《信息安全及实践》课程实验报告

学院 信息学院 专业 计算机科学与技术 年级 2020级

姓名 黄珀芝 学号 20201050331

实验时间 2022 年 11 月 5 日

实验名称 标准分组过滤器实验、扩展分组过滤器实验

实验成绩

标准分组过滤器实验

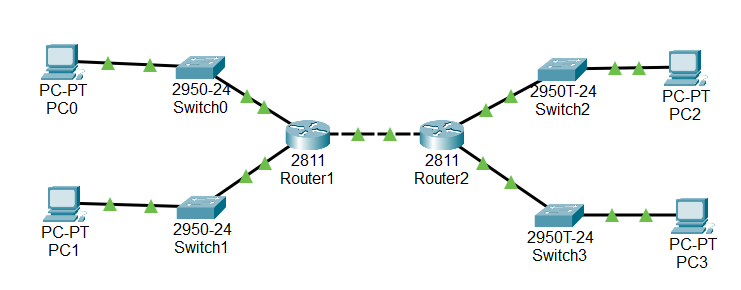
一、实验目的

(1)验证标准分组过波器过IP分组的原理和过程

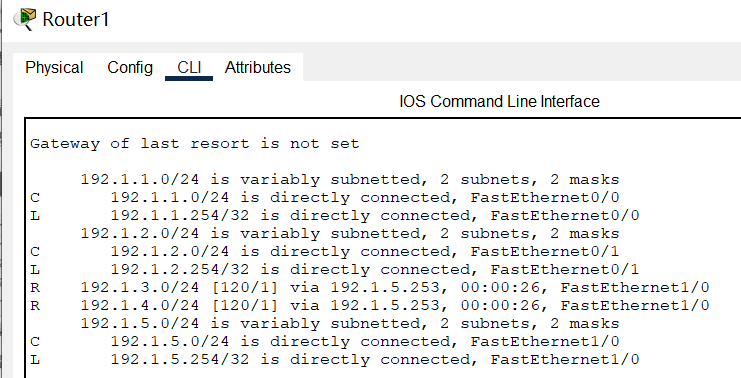
(2)验证路由器标准分组过器的配置过程

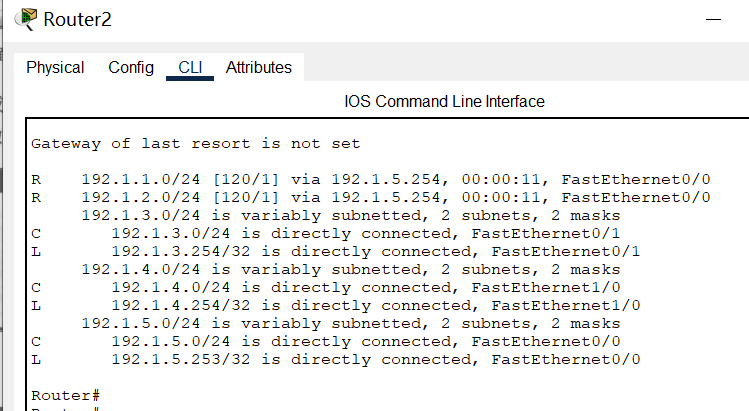
(3)验证标准分组过器防御源IP地址欺攻击的原理和过程

1. 实验步骤(含程序清单)
2. 完成设备放置和连接后的逻辑工作区。



