单元 10 访问控制列表

主编：钟祥睿等

上海交通大学出版社

目录

单元学习目标

知识目标

1. 了解 ACL 的应用场景
2. 理解 ACL 的基本原理和基本作用
3. 能够区分 ACL 的不同种类及特点
4. 理解 ACL 规则的基本组成结构和匹配顺序
5. 了解 ACL 常见的应用场景

技能目标

1. 掌握基本 ACL 和高级 ACL 的配置方法
2. 掌握 ACL 在接口下的应用方法
3. 掌握 ACL 中通配符的使用方法
4. 掌握 ACL 流量过滤的典型应用

一 项目描述

随着网络的快速普及和应用的日益深入，各种增值业务得到了广泛部署，网络中断可能会导致大量业务出现异常，造成重大经济损失。因此，作为承载业务主体的基础网络，其可靠性已成为备受关注的焦点，其中网络安全、网络服务质量 QoS （ Quality of Service ）的问题尤为突出：

1. 园区内网重要的服务器资源被随意访问，园区机密信息容易泄露，造成安全隐患。
2. 网络攻击、 Internet 病毒肆意侵略园区内网，网络环境的安全性堪忧。
3. 网络带宽被各类业务随意挤占，服务质量要求最高的语音、视频业务的带宽常常得不到保障，造成用户体验差。

以上种种问题，都对正常的网络通信造成了极大的影响。而访问控制列表技术的出现，则有效地解决了上述问题，切实保障了网络的安全性、传输的稳定性和可靠性。

一 项目描述

例如，某公司的园区网拓扑如下图所示，为保证财务数据的安全，公司禁止研发部门访问财务部服务器，但总裁办公室不受限制。要实现此功能需求，可通过访问控制列表技术在网络上实施不同流量的过滤。

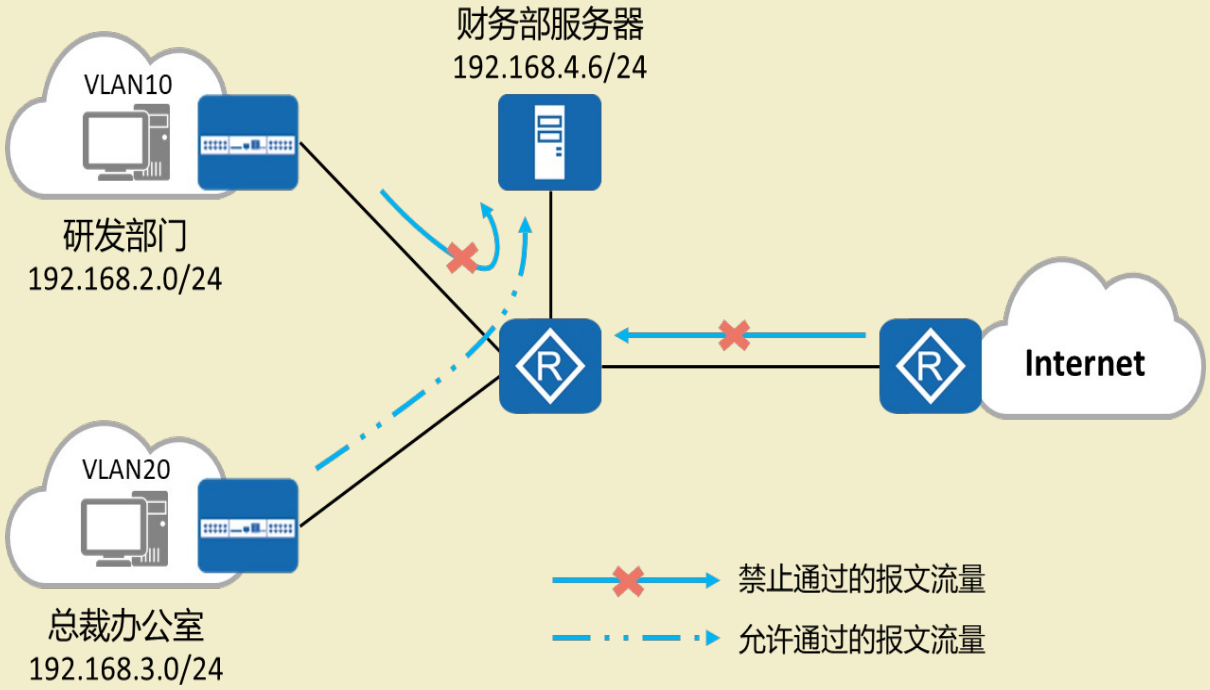


图 10-1 网络流量过滤

二 项目分析

访问控制列表通过规则对报文进行分类，这些规则应用到网络设备上，网络设备根据这些规则判断哪些报文可以接收，哪些报文需要拒绝，从而极大地提升了网络的安全性。

访问控制列表通常应用在企业的出口控制上，通过实施访问控制列表，可以有效地部署企业网络的出网安全策略及控制对局域网内部资源的访问能力，进而来保障内网资源的安全性及内外网通信的可靠性。总体而言，访问控制列表具有以下功能和作用。

1. 限制网络流量、提高网络性能。例如，访问控制列表可以根据数据包的协议，指定这种类型的数据包具有更高的优先级，同等情况下可预先被网络设备处理。

二 项目分析

2. 提供对通信流量的控制手段。
3. 提供网络访问的基本安全手段。
4. 在网络设备接口处，决定哪种类型的通信流量被转发或被阻塞。

接下来，我们将通过学习访问控制列表的基本原理和作用、访问控制列表的不同种类及特点、访问控制列表的基本组成和匹配顺序、通配符的使用方法及访问控制列表的相关配置命令等知识内容，完成访问控制列表在典型应用场景（在本项目中，只介绍访问控制列表的流量过滤功能）下的部署与实现。

三 相关知识

10.1 ACL 的基本原理

一、 ACL 的概念

访问控制列表（ Access Control List ），简称 ACL ，是一种基于包过滤的网络安全访问控制技术，它可以根据设定的条件对接口上的数据包进行过滤，允许其通过或丢弃。

ACL 被广泛地应用于路由器和三层交换机，借助于访问控制列表，可以有效地控制用户对网络的访问，从而最大程度地保障网络安全。

二、 ACL 的组成

ACL 是由一系列规则组成的集合， ACL 通过这些规则对报文进行分类，从而使设备可以对不同类型的报文进行不同的处理。在华为设备上， ACL 的组成结构如下图所示。

