计算机网络

第六章：应用层

阮晓龙

13938213680 / rxl@hactcm.edu.cn
http://network.xg.hactcm.edu.cn

河南中医学院管理信息工程学科
河南中医学院网络信息中心

2017.9

本章教学计划

- 域名系统DNS
- 文件传送协议
- 远程终端协议TELNET
- 万维网WWW
- 电子邮件

常用服务协议

- 动态主机配置协议DHCP
- 简单网络管理协议SNMP

基本网管协议

本章教学计划

- 本章讨论通信服务是如何提供给应用进程来使用的。也就是说，讨论各种应用进程通过什么样的应用层协议来使用网络所提供的通信服务。
- 不同的网络应用的应用进程之间，需要有不同的通信规则。因此在运输层协议之上，需要有应用层协议（Application Layer Protocol）。
- 应用层的具体内容就是精确定义这些通信规则。

本章教学计划

- 应用层协议需要定义的内容有：
  - 应用进程交换的报文类型，如请求报文和响应报文。
  - 各种报文类型的语法，如报文中的各个字段及其详细描述。
  - 字段的语义，即包含在字段中的信息的含义。
  - 进程何时、如何发送报文，以及对报文进行响应的规则。

- 应用层的许多协议都是基于客户-服务器方式。客户是服务请求方，服务器是服务提供方。

1.域名系统DNS

- 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。
- DNS（域名系统）是一种把计算机主机名称解析为对应的IP地址的服务。在Unix和Linux操作系统中的DNS服务称之为BIND（伯克利因特网名称域服务）。
- 许多应用层软件经常直接使用域名系统DNS (Domain Name System)，但计算机的用户只是间接而不是直接使用域名系统。

1.域名系统DNS

- 为什么要使用域名系统DNS呢？
  - 其根本原因在于：IP地址标识的不足。
  - 不便记忆：十进制的IPv4地址仍然比较长，远没有以字符串命名的DNS名称好记。
  - 不便地址变更：每次更改服务器地址都要更改IP地址的话，是很难做到的。
  - 不安全：IP地址一旦对外公布的话，很容易受到攻击。

