湖南大學

HUNAN UNIVERSITY

路由与交换机
实验报告

小组成员： 计科1802 张继伟 谢正宇

实验 003 信号的提取

一.实验目的

1、SignalTap II Logic Analyzer 使用方法；
2、掌握捕获条件的设置
3、学会硬件信号分析，了解硬件信号监视和软件调试的差异

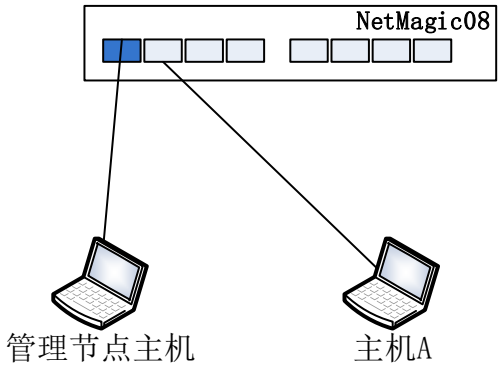
二.实验内容

1、基础要求：上一次在 2 口进 3 口出的基本功能 UM_my/UM.v 模块中设计一个信号量或者直接对信号量 输入端口 in_port 进行监视。
2．设置触发捕获的条件，在某端口有信号进入时捕获数据。
3、利用原有的信号捕获设置，尝试捕获广播包（这里的数据帧头从 139 到 127 位）

138:136 （头尾标识）	135:132 （有效字节数）	131:128 （输入端口号）	127:0 （报文数据）
101	1111	port_num	报文前 16 字节

从 127 到 0 为链路层的帧数据，大家可以查相关资料，了解如何捕获出广播帧。
4、设置条件，尝试捕获 ARP 类型的包，在验收环节和实验报告中描述是否有办法在交换机硬件中防止 ARP 攻击。

三.实验环境



1．1 台管理节点主机；1 台主机 A；（分别连接到 2 口和 3 口）
2． 2 根网线；
3． NetMagic08 开发平台；
4． 软件 Quartus 16。

四.实验步骤

1. 打开 SignalTap II Logic Analyzer。
   a) 如图 1 所示,在 Quartus 的菜单栏选择“Tools”,选择“SignalTap II Logic Analyzer”。
   b) 单击打开 SignalTap II Logic Analyzer 分析器，如图 2 所示。

