

第 6 篇 配置安全的分支网络

第 27 章 用访问控制列表实现包过滤

第 28 章 网络地址转换

第27章 用访问控制列表实现包过滤

要增强网络安全性，网络设备需要具备控制某些访问或某些数据的能力。ACL 包过滤就是一种被广泛使用的网络安全技术。它使用 ACL（Access Control List，访问控制列表）来实现数据识别，并决定是转发还是丢弃这些数据包。ACL 通过一系列的匹配条件对报文进行分类，这些条件可以是报文的源地址、目的地址、端口号等信息。

另外，由 ACL 定义的报文匹配规则，可以被其它需要对流进行区分的场合引用，如 QoS 的数据分类、NAT 转换源地址匹配等。

27.1 本章目标

课程目标

学习完本课程，您应该能够：

- 了解ACL定义及应用
- 掌握ACL包过滤工作原理
- 掌握ACL的分类及应用
- 掌握ACL包过滤的配置
- 掌握ACL包过滤的配置应用注意事项



27.2 ACL概述

ACL概述



● **ACL (Access Control List, 访问控制列表)** 是用来实现数据包识别功能的

● **ACL可以应用于诸多方面**

- 包过滤防火墙功能
- NAT (Network Address Translation, 网络地址转换)
- QoS (Quality of Service, 服务质量) 的数据分类
- 路由策略和过滤
- 按需拨号

www.h3c.com

ACL (Access Control List, 访问控制列表) 是用来实现数据识别功能的。为了实现数据识别, 网络设备需要配置一系列的匹配条件对报文进行分类, 这些条件可以是报文的源地址、目的地址、端口号、协议类型等。

需要用到访问控制列表的应用有很多, 主要包括:

- **包过滤 (packet-filter) 功能:** 配置基于访问控制列表的包过滤, 可以在保证合法用户的报文通过的同时拒绝非法用户的访问。比如, 要实现只允许财务部的员工访问服务器而其他部门的员工不能访问, 可以通过包过滤\丢弃其他部门访问服务器的数据包来实现;
- **NAT (Network Address Translation, 网络地址转换):** 公网地址的短缺使 NAT 的应用需求旺盛, 而通过设置访问控制列表可以来规定哪些数据包需要进行地址转换。比如, 通过设置 ACL 只允许属于 192.168.1.0/24 网段的用户通过 NAT 转换访问 Internet;
- **QoS (Quality of Service, 服务质量) 的数据分类:** QoS 是指网络转发数据报文的品质保障。新业务的不断涌现对 IP 网络的服务品质提出了更高的要求, 用户已不再满足于简单地将报文送达目的地, 而是希望得到更好的服务, 诸如为用户提供专用带宽、减少报文的丢失率等。QoS 可以通过 ACL 可以实现数据分类, 并进一步对不同类别的数据提供有差别的服务。比如, 通过设置 ACL 来识别语音数据包并对其设置

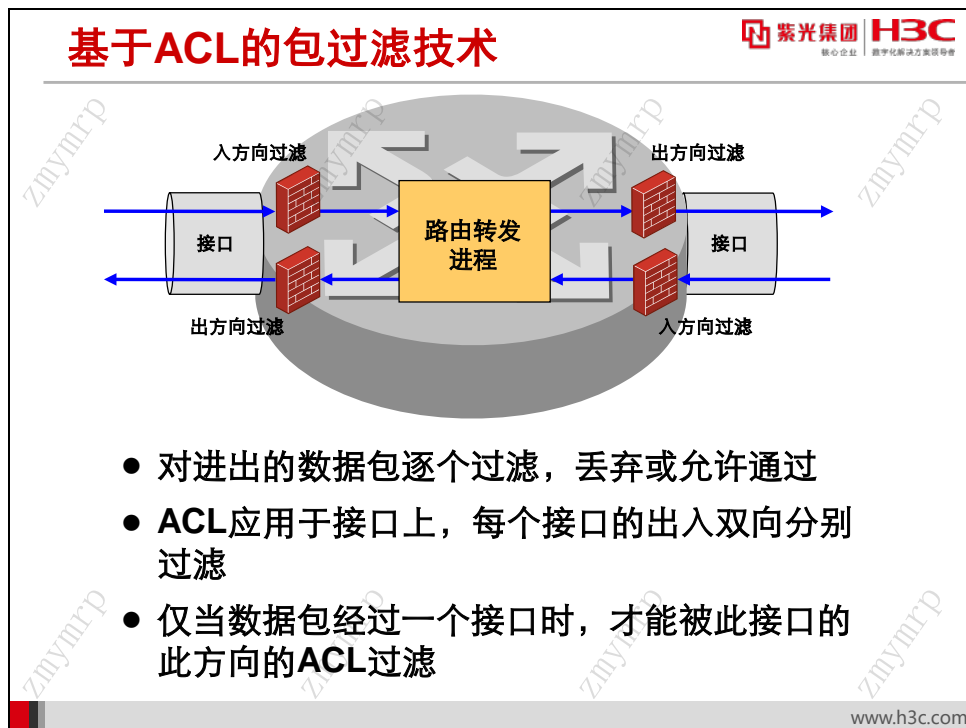
较高优先级，就可以保障语音数据包优先被网络设备所转发，从而保障 IP 语音通话质量；

- **路由策略和过滤：**路由器在发布与接收路由信息时，可能需要实施一些策略，以便对路由信息进行过滤。比如，路由器可以通过引用 ACL 来对匹配路由信息的目的网段地址实施路由过滤，过滤掉不需要的路由而只保留必须的路由；
- **按需拨号：**配置路由器建立 PSTN/ISDN 等按需拨号连接时，需要配置触发拨号行为的数据，即只有需要发送某类数据时路由器才会发起拨号连接。这种对数据的匹配也通过配置和引用 ACL 来实现。

本章我们重点学习 MSR 路由器基于 ACL 的包过滤的工作原理。

27.3 基于ACL的包过滤

27.3.1 基本工作原理



在路由器上实现包过滤功能的核心内容就是 ACL。

包过滤配置在路由器的接口上，并且具有方向性。每个接口的出站方向（Outbound）和入站方向（Inbound）均可配置独立的 ACL 进行包过滤。

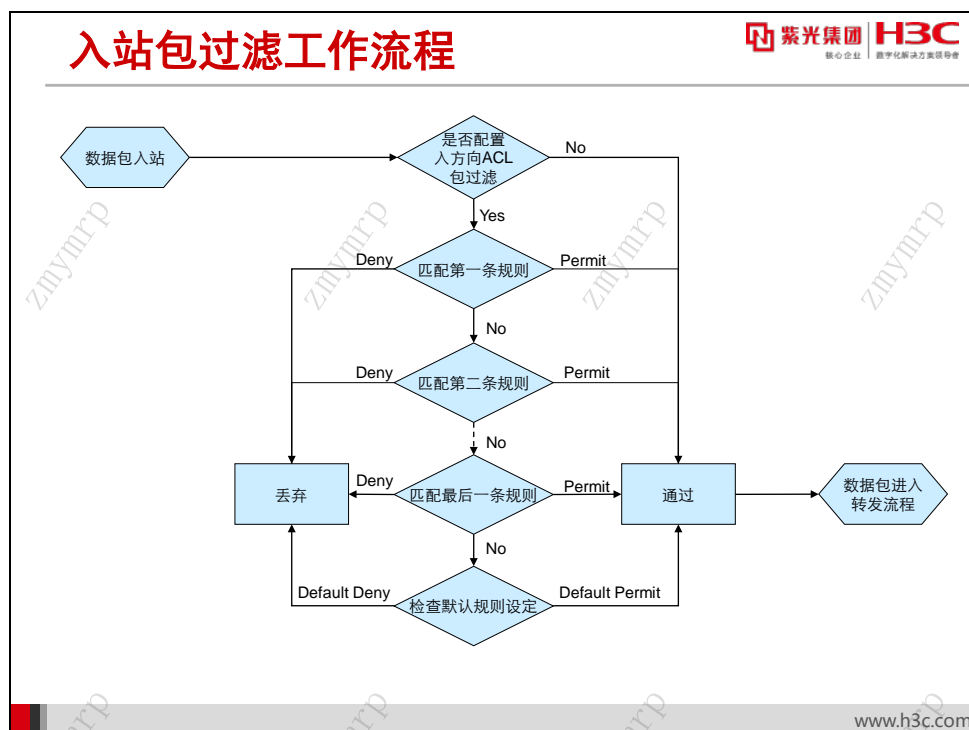
当数据包被路由器接收时，就会受到入接口上入站方向的防火墙过滤；反之，当数据包即将从一个接口发出时，就会受到出接口上出站方向的防火墙过滤。当然，如果该接口该方向上没有配置包过滤，数据包就不会被过滤，而直接通过。

包过滤防火墙对进出的数据包逐个检查其 IP 地址、协议类型、端口号等信息，与自身所引用的 ACL 进行匹配，根据 ACL 的规则（rule）设定丢弃数据包或转发之。

注意：

虽然 H3C 交换机也支持 ACL 包过滤，但不同设备的 ACL 实现有细微差别。本书以 MSR 路由器为范例讲解 ACL 的工作。

27.3.2 ACL 包过滤工作流程



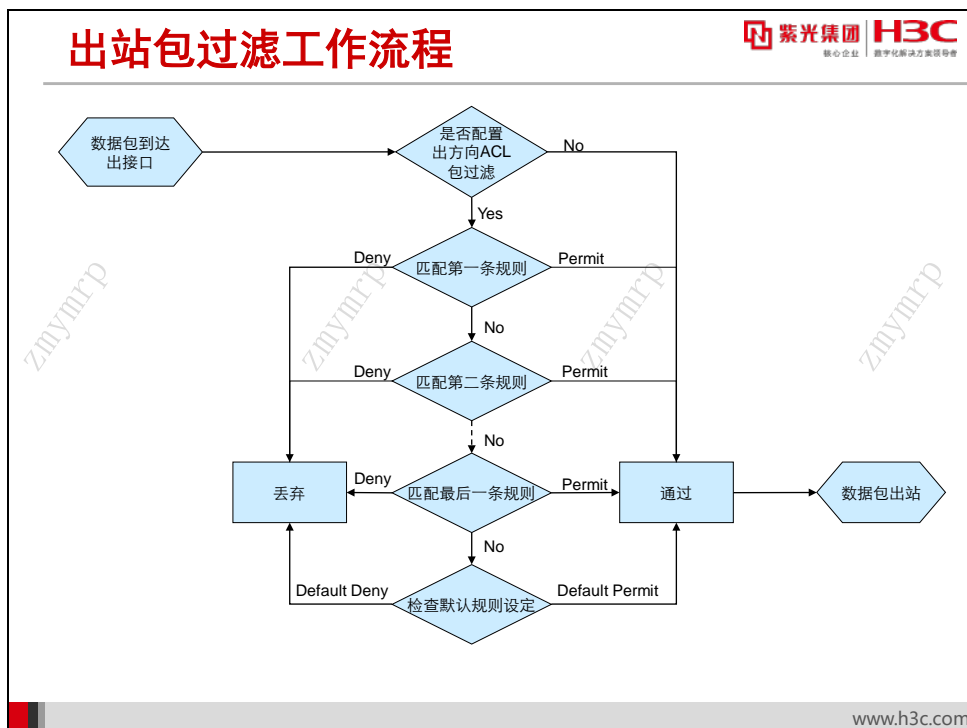
包过滤防火墙的规则设定通过引用 **ACL** 来实现。一个 **ACL** 可以包含多条规则（**rule**），每条规则都定义了一个匹配条件及其相应动作。

ACL 规则的匹配条件主要包括数据包的源 **IP** 地址、目的 **IP** 地址、协议号、源端口号、目的端口号等；另外还可以有 **IP** 优先级、分片报文位、**MAC** 地址、**VLAN** 信息等。不同的 **ACL** 分类所能包含的匹配条件也不同。

ACL 规则的动作有两个：允许（**Permit**）或拒绝（**Deny**）。

当路由器收到一个数据包时，如果入接口上没有启动包过滤，则数据包直接被提交给路由转发进程去处理；如果入接口上启动了 **ACL** 包过滤，则将数据包交给入站防火墙进行过滤，其工作流程如下：

- 1) 系统用 **ACL** 中第一条规则的条件来尝试匹配数据包中信息；
- 2) 如果数据包信息符合此规则的条件（即数据包命中此规则），则执行规则所设定的动作。若动作为 **permit**，则允许此数据包穿过防火墙，将其提交给路由转发进程去处理；若动作为 **deny**，则丢弃此数据包；
- 3) 如果数据包信息不符合此规则的条件，则转下一条 **ACL** 规则继续尝试匹配；
- 4) 如果数据包信息不符合任何一条规则的条件，则执行防火墙的默认动作。若默认动作为 **permit**，则允许此数据包穿过防火墙，将其提交给路由转发进程去处理；若动作为 **deny**，则丢弃此数据包。



ACL 包过滤具有方向性，可以指定对出或入接口方向的数据包过滤。


当路由器准备从某接口上发出一个数据包时，如果出接口上没有启动包过滤，则数据包直接由接口发出；如果出接口上启动了 ACL 包过滤，则将数据包交给出站防火墙进行过滤，其工作流程如下：