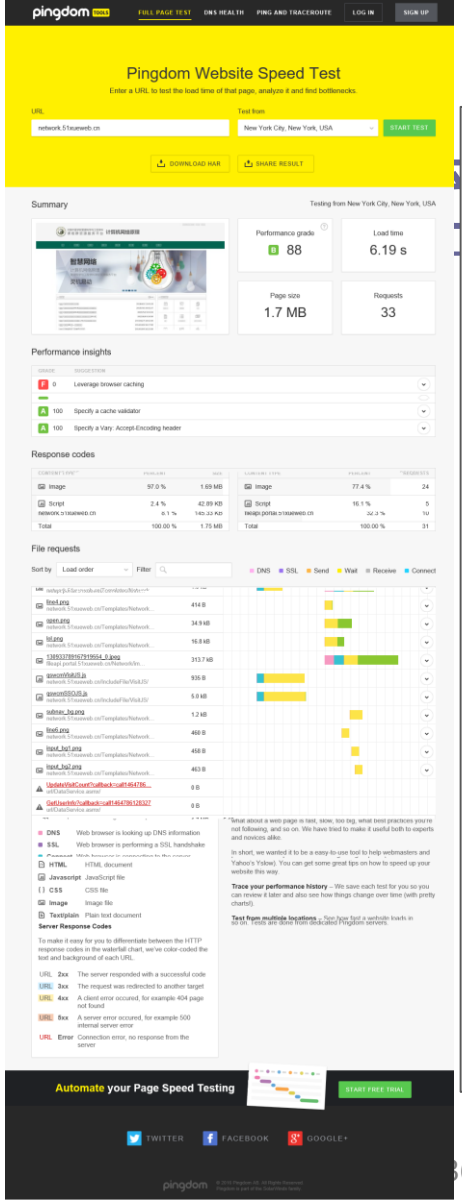
1.域名系统DNS

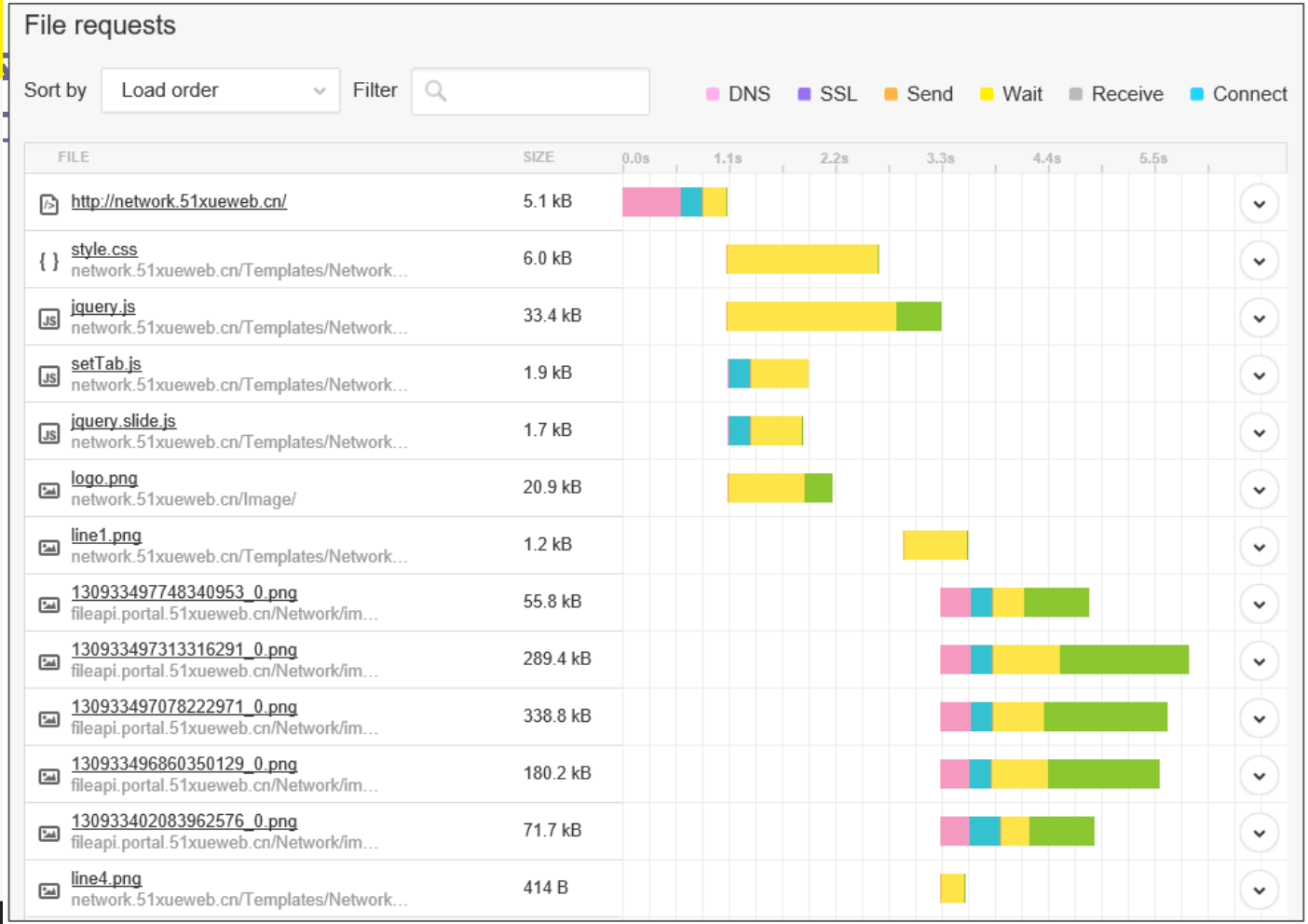
- 名字系统的实现方式有哪些？
  - 在ARPANET时代，使用hosts的文件，列出所有主机名字和相应的IP地址。
  - 随着计算机数量的增多，采用域名系统DNS。

