项目 11 网络地址转换

主编：钟祥睿等

上海交通大学出版社

目录

单元学习目标

知识目标

1. 了解 NAT 的技术背景
2. 理解不同类型 NAT 的技术原理
3. 知道在不同场景下如何选用不同类型的 NAT 技术

技能目标

1. 掌握静态 NAT 的配置方法
2. 掌握动态 NAT 的配置方法
3. 掌握动态 NAPT 的配置方法
4. 掌握 Easy IP 的配置方法
5. 掌握 NAT Server 的配置方法

一 项目描述

当今的 Internet 使用 TCP/IP 实现了全世界的计算机互联互通，每一台连入 Internet 的计算机要和别的计算机通信，都必需拥有一个唯一的、合法的 IP 地址，此 IP 地址由 Internet 管理机构 NIC 统一进行管理和分配。而 NIC 分配的 IP 地址称为公有的、合法的 IP 地址，这些 IP 地址具有唯一性，连入 Internet 的计算机只要拥有 NIC 分配的 IP 地址就可以和其他计算机通信。

但是，由于当前普遍使用的 TCP/IP 协议版本还是 IPv4，它具有天生的缺陷，就是 IP 地址数量不够多，难以满足目前爆炸性增长的 IP 需求。所以，不是每一台计算机都能申请并获得 NIC 分配的 IP 地址。一般而言，需要连上 Internet 的个人或家庭用户，通过 Internet 的服务提供商 ISP 间接获得合法的公有 IP 地址（例如，用户通过 ADSL 线路拨号，从电信获得临时租用的公有 IP 地址）；对于大型机构而言，它们可能直接向 Internet 管理机构申请并使用永久的公有 IP 地址，也可能是通过 ISP 间接获得永久或临时的公有 IP 地址。

一 项目描述

由于无论是通过哪种方式获得公有的 IP 地址，实际上当前的可用 IP 地址数量依然不足。 IP 地址作为有限的资源， NIC 要为网络中数以亿计的计算机都分配公有的 IP 地址是不可能的。同时，为了使计算机能够具有 IP 地址并在专用网络（内部网络）中通信， Internet 管理机构 NIC 定义了供专用网络内的计算机使用的专用 IP 地址。这些 IP 地址是在局部使用的（非全局的、不具有唯一性）、非公有的（私有的） IP 地址，这些 IP 地址的地址范围具体如下：

A 类地址： 10.0.0.0 ～ 10.255.255.255

B 类地址： 172.16.0.0 ～ 172.31.255.255

C 类地址： 192.168.0.0 ～ 192.168.255.255

一 项目描述

组织机构可根据自身园区网的大小以及计算机数量的多少来采用不同类型的专用地址范围或者它们的组合。但是，这些 IP 地址不可能出现在 Internet 上，也就是说源地址或目的地址为这些专有 IP 地址的数据包是不可能在 Internet 上被传输的，这样的数据包只能在内部专用网络中被传输。

为解决 IPV4 公有地址不足，而私有地址又不能在公网上使用的问题， NAT （ Network Address Translation ，网络地址转换）技术应需而生。

二 项目分析

随着 Internet 的发展和网络应用的增多，有限的 IPv4 公有地址已经成为制约网络发展的瓶颈。为解决这个问题， NAT （ Network Address Translation ， 网络地址转换）技术应需而生。

NAT 技术主要用于实现内部网络的主机访问外部网络。一方面 NAT 缓解了 IPv4 地址短缺的问题，另一方面还带来了两个好处：

1. 可以有效避免来自外部网络的攻击，很大程度上提高了网络的安全性。

2. 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相互通信的问题。

由于私有地址无法在 Internet 上路由转发，访问 Internet 的 IP 数据包将缺乏路由无法到达私有网络出口设备。因此，如果使用了私有地址的私有网络需要访问 Internet ，就必须在网络出口设备上配置 NAT ，将访问 Internet 的 IP 数据报文中的私有

二 项目分析

通过私有地址的使用，并结合 NAT 技术，可以有效节约公网 IPv4 地址。

NAT 可以应用于多种场景，其中最为常见的应用场景有：

1. 在私有网络内部（园区网络、家庭网络）使用私有地址，有多个公有地址可用（公有地址远少于内网使用的私有地址），出口设备部署 NAT，对于“从内到外”的流量，网络设备通过 NAT 将数据包的源地址进行转换，将其转换成特定的公有地址。

2. 在私有的园区网络使用私有地址，内部部署有允许外部访问的服务器，出口设备部署了 NAT，对于“从外到内的”流量，则对数据包的目的地址进行转换，将其转换成服务器的私有地址。

3. 在小型的私有网络内部使用私有地址，只有一个公有地址可用，该地址配置在出口设备的出接口上，出口设备部署 NAT，对于“从内到外”的流量，网络设备通过 NAT 将数据包的

三 相关知识

11.1 NAT 概述

NAT （ Network Address Translation ， 网络地址转换），是一种 IETF （ Internet Engineering Task Force, Internet 工程任务组）标准，在当前网络中被广泛部署的技术，是把内部私有网络地址转换成合法外部公有网络地址的技术，一般部署在网络出口设备，例如路由器或防火墙上。

由于当前常用的 TCP/IP 协议版本 IPv4 ，具有天生缺陷， IP 地址数量不够多，难以满足目前爆炸性增长的 IP 需求。如果专用网络的计算机要访问 Internet ，则组织机构在连接 Internet 的设备上至少需要一个公有 IP 地址，然后采用 NAT 技术，将内部网络的计算机私有 IP 地址转换为公有 IP 地址，从而让使用私有 IP 地址的计算机能够和 Internet 中的计算机进行通信，转换过程见下图所示。

