NAT 技术白皮书

目 录

1 概述

1.1 产生背景

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，IPv6 在实际引入上进展缓慢。在 IPv6 广泛应用之前，即 IPv4 向 IPv6 过渡期间，使用 NAT（Network Address Translation，网络地址转换）能够提高 IPv4 地址的利用率，保证业务的平滑过渡，为 IPv6 的部署争取时间。

1.2 技术优点

作为一种过渡方案，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。它具备以下优点：

- 对于内部通讯可以利用私网地址，如果需要与外部通讯或访问外部资源，则可通过将私网地址转换成公网地址来实现。
- 通过公网地址与端口的结合，可使多个私网用户共用一个公网地址。
- 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行为。
- 方便网络管理，如通过改变地址映射表就可实现私网服务器的迁移，内部网络的改变也很容易。

2 NAT 技术实现

2.1 NAT基本概念

NAT 基本概念如下：

- NAT 设备：配置了 NAT 功能的连接内部网络和外部网络的边缘设备。
- NAT 规则：用于进行地址转换的 NAT 配置称为 NAT 规则。
- NAT 地址：用于进行地址转换的公网 IP 地址，与外部网络路由可达，可静态指定或动态分配。
- NAT 表项：NAT 设备上用于记录网络地址转换映射关系的表项。
- Easy IP 功能：NAT 转换时直接使用设备上接口的 IP 地址作为 NAT 地址。设备上接口的地址可静态指定或通过 DHCP 协议动态获取。

2.2 NAT基本原理

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。这个过程对于私网侧或公网侧设备透明。基于这种基本的地址转换原理，数量庞大的内网主机就不再需要公网 IP 地址了。

2.3 NAT实现方式

2.3.1 静态方式

静态方式的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，即一个公网 IP 地址唯一对应一个内部主机。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。

2.3.2 NO-PAT 方式

NO-PAT 方式属于一对一的地址转换，在这种方式下只转换 IP 地址，而对 TCP/UDP 协议的端口号不处理，一个公网 IP 地址不能同时被多个用户使用。

如图 1 所示，NO-PAT 方式的处理过程如下：

(1) NAT 设备收到私网侧主机发送的访问公网侧服务器的报文。

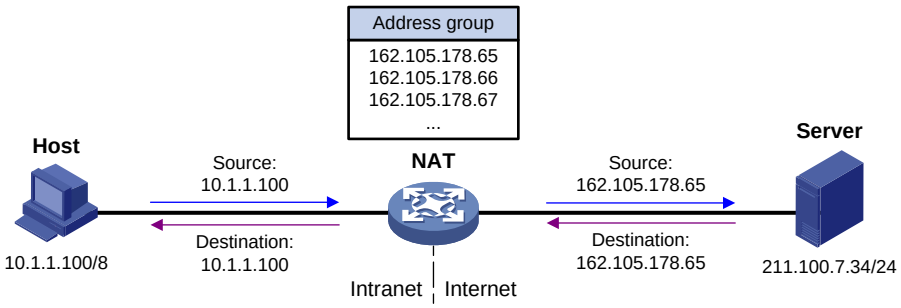
(2) NAT 设备从地址池中选取一个空闲的公网 IP 地址，建立与私网侧报文源 IP 地址间的 NAT 转换表项，并依据查找 NAT 表项的结果将报文转换后向公网侧发送。

(3) NAT 设备收到公网侧的回应报文后，根据其目的 IP 地址反向查找 NAT 表项，并依据查表结果将报文转换后向私网侧发送。

说明

由于 NO-PAT 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。

图1 NO-PAT 方式原理图



2.3.3 PAT 方式

由于 NO-PAT 方式并未实现地址复用，因此并不能解决公网地址短缺的问题，而 PAT（Port Address Translation）方式则可以解决这个问题。

PAT 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，实现了地址的复用，因此是地址转换实现的主要形式。

目前 PAT 仅支持对传输层协议为 TCP、UDP 或 ICMP 的报文进行“IP 地址＋端口号”转换。

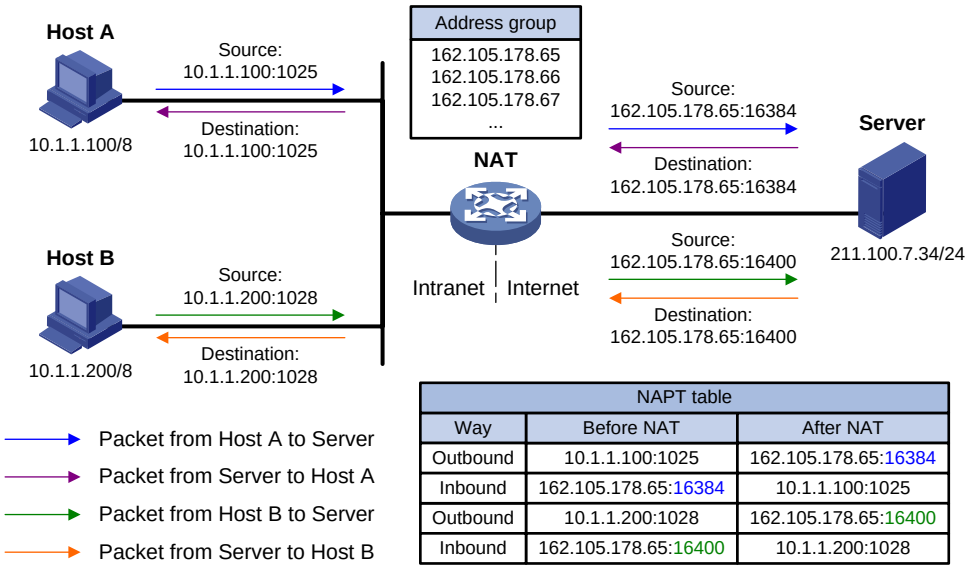
如图 2 所示，PAT 方式的处理过程如下：

(1) NAT 设备收到私网侧主机发送的访问公网侧服务器的报文。

(2) NAT 设备从地址池中选取一对空闲的“公网 IP 地址＋端口号”，建立与私网侧报文“源 IP 地址＋源端口号”间的 PAT 转换表项，并依据查找 PAT 表项的结果将报文转换后向公网侧发送。

