20180417 网络地址转换协议NAT功能详解及NAT基础知识介绍

在本专用网内使用的专用地址），但现在又想和因特网上的主机通信（并不需要加密）时，可使用NAT方法。

仅能解决了lP地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。把内网的私有地址，转化成外网的公有地址

装有NAT软件的路由器叫做NAT路由器，它至少有一个有效的外部全球IP地址。这样，所有使用本地地址的主机在和外界通信时，都要在NAT路由器上将其本地地址转换成全球IP地址，才能和因特网连接

宽带分享
安全性： 外界scanport的时候，就扫描不到内部ip

解决IP地址不足的问题
第四层是TCP或UDP的数据包，NAT通过更改源端口号，来实现多对少的映射。
对于ICMP包，NAT通过更改ICMP的ID，来实现多对少的映射。

用NAT来做到负载分担，它的分担方式是基于每次访问的。把这三台服务器的IL映射为同一个IG，这时外部用户访问该IG地址时，NAT会进行基于每次访问的负载分担。用户第一次访问时会定向到Server1，第二次则是Server2，第三次则是Server3，轮循完后又回到Server1，服务器依次轮流对外提供服务

缺点：
1- 并没有建立真正的端对端连接，并且不能参与一些因特网协议。 需要初始化从外部网络建立的TCP连接，和使用无状态协议（比如UDP）的服务将被中断

2- 违反了IP地址结构模型的设计原则。 多对一
3- NAT使得IP协议从面向无连接变成面向连接。NAT必须维护专用IP地址与公用IP地址以及端口号的映射关系。在TCP/IP协议体系中，如果一个路由器出现故障，不会影响到TCP协议的执行。因为只要几秒收不到应答，发送进程就会进入超时重传处理。而当存在NAT时，最初设计的TCP/IP协议过程将发生变化，Internet可能变得非常脆弱。

4- PAT端口地址转换，又叫网络地址端口转换（NAPT）或NAT的端口复用（用IP地址+端口号来对应和区别各个数据流进行网络地址转换，以达到多内部主机通过一个或少量合法IP地址来访问外部网络）

原文： https://zhuanlan.zhihu.com/p/26992935

NAT是什么?

NAT（Network Address Translation，网络地址转换）是1994年提出的。当在专用网内部的一些主机本来已经分配到了本地IP地址（即仅在**本专用网内使用的专用地址**），但现在**又想和因特网上的主机通信（并不需要加密）时，可使用NAT方法。**

这种方法需要在专用网连接到因特网的路由器上安装NAT软件。**装有NAT软件的路由器叫做NAT路由器，它至少有一个有效的外部全球IP地址。这样，所有使用本地地址的主机在和外界通信时，都要在NAT路由器上将其本地地址转换成全球IP地址，才能和因特网连接。**

NAT的功能：

NAT不仅能**解决了IP地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。把内网的私有地址，转化成外网的公有地址**。使得内部网络上的（被设置为私有IP地址的）主机可以访问Internet。

1.**宽带分享**：这是 NAT 主机的最大功能。

2.安全防护：NAT 之内的 PC 联机到 Internet 上面时，他所显示的 IP 是 NAT 主机的公共 IP，所以 Client 端的 PC 当然就具有一定程度的安全了，外界在进行 portscan（端口扫描） 的时候，**就侦测不到源Client 端的 PC 。**

NAT分为哪几种?

NAT可以**分为Basic NAT和PAT**：

- Basic NAT只转化IP，不映射端口。

- PAT除了转化IP，还做端口映射，可以用于多个内部地址映射到少量（甚至一个）外部地址。

NAT还可以分为静态NAT和动态NAT：

- 静态NAT，将内部网络中的每个主机都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，则是在外部网络中定义了一个或多个合法地址，采用动态分配的方法映射到内部网络。

为什么需要有NAT?

NAT的主要作用，是**解决IP地址数量紧缺**。当大量的内部主机只能使用少量的合法的外部地址，就可以使用NAT把内部地址转化成外部地址。

NAT还可以防止外部主机攻击内部主机（或服务器）。

怎样映射?

如何将大量的内部地址，映射成少量的外部地址?

