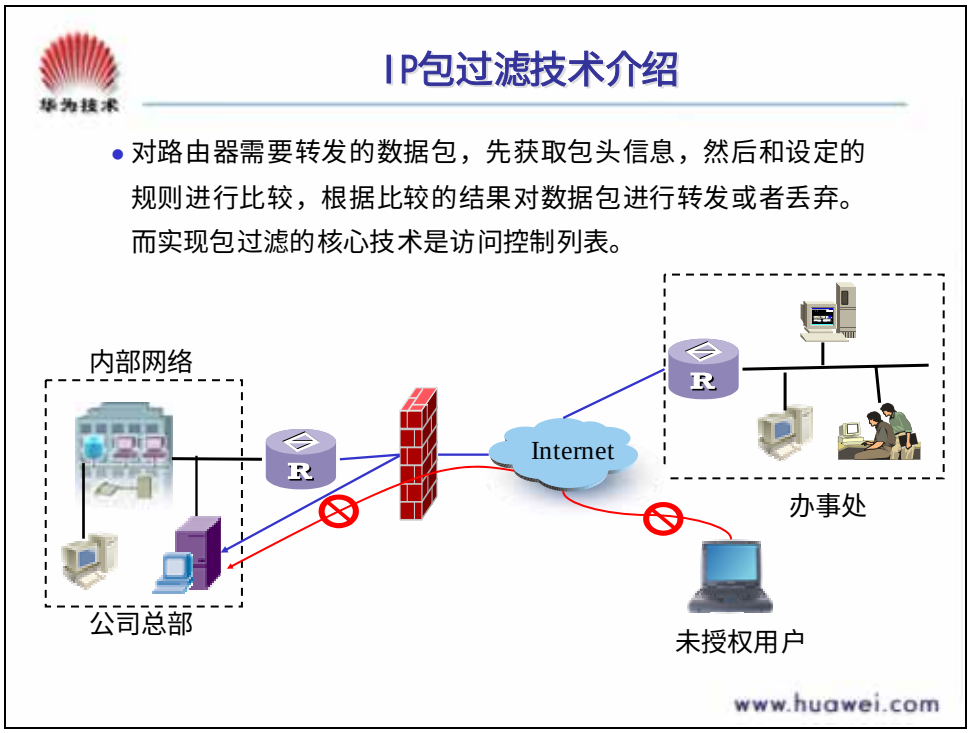
8.1 访问控制列表概述

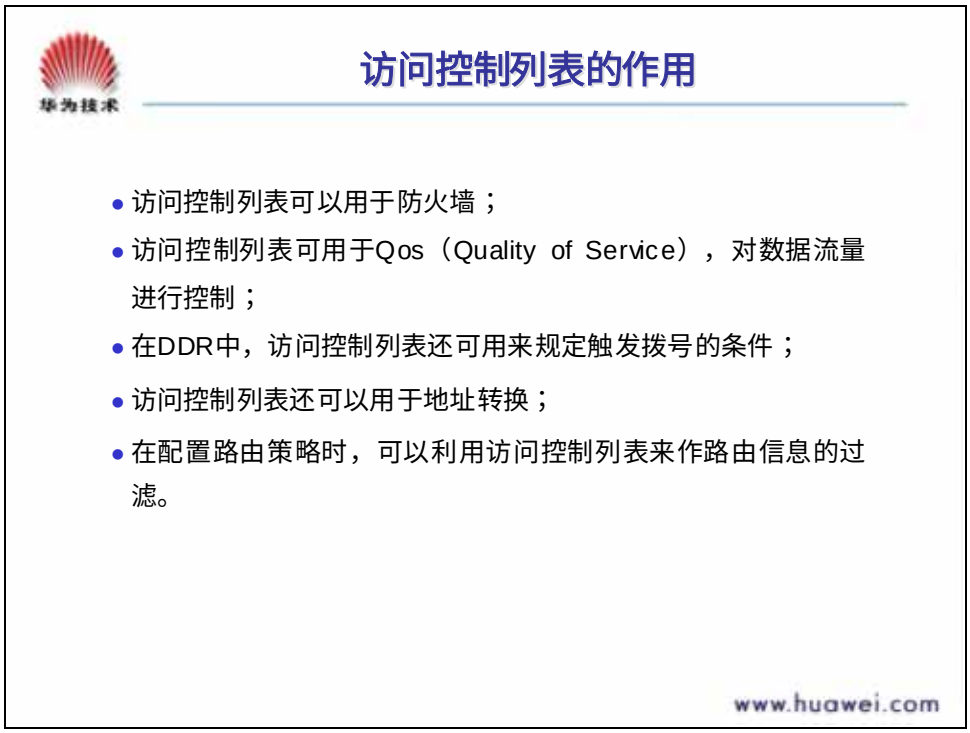
8.1.1 IP 包过滤技术介绍



随着越来越多的私有网络连入公有网，网络管理员们逐渐需要面对这样一个问题：如何在保证合法访问的同时，对非法访问进行控制。这就需要对路由器转发的数据包做出区分，即需要包过滤。路由器对需要转发的数据包，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、源端口号和目的端口等，然后与设定的规则进行比较，根据比较的结果对数据包进行转发或者丢弃。

包过滤技术是在路由器上实现防火墙的一种主要方式，而实现包过滤技术最核心内容就是使用访问控制列表。

8.1.2 访问控制列表的作用



访问控制列表具有区分数据包的功能，因此，它可以控制“什么样的数据包”可以做“什么样的事情”。例如：

将访问控制列表应用于防火墙，可以在保证合法用户访问的同时拒绝非法用户的访问。 也可以允许某种服务（如 Telnet)通过，而拒绝另一种服务（如 DNS)。

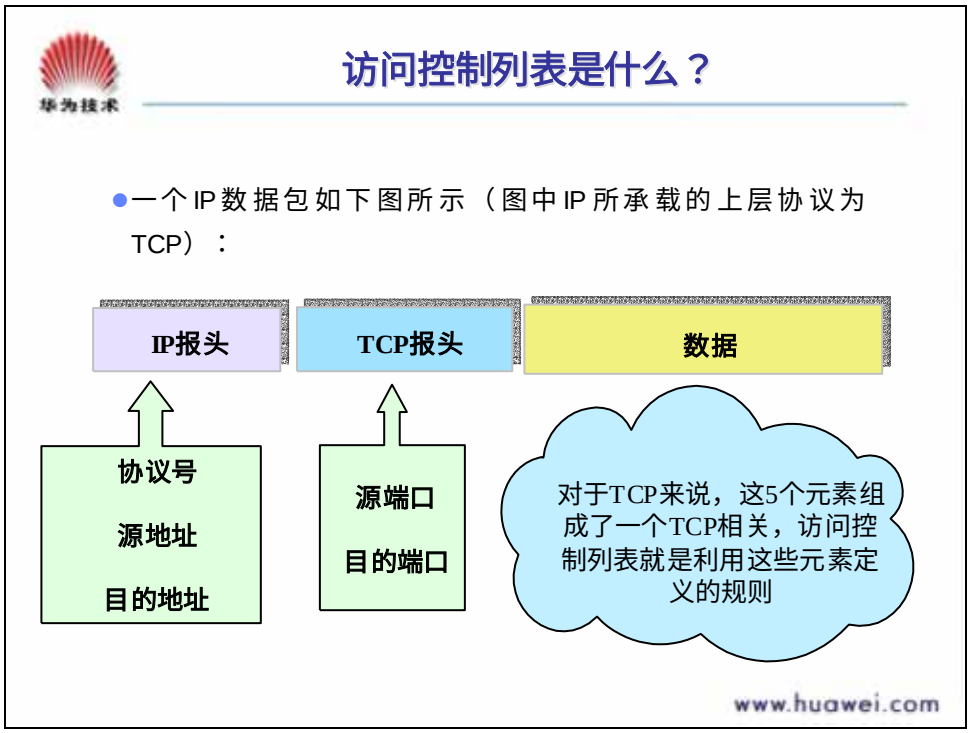
在 Qos 的应用中，我们可以利用访问控制列表对网络中的数据流量进行控制，重要的数据得到优先处理，不重要的数据后处理，不需要的数据被丢弃。

在 DDR 中我们则可以用访问控制列表来规定哪些数据包可以触发拨号（请参见 DDR 一章的内容)。

在地址转换中，访问控制列表还可以用来规定哪些数据包需要进行地址转换。

另外访问控制列表还广泛应用于路由策略中，主要用作路由信息的过滤。

8.1.3 访问控制列表原理



IP 数据包具有一定的特征，例如，对于每个 TCP 数据包，都包含有源地址、目的地址、协议号、源端口、目的端口，利用这 5 个元素就可以描述出一个数据包的特征。

访问控制列表利用的就是利用这些信息来定义规则，区分不同的数据包（例如所有源地址是 202.10.10.0 地址段的数据包、所有使用 Telnet 访问的数据包等等），路由器将在使能访问控制列表的接口上对所有的数据包进行规则的匹配检查。

例如，我们可以定义下面的规则：

- 允许 202.38.0.0/16 网段的主机使用协议 HTTP 访问 129.10.10.1。

  acl 101

  rule permit tcp source 202.38.0.0 0.0.255.255 destination 192.10.10.1 0.0.0.0 destination-port equal www

- 禁止从 202.110.0.0/16 网段发出的所有访问。

  acl 1

  rule deny source 202.110.0.0 0.0.255.255

- 不让任何主机使用 Telnet 登录。

  acl 101

rule deny tcp source any destination any destination-port equal telnet

- 某台主机 10.0.0.1/16 能通过 SMTP 把邮件发给我们，但是没有其他主机能这样做。

  acl 101

  rule permit tcp source 10.0.0.1 0.0.255.255 destination any destination-port equal smtp

  rule deny tcp any destination any destination-port equal smtp

然而，你不可以这样说：

- 这个用户能从外部远程登录，但是其它用户不能这样做。因为“用户名”不是访问控制列表所能辨认的信息。
- 你能发送这些文件而不能发送那些文件。因为“文件”也不是包过滤系统所能辨认的信息。

