配置常用的IP ACL

Contents

Introduction

本文档提供了常用 IP 访问控制列表 (ACL) 的配置示例，ACL 将根据以下内容过滤 IP 数据包：

- 源地址
- 目的地地址
- 信息包的类型
- 这些项目的任何组合

为了过滤网络流量， ACL控制路由信息包是否转发或被阻拦在路由器接口。您的路由器是否检查每个信息包为了确定转发或丢弃根据您在ACL内指定的标准的信息包。ACL标准包括：

- 数据流的源地址
- 数据流的目的地地址
- 上层协议

完成这些步骤为了修建ACL，在本文的示例显示：

1. 创建ACL。
2. 适用ACL于接口。

IP ACL是许可证的连续收藏并且拒绝适用于IP信息包的情况。条件的路由器测试信息包在一次一个ACL。

第一匹配确定Cisco IOS软件是否接受或拒绝信息包。由于Cisco IOS软件在第一匹配以后终止测试条件，条件的命令是重要。如果情况不配比，路由器拒绝信息包由于含蓄拒绝所有条款。

这些是的IP ACL示例可以在Cisco IOS软件被配置：

- 标准ACL
- 扩展ACL
- 动态(锁和密钥) ACL
- IP已命名ACL
- 自反ACL
- 使用时间范围的基于时间的ACL
- 被评论的IP ACL条目
- 基于上下文的ACL
- 身份验证代理
- Turbo ACL
- 基于时间的分布式ACL

本文讨论一些常用的标准和扩展ACL。参考配置IP访问列表关于支持Cisco IOS软件不同种类的ACL的更多信息和如何配置和编辑ACL。

标准ACL的命令语法格式是**访问列表access-list-number {许可证|拒绝} {主机|来源source-wildcard|其中任一}**。

标准ACL与在ACL为了控制数据流配置的地址比较IP信息包的源地址。

扩展ACL与在ACL为了控制数据流配置的地址比较IP信息包的源地址和目的地址。您能也做扩展ACL粒状和配置对过滤流量由标准例如：

- 协议
- 端口号
- 差分服务代码点值
- 优先值
- 同步序号(SYN)位的状态

扩展ACL命令语法格式是：

IP

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
  {deny | permit} protocol source source-wildcard destination
    destination-wildcard
  [precedence precedence] [tos tos] [log | log-input]
    [time-range time-range-name][fragments]
```

互联网控制消息协议(ICMP)

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit}
 icmp source source-wildcard destination destination-wildcard [icmp-type
 [icmp-code] | [icmp-message]] [precedenceprecedence] [tos tos] [log |
```

```
 log-input] [time-range time-range-name][fragments]
```
传输控制协议

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} tcp
 source source-wildcard [operator [port]] destination destination-wildcard
 [operator [port]] [established] [precedence precedence] [tos tos] [log |
 log-input] [time-range time-range-name][fragments]
```
用户数据报协议(UDP)

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} udp
 source source-wildcard [operator [port]] destination destination-wildcard
 [operator [port]] [precedence precedence] [tos tos] [log | log-input]
 [time-range time-range-name][fragments]
```

Prerequisites

Requirements

在尝试进行此配置之前，请确保满足以下要求：

- IP编址基本的了解

请参见新用户IP寻址和划分子网其他信息。

Components Used

This document is not restricted to specific software and hardware versions.

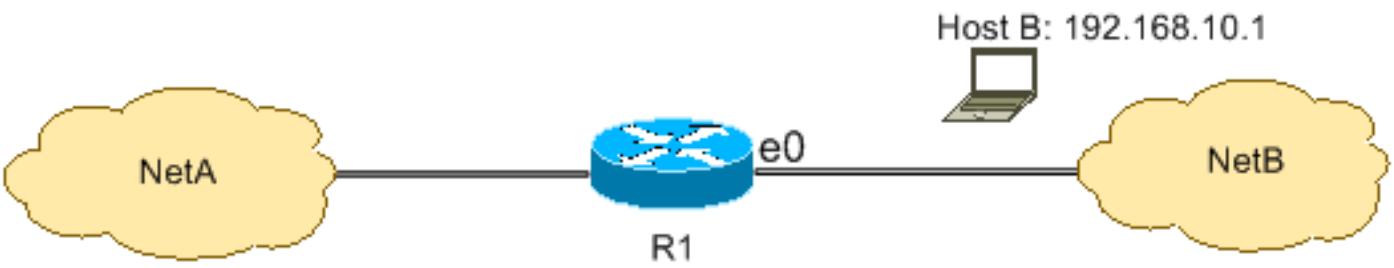
The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