三 相关知识

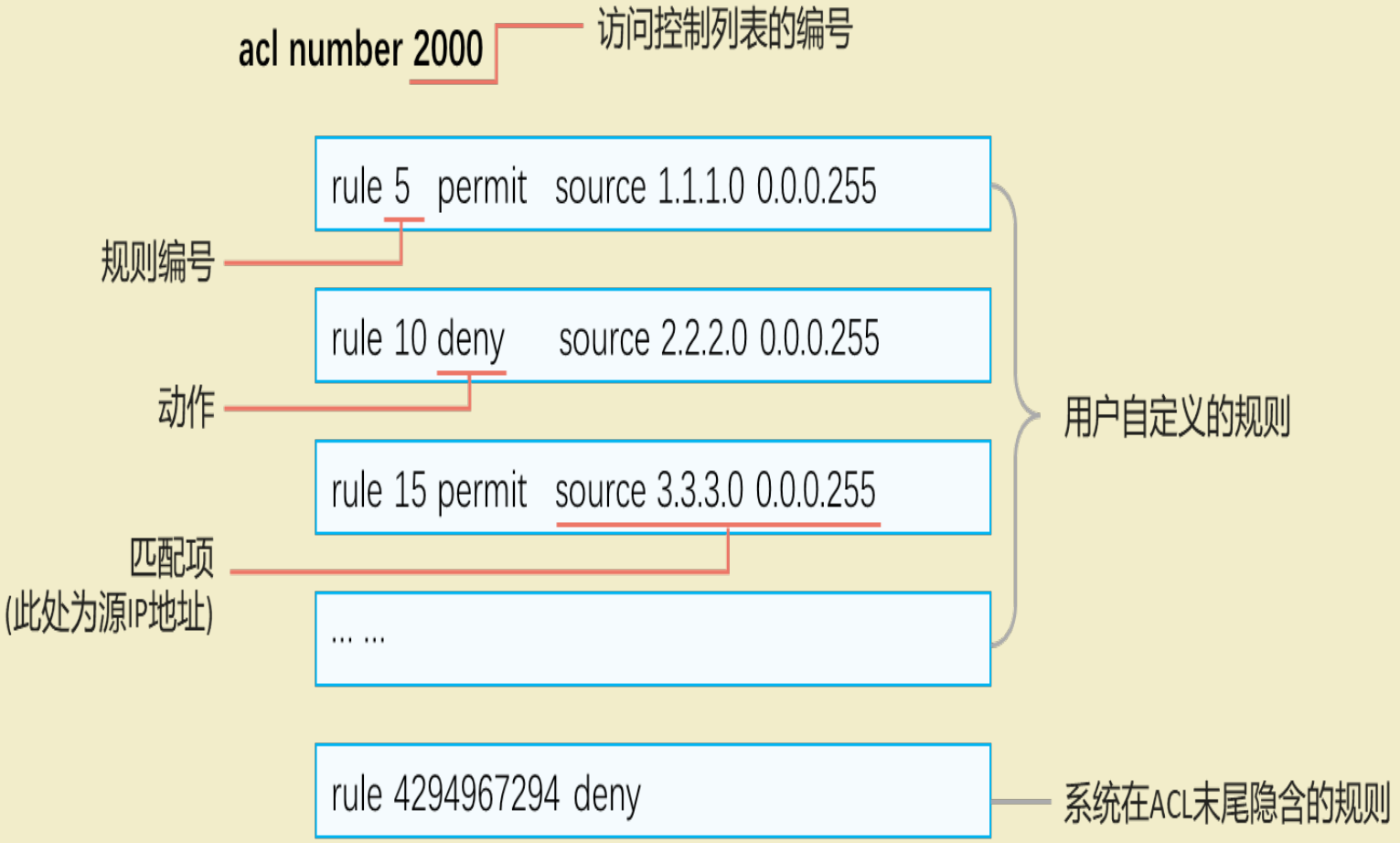


图 10-2 ACL 的组成

三 相关知识

从上图可以看出，一个 ACL 由一个 ACL 编号和多条 rule 语句构成，各组成部分的含义如下：

1. ACL 编号：在网络设备上配置 ACL 时，每个 ACL 都需要分配一个编号，称为 ACL 编号，用来标识 ACL 。

2. 规则：一个 ACL 通常由若干条“ permit/deny”语句组成，每条语句就是该 ACL 的一条规则。

3. 规则编号：每条规则都有一个相应的编号，称为规则编号，用来标识 ACL 规则。可以自定义，也可以系统自动分配。 ACL 规则的编号范围是 0 ～ 4294967294 ，所有规则均按照规则编号从小到大进行排序。

4. 动作：每条规则中的 permit 或 deny ，就是与这条规则相对应的处理动作。 permit 表示“允许”， deny 表示“拒绝”，但是 ACL 一般是结合其他技术使用，不同的场景，处理动作的含义也有所不同。比如， ACL 如果与流量过滤技术结合使用（即流量过滤中调用 ACL ）， permit 就是“允许通行”的意思， deny 就是“拒绝通行”的意思。…？

5. 匹配项： ACL 定义了极其丰富的匹配项。例子中体现的源地址， ACL 还支持很多其他规则匹配项。例如，二层以太网帧头信息（如源 MAC 、目的 MAC 、以太帧协议类型）、三层报文信息（如目的地址、协议类型）以及四层报文信息（如 TCP/UDP 端口号）等。

三、 ACL 的规则编号

从上面 ACL 的组成结构可看出， ACL 的规则编号可以自定义，也可以系统自动分配。系统自动为 ACL 规则分配编号时，每个相邻规则编号之间会有一个差值，这个差值称为“步长”。缺省步长为 5 ，所以规则编号就是 5/10/15 … ，以此类推。

1. 如果手工指定了一条规则，但未指定规则编号，系统就会使用大于当前 ACL 内最大规则编号且是步长整数倍的最小整数作为规则编号。

2. 步长可以调整，如果将步长改为 2 ，系统则会自动从当前步长值开始重新排列规则编号，规则编号就变成 2 、 4 、 6 … 。

那么步长起什么作用呢？能否直接 rule 1/2/3/4 … ？

三 相关知识

例【 10.1 】：有一个 ACL 2000 ，采用系统自动编号，其内容如下所示。

```
acl number 2000
rule     5   deny    source  10.1.1.1  0
rule     10  deny    source  10.1.1.2  0
rule     15  permit source  10.1.1.0  0.0.0.255
```

如果希望在该 ACL 中增加一条规则，要求新规则的位置介于 rule10 与 rule15 之间，那么该如何处理呢？

答案是，可以在 rule 10 和 rule 15 之间，手工加入一条 rule 11 ，如下所示。

```
rule 11 deny source 10.1.1.3 0
```

、

命令执行后， ACL 变成：

```
acl number 2000
rule     5   deny    source  10.1.1.1  0
rule     10  deny    source  10.1.1.2  0
rule     11  deny    source  10.1.1.3  0
rule     15  permit source  10.1.1.0  0.0.0.255
```

因此，设置一定长度的步长的作用，是方便后续在旧规则之间插入新的规则。

思考： rule 15 permit source 10.1.1.0 0.0.0.255 是什么意思？

四、 ACL 的通配符掩码

从 ACL 规则的结构，我们可以看到每一条规则的匹配项都有一个与网络掩码类似的掩码，该掩码是什么东西？又起什么作用呢？

每一条规则，当需要进行 IP 地址匹配的时候，后面都会跟着一个 32 位掩码位，这 32 位称为通配符掩码，用于指示 IP 地址中，哪些比特位需要严格匹配，哪些比特位无需匹配。

通配符掩码通常采用类似网络掩码的点分十进制形式表示，但是含义却与网络掩码完全不同。通配符掩码，换算成二进制后，“ 0” 表示“匹配”，“ 1” 表示“不关心”。

例【 10.2 】：如果要精确匹配 192.168.1.1/24 这个 IP 地址对应的网段地址，通配符掩码是多少？

解答：网络位需要严格匹配，主机位无所谓，因此通配符为“ 0.0.0.11111111”， 192.168.1.xxxxxxxx 的后 8 位可以为任意值，所以匹配的是 192.168.1.0/24 网段。

四、 ACL 的通配符掩码

例【 10.3 】： 如果想匹配 192.168.1.0/24 网段中的奇数 IP 地址，通配符掩码是多少呢？

解答：先看一看奇数 IP 地址都有哪些：

192.168.1.1 、 192.168.1.3 、 192.168.1.5…… 后八位写成二进制：

192.168.1.00000001 、 192.168.1.00000011 、 192.168.1.00000101 …… 可以看出共同点： 最后 8 位的高 7 位是任意值， 最低位固定为 1 ， 因此答案是： 192.168.1.1 0.0.0.254 （ 0.0.0.11111110 ）。

如下图所示：

三 相关知识

由此可得出通配符的一个特点：通配符中的 1 或者 0 是可以不连续的。

此外，在 ACL 的规则中，还有两个特殊的通配符 0 和 any 也很常用。

1. 0 ： 当通配符全为 0 去匹配 IP 地址时，表示精确匹配某个 IP 地址。如精确匹配 192.168.1.1 这个 IP 地址，表示为：192.168.1.1 0.0.0.0 ， 可简化为 192.168.1.1 0 。

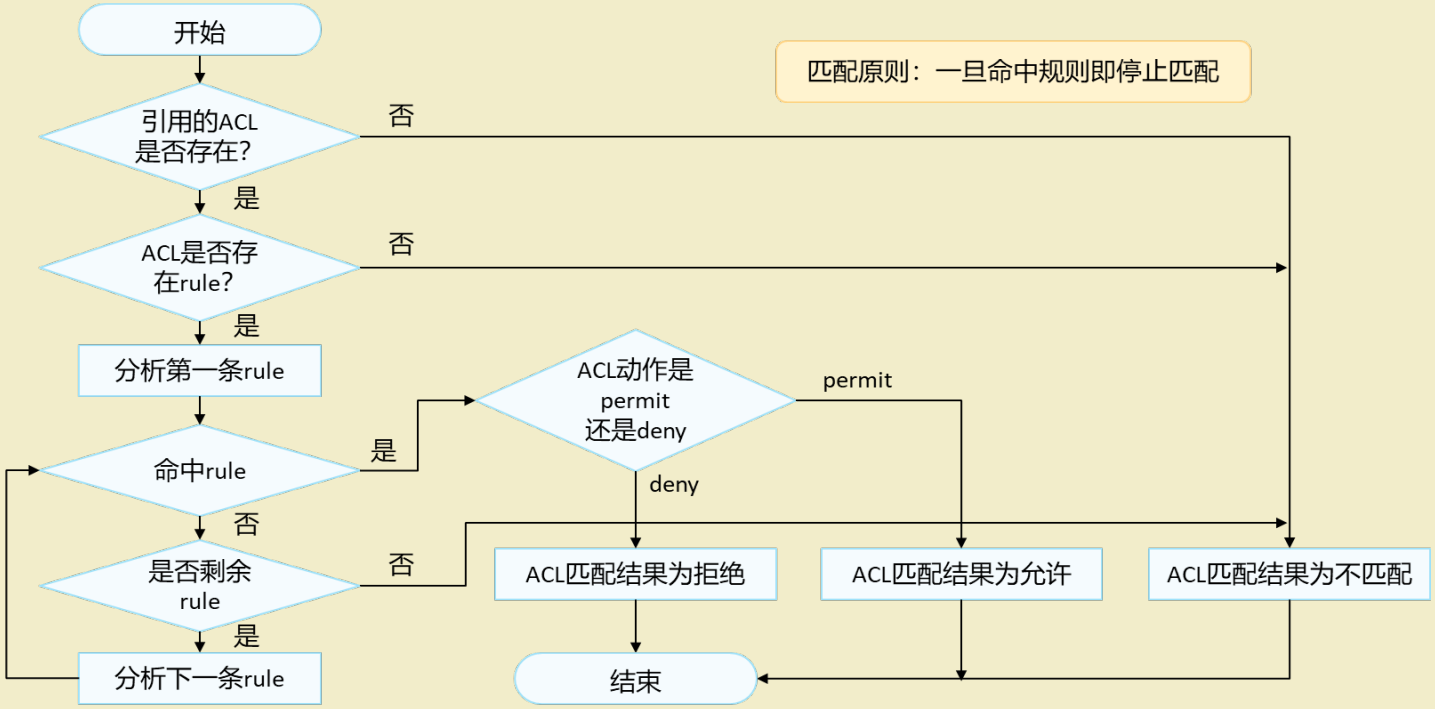
2. any ： 当通配符全为 1 去匹配 0.0.0.0 地址时，表示匹配了所有 IP 地址。如匹配所有 IP 地址，表示为： 0.0.0.0 255.255.255 ， 可简化为 any 。

