# Tcpdump课堂实践

# 任务要求

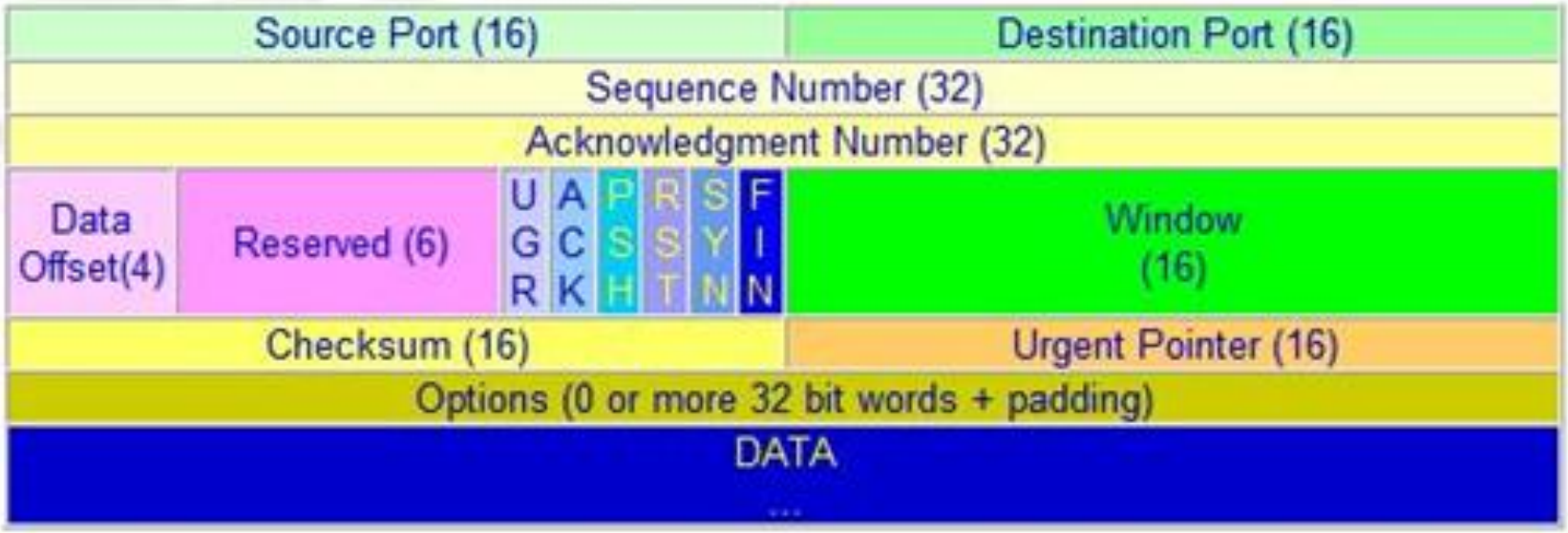
使用tcpdump开源软件对在本机上访问www.tianya.cn网站过程进行嗅探，回答问题：你在访问www.tianya.cn网站首页时，浏览器将访问多少个Web服务器？他们的IP地址都是什么？

# 实践过程--三次握手过程

1. Caller sends SYN
2. Recipient responds with SYN, ACK
3. Caller sends ACK

用tcpdump监测step1 就能看到浏览器发送的请求

# 实践过程—tcp数据包




按照上图所示, TCP[13]即TCP包的第13字节（从第0字节开始计）包含如下八位

| Reserved | Reserved | URG | ACK | PSH | RST | SYN | FIN |
|---|---|---|---|---|---|---|---|

要想得到step1的数据包则需要设定规则 tcp[13]==2

# 实践过程—tcpdump命令

tcpdump –n src *主机IP* and tcp port 80 and tcp[13] == 2

该命令表示捕获所有由主机发出的，SYN位置1，其它位置0的，发往80端口（HTTP）数据包。

# 实践过程—访问网站

打开浏览器，输入网址www.tianya.cn，等待网页载入完成。

# 实践过程—观察tcpdump结果

- 可以看到由主机发往多个ip的握手请求
- 将这些ip汇总
- 有兴趣的同学还可以对这些ip进行ip2location定位