南 开 大 学

计算机学院

网络技术与应用课程报告

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**第7次实验报告**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

学号：2012522

姓名：郭坤昌

年级：2020

专业：计算机科学与技术

2022年12月4日

1. **实验内容说明**

实验7：防火墙和SSL实验

1. 防火墙实验在虚拟仿真环境下完成，要求如下：

（1）了解包过滤防火墙的基本配置方法、配置命令和配置过程。

（2）利用标准ACL，将防火墙配置为只允许某个网络中的主机访问另一个网络。

（3）利用扩展ACL，将防火墙配置为拒绝某个网络中的某台主机访问网络中的Web服务器。

（4）将防火墙配置为允许内网用户自由地向外网发起TCP连接，同时可以接收外网发回的TCP应答数据包。但是，不允许外网的用户主动向内网发起TCP连接

2. SSL实验在实体环境下完成，要求如下（选做）

（1）完成Web服务器的证书生成、证书审批、证书安装、证书允许等整个过程。

（2）实现浏览器与Web服务器的安全通信。

1. **实验准备**
2. 访问控制列表相关知识与配置
3. 标准ACL

利用P数据报中的源IP地址对过往的数据包进行控制。添加所用命令为

Access-list ListNum {permit|deny} SrcIPAddr SrcWildMask

其中，ListNum为ACL的列表号，取值范围为1~99。相同ListNum的规则属于同一个ACL，其先后顺序按照加入的先后顺序定。

匹配成功后，网络设备采取允许通过或丢弃动作。

SrcIPAddr表示源IP地址，SRCWildMask表示通配符，用以定义IP地址的范围。在指定一台主机是，可以使用host关键词；如果要指定任意主机，可以使用any关键词

1. 扩展ACL

按照协议类型、源P地址、目的P地址、源端口号、目的端口号对过往的数据包进行控制。添加所用命令为：

Access-list ListNum {permit|deny} Protocol SrcIPAddr SrcPort DesPort DesPort

其中，ListNum为ACL的列表号，其取指范围为101~199，相同ListNum的规则属于同一个ACL，其先后顺序按照加入的先后顺序定。

匹配成功后，网络设备采取允许通过或丢弃动作。

Protocol表示该条规则使用的协议类型，可以是IP，ICMP，TCP，UDP等。

SRCIPAddr表示源IP地址范围，若未连续多个IP地址，则可以采用“起始IP地址 通配符”的方式定义；若只有一个IP地址，可以采用“host IP地址”的方式；若表示任意主机，可以使用any关键词。DesIPAddr表示目的IP地址范围，指定方式与SrcIPAddr相同

SrcPort指定源TCP或UDP端口范围，可以使用“操作符 端口号”的方式，其中“eq 端口号”用以指定一个具体端口，“gt 端口号”用以指定大于某个数值的所有端口，“lt 端口号”用以指定小于某个数值的所有端口。DesPort指定目的TCP或UDP端口范围，指定方式与SrcPort指定方式相同