(3) NAT 设备收到公网侧的回应报文后，根据其“目的 IP 地址＋目的端口号”反向查找 PAT 表项，并依据查表结果将报文转换后向私网侧发送。

图2 PAT 方式原理图



NAPT table		
Way	Before NAT	After NAT
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

2.3.4 NAT Server 方式

出于安全考虑，大部分私网主机通常并不希望被公网用户访问。但在某些实际应用中，需要给公网用户提供一个访问私网服务器的机会。而在 NO-PAT 或 PAT 方式下，由于由公网用户发起的访问无法动态建立 NAT 表项，因此公网用户无法访问私网主机。NAT Server（NAT 内部服务器）方式就可以解决这个问题——通过静态配置“公网 IP 地址＋端口号”与“私网 IP 地址＋端口号”间的映射关系，NAT 设备可以将公网地址“反向”转换成私网地址。

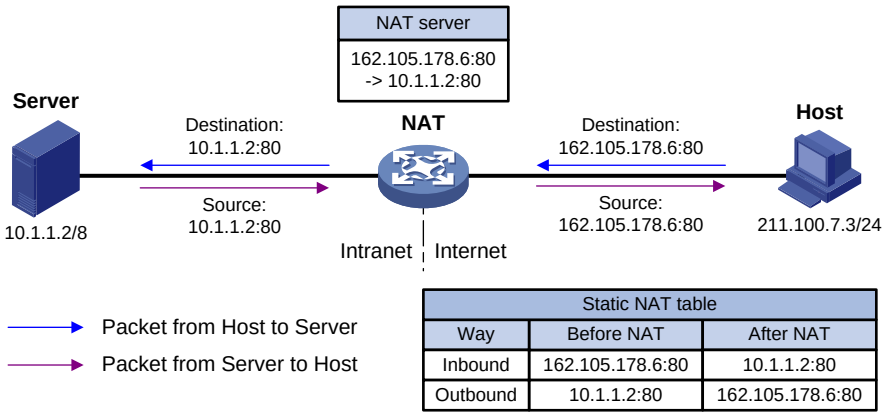
如图 3 所示，NAT Server 方式的处理过程如下：

(1) NAT 设备收到公网侧主机发送的访问私网侧服务器的报文。

(2) NAT 设备根据公网侧报文的“目的 IP 地址＋目的端口号”反向查找静态 NAT 表项，并依据查表结果将报文转换后向私网侧发送。

(3) NAT 设备收到私网侧的回应报文后，根据其“源 IP 地址＋源端口号”查找静态 NAT 表项，并依据查表结果将报文转换后向公网侧发送。

图3 NAT Server 方式原理图



Static NAT table		
Way	Before NAT	After NAT
Inbound	162.105.178.6:80	10.1.1.2:80
Outbound	10.1.1.2:80	162.105.178.6:80

2.3.5 Easy IP 方式

EASY IP 方式是指直接使用接口的公网 IP 地址作为转换后的源地址进行地址转换，它可以动态获取出接口地址，从而有效支持出接口通过拨号或 DHCP 方式获取公网 IP 地址的应用场景。

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。

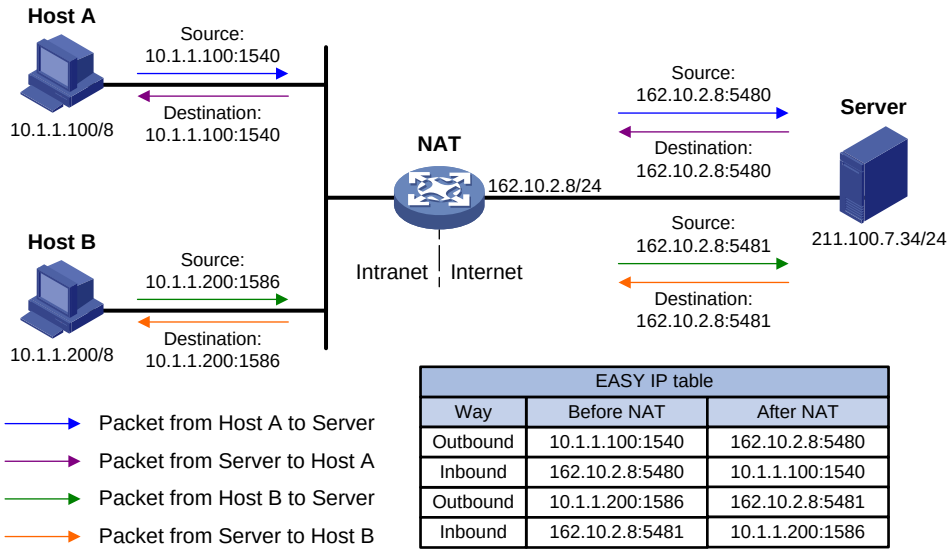
如图 4 所示，EASY IP 方式的处理过程如下：

(1) NAT 设备收到私网侧主机发送的访问公网侧服务器的报文。

(2) NAT 设备利用公网侧接口的“公网 IP 地址＋端口号”，建立与私网侧报文“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。

(3) NAT 设备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私网侧发送。

图4 EASY IP 方式原理图



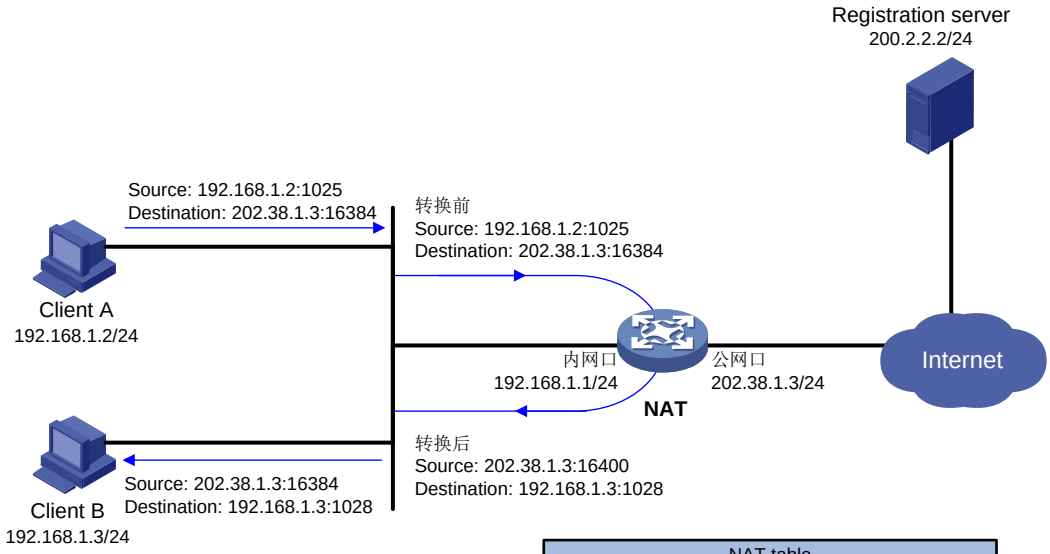
EASY IP table		
Way	Before NAT	After NAT
Outbound	10.1.1.100:1540	162.10.2.8:5480
Inbound	162.10.2.8:5480	10.1.1.100:1540
Outbound	10.1.1.200:1586	162.10.2.8:5481
Inbound	162.10.2.8:5481	10.1.1.200:1586

