第七讲 防火墙配置与NAT配置

防火墙配置与NAT配置

- 防火墙技术与访问控制列表介绍
- 访问控制列表与防火墙配置
- NAT技术
- NAT配置

防火墙技术 — 概念

- 防火墙（Firewall）的本义是一种建筑结构，它用来防止大火从建筑物的一部分蔓延到另一部分。

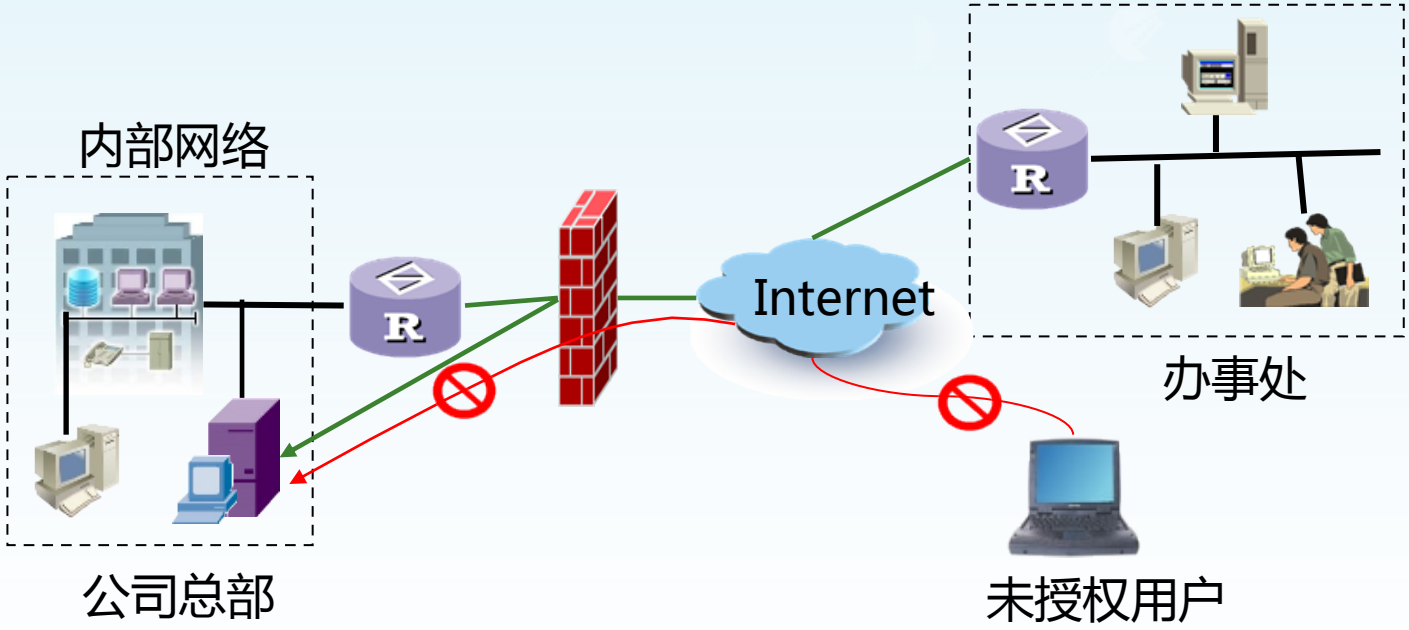
- 在计算机网络中，防火墙是指用于完成下述功能的软件或硬件：
  - 对单个主机或整个计算机网络进行保护，使之能够抵抗来自外部网络的不正当访问。

防火墙技术 — 分类

- 包过滤防火墙（Packet Filter Firewall）：对IP包进行过滤，先获取包头信息，包括IP 层所承载的上层协议的协议号、数据包的源地址、目的地址、源端口和目的端口等，然后和设定的规则进行比较，根据比较的结果决定数据包是否被允许通过。

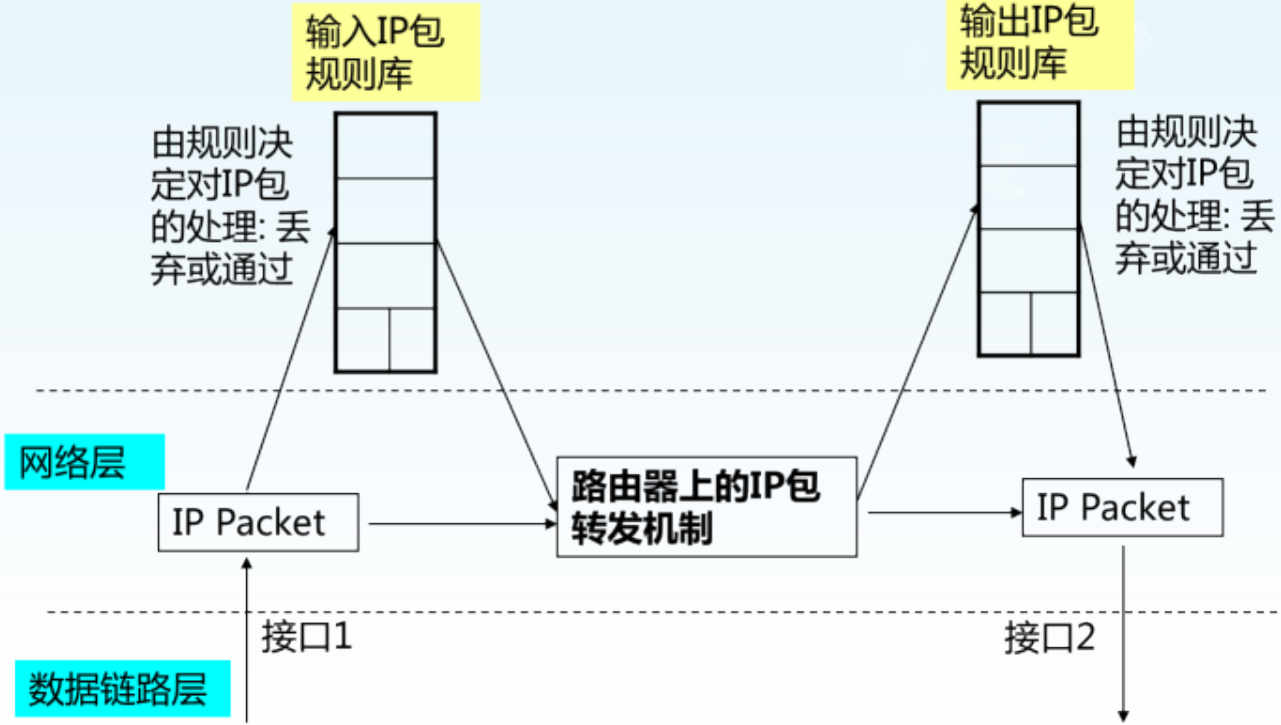
- 应用层报文过滤（Application Specific Packet Filter）：也称为状态防火墙，它维护每一个连接的状态，并且检查应用层协议的数据，以此决定数据包是否被允许通过。