1. 绑定ACP至端口

一个ACL 的规则添加完成后，需要通知网络设备在哪个接口的哪个方向上应用该规则，需要在端口配置模式下，使用命令

Ip access-group ListNum {in|out}

其中，ListNum表示需要绑定的ACL，in表示在这个接口的入站方向应用该ACL，out表示在这个接口的出站方向应用该ACL

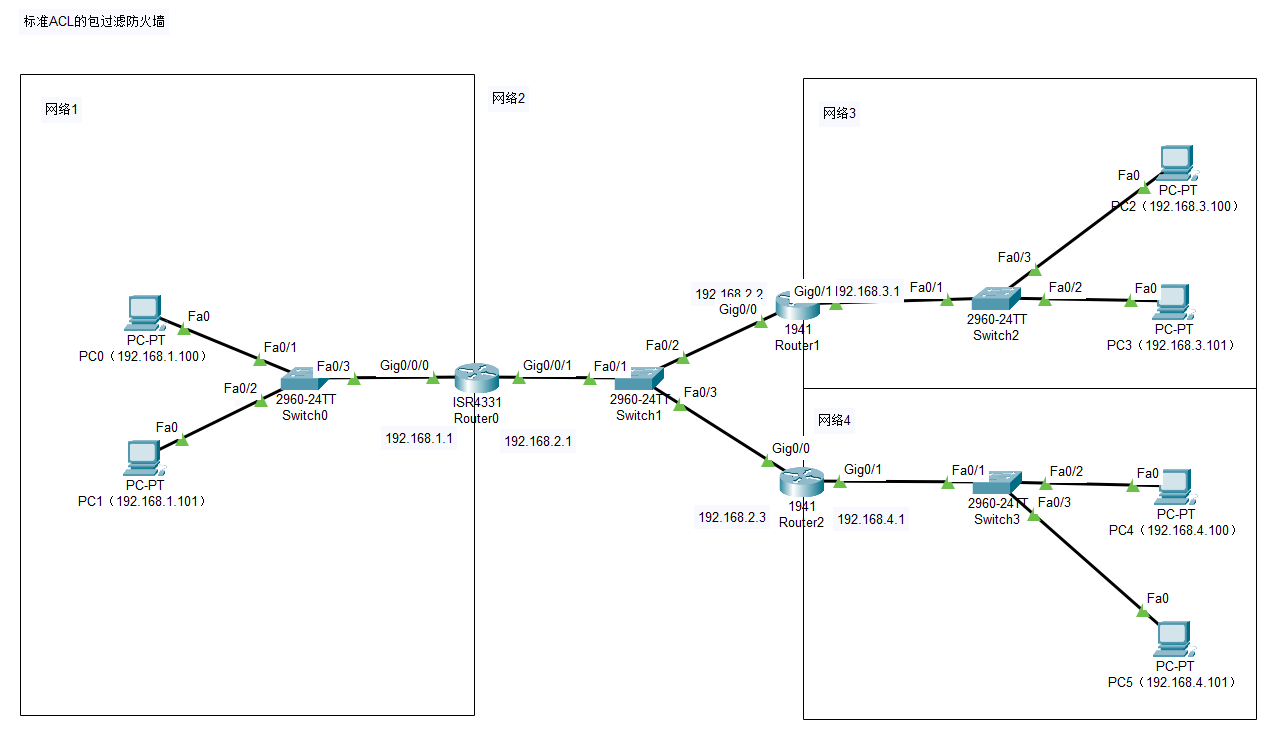
1. 删除ACL

删除ACL可以使用命令

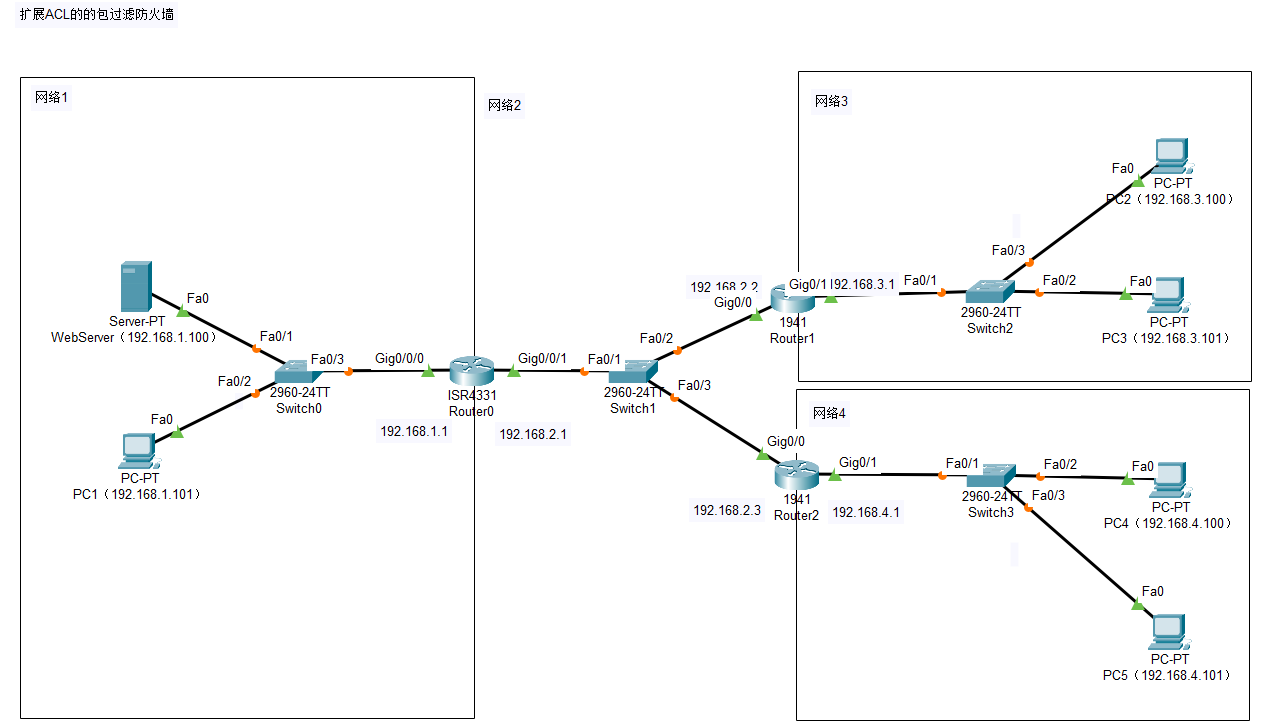
No access-list ListNum

