计算机网络实验实验报告

学院（系）名称：信息学院

姓名	高星杰	**学号**	2021307220712	**专业**	计算机科学与技术
班级	21 级 2 班	**实验项目**	访问控制列表的配置与应用		
课程名称		计算机网络实验		**课程代码**	3103009336
实验时间		2023 年 1 月 4 日		**实验地点**	逸夫楼 C207

考核内容	目的和原理 40	内容及过程分析 30	实验方案设计 10	实验结果（结论正确性以及分析合理性）20	**成绩**	
各项得分						
考核标准	○原理明确 ○原理较明确 ○原理不明确	○分析清晰 ○分析较清晰 ○分析不清晰	○设计可行 ○设计基本可行 ○设计不可行	○结论正确，分析合理 ○结论正确，分析不充分 ○结论不正确，分析不合理	**教师签字：**	

1. 实验目的：

1.1 理解访问控制列表的原理

1.2 掌握访问控制列表的配置

1.3 掌握访问控制列表在网络中的应用

2. 实验原理：

经过之前的实验我们已经明白了路由是如何配置的及如何实现的，但是我们又可以发现一个问题在一个复杂的网络环境中，如果我们对所有发送过来的数据进行转发那么很可能会导致自己的网络带宽被占用并且还会导致安全问题，所以我们要对要转发的数据进行控制——访问控制列表应运而生。

之前学习的都是让网络如何连通，今天是在网络连通环境基础上来进行相应的限制

2.1 什么是访问控制列表？

访问控制列表（Access Control List，ACL）是**一种网络安全机制**，用于控制和管理网络设备（如路由器、交换机、防火墙）上的流量传输和访问权限。

访问控制列表可以被看作是一张“清单”，它控制着网络设备上的流量和访问权限。就像我们在家里有一把钥匙可以锁门一样，ACL 可以帮助我们在网络中管理谁能访问哪些资源。

想象一下，你有一个家庭网络，有多台电脑、手机和其他设备连接在一起。你希望某些设备可以访问互联网，但不希望其他设备有这个权限。这时，你可以设置一个 ACL 来控制网络访问。ACL 的工作方式类似于一个安全门禁系统。每个设备进入你的网络时，就会被检查 ACL 的规则。这些规则定义了

哪些设备被允许通过，哪些设备被禁止。规则可能基于设备的 IP 地址、端口号或其他标识来进行匹配。

假设你设置了一个 ACL 规则，只允许你的笔记本电脑通过网络访问。当你的笔记本电脑试图连接到网络时，网络设备会检查 ACL 规则，发现匹配的规则允许笔记本电脑通过，于是它可以顺利上网。但如果其他设备，比如陌生人的手机，尝试连接到网络，ACL 规则会发现没有匹配的规则，因此它会被拒绝访问。

当网络设备收到流量时，它会按照配置的 ACL 规则逐条进行匹配，并根据匹配结果执行相应的动作。如果流量匹配了允许通过的规则，设备将允许该流量通过；如果匹配了拒绝的规则，设备将阻止该流量；如果没有匹配任何规则，设备可能会根据默认配置执行动作。

ACL 还可以限制特定类型的流量。举个例子，你可能希望阻止某些应用程序，比如游戏或流媒体服务，占用太多网络带宽。通过设置 ACL 规则，你可以限制这些应用程序的访问，以确保网络资源被合理利用。

