China-pub.com
下载

第9章　用访问列表管理基本通信量

认证目标

9.01　标准IP访问列表
9.02　扩展IP访问列表
9.03　命名访问列表
9.04　标准IPX访问列表
9.05　IPX SAP过滤
9.06　AppleTalk访问列表

数据包过滤用来控制跨越网络的数据流。通过实现它，可以限制网络通信量，限制网络访问到特定的用户和设备。在 Cisco路由器上，可通过使用访问列表来执行数据包过滤。访问列表可用来控制网络上数据包的传递，限制虚拟终端线路的通信量或者控制路由选择更新。对于每个访问列表，你可以输入规则来允许或者禁止数据包，访问列表用号码来标识。对一个表的所有语句必须使用相同的号码。使用什么号码可由你随意决定，但必须符合表 9-1的范围，号码的由你正在应用的访问列表的设备来决定。标星号的协议是本章中将要讨论的，并出现在考试中。

本章中将介绍如何创建一个访问列表，并将其运用到接口和服务上。

表9-1　访问列表的号码范围

协　　议	范　　围
IP*	1~99
扩展IP*	100~199
Ethernet类型码	200~299
DECnet	300~399
XNS	400~499
扩展XNS	500~599
AppleTalk*	600~699
Ethernet地址	700~799
IPX*	800~899
扩展IPX	900~999
IPX SAP*	1000~1099

9.1　认证目标9.01：标准IP访问列表

IP访问列表是应用于 IP地址的允许和禁止规则的集合。对于每个数据包，路由器顺序执行每个访问列表中的规则。如果路由器到达了访问列表的底端而没有找到与该数据包相匹配

China-pub.com 下载

的语句，则遗弃该数据包 (这叫作隐式DENY ANY)。因此，每个访问列表都必须包含至少一个允许的语句是十分重要的。由于第一个匹配的语句将执行，所以顺序是十分重要的。

Cisco IOS 11.1版在访问列表的语法和执行上有显著的改变，但是它提供了向下兼容性，如果你是从以前的版本升级到11.1版的话，它会自动将访问列表转化成新的格式。

有三种基本的IP访问列表：标准型、扩展型和动态扩展型。标准访问列表源寻址作为使用规则。这提供了十分基本的过滤格式。扩展访问列表同时使用源地址和目标地址作为过滤，甚至允许用协议类型来过滤。最后，动态扩展访问列表通过认证过程对每个用户确定对目标的访问权。

路由器使用通配符掩码(或者称作反掩码)与源或目标地址一起来分辨匹配的地址范围。像子网掩码告诉路由器IP地址的哪一位属于网络号一样，通配符掩码告诉路由器为了判断出匹配，它需要检查IP地址中的多少位。这个地址掩码对使我们可以只使用两个 32位的号码来确定IP地址的范围。这是十分方便的，因为如果没有掩码的话，你不得不对每个匹配的 IP客户地址加入一个单独的访问列表语句。这将造成很多额外的输入和路由器大量额外的处理过程。所以地址掩码对相当有用。

你已经知道，在子网掩码中，将掩码的一位设成1表示IP地址对应的位属于网络地址部分。相反，在访问列表中将通配符掩码中的一位设成1表示IP地址中对应的位既可以是1又可以是0。有时，可将其称作“无关”位，因为路由器在判断是否匹配时并不关心它们。掩码位设成 0则表示IP地址中相对应的位必须精确匹配。

这里有一些在访问列表可能出现的一些地址掩码对，你可以看看是如何工作的：

```
124.220.7.0 0.0.0.255
```

最后的八位位组掩码是所有的值，所以路由器认为这些位上所有的值都匹配。它会试图精确匹配前三个八位位组。这个掩码对匹配从124.220.7.0到124.220.7.255的IP地址。

```
193.62.0.0 0.0.255.255
```

该掩码的最后两个八位位组是所有的值，所以路由器认为这些位上所有的值都匹配。也就是说只要IP地址的前两个八位位组是193.62，则最后两个八位位组上可以是任何值。这个地址掩码对将匹配193.62.0.0到193.62.255.255中所有的IP地址。

```
172.16.16.0 0.0.7.255
```

并不是所有的掩码在“精确匹配”位和“无关”位间都有两个八位位组的边界。有时，计算什么匹配什么不匹配是十分困难的事。让我们来看看最后一个例子中第三个八位位组的二进制分解：

地址位：16=00010000

掩码位：7=00000111

可以看出，如果不管掩码中为1的相对应的地址位，这对数字描述了八种可能的数字范围，从16~23。如下所示，可以用二进制从16~24来验证它：

```
=00010000
=00010001
=00010010
=00010011
```

China-pub.com
下载


```
=00010100
=00010101
=00010110
=00010111
=00011000
```

注意，当我们数到24时，地址上的2^3位从0变成了1。2^3位不再符合掩码，所以它不再属于这对描述的范围内。

看看整个的地址掩码对，IP地址范围是从172.16.16.0到172.16.23.255。

对于访问列表，判断是否匹配的过程实际分为三个步骤。在数据包过滤中，为进行匹配，我们检查IP地址的IP数据包报头。不妨设访问列表语句中包含地址掩码对 172.16.0.0 0.0.255.255。一个数据包中包含源IP地址172.16.10.22，路由器将如下操作：

1) 用访问列表语句中的掩码和地址执行逻辑或。结果地址或掩码中为1的位，结果中仍然为1。该操作的结果为172.16.255.255。

2) 用访问列表语句中的掩码和数据包报头中的IP地址执行逻辑或，结果是172.16.255.255。

3) 将两个结果相减。如果两个结果相等，相减的结果精确为零，则匹配；如果相减的结果不为零，则不匹配，对下条语句重复执行上述三个步骤。

在IP访问列表地址掩码对中，有两个关键字可用来省略一些输入。第一个是“ any”，它可用来代替地址掩码对0.0.0.0 255.255.255.255。可以看到，该地址掩码对匹配任何的IP地址。另一个是“ host”，它只能用于扩展访问列表中，用来代替掩码 0.0.0.0。在标准访问列表中，当掩码是0.0.0.0时省略它，如果省略了掩码，则表示该掩码是0.0.0.0。