思考：如果希望只匹配网络 192.168.10.0/24 和 192.168.11.0/24 ， 通配符掩码该是多少呢？

五、 ACL 规则的匹配机制

1. 匹配流程

当报文到达设备（配置了 ACL ）时，设备从报文中提取信息，将该信息与 ACL 中的规则进行匹配，并遵循“一旦命中即停止匹配”的机制，整个匹配流程如图 10-4 所示。



三 相关知识

从 ACL 规则匹配流程图可以看出，首先系统会查找设备上是否配置了 ACL：

（1）如果 ACL 不存在，则返回 ACL 匹配结果”不匹配”。

（2）如果 ACL 存在，则查找设备是否配置了 ACL 规则。

① 如果规则不存在，则返回 ACL 匹配结果”不匹配”。

② 如果规则存在，则系统会从 ACL 中编号最小的规则开始查找。

如果匹配上了 permit 规则，则停止查找规则，并返回结果”匹配（允许）”。

如果匹配上了 deny 规则，则停止查找规则，并返回结果“匹配（拒绝）”。

如果没有匹配上规则，则继续查找下一条规则，以此循环。如果一直查到最后一条规则，报文仍未匹配上，则返回结果“不匹配”。

三 相关知识

从上面整个 ACL 匹配流程可以看出，报文与 ACL 规则匹配后，会产生两种匹配结果：“匹配”和“不匹配”。

（1）匹配（命中规则）：指存在 ACL，且在 ACL 中查找到了符合匹配条件的规则。不论匹配的动作是“ permit”还是“ deny”，都称为“匹配”，而不是只是匹配上 permit 规则才算“匹配”。

（2）不匹配（未命中规则）：指不存在 ACL，或 ACL 中无规则，又或者在 ACL 中遍历了所有规则都没有找到符合匹配条件的规则。以上三种情况，都叫做“不匹配”。

2. 匹配顺序

由于一条 ACL 可以由多条“ permit 或 deny”语句组成，每一条语句描述一条规则，这些规则可能存在包含关系，也可能有重复或矛盾的地方，因此 ACL 的匹配顺序就显得十分重要了。

华为设备支持两种匹配顺序：自动排序（ auto 模式）和配置顺序（ config 模式）。缺省的 ACL 匹配顺序是 config 模式。

三 相关知识

（1）自动排序，是指系统使用“深度优先”的原则，将规则按照精确度从高到低进行排序，并按照精确度从高到低的顺序进行报文匹配。

（2）配置顺序，系统按照 ACL 规则编号从小到大的顺序进行报文匹配，规则编号越小越容易被匹配。

如果后面又添加了一条规则，则这条规则会被加入到相应的位置，报文仍然会按照从小到大的顺序进行匹配。

三 相关知识

例【 10.5 】：配置顺序示例，如下图所示，以 192.168.1.3/24 的报文匹配为例。

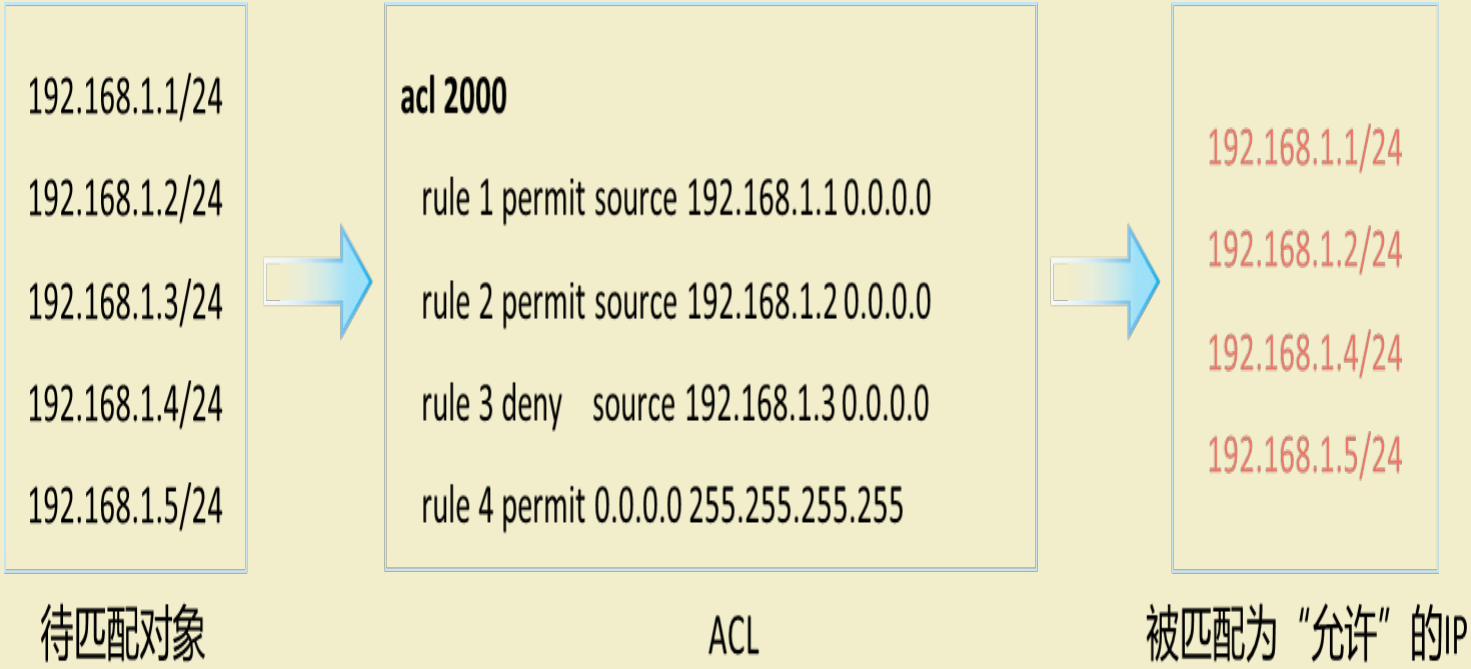


图 10-5 匹配顺序示例

三 相关知识

首先理解 ACL 2000 的含义：
rule 1 ： 允许源 IP 地址为 192.168.1.1 的报文
rule 2 ： 允许源 IP 地址为 192.168.1.2 的报文
rule 3 ： 拒绝源 IP 地址为 192.168.1.2 的报文
rule 4 ： 允许其他所有 IP 地址的报文
当源 IP 地址为 192.168.1.3 的报文经过配置了 ACL 的设备时：
首先查看 rule 1 ， 发现不匹配；
继续查看 rule 2 ， 发现仍不匹配；
继续查看 rule 3 ， 发现匹配，且是“拒绝”动作。
结果是： 192.168.1.3 的报文被 ACL 匹配上，并丢弃。
3. 匹配位置
当我们创建好 ACL ， 并定义了相应的规则后，如何让 ACL 在设备（路由器、三层交换机）上生效呢？对于配置了 ACL 的设备而言，可以在数据报文进入设备或者从设备出去的接口上执行 ACL ， 如图 10-6 和图 10-7 所示。