2.2 通过几个问题更加深入理解访问控制列表

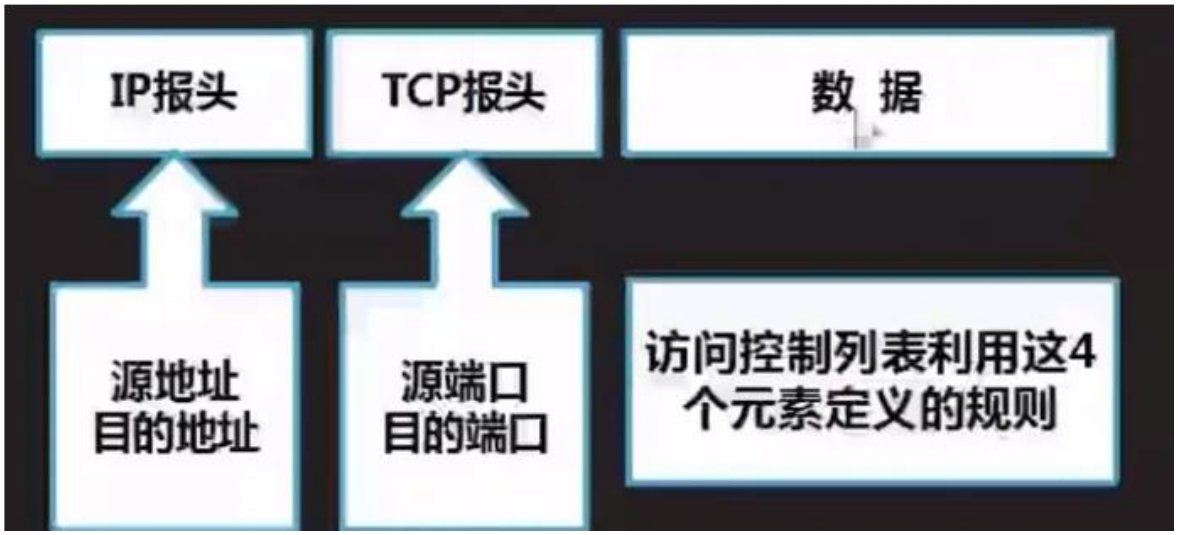
为什么叫访问控制列表？虽然网络是连通的，但是不允许通信的主机就不能访问，或者说允许访问的是哪个主机，以及访问主机里的什么服务可以做更加细化的限制所以叫访问控制

网络当中访问控制的对象是谁？是某个节点当中的主机。

如何标识和区分控制的对象呢？得用到 IP 地址。哪个 IP 地址的主机可以访问，或者说可以访问的哪个 IP 地址的主机以及该主机当中的具体哪个服务，因此有关于 ACL 访问控制可以对第几层信息进行过滤？网络层也就是第三层，要看地址是被允许的还是被拒绝的。

控制访问的是主机以及主机里的服务，那么服务用端口号来标识。

因此 ACL 访问控制不仅对三层信息（也就是网络层信息）进行过滤，还可以对四层信息进行过滤，要读取 IP 地址里的数据包和端口号，再根据预告定义好的规则，对数据包做一个过滤。



2.3 访问控制列表解决了什么问题？

访问控制列表（Access Control List，ACL）解决了以下几个问题：

控制网络访问权限：ACL 允许网络管理员限制特定用户、设备或 IP 地址对网络资源的访问。通过 ACL，可以明确规定谁能够访问网络资源，从而确保只有授权的用户或设备能够使用特定的网络服务或访问敏感数据。

管理流量传输：ACL 可以控制特定类型的流量在网络中的传输。管理员可以配置 ACL 规则，以阻止或限制某些类型的流量，如恶意流量、垃圾邮件或特定应用程序的流量。这有助于减轻网络拥塞、提高网络性能，并增强网络的安全性。

增强网络安全性：ACL 可以帮助阻止未经授权的访问和网络攻击。通过配置 ACL 规则，管理员可以限制来自特定 IP 地址或 IP 地址范围的流量，阻止潜在的入侵者进入网络。ACL 还可以用于阻止特定协议或端口的流量，以防止特定类型的攻击。

实现资源隔离：ACL 可以用于实现不同用户、设备或部门之间的资源隔离。通过配置 ACL 规则，可以限制某些用户或设备对特定资源的访问权限，确保数据的保密性和隐私性。ACL 还可以用于实现虚拟局域网（VLAN）之间的隔离，确保不同部门或用户组之间的数据隔离。

时间段访问控制：ACL 允许管理员根据特定的时间段来控制访问权限。这意味着可以配置 ACL 规则，仅在特定时间段内允许或拒绝特定 IP 地址或用户对资源的访问。这对于实施时间限制的访问策略是很有用的，例如只允许在工作时间内访问某些资源