- 域名系统要解决的两个关键问题？
  - 性能：抛弃整个因特网使用一个域名服务器的集中式解决方案，采用分布式的域名系统DNS。（RFC 1034，1035）
  - 冲突：采用层次树状结构的命名方法，确保不存在相同的域名，杜绝了名字冲突。

1.域名系统DNS

- 域名到IP地址的解析过程：
  - 当某一个应用进程需要把主机名解析为IP地址时，该应用进程就调用解析程序（resolver）。
  - 作为DNS的一个客户，把待解析的域名放在DNS请求报文中，以UDP用户数据报方式发给本地域名服务器。
  - 本地域名服务器在查找域名后，把对应的IP地址放回到回答报文中返回。
  - 应用进程获得目的主机的IP地址后即可进行通信。
  - 如果本地域名服务器不能够回答该请求，则本地域名服务器就暂时成为DNS中的一个客户机，向其他域名服务器发出查询请求。


pingdom
FILE PAGE TEST
DNS HEALTH
PING AND TRACEROUTE
LOG IN
SIGN UP
Pingdom Website Speed Test
Enter a URL to test the load time of that page, analyze it and find bottlenecks.
URL
network.51xueweb.cn
Test from
New York City, New York, USA
START TEST
DOWNLOAD HAR
SHARE RESULT
Summary
Testing from New York City, New York, USA
Performance grade
B 88
Load time
6.19 s
Page size
1.7 MB
Requests
33
Performance insights
Leverage browser caching
Specify a cache validator
Specify a Vary: Accept-Encoding header
Response codes
File requests
Sort by
Load order
Filter
DNS
SSL
Send
Wait
Receive
Connect
Automate your Page Speed Testing
START FREE TRIAL
TWITTER
FACEBOOK
GOOGLE+


File requests
Sort by
Load order
Filter
DNS
SSL
Send
Wait
Receive
Connect
FILE
SIZE
0.0s
1.1s
2.2s
3.3s
4.4s
5.5s
http://network.51xueweb.cn/ 5.1 kB
style.css network.51xueweb.cn/Templates/Network... 6.0 kB
jquery.js network.51xueweb.cn/Templates/Network... 33.4 kB
setTab.js network.51xueweb.cn/Templates/Network... 1.9 kB
jquery.slide.js network.51xueweb.cn/Templates/Network... 1.7 kB
logo.png network.51xueweb.cn/Image/ 20.9 kB
line1.png network.51xueweb.cn/Templates/Network... 1.2 kB
130933497748340953_0.png fileapi.portal.51xueweb.cn/Network/im... 55.8 kB
130933497313316291_0.png fileapi.portal.51xueweb.cn/Network/im... 289.4 kB
130933497078222971_0.png fileapi.portal.51xueweb.cn/Network/im... 338.8 kB
130933496860350129_0.png fileapi.portal.51xueweb.cn/Network/im... 180.2 kB
130933402083962576_0.png fileapi.portal.51xueweb.cn/Network/im... 71.7 kB
line4.png network.51xueweb.cn/Templates/Network... 414 B