三 相关知识

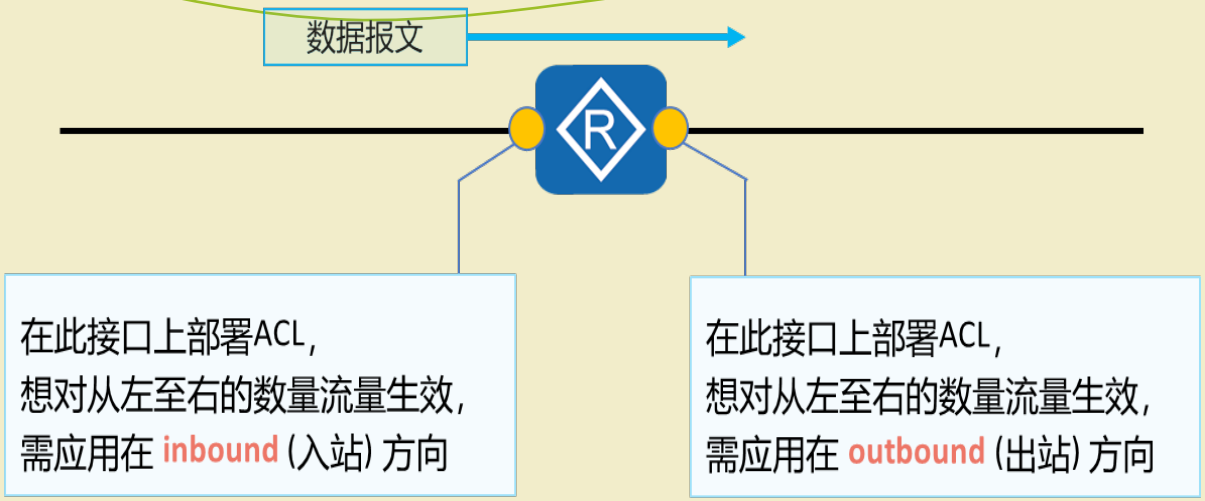


图 10-6 ACL 匹配位置

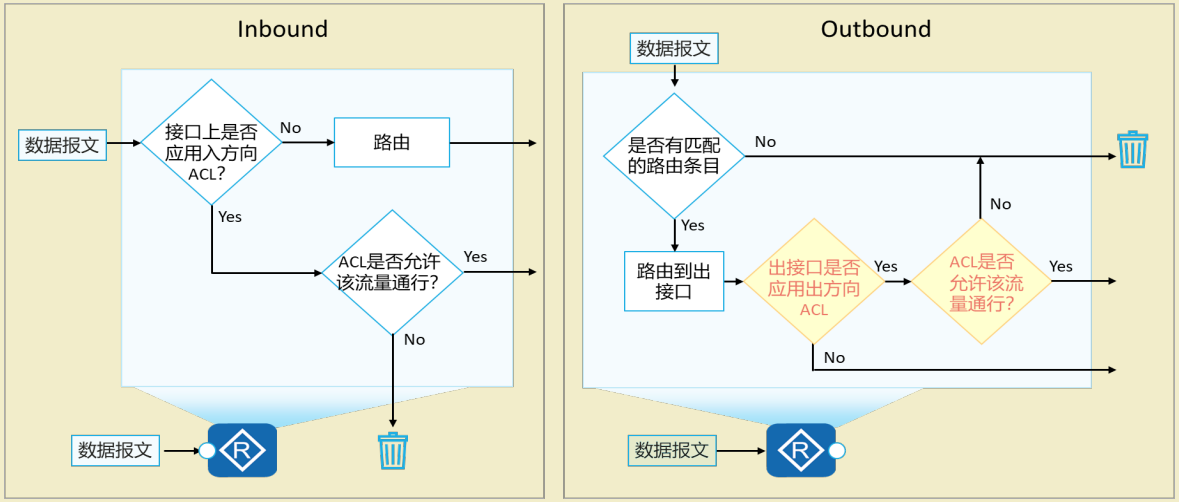


图 10-7 ACL 的入站和出站

六、 ACL 的分类与标识

根据 ACL 所具备的特性不同， ACL 存在如下两种不同方式的分类。

1. 基于 ACL 规则定义方式的分类

分为基本 ACL 、高级 ACL 、二层 ACL 、用户自定义 ACL 和用户 ACL 五

分类	编号范围	规则定义描述
基本 ACL	2000~2999	仅使用报文的源 IP 地址、分片信息和生效时间段信息来定义规则。
高级 ACL	3000~3999	可使用 IPv4 报文的源 IP 地址、目的 IP 地址、 IP 协议类型、 ICMP 类型、 TCP 源 / 目的端口号、 UDP 源 / 目的端口号、生效时间段等来定义规则。
二层 ACL	4000~4999	使用报文的以太网帧头信息来定义规则，如根据源 MAC 地址、目的 MAC 地址、 802.1p 优先级、链路层协议类型等。
用户自定义 ACL	5000~5999	使用报文头、偏移位置、字符串掩码和用户自定义字符串来定义规则。
用户 ACL	6000~6999	既可使用 IPv4 报文的源 IP 地址或源 UCL （ User Control List ）组，也可使用目的 IP 地址或目的 UCL 组、 IP 协议类型、 ICMP 类型、 TCP 源端口 / 目的端口、 UDP 源端口 / 目的端口号等来定义规则。

三 相关知识

2. 基于 ACL 标识方法的分类

分为数字型 ACL 和命名型 ACL 两种类型。

分类	规则定义描述
数字型 ACL	传统的 ACL 标识方法。创建 ACL 时，指定一个唯一的数字标识该 ACL 。
命名型 ACL	通过名称代替编号来标识 ACL 。

三 相关知识

我们知道，用户在创建 ACL 时可以为其指定编号，不同的编号对应不同类型的 ACL 。然而为了便于记忆和识别，用户还可以创建命名型 ACL ，即在创建 ACL 时为其设置名称。

命名型 ACL ，也可以是“名称 数字”的形式，即在定义命名型 ACL 时，同时指定 ACL 编号。如果不指定编号，系统则会自动为其分配一个数字型 ACL 的编号。例如： acl name to_internet 2000 就是创建了一个命名型 ACL 。

在 ACL 的应用中，比较常用的是基本 ACL 和高级 ACL 两类。因此，本项目主要学习的也就是这两类 ACL 。

1. 基本 ACL

基本 ACL 主要针对 IP 报文的源 IP 地址进行匹配，对设备的 CPU 消耗较少，可用于简单的部署，但是使用场景有限，不能提供强大的安全保障。

基本 ACL 的编号范围是 2000-2999 。例如，如果执行命令： acl number 2000 （可省略 number 关键字），就意味着创建的是基本 ACL

2. 高级 ACL

相较于基本 ACL，高级 ACL 提供更高的扩展性，可以对流量进行更精细的匹配，通过配置高级 ACL，可以阻止特定主机或者整个网段的源或者目标 IP 地址，除此之外，还可以使用协议信息（IP、ICMP、TCP、UDP）去过滤相应的流量。

可以理解为：基本 ACL 是高级 ACL 的一个子集，高级 ACL 可以比基本 ACL 定义出更精确、更复杂、更灵活的规则。

高级 ACL 编号范围为 3000 ～ 3999。例如，如果执行命令：acl number 3000（可省略 number 关键字），就意味着创建的是高级 ACL。

10.2 ACL 的应用场景

基于强大的数据报文过滤功能，ACL 可以应用于众多网络控制的场景下，下面介绍一些典型的应用场景。

一、使用 ACL 限制 Telnet 登录权限

ACL 应用在 Telnet 模块中，可以使设备作为 Telnet 服务器时对哪些 Telnet 客户端以 Telnet 方式登录到本设备能加以控

2. 高级 ACL

相较于基本 ACL，高级 ACL 提供更高的扩展性，可以对流量进行更精细的匹配，通过配置高级 ACL，可以阻止特定主机或者整个网段的源或者目标 IP 地址，除此之外，还可以使用协议信息（IP、ICMP、TCP、UDP）去过滤相应的流量。

可以理解为：基本 ACL 是高级 ACL 的一个子集，高级 ACL 可以比基本 ACL 定义出更精确、更复杂、更灵活的规则。

高级 ACL 编号范围为 3000 ～ 3999。例如，如果执行命令：acl number 3000（可省略 number 关键字），就意味着创建的是高级 ACL。

图 10-8 使用 ACL 限制 Telnet 登录权限

二、 SNMP 中应用 ACL 过滤非法网管

ACL 应用在 SNMP 模块中，可以使网管对设备的管理权限得到控制，从而有效防止非法网管操作设备。

如图 10-9 所示，为简单而方便的配置和管理远程设备（ Router ），管理员在 Router 上配置了 SNMP Agent 服务， Agent 及时地向网管报告设备的当前状态信息，使网管可以远端控制设备。同时，管理员配置了基于 ACL 的网管访问权限限制，保证只有可信任的网管（ NMS2 ）才能管理该设备。

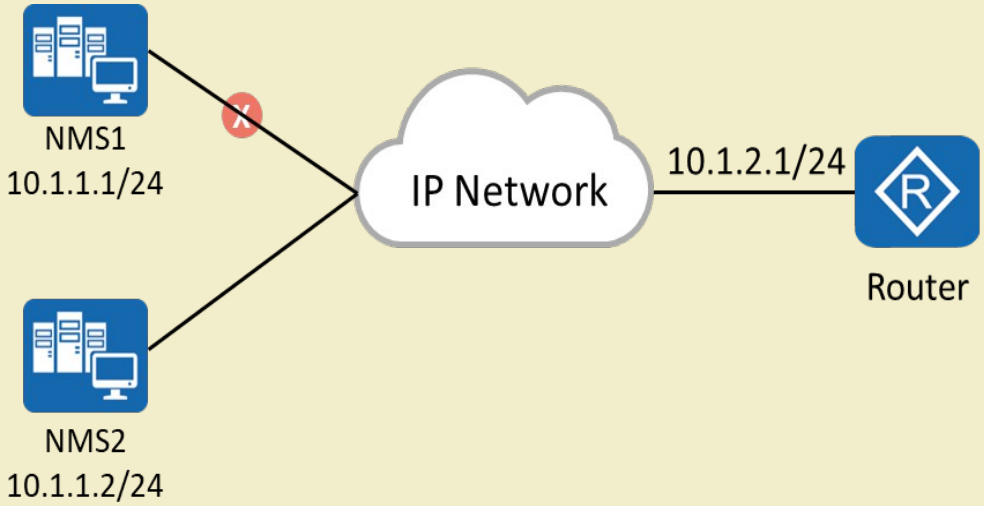


图 10-9 SNMP 中应用 ACL 过滤非法网管

三、使用 ACL 限制不同网段用户的互访

ACL 应用在 QoS 的流策略 / 简化流策略中，可以实现不同网段用户之间访问权限的限制，从而避免用户之间随意访问形成安全隐患。

如图 10-10 所示，某公司为财务部和市场部规划了两个网段的 IP 地址。为了避免两个部门之间相互访问造成公司机密的泄露，管理员在两个部门连接 Router 的接口（ Interface1 和 Interface2 ）的入方向上应用绑定了 ACL 的流策略 / 简化流策略，禁止两个部门的互访。