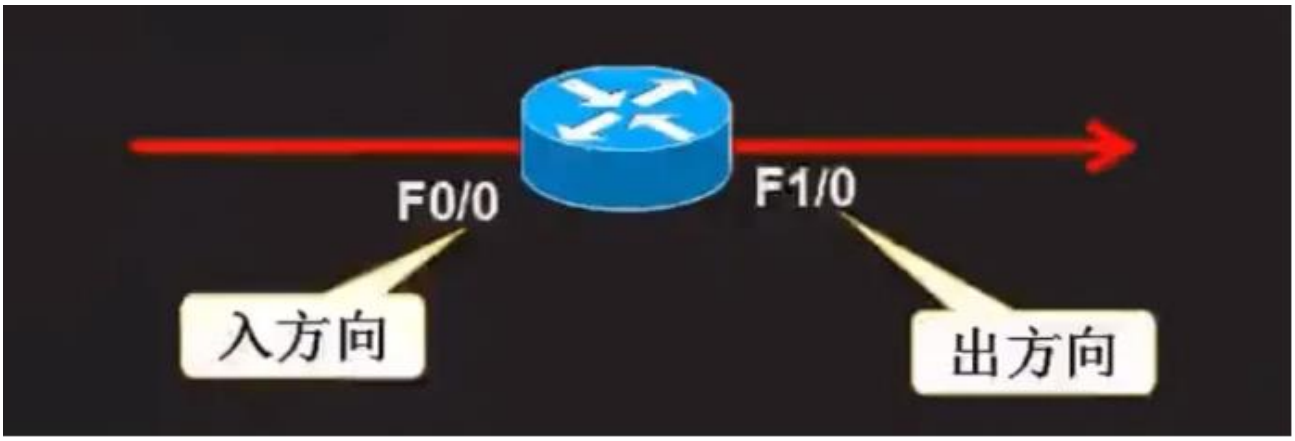
2.4 访问控制列表的工作过程是什么？

首先我们明白访问控制列表在接口应用的方向

-出：已经过路由器的处理，正离开路由器接口的数据包

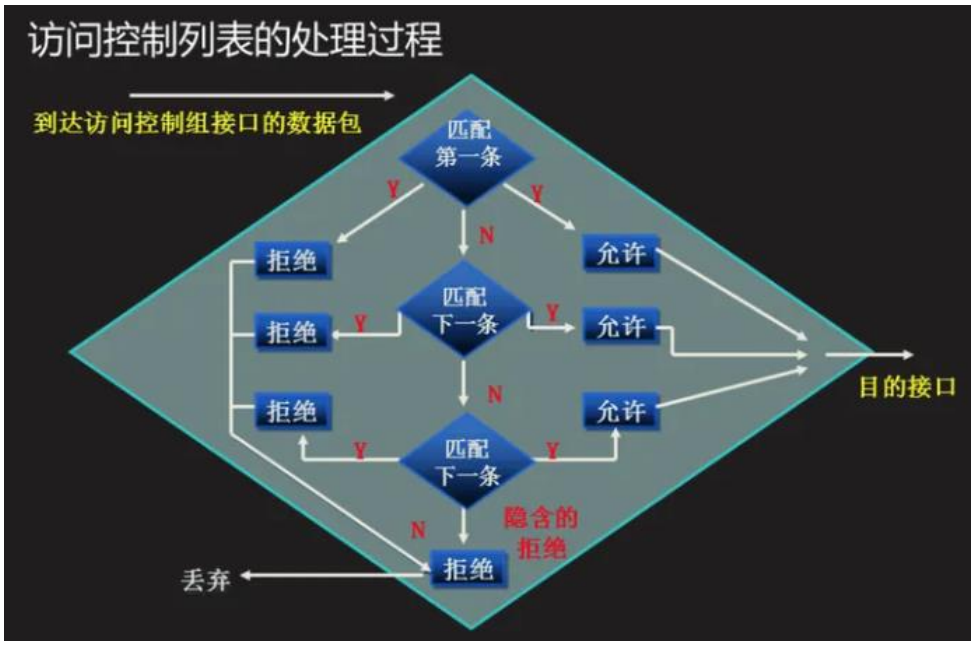
-入：已经到达路由器接口的数据包，将被路由器处理

列表应用到接口的方向与数据方向有关。



访问控制列表处理语句有一个严格的匹配顺序，拒绝和允许都不匹配才会允许读下一条

访问控制列表的处理过程：如果匹配第一条规则，则不再往下检查，路由器将决定该数据包允许通过或拒绝通过。如果不匹配第一条规则，则依次往下检查直到有任何一条规则匹配。如果最后没有任何一条规则匹配，则路由器根据默认的规则将丢弃该数据包。



