**网络实验报告 exp11**

**2020K8009929032 刘耕印**

1. **实验内容**

本实验要求实现NAT节点，完成私网地址与公网地址的转换。其中，又分为SNAT和DNAT，即以公网为目标的数据包和以私网为目标的数据包。

1. **实验思路与代码实现**

分析数据结构，可知需要实现的NAT节点拥有一个内部iface和一个外部iface，每个iface对应许多端口。观察给定的nat\_translate\_packet函数可知，对于发到NAT的数据包，需要先判定其方向，然后进行相应的地址转换。如果是IN方向，即目标地址是一个公网地址，则需要通过转换将目标转为私网地址；如果是OUT方向，即源地址是私网地址，则需要将源地址转换为公网地址。

首先，实现方向判断函数。根据讲义，判断源/目的地址是内部地址还是外部地址，关键看其转出接口是内部iface还是外部iface。因此，在路由表给定的情况下，有如下判断逻辑：

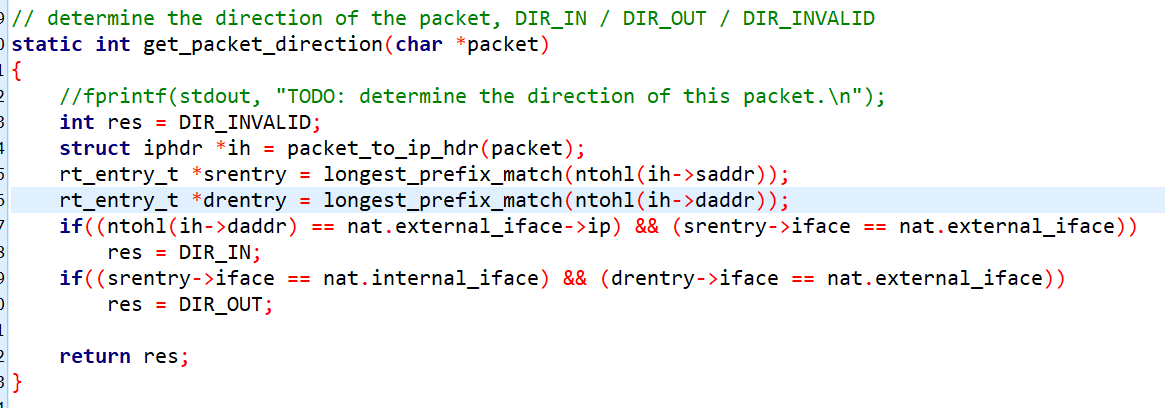


Figure 判断包的方向