8.1.4 访问控制列表的分类

列表的种类	数字标识的范围
IP standard list	1－99
IP extended list	100－199

在配置访问控制列表时，我们必须定义一个序列号，并利用这个序列号来唯一的标识一条访问控制列表，同时我们也可以通过序列号来引用一条访问控制列表。当然，这个序列号必须保证在协议所允许的范围之内，通过定义序列号的范围，我们可以将访问控制列表分为如上图所示的两类。序列号的范围表示了它属于什么样的访问控制列表。例如：

acl 1

rule permit ip source 202.110.10.0 0.0.0.255

表示序号为 1 的访问控制列表，它是标准访问列表。

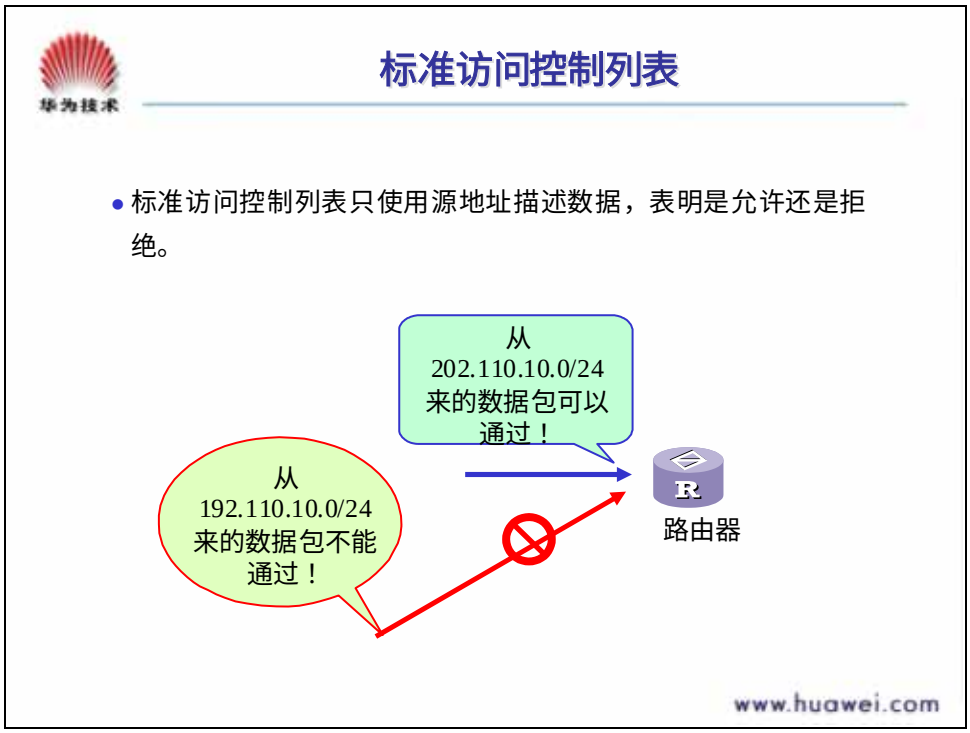
acl 100

rule deny udp source any destination any destination-port

表示序号为 100 的访问控制列表，它是扩展访问列表。

8.2 标准访问控制列表

8.2.1 标准访问控制列表概况

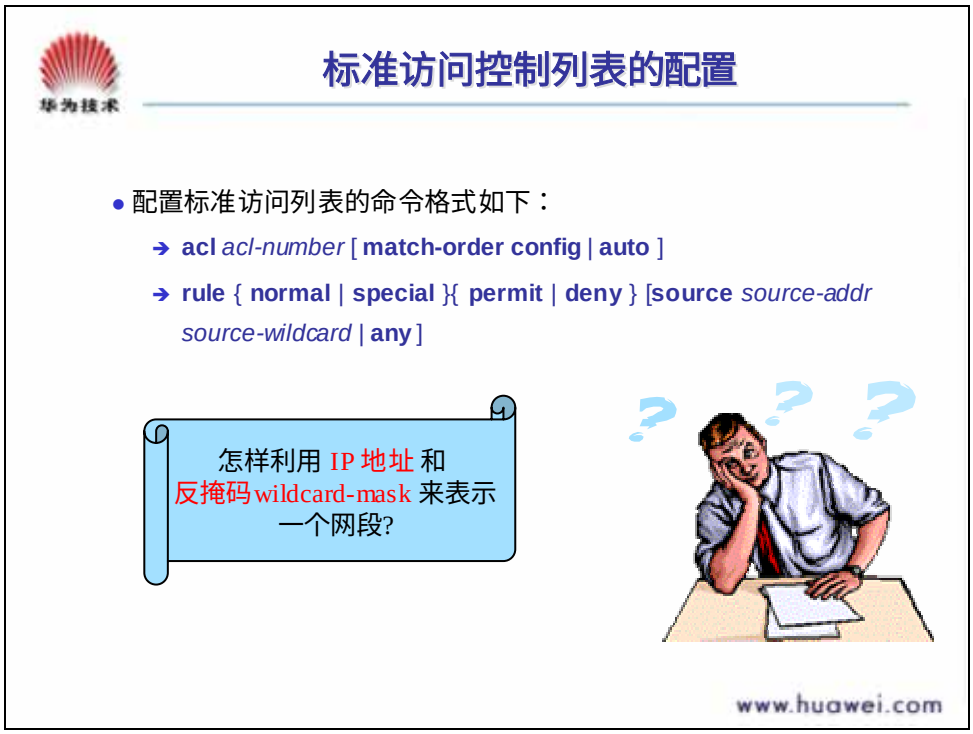


规则序列号范围在 1 到 99 之间的访问控制列表为标准列表。标准访问控制列表只是根据数据包的**源地址**对数据包进行区分。

例如在上图中，如果需要允许从 202.110.10.0 网段来的数据包通过，而拒绝从 192.110.10.0 网段来的数据通过，可以用标准访问控制列表表示：

```
acl 1
rule permit ip source 202.110.10.0 0.0.0.255
rule deny ip source 192.110.10.0 0.0.0.255
```

8.2.2 标准访问控制列表的配置命令



此命令格式表示：允许或拒绝来自指定网络的数据包，该网络由 IP 地址（source-address）和反掩码（source-wildcard）指定。其中：

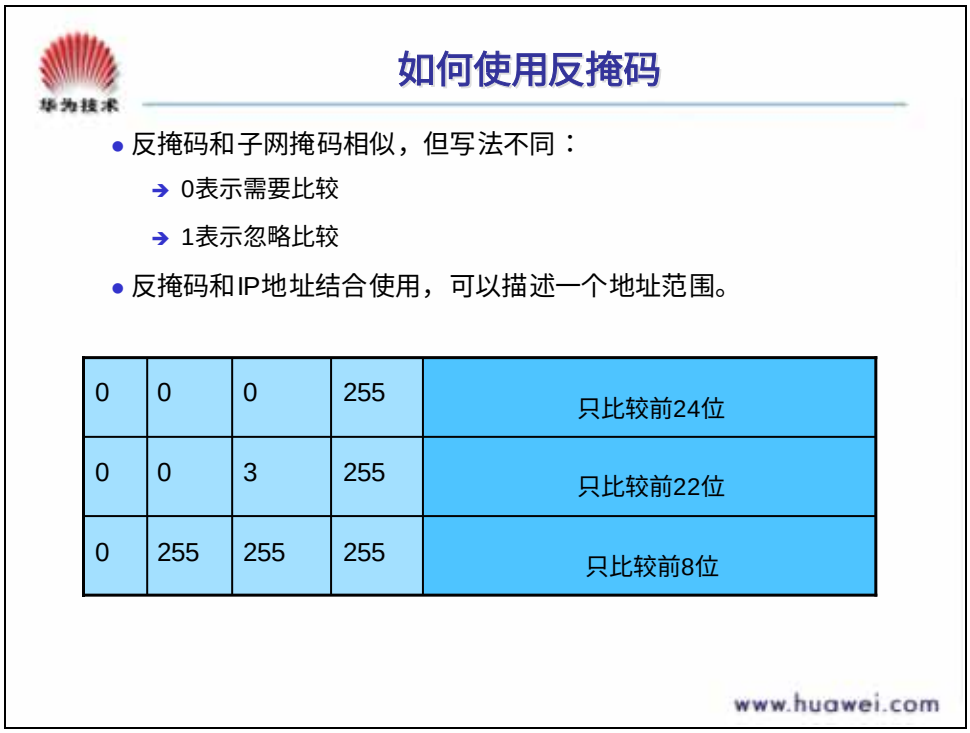
normal 和 special 表示该规则是在普通时间段中有效还是在特殊时间段中有效。

listnumber 为规则序号，标准访问列表的规则序号范围为 1-99。

permit 和 deny 表示如果满足条件则允许或禁止该数据包通过 。

source-address 和 source-wildcard 分别为 IP 地址和反掩码，用来指定某个网络。

8.2.3 反掩码简介



反掩码的作用和子网掩码很相似。通常情况下反掩码看起来很象一个颠倒过来的 IP 地址子网掩码，但是用法上是不一样的。IP 地址与反掩码的关系语法规定如下：在反掩码中相应位为 1 的地址中的位在比较中被忽略，为 0 的必须被检查。IP 地址与反掩码都是 32 位的数。

例如：192.168.0.1/22 网段

用子网掩码表示　192.168.0.1　255.255.252.0

用反掩码表示　192.168.0.1　0.0.3.255

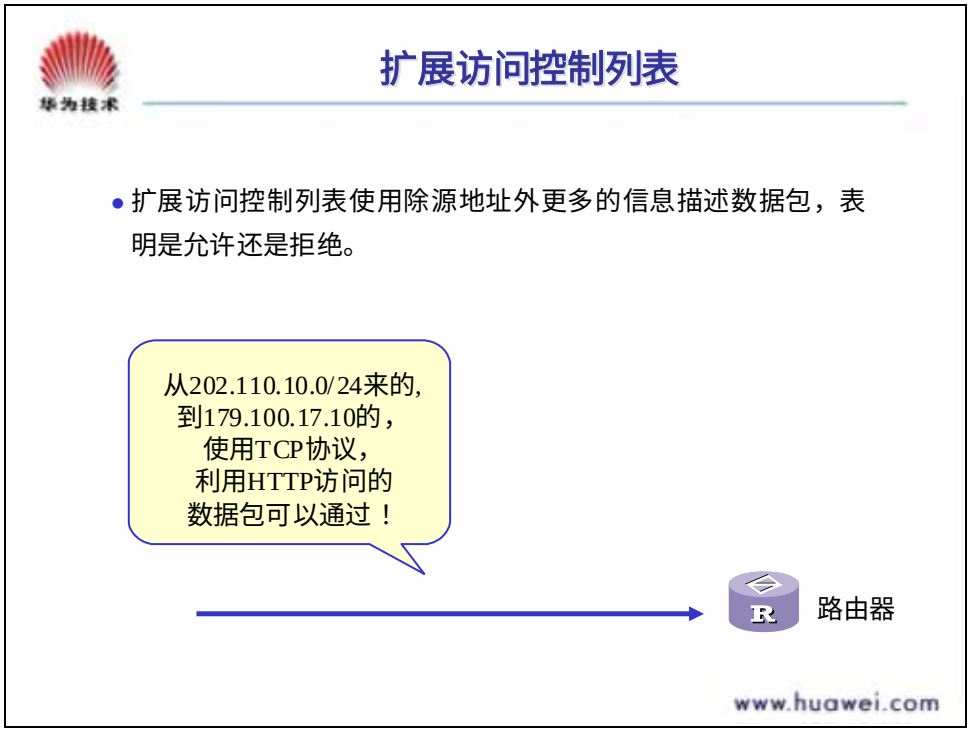
例如：允许从 202.110.10.0 网段来的数据包通过，而拒绝从 192.110.10.0 网段来的数据通过，可以用标准访问控制列表表示：

```
acl 1
rule permit source 202.110.10.0 0.0.0.255
rule deny 192.110.10.0 0.0.0.255
```