防火墙技术 — 示意图



- 防火墙一般被放置在内部网和Internet之间

防火墙技术 — 路由器实现包过滤防火墙



路由器可以在输入和输出两个方向上对IP包进行过滤

访问控制列表 — 概念

- 访问控制列表（Access Control List, ACL）是实现包过滤规则库的一般方法，它由一系列“permit”或“deny”的规则组成。它是一或多条规则的集合，用于识别报文流。这里的规则是指描述报文匹配条件的判断语句，匹配条件可以是报文的源地址、目的地址、端口号等。网络设备依照这些规则识别出特定的报文，并根据预先设定的策略对其进行处理。

- 除安全之外，访问控制列表还有以下两种应用：
  - QoS（Quality of Service）
  - NAT（Network Address Translation）

访问控制列表 — 常见分类（V5&V7）

ACL类型	编号范围	适用的IP版本	规则制订依据
基本ACL	2000～2999	IPv4	报文的源IPv4地址
		IPv6	报文的源IPv6地址
高级ACL	3000～3999	IPv4	报文的源IPv4地址、目的IPv4地址、报文优先级、IPv4承载的协议类型及特性等三、四层信息
		IPv6	报文的源IPv6地址、目的IPv6地址、报文优先级、IPv6承载的协议类型及特性等三、四层信息
二层ACL	4000～4999	-	报文的源MAC地址、目的MAC地址、802.1p优先级、链路层协议类型等二层信息

ACL本身只能识别报文，而无法对识别出的报文进行处理，对这些报文的具体处理方式由应用ACL的业务模块来决定。

访问控制列表 — 创建ACL（ V5&V7 ）

- [H3C] acl number *acl-number* [match-order { config | auto }]
  - config：匹配规则时按用户的配置顺序。 //缺省值
  - auto：匹配规则时按“深度优先”的顺序。

- 创建ACL后，将进入ACL视图：
  - [H3C-acl-adv-3000]
  - 进入ACL 视图之后，就可以配置ACL的规则了。

访问控制列表 — 创建ACL（模拟器）

高级　基本　二层

- [H3C] acl [advanced | basic | mac] *acl-number* [match-order { config | auto }]
  - config：匹配规则时按用户的配置顺序。
  - auto：匹配规则时按“深度优先”的顺序。
  - 例：[H3C]acl basic 2000 match-order auto

- 创建ACL后，将进入ACL视图：
  - [H3C-acl-ipv4-basic-2000]
  - 进入ACL 视图之后，就可以配置ACL的规则了。

访问控制列表 — Basic ACL

- [H3C-acl-basic-*acl-number*] rule [*rule-id*] { permit | deny } [source *sour-addr sour-wildcard* | any] [time-range *time-name*]
  - *rule-id*：可选参数，规则编号，范围为0～65534。
  - time-range：可选参数，指定访问控制列表的生效时间。
- 举例：

  [H3C-acl-basic-2000] rule permit source *192.168.1.1 0.0.0.0*

访问控制列表 — 反掩码（通配符）

- 反掩码和子网掩码功能相似，但写法不同：
  - 0表示需要比较
  - 1表示忽略比较
- 反掩码和IP地址结合使用，可以描述一个地址范围。

0	0	0	255	只比较前24位
0	0	3	255	只比较前22位
0	255	255	255	只比较前8位

例如：[H3C-acl-basic-2000] rule permit source *192.168.1.0 0.0.0.255*

访问控制列表 — Advanced ACL

- [H3C-acl-adv-*acl-number*] rule [*rule-id*] { permit | deny } *protocol* [source *sour-addr sour-wildcard* | any] [destination *dest-addr dest-wildcard* | any] [source-port *operator port1* [*port2*]] [destination-port *operator port1* [*port2*]] [icmp-type { *icmp-message* | *icmp-type icmp-code*}] [time-range *time-name*]
  - *protocol*: ip, ospf, igmp, gre, icmp, tcp, udp, etc.

Operator的语法	意义
eq	等于端口号 portnumber
gt	大于端口号portnumber
lt	小于端口号portnumber
neq	不等于端口号portnumber
range	介于端口号portnumber1 和portnumber2 之间

访问控制列表 — Advanced ACL（续）

- 配置TCP/UDP协议的高级ACL举例：
  rule deny tcp source *192.168.0.1 0.0.0.0* destination *202.118.66.66 0.0.0.0* destination-port *equal 80*
- 配置ICMP协议的高级ACL ：
  rule { permit | deny } icmp [source *source-addr source-wildcard* | any] [destination *dest-addr dest- wildcard* | any] [icmp-type *icmp-type icmp-code*]
  注：缺省为全部ICMP消息类型
- 配置ICMP协议的高级ACL举例 ：
  rule deny icmp source any destination *210.30.103.0 0.0.0.255* icmp-type *echo*

访问控制列表 — Advanced ACL（续）

- ICMP协议消息类型的助记符 ：

echo	Type=8, Code=0
echo-reply	Type=0, Code=0
host-unreachable	Type=3, Code=1
net-redirect	Type=5, Code=0
net-unreachable	Type=3, Code=0
parameter-problem	Type=12,Code=0
port-unreachable	Type=3, Code=3
protocol-unreachable	Type=3, Code=2
ttl-exceeded	Type=11,Code=0

访问控制列表 — Advanced ACL（续）

- 配置其它协议的高级ACL ：
  rule { permit | deny } *protocol* [source *source-addr source-wildcard* | any] [destination *dest-addr dest-wildcard* | any]

- 配置其它协议的高级ACL 举例：
  rule permit ip source *192.168.1.0 0.0.0.255* destination any

防火墙配置— 启动/禁止（V5&V7）

- 启动防火墙
  - [H3C] firewall enable
- 禁止防火墙
  - [H3C] undo firewall enable
- 缺省情况下，防火墙处于“禁止”状态。（此处对应V5版本，V7版本状态相反）

防火墙配置 — 缺省过滤方式（V5&V7）

- 缺省过滤方式：当访问规则中没有找到一条匹配的规则来判定网络包是否可以通过的时候，将根据缺省过滤方式来决定“允许”还是“禁止”网络包通过。
- 设置缺省过滤方式为“允许”：
  - [H3C] packet-filter default permit
- 设置缺省过滤方式为“禁止”：
  - [H3C] packet-filter default deny
- 系统缺省的报文过滤动作为Permit，即允许未匹配上ACL规则的报文通过。通过本配置可更改报文过滤的缺省动作为Deny，即禁止未匹配上ACL规则的报文通过

