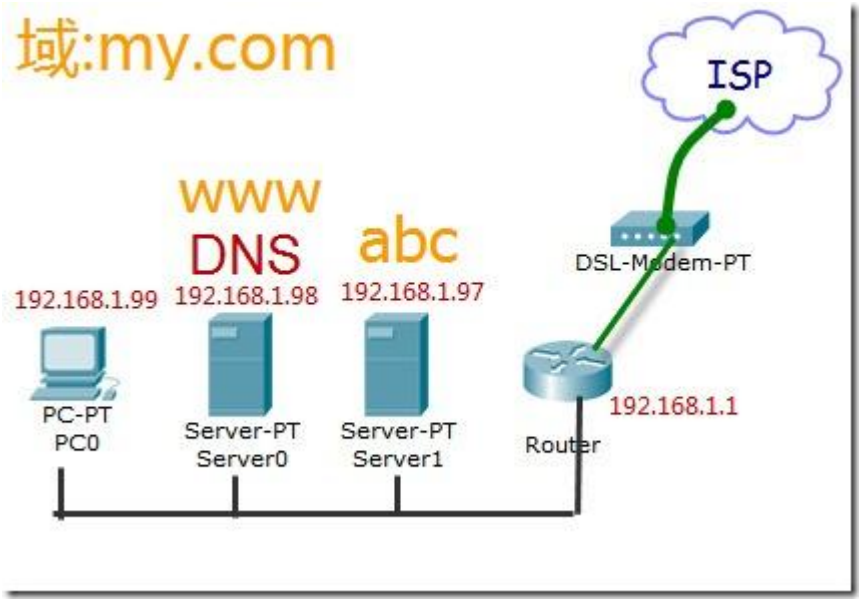
Ubuntu 12.04 Server 中利用 Bind9 搭建 DNS 服务器

- DNS(域名服务器)的作用是把域名转换成 IP 地址，或反过来。
- 此实验，将在局域网的一台主机上用 Bind9 搭建 DNS 服务器，提供域名解析服务。另有两台 HTTP 服务器，设定域名为 www.my.com 和 abc.my.com（随便取一个域名）。网络结构图：



上图中两台服务器 Server0 和 Server1 是在 VirtualBox 下虚拟的，网卡类型用桥接。根据实际情况，宿主系统（WinXP）ip 地址是 192.168.1.99，Server0 是 192.168.1.98，Server2 是 192.168.1.97，网关（路由）是 192.168.1.1，接电信 ISP。

Server0 上安装 HTTP 服务器和 DNS 服务器，Server1 上安装 HTTP 服务器。上面的网络搭建好之后，三台机器之间能够互 ping 得通。

先为两台服务器安装 HTTP 服务器 如果在安装 Ubuntu 已选择安装 LAMP 则跳过这步。否则 执行 sudo apt-get install nginx 安装 nginx，它是一个小巧的 HTTP 服务器，安装完它会自动启动，在浏览器测试一下 http://192.168.1.97，看到"Welcome to nginx!"即成功。

实验目的是使得三台电脑都能用 www.my.com 访问 server0，abc.my.com 访问 server1.

◆ 安装 Bind9：

```
sudo apt-get install bind9 dnsutils bind9-doc
```

其中只需 bind9 就可，后面两个是 dns 的测试工具和 bind9 的文档。

DNS 记录类型请看维基百科，常用有 A 记录、CNAME 记录、MX 记录和 NS 记录。

◆ 转发配置

是当本地的 DNS 服务器在本地数据文件里找不到对应网站后，移交给下一步查询的 DNS 服务器（递推）。编辑**/etc/bind/named.conf.options** 文件 ,取消 forwarders{}的注释 ,在{}加入 **8.8.8.8;** 这是 Google 的 DNS 服务器。

◆ Zone 概念：

zone 即域的意思，像 g.cn、 twitter.com 这样的形式就是域，www.g.cn，ditu.g.cn 这些就是子域。Bind9 的配置文件中，一个域用一个文件来存放，在文件中指明每个子域对应的 IP 地址。

◆ 主 DNS 服务器配置：

编辑**/etc/bind/named.conf.local** 文件，添加域 my.com：

```
zone "my.com"{
        type master;
        file "db.my.com";
};
```

注意别漏了分号，type 指定这台 DNS 服务器为主服务器，file 指定该域的解析文件，默认路径在

/etc/var/cache/bind ， **/etc/bind/db.local** 是 bind 自带的模板文件，复制一份到**/etc/var/cache/bind** ，