另外，对于任何地址（255.255.255.255），我们可以使用通配符 any 来代替，以便简化输入。

8.3 扩展访问控制列表

8.3.1 扩展访问控制列表概况



与标准访问控制列表不同的是，扩展访问控制列表使用数据包的源地址的同时，还使用目的地址和协议号（TCP、UDP 等）。

对于使用 TCP、UDP 协议传输的数据包还可以同时使用目的端口号来对数据包做出区分。

例如，利用扩展列表可以描述“从 202.110.10.0/24 的网段到 110.10.10.0/24 的网段的所有 IP 数据包是被拒绝的”，或者“从 202.110.10.0/24 网段到 110.10.10.0/24 网段的所有 Telnet（使用 TCP 协议的 23 端口）访问是被拒绝的”。它们到底如何表示？我们将从具体配置命令来进行介绍。

8.3.2 扩展访问控制列表的配置命令

扩展访问控制列表的配置命令

- 配置TCP/UDP协议的扩展访问列表：
  - rule { normal | special }{ permit | deny } { tcp | udp } [source *source-addr source-wildcard* | any] [source-port *operator port1* [*port2*]] [destination *dest-addr dest- wildcard* | any] [destination-port *operator port1* [*port2*]] [logging]
- 配置ICMP协议的扩展访问列表：
  - rule { normal | special }{ permit | deny } icmp [source *source-addr source-wildcard* | any] [destination *dest-addr dest- wildcard* | any] [icmp-type *icmp-type icmp-code*] [logging]
- 配置其它协议的扩展访问列表：
  - rule { normal | special }{ permit | deny } { ip | ospf | igmp | gre } [source *source-addr source-wildcard* | any] [destination *dest-addr dest- wildcard* | any] [logging]

www.huawei.com

normal 和 special 表示该规则是在普通时间段生效还是在特殊时间段有效，缺省的情况是在普通时间段。

listnumber 为访问控制列表序号，扩展访问控制列表的序号范围为 100-199。

permit 和 deny 表示允许或禁止满足该规则的数据包通过 。

protocol 可以指定为 0-255 之间的任一协议号（如 1 表示 ICMP 协议），对于常见协议（如 TCP 和 UDP、ICMP），可以直观地指定协议名，若指定为 IP ，则该规则对所有 IP 包均起作用。

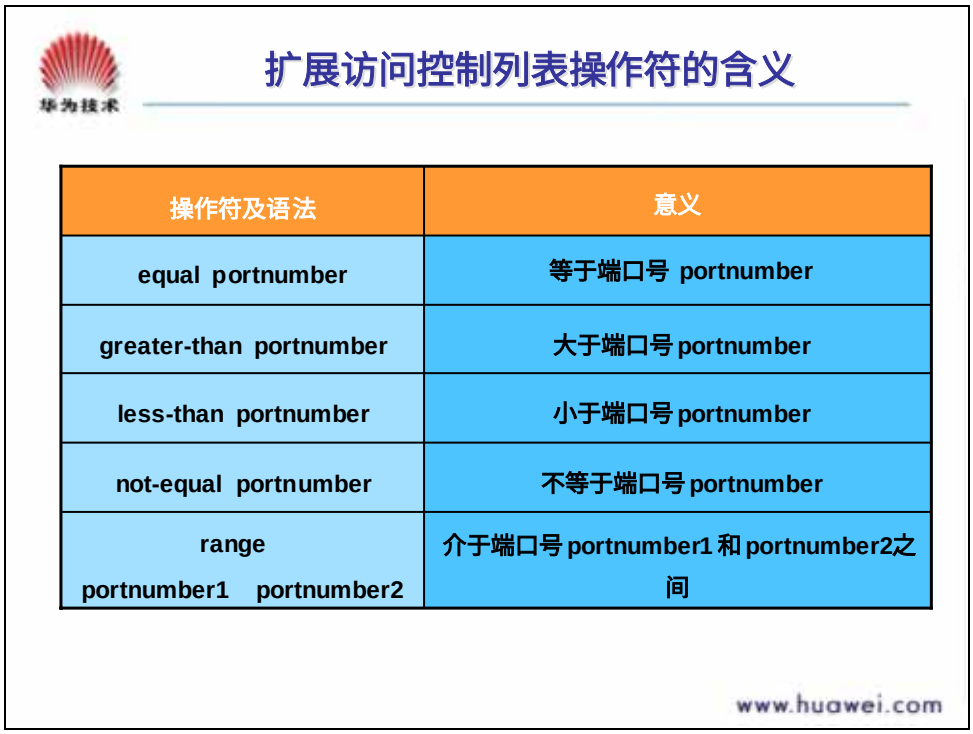
source -addr 和 source-wildcard 分别为源地址和源地址的通配符。

dest-address 和 dest-wildcard 分别为目的地址和目的地址的通配符。

如果 IP 地址指定为 any，则表示所有 IP 地址，而且不需配置指定相应的通配符。

Destination-port operator port1 - port2 用于指定端口范围，缺省为全部端口号 0-65535，只有 TCP 和 UDP 协议可以指定端口范围。operate 的意义如下页表所示。

8.3.3 扩展访问列表的操作符 operate 定义



操作符及语法	意义
equal portnumber	等于端口号 portnumber
greater-than portnumber	大于端口号 portnumber
less-than portnumber	小于端口号 portnumber
not-equal portnumber	不等于端口号 portnumber
range portnumber1 portnumber2	介于端口号 portnumber1 和 portnumber2之间

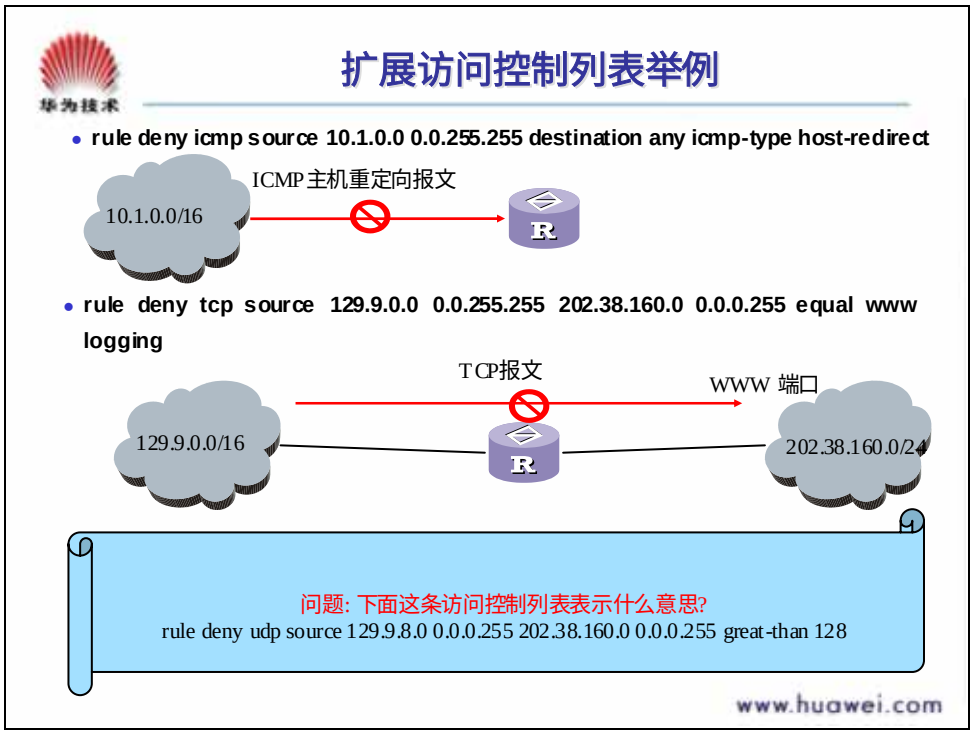
在访问控制列表的协议为 TCP 和 UDP 时，我们还可以在访问控制列表中定义端口的范围，以进行更精确的控制。上面的胶片中给出了利用操作符 operate 定义端口范围的语法及含义。在指定 portnumber 时，对于常用的端口号可以使用“助记符”代替。如 FTP、Telnet 等。下面是一个简单的例子：

acl 101

rule deny tcp source 129.9.0.0 0.0.255.255 destination 202.38.160.0 0.0.0.255 destination-port equal ftp

禁止 129.9.0.0 网段内的主机访问 202.38.160.0 网段内的主机的 ftp 端口（21）。

8.3.4 扩展访问控制列表的举例



下列表格所列为可能用到的各类端口号与助记符的对照表，供参考。

协议	助记符	意义及实际值
TCP	Bgp	Border Gateway Protocol (179)
	Chargen	Character generator (19)
	Cmd	Remote commands (rcmd, 514)
	Daytime	Daytime (13)
	Discard	Discard (9)
	Domain	Domain Name Service (53)
	Echo	Echo (7)
	Exec	Exec (rsh, 512)
	Finger	Finger (79)
	Ftp	File Transfer Protocol (21)
	Ftp-data	FTP data connections (20)
	Gopher	Gopher (70)
	Hostname	NIC hostname server (101)
	Irc	Internet Relay Chat (194)
	Klogin	Kerberos login (543)
	Kshell	Kerberos shell (544)
	Login	Login (rlogin, 513)
	Lpd	Printer service (515)
	Nntp	Network News Transport Protocol (119)
	Pop2	Post Office Protocol v2 (109)
	Pop3	Post Office Protocol v3 (110)
	Smtp	Simple Mail Transport Protocol (25)
	Sunrpc	Sun Remote Procedure Call (111)
	Syslog	Syslog (514)
	Tacacs	TAC Access Control System (49)
	Talk	Talk (517)
	Telnet	Telnet (23)