防火墙配置 — 在接口上应用ACL（V5&V7）

- 在接口上应用ACL的命令为：
  [H3C-Serial*x/x*] packet-filter { *acl-number* | name *acl-name* } { inbound | outbound }
  - inbound：入方向
  - outbound：出方向

- 在一个接口的一个方向上，可以配置多个ACL（最多32个），匹配时从*acl-number*大的ACL开始

- ACL最基本的应用就是进行报文过滤，即通过将ACL规则应用到指定接口的入或出方向上，从而对该接口收到或发出的报文进行过滤。缺省情况下，接口不对报文进行过滤

防火墙配置 — 显示配置信息（V5&V7）

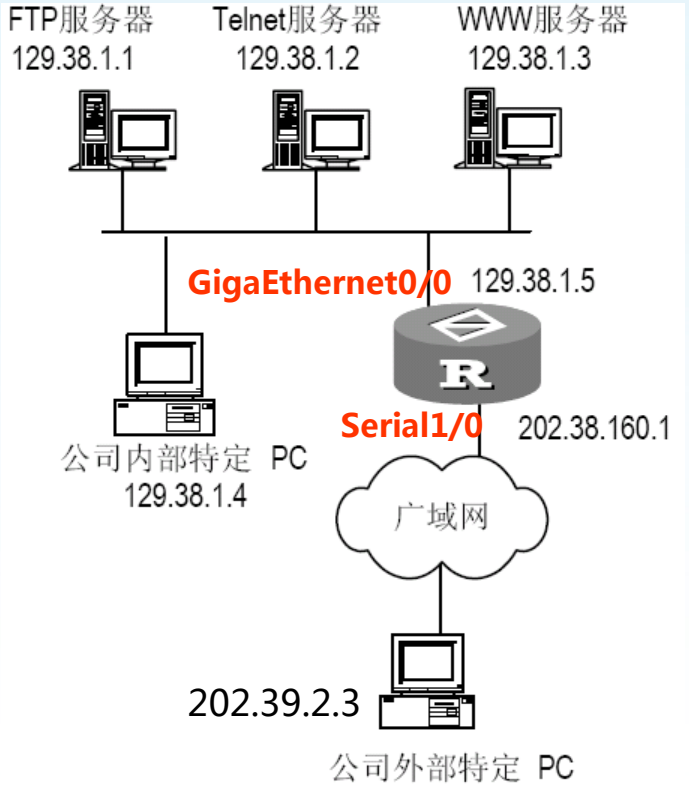
- 显示ACL的配置及运行情况
  [任意视图] display acl { all | *acl-number* }

- 显示ACL在报文过滤中应用的统计信息以及报文过滤缺省动作的统计信息
  [任意视图] display packet-filter { interface interface-type interface-number { inbound | outbound }

- 显示防火墙状态
  [任意视图] display firewall-statistics { all | interface type number }

注意：不同型号的设备操作可能会有差异，具体见相应的配置指导。

防火墙配置 — 举例（V5&V7）



防火墙配置要求：

- 只有外部特定PC可以访问内部服务器
- 只有内部特定PC可以访问外部网络

防火墙配置 — 举例（V5&V7）续

打开防火墙功能。
[H3C] firewall enable//v7不需要这个命令

设置防火墙缺省过滤方式为允许包通过。
[H3C] firewall default permit//v7不需要这个命令

配置G0/0入方向访问规则禁止所有包通过。
[H3C] acl number 3001 match-order auto
[H3C-acl-adv-3001] rule deny ip source any destination any

允许内部特定PC访问外部网，允许内部服务器与外部特定PC通讯。
[H3C-acl-adv-3001] rule permit ip source 129.38.1.4 0 destination any
[H3C-acl-adv-3001] rule permit ip source 129.38.1.1 0 destination 202.39.2.3 0
[H3C-acl-adv-3001] rule permit ip source 129.38.1.2 0 destination 202.39.2.3 0
[H3C-acl-adv-3001] rule permit ip source 129.38.1.3 0 destination 202.39.2.3 0

防火墙配置 — 举例（V5&V7）续

配置Serial1/0入方向访问规则禁止所有包通过。
[H3C] acl number 3002 match-order auto
[H3C-acl-adv-3002] rule deny ip source any destination any

允许外部网与内部特定PC通讯。
[H3C-acl-adv-3002] rule permit ip source any destination 129.38.1.4 0

允许外部特定PC访问内部服务器。
[H3C-acl-adv-3002] rule permit ip source 202.39.2.3 0 destination 129.38.1.1 0
[H3C-acl-adv-3002] rule permit ip source 202.39.2.3 0 destination 129.38.1.2 0
[H3C-acl-adv-3002] rule permit ip source 202.39.2.3 0 destination 129.38.1.3 0

防火墙配置 — 举例（V5&V7）续

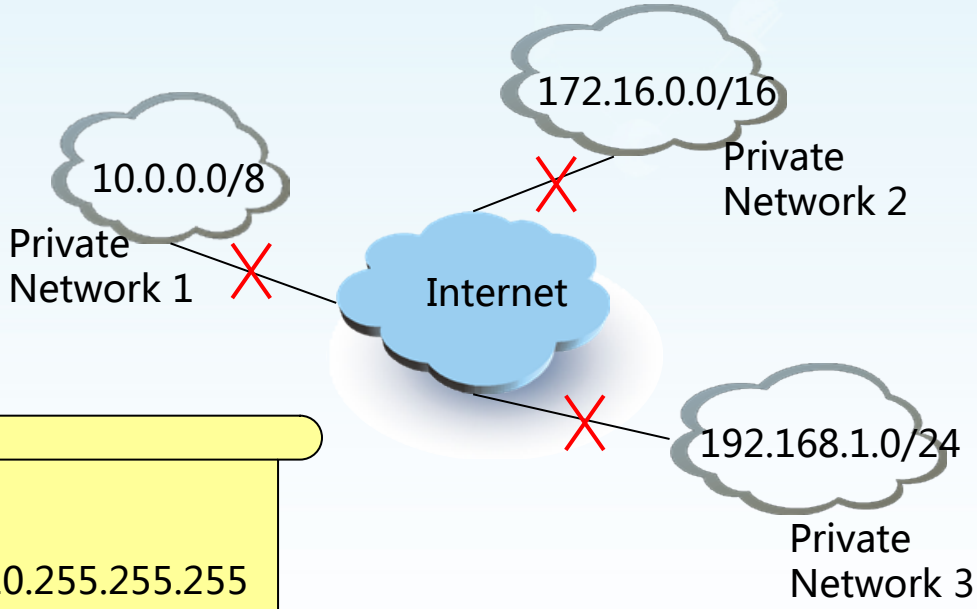
- # 将规则3001 作用于从接口G0/0 进入的包。
  [H3C-GigaEthernet0/0] firewall packet-filter 3001 inbound //v7去掉firewall关键词