并改名成 db.my.com：

```
sudo cp /etc/bind/db.local /var/cache/bind/db.my.com
```

然后编辑**/var/cache/bind/db.my.com**，最终如下：

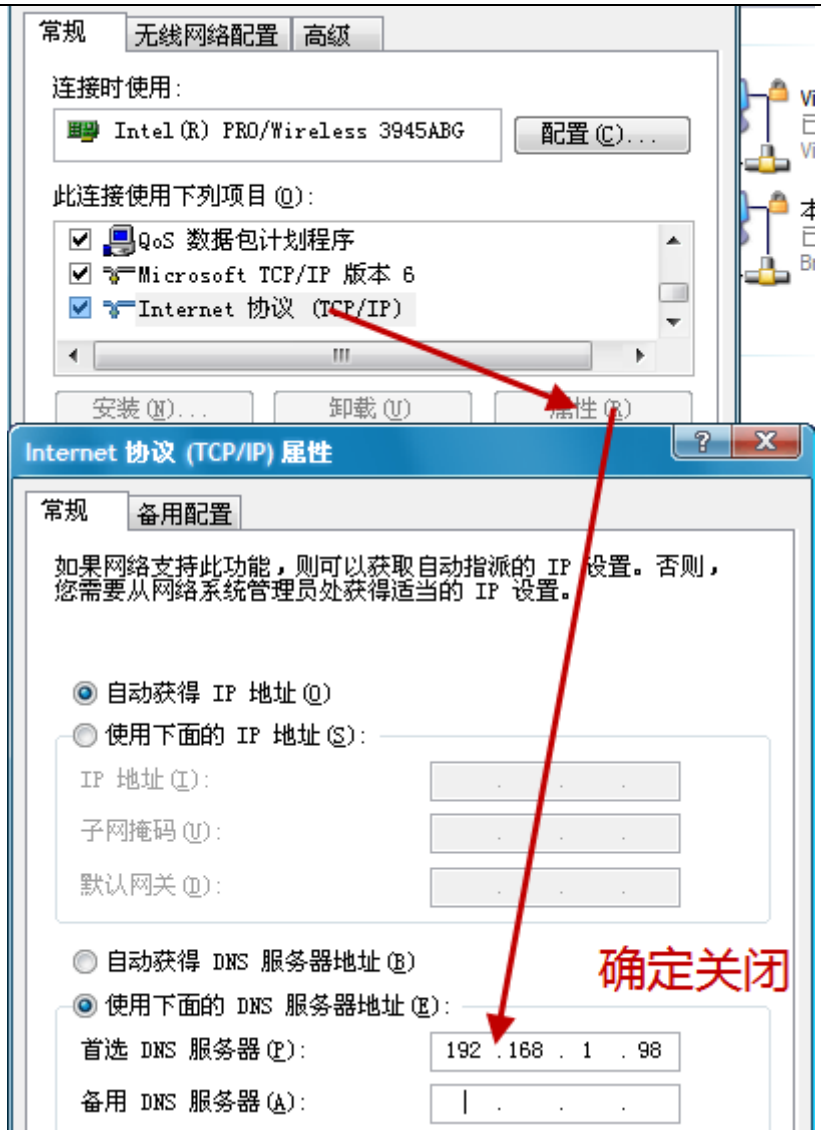
```
$TTL    604800
@       IN      SOA     my.com. root.my.com. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
@       IN      A       127.0.0.1
;@      IN      AAAA    ::1
www     IN      A       192.168.1.98
abc     IN      A       192.168.1.97
server  IN      CNAME   abc
```

从上往下看，$TTL 设置记录在 DNS 缓存服务器上的生存周期（秒）。SOA 记录定义了 my.com 这个域，以及相关参数，默认就行。最后三行，添 加 A 记录，www 指向 server0 的 IP，abc 指向 server1 的 IP，server 则 CNAME 到 abc（这一行非必须，仅演示 CNAME）。

修改完成后重启 bind：

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

此时 DNS 服务器已经开始工作了，要使用该 DNS 服务器，以 XP 为例，到"控制面板"-"网络连接"，找到上网的网卡，右键选择"属性"，如图设置：



然后打开浏览器，访问 www.my.com，abc.my.com，server.my.com 吧。

Linux 修改 DNS，请修改**/etc/resolv.conf** 文件。

关于反向解析：即从 IP 解析到域名。本实验中，该功能没什么用途。在反垃圾邮件方面，它很有作用，由于邮件的协议，伪装域名发送邮件是可能的，这时候，邮件服务器端收到邮件后，根据邮件的 IP 地址反解析，得到域名，如果域名和邮件的发信人域名一致，则收下，否则拒绝。