应用该命令后将删除指定的整个ACL，不能删除ACL中的某条特定规则

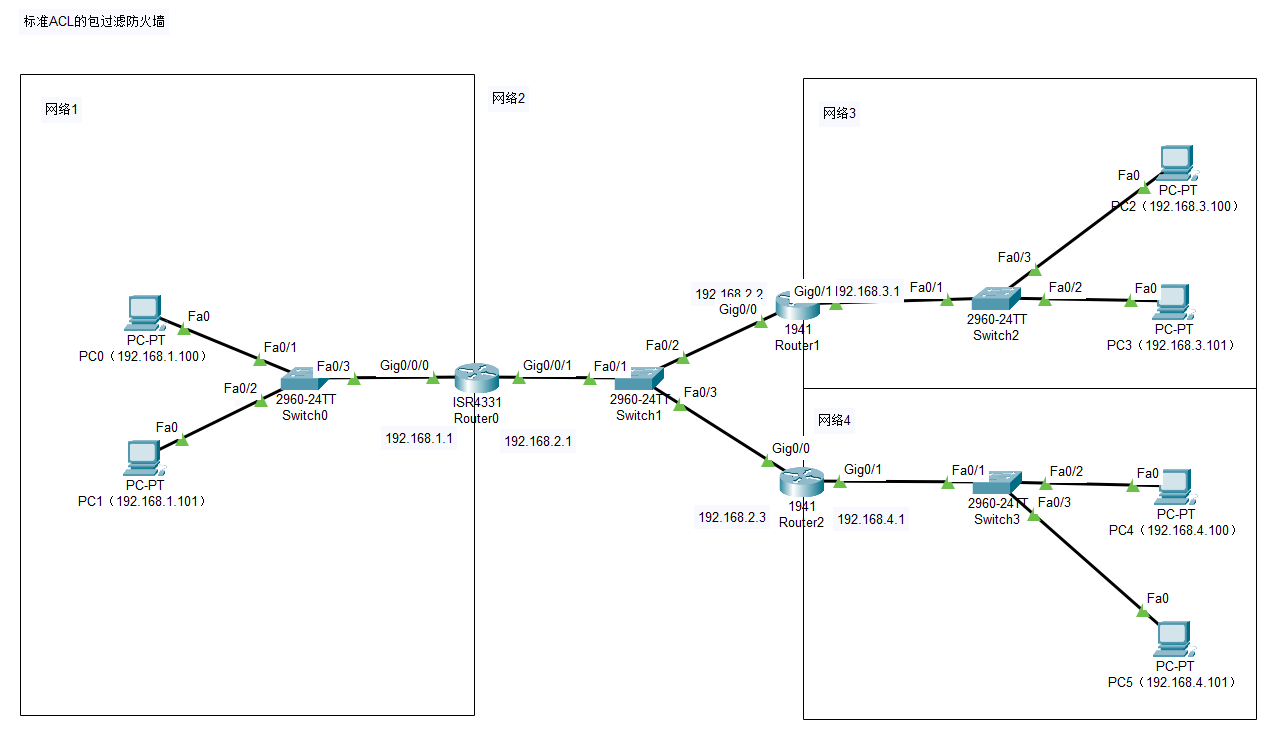
1. 标准ACL配置实验网络拓扑结构图



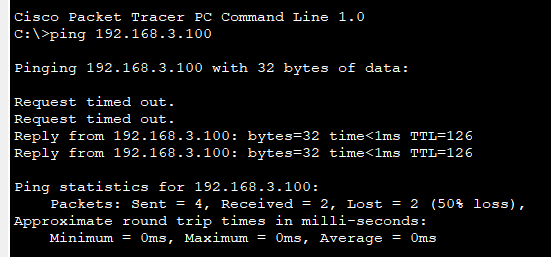
1. 扩展ACL配置实验拓扑结构图



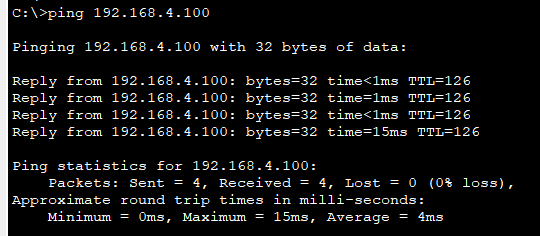
1. **实验过程**
2. 标准访问控制列表实验
3. 按照如下拓扑结构配置主机IP地址、路由器IP地址、路由器的路由表，使得不同网络中的主机能够相互访问



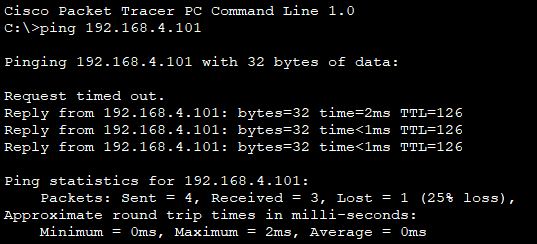
网络1与网络2主机通信：使用主机1 ping 主机2



网络1与网络3主机通信：使用主机1 ping 主机4



网络2与网络3主机通信：使用主机3 ping 主机5

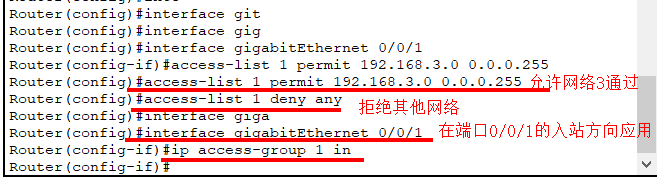


因此，不同网络的主机间能相互通信。

1. 本实验配置为对于网络1中的主机，只允许网络3中的主机访问，不允许其他网络中的主机的访问。

因此对路由器0的gig 0/0/1端口的入站方向应用ACL，包含两条规则：只允许网络3（192.168.3.0/24）中的主机对网络1（192.168.1.0/24）中的主机进行访问，拒绝其他所有网络的数据报送来的数据。

