计算机网络“服务+协议”实验教学探索①

张兰芳[1], 年 梅[1], 张书芳[2]

[1](新疆师范大学 计算机科学技术学院 网络信息安全与舆情分析重点实验室, 乌鲁木齐 830054)
[2](新疆呼图壁县农机局, 呼图壁 831200)

摘 要: 针对计算机网络协议教学, 提出了一套实践到理论、实践与理论对比的教学手段. 该教学手段中实践到理论的教学实验利用 VMware workstation 软件搭建实验环境, 配置虚拟计算机, 并在虚拟计算机上配置网络服务, 利用 Wireshark 抓包软件抓取网络服务的协议数据包, 通过对协议数据包的分析, 理解网络协议的工作原理和过程, 同时对网络服务的配置过程和原理有了更进一步的理解. 以 DNS 为例设计“服务+协议”实验, 模拟 DNS 域名解析的递归查询过程, 通过 Wireshark 抓取 DNS 数据包, 分析了解数据包的组织结构和 DNS 协议的工作过程, 加深学生对 DNS 网络协议的理解. 实验证明此种实验教学方法适合高校的实验现状和学生的认知规律, 促进学生积极、主动、快乐的学习.

关键词: 服务; DNS 协议; 抓包; Wireshark;

Computer Network “Service + Protocol” Teaching Exploration

ZHANG Lan-Fang[1] , NIAN Mei[1], ZHANG Shu-Fang[2]

[1](Network Information Security and public opinion analysis Laboratory, College of computer science and technology, Xinjiang Normal University, Urumqi 830054, China)
[2](Xinjiang Hutubi County Agricultural Bureau, Hutubi 831201, China)

Abstract: According to the teaching of computer network protocol, this paper presented a set of practice to theory, practice and theory of comparative teaching methods. In this teaching means, the experiment of practice to theory uses VMware workstation software to build the experimental environment, configures virtual computer, and configures the network services on virtual computer. This means uses Wireshark capture software to crawl the web service protocol packets.Through the analysis of protocol packet, understands the working principle and process of network protocols, and has a further understanding of the principle and configuration of network services. For example in DNS, the work designs “services + protocol” experiment, simulates of recursive queries to DNS domain name resolution. Through the Wireshark grabs DNS data packet, analyses of the organizational structure of the packet and the working process of DNS protocol to enhance the students understanding of the DNS network protocol. Experiments show that this method is suitable for the current experimental status of universities, and suitable for students cognitive law. It promotes the student positive, active, happy learning.

Keyword: service; DNS protocols; packet capture; Wireshark

0 引言

《计算机网络》是计算机本科阶段的必修课, 该课程的有效实施能够使学生熟练掌握计算机网络的体系结构、局域网、广域网、网络互连和 Internet 协议等计算机网络基本原理和网络服务配置技术, 为学生的后续学习和未来工作打下扎实的理论基础和最基本的网络配置操作技能. 目前大多数学校都采用理论、实验课方式来完成《计算机网络》的教学. 理论课上,

① 基金项目: 国家自然科学基金(61163064);新疆师范大学研究生科技创新项目基金(20131204);新疆师范大学网络信息安全与舆情分析实验室资助项目(2013 年)

收稿时间: 2013-10-31; 收到修改稿时间:2013-12-09

教师们大都采用 PPT 给学生讲授计算机网络的原理和配置. 实验课上, 教师们多采用 VMware 软件搭建实验平台完成 Windows 2003 的服务器实验, 采用仿真软件(如: Cisco Packet Tracer)完成交换机、路由器的协议配置实验. 通过这些实验学生们可以形成对理论知识的深入理解, 掌握交换机、路由器等设备的配置方法及各种网络协议的加载配置方法, 但是对各种协议的工作原理、过程、报文的封装却不能十分理解. 这部分知识的掌握是《计算机网络》教学中的难点, 也是学生们学习《计算机网络》的瓶颈.