对于**第四层是TCP或UDP的数据包，NAT通过更改源端口号，来实现多对少的映射。**

例如：内部IP1~IP4，4个地址映射成外部一个地址IP5。

(IP1，Port1）映射成（IP5，Port1）

（IP2，Port1）映射成（IP5，Port2）

（IP3，Port2）映射成（IP5，Port3）

（IP4，Port2）映射成（IP5，Port4）

对于ICMP包，NAT通过更改ICMP的ID，来实现多对少的映射。

TCP或UDP的端口，原本是用来做什么的?

端口号是用来连接上层程序的。例如，端口号23，对应了Telnet；端口号80，对应了Http等等。

因此，在本动画中，当R1转化H1发送给Server的TCP包的时候，不能转化目的地端口。Server正是通过端口号23，才知道把收到的TCP交给Telnet处理。

NAT有什么弊端?

在一个具有NAT功能的路由器下的主机**并没有建立真正的端对端连接，并且不能参与一些因特网协议。**一些**需要初始化从外部网络建立的TCP连接，和使用无状态协议（比如UDP）的服务将被中断。**除非NAT路由器作一些具体的努力，**否则送来的数据包将不能到达正确的目的地址。**（一些协议有时可以在应用层网关的辅助下，在参与NAT的主机之间容纳一个NAT的实例，比如FTP。）NAT也会使安全协议变的复杂。

NAT局限性

（1）NAT**违反了IP地址结构模型的设计原则。**IP地址结构模型的基础是每个IP地址均标识了一个网络的连接。Internet的软件设计就是建立在这个前提之上，而NAT使得有很多主机可能在使用相同的地址，如10.0.0.1。

（2）NAT使得IP协议从面向无连接变成面向连接。NAT必须维护专用IP地址与公用IP地址以及端口号的映射关系。在TCP/IP协议体系中，如果一个路由器出现故障，不会影响到TCP协议的执行。因为只要几秒收不到应答，发送进程就会进入超时重传处理。而当存在NAT时，最初设计的TCP/IP协议过程将发生变化，Internet可能变得非常脆弱。

（3）**NAT违反了基本的网络分层结构模型的设计原则。**因为在传统的网络分层结构模型中，**第N层是不能修改第N+1层的报头内容的。NAT破坏了这种各层独立的原则。**

（4）有些应用是将IP地址插入到正文的内容中，例如标准的FTP协议与IP　Phone协议H.323。如果NAT与这一类协议一起工作，**那么NAT协议一定要做适当地修正**。同时，网络的传输层也可能使用TCP与UDP协议之外的其他协议，那么NAT协议必须知道并且做相应的修改。由于NAT的存在，**使得P2P应用实现出现困难**，因为P2P的文件共享与语音共享都是建立在IP协议的基础上的。

（5）NAT同时存在对高层协议和安全性的影响问题。RFC对NAT存在的问题进行了讨论。NAT的反对者认为这种**临时性的缓解IP地址短缺的方案推迟了Ipv6迁移的进程**，而并没有解决深层次的问题，他们认为是不可取的。

名词解释：

NAT网络地址转换（正常数据转发时，IP头部的源和目的地址以及端口号是不会被更改的，而使用了NAT技术后，它**将更改头部内容以达实现隐藏内外部主机真实地址、多台主机共享少量IP访问内外部网络、解决IP地址空间重叠、服务器负载均衡等功能**）

PAT端口地址转换，又叫网络地址端口转换（NAPT）或NAT的端口复用（用IP地址+端口号来对应和区别各个数据流进行网络地址转换，以达到多内部主机通过一个或少量合法IP地址来访问外部网络）

Inside内部

Outside外部

Inside local内部本地地址（内部主机的实际地址，一般为**私有地址**）

Inside global内部全局地址（内部主机经NAT转换后去往外部的地址，是**ISP分配的合法IP地址**）

Outside local外部本地地址（外部主机由NAT设备转换后的地址，一般为私有地址，内部主机访问该外部主机时，认为它是一个内部的主机而非外部主机）

Outside global 外部全局地址（外部主机的真实地址，互联网上的合法IP地址）

NAT超时：

没有使用PAT时则为24小时

使用PAT：

UDP超时值： 5分钟

DNS： 1分钟

TCP： 24小时

NAT的实现示范：

1，ip nat inside source

2，ip nat inside destination

都是内部地址转换，ip nat inside source

即是IL->IG (由内部发起的流量)

ip nat inside destination

即是IG->IL (由外部发起的流量)

