

网络模拟

抓包工具WireShark

- 只有流经抓包工具所在网卡的数据包才能被抓包工具捕获
- 数据包分析
- 使用筛选器

网络模拟软件GNS3

- 安装GNS3

WinPCAP：抓包必需组件之一，建议安装，如果已经安装过可忽略；
Wireshark：最流行的开源抓包工具，需在线下载，建议安装，也可自行安装；
SolarWinds Response Time Viewer for Wireshark：一个Wireshark的辅助分析工具，需在线下载，文件大耗时较长，新手不建议安装；
Dynamips：一个用于模拟思科路由器的工具，必须安装；
QEMU：是一套由Fabrice Bellard所编写的模拟处理器的自由软件，必须安装；
VPCS：GNS3中模拟客户端的工具，必须安装；
Cpulimt：一款限制CPU进程的工具软件，优化系统资源的占用率，可选安装；
GNS3：核心组件，必须安装；
SuperPutty：GNS3自带终端工具，可选安装。

- 配置思科路由器
- 布置网络及划分网段
- 配置ip地址、子网掩码、网关地址、时钟频率、路由表

配置PC

```
ip 192.168.10.2 255.255.255.0 192.168.10.10（配置IP地址、子网掩码、网关）  
save（保存配置）  
show（查看配置）
```

配置路由器

```
// 配置地址  
config terminal（进入全局配置模式）  
interface fastEthernet 0/0（进入接口配置模式）  
ip address 192.168.10.10 255.255.255.0（配置地址）  
no shutdown（启用接口）  
  
//配置DCE路由器的时钟频率  
show controller serial 1/0（查看接口是DCE还是DTE）  
config terminal  
interface serial 1/0  
clock rate ?（查看可以配置的时钟频率）  
clock rate 64000（配置时钟频率）
```

```
encapsulation ppp（配置帧封装格式）
ip address 172.16.0.1 255.255.255.0
no shutdown
exit
exit
copy running-config startup-config（保存配置）

// 配置路由表
config t（进入全局配置模式）
ip route 192.16.80.0 255.255.255.0 192.168.20.20（如果目标地址网段是
192.16.80.0，则下一跳地址为192.168.20.20）

// 其他命令
no ip address（去掉所配置的地址）
exit（退出）
enable（进入特权模式，用于发PING）
show running-config（查看配置）
show ip route（查看路由表）
```

- ping、抓包

虚拟机软件VMware Workstation

软件本身拥有20个虚拟交换机，分别是VMNet0、VMNet1、VMNet2、…、VMNet19，每个交换机都可以使得连接在该交换机上的所有虚拟机形成一个网络。

同时软件可以在物理机上创建出20个与虚拟交换机对应的虚拟网卡，使得连接在虚拟交换机上的虚拟机可以和物理机进行通信。

虚拟交换机、主机物理网卡、主机虚拟网卡之间的关系

① 不和主机网卡相连

虚拟机 -> 虚拟交换机

无法和主机通信，由所有连接在虚拟交换机上的虚拟机构成一个网络

② 和主机网卡相连（即将虚拟交换机和主机网卡进行绑定）

桥接模式：虚拟机 -> 虚拟交换机 = 主机物理网卡 -> 主机（与主机可以通信，并且能够连接因特网）

其他模式：虚拟机 -> 虚拟交换机 = 主机虚拟网卡 -> 主机（与主机可以通信，但不能够连接因特网）

注意

- 虚拟机的网段要和虚拟交换机设定的网段一致，其网关就是主机网卡的地址或者路由器地址
- 关闭防火墙 wf.msc

路由器

路由器用于不同网段的连接，使得不同网段的两台计算机可以进行通信。

路由器需要设置路由表，路由表用于指出数据包要到达目标网段，下一跳路由器的接口地址应该是什么

交换机和集线器

交换机

第一次将发送到交换机上的数据包广播到该网段上的所有计算机上，同时认识每个接口连接的是哪一个计算机，第二次以后就不需要广播了

集线器

集线器始终通过广播来转发数据包



网关

一个主机要与另一个网段的主机进行通信，就需要网关进行信息转发，因此网关地址一般就是路由器接口地址。如果仅仅是与同网段的主机进行通信，那么一般就不需要设置网关地址。