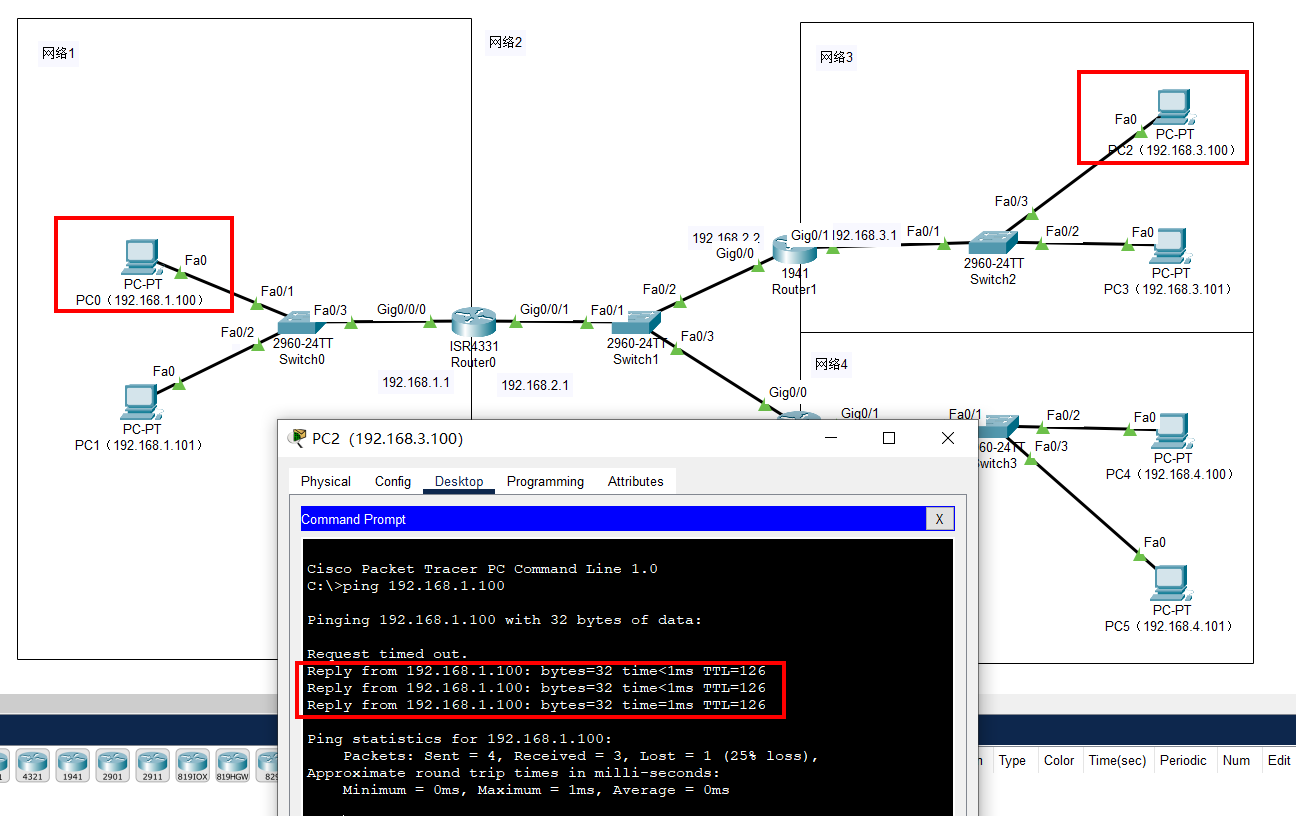
配置方式如下



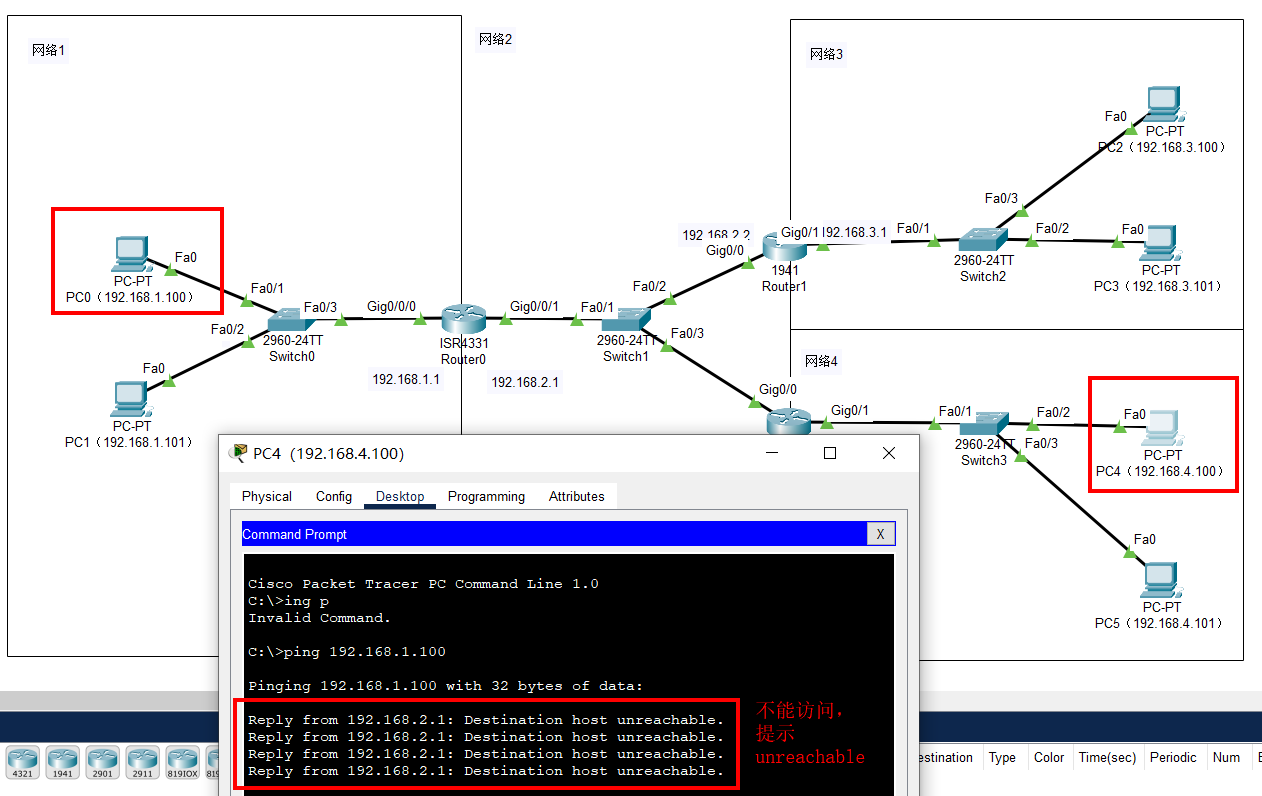
这里，拒绝其他网络的设置是默认的，因此也可以不主动配置该条命令

1. 测试包过滤防火墙

使用网络3中的主机2 ping 网络1中的主机0，能够访问

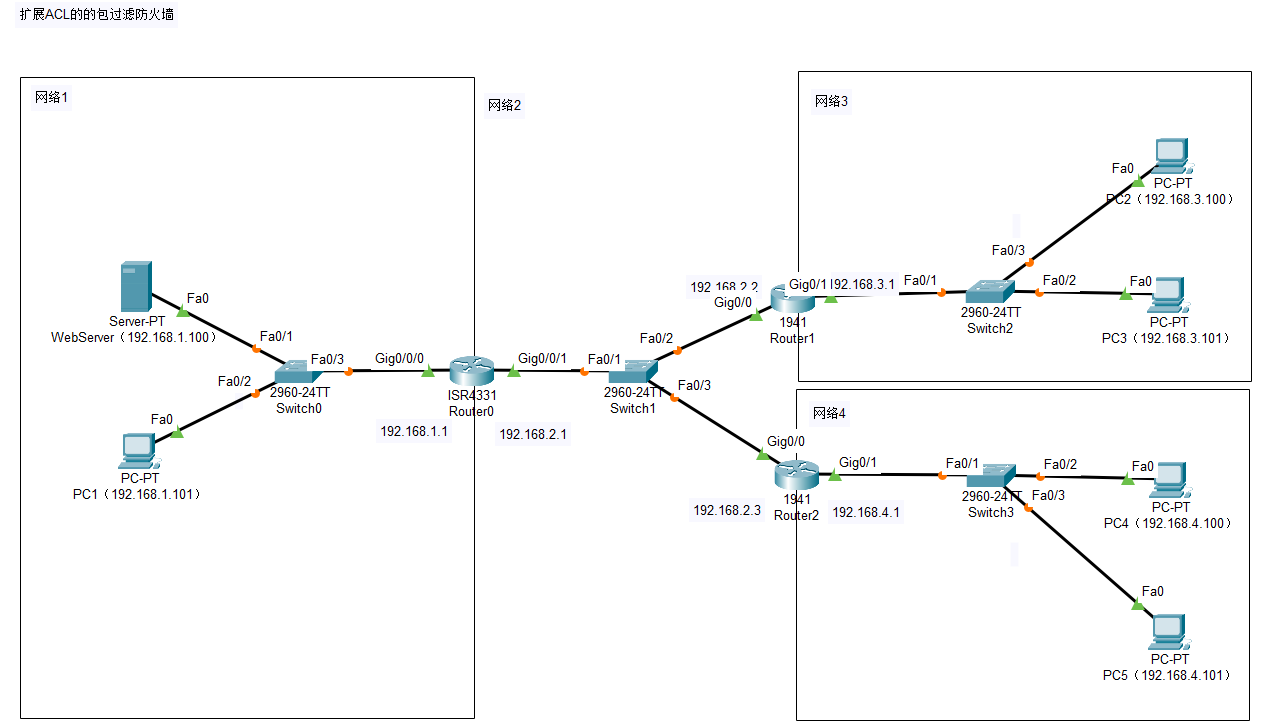


