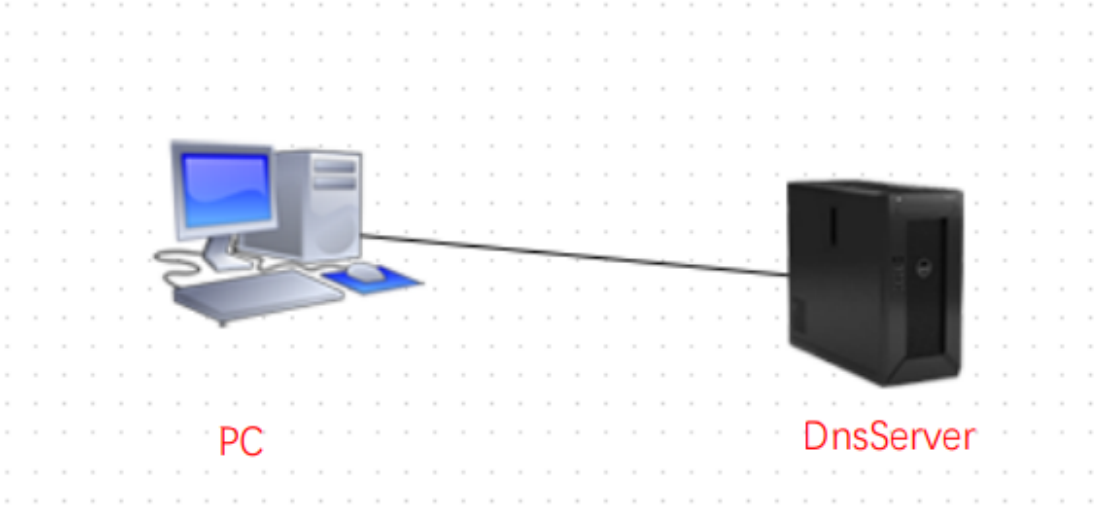
UDP 实验

一、实验目的

1.掌握传输层的 UDP 协议内容；
2.理解 UDP 协议的工作原理；
3.了解应用层协议与传输层协议的关系。

二、实验环境

右上角选择“UDP”，网络拓扑图如图所示，两台主机所在子网网段为“10.3.10.0/24
“，其中一台主机为 Centos7 系统（IP：10.3.10.13），用于搭建一个本地 DNS 服务器；另一台主机为 WinXp 系统（IP：10.3.10.8），用于测试 DNS 服务器和分析 DNS 数据报。（注：子网网段、IP 地址等信息会因具体的实验环境而不同。）



三、实验内容

1.学习 UDP 协议的通信过程；
2.分析 UDP 协议报文格式；
3.学会计算 UDP 的校验和。

四、实验原理

UDP(UserDatagramProtocol）用户数据报协议（RFC768）一种无连接的传输层协议，提供面向事务的简单不可靠信息传送服务。UDP 协议基本上是 IP 协议与上层协议的接口。由于大多数网络应用程序都在同一台机器上运行，计算机上必须能够确保目的地机器上的软件程序能从源地址机器处获得数据包，以及源计算机能收到正确的回复。这是通过使用 UDP 的“端口号”完成的。例如，如果一个工作站希望在工作站 128.1.123.1 上使用域名服务系统，

它就会给数据包一个目的地址 128.1.123.1，并在 UDP 头插入目标端口号 53。源端口号标识了请求域名服务的本地机的应用程序，同时需要将所有由目的站生成的响应包都指定到源主机的这个端口上。

与 TCP 不同，UDP 并不提供对 IP 协议的可靠机制、流控制以及错误恢复功能等。由于 UDP 比较简单，UDP 头包含很少的字节，比 TCP 负载消耗少。

UDP 适用于不需要 TCP 可靠机制的情形，比如，当高层协议或应用程序提供错误和流控制功能的时候。UDP 是传输层协议，服务于很多知名应用层协议，包括网络文件系统（NFS）、简单网络管理协议（SNMP）、域名系统（DNS）以及简单文件传输系统（TFTP）。

UDP 协议结构：

(1)SourcePort—16 位。源端口是可选字段。当使用时，它表示发送程序的端口，同时它还被认为是没有其它信息的情况下需要被寻址的答复端口。如果不使用，设置值为 0。

(2)DestinationPort—16 位。目标端口在特殊因特网目标地址的情况下具有意义。

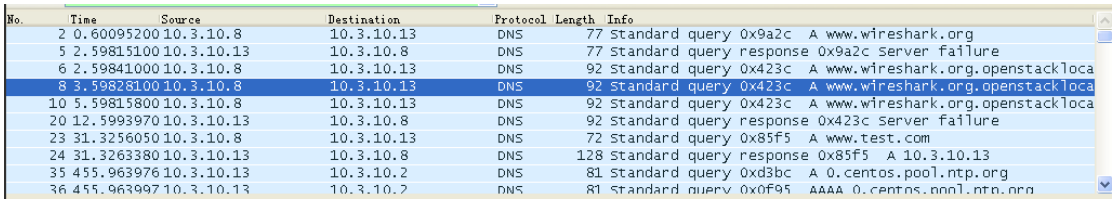
(3)Length—16 位。该用户数据报的八位长度，包括协议头和数据。长度最小值为 8。

(4)Checksum—16 位。IP 协议头、UDP 协议头和数据位，最后用 0 填补的信息假协议头总和。

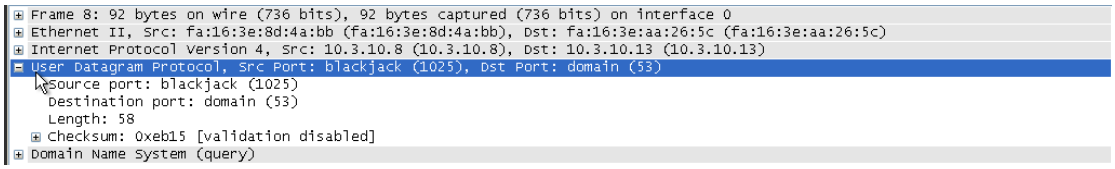
五、实验步骤

1.启动 Wireshark 软件，开始 UDP 报文捕获。请说明你是如何获得 UDP 数据报的，并附上捕获的截图。例如，进行应用层的 DNS 实验，在 windows 端进行抓包就得到了 UDP 数据报。

捕获 UDP 数据报在协议分析界面，可将 filter 一栏填入 udp，则只显示 UDP 协议信息。



2.根据捕获的数据包，分析 UDP 的报文结构。



3.通过分析实验结果，UDP 报文结构由哪几部分组成，其功能是什么？

4.分析 UDP 协议的特点，为什么 UDP 是无连接的、不可靠的协议？

5.计算 UDP 检验和，并与实验结果相比较。