2.5 访问控制列表有哪几种？

访问控制列表的类型：

1、标准访问控制列表

-基于源 IP 地址过滤数据包

-标准访问控制列表的访问控制列表号是 1~99

（基于源 IP，也就是说只要源匹配则通过或者拒绝）

2、扩展访问控制列表

-基于源 IP 地址、目的 IP 地址、指定协议、端口来过滤数据包

-扩展访问控制列表的访问控制列表号是 100~199

（不仅要源 IP 还要看你访问谁，也就是目的 IP，不仅访问源目标以及目标里边的服务，服务对应的有协议和端口）

区分标准访问控制和扩展访问控制要根据列表号来区分。

3、命名访问控制列表

-命名访问控制列表允许在标准和扩展访问控制列表中使用名称代替表号。

（也就是说命名既有标准的命名又有扩展的命名）

3. 实验分析：

通过对原理的了解，我们可以大致的清楚了访问控制列表是干什么的了，那么我们该如何配置一个访问控制列表呢？

3.1 如何配置访问控制列表？

我们需要先决定要使用哪种访问控制，如果比较简单的不需要判断端口，我们可以直接使用标准的访问控制，而对于需要判断端口我们就需要的使用的扩展的访问列表。

其次我们需要确定需要筛选的 ip 地址（可能包括端口）。其次如果我们要限制的是出口和入口那么我们需要知道源地址和目的地址。

然后就是确定需要配置访问控制的接口。

3.2 outbound 和 inbound 有什么区别？

outbound:指规则应用到接口的输出或者离开方向。过滤或检查从接口发送出去的包。

例如,通过交换机的 fa0/1 接口离开到外部网络的流量。

inbound:指规则应用到接口的输入或者进入方向。过滤或检查进入接口的包。

例如,通过交换机的 fa0/1 接口进入内部网络的流量。

区别在于：

outbound 过滤规则检查包的发送方向,即从交换机接口发送到外部的流量。

inbound 过滤规则检查包的接收方向,即从外部接收进入交换机接口的流量。

通常:

边界路由器 ACL 使用 inbound 命令,过滤外网进入内网的流量。

内部交换机 ACL 使用 outbound 命令,过滤内网主机发往外网的流量。

所以:

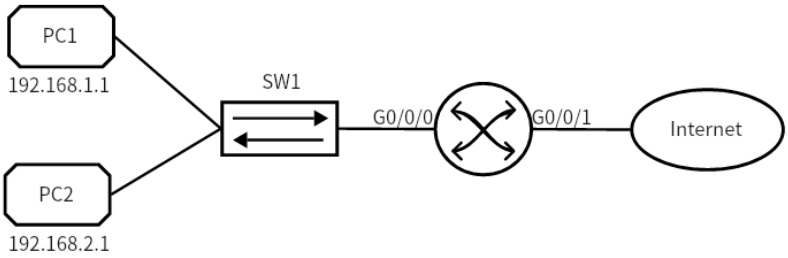
inbound 对应 ingress 方向,检查接口接收流量。

outbound 对应 egress 方向,检查接口发送流量。

两者根据过滤对象流量的方向不同而区分,共同实现对接口流量的分类和控制。正确区分和应用有助于 ACL 规则的 targeting。

4. 实验设计：

4.1 设计拓扑图



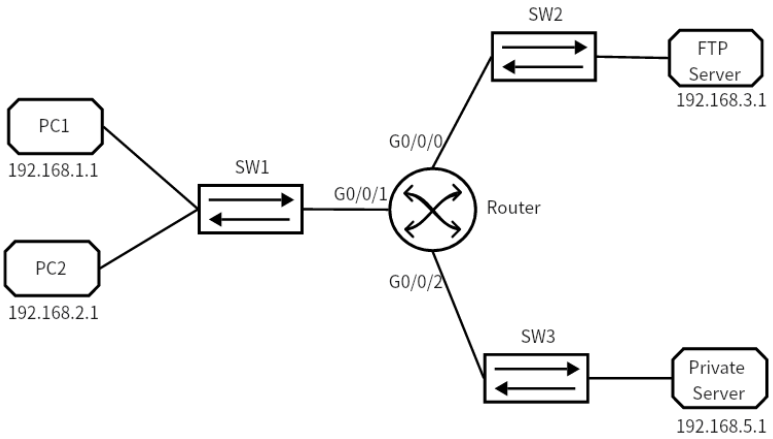
要求PC1禁止通过路由器访问Internet，而PC2可以通过路由器访问Internet