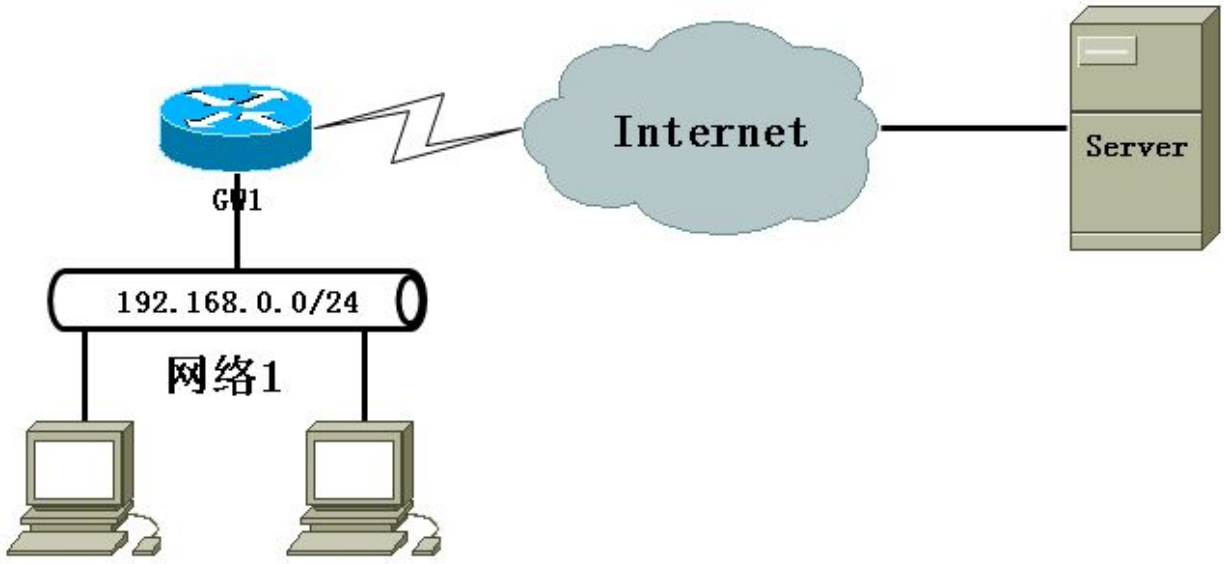
撇开流量的发起方不说，达到的效果是一样的(都是IL与IG之间转换)，即NAT Translation表的IL和IG项都一样。

但是对于ip nat inside destination需要注意：

①只有TCP流量才会转换，ping 流量是不会触发NAT的Destination转换的！

②nat pool 一定要设置type为 rotary！！

ip nat inside source举例



说明: ip nat inside / ip nat ouside -

假定ISP为网络1分配了IG地址段：100.0.0.0/28

配置：

GW1：

GW1(config)#int s0

GW1(config-if)#ip nat outside /定义外部接口

GW1(config-if)#int e0

GW1(config-if)#ip add 192.168.0.1 255.255.255.0

GW1(config-if)#ip nat inside /定义内部接口

GW1(config-if)#exit

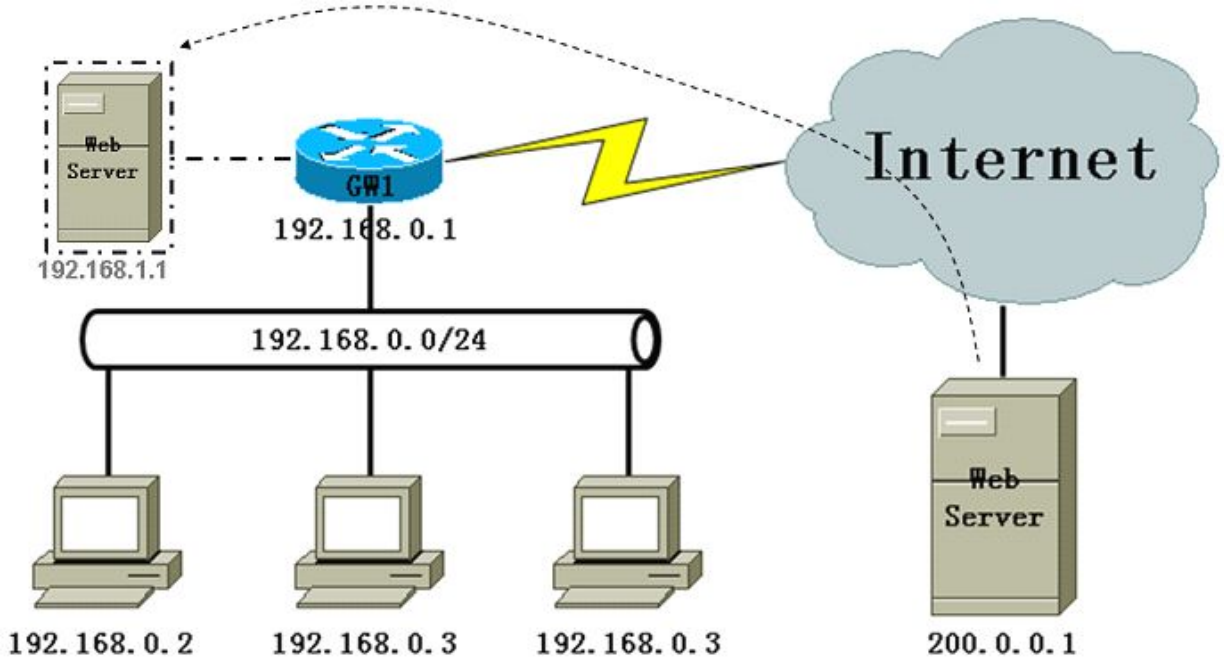
GW1(config)#access-list 1 permit 192.168.0.0 0.0.0.255 /用ACL捕捉IL地址