如果源地址对应的端口是内部端口，而目的地址对应的端口是外部端口，则方向为OUT，反之为IN。

判断好方向之后，需要根据nat本地的映射关系进行相应的地址转换。我们首先先在数据库中进行该映射的查找：

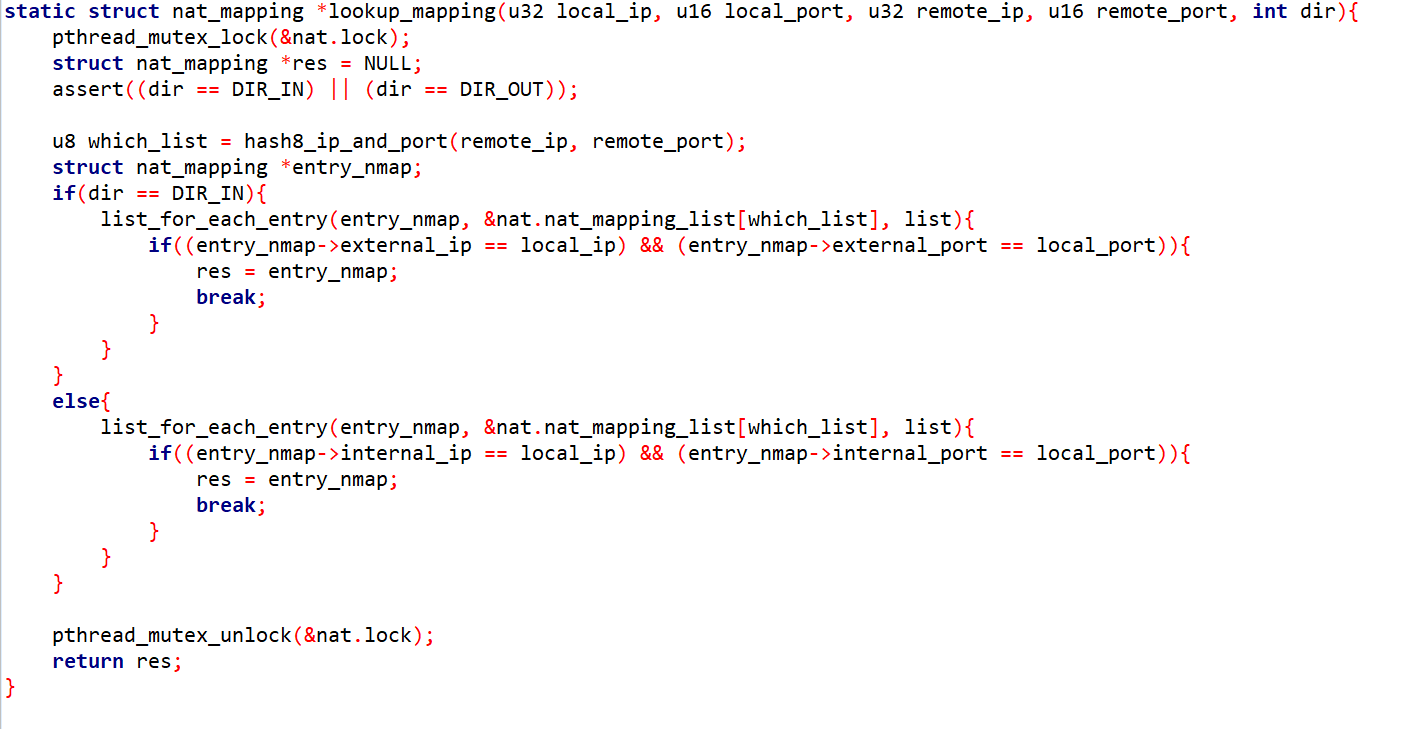


Figure 在数据库中查找映射关系

此查找是一次半hash半遍历查找，先通过remote\_ip与remote\_porthash到对应的链表，再遍历该链表进行匹配。

在第一次发包时，数据库中肯定没有相应的映射关系，所以如果包有TCP\_SYN的tag，就尝试为其建立一个映射。建立映射的过程稍显繁琐，代码就不贴了。具体流程是，如果方向为OUT，就直接申请一个external port与该映射绑定，并将映射加入数据库中。如果方向为IN，首先查找rules，若有对应的规则，就按规则绑定对应的内部端口和ip。

在建立/查找到映射关系后，根据方向的不同，可以相应地改写ip头和tcp头的源或目的。如以OUT为例，将ip头的源ip改为相应外部端口ip，tcp头的源port改为相应外部port，最后重新计算checksum：