Configure

这些配置示例使用最普通的IP ACL。

允许选定主机访问网络

此图显示被同意的一个选定主机权限访问网络。从主机B发出的所有数据流被注定对NetA允许，并且从NetB发出的其他数据流被注定了对NetA被否决。



在R1表的输出显示网络如何准许对主机的访问。此输出显示那：

- 配置通过以太网提供有IP地址192.168.10.1的仅主机在R1的0个接口。
- 此主机访问NetA IP服务。
- 其他主机在NetB不访问NetA。
- Deny语句在ACL没有被配置。

默认情况下，有含蓄的拒绝所有条款在每个ACL结束时。没有明确地允许的任何被拒绝。

R1

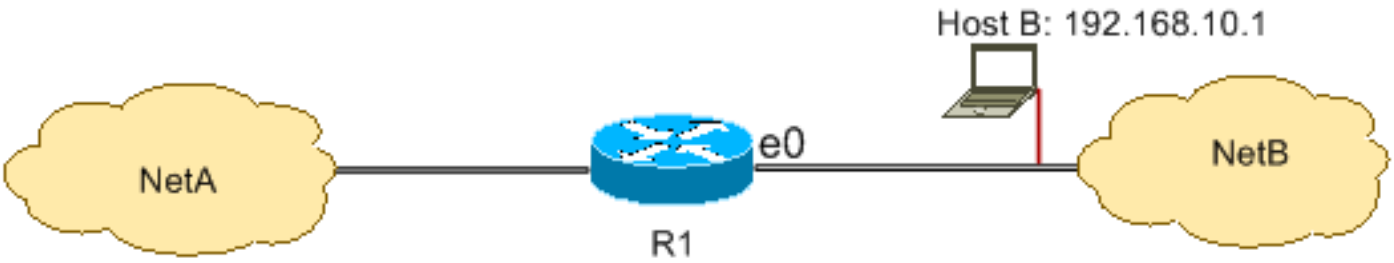
```
hostname R1
!
interface ethernet0
ip access-group 1 in
!
access-list 1 permit host 192.168.10.1
```

> **Note**: ACL过滤自NetB的IP信息包到NetA，除了信息包从NetB来源。从主机B发出的信息包对NetA仍然允许。

> **Note**:ACL**访问列表1许可证192.168.10.1 0.0.0.0**是另一个方式配置同一个规则。

拒绝选定主机访问网络

此图表示，从主机B发出的数据流被注定对NetA被否决，而从访问NetA的NetB的其他数据流允许。



此配置丢弃自主机192.168.10.1/32通过以太网0的所有信息包在R1并且允许一切别的东西。因为有含蓄的拒绝与每个ACL的所有条款您必须使用access list 1 permit any命令明确地允许一切别的东西。

R1

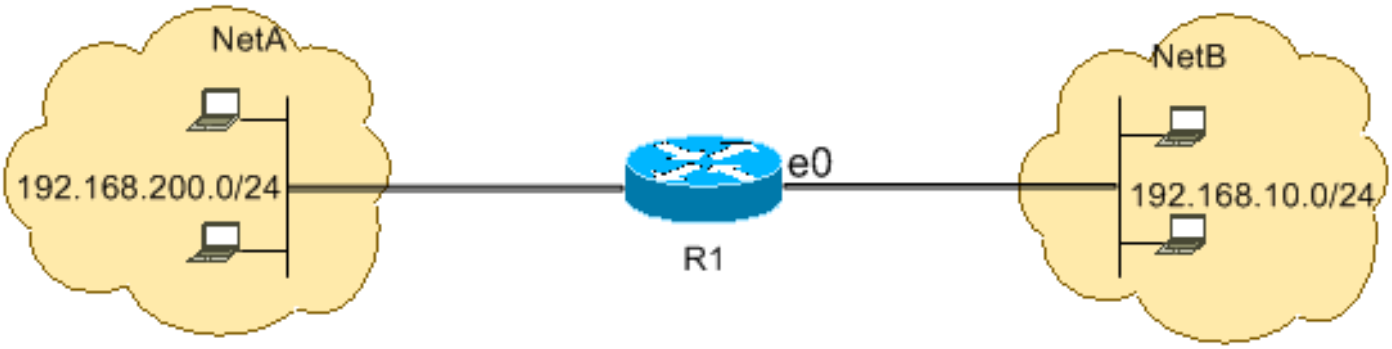
```
hostname R1
!
interface ethernet0
ip access-group 1 in
!
access-list 1 deny host 192.168.10.1
access-list 1 permit any
```

