**Lab19\_NAT网络地址转换实验项目**

学生姓名：苏家铭 合作学生：无

实验地点：济世楼330 实验时间：2023年12月13日

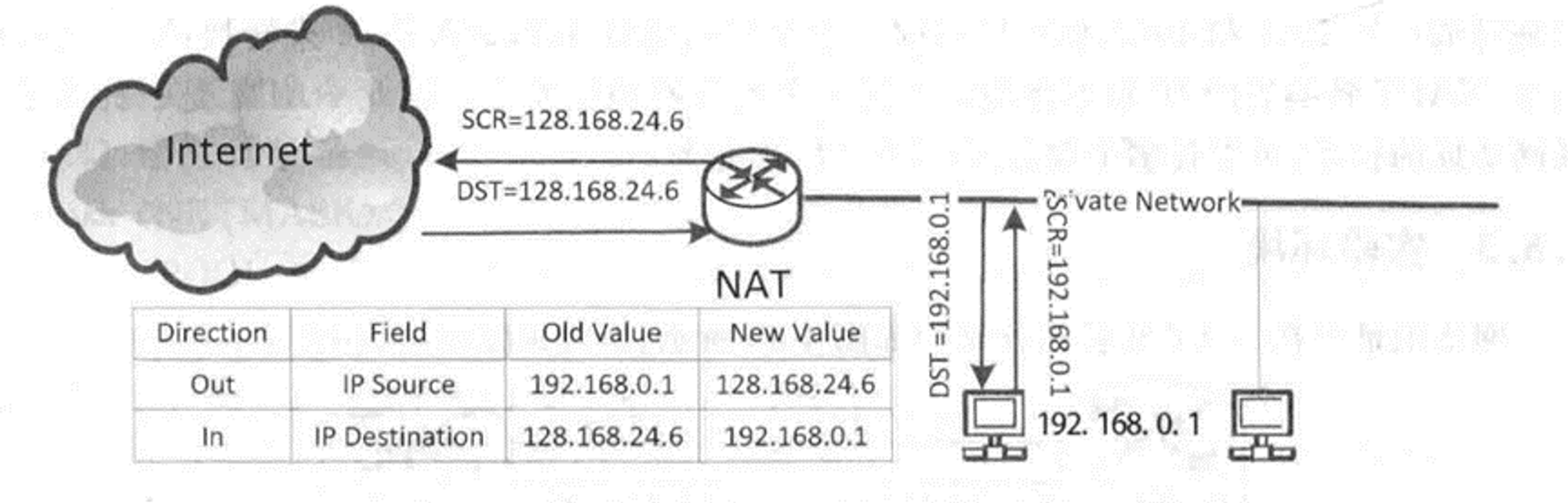
**【实验目的】**

通常情况下，不管穿越多少个IP子网，IP数据包地址始终不改变。网络地址转换（Network Address Translation，NAT），是指实施包过滤机制时，通过对IP数据包地址进行改变而实现不同地址类型转换的一种网络技术。网络地址转换用途广泛，可用于私有网络与互联网互通，家庭接入互联网那个共享等网络应用。本实验利用路由器的NAT功能，结合访问控制列表，实现具有一定安全保护能力的私网与互联网互通。

1. 了解地址转换原理，理解私有网与互联网互通和互联网接入共享原理；
2. 了解NAT技术和NAPT技术。
3. 理解与掌握网络地址转换技术，应用于网络安全。

**【实验原理】**

NAT（Network Address Translation）是一种常见的网络地址转换技术，被广泛应用于不同类型的网络和各种Internet接入方式。



NAT的主要作用是解决IP地址不足的问题。随着互联网的发展，IPv4地址资源变得有限，无法满足日益增长的网络设备需求。NAT通过将私有IP地址转换为公共IP地址，实现了多个内部设备共享一个公共IP地址的功能。这种方式大大提高了IP地址的利用率，减轻了IPv4地址短缺的压力。

除了解决地址不足问题，NAT还具有一定的安全性能。当内部计算机通过NAT路由器连接到Internet时，NAT会将内部计算机的私有IP地址转换为公共IP地址。这样，外部网络无法直接访问内部网络中的计算机，从而隐藏和保护了内部网络的真实IP地址和计算机信息。这种隐蔽性提供了一定程度上的安全保护，可以有效地避免来自网络外部的攻击。

NAT主要分为三种类型：静态NAT、动态NAT和NAT Overload（也称为PAT，Port Address Translation）。静态NAT是将固定的私有IP地址映射为对应的公共IP地址，一对一的映射关系；动态NAT是将内部计算机通过动态方式映射为公共IP地址，使得内部设备可以共享较少数量的公共IP地址；NAT Overload则是最常用的形式，它使用端口号来区分内部设备，实现多个内部设备共享一个公共IP地址。

尽管NAT在解决IP地址不足和提供一定安全性方面具有优势，但也存在一些限制。NAT会引入一定的网络复杂性和延迟，并且在某些特定应用场景下（如IPSec VPN）可能会导致问题。此外，NAT破坏了端到端的连接性原则，对某些应用程序或服务可能会造成不兼容或功能受限。