（2）完成路由器各个接口IP地址和子网掩碍配置过程,完成路由器RIP配置过程。完成上述配置过程后,路由器 Routerl和 Router2的路由表分别如图所示。

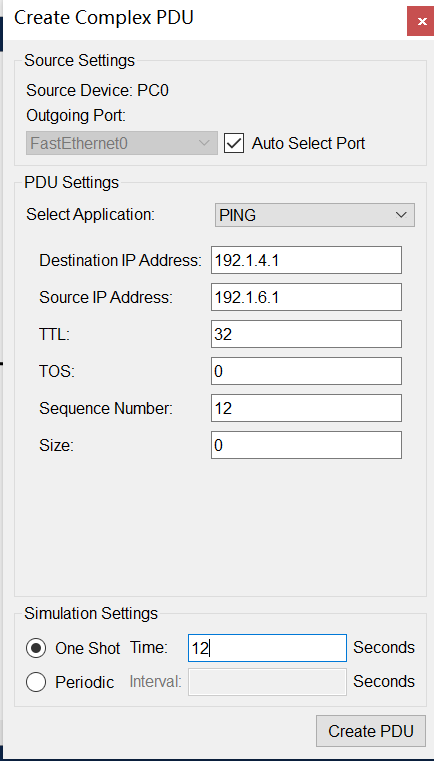


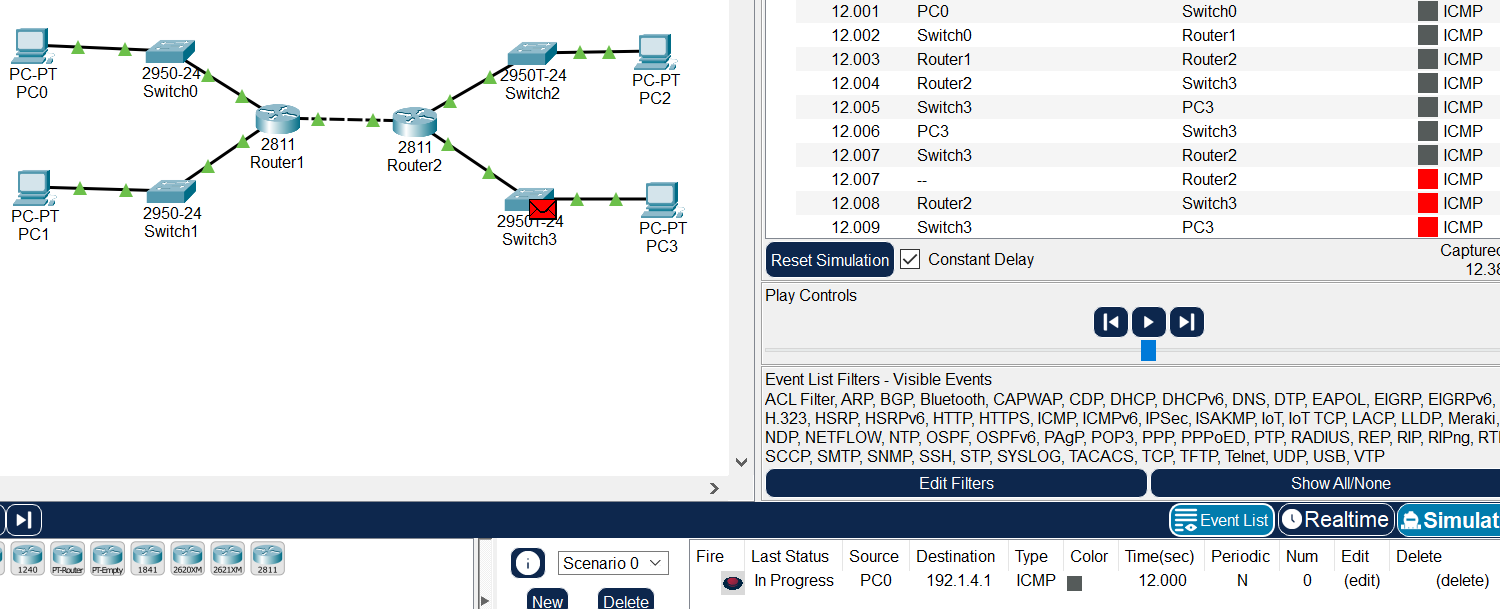


（3）完成各个终端的网络信息配置，此过程很简单，按照所给图配置，不再给出过程。

（4）切换模拟操作模式，在PC0上创建ICMP报文，封装该ICMP报文的IP分组的圆目的和目的地。目的IP地址是PC3的1P地址192.1.4.1,源IP地址是伪造的IP地址192.1.6.1(PC0的IP地址是192.1.1.1)启动该IP分组PCO至PC3的传输过程,路由器 Routerl接口 FastEthernet0/0输入方向允许输入该IP分组,