> **Note**:语句顺序对ACL的操作至关重要。如果条目的定货被倒转，当此命令显示，第一行匹配每信息包源地址。所以， ACL不能阻拦从访问NetA的主机192.168.10.1/32。

```
access-list 1 permit any
   access-list 1 deny host 192.168.10.1
```

对范围内的连续IP地址的允许

此图表示，所有主机在有网络地址的192.168.10.0/24 NetB能访问在NetA的网络192.168.200.0/24。



此配置允许与有源地址在网络192.168.10.0/24和在网络192.168.200.0/24访问的一个目的地地址对NetA的IP头的IP信息包。有通过以太网0拒绝其他数据流段落入站在R1的含蓄的拒绝所有条款在ACL结束时。

R1

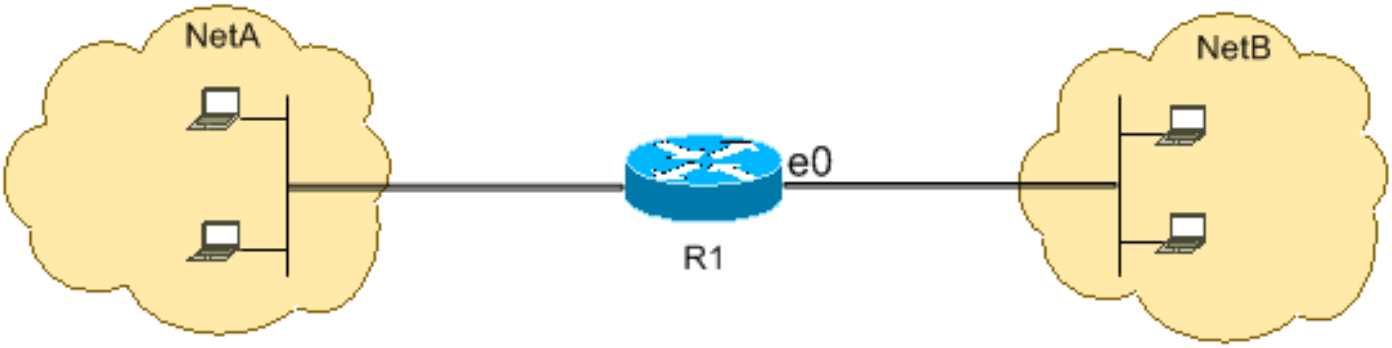
```
hostname R1
!
interface ethernet0
ip access-group 101 in
!
access-list 101 permit ip 192.168.10.0  0.0.0.255
  192.168.200.0  0.0.0.255
```

> **Note**:在access-list 101命令**许可证ip 192.168.10.0 0.0.0.255 192.168.200.0 0.0.0.255中**，"0.0.0.255"是网络192.168.10.0反码与掩码255.255.255.0的。ACL使用反码知道在网络地址的多少位需要配比。在表里， ACL允许有源地址在192.168.10.0/24网络和目的地地址的所有主机在192.168.200.0/24网络。

请参见配置IP访问列表的掩码部分关于网络地址的掩码的更多信息和如何计算为ACL需要的反码。

否决Telnet数据流(TCP，端口23)