默认情况下，内部网络使用的私有IP地址是无法直接路由到外部网络的，因为私有IP地址在全球范围内并不唯一，无法在Internet上进行识别和路由。

当内部主机需要与外部网络或Internet进行通信时，数据包到达NAT路由器后，NAT会将数据包头中的源IP地址替换为一个合法的外部网络IP地址，并在NAT转换表中记录这个转换关系。这里的合法外网IP地址是可以被外部网络识别和路由的。

当外部主机对这个转换后的IP地址发送回复时，数据包到达NAT路由器。NAT路由器会查找NAT转换表，找到对应的转换记录，然后将外部IP地址替换为内部网络中的对应私有IP地址，以确保回复可以正确地路由到内部主机。

这种转换过程使得内部网络的设备可以使用私有IP地址进行通信，而无需向外部网络申请大量的公共IP地址。同时，NAT路由器充当了一个网关的角色，保护了内部主机的真实IP地址和网络拓扑信息，提高了网络的安全性。

除了基本的静态 NAT和动态 NAT转换方式，NAT还可以实现端口地址转换（PAT），也称为NAT Overload。PAT通过使用不同的端口号来区分内部网络中的不同设备，使得多个内部设备可以共享一个公共IP地址。这种方式进一步提高了IP地址的利用率。

NAT将网络划分为内部网络和外部网络两部分，内部网络通常是局域网，而外部网络可以是Internet或其他公共网络。当局域网主机通过NAT访问外部网络时，NAT会对数据包进行转换，将局域网内部的本地地址（私有IP地址）转换为全局地址（外部网络或互联网合法的IP地址），然后将转换后的数据包转发到外部网络。

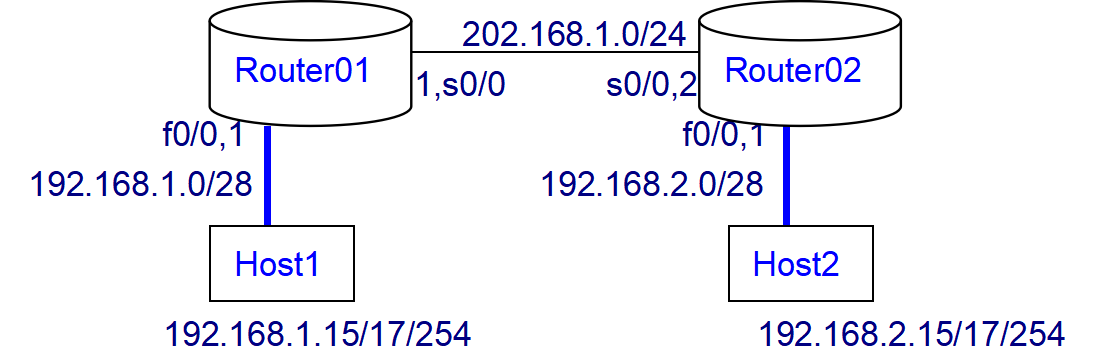
NAT分为两种主要类型：NAT（Network Address Translation）和NAPT（Network Address and Port ranslation）。静态NAT实现内部地址与外部地址的一对一映射，通常在现实中用于服务器等需要直接对外提供服务的设备。动态NAT定义一个地址池，自动进行映射，允许多个内部地址映射到一个外部地址，但是通常用得较少。

NAPT（Network Address and Port Translation）也称为PAT（Port Address Translation）是NAT的一种扩展形式。NAPT使用不同的端口号来映射多个内网IP地址到一个指定的外网IP地址，实现了多对一的映射关系。对于外部网络来说，看起来像是一个设备通过不同的端口与外部进行通信，而实际上是多个内部设备共享一个公共IP地址。

NAT的引入使得企业或家庭网络可以使用私有IP地址，而无需每个设备都申请公共IP地址，从而节省了IP地址资源。同时，NAT也提供了一定程度的网络安全，因为外部网络无法直接访问内部局域网的设备，只能与NAT路由器进行通信，从而隐藏了内部设备的真实IP地址。

然而，NAT也可能引入一些问题。例如，由于NAT在转换过程中需要修改IP头部信息，这会增加一定的处理延迟和复杂性，可能会对某些实时应用或服务的性能产生影响。此外，某些应用程序或协议可能对NAT不兼容，需要采取特殊的技术或配置来解决。

**【实验网络拓扑】**



两台路由器，使用串行线将两个 0 串口对接；两台计算机作为操作平台；一台交换机担当网络连接。

**【实验设备】**

实验环境主要由2台路由器、2台计算机组成

**【实验内容】**

1. 实验概况

构建一个私有网与互联网互通的实验场景。让私网内的某些 IP 地址转换成

互联网地址，从而能接受互联网访问，没有转换的地址就不能接受互联网访问。

路由器 A 以太网端口所连的是私网，将 192.168.1.0/24 视作私网地址;路由器 B以太网端口所连子网和两个路由器的连接子网为互联网，将 192.168.2.0/24 和202.168.1.0/24 视作互联网地址。

