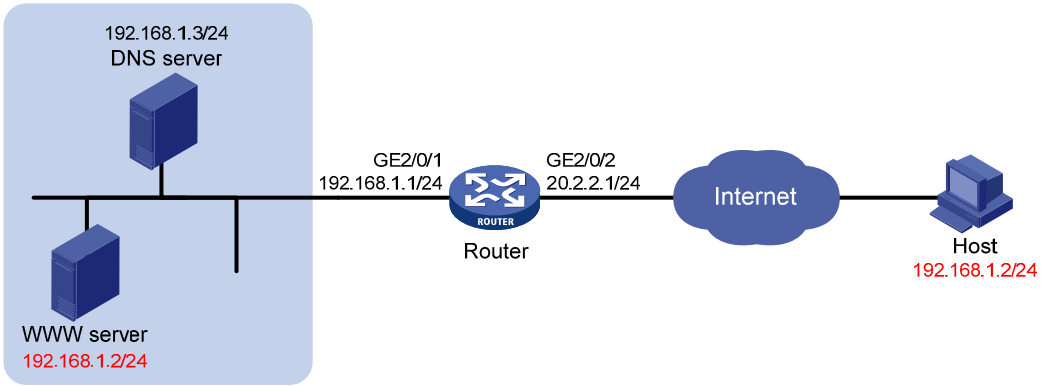
1. 组网需求

- 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1-11 外网用户通过域名访问内网服务器（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 GigabitEthernet2/0/2。

4. 配置步骤

按照组网图配置各接口的 IP 地址，具体配置过程略。

开启 DNS 协议的 ALG 功能。

```
<Router> system-view
[Router] 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。

```
[Router] acl number 2000
[Router-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Router-acl-basic-2000] quit
```

创建地址组 1。

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

添加地址组成员 202.38.1.2。

```
[Router-nat-address-group-1] address 202.38.1.2 202.38.1.2
[Router-nat-address-group-1] quit
```

创建地址组 2。

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

添加地址组成员 202.38.1.3。

```
[Router-nat-address-group-2] address 202.38.1.3 202.38.1.3
[Router-nat-address-group-2] quit
```

在接口 GigabitEthernet2/0/2 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。

```
[Router] interface gigabitethernet 2/0/2
[Router-GigabitEthernet2/0/2] nat server protocol udp global 202.38.1.4 inside 192.168.1.3
domain
```

在接口 GigabitEthernet2/0/2 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。

```
[Router-GigabitEthernet2/0/2] nat outbound 2000 address-group 1 no-pat reversible
```

在接口 GigabitEthernet2/0/2 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。

```
[Router-GigabitEthernet2/0/2] nat inbound 2000 address-group 2
[Router-GigabitEthernet2/0/2] quit
```

配置到达 202.38.1.3 地址的静态路由，出接口为 GigabitEthernet2/0/2，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）。

```
[Router] ip route-static 202.38.1.3 32 gigabitethernet 2/0/2 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。

```
[Router] display nat all
NAT address group information:
  Totally 2 NAT address groups.
  Address group 1:
    Port range: 1-65535
    Address information:
      Start address         End address
      202.38.1.2            202.38.1.2

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

NAT inbound information:
  Totally 1 NAT inbound rules.
  Interface: GigabitEthernet2/0/2
    ACL: 2000         Address group: 2      Add route: N
    NO-PAT: N         Reversible: N
    Config status: Active

NAT outbound information:
  Totally 1 NAT outbound rules.
  Interface: GigabitEthernet2/0/2
    ACL: 2000         Address group: 1      Port-preserved: N
    NO-PAT: Y         Reversible: Y
    Config status: Active

NAT internal server information:
  Totally 1 internal servers.
  Interface: GigabitEthernet2/0/2
    Protocol: 17(UDP)
    Global IP/port: 202.38.1.4/53
    Local IP/port : 200.1.1.3/53
    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

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

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

```
[Router] display nat session verbose
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/VLL ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/1
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/VLL ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/2
State: TCP_ESTABLISHED
Application: HTTP
```

```
Start time: 2014-06-15 14:53:29  TTL: 3597s
Initiator->Responder:            7 packets        308 bytes
Responder->Initiator:            5 packets        312 bytes