为了满足更高的安全性关心，您也许必须禁用对您的专用网络的Telnet访问从公共网络。此图显示从NetB (公共)的Telnet数据流被注定对NetA (专用)如何被否决，允许NetA起动和建立有NetB的一远程登录会话，当其他IP数据流允许时。



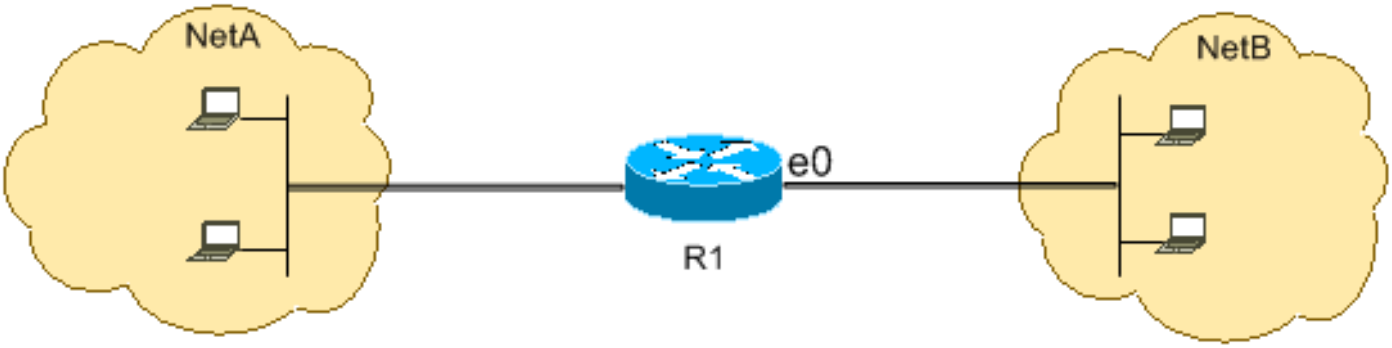
Telnet使用TCP，端口23。此配置表示，所有TCP通信流被注定对端口的23 NetA被阻塞，并且其他IP数据流允许。

R1

```
hostname R1
!
interface ethernet0
ip access-group 102 in
!
access-list 102 deny tcp any any eq 23
access-list 102 permit ip any any
```

允许仅内部网络起动TCP会话

此图表示，从NetA发出的TCP通信流被注定对NetB允许，当从NetB的TCP通信流被注定了对NetA时被拒绝。



ACL的目的在本例中的对：

- 允许在NetA的主机起动和建立TCP会话到主机在NetB。
- 在从起动和建立TCP会话的NetB拒绝主机被注定对主机在NetA。

当数据包有时，此配置允许数据包穿过以太网接口0入站在R1 ：

- 设置的被承认的(ACK)或重置(RST)位(指示一个建立的TCP会话)
- Port值的目的地非常地比1023

R1

```
hostname R1
!
interface ethernet0
ip access-group 102 in
!
```

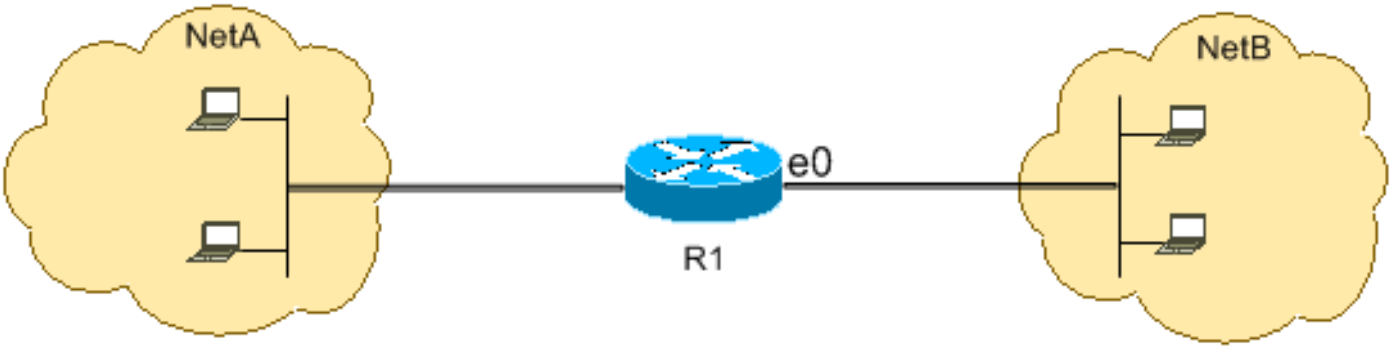
```
access-list 102 permit tcp any any gt 1023 established
```

