配置常用 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
- 目的地址
- 数据包类型
- 以上项目的任意组合

为了过滤网络流量，ACL 在路由器接口处控制是转发还是阻止路由数据包。路由器检查每个数据包，从而基于在 ACL 中指定的标准来决定是转发还是丢弃数据包。ACL 条件包括：

- 流量的源地址
- 流量的目的地址
- 上层协议

完成以下步骤，以构建本文档中示例所示的 ACL：

1. 创建 ACL。
2. 将 ACL 应用于接口。

IP ACL 是由应用于 IP 数据包的允许和拒绝条件组成的一个有序集合。路由器按照 ACL 中的条件逐个测试数据包。

第一个匹配的条件决定了思科 IOS® 软件是接受还是拒绝数据包。因为思科 IOS 软件将在匹配第一个条件之后停止测试，所以条件的顺序至关重要。如果任何条件均不匹配，则路由器会由于隐式 deny all 而拒绝该数据包。

以下是可以在思科 IOS 软件中配置的 IP ACL 示例：

- 标准 ACL
- 扩展 ACL
- 动态（锁定和密钥）ACL
- IP 命名 ACL
- 自反 ACL
- 基于时间的 ACL（使用时间范围）
- 附有注释的 IP ACL 条目
- 基于情景的 ACL
- 身份验证代理
- Turbo ACL
- 基于时间的分布式 ACL

本文档描述一些常用的标准 ACL 和扩展 ACL。有关思科 IOS 软件支持的各种类型 ACL 以及如何配置和编辑 ACL 的详细信息，请参阅 配置 IP 访问列表。

标准 ACL 的命令语法格式为 **access-list access-list-number {permit|deny} {host|source source-wildcard|any}**。