- # 将规则3002 作用于从接口Serial1/0 进入的包。
  [H3C-Serial1/0] firewall packet-filter 3002 inbound //v7去掉firewall关键词

NAT技术 — 概述

- NAT (Network Address Translation)是目前用于解决IP地址紧缺问题的主要技术。
- NAT的标准文档是RFC 2663，1999年和RFC 3022，2001年（obsolete RFC 1631，1994年）.
- NAT是在路由器上实现的，它的主要操作是在私网IP地址和公网IP地址之间作相互转换。
- 通过这种转换，一个网络能够在其内部使用私网IP地址，而在外部使用一个或少数几个公网IP地址连接到Internet上。

NAT技术 — 私网IP地址

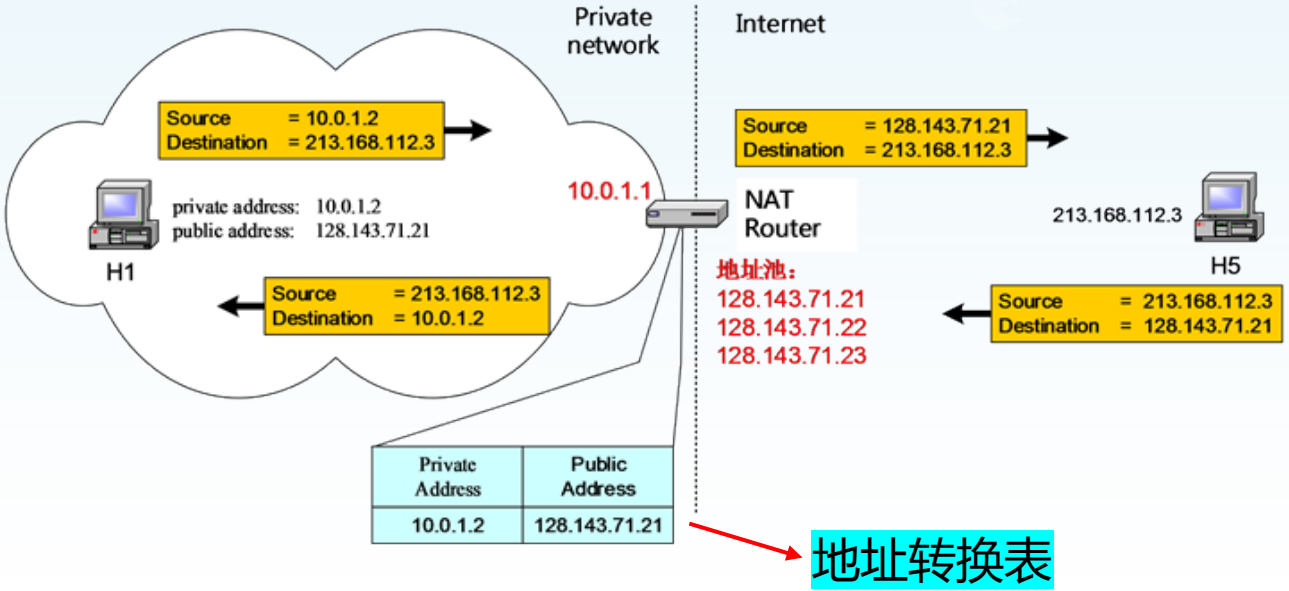


私网IP地址范围：

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

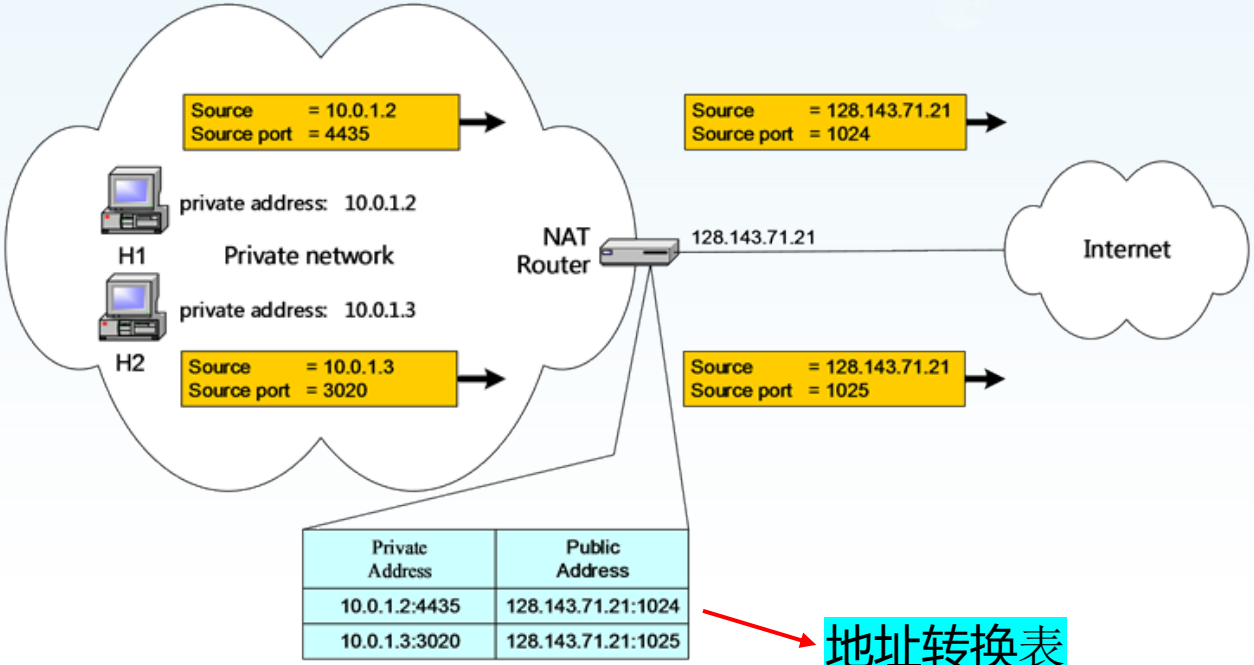