从大多IP服务使用值的众所周知的端口少于1023，与目的地端口的所有数据包少于1023或没设置的ACK/RST位由ACL 102拒绝。所以，当从NetB的一台主机通过发送第一个TCP信息包(没有请同步/启动设置的信息包(SYN/RST)位)端口编号的首次TCP连接时少于1023，它否认，并且TCP会话发生故障。因为他们有为返回信息包设置的ACK/RST位并且使用极大端口值比1023，从NetA起动的TCP会话被注定对NetB允许。

参考端口一张完全列表的RFC 1700。

否决FTP数据流(TCP，端口21)

此图表示， FTP (TCP，端口21)，并且FTP从NetB发出的数据(端口20)数据流被注定了对NetA被否决，而其他IP数据流允许。



FTP使用端口21和端口20。TCP通信流被注定了对端口21，并且端口20被拒绝，并且一切别的东西明确地允许。

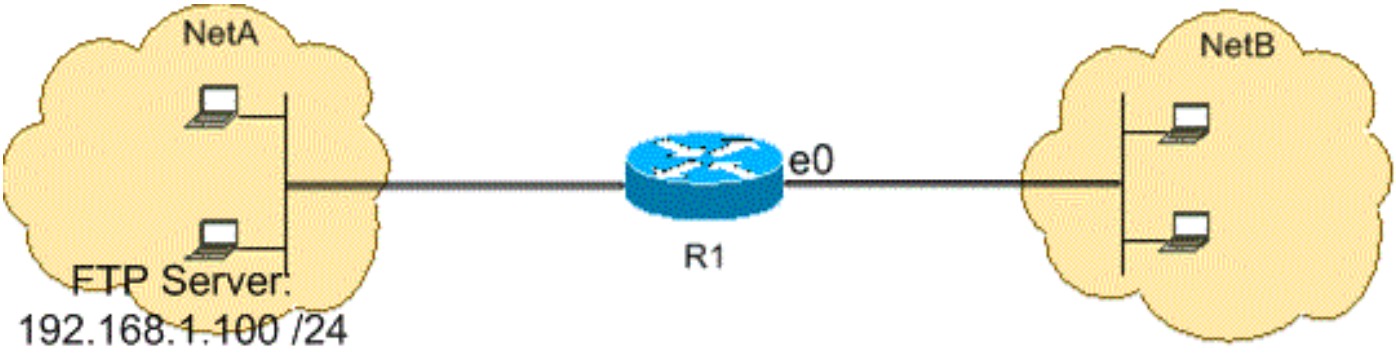
R1

```
hostname R1
!
interface ethernet0
ip access-group 102 in
!
access-list 102 deny tcp any any eq ftp
access-list 102 deny tcp any any eq ftp-data
access-list 102 permit ip any any
```

允许FTP数据流(活动FTP)

FTP在名为激活和被动的两个不同的模式下能运行。参考FTP操作知道活动和无源FTP如何工作。

当FTP在激活模式时运行， FTP服务器使用端口21控制和端口20数据。FTP服务器(192.168.1.100)位于NetA。此图表示， FTP (TCP，端口21)，并且FTP从NetB发出的数据(端口20)数据流被注定了对FTP服务器(192.168.1.100)允许，而其他IP数据流被否决。