标准 ACL 将 IP 数据包的源地址与 ACL 中配置的地址进行比较，以实现流量控制。

扩展 ACL 将 IP 数据包的源地址和目的地址与 ACL 中配置的地址进行比较，以实现流量控制。也可以更精细地配置扩展 ACL，从而按照以下标准过滤流量：

- **协议**
- 端口号
- 差分服务代码点 (DSCP) 值
- 优先级值
- 同步序列号 (SYN) 位的状态

扩展 ACL 的命令语法格式如下：

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 (TCP)

```
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：

- 基本了解 IP 寻址

有关详细信息，请参阅 IP 寻址和子网划分入门。

Components Used

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

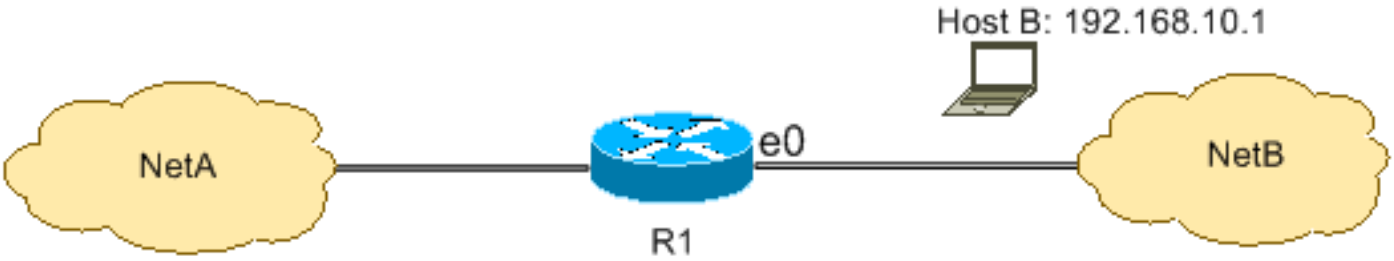
The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

Configure

以下配置示例使用最常见的 IP ACL。

允许指定主机访问网络

下图显示，指定主机被授予网络访问权限。主机 B 发往 NetA 的所有流量均被允许通过，而 NetB 发往 NetA 的所有其他流量均被拒绝通过。



R1 表上的输出显示网络向主机授予访问权限。此输出表明以下几点：

- 此配置仅允许 IP 地址为 192.168.10.1 的主机访问 R1 的 Ethernet 0 接口。
- 此主机具有对 NetA 的 IP 服务访问权限。
- NetB 中的任何其他主机均无法访问 NetA。
- ACL 中未配置 deny 语句。

默认情况下，每个 ACL 的末尾处都会有一个隐式 deny all 子句。系统会拒绝未显式允许的任何内容。

R1

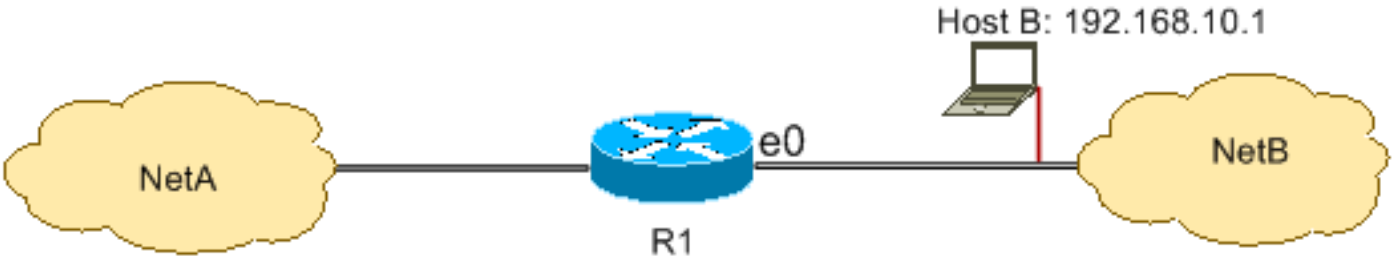
```
hostname R1
!
interface ethernet0
ip access-group 1 in
!
access-list 1 permit host 192.168.10.1
```

> **Note**: ACL 过滤从 NetB 到 NetA 的 IP 数据包，源自主机 B 的数据包除外。主机 B 发往 NetA 的数据包仍然允许通过。

> **Note**:通过 ACL **access-list 1 permit 192.168.10.1 0.0.0.0** 也可以配置相同的规则。

拒绝指定主机访问网络

下图显示，主机 B 发往 NetA 的流量均被拒绝通过，而从 NetB 到 NetA 的所有其他流量均被允许通过。



此配置拒绝主机 192.168.10.1/32 发送的所有数据包通过 R1 的 Ethernet 0 接口，而允许所有的其他数据包通过该接口。由于每个 ACL 都包含隐式 deny all 子句，因此必须使用命令 access list 1 permit any 以明确允许所有的其他数据包通过。