Total sessions found: 1
```

1.12.7 内网用户通过NAT地址访问内网服务器

1. 组网需求

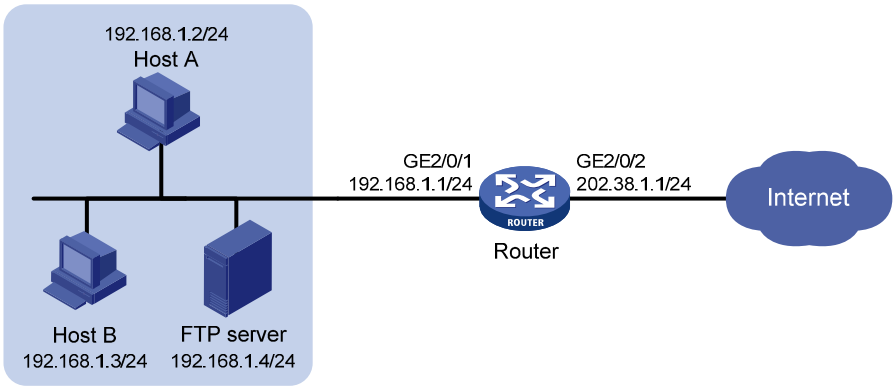
- 某公司内部网络中有一台 FTP 服务器，地址为 192.168.1.4/24。
- 该公司拥有两个外网 IP 地址：202.38.1.1 和 202.38.1.2。

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1-12 内网用户通过 NAT 地址访问内网服务器



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，需要在内网侧接口使能 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

按照组网图配置各接口的 IP 地址，具体配置过程略。

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。

```
<Router> system-view
[Router] acl number 2000
[Router-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
```

```
[Router-acl-basic-2000] quit
```

在接口 GigabitEthernet2/0/2 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。

```
[Router] interface gigabitethernet 2/0/2
[Router-GigabitEthernet2/0/2] nat server protocol tcp global 202.38.1.2 inside 192.168.1.4 ftp
```

在接口 GigabitEthernet2/0/2 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 GigabitEthernet2/0/2 的 IP 地址进行源地址转换。

```
[Router-GigabitEthernet2/0/2] nat outbound 2000
[Router-GigabitEthernet2/0/2] quit
```

在接口 GigabitEthernet2/0/1 上使能 NAT hairpin 功能。

```
[Router] interface gigabitethernet 2/0/1
[Router-GigabitEthernet2/0/1] nat hairpin enable
[Router-GigabitEthernet2/0/1] 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。

```
[Router]display nat all
NAT outbound information:
  Totally 1 NAT outbound rules.
  Interface: GigabitEthernet2/0/2
    ACL: 2000         Address group: ---    Port-preserved: N
    NO-PAT: N         Reversible: N
    Config status: Active

NAT internal server information:
  Totally 1 internal servers.
  Interface: GigabitEthernet2/0/2
    Protocol: 6(TCP)
    Global IP/port: 202.38.1.2/21
    Local IP/port : 192.168.1.4/21
    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

NAT hairpinning:
  Totally 1 interfaces enabled with NAT hairpinning.
  Interface: GigabitEthernet2/0/1
    Config status: Active
```

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

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

```
[Router] display nat session verbose
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/VLL ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/1
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/VLL ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/2
State: TCP_ESTABLISHED
Application: FTP
Start time: 2014-06-15 14:53:29  TTL: 3597s
Initiator->Responder:            7 packets        308 bytes
Responder->Initiator:            5 packets        312 bytes

Total sessions found: 1
```

1.12.8 内网用户通过NAT地址互访

1. 组网需求

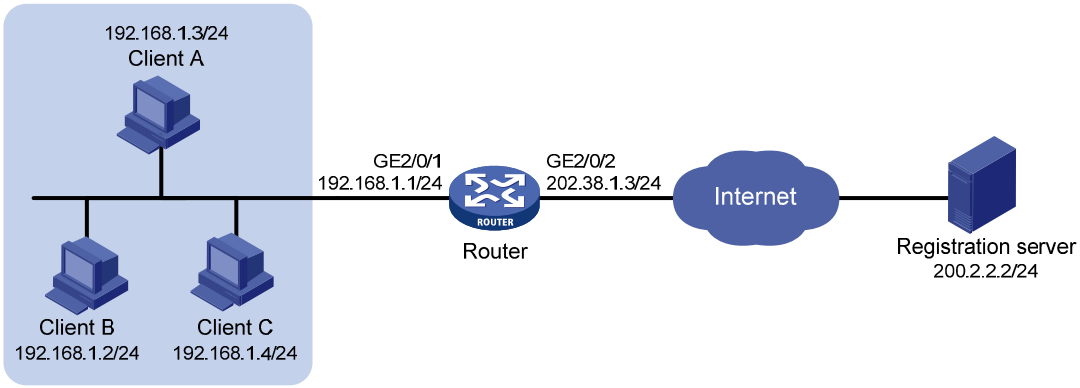
某 P2P 应用环境中，内网中的客户端首先需要向外网服务器进行注册，外网服务器会记录客户端的 IP 地址和端口号。如果内网的一个客户端要访问内网的另一个客户端，首先需要向服务器获取对方的 IP 地址和端口号。