三 相关知识

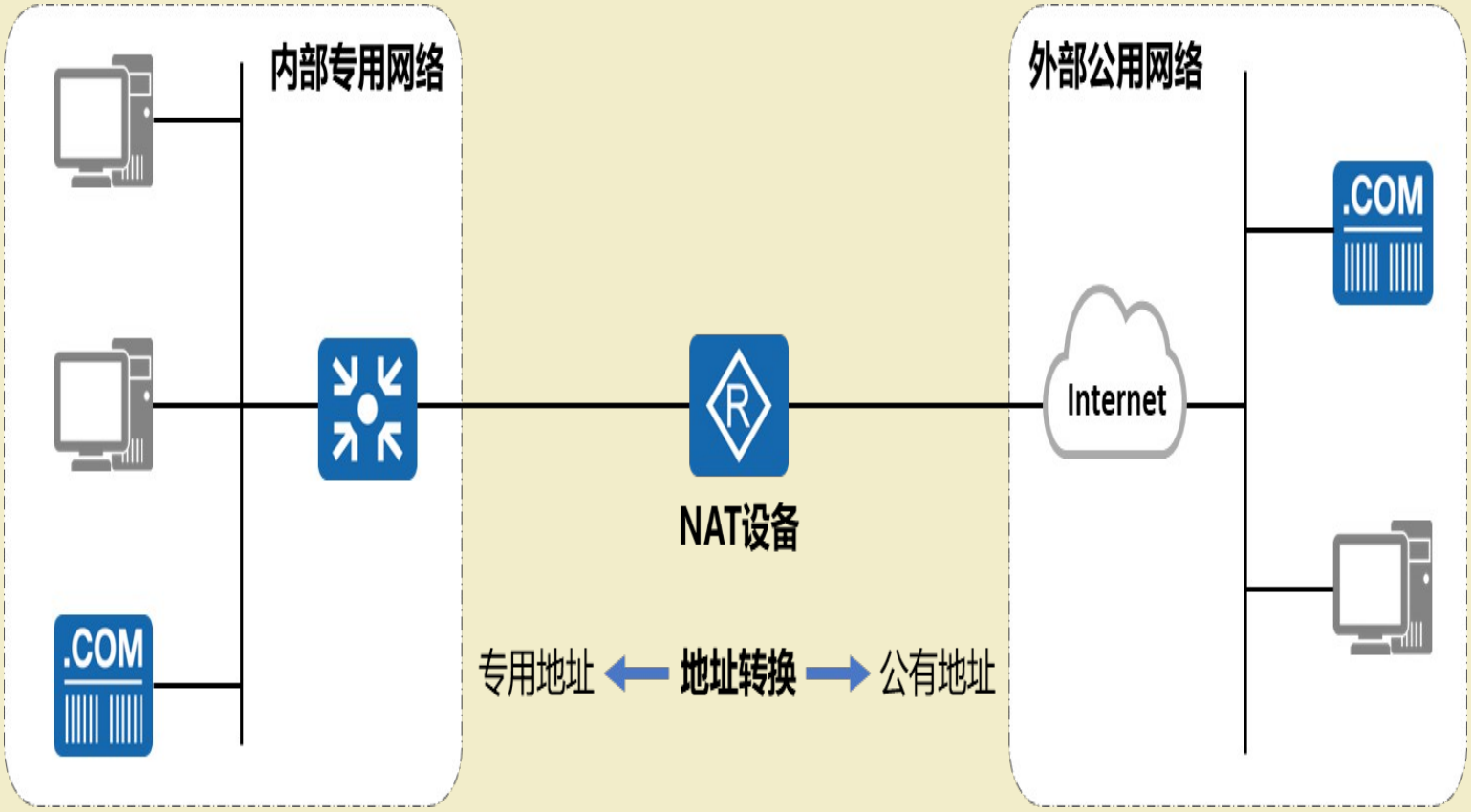


图 11-1 网络地址转换

11.2 NAT 工作原理

根据工作方式不同， NAT 可以分为静态 NAT 、动态 NAT 、动态 NAPT 等类型，下面将分别详细介绍各类 NAT 的工作原理及配置命令。

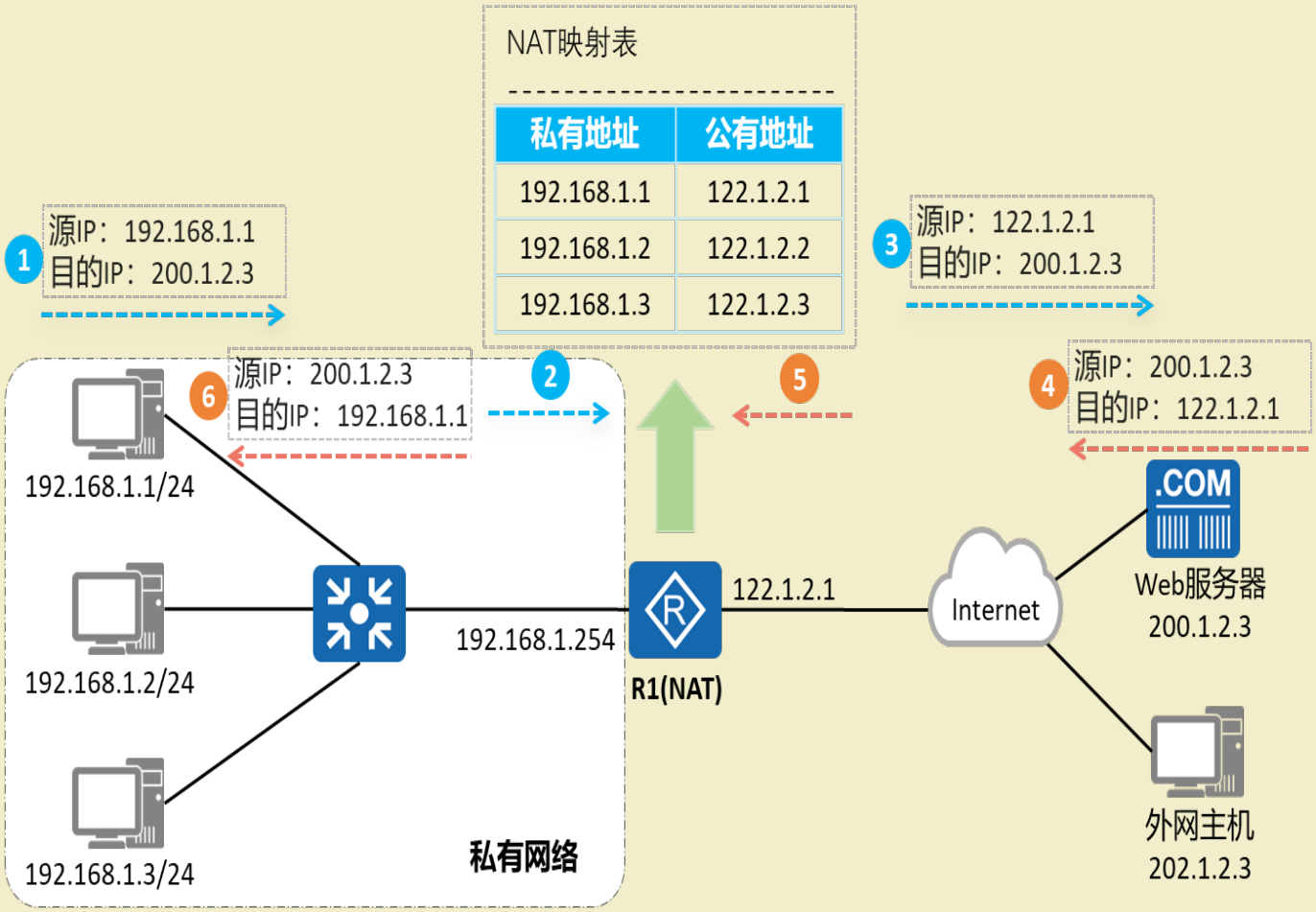
1. 静态 NAT

将私有 IP 地址转换为公有 IP 地址，每个私有地址都有一个与之对应并且固定的公有地址，即私有地址和公有地址之间的关系是一对一映射。静态 NAT 通常应用在允许外网用户访问内网服务器的场景。

静态 NAT 支持双向互访，即私有地址访问 Internet 经过出口设备 NAT 转换时，会被转换成对应的公有地址。同时，外部网络访问内部网络时，其报文中携带的公有地址（目的地址）也会被 NAT 设备转换成对应的私有地址。

三 相关知识

静态 NAT 的工作过程如图 11-2 所示。



三 相关知识

第①步：计算机 A （ 192.168.1.1 ）发送数据包给 web 服务器，数据包的源 IP 地址为 192.168.1.1 ， 目标 IP 地址为 200.1.2.3 。

第②步：数据包到达路由器 R1 时，路由器将查询本地的 NAT 映射表，找到映射条目后将数据包的源地址（ 192.168.1.1 ）转换为公网 IP 地址（ 122.1.2.1 ），目的地址保持不变。 NAT 路由器上有一个公有的 IP 地址池，在本次通信前，网络管理员已经在 NAT 路由器上做静态 NAT 地址映射关系，指定 192.168.1.1 与 122.1.2.1 映射。

第③步：转换后的数据包经在公网中传输，最终将被 Web 服务器接收。

第④步： Web 服务器收到数据包后，将响应内容封装在目的地址为 122.1.2.1 的数据包中，然后将该数据包发送出去。

第⑤步：目的地址为 122.1.2.1 数据包到达路由器 R1 后，路由器将对照自身的 NAT 映射表，找出对应关系，将源地址 122.1.2.1 转换为 192.168.1.1 ，然后将该数据包发送到内部网络中。

