计算机网络体系结构

2023年秋季课 程

Instructor: 江 勇 教 授
Room: 信息大 楼 2211

1 NAT

NAT 协议能够有效缓解IPv4 地址缺乏问题。它是一种把内部私有网络IP 地址翻译成公共网络IP 地址的技术，允许一个组织以一个或多个全球唯一IP 地址(global address, 以下也成为公有地址) 出现在互联网上。

1.1 实验目的

掌握NAT 服务器的配置技术，理解NAT 协议的原理，理解地址翻译技术。

1.2 实验地点

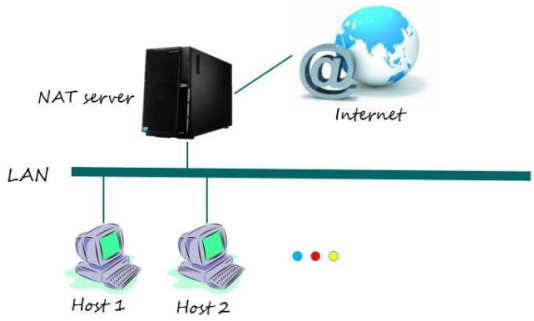
信息大楼2211

1.3 协议简介

请参考相关网络书籍如《计算机网络》，也可查阅网上资料。

1.4 实验内容

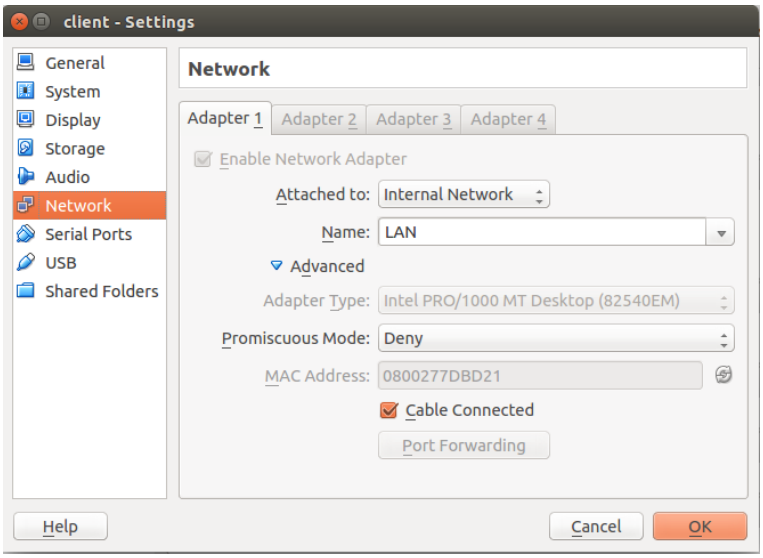
1.4.1 实验拓扑



1.4.2 实验方案

1、客户机Host1设置

(1)网卡编辑使用Virtualbox 工具设置客户机只有一个网卡，并采用internal network 模式



（2）IP 地址设定：

```
sudo ifconfig eth0 192.168.0.2
```

（3）、DNS 服务器设定：

```
sudo  gedit  /etc/resolv.conf
```

修改默认 DNS 如下：

nameserver 114.114.114.114