所有的访问列表是在全局配置模式下生成的。增加标准访问列表的基本格式如下：

ACCESS-LIST *access-list-number* {DENY|PERMIT}
{SOURCE[*source-wildcard*]|ANY}

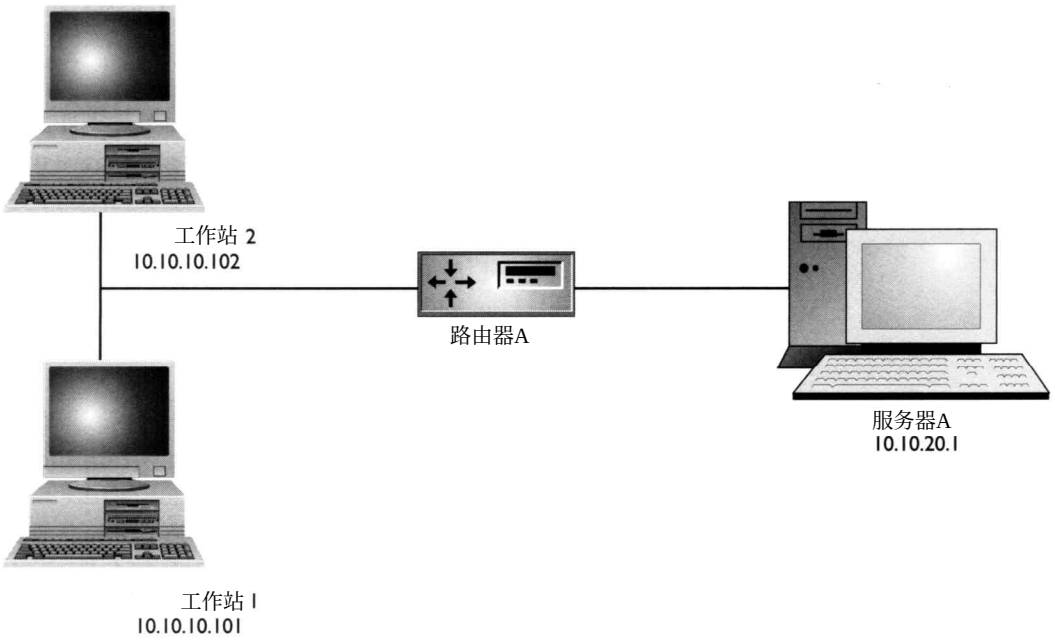

图9-1 标准IP访问列表数据包过滤

China-pub.com 下载

参数ACCESS-LIST-NUMBER是一个有特定范围的号码，用来表示输入的命令将加入到哪个表中。然后规定条目是否允许或禁止从特定地址来的通信量，参数 SOURCE顾名思义，指明了访问列表规则应用的源IP地址。如果想增加子网地址，则可以将源地址从特定指明的主机变为一个IP地址范围。参数SOURCE-WILDCARD基本指明了地址字段中哪些位是匹配的。如果在末尾加上参数ANY，则表示地址0.0.0.0和子网掩码255.255.255.255。显而易见，这时所有的地址都是匹配的。这里是一个标准IP访问列表的例子，它出现在如图9-1所描述的网络中：

```
ACCESS-LIST 1 PERMIT 10.10.10.101
ACCESS-LIST 1 DENY 10.10.10.0 0.0.0.255
```

现在我们还没有完成所有的工作。访问列表配置是一个两步的工作，顺序并没有关系。你不仅需要建立想用的访问列表，同时还必须将它提供给每个想用它的接口。需要注意的事是，如果你在定义一个访问列表语句前将其提供给接口，或者删除一个已应用于某个接口的访问列表时，会得到一个未定义的表。

如果想将上面的表应用为数据包过滤，有两种选择。我们可将其用作路由器 A与网络10.10.10.0的接口的入站过滤，或者用作路由器 A与网络10.10.20.0的接口的出站过滤。对于路由器来说，出站过滤工作量少一些，所以将其应用为出站过滤。

进入接口配置模式，使用命令IP ACCESS-GROUP 1 OUT将该接口放入使用访问列表101作为过滤的组。一个访问列表可用于同一个路由器的许多不同的接口，如果这样对你的网络合适的话。并不需要对每个需要它的接口定义相同的访问列表。注意命令末端的参数 OUT，OUT是默认参数，它表示数据包将在从路由器到出站的路上进行过滤。因为 OUT是默认参数，所以可以省略，所以IP ACCESS-GROUP 101表示同样的意思。

如果将其用作网络 10.10.10.0的接口的入站数据包过滤，使用命令 IP ACCESS-GROUP 101 IN。

从本例中可看出，因为明确接受工作站 1，允许通过服务器A。然而第二个服务器被第二条语句禁止，网络 10.10.10.0上所有的系统都被禁止。初看，似乎工作站 1也被禁止，但这是DENY语句在第一条时的情况。记住，在IP访问列表中，顺序是十分重要的。

IP访问列表的另一个有趣的特征是语句末尾默认的 DENY参数。我在前面简单提过，它表示你必须明确允许通信量，否则自动设成禁止。基于这点，我们来看看图9-1所示的例子，实际上最后一行并不需要，它已经可推断出来。记住，这并不是没有访问列表的情况，如果你不给接口提供任何访问列表，或者提供一个未定义的访问列表，则默认情况下它将传递所有通信量。

访问列表建立后，任何对该表的增加都被放在表的末端，不幸的是，这表示你不能有选择地增加或删除语句。唯一可做的删除是删除整个访问列表，显然，当访问列表很大时是十分麻烦的。为了节省时间，你可以将表剪切，然后粘贴成文本文档来编辑。

当访问列表创建后，你需要将其与某个接口联系。该操作的格式为 IP ACCESS-GROUP ACCESS-LIST-NUMBER {IN|OUT}。在你想联系的接口的配置模式下输入该命令。

大多数参数都是不言自明的，参数 ACCESS-LIST-NUMBER是前面创建的访问列表的号码，参数IN|OUT表示是入站还是出站。如果你想让访问列表对两个方向都有用，则两个参数都要加上，一个表示入站，一个表示出站。对于每个协议的每个接口的每个方向，只能提供一个访问列表。

你也可以限制虚拟终端线路的通信量，这将使用 ACCESS-CLASS命令：

China-pub.com
下载


```
ACCESS-CLASS ACCESS-LIST-NUMBER {IN|OUT}
```

下面的例子表示只有子网10.10.10.0中的客户才可以与路由器的端口建立联系。

```
CONFIG TERMINAL
ACCESS-LIST 1 PERMIT 10.10.10.0 0.0.0.255
ACCESS-CLASS 1 IN
```

来自教室的信息

建立访问列表

记住隐式的DENY ANY

多少次，我像个疯子一样，在课堂上挥舞手臂、喊叫、恳求学生注意隐式的拒绝，然而只看见他们在试验中建立一个拒绝Telnet通信量的访问列表。然后，所有的动态获知路由从路由选择表中消失了，他们抱怨他们再也ping不通网络那边。“看看你们定义的通信量”，我说，“现在告诉我你允许了什么”。如果表中只有一个语句，而那个语句是拒绝的，则一旦你将该表作为通信量过滤，则关闭了该协议的所有接口。原因是隐式的DENY ANY。你的访问列表必须至少包括一条PERMIT语句。否则，你也许只节省了某些路由器的处理器周期，而没有在第一个位置配置接口的协议。

当你计划一个访问列表时，有两种不同的方法。如果你明确知道想允许的通信量，而且可用几条简单的语句描述出来，则可以明确允许那些通信量，拒绝其他的通信量。相反，如果你能够用几条简单的语句描述你想禁止的通信量，你可以明确拒绝那些通信量，然后用允许一切来结尾。这两种方法谈不上谁比谁好一些，但是尽可能少的语句可以节省CPU周期。

为提高性能，在访问列表使用几天后，你也许需要看看它看是否需要调整。记住路由器在找到第一个匹配数据包的语句时就停止工作，所以如果匹配的语句靠近表的前面，则会得到更好的性能。路由器会对表中的每条语句记录下匹配的次数，你可以利用这条信息来调整访问列表，使匹配次数多的语句在表头或者接近表头。注意，应将同一个网络或子网中特指的语句放在通用的语句前面。

注意，当你创建访问列表时，如果在开始配置访问列表语句之前就将其应用为某个接口的通信量过滤的话，则一旦在路由器配置中输入第一条语句，默认的 DENY ANY会起作用。先配置语句，然后检查几遍，最后将其应用于接口中会更好。

你可以将同样的表用于任意数量的接口，如果路由器中有20个不同的接口，所有的接口都有同样的约束，则可以重复使用同样的表。

这里最好做个文档，在你为网络保存的文档中，对于每一个访问列表、逐条语句，精确说明每条语句的功能。这有两个目的：如果可以这样描述表，表明你已经仔细思考过了；另外，由于我们都已经有太多的东西需要记忆，将来终有一天，它可以节省你的时间，使你不必再计算为何要拒绝此特定网络通信量。

最后记住隐式的DENY ANY。

—— Pamela Forsyth, CCIE, CCSI, CNX

China-pub.com 下载

9.2 认证目标9.02：扩展IP访问列表

扩展的IP访问列表可以更加细微地控制通信量。在访问列表中匹配数据包时，扩展 IP访问列表同时使用源地址和目标地址，你可以有选择地使用协议类型信息来优化控制。

许多在标准IP访问列表中使用的规则同样适用于扩展 IP。但也有一些不同，如下：

- 不能有选择地增加或删除表中的条目，当增加条目时，它放在表的底部。
- 访问列表本身不起任何作用，必须将其应用于某个接口。
- 在访问列表的结尾，默认情况下，有隐式的 DENY ALL语句。

