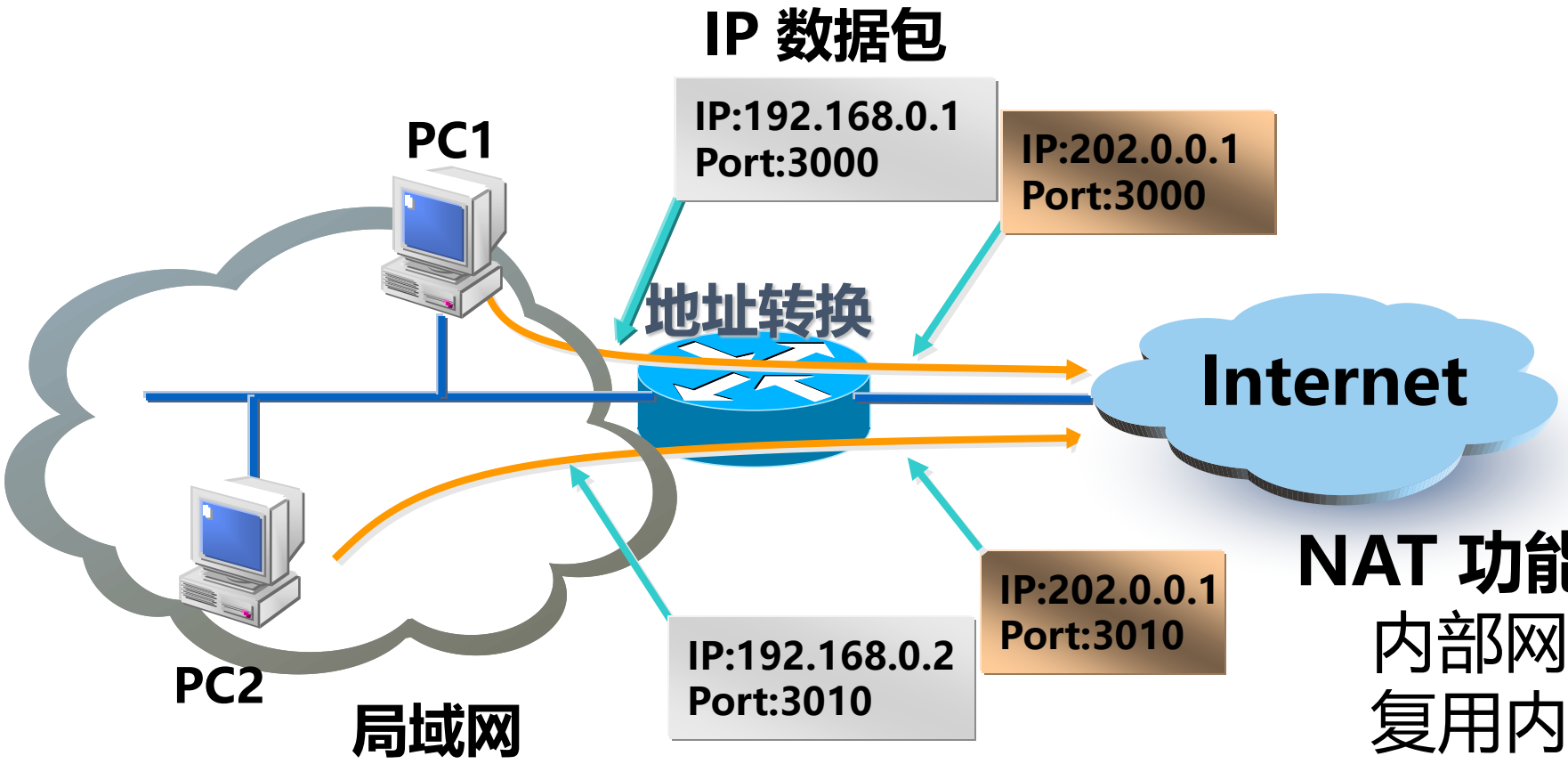
NAT

网络地址转换

NAT(Network Address Translator)