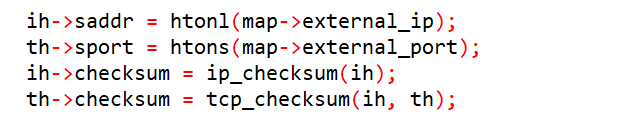


Figure 翻译包头

同时，更新连接状态，存储到conn结构中：

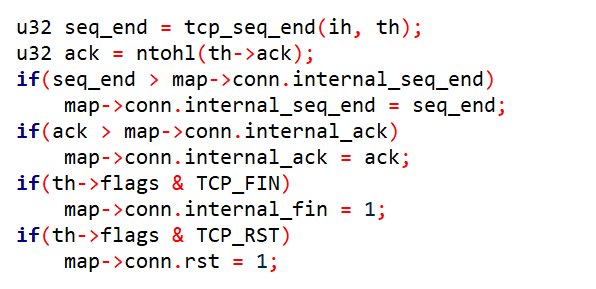


Figure 连接状态更新

至此基本实现完成。

然后，考虑数据库的老化操作，在清扫线程内不断检查连接是否已结束，或连接已超时：

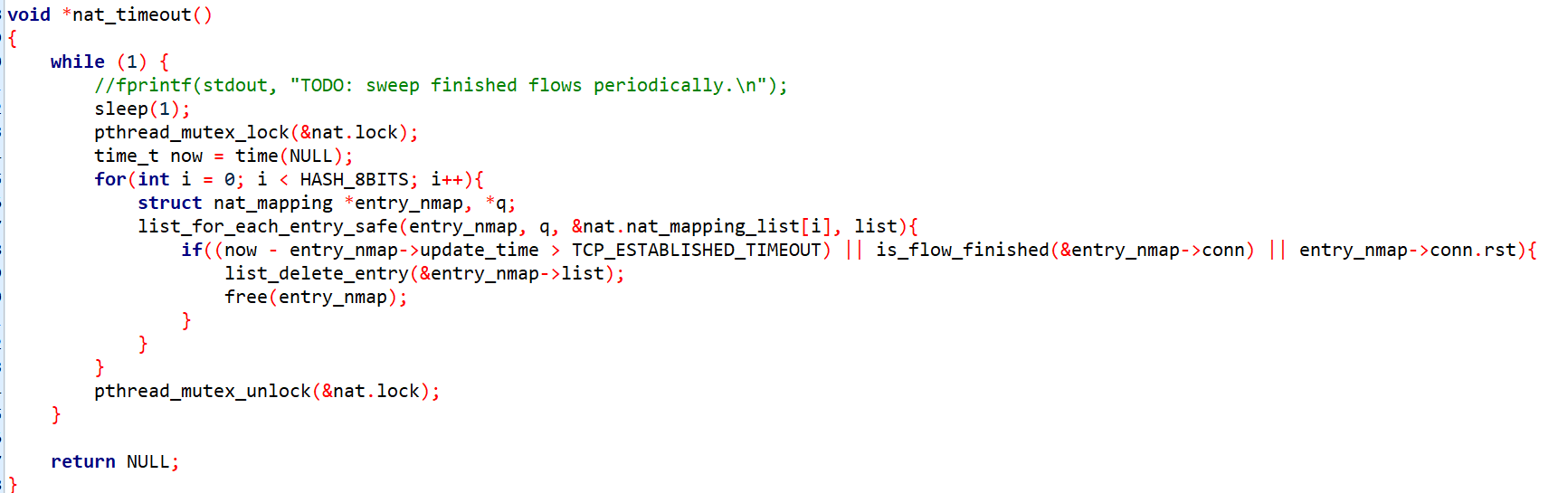


Figure 清扫线程

若需要老化则将该表项去除。

另外，NAT节点的配置（内外端口，rules）需要读取配置文件并解析生成。这项工作没什么建设性，就不放了。

1. **实验结果**

本地首先运行SNAT，h1 h2 wget h3：

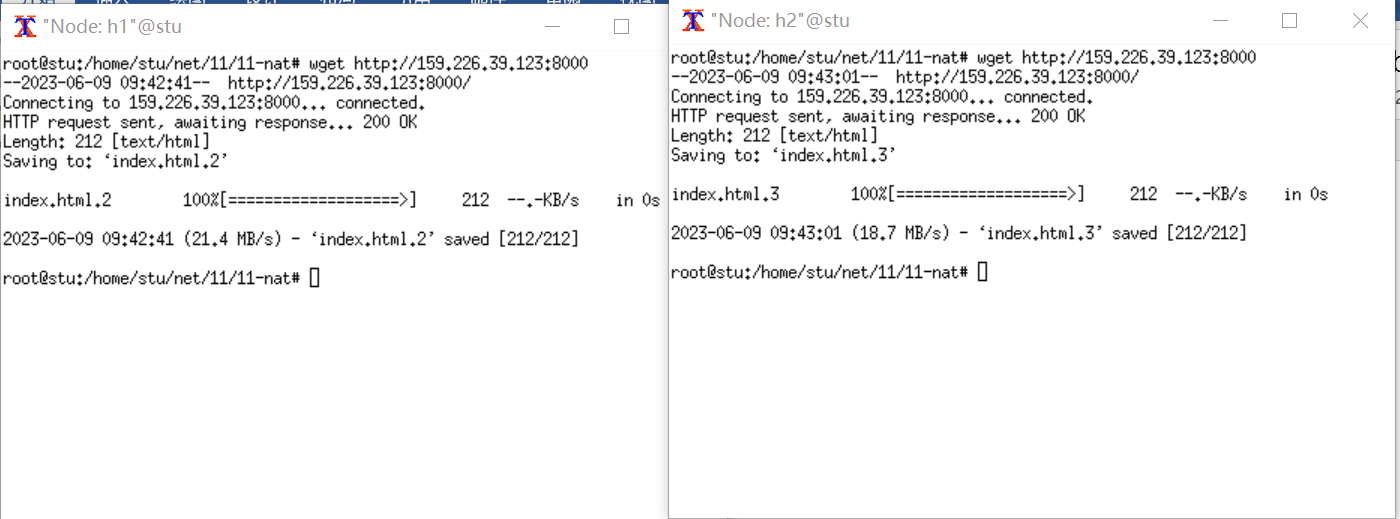


Figure exp1

功能正常。

然后运行DNAT，h3 wget h1 h2：

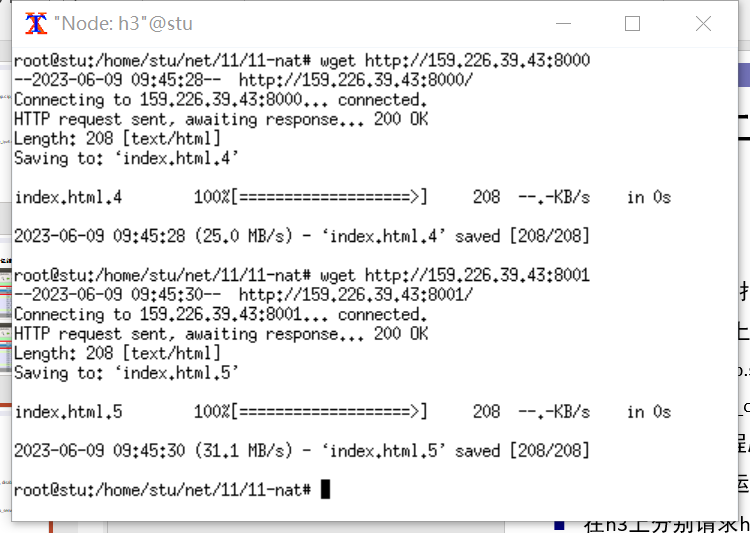


Figure exp2

功能正常。

最后，自行按课件形式构造拓扑，h1 wget n2.external：