2.3.6 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。开启 NAT hairpin 的内网侧接口上会对报文同时进行源地址和目的地址的转换。它支持两种组网模式：

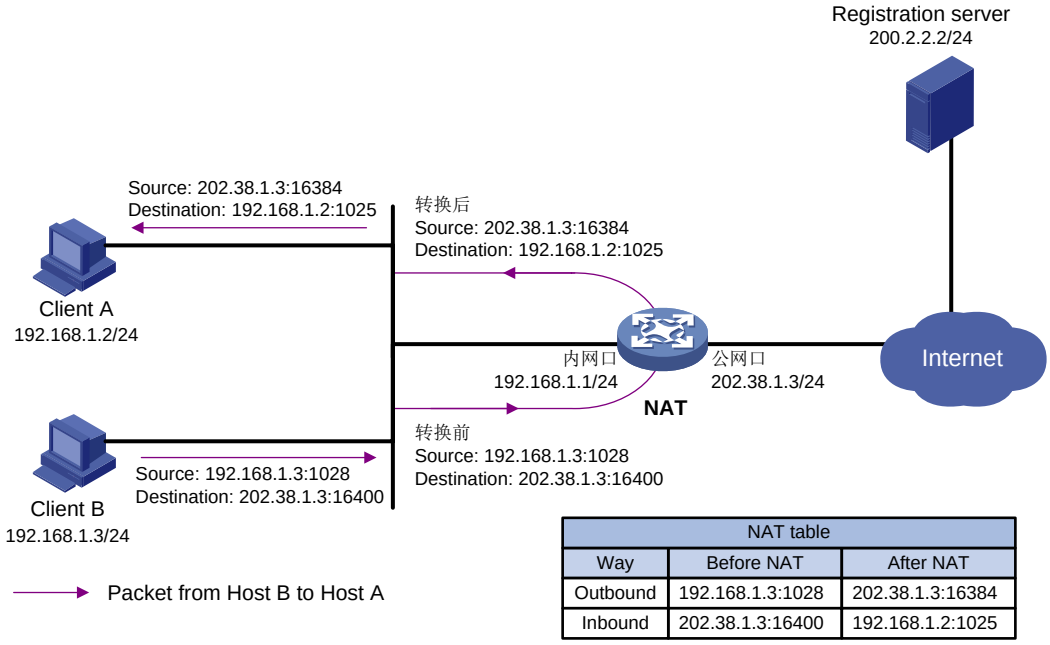
(1) P2P：位于内网侧的用户之间通过 NAT 地址互访。内网各主机首先向外网服务器注册自己 NAT 转换后的外网 IP 地址和端口号信息。如图 5 和图 6 所示，当内网的一个客户端使用 NAT 地址访问内网的另一个客户端时，首先从服务器获取对方注册的 IP 地址和端口号信息，然后根据该信息与对方建立连接。

图5 P2P 组网模式下的 NAT hairpin（Packet from Host A to Host B）



NAT table		
Way	Before NAT	After NAT
Outbound	192.168.1.2:1025	202.38.1.3:16400
Inbound	202.38.1.3:16384	192.168.1.3:1028

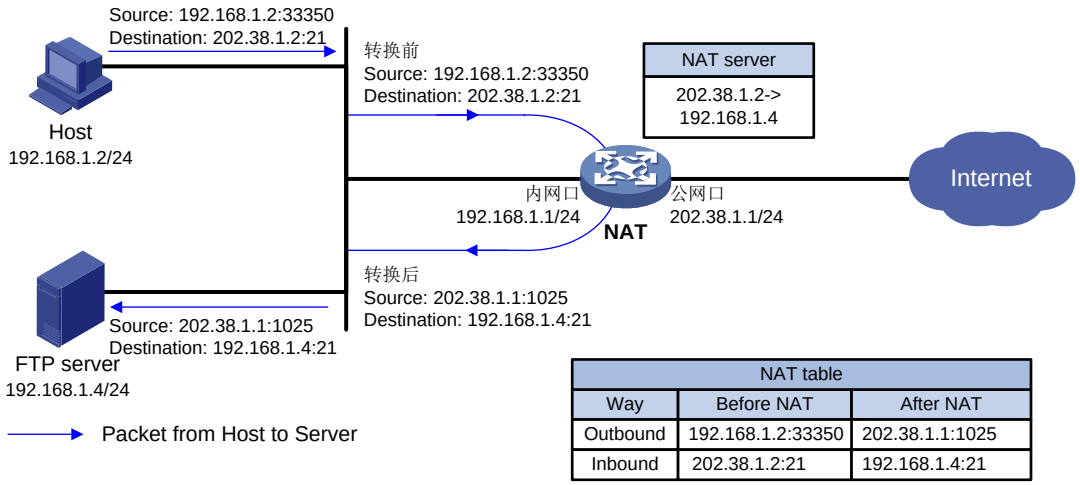
图6 P2P 组网模式下的 NAT hairpin（Packet from Host B to Host A）



NAT table		
Way	Before NAT	After NAT
Outbound	192.168.1.3:1028	202.38.1.3:16384
Inbound	202.38.1.3:16400	192.168.1.2:1025