4.2 配置主机 IP 地址

4.3 连接主机与路由器的 console 口，配置基本访问控制列表

4.4 验证基本访问控制列表

4.5 设计高级 ACL 使用场景的拓扑图并且连线



要求PC1禁止通过路由器访问FTP文件服务器，而PC2禁止路由器访问私人服务器

4.6 配置新增的主机 IP 地址

4.7 配置高级访问控制列表

4.8 验证高级访问控制列表

5. 实验过程：

5.1 根据拓扑图搭建网络

首先根据拓扑图，搭建简单的单臂路由链路。搭建时，需注意交换机、路由器配置的端口号，并严格按照拓扑图进行搭建，方便后期测试工作的进行。

5.2 配置主机 IP 地址

根据拓扑图，为单臂路由的两台主机配置 IP 地址

主机 PC1 配置 IP 为 192.168.1.1；PC2 配置 IP 为 192.168.2.1

5.3 配置路由器的 ACL

① 首先设置访问控制列表 acl2000

```
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]acl 2000
[Huawei-acl-basic-2000]rule deny source 192.168.1.0 0.0.0.255
[Huawei-acl-basic-2000]interface Gi
[Huawei-acl-basic-2000]interface Gi
[Huawei-acl-basic-2000]quit
```

② 进入端口模式将访问控制列表应用在端口

```
[Huawei]interface GigabitEthernet 0/0/0
[Huawei-GigabitEthernet0/0/0]traffic-filter outbound acl 2000
                                                        ^
Error: Unrecognized command found at '^' position.
[Huawei-GigabitEthernet0/0/0]traffic-filter outbound acl 2000
[Huawei-GigabitEthernet0/0/0]traffic-filter outboun
[Huawei-GigabitEthernet0/0/0]traffic-filter outbound a
[Huawei-GigabitEthernet0/0/0]traffic-filter outbound acl 2000
[Huawei-GigabitEthernet0/0/0]display ac
```

5.4 验证基本访问控制列表

```
[Huawei-GigabitEthernet0/0/0]display traffic-filter applied-record
-------------------------------------------------------------
Interface                 Direction  AppliedRecord
-------------------------------------------------------------
GigabitEthernet0/0/0      outbound   acl 2000
-------------------------------------------------------------
```

5.5 根据高级 ACL 使用场景的拓扑图连线

首先根据拓扑图，搭建链路。搭建时，需注意交换机、路由器配置的端口号，并严格按照拓扑图进行搭建，方便后期测试工作的进行。

5.6 配置新增的主机 IP 地址

5.7 配置路由的高级访问控制列表

①首先设置高级访问控制列表

```
[Huawei-GigabitEthernet0/0/0]ac
[Huawei-GigabitEthernet0/0/0]acl 3000
[Huawei-acl-adv-3000]ru
[Huawei-acl-adv-3000]rule deny
[Huawei-acl-adv-3000]rule deny tc
[Huawei-acl-adv-3000]rule deny tcp s
[Huawei-acl-adv-3000]acl 3000y tcp source 192.168.1.0 0.0.0.255 de
[Huawei-acl-adv-3000]rule deny tcp source 192.168.1.0 0.0.0.255 destination-port
[Huawei-acl-adv-3000]
[Huawei-acl-adv-3000]
```

```
[Huawei-acl-adv-3000]rule deny tcp s
[Huawei-acl-adv-3000]rule deny tcp source 192.168.2.0 0.0.0.255 destination 172.16.10.2 0.0.0.0
[Huawei-acl-adv-3000]rule permi
[Huawei-acl-adv-3000]rule per
[Huawei-acl-adv-3000]rule permit ip
```

②进入端口模式将访问控制列表应用在端口

```
[Huawei]interface GigabitEthernet 0/0/1
[Huawei-GigabitEthernet0/0/1]tra
[Huawei-GigabitEthernet0/0/1]trace-
[Huawei-GigabitEthernet0/0/1]traffic-filter outbound acl 3000
[Huawei-GigabitEthernet0/0/1]quit
```

5.8 验证高级访问控制列表

```
[Huawei]dis
[Huawei]display acl
[Huawei]display acl 3000
Advanced ACL 3000, 3 rules
Acl's step is 5
 rule 5 deny tcp source 192.168.1.0 0.0.0.255 destination 172.16.10.1 0 destination-port eq ftp
 rule 10 deny tcp source 192.168.2.0 0.0.0.255 destination 172.16.10.2 0
 rule 15 permit ip

[Huawei]disp
[Huawei]display tr
[Huawei]display traf
[Huawei]display traffic-filter ap
[Huawei]display traffic-filter applied-record
-------------------------------------------------------------
Interface                 Direction  AppliedRecord
-------------------------------------------------------------
GigabitEthernet0/0/0      outbound   acl 2000
GigabitEthernet0/0/1      outbound   acl 3000
-------------------------------------------------------------
[Huawei]
```