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1-13 内网用户通过 NAT 地址互访



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，需要在内网侧接口使能 NAT hairpin 功能。

4. 配置步骤

按照组网图配置各接口的 IP 地址，具体配置过程略。

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。

```
<Router> system-view
[Router] acl number 2000
[Router-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Router-acl-basic-2000] quit
```

在外网侧接口 GigabitEthernet2/0/2 上配置 Easy IP 方式的出方向动态地址转换，允许使用接口 GigabitEthernet2/0/2 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。

```
[Router] interface gigabitethernet 2/0/2
[Router-GigabitEthernet2/0/2] nat outbound 2000
[Router-GigabitEthernet2/0/2] 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。

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

在内网侧接口 GigabitEthernet2/0/1 上使能 NAT hairpin 功能。

```
[Router] interface gigabitethernet 2/0/1
[Router-GigabitEthernet2/0/1] nat hairpin enable
[Router-GigabitEthernet2/0/1] 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。

```
[Router] display nat all
NAT outbound information:
  Totally 1 NAT outbound rules.
  Interface: GigabitEthernet2/0/2
    ACL: 2000         Address group: ---    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

NAT hairpinning:
  Totally 1 interfaces enabled with NAT hairpinning.
  Interface: GigabitEthernet2/0/1
    Config status: Active

NAT mapping behavior:
  Mapping mode : Endpoint-Independent
  ACL          : 2000
  Config status: Active

NAT ALG:
  DNS        : Enabled
  FTP        : Enabled
  H323       : Enabled
  ICMP-ERROR : Enabled
  ILS        : Enabled
```

```
  MGCP        : Enabled
  NBT         : Enabled
  PPTP        : Enabled
  RSH         : Enabled
  RTSP        : Enabled
  SCCP        : Enabled
  SIP         : Enabled
  SQLNET      : Enabled
  TFTP        : Enabled
  XDMCP       : 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。

```
[Router] display nat session verbose
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/VLL ID: -/-/-
  Protocol: UDP(17)
  Inbound interface: GigabitEthernet2/0/1
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/VLL ID: -/-/-
  Protocol: UDP(17)
  Inbound interface: GigabitEthernet2/0/2
State: UDP_READY
Application: TFTP
Start time: 2014-06-15 15:53:36  TTL: 46s
Initiator->Responder:            1 packets         56 bytes
Responder->Initiator:            1 packets         72 bytes

Total sessions found: 1
```

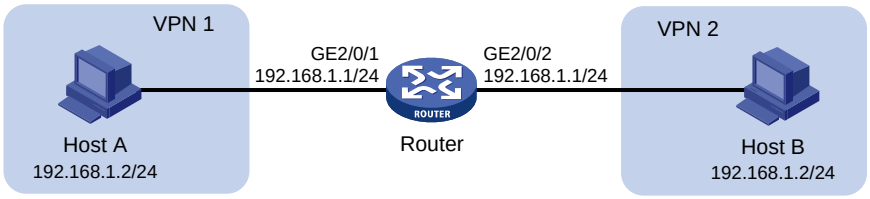
1.12.9 地址重叠的两个VPN之间互访

1. 组网需求

某公司两个部门由于需要业务隔而分属不同的 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1-14 地址重叠的两个内网之间互访



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。

4. 配置步骤

按照组网图配置各接口的 VPN 实例和 IP 地址，具体配置过程略。

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。

```
<Router> system-view
[Router] 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。

```
[Router] nat static outbound 192.168.1.2 vpn-instance vpn2 172.16.2.2 vpn-instance vpn1
```

在接口 GigabitEthernet2/0/2 上使能静态地址转换。

```
[Router] interface gigabitethernet 2/0/2
[Router-GigabitEthernet2/0/2] nat static enable
[Router-GigabitEthernet2/0/2] quit
```