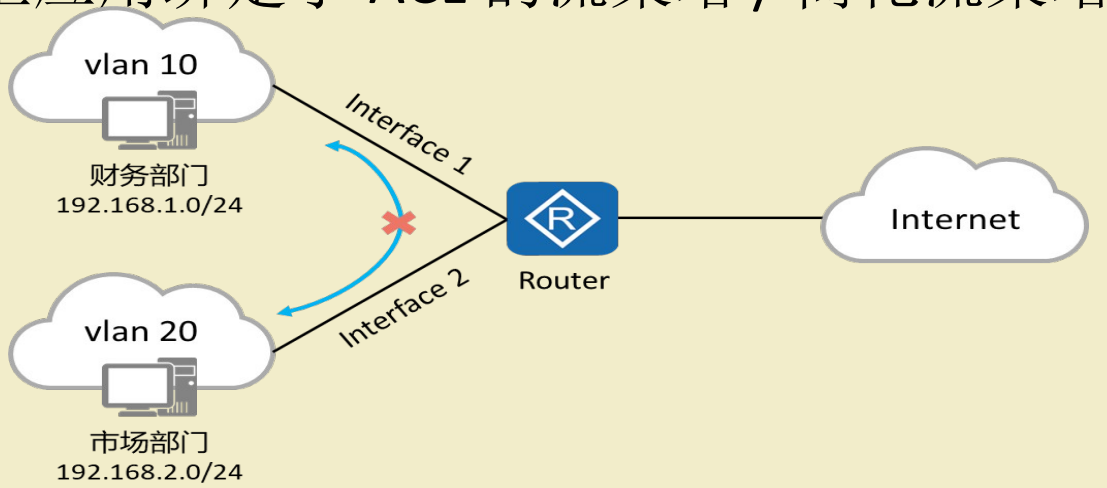


图 10-10 使用 ACL 限制不同网段用户的互访

四、使用 ACL 禁止特定用户主机在特定时间内上网

ACL 应用在 QoS 的流策略 / 简化流策略中，可以实现特定用户主机在特定时间范围内上网权限的限制。

如图 10-11 所示，某公司通过 router 连接到 Internet 。部分员工经常在上班时间访问与工作无关的网站，工作效率低下。所以，管理员配置了基于时间的 ACL ，并在这些用户连接 router 的接口（ Interface 1 ）的入方向上应用绑定了 ACL 的流策略 / 简化流策略，禁止这些用户在工作时间内上网，其余时间均可以上[illegible]

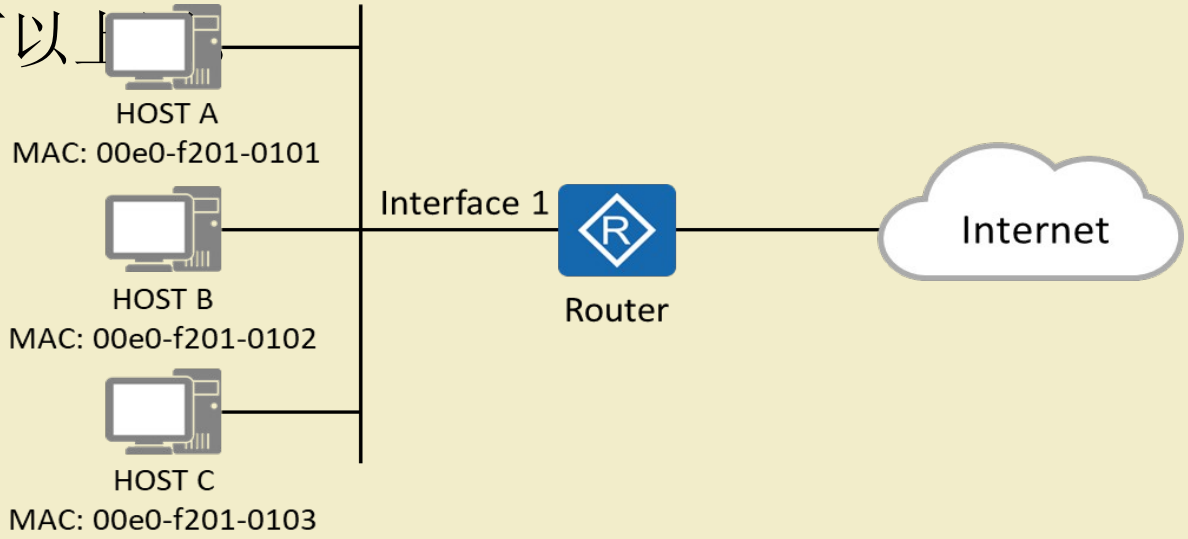


图 10-11 使用 ACL 禁止特定用户在特定时间内上网

五、在 QoS 中使用 ACL 实施流量监管

ACL 应用在 QoS 的流策略 / 简化流策略中，可以实现对不同流量进入网络的速率的监督，对超出部分的流量进行“惩罚”，使进入的流量被限制在一个合理的范围之内，从而保护网络资源和用户的利益。

如图 10-12 所示，某公司的数据业务、视频业务、语音业务分别属于 VLAN 100 、 VLAN 110 、 VLAN120 。由于语音业务对服务质量的要求最高，视频业务次之，数据业务要求最低，所以管理员配置了基于 ACL 的流量监管功能，使设备可以对该公司不同的业务流按照 VLAN ID 进行分类，并对匹配 ACL 规则的报文进行限速，从而将不同业务的流量限制在一个合理的范围之内，保证各业务的带宽需求。

三 相关知识

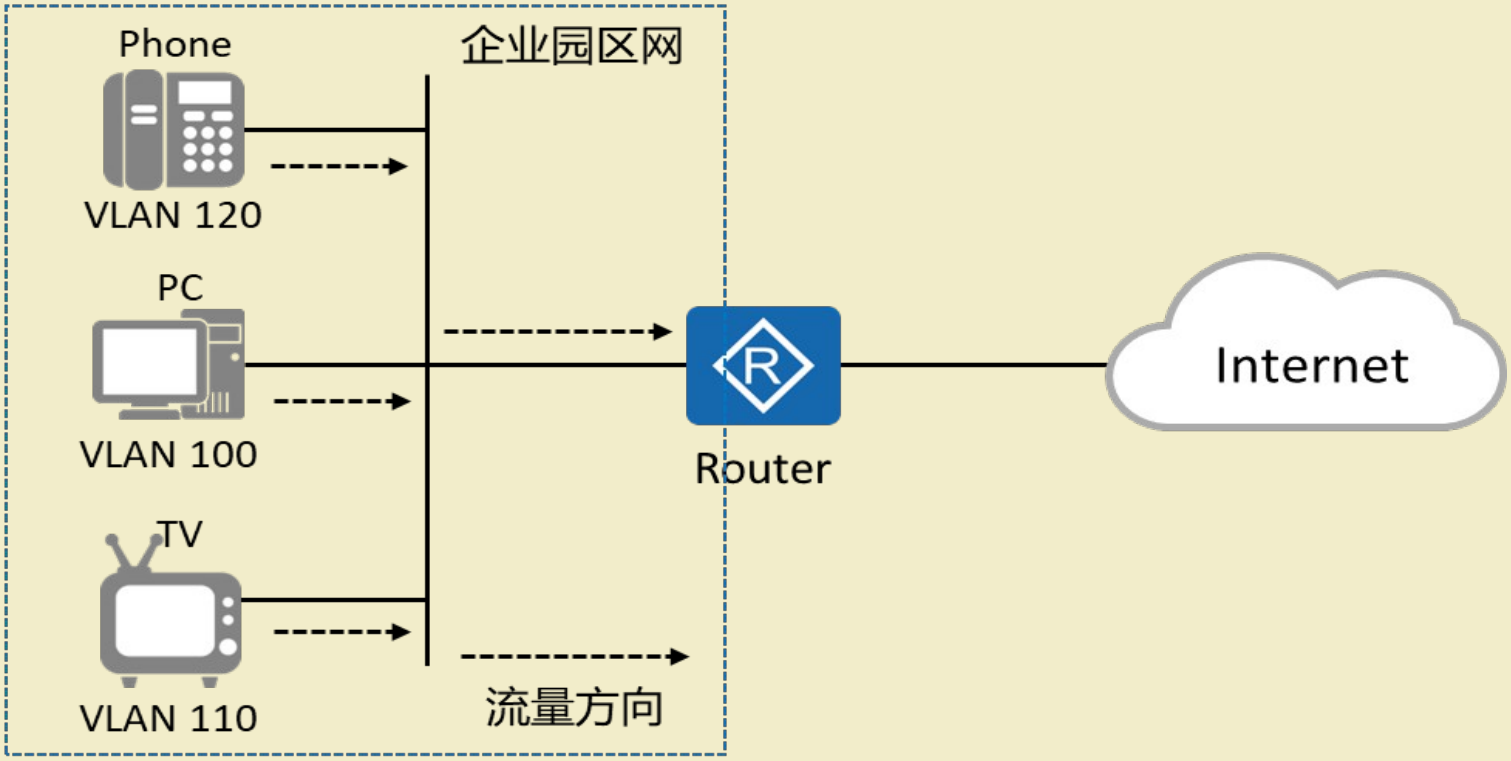


图 10-11 在 QoS 中使用 ACL 实施流量监管

图 10-12 在 OSPF 中使用 ACL 过滤路由信息

三 相关知识

管理员可以在 RouterA 上配置 ACL 和路由策略，使其在路由发布时运用路由策略，仅提供路由 172.16.17.0/24 、 172.16.18.0/24 、 172.16.19.0/24 给 RouterB ，实现 OSPF 网络中只能访问 172.16.17.0/24 、 172.16.18.0/24 和 172.16.19.0/24 三个网段的网络；并且在 RouterC 上配置 ACL 和路由策略，使其在路由引入时运用路由策略，仅接收路由 172.16.18.0/24 ，实现 RouterC 连接的网络只能访问 172.16.18.0/24 网段的网络。