- 合法的IP地址资源日益短缺;
- 一个局域网内部有很多台主机，但不是每台主机都有合法的IP地址，为了使所有内部主机都可以连接因特网，需要使用地址转换;
- 地址转换技术可以有效地隐藏内部局域网中的主机，具有一定的网络安全保护作用;
- 地址转换可以在局域网内部提供给外部FTP、WWW、Telnet等服务;
- NAT的原理：改变IP包头，把内部地址翻译成合法的外部地址;

NAT功能



NAT 功能：

内部网络地址转换

复用内部的全局地址

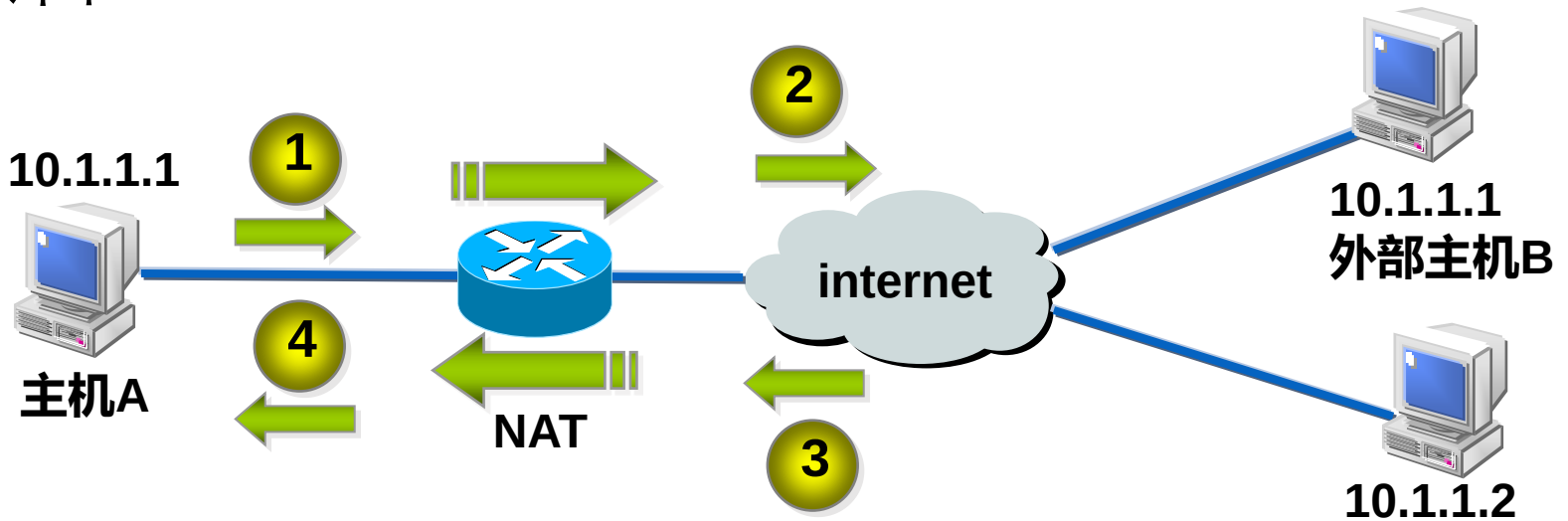
TCP 负载均衡

解决网络地址重叠

NAT术语

- 内部本地地址：私有IP，不能直接用于互连网。
- 内部全局地址：用来代替内部本地IP地址的，对外，或在互联网上是合法的的IP地址。
- 外部全局地址：外部合法地址。在我这个局域网来看，对方的出接口处用来代替内部本地IP地址的。
- 外部本地地址：私有ip地址。在我这个局域网来看，对方的内部局域网的私有IP地址。