Routerl1正常转发该IP分组。



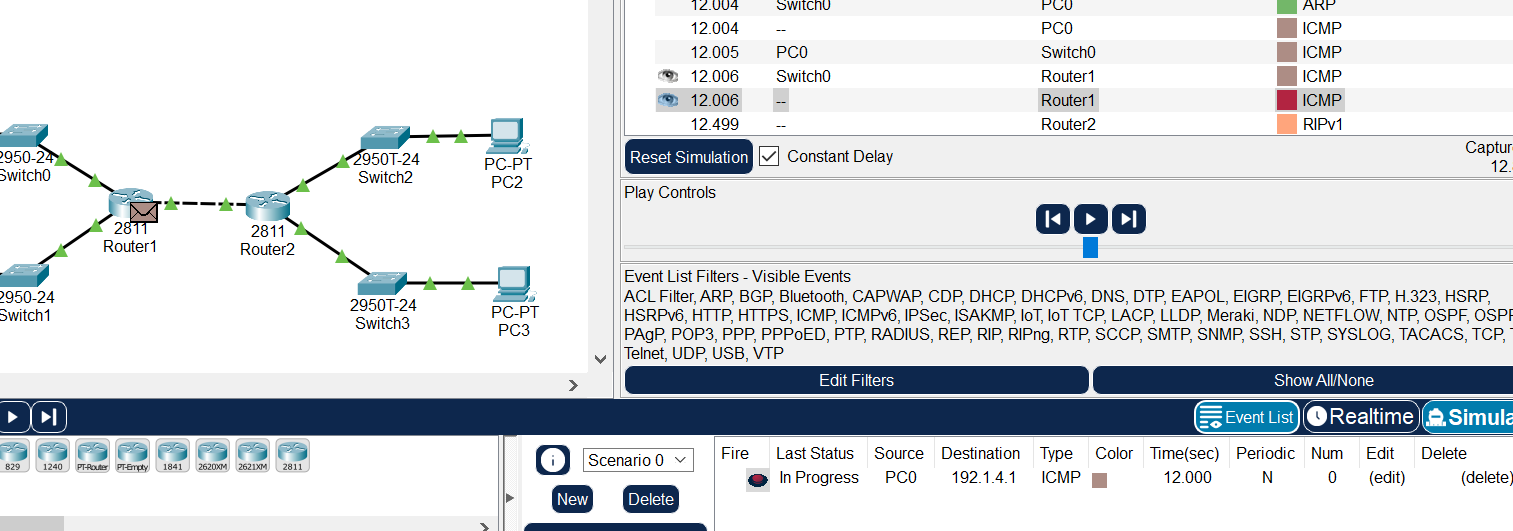


Router1正常转发伪造源ip地址的ip分组

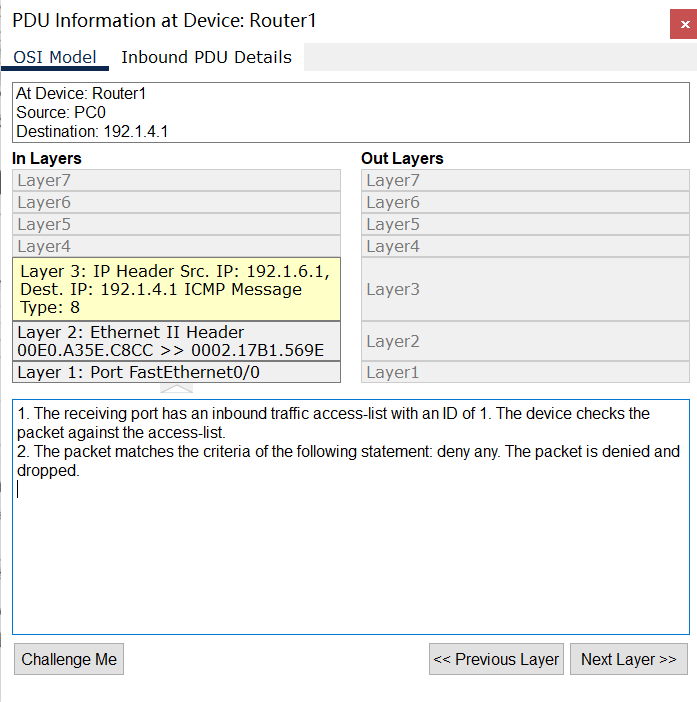
1. 切换到实时操作模式,在CLI(命令行接口）配置方式下,完成路由器 Routerl标准分组过滤器配置过程,并将其作用到接口 FastEthernet0/0输入方向使路由器 Routerl1只允许继续转发源IP地址属于CIDR地址块192.1.1.0/24的IP分组。