1　问题的解决

随着计算机网络分析技术的不断发展, 出现了各种网络分析工具, 如 Sniffer, Wireshark 等, 这些工具的出现可以帮助教师在有限的条件下实施网络协议实验. 此外, 我们可以使用 VMware 软件, 在一台物理机上虚拟出多台不同操作系统的计算机, 并在各虚拟计算机上配置各种服务, 如 DNS、DHCP、WWW、FTP 等, 同时在各虚拟机上安装网络分析工具, 在配置或发布测试命令时捕获各虚拟机上数据包, 通过分析捕获的数据包将服务和协议对照结合起来理解, 通过拆分数据包了解数据包的封装、拆分过程和数据包的组成结构, 分析出各种协议的工作过程, 从而掌握各种协议的工作原理. 网络分析工具和虚拟机软件都可以在普通的计算机上安装, 一般的学校计算机实验室都可以提供这些实验功能, 这些条件的具备为网络协议实验的开设奠定的基础. 有了这些基础条件, 接下来关键就是设计出“服务+协议”的实验, 以实验为平台掌握计算机网络服务的配置方法和步骤, 理解计算机网络协议的原理和工作过程.

1.1　Wireshark 抓包软件简介

Wireshark(前称 Ethereal)是一个网络封包分析软件. 网络封包分析软件的功能是撷取网络封包, 并尽可能显示出最为详细的网络封包资料. [1]网络管理员可以使用 Wireshark 来分析检测网络问题, 网络安全工程师可以使用 Wireshark 来检查资讯安全相关问题, 网络协议开发人员可以使用 Wireshark 来测试协议执行情况, 我们可以使用 Wireshark 来学习网络协定的相关知识.

1.2 分析数据包

wireshark 抓包结果窗口分为三部分: 最上面为数据包列表, 用来显示截获的每个数据包的总结性信息; 中间为协议树, 用来显示选定的数据包所属的协议信息; 最下边是以十六进制形式表示的数据包内容, 用来显示数据包在物理层上传输时的最终形式. 使用 wireshark 可以很方便地对截获的数据包进行分析, 包括该数据包的源地址、目的地址、所属协议等. [2] 我们可以设定要抓取的数据包的协议类型来过滤出我们要分析的数据包, 对过滤出的数据包选定某个数据包展开它的协议树, 就能看到该协议的具体信息, 其中包括各个字段的组成结构和每个位所表示的含义.

2　计算机网络“服务+协议”实验设计

我们以 DNS 协议为例, 设计实验配置 DNS 服务, 抓取 DNS 协议数据包, 通过实验掌握配置 DNS 服务的方法和步骤, 通过分析 DNS 数据包理解 DNS 协议工作的原理和过程.

2.1　域名系统 DNS 概述

域名系统 DNS(Domain Name System)是因特网使用的命名系统, 用来把便于人们使用的机器名字转换为 IP 地址. 许多应用层软件经常直接使用域名系统 DNS, 但计算机的用户只是间接而不是直接使用域名系统. [3]用户浏览网页、收发电子邮件等都会使用域名系统 DNS.

DNS 报文格式如图 1 所示, 它由 12 字节长的首部和 4 个长度可变的字段组成[4].

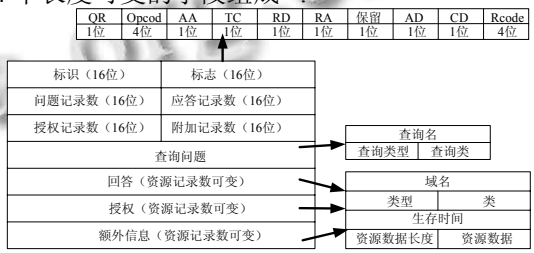

图 1　DNS 报文格式

①标识: 占两个字节, 由客户程序设置并由服务器返回. 客户程序通过它来确定响应与查询是否匹配.

②标志: 16 位的标志字段. QR(查询/响应): 该位为 0 时是查询报文; 为 1 时是响应报文. Opcode: 该位为 0 时是标准查询; 为 1 时响应报文; 为 2 时是服务器状态请求. AA(授权回答): 这是 1 位字段, 当它设置为 1 时, 表示名字服务器是权限服务器, 它只用在响应报文中有效. TC(截断的): 该位只在响应报文中有效, 它表示

响应报文被切割, 因为响应报文过大而无法适用于数据包的数据部分. RD(要求递归): 如果目标名称服务器不包含所请求的信息, 该域表示客户端请求递归查询. RA(递归可用): 该域在响应中有效, 它表示响应名称服务器是否提供递归查询. AD(可信数据): 这位用来指定所有的数据已经被服务器认证. CD(验证无效): 这位指定了没有被认证的数据对于询问者来说是可以接受的. Rcode: 该域长度为 4 位, 用于 DNS 响应中, 表示是否出现错误, Rcode 值为 0 时表示没有差错, 值为 1 时表示报文格式出错, 值为 2 时表示服务器查询失败, 值为 3 时表示名字出错.