NAT术语



主机A发出的包	1
SA=10.1.1.1	DA = 193.3.3.1
内部本地地址	外部本地地址

经过路由器转换的包	2
SA=192.2.2.1	DA=10.1.1.1
内部全局地址	外部全局地址

经过路由器转换的包	4
SA=193.3.3.1	DA=10.1.1.1
外部本地地址	内部本地地址

外部主机B返回的包	3
SA=10.1.1.1	DA=192.2.2.1
外部全局地址	内部全局地址

NAT实现方式

- NAT的3种实现方式：

  静态NAT（static NAT）设置起来最为简单，内部网络中的每个主机都被永久映射成外部网络中的某个合法的地址，多用于服务器。

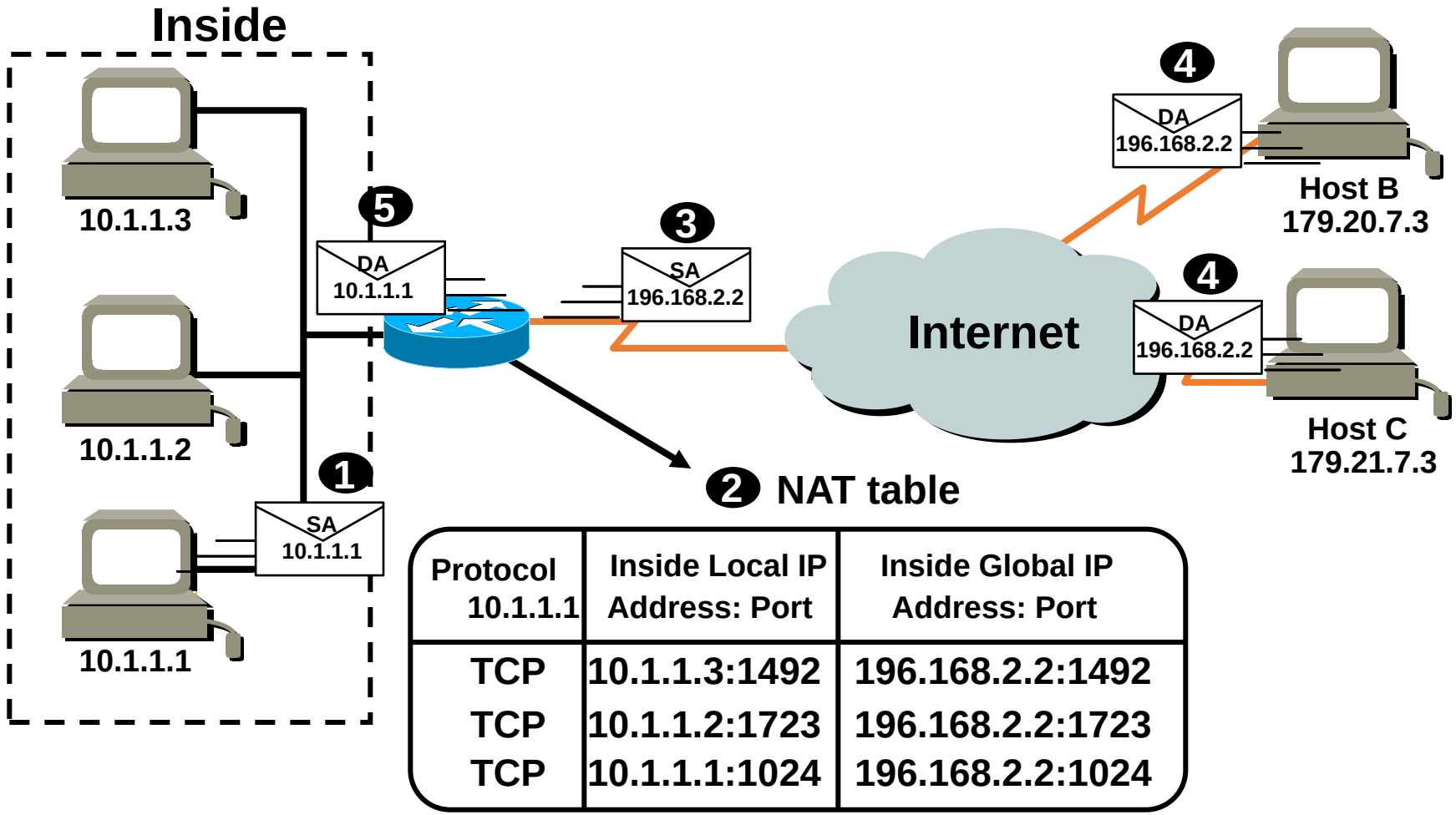
  动态NAT（pooled NAT）则是在外部网络中定义了一系列的合法地址，采用动态分配的方法映射到内部网络,多用于网络中的工作站。