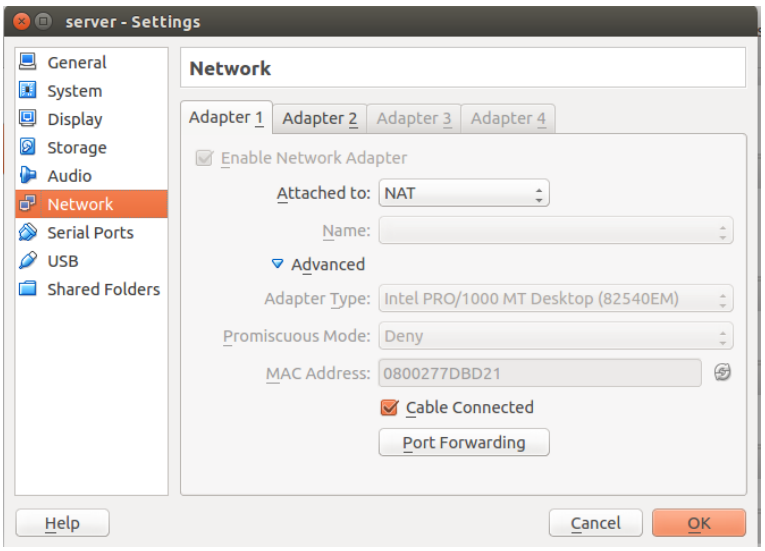
（4）、网关设定：

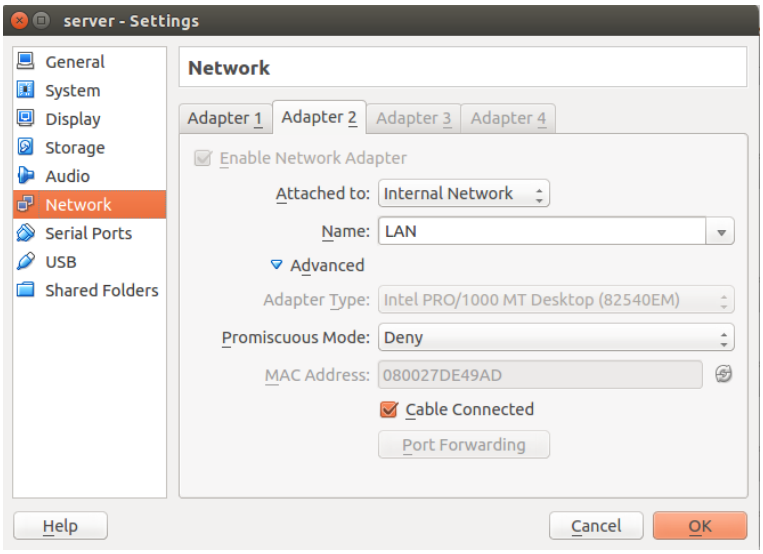
```
sudo route add default gw 192.168.0.1
```

2、NAT 服务器设置

（1）、网卡编辑

使用 virtualbox 工具编辑服务器的网卡，一个网卡采用 NAT 模式与物理主机（即 Internet）相连，一个网卡采用 internal network 模式，和 Host 在同一个 LAN 中。





（2）设置 IP 地址

对于 NAT 到物理主机的网卡，即 eth0，用 DHCP 的方式为其分配 IP 地址:

```
sudo dhclient eth0
```

对于和 host 在同一个局域网内的网卡 eth1，静态指定其 IP 地址：

```
sudo ifconfig eth1 192.168.0.1
```

（3）、打开转发功能

```
sudo gedit  /etc/sysctl.conf
```

取消对于 net.ipv4.ip_forward=1 的注释

（4）、添加 NAT 功能

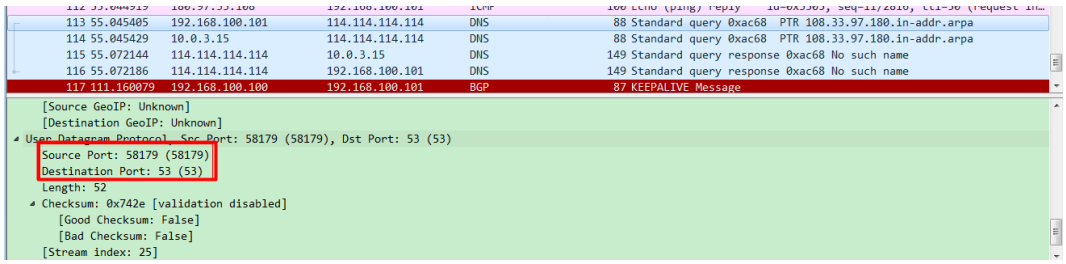
```
iptables -t nat -A POSTROUTING -s "192.168.0.1/24" -o eth0 -j MASQUERADE
```

