Network03 三层交换机 OSPF 传输层 ACL

一 vlan 优点

控制广播,隔离广播域

增加安全

带宽利用率提高

降低数据传递延迟

二 路由器

实现不同网段的链接

隔离控制广播

三 三层交换机

交换机 二层设备

路由器 三层设备

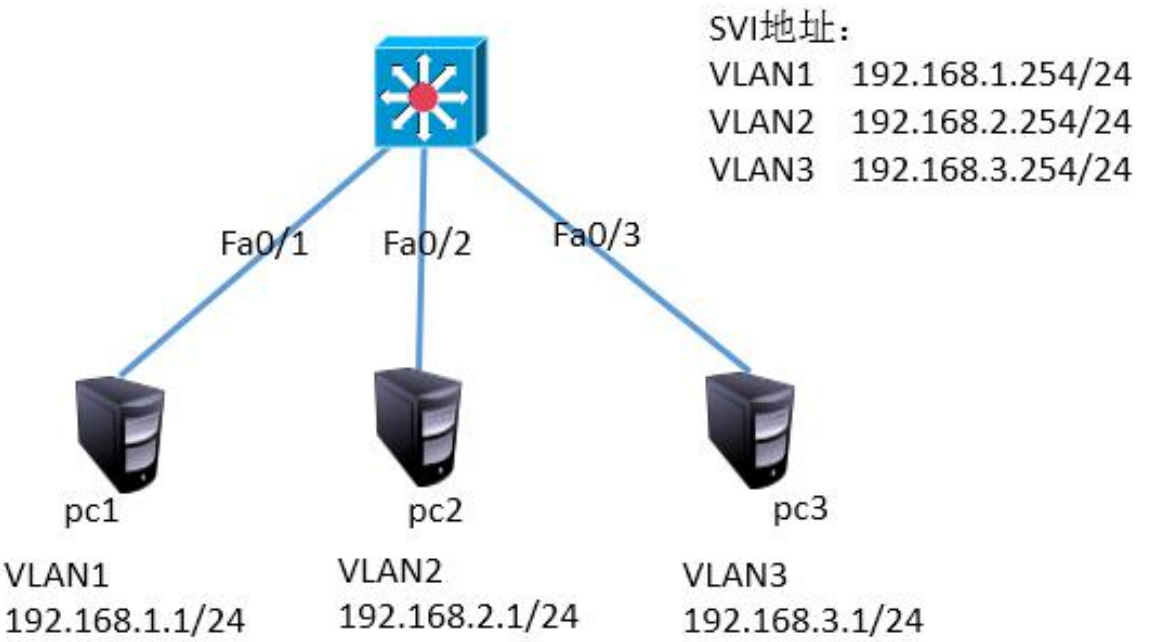
三层交换机=二层交换+三层路由转发 //功能上的相加

S5700

三层交换机接口无法配置 IP,在虚拟接口配置 IP,所有的 vlan 可充当虚拟接口

问题

按照图的拓扑结构配置 ip 地址并通过三层交换实现 VLAN 间通信



步骤

三层交换机配置 S5700

用户视图 sys

系统视图:in g0/0/2

接口视图: port link-type access

port default vlan 2 //将端口加入 vlan,g0/0/1 默认在 vlan 1

g0/0/3 相同方法设置

系统视图:dis vlan

[Huawei]vlan batch 2 3

[Huawei]interface Vlanif 1 //Vlanif 表示虚拟接口

[Huawei-Vlanif1]ip address 192.168.1.254 24

[Huawei]interface Vlanif 2

[Huawei-Vlanif1]ip address 192.168.2.254 24

[Huawei]interface Vlanif 3

[Huawei-Vlanif1]ip address 192.168.3.254 24

添加交换机 3700

四 动态路由

动态路由,基于某种路由协议实现

特点:减少了管理任务,占用了网络带宽

适合大中型网络使用

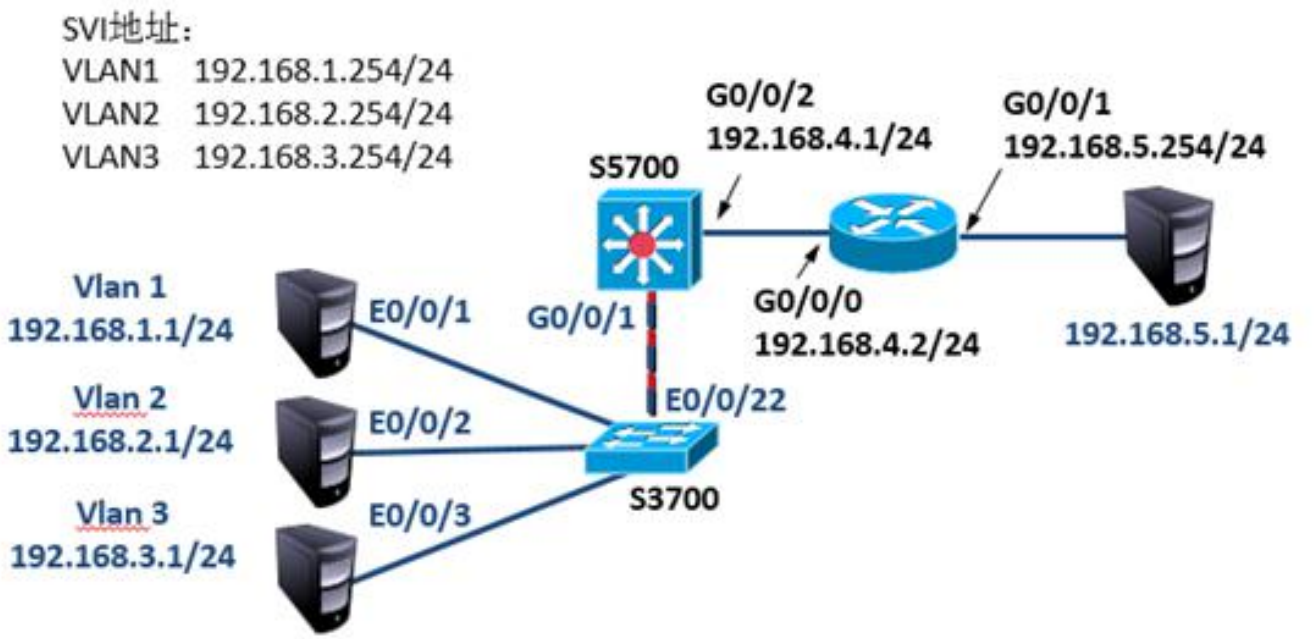
动态路由协议之一