  端口复用NAT（easy-ip）则是把内部地址映射到外部网络的一个端口IP地址上。

复用内部的全局地址

- 将一个内部全局地址用于同时代表多个内部本地地址。
- 主要用IP地址和端口号的组合来唯一区分各个内部主机。
- 目前在公司内普遍应用。（如下图）

复用内部的全局地址

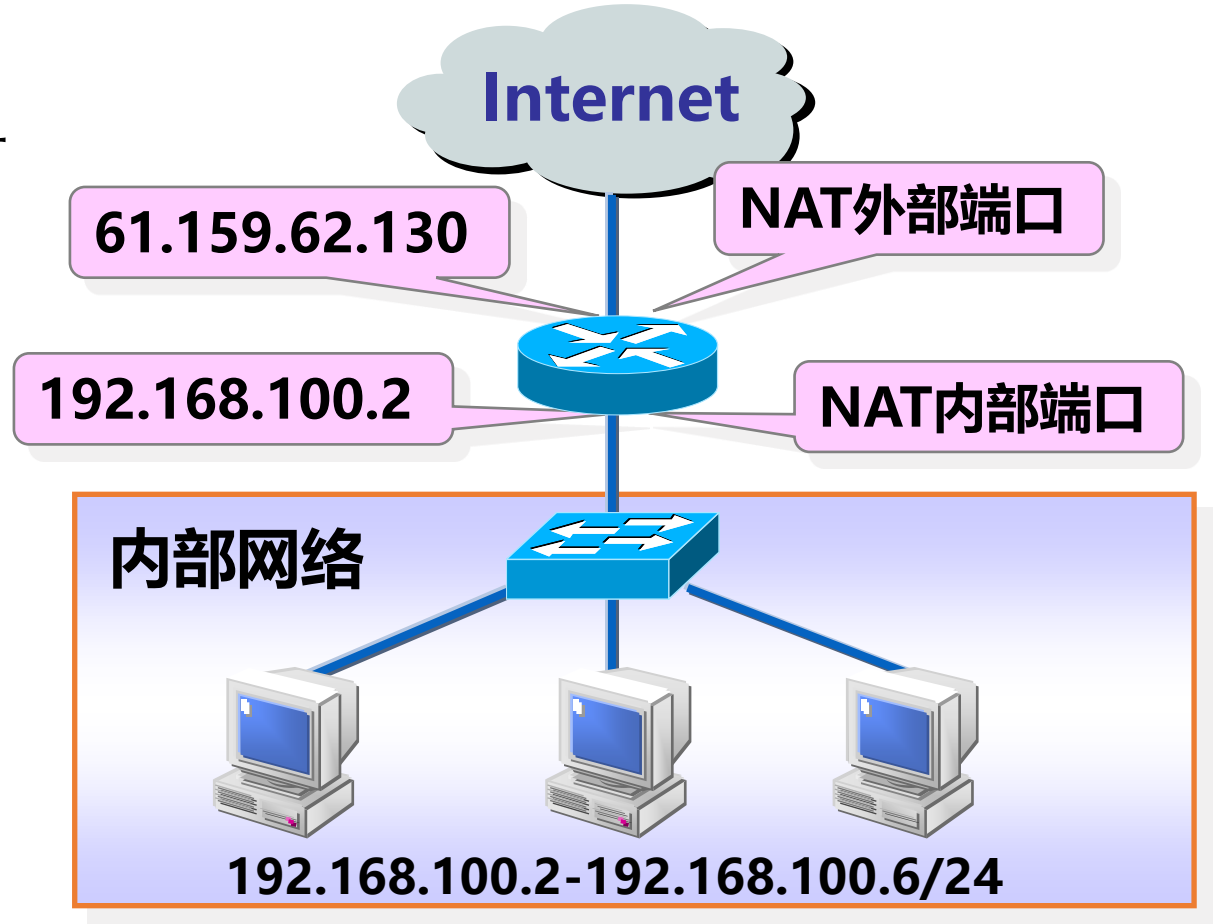


Protocol 10.1.1.1	Inside Local IP Address: Port	Inside Global IP Address: Port
TCP	10.1.1.3:1492	196.168.2.2:1492
TCP	10.1.1.2:1723	196.168.2.2:1723
TCP	10.1.1.1:1024	196.168.2.2:1024

NAT配置步骤

- NAT配置步骤
  1、接口IP地址配置
  2、使用访问控制列表定义哪些内部主机能做NAT
  3、决定采用什么实现方式，静态、动态NAT或easy-ip
  4、指定地址转换映射