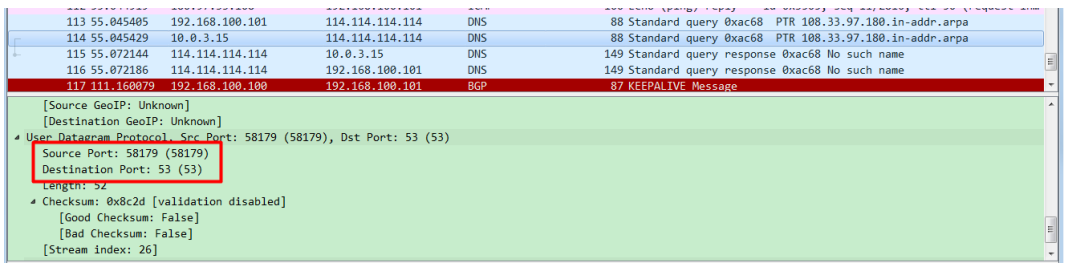
1.4.3 观察

1、观察 NAT 服务器对分组进行地址和端口翻译的过程。提示：PC 1 往外发的分组经过 NAT 时，和网管将翻译分组中的地址为自身的地址、端口。有应答时，翻译为 PC 1 的地址和端口。

2、观察 NAT 对分组校验和的修改。提示：地址和端口完成翻译后，校验和也要重新计算。

3、部分示例数据：





1.5 思考题

- NAT 协议中，需要对UDP 会话中的UDP 校验和进行修改, 选哪个修改。为什么UDP 校验和为0 时不需要修改？请结合UDP 原理回答。
- 跨越NAT 网关还能使用ping 和traceroute 么？
- 分析NAT 技术的优缺点。

2 OSPF 协议

开放最短路径优先协议OSPF（Open Shortest Path First）是一个内部网关协议（Interior Gateway Protocol，IGP），用于在一个自治系统内部动态交互、计算路由，采用链路状态路由算法。OSPF 通过在路由器之间通告网络接口的状态来建立链路状态数据库，生成最短路径树。

2.1 实验目的

通过配置、观察OSPF 实际的运行过程，可对协议有直观的认识。

2.2 实验地点

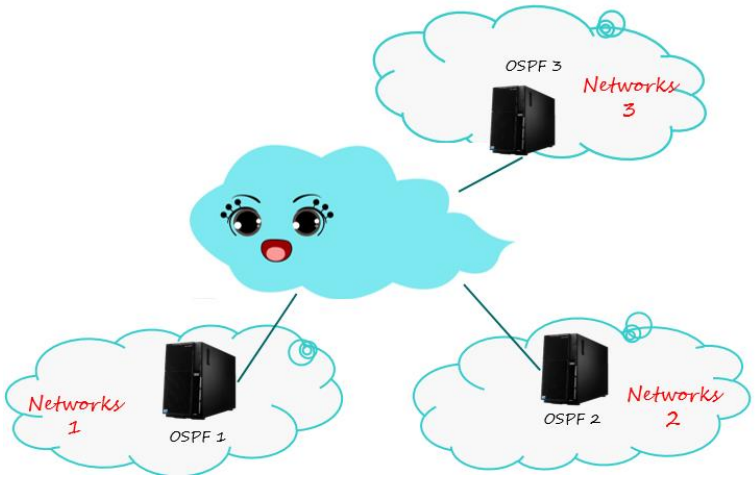
信息大楼2211

2.3 协议简介

OSPF 是一个链路状态协议，能解决RIP 协议收敛速度慢等问题。RFC2328 是OSPFv2 的标准。OSPF 的核心是链路状态信息洪泛和Dijkstra 最短路径算法。通过链路状态信息洪泛，路由器向自治系统内的所有其他OSPF 路由器洪泛它的本地拓扑信息，同时接收所有其他OSPF 路由器的本地拓扑信息。由此，每台路由器能够得到完整的全局拓扑信息，并以此为输入，通过Dijkstra 算法计算出以自身为根节点的最短路径树。从每个最短路径树即可以得到转发表。

2.4 实验内容

2.4.1 实验拓扑



2.4.2 实验方案

本实验可以自己构建一个虚拟网络，设置多台虚拟机来完成，也可以配置自己的 OSPF 与实验室其他人的 OSPF 进行交互来完成。下面演示方案中，假设路由器连接两个网卡（eth0 和 eth1），etho 连接网段 192.168.0.1/24，eth1 连接网段 192.168.1.1/24，并且假设 192.168.0.1/24 网段内还有另一个 OSPF 路由器。具体的网卡编辑和 IP 地址设定参考 1.3 节内容。