OSPF: **O**pen **S**hortest **P**ath **F**irst(开放式最短路径优先),**兼容性最强**

案例 1：动态路由(以上个案例为基础)

1.1 问题

通过配置静态路由协议 ospf 实现全网互通



1.2 步骤

S3700 交换机配置

```
[Huawei]vlan batch 2 3          //创建 VLAN2、3

[Huawei]interface Ethernet0/0/2

[Huawei-Ethernet0/0/2]port default vlan 2

[Huawei]interface Ethernet0/0/3

[Huawei-Ethernet0/0/3]port default vlan 3

[Huawei]interface Ethernet0/0/22

[Huawei-Ethernet0/0/22]port link-type trunk              //配置中继链路

[Huawei-Ethernet0/0/22]port trunk allow-pass vlan all
```

S5700 交换机配置

```
[Huawei]vlan batch 2 3 4          //创建 VLAN2、3、4

[Huawei]interface Vlanif 1

[Huawei-Vlanif4]ip address    192.168.1.254 24

[Huawei]interface Vlanif 2

[Huawei-Vlanif4]ip address    192.168.2.254 24

[Huawei]interface Vlanif 3

[Huawei-Vlanif4]ip address    192.168.3.254 24

[Huawei]interface Vlanif 4

[Huawei-Vlanif4]ip address    192.168.4.1 24
```