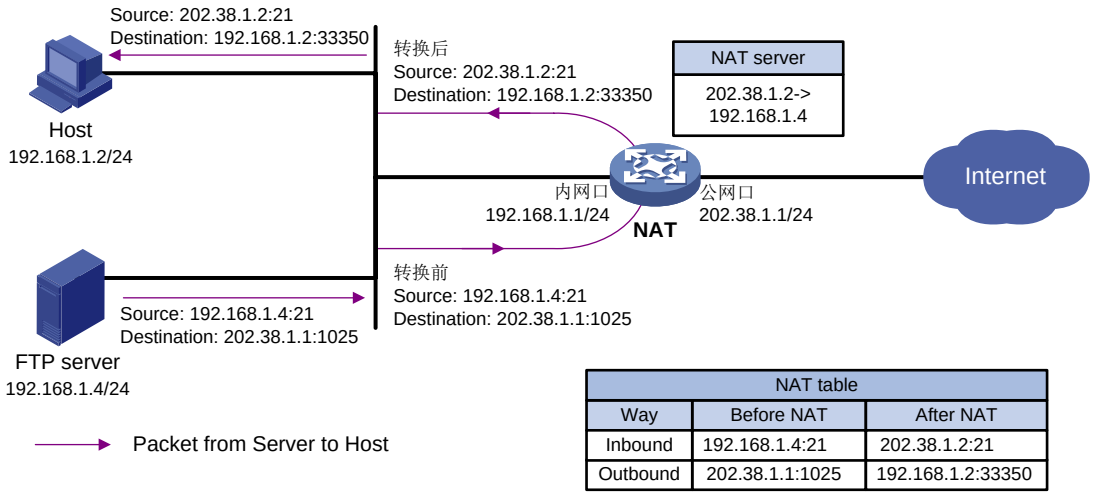
(2) C/S：位于内网侧的用户使用 NAT 地址访问内网服务器。如图 7 和图 8 所示，内部网络中有一台 FTP 服务器，内网用户使用 NAT 地址访问该 FTP 服务器时，NAT 设备同时转换访问内网服务器的报文的源和目的 IP 地址，其中，目的 IP 地址转换通过匹配外网接口上的内部服务器配置来完成，源地址转换通过匹配内部服务器所在接口上的出方向动态地址转换或出方向静态地址转换来完成。

图7 C/S 组网模式下的 NAT hairpin（Packet from Host to Server）



NAT table		
Way	Before NAT	After NAT
Outbound	192.168.1.2:33350	202.38.1.1:1025
Inbound	202.38.1.2:21	192.168.1.4:21

图8 C/S 组网模式下的 NAT hairpin（Packet from Server to Host）



NAT table		
Way	Before NAT	After NAT
Inbound	192.168.1.4:21	202.38.1.2:21
Outbound	202.38.1.1:1025	192.168.1.2:33350

2.4 NAT ALG机制

2.4.1 NAT ALG 机制简介

通常情况下，NAT 只改变 IP 报文头部地址信息，而不对报文载荷进行分析，这对于普通的应用层协议（如 Telnet）来说，并不会影响其业务的开展；然而有一些应用层协议，其报文载荷中可能也携带有地址或端口信息，若这些信息不能被有效转换，就可能导致问题。譬如，某些应用层协议会在客户端与服务器之间协商端口号，然后服务器使用协商出的端口号向客户端发起连接。如果 NAT 设备对二者的协商过程一无所知，那么当服务器向客户端发起连接时，就会因为在 NAT 设备上找不到内部与外部的 IP 地址/端口号对应关系而造成连接失败。

这个问题可以通过 ALG（Application Level Gateway，应用层网关）来解决。ALG 主要完成对应用层报文的解析和处理。NAT 利用 ALG 技术可以对应用层协议的报文载荷进行信息解析，改变封装在其中的地址和端口信息，并完成其它必要的工作以使应用协议可以穿越 NAT。

ALG 机制可处理的应用层协议包括 DNS、FTP、H.323、ILS 和 SIP 等。

2.4.2 基本概念

1. 会话

会话记录了传输层报文之间的交互信息，包括源 IP 地址、源端口、目的 IP 地址、目的端口，协议类型和源/目的 IP 地址所属的 VPN 实例。

2. 动态通道

当应用层协议报文中携带地址信息时，这些地址信息会被用于建立动态通道，后续符合该地址信息的连接将使用已经建立的动态通道来传输数据。

2.4.3 FTP 协议的 ALG 处理

在 FTP 工作过程中，客户端与服务器之间将建立两条 TCP 连接：一条为控制连接，负责传输诸如用户指令和参数等控制信息，其中包括发起数据连接时要用到的端口信息；另一条为数据连接，负责在服务器与客户端之间建立数据通道以传送文件。

FTP 有两种不同的工作模式：PORT（主动模式）和 PASV（被动模式）。不同模式下，FTP 连接建立过程中 NAT ALG 的处理机制有所不同。下面介绍两种不同模式下 FTP 的连接建立过程。

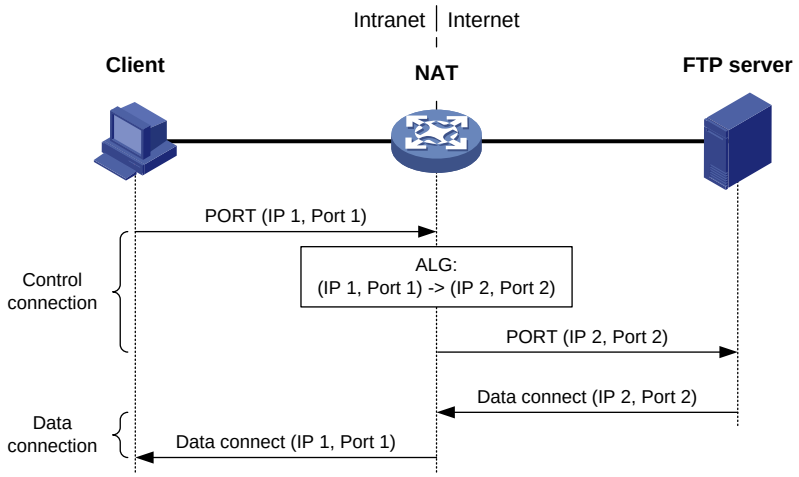
1. 主动模式下的 FTP 连接建立过程

在主动模式下，在由客户端发起控制连接中，客户端将指定的端口通过 PORT 指令发送给服务器，然后由服务器向该端口发起数据连接。

主动模式下，是否需要在控制连接中进行 ALG 处理与服务器和客户端所处的位置有关，具体如下：

- 客户端位于公网而服务器位于私网的情况下，由于客户端向服务器通告的是公网地址和端口，服务器可直接向其发起数据连接，因此无需在控制连接中进行 ALG 处理。
- 客户端位于私网而服务器位于公网的情况下，由于客户端向服务器通告的是私网地址和端口，因此需在控制连接中通过 ALG 处理将其转换为公网地址和端口，以供服务器发起数据连接所用。

