NAT 及静态转换、动态转换及 PAT

NAT（网络地址转换）

1、作用：通过将内部网络的私有 **IP** 地址翻译成全球唯一的公网 **IP** 地址，使内部网络可以连接到互联网等外部网络上。

2、优点：

节省公有合法 **IP** 地址

处理地址重叠

增强灵活性

安全性

3、**NAT** 的缺点

延迟增大

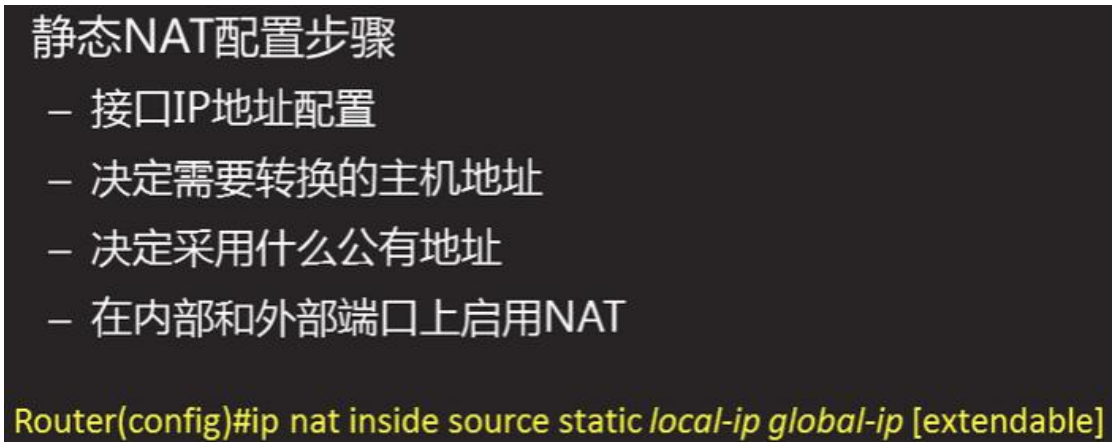
配置和维护的复杂性

不支持某些应用，可以通过静态 **NAT** 映射来避免

4、NAT 实现方式（静态转换、动态转换、端口多路复用）

1）静态转换

IP 地址的对应关系是一对一，而且是不变的，借助静态转换，能实现外部网络对内部网络中某些特设定服务器的访问。



静态 NAT 配置：

配置接口 **IP** 及路由

全局：

Ip nat inside source static 192.168.1.1 61.159.62.131

在内外接口上启用 **NAT**：

进入出口配置：**ip nat outside**

进入入口配置：**ip nat inside**

端口映射：

ip nat inside source static tcp 192.168.1.6 80 61.159.62.133 80

2）动态转换

IP 地址的对应关系是不确定的，而是随机的，所有被授权访问互联网的私有地址可随机转换为任何指定的合法的外部 **IP** 地址。(内部网络同时访问 **Internet**

的主机数少于配置的合法地址中的 **IP** 个数时适用）

动态 NAT 的配置：

全局：**access-list 1 permit 192.168.1.0 0.0.0.255**
(定义将要转换的地址列表**)**
全局：**ip nat pool nsd 61.159.62.131 61.159.62.132 netmask 255.255.255.248**
（定义地址池名称为 **nsd,** 地址池 **IP** 范围 **61.159.62.131** 到 **61.159.62.132**）
全局：**ip nat inside source list 1 pool nsd**
（将列表 **1** 转换为 **pool nsd**）