第⑥步：目的地址为 192.168.1.1 的数据包在内部网络中传送，最终到达计算机 A 。计算机 A 通过数据包的源地址（ 200.1.2.3 ），只知道此数据包是路由器发送过来的，实际上，该数据包是 Web 服务器发送的。

静态 NAT 的配置命令如下：

方式一：接口视图下配置静态 NAT

[Huawei-GigabitEthernet0/0/0] nat static global { global-address} inside {host-address }

其中 global-address 为公有地址， host-address 为私有地址。

方式二：系统视图下配置静态 NAT

[Huawei] nat static global { global-address} inside {host-address }

在接口下使能 nat static 功能。

[Huawei-GigabitEthernet0/0/0] nat static enable

例【 11.1 】：静态 NAT 配置案例，网络拓扑如图 11-2 所示。

在 R1 上配置静态 NAT ，将内网主机的私有地址一对一映射到公有地址。

[R1] interface GigabitEthernet0/0/1

[R1-GigabitEthernet0/0/1] ip address 122.1.2.1 24

[R1-GigabitEthernet0/0/1] nat static global 122.1.2.1 inside 192.168.1.1

[R1-GigabitEthernet0/0/1] nat static global 122.1.2.2 inside 192.168.1.2

[R1-GigabitEthernet0/0/1] nat static global 122.1.2.3 inside 192.168.1.3

2. 动态 NAT

静态 NAT 严格地一对一进行地址映射，这会导致即便内网主机长时间离线或者不发送数据时，与之对应的公有地址也处于使用状态。为了避免地址浪费，动态 NAT 提出了地址池的概念，即将所有可用的公有地址组成地址池。