- 1) 系统用 ACL 中第一条规则的条件来尝试匹配数据包中信息；
- 2) 如果数据包信息符合此规则的条件，则执行规则所设定的动作。若动作为 **permit**，则允许此数据包穿过防火墙，将其提交给路由转发进程去处理；若动作为 **deny**，则丢弃此数据包；
- 3) 如果数据包信息不符合此规则的条件，则转下一条 ACL 规则继续尝试匹配；
- 4) 如果数据包信息不符合任何一条规则的条件，则执行防火墙的默认动作。若默认动作为 **permit**，则允许此数据包穿过防火墙，将其提交给路由转发进程去处理；若动作为 **deny**，则丢弃此数据包。

默认动作用来定义对 ACL 以外数据包的处理方式，即在没有规则去判定用户数据包是否可以通过的时候，防火墙采取的策略是允许 (**permit**) 还是拒绝 (**deny**) 该数据包通过。默认动作可以通过命令进行修改。

27.3.3 通配符掩码

通配符掩码



- 通配符掩码和IP地址结合使用，以描述一个地址范围
- 通配符掩码和子网掩码相似，但含义不同
 - 0 表示对应位须比较
 - 1 表示对应位不比较

通配符掩码	含义
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

www.h3c.com

ACL 规则都使用 IP 地址和通配符掩码来设定匹配条件。

通配符掩码也称为反掩码。和子网掩码一样，通配符掩码也是由 0 和 1 组成的 32 比特数，也以点分十进制形式表示。通配符掩码的作用与子网掩码的作用相似，即通过与 IP 地址执行比较操作来标识网络。不同的是，通配符掩码化为二进制后，其中的 1 表示“在比较中可以忽略相应的地址位，不用检查”，地址位上的 0 表示“相应的地址位必须被检查”。

在进行 ACL 包过滤时，具体的比较算法是：

- 1) 用 ACL 规则中配置的 IP 地址与通配符掩码做异或（XOR）运算，得到一个地址 X；
- 2) 用数据包的 IP 地址与通配符掩码做异或运算，得到一个地址 Y；
- 3) 如果 X=Y 则此数据包命中此条规则，反之则未命中此规则。

通配符掩码的应用示例		
IP地址	通配符掩码	表示的地址范围
192.168.0.1	0.0.0.255	192.168.0.0/24
192.168.0.1	0.0.3.255	192.168.0.0/22
192.168.0.1	0.255.255.255	192.0.0.0/8
192.168.0.1	0.0.0.0	192.168.0.1
192.168.0.1	255.255.255.255	0.0.0.0/0
192.168.0.1	0.0.2.255	192.168.0.0/24和192.168.2.0/24

例如，要使一条规则匹配子网 192.168.0.0/24 中的地址，其条件中的 IP 地址应为 192.168.0.0，通配符掩码应为 0.0.0.255，表明只比较 IP 地址的前 24 位。

再如，要使一条规则匹配子网 192.168.0.0/22 中的地址，其条件中的 IP 地址应为 192.168.0.0，通配符掩码应为 0.0.3.255，表明只比较 IP 地址的前 22 位。

通配符掩码中的 0 和 1 可以是不连续的，从这种意义上说，“反掩码”的称呼并不精确。

例如通配符掩码 0.0.2.255 的二进制表现形式是 00000000 00000000 00000010 11111111，表示 IP 地址的前 22 位和第 24 位必须比较，而第 23 位和末 8 位不比较。如果某规则的条件是 IP 地址 192.168.0.1，通配符掩码 0.0.2.255，表示其可以被子网 192.168.0.0/24 和 192.168.2.0/24 中的地址命中。

27.4 ACL 分类

27.4.1 ACL 的标识

ACL 的标识

紫光集团 H3C
核心企业 数字化转型最佳实践者

- 利用数字序号标识访问控制列表

访问控制列表的类型	数字序号的范围
基本访问控制列表	2000~2999
高级访问控制列表	3000~3999
基于二层的访问控制列表	4000~4999

- 可以给访问控制列表指定名称，便于维护

www.h3c.com

根据所过滤数据包类型的不同，MSR 路由器上的 ACL 包含 IPv4 ACL 和 IPv6 ACL。本章讲述 IPv4 ACL。如无特别声明，本书所称的 ACL 均指 IPv4 ACL。

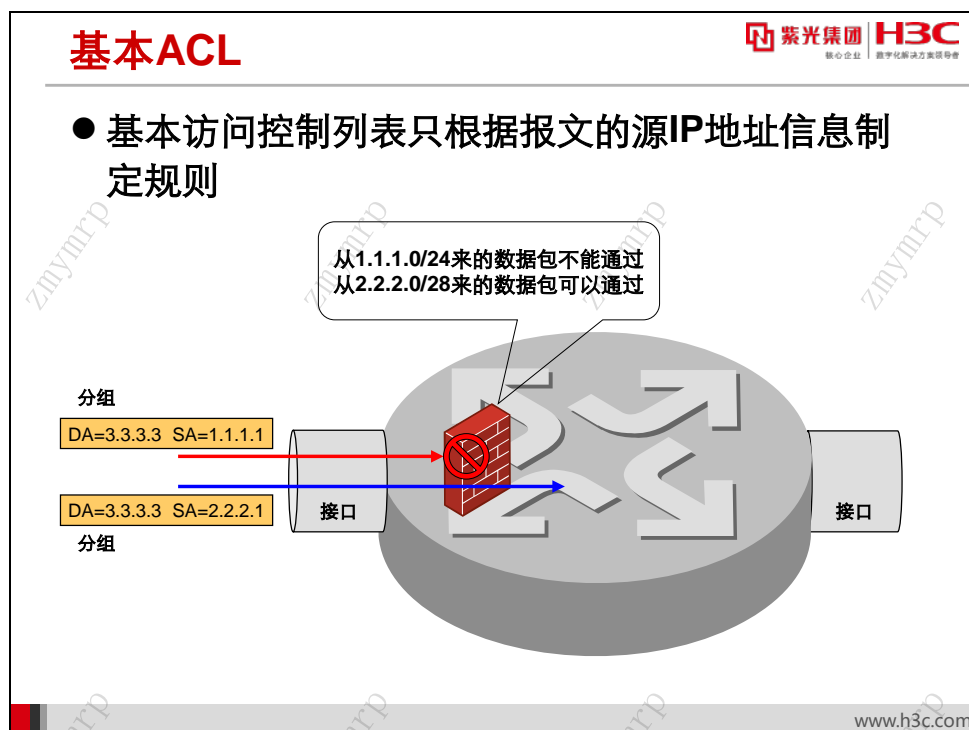
在配置 IPv4 ACL 的时候，需要定义一个数字序号，并且利用这个序号来唯一标识一个 ACL。

ACL 为如下所示的几类：

- 基本 ACL（序号为 2000~2999）：只根据报文的源 IP 地址信息制定规则；
- 高级 ACL（序号为 3000~3999）：根据报文的源 IP 地址信息、目的 IP 地址信息、IP 承载的协议类型、协议的特性等三、四层信息制定规则；
- 二层 ACL（序号为 4000~4999）：根据报文的源 MAC 地址、目的 MAC 地址、VLAN 优先级、二层协议类型等二层信息制定规则。

指定序列号的同时，可以为 ACL 指定一个名称，称为命名的 ACL。命名 ACL 的好处是容易记忆，便于维护。命名的 ACL 使用户可以通过名称唯一地确定一个 ACL，并对其进行相应的操作。

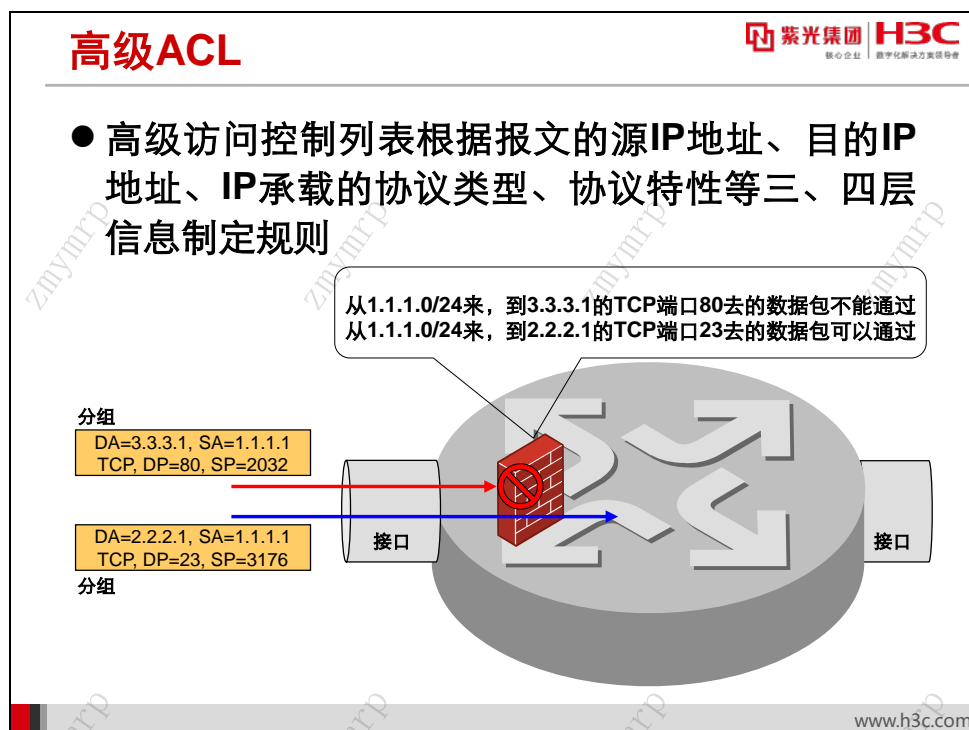
27.4.2 基本 ACL



因为基本访问控制列表只根据报文的源 IP 地址信息制定规则，所以比较适用于过滤从特定网络来的报文的情况。

在上图例子中，用户希望拒绝来自网络 1.1.1.0/24 的数据报文通过，而允许来自网络 2.2.2.0/28 的数据报文被路由器转发。这种情况下就可以定义一个基本访问控制列表，包含两条规则，其中一条规则匹配源 IP 地址 1.1.1.0/24，动作是 deny；而另一条规则匹配源 IP 地址 2.2.2.0/28，动作是 permit。

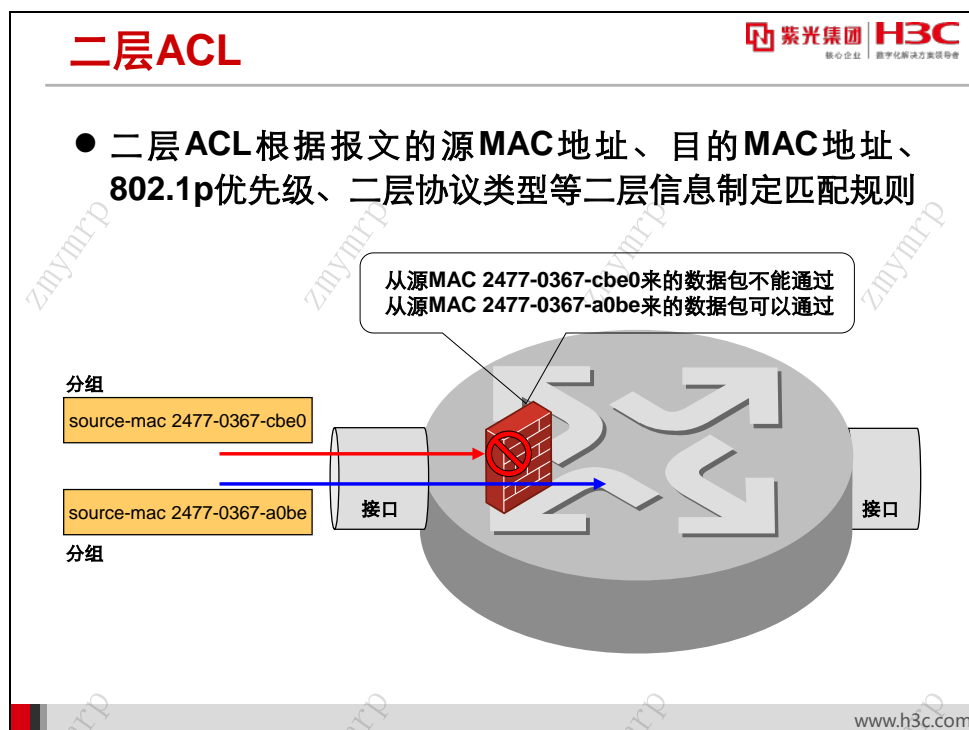
27.4.3 高级 ACL



因为高级访问控制列表根据报文的源 IP 地址信息、目的 IP 地址信息、IP 承载的协议类型、协议的特性等三、四层信息制定规则，所以比较适合于过滤某些网络中的应用及过滤精确的数据流的情形。

在上图的例子中，用户希望拒绝从网络 1.1.1.0/24 到 3.3.3.1 的 HTTP 协议访问，而允许从网络 1.1.1.0/24 到 2.2.2.1 的 Telnet 协议访问。这种情况下就可以定义一个高级访问控制列表，其中的一条规则匹配源 IP 地址 1.1.1.0/24、目的 IP 地址 3.3.3.1/32、目的 TCP 端口 80(HTTP) 的数据报文，动作是 deny；另一条规则匹配源 IP 地址 1.1.1.0/24、目的 IP 地址 2.2.2.1/32、目的 TCP 端口 23 (Telnet) 的数据报文，动作是 permit。