使用网络4中的主机4 ping 网络1中的主机0，不能访问，提示unreachable



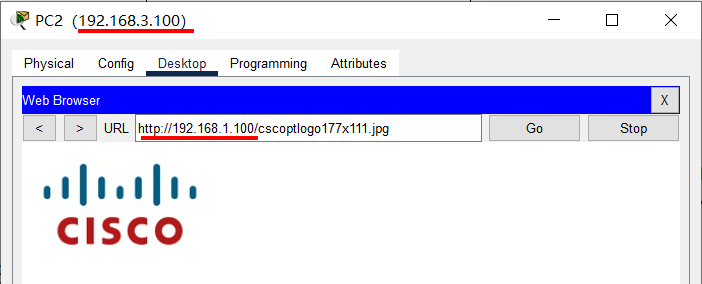
因此，使用标准ACL包过滤防火墙成功

1. 扩展访问控制列表实验
2. 与标准ACL类似，按如下拓扑结构配置IP地址、路由表，使不同网络中的主机能互相访问



不同网络间的访问类似标准ACL中的方式进行验证，不做赘述。

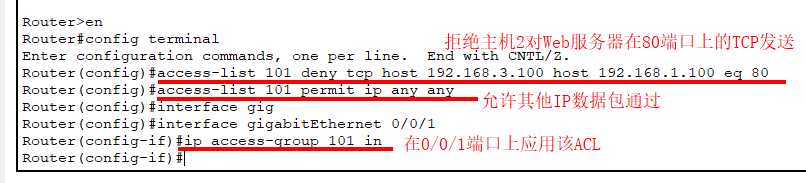
开启Web服务器的HTTP服务，通过网络3中的主机2访问成功



1. 本实验配置为，不允许网络3中的主机2对Web服务器进行Web请求

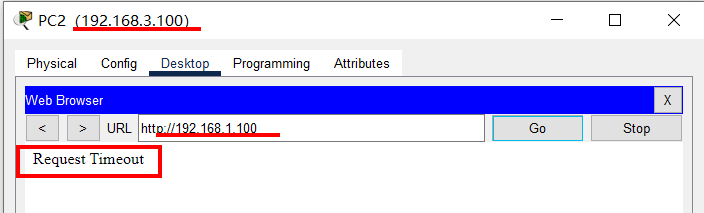
因此对路由器0的gig 0/0/1端口的入站方向应用ACL，包含两条规则：抛弃网络3中的主机2（192.168.3.100）送往网络1中Web服务器（192.168.1.100）的TCP数据包，允许其他网络中的TCP数据包送往Web服务器。