图9 主动模式下的 ALG 处理



如图 9 所示，位于内部网络的客户端以 PORT 方式访问位于外部网络的 FTP 服务器，NAT 设备上配置了内网地址 IP1 到外网地址 IP2 的映射。同时，在 NAT 设备上开启 ALG 功能。

(2) 首先，由客户端向服务器发送 PORT 指令，以向服务器通知发起数据连接所应使用的地址和端口（IP 1，Port 1）；

(3) NAT 设备收到该指令后，将其中载荷所携带的私网地址和端口（IP 1，Port 1）替换为公网地址和端口（IP 2，Port 2），并据此创建相应的 PAT 表项——此过程即为 ALG 处理；

(4) 服务器收到该指令后，主动向公网地址和端口（IP 2，Port 2）发起数据连接，并在通过 NAT 设备时被转化为私网地址和端口（IP 1，Port 1）。

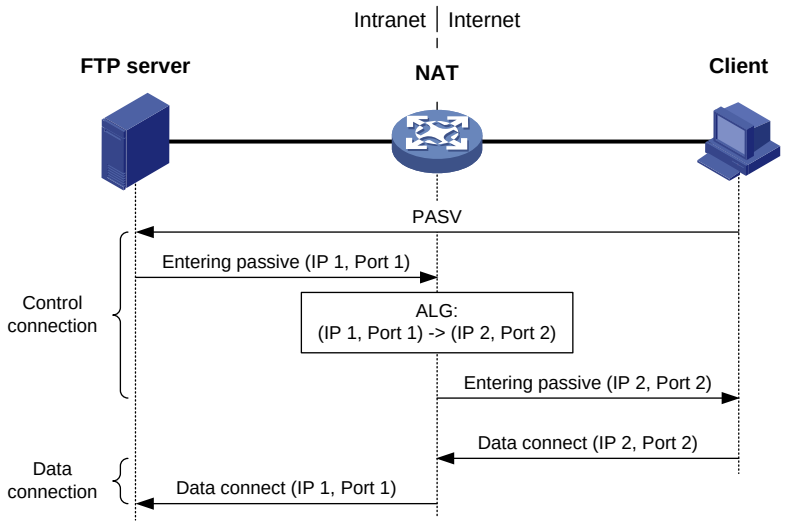
2. 被动模式下的 FTP 连接建立过程

在被动模式下，在由客户端发起控制连接中，客户端向服务器发送 PASV 请求来通知服务器它将发起被动模式，服务器再将指定的端口通过 PASV 响应发送给客户端，然后由客户端向该端口发起数据连接。

被动模式下，是否需要在控制连接中进行 ALG 处理与服务器和客户端所处的位置有关，具体如下：

- 服务器位于公网而客户端位于私网的情况下，由于服务器向客户端通告的是公网地址和端口，客户端可直接向其发起数据连接，因此无需在控制连接中进行 ALG 处理。
- 服务器位于私网而客户端位于公网的情况下，由于服务器向客户端通告的是私网地址和端口，因此需在控制连接中通过 ALG 处理将其转换为公网地址和端口，以供客户端发起数据连接所用。

图10 被动模式下的 ALG 处理



如图 10 所示，位于外部网络的 FTP 客户端以 PASV 方式访问位于内部网络的 FTP 服务器，NAT 设备上配置了内网地址 IP1 到外网地址 IP2 的映射，开启 ALG 功能后的地址转换过程如下：

(2) 客户端向服务器发送 PASV 请求；

(3) 服务器收到该请求后，选择并打开服务器端数据通道的地址和端口（IP 1，Port 1），并通过 PASV 响应向客户端返回该地址和端口；

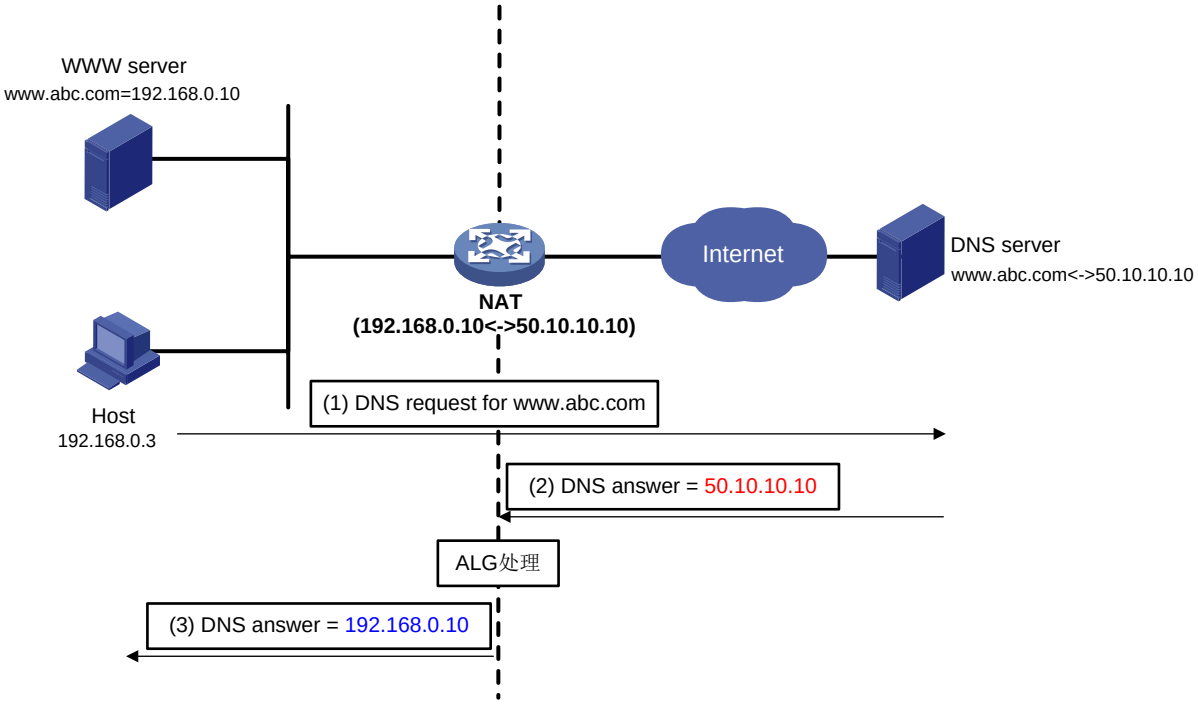
(4) NAT 设备收到该响应后，将其中载荷所携带的私网地址和端口（IP 1，Port 1）替换为公网地址和端口（IP 2，Port 2），并据此创建相应的 PAT 表项——此过程即为 ALG 处理；