③问题记录数: 占两个字节, 表示查询问题包含的条目数量.

④应答记录数: 占两个字节, 表示回答部分包含的回答记录数, 在查询报文中它是 0.

⑤授权记录数: 占两个字节, 包含在响应报文授权部分的授权记录数, 在查询报文中它的值是 0.

⑥附加记录数: 占两个字节, 包含在响应报文附加部分的附加记录数, 在查询报文中它的值是 0.

⑦查询问题: DNS 查询或响应报文中会有查询部分. 查询名: 表示要查找的名字, 它是一个或多个标识符序列. 查询类型: 表示查询问题时的类型. 最常用的查询类型是 A 类型, 表示期望获得查询名的 IP 地址; 而一个 PTR 查询则请求获得一个 IP 地址对应的域名. 查询类: 表示查询的类别. 其值通常是 1, 表示 Internet 类型.

⑧回答(资源记录数可变): DNS 响应报文中会有回答部分. 回答部分包括从服务器到客户(解析程序)的回答. 域名: 表示当中资源数据对应的名字. 它的格式和查询名字字段格式相同. 类型: 表示资源记录的类型. 它的值和查询类型的值是一样的. 类: 表示资源记录的类别. 它的值和查询类的值是一样的. 生存时间: 表示客户程序保留该资源记录的秒数. 资源数据长度: 表示资源数据的数量. 该数据的格式依赖于类型字段的值. 资源数据: 表示该资源数据的内容.

⑨授权(资源记录数可变): DNS 响应报文中会有授权部分, 它为该查询给出关于一个或多个授权服务器的信息(域名).

⑩额外信息(资源记录数可变): DNS 响应报文中会有额外信息部分, 它提供有助于解析程序的附加信息.

2.2 用 Wireshark 抓包分析 DNS 数据包网络结构

我们在主机上安装 Wireshark 软件, 选定主机的接口, 设定过滤 DNS, 启动抓包; 同时启动 cmd 程序, 输入 nslookup 命令进入域名解析交互模式, 在此模式下输入域名 www. 163. com, 将返回该域名的 IP 地址, Wireshark 抓取的 DNS 数据包如图 2 所示.

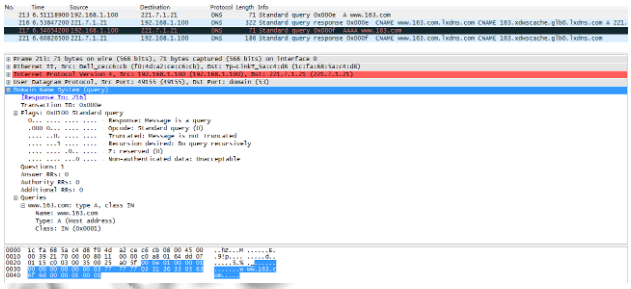

图 2 Wireshark 抓取的 DNS 数据包

第一行是该包的信息, 记录了该包的序号、长度、端口 id、到达时间、时间戳、协议封装(eth:ip:udp:dns)等信息; 第二行是以太网信息, 属于链路层, 记录了目的 MAC 地址、源 MAC 地址, 并指出上一层数据是 IP 数据包; 第三行是 IP 数据包信息, 属于网络层, 记录了源 IP 地址、目标 IP 地址上层的协议号、数据包长度和生存时间等信息; 第四行为 UDP 数据包信息, 属于传输层, 记录了源端口号、目标端口号, 长度等信息; 第五行为 DNS 的有关数据信息, 属于应用层, 展开 Domain Name System(query)显示 DNS 查询报文各个字段的记录信息, 在 Packet Details 面板中可以看到 DNS 数据报的格式, 也可以从底下蓝色的数据看到 DNS 数据包的内容. 根据以上信息, 我们可以画出图 3 所示的数据包结构图, 将抓取的数据包和 TCP/IP 网络数据结构做比较, 可以看出通过 Wireshark 抓包分析的数据结构与 TCP/IP 网络数据结构之间的对应关系.