静态NAT配置



将内部网络地址192.168.100.2-192.168.100.6

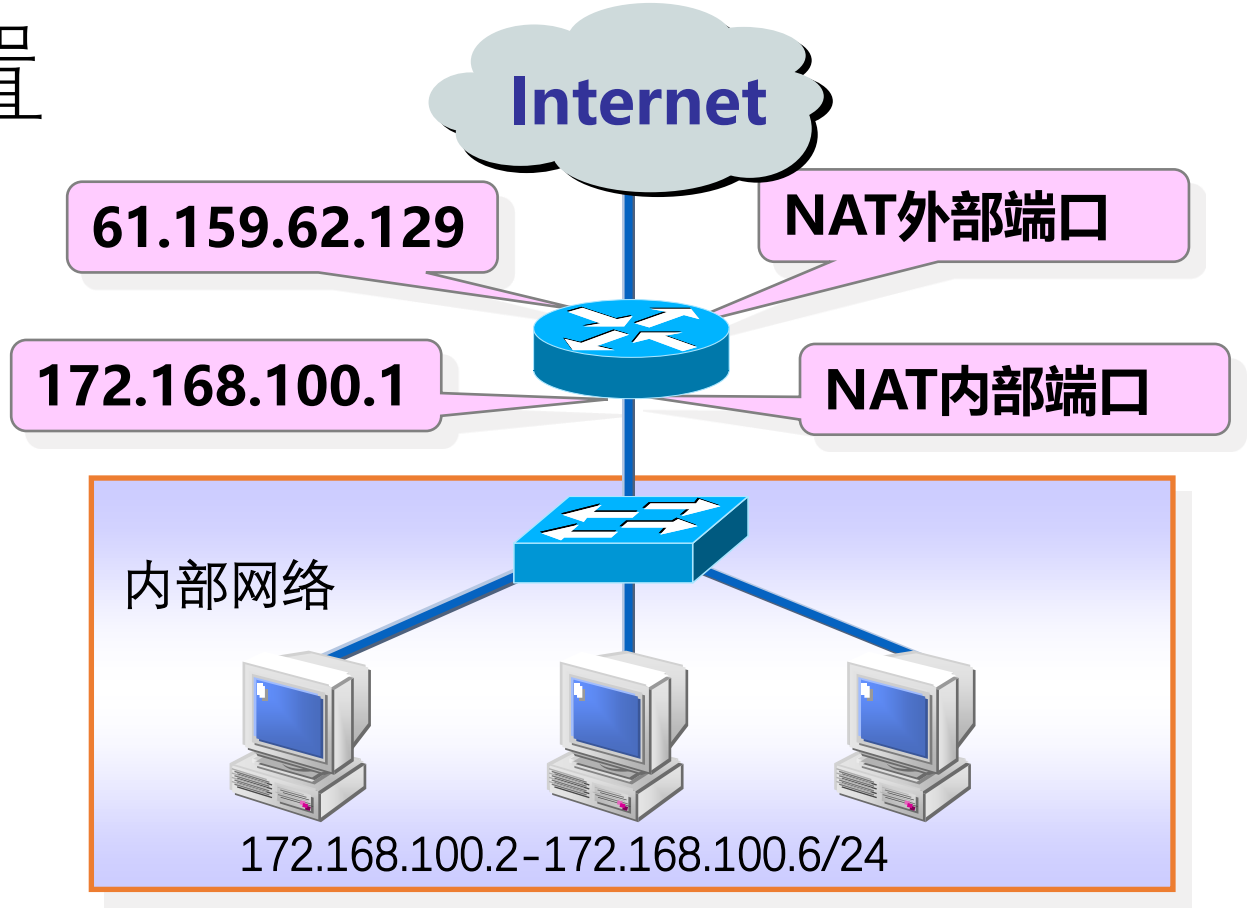
转换为合法的外部地址61.159.62.130-61.159.62.134

静态NAT配置

- 第一步： 设置外部端口IP
  - [Huawei]int g0/0/1
  - [Huawei-GigabitEthernet0/0/1]ip address 100.1.1.1 255.255.255.0
- 第二步： 设置内部端口IP
  - [Huawei]int g0/0/0
  - [Huawei-GigabitEthernet0/0/1]ip address 172.16.1.1 255.255.255.0
- 第三步： 在外部接口上启用静态NAT
  - [Huawei-GigabitEthernet0/0/1]nat static global 100.1.1.10 inside 172.16.1.1（其中公网地址向运营商买）

