

** **HUNAN UNIVERSITY**

课程名

实验报告

|  |  |  |
| --- | --- | --- |
|  | 小组成员： | 计科1801孙晶铭，刘怡聪，樊佳婷 |

## 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

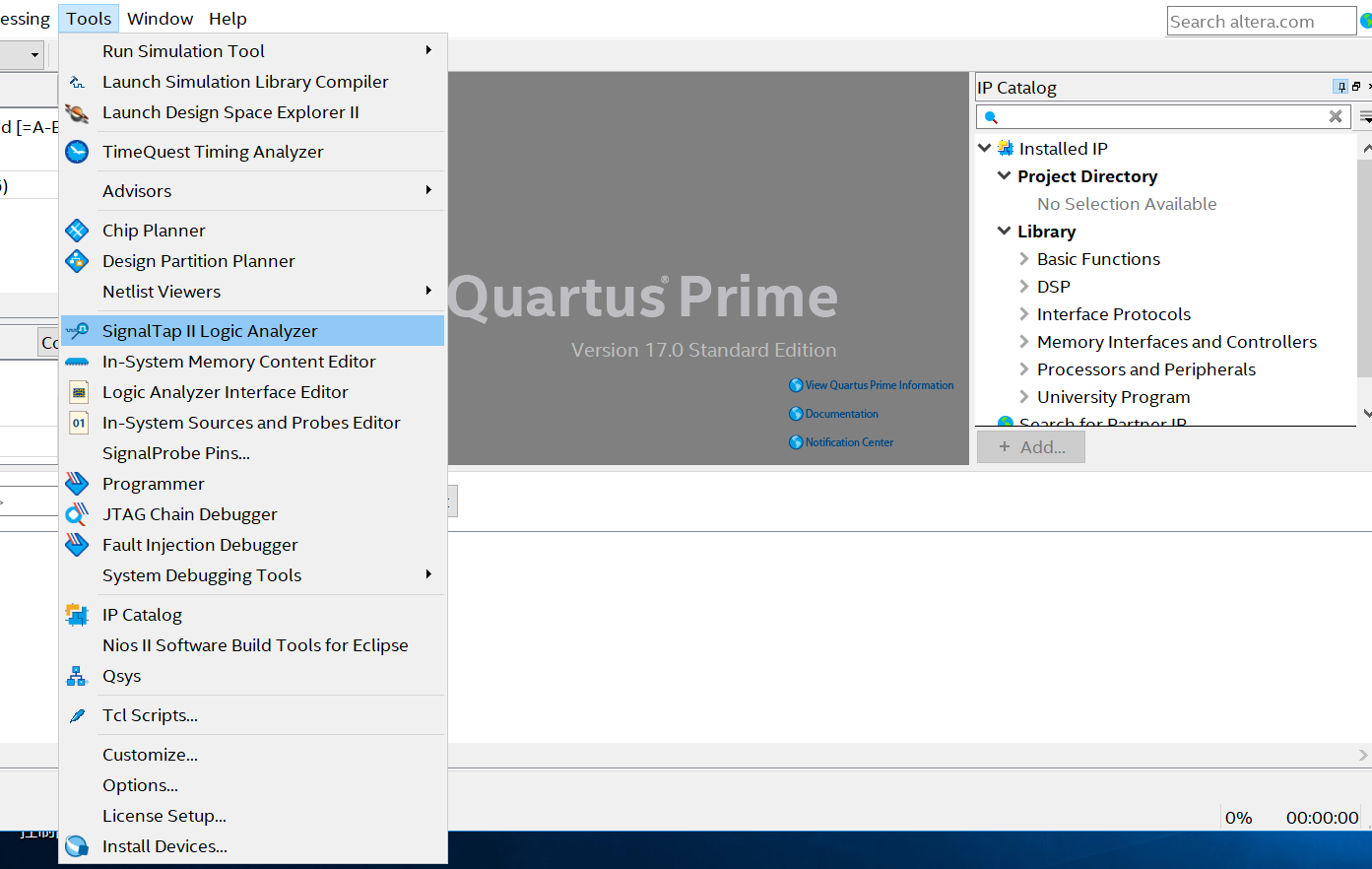


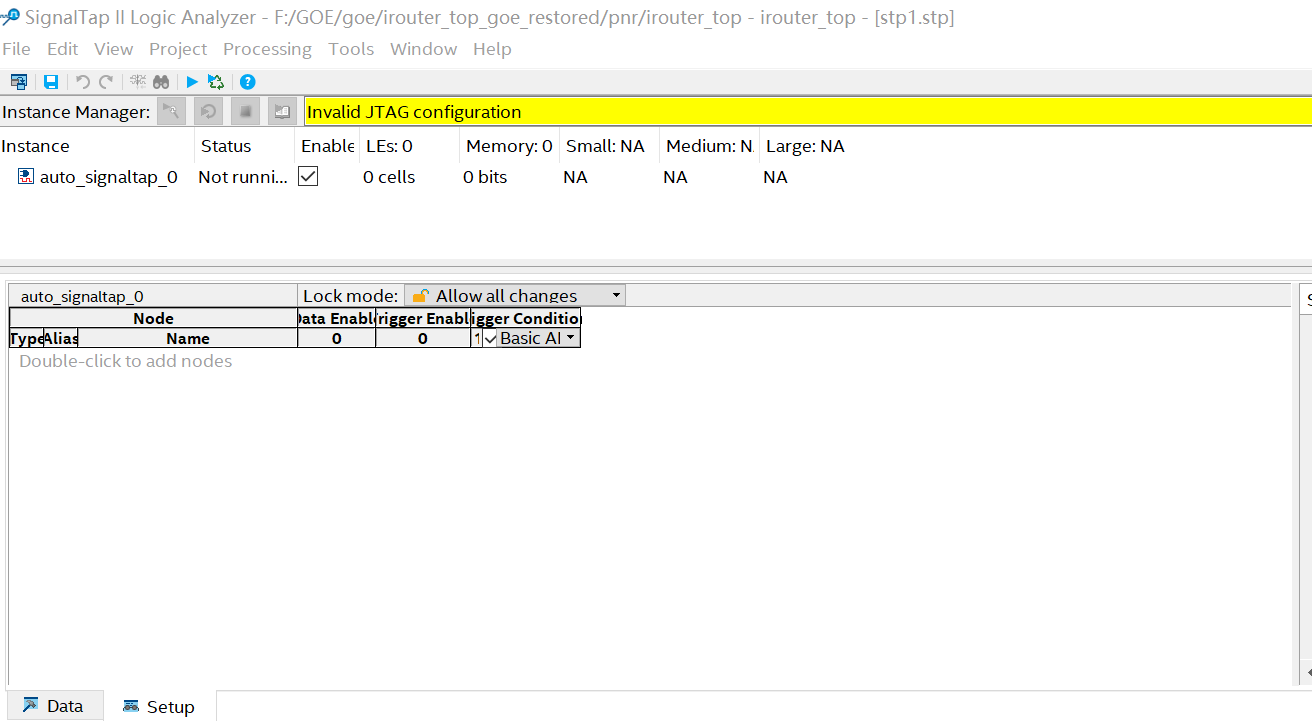
1. 1台管理节点主机；1台主机A；（分别连接到2口和3口）
2. 2根网线；
3. NetMagic08开发平台；
4. 软件Quartus 16。