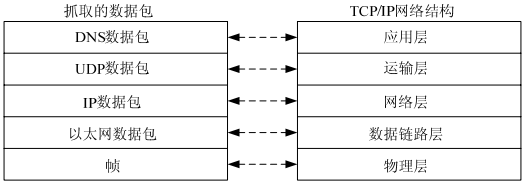

图 3 数据包的结构

2.3 用 Wireshark 抓包分析 DNS 报文

2.3.1 查询报文分析

图 2 中抓取报文的第一行、第三行是查询报文, 我们展开 Domain Name System(query), 显示 DNS 查询报

文的信息, 同时下面蓝色高亮显示 DNS 16 进制数字, 我们把这些 16 进制数字填到图 1 所对应的位中, 就可以了解 DNS 查询报文的含义, 如表 1 所示.

表 1　查询报文分析

标识(16 位)00 0e Response In:216(回应报文在 216)	标志(16 位)01 00 Standard query(标准查询)
问题记录数(16 位) 00 01(1 个问题)	应答记录数(16 位) 00 00
授权记录数(16 位)00 00	附加记录数(16 位)00 00
查询问题 (查询 www. 163. com 的 IP 地址, 类型是 Internet)	

表 1 中查询报文由个 12 字节的首部和 1 个长度可变的字段组成. 第 1、2 个字节是标识位, 数据是 000e, 这是客户程序设置并由服务器返回用来确定响应是否与查询匹配, 该查询报文设置回应报文在 216. 第 3、4 个字节是标志位, 数据是 0100, 转成二进制数是 0000000100000000, 对应到图 1 标志字段, QR=0, 表示该报文是查询报文; Opcode=0000, 表示该报文是标准查询; AA=0, TC=0, 该位只在响应报文中有效, 在查询报文中不予考虑; RD=1, 表示目标服务器在查不到所请求信息的时候客户端请求递归查询; RA=0, AD=0, CD=0, Rcode=0000, 只在响应报文中有效, 在查询报文中不予考虑. 第 5、6 个字节是问题记录数, 数据是 0001, 表示查询问题有 1 条. 第 7、8、9、10、11、12 个字节的值与响应部分相关, 在查询报文中不予考虑. 1 个长度可变的字段是查询问题, 查询名是 www. 163. com, 查询类型是 A, 表示要获得 IP 地址, 查询类是 0000000000000001, 表示 Internet 类型.

2. 3. 2　响应报文分析

图 2 中抓取报文的第二行、第四行是响应报文, 表 2 是响应报文的分析.

表 2　查询报文分析

标识(16 位)00 0e Request In:213(请求报文在 213)	标志(16 位)81 80 Standard response, No error(标准响应, 没有错误)
问题记录数(16 位) 00 01(1 个问题)	应答记录数(16 位) 00 03(三条应答记录)
授权记录数(16 位) 00 05(5 条授权记录)	附加记录数(16 位) 00 05(5 条附加记录)
查询问题(查询 www. 163. com 的 IP 地址, 类型是 Internet)	
回答(资源记录数可变)(列出了 www. 163. com 的 IP 地址、别名记录, 及各条资源记录的类别、生存时间、数据长度)	
授权(资源记录数可变)(列出该查询的授权服务器的域名、记录类型、类别、生存时间、数据长度、域名服务器)	
额外信息(资源记录数可变)(列出域名服务器的域名、类型、类别、生存时间、数据长度、IP 地址)	

表 2 中响应报文由 12 个字节的首部和 4 个长度可变的字段组成. 第 1、2 个字节是标识位, 数据是 000e, 与表 1 中的查询报文相对应, 表示此报文是响应 213 查询报文的响应报文. 我们在图 2 中看到 No. 213 就是表 1 查询报文, No. 216 就是表 2 响应报文. 第 3、4 个字节是标志位, 数据是 8180, 转成二进制数是 1000000110000000, 对应图 1 的标志字段, QR=1, 表示该报文是响应报文; Opcode=0000, 表示该报文是标准查询; AA=0, 授权回答位, 表示名字服务器不是权限服务器; TC=0, 表示响应报文没有被切割; RD=1, 是客户端请求递归查询; RA=1, 表示响应名称服务器提供递归查询; AD=0, 所有数据已经被服务器认证; CD=0, 表示没有被认证的数据对于询问者来说是可以接授的; Rcode=0000, 表示没有差错.

通过表 1、表 2 DNS 查询报文和响应报文的分析, 学生对 DNS 协议内容有更加清楚和直观的理解.