NAT技术 — 基本思想

- 每个NAT路由器都维护一张地址转换表。

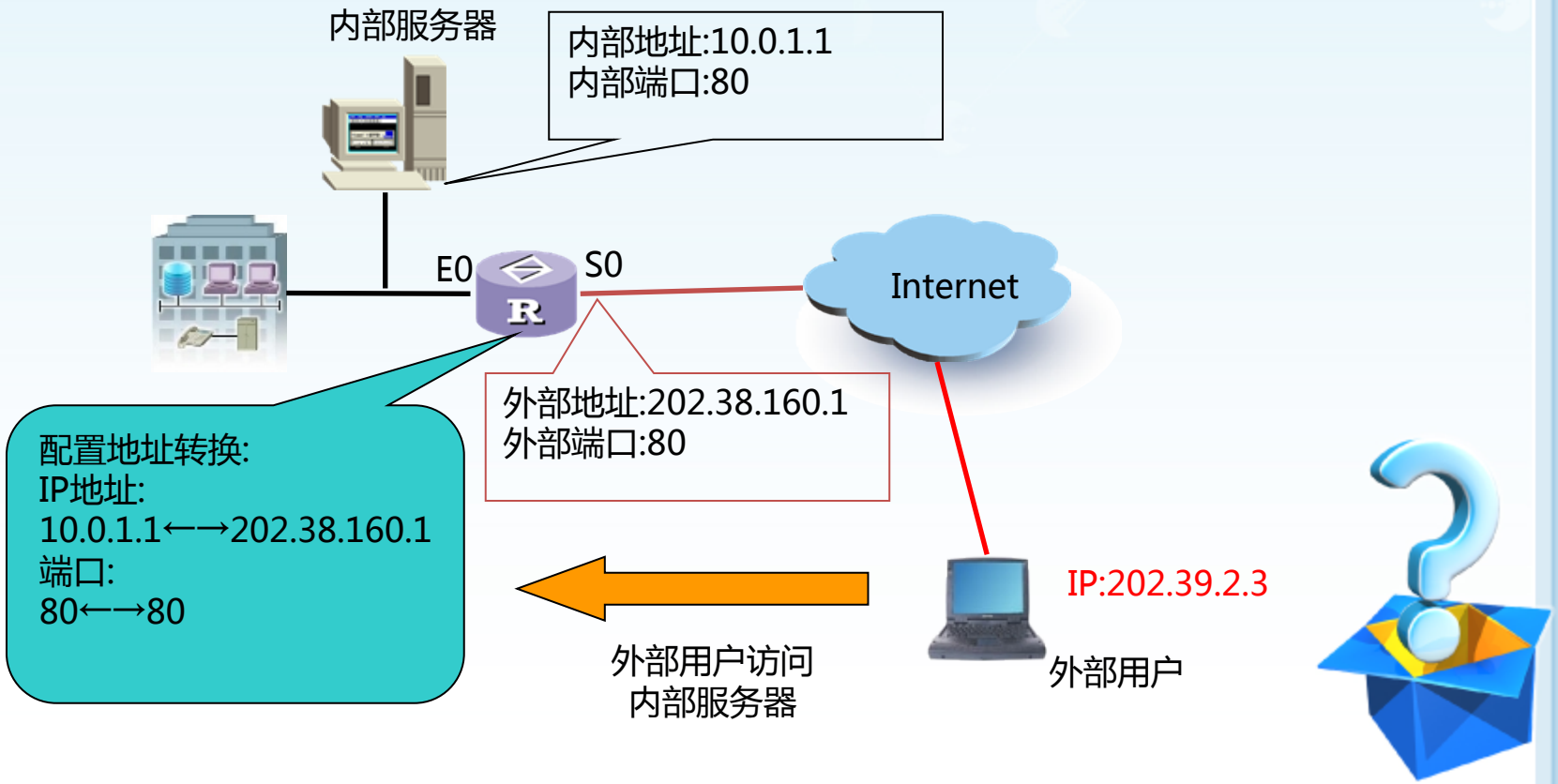


NAT技术 — 基本思想（NAPT）

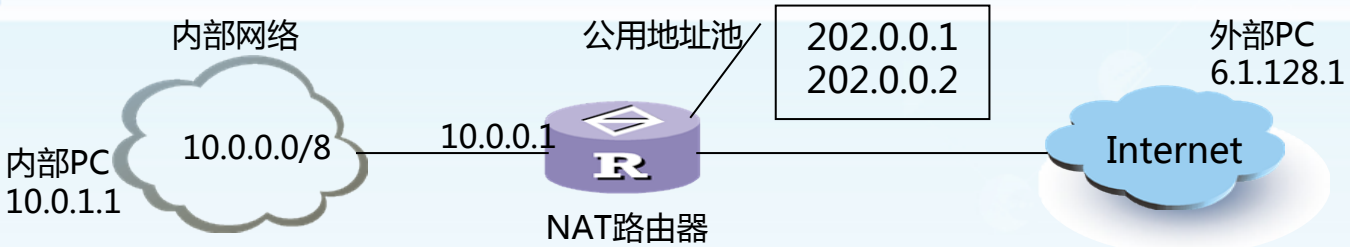
- NAT的最常见形式 -- NAPT (Network Address Port Translation):



NAT技术 — 基本思想（内部服务器）



NAT技术 — 私网访问公网具体步骤



私网地址	私网端口	公网地址	公网端口
10.0.1.1	1001	202.0.0.1	1044

1 dstIP:6.1.128.1, srcIP:10.0.1.1
dstPort:21, srcPort:1001 →

增加地址转换表项，更改源IP和端口

2

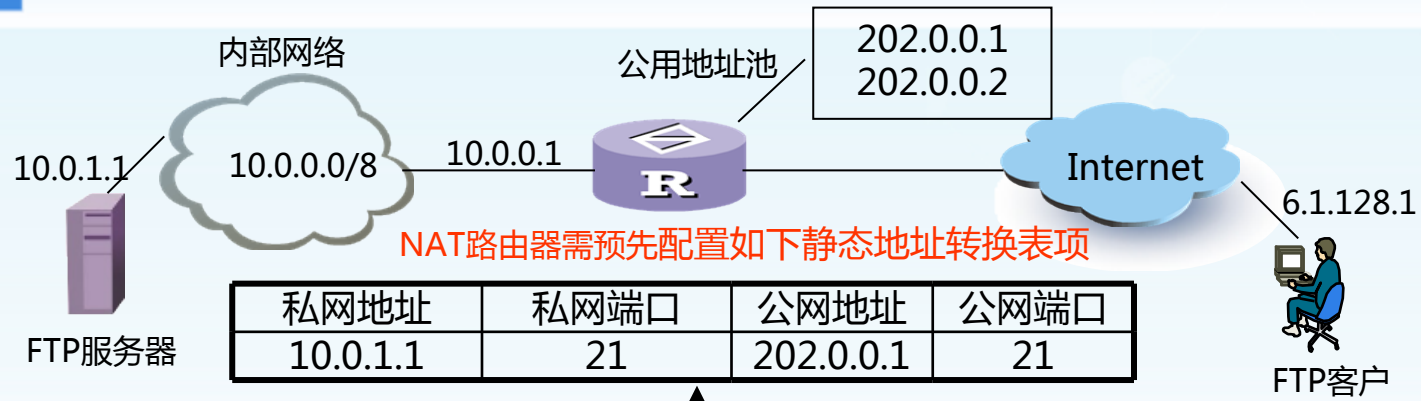
3 → dstIP:6.1.128.1, srcIP:202.0.0.1
dstPort:21, srcPort:1044

