Workshop 7:

解码因特网数据包（2）

1: 数据包解码软件

网络管理员有时需要软件来监管网络中的数据包，管理员甚至需要使用软件来解码数据包，并分析其主要的头部字段。

可以在大多数的Windows和Unix系统中安装包捕获软件。其中一类非常流行的软件是 Berkeley Packet Filter (BPF). Ethereal 和 Tcpdump 这两款应用使用的就是BPF。 在Windows环境下有非常多的包捕获工具，此处不再列举。

我们将会查看一个TCP会话和一组UDP报文交换。在每一部分中，你将会看到如下两个链接：

- 计算机的IP地址已经转换成机器的名字。
- 但是IP地址使用点分十进制表示法，并且没有字符类型的机器名。

开始的时候，你可以查看包含机器名的已经译码的数据包。

1.1 Trace 1: 一个 HTTP 传输

- 使用机器名的解码格式数据包
- 使用IP地址的解码格式数据包

Trace 1 展示了从机器 henry.it.bond.edu.au 到网页 http://www.cs.adfa.edu.au/teaching/studinfo/osrts/index.html. 的HTTP 1.0 请求。因为Bond大学有一个网络代理，所以 henry 无法直接访问服务器 www.cs.adfa.edu.au 的 TCP 80端口，而是必须和网络代理服务器 iris.bond.edu.au 的8080端口建立TCP连接。

这个数据包包含一些初始化包，这些包并不是连接的一部分。你可以忽略数据包1、2、4和5。三次握手连接所涉及的包分别是3、6和7.

在数据包8中，henry 向上述的网页发出请求，并且也识别了请求页面的应用程序（Mozilla/4.76）。Iris 在数据包9中确认了TCP的连接并开始向henry传回网页。

返回的网页太大了，无法完全放入一个数据包中，所以iris 将页面作为数据段放到数据包10到30传回去。注意，在数据包10中的有效数据载荷是1460字节，加上IP首部（20字节）和TCP首部（20字节），总共1500字节，可以完整的放入一个以太网帧中。

你可以参考 RFC 1945 来了解 HTTP 1.0 标准的更多内容。

1.2 Trace 2: DNS 查询

- 使用机器名的解码格式数据包
- 使用IP地址的解码格式数据包

Trace 2 演示了一个客户端向DNS服务器发送的若干个请求和从域名服务器得到反馈的情况。通过DNS系统，可以将文本的域名系统（james.bond.edu.au）转换成IP地址（131.245.7.97），反之也是可以的。

注意，和上面的一样，客户端在本次实验中选择的端口号是随意的，但是所有的DNS服务器都

会监听UDP 53端口。

和HTTP不同，DNS传送协议将它一部分的数据以二进制的格式发送出去，从tcpshow中得到的结果是请求/回复中可打印ASCII部分，不可打印的部分用句点代替。

一些DNS记录查询:

Source Of Authority (SOA)	查找给定网络域的主域名服务器
Address (A)	查找给定文本域名对应的IP地址
Mail eXchange (MX)	查找愿意接收发送给特定主机邮件的所有计算机（比如，所有发送到cs.adfa.edu.aucomputer的邮件都会被发送到csadfa）
Canonical NAMEs (CNAME)	将www这样的别名映射为真正的系统名
PoinTeR (PTR)	将一个IP地址映射回它的域名
TEXT (TXT)	一些说明信息

分辨出哪种查询是哪种类型非常困难，但是数据包1好像是对www.ibm.com的A查询，数据包3好像是对hotmail.com域的SOA查询，数据包5看起来是一个对地址130.37.24.11的PTR请求，数据包7应该是一个对bond.edu.au的关于邮件的MX请求。

UDP并不可靠，它也不分割和重装配数据流。因此，没有建立连接阶段：一个数据包作为请求，一个数据包作为应答。UDP 也不会对包进行重传：如果一个应用程序的UDP包丢失了，应用程序必须要能够感知到包的丢失，如果需要的话应用程序会再次对数据包的发送请求。