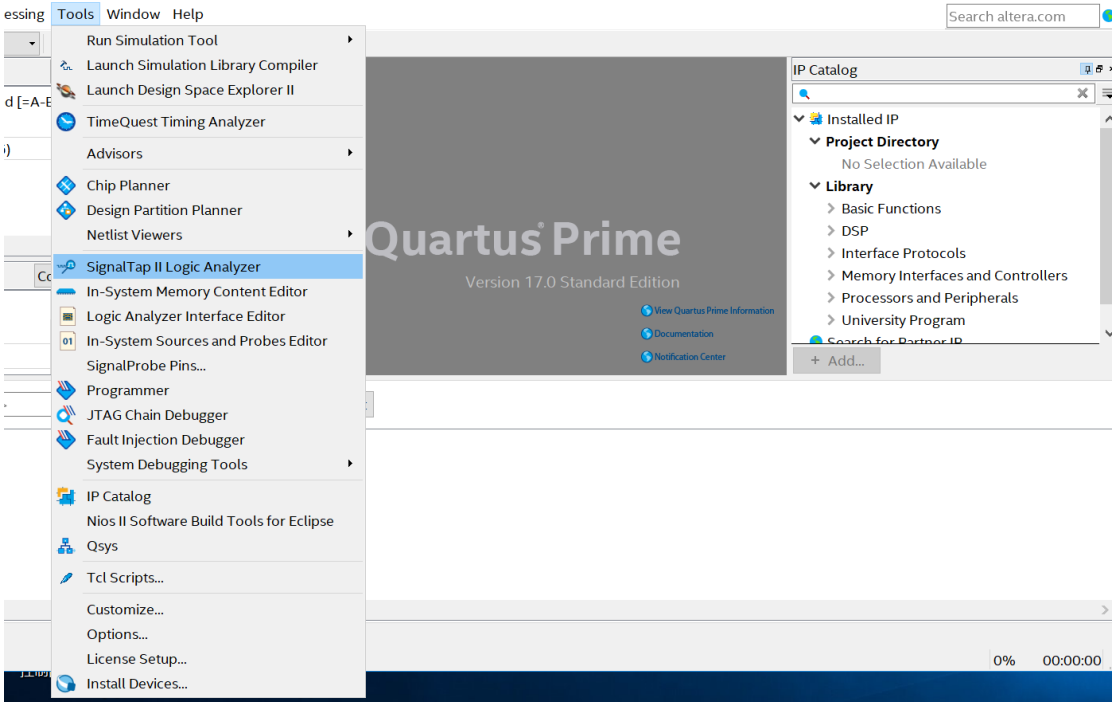


图 1

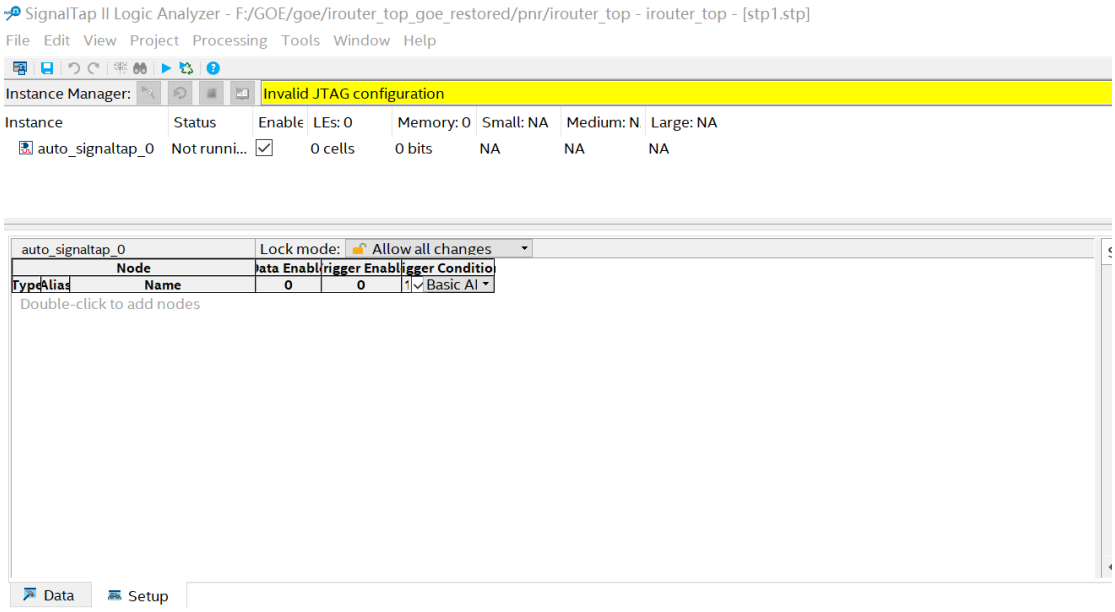


图 2

2. 新建实例
   a) 在 InstanceManager 中右击空白处，弹出菜单选项，选择 “Create Instance” 新建实例，如图 3 所示。

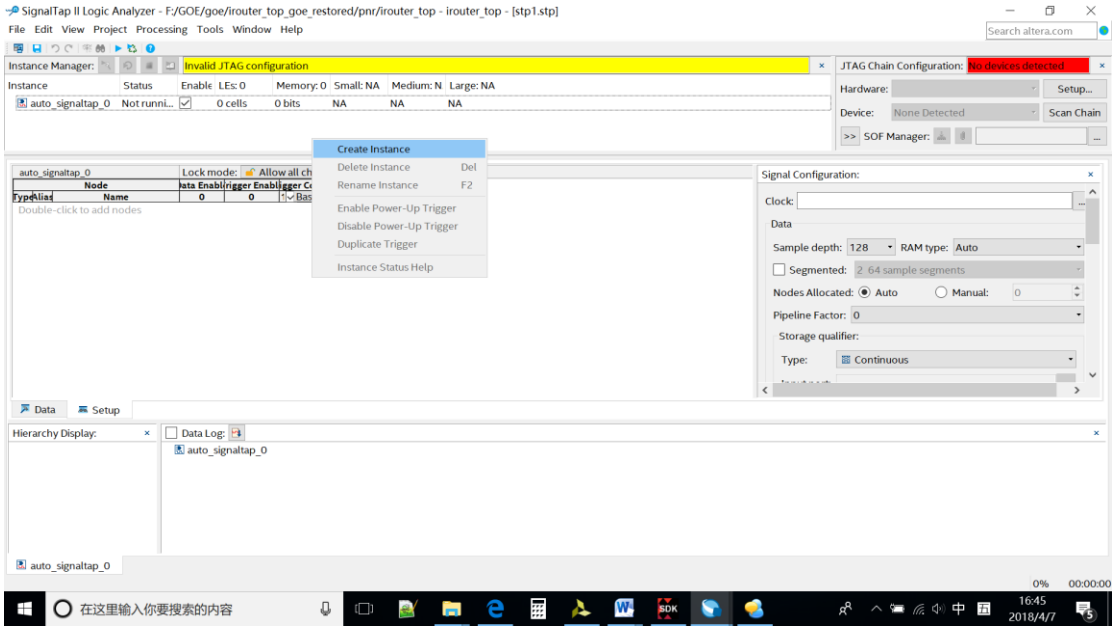


图 3