4 ← dstIP:202.0.0.1, srcIP:6.1.128.1
dstPort:1044, srcPort:21

5 查找地址转换表，更改目的IP和端口

6 ← dstIP:10.0.1.1, srcIP:6.1.128.1
dstPort:1001, srcPort:21

NAT技术 — 公网访问内部服务器具体步骤



NAT路由器需预先配置如下静态地址转换表项

私网地址	私网端口	公网地址	公网端口
10.0.1.1	21	202.0.0.1	21

1 dstIP:202.0.0.1, srcIP:6.1.128.1
dstPort:21, srcPort:1044

2 查找地址转换表，
更改目的IP和端口

3 dstIP:10.0.1.1, srcIP:6.1.128.1
dstPort:21, srcPort:1044

4 dstIP:6.1.128.1, srcIP:10.0.1.1
dstPort:1044, srcPort:21

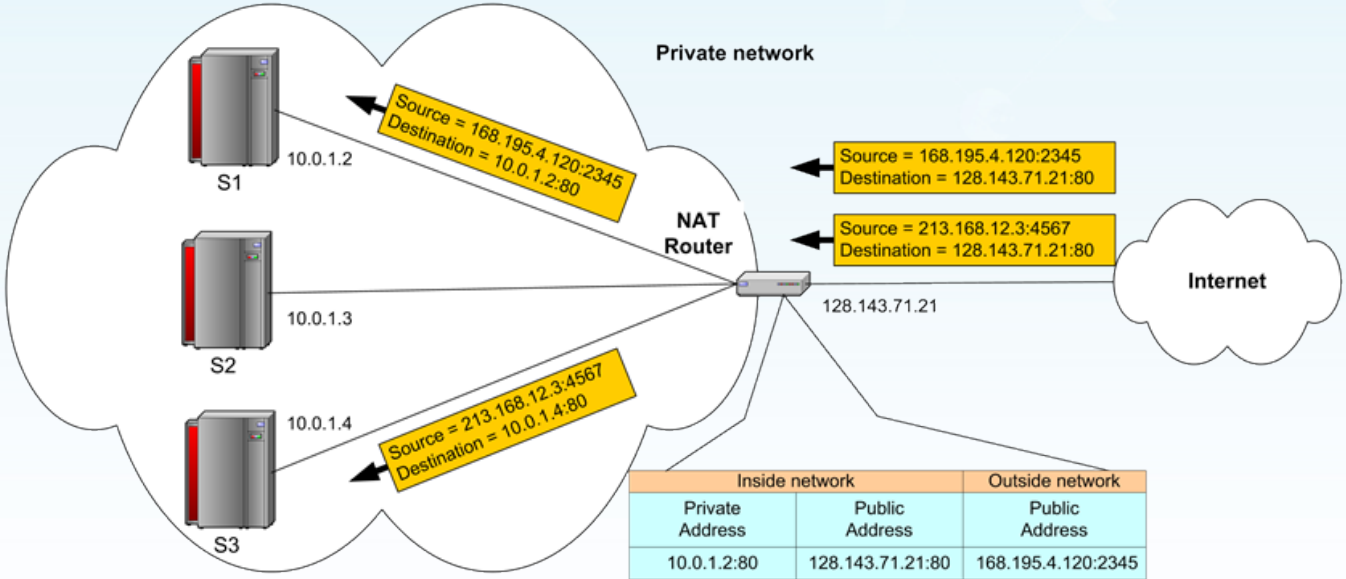
5 查找地址转换表，
更改源IP和端口

6 dstIP:6.1.128.1, srcIP:202.0.0.1
dstPort:1044, srcPort:21

NAT技术 — 其它用途

- 使易于更换ISP
- IP伪装 (IP Masquerading)
- 服务器前端 (Front End)，在多个服务器之间分配负载

NAT技术 — 服务器前端



Inside network		Outside network
Private Address	Public Address	Public Address
10.0.1.2:80	128.143.71.21:80	168.195.4.120:2345
10.0.1.4:80	128.143.71.21:80	213.168.12.3:4567

地址转换表

NAT技术 — 批评

- 开销增加
  - NAT: 重新计算IP Header Checksum
  - NAPT: 重新计算TCP/UDP Header Checksum
- 违反了协议分层的原则。
- 使在应用层的数据中携带有IP地址或端口号的协议不能正常运行。

欲知有关NAT各方面影响的详细讨论，请参见RFC 2993.

NAT配置（V5）— 定义地址池

- 地址池是一些连续的IP 地址的集合，当内部IP包通过地址转换到达外部网络时，将会选择地址池中的某个地址作为转换后的源地址
- 定义地址池命令：
  - [H3C] nat address-group *group-number start-addr end-addr*
- 举例：
  - [H3C] nat address-group *1 210.30.101.1 210.30.101.4*

NAT配置（V5）— 定义地址池与ACL的关联

- 当内部网络有数据包要发往外部网络时，首先根据该ACL判定是否是允许的数据包，然后再根据定义的关联找到与之对应的地址池，最后再把源地址转换成这个地址池中的某一个地址
- 定义关联命令：
  - [H3C-Serial*x/x*] nat outbound *acl-number* address-group *group-number*

- 举例：
  - [H3C] acl number 2000 match-order auto
  - [H3C-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
  - [H3C-acl-basic-2000] rule deny source any
  - [H3C] nat address-group *1 210.30.101.1 210.30.101.4*
  - [H3C-Serial1/0] nat outbound *2000* address-group *1*

NAT配置（V5）— 定义接口与ACL的关联

- 接口与ACL的关联又称EASY IP 特性，它是指在地址转换的过程中直接使用接口的IP 地址作为转换后的源地址
- 定义关联命令：
  - [H3C -Serial*x/x*] nat outbound *acl-number*

- 举例：
  - [H3C] acl 2000 match-order auto
  - [H3C -acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
  - [H3C -acl-basic-2000] rule deny source any
  - [H3C -Serial1/0] nat outbound *2000*