增加或删除条目的语法格式如下：

```
{NO} ACCESS-LIST access-list-number {DENY | PERMIT} protocol source source-wildcard destination destination-wildcard
```

让我们来分解这条命令，首先输入的是 ACCESS-LIST命令，然后是访问列表的号码，紧跟的参数是说明允许或者拒绝特定的通信量。然后你需要指明将使用什么协议：如 TCP、UDP、ICMP或者IP。你可以告诉路由器明确的源地址和目标地址，也可以使用通配符例如 ANY。

这里是一个如何使用扩展IP访问列表的例子。图9-2显示了一个将限制特定IP通信量的网络。

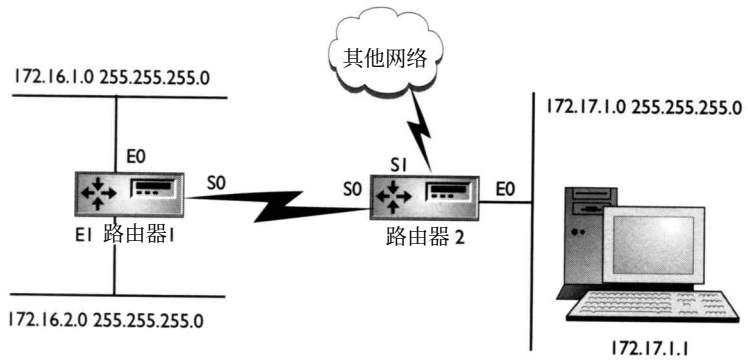

图9-2 在小型网络中限制IP通信量

网络管理程序配置路由器2使用如下访问列表：

```
ACCESS-LIST 102 PERMIT TCP 172.16.1.0 0.0.0.255 HOST 172.17.1.1 EQ TELNET
ACCESS-LIST 102 PERMIT TCP 172.16.2.0 0.0.0.255 HOST 172.17.1.1 EQ FTP
ACCESS-LIST 102 PERMIT ICMP 172.16.0.0 0.0.255.255 ANY
ACCESS-LIST 102 DENY IP ANY ANY
```

该访问列表用来作为Ethernet 0的出站通信量过滤，使用IP ACCESS-GROUP命令：

```
INTERFACE ETHERNET 0
IP ACCESS-GROUP 102 OUT
```

该访问列表是非常严格的， 172.17.1.0上唯一允许的通信量是来自网络 172.16.2.0上的Telnet，来自网络172.16.2.0到172.17.1.1上的FTP和到任何目的的ICMP通信量。其他所有的通信量都被禁止了。如果DENY IP ANY ANY语句没有在表中，访问列表还是一样工作，因为任何没有明确允许的通信量都将被禁止。注意IP协议，TCP应用Telnet和FTP中的关键字。

注意在路由器2的Ethernet 0接口的过滤下，网络172.16.1.0和172.16.2.0中的用户仍可以通

China-pub.com
下载

过路由器1的系列1接口访问其他的网络。考虑如果在路由器 1上配置相同的访问列表，在路由器1的串口0接口中使用IP ACCESS-GROUP 102 OUT命令时不同的效果。在新的配置下，网络172.16.1.0和172.16.2.0上的主机只能被允许向其他网络发送 ICMP通信量(如ping)。而从前还可以向主机172.17.1.1发送Telnet和FTP通信量。

9.3 认证目标9.03：命名访问列表

在IOS 11.2版中，你也可以使用命名访问列表。由于这是11.2版中新增加的功能，所以它并不向下兼容。通过命名列表，你可以标识IP访问列表，无论是标准型或者扩展型，用一个字母名字来代替号码。这可以使你突破原来标准99个扩展100个访问列表的限制。你不能假设所有使用号码的访问列表都可以使用名字。如果你选择使用名字，则模式和命令语法都会有所不同。

要使用这种访问列表，首先需要输入命令将模式转变到输入命名访问列表的方式： IP ACCESS-LIST STANDARD name or IP ACCESS-LIST EXTENDED name。

然后输入如下命令：{DENY | PERMIT} protocol source source-wildcard destination destination-wildcard。

对于普通的标准和扩展访问列表来说，使用的规则是一样的。上面的语法例子是扩展命名访问列表的，也可以变成匹配标准访问列表语法。

然后简单输入Exit退出访问列表配置状态。最后需要注意的是只有数据包和路由过滤可以使用命名访问列表。

检验IP访问列表

配置完IP访问列表后，你会想知道是否正确。你可以使用 SHOW ACCESS-LISTS命令和SHOW IP INTERFACES命令来检验IP访问列表。

SHOW ACCESS-LISTS命令显示路由器中所有的访问列表，包括IP、IPX和AppleTalk。这里是一些SHOW ACCESS-LISTS命令的输出结果，显示了路由器中配置的标准和扩展访问列表。

```
Router1#show access-lists
IPX access list 800
    deny C011
    permit FFFFFFFF
IPX access list 900
    permit any
    permit any any all AA11.00cf.b200.0000 0000.00ff.ffff all
    permit any BB22 all AA11
IPX SAP access list 1009
    deny FFFFFFFF 0 parallel
    permit FFFFFFFF
Standard IP access list 40
    deny   12.1.0.0, wildcard bits 0.0.255.255
    permit any
Standard IP access list list1
    deny   13.0.0.0, wildcard bits 0.255.255.255
    permit 172.16.0.0, wildcard bits 0.0.255.255
Extended IP access list 130
    permit ospf any any (452 matches)
    permit icmp any any echo (63 matches)
    permit icmp any any echo-reply (10 matches)
    permit tcp any any eq ftp
    permit tcp any any eq telnet (958 matches)
Extended IP access list list2
```

China-pub.com 下载

```
    permit ospf any any (12 matches)
    permit ip 136.25.16.0 0.0.7.255 any
    permit tcp host 10.1.0.1 any
Extended IP access list list3
    permit ospf any any
    deny   tcp any any eq telnet
    permit ip any any
Router1#
```

可以看到，SHOW ACCESS-LISTS命令显示了路由器中所有类型的访问列表的配置细节，而不单单是IP访问列表。我们可以在命令行中指定特定的访问列表号来单独显示一个访问列表。

我们可以看到不同 IP访问列表的配置。 list 40是标准的IP访问列表，拒绝任何从子网12.1.0.0中来的数据包，允许其余所有的。 list 130是扩展IP访问列表。我们可看到不同的协议关键字，允许任何的OSPF数据包、ping数据包、FTP数据包和Telnet数据包。

那么在list 130中拒绝了什么呢？所有其他的IP数据包！记住默认的DENY ANY。由于这是一个扩展的IP访问列表，而不是TCP或者ICMP，所以DENY ANY作用于所有的IP。

注意圆括号中的注释，它指示了每行匹配的次数。路由器记录了 IP访问列表中每行语句的匹配次数。从IP访问list 130的输出可以看出：

- 从将该访问列表用于接口后，收到了452个OSPF数据包。
- 63次对ping命令的响应(对邻近的路由器的ping的响应，这是一个输入数据包过滤)。
- 该路由器发出10次ping命令。
- 该接口收到958次Telnet数据包。

我们还可以看到三个名字 IP访问列表， list1、list2和list3。List1是一个标准IP访问列表。List2被应用了，有一些匹配。 List3在路由器配置中定义了，但没有应用于任何接口中，因此未用作数据包过滤。List3没有任何匹配。

SHOW IP INTERFACES命令提供了接口配置的IP指定方面的信息。它被专用来看什么数据包过滤应用于接口。它并不显示访问列表的内容，而只有访问列表的号码。你需要使用SHOW ACCESS-LIST <NUMBER>命令来看访问列表的过滤规则。数据包过滤在行“ Inbound access list is ”和“ Outgoing access-list is ”中指明。这里我们看到扩展IP访问列表130，作为串口1接口的入站数据包过滤。

```
Router1#show ip interface serial 1
Serial1 is up, line protocol is up
  Internet address is 10.1.0.2/16
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is enabled
Multicast reserved groups joined: 224.0.0.5 224.0.0.6
Outgoing access list is not set
Inbound  access list is 130
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is enabled
IP multicast fast switching is enabled
```