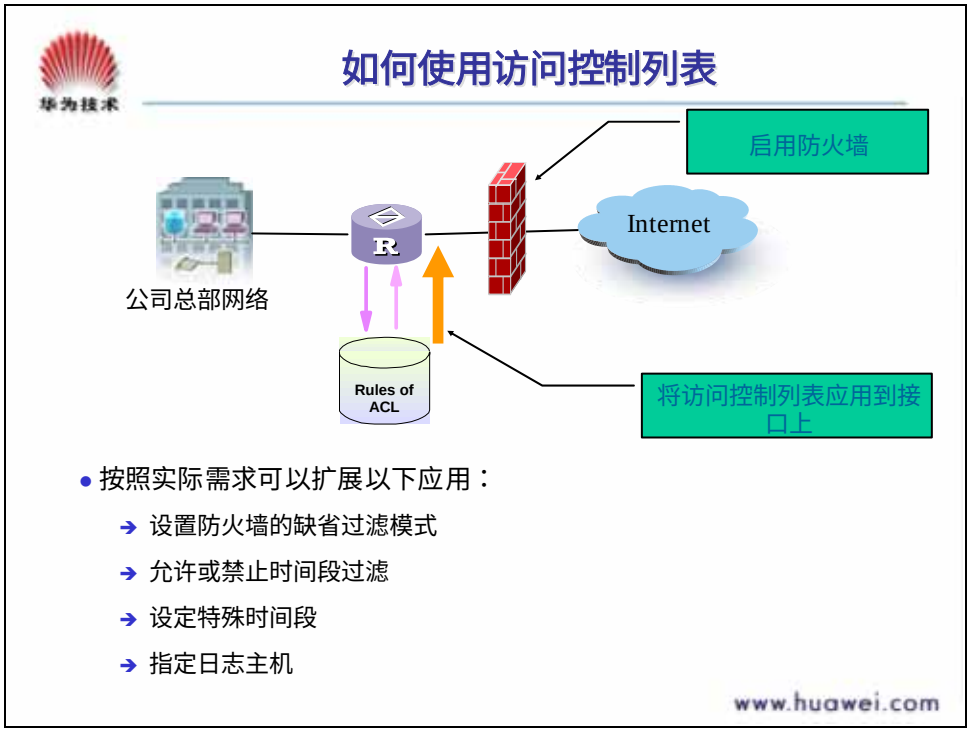
	Time	Time (37)
	Uucp	Unix-to-Unix Copy Program (540)
	Whois	Nicname (43)
	Www	World Wide Web (HTTP, 80)
UDP	biff	Mail notify (512)
	bootpc	Bootstrap Protocol Client (68)
	bootps	Bootstrap Protocol Server (67)
	discard	Discard (9)
	dns	Mail notify (512)
	dnsix	DNSIX Securit Attribute Token Map (90)
	echo	Echo (7)
	mobilip-ag	MobileIP-Agent (434)
	mobilip-mn	MobilIP-MN (435)
	nameserver	Host Name Server (42)
	netbios-dgm	NETBIOS Datagram Service (138)
	netbios-ns	NETBIOS Name Service (137)
	netbios-ssn	NETBIOS Session Service (139)
	ntp	Network Time Protocol (123)
	rip	Routing Information Protocol (520)
	snmp	SNMP (161)
	snmptrap	SNMPTRAP (162)
	sunrpc	SUN Remote Procedure Call (111)
	syslog	Syslog (514)
	tacacs-ds	TACACS-Database Service (65)
	talk	Talk (517)
	tftp	Trivial File Transfer (69)
	time	Time (37)
	who	Who(513)
	xdmcp	X Display Manager Control Protocol (177)

对于 ICMP 协议可以指定 ICMP 报文类型,缺省为全部 ICMP 报文。指定 ICMP 报文类型时，可以用数字（0-255），也可以用助记符。助记符如下：

助记符	意义
echo	Type=8, Code=0
echo-reply	Type=0, Code=0
fragmentneed-DFset	Type=3, Code=4
host-redirect	Type=5, Code=1
host-tos-redirect	Type=5, Code=3
host-unreachable	Type=3, Code=1
information-reply	Type=16,Code=0
information-request	Type=15,Code=0
net-redirect	Type=5, Code=0
net-tos-redirect	Type=5, Code=2
net-unreachable	Type=3, Code=0
parameter-problem	Type=12,Code=0
port-unreachable	Type=3, Code=3
protocol-unreachable	Type=3, Code=2
reassembly-timeout	Type=11,Code=1
source-quench	Type=4, Code=0
source-route-failed	Type=3, Code=5
timestamp-reply	Type=14,Code=0
timestamp-request	Type=13,Code=0
ttl-exceeded	Type=11,Code=0

8.4 如何使用访问控制列表

8.4.1 访问控制列表的配置



前面我们简单的介绍了 Quidway 系列路由器配置访问控制列表的相关内容。通过前面的介绍，大家应该初步掌握了如何配置一条标准或扩展访问控制列表。但是如果需要访问控制列表真正发挥作用，达到包过滤的目的，我们还需要进行一些其他的配置下面我们为大家介绍完成访问控制列表配置的步骤。

- 允许/禁止防火墙（Quidway 系列路由器默认是禁止防火墙功能）
- 定义访问控制列表（标准或扩展）
- 在接口上应用访问控制列表

在实际的使用中，还可能用到以下的扩展应用：

1. 设置防火墙的缺省过滤模式；
2. 允许或禁止时间段；
3. 设定时间段；
4. 允许日志主机；
5. 指定日志主机；
6. 显示配置状况。

其中，2 和 4 均在配置访问控制列表中设置，1、3、5 和 6 由专门的命令完成。

8.4.2 防火墙的属性配置命令

在防火墙的属性配置命令中，首先是打开防火墙：

firewall {enable | disable} 允许/ 禁止防火墙过滤；

其次，是设置防火墙的缺省过滤模式：

firewall default {permit | deny } 缺省方式是禁止还是允许；

缺省过滤模式用来定义对访问列表控制以外的 IP 或者 TCP 等数据包的处理方式，Quidway 系列路由器防火墙的默认过滤模式是允许。

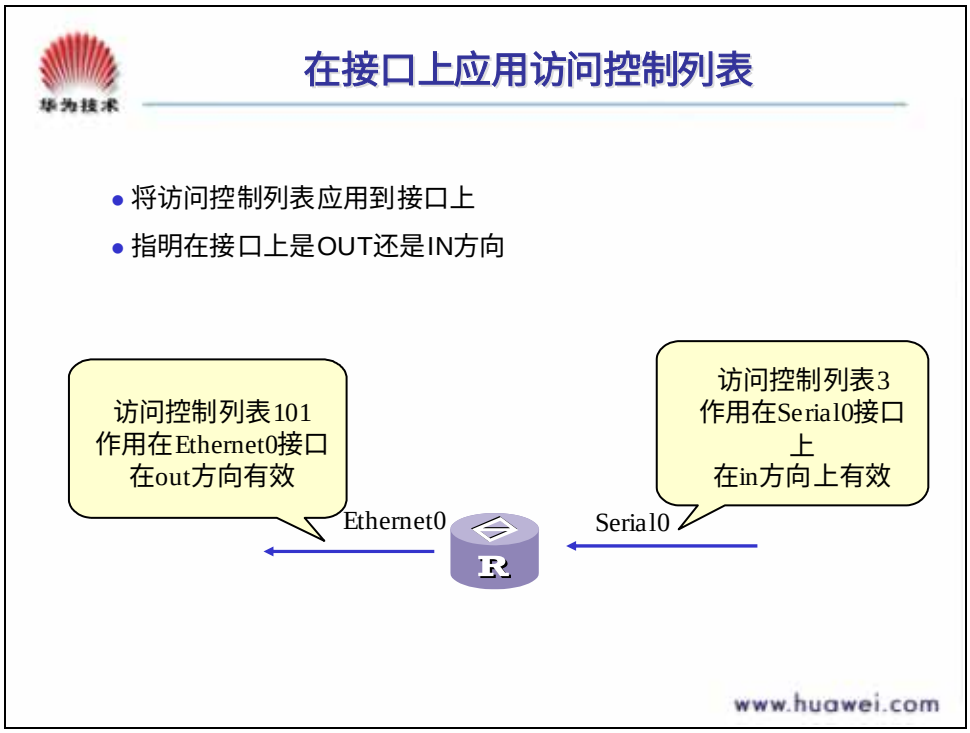
用 display firewall 命令可以 显示防火墙状态信息。

[Quidway]display firewall

```
  Firewall is enable, default filtering method is 'permit'.
 TimeRange packet-filtering disable.
 InBound : 0 packets, 0 bytes, 0% permitted,
           0 packets, 0 bytes, 0% denied,
           634 packets, 32968 bytes, 100% permitted defaultly,
           0 packets, 0 bytes, 0% denied defaultly;
     From 00:40:09 to 00:40:13
           0 packets, 0 bytes, permitted,
           0 packets, 0 bytes, denied,
```

```
                0 packets, 0 bytes, permitted defaultly,
                0 packets, 0 bytes, denied defaultly;
        OutBound: 0 packets, 0 bytes, 0% permitted,
                0 packets, 0 bytes, 0% denied,
                2297 packets, 151316 bytes, 100% permitted defaultly,
                0 packets, 0 bytes, 0% denied defaultly.
           From 00:40:09 to 00:40:13
                0 packets, 0 bytes, permitted,
                0 packets, 0 bytes, denied,
                1 packets, 64 bytes, permitted defaultly,
                0 packets, 0 bytes, denied defaultly;.
```

8.4.3 在接口上应用访问控制列表



为了使访问控制列表生效，必须将访问控制列表定义在接口上。

基于接口配置访问列表，使访问列表生效：

firewall packet-filter *acl-number* [**inbound** | **outbound**]

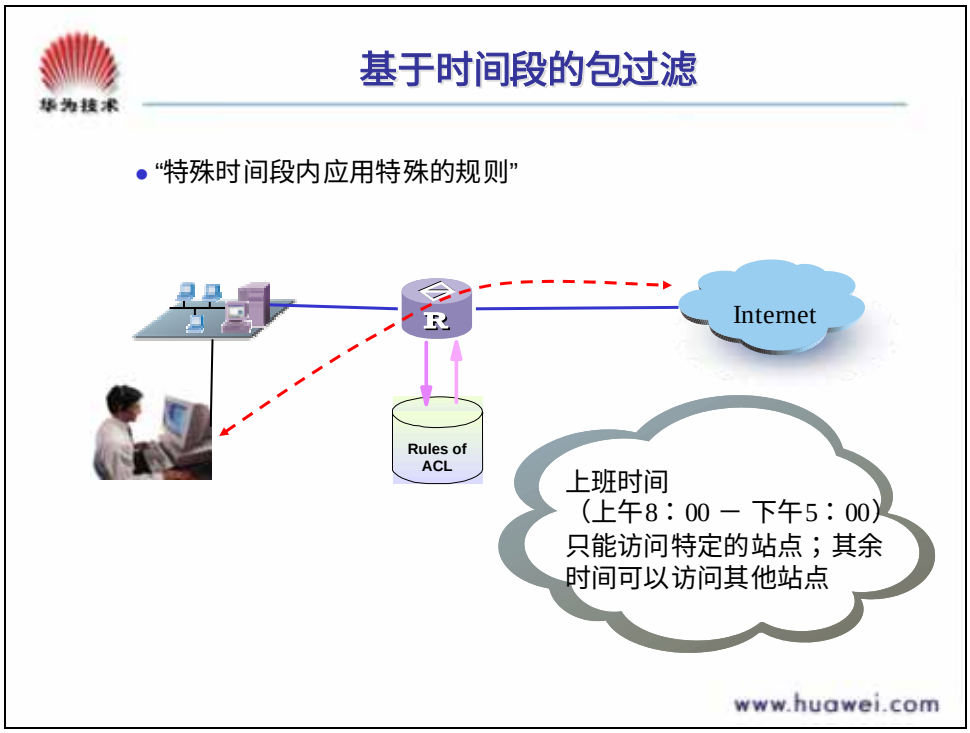
使用此命令来将规则应用到接口上。如果要过滤从接口收上来的报文则使用 **inbound** 关键字，如果要过滤从接口转发的报文则使用 **outbound** 关键字，如果不带方向参数则认为采用 **outbound** 关键字。