NAT配置（V5）— 建立内部服务器映射

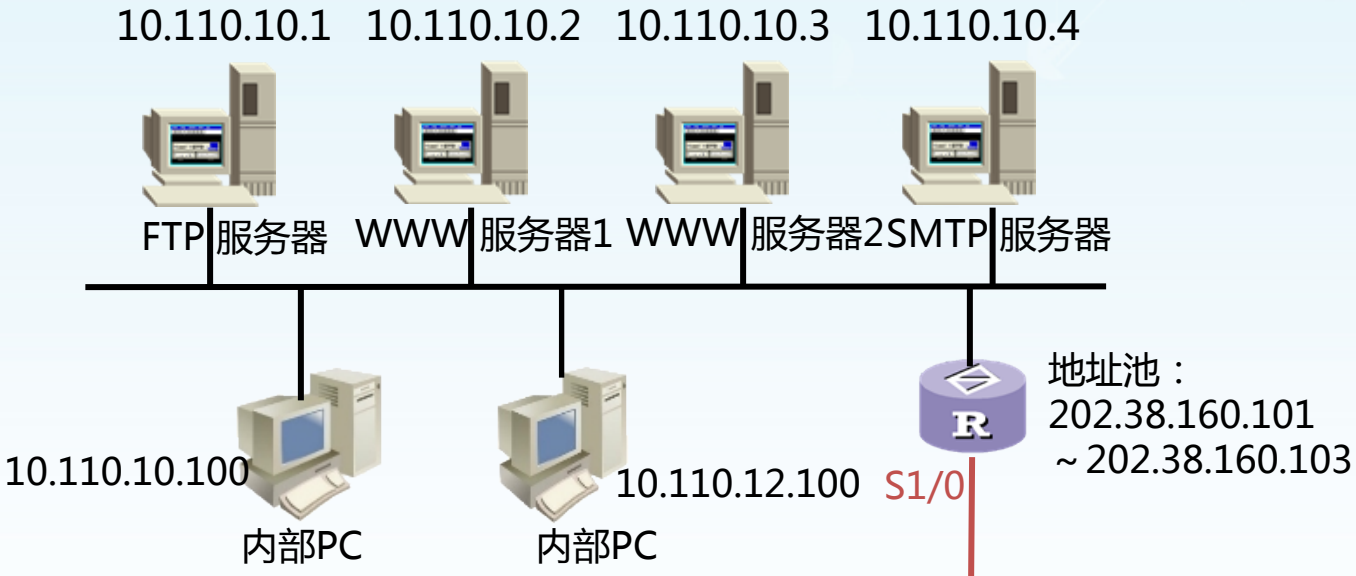
- 用户可将内部服务器的IP地址和端口号映射到NAT路由器的外部地址以及端口号上，从而实现由外部网络访问内部服务器的功能。
- 建立映射命令：
  - [H3C-Serial*x/x*] nat server protocol { protocol-number | ip | icmp | tcp | udp } global *global-addr* { *global-port* | any | domain | ftp | pop3 | smtp | telnet | www } inside *inside-addr* { *inside-port* | any | domain | ftp | pop3 | smtp | telnet | www }
- 举例：
  - [H3C-Serial1/0] nat server protocol tcp global 210.30.103.22 8080 inside 192.168.1.4 www

NAT配置（V5）— 配置信息显示

- 查看地址转换的配置信息：
  - [任意视图] display nat { address-group | all | outbound | server | statistics }

- 查看当前生效的配制NAT的命令：
  - [任意视图] display current-configuration

NAT配置（V5）— 举例



网络地址转换配置要求：

- 内部10.110.10.0/24 网段的PC 机可访问Internet，其它网段的PC 机不能访问Internet。
- 外部PC 机可以访问内部的服务器。

NAT配置（V5）— 举例（续）

```
# 配置地址池和ACL
[H3C] nat address-group  1  202.38.160.101 202.38.160.103
[H3C] acl 2000 match-order auto
[H3C -acl-basic-2000]rule permit source 10.110.10.0 0.0.0.255
[H3C -acl-basic-2000]rule deny source 10.110.0.0 0.0.255.255

# 允许10.110.10.0/24 的网段进行地址转换
[H3C –Serial1/0] nat outbound 2000 address-group 1
# 设置内部FTP 服务器
[H3C –S1/0] nat server protocol  tcp global 202.38.160.101 ftp inside 10.110.10.1 ftp
# 设置内部WWW服务器1
[H3C –S1/0] nat server protocol  tcp global 202.38.160.102 www inside 10.110.10.2 www
# 设置内部WWW服务器2
[H3C –S1/0] nat server protocol  tcp global 202.38.160.102 8080 inside 10.110.10.3 www
# 设置内部SMTP 服务器
[H3C –S1/0] nat server protocol  tcp global 202.38.160.103 smtp inside 10.110.10.4 smtp
```

NAT技术（V7）— 定义地址池

- 地址池是一些连续的IP 地址的集合，当内部IP包通过地址转换到达外部网络时，将会选择地址池中的某个地址作为转换后的源地址
- 定义地址池命令：
  - [H3C] nat address-group *group-number*
- [H3C-address-group-*group-number*] address *start-address end-address*
- 举例：
  - [H3C] nat address-group *1*
  - [H3C-address-group-1] address *210.30.101.1 210.30.101.4*

NAT技术（V7）— 定义地址池与ACL的关联

- ACL在NAT中的作用是 “描述将被做地址转换的IP包” 。
- 当内部网络有数据包要发往外部网络时，首先根据该ACL判定是否是允许的数据包，然后再根据定义的关联找到与之对应的地址池，最后再把源地址转换成这个地址池中的某一个地址
- 定义关联命令：
  - [H3C-Serial*x/x*] nat outbound [*acl-number*] [address-group *group-number*]
  - 举例：
  - [H3C] acl number 2000 match-order auto
  - [H3C-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
  - [H3C-acl-basic-2000] rule deny source any
  - [H3C] nat address-group *1*
  - [H3C-address-group-1] address *210.30.101.1 210.30.101.4*
  - [H3C-Serial1/0] nat outbound *2000* address-group *1*

NAT技术（V7）— 定义接口与ACL的关联

- 接口与ACL的关联又称EASY IP 特性，它是指在地址转换的过程中直接使用接口的IP 地址作为转换后的源地址
- 定义关联命令：
  - [H3C-Serial*x/x*] nat outbound *acl-number*
- 举例：
  - [H3C] acl number 2000 match-order auto
  - [H3C-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
  - [H3C-acl-basic-2000] rule deny source any
  - [Quidway-Serial1/0] nat outbound *2000*