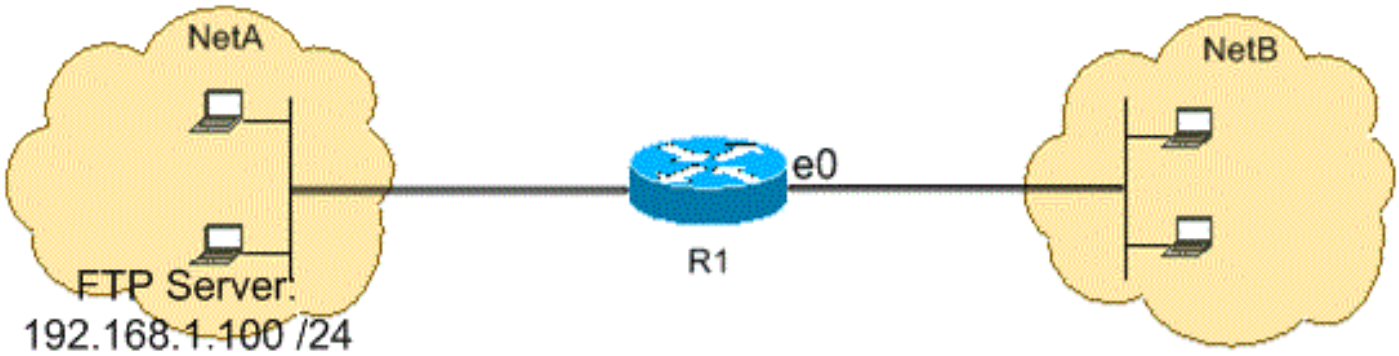
R1

```
hostname R1
!
interface ethernet0
ip access-group 102 in
!
access-list 102 permit tcp any host 192.168.1.100 eq ftp
access-list 102 permit tcp any host 192.168.1.100 eq ftp-data established
!
interface ethernet1
 ip access-group 110 in
!
access-list 110 permit host 192.168.1.100 eq ftp any established
access-list 110 permit host 192.168.1.100 eq ftp-data any
```

允许FTP数据流(无源FTP)

FTP在名为激活和被动的两个不同的模式下能运行。参考FTP操作为了知道活动和无源FTP如何工作。

当FTP在被动模式下时运行，FTP服务器使用端口21控制和动态端口大于或等于1024数据的。FTP服务器(192.168.1.100)位于NetA。此图表示，FTP (TCP，端口21)，并且FTP从NetB发出的数据(端口大于或等于1024)数据流被注定了对FTP服务器(192.168.1.100)允许，而其他IP数据流被否决。



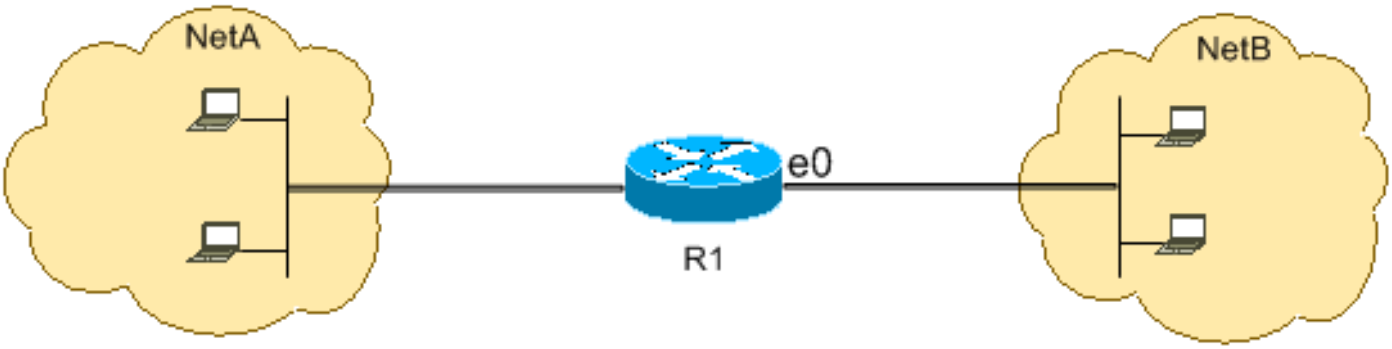
R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit tcp any host 192.168.1.100 eq ftp
access-list 102 permit tcp any host 192.168.1.100 gt 1023
```

