**北 京 林 业 大 学**

**2018学年— 2019 学年第 1 学期 计算机网络A实验报告书**

专 业： 网络工程 班 级： 网工17

姓 名： 杜文基 学 号： 171002408

实验地点： 学研N05 任课教师： 齐建东

实验题目： IP 协议分析，熟悉 GNS3 软件

实验环境： 机房windows7，自己电脑windows10&&GNS3

1.1 实验目的及内容

（1）对 IP 数据包，进行协议分析。（使用 ping 命令触发）

（2）安装并学习使用 GNS 软件。

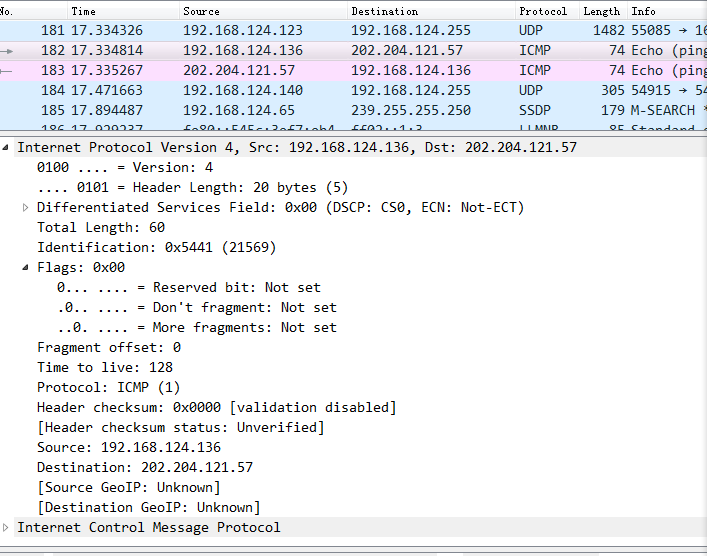
1.2 实验分析 就 wireshark 的捕获结果：

（1） 查看 IPv4 header

（2） 关于 GNS3，本次实验能做到以下即可： a) 安装 GNS3 软件。 b) 阅读 official guide，学习 GNS 的基本使用；学习 ios 的基本操作。 后续（非本次）实验，将捕获路由协议报文，需要在 GNS3 环境下完成。

1.3 实验步骤说明 下载安装 GNS3：https://gns3.com/software。当前最新版是 2.1.15，已经下载 到 ftp 服务器上，无须从官网下载。 什么是 GNS3？ 你现在知道：Vmware（或 Virtualbox）可以虚拟化出来一台 PC 机（通过 在 vmware 中加载 windows、linux 等 OS）。那：GNS3/dynamips 可以虚拟化出来一 台路由器（通过在 GNS3 中加载 ios，ios：Cisco 公司的路由器中的操作系统）。GNS3 不仅仅可 以虚拟化为路由器，也可以虚拟化为防火墙的等等硬件设备。 GNS3 的基本使用。 ⎫ 请去官网 ， 阅 读 “official guide 、 documentation 、 tutorial etc.” 等 （https://docs.gns3.com/），因为只有官方文档才是最 update 的。（学习、 掌握任何软件或解决方案，第一步都是去 official website 阅读 official guide，而不是首先 baidu 或 google 非 official document。） ⎫ Getting Started with GNS3：在 windows 下安装 GNS3： https://docs.gns3.com/11YYG4NQlPSl31YwvVvBS9RAsOLSYv0Ocy-uG2K8ytIY/index.html ⎫ GNS3 Setup Wizard - Local server：以 Local server 方式配置 GNS： https://docs.gns3.com/1yL-p0vPROWPTkQqkEzL2IaDu7iYW-PUzpFamnksHH98/index.html tips：先看英文文档，再去 google 中文文档。在 google 时，注意软件的 版本号！不同版本，会有差异。 你看到的“帖子”，不一定适用于你的 环境。 ios，ftp 服务器上可以下载，非商业使用。法律上，cisco 公司禁止传播加载 在其路由器中的操作系统（即 ios）。请使用“unzip-c7200-advsecurityk9- mz.124-9.T1”。 1.4 实验要求 （1）截图（wireshark 中的 packet）； （2）并就所捕获报文的截图，对报文结构或交互过程进行分析、说明。 （3）复现（reproduce）GNS3 官网上最基本的实验：“Your First GNS3 Topology” <https://docs.gns3.com/1d1huu6z9-wWGD_ipTSQZqy2mpaxiqzymu-YQo6at_Jg/index.html>