NAT配置（V7）— 建立内部服务器映射

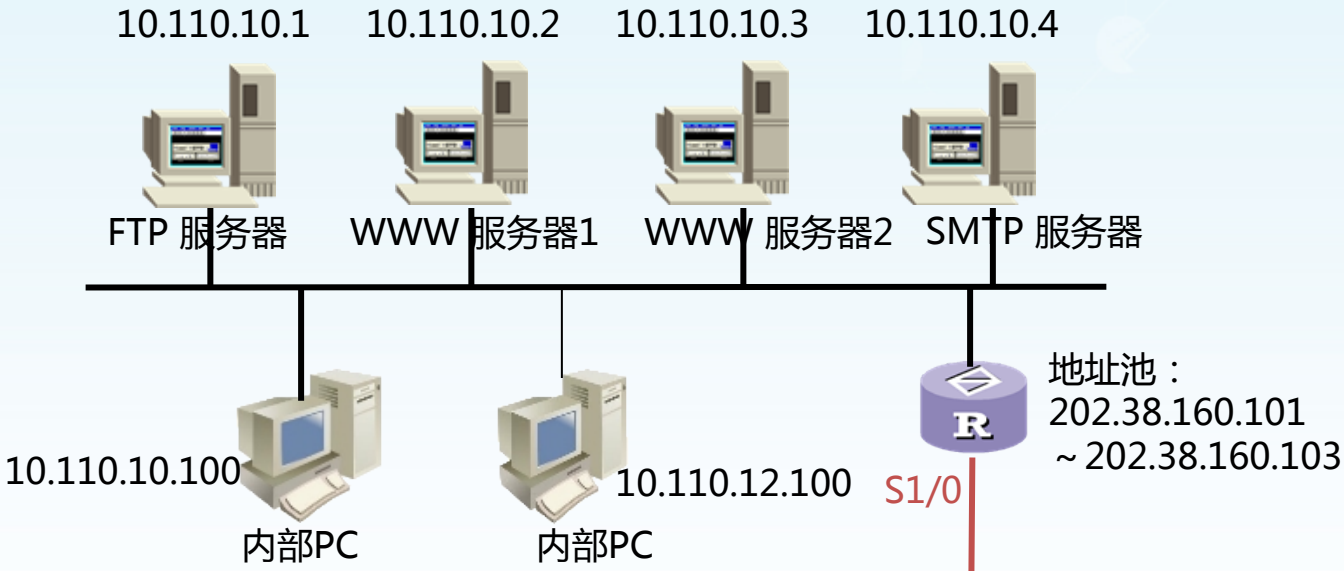
- 用户可将内部服务器的IP地址和端口号映射到NAT路由器的外部地址以及端口号上，从而实现由外部网络访问内部服务器的功能。
- 建立映射命令：
  - [H3C-Serial*x/x*] nat server **protocol** *pro-type* **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* }
    [*global-port*] [**vpn-instance** *global-name*] **inside** *local-address* [*local-port*] [**vpn-instance** *local-name*] [**acl** *acl-number*]

  举例：
  - [H3C-Serial1/0] nat server protocol tcp global 210.30.103.22 8080 inside 192.168.1.4 http

NAT配置（V7）— 配置信息显示

- 查看地址转换的配置信息：
  - [任意视图] display nat { address-group | all | outbound | server | statistics }
- 查看当前生效的配制NAT的命令：
  - [任意视图] display current-configuration

NAT配置（V7）— 举例



网络地址转换配置要求：

- 内部10.110.10.0/24 网段的PC 机可访问Internet，其它网段的PC 机不能访问Internet。
- 外部PC 机可以访问内部的服务器。

NAT配置（V7）— 举例（续）

```
# 配置地址池和ACL
[H3C] nat address-group  1
[H3C-address-group-1]address 202.38.160.101 202.38.160.103
[H3C] acl number 2000 match-order auto
[H3C-acl-basic-2000]rule permit source 10.110.10.0 0.0.0.255
[H3C-acl-basic-2000]rule deny source 10.110.0.0 0.0.255.255

# 允许10.110.10.0/24 的网段进行地址转换
[H3C -Serial1/0] nat outbound 2000 address-group 1
```

NAT配置— 举例V7（续）

设置内部FTP 服务器
[H3C -S1/0] nat server protocol tcp global 202.38.160.101 ftp inside 10.110.10.1 ftp

设置内部WWW服务器1
[H3C -S1/0] nat server protocol tcp global 202.38.160.102 80 inside 10.110.10.2 80

设置内部WWW服务器2
[H3C -S1/0] nat server protocol tcp global 202.38.160.102 8080 inside 10.110.10.3 80

设置内部SMTP 服务器
[H3C-S1/0] nat server protocol tcp global 202.38.160.103 smtp inside 10.110.10.4 smtp

附录 — display current-configuration

[任意视图] **display current-configuration**
#
sysname Quidway
#
local-user *sws* service-type ppp password simple *123456*
#
interface Ethernet0/0
 description Don't change the configuration
please
 ip address 10.110.98.137 255.255.255.0
#
interface Serial0/0
 link-protocol ppp
 ip address 100.110.1.1 255.255.255.0
 ppp authentication-mode pap
#
acl 2000 match-order auto
 rule permit source 192.168.1.0 0.0.0.255；
 rule deny source any

列出所有视图，以及在该视图下生效的命令；
列出rule的顺序即为匹配rule的顺序

附录 — Windows7如何安装IIS（互联网信息服务）

点击“Windows”键进入“开始”菜单，在应用菜单里点击“Windows系统”里的“控制面板”。在控制面板对话框里点击“程序”，在“程序”对话框里点击“启用或关闭Windows功能”，在“Windows功能”对话框里选中“Internet 信息服务”，选中功能就行了。并点击“确定”按钮，Windows功能开始下载并安装你要的功能的程序，直到出现“Windows已完成请求的更改”。在IE地址里输入localhost,能打开，就代表安装成功了。

附录 — Win7远程桌面连接怎么设置

右键Win7系统桌面上的“计算机”,然后选择“属性”，点击系统设置窗口左侧导航上的“远程设置”，点击进入系统属性对话框，将远程桌面下第二项的“允许运行任意版本远程桌面的计算机连接（L）”的选项勾选中，这样本台电脑的远程桌面就允许远程连接到计算机了。(也可以点击“远程桌面用户”窗口下面的添加，进行添加远程连接用户，在选择用户窗口里添加你想要的用户，添加成功的用户才有权限远程访问你的电脑)。

另：右键Win7系统桌面上的“计算机”,然后选择“管理”，进入“本地用户和组”，左键点击“用户”，左键双击选中administrator用户，将账户已禁用取消即可（如账户原来没有禁用则忽略此步骤）。右键单击administrator,设置密码为admin（与实验报告册对应）。