当内部主机访问外部网络时临时分配一个地址池中未使用的地址，并将该地址标记为“ In Use”。当该主机不再访问外部网络时回收分配的地址，重新标记为“ Not Use”。

动态 NAT 的工作过程如图 11-3 所示。

三 相关知识

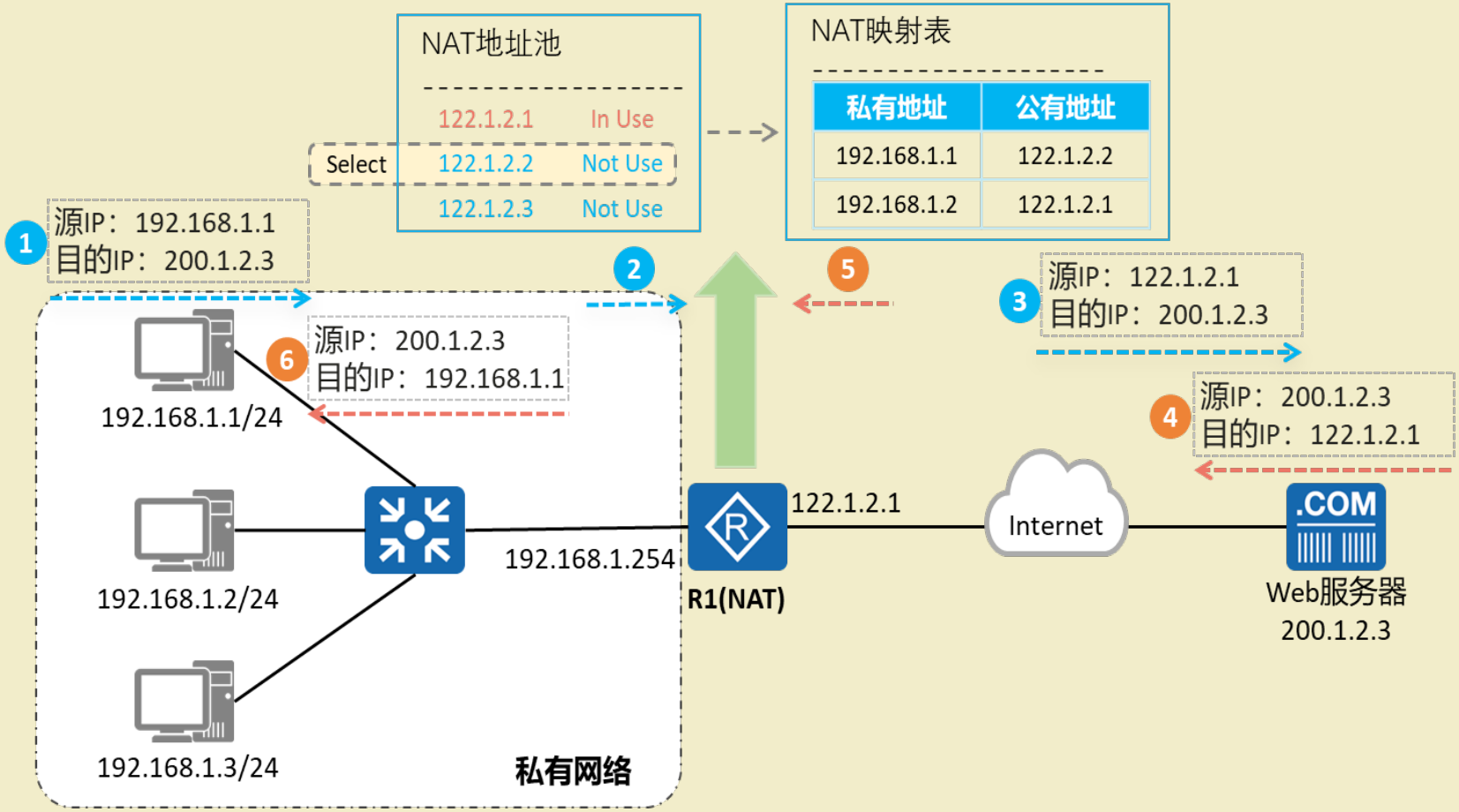


图 11-3 动态 NAT 工作过程

三 相关知识

与静态 NAT 类似，路由器上有一个公有 IP 地址池，地址池中有三个公有 IP 地址，它们是 122.1.2.1/24-122.1.2.3/24 。如图 11-3 所示，假设专用网络的计算机 A （ 192.168.1.1 ）需要和互联网的 Web 服务器（ 200.1.2.3 ）通信，其通信过程如下 。

第①步：计算机 A 发送源 IP 地址为 192.168.1.1 的数据包给 Web 服务器。

第②步：数据包经过路由器 R1 的时候，路由器调用 NAT 技术，查找 NAT 映射表，将数据包的源地址（ 192.168.1.1 ）转换为公有 IP 地址（ 122.1.2.2 ）。为什么会转换为 122.1.2.2 呢？由于路由器上的地址池有多个公有 IP 地址，当需要进行地址转换时，路由器会在地址池中选择一个未被占用的地址来进行转换。

这里假设后面两个地址未被占用，因此路由器挑选了第一个未被占用的地址（ 122.1.2.2 ）作为转换后的地址，同时将该地址的标记变为“ In Use”，同时生成一个临时的 NAT 映射表。地址池中的公有 IP 地址的数量决定了可以同时访问 Internet 的内网计算机的数量，如果地址池中的 IP 地址都被使用了，那么内网的其他计算机就不能够和 Internet 的计算机通信了。当内网计算机和外网计算机的通信连接结束后，路由器将释放被占用的公有 IP 地址，同时将该地址的标记变为“ Not Use”，这样，被释放的 IP 地址则又可以为其他内网计算机提供公网接入服务了。