China-pub.com
下载


```
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
Probe proxy name replies are disabled
Gateway Discovery is disabled
Policy routing is disabled
Network address translation is disabled
```

9.4 认证目标9.04：标准IPX访问列表

IPX访问列表允许或禁止基于特定网络节点或使用特定协议和服务的经过接口的通信量。像IP访问列表中一样，访问列表中规则的顺序十分重要。第一个匹配的条目，不管是允许或拒绝都将执行。也和IP访问列表一样，没有明确地在末尾输入 Permit Anything，则隐含着在末尾DENY ALL。IPX访问列表中有两点需要重视，首先，如果你能过滤 NLSP、RIP和SAP的边界，则不能过滤NLSP区域。第二，标准IPX访问列表与IP表不同的是其同时过滤源地址和目标地址。

你可以将IPX访问列表分成五类，如表9-2所示。

表9-2 IP访问列表类型

类 型	通信量限制基于...	访问列表号码范围
标准访问列表	源和目标网络和节点地址	800~899
扩展访问列表	完整的源地址和目标地址(网络、节点、套接字和协议)	900~999
SAP访问列表	SAP类型、服务名和服务网络/节点地址	1000~1099
NLSP路由	网络区域	1200~1299
NetBIOS访问列表	基于名字的“ Host ”过滤，基于号码的“ bytes ”过滤	名字

在本节中，我们将主要讨论标准访问列表。SAP版本的访问列表常称作过滤器，下节讨论它。

标准访问列表允许或拒绝基于源网络号码的通信量。你也可以有选择地选用目标地址，或者甚至使用它们的掩码。标准 IPX访问列表的号码可以是从800~899中的任意数字。

```
ACCESS-LIST access-list-number {DENY | PERMIT}
SOURCE-NETWORK [OPTIONS]
```

SOURCE-NETWORK变量是八位十六进制的地址，从1到FFFFFFFD，指示数据包的来由。你也可以用0表示本地网络，用-1表示所有的网络。注意，我说过地址必须是八位十六进制的数字，但我将1作为有效的输入，这是因为前导零不需要表示出来，所以 1＝00000001。

看如图9-3所示的例子。我们希望中止网络 AA上的用户使用网络 BB上的服务，但是希望网络BB上的用户可以使用网络 AA上的服务。如果在 Ethernet 1上应用一个访问列表作为出站数据包过滤，则可以阻塞从网络 AA来的数据包。然而， Ethernet 0不需要访问列表，这样没有访问列表隐含有PERMIT ALL。如果访问列表中只用一个网络号来过滤，则网络 AA上对网络BB上用户的响应数据包也会被过滤出来。为了只过滤请求服务数据包而不过滤响应的数据包，我们需要知道服务器上服务的节点地址。让我们来看看这是如何工作的：

```
ACCESS-LIST 850 DENY ALL BB.072C.FA34.0075
ACCESS-LIST 850 PERMIT -1
```

我们使用IPX ACCESS-GROUP命令将该表作为Ethernet 1的数据包过滤。

China-pub.com 下载

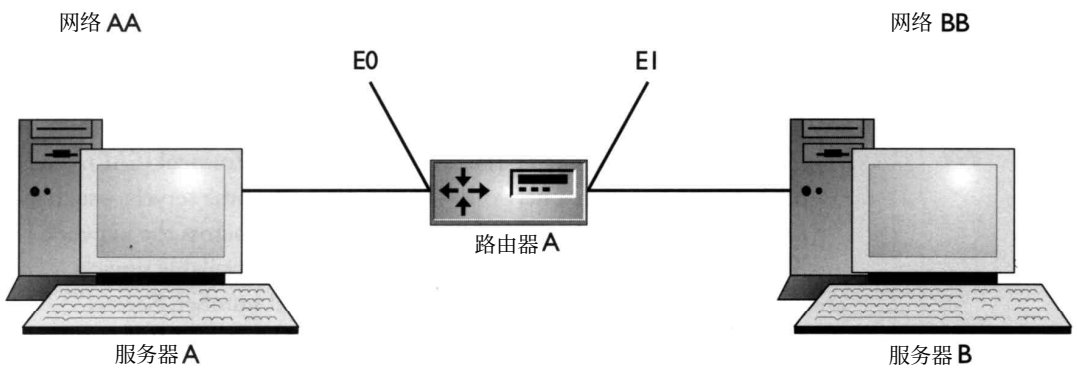

图9-3 标准IPX访问列表用作数据包过滤

该访问列表的效果是所有从网络 AA到服务器B的数据包，当它们经过路由器 A的Ethernet 1的接口时将被阻塞，而从服务器 A到网络BB上的用户的数据包将被最后一行语句允许。 IPX访问列表中的PERMIT -1与IP中的PERMIT ANY效果相同。

9.5 认证目标9.05：IPX SAP过滤

通过使用服务通告协议(Service Advertising Protocol，SAP)，所有NetWare网络类型服务器可以动态通告它们的服务和地址。网络的其余组成部分——除了其他的服务器——例如路由器，保存了一份完整的网络上可用的服务列表，这些服务同步通告可使用服务的列表。

每个SAP服务用一个十六进制数字来辨识，一些普通的例子如文件服务器 -4，打印服务器-7和远程网桥服务器(路由器)-24。Cisco路由器并不转发每个它收到的广播，而是按照计划好的间隔定时通告整个 SAP表，默认情况下每60秒一次。Cisco路由器像NetWare服务器一样，它们从其他服务器和路由器上接受 SAP广播，然后建立它们内部的 SAP表。

由于通过WANS上的广播类型的通信量是应该尽可能避免的， SAP需要被过滤，过滤可同时用于入站和出站通信量。为使该功能更加有效， Cisco IOS允许你指定需要加入SAP表中的服务。这可用命令IPX INPUT-SAP-FILTER {access-list-number|name}来完成。图9-4是一个例子。

如果想为路由器 1配置一个SAP过滤，用来过滤服务器 A的通告而允许段上的其他服务器的通告，应该在全局配置模式下输入下面的命令：

```
ACCESS-LIST 1001 DENY IA01.0000.0000.0001
ACCESS-LIST 1001 PERMIT -1
```

第一条语句拒绝所有从 IPX地址1a01.0000.0000.0001来的服务。在真实的 Novell网络中，节点地址0000.0000.0001总是指示NetWare服务器的内部IPX网络号，这是所有服务器中服务的地址，所以这条语句的效果是拒绝所有从内部 IPX网络号是1a01的服务器的服务， -1是IPX访问列表中指示所有网络的方法。

有两种方法来使用访问列表，如果根本不想让服务器 A的服务条目被路由器 1的SAP表接受，可在Ethernet 0的接口配置模式下，使用命令IPX INPUT-SAP-FILTER 1001将访问列表作为输入SAP过滤。

数字1001明显是指示访问列表 1001，该命令的效果是，在 Ethernet 0的接口接受的所有

China-pub.com
下载

SAP数据包中，路由器1会检查该数据包，过滤掉所有服务地址为 1a01.0000.0000.0001的数据包。注意路由器在SAP数据包中检查单独的条目来查找这个地址，而不是在 SAP数据包的IPX头中的源地址。