在接口 GigabitEthernet2/0/1 上使能静态地址转换。

```
[Router] interface gigabitethernet 2/0/1
[Router-GigabitEthernet2/0/1] nat static enable
[Router-GigabitEthernet2/0/1] 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。

```
[Router] 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: GigabitEthernet2/0/1
    Config status: Active
```

```
  Interface: GigabitEthernet2/0/2
    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

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

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

```
[Router] display nat session verbose
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/VLL ID: vpn1/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet2/0/1
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/VLL ID: vpn2/-/-
  Protocol: ICMP(1)
```

```
  Inbound interface: GigabitEthernet2/0/2
State: ICMP_REPLY
Application: INVALID
Start time: 2014-06-16 09:30:49  TTL: 27s
Initiator->Responder:            5 packets        420 bytes
Responder->Initiator:            5 packets        420 bytes

Total sessions found: 1
```

1.12.10 负载分担内部服务器典型配置举例

1. 组网需求

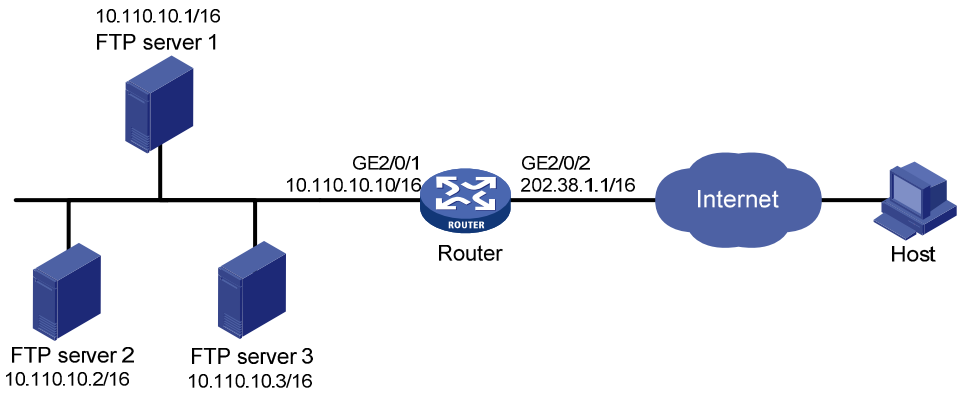
某公司内部拥有 3 台 FTP 服务器对外提供 FTP 服务。

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1-15 负载分担内部服务器典型配置组网图



3. 配置步骤

按照组网图配置各接口的 IP 地址，具体配置过程略。

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。

```
<Router> system-view
[Router] nat server-group 0
[Router-nat-server-group-0] inside ip 10.110.10.1 port 21
[Router-nat-server-group-0] inside ip 10.110.10.2 port 21
[Router-nat-server-group-0] inside ip 10.110.10.3 port 21
[Router-nat-server-group-0] quit
```

在接口 Gigabitethernet2/0/2 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。

```
[Router] interface gigabitethernet 2/0/2
[Router-GigabitEthernet2/0/2] nat server protocol tcp global 202.38.1.1 ftp inside
server-group 0
```

```
[Router-GigabitEthernet2/0/2] 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。

```
[Router] 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: GigabitEthernet2/0/2
    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: 2)
                    10.110.10.3/21         (Connections: 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

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

NAT ALG:
  DNS        : Enabled
  FTP        : Enabled
  H323       : Enabled
  ICMP-ERROR : Enabled
  ILS        : Enabled
  MGCP       : Enabled
  NBT        : Enabled
  PPTP       : Enabled
  RSH        : Enabled
```

```
  RTSP       : Enabled
  SCCP       : Enabled
  SIP        : Enabled
  SQLNET     : Enabled
  TFTP       : Enabled
  XDMCP      : Enabled
```

通过以下显示命令，可以看到外网主机访问内网某 FTP server 时生成 NAT 会话信息。

```
[Router] display nat session verbose
Initiator:
  Source      IP/port: 202.38.1.25/53957
  Destination IP/port: 202.38.1.1/21
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/1
Responder:
  Source      IP/port: 10.110.10.3/21
  Destination IP/port: 202.38.1.25/53957
  VPN instance/VLAN ID/VLL ID: -/-/-
  DS-Lite tunnel peer: -
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/2
State: TCP_ESTABLISHED
Application: FTP
Start time: 2014-06-16 11:06:07  TTL: 26s
Initiator->Responder:            1 packets         60 bytes
Responder->Initiator:            2 packets        120 bytes