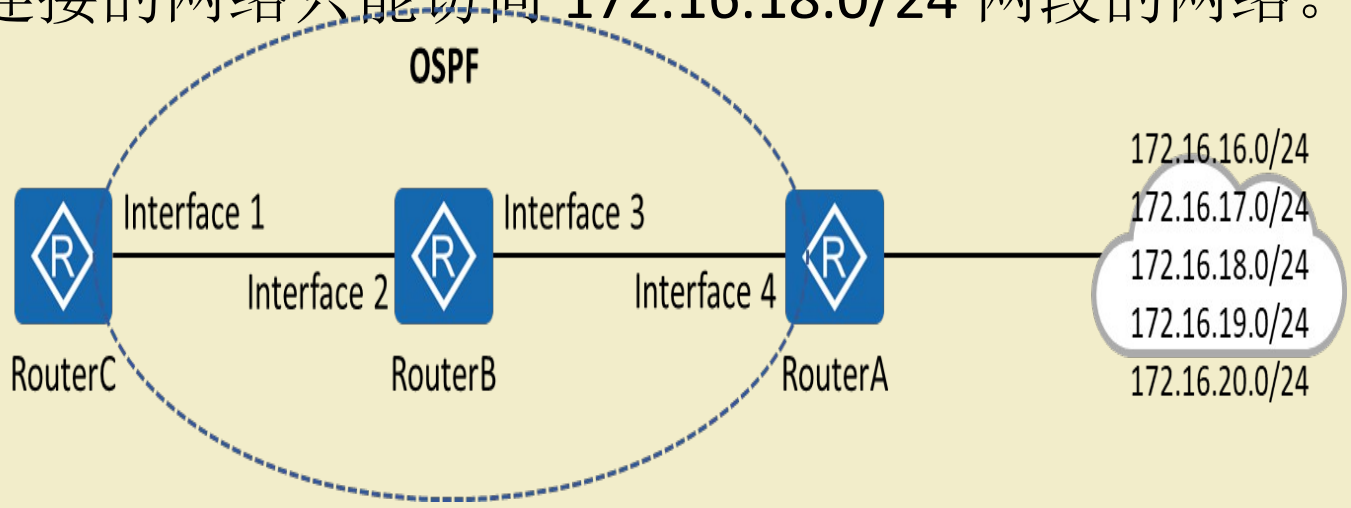


图 10-12 在 OSPF 中使用 ACL 过滤路由信息

七、在 NAT 中使用 ACL 过滤流量

ACL 可以应用在 NAT 过滤功能中，让 NAT 设备对外网发送到内网的流量进行过滤。 NAT 过滤是指 NAT 设备对外网发到内网的流量进行过滤，包括下面三种类型：

（1）与外部地址无关的 NAT 过滤行为。

（2）与外部地址相关的 NAT 过滤行为。

（3）与外部地址和端口都相关的 NAT 过滤行为。

如图 10-13 所示，私网用户 PC-1 通过 NAT 设备与外网用户 PC-2 、 PC-3 进行通信。数据报文 1 代表私网主机 PC-1 访问公网主机 PC-2 ， PC-1 使用的端口号为 1111 ，访问 PC-2 的端口 2222 ；经过 NAT 设备时，源 IP 转换为 3.3.3.3 。

当私网主机向某公网主机发起访问后，公网主机发向私网主机的流量经过 NAT 设备时需要进行过滤。数据报文 2’ 、数据报文 3’ 和数据报文 4’ 代表三种场景，分别对应上述三种 NAT 过滤类型：

三 相关知识

（1）数据报文 2’ 代表公网主机 PC-3 （与报文 1 的目的地址不同）访问私网主机 PC-1，目的端口号为 1111，只有配置了外部地址无关的 NAT 过滤行为，才允许此报文通过，否则被 NAT 设备过滤掉。

（2）数据报文 3’ 代表公网服务器 PC-2 （与报文 1 的目的地址相同）访问私网主机 PC-1，目的端口号为 1111，源端口号为 3333 （与报文 1 的目的端口不同），只有配置了外部地址相关的 NAT 过滤行为或者配置了外部地址无关的 NAT 过滤行为，才允许此报文通过，否则被 NAT 设备过滤掉。

（3）数据报文 4’ 代表公网服务器 PC-2 （与报文 1 的目的地址相同）访问私网主机 PC-1，目的端口号为 1111，源端口号为 2222 （与报文 1 的目的端口相同），这属于外部地址和端口都相关的 NAT 过滤行为，是缺省的过滤行为，不配置或者配置任何类型的 NAT 过滤行为，都允许此报文通过，不会被过滤掉。

三 相关知识

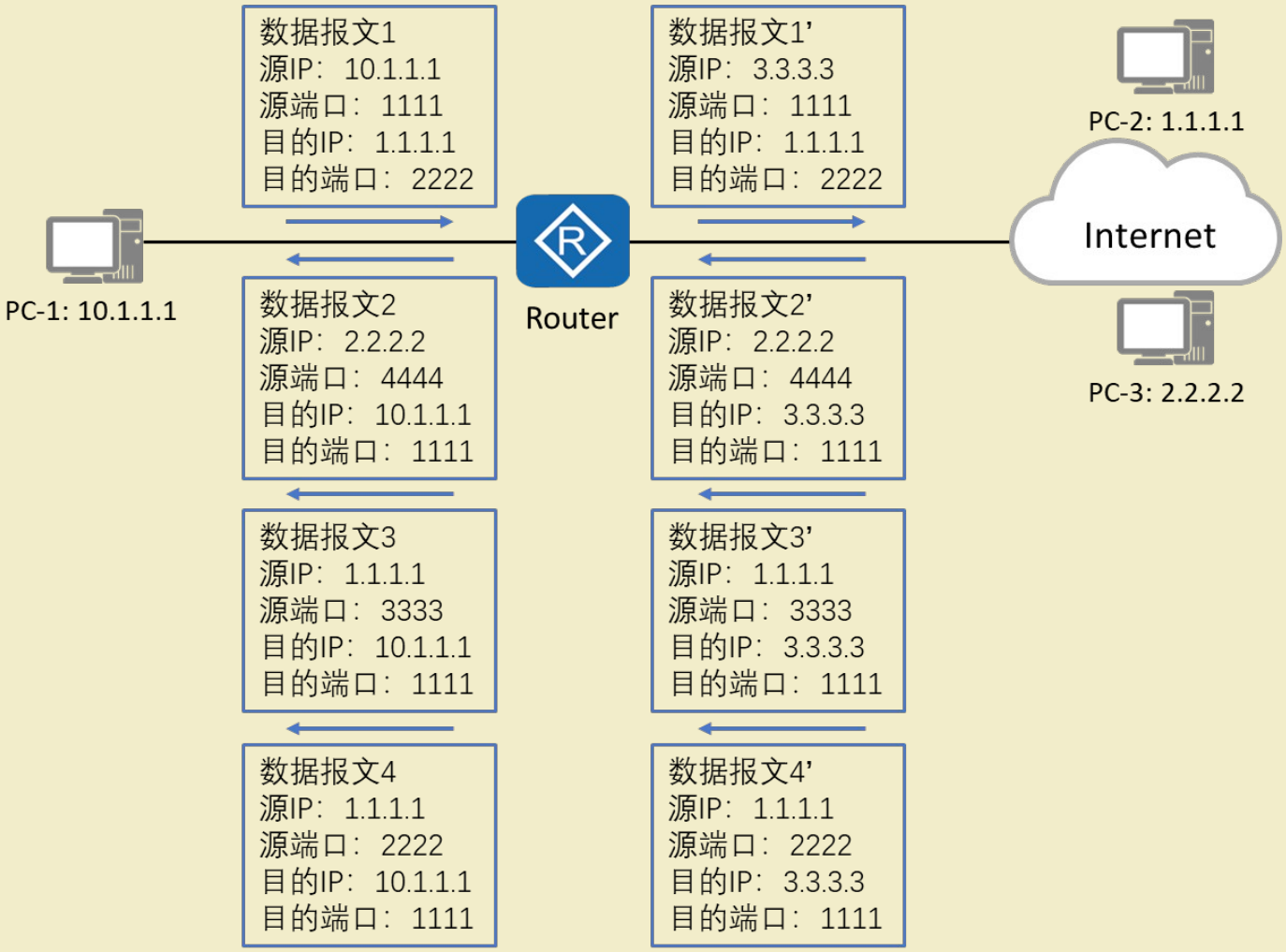


图 10-13 在 NAT 中使用 ACL 过滤流量

八、在防火墙中使用 ACL

防火墙用在内外网络边缘处，防止外部网络对内部网络的入侵，也可以用来保护网络内部大型机和重要的资源（如数据）。

如图 10-14 所示，只允许外部特定主机 PC-A 访问内部网络中的数据中心，别的访问都不允许。在 Router 上部署防火墙并配置 ACL，就可以达到这个要求。