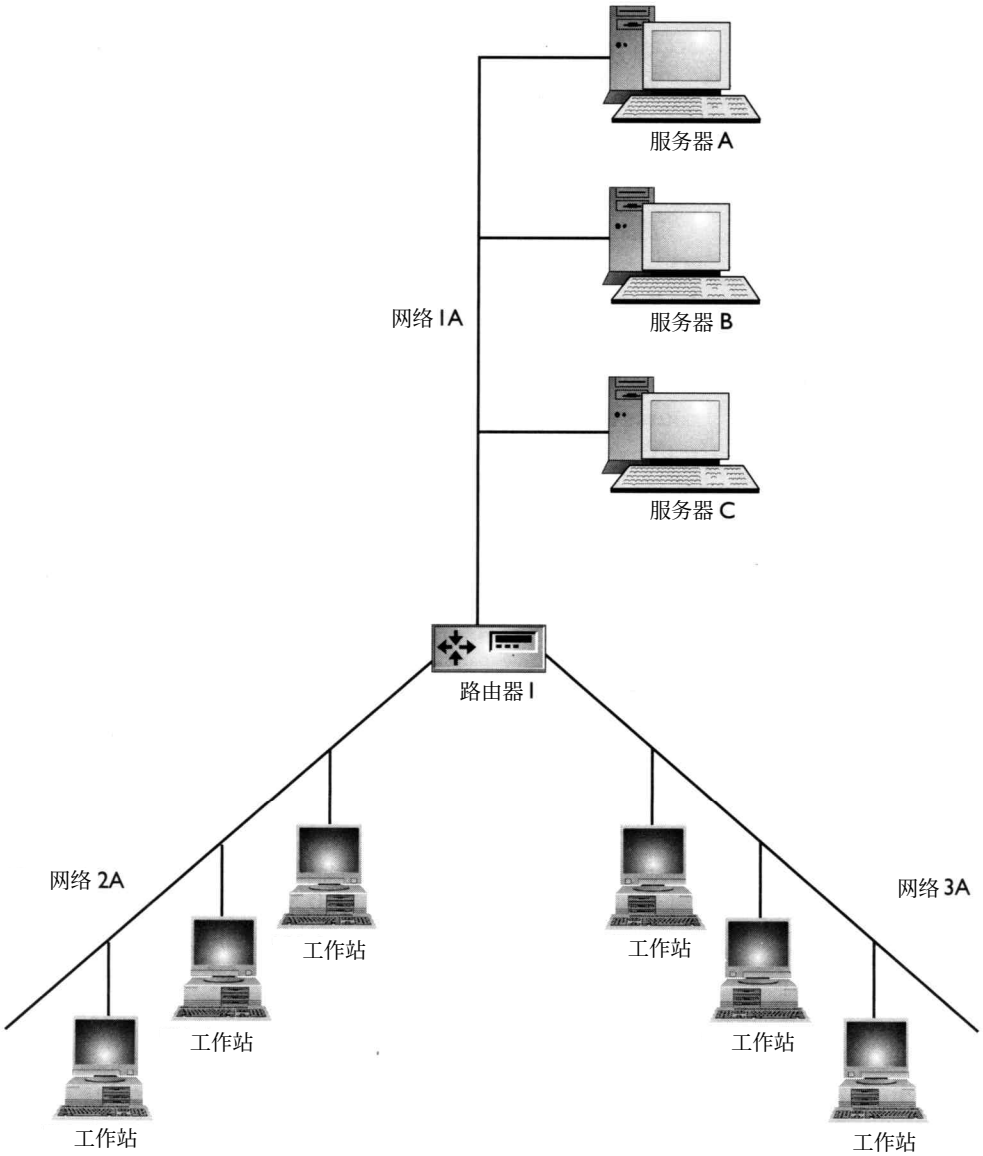

图9-4 IPX网络中的SAP过滤

第二种使用该表的方法是输出 SAP过滤，假设我们希望网络 1a01的服务通告在网络 2a上而不通告在网络3a上。如果在Ethernet 0上使用输入SAP过滤，则将阻塞所有的通告。但是如果在Ethernet 1上使用输出SAP过滤，则路由器将过滤掉SAP条目中服务地址是1a01.0000.0000.0001的数据包。用来配置一个输出 SAP过滤的命令是IPX OUTPUT-SAP-FILTER 1001，这个命令和INPUT-SAP-FILTER命令一样，是接口配置命令。

在SAP访问列表中，还有两种其他的方式，我们可以通过协议类型和服务名来过滤。如

China-pub.com 下载

果想通过名称来过滤服务器A的服务，可以用像如下的语句：ACCESS-LIST 1001 DENY -1 0 SERVERA。

这里，“-1”指任何网络，“0”指所有的服务类型，即使指定了ANY和ALL，这些参数仍然是必须的，用来维护语句的语法。SERVERA显然是路由器检查SAP条目时过滤的字符串。这些字符串是大小写相关的，所以最好检查SHOW IPX SERVERS命令的输出来看看精确的字符串名。

假设我们只想过滤服务器A上类型4的文件服务，有两种方法。第一个是指定服务类型4的内部IPX网络号，用命令ACCESS-LIST 1001 DENY 1A01 4实现。

1A01是服务器A上的IPX内部网络号的网络服务地址，我们并不实际需要节点地址。如果我们指定内部IPX网络号，则节点总是0000.0000.0001，而没有其他网络上的节点，所以可以不考虑它。“4”代表类型4服务，所以只有服务器A上的文件服务被拒绝。

我们也可以使用字符串SERVERA来过滤服务器A上的类型4服务：ACCESS-LIST 1001 DENY -1 4 SERVERA。

我们用-1指定所有的网络，但这次用类型4跟着字符串SERVERA来代替所有的服务。不要忘记：所有的访问列表在末尾隐含有DENY ALL，所以，如果不在访问列表的其他地方允许一些服务，则所有的SAP将被筛除。

IPX SAP的另一部分是获取最近服务器(Get Nearest Server，GNS)请求。GNS是Novell客户发出的数据包用来请求未指定服务器的服务，最近的NetWare服务器用另一个SAP来响应提出的服务。GNS响应将一个可用的服务器源分配给客户，客户然后登录到服务器上。一旦客户登录到服务器上，他就可以直接得到服务器的服务，不再需要进一步的GNS。如果GNS请求被一个Cisco路由器收到，它能够使SAP表中的第一个服务器作出响应。只有当是已知的本地服务器时，这才能发生，因为它实际上是第一个响应的。你可以用命令IPX OUTPUT-GNS-FILTER access-list-number来创建一个GNS过滤。

刚开始时，本地服务器应是第一个响应的，如果在你的Novell IPX网络上没有发生，你可设置一个GNS延迟。延迟用1/100秒来计算，默认情况没有延迟：IPX GNS-RESPONSE-DELAY milliseconds。

如果你想看看通过SAP，哪些网络上的IPX服务器被禁止了，可以使用命令SHOW IPX SERVERS {UNSORTED} | {SORTED[NAME|NET|TYPE]} {REGEXP NAME}。默认情况下，输出按照SAP服务类型的号码排序。

你可以通过改变参数UNSORTED和SORTED来改变默认的顺序。UNSORTED没有顺序显示IPX服务器。SORTED允许你按照服务器名(NAME)、网络号(NET)或者默认的SAP服务类型(TYPE)来排序。参数REGEXP NAME只显示匹配你列出的名字或表达式的IPX服务器。

下面是一个SHOW IPX SERVERS命令的输出例子。

```
east#show ipx servers
Codes: S - Static, P - Periodic, E - EIGRP, N - NLSP, H - Holddown, + =
       detail
10 Total IPX Servers

Table ordering is based on routing and server info

   Type Name                    Net      Address     Port      Route Hops Itf
S     4 EAST-D04                B00D.0000.0000.0001:0451       conn    2  Lo13
S     4 EAST-F04                B00F.0000.0000.0001:0451       conn    2  Lo15
```

China-pub.com
下载


```
P     4 DABNEY              BBBB0002.0000.0000.0001:0451      2/01   1  Et0.2
P     4 DESTINY             AAAA0001.0000.0000.0001:0451      2/01   1  Et0.2
N     4 WEST-D04                C0OD.0000.0000.0001:0451     82/02   4  Se0
N     4 WEST-F04                C0OF.0000.0000.0001:0451     82/02   4  Se0
P    47 PRINTSRV            BBBB0002.0000.0000.0001:8060      2/01   2  Et0.2
P   107 DABNEY              BBBB0002.0000.0000.0001:8104      2/01   2  Et0.2
P   26B UNIVERSE_1_________ AAAA0001.0000.0000.0001:0005      2/01   1  Et0.2
P   278 UNIVERSE_1_________ AAAA0001.0000.0000.0001:4006      2/01   1  Et0.2
```