(5) 客户端收到该响应后，向公网地址和端口（IP 2，Port 2）发起数据连接，并在通过 NAT 设备时被转换为私网地址和端口（IP 1，Port 1）。

2.4.4 DNS 协议的 ALG 处理

如图 11 所示，私网侧主机要使用域名访问内部 WWW 服务器（域名为 www.abc.com，对外公网地址为 50.10.10.10），但它查询的 DNS 服务器位于公网，DNS 服务器的响应报文中包含的是内部 WWW 服务器的公网地址，导致收到响应报文的私网用户无法利用域名访问内部服务器。此时，需要 NAT 设备在转换 DNS 报文的同时进行 ALG 处理，将 DNS 响应报文中携带的公网地址转换为服务器的私网地址。

图11 DNS 报文载荷的 ALG 处理示意图



DNS 报文载荷的 NAT ALG 处理机制如下：

(2) 私网主机向公网的 DNS 服务器发起 DNS 查询。

(3) DNS 服务器收到查询报文后进行查询处理，并将查询到的结果（域名 www.abc.com 对应 IP 地址 50.10.10.10）放在 DNS 响应报文（DNS Answer）中发送给私网主机对应的公网地址。

(4) DNS 响应报文在到达具有 ALG 特性的 NAT 设备时，报文载荷中的公网地址会被映射成为内部 WWW 服务器的私网地址。即，NAT 设备将收到的 DNS 响应报文数据载荷中的 IP 地址 50.10.10.10 替换为 192.168.0.10 后，将 DNS 响应报文发往私网。

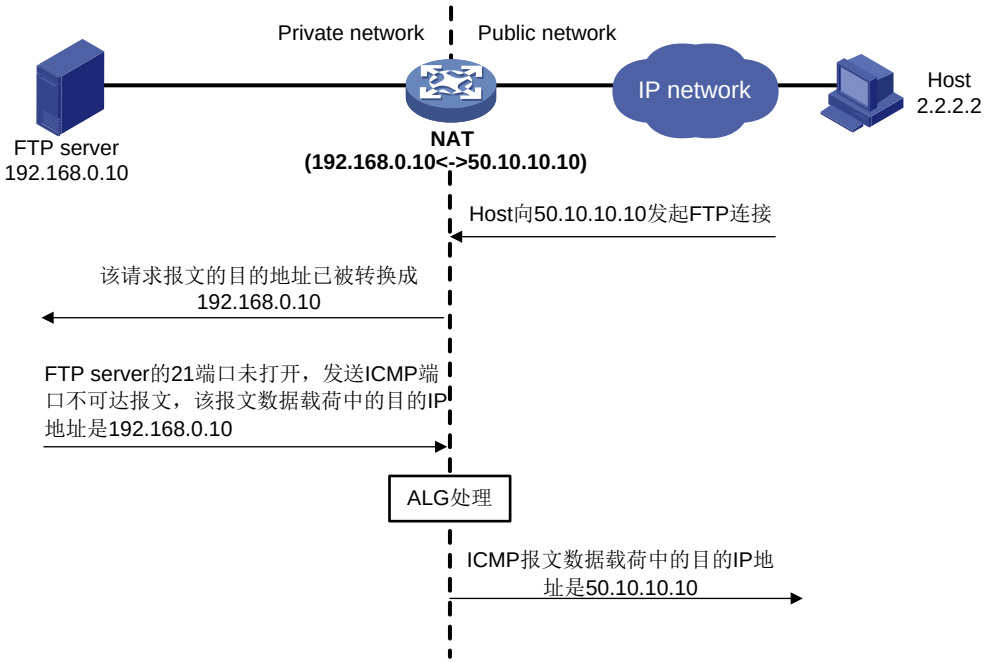
(5) 这样，私网主机收到的 DNS 响应报文中就携带了 www.abc.com 的私网 IP 地址，从而实现私网客户端通过公网 DNS 服务器以域名方式访问私网服务器的功能。

2.4.5 ICMP 协议的 ALG 处理

如图 12 所示，公网侧的主机要访问私网中的 FTP 服务器，该内部服务器对外的公网地址为 50.10.10.10。若内部 FTP 服务器的 21 端口未打开，那么它会向主机发送一个 ICMP 差错报文，该差错报文的数据载荷中的 IP 地址信息为 FTP 服务器的私网 IP 地址。在这种情况下，如果 ICMP 差错报文未经 ALG 处理直接从私网发送到公网，那么公网主机就无法识别该差错报文属于哪个应用程序，同时也会将 FTP 服务器的私网地址泄漏到公网中。

因此，需要 NAT 设备对 ICMP 差错报文进行 ALG 处理。ALG 会根据原始 FTP 会话的地址转换信息记录，将其数据载荷中的私网地址 192.168.0.10 还原成公网地址 50.10.10.10，再将该 ICMP 差错报文发送到公网。这样，公网主机就可以正确识别出错的应用程序，同时也避免了私网地址的泄漏。