- 查看：[Huawei]dis nat static

动态NAT配置



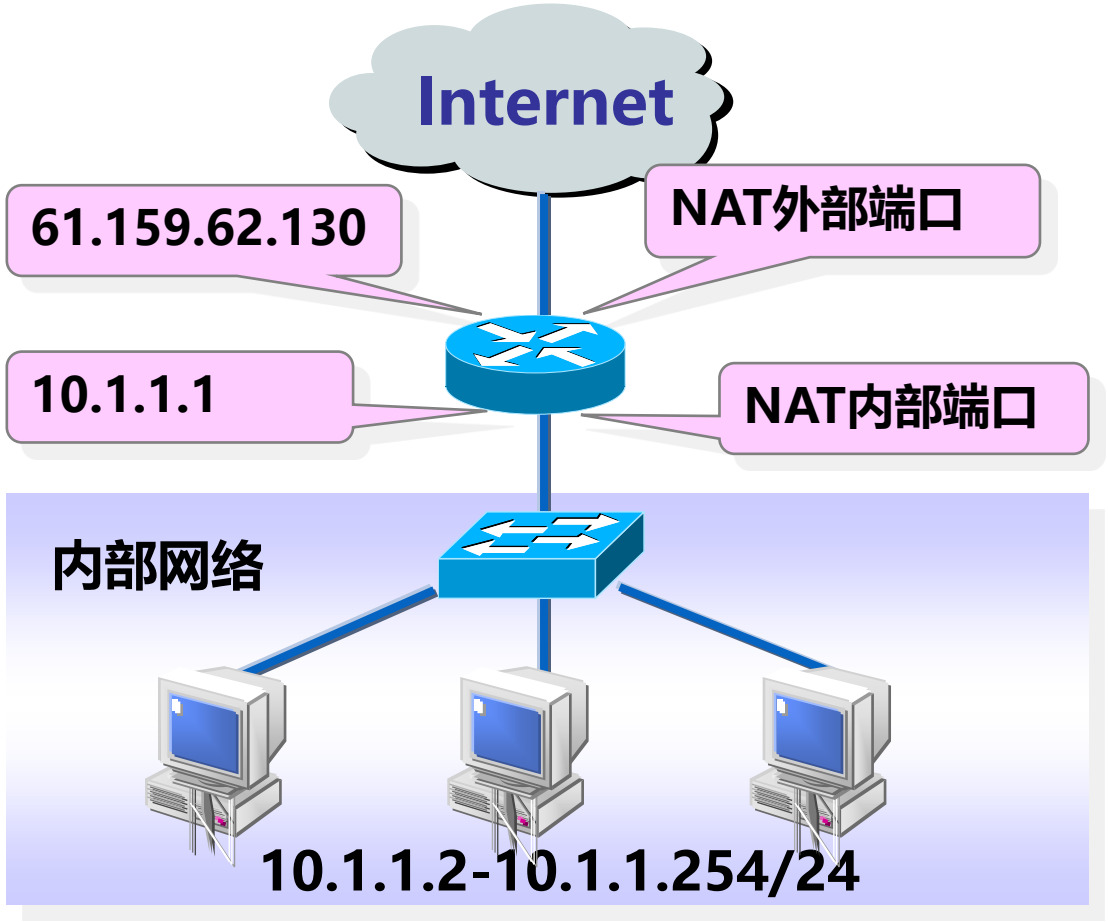
将内部网络地址172.168.100.1-172.168.100.254

转换为合法的外部地址61.159.62.130-61.159.62.190

动态NAT

- 第一步： 设置外部端口IP地址
  - [Huawei]int g0/0/1
  - [Huawei-GigabitEthernet0/0/1]ip address 100.1.1.1255.255.255.0
- 第二步： 设置内部端口IP地址
  - [Huawei]int g0/0/0
  - [Huawei-GigabitEthernet0/0/1]ip address 172.16.1.1255.255.255.0
- 第三步：定义内部网络中允许访问外部的访问控制列表
  - [Huawei]acl 2000
  - [Huawei-acl-basic-2000]rule 5 permit source 172.16.1.0 0.0.0.255
- 第四步：定义转换地址池
  - [Huawei]nat address-group 1 100.1.1.3 100.1.1.10
- 第五步：外部接口上开启动态NAT
  - [Huawei]int g0/0/1
  - [Huawei-GigabitEthernet0/0/1]nat outbound 2000 address-group 1 no-pat

easy-ip-配置



将内部网络地址10.1.1.1-10.1.1.254
转换为合法的外部地址61.159.62.130

easy-ip配置

- 第一步： 设置外部端口IP地址
  - [Huawei]int g0/0/1
  - [Huawei-GigabitEthernet0/0/1]ip address 100.1.1.1255.255.255.0