服务器按照服务类型号排序。类型 4是文件服务，需要登录 (在Novell术语中称作普通服务)。这些服务器将被用作路由器的GNS响应。

如果你想建立一个基于地址的 SAP过滤，则可以看“ net.address ”列，注意地址都是0000.0000.0001。这是因为服务是用服务器上的内部 IPX网络号来通告的，而不是用 NIC的物理地址。这个内部IPX网络号是SAP过滤器用来过滤的。你可以通过匹配它们的内部 IPX网络号来看那些服务是在哪个物理服务器上的。

检验IPX访问列表配置

命令SHOW IPX INTERFACES使你能浏览所有能为 IPX数据包、路由、路由器 SAP和NetBIOS数据包设置的不同类型的过滤。 Cisco IOS有很多在网络上帮助你管理IPX通信量的命令，所有这些参数都是可以配置的。

```
east#show ipx interface ethernet 0.2
Ethernet0.2 is up, line protocol is up
  IPX address is D.0000.0c47.6643, NOVELL-ETHER [up]
  Delay of this IPX network, in ticks is 1 throughput 0 link delay 0
  IPXWAN processing not enabled on this interface.
  IPX SAP update interval is 1 minute(s)
  IPX type 20 propagation packet forwarding is disabled
  Incoming access list is 800
  Outgoing access list is not set
  IPX helper access list is not set
  SAP GNS processing disabled, delay 500 ms, output filter list is 1000
  SAP Input filter list is not set
  SAP Output filter list is 1013
  SAP Router filter list is not set
  Input filter list is not set
  Output filter list is not set
  Router filter list is not set
  Netbios Input host access list is not set
  Netbios Input bytes access list is not set
  Netbios Output host access list is not set
  Netbios Output bytes access list is not set
  Updates each 60 seconds, aging multiples RIP: 3 SAP: 3
  SAP interpacket delay is 55 ms, maximum size is 480 bytes
  RIP interpacket delay is 55 ms, maximum size is 432 bytes
  IPX accounting is disabled
  IPX fast switching is configured (enabled)
  RIP packets received 294, RIP packets sent 152
  SAP packets received 295, SAP packets sent 150
```

注意黑体的行，“ Incoming access list is 800 ”表示路由器的入站数据包过滤命令是 IPX ACCESS-GROUP 800 IN。“ SAP Output filter list is 1013 ”表示访问列表1013通过命令IPX OUTPUT-SAP-FILTER 1013作为输出SAP过滤。

命令SHOW ACCESS-LISTS将显示所有的访问列表，而不仅仅是IP或者IPX。在下面的例

China-pub.com 下载

子里，同时显示了路由器上配置的 IP和IPX访问列表。如果你只想单独显示 IPX访问列表，使用访问列表号作为命令的一个参数。

```
Router1#sh access-lists
IPX access list 800
    deny C011
    permit FFFFFFFF
IPX access list 900
    permit any
    permit any any all AA11.00cf.b200.0000 0000.00ff.ffff all
    permit any BB22 all AA11
IPX SAP access list 1000
    deny B00F 47
    permit FFFFFFFF
IPX SAP access list 1009
    deny FFFFFFFF 0 parallel
    permit FFFFFFFF
IPX SAP access list 1013
    deny C000.0000.0000.0000 F.ffff.ffff.ffff
    deny FFFFFFFF 47 E*
    permit FFFFFFFF
Standard IP access list 40
    deny   12.1.0.0, wildcard bits 0.0.255.255
    permit any
```

9.6 认证目标9.06：AppleTalk访问列表

访问列表通常有三种实现方式。最常见的方法是使用它们控制通过一个接口的数据包。也可以通过DDR连接用它们来指定有兴趣的通信量，或者控制路由选择更新。 AppleTalk网络上的访问列表基本上类似于 IP和IPX访问列表。你可用 600~699之间的数字来引用访问列表，表中可以加入任意多的访问列表命令。

在配置模式下，输入下述命令建立访问列表： ACCESS-LIST access-list-number {DENY|PERMIT} options。

参数access-list-number是600~699之间的数字，用来引用你增加或创建的表。参数PERMIT或DENY用来允许或拒绝特定类型的通信量。

AppleTalk访问列表可分为两种基本类型： AppleTalk类型和IP类型。AppleTalk类型访问列表基于AppleTalk区和NBP名字实体。NBP就是名字绑定协议(Name Binding Protocol)，它是AppleTalk地址的映像网络名。它使你在网络实体层次上控制网络访问。你可以使用映像名来允许或拒绝从特定 NBP实体上来的NBP数据包，或者特定区域里所有的 NBP实体上来的数据包。NBP实体的名字也可称作NBP元组。

一个AppleTalk区域是一个逻辑上的网络组，每个 AppleTalk网络的结构基于两种 Phase之一：Phase 1网络是为工作组设计的，只能有一个区域； Phase 2网络比Phase 1有许多改进之处，包括有为大型网络设计的路由选择功能。 Phase 2网络可以最多有 255个区域。使用 AppleTalk类型的一个好处是在增加新网段时，不需重新配置每个路由器。这是因为在你定义逻辑实体访问时，它并不考虑拓扑关系。这个功能是 IP类型所没有的。

要建立基于区域的访问列表，在配置模式下输入下述命令： ACCESS-LIST access-list-number {PERMIT|DENY} ZONE zonename。

参数zonename可以包括Apple Macintosh类型的特殊字符，如果你想用特殊字符，则在冒

China-pub.com
下载

号后输入对应的两个十六进制数。如果zonename的第一个字符是空格，则输入:20。

你可以为特定的NBP实体定义访问列表，例如同一类型的 NBP实体像打印机，或者属于同一区域的NBP实体。要为NBP名字实体建立访问列表，可在配置模式下遵循下面的语法：ACCESS-LIST access-list-number {PERMIT|DENY} NBP seq {type|object|zone} STRING。

参数seq表示顺序号，它使你能将NBP名字的两三部分联系起来，即使你不想联系名字的部分，这个参数仍是必须的，它使你能在实体层次上允许或拒绝数据包。顺序号还可记录访问列表中的NBP实体数。参数STRING表示实体名的类型、对象或者区域。同样， Macintosh字符和前导空格也是允许的。下面是一个例子，转发所有的数据包，但从区域 sales和AFPServer型的服务器来的数据包除外。

```
ACCESS-LIST 601 DENY NBP 1 ZONE SALES
ACCESS-LIST 601 DENY NBP 1 TYPE AFPSERVER
ACCESS-LIST 601 PERMIT OTHER-NBPS
ACCESS-LIST 601 PERMIT OTHER-ACCESS
```

AppleTalk和IP或IP访问列表的一个区别是不用考虑命令的顺序。在 IP和IPX访问列表中，数据包在命令中查找第一次匹配的规则，然后立即执行。在 AppleTalk中，顺序是不重要的，因为你不能在一个表中用另一个条目来覆盖前一个条目。下面是一个简单的覆盖的例子，当你覆盖规则时，后一条会覆盖前一条，然后将前一条删除。

```
ACCESS-LIST 601 PERMIT NETWORK 10
ACCESS-LIST 601 DENY NETWORK 10
```

如果在一个路由器上输入这个例子， SHOW RUN命令只会列出ACCESS-LIST 601 DENY NETWORK 10语句。

如果你有一个多区域网络，只想拒绝某些访问，可以明确定义要拒绝的，然后在末尾加上PERMIT OTHER-ACCESS语句。例如，想允许所有区域的访问，除了 Sales和Accounting区域，可以输入以下语句：

```
ACCESS-LIST 601 DENY ZONE SALES
ACCESS-LIST 601 DENY ZONE ACCOUTING
ACCESS-LIST 601 PERMIT ADDITIONAL-ZONES
```