用wireshark截的数据包



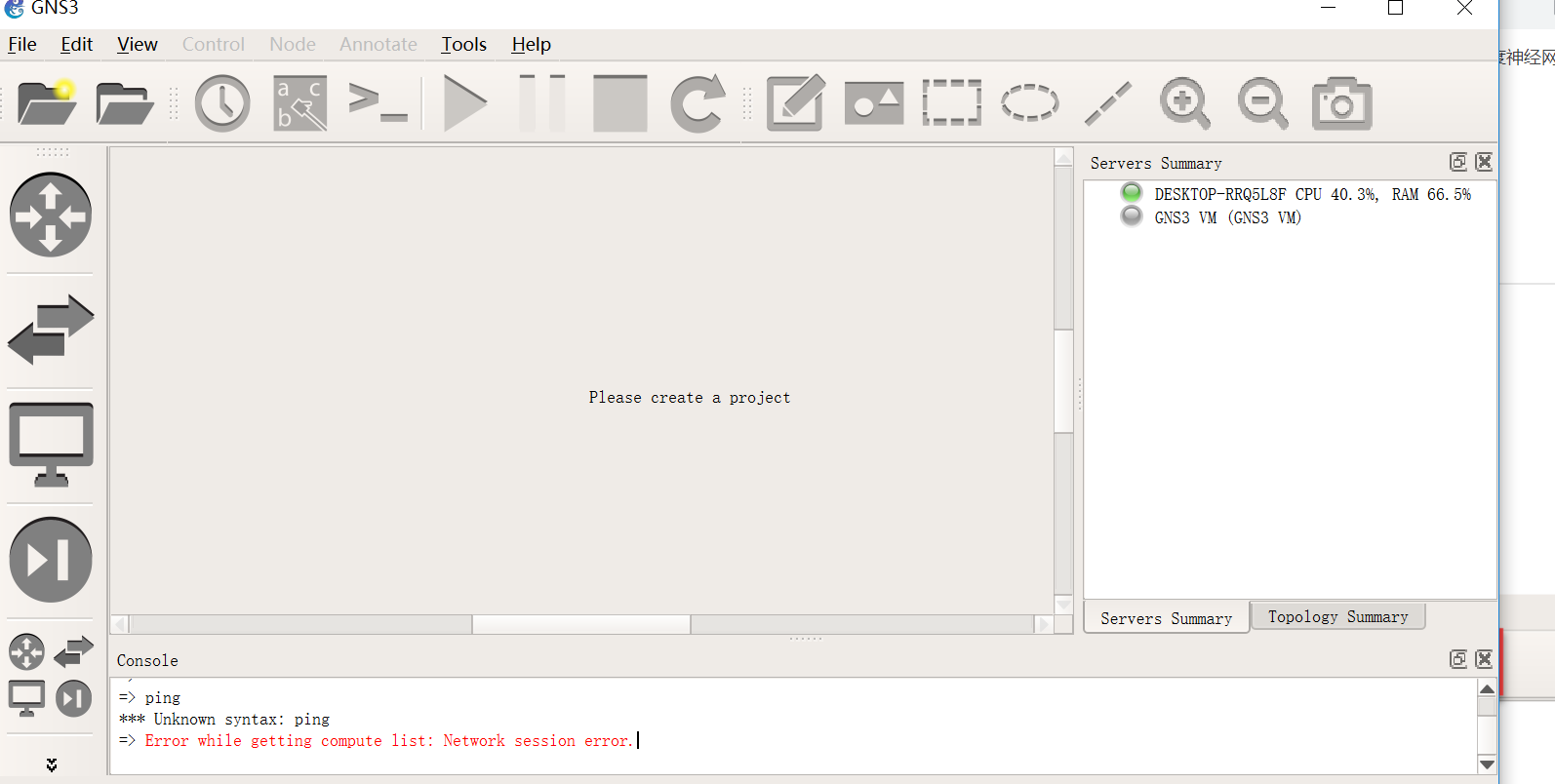
Version  
IP 协议的版本号，4个bit。版本为4   
Header Length   
IP header 的长度，包括 IP Options 的长度，但不包括所负载的数据长度。这个字段占4个bit，每一个bit表示4个字节（units of 32 bits），这个字段最大值是0xFFFF (15)，所以 IPv4 Header 最长占60个字节，去掉IP Header 中固定的20个字节的长度，剩下可有40个字节的长度留给 IP Options。图中为20bytes。  
Total Length  
整个IP数据报的长度，以字节为单位，包括 IP Header 的长度和所负载的数据的长度，占16个bit。IP数据报所负载的数据长度最小为0，最大为64K 字节。图中为60字节。  
Identification : 标识符，大小16位，在三层把流量区分开来，可以类比于动态端口号，与流量一一对应，同一种流量在网络层的标识符就是相同的，用于流量分片。