主机及网络详细配置参照附带的实验环境拓扑及软件配置文档。

### 四、实验步骤

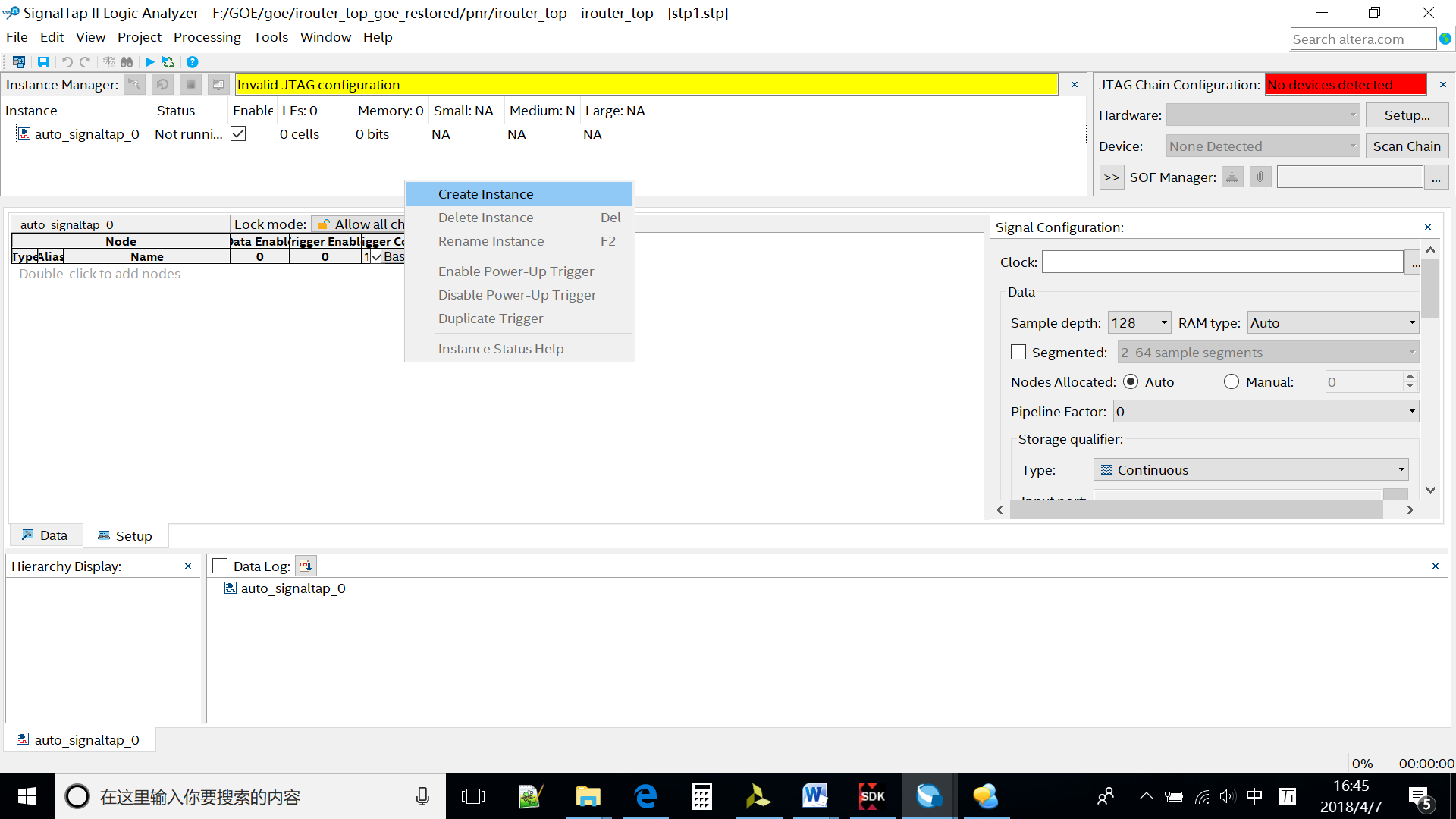
1. 在Quartus中打开实验002的工程文件，打开Tools->SignalTap II Logic Analyzer。