配置如下

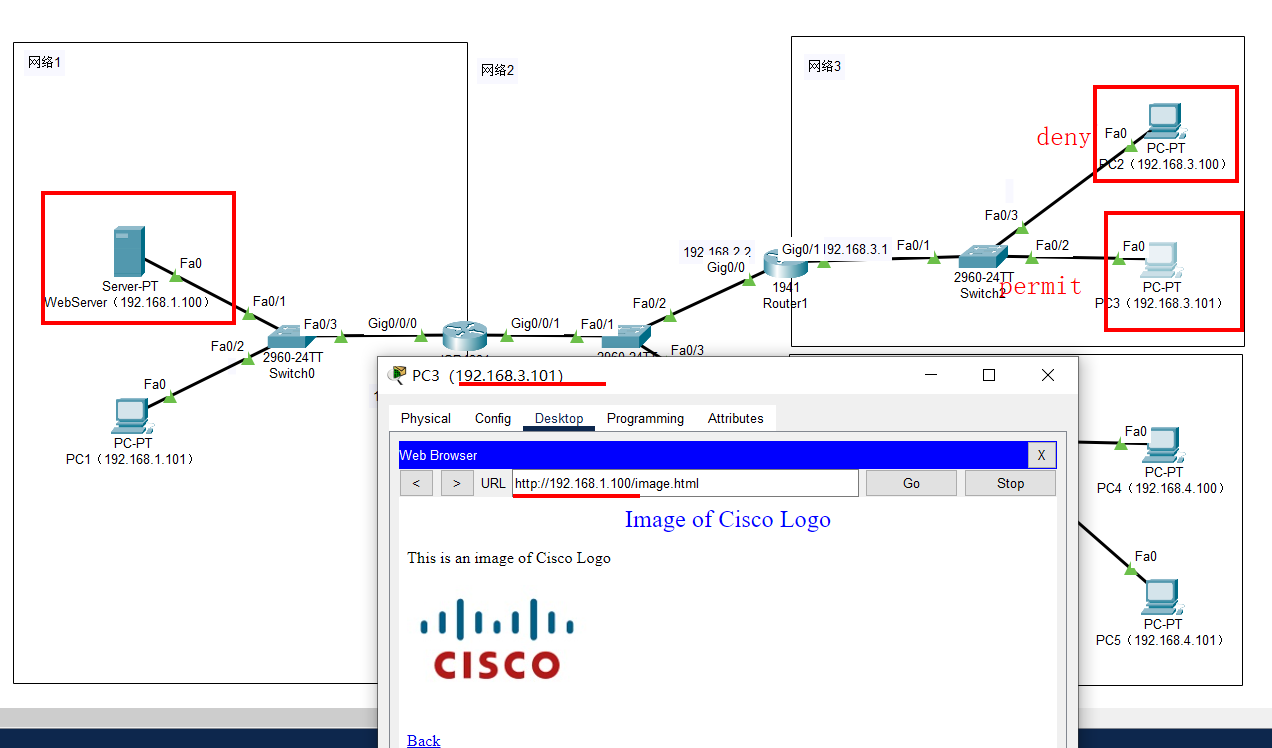


1. 包过滤防火墙测试

使用被拒绝的主机2访问Web服务器的Web服务时，提示超时



而使用同一网络下的主机3访问Web服务器时，可以正常进行Web服务的交互



至此，基于扩展ACL的包过滤防火墙配置成功

1. **特殊现象分析**
2. 在扩展ACL实验中，当关闭程序再次打开后，对于主机二之外的其他主机，第一次向Web服务器提起Web请求时，出现request timeout情况

原因为：第一次提起Web请求未成功使用ARP协议对IP地址进行解析。第二次提起Web请求后，建立了ARP协议和IP地址的对应关系，因此可以正常访问