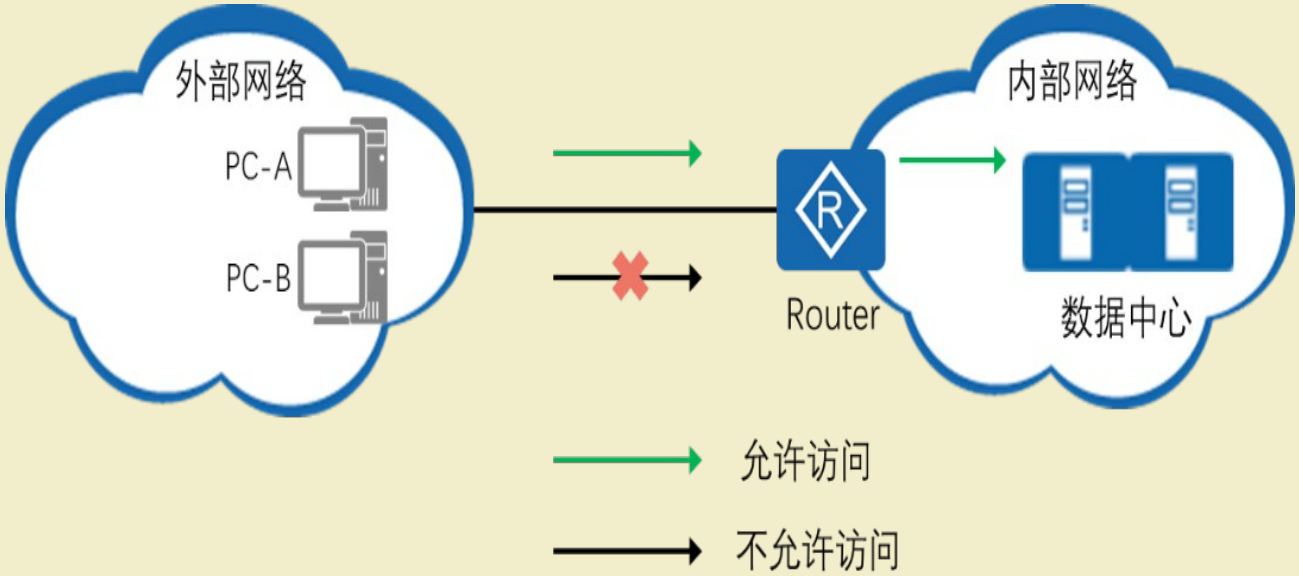


图 10-14 在防火墙中使用 ACL

10.3 ACL 的配置

一、配置基本 ACL

1. 创建基本 ACL

（1）使用编号（2000 ～ 2999）创建一个数字型的基本 ACL，并进入基本 ACL 视图。

[Huawei] acl [number] acl-number [match-order config]

acl-number：指定访问控制列表的编号。

match-order config：指定 ACL 规则的匹配顺序，config 表示配置顺序。

（2）使用名称创建一个命名型的基本 ACL，并进入基本 ACL 视图。

[Huawei] acl name acl-name { basic | acl-number } [match-order config]

acl-name：指定创建的 ACL 的名称。

basic：指定 ACL 的类型为基本 ACL。

2. 配置基本 ACL 的规则

在基本 ACL 视图下，通过此命令来配置基本 ACL 的规则。

[Huawei-acl-basic-2000] rule [rule-id] { deny | permit } [source { source-address source-wildcard | any } | time-range time-name]

rule-id：指定 ACL 的规则 ID 。

deny：指定拒绝符合条件的报文。

permit：指定允许符合条件的报文。

source { source-address source-wildcard | any }：指定 ACL 规则匹配报文的源地址信息。如果不配置，表示报文的任何源地址都匹配。其中：

source-address：指定报文的源地址。

source-wildcard：指定源地址通配符。

any：表示报文的任意源地址。相当于 source-address 为 0.0.0.0 或者 source-wildcard 为 255.255.255.255 。

三 相关知识

time-range time-name ： 指定 ACL 规则生效的时间段。其中， time-name 表示 ACL 规则生效时间段名称。如果不指定时间段，表示任何时间都生效。

例【 10.4 】：使用基本 ACL 过滤数据流量示例，网络拓扑如下图所示。

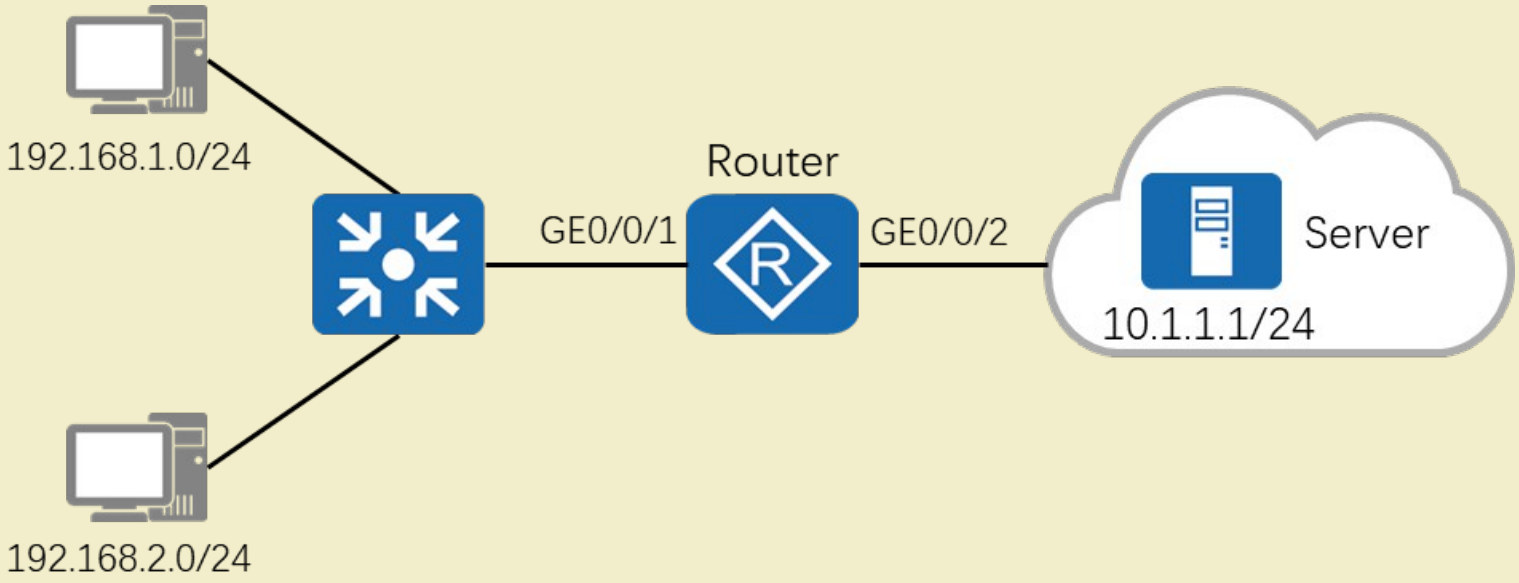


图 10-15 基本 ACL 的应用

2. 配置需求

在 Router 上部署基本 ACL，将试图穿越 Router 的源地址为 192.168.1.0/24 网段的数据包过滤掉，从而禁止 192.168.1.0/24 网段的用户访问 Router 右侧的服务器网络，而 192.168.2.0/24 等其他网段的流量则不受影响。

3. 配置思路

配置基本 ACL 和流量过滤，使设备可以对特定网段的报文进行过滤。

4. 配置步骤

（1）完成上图所示的路由器接口 IP 地址及路由的相关配置（略）。

（2）在 Router 上创建基本 ACL，禁止 192.168.1.0/24 网段访问服务器所在网络，允许其他网段的报文通过。

三 相关知识

[Router] acl 2000
[Router-acl-basic-2000] rule deny source 192.168.1.0 0.0.0.255
[Router-acl-basic-2000] rule permit source any
（3）由于从接口 GE0/0/1 进入 Router，所以在接口 GE0/0/1 的入方向配置流量过滤。
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] traffic-filter inbound acl 2000
[Router-GigabitEthernet0/0/1] quit
备注： traffic-filter 命令是用来在接口上配置 ACL 对报文进行过滤，其命令格式为：
traffic-filter { inbound | outbound } acl { acl-number | name acl-name }
inbound：指定在接口入方向上配置报文过滤。
outbound：指定在接口出方向上配置报文过滤。
acl：指定基于 IPv4 ACL 对报文进行过滤。