IP类型的访问列表基于网络号，如果使用这种类型，通过限制网络号和区域，它会防止对冲突网络号的分配。如前所述，它有一个最大的缺点是它忽略 AppleTalk区建立的逻辑映像。如果增加或改变网络的拓扑结构，你不得不重新配置路由器来适应改变。

IP类型访问列表既可以用于网络上也可以用于电缆范围。要为一个不扩展的孤立网络定义访问列表，可在配置模式下输入下述命令：ACCESS-LIST access-list-number {PERMIT|DENY} NETWORK network。

例如，你有两个网络，你想拒绝网络 1的数据包，但允许网络 2的数据包，可以使用下述访问列表：

```
ACCESS-LIST 601 DENY NETWORK 1
ACCESS-LIST 601 PERMIT NETWORK 2
```

如果你想为一个扩展网络的电缆范围设置访问列表，可在配置模式下输入下述命令：ACCESS-LIST access-list-number {PERMIT|DENY} CABLE-RANGE cable-range。

China-pub.com 下载

例如，你想转发所有从电缆范围200~250来的数据包，但是禁止从电缆范围300~350来的数据包，可以输入如下语句：

```
ACCESS-LIST 601 PEMIT CABLE-RANGE 200~250
ACCESS-LIST 601 DENY CABLE-RANGE 300~350
```

Cisco IOS提供了定义AppleTalk访问列表的功能，既能为扩展网络也能为非扩展网络，它们都完全包括特定的电缆范围：

```
ACCESS-LIST6 access-list-number {PERMIT|DENY} WITHIN cable-range
```

下述的例子允许任何网络和电缆范围200~250之间的所有访问：

```
ACCESS-LIST 601 PERMIT WITHIN 200~250
```

你也可以将参数WITHIN改为INCLUDES，这样提供更加灵活的网络包括功能，在下述例子中，允许任何包括网络200~250任意部分的网络。

```
ACCESS-LIST 601 PERMIT INCLUDES 200~250
```

你还可以允许或拒绝包括电缆范围或网络号区域的扩展或非扩展网络访问：

```
ACCESS-LIST access-list-number {PERMIT|DENY} INCLUDES cable-range
```

问 题 与 答 案

我添加了到一个新服务器的一个IP访问列表条目，但仍然无法访问它。	确定在访问列表开头有显式的允许语句(执行第一个匹配的语句)。
我在路由器上增加了如下语句，但它似乎并不工作： ACCESS-LIST 550 DENY NBP 1 ZONE SALES	AppleTalk访问列表的范围是600~699。将550改为该范围内的数字。
我该使用AppleTalk访问列表的哪种方式：IP或AppleTalk类型？我需要最有灵活性的方案。	AppleTalk可能是更好的选择，在改变网段时，你不需重新配置路由器。
一个网络上的服务器看不到其他网络上的服务器，但其他网络上的服务器却看得见它。我该查哪里呢？	检查你的绑定在另一边接口，能看到其他网络的SAP过滤。
使用协议分析器时，我看到我的64Kbps的连接上有许多远程服务器的请求，我该如何减少它们呢？	使用输出GNS过滤，使路由器不响应这些远程服务器的GNS请求。

9.7 认证总结

在IP访问列表中，源地址或目标地址用来检测表中的条目。第一个匹配的条目用来决定该数据包是应被允许还是拒绝。因为第一个匹配的语句将执行，所以条目的顺序是十分重要的。在建立IP表时，如果没有任何合适的规则，则默认拒绝。正确的允许或拒绝的语法如下：

China-pub.com
下载

ACCESS-LIST access-list-number {DENY|PERMIT} {SOURCE[source-wildcard]ANY}

IPX访问列表基于特定的网络节点或使用特定协议或服务的消息来允许或拒绝通信量。像在IP访问列表中一样，表中各条目的顺序是十分重要的。第一个匹配的条目，不管是 PERMIT还是DENY都将执行。同样，类似 IP表，如果你不在表尾明确输入 PERMIT EVERYTHING，则默认为DENY ALL。基本IPX访问列表的语法如下：

ACCESS-LIST access-list-number {DENY|PERMIT} SOURCE-NETWORK[OPTIONS]

通过使用服务通告协议(Service Advertisement Protocol，SAP)，所有NetWare网络类型服务器可以动态通告它们的服务和地址。网络的其余组成部分 —— 除了其他的服务器 —— 例如路由器，保存了一份完整的网络上可用的服务列表，这些服务同步通告可使用服务的列表。你可以使用命令ACCESS-LIST 1001 DENY 1A01.0000.0000.0001拒绝SAP类型的通信量。

AppleTalk访问列表可分为两种基本类型： AppleTalk类型和IP类型。AppleTalk类型访问列表基于AppleTalk区和NBP名字实体。NBP就是名字绑定协议(Name Binding Protocol)，它是AppleTalk地址的映像网络名。它使你在网络实体层次上控制网络访问。你可以使用映像名来允许或拒绝从特定 NBP实体上来的NBP数据包，或者特定区域里所有的 NBP实体上来的数据包。NBP实体的名字也可称作NBP元组。正确建立AppleTalk访问列表的语法是：

ACCESS-LIST access-list-number {DENY|PERMIT} options

9.8 2分钟练习

• 在Cisco路由器上，可通过使用访问列表来执行数据包过滤。访问列表可用来控制网络上数据包的传递，限制虚拟终端线路上的通信量或者控制路由选择更新。

• IP访问列表是关于IP地址的允许和拒绝规则的集合。

• Cisco IOS 11.1版在访问列表的语法和执行上有显著的改变。

• 有三种基本的IP访问列表：标准型、扩展型和动态扩展型。

• 增加标准访问列表的基本格式如下：

ACCESS-LIST access-list-number {DENY|PERMIT}
{SOURCE[source-wildcard]|ANY}

• 扩展IP同时使用源地址和目标地址，你可以有选择地使用协议类型信息来优化控制。

• 增加或删除访问列表的语法格式如下：

{NO} ACCESS-LIST access-list-number {DENY | PERMIT} protocol source source-wildcard destination destination-wildcard

• 通过命名列表，你可以标识IP访问列表，无论是标准型或者扩展型，用一个字母名字来代替号码。

• 你可以使用SHOW ACCESS-LISTS命令和SHOW IP INTERFACE命令来检验你的IP访问列表。

• IPX访问列表允许或拒绝基于特定网络节点或使用特定协议和服务数据的经过接口的通信量。

• 通过使用服务通告协议(Service Advertising Protocol，SAP)，所有NetWare网络类型服务器可以动态通告它们的服务和地址。

• 命令SHOW IPX INTERFACES使你能浏览所有能为IPX数据包、路由、路由器SAP、和

China-pub.com 下载

NetBIOS数据包设置的不同类型的过滤。

- 命令SHOW ACCESS-LISTS将显示所有的访问列表，而不仅仅是IP或者IPX。
- AppleTalk网络上的访问列表基本上类似IP和IPX访问列表。
- AppleTalk访问列表可分为两种基本类型： AppleTalk类型和IP类型。

9.9 自我测试

下面的问题将帮助你检查你对本章中材料的理解程度，仔细读下面的选项，可能有不止一个正确答案。选出每个问题中的正确答案。

1) Match which of these protocols go with which access list range (匹配下列协议和访问列表范围)？

A. Novell SAP ① 800~899
B. AppleTalk ② 1000~1099
C. Novell ③ 1~99
D. IP ④ 600~699

2) What happens to access lists previously created if the IOS is upgraded from version 10.1 to 11.1 (如果IOS从10.1版升级到11.1版时，以前创建的访问列表会发生什么事情)？

A. They are dropped since they are no longer applicable
B. Access lists didn’t exist prior to version 9.1
C. They will be converted to the new format
D. They will be left alone since IOS 11.1 provides backward compatibility