第③步：源地址为 122.1.2.2 的数据包在 Internet 上转发，最终被 Web 服务器接收。

第④步： Web 服务器收到源地址为 122.1.2.2 的数据包后，将响应内容封装在目的地址为 122.1.2.2 的数据包中，然后将该数据包发送出去。

第⑤步：目的地址为 122.1.2.2 的数据包经过 Internet 其他路由器的转发，最终到达连接专用网络的路由器 R1 上，路由器查找 NAT 映射表，根据公有地址查找私有地址，将目的地址为 122.1.2.2 的数据包转换为目的地址为 192.168.1.1 的数据包，然后发送到内部专用网络中。

第⑥步：目的地址为 192.168.1.1 的数据包在专用网络中传送，最终到达计算机 A 。计算机 A 通过数据包的源地址（ 200.1.2.3 ）知道此数据包是 Internet 上的 Web 服务器发送过来的。

三 相关知识

动态 NAT 的配置命令如下：

（1）创建公有地址池

[Huawei] nat address-group group-index start-address end-address

配置公有地址范围，其中 group-index 为地址池编号， start-address 、 end-address 分别为地址池起始地址、结束地址。

（2）配置地址转换的 ACL 规则

[Huawei] acl number

[Huawei-acl-basic-number] rule permit source source-address source-wildcard

配置基础 ACL，匹配需要进行动态转换的源地址范围。

（3）接口视图下配置带地址池的 NAT Outbound

[Huawei-GigabitEthernet0/0/0] nat outbound acl-number address-group group-

index [no-pat]

三 相关知识

接口下关联 ACL 与地址池进行动态地址转换， no-pat 参数指定不进行端口转换。

例【 11.2 】：动态 NAT 配置案例，网络拓扑如图 11-3 所示。

在 R1 上配置动态 NAT ，将内网主机的私有地址动态映射到公有地址。

```
[R1] nat address-group 1 122.1.2.1 122.1.2.3
[R1] acl 2000
[R1-acl-basic-2000] rule 5 permit source 192.168.1.0 0.0.0.255
[R1-acl-basic-2000] quit
[R1] interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1] nat outbound 2000 address-group 1 no-pat
```

3. 动态 NAPT

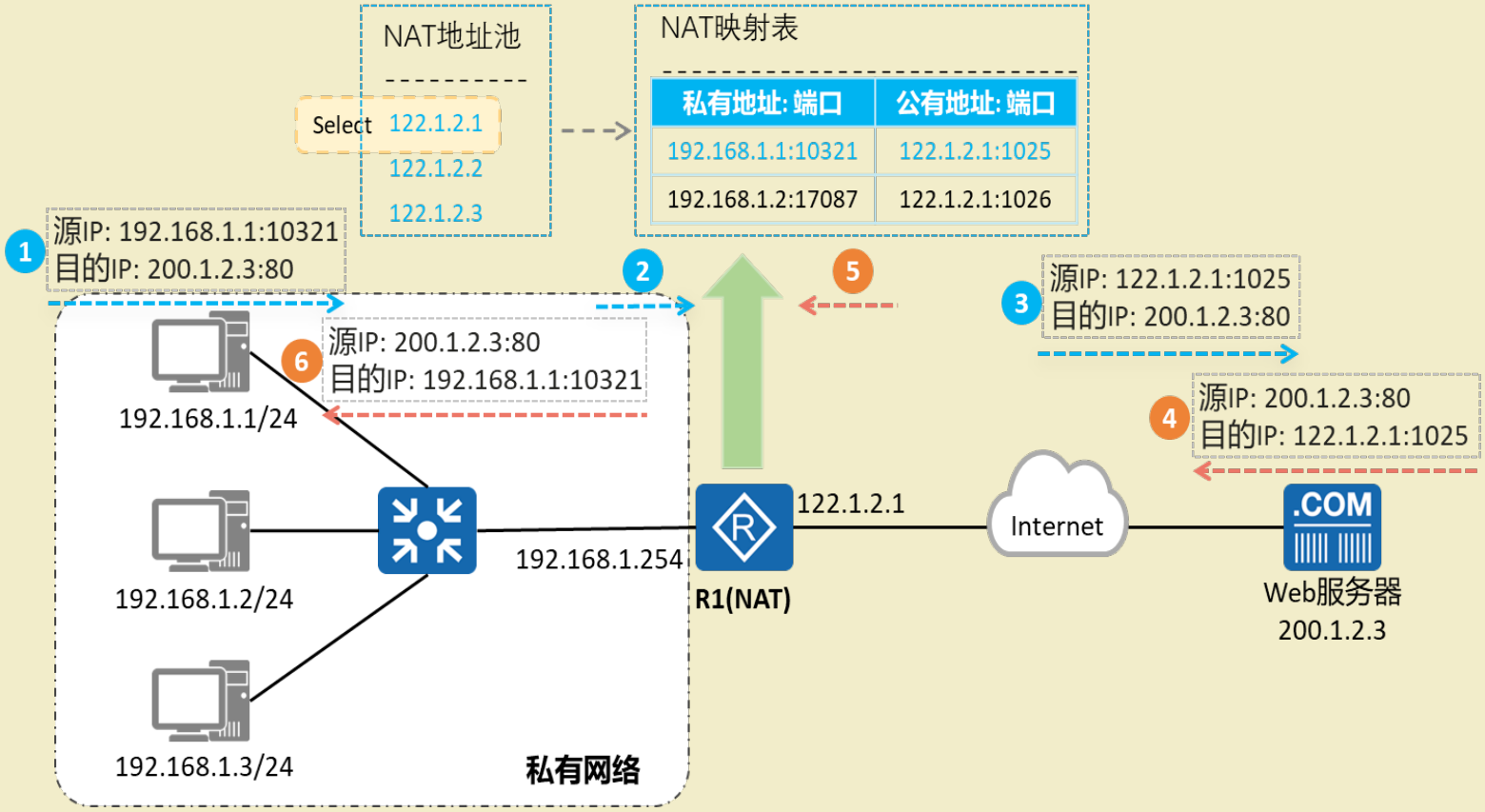
动态 NAT 选择地址池中的地址进行地址转换时不会转换端口号，即 No-PAT （ No-Port Address Translation ， 非端口地址转换），公有地址与私有地址还是 1:1 的映射关系，无法提高公有地址利用率。