Time To Live (TTL)  
IP数据报在网络上存活的时间，其实是数据报在网络上路由器间转发的次数。每个路由器在接受到一个数据报时都会把它的TTL值减1，当TTL值为0时就会 被路由器丢弃，并会向IP数据报中 source IP 发送一个 ICMP 的错误信息。TTL占8个bit，最大跳数为255。这里为128次。  
Protocol  
传输层协议字段，这个字段表明这个IP数据报是使用 L4 中哪一种协议的，这里图中为ICMP（1）。  
Header checksum ：头部校验（16位）和计算数据帧的完整性，TTL不参与校验，随路由次数一直改变，IPV6删除该字段，由于各层也在校验数据帧的完整性。  
Source Address, Destination Address  
IP数据报的发送和接受IP地址，图中发送地址为192.168.124.136

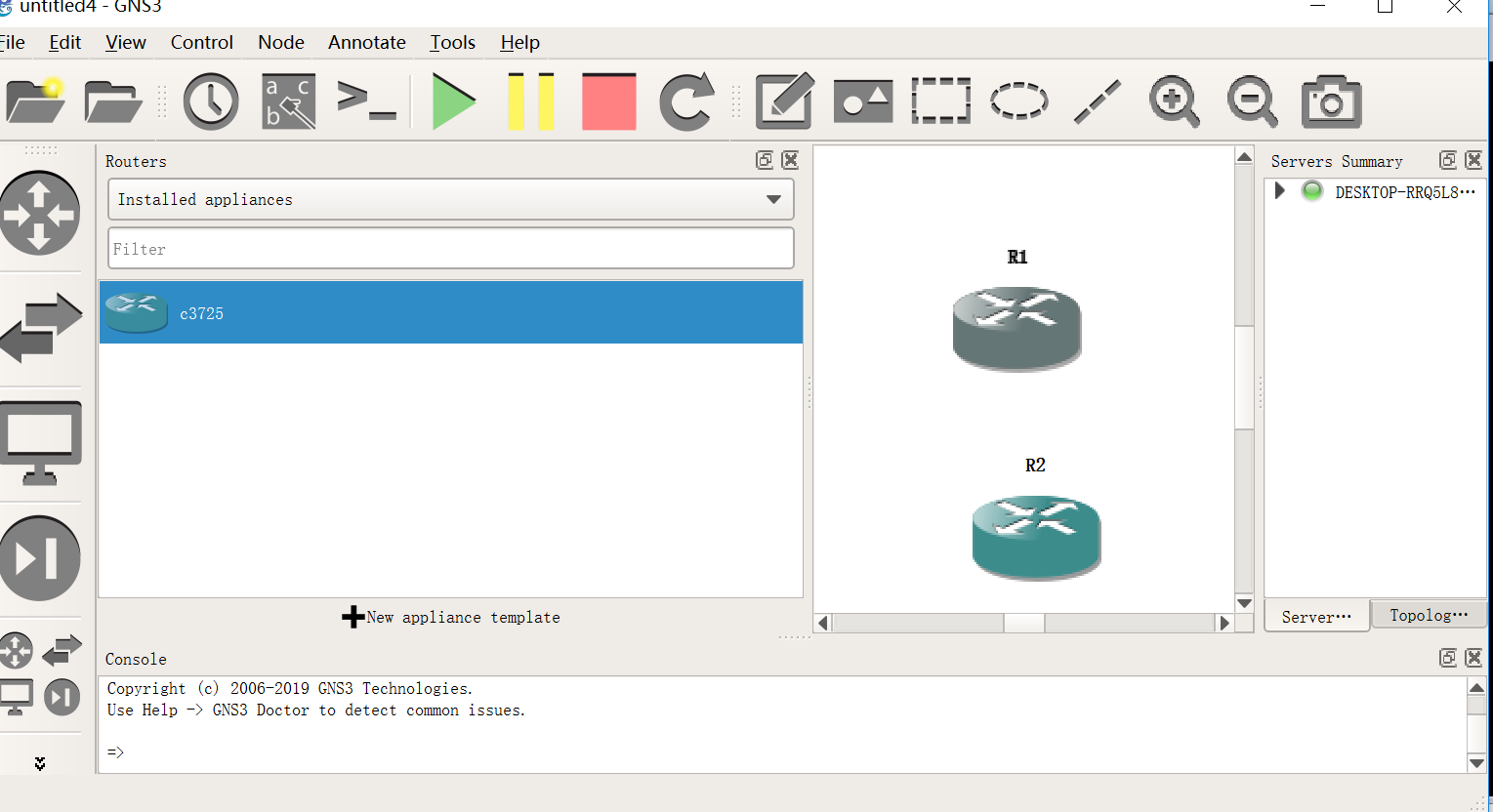
图中目的地址为202.204.121.57  
Flags：标记位，大小3位，分为三部分，保留位（reserved bit），分片位（Don’t fragment）为1代表数据未分片，为0则未分片，更多位（more fragment），