例如：要将 1 号访问控制列表应用到串口 0 上，则在在 Serial0 口配置模式下执行如下命令：

```
firewall packet-filter 1 inbound
```

这样将在 Serial0 口上，对进入路由器的数据包，使用访问控制列表 1 进行过滤。

8.4.4 时间段包过滤



基于时间段，用户可以指定一天 24 小时中的任意时间段为特殊时间段（可以是多个），不在任何特殊时间段的其他时间称为普通时间段。用户在定义访问列表时，可以指定该规则是在特殊时间段还是在普通时间段生效。

时间段的配置命令

- time range 命令
  - timerange { enable|disable }
- [no] settr 命令
  - settr begin-time end-time [begin-time end-time .....]
  - no settr
- show isintr 命令
  - display isintr
- show timerange 命令
  - display timerange

www.huawei.com

timerange { enable|disable } 允许 | 禁止时间段

Quidway 防火墙默认为禁止时间段。

settr begin-time end-time [begin-time end-time .....] 设置特殊时间段

display isintr 显示当前时间是否在特殊时间段内

display timerange 显示配置的时间段

8.4.5 日志功能

日志功能用以记录下所有来犯防火墙的操作信息，在访问列表允许日志功能后，需再配置另一条命令 logging host，以指定日志主机的位置。日志主机可以是一台普通的网络工作站，也可以是专用的服务器，它们之上需运行标准的日志程序，以接收路由器发回的日志记录。

路由器侧的配置举例如下：

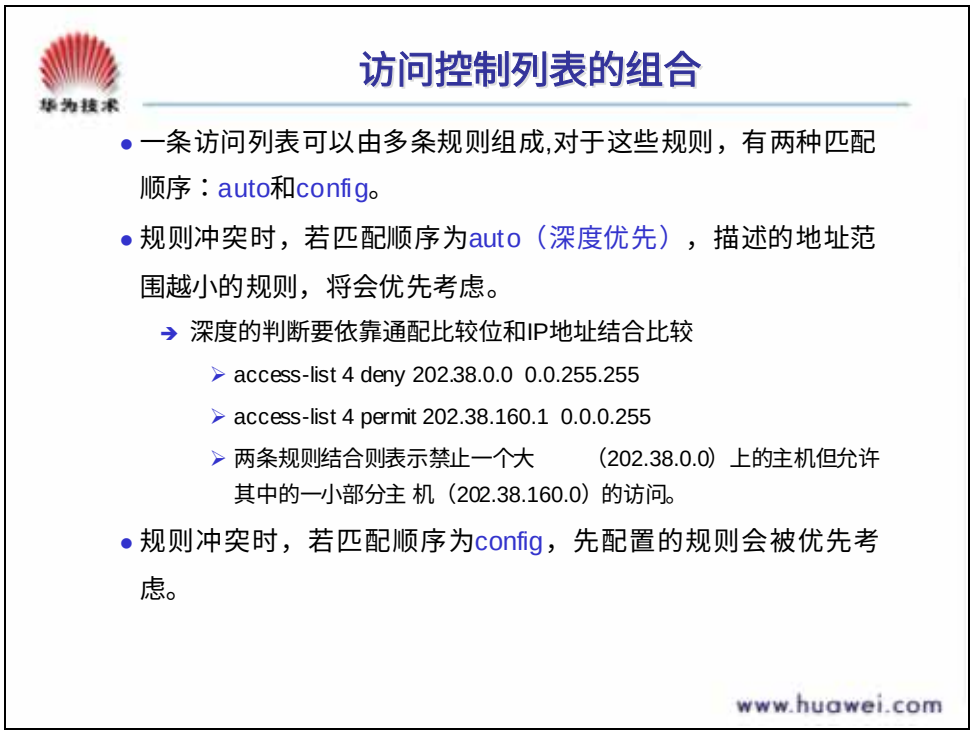
！开启日志系统。

[Quidway]info-center enable

！将 ip 地址为 10.110.12.119 的主机用作日志主机。

[Quidway]info-center loghost 0 10.110.12.119 514

8.4.6 访问控制列表的组合



一条访问控制列表可以包含多条规则。而对于一条访问控制列表中的多条规则，华为路由器上定义了两种匹配顺序：**auto** 和 **config**。其中 **auto** 表示采用深度优先原则对访问控制列表进行自动排序；**config** 则表示依据用户输入的配置顺序进行匹配，先配置的访问列表规则一定会先匹配。我们可以用下列命令来配置访问控制列表的匹配顺序：

acl *acl-number* **match-order** [**config** | **auto**]

如果两条规则有冲突，而访问控制列表的匹配顺序为 **auto**，即“深度优先”时，在这种情况下描述的地址范围越小的规则，将会优先考虑。例如：

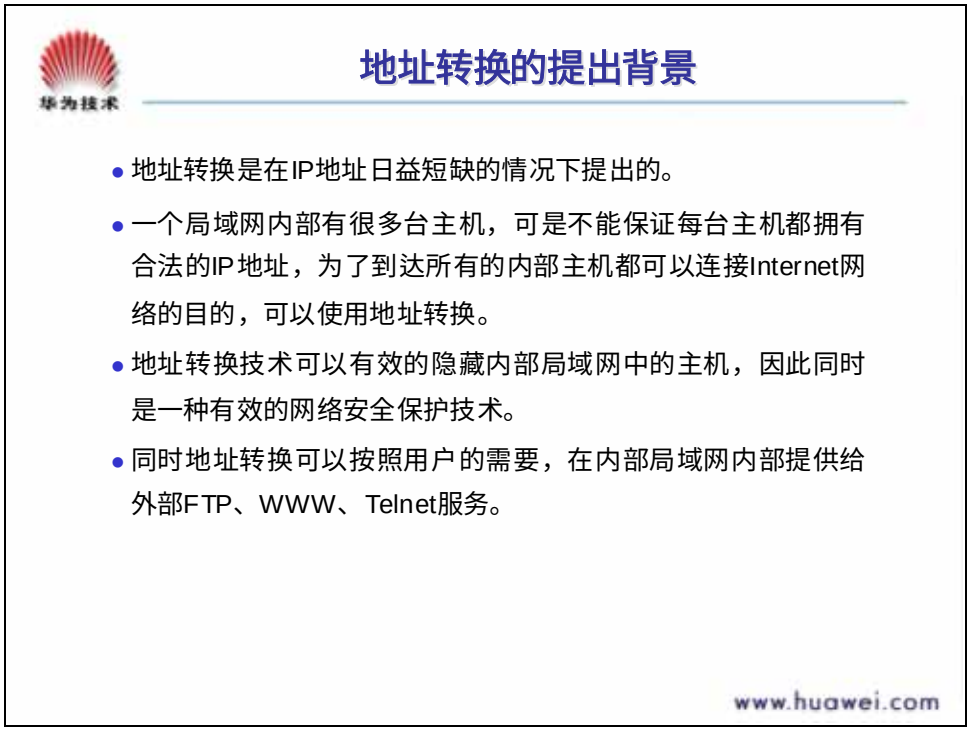
access-list 1 permit 202.38.160.0 0.0.255.255

access-list 1 deny 202.38.160.0 0.0.0.255

对于 202.38.160.23 这样的地址，访问列表是认为是拒绝的。因为第二条指定的地址范围小。

如果两条规则有冲突，而访问控制列表的匹配顺序为 **config**。这时先配置的访问列表规则则会被优先考虑。

8.5 地址转换简介



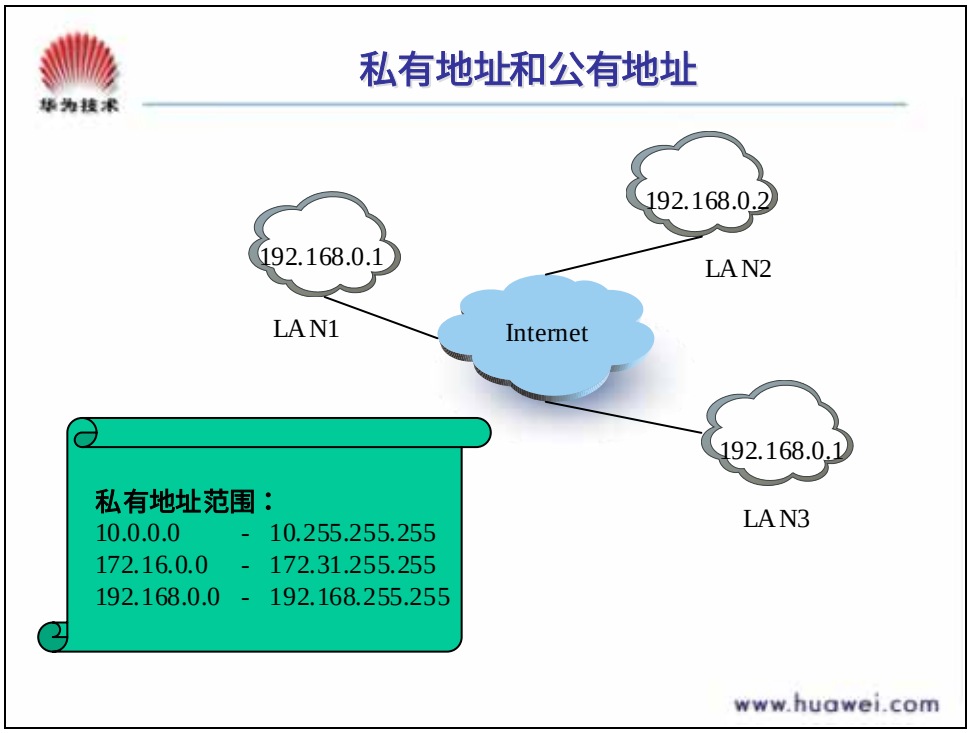
地址转换是在 IP 地址日益短缺的情况下提出的。

一个局域网内部有很多台主机，可是不能保证每台主机都拥有合法的公网 IP 地址，为了到达所有的内部主机都可以连接 Internet 网络的目的，可以使用地址转换。

地址转换技术可以有效的隐藏内部局域网中的主机，因此地址转换同时也是一种有效的网络安全保护技术。

地址转换还可以按照用户的需要，通过局域网内部的服务器向外部网络提供 FTP、WWW、Telnet 等服务。

8.5.1 私有地址和公有地址



私有地址是指内部网络（局域网内部）的主机地址，而公有地址是局域网的外部地址（在 Internet 上的全球唯一的 IP 地址）。 Internet 地址分配组织规定以下的三个网络地址保留用做私有地址：