三、实验结果及分析

模拟操作模式,在PCO上创建mP报文,封装该ICMP报文的IP分组的源和目的IP地址如图8.6所示启动该IP分组PCO至PC3的传输过程,路由器Routerl接口FastEthernet0/0输入方向丢弃该IP分组,如图所示。丢弃原因如图所示,该IP分组符合属于编号为1的标准分组过滤器,且动作是deny、条件是any的规则。



Router1丢弃伪造源ip地址的ip分组



扩展分组过滤器实验

1. 实验目的

(1)验证扩展分组过滤器的配置过程。

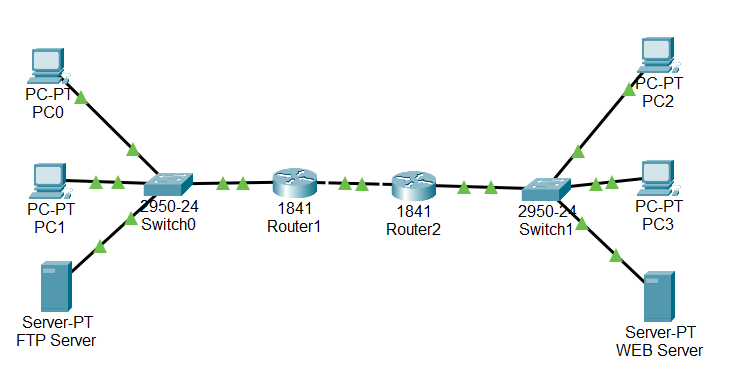
(2)验证扩展分组过滤器实现访问控制策略的过程。

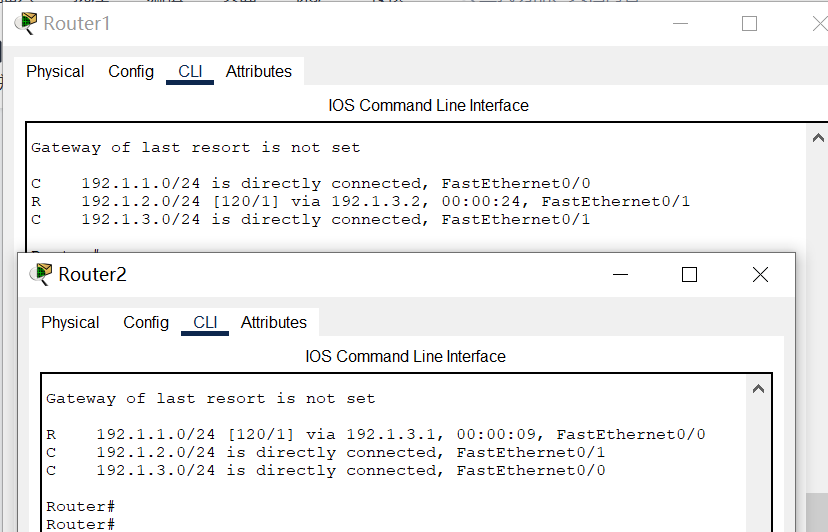
(3)验证过滤规则设置原则和方法。

(4)验证过滤规则作用过程。

1. 实验步骤(含程序清单)