GW1(config)#ip nat pool POOL_NAME 100.0.0.1 100.0.0.14 prefix-length 28 /定义IG地址池

GW1(config)#ip nat inside source list 1 pool POOL_NAME /将ACL1里指定的IG地址从名为POOL_NAME的地址池里动态顺序地取IG地址进行映射

ip nat inside destination 举例（服务器负载均衡）

当我们内部有几台提供相同服务的服务器时，我们可以**用NAT来做到负载分担，它的分担方式是基于每次访问的**，如下图，如果用NAT做了负载分担，我们**把这三台服务器的IL映射为同一个IG，这时外部用户访问该IG地址时，NAT会进行基于每次访问的负载分担。用户第一次访问时会定向到Server1，第二次则是Server2，第三次则是Server3，轮循完后又回到Server1，服务器依次轮流对外提供服务**。



说明: ip nat inside / ip nat ouside -

配置：

GW1(config)#int s0

GW1(config-if)#ip nat outside /定义外部接口

GW1(config-if)#int e0

GW1(config-if)#ip add 192.168.0.1 255.255.255.0

GW1(config-if)#ip nat inside /定义内部接口

GW1(config-if)#exit

GW1(config)#access-list 1 permit host 100.0.0.1 /定义IG

GW1(config)#ip nat pool POOL1 192.168.0.1 192.168.0.3 prefix-length 24 type rotary

/建立一个IL地址池，范围是服务器所占用的地址范围，类型为rotary是指将在这段地址内轮循
GW1(config)#ip nat inside destination list 1 pool POOL1 /对目的地址为列表内匹配的访问进行地址转换，把目的地址轮流转换成pool指定的地址，要注意的是如果服务器群里有一台或多台甚至是全部服务器不再工作了，路由器是无法辨别的，依旧会将流量进行轮循，不管服务器能否应答。