R1

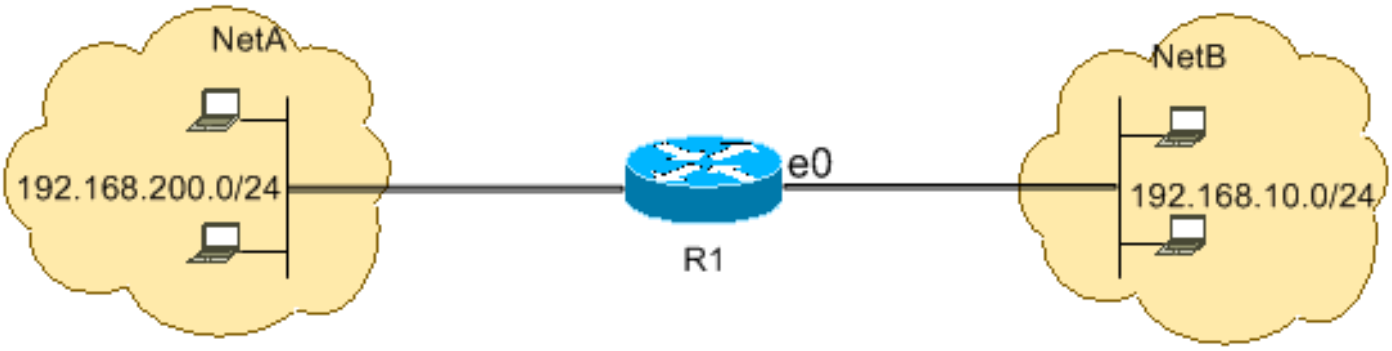
```
hostname R1
!
interface ethernet0
ip access-group 1 in
!
access-list 1 deny host 192.168.10.1
access-list 1 permit any
```

> **Note**:语句的顺序对于 ACL 操作至关重要。如果条目顺序颠倒（如以下命令所示），则第一行会匹配每个数据包的源地址。于是，ACL 就无法阻止主机 192.168.10.1/32 访问 NetA。

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

允许访问一组连续的 IP 地址

下图显示，NetB 中网络地址为 192.168.10.0/24 的 所有主机均可访问 NetA 中的 192.168.200.0/24 网络。



此配置允许 IP 报头中源地址位于 192.168.10.0/24 网络内、目的地址位于 192.168.200.0/24 网络内的 IP 数据包访问 NetA。此 ACL 末尾的隐式 deny all 子句拒绝所有其他流量通过 R1 的 Ethernet 0 接口入站。

R1

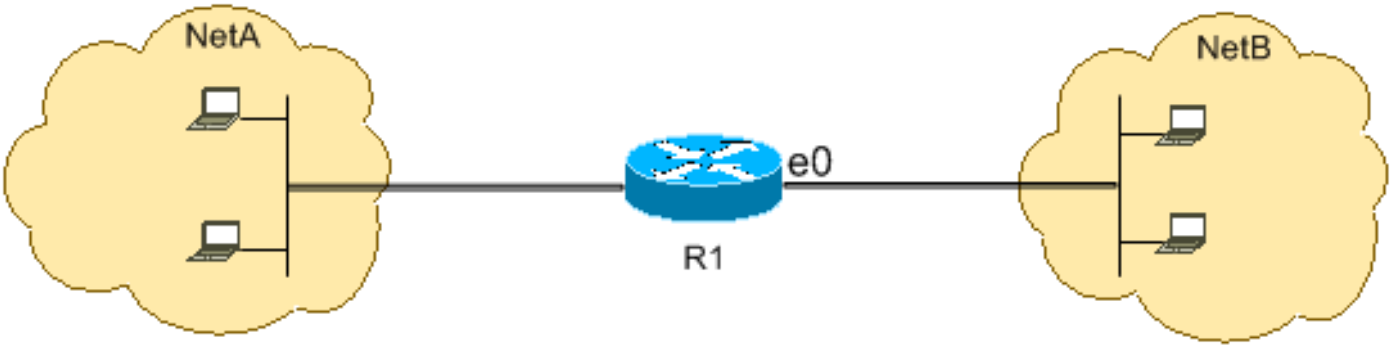
```
hostname R1
!
interface ethernet0
ip access-group 101 in
!
access-list 101 permit ip 192.168.10.0  0.0.0.255
  192.168.200.0  0.0.0.255
```

> **Note**:在命令 access-list 101 **permit ip 192.168.10.0 0.0.0.255 192.168.200.0 0.0.0.255** 中，“0.0.0.255”为网络 192.168.10.0（掩码：255.255.255.0）的反掩码。ACL 使用反掩码来确定网络地址中有多少位需要匹配。在上表中，ACL 允许源地址位于 192.168.10.0/24 网络内、目的地址位于 192.168.200.0/24 网络内的所有主机流量。

有关网络地址掩码以及如何计算 ACL 所需的反掩码的详细信息，请参阅配置 IP 访问列表的掩码部分。

拒绝 Telnet 流量（TCP 端口 23）

为了满足更高的安全要求，可能需要禁用公共网络对专用网络的 Telnet 访问。下图显示 ACL 如何拒绝 NetB（公用网络）发往 NetA（专用网络）的 Telnet 流量（但允许 NetA 向 NetB 发起并建立 Telnet 会话），而允许所有其他 IP 流量。



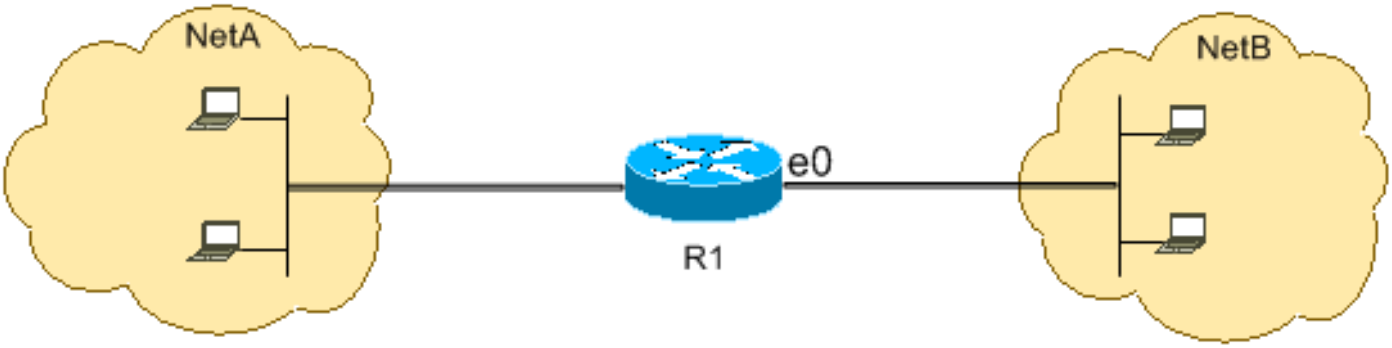
Telnet 使用 TCP 端口 23。此配置显示，所有发往 NetA 端口 23 的 TCP 流量均被阻止通过，而所有其他 IP 流量均被允许通过。

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
```