图12 ICMP 差错报文载荷的 ALG 处理示意图



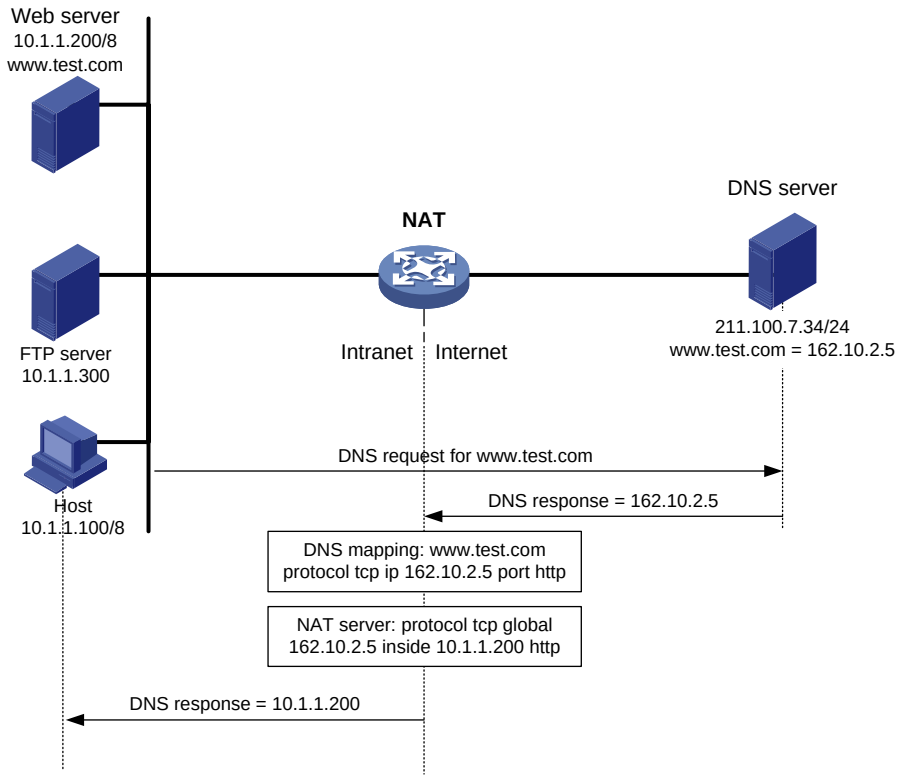
2.4.6 DNS Mapping 方式

DNS Mapping 主要用于解决普通的 NAT ALG 在特定组网时的问题。如图 13 所示，DNS 服务器位于公网，NAT 设备使用一个公网地址映射内部的多个服务器，内网主机通过域名访问内网 Web 服务器时，由于 NAT 设备开启了 DNS ALG 功能，因此会将 DNS 响应报文中的公网地址修改为内部服务器的私网地址。但是，由于 DNS 服务器的响应报文的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。所以 NAT 设备在修改 DNS 响应报文载荷中的外网 IP 地址时，有可能将其修改为 FTP 服务器的私网地址。这种情况下，内部主机收到响应报文后向 FTP 服务器发起 HTTP 访问，该访问将以失败告终。。

为了解决上述问题，需要借助 DNS mapping，通过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，进而精确匹配内部服务器配置获取应用服务器的内网 IP 地址。

当 NAT 设备收到 DNS 响应报文后，载荷中域名 www.test.com 对应的 IP 地址为 162.10.2.5，NAT 设备查找 DNS Mapping，得到“域名—公网 IP 地址—公网端口—协议类型”的对应关系，然后再从 NAT server 配置中得到对应的 Web 服务器的私网地址 10.1.1.200，NAT 设备将 DNS 响应报文中的地址修改为 10.1.1.200 后发送给内部主机。内部主机收到该 DNS 相应后，向 10.1.1.200 对应的服务器发起 HTTP 访问。

图13 DNS Mapping 方式原理图



2.5 NAT支持多VPN实例

NAT 多实例主要针对 MPLS L3VPN 用户访问公网或为公网提供服务而提出，可实现不同 VPN 内使用相同私网地址的用户同时访问外部网络。NAT 多实例在转换过程中增加了对 VPN 的识别和处理，把 VPN 作为区分会话的参数之一，以此实现了多实例同时访问公网的功能。

1. 多实例 NO-PAT

与单实例一样，多实例的 NO-PAT 只对私网的 IP 地址进行转换，但不同的是多实例 NO-PAT 在原有私网 IP 地址转换的基础上增加了对 VPN 的识别和处理，即在 NAT 转换表项中增加了 VPN 信息，并将其作为转换依据之一，以确保将不同 VPN 内相同的私网 IP 地址转换成不同的公网 IP 地址。

2. 多实例 PAT

与单实例相比，多实例的 PAT 在原有私网 IP 地址和端口号转换的基础上，增加了对 VPN 的识别和处理，即在 PAT 转换表项中增加了 VPN 信息，并将其作为转换依据之一，以确保将不同 VPN 内相同的“私网 IP 地址＋端口号”转换成不同的“公网 IP 地址＋端口号”。

3. 多实例 NAT Server

与单实例相比，多实例的 NAT Server 增加了私网侧对 VPN 的支持，即在所配置的静态 NAT 转换表项中增加了 VPN 信息，并将其作为转换依据之一，以确保将访问不同 VPN 的报文送达正确的 VPN，其处理流程与单实例相同。

4. 多实例 EASY IP

与单实例相比，多实例的 EASY IP 在原有私网 IP 地址和端口号转换的基础上，增加了对 VPN 的识别和处理，即在 EASY IP 转换表项中增加了 VPN 信息，并将其作为转换依据之一，以确保将不同 VPN 内相同的“私网 IP 地址＋端口号”转换成不同的“公网 IP 地址＋端口号”。

5. 多实例 DNS Mapping

与单实例相比，多实例的 DNS Mapping 增加了私网侧对 VPN 的支持，即在所配置的 DNS Mapping 映射表项中增加了 VPN 信息，并将其作为转换依据之一，以确保将访问不同 VPN 的报文送达正确的 VPN，其处理流程与单实例相同。