（1）完成设备放置和连接后的逻辑工作区界面如图所示,完成路由器 Routerl和 Router2各个接口的配置过程,完成各台路由器RIP配置过程。。完成各个终端和服务器网络信息配置过程,验证终端和终端之间、终端和服务器之间、服务器和服务器之间的连通性。

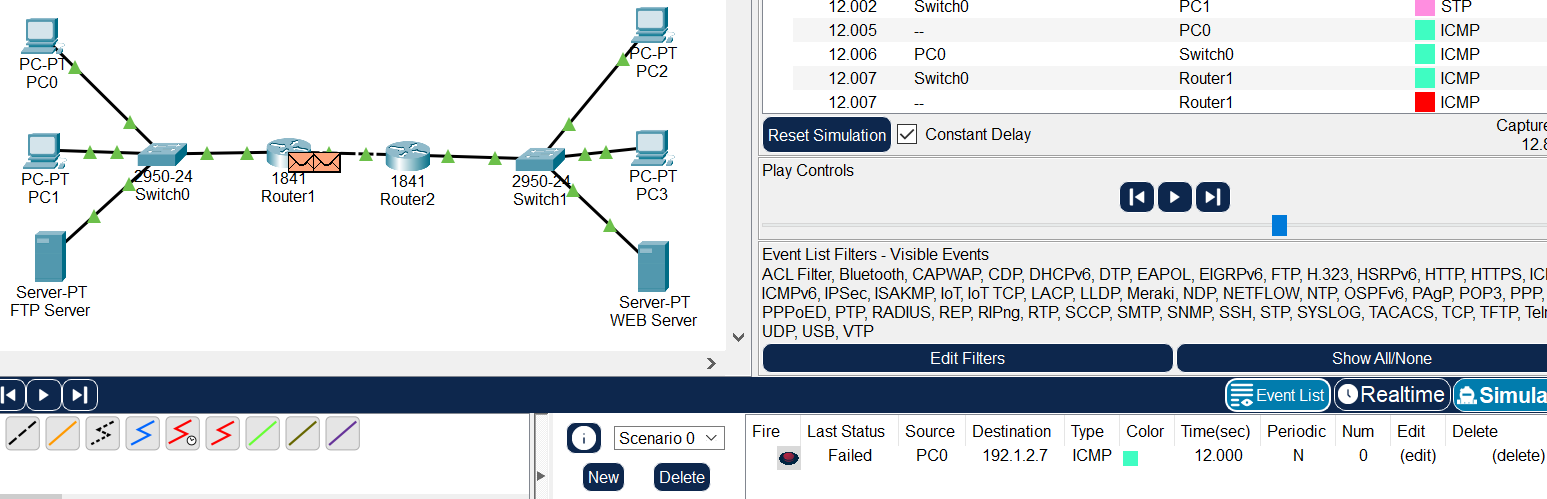


完成上述配置过程后的路由器 Routerl和 Router22路由表分别如图所示

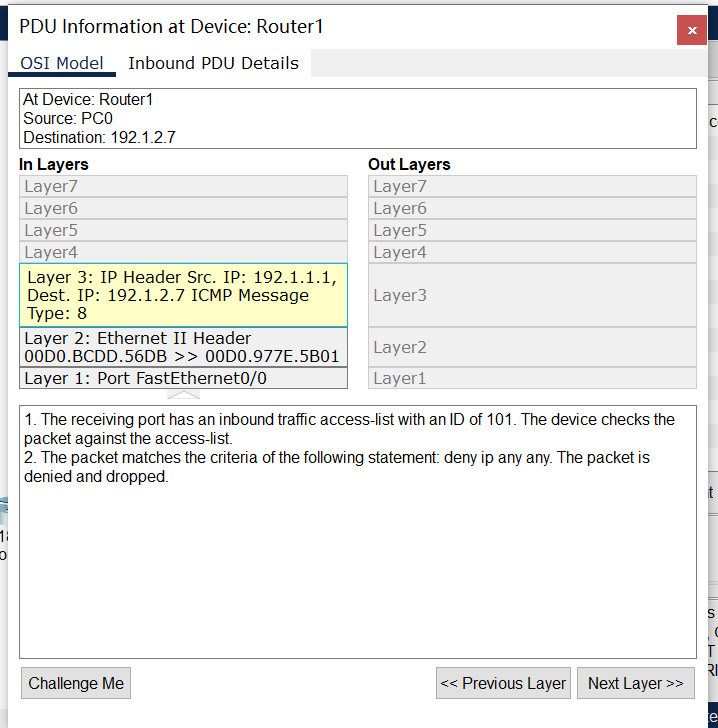