NAPT （ Network Address and Port Translation ， 网络地址端口转换），从地址池中选择地址进行地址转换时不仅转换 IP 地址，同时也会对端口号进行转换，从而实现公有地址与私有地址的 1:n 映射，可以有效提高公有地址利用率。

NAPT 借助端口可以实现一个公有地址同时对应多个私有地址。该模式同时对 IP 地址和传输层端口（ TCP 或 UDP ）进行转换，实现不同私有地址（不同的私有地址，不同的源端口）映射到同一个公有地址（相同的公有地址，不同的源端口）。

三 相关知识

动态 NAPT 的工作过程如图 11-4 所示。



三 相关知识

“IP 地址”到“ IP 地址”的转换关系局限性很大，因为公有 IP 地址一旦被占用，内网的其他计算机就不能再使用被占用的公有 IP 地址访问外网。对于“ IP 地址 + 端口”的转换关系则非常灵活，一个 IP 地址可以和多个端口进行组合（自由使用的端口号有几万个： 1024-65535 ），所以，路由器上可用的网络地址映射关系条目数量就很多，完全可以满足大量的内网计算机访问外网需求。

如图 11-4 所示。假设私有网络的计算机 A （ 192.168.1.1 ）要访问外网的 Web 服务器站点，其通信过程如下。
第①步：计算机 A 发送数据包给 Web 服务器。数据包的源 IP 地址为 192.168.1.1 ，源端口号为 10321 （ 10321 为一个计算机 A 随机分配的端口号）；数据包的目的地址为 200.1.2.3 ，目的端口号为 80 （ Web 服务器默认端口号是 80 ）

第②步：数据包经过路由器的时候，路由器采用了动态NAPT 技术，以“ IP+ 端口”形式进行转换。数据包的源地址及源端口号将从 192.168.1.1:10321 转化为122.1.2.1:1025 （ 1025 为路由器随机分配的端口号），目的地址及端口号不变，仍然指向 Web 服务器的 Web 服务。转换后的源 IP 地址为路由器在外网的接口 IP 地址，源端口为路由器上未被使用的可分配端口号，这里假设为 1025 。

第③步：转换后的数据包在 Internet 上转发，最终被 Web 服务器接收。

第④步： Web 服务器收到数据包后，将响应内容封装在目的地址为 122.1.2.1 ，目的端口号为 1025 的数据包中（源地址及端口为 200.1.2.3:80 ），然后将数据包发送出去。

第⑤步：响应的数据包最终经过 Internet 转发，到达连接私有网络的路由器上，路由器查找 NAT 映射表，根据“公有地址 + 端口”信息查找对应的“私有地址 + 端口”，并进行 IP 数据报文目的地址、端口转换，将目的地址及端口号为 122.1.2.1:1025 的数据包转换为目的地址及端口号为 192.168.1.1:10321 的数据包，然后发送到私有网络中。

第⑥步：目的地址及端口号为 192.168.1.1:10321 的数据包在私有网络中传送，最终到达计算机 A 。计算机 A 通过数据包的源地址及端口号（ 200.1.2.3:80 ）知道此数据包是外网的 Web 服务器发送过来的。

动态 NAPT 的内外网“ IP+ 端口号”映射关系是临时性的，因此，它主要应用在为内网计算机提供外网访问服务的场景。典型的应用有：家庭的宽带路由器拥有动态 NAPT 功能，它可以满足家庭电子设备访问 Internet ；网吧的出口网关也拥有动态 NAPT 功能，它可以满足网吧电脑访问 Internet 。

动态 NAPT 的配置命令：*与动态 NAT 的配置命令相似，可参考之。*

例【 11.3 】：动态 NAPT 配置案例，网络拓扑如图 11-4 所示。

在 R1 上配置 NAPT，让内网所有私有地址转换为公有 IP 122.1.2.1 访问公网。

```
[R1] nat address-group 1 122.1.2.1 122.1.2.1
[R1] acl 2000
[R1-acl-basic-2000] rule 5 permit source 192.168.1.0 0.0.0.255
[R1-acl-basic-2000] quit
[R1] interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1] nat outbound 2000 address-group 1
```

4. Easy IP

实现原理和 NAPT 相同，同时转换 IP 地址、传输层端口，区别在于 Easy IP 没有地址池的概念，因为 Easy IP 只会用到一个公有 IP 地址，该 IP 地址就是路由器连接公网的出口 IP 地址。 Easy IP 具有以下特点：