27.4.4 二层 ACL



MSR 路由器还支持二层 ACL。


二层 ACL 可根据报文的源 MAC 地址、目的 MAC 地址、VLAN 优先级、二层协议类型等二层信息制定规则。

例如，用户可以禁止 802.1p 优先级为 3 的报文通过路由器，而允许其他报文通过。因为 802.1p 优先级是属于带有 VLAN 标签的以太网帧头中的信息，所以可以使用二层 ACL 来匹配。

27.5 配置ACL包过滤

27.5.1 ACL 包过滤配置任务

ACL包过滤配置任务



- 设置包过滤功能的默认过滤规则
- 根据需要选择合适的ACL分类
- 创建正确的规则
 - 设置匹配条件
 - 设置合适的动作 (Permit/Deny)
- 在路由器的接口上应用ACL，并指明过滤报文的方向（入站/出站）

www.h3c.com

ACL 包过滤配置任务包括：

- 设置包过滤功能默认的过滤规则

系统包过滤功能默认开启，可以通过设置来修改其默认的过滤规则。

- 根据需要选择合适的 ACL 分类

不同的 ACL 分类其所能配置的报文匹配条件是不同的，应该根据实际情况的需要来选择合适的 ACL 分类。比如，如果只需要过滤来自于特定网络的 IP 报文，那么选择基本 ACL 就可以了；如果需要过滤上层协议应用，那么就需要用到高级 ACL。

- 创建规则，设置匹配条件及相应的动作（Permit/Deny）

要注意定义正确的通配符掩码以命中需要匹配的 IP 地址范围；选择正确的协议类型、端口号来命中需要匹配的上层协议应用；并给每条规则选择合适的动作。如果一条规则不能满足需求，那还需要配置多条规则并注意规则之间的排列顺序。

- 在路由器的接口应用 ACL，并指明是对入接口或出接口的报文进行过滤

只有在路由器的接口上应用了 ACL 后，包过滤才会生效。另外，对于接口来说，可分为入接口的报文和出接口的报文，所以还需要指明是对哪个方向的报文进行过滤。

27.5.2 设置包过滤规则

设置包过滤规则

 紫光集团

 H3C

核心企业 | 数字化转型方案领导者

- 包过滤功能默认开启
- 设置包过滤的默认过滤方式
 - 系统默认的过滤方式是permit，即允许未匹配上ACL规则的报文通过
 - 可以配置包过滤的缺省动作为deny

[H3C] packet-filter default deny

www.h3c.com

路由器系统内嵌的包过滤防火墙功能默认开启。系统默认的包过滤方式为 **permit**，即允许未匹配上 **ACL** 规则的报文通过。

可以通过设置来修改包过滤防火墙的默认动作为 **deny**。默认动作用来定义对访问控制列表以外数据包的处理方式，即在没有规则去判定用户数据包是否可以通过的时候，防火墙采取的策略是允许还是禁止该数据包通过。

通过以下命令：

```
[H3C] packet-filter default deny
```

可以修改包过滤的默认动作为 **deny** 后，即可禁止未匹配上 **ACL** 规则的报文通过。

27.5.3 配置基本 ACL

配置基本ACL

紫光集团
核心企业 | 数字化转型方案领导者

- **配置基本ACL，并指定ACL序号**
→ 基本IPv4 ACL的序号取值范围为2000~2999

[H3C] acl basic acl-number

- **定义规则**
→ 制定要匹配的源IP地址范围
→ 指定动作是permit或deny

[H3C-acl-ipv4-basic-2000] rule [rule-id] { deny | permit } [counting | fragment | logging | source { object-group address-group-name | source-address source-wildcard | any } | time-range time-range-name | vpn-instance vpn-instance-name]

www.h3c.com

基本访问控制列表的配置可以分为两部分：

第1步：设置访问控制列表序列号，基本访问控制列表的序列号范围为 2000-2999：

[H3C] acl basic acl-number

第2步：定义规则，允许或拒绝来自指定网络的数据包，并定义参数：

[H3C-acl-ipv4-basic-2000] rule [rule-id] { deny | permit } [counting | fragment | logging | source { object-group address-group-name | source-address source-wildcard | any } | time-range time-range-name | vpn-instance vpn-instance-name]

其中主要的参数含义如下：


- **deny：**表示拒绝符合条件的报文；
- **permit：**表示允许符合条件的报文通过；
- **counting：**表示使能了规则匹配统计功能，缺省为关闭；
- **fragment：**分片信息。定义规则仅对非首片分片报文有效，而对非分片报文和首片分片报文无效。若未指定本参数，表示该规则对非分片报文和分片报文均有效；
- **logging：**对符合条件的报文可记录日志信息；
- **source {object-group address-group-name | source-address source-wildcard | any }：**指定规则的源 IP 地址信息。*address-group-name* 表示源 IP 地址对象组的名

称, *source-address* 表示报文的源 IP 地址, *source-wildcard* 表示源 IP 地址的通配符掩码 (为 0 表示主机地址), *any* 表示任意源 IP 地址。**object-group** 参数的支持情况与设备型号有关, 请以设备的实际情况为准;

- **time-range** *time-range-name*: 指定规则生效的时间段;
- **vpn-instance** *vpn-instance-name*: 表示对指定 VPN 实例中的报文有效。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。若未指定本参数, 表示该规则对非 VPN 报文有效, 对 VPN 报文无效。

27.5.4 配置高级 ACL

配置高级ACL



紫光集团 H3C
核心企业 数字化转型方案领导者

- **配置高级IPv4 ACL, 并指定ACL序号**
→ 高级IPv4 ACL的序号取值范围为3000~3999

[H3C] acl advanced *acl-number*

- **定义规则**
→ 需要配置规则来匹配源IP地址、目的IP地址、IP承载的协议类型、协议端口号等信息
→ 指定动作是permit或deny

```
[H3C-acl-ipv4-adv-3000] rule [ rule-id ] { deny | permit } protocol [ { { ack ack-value | fin fin-value | psh psh-value | rst rst-value | syn syn-value | urg urg-value } | established } | counting | destination { object-group address-group-name | dest-address dest-wildcard | any } | destination-port { object-group port-group-name | operator port1 [ port2 ] } | { dscp dscp | precedence precedence | tos tos } } | fragment | icmp-type { icmp-type [ icmp-code ] | icmp-message } | logging | source { object-group address-group-name | source-address source-wildcard | any } | source-port { object-group port-group-name | operator port1 [ port2 ] } | time-range time-range-name | vpn-instance vpn-instance-name }
```

www.h3c.com

高级访问控制列表的配置可以分为两部分, 如下:

第1步: 设置访问控制列表序列号, 高级访问控制列表的序列号范围为 3000-3999:

[H3C] acl advanced *acl-number*

第2步: 定义规则, 其规则在基本访问列表的基础上增加了目的地址、协议号、端口以及操作符等信息:

```
[H3C-acl-ipv4-adv-3000] rule [ rule-id ] { deny | permit } protocol [ { { ack ack-value | fin fin-value | psh psh-value | rst rst-value | syn syn-value | urg urg-value } | established } | counting | destination { object-group address-group-name | dest-address dest-wildcard | any } | destination-port { object-group port-group-name | operator port1 [ port2 ] } | { dscp dscp | precedence precedence | tos tos } } | fragment | icmp-type { icmp-type [ icmp-code ] | icmp-message } |
```

```
logging | source { object-group address-group-name | source-address
source-wildcard | any } | source-port { object-group port-group-name | operator
port1 [ port2 ] } | time-range time-range-name | vpn-instance vpn-instance-name ]
```

其中主要的参数含义如下：

- **deny**: 表示拒绝符合条件的报文；
- **permit**: 表示允许符合条件的报文通过；
- **protocol**: 表示 IPv4 承载的协议类型。用数字表示时，取值范围为 0~255；用名字表示时，可以选取 gre (47)、icmp (1)、igmp (2)、ip、ipinip (4)、ospf (89)、tcp (6)、udp (17)；
- { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } : TCP 报文标识，定义对携带不同标志位（包括 ACK、FIN、PSH、RST、SYN 和 URG 六种）的 TCP 报文的处理规则；
- **established**: TCP 连接建立标识，定义对 TCP 连接报文的处理规则；
- **counting**: 表示使能了规则匹配统计功能，缺省为关闭；
- **source** { **object-group** *address-group-name* | *source-address* *source-wildcard* | **any** } : 用来确定报文的源 IP 地址，点分十进制表示；
- **destination** { **object-group** *address-group-name* | *dest-address* *dest-wildcard* | **any** } : 用来确定报文的目的 IP 地址，点分十进制表示；
- **operator**: 端口操作符，取值可以为 lt（小于）、gt（大于）、eq（等于）、neq（不等于）或者 range（在范围内，包括边界值）。只有操作符 range 需要两个端口号做操作数，其他的只需要一个端口号做操作数；
- **port1**、**port2**: TCP 或 UDP 的端口号，用数字表示时，取值范围为 0~65535，也可以用文字表示；
- **logging**: 对符合条件的报文可记录日志信息。

27.5.5 配置二层 ACL

配置二层ACL

紫光集团 H3C
核心企业 数字化转型方案领导者

- **配置二层 ACL，并指定ACL序号**
 - 二层ACL的序号取值范围为4000~4999

[H3C] acl mac acl-number

- **定义规则**
 - 需要配置规则来匹配源MAC地址、目的MAC地址、802.1p 优先级、二层协议类型等二层信息
 - 指定动作是permit或拒绝deny

[H3C-acl-mac-4000] rule [rule-id] { deny | permit } [cos dot1p | counting | dest-mac dest-address dest-mask | { lsap lsap-type lsap-type-mask | type protocol-type protocol-type-mask } | source-mac source-address source-mask | time-range time-range-name]

www.h3c.com

规则序列号在 4000 到 4999 之间的访问控制列表为二层访问控制列表，二层 ACL 根据报文的源 MAC 地址、目的 MAC 地址、802.1p 优先级、二层协议类型等二层信息制定匹配规则，对报文进行相应的分析处理。

二层自定义的访问控制列表的配置可以分为两部分，如下：

第1步：设置访问控制列表序列号，二层访问控制列表的序列号范围为 4000~4999：

[H3C] acl mac acl-number

第2步：配置规则，规则上主要为源 MAC、目的 MAC 以及 COS 值等信息：

[H3C-acl-mac-4000] rule [rule-id] { deny | permit } [cos dot1p | counting | dest-mac dest-address dest-mask | { lsap lsap-type lsap-type-mask | type protocol-type protocol-type-mask } | source-mac source-address source-mask | time-range time-range-name]


其中主要的参数含义如下：

- **deny：**表示拒绝符合条件的报文；
- **permit：**表示允许符合条件的报文通过；
- **cos vlan-pri：**定义规则的 802.1p 优先级；
- **dest-mac dest-address dest-mask：**定义规则的目的 MAC 地址范围；
- **lsap lsap-type lsap-type-mask：**定义规则中 LLC 封装中的 DSAP 字段和 SSAP 字段；

- **source-mac** *source-address source-mask*: 定义规则的源 MAC 地址范围;
- **time-range** *time-range-name*: 指定规则生效的时间段。

27.5.6 在接口上应用 ACL

在接口上应用ACL



- 将ACL应用到接口上，配置的ACL包过滤才能生效
- 指明在接口上应用的方向是Outbound还是Inbound

```
[H3C-Serial2/0] packet-filter [ ipv6 | mac ] { acl-  
number | name acl-name } { inbound | outbound }
```

www.h3c.com

只有将 ACL 应用在接口上才能实现包过滤防火墙的功能。

对于路由器而言，接口的方向只有两个：inbound 方向和 outbound 方向。数据包进入路由器的方向是 inbound 方向，而数据包离开路由器的方向是 outbound 方向。

将访问控制列表应用在接口的命令如下：

```
[H3C-Serial2/0] packet-filter [ ipv6 | mac ] { acl-number | name acl-name }  
{ inbound | outbound }
```

其中主要的参数含义如下：

- **ipv6**: 指定 ACL 类型为 IPv6 ACL;
- **mac**: 指定 ACL 类型为二层 ACL;
- **acl-number**: 访问控制列表号，取值范围为 2000~4999;
- **name acl-name**: 指定访问控制列表的名称;
- **inbound**: 过滤接口接收的数据包;
- **outbound**: 过滤接口转发的数据包。

27.5.7 ACL 包过滤信息显示与调试

操作	命令
查看包过滤的统计信息	display packet-filter statistics { interface interface-type interface-number { inbound outbound } [default [ipv6 mac] { acl-number name acl-name }] } zone-pair security source source-zone-name destination destination-zone-name [[ipv6] { acl-number name acl-name }] } [brief]
清除包过滤的统计信息	reset packet-filter statistics { interface [interface-type interface-number] { inbound outbound } [default [ipv6 mac] { acl-number name acl-name }] } zone-pair security [source source-zone-name destination destination-zone-name] [[ipv6] { acl-number name acl-name }] }
显示配置的IPv4 ACL信息	display acl [ipv6 mac wlan] { acl-number all name acl-name }
清除IPv4 ACL统计信息	reset acl [ipv6 mac] counter { acl-number all name acl-name }

ACL 包过滤配置完成后，可通过命令查看到防火墙的统计信息、默认过滤规则、接口上应用的 ACL 情况以及数据包被允许或者拒绝的情况。

显示配置的 ACL 信息：

```
<Sysname> display acl all
Basic IPv4 ACL 2001, 2 rules, match-order is auto,
This is an IPv4 basic ACL.
ACL's step is 5
ACL accelerated
rule 5 permit source 1.1.1.1 0 (5 times matched)
rule 5 comment This rule is used on GigabitEthernet1/0/1.
rule 10 permit source object-group permit (5 times matched)
Advanced IPv4 ACL 3001, 1 rule,
ACL's step is 5
rule 0 permit ip source 1.1.1.0 0.0.0.255 destination 3.3.3.0 0.0.0.255 (Dynamic)
```