6. 多实例 ALG 处理

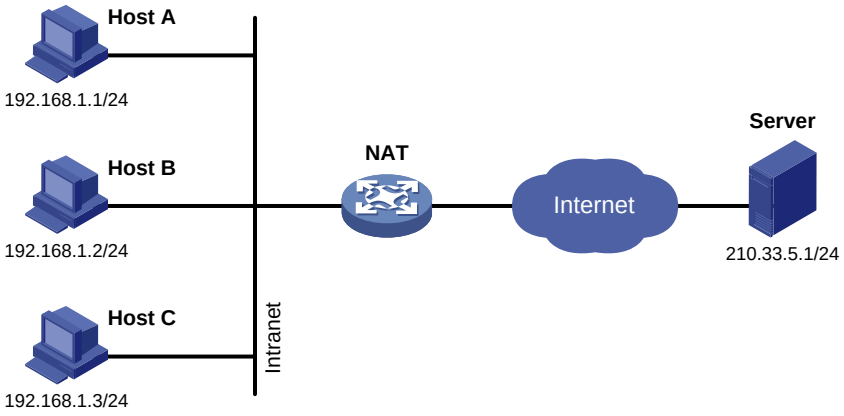
多实例的 ALG 处理流程与单实例基本相同，不同的是 NAT 设备在创建公网与私网的地址端口映射表项时，NAT 多实例在私网侧地址和端口基础上增加了对 VPN 的识别与处理，即在映射表项中增加了 VPN 信息，譬如将私网侧的（VPN A，IP 1，Port 1）与公网侧的（IP 2，Port 2）进行映射。

3 典型组网应用

3.1 私网主机访问公网服务器

在许多小区、学校和企业网的内网规划中，由于公网地址资源有限，内部用户实际使用的都是私网地址，在这种情况下，可以使用 NAT 技术来实现内部用户对公网的访问。如图 14 所示，通过在 NAT 网关上配置 NAT 转换规则，可以实现私网主机访问公网服务器。

图14 私网主机访问公网服务器组网图

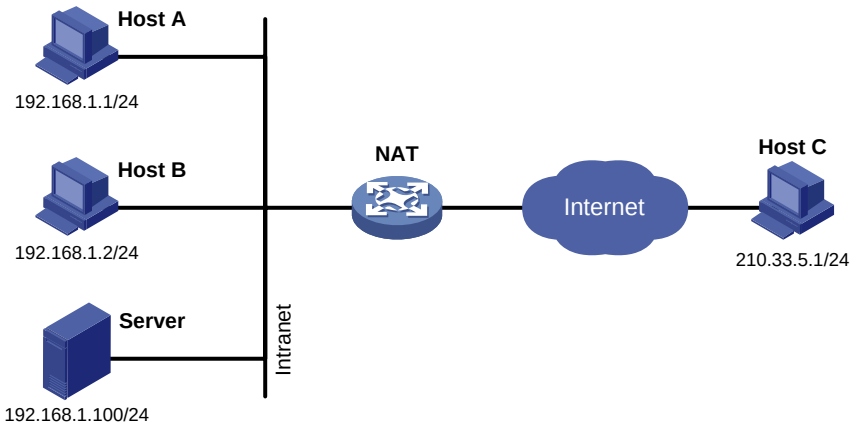


3.2 公网主机访问私网服务器

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 15 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，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。

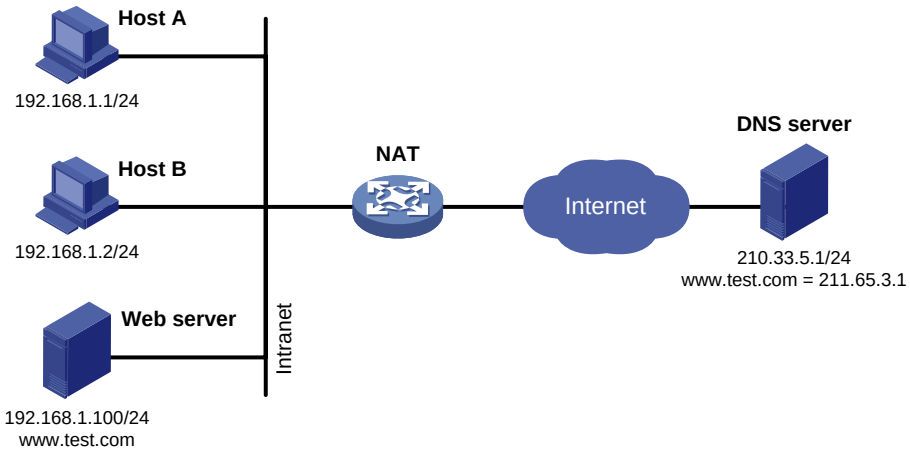
图15 公网主机访问私网服务器组网图



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 16 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。

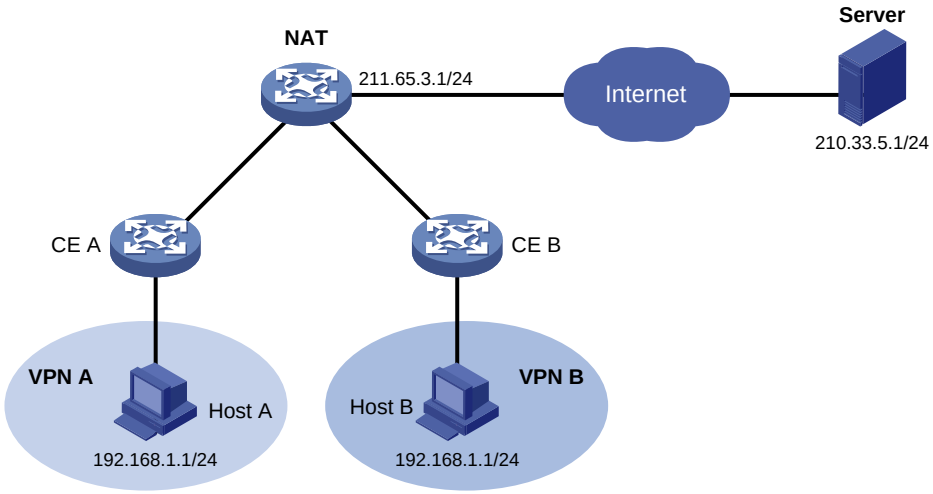
图16 私网主机通过域名访问私网服务器组网图



3.4 不同VPN的主机使用相同的私网地址访问公网

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 17 所示，Host A 和 Host B 具有相同的私网地址，且分属不同的 VPN，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17 NAT 多实例组网图



4 参考文献

- RFC 1631：The IP Network Address Translator (NAT)
- RFC 2663：IP Network Address Translator (NAT) Terminology and Considerations
- RFC 2993：Architectural Implications of NAT
- RFC 3022：Traditional IP Network Address Translator (Traditional NAT)
- RFC 3027：Protocol Complications with the IP Network Address Translator