10.0.0.0 - 10.255.255.255

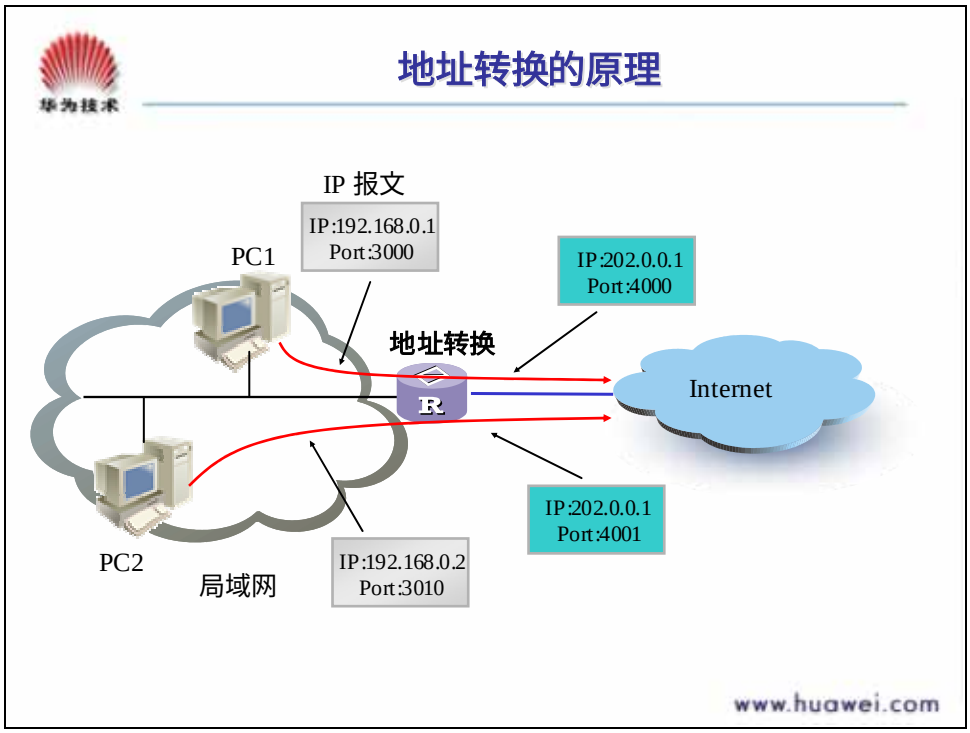
172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

也就是说这三个网络的地址不会在 Internet 上被分配，但可以在一个企业（局域网）内部使用。各个企业根据在可预见的将来主机数量的多少，来选择一个合适的网络地址。不同的企业，他们的内部网络地址可以相同。如果一个公司选择其他的网段作为内部网络地址，则有可能会引起路由表的混乱，因此构建自己的内部局域网的时候，都应该选择上面这三个网段的地址做为自己的 IP 地址。

公有地址就是从 Internet 地址分配组织得到的合法 IP 地址，对于用户来说，一般该地址都是从 ISP 申请的。

8.5.2 地址转换的原理



因为不同的局域网中的计算机可以采用相同的私有地址，所以如果局域网中的计算机在同 Internet 中的计算机通信时，必须将自己的私有地址转换为公有地址，否则可能会同其他局域网中的计算机产生冲突。

因为地址资源日渐稀少，所以在实际的应用中，可供转换的公有地址往往少于局域网中的主机数，所以我们一般采用 PAT（Port Address Translation）方式进行地址转换。PAT 方式的地址转换是采用了“地址＋端口”的映射方式，因此可以使内部局域网的许多主机共享一个 IP 地址访问 Internet。

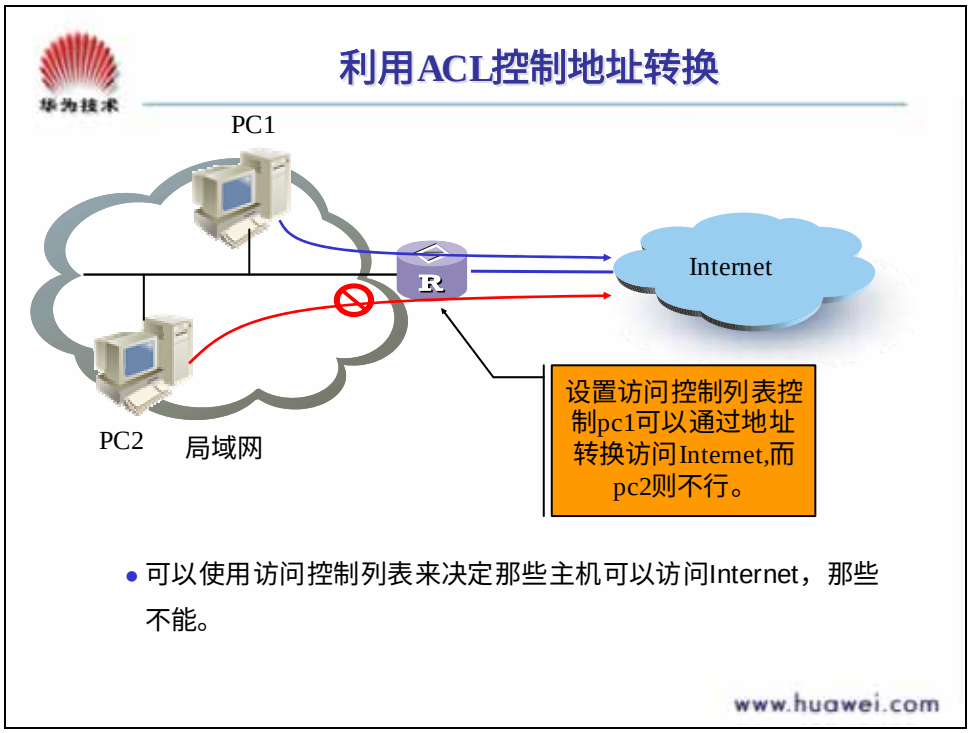
例如：在上图中，主机 1 发出一个源地址为 192.168.0.1，源 端口号为 3000 的数据包，局域网的出口路由器在处理这个数据包的时候，会将它的源地址改为公网地址 202.0.0.1，源端口号改为 4000，再将它送到 Internet 中，这样一来，就不会同其他局域网中的计算机产生冲突了。

同理，当局域网的出口路由器收到一个目的地址为 202.0.0.1，目的端口号为 4000 的数据包时，路由器会将数据包的目的地址改为 192.168.0.1，目的端口号改为 3000，再将它送到局域网中。这样数据包就会被准确的送达主机 1。

需要注意的是，并不是在所有的情况下都可以使用地址转换。由于地址转换会对报文头进行修改，因此在报文头被加密或受保护的情况下是无法使用地址转换

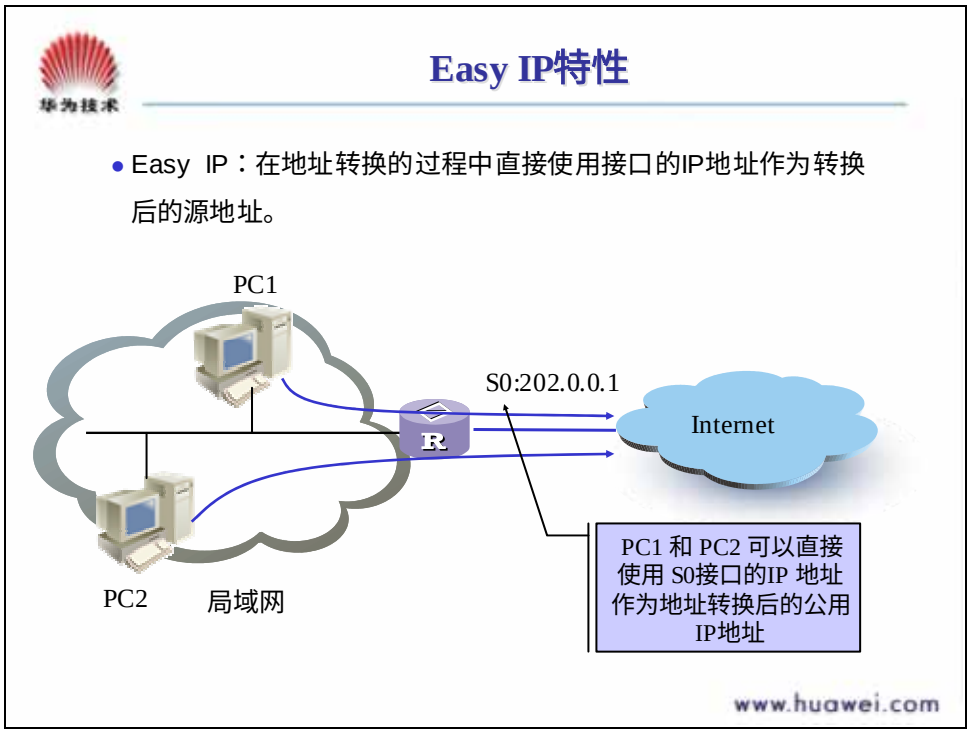
的。比如：利用 IPSEC（IP Security）进行了加密保护的数据包就无法进行地址转换。

8.5.3 地址转换的方式



通常在一个局域网中，并不是所有的主机都需要通过地址转换来访问 Internet，因此我们可以通过将访问控制列表同地址转换结合使用，来控制局域网内的主机对外部网络的访问。此时，对于需要进行地址转换的数据包，首先要通过访问控制列表的过滤，通过之后才能进行地址转换。对于无需地址转换的数据包，这些访问控制列表不起作用。

8.5.4 EASY IP 特性



在路由器上配置地址转换通常有两种方法：一种是配置访问控制列表和接口的关联（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，适用于两种情况：

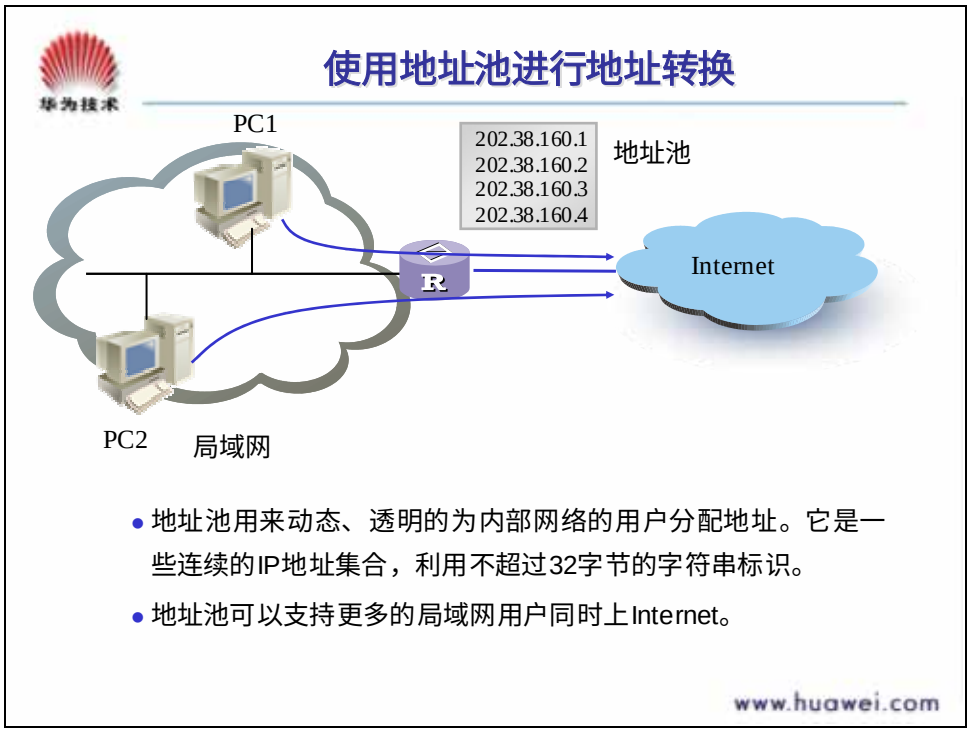
1、在拨号方式下，用户希望由协商方式得到的接口 IP 地址作为地址转换后的源地址。例如在一个局域网中的主机通过一台路由器拨号访问 Internet，而路由器拨号接口的 IP 地址是由接入服务器协商分配的且不固定，对于这种情况我们可以配置访问控制列表和接口的关联，以对端分配的 IP 地址作为地址转换后的地址；