1、下载 quagga 软件

```
sudo apt-get install quagga（已完成）
```

2、打开 ospf 进程

```
sudo gedit /etc/quagga/daemons
```

修改 ospf 和 zebra 为 yes，如下：

```
zebra=yes
bgpd=no
ospfd=yes
ospf6d=no
ripd=no
ripngd=no
isisd=no
babeld=no
```

3、生成 zebra 和 ospfd 的配置文件，并设定权限

```
cd /etc/quagga/
sudo touch zebra.conf ospfd.conf
sudo chown quagga.quagga  zebra.conf ospfd.conf
```

4、初始化配置文件只含有一个默认密码

```
sudo gedit zebra.conf
```

添加：

password zebra

```
sudo gedit ospfd.conf
```

添加：

password ospf

5、启动 quagga

```
sudo /etc/init.d/quagga start
```

6、配置 zebra

Zebra 用来设置路由器端口信息，下面内容仅供参考，具体细节随网卡配置的不同而不同。

```
sudo telnet localhost 2601
enable
configure terminal
interface eth0
ip address 192.168.0.1/24
no shutdown
interface eth1
ip address 192.168.1.1/24
no shutdown
write
exit
exit
exit
```

配置之后的配置文件 zebra.conf 如下：

```
!
! Zebra configuration saved from vty
!   2015/11/10 19:48:01
!
password zebra
!
interface eth0
 ip address 192.168.0.1/24
 ipv6 nd suppress-ra
!
interface eth1
 ip address 192.168.1.1/24
 ipv6 nd suppress-ra
!
interface lo
!
ip forwarding
!
!
line vty
!
```

7、配置 ospf

ospfd 用来设置路由器通告信息，下面内容仅供参考，具体细节随网卡配置的不同而不同。

```
sudo telnet localhost 2604
enable
configure terminal
router ospf
network 192.168.0.0/24 area 0.0.0.0   // eth0 对应的通告信息
```

```
network 192.168.1.0/24 area 0.0.0.1   // eth1 对应的通告信息
write
exit
exit
exit
```

配置之后的配置文件 ospfd.conf 如下：

```
!
! Zebra configuration saved from vty
!     2015/11/10 19:50:33
!
password ospf
!
!
!
interface eth0
!
interface eth1
!
interface lo
!
router ospf
  network 192.168.1.1/24 area 0.0.0.1
  network 192.168.0.1/24 area 0.0.0.0
!
line vty
!
```

8、重启服务

```
sudo /etc/init.d/quagga restart
```

9、重启服务

查看路由表是否正确

```
sudo route
```

本例的路由如下：

Kernel IP routing table

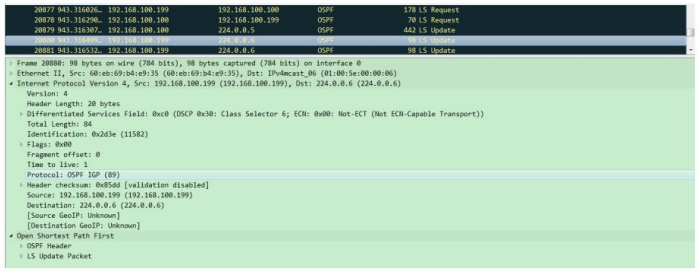
Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.0.0	*	255.255.255.0	U	0	0	0	eth0
192.168.1.0	*	255.255.255.0	U	0	0	0	eth1
192.168.2.0	192.168.0.2	255.255.255.0	UG	20	0	0	eth0

2.4.3 观察

1、观察链路状态更新分组。

2、观察 LSA。从上面的 LS Update 分组中找到 LSA，解析其内容。

3、 部分示例数据



2.5 思考问题

- 改变OSPF Area 类型时，OSPF 的邻居关系会发生震荡么？
- 两条“等价”路径存在时，OSPF 如何处理在网络中建立几条路径？
- 拓展http://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first -ospf/9237-9.html