（1） Easy IP 会建立并维护一张动态地址及端口映射表，且会将表中公有 IP 地址绑定成路由器公网出口 IP 地址；

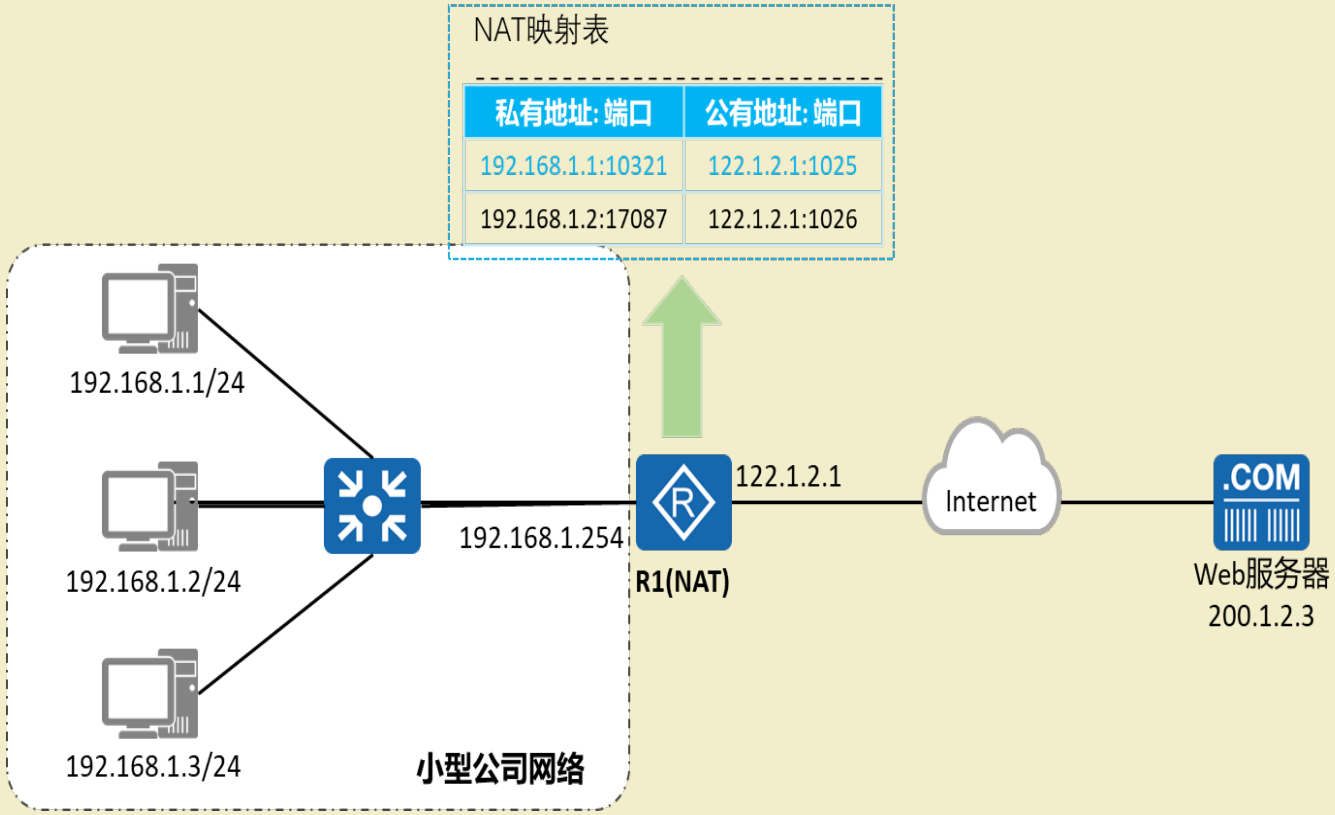
（2）路由器出口 IP 地址如果发生了变化，表中公有 IP 地址也会自动跟着变化；

（3）路由器出口 IP 地址可是手工配置，也可是动态分配。

Easy IP 适用于不具备固定公网 IP 地址的场景，如小型规模局域网。小规模局域网通常部署在小型的网吧或者办公室中，这些地方内部主机不多，出接口可以通过 PPPoE 拨号方式获取一个临时公网 IP 地址。 Easy IP 可以实现内部主机使用这个临时公网 IP 地址访问 Internet 。