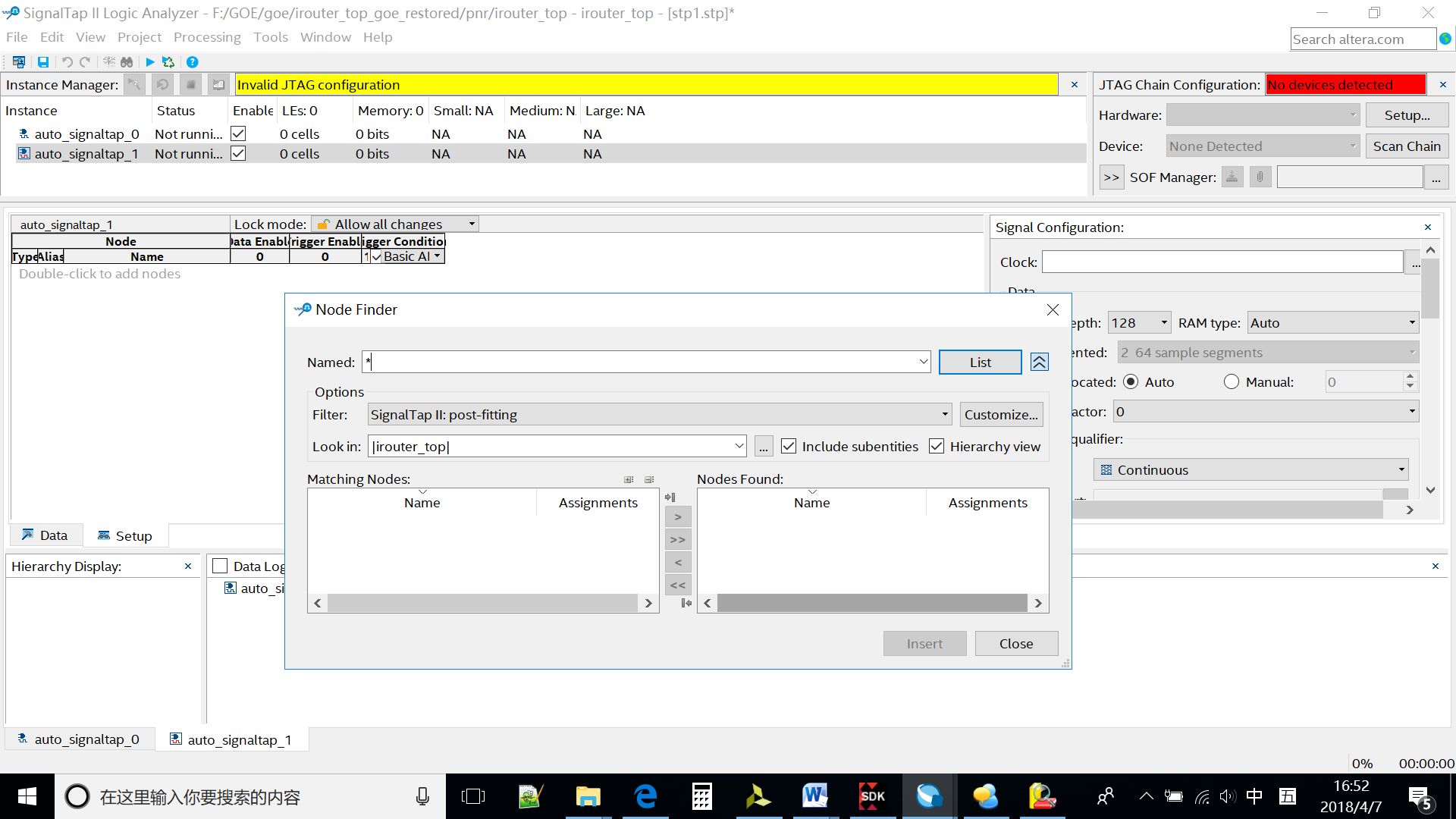


1. 新建实例