选中新添加的实例，双击实例对应的文本框，弹出 Node Finder 文本框，如图 4 所示。

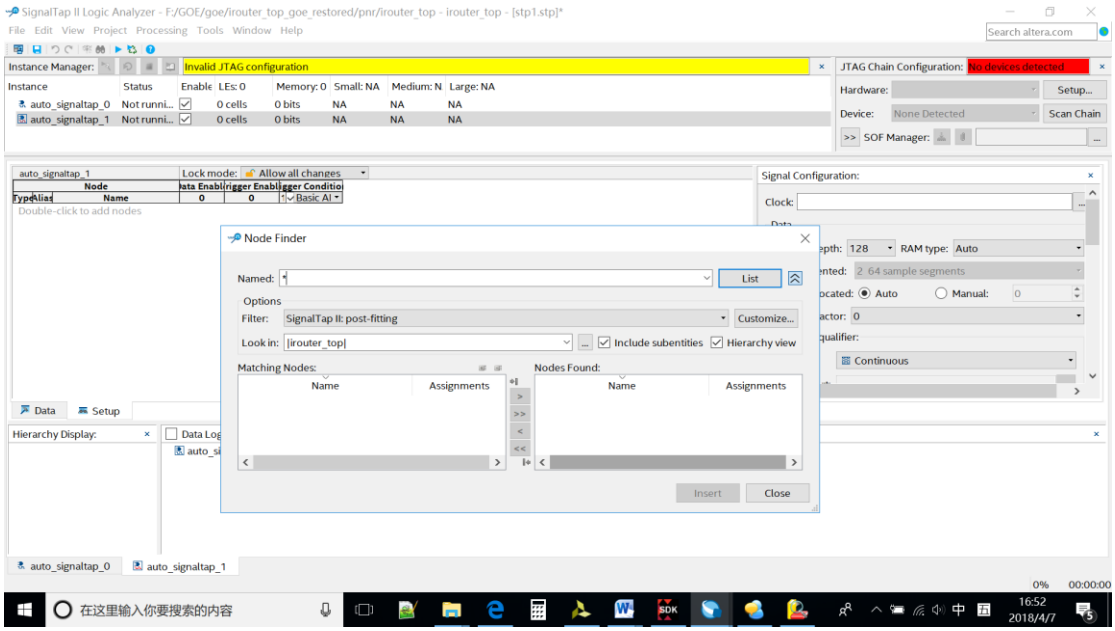


图 4

b) 在 Node Finder 文本框单击 look in 项后的 “…”按钮，如图 5 所示，选择要查看 signaltap 的模块；在 Options Filter 下拉列表框选择过滤信号的选项；Named 为过滤的信号名。然后单击“List”按钮。