Fragment Offest ：分片偏移，大小13位，用来重排序。第一个分片数据报文偏移为0，第二个为第一个数据报文的大小，以此类推，第n个为前n-1个数据报文的大小之和。

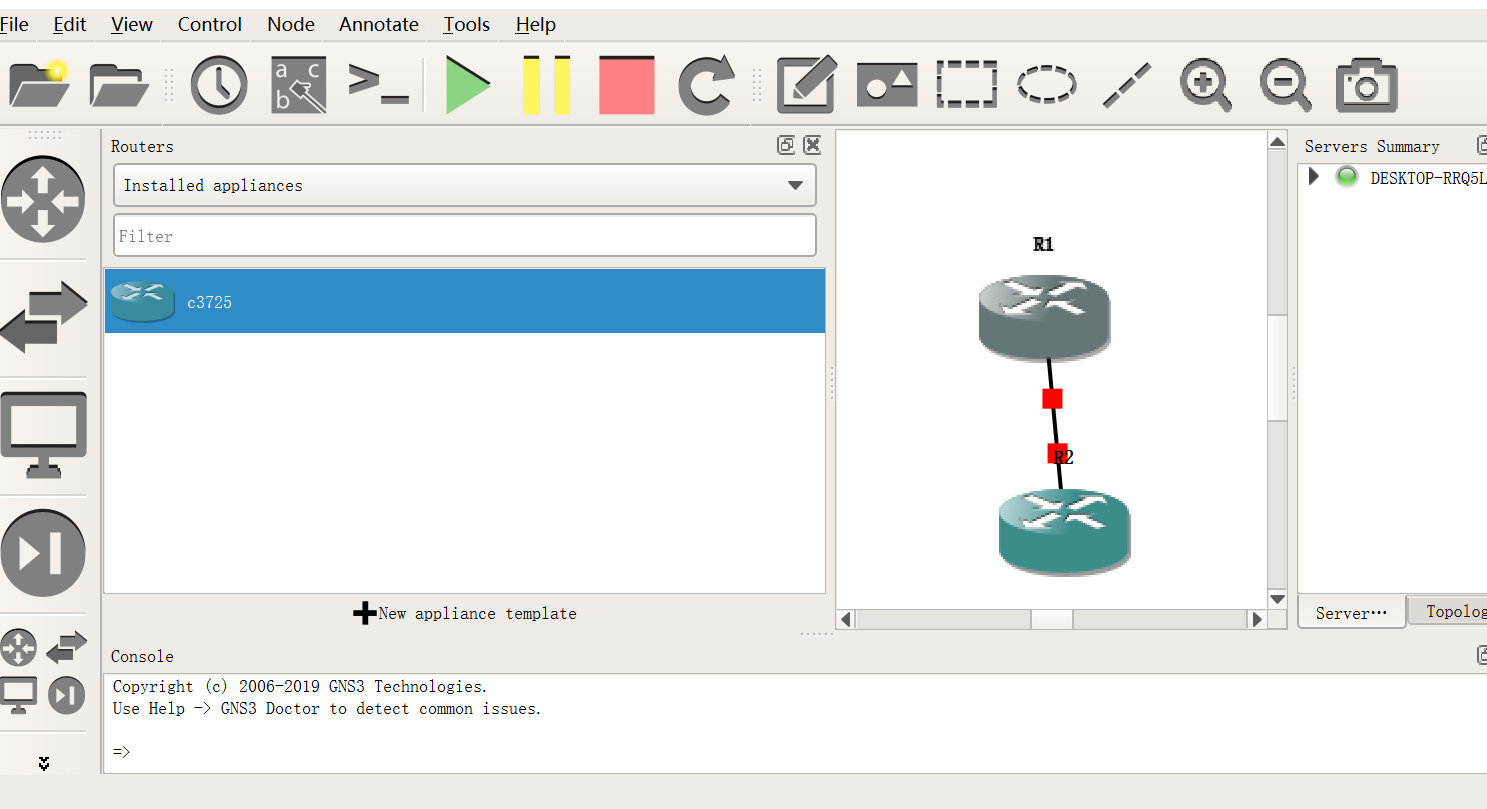
这是我安装后的GNS3界面