2. 配置高级 ACL 的规则

根据 IP 承载的协议类型不同，可以在设备上配置不同的高级 ACL 规则。对于不同的协议类型，有不同的参数组合。

（1）当参数 protocol 为 IP 时，在高级 ACL 视图下，配置其规则的命令格式为：

rule [rule-id] { deny | permit } ip [destination { destination-address destination-
wildcard | any } | source { source-address source-wildcard | any } | time-range time-name | [dscp dscp | [tos tos | precedence precedence]]]

ip ：指定 ACL 规则匹配报文的协议类型为 IP 。

destination { destination-address destination-wildcard | any } ：指定 ACL 规则匹配报文的目的地址信息。如果不配置，表示报文的任何目的地址都匹配。

dscp dscp ： 指定 ACL 规则匹配报文时，区分服务代码点（Differentiated Services Code Point ），取值为 0%63

二、配置高级 ACL

1. 创建高级 ACL

使用编号（ 3000 ～ 3999 ）创建一个数字型的高级 ACL ， 并进入高级 ACL 视图。

[Huawei] acl [number] *acl-number* [match-order config]

acl-number ： 指定 ACL 的编号。

match-order config ： 指定 ACL 规则的匹配顺序， config 表示配置顺序。

使用名称创建一个命名型的高级 ACL ， 并进入高级 ACL 视图。

[Huawei] acl name*acl-name* { advance | acl-number } [match-order config]

acl-name ： 指定创建的 ACL 的名称。

advance ： 指定 ACL 的类型为高级 ACL 。

2. 配置高级 ACL 的规则

根据 IP 承载的协议类型不同，可以在设备上配置不同的高级 ACL 规则。对于不同的协议类型，有不同的参数组合。

（1）当参数 protocol 为 IP 时，在高级 ACL 视图下，配置其规则的命令格式为：

rule [rule-id] { deny | permit } ip [destination { destination-address destination-
wildcard | any } | source { source-address source-wildcard | any } | time-range time-name | [dscp dscp | [tos tos | precedence precedence]]]

ip ：指定 ACL 规则匹配报文的协议类型为 IP 。

destination { destination-address destination-wildcard | any } ：指定 ACL 规则匹配报文的目的地址信息。如果不配置，表示报文的任何目的地址都匹配。

三 相关知识

dscp dscp：指定 ACL 规则匹配报文时，区分服务代码点（Differentiated Services Code Point），取值为：0~63。

tos tos：指定 ACL 规则匹配报文时，依据服务类型字段进行过滤，取值为：0~15。

precedence precedence：指定 ACL 规则匹配报文时，依据优先级字段进行过滤。precedence 表示优先级字段值，取值为：0~7。

（2）当参数 protocol 为 TCP 时，在高级 ACL 视图下，配置其规则的命令格式为：

rule [rule-id] { deny | permit } { protocol-number | tcp } [destination { destination-address destination-wildcard | any } | destination-port { eq port | gt port | lt port | range port-start port-end } | source { source-address source-wildcard | any } | source-port { eq port | gt port | lt port | range port-start port-end } | tcp-flag { ack | fin | syn } * | time-range time-name] *

三 相关知识

protocol-number | tcp：指定 ACL 规则匹配报文的协议类型为 TCP 。可以采用数值 6 表示指定 TCP 协议。

destination-port { eq port | gt port | lt port | range port-start port-end}：指定 ACL 规则匹配报文的 UDP 或者 TCP 报文的目的端口，仅在报文协议是 TCP 或者 UDP 时有效。如果不指定，表示 TCP/UDP 报文的任何目的端口都匹配。其中：

eq port：指定等于目的端口；

gt port：指定大于目的端口；

lt port：指定小于目的端口；

range port-start port-end：指定源端口的范围。

tcp-flag：指定 ACL 规则匹配报文的 TCP 报文头中 SYN Flag 。

例【 10.5 】：使用高级 ACL 限制不同网段的用户互访示例，网络拓扑如下图所示。

三 相关知识

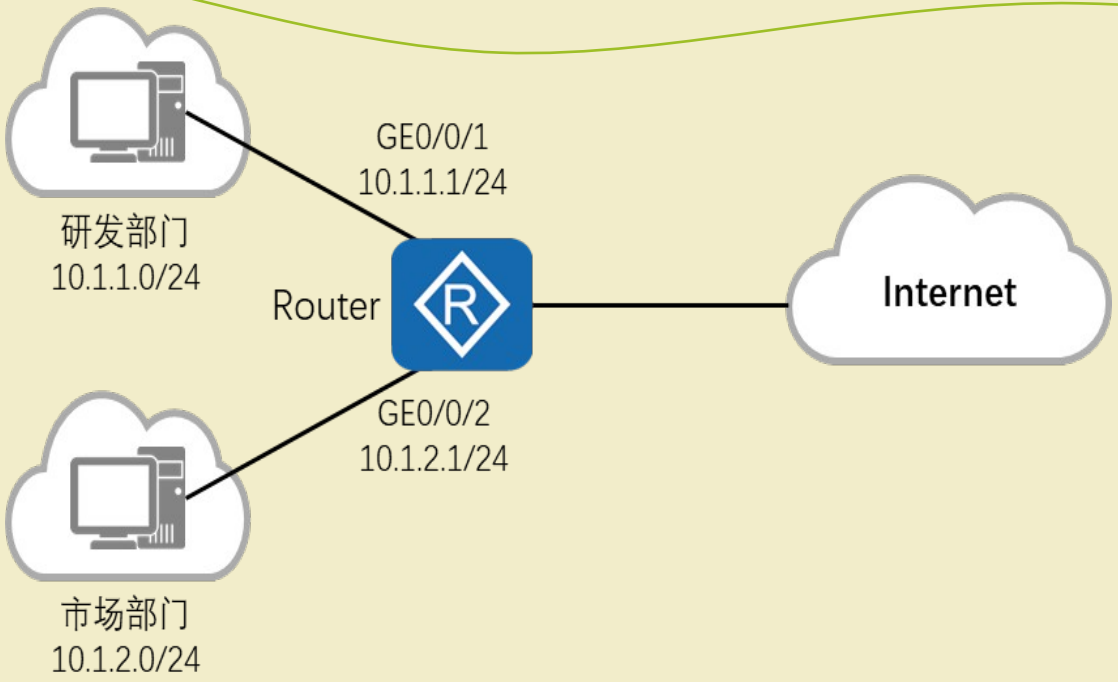


图 10-16 高级 ACL 的应用

2. 配置需求

（1）某公司通过 Router 实现各部门之间的互连。为方便管理网络，管理员为公司的研发部和市场部规划了两个网段的 IP 地址。

（2）现要求 Router 能够限制两个网段之间互访，防止公司机密泄露。

3. 配置思路

配置高级 ACL 和流量过滤，使设备可以对研发部与市场部互访的报文进行过滤。

4. 配置步骤

（1）完成上图所示的路由器接口 IP 地址及路由的相关配置（略）。

（2）创建高级 ACL 3001 并配置 ACL 规则，拒绝研发部访问市场部的报文通过。

```
[Router] acl 3001
[Router-acl-adv-3001] rule deny ip source 10.1.1.0 0.0.0.255
destination 10.1.2.0 0.0.0.255
[Router-acl-adv-3001] quit
```

（3）创建高级 ACL 3002 并配置 ACL 规则，拒绝市场部访问研发部的报文通过。

```
[Router] acl 3002
[Router-acl-adv-3002] rule deny ip source 10.1.2.0 0.0.0.255
destination 10.1.1.0 0.0.0.255
[Router-acl-adv-3002] quit
```

（4）由于研发部和市场部互访的流量分别从接口 GE0/0/1 和 GE0/0/2 进入 Router，所以在接口 GE0/0/1 和 GE0/0/2 的入方向配置流量过滤。

```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] traffic-filter inbound acl 3001
[Router-GigabitEthernet0/0/1] quit
[Router] interface GigabitEthernet 0/0/2
[Router-GigabitEthernet0/0/2] traffic-filter inbound acl 3002
[Router-GigabitEthernet0/0/2] quit
```

四 项目实施及总结

具体实施过程参考实训报告

【项目总结】

本项目详细介绍了 ACL 技术的基本原理、应用场景及配置，主要学习了以下知识内容。

1. ACL 是一种基于包过滤的网络安全访问控制技术，它可以根据设定的条件对接口上的数据包进行过滤，允许其通过或丢弃。

2. ACL 技术总是与防火墙、路由策略、 QoS 、流量过滤及 NAT 等其他技术结合使用。

3. 一个 ACL 通常由若干条语句（ rule ）组成，每条语句就是该 ACL 的一条规则，每条语句中的“ permit （允许）或 deny （拒绝）”就是与这条规则相对应的处理动作。

4. 常见的 ACL 分为基本 ACL 和高级 ACL 两种类型。基本 ACL 仅仅只使用源地址进行过滤，根据数据包的源 IP 地址来允许或拒绝数据包：

而高级 ACL 则基于源和目的地址、传输层协议和应用端口号进行过滤，每个调都必须匹配，才会施加允许或拒绝条件，使用扩展 ACL 可实现更加精确的流量控制。

5. 当进行 IP 地址匹配的时候，后面会跟着 32 位的通配符掩码，用于指示 IP 地址中，哪些比特位需要严格匹配，哪些比特位无需匹配，其中“ 0”表示“匹配”，“ 1”表示“不关心”。

6. ACL 在现有网络中有非常多的应用场景，典型场景有：使用 ACL 限制 Telnet 登录权限、 SNMP 中应用 ACL 过滤非法网管、使用 ACL 限制不同网段用户的互访、使用 ACL 禁止特定用户主机在特定时间内上网、在 QoS 中使用 ACL 实施流量监管
在、 OSPF 中使用 ACL 过滤路由信息、在 NAT 中使用 ACL 过滤流量、在防火墙中使用 ACL 等。

7. ACL 的使用分为两个步骤。第一步创建 ACL 并定义相关的过滤规则，第二步在准备应用 ACL 的网络设备接口（ INBOUND 或 OUTBOUND 方向）上调用第一步创建的 ACL 进行数据包的过滤

谢谢！