- 第二步： 设置内部端口IP地址
  - [Huawei]int g0/0/0
  - [Huawei-GigabitEthernet0/0/1]ip address 172.16.1.1255.255.255.0
- 第三步： 定义内部网络中允许访问外部的访问控制列表
  - [Huawei]acl 2000
  - [Huawei-acl-basic-2000]rule 5 permit source 172.16.1.0 0.0.0.255
- 查看：dis nat outbound

NAT服务器配置

- 第一步： 设置外部端口IP地址
  - [Huawei]int g0/0/1
  - [Huawei-GigabitEthernet0/0/1]ip address 100.1.1.1255.255.255.0
- 第二步： 设置内部端口IP地址
  - [Huawei]int g0/0/0
  - [Huawei-GigabitEthernet0/0/1]ip address 172.16.1.1 =255.255.255.0
- 第三步： 定义NAT服务器
  - [Huawei-GigabitEthernet0/0/1]nat server protocol tcp global 100.1.1.10 www inside 172.16.1.1 www

查看NAT

- dis nat outbound
- dis nat address-group 1
- dis nat static

NAT检查与排错

- 常见问题
  - 动态地址池中是否有正确的范围的地址
  - 动态地址池中是否有重复的地址
  - 静态映射的地址与动态地址池中的地址之间是否有重复
  - 访问列表是否指明了要转换的正确地址，是否漏掉一些地址，是否包括了一些不该包括的地址
  - 是否指明了正确的内部和外部接口
  - 不对称路由问题