仅允许内部网络发起 TCP 会话

下图显示，NetA 发往 NetB 的 TCP 流量均被允许通过，而从 NetB 到 NetA 的 TCP 流量均被拒绝通过。



在本例中，ACL 的作用如下：

- 允许 NetA 中的主机向 NetB 中的主机发起并建立 TCP 会话。
- 拒绝 NetB 中的主机向 NetA 中的主机发起并建立 TCP 会话。

此配置允许符合以下条件的数据报通过 R1 的 Ethernet 0 接口入站：

- 已设置 ACK 或 RST 位（表示已建立 TCP 会话）
- 目的端口值大于 1023

R1

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

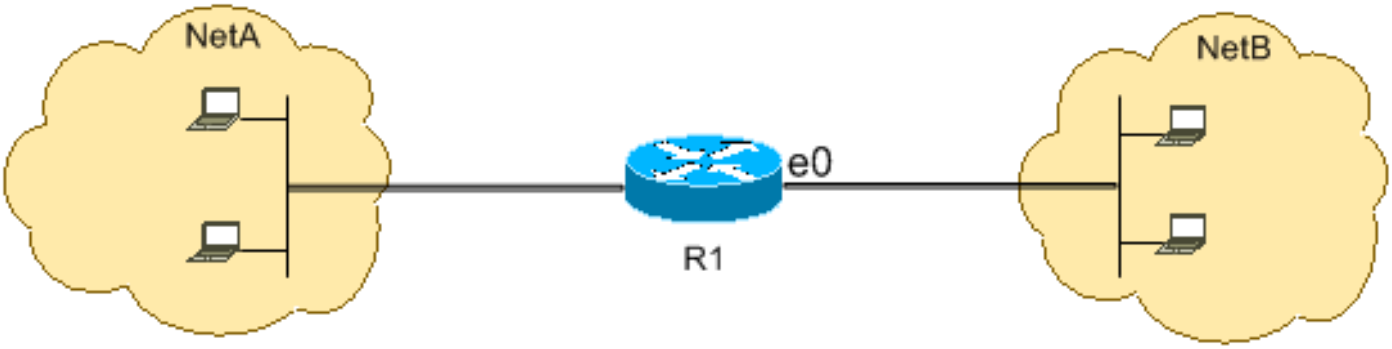
```
access-list 102 permit tcp any any gt 1023 established
```

由于 IP 服务的大多数公认端口值都小于 1023，因此目的端口小于 1023 或未设置 ACK/RST 位的数据报会被 ACL 102 拒绝。因此，当 NetB 中的主机通过向小于 1023 的端口发送第一个 TCP 数据包（未设置 SYN/RST 位）来发起 TCP 连接时，就会被拒绝，TCP 会话失败。NetA 向 NetB 发起的 TCP 会话由于为返回数据包设置了 ACK/RST 位，并且使用大于 1023 的端口号，因此被允许通过。