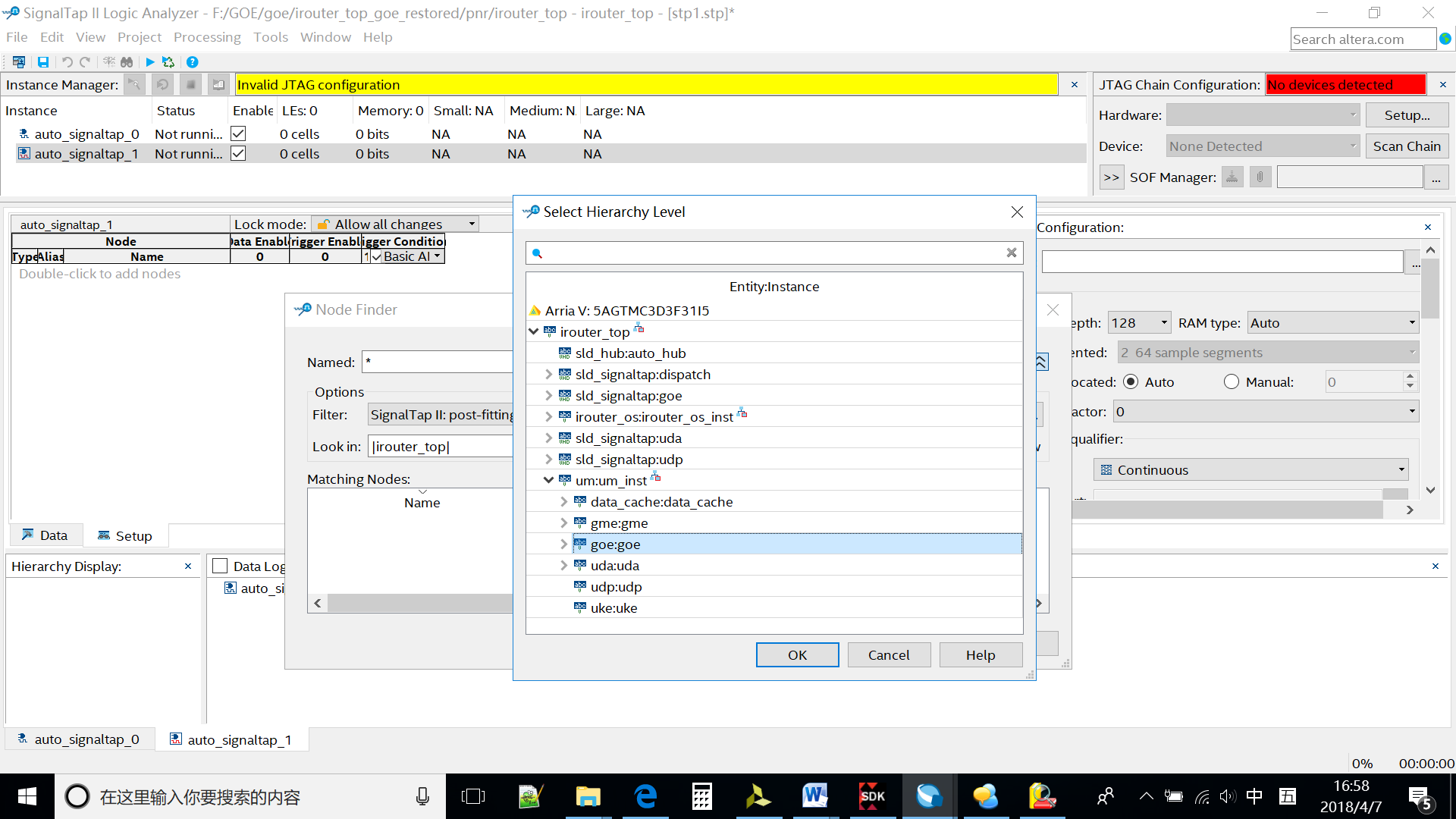
在InstanceManager中右击空白处，选择“Create Instance”新建实例