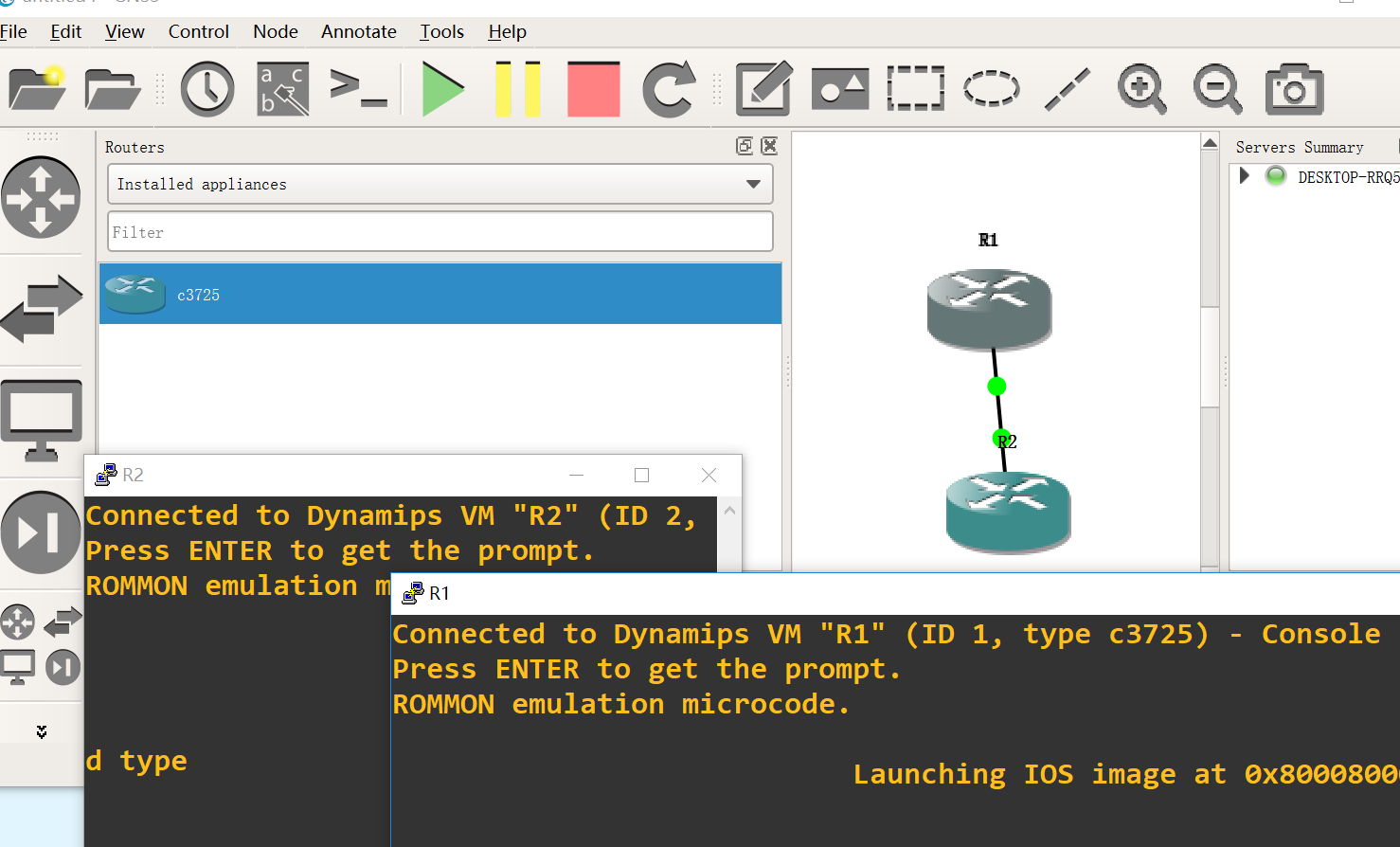
创立两个路由器



R1和R2



进行连接



由于打开的R1和R2正在加载，之后的操作继续进行。

最终完成了复现（reproduce）GNS3 官网上最基本的实验：“Your First GNS3 Topology”