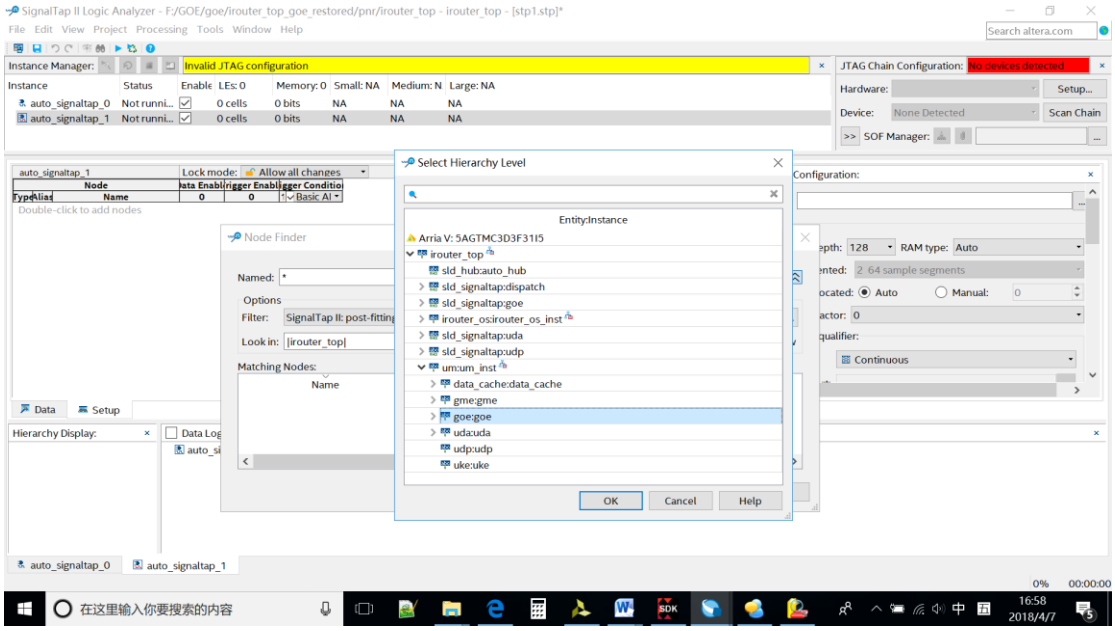


图 5

c) 单击“List”按钮后，匹配的结点就会在 Matching Node 文本框列出，如图 6 所示。

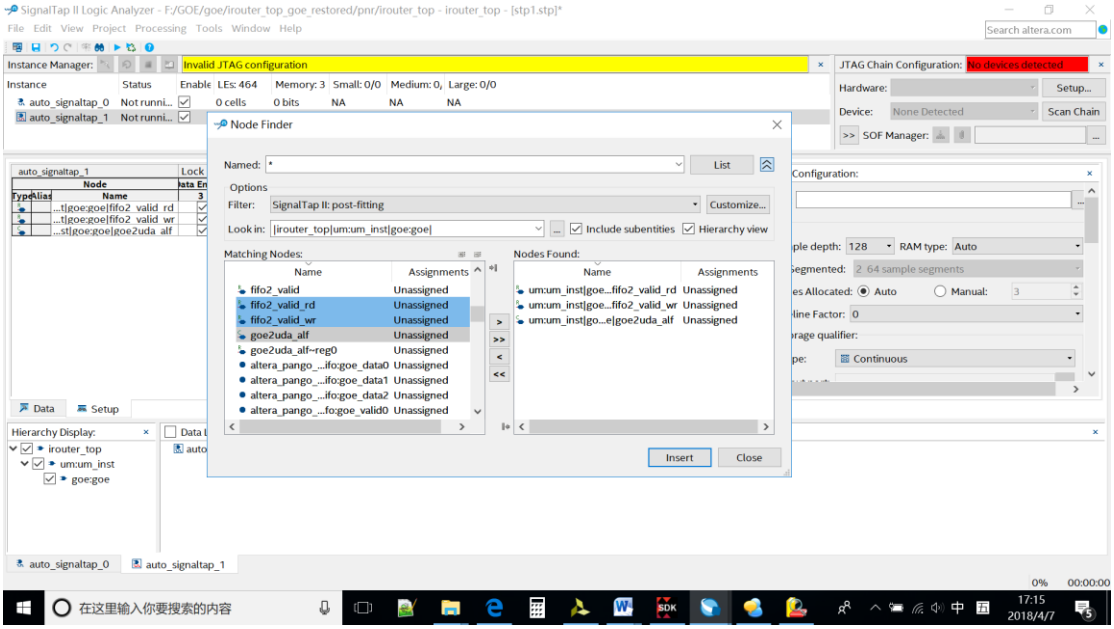


图 6

d) 在左侧的 Matching Node 文本框选中要观察的信号点击中的“>”箭头将其添加到右边的文本框中。

e) 当想要观察的信号全部添加到右文本框后，点击“Insert”按钮将其插入到实例列表框中，点击“Close”按钮关闭 Node Finder 文本框，如图 7 所示。