3 BGP协议

BGP 是一个不同自治域系统（AS，Autonomous System）的路由器之间进行路由信息交换的外部网关协议，是ARPANET 所使用的EGP 的替代协议。

3.1 实验目的

掌握BGP 协议的工作原理，理解BGP 四种报文格式。

3.2 实验地点

信息大楼2211。

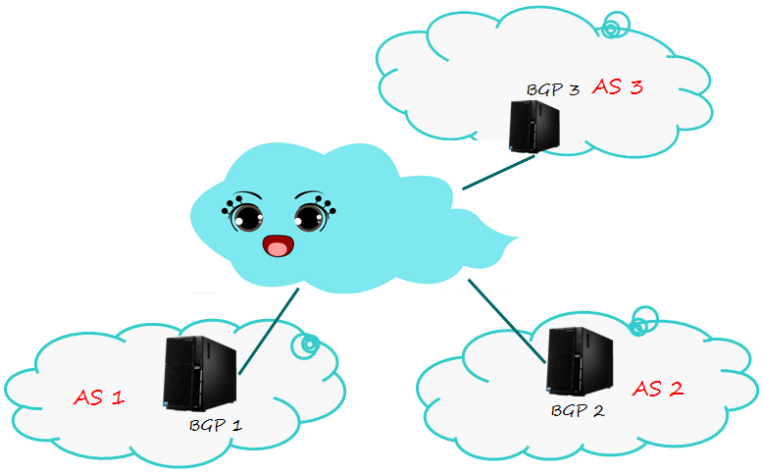
3.3 协议简介

边界网关协议（BGP，Border Gateway Protocol）是一个自治系统之间的动态路由发现协议，在自治系统之间自动交换无回路路由信息。对等体处于不同AS 的BGP 对等体之间的协议称为EBGP（External BGP）协

议，完成 AS 之间的路由选择。

3. 4 实验内容

3.4.1 实验拓扑



3.4.2 实验方案

本实验可以自己构建一个虚拟网络，设置多台虚拟机来完成，也可以配置自己的 BGP 与实验室其他人的 BGP 进行交互来完成。下面演示方案中，假设路由器连接两个网卡（eth0 和 eth1），etho 连接网段 192.168.0.1/24，eth1 连接网段 192.168.1.1/24，并且假设 192.168.0.1/24 网段内还有另一个 BGP 路由器，两者进行交互。具体的网卡编辑和 IP 地址设定参考 1.3 节内容。

注意 OSPF 和 BGP 的区别。下面内容大部分与 2.3 重复，请读者甄别。

1、下载 quagga 软件

```
sudo apt-get install quagga（已完成）
```

2、打开 bgpd 进程

```
sudo gedit /etc/quagga/daemons
```

修改 bgp 和 zebra 为 yes，如下：

```
zebra=yes
bgpd=yes
ospfd=no
ospf6d=no
ripd=no
ripngd=no
isisd=no
babeld=no
```

3、生成 zebra 和 bgpd 的配置文件，并设定权限

```
cd /etc/quagga/
sudo touch zebra.conf bgpd.conf
sudo chown quagga.quagga  zebra.conf bgpd.conf
```

4、初始化配置文件只含有一个默认密码

```
sudo gedit zebra.conf
```

添加：

password zebra

```
sudo gedit bgpd.conf
```
添加：

password bgp

5、启动 quagga

```
sudo /etc/init.d/quagga start
```

6、配置 zebra

Zebra 用来设置路由器端口信息，下面内容仅供参考，具体细节随网卡配置的不同而不同。

```
sudo telnet localhost 2601
enable
configure terminal
interface eth0
ip address 192.168.0.1/24
no shutdown
interface eth1
ip address 192.168.1.1/24
no shutdown
write
exit
exit
exit
```

配置之后的配置文件 zebra.conf 如下：

```
!
! Zebra configuration saved from vty
!   2015/11/10 19:48:01
!
password zebra
!
interface eth0
 ip address 192.168.0.1/24
 ipv6 nd suppress-ra
!
interface eth1
 ip address 192.168.1.1/24
 ipv6 nd suppress-ra
!
interface lo
!
ip forwarding
!
!
line vty
!
```