从以上输出信息我们可以知道，ACL 2001 包含了两条规则，并且有 5 个数据报文命中。

查看 ACL 在包过滤中应用的统计信息：

```
<Sysname> display packet-filter statistics interface gigabitethernet 1/0/1
inbound
Interface: GigabitEthernet1/0/1
Inbound policy:
IPv4 ACL 2001
From 2011-06-04 10:25:21 to 2011-06-04 10:35:57
rule 0 permit source 2.2.2.2 0 counting (2 packets, 256 bytes)
rule 5 permit source 1.1.1.1 0 counting (Failed)
rule 10 permit vpn-instance test counting (No resource)
Totally 2 packets 256 bytes permitted, 0 packets 0 bytes denied
```

```
Totally 100% permitted, 0% denied

IPv6 ACL 2000

MAC ACL 4000
  rule 0 permit

IPv4 default action: Deny

IPv6 default action: Deny
MAC default action: Deny
```

从以上输出我们可以得知，在接口 **GigabitEthernet1/0/1** 的入方向上，应用了包过滤策略 **ACL 2001**。包过滤策略有三条规则，总计允许通过了两个报文，无阻塞报文，报文通过率 **100%**。


另外，在用户视图下可以使用命令 **reset packet-filter statistics interface GigabitEthernet 1/0/1 inbound 2001** 来清除接口 **GigabitEthernet1/0/1** 入方向上 **IPv4** 基本 **ACL 2001** 在报文过滤中应用的统计信息：

```
<H3C> reset packet-filter statistics interface GigabitEthernet 1/0/1 inbound 2001
```

27.6 ACL包过滤的注意事项

27.6.1 ACL 规则的匹配顺序

ACL规则的匹配顺序



- 匹配顺序指ACL中规则的优先级
- ACL支持两种匹配顺序：
 - 配置顺序（config）：按照用户配置规则的先后顺序进行规则匹配
 - 自动排序（auto）：按照“深度优先”的顺序进行规则匹配，即地址范围小的规则被优先进行匹配
- 配置ACL的匹配顺序：

```
[H3C] acl [ ipv6 ] { advanced | basic } { acl-number |
name acl-name } [ match-order { auto | config } ]
```

www.h3c.com

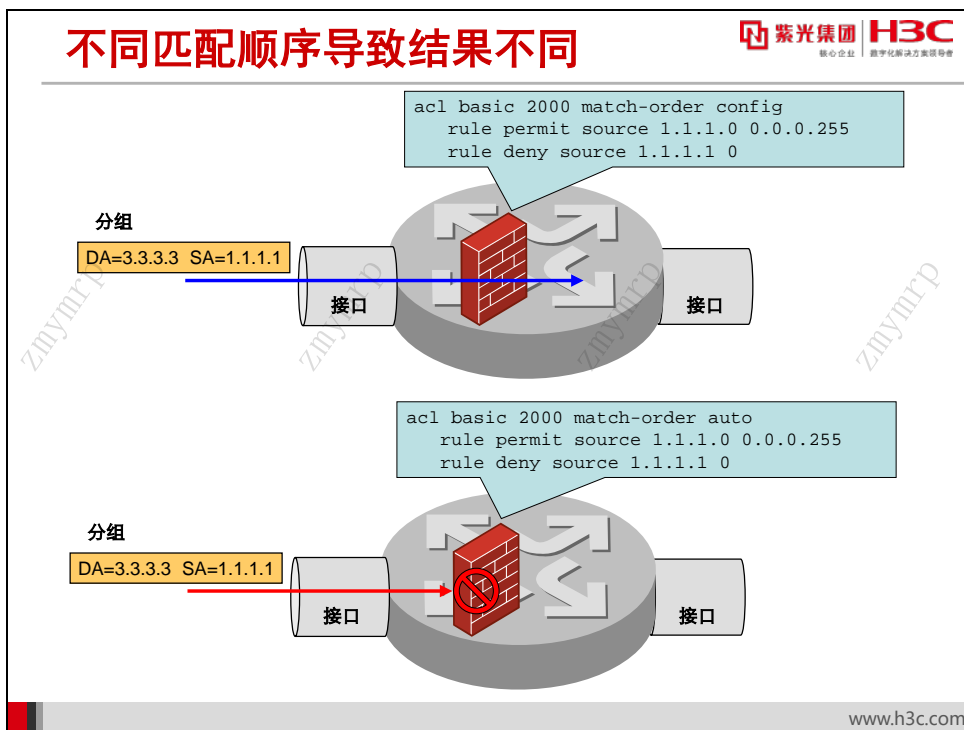
一个 ACL 中可以包含多个规则，而每个规则都指定不同的报文匹配选项，这些规则可能存在动作冲突。由于 ACL 规则是顺序匹配的，如果发生动作冲突，将以先命中的规则的动作为准。

ACL 支持两种匹配顺序：

- 配置顺序（config）：按照用户配置规则的先后顺序进行规则匹配；
- 自动排序（auto）：按照“深度优先”的顺序进行规则匹配，即系统优先考虑地址范围小的规则。

在配置 ACL 的时候，系统默认的匹配顺序是 config。可通过命令来配置 ACL 的匹配顺序：

```
[H3C] acl [ ipv6 ] { advanced | basic } { acl-number | name acl-name }
[ match-order { auto | config } ]
```



同样的一条 ACL，因为匹配顺序不同，会导致不同的结果。

在图示上方的例子中，ACL 的匹配顺序是 **config**，系统会按照用户配置规则的先后顺序进行规则匹配。所以主机 1.1.1.1 所发出的数据报文被系统允许通过。而在图示下方的例子中，因为匹配顺序是 **auto**，系统会按照“深度优先”的规则来匹配，数据报文优先匹配 IP 地址范围小的第二条规则，所以路由器会丢弃源地址是 1.1.1.1 的数据报文。

不同类型的 ACL 的深度优先的判断原则可能略有不同。

基本 ACL 的“深度优先”顺序判断原则如下：

- 1) 先判断规则的匹配条件中是否包含 VPN 实例，包含者优先；
- 2) 如果 VPN 实例的包含情况相同，再比较源 IP 地址范围，源 IP 地址范围小（反掩码中“0”位的数量多）的规则优先；
- 3) 如果源 IP 地址范围相同，则先配置的规则优先。

高级 ACL 的“深度优先”顺序判断原则如下：

- 1) 先判断规则的匹配条件中是否包含 VPN 实例，包含者优先；
- 2) 如果 VPN 实例的包含情况相同，再比较协议范围，指定了 IP 协议承载的协议类型的规则优先；
- 3) 如果协议范围相同，则比较源 IP 地址范围，源 IP 地址范围小（反掩码中“0”位的数量多）的规则优先；

- 4) 如果源 IP 地址范围也相同，则比较目的 IP 地址范围，目的 IP 地址范围小（反掩码中“0”位的数量多）的规则优先；
- 5) 如果目的 IP 地址范围也相同，则比较第四层端口号（即 TCP/UDP 端口号）范围，四层端口号范围小的规则优先；
- 6) 如果上述范围都相同，再比较配置的先后次序，先配置者优先。

二层 ACL 的“深度优先”顺序判断原则如下：

- 1) 先比较源 MAC 地址范围，源 MAC 地址范围小（掩码中“1”位的数量多）的规则优先；
- 2) 如果源 MAC 地址范围相同，则比较目的 MAC 地址范围，目的 MAC 地址范围小（掩码中“1”位的数量多）的规则优先；
- 3) 如果源 MAC 地址范围、目的 MAC 地址范围相同，则先配置的规则优先。

27.6.2 在网络中的正确位置配置 ACL 包过滤

在网络中的正确位置配置ACL包过滤

紫光集团 H3C
核心企业 数字化转型专家

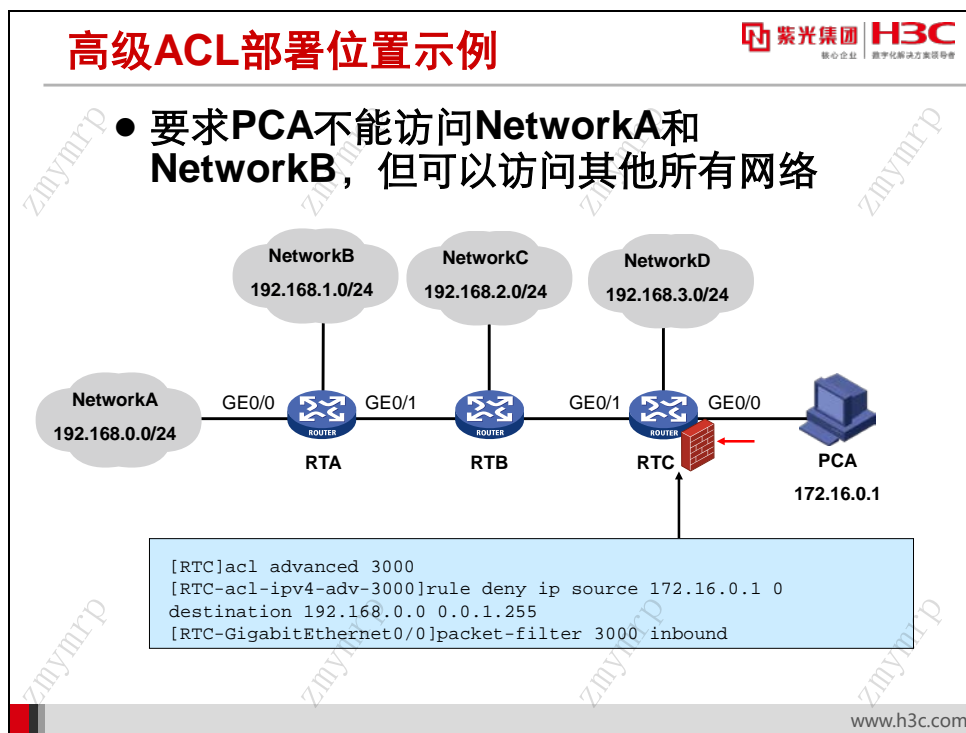
- 尽可能在靠近数据源的路由器接口上配置ACL，以减少不必要的流量转发
- 高级ACL
 - 应该在靠近被过滤源的接口上应用ACL，以尽早阻止不必要的流量进入网络
- 基本ACL
 - 过于靠近被过滤源的基本ACL可能阻止该源访问合法目的
 - 应在不影响其他合法访问的前提下，尽可能使ACL靠近被过滤的源

www.h3c.com

当在网络中部署 ACL 包过滤防火墙时，需要慎重考虑在哪个位置实施。如果一个网络中有多个路由器，部署的原则是，尽量在距离源近的地方应用 ACL 以减少不必要的流量转发。

高级 ACL 的条件设定比较精确，应该部署在靠近被过滤源的接口上，以尽早阻止不必要的流量进入网络。

基本 ACL 只能依据源 IP 地址匹配数据包，部署位置过于靠近被拒源的基本 ACL 可能阻止该源访问合法目的。因此应在不影响其他合法访问的前提下，尽可能使 ACL 靠近被拒绝的源。

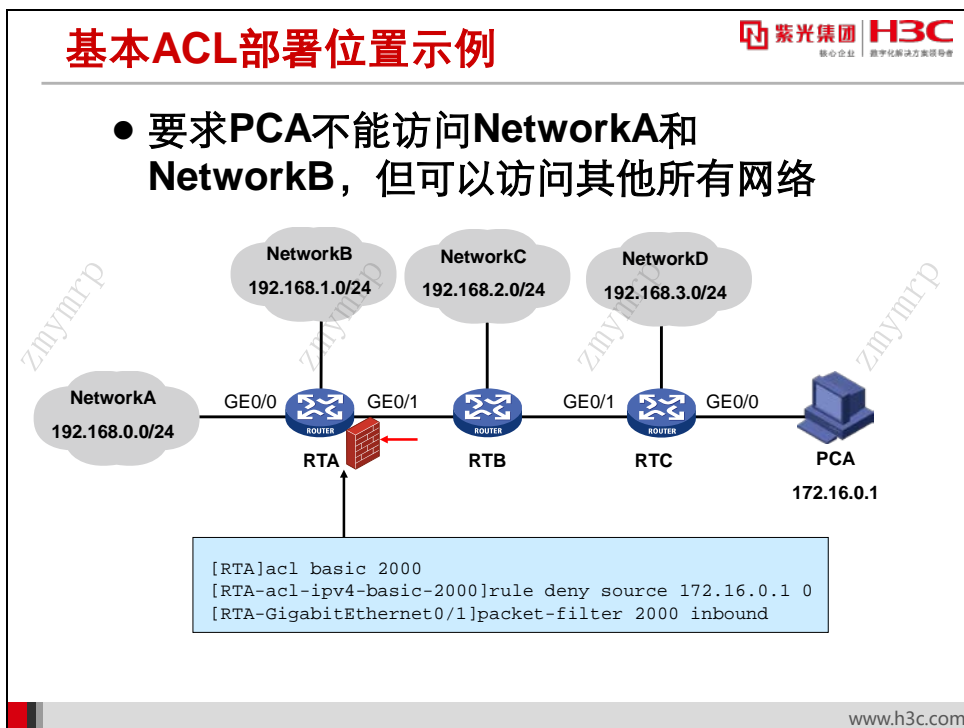


在上图中，用户想要实施 ACL 包过滤来阻断从主机 PCA 到 NetworkA 和 NetworkB 的数据包。如果用高级 ACL 来实现，在任意一台路由器上实施 ACL 都可以达到目的。但最好的实施位置是在路由器 RTC 的 G0/0 接口上，因为可以最大程度地减少不必要的流量处理与转发。