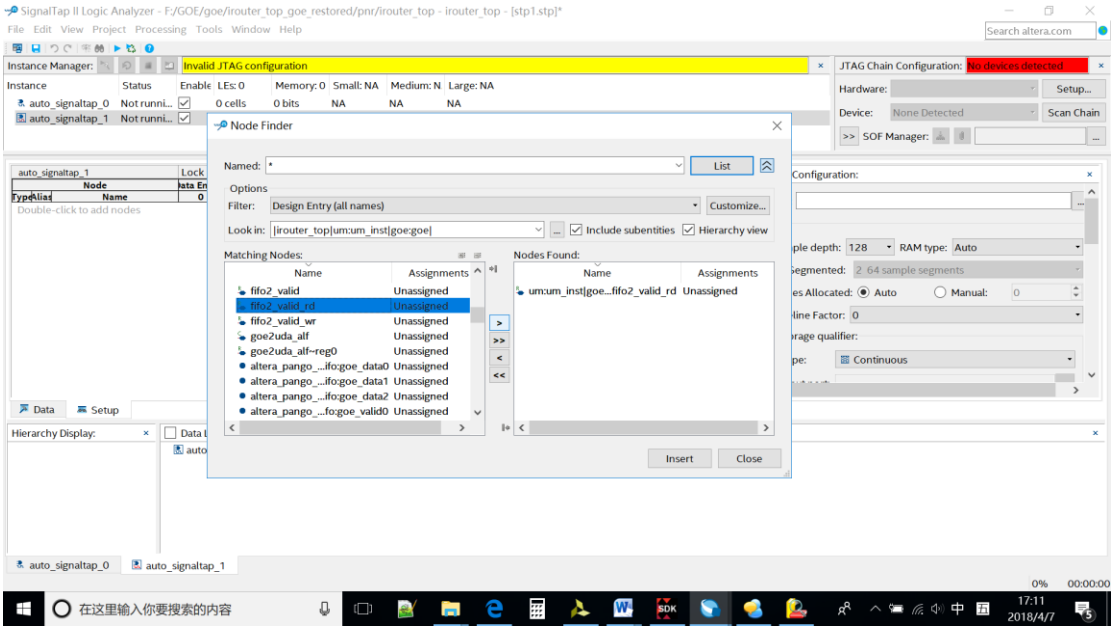
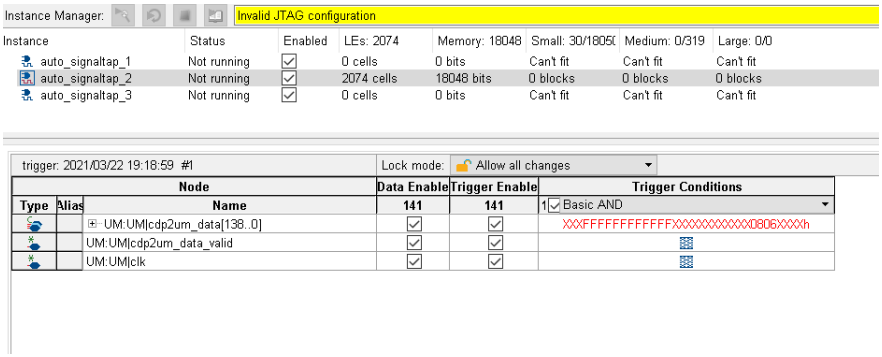


图 7

f) 添加完信号之后，需要添加信号的采样时钟信号。即在 Singal Configuration 框中选择“Clock”选项的“…”按钮，在 Node Finder 中选择信号的采样时钟。如步骤 c-f。Ps：在我们的设备和工程中时钟信号是 clk。