[Huawei]interface GigabitEthernet 0/0/1

[Huawei-GigabitEthernet0/0/1] port link-type trunk　　//配置中继链路

[Huawei-GigabitEthernet0/0/1] port trunk allow-pass vlan all

[Huawei]interface GigabitEthernet 0/0/2　　//配置 g0/0/2

[Huawei-GigabitEthernet0/0/2] port link-type access

[Huawei-GigabitEthernet0/0/2] port default vlan 4

[Huawei]ospf 1　　//开起动态路由 ospf

[Huawei-ospf-1]area 0

//进入第一个区域,一般超大型网络才需要多个区域

中小规模只使用第一个也就是 0 区域即可

[Huawei-ospf-1-area-0.0.0.0]network 192.168.1.0 0.0.0.255　//反子掩

//宣告设备自身所链接的网段

[Huawei-ospf-1-area-0.0.0.0]network 192.168.2.0 0.0.0.255

[Huawei-ospf-1-area-0.0.0.0]network 192.168.3.0 0.0.0.255

[Huawei-ospf-1-area-0.0.0.0]network 192.168.4.0 0.0.0.255

[Huawei]ip route-static 0.0.0.0 0.0.0.0 192.168.4.2

路由器 AR2220 配置

[Huawei]interface GigabitEthernet 0/0/0

[Huawei-GigabitEthernet0/0/0] ip address　192.168.4.2 24

[Huawei]interface GigabitEthernet 0/0/1

[Huawei-GigabitEthernet0/0/0] ip address 192.168.5.254 24

[Huawei]ospf 1

[Huawei-ospf-1]area 0

[Huawei-ospf-1-area-0.0.0.0]network 192.168.4.0 0.0.0.255

[Huawei-ospf-1-area-0.0.0.0]network 192.168.5.0 0.0.0.255

[Huawei]ip route-static 0.0.0.0 0.0.0.0 192.168.4.1

三层交换机 路由器 display ip routing-table | linclude /24 查看路由表

五 默认路由

直连路由: 配置 IP,并开启端口自动生成 direct

静态路由: 手动设置,要注意 nexthop static

动态路由: 需要进行宣告 ospf

默认路由: 是特殊的静态路由,能够匹配任意网段 static

当路由表中无法查询到目标网络时,最后才使用默认路由

0.0.0.0 0

任意网段 子掩(0.0.0.0 的写法,同 255.255.255.0 写为 24)

三层交换机 S5700 (接上例)

系统视图

ip route-static 0.0.0.0 0 192.168.4.2

路由器 AR2220 (接上例)

系统视图

ip route-static 0.0.0.0 0 192.168.4.1

三层交换机 路由器 dis ip routing-table 查看

六 传输层

层	配置项目	数据传输类型
传输层	端口号	端到端传输数据
网络层	路由器 ip	点到点传输数据
数据链路层	交换机 vlan trunk mac	点到点传输数据

6.1 传输层协议

TCP: **T**ransmission **C**ontrol **P**rotocol 传输控制协议

可靠的 面向连接的协议(面向连接即数据检查)