3，ip nat outside source

/外部地址转换，即是OG->OL，由外部发起的流量，用法为隐藏外部主机真实地址。

ip nat ouside source static (OG) (OL) add-route

/add-route 是为了产生一条去往OL的路由.（查看路由表，多了一条去往OL的路由）

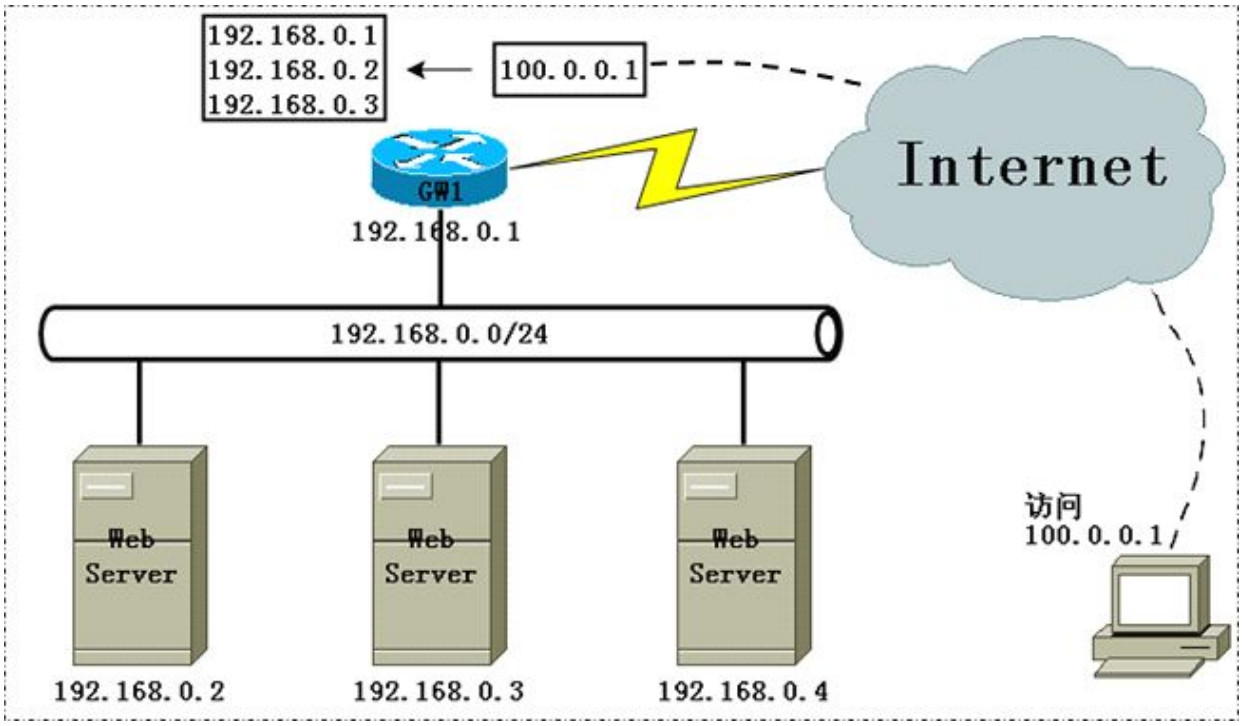
注意:如果ip nat ouside source list (list number) pool (pool name) add-route

虽然能转换OG->OL，但是这样是产生不了一条去往(pool name)的路由，即使(pool name)只有一个地址。结局也是通信不成功的。

所以一般都是这样用ip nat ouside source static (OG) (OL) add-route ，单个地址映射。

ip nat outside source举例（隐藏外部主机真实地址）

如果希望禁止内部主机访问外网的同时让内部主机能访问指定的外部主机，但又不希望让内部主机了解其实自己已经访问了外网时，那么可将需要被访问的外部主机的OG地址转换成为一个内部或者一个虚假的空OL地址，外部主机只用访问这个虚假的OL地址就可以访问到真实的服务器了，达到隐藏真实IP的效果。



说明: ip nat inside / ip nat ouside -

配置:

GW1(config)#int s0

GW1(config-if)#ip nat outside /定义外部接口

GW1(config-if)#int e0

GW1(config-if)#ip add 192.168.0.1 255.255.255.0

GW1(config-if)#ip nat inside /定义内部接口

GW1(config-if)#exit

GW1(config-if)#ip nat outside source static 200.0.0.1 192.168.1.1 add-route

/定义OG转换为OL，后面加一个add-route是为了产生一条去往192.168.1.0的静态路由，否则内部主机去往网关后，网关查表时没有相关路由则丢弃报文。如果有默认路由或者本来就已经有路由了，则可省略该参数，也可以手工配置路由。

4，ip nat outside destination

cisco2691,3640,7200都无此条命令！！

注:①ip nat inside source list n pool POOL_NAME

当list n为标准访问列表---access-list 1 permit a.b.c.d ，数据包的源地址满足listn （a.b.c.d），源地址转换为POOL_NAME地址

当list n为扩展访问列表--- access-list 100 permit tcp A B ，数据包的协议、源地址、目的地址、端口号等都要匹配list n ， 源地址转换为POOL_NAME地址

②ip nat inside destination list n pool POOL_NAME

当list n为标准访问列表---access-list 1 permit a.b.c.d ，数据包的目的地址

满足list n （a.b.c.d）， 目的地址转换为POOL_NAME地址

当list n为扩展访问列表--- access-list 100 permit tcp A B ，数据包的协议、源地址、目的地址、端口号等 都要匹配list n ， 目的地址转换为POOL_NAME地址.