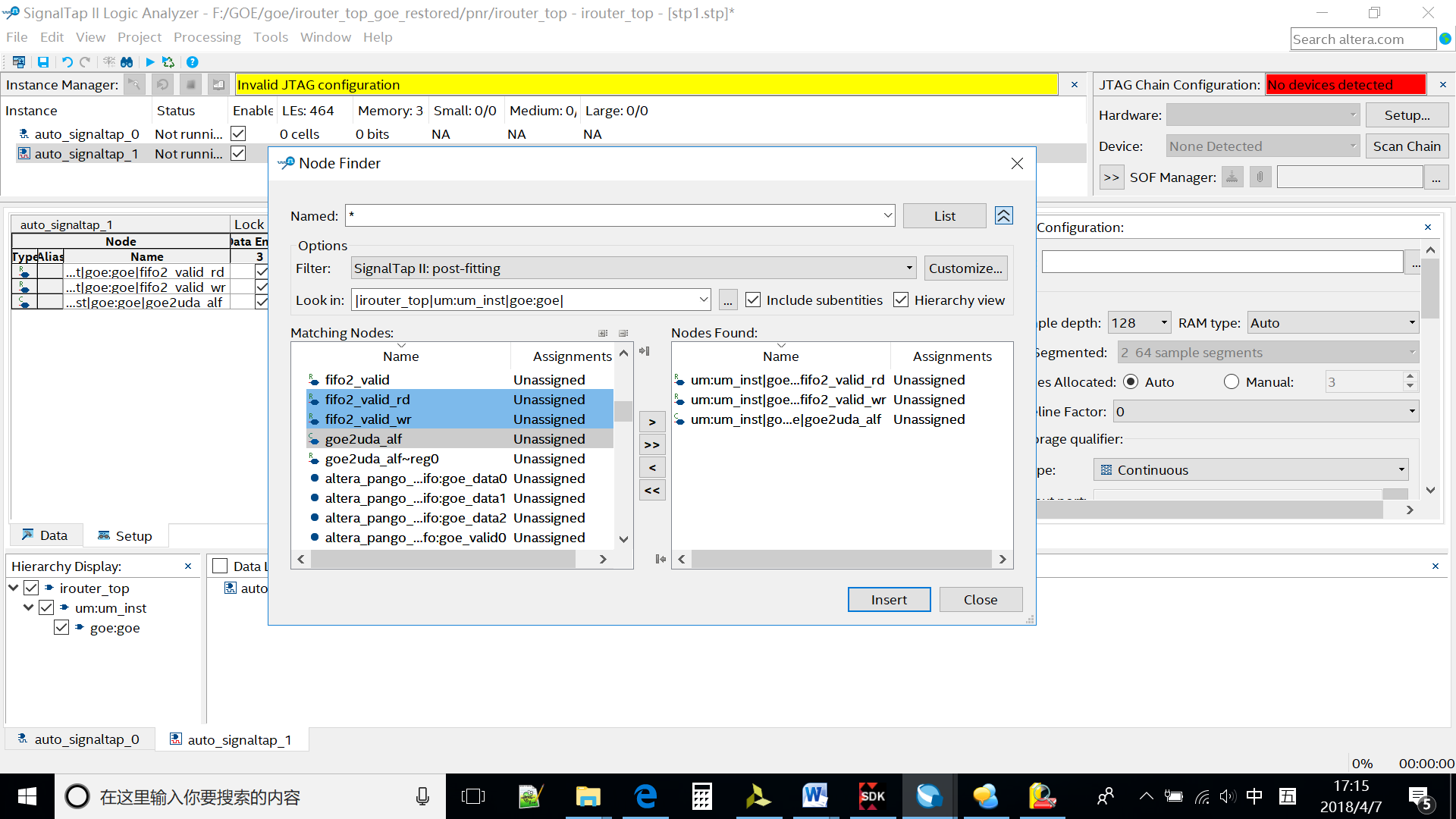


选中新添加的实例，在下方Node处右键，选择Add Nodes后弹出Node Finder文本框



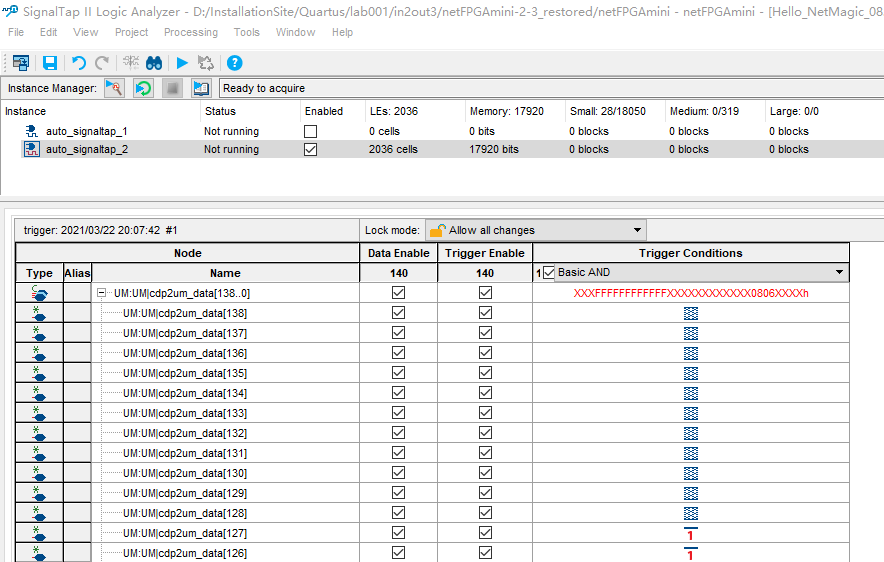
在Named中输入cdp2um\*，Options Filter选择Design Entry(all names)，Look in选择工程下的UM目录，之后点击List选择节点cdp2um\_data和cdp2um\_data\_vaild。