完整的端口列表请参阅 RFC 1700。

拒绝 FTP 流量（TCP 端口 21）

下图显示，NetB 发往 NetA 的 FTP 流量（TCP 端口 21）和 FTP 数据流量（端口 20）均被拒绝通过，而所有其他 IP 流量均被允许通过。



FTP 使用 21 和 20 端口。发往 21 和 20 端口的 TCP 流量均被拒绝，其他流量均被明确允许通过。

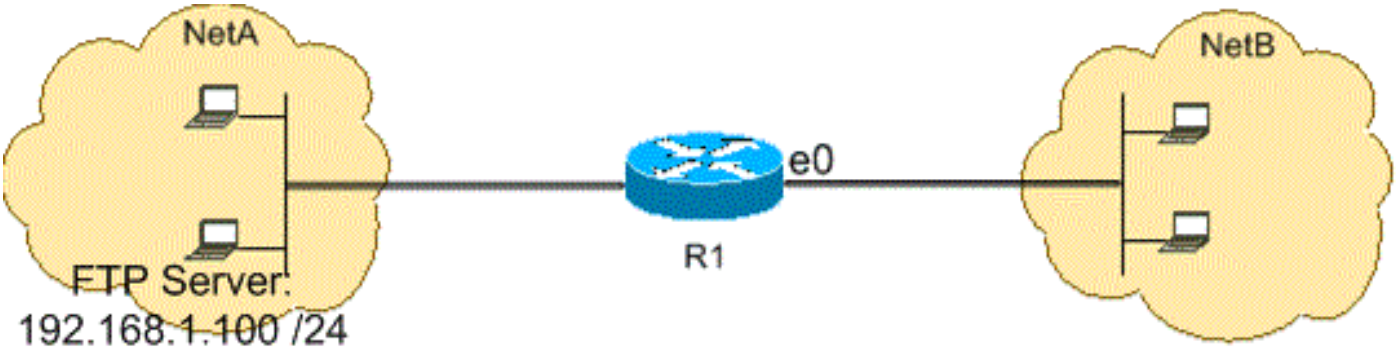
R1

```
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 流量（主动 FTP）

FTP 可在主动和被动两种不同的模式下运行。请参阅 FTP 操作以了解主动和被动 FTP 的工作原理。

当 FTP 在主动模式下工作时，FTP 服务器将 21 端口用于控制流量，将 20 端口用于数据流量。FTP 服务器 (192.168.1.100) 位于 NetA 中。下图显示，NetB 发往 FTP 服务器 (192.168.1.100) 的 FTP 流量（TCP 端口 21）和 FTP 数据流量（端口 20）均被允许通过，而所有其他 IP 流量均被拒绝通过。



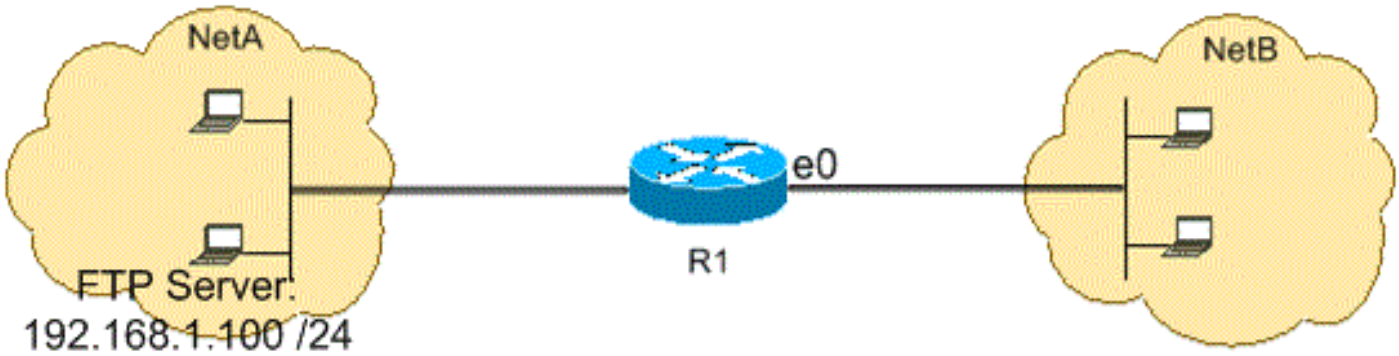
R1

```
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 流量（被动 FTP）

FTP 可在主动和被动两种不同的模式下运行。请参阅 FTP 操作以了解主动和被动 FTP 的工作原理。

当 FTP 在被动模式下工作时，FTP 服务器将 21 端口用于控制流量，将大于或等于 1024 的动态端口用于数据流量。FTP 服务器 (192.168.1.100) 位于 NetA 中。下图显示，NetB 发往 FTP 服务器 (192.168.1.100) 的 FTP 流量（TCP 端口 21）和 FTP 数据流量（大于或等于 1024 的端口）均被允许通过，而所有其他 IP 流量均被拒绝通过。