3) In what ways are access lists typicallyimplemented on AppleTalk networks (在AppleTalk网络中，通常访问列表是如何实现的)？

A. To control packets transmitted across an interface
B. To specify interesting traffic to launch a DDR connection
C. To restrict SAP broadcasts
D. To advertise available servers

4) What do NetWare servers do to advertise their services and addresses to other servers (NetWare服务器如何对其他服务器通告其服务和地址)？

A. Broadcast NetBIOS packets
B. Register with an SAP server
C. Broadcast SAP packets
D. Register with a NetBIOS server

5) In the event of no matching rule being found in an IP access list, what happens to the transmission packet at the end (在IP访问列表中，如果到最后也没有找到匹配，则传输数据包将如何)？

A. It is dropped
B. It is allowed to pass
C. A broadcast is sent out notifying the sending host
D. A Packet Return (PR) is issued to the sending host

China-pub.com
下载

6) For which of the following reasons are IP-style AppleTalk access lists implemented (下列哪个是IP类型AppleTalk访问列表实现的原因)？

A. For controlling the disposition of networks that overlap a network number range

B. For controlling the disposition of networks that are contained within a network number range

C. For controlling the disposition of networks that no longer exist within a network number range

D. For controlling the disposition of networks that exactly match a network number range

7) Which of the following statements are true regarding IP access lists (考虑IP访问列表，下列哪个陈述是正确的)？

A. After an access list is created, any additions to that list are placed at the end

B. You can't selectively add or remove items

C. You need to explicitly associate the access list to whatever it is you are intending to use it for, such as an interface

D. There is an implicit DENY statement at the end

8) On what basis do IPX access lists permit or deny traffic (IPX访问列表基于什么允许或拒绝通信量)？

A. Specified network nodes

B. Messages sent using a particular ICMP

C. Messages sent using a particular protocol

D. Messages sent using a particular service

9) How often does a Cisco router broadcast periodic SAP advertisements (Cisco路由器广播SAP通告的周期是多长时间)？

A. As soon as it receives the complete packet

B. Every 30 Seconds

C. Every 60 Seconds

D. Every 300 Seconds (5 Minutes)

10) What is GNS (GNS是什么)？

A. An ICMP connectivity error packet

B. Generic NetWare Service (Allows a Cisco router to appear as a NetWare server)

C. AppleTalk's default network routing algorithm

D. A packet sent out to request specific services from servers

11) Which of the following are valid types of IPX access lists (下列哪个是有效的IPX访问列表类型)？

A. SAP

B. NetBIOS

C. ICMP

D. Extended

12) What are the two basic styles of AppleTalk lists (两种基本的AppleTalk表样式是什么)？

China-pub.com 下载

A. AppleTalk style

B. Macintosh style

C. NBP style

D. IP style

13) Which of the following are true statements regarding Phase 1 and Phase 2 AppleTalk networks (下面哪些是关于Phase 1和Phase 2 AppleTalk网络的正确描述)？

A. Phase 1 networks are more efficient at WAN communication

B. Phase 2 networks can have up to 255 zones

C. Phase 1 networks can have only 1 zone

D. Phase 2 networks introduced routing

14) How should you arrange your entries in AppleTalk access lists (你该如何安排AppleTalk访问列表中的条目顺序)？

A. The order doesn't matter

B. From the most specific to the most general

C. From the most general to the most specific

D. Zones first, followed by systems

15) What will happen to packets that cross an interface where no access list has been defined (当数据包经过一个未定义访问列表的接口时会如何)？

A. They will be discarded

B. They will be allowed to pass through

C. They will be queued up

D. They will be returned to the sending host

16) Which of the following examples follow the correct syntax for adding special Macintosh characters in zone names (下列哪个例子正确表达了在区域名中加入特殊 Macintosh字符的语法)？

A. /B2

B. -B2

C. [B2]

D. :B2

17) Which of these are valid types of IP access lists (下列哪些是有效的IP访问列表类型)？

A. Dynamic

B. Dynamic Extended

C. Extended

D. Standard

18) Which of the following examples uses the correct syntax to define an AppleTalk access list for an extended or a non-extended network that is completely contained within a specific cable-range (下列哪些例子正确定义了 AppleTalk访问列表，既能为扩展网络也能为非扩展网络，且完全包括特定的电缆范围)？

A. ACCESS-LIST 599 PERMIT WITHIN 100~150

China-pub.com
下载

B. access-list permit 225~240 within 699

C. access-list permit 225~240 within 599

D. access-list 699 permit within 100~150

19) Which of the following statements regarding SAP broadcasts is correct (考虑SAP广播, 下列哪个陈述是正确的)？

A. SAP-type broadcasts do not work well across WANs

B. Each SAP service is identified by an eight-digit binary number

C. Because of sequencing issues, the times between SAP table updates cannot be changed

D. SAP stands for Secondary Addressing Protocol

20) Consider the following access list:

ACCESS-LIST 50 DENY 136.120.3.1

ACCESS-LIST 50 DENY 143.22.1.0 0.0.0.255

Which statement represents the most complete description of the results of applying this list as a packet filter (考虑下述访问列表：

ACCESS-LIST 50 DENY 136.120.3.1

ACCESS-LIST 50 DENY 143.22.1.0 0.0.0.255

下列哪个陈述最完全地描述了访问列表作为数据包过滤的结果)？

A. It will deny all traffic destined for any host on network 136.120.3.0

B. It will deny all traffic destined for network 143.22.1.0

C. It will deny all traffic from the host at 136.120.3.1

D. It will deny all IP traffic

21) Which command would be used to configure a packet filter for IP traffic (下列哪个命令可用来配置IP通信量的数据包过滤)？

A. ROUTER(CONFIG-IF)#IP ACCESS-LIST 100

B. Router(config-if)#ip access-group 42

C. Router(config)#access-group 102

D. Router(config-if)#access-group 75

E. Router(config-if)#ip output-packet-filter 112

22) Which command would be used to configure an inbound packet filter for TCP traffic (下列哪个命令可用来配置TCP通信量的入站数据包过滤)？

A. ROUTER(CONFIG-IF)#TCP PACKET-FILTER 101

B. Router(config-if)#ip packet-filter 101 in

C. Router(config-if)#ip access-group 99 in

D. Router(config-if)#ip access-group 100 in

E. Router(config-if)#ip access-group 100

23) The address mask pair 172.16.64.0 0.0.3.255 specifies which range of IP addresses (地址掩码对172.16.64.0 0.0.3.255指定了什么IP地址范围)？

A. 172.16.64.255 through 172.16.67.255

B. 172.16.67.0 through 172.16.70.255

China-pub.com 下载

C. 172.16.64.0 through 172.16.67.255

D. 172.16.63.0 through 172.16.64.255

24) The following statement appears in an IP extended access list:

ACCESS-LIST 125 PERMIT IP ANY HOST 136.25.2.128

What does this line permit (下述是IP扩展访问列表中的语句：

ACCESS-LIST 125 PERMIT IP ANY HOST 136.25.2.128

HOST 136.25.2.128

该行允许了什么)？

A. Any IP traffic from host 136.25.2.128

B. IP traffic to any host on network 136.25.2.128

C. IP traffic from any address to the host at 136.25.2.128

D. The statement is invalid because there is no mask

25)The following access list, containing only one line, is applied as a packet filter on an interface.

ACCESS-LIST 100 PERMIT TCP 145.22.3.0 0.0.0.255 ANY EQ TELNET

What is the best description of the traffic that is denied by the implicit DENY ALL (下述访问列表，只有一行，用作一个接口的数据包过滤

ACCESS-LIST 100 PERMIT TCP 145.22.3.0 0.0.0.255 ANY EQ TELNET

对于隐含的DENY ALL，最合适的描述是什么)？

A. All IP traffic

B. All Telnet traffic

C. All TCP traffic

D. All TCP traffic except Telnet