传输效率低

UDP: **U**ser **D**atagram **P**rotocol 用户数据报协议

不可靠 无连接的服务 传输效率高

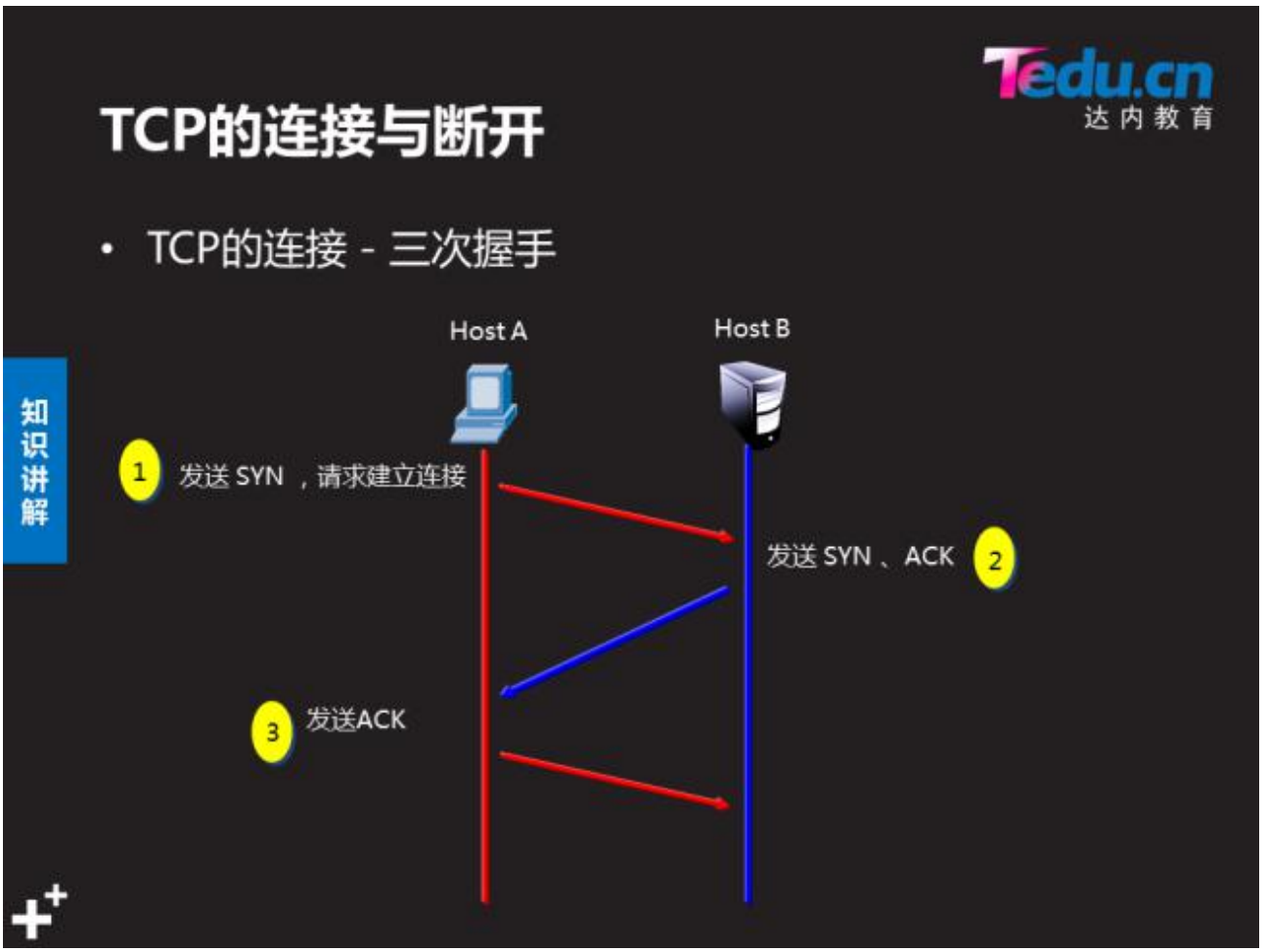
TCP 封装格式

SYN: 请求与对方建立连接

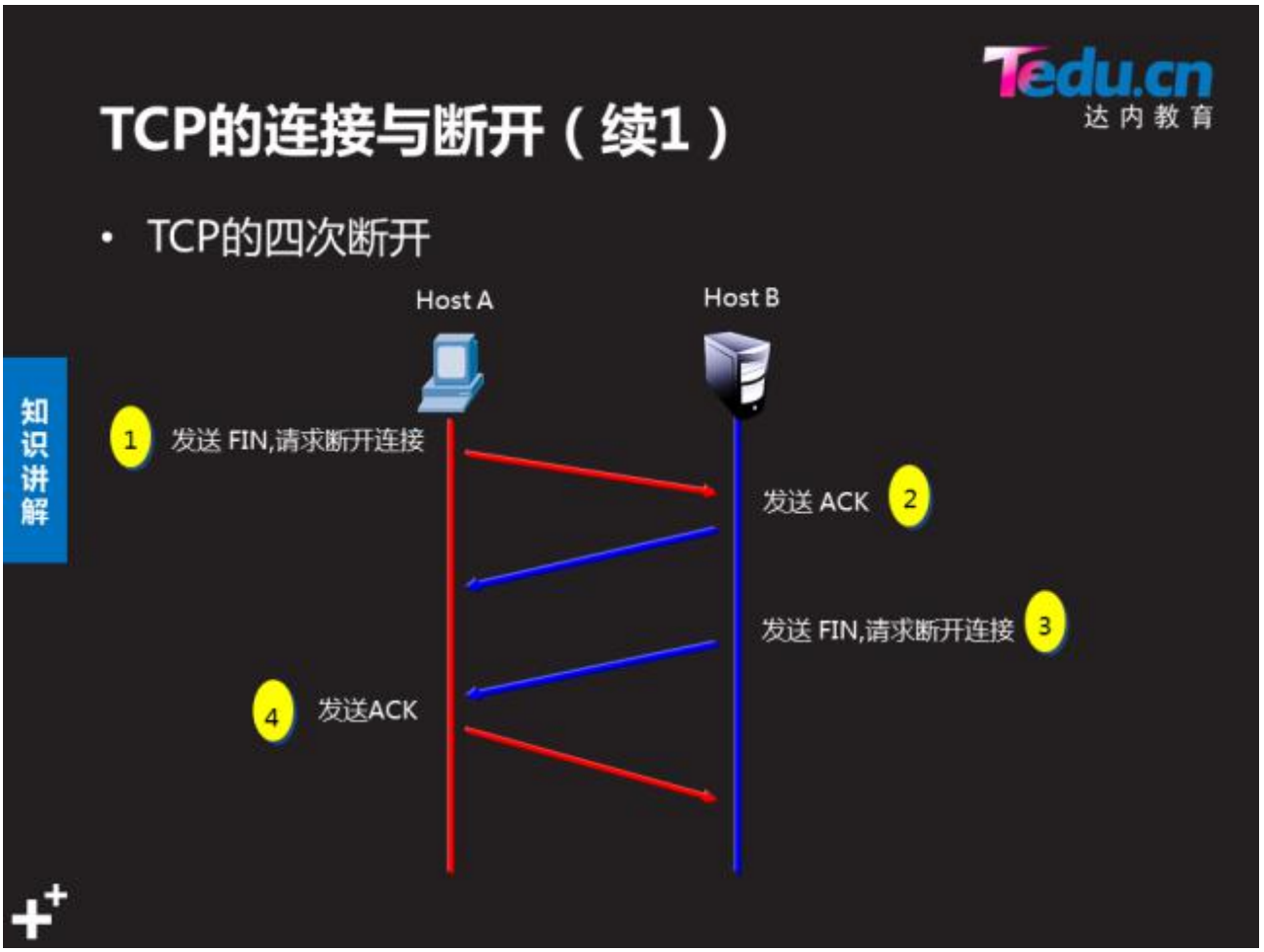
ACK: 确认连接

FIN: 请求与对方断开连接

6.2 TCP 连接的三次握手　　syn-> ack , syn-> ack



6.3 TCP 的四次断开　　fin-> ack ,　fin-> ack



TCP 的应用

端口	协议	说明
21	FTP	文件传输协议,用于上传下载
23	Telnet	用于远程登录,通过连接目标计算机的这一端口可以远程控制管理目标计算机
25	SMTP	简单邮件传输协议,用于发送邮件
53	DNS	域名服务,当用户输入网站的名称后,由 DNS 负责将它解析成 IP 地址
80	HTTP	超文本传输协议,通过 HTTP 实现网络上超文本的传输

UDP 的应用

端口	协议	说明
69	TFTP	简单文本传输协议
53	DNS	域名服务
123	NTP	网络时间协议

6.4 ACL

访问控制列表,应用在路由器接口的指令列表(即规则)