1.域名系统DNS

1.1域名系统概述

网络 - BBC - Homepage

查看器 | 控制台 | 调试器 | { } 样式编辑器 | 性能 | 网络

状态	方法	文件	域名	类型	已传输	大小	0 毫秒	20.48 秒	40.96 秒
200	GET	/	www.bbc.com	html	33.27 KB	199.76 KB	→ 456 ms		
200	GET	orb.min.css	static.bbci.co.uk	css	4.73 KB	26.01 KB	→ 400 ms		
200	GET	api.min.js	static.bbci.co.uk	js	0.27 KB	0.38 KB	→ 279 ms		
200	GET	id-cta.css	static.bbc.co.uk	css	2.18 KB	24.67 KB	→ 260 ms		
200	GET	main.min.css	mybbc.files.bbci.co.uk	css	11.28 KB	97.37 KB	→ 311 ms		
200	GET	wwhp.min.css	static.bbci.co.uk	css	17.20 KB	90.42 KB	→ 309 ms		
200	GET	modernizr.js	static.bbci.co.uk	js	4.30 KB	10.34 KB	→ 328 ms		
200	GET	bbc-blocks-light.png	static.bbci.co.uk	png	0.71 KB	0.71 KB	→ 536 ms		
200	GET	orb-search-light.png	static.bbci.co.uk	png	0.26 KB	0.26 KB	→ 549 ms		
200	GET	_89854240_89854236.jpg	ichef.bbci.co.uk	jpeg	3.81 KB	3.81 KB	→ 201 ms		

消息头 | Cookie | 参数 | 响应 | 耗时

DNS 解析: → 67 ms
连接: → 113 ms
发送: → -1 ms
等待: → 98 ms
接收: → 122 ms

网络 - BBC - Homepage

查看器 | 控制台 | 调试器 | { } 样式编辑器 | 性能 | 网络

状态	方法	文件	域名	类型	已传输	大小	0 毫秒	20.48 秒	40.96 秒
200	GET	/	www.bbc.com	html	33.27 KB	199.76 KB	→ 456 ms		
200	GET	orb.min.css	static.bbci.co.uk	css	4.73 KB	26.01 KB	→ 400 ms		
200	GET	api.min.js	static.bbci.co.uk	js	0.27 KB	0.38 KB	→ 279 ms		
200	GET	id-cta.css	static.bbc.co.uk	css	2.18 KB	24.67 KB	→ 260 ms		
200	GET	main.min.css	mybbc.files.bbci.co.uk	css	11.28 KB	97.37 KB	→ 311 ms		
200	GET	wwhp.min.css	static.bbci.co.uk	css	17.20 KB	90.42 KB	→ 309 ms		
200	GET	modernizr.js	static.bbci.co.uk	js	4.30 KB	10.34 KB	→ 328 ms		
200	GET	bbc-blocks-light.png	static.bbci.co.uk	png	0.71 KB	0.71 KB	→ 536 ms		
200	GET	orb-search-light.png	static.bbci.co.uk	png	0.26 KB	0.26 KB	→ 549 ms		
200	GET	_89854240_89854236.jpg	ichef.bbci.co.uk	jpeg	3.81 KB	3.81 KB	→ 201 ms		

消息头 | Cookie | 参数 | 响应 | 耗时

DNS 解析: → 68 ms
连接: → 113 ms
发送: → -1 ms
等待: → 98 ms
接收: → 0 ms

网络 - BBC - Homepage

查看器 | 控制台 | 调试器 | { } 样式编辑器 | 性能 | 网络

状态	方法	文件	域名	类型	已传输	大小	0 毫秒	20.48 秒	40.96 秒
200	GET	/	www.bbc.com	html	33.27 KB	199.76 KB	→ 456 ms		
200	GET	orb.min.css	static.bbci.co.uk	css	4.73 KB	26.01 KB	→ 400 ms		
200	GET	api.min.js	static.bbci.co.uk	js	0.27 KB	0.38 KB	→ 279 ms		
200	GET	id-cta.css	static.bbc.co.uk	css	2.18 KB	24.67 KB	→ 260 ms		
200	GET	main.min.css	mybbc.files.bbci.co.uk	css	11.28 KB	97.37 KB	→ 311 ms		
200	GET	wwhp.min.css	static.bbci.co.uk	css	17.20 KB	90.42 KB	→ 309 ms		
200	GET	modernizr.js	static.bbci.co.uk	js	4.30 KB	10.34 KB	→ 328 ms		
200	GET	bbc-blocks-light.png	static.bbci.co.uk	png	0.71 KB	0.71 KB	→ 536 ms		