1. 配置单向路由。路由器 A 上配置静态路由表，路由器 B 只配端口地址，不配路由表。
2. 路由器 A 上配置访问控制组和地址转换池。设置 192.168.1.16—192.168.1.31 地址段为访问控制组，外出时将转换成互联网地址 202.168.1.4—6，允许该组地址访问 192.168.2.0 网络，其他地址不予转换，从而不允许访问。
3. 转换测试，将 Hostl 网卡地址设置为 192.168.1.15 时，连通 Host2.网卡;将网卡地址设为 192.168.1.17 时，无法连通 Host2 网卡。
4. 主要配置命令
5. 建立地址池:ip nat pool〈POOL\_NAME〉〈IP\_ADDRESS1〉〈IP\_ ADDRESS2〉netmask〈NETMASK〉其中，POOL\_NAME 指 IP 地址池名，IP\_ADDRESS1 指起始 IP 地址，IP\_ADDRESS2 指终止 IP 地址，NETMASK 指地址掩码。

例如， ip nat pool mypool 202.168.1.4 202.168.1.6 netmask 255.255.255.0

1. 设置动态 NAT 转换功能:ip nat inside source list〈No〉 pool 〈POOL\_NAME〉

其中，No 表示访问控制组编号，POOL\_NAME 指 IP 地址池名。

**【实验步骤】**

1. 连接路由器
2. 打开路由器电源
3. 使用 console 线将计算机串口 com1 与路由器 console 口直接相连；
4. 建立 HyperTerminal：开始→程序→附件→通讯→超级终端→名称=router→连接=com1→Baut Rate=9600，8，no parity，1 stop bit；
5. 进入特权模式：router01>en(able)，Enable Secret Password=cisco
6. 内部地址转换
7. 转换方案 192.168.1.16—31→202.168.1.4--6
8. 建立 NAT
9. 建 立 访 问 控 制 组 ： router01(config) # access-list 1 permit 192.168.1.16 0.0.0.15
10. 建立转换地址池 mypool：router01(config) # ip nat pool mypool 202.168.1.4 202.168.1.6 netmask 255.255.255.0
11. 设置动态 NAT 关系：router05(config) # ip nat inside source list 1 pool mypool
12. 端口设置
13. 设置端口：router01 (config) #in s0/0#端口 s0/0
14. 设 置 地 址 ： router01 (config-if) #ip address 202.168.1.1 255.255.255.0
15. 设置转换方向：router01 (config-if) #ip nat outside#出口
16. 设置端口：router01 (config) #in f0/0#端口 f0/0
17. 设 置 地 址 ： router01 (config-if) #ip address 192.168.1.1 255.255.255.0
18. 设置转换方向：router01 (config-if) #ip nat inside#进口
19. 设置单向路由：router01 (config) #ip route 0.0.0.0 0.0.0.0 202.168.1.2
20. 测试
21. 检测：router01# debug ip nat
22. 配置计算机 IP 地址：192.168.1.15
23. 测试连通(从计算机) ：ping 192.168.2.1
24. 配置计算机 IP 地址：192.168.1.17
25. 测试连通(从计算机) ：ping 192.168.2.1
26. 查看转换地址表：router01# sh ip nat translation#动态转换只有才完成时才会显示。

**【分析讨论】**

在工程应用中，NAT（Network Address Translation）展现出了强大的功能，特别是在解决私有网络与外网之间的互联问题方面。一项引人瞩目的特点是将外网地址用作工作地址，这为私有网络的设备提供了一种直接使用互联网地址的方案。在私有网络内，设备可以直接使用互联网地址，而互联网无法直接访问私有网络地址，必须通过地址转换来实现。这种使用外网地址作为工作地址的策略为私有网络与互联网的无缝连接提供了有效的解决方案。

在这个过程中，NAT充当了关键的角色，使得私有网络服务器可以同时为内网和外网提供服务，实现了信息服务的共享。这种灵活性使得私有网络内的资源能够以一种统一的方式向内外提供服务，提高了整体的网络效率和资源利用率。通过NAT，我深刻理解了如何在网络设计中巧妙地处理内外网设备的地址分配问题，使得网络架构更为灵活和可管理。

除了提供方便的内外网互通，NAT还具有重要的安全保障作用。它能够有选择地对私有网络内的主机地址进行转换，使得只有经过授权的地址可以接受外部访问，而未经授权的地址则受到了保护，外部无法直接访问。这种机制为网络安全提供了一定的控制和保护机制，使得私有网络在互联网环境中能够更好地保护内部资源和数据。

通过学习和实践NAT的应用，我对其在私有网络与互联网互联方面的作用有了更加深刻的认识。NAT不仅为私有网络的设备提供了更广阔的互联网资源，同时通过灵活的地址转换和安全保护机制，使得私有网络能够更安全、更高效地与外部网络进行通信。这样的学习经验将在我的网络工程实践中发挥积极的作用。