```
!
interface ethernet1
 ip access-group 110 in
!
access-list 110 permit host 192.168.1.100 eq ftp any established
access-list 110 permit host 192.168.1.100 gt 1023 any established
```

允许Ping (ICMP)

此图表示，从NetA来源的ICMP被注定对NetB允许，并且从NetB来源的ping被注定了对NetA被拒绝。



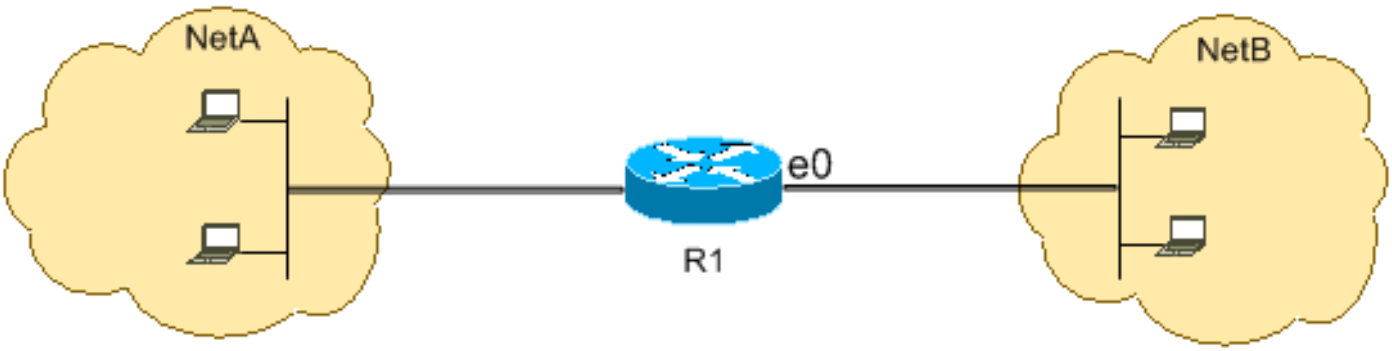
此配置在从NetB的以太网接口0允许仅ECHO回复(ping响应)信息包进来往NetA。然而，当ping在NetB来源并且被注定对NetA时，配置阻拦所有echo-request ICMP信息包。所以，在NetA的主机能ping主机在NetB，但是主机在NetB不能ping在NetA的主机。

R1

```
hostname R1
!
interface ethernet0
ip access-group 102 in
!
access-list 102 permit icmp any any echo-reply
```

允许HTTP， Telnet，邮件， POP3， FTP

此图表示，仅HTTP、Telnet、简单邮件传输协议(SMTP)、POP3和FTP数据流允许，并且从NetB发出的数据流的其余被注定了对NetA被否决。



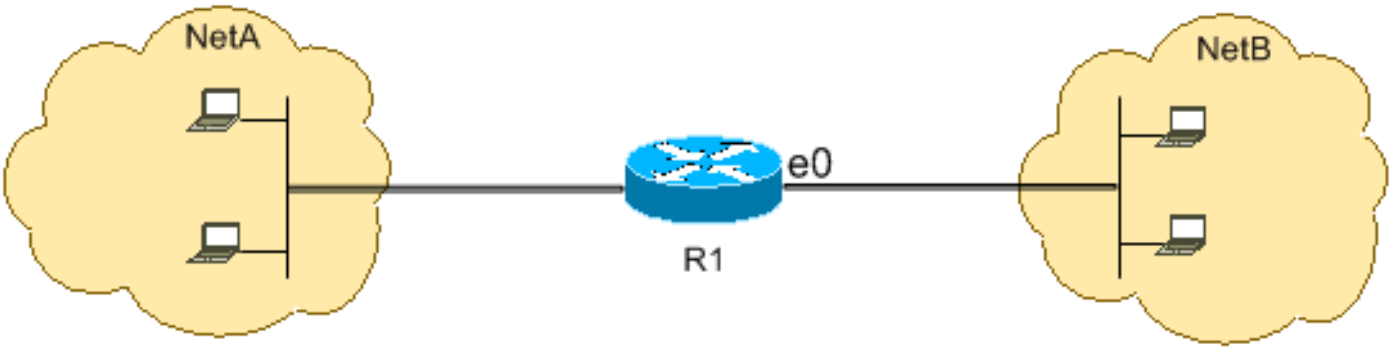
此配置允许与匹配WWW的目的地端口值的TCP通信流(端口80)， Telnet (端口23)， SMTP (端口25)， POP3 (端口110)， FTP (端口21)，或者FTP数据(端口20)。注意含蓄拒绝所有条款在ACL结束时否决其他数据流，不匹配许可证子句。

R1