应当在 RTC 上配置如下：

```

[RTC] acl advanced 3000
[RTC-acl-ipv4-adv-3000] rule deny ip source 172.16.0.1 0 destination 192.168.0.0
0.0.1.255
[RTC-GigabitEthernet0/0] packet-filter 3000 inbound
  
```



用基本 ACL 来实现同样的要求，则需要更细心地考虑。如果仍在 RTC 的 G0/0 接口上配置入方向的基本 ACL 过滤，则 PCA 将不能访问任何一个网络！如果在 RTA 的 G0/0 接口上配置出方向的基本 ACL 过滤，则 PCA 虽然不能访问 NetworkA，却仍然可以访问 NetworkB。而在 RTA 的 G0/1 接口上配置入方向的基本 ACL 过滤，则既可以阻止 PCA 访问 NetworkA 和 NetworkB，也可以允许其访问其他所有网络。

应当在 RTA 上配置如下：


```

[RTA]acl basic 2000
[RTA-acl-ipv4-basic-2000]rule deny source 172.16.0.1 0
[RTA-GigabitEthernet0/1]packet-filter 2000 inbound
    
```

27.6.3 ACL 包过滤的局限性

ACL 包过滤的局限性

- **ACL 包过滤是根据数据包头中的二、三、四层信息来进行报文过滤的，对应用层的信息无法识别**
 - 无法根据用户名来决定数据是否通过
 - 无法给不同的用户授予不同的权限级别
- **ACL 包过滤防火墙是静态防火墙，无法对应用层的协议进行动态检测**



紫光集团 H3C
核心企业 数字化转型方案领导者

www.h3c.com

尽管基于 ACL 的包过滤防火墙功能强大，但是包过滤防火墙工作于 OSI 七层协议的四层以下，只能根据数据包头中的信息对报文进行过滤，不能够根据用户名来允许或拒绝数据通过，更加不能给不同的用户授权。如果想实现上述要求，必须在网络中使用其它网络安全技术，例如 802.1X、AAA（认证、授权和计费）等。

另外，ACL 的包过滤防火墙属于静态防火墙，即所有的过滤规则都在预先人为定义好的，不能由系统自动根据情况改变。这样在过滤某些应用层协议时会存在一些限制。比如，有些应用层协议会在客户端与服务器之间动态协商进行数据传输的协议和端口号，而 ACL 包过滤无法检测这些动态建立的传输会话，也就不能很好的进行过滤。如果想实现上述要求，可以使用状态防火墙，如 ASPF（Application Specific Packet Filter，基于应用层状态的包过滤）来实现。

27.7 本章总结

本章总结

- 包过滤防火墙使用**ACL**过滤数据包；**ACL**还可用于**NAT**、**QoS**、路由策略、按需拨号等
- 基本**ACL**根据源**IP**地址进行过滤；高级**ACL**根据**IP**地址、**IP**协议号、端口号等进行过滤
- **ACL**规则的匹配顺序会影响实际过滤结果
- **ACL**包过滤防火墙的配置位置应尽量避免不必要的流量进入网络

www.h3c.com

第28章 网络地址转换

当前的 Internet 主要基于 IPv4 协议,用户访问 Internet 的前提条件是拥有属于自己的 IPv4 地址。IPv4 地址共 32 位,理论上支持约 40 亿的地址空间,但随着 Internet 用户的快速增长,加上地址分配不均等因素,很多国家已经陷入 IP 地址不敷使用的窘境。

为了解决 IPv4 地址短缺的问题,IETF 提出了 NAT (Network Address Translation, 网络地址转换) 解决方案。IP 地址分为公有地址 (Global Address) 和私有地址 (Private Address)。公有地址由 IANA 统一分配,用于 Internet 通讯;私有地址可以自由分配,用于私有网络内部通讯。NAT 技术的主要作用是将私有地址转换成公有地址,使私有网络中的主机可以通过共享少量公有地址访问 Internet。

但 NAT 只是一种过渡技术,从根本上解决地址供需问题的方法是采用支持更大地址空间的下一代 IP 技术,即 IPv6 协议。它提供了几乎取之不尽的地址空间,是下一代 Internet 的协议基础。

与 NAT 相关的标准有 RFC 2663、RFC 3022、RFC 3027 等,其中 RFC 3022 是关于传统 NAT 的标准,它详细描述了传统 NAT 的分类和实现机制。

28.1 本章目标

课程目标

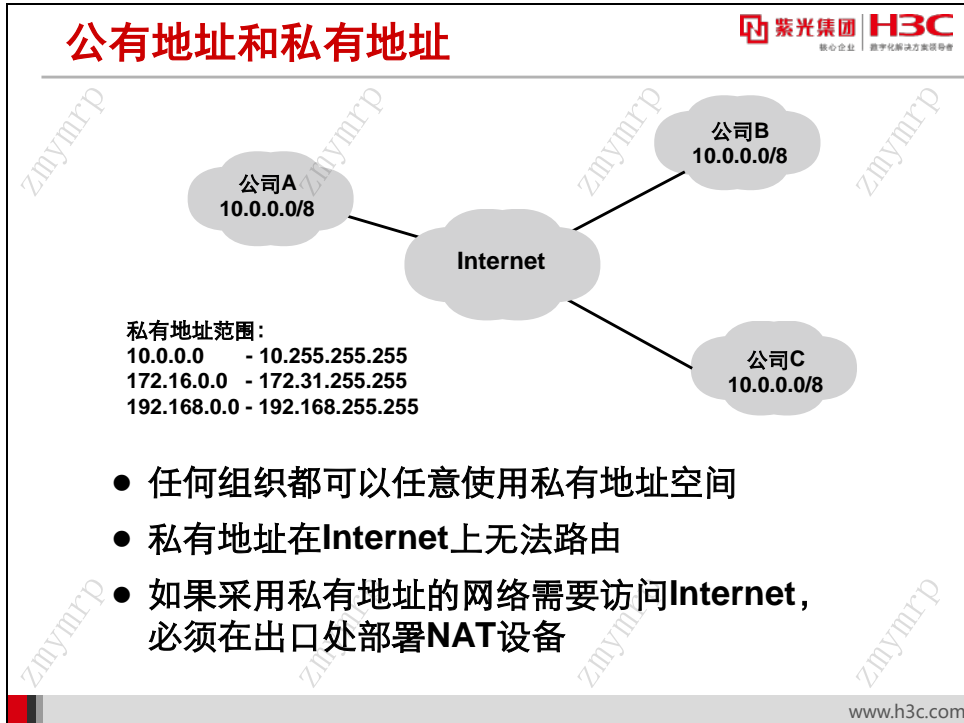
○ 学习完本课程,您应该能够:

- 理解 NAT 技术出现的历史背景
- 理解 NAT 的分类及原理
- 配置常见 NAT 应用
- 处理常见 NAT 问题
- 在实际网络中灵活使用 NAT 技术



28.2 NAT概述

28.2.1 公有地址和私有地址

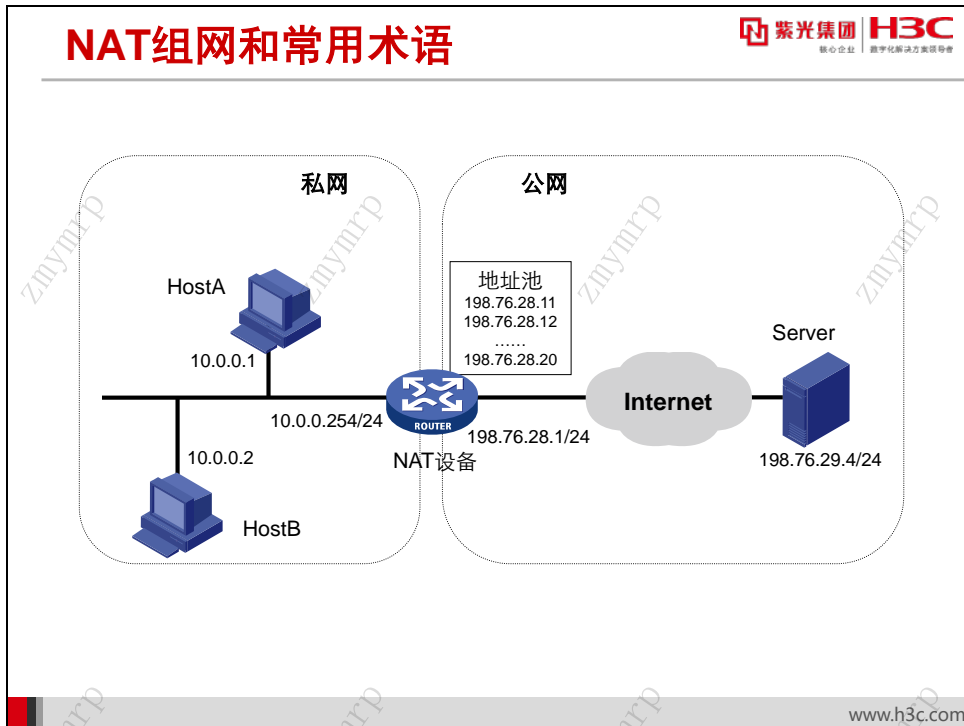


根据 RFC1918 的规定,IPv4 单播地址中预留了三个私有地址段(Private Address Space),供使用者任意支配,但仅限于私有网络使用,它们是 10.0.0.0/8、172.16.0.0/12 和 192.168.0.0/16。其他的 IPv4 单播地址(不包括 0.0.0.0/8 和 127.0.0.0/8)可以在 Internet 上使用,由 IANA 统一管理,称为公有地址(Global Address)。

在企业网络中,可以使用私有地址进行组网,尤其是在公有地址稀缺的情况下。采用私有地址的好处是可以任意分配巨大的私有地址空间,而无需征得 IANA 的同意。但私有地址在 Internet 上是无法路由的,如果采用私有地址的网络需要访问 Internet,必须在网络的出口处部署 NAT 设备,将私有地址转换成公有地址。

NAT 技术的出现,主要目的是解决 IPv4 地址匮乏的问题,另外 NAT 屏蔽了私网用户真实地址,也提高了私网用户的安全性。

28.2.2 NAT 组网和常用术语



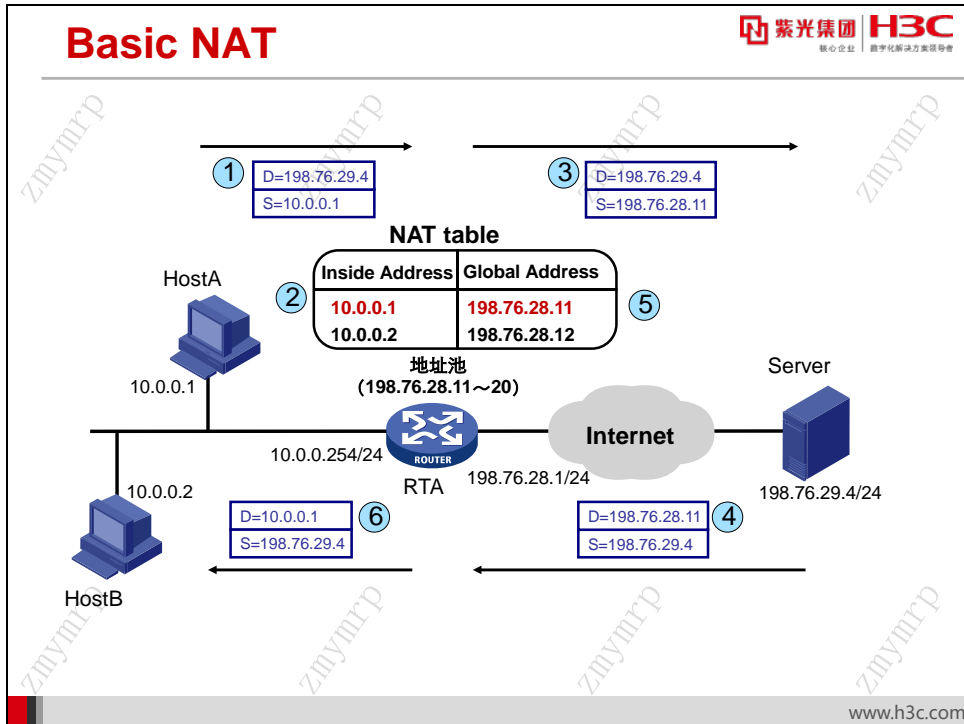
图中是典型的 NAT 组网模型。网络被划分为私网（Private Network）和公网（Public Network）两部分，各自使用独立的地址空间（Address realm）。私网使用私有地址 10.0.0.0/24，而公网节点均使用 Internet 地址。为了使私网客户端 HostA 和 HostB 能够访问 Internet 上的服务器 Server（IP 地址为 198.76.29.4），在网络边界部署一台 NAT 设备（NAT device）用于执行地址转换。