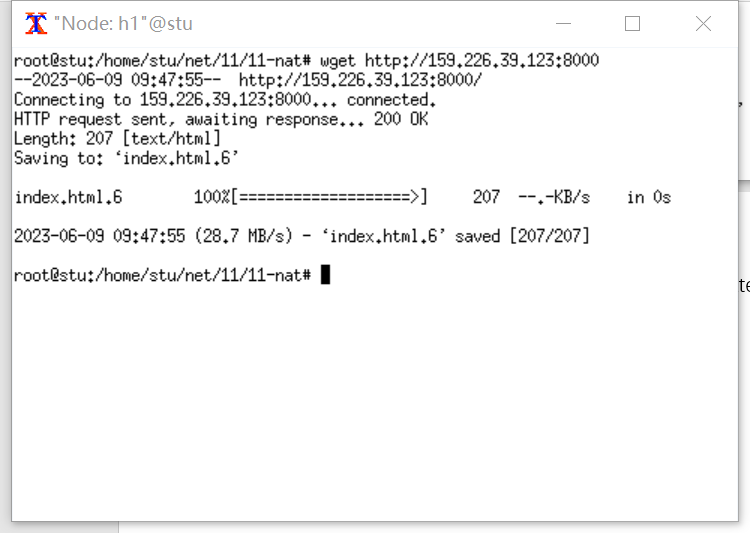
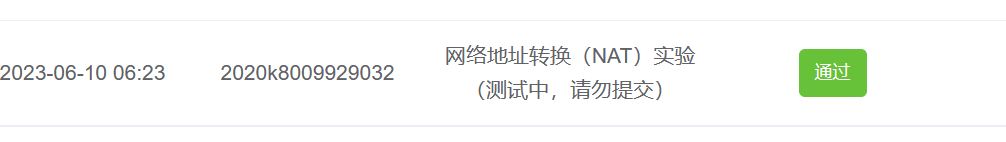


Figure exp3

正常。

oj结果：



1. **思考**

**实验中的NAT系统可以很容易实现支持UDP协议，现实网络中NAT还需要对ICMP进行地址翻译，请调研说明NAT系统如何支持ICMP协议。**

由于ICMP包没有端口的概念，因此NAT设备会根据其identifier字段和源地址为其建立一个伪端口，帮助按通用流程处理。

**给定一个有公网地址的服务器和两个处于不同内网的主机，如何让两个内网主机建立TCP连接并进行数据传输。（提示：不需要DNAT机制）**

使用NAT穿透方法。我们要完成两件事：

1. 每台主机获取自己的公网地址
2. 两台主机交换公网地址

完成后，两台主机都有了对方的公网地址，就可以建立连接。

为完成1，对于每台主机，我们首先向服务器发送一个数据包，申请获知自己的公网地址；服务器收到请求后，由于该请求的源地址就是主机公网地址，所以将公网地址发回给主机。

为完成2，两台主机通过服务器交换公网地址即可。