1.3 作业

根据上面的2个练习来回答下列问题：

1. henry, iris, 和 kirk 的IP地址是多少？
2. henry 的数据链路地址（物理地址）是多少？
3. iris一直在监听的TCP端口号是多少？
4. henry使用的生存周期值（TTL）是多少？
5. 2个服务使用的生存周期值（TTL）各是多少？
6. 在trace 1中，使用了TCP首部的哪些字段来进行确认的捎带。
7. 在trace 1中，从服务器经由iris传回给客户端henry的应用程序数据有多少字节？
8. 你认为从henry 到 iris的链路的最大传输单元 是多少？是如何计算出来的？
9. 在trace 2中，henry 向DNS发送的每次请求使用的UDP端口号相同吗？他的这种端口选择方式和在trace1中henry的端口选择相同吗？

2：总结

作为一个网路管理员，你常常需要专心于数据包解码工作。显然，拥有像Tcpdump和Ethereal这样的包捕获和分析工具是非常必要的。正像我们上面所做的一样，这些类似的工具可以统计出某一协议现在有多少数据包正在通过链路，并且这些工具可以让你有选择的去监听一些协议。

大部分的数据包分析工具的一个缺点是它们无法知道现在使用的每一个协议。比如，当你开始

在本地局域网中去探测以太网帧，帧类型字段Type=BEAF，你会发现包分析器无法获得这个协议的线索。正像前面所看到的，我们可以对IP和TCP首部进行解码，但是在DNS查询中传输的二进制数据无法解码。

为了能够成功的维护和管理任何计算机网路，包捕获和分析工具是必须的。通过它们，你会最终发现在你网络中发生的一切。

3：TCP/UDP练习

3.1 作业

1．当数据链路层将一个帧从一个链路发送到另一个链路的时候，它依靠哪种标识来转发这个帧？（?? ）
a.主机ID
b. IP 地址
c. 域名
d. 物理地址

2．网络中ARP协议的目的是通过给定的（?? ）来查找（?? ）。
a. IP地址, 域名
b. IP地址, 网络号
c. IP地址, 物理地址
d. 物理地址, IP地址

3．下列哪个属于B类IP地址？
a. 230.0.0.0
b. 130.4.5.6
c. 260.0.0.1
d. 30.4.5.6

4．在传输层中使用的UDP数据单元称为（?? ?）。
a. 用户数据报
b. 报文
c. 段
d. 帧

5．应用程序PING发出的是(??)报文。
a. TCP请求报文
b. TCP应答报文
c. ICMP请求报文
d. ICMP应答报文

6．TCP和UDP协议的相似之处是（?? ）。
a. 面向连接的协议
b. 面向非连接的协议
c. 传输层协议
d. 以上均不对

7．传输层可以通过（ ?）标识不同的应用。
a. 物理地址
b. 端口号
c. IP地址
d. 逻辑地址

8．在TCP/IP中，解决计算机到计算机之间通信问题的层次是（？ ）。
a. 网络接口层
b. 网际层
c. 传输层
d. 应用层

9．对于下列说法，错误的是（ ??）。
a. TCP协议可以提供可靠的字节流传输服务。
b. TCP协议可以提供面向连接的字节流传输服务。
c. TCP协议可以提供全双工的字节流传输服务。
d. TCP协议可以提供面向非连接的字节流传输服务。

10．以下关于TCP/IP协议的描述，（ ??）是错误的。
a. TCP/IP协议属于应用层
b. TCP、UDP协议都要通过IP协议来发送、接收数据
d. TCP协议提供可靠的面向连接服务
d. UDP协议提供简单的无连接服务

11．在TCP协议中，建立连接时需要将控制字段中的（？ ）标志位置1。
a. ACK
b. SYN
c. ACK
d. SYN

12．Internet运输层协议包括（?? ）。
a. ICMP
b. TCP
c. UDP
d. ARP

13．对于下列说法，错误的是（ ??）
a. 运输层的作用是在收发双方主机中的应用进程之间传输数据
b. 运输层的作用是在收发双方主机之间传输数据
c. IP层不提供可靠性保障

d. TCP提供可靠性保障

3.2 作业

1. 在因特网中使用物理地址、IP地址和端口号。在因特网体系结构中，它们都属于哪个层？

2. 对比一下，UDP和TCP的特点各有哪些？

3. 解释TCP数据传输为什么是可靠的。

4. 在不使用IP的情况下，TCP能够直接跨越一个网络吗？为什么？

5. P231, 习题5-11

6. P231, 习题5-15

7. P232, 习题5-23