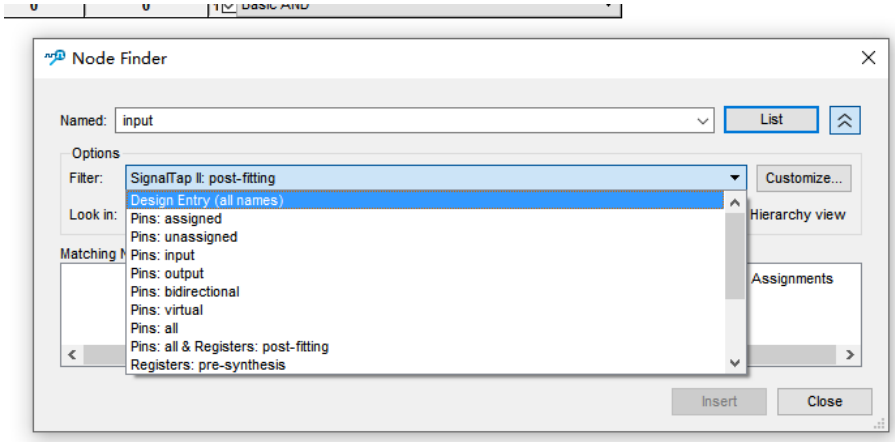
g) 修改 Trigger Conditions



h) 保存 Signaltap 文件，然后编译工程。

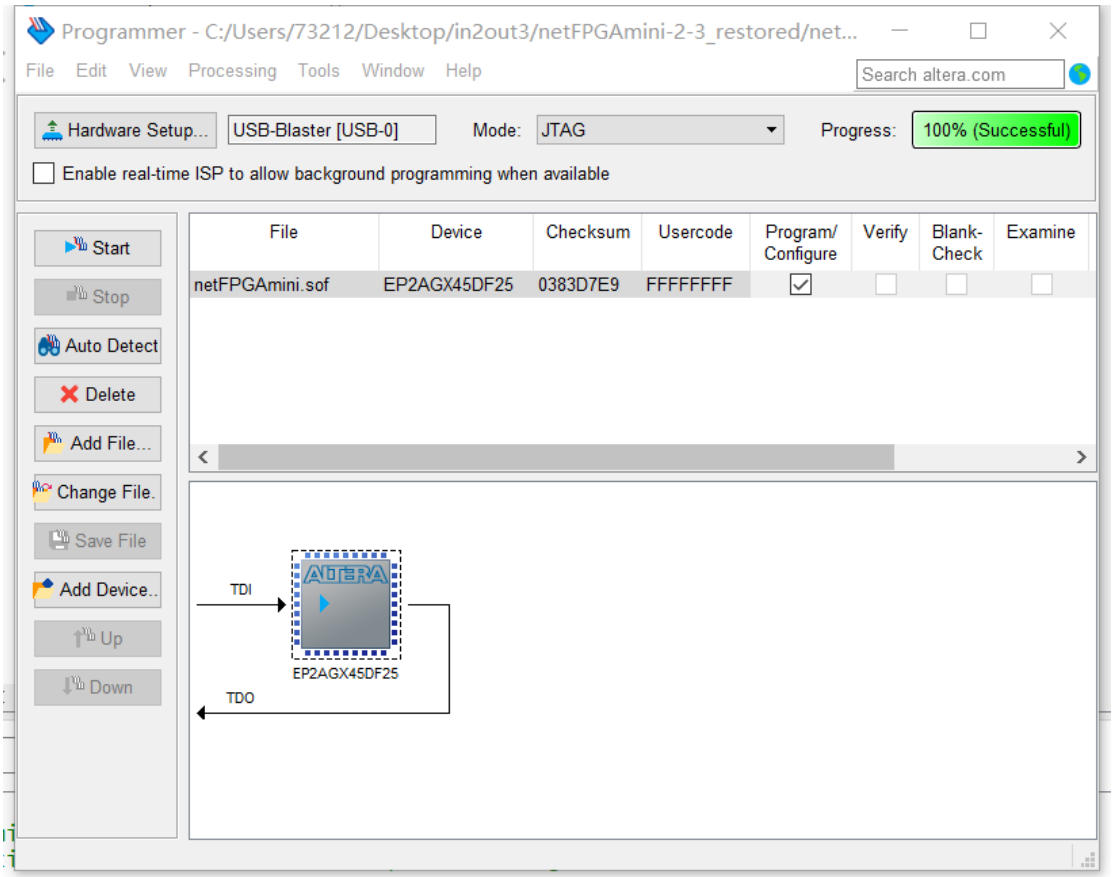
特别注意事项：

一定要在 Filter 中选择 Design Entry(all names)否则会找不到所需信号