在讲述 NAT 原理的过程中，会频繁使用一些与 NAT 相关的常用术语：

- **公网（Public Network）：**指使用 IANA 分配的公有 IP 地址空间的网络，或者在互连的两个网络中不需要作地址转换的一方。在讨论 NAT 时，公网也常常被称为全局网络（Global Network）或外网（External Network）。相应地，公网节点使用的地址称为公有地址（Public Address）或全局地址（Global Address）；
- **私网（Private Network）：**指使用独立于外部网络的私有 IP 地址空间的内部网，或者在互连的两个网络中，需要作地址转换的一方。在讨论 NAT 时，私网也常常被称为本地网络（Local Network）或内网（Internal Network）。相应地，私网节点使用的地址称为私有地址（Private Address）或本地地址（Local Address）；
- **NAT 设备（NAT device）：**介于公网和私网之间的设备，负责执行公有地址和私有地址之间的转换。通常由一台路由器来完成这个任务；
- **TU Port：**指与某个 IP 地址相关联的 TCP/UDP 端口，如 HTTP 的 TU Port 为 80；
- **地址池（Address Pool）：**一般为公有地址的集合。配置动态地址转换后，NAT 设备从地址池中为私网用户动态分配公有地址。

28.3 Basic NAT

28.3.1 Basic NAT 原理



Basic NAT 是最简单的一种地址转换方式，只对数据包的 IP 层参数进行转换。

在上图中，私网主机 HostA（10.0.0.1）需要访问公网的 Server（198.76.29.4），在 RTA 上配置 NAT，地址池为 198.76.28.11~198.76.28.20，地址转换过程如下：

1) HostA 产生目的地为 Server 的 IP 报文，发送给缺省网关 10.0.0.254，报文源地址为 10.0.0.1，目的地址为 198.76.29.4；

2) RTA 收到 IP 报文后，查找路由表，将 IP 报文转发至出接口，由于在出接口上配置了 NAT，因此 RTA 需要将源地址 10.0.0.1 转换成公网地址；

3) RTA 从地址池中查找第一个可用的公网地址，本例中为 198.76.28.11，用这个地址替换数据包的源地址，转换后的报文源地址为 198.76.28.11，目的地址为 198.76.29.4。同时，RTA 在自己的 NAT 表（NAT Table）中添加一个表项（10.0.0.1→198.76.28.11），记录由内部地址 10.0.0.1 到全局地址 198.76.28.11 的映射。然后 RTA 将报文转发给目的地 198.76.29.4；

4) Server 收到 IP 报文后做相应的处理；

5) Server 发送回应报文时，报文的源地址为 198.76.29.4，目的地址为 198.76.28.11；

6) RTA 收到 IP 报文，发现报文的目的地址 198.76.28.11 在 NAT 地址池内，遂检查 NAT 表，找到相应表项（10.0.0.1→198.76.28.11）后，用私网地址 10.0.0.1 替换公网地址


198.76.28.11，转换后的报文源地址为 198.76.29.4，目的地址为 10.0.0.1。然后 RTA 将报文转发给 HostA：

7) HostA 收到 IP 报文，地址转换过程结束。

如果在这个过程中，HostB 也同时要访问 Server，则 RTA 将会从地址池中为其分配另一个可用公网地址（本例中为 198.76.28.12），并在 NAT 表中添加一个相应的表项（10.0.0.2→198.76.28.12），记录 HostB 的私网地址 10.0.0.2 到公网地址 198.76.28.12 的映射。

28.3.2 配置 Basic NAT

配置 Basic NAT



- **配置ACL**
 - 用于判断哪些数据包的地址应被转换
 - 被ACL允许（permit）的报文将被进行NAT转换，被拒绝（deny）的报文将不会被转换
- **配置地址池**
 - **nat address-group group-number**
 - **address start-address end-address**
- **配置地址转换**
 - **nat outbound acl-number address-group group-number no-pat**

www.h3c.com

配置 Basic NAT 时，首先需要配置一个公网地址池，为私网用户动态分配公网地址。地址池是一些连续的公网 IP 地址集合。地址池的配置由 **nat address-group** 命令完成。

操作	命令
配置地址池	[H3C] nat address-group group-number [H3C-nat-address-group-1] address start-address end-address
删除地址池	[H3C] undo nat address-group group-number

如果地址池的起始 IP 地址 *start-address* 与结束 IP 地址 *end-address* 相同，则表示地址池只有一个地址。

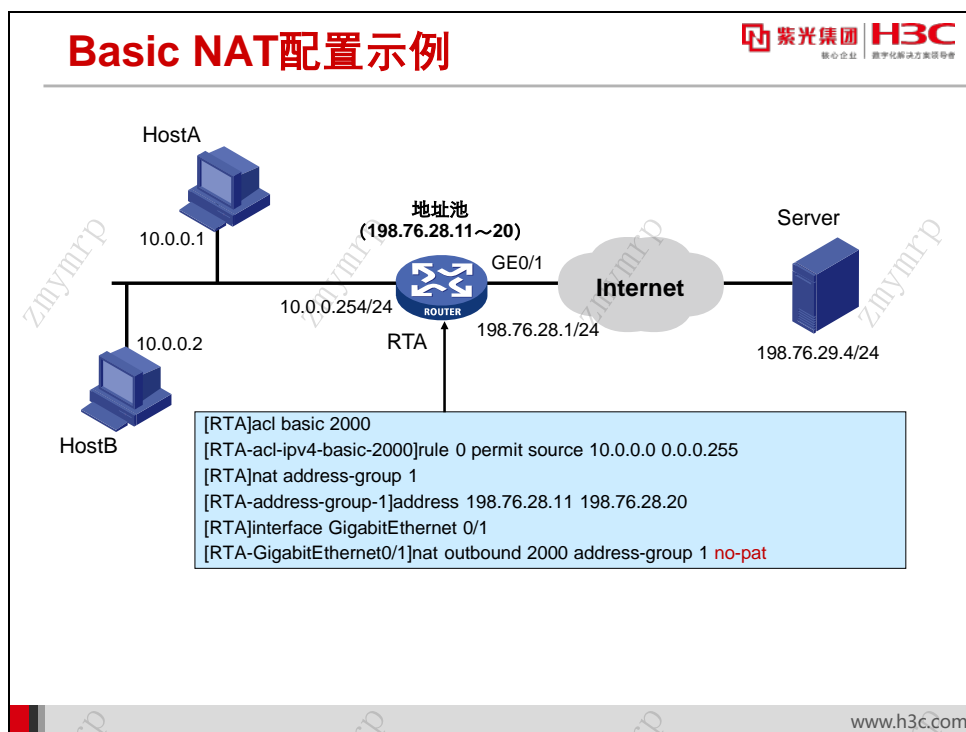
然后要配置一个 ACL，用于匹配“需要被 NAT 转换的报文”。ACL 的配置与用于包过滤的 ACL 没有区别。被 ACL 允许（permit）的报文将被进行 NAT 转换；被拒绝（deny）的报文不会被转换。

最后要在通向公网的出接口上配置 ACL 与 NAT 地址池的关联，这样，凡是经由此接口向外转发并被某 ACL 规则允许（permit）的数据报文均会被进行地址转换，其源地址会被转换成地址池内的某个可用的公网地址。这一步通过 **nat outbound** 命令实现。

操作	命令
配置网络地址转换	[H3C-GigabitEthernet0/0] nat outbound acl-number address-group group-number no-pat
取消网络地址转换	[H3C-GigabitEthernet0/0] undo nat outbound acl-number address-group group-number no-pat

关键字 **no-pat** 表示这是一个 Basic NAT 转换，即只做一对一的地址转换，且只转换数据包的地址而不转换端口。

28.3.3 Basic NAT 配置示例



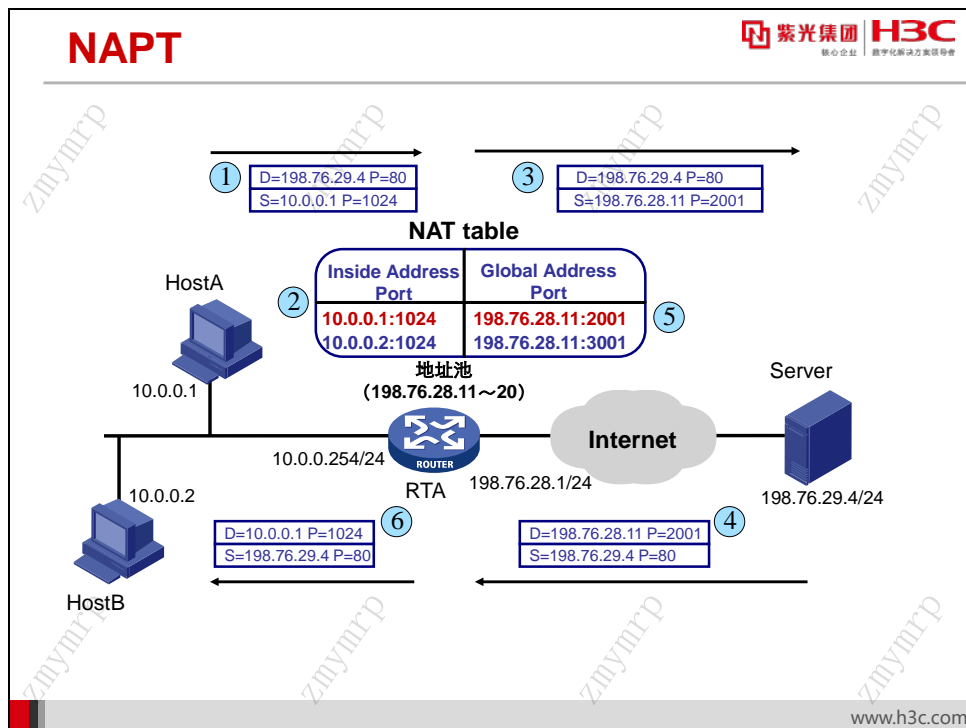
在本例中，私网客户端 HostA、HostB 需要访问公网服务器。通过 ACL 定义一条 rule，匹配源地址属于 10.0.0.0/24 网段的数据。在 RTA 上配置公网地址池 address-group 1，地址范围为 198.76.28.11-198.76.28.20，动态为 HostA、HostB 分配公网地址。最后在接口出方向上应用 NAT，将地址池 1 与 ACL 相关联。

路由器 RTA 收到 HostA 始发的流量（源 IP 地址为 10.0.0.1，目的 IP 地址为 198.76.29.4），匹配 ACL 2000 成功后，会将源地址 10.0.0.1 转换成公网地址并在内部建立地址转换表（10.0.0.1:1024→198.76.28.11:1024），公网地址按一定的方式在地址池中选取，比如按地址由小到大方式选取。当 RTA 收到 Server 端始发的回程流量（源 IP 地址为 198.76.29.4，目的

IP 地址为 198.76.28.11)后, 查找地址转换表, 根据表项(10.0.0.1:1024→198.76.28.11:1024)将目的地址 198.76.28.11 转换成 10.0.0.1 后, 再依照路由器路由表转发。

28.4 NAT

28.4.1 NAT 原理



在 Basic NAT 中，内部地址与外部地址存在一一对应关系，即一个外部地址在同一时刻只能被分配给一个内部地址。它只解决了公网和私网的通信问题，并没有解决公有地址不足的问题。

NAPT（Network Address Port Translation，网络地址端口转换）对数据包的 IP 层和传输层信息同时进行转换，可以显著提高公有 IP 地址的利用效率。

在上图中，私网主机 HostA（10.0.0.1）需要访问公网的 Server（198.76.29.4）的 WWW 服务。在 RTA 上配置 NAPT，地址池为 198.76.28.11~198.76.28.20，地址转换过程如下：

1) HostA 产生目的地为 Server 的 IP 报文，发送给缺省网关 RTA，报文源地址/端口为 10.0.0.1:1024，目的地址/端口为 198.76.29.4:80；

2) RTA 收到 IP 报文后，查找路由表，将 IP 报文转发至出接口，由于在出接口上配置了 NAPT，因此 RTA 需要将私网地址/端口 10.0.0.1:1024 转换成公网地址/端口；

3) RTA 从地址池中查找第一个可用的公网地址，本例中为 198.76.28.11，用这个地址替换数据包的源地址；并查找该公网地址的一个可用端口，本例中为 2001，用这个端口替换源端口。转换后的报文源地址/端口为 198.76.28.11:2001，目的地址/端口为 198.76.29.4:80。同时，RTA 在自己的 NAT 表（NAT Table）中添加一个表项（10.0.0.1:1024→198.76.28.11:2001），

记录由内部地址/端口 10.0.0.1:1024 到全局地址/端口 198.76.28.11:2001 的映射。然后 RTA 将报文转发给目的地 198.76.29.4;

4) Server 收到 IP 报文后做相应的处理;

5) Server 处理完报文后, 发送回应报文, 报文源地址/端口为 198.76.29.4:80, 目的地址/端口为 198.76.28.11:2001;

6) RTA 收到 IP 报文, 发现报文的地址在 NAT 地址池内, 遂检查 NAT 表项, 找到相应表项 (10.0.0.1:1024→198.76.28.11:2001), 用私网地址/端口 10.0.0.1:1024 替换公网地址/端口 198.76.28.11:2001, 然后转发给 HostA。转换后的报文源地址/端口为 198.76.29.4:80, 目的地址/端口为 10.0.0.1:1024;


7) HostA 收到 IP 报文, 地址转换过程结束。

如果在这个过程中, HostB 也同时要访问 Server, 则 RTA 可以从地址池中为其分配同一个可用公网地址 198.76.28.11, 但分配另一个端口 3001, 并在 NAT 表中添加一条相应的表项 (10.0.0.2:1024→198.76.28.11:3001), 记录 HostB 的私网地址/端口到公网地址/端口的映射。