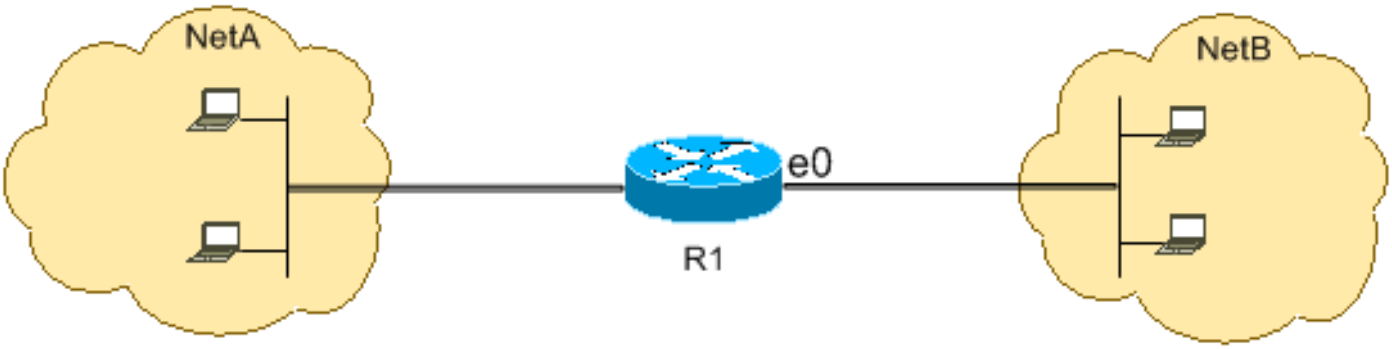
R1

```
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)

下图显示，NetA 发往 NetB 的 ICMP 流量均被允许通过，而从 NetB 到 NetA 的 ping 流量均被拒绝通过。



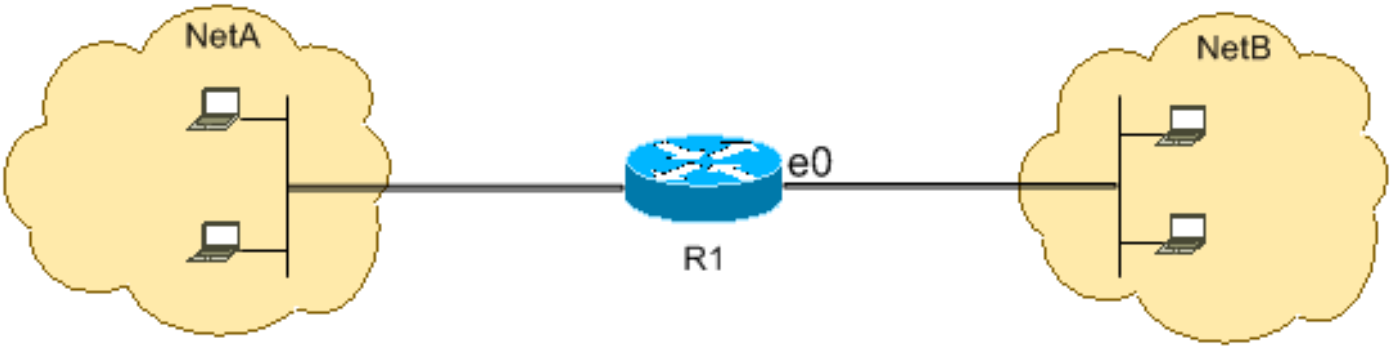
此配置仅允许来自 NetB 的回应应答（ping 响应）数据包通过 Ethernet 0 接口传入 NetA。但是，此配置阻止因 ping 操作而从 NetB 发往 NetA 的所有回应请求 ICMP 数据包。因此，NetA 中的主机可以 ping NetB 中的主机，而 NetB 中的主机不能 ping NetA 中的主机。

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

下图显示从 NetB 到 NetA 仅允许 HTTP、Telnet、简单邮件传输协议 (SMTP)、POP3、和 FTP 流量，而从 NetB 发往 NetA 的其他流量则一概拒绝。



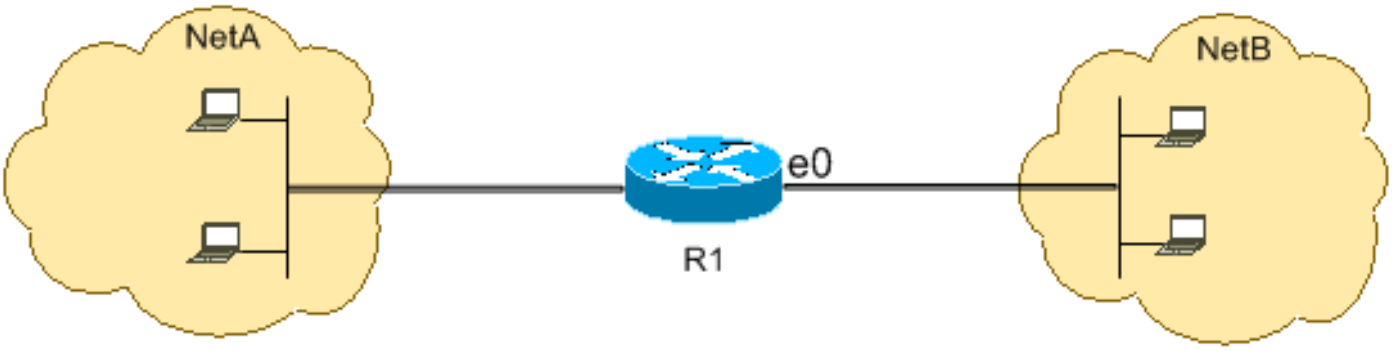
此配置允许目的端口值匹配 WWW（80 端口）、Telnet（23 端口）、SMTP（25 端口）、POP3（110 端口），FTP（21 端口）或 FTP 数据（20 端口）的 TCP 流量通过。请注意，ACL 末尾的隐式 deny all 子句拒绝与 permit 子句不匹配的所有其他流量通过。

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

下图显示从 NetB 到 NetA 仅允许域名系统 (DNS) 流量，而 NetB 发往 NetA 的其余流量均被拒绝。



此配置允许目的端口号为 53 的 TCP 流量通过。ACL 末尾的隐式 deny all 子句拒绝与 permit 子句不匹配的所有其他流量通过。

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
```