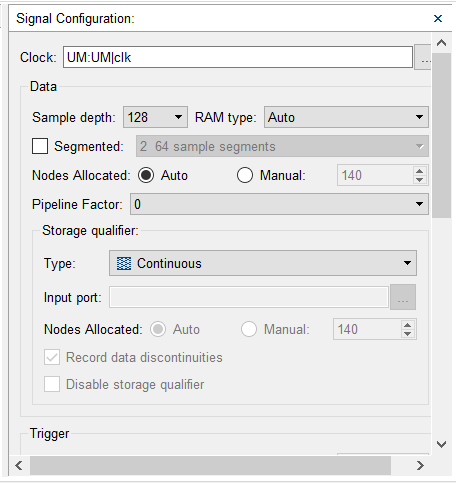


点击“>>”将这两个节点添加到右边的文本框中，点击“Insert”按钮将其插入到实例列表框中，点击“Close”按钮关闭Node Finder文本框。

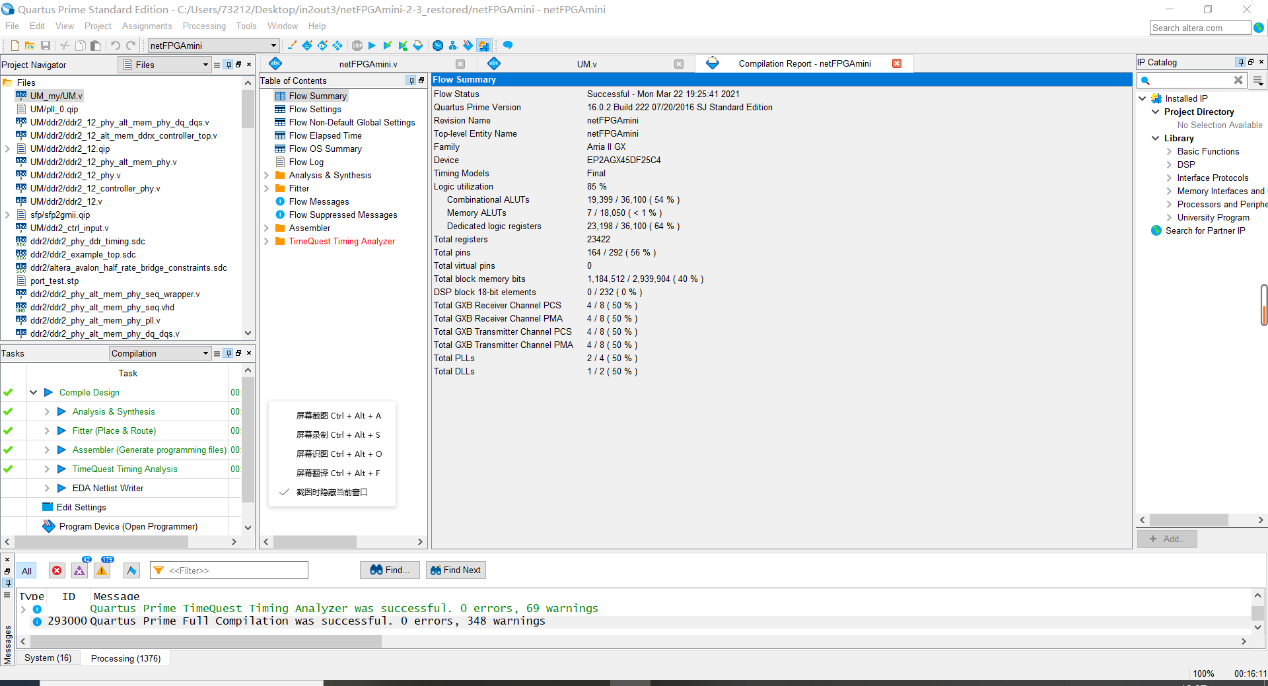
设置cdp2um\_data的80-127位为高电平，FFFFFFFF之后隔12位设置4位0806

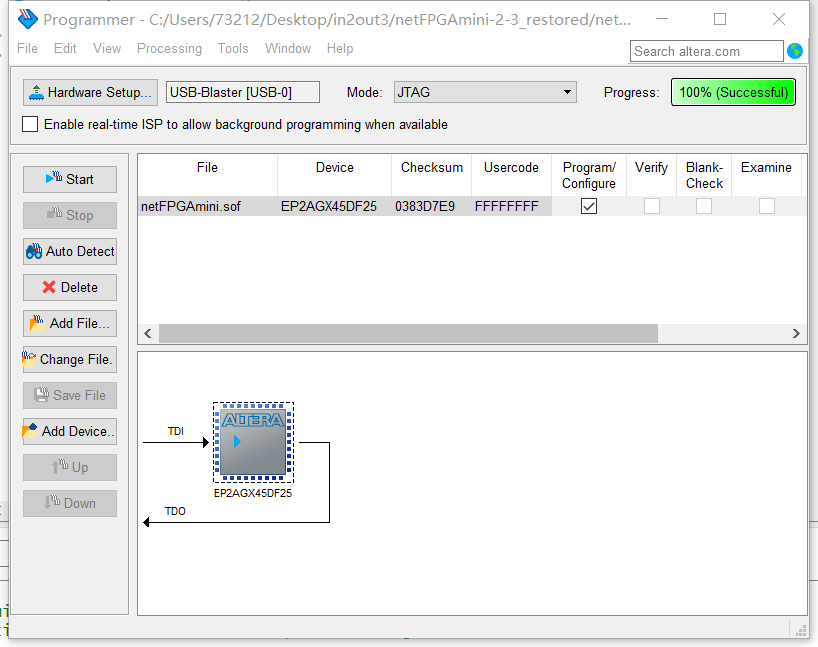


添加完信号之后需要添加信号的采样时钟信号。在Singal Configuration框中选择“Clock”选项的“…”按钮，在Node Finder中选择信号的采样时钟（Options Filter选择Design Entry(all names)，Look in选择工程下的UM目录，之后点击List选择节点）。