通过这种方法, NAPT 提供了公网地址复用的能力。地址池中的公网地址可以大大少于需要访问公网的私网主机数, 从而节约了公网地址。

28.4.2 配置 NAPT

配置 NAPT



紫光集团 H3C
核心企业 数字化转型方案领导者

- **配置 ACL**
 - 用于判断哪些数据包的地址应被转换
 - 被 ACL 允许 (permit) 的报文将被进行 NAT 转换, 被拒绝 (deny) 的报文将不会被转换
- **配置地址池**
 - **nat address-group group-number**
 - **address start-address end-address**
- **配置地址转换**
 - **nat outbound acl-number address-group group-number**

www.h3c.com

NAPT 的配置方法与 Basic NAT 基本相同。

首先要配置一个公网地址池，为私网用户动态分配公网地址和端口，地址池是一些连续的公网 IP 地址集合。地址池的配置通过 **nat address-group** 命令完成。

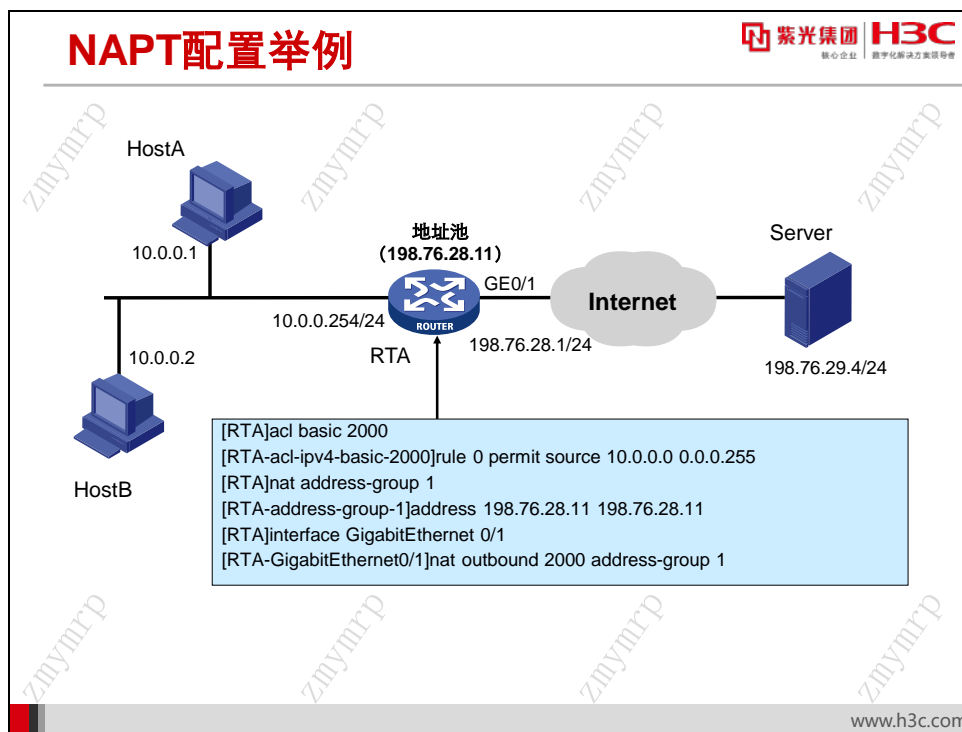
然后要配置一个 ACL，用于筛选出“需要被 NAT 转换的报文”。

最后要在通向公网的出接口上配置 ACL 与 NAT 地址池的关联。这一步通过 **nat outbound** 命令实现。

操作	命令
配置网络地址转换	[H3C-GigabitEthernet0/0] nat outbound acl-number address-group group-number
取消网络地址转换	[H3C-GigabitEthernet0/0] undo nat outbound acl-number address-group group-number

NAPT 与 Basic NAT 的配置区别在于，前者使用 **nat outbound** 命令时不加 **no-pat** 关键字，表示允许端口转换；而后者加 **no-pat** 关键字，表示禁止端口转换。

28.4.3 NAPT 配置示例




在本例中，私网客户端 HostA、HostB 需要访问公网服务器。通过 ACL 定义一条 rule，匹配源地址属于 10.0.0.0/24 网段的数据。在 RTA 上配置公网地址池 address-group 1，地址内只有一个公网地址 198.76.28.11，动态为 HostA、HostB 分配公网地址和协议端口。最后在接口出方向上应用 NAT，将地址池 1 与 ACL 相关联。

HostA 和 HostB 的源地址都会转换成同一个公网地址 198.76.28.11，不同的源端口号。这样 RTA 在收到 Server 始发回程数据流后，就能根据数据流中的目的端口号来区分转换后的目的地址为 10.0.0.1 还是 10.0.0.2。

28.5 Easy IP

28.5.1 Easy IP 原理

Easy IP



- NAT设备直接使用出接口的IP地址作为转换后的源地址
- 不用预先配置地址池
- 工作原理与普通NAPT相同，是NAPT的一种特例
- 适用于拨号接入Internet或动态获得IP地址的场合


www.h3c.com

在标准的 NAPT 配置中需要创建公网地址池，也就是必须预先得到确定的公网 IP 地址范围。而对于拨号接入这类常见的上网方式，其公网 IP 地址是由运营商方面动态分配的，无法事先确定，标准的 NAPT 无法为其做地址转换。


要解决这个问题，就要引入 Easy IP 特性。Easy IP 也称为基于接口的地址转换。在地址转换时，直接使用相应接口的 IP 地址作为转换后的源地址。Easy IP 适用于拨号接入 Internet 或动态获得 IP 地址的场合。

28.5.2 配置 Easy IP

配置Easy IP


核心企业 数字化转型方案领导者

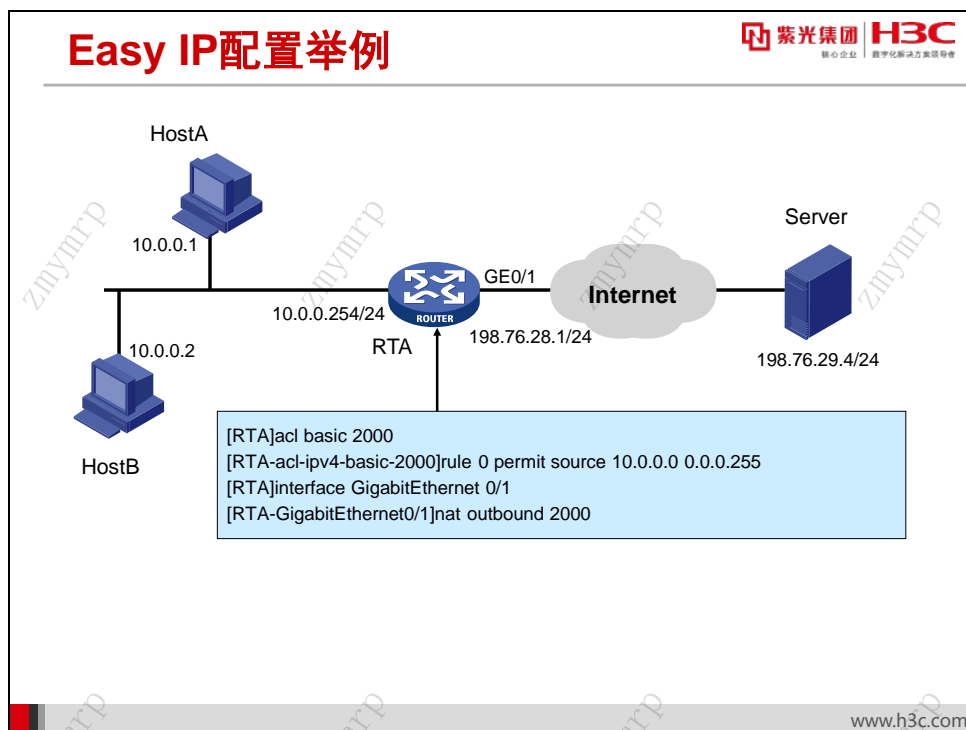
- 配置ACL
 - 用于判断哪些数据包的地址应被转换
 - 被ACL允许（**permit**）的报文将被进行NAT转换，被拒绝（**deny**）的报文将不会被转换
- 配置地址转换
 - **nat outbound** *acl-number*

www.h3c.com

Easy IP 的配置非常简单，无需配置地址池，只需在 NAT 设备通向公网的出接口的接口视图下使用 **nat outbound** 命令，将 ACL 与接口关联起来即可。

操作	命令
配置网络地址转换	[H3C-GigabitEthernet0/0] nat outbound <i>acl-number</i>
取消网络地址转换	[H3C-GigabitEthernet0/0] undo nat outbound <i>acl-number</i>

28.5.3 Easy IP 配置示例



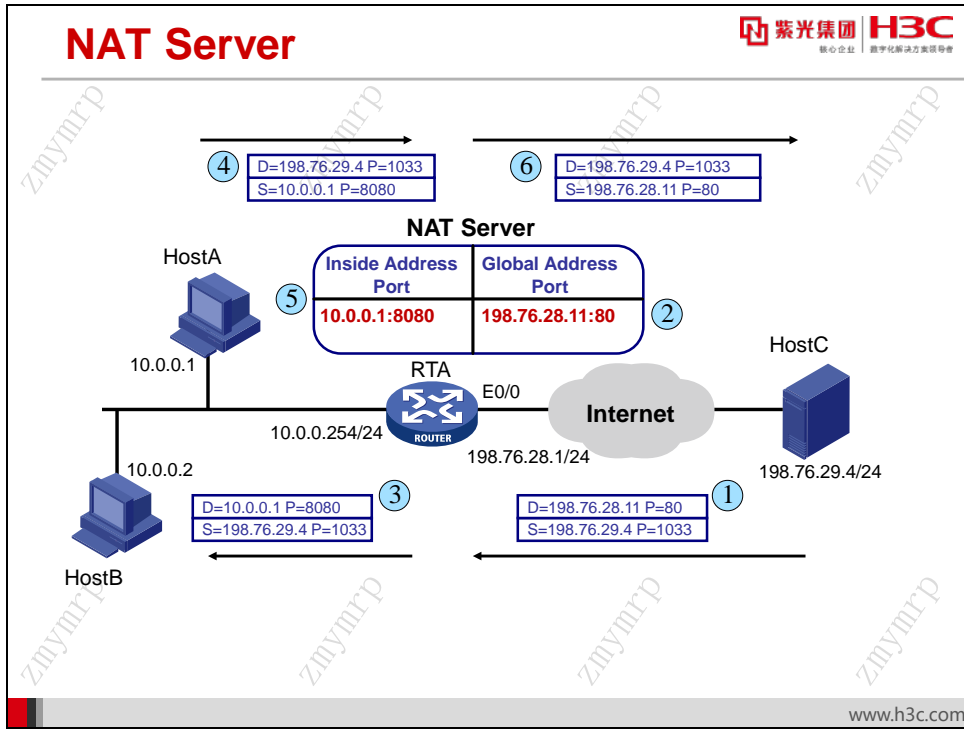
在本例中，私网客户端 HostA、HostB 需要访问公网服务器。通过 ACL 定义一条 rule，匹配源地址属于 10.0.0.0/24 网段的数据，并在接口出方向上应用 NAT，将其与 ACL 相关联，使用公网接口 IP 地址动态为 HostA、HostB 分配公网地址和协议端口。

注意：

在前述的几个例子中，如果 Server 端首先发起连接，是无法与 Host 端建立通信的，因为此时在 RTA 中并没有生成 NAT 转发表项。必须等待 Host 发起连接，RTA 建立起 NAT 转发表项后，Server 才能主动与 Host 进行通信。

28.6 NAT Server

28.6.1 NAT Server 原理



从 Basic NAT 和 NAPT 的工作原理可见，NAT 表项由私网主机主动向公网主机发起访问而触发建立，公网主机无法主动向私网主机发起连接。因此 NAT 隐藏了内部网络的结构，具有屏蔽内部主机的作用。但是在实际应用中，在使用 NAT 的同时，内部网络可能需要对外提供服务，例如 Web 服务、FTP 服务等，常规的 NAT 就无法满足要求了。

为了满足公网客户端访问私网内部服务器的需求，需要引入 NAT Server 特性，将私网地址/端口静态映射成公网地址/端口，以供公网客户端访问。当然 NAT Server 并不是一种独立的技术，只是 Basic NAT 和 NAPT 的一种具体应用而已。

本图中，HostA 的私网地址为 10.0.0.1，由端口 8080 提供 Web 服务，在对公网提供 Web 服务时要求端口号为 80。配置时应在 NAT 设备上启用 NAT Server，将私网 IP 地址和端口 10.0.0.1:8080 映射成公网 IP 地址和端口 198.76.28.11:80，这样公网主机 HostC 便可以通过 198.76.28.11:80 访问 HostA 的 Web 服务。

28.6.2 配置 NAT Server

配置 NAT Server



紫光集团 H3C
核心企业 数字化转型方案领导者

● NAT Server 配置命令

→ **nat server** [**protocol** *pro-type*] **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } [*global-port*] [**vpn-instance** *global-vpn-instance-name*] **inside** *local-address* [*local-port*] [**vpn-instance** *local-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**reversible**] [**rule** *rule-name*] [**disable**] [**counting**]

www.h3c.com

配置 NAT Server 时，需要指定协议类型、公网 IP 地址和端口、私网 IP 地址和端口，这些配置通过在通向公网的出接口的接口视图下使用 **nat server** 命令实现。