允许路由更新

将入站 ACL 应用到接口上时，确保路由更新未被过滤掉。使用以下列表中的相关 ACL 以允许路由协议数据包通过：

输入以下命令以允许路由信息协议 (RIP) 数据包通过：

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

输入以下命令以允许内部网关路由协议 (IGRP) 数据包通过：

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

输入以下命令以允许增强型 IGRP (EIGRP) 数据包通过：

```
access-list 102 permit eigrp any any
```
输入以下命令以允许开放最短路径优先 (OSPF) 数据包通过：

```
access-list 102 permit ospf any any
```
输入以下命令以允许边界网关协议 (BGP) 数据包通过：

```
access-list 102 permit tcp any any eq 179
access-list 102 permit tcp any eq 179 any
```
基于 ACL 调试流量

debug 命令的使用需要分配内存和处理能力等系统资源，在极端情况下可能会导致系统因负载过重而停机。请谨慎使用 **debug** 命令。可以使用 ACL 来选择性地指定需要检查的流量，从而减少 debug 命令带来的影响。此类配置不会过滤任何数据包。

此配置仅面向主机 10.1.1.1 和 172.16.1.1 之间的数据包开启 **debug ip packet** 命令。

```
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
```
有关 debug 命令影响的详细信息，请参阅关于 debug 命令的重要信息。

有关通过 **debug**命令使用 ACL 的详细信息，请参阅了解 Ping 和 Traceroute 命令的使用 Debug 命令部分。

MAC 地址过滤

可以过滤具有特定 MAC 层站点源地址或目的地址的帧。系统中可以配置任意数量的地址，而且不会影响性能。要通过 MAC 层地址进行过滤，请在全局配置模式下使用以下命令：

```
Router#config terminal
       bridge irb
       bridge 1 protocol ieee
       bridge 1 route ip
```
将网桥协议应用到需要通过创建的访问列表过滤流量的接口上：

```
Router#int fa0/0
       no ip address
       bridge-group 1 {input-address-list 700 | output-address-list 700}
       exit
```
创建网桥虚拟接口，并应用分配给以太网接口的 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
```

通过此配置，路由器仅允许访问列表 700 上配置的 MAC 地址。通过访问列表，拒绝不得具有访问权限的 MAC 地址，然后允许剩余的地址。

Note:在访问列表中，为每个 MAC 地址添加相应的配置行。

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