```
hostname R1
!
interface ethernet0
ip access-group 102 in
!
access-list 102 permit tcp any any eq www
access-list 102 permit tcp any any eq telnet
access-list 102 permit tcp any any eq smtp
access-list 102 permit tcp any any eq pop3
access-list 102 permit tcp any any eq 21
access-list 102 permit tcp any any eq 20
```

允许DNS

此图表示，仅域名系统(DNS)数据流允许，并且从NetB发出的数据流的其余被注定了对NetA被否决。



此配置允许与目的地Port值53的TCP通信流。含蓄拒绝所有条款在ACL结束时否决其他数据流，不匹配许可证子句。

R1

```
hostname R1
!
interface ethernet0
ip access-group 102 in
!
access-list 112 permit udp any any eq domain
access-list 112 permit udp any eq domain any
access-list 112 permit tcp any any eq domain
access-list 112 permit tcp any eq domain any
```

许可证路由更新

当您适用INBOUND ACL于接口时，请保证路由更新没有过滤。请使用从此列表的相关ACL允许路由协议信息包：

输入此命令为了允许路由信息协议(RIP) ：

```
access-list 102 permit udp any any eq rip
```

输入此命令为了允许增强型内部网关路由协议(EIGRP) ：

```
access-list 102 permit igrp any any
```

输入此命令为了允许改进的IGRP (EIGRP) ：

```
access-list 102 permit eigrp any any
```

输入此命令为了允许开放最短路径优先(OSPF) ：

```
access-list 102 permit ospf any any
```

输入此命令为了允许边界网关协议(BGP) ：

```
access-list 102 permit tcp any any eq 179
access-list 102 permit tcp any eq 179 any
```

调试根据ACL的数据流

使用调试指令要求系统资源的分配类似内存，并且处理功率和在极其情况能造成一个大量装载的系统停止。小心请使用调试指令。请使用ACL为了选择性地定义需要被检查减少thedebug命令的影响的数据流。这样配置不过滤任何信息包。

此配置打开仅**debug ip packet命令**信息包的在主机10.1.1.1和172.16.1.1之间。

```
R1(config)#access-list 199 permit tcp host 10.1.1.1 host 172.16.1.1
   R1(config)#access-list 199 permit tcp host 172.16.1.1 host 10.1.1.1
   R1(config)#end
   R1#debug ip packet 199 detail
   IP packet debugging is on (detailed) for access list 199
```

请参见关于调试指令的重要信息关于调试指令的更多信息影响。

请参见使用了解Ping和Traceroute命令的Debug Command部分关于使用ACL的更多信息用调试指令。

MAC地址过滤

您能过滤与一个特定的MAC层位置源或目的地地址的帧。任何数量的地址可以被配置到系统，不用影响性能。为了由MAC层地址过滤，请使用此in命令全局配置模式：

```
Router#config terminal
       bridge irb
       bridge 1 protocol ieee
       bridge 1 route ip
```

运用网桥协议于您与被建立的访问列表一起需要过滤流量的接口：

```
Router#int fa0/0
       no ip address
       bridge-group 1 {input-address-list 700 | output-address-list 700}
       exit
```

创建桥接虚拟接口并且适用分配到以太网接口的IP地址：

```
Router#int bvi1
       ip address
       exit
```

```
!
!
       access-list 700 deny <mac address> 0000.0000.0000
       access-list 700 permit 0000.0000.0000 ffff.ffff.ffff
```

使用此配置，路由器只允许在访问列表配置的MAC地址700。使用访问列表，请拒绝不能访问的MAC adddress然后允许其余。

Note:创建访问列表每条线路每MAC地址的。

Verify

当前没有可用于此配置的验证过程。

Troubleshoot

目前没有针对此配置的故障排除信息。

Related Information

- **配置IP访问列表**
- **访问列表支持页面**
- **IP 路由支持页**
- **IP 路由协议支持页**
- Technical Support & Documentation - Cisco Systems