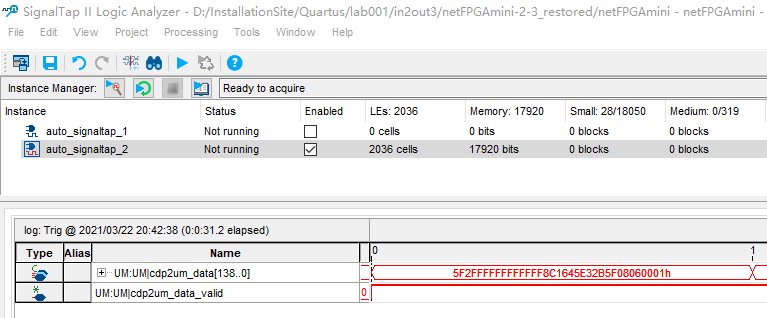


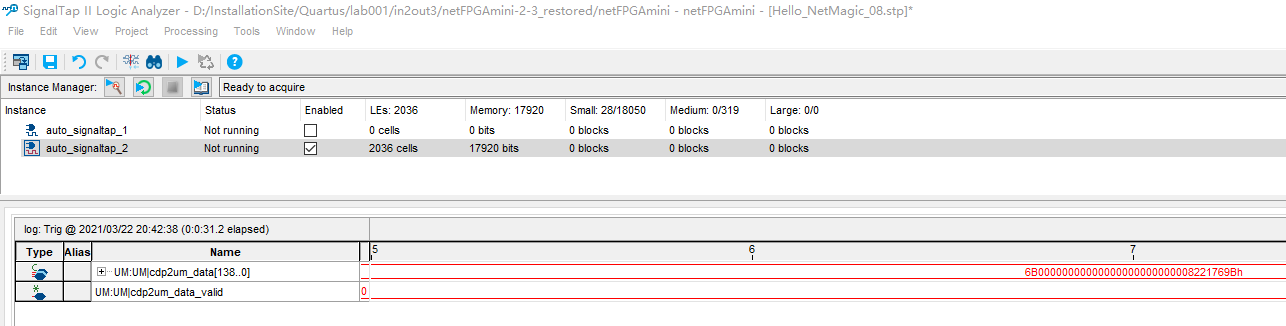
保存Signaltap文件，点击上方的编译按钮编译工程。



成功后使用网线链接NetMagic08盒子烧录工程，烧录成功。

烧录使用的主机连接2号端口，该主机的IP地址是192.168.1.2，另一台主机的IP地址是192.168.1.1，我们在第二台主机上通过ping命令试图连接IP地址为192.168.1.3的“主机”，在第一台主机上可以观察节点的电平变化。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。





0-1时刻的数据为“5F2FFFFFFFF8C1645E32B5F0806001h”，解释如下：

⭐5是报文的头部标示位，101（5）表示报文首部，100（4）表示报文中间数据，110（6）表示报文尾部

⭐F表示有效字节数，这里表示16字节全部有效

⭐2表示输入端口号，四位通道口对应8个物理端口，对应序号为0-7，另外的8-15保留不被使用

⭐之后连续的12个F表示48位目的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2号端口的回复报文

⭐0806是最初设置的cdp2um\_data，代表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

⭐h表示以上数据以16进制显示

### 五、实验验收

项目1验收要求：能观察到条件捕获信号生效，捕获到一个广播报文。

项目2验收要求：捕获到一个ARP协议广播报文。

### 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，无法再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\*/

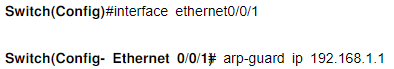
方法2：（\*noprune\*）reg[15:0]    data;

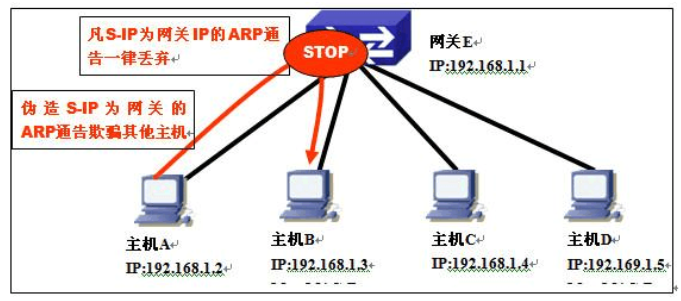
**2、实际的交换机产品中有具备反ARP攻击的功能么，如果有列出品牌和型号。如果没有，请简述理由。**

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)。





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、实验心得

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。在这里第一次使用了SignalTap II Logic Analyzer分析器，我们小组在最初的尝试中忘记了clock要在右侧的Singal Configuration中添加采样信号，导致了一次编译结果错误。第二次又忘记了设置cdp2um\_data的IP报文协议域为ARP广播报文即0806，又导致了结果不符合要求。经过几次修改和三次编译，浪费了很多时间，也认识到做实验要一丝不苟，记住每一个要求的细节，否则只能重新编译，失之毫厘差之千里。