三 相关知识

Easy IP 的工作过程与 NAPT 完全一样。下图所示是一个小型公司 Easy IP 的网络拓扑。



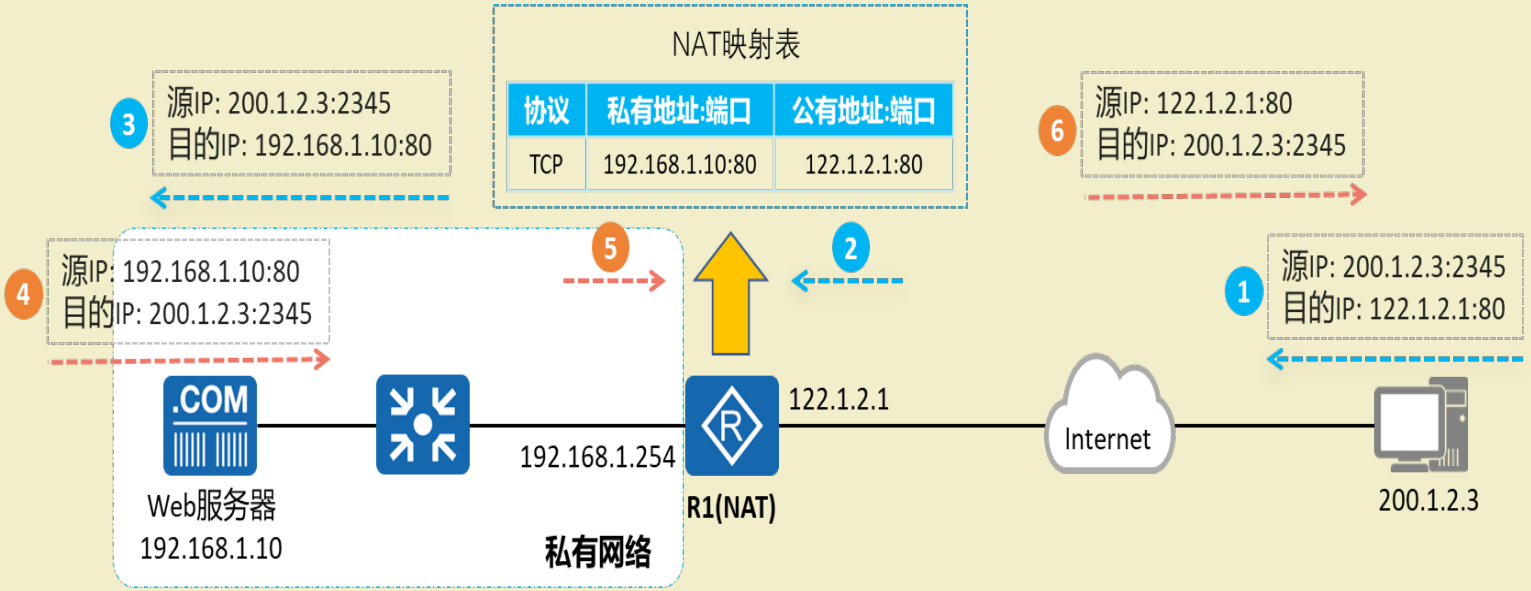
三 相关知识

例【 11.4 】： Easy IP 配置案例，网络拓扑如图 11-5 所示。在 R1 上配置 Easy IP ，让内网所有私有地址转换为 R1 出接口的 IP 访问公网。

```
[R1] acl 2000
[R1-acl-basic-2000] rule 5 permit source 192.168.1.0 0.0.0.255
[R1-acl-basic-2000] quit
[R1] interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1] nat outbound 2000
```

5. NAT Server

NAT Server，又称静态 NAPT。指定“公有地址：端口”与“私有地址：端口”的一对一映射关系，将内网服务器映射到公网，当私有网络中的服务器需要对公网提供服务时使用。外网主机主动访问“公有地址：端口”实现对内网服务器的访问。 NAT Server 的工作过程如图 11-6 所示。



三 相关知识

如图 11-6 所示，假设外网的计算机 A （ 200.1.2.3 ）需要访问私有网络的 Web 服务器（ 192.168.1.10 ），其通信过程如下：

第①步：计算机 A 发送数据包给 Web 服务器。数据包的源 IP 地址为 200.1.2.3 ，源端口号为 2345 （随机端口号）；数据包的目的地址为 122.1.2.1 ，目的端口号为 80 （ Web 服务器默认端口号是 80 ）。

第②步：数据包经过路由器 R1 的时候，路由器查询 NAT 地址映射表，找到对应的映射条目后，数据包的目的地址及目的端口号将从 122.1.2.1:80 转化为 192.168.1.10:80 ，源地址及目的端口号不变。这里转换后的目的 IP 地址为内网 Web 服务器的 IP 地址，目的端口为 Web 服务器的 web 服务端口号 80 。

第③步：转换后的数据包在私有网络上转发，最终被 Web 服务器接收。

第④步： Web 服务器收到数据包后，将响应内容封装在目的地址为 200.1.2.3 ，目的端口号为 2345 的数据包中，然后将数据包发送出去。

第⑤步：响应数据包经过路由转发，将到达路由器 R1 上，路由器对照 NAT 映射表，找出对应关系，将源地址及端口号为 192.168.1.10:80 的数据包转换为源地址及端口号为 122.1.2.1:80 的数据包，然后发送到 Internet 中。

第⑥步：目的地址及端口号为 200.1.2.3:2345 的数据包在 Internet 中传送，最终到达计算机 A 。计算机 A 通过数据包的源地址及端口号（ 122.1.2.1:80 ）知道这是它访问 Web 服务的响应数据包。但是，计算机 A 并不知道 Web 服务其实是由私有网络内的 Web 服务器所提供的，它只知道这个 Web 服务是由 Internet 上的 IP 地址为 122.1.2.1 的机器提供的。

NAT Server 的内外网“ IP+ 端口”映射关系是永久性的，因此，它主要应用在为内网服务器的指定服务（如 Web 、 FTP 等）向外网提供服务的场景。典型的应用为公司将内部网络的门户网站映射到公网 IP 的 80 端口上，满足互联网用户访问公司门户网站需求。

三 相关知识

例【 11.5 】： NAT Server 配置案例，网络拓扑如图 11-6 所示。

在 R1 上配置 NAT Server ，将内网服务器 192.168.1.10 的 80 端口映射到公有地址 122.1.2.1 的 80 端口。

```
[R1] interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1] ip address 122.1.2.1 24
[R1-GigabitEthernet0/0/1] nat server protocol tcp global
122.1.2.1 www inside 192.168.1.10 80
```

四 项目实施及总结

具体实施过程参考实训报告

【项目总结】

本项目详细介绍了不同类型网络地址转换技术的工作原理及应用，主要学习了以下知识内容。

1. 在私有网络内使用私有地址，并在网络出口使用 NAT 技术，可以有效减少网络所需的 IPv4 公有地址数目， NAT 技术有效地缓解了 IPv4 公有地址短缺的问题。

2. 动态 NAT 、 NAPT 、 Easy IP 实现了私有网络的主机访问公网（提供源地址转换），其中 Easy IP 应用在私有网络只有一个公有地址的场景。

3. NAT Server 实现了私有网络的服务器对公网提供服务（提供目的地址转换）。

4. 静态 NAT 提供了一对一映射，支持内外双向互访。

谢谢！