7、配置 bgp

bgpd 用来设置路由器通告信息，下面内容仅供参考，具体细节随网卡配置的不同而不同。

```
sudo telnet localhost 2605
enable
configure terminal
router bgp 100                    //自己的 AS 编号
network 192.168.1.0/24             //通告的网络前缀
neighbor 192.168.0.2 remote-as 200   // 会话邻居的 IP 地址和 AS 编号
neighbor 192.168.0.2 description “two”   // 会话邻居的 IP 地址和 AS 编号
write
exit
exit
exit
```

配置之后的配置文件 ospfd.conf 如下：

```
!
! Zebra configuration saved from vty
!     2015/11/10 20:50:31
!
password bgp
!
router bgp 100
 bgp router-id 192.168.1.1
 network 192.168.1.0/24
 neighbor 192.168.0.2 remote-as 200
 neighbor 192.168.0.2 description "two"
!
line vty
!
```

8、重启服务

```
sudo /etc/init.d/quagga restart
```

9、重启服务

查看路由表是否正确

```
sudo route
```

3.4.3 观察

1、 观察 OPEN 报文：

（1）传输协议层 TCP 中的端口号是否为 179？

（2）Marker 字段的值是否全为 1？所观察到的值代表什么含义？

（3）Length 字段的值？OPEN 报文各个字段的总长度？二者是否相等。

（4）Type 字段的值是否与 OPEN 报文的类型值对应。

（5）Version 字段是否为 4？

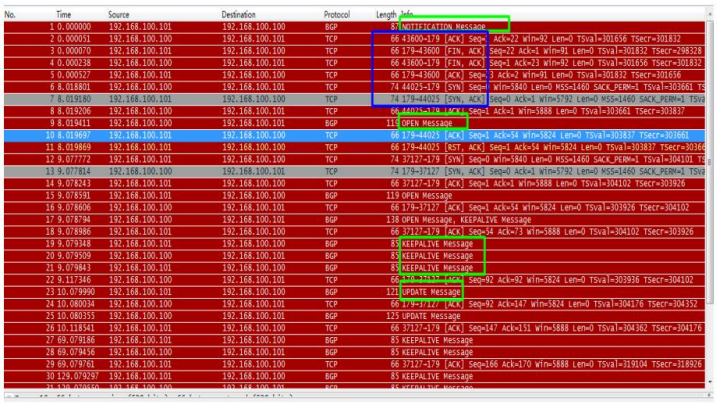
（6）观察 My As 字段，Hold Time 字段，IP 地址字段，确认这个 OPEN 报文发送者所在的 AS 号，建议的保持时间，以及 IP 地址。

2、观察 KEEPALIVE 报文。

3、观察 UPDATE 报文，重启 quagga。

4、观察 NOTIFICATION 报文。

5、部分示例数据



3.4 思考问题

- 重启quagga 程序后，出现的UPDATE 消息是成对的，即两个BGP 对等体都向对方那个发送了一个UPDATE 消息。请结合这个具体例子，思考产生这个现象的原因。
- 如何验证BGP 声明的正确性？