2. 4　用 Wireshark 抓包分析 DNS 域名解析过程

客户主机访问某个网址的过程中包含 DNS 域名解析的过程. DNS 正向域名解析的过程就是客户主机的本地域名服务器把客户主机访问的网址(通常是域名)映射成 IP 地址返回给客户主机. 客户主机(解析程序)向本地域名服务器请求某个域名的 IP 地址一般都是递归查询. 本地域名服务器向根域名服务器的查询通常采用迭代查询, 也可以采用递归查询. 图 4 为客户主机(解析程序)请求某个域名的两种查询过程举例, 其中实线表示递归查询过程, 虚线表示迭代查询过程.

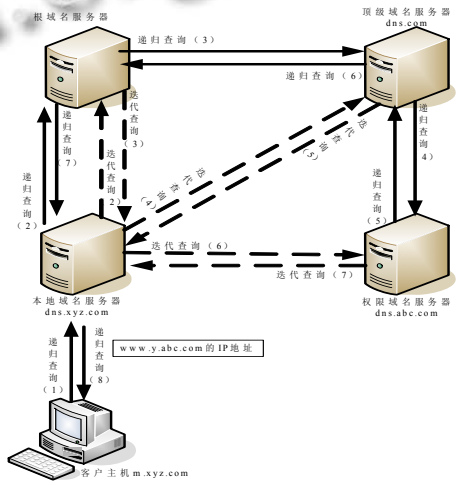

图 4　DNS 域名解析举例: 递归查询、迭代查询

2.4.1 DNS 域名解析过程

我们用图 4 来说明域名解域的过程. 假定域名为 m. xyz. com 的客户主机想发邮件给主机(域名为 www. y. abc. com), 就必须知道主机 www. y. abc. com 的 IP 地址, 下面是查询的过程:

①客户主机 m. xyz. com 向其本地域名服务器 dns. xyz. com 进行递归查询. 如果本地域名服务器采用迭代查询, 则过程如下: ②本地域名服务器先向一个根域名服务器查询. ③根域名服务器告诉本地域名服务器, 下一次应查询的顶级域名服务器 dns. com 的 IP 地址. ④本地域名服务器向顶级域名服务器 dns. com 进行查询. ⑤顶级域名服务器 dns. com 告诉本地域名服务器, 下次应查询的权限域名服务器 dns. abc. com 的 IP 地址. ⑥本地域名服务器向权限域名服务器 dns. abc. com 进行查询. ⑦权限域名服务器 dns. abc. com 告诉本地域名服务器所查询主机 www. y. abc. com 的 IP 地址. ⑧本地域名服务器最后把 www. y. abc. com 的 IP 地址告诉客户主机.

本地域名服务器经过三次迭代查询后, 从权限域名服务器 dns. abc. com 得到 www. y. abc. com 的 IP 地址, 最后把结果返回给发起查询的主机 m. xyz. com.

如果本地域名服务器采用递归查询, 则过程如下: ②本地域名服务器向一个根域名服务器查询. ③根域名服务器继续向顶级域名服务器 dns. com 进行查询. ④顶级域名服务器 dns. com 继续向权限域名服务器 dns. abc. com 查询. ⑤权限域名服务器 dns. abc. com 向顶级域名服务器返回 www. y. abc. com 的 IP 地址. ⑥顶级域名服务器 dns. com 向根域名服务器返回 www. y. abc. com 的 IP 地址. ⑦根域名服务器向本地域名服务器返回 www. y. abc. com 的 IP 地址. ⑧本地域名服务器 dns. xyz. com 告诉客户主机 www. y. abc. com 的 IP 地址.

迭代查询和递归查询都使用了 8 个 UDP 报文完成查询任务. 它们的区别在于: 迭代查询中本地域名服务器进行②—⑦步的查询, 获得查询结果, 在第⑧步把查询结果返回给查询主机; 递归查询中②—⑦的查询在各域名服务器间进行, 获得查询结果, 在第⑧步由本地域名服务器把查询结果返回给查询主机.