2、另一种情况是接口的 IP 地址固定，而用户希望就使用接口本身的 IP 地址作为地址转换后的源地址。

配置访问控制列表和接口的关联（又称 EASY IP 特性）的命令如下：

nat outbound *acl-number* **interface**

在接口模式下进行配置，缺省情况下，访问控制列表不与任何接口关联。



另一种配置地址转换的方法是利用地址池进行地址转换。

地址池，顾名思义就是一些地址的集合。在地址转换中，应该是一些合法 IP 地址（公有网络 IP 地址的集合）。用户可根据自己拥有的合法 IP 地址的多少、内部网络主机的多少、以及实际应用情况，配置合适的 IP 地址池。地址转换的过程中，将会从地址池中挑选一个地址做为转换的源地址。

地址池是一些连续的 IP 地址集合，当内部数据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。有关地址池的配置在全局模式下进行，其命令如下：

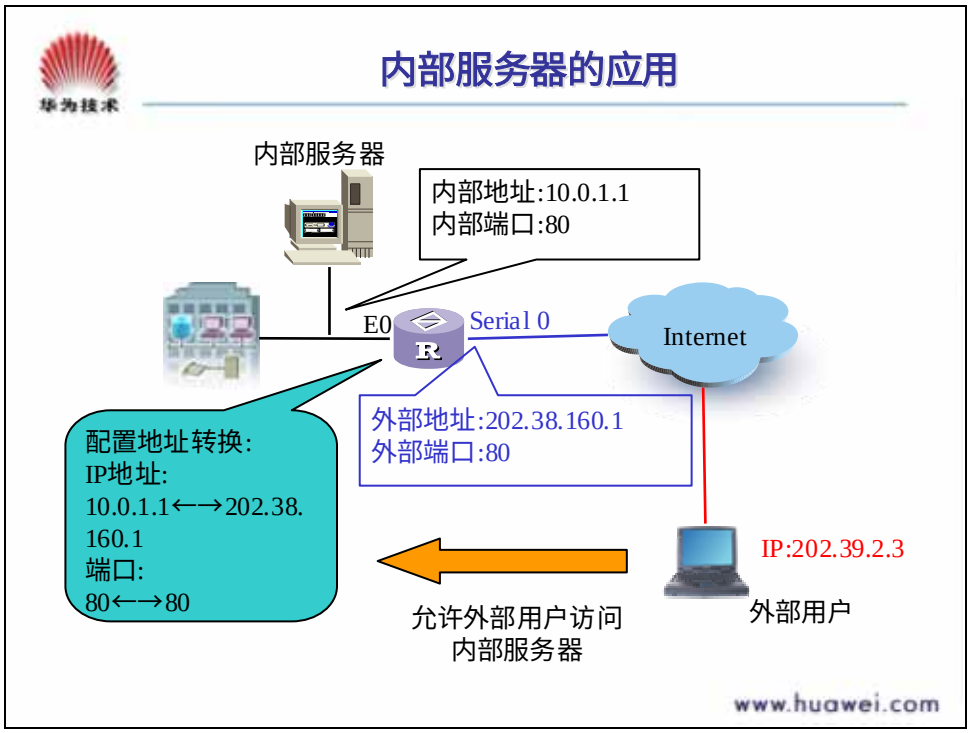
- 定义一个地址池：**nat address-group** *start-addr end-addr pool-name*

  删除一个地址池：**undo nat address-group** *pool-name*

每个地址池中的地址必须是连续的，每个地址池内最多可定义 64 个地址。

需要注意的是：当某个地址池已经和某个访问控制列表关联进行地址转换，是不允许删除这个地址池的。

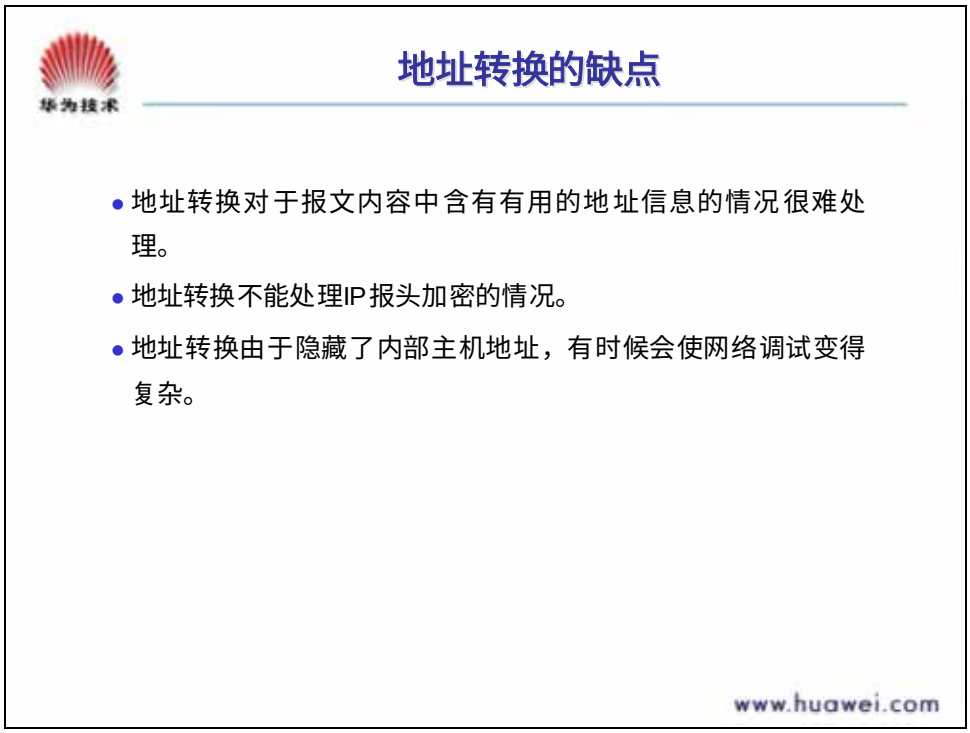
8.5.5 内部服务器的应用



在实际的应用中，有时需要将局域网中的服务（如 FTP 服务、邮件服务等）向 Internet 开放，在提供这些服务的过程中，流经出口路由器的数据包的内容部分可能也会包含需要转换的 IP 地址和端口号，这时，我们就不仅需要对数据包的包头进行地址转换，而且还需要对数据包的内容部分进行地址转换。一般情况下，路由器是不会做这样的工作的，所以，当我们需要开放局域网中的一项服务时，就需要在路由器上指明所开放的服务的外部地址、外部端口、内部服务器地址、内部服务器端口以及协议的类型。

如胶片中的示意图所示，一台局域网中的服务器需要向特定的外部用户提供服务。对于这种情况，我们可以在出口路由器上配置服务器的内部地址/端口到外部地址/端口的映射关系。而外部用户则可以通过服务器的外部地址/端口进行访问，并在路由器上进行一种反向的地址转换。这样既屏蔽了内部网络中的主机，又允许了外部的用户访问设置在内部局域网内的服务器。

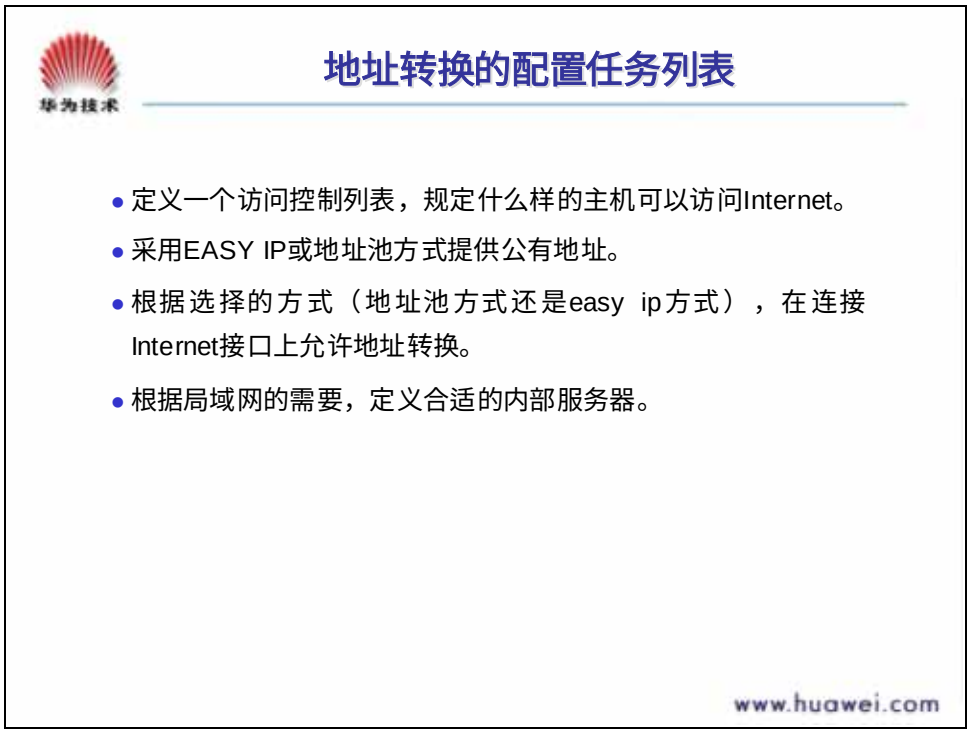
8.5.6 地址转换的缺点



在地址转换的过程中，转换了数据包的地址。但是如果数据包的数据中包含了有用的地址转换信息，这样的情况地址转换就很难处理。例如假设具有某种协议，在数据包中指明发送数据包的地址转换信息，而这个地址信息被对方使用。这样的情况地址转换很难处理了，因为地址转换不指定数据包内容中是否有有用的 IP 地址。