Total sessions found: 5
```

1.12.11 NAT DNS mapping典型配置举例

1. 组网需求

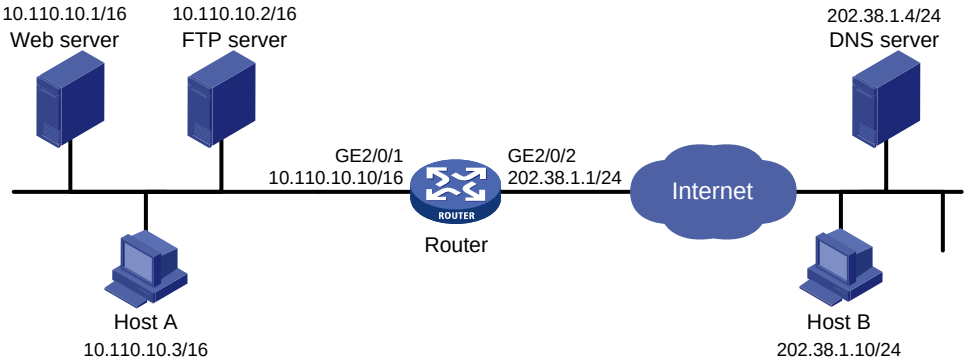
某公司内部对外提供 Web 和 FTP 服务。公司内部网址为 10.110.0.0/16。其中，Web 服务器地址为 10.110.10.1/16，FTP 服务器地址为 10.110.10.2/16。公司具有 202.38.1.1 至 202.38.1.3 三个公网 IP 地址。另外公司在外网有一台 DNS 服务器，IP 地址为 202.38.1.4。

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1-16 NAT DNS mapping 典型配置组网图



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

按照组网图配置各接口的 IP 地址，具体配置过程略。

开启 DNS 的 NAT ALG 功能。

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

进入接口 GigabitEthernet2/0/2。

```
[Router] interface gigabitethernet 2/0/2
```

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。

```
[Router-GigabitEthernet2/0/2] 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。

```
[Router-GigabitEthernet2/0/2] nat server protocol tcp global 202.38.1.2 inside 10.110.10.2
ftp
```

在接口 GigabitEthernet2/0/2 上配置 Easy IP 方式的出方向动态地址转换。

```
[Router-GigabitEthernet2/0/2] nat outbound
[Router-GigabitEthernet2/0/2] quit
```

配置两条 DNS mapping 表项：Web 服务器的域名 www.server.com 对应 IP 地址 202.38.1.2；FTP 服务器的域名 ftp.server.com 对应 IP 地址 202.38.1.2。

```
[Router] nat dns-map domain www.server.com protocol tcp ip 202.38.1.2 port http
[Router] nat dns-map domain ftp.server.com protocol tcp ip 202.38.1.2 port ftp
[Router] quit
```

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。

```
[Router] display nat all
NAT outbound information:
  Totally 1 NAT outbound rules.
  Interface: GigabitEthernet2/0/2
    ACL: ---          Address group: ---    Port-preserved: N
    NO-PAT: N         Reversible: N
    Config status: Active

NAT internal server information:
  Totally 2 internal servers.
  Interface: GigabitEthernet2/0/2
    Protocol: 6(TCP)
    Global IP/port: 202.38.1.2/21
    Local IP/port : 10.110.10.2/21
    Config status : Active

  Interface: GigabitEthernet2/0/2
    Protocol: 6(TCP)
    Global IP/port: 202.38.1.2/80
    Local IP/port : 10.110.10.1/80
    Config status : Active

NAT DNS mapping information:
  Totally 2 NAT DNS mappings.
  Domain name: ftp.server.com
  Global IP  : 202.38.1.2
  Global port: 21
  Protocol   : TCP(6)
  Config status: Active

  Domain name: www.server.com
  Global IP  : 202.38.1.2
  Global port: 80
  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
```

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

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

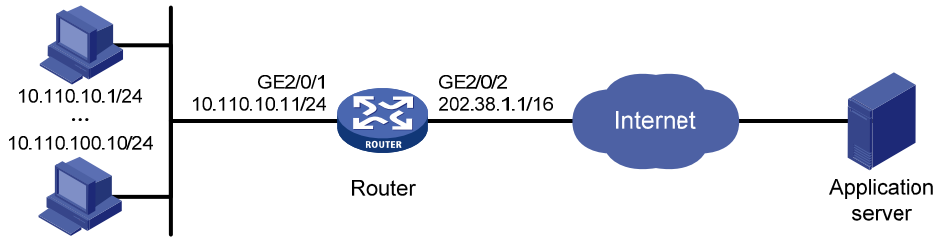
1.12.12 NAT444 端口块静态映射配置举例

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1-17 NAT444 端口块静态映射配置组网图



3. 配置步骤

按照组网图配置各接口的 IP 地址，具体配置过程略。

创建 NAT 端口块组 1。

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

添加私网地址成员 10.110.10.1～10.110.10.10。

```
[Router-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。