2.4.2 在一台物理机上搭建实验环境模拟 DNS 递归查询, 在虚拟客户主机上用 Wireshark 抓包分析 DNS 解析报文

我们在一台物理机上安装四台 Windows 2003 server 虚拟机和一台 windows xp 虚拟机. 四台虚拟机服务器要求安装 DNS 服务并配置正向查找区域、反向查找区域. Windows xp 虚拟机为客户主机, 要求安装 Wireshark 软件. 四台服务器分别模拟本地域名服务器、根域名服务器、顶级域名服务器、权限域名服务器, 实现客户主机访问域名时各域名服务器之间的 DNS 递归查询. 我们在各服务器上配置转发器, 本地域名服务器转发器的 IP 地址是根域名服务器的 IP 地址, 根域名服务器转发器的 IP 地址是顶级域名服务器的 IP 地址, 顶级域名服务器转发器的 IP 地址是权限域名服务器, 在“转发器”配置选项中取消“不对这个域使用递归”选项, 在“高级”配置选项中取消“启用循环”和“禁用递归(也禁用转发器)”选项. 图 5 是 Wireshark 在客户机上捕捉到的 DNS 报文.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.00085800	192.168.88.88	192.168.88.10	DNS	73	Standard query 0x0004 A www.y.abc.com
6	0.00164600	192.168.88.10	192.168.88.20	DNS	73	Standard query 0x390d A www.y.abc.com
9	0.00221400	192.168.88.20	192.168.88.30	DNS	73	Standard query 0x0114 A www.y.abc.com
12	0.00305800	192.168.88.30	192.168.88.40	DNS	73	Standard query 0x387c A www.y.abc.com
13	0.00356200	192.168.88.40	192.168.88.30	DNS	89	Standard query response 0x387c A 192.168.88.110
14	0.00389300	192.168.88.30	192.168.88.20	DNS	89	Standard query response 0x0114 A 192.168.88.110
15	0.00412800	192.168.88.20	192.168.88.10	DNS	89	Standard query response 0x390d A 192.168.88.110
16	0.00426700	192.168.88.10	192.168.88.88	DNS	89	Standard query response 0x0004 A 192.168.88.110

图 5 模拟 DNS 递归查询捕获的报文

从图中可以看到 DNS 递归查询过程. 客户机 192. 168. 88. 88 要查询 www. y. abc. com 的 IP 地址, 首先向本地域名服务器 192. 168. 88. 10 进行递归查询, 本地域名服务器采用递归查询, 它向根域名服务器 192. 168. 88. 20 查询, 根域名服务器再向顶级域名服务器 192. 168. 88. 30 查询, 顶级域名服务器又向权限域名服务器 192. 168. 88. 40 查询, 权限域名服务器查询到 www. y. abc. com 的 IP 地址是 192. 168. 88. 110, 它把结果返回给顶级域名服务器 192. 168. 88. 30, 顶级域名服务器再把结果返回给根域名服务器 192. 168. 88. 20, 根域名服务器再把结果返回给本地域名服务器 192. 168. 88. 10, 最后由本地域名服务器把结果返回给客户机 192. 168. 88. 88. 整个查询使用了 8 个 UDP 报文, 实现了客户主机→本地域名服务器→根域名服务器→顶级域名服务器→权限域名服务器的递归查询.

3 结束语

在《计算机网络》教学中的很多服务+协议的实验

我们都可以采用虚拟机和抓包软件搭建实验环境, 在虚拟机模拟实现各种 Windows 2003 Server 服务(如: FTP、DHCP、WWW 等), 抓包软件抓取这些服务的数据包并进行分析, 在分析数据包的过程中了解各种数据包的组织结构和各种协议的工作过程, 掌握协议的工作原理, 了解 TCP/IP 传输数据的过程. 教学中, 这些

实验可以作为理论课的内容在教师的指导下进行理解, 也可以作为实验课的内容让学生在自己的电脑上实现, 通过实验从实践中总结出理论, 再与教材中原理进行对照学习, 可以达到事半功倍的效用.

参考文献

1 百度百科. Wireshark,http://baike.baidu.com/link?url=W1Su2atwHdLqM0wSTk2QsXPkHdF0VZrPF7lDXUgWsE_fZtFmMs54YEcOwmp1GlRR. 2013-10-22/2013-10-31

2 wireshark 抓包及数据包分析.http://blog.sina.com.cn/s/blog_5fbb094301011p1z. html. 2012-04-11.

3 谢希仁.计算机网络.北京:电子工业出版社,2008.9:224-232

4 蒋一川,王陈章,曹岩,高菲,等.计算机网络实验教学系统 V1.1 实验教程(IPv4 网络协议篇).吉林中软吉大信息技术有限公司.2011.8:162–175

5 朱小明.中等职业学校“计算机网络”实践教学的研究与思考.中国电化教育,2013,2(313):102–105.

6 吴海涛,郭丽红.DNS 协议分析与安全检测.计算机安全,2009,4:24–27