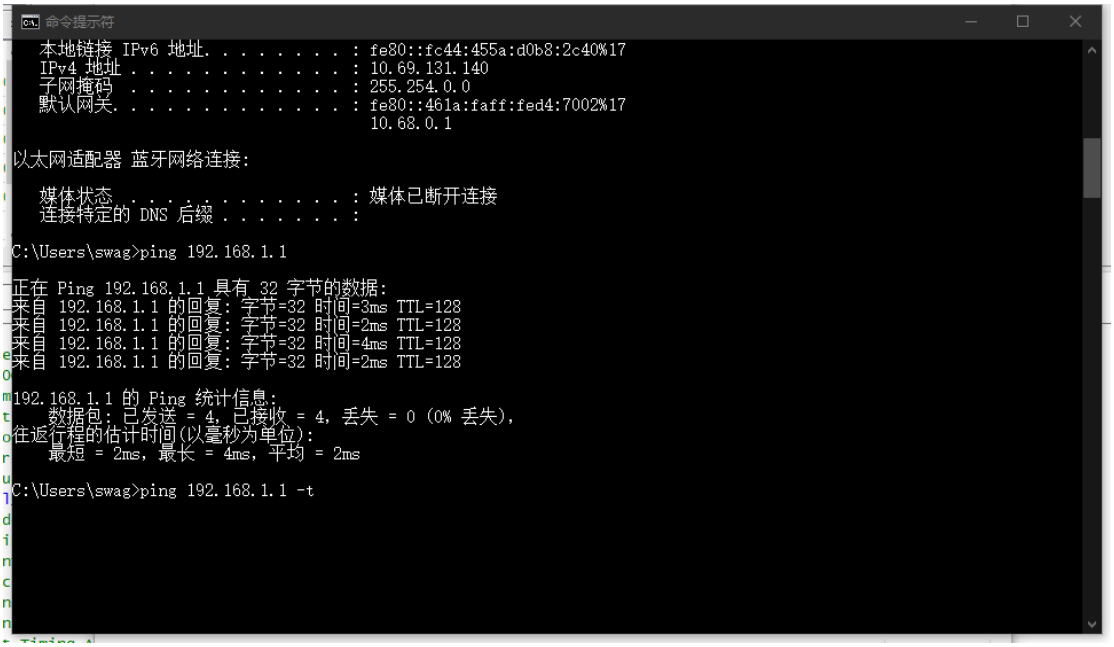


3. 信号提取

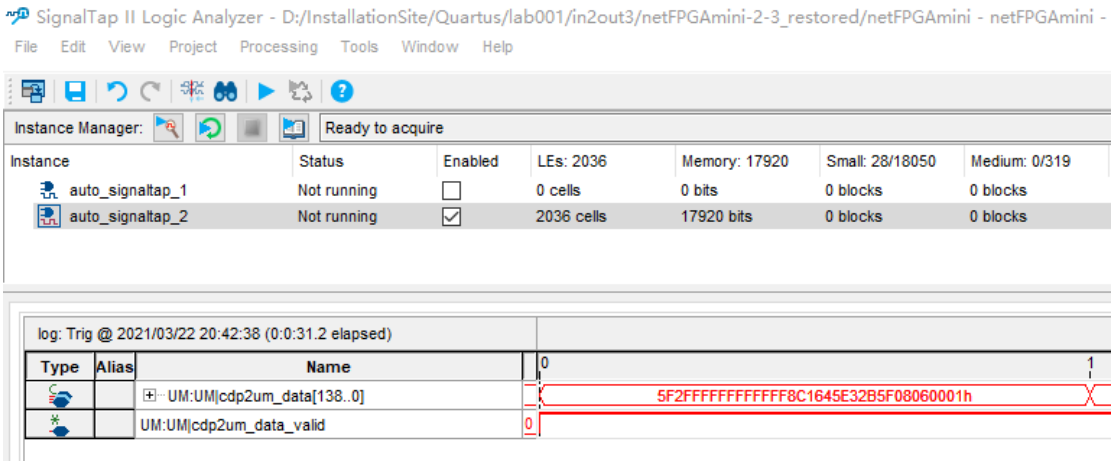
a) 编译成功以后将工程下载到机器中



b) 连接网线，并运行，ping 一个不存在的地址，注意是 2 号端口 ping3 号端口捕获到符合条件的信号后将自动停止，如果没有自动停止的话，需要一直 ping，一直发送包。