1. 在CLI(命令行接口)配置方式下,完成路由器 Routerl编号为101的扩展分组过滤器的配置过程,并将其作用到路由器接口 FastEthernet0/0输入方向完成路由器 Router2编号为101的扩展分组过滤器的配置过程,并将其作用到路由器接口FastEthernet0/0输入方向。

（3）验证不同网络的终端之间和服务器之间不能ping通PCo发送给Web服务器

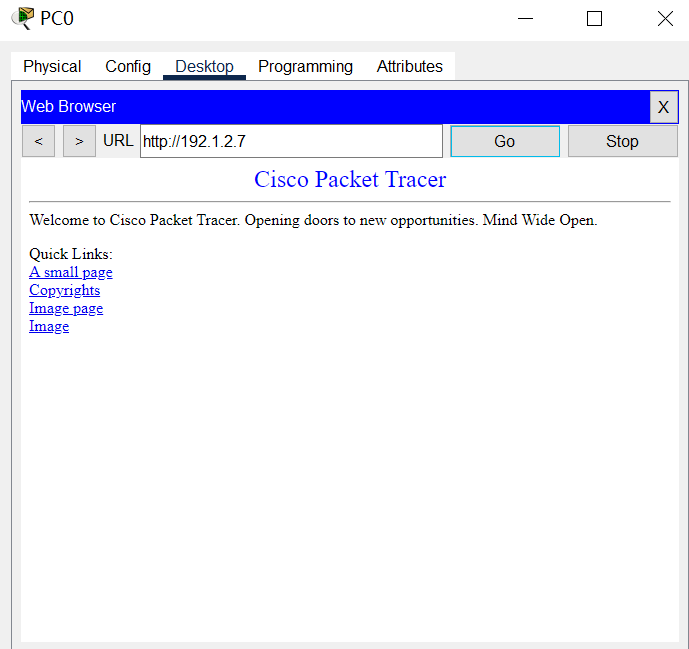
的ICMP报文,封装成IP分组后沿PCO至Web服务器的IP传输路径传输,到达路由器Routerl接口 Fast Etherneto/0时,被路由器 Routerl丢弃。