相同的原因，如果对 IP 报头进行了加密处理，地址转换也不能知道真实的 IP 报头的内容，也就不能进行地址转换了。

8.5.7 地址转换的配置



下面我们再来总结一下地址转换的配置任务列表：

1. 定义一个访问控制列表

acl listnumber

rule { permit | deny } ip-address [wildcard-mask]

2. **EASY IP 方式的地址转换：** [undo] nat outbound acl-number interface

3. **使用地址池方式的地址转换：**

定义地址池： nat address-group start-addr end-addr pool-name

undo nat address-group pool-name

在接口上使用地址池方式进行地址转换：

[undo] nat outbound acl-number pool-name

4. **配置内部服务器**

nat server global *global-addr* { *global-port* | **any** | **domain** | **ftp** | **pop2** | **pop3** | **smtp** | **telnet** | **www** } **inside** *inside-addr* { *inside-port* | **any** | **domain** | **ftp** | **pop2** | **pop3** | **smtp** | **telnet** | **www** } { *protocol-number* | **ip** | **icmp** | **tcp** | **udp** }

undo nat server { **global** | **inside** } *address* { *port* | **any** | **domain** | **ftp** | **pop2** | **pop3** | **smtp** | **telnet** | **www** } { *protocol-number* | **ip** | **icmp** | **tcp** | **udp** }

需要注意：(1) *inside-port* 是必须的，可为 0 或取值在 1～65535 之间的整数。

(2) 若未定义 *global-port*，*global-port* 的值就等于 *inside-port* 的值。

8.5.8 地址转换的监控和维护

在地址转换的监控和维护方面，我们可以使用胶片中所示的命令来设置地址转换的连接有效时间。缺省情况下，TCP 地址转换有效时间为 240 秒；UDP 地址转换有效时间为 40 秒；ICMP 地址转换有效时间为 20 秒。

另外，我们还可以用下面的命令来察看地址转换的状态：

[Quidway]display nat

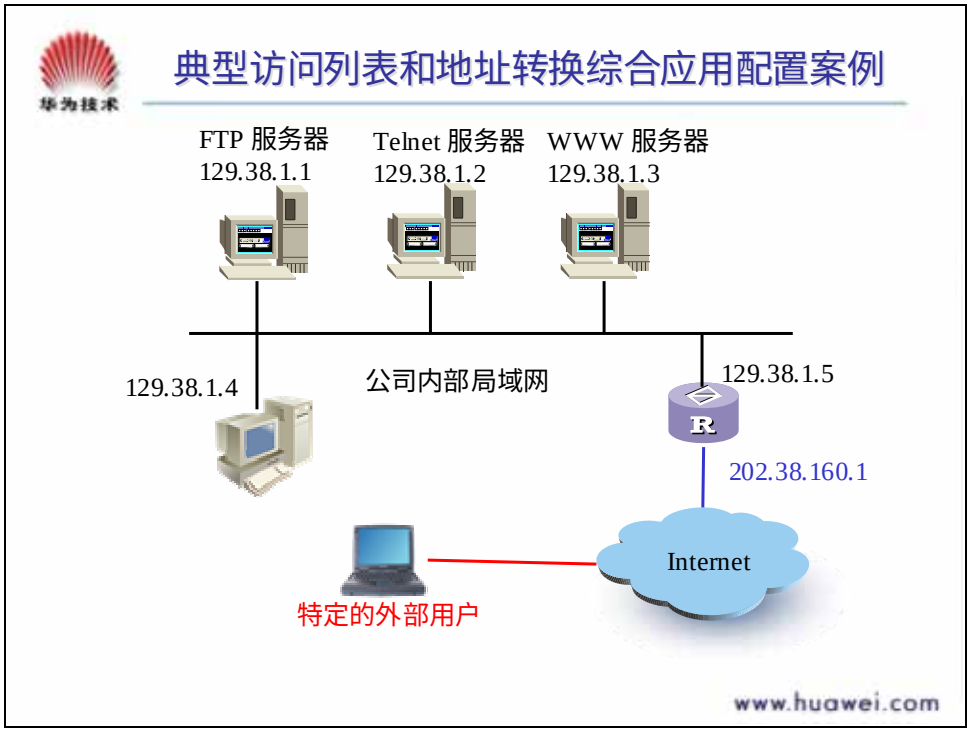
```
Nat pool：
   pool1  from 202.110.10.10  to  202.110.10.12
   pool2  from 202.110.100.10 to  202.110.100.12
Nat inside：
   (Interface:Serial0): access-list(1) ---- Nat pool (pool1 )
Nat server:
Interface global-address global-port host-address host-port protocol
Serial0   202.110.10.100   8080     10.110.10.10  80 (www)  6 (tcp)
Serial0   202.110.10.100   2121     10.110.10.10  21 (ftp)  6 (tcp)
Serial0   202.110.10.100   23(telnet)10.110.10.12  23(telnet) 6(tcp)
Nat timeout:
    tcp timeout value      --------------   100
    udp timeout value      --------------   60
```

```
    icmp timeout value     ---------------  20
```

以上信息表明：配置了 pool1、pool2 两个地址池，地址范围分别是 202.110.10.10 到 202.110.10.12 和 202.110.100.10 到 202.110.100.12。在 Serial0 配置了地址转换，允许地址列表 1 中的地址选择地址池 pool1 中的地址进行地址转换。在 Serial0 配置了 3 个内部服务器。http://202.110.10.100:8080 的 www 服务器，内部地址是 10.110.10.10；ftp://202.110.10.100:2121 的 ftp 服务器，内部地址是 10.110.10.10 ；telnet://202.110.10.100，内部地址为 10.110.10.12。最后一行是各种连接的有效时间。

8.6 访问列表和地址转换的综合应用举例

8.6.1 组网图



在实际应用中，访问控制列表和地址转换通常被综合使用，下面我们通过这样的一个例子来说明这个问题。

例：

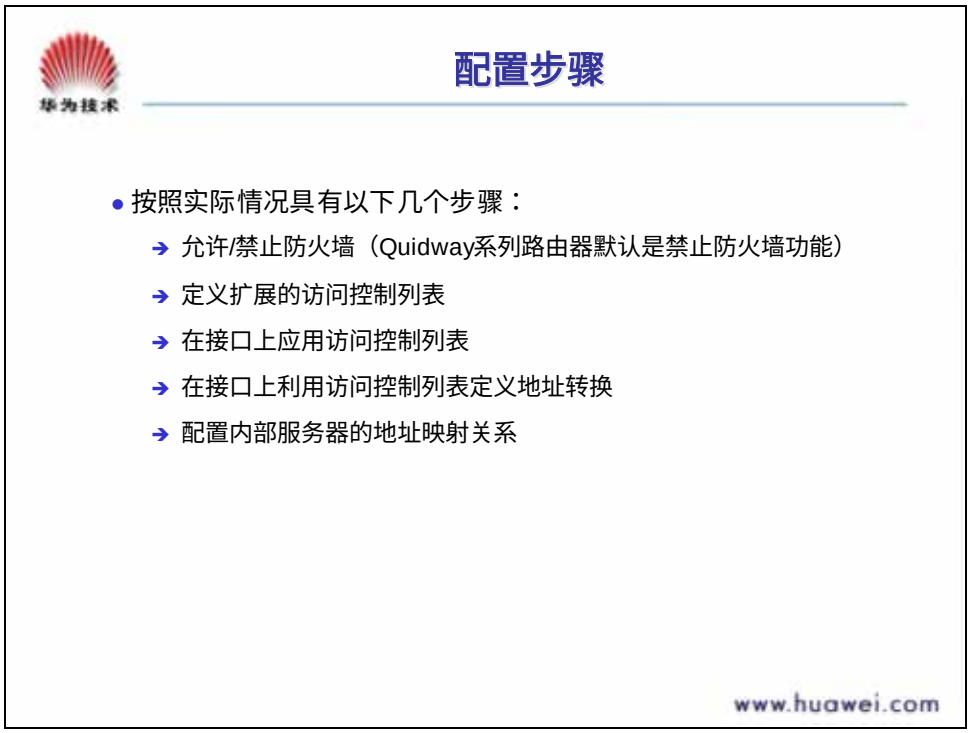
某公司通过一台 Quidway 2501 路由器的接口 Serial0 访问 Internet ，公司内部对外提供 www、ftp 和 telnet 服务，公司内部子网为 129.38.1.0，其中，内部 ftp 服务器地址为 129.38.1.1，内部 telnet 服务器地址为 129.38.1.2，内部 www 服务器地址为 129.38.1.3，公司对外的 IP 地址为 202.38.160.1。在路由器上配置了地址转换，这样内部特定 PC 机（129.38.1.4）可以访问 Internet ，外部 PC 可以访问内部服务器。通过配置防火墙，希望实现以下要求：

外部网络只有特定用户可以访问内部服务器。

内部网络只有特定主机可以访问外部网络。

假定外部特定用户的 IP 地址为 202.39.2.3 。

8.6.2 配置示例



参考配置如下：

！ 允许防火墙

[Quidway]firewall enable

！ 设置防火墙缺省过滤方式为允许包通过

[Quidway]firewall default permit

！配置访问规则禁止所有包通过

[Quidway]acl 101

[Quidway-acl-101]rule deny ip source any destination any

！配置规则允许特定主机访问外部网，允许内部服务器访问外部网

[Quidway-acl-101]rule permit ip source 129.38.1.1 0 destination any

[Quidway-acl-101]rule permit ip source 129.38.1.2 0 destination any

[Quidway-acl-101]rule permit ip source 129.38.1.3 0 destination any

[Quidway-acl-101]rule permit ip source 129.38.1.4 0 destination any

！配置规则允许特定用户从外部网访问内部服务器

[Quidway-acl-101]acl 102

[Quidway-acl-102]rule permit tcp source 202.39.2.3 0 destination 202.38.160.1 0

！配置规则允许特定用户从外部网取得数据（只允许端口大于 1024 的包）

[Quidway-acl-102]rule permit tcp source any destination 202.38.160.1 0 destination-port greater-than 1024

！将规则 101 作用于从接口 Ethernet0 进入的包

[Quidway-Ethernet0]firewall packet-filter 101 inbound

！ 将规则 102 作用于从接口 Serial0 进入的包

[Quidway-Serial0]firewall packet-filter 102 inbound

！在接口 Serial0 上使用访问控制列表 101 作地址转换的条件（Easy IP）：

[Quidway-Serial0]nat outbound 101 interface

！设置内部 FTP 服务器

[Quidway-Serial0]nat server global 202.38.160.1 inside 129.38.1.1 ftp tcp

！ 设置内部 telnet 服务器

[Quidway-Serial0]nat server global 202.38.160.1 inside 129.38.1.2 telnet tcp

！ 设置内部 WWW 服务器

[Quidway-Serial0]nat server global 202.38.160.1 inside 129.38.1.1 ftp www

其他内容如各端口 IP 地址，封装协议等这里不再赘述