作用,对匹配的数据进行限制

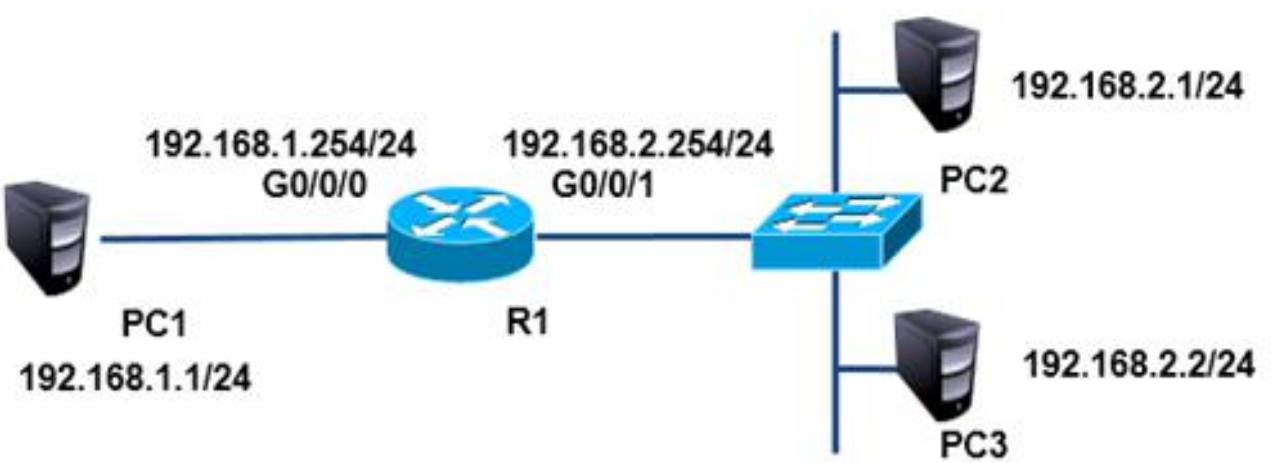
基本 ACL: 列表号 2000-2999 可以对源 IP 限制

高级 ACL: 列表号 3000-3999 可以对源 IP 目标 IP 协议端口 限制

案例 2：基本 ACL 的配置（1）

2.1 问题

按照图-2 所示拓扑结构，禁止主机 pc2 与 pc1 通信，而允许所有其他流量



2.2 步骤

路由器 AR2220

[Huawei]interface GigabitEthernet 0/0/0

[Huawei-GigabitEthernet0/0/0] ip address 192.168.1.254 24

[Huawei]interface GigabitEthernet 0/0/1

[Huawei-GigabitEthernet0/0/1]ip address 192.168.2.254 24

[Huawei]acl 2000 //创建 acl,列表号是 2000,表示即将使用基本 acl

[Huawei-acl-basic-2000]rule deny source 192.168.2.1 0

//创建规则,拒绝源 IP 为 192.168.2.1 的数据通过

0 表示 1 台主机,不是一个网段

[Huawei-GigabitEthernet0/0/1]traffic-filter inbound acl 2000

//进入 g0/0/1 接口后,放置 acl 2000,用来过滤即将进入路由器的数据

//接口选择以节约硬件资源为准,选择数据进的接口

deny: 阻止 permit: 允许 source: 源

//sys //用于案例 3

//acl 2000 //重新进入 acl 2000

//dis this //查看

//undo rule 5 //删除之前的条目,根据序号删除

//dis this

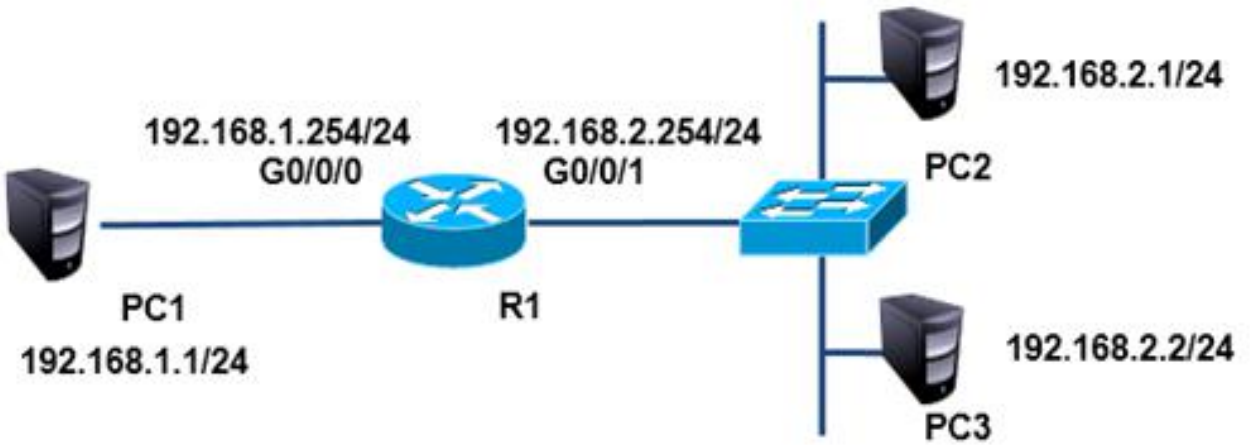
//rule permit source 192.168.2.1 0 //创建新条目,允许源 IP 192.168.2.1 的主机通过