c) 接收成功



5：表示报文的头部标示位，101 报文头部，100 报文中间数据，110 报文尾部

F：表示有效字节数，1111 表示 16 个字节全部有效，1110 表示最高的 15 个字节有效，1101 表示最高的 14 个字节有效，以此类推

2：表示输入端口号，位四位通道号，对应 8 个物理端口，序号为 0-7，序号 8-15 保留不被使用

F：之后连续的 12 个 F 表示 48 位的目的 MAC 地址，这里是一个广播地址

8C1645E32B5F：代表源 MAC 地址，这里是从 3 号端口返回到 2 号端口的回复报文

0806：代表的是 IP 报文的协议域，这里是 ARP 协议广播报文

0001：代表 IP 报文的头部格式

六.实验思考

1.信号如果没有实际保留意义，在电路设计时会被优化掉，无法在信号分析工具中查看到。如何避免？

SignalTap II 可以通过如下语句对所要观察的寄存器约束，避免其被优化掉：

方法 1： reg[15:0] data; /*synthesis noprune*/

方法 2：(*noprune*) reg[15:0] data;

2.实际的交换机产品中有具备反 ARP 攻击的功能么，如果有列出品牌和型号。如果没有，请简述理由。

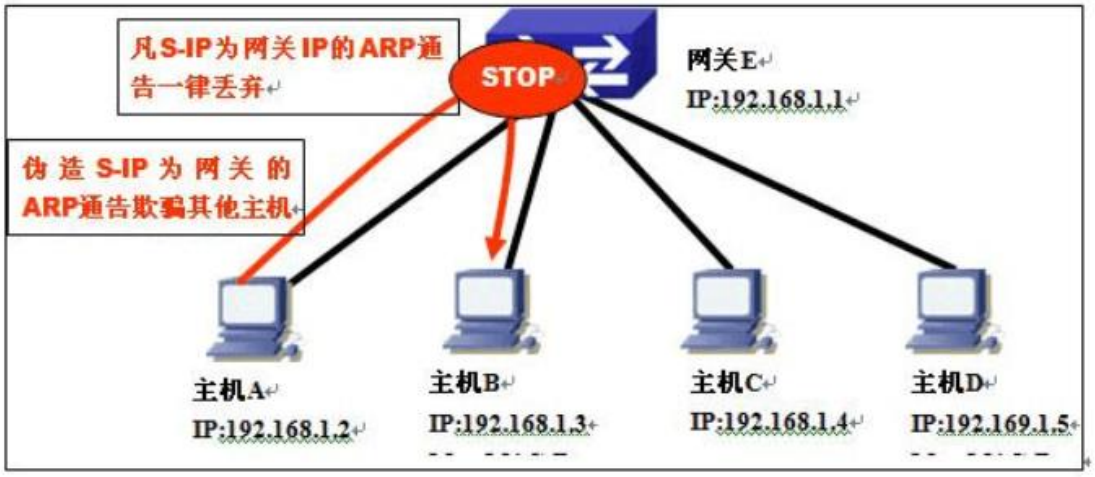
有。如神州数码网络公司从客户端理序、接入交换机、汇聚交换机，最后到网关设备，都研发了 ARP 攻击防护功能，可以通过根据自己网络特点，

选取相关的哪络设备和方案进行实施。如 ARP Guard,基本原理就是利用交换机的过滤表项，检测从端口输入的所有 ARP 报文，如果 ARP 报文的源 IP 地址是受到保护的 IP 地址，就直接丢弃报文，不再转发。

举例:在端口 Ethernet0/0/1 启动配置 ARP Guard 地址 192. 168.1.1（设为网关地址)。

```
Switch(Config)#interface ethernet0/0/1

Switch(Config- Ethernet 0/0/1)# arp-guard ip 192.168.1.1
```



端口 Ethernet0/0/1 端口发出的仿冒网关 ARP 报文都会被丢弃，所以 ARP Guard 功能常用于保护网关不被攻击。

功能优点：配置简单，适用于 ARP 仿冒网关攻击防护快速部署。

功能缺点：需要占用芯片 FFP 表项资源，交换机每端口配置数量有限。

七.实验思考（个人部分单独完成）

这次实验是在上一次实验 2 进 3 出的基础上进行的修改，要求在确定的触发条件下截取广播包。我们通过老师发的实验教程一步一步的使用了 SignalTap II Logic Analyzer 分析器，然后编译文件并烧到盒子里，处处小心谨慎，最终快速的完成了实验。通过本次实验，我认识到了硬件编程的速度慢与硬件编程的小心谨慎，也认识到做实验要一丝不苟，记住每一个要求的细节，否则编译了十分钟的文件最终无法使用，否则只能重新编译。