可见 ACL3002 为高级 ACL,步长为 5，共有三条规则，首先匹配源地址为 192.168.1 的网络访问目的地址 192.168.3.1 的21端口的TCP数据报;其次匹配源地址为192.168.2的网络访问目的地址192.168.5.1的TCP数据报；最后匹配所有 IP 数据报。三条规则严格按照顺序匹配，这样可以有序的放行、禁止各类数据报。

6. 结论与分析：

6.1 防火长城与访问控制列表

老师上课介绍访问控制原理是提到了他的在我国的一个应用，我产生了好奇并查阅资料了解了相关知识。

防火长城的原理之一是 IP 地址封锁

IP 地址封锁是GFW（Grate Fire Wall）通过路由器来控制的，在通往国外的最后一个网关上加上一条伪造的路由规则，导致通往某些被屏蔽的网站的所有 IP 数据包无法到达。路由器的正常工作方式是学习别的路由器广播的路由规则，遇到符合已知的 IP 转发规则的数据包，则按已经规则发送，遇到未知规则 IP 的数据，则转发到上一级网关。

而GFW对于境外(中国大陆以外)的XX网站会采取独立IP封锁技术。然而部分XX网站使用的是由虚拟主机服务提供商提供的多域名、单(同)IP 的主机托管服务，这就会造成了封禁某个 IP 地址，就会造成所有使用该服务提供商服务的其它使用相同 IP 地址服务器的网站用户一同遭殃，就算是正常的网站，也不能幸免。其中的内容可能并无不当之处，但也不能在中国大陆正常访问。现在GFW通常会将包含XX信息的网站或网页的URL加入关键字过滤系统，并可以防止民众透过普通海外HTTP代理服务器进行访问。

防火长城的原理之一是特定端口封锁

GFW 会丢弃特定 IP 地址上特定端口的所有数据包，使该 IP 地址上服务器的部分功能(如 SSH 的 22、VPN 的 1723 或 SSL 的 443 端口等)无法在中国大陆境内正常使用。

防火长城的原理之一是 DNS 劫持和污染

GFW 主要采用 DNS 劫持和污染技术，使用 Cisco 提供的 IDS 系统来进行域名劫持，防止访问被过滤的网站，2002 年 Google 被封锁期间其域名就被劫持到百度。中国部分 ISP 也会通过此技术插入广告。

对于含有多个 IP 地址或经常变更 IP 地址逃避封锁的域名，GFW 通常会使用此方法进行封锁。具体方法是当用户向DNS服务器提交域名请求时，DNS返回虚假(或不解析)的IP地址。

全球一共有13组根域名服务器(Root Server)，目前中国大陆有F、I这2个根域DNS镜像，但现在均已因为多次DNS污染外国网络，而被断开与国际互联网的连接。

DNS 劫持和污染是针对某些网站的最严重的干扰。

干扰的方式有两种：

一种是通过网络服务提供商(Internet Service Provider)提供的DNS服务器进行DNS欺骗，当人们访问某个网站时，需要要把域名转换为一个 IP 地址，DNS 服务器负责将域名转换为 IP 地址，中国大陆的 ISP 接受通信管理局的屏蔽网站的指令后在 DNS 服务器里加入某些特定域名的虚假记录，当使用此 DNS 服务器的网络用户访问此特定网站时，DNS 服务便给出虚假的 IP 地址，导致访问网站失败，甚至返回 ISP 运营商提供的出错页面和广告页面。

另一种是 GFW 在 DNS 查询使用的 UDP 的 53 端口上根据 blacklist 进行过滤，遇到通往国外的使用 UDP53 端口进行查询的DNS请求，就返回一个虚假的IP地址。

6.2 实验感悟

如果我们稍微留心一点，我们就会发现我们生活中可以看见到处都是计算机网络的影子，我们在不清楚原理的情况下已经使用了这么久，然后通过本次实验将课上的理论应用到了实际，书本上的知识不在是死知识，而是能够通过实践证明的的知识。看着这一个个协议看似紊乱实则高度有序的工作，我不禁感受到无数前人的伟大，完整的大厦不是一蹴而就的，也不是一人之作，是千千万万的学者和工程师的汗水，才让我们今天能够直接尝到果实。但是我们作为新一代计算机科学的学者，在享受这些成果的同时也要的发展它，而发展它就要求我们首先要继承之前学者的智慧，站在巨人的肩膀上，才能远眺和发展。

【过程记录（源程序、测试用例、测试结果等）】