//rule deny //创建新条目,拒绝所有

案例 3：基本 ACL 的配置（2）

3.1 问题

按照图所示拓扑结构，允许主机 pc2 与 pc1 互通，而禁止其他设备访问 pc1



3.2 步骤

注：此案例需要提前配置好所有设备的 ip 地址

[Huawei]acl 2001

[Huawei-acl-basic-2001]rule permit source 192.168.2.1 0

[Huawei-acl-basic-2001]rule deny source any

[Huawei]interface GigabitEthernet 0/0/1

[Huawei-GigabitEthernet0/0/1]undo traffic-filter inbound acl 2000

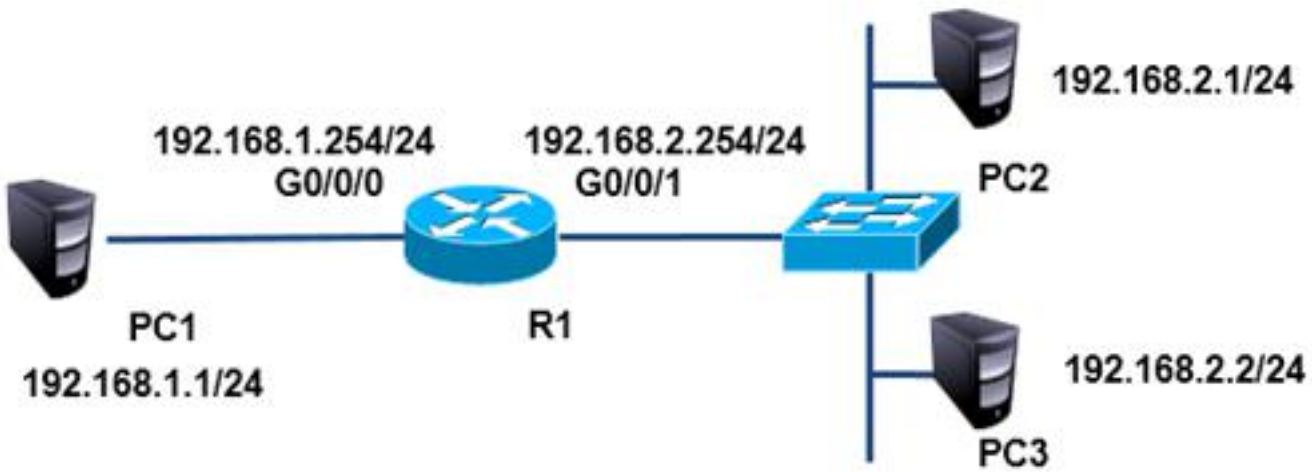
//同接口的同方向,只能放一条 acl 列表

[Huawei-GigabitEthernet0/0/1] traffic-filter inbound acl 2001

案例 4：高级 ACL

4.1 问题

按照图所示拓扑结构，禁止 pc2 访问 pc1 的 ftp 服务，禁止 pc3 访问 pc1 的 www 服务，所有主机的其他服务不受限制



4.2 步骤

注：此案例需要提前配置好所有设备的 ip 地址

[Huawei]acl 3000

[Huawei-acl-adv-3000]rule deny tcp source 192.168.2.1 0 destination 192.168.1.1

0 destination-port eq 21

[Huawei-acl-adv-3000]rule deny tcp source 192.168.2.2 0 destination 192.168.1.1

0 destination-port eq 80

[Huawei]interface g0/0/1

[Huawei-GigabitEthernet0/0/1]traffic-filter inbound acl 3000　　//在接口中应用 acl