4 配置DNS 服务器

DNS（Domain Name System）服务器主要完成主机名称和主机IP 地址的翻译工作。

4.1 实验目的

指导读者配置一台DNS 服务器，促进读者对DNS 工作原理的理解。

4.2 实验地点

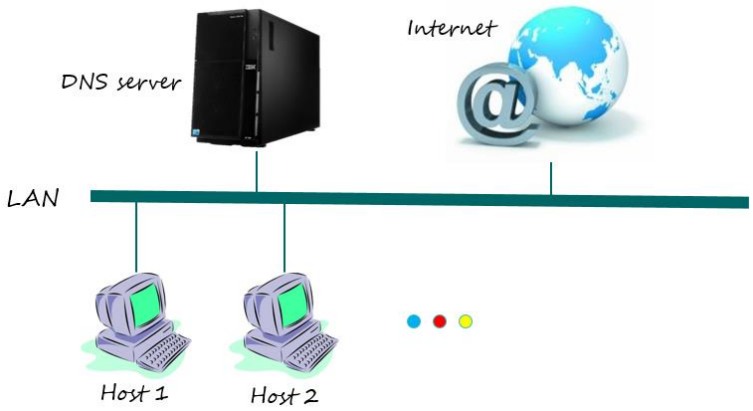
信息大楼2211。

4.3 DNS层次结构

DNS 采用分层结构，并有两种查询方式。自行查阅资料了解具体细节

4. 4 实验内容

4.4.1 实验拓扑



4.4.2 实验方案

在 DNS 服务器上面配置对于 yourname.com 域名的解析，使得主机 A 能够 ping 通 yourname.com 的域名。本演示为了简化在 DNS 服务器和主机 A 部署在同一台主机（虚拟机）上。令，主机采用单网卡（NAT 模式），网卡编辑和地址获取等细节参照 1.3。

1、安装 bind 软件

```
sudo apt-get install bind9（已安装）
```

2、设置 DNS 服务器

```
sudo gedit /etc/resolv.conf
```

修改 DNS 服务器为：

nameserver 127.0.0.1

3、在配置文件/etc/bind/named.conf.local 添加新的域，如下：

```
sudo gedit named.conf.local
```

示例如下：

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "leehengtong.com"{
        type master;
        file "/etc/bind/db.leehengtong.com";
        };
```

4、以 db.local 为模板设置自己的 DNS 映射

```
sudo cp db.local db.leehengtong.com
sudo gedit db.leehengtong.com
```

示例如下：

```
;
```

```
; BIND data file for local loopback interface
;
$TTL604800
@    IN    SOA leehengtong.com. mail.leeheng.com. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@    IN    NS    leehengtong.com.
@    IN    A     180.97.33.108
@    IN    AAAA      ::1
*    IN    A     180.97.33.108
```

从而将*.leehengtong.com 的地址映射到百度 IP 地址。

5、启动 bind9

```
sudo /etc/init.d/bind9 start
```

6、清空 DNS 缓存

```
sudo /etc/init.d/dns-clean start
```

7、测试

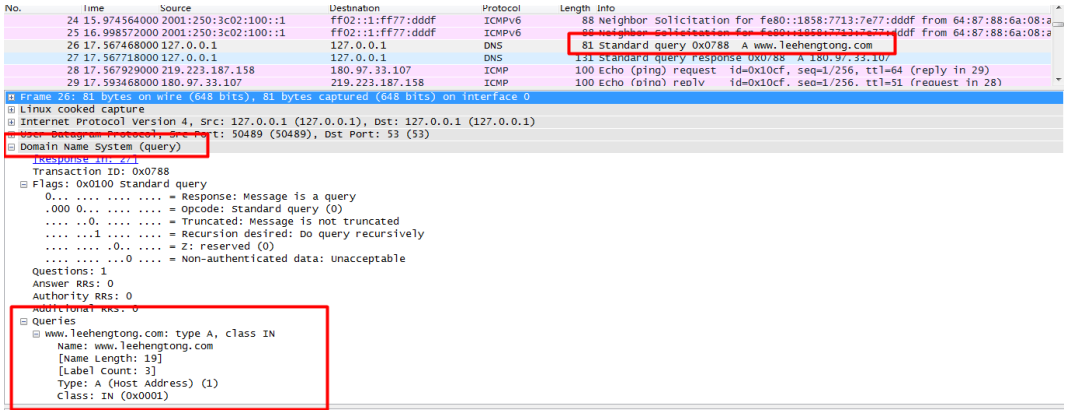
```
ping www.leehengtong.com
```

4.4.3 观察

1、www.youname.com 和其他地址的解析过程

2、使用 wireshark 抓包分析域名请求和应答过程

2、 部分示例数据



4.5 思考问题

1、一个 DNS 查询的答复中是否会包含几个应答记录？如果是，对同一查询多执行几次，看看每次应答记录的顺序是否相同，试分析为什么。

2、思考一下如何劫持 www.naichabiao.com 到 www.jd.com.

推荐资源

1、几个推荐的 google 镜像：

https://g.weme.so/

http://g.bt.gg/
https://www.guge.date/
https://gl.lamkakyun.com/

备注：*(1) 实验方案部分只提供参考思路，不保证完全正确；*
(2) 部分内容参考自上一年的实验指导。