```
[Router-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。

```
[Router-port-block-group-1] block-size 500
[Router-port-block-group-1] port-range 10001 15000
[Router-port-block-group-1] quit
```

在接口 GigabitEthernet2/0/2 上配置 NAT444 端口块静态映射，引用端口块组 1。

```
[Router] interface gigabitethernet 2/0/2
[Router-GigabitEthernet2/0/2] nat outbound port-block-group 1
[Router-GigabitEthernet2/0/2] 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。

```
[Router] 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

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

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

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: GigabitEthernet2/0/2
    Port block group: 1
    Config status   : Active
```

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。

```
[Router]display nat port-block static
Slot 0:
Static port-block mapping tables:
Local VPN     Local IP         Global IP        Port block     Connections
---           10.110.10.1      202.38.1.100     10001-10500    2
---           10.110.10.2      202.38.1.100     10501-11000    0
---           10.110.10.3      202.38.1.100     11001-11500    0
---           10.110.10.4      202.38.1.100     11501-12000    0
---           10.110.10.5      202.38.1.100     12001-12500    1
---           10.110.10.6      202.38.1.100     12501-13000    0
---           10.110.10.7      202.38.1.100     13001-13500    0
---           10.110.10.8      202.38.1.100     13501-14000    0
---           10.110.10.9      202.38.1.100     14001-14500    0
---           10.110.10.10     202.38.1.100     14501-15000    0
```

1.12.13 NAT444 端口块动态映射配置举例

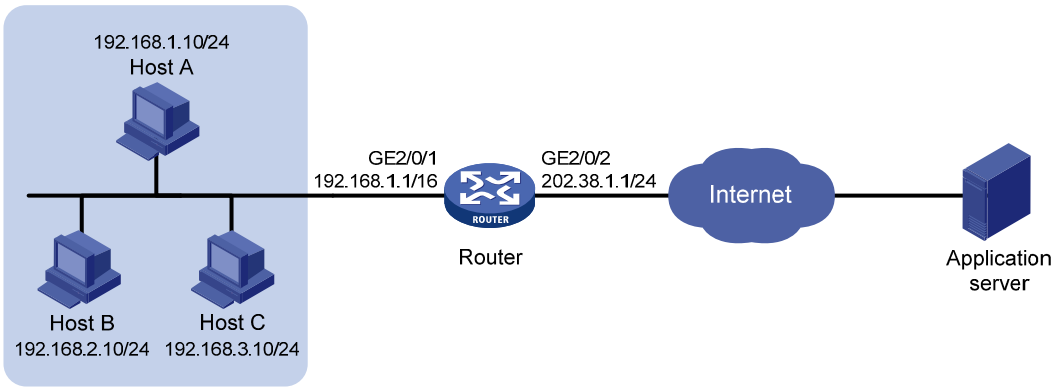
1. 组网需求

- 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。

需要实现，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1-18 NAT444 端口块动态映射配置组网图



3. 配置步骤

按照组网图配置各接口的 IP 地址，具体配置过程略。

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。

```
<Router> system-view
[Router] nat address-group 0
[Router-address-group-0] address 202.38.1.2 202.38.1.3
[Router-address-group-0] port-range 1024 65535
[Router-address-group-0] port-block block-size 300 extended-block-number 1
[Router-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。

```
[Router] acl number 2000
[Router-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Router-acl-basic-2000] quit
```

在接口 GigabitEthernet2/0/2 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。

```
[Router] interface gigabitethernet 2/0/2
[Router-GigabitEthernet2/0/2] nat outbound 2000 address-group 0
[Router-GigabitEthernet2/0/2] 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。

```
[Router]display nat all
NAT address group information:
  Totally 1 NAT address groups.
  Address group 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

NAT outbound information:
  Totally 1 NAT outbound rules.
  Interface: GigabitEthernet2/0/2
    ACL: 2000         Address group: 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

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

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

通过以下显示命令，可以看到系统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。

```
[Router]display nat statistics
Slot 0:
  Total session entries: 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
```