3）端口多路复用（**PAT**）

通过改变外出数据包的源 **IP** 地址和源端口并进行端口转换，内部网络的所有主机均可共享一个合法 **IP** 地址实现互联网的访问，节约 **IP**。

PAT 的配置：

全局：**ip nat inside source list 1 interface f0/1 overload**

（**f0/1** 外部接口）

- 定义内部访问列表

```
Router(config)#access-list 1 permit 192.168.10 0.0.0.255
```

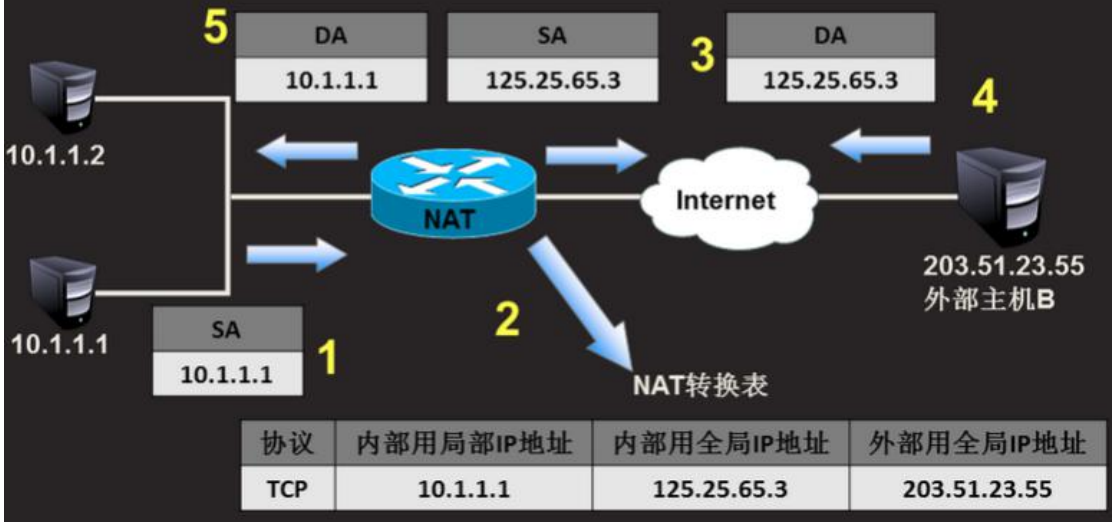
- 定义合法的IP地址池
  - 由于直接使用外部接口地址，所以不再定义IP地址池
- 设置复用动态IP地址转换

外部接口

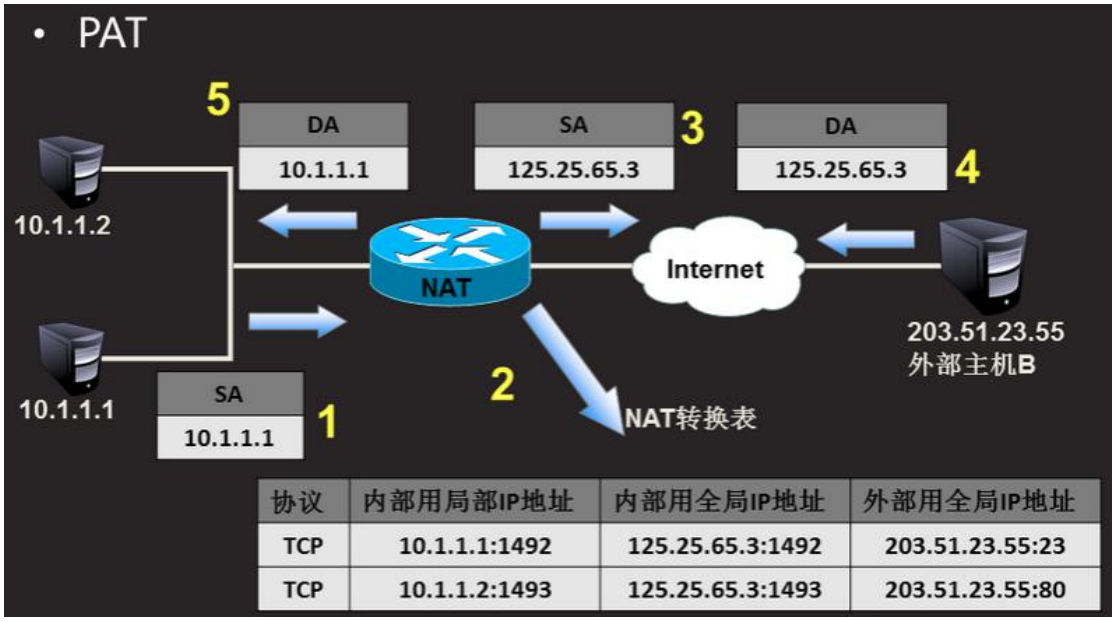
```
Router(config)#ip nat inside source list 1 interface FastEthernet 0/1 overload
```

- 在内部和外部端口上启用NAT，以及配置默认路由
  - 与静态NAT配置相同

- 静态转换和动态转换



协议	内部用局部IP地址	内部用全局IP地址	外部用全局IP地址
TCP	10.1.1.1	125.25.65.3	203.51.23.55



5、NAT 三种实现方式的区别：
静态转换的对应关系一对一且不变，并且没有节约公用 **IP**，只隐藏了主机的真实地址。
动态转换虽然在一定情况下节约了公用 **IP**，但当内部网络同时访问 **Internet** 的主机数大于合法地址池中的 **IP** 数量时就不适用了。
端口多路复用可以使所有内部网络主机共享一个合法的外部 **IP** 地址，从而最大限度地节约 **IP** 地址资源。

查看 NAT 转换条目

特权：**show ip nat translations** 显示当前存在的转换

清除 NAT 转换条目

特权： **clear ip nat translation *** 清除 **NAT** 转换条目中的所有所条目
注：静态 **NAT** 条目不会被清除

NAT 常见问题

ACL 阻止转换后的流量
进行地址转换的 **ACL** 不全
overload 参数漏配
不对称路由问题
动态地址池 **IP** 地址范围配置错误
动态地址池与静态转换地址重叠
Inside 和 **outside** 接口配置错误

显示每个转换的数据包

特权：**debug ip nat**
S 表示源地址
D 表示目的地址

192.168.1.2->61.159.62.130 表 示 将 192.168.1.2 转 换 为 61.159.62.130