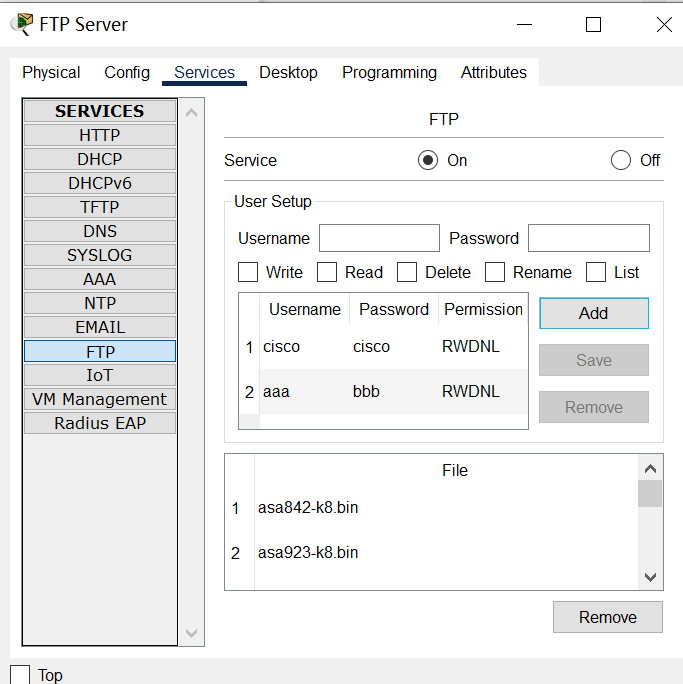
丢弃原因如图所示,被编号为101的扩展分组过滤器丢弃。



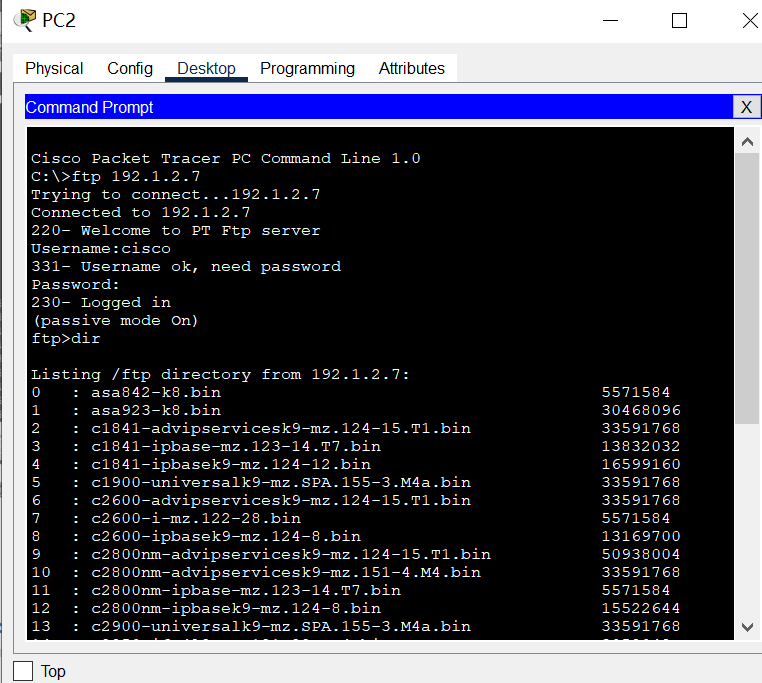
（4）允许PC0通过浏览器访问web服务器，如图所示。



FTP服务器配置页面创建两个用户名分别为aaa和cisco的授权用户，访问权限是全部功能。



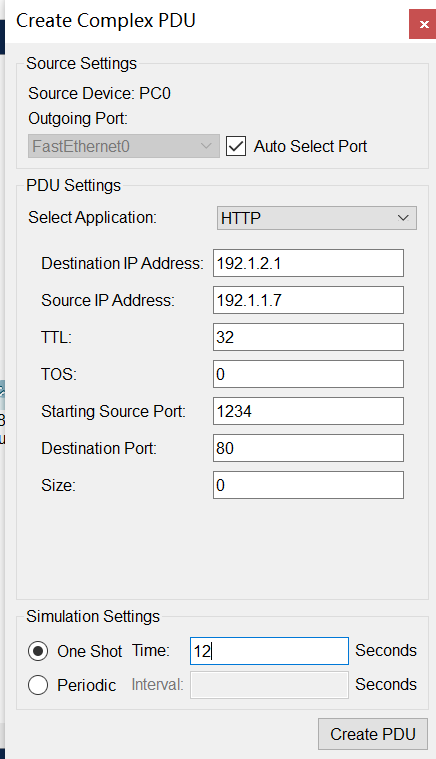
PC2访问FTP服务器。

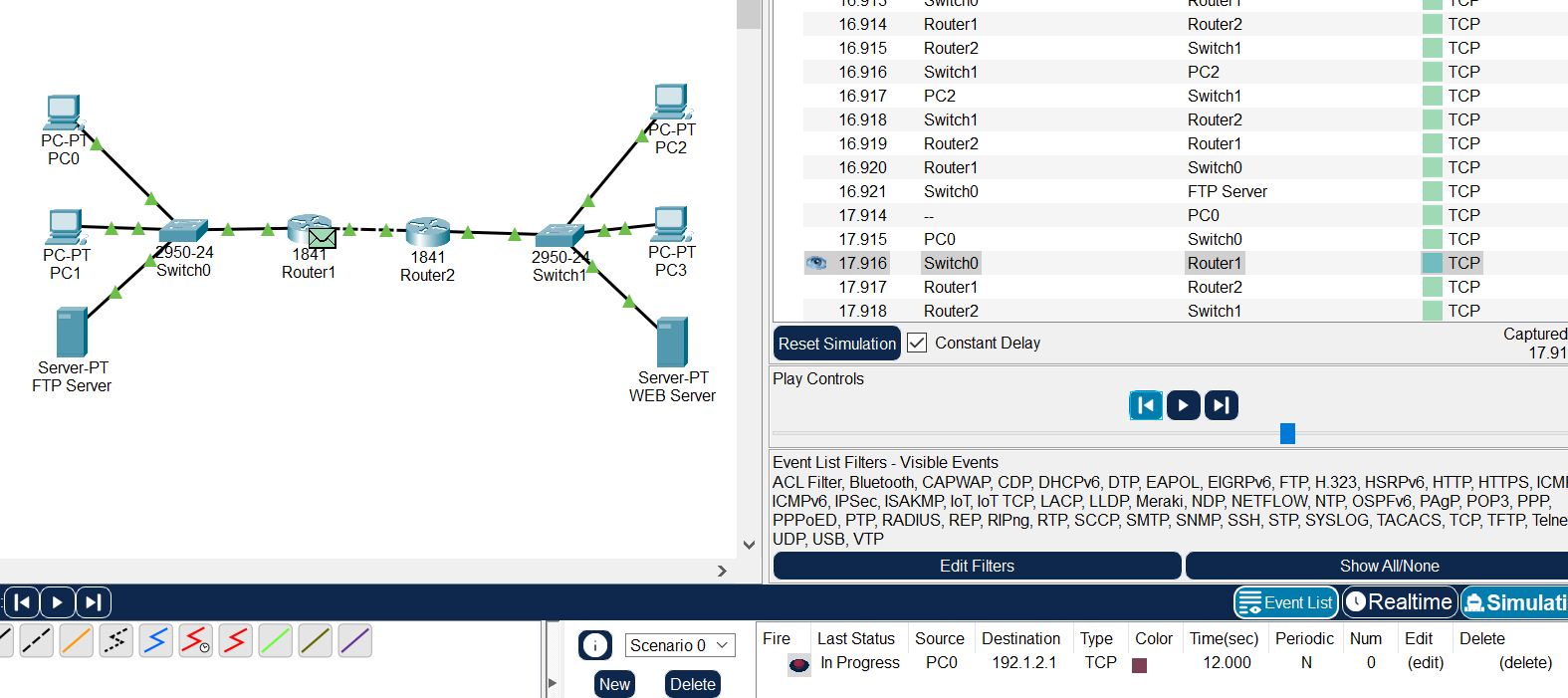


三、实验结果及分析

如果要求实现只允许PC2发起访问FT服务器的访问控制策略,应该实施以下

信息交换控制机制,必须在PC2向FTP服务器发送了FP请求消息后,才能由FTP服务器向PC2发送对应的FTP响应消息为此,在作用到路由器 Routerl接口。 FastEthernet0/0输入方向的编号为101的扩展分组过滤器中设置了规则②和③,设置这两个规则的目的是只允许FTP服务器向PC2发送FTP响应消息,但扩展分组过滤器中的规则②和③并不能实现这一控制功能。TCP报文如图8.19所示,该TCP报文并不是FTP服务器发送给PC2的FTP响应消息,但与规则③匹配,因此被允许输入路由器Routerl接口 Fast Ethernet0/0这也说明,用扩展分组过滤器实施精确控制是有困难的。



 破坏访问控制策略的TCP报文