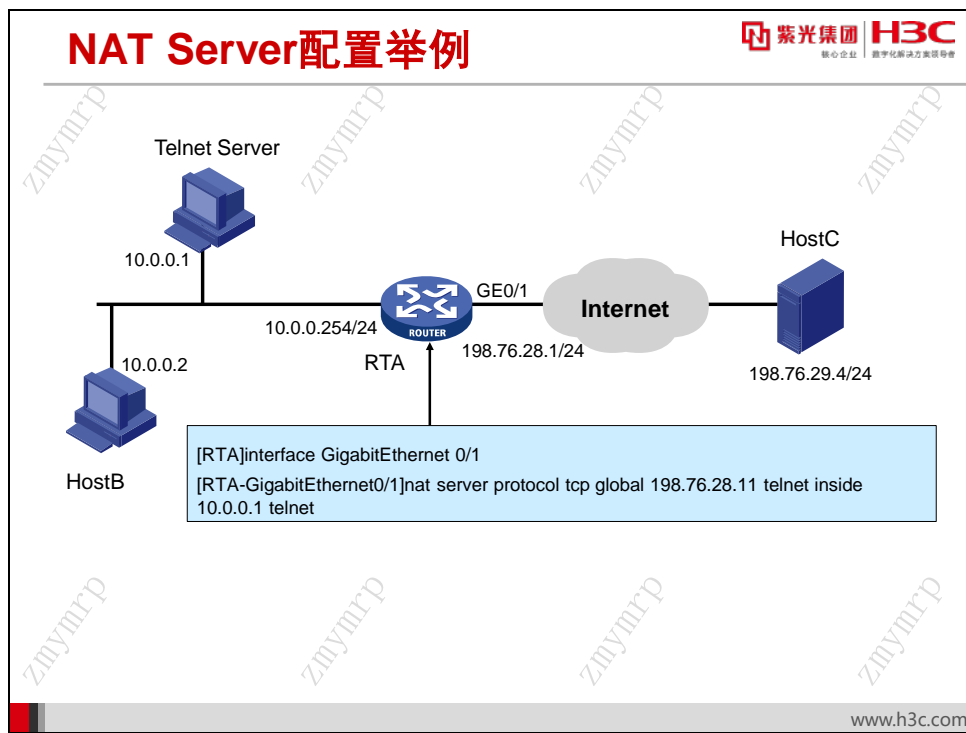
操作	命令
配置一个内部服务器	<pre>[H3C-GigabitEthernet0/0] nat server [protocol pro-type] global { global-address current-interface interface interface-type interface-number } [global-port] [vpn-instance global-vpn-instance-name] inside local-address [local-port] [vpn-instance local-vpn-instance-name] [acl { ipv4-acl-number name ipv4-acl-name }] [reversible] [rule rule-name] [disable] [counting]</pre>
删除一个内部服务器	<pre>[H3C-GigabitEthernet0/0] undo nat server [protocol pro-type] global { global-address current-interface interface interface-type interface-number } [global-port] [vpn-instance global-vpn-instance-name] inside local-address [local-port] [vpn-instance local-vpn-instance-name] [acl { ipv4-acl-number name ipv4-acl-name }] [reversible] [rule rule-name] [disable] [counting]</pre>

其中主要的参数含义如下：

- **protocol pro-type**: 指定协议类型。只有当协议类型是 TCP、UDP 协议时，配置的内部服务器才能带端口参数。如果不指定协议类型，则表示对所有协议类型的报文都生效。用数字表示时，取值范围为 1~255；用协议名称表示时，取值包括 **icmp**、**tcp** 和 **udp**；
- **global**: 指定服务器向外提供服务的外网信息；
- **global-address**: 内部服务器向外提供服务时对外公布的外网 IP 地址；
- **current-interface**: 使用当前接口的主用 IP 地址作为内部服务器的外网地址，即实现 Easy IP 方式的内部服务器；
- **interface interface-type interface-number**: 表示使用指定接口的主用 IP 地址作为内部服务器的外网地址，即实现 Easy IP 方式的内部服务器。**interface-type interface-number** 表示接口类型和接口编号。目前只支持 Loopback 接口。
- **global-port**: 内部服务器的外网端口号。用数字表示时，取值范围为 1~65535（FTP 数据端口号 20 除外）；用协议名称表示时，为 1~15 个字符的字符串，例如 **http**、**telnet** 等；
- **vpn-instance global-vpn-instance-name**: 对外公布的外网地址所属的 VPN 实例。**global-vpn-instance-name** 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示对外公布的外网地址不属于任何一个 VPN 实例。
- **inside**: 指定服务器的内网信息；
- **local-address**: 服务器的内网 IP 地址；
- **local-port**: 内部服务器的内网端口号，缺省值以及取值范围的要求和 **global-port** 的规定一致；
- **vpn-instance local-vpn-instance-name**: 内部服务器所属的 VPN 实例。**local-vpn-instance-name** 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示内部服务器不属于任何一个 VPN 实例；
- **acl**: 指定 ACL 的编号或名称。若指定了该参数，则表示与指定的 ACL permit 规则匹配的报文才可以使用内部服务器的映射表进行地址转换；
- **reversible**: 表示支持私网侧内部服务器主动访问外网。内部服务器主动访问外网时，将私网地址转换为内部服务器向外提供服务的外网 IP 地址；
- **rule rule-name**: NAT 规则的名称，取值范围为 1~63 个字符的字符串，区分大小写，不能包括“\”、“/”、“:”、“*”、“?”、“<”、“>”、“|”、“”和“@”。如果不指定该参数，则表示该规则无名称；
- **disable**: 表示禁用该地址转换映射。如果不指定该参数，则地址转换映射处于启用状态；

- **counting**: 开启 NAT 转换计数功能，即对每一次首报文地址转换进行计数。

28.6.3 NAT Server 配置示例

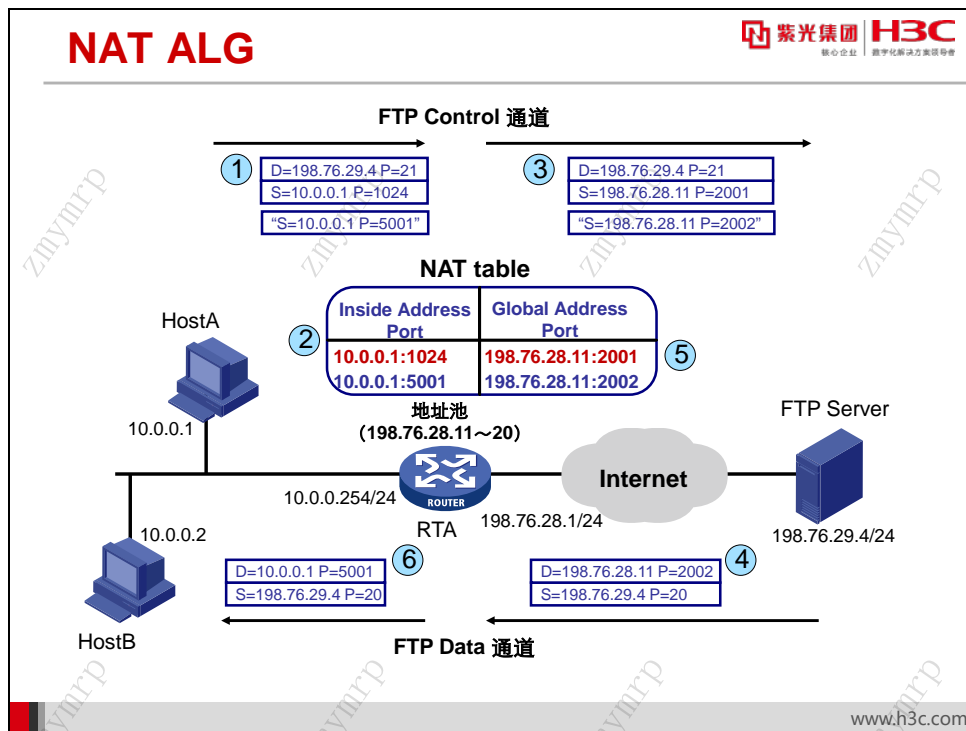


在本例中，HostA 是一台 Telnet Server，私网地址为 10.0.0.1，由端口 23 提供 Telnet 服务，在 RTA 上为 HostA 静态映射公网地址 198.76.28.11 和协议端口。配置如下即可：

```

[RTA]interface GigabitEthernet 0/1
[RTA-GigabitEthernet0/1]nat server protocol tcp global 198.76.28.11 telnet inside 10.0.0.1 telnet
  
```

28.7 NAT ALG



传统 NAT (Basic NAT 和 NAT) 只能识别并修改 IP 报文中的 IP 地址和 TU Port 信息, 不能修改报文内部携带的信息, 因此对于一些在 IP 报文载荷 (Payload) 中内嵌网络底层信息 (IP 地址或 TU 端口等) 的协议——例如 FTP、H.323、SIP 等, 是无法正确转换的。

ALG 是传统 NAT 的增强特性。它能够识别应用层协议内嵌的网络底层信息, 在转换 IP 地址和 TU Port 的同时, 对应用层数据中的网络底层信息进行正确转换。

下面以 FTP 的 Active 模式为例详细说明 ALG 的处理过程。

FTP 是一种基于 TCP 的协议, 用于在客户端和服务端间传输文件。FTP 协议工作时建立 2 个通道: Control 通道和 Data 通道。Control 用于传输 FTP 控制信息, Data 通道用于传输文件数据。

在上图中, 私网主机 HostA (10.0.0.1) 需要访问公网 Server (198.76.29.4) 的 FTP 服务, 在 RTA 上配置 NAT, 地址池为 198.76.28.11~198.76.28.20, 地址转换过程如下:

1) HostA 发起到 Server 的 FTP Control 通道建立请求, 告诉 Server 自己使用 TCP 端口 5001 传输 Data, 报文源地址/端口为 10.0.0.1:1024, 目的地址/端口为 198.76.29.4:21, 携带数据 "Request command=PORT IP=10.0.0.1 port=5001";

2) RTA 收到 FTP 报文, 建立映射关系 (10.0.0.1:1024→198.76.28.11:2001), 转换源 IP 地址和 TCP 端口, 根据目的端口 21, RTA 识别出这是一个 FTP 报文, 因此还要检查应用层数据, 发现原始数据为 "Request command=PORT IP=10.0.0.1 port=5001", 遂为 Data 通道

(10.0.0.1:5001) 建立第二个映射关系 (10.0.0.1:5001→198.76.28.11:2002)，处理后的报文源地址/端口为 198.76.28.11:2001，目的地址/端口为 198.76.29.4:21，携带数据 “Request command=PORT IP=198.76.28.11 port=2002”；

3) Server 收到 FTP 报文，向客户端回应 command okay 报文，FTP Control 通道建立成功。同时 Server 根据应用层数据确定客户端 Data 通道的网络参数 (IP 地址为 198.76.28.11，TCP 端口为 2002)；

4) HostA 需要从 FTP 服务器下载文件，于是发起获取文件请求 (RETR file)。Server 收到请求后，发起到 HostA 的 Data 通道建立请求，目的 IP 地址/端口为 198.76.28.11:2002。IP 报文的源地址/端口为 198.76.29.4:20，目的地址/端口为 198.76.28.11:2002，携带 FTP 数据；

5) RTA 收到 FTP 数据包，查找地址转换表，根据表项 (10.0.0.1:5001→198.76.28.11:2002) 进行转换，转换后将数据包转发给 HostA，进行 FTP 文件下载。此时的 IP 报文源地址/端口为 198.76.29.4:20，目的地址/端口为 10.0.0.1:5001，携带数据为 FTP 数据。


当然完整的 FTP ALG 过程还涉及很多细节，包括 IP 报文长度、TCP 校验和、TCP 序号调整等，这里不再详述。

NAT 设备 ALG 支持的协议种类是有限的，常见的有 FTP、DNS、H.323、SIP 等。在实际网络环境中，有可能存在诸如 MSN、QQ 等非标准或新出现的应用，在早期的 NAT 实现中并没有集成这些应用的 ALG，从而无法支持这些应用。

ALG 故障的表现通常为大部分应用能够正常使用，而一些应用的部分或全部功能存在问题。如果碰到 ALG 故障，首先应该确定具体应用的种类，然后根据应用类型采取相应的措施。比较常见的应用可以通过升级 NAT 设备软件的方法尝试解决。

28.8 NAT的信息显示和调试

NAT的信息显示和调试



紫光集团 H3C
核心企业 数字化转型方案领导者

- 显示地址转换信息


```
<H3C> display nat { address-group group-number | all | outbound
port-block-group | server | statistics | session }
```
- 调试地址转换过程


```
<H3C> debugging nat { alg | config | event | packet acl number }
```
- 清除地址转换连接


```
<H3C> reset nat session
```

www.h3c.com

为了便于在 NAT 环境下迅速定位故障，系统为用户提供了功能强大的显示和调试的工具。

输入下列命令，可以查看地址转换状态：

```
<H3C> display nat { address-group group-number | all | outbound port-block-group |
server | statistics | session }
```

在用户视图下输入下列命令，可以调试地址转换过程：

```
<H3C> debugging nat { alg | config | event | packet acl number }
```

28.9 本章总结

本章总结

- NAT可以有限缓解IPv4地址短缺，并提高安全性
- Basic NAT实现私网地址与公网地址一对一转换
- NAPT实现私网地址与公网地址的多对一转换，而Easy IP适用于出接口地址无法预知的场合
- NAT Server使公网主机可以主动连接私网服务器获取服务
- 对FTP等上层应用需要作ALG处理

www.h3c.com