消息头 | Cookie | 参数 | 响应 | 耗时

DNS 解析: → 0 ms
连接: → 209 ms
发送: → 0 ms
等待: → 98 ms
接收: → 2 ms

1.域名系统DNS

- 因特网采用层次树状结构的命名方法，就像全球邮政系统和电话系统一样。
- 任何一个连接在因特网的主机或路由器，都有一个唯一的层次结构的名字，即域名（domain name）。
- 域可以划分为子域，子域还可继续划分为子域的子域，就形成了顶级域、二级域、三级域、四级域，等等。

…. 三级域名. 二级域名. 顶级域名

1.域名系统DNS

- DNS对域名中的标号的定义：
  - 域名中的标号都由英文字母和数字组成。
  - 每一个标号不超过63个字符。
  - 标号不区分大小写。
  - 多个标号组成的完整域名总共不超过255个字符。
- DNS不规定一个域名包含多少个下级域名，也不规定每一级的域名代表什么含义。
- 各级域名有其上一级的域名管理机构管理，而最高的顶级域名则有ICANN进行管理。

1.域名系统DNS

- 域名只是个逻辑概念，并不代表计算机所在的物理地点。
- 变长的域名和使用有助记忆的字符串，是为了便于人来使用。而 IP 地址是定长的 32 位二进制数字则非常便于机器进行处理。
- 域名中的“点”和点分十进制 IP 地址中的“点”并无一一对应的关系。点分十进制 IP 地址中一定是包含三个“点”，但每一个域名中“点”数目则不一定是三个。

1.域名系统DNS

- 顶级域名TLD（Top Level Domain）
  - 国家顶级域名 nTLD：如: .cn 表示中国，.us 表示美国，.uk 表示英国，等等。
  - 通用顶级域名 gTLD：最早的顶级域名是：
    - .com （公司和企业）
    - .net （网络服务机构）
    - .org （非赢利性组织）
    - .edu （美国专用的教育机构）
    - .gov （美国专用的政府部门）
    - .mil （美国专用的军事部门）
    - .int （国际组织）
  - 基础结构域名(infrastructure domain)：这种顶级域名只有一个，即 arpa，用于反向域名解析，因此又称为反向域名。

1.域名系统DNS

- 通用顶级域名 gTLD
  - .aero （航空运输企业）
  - .biz （公司和企业）
  - .cat （加泰隆人的语言和文化团体）
  - .coop （合作团体）
  - .info （各种情况）
  - .jobs （人力资源管理者）
  - .mobi （移动产品与服务的用户和提供者）
  - .museum （博物馆）
  - .name （个人）
  - .pro （有证书的专业人员）
  - .travel （旅游业）

English العربية Español Français Русский 中文 Search ICANN.org Log In | Sign Up

ICANN GET STARTED NEWS & MEDIA POLICY PUBLIC COMMENT RESOURCES COMMUNITY IANA STEWARDSHIP & ACCOUNTABILITY

Learn More

1,000 new generic top-level domains (gTLDs) have been introduced into the Internet. This expansion is contributing to choice, competition and innovation in the domain name industry.

Read the Blog Post

News and Announcements

Download the ICANN56 Mobile App or View on Your Desktop

Our ICANN56 Mobile App is now available for download from the Apple App Store, Google Play, Windows Store and Blackberry World. You can also view the app on your desktop. Be sure to download the app today and start preparing for ICANN56 in Helsinki, Finland from 27-30

Quicklinks

- Quarterly Reporting
- New gTLDs
- Domain Name Transfer
- WHOIS

A note about tracking cookies:

This site is using "tracking cookies" on your computer to deliver the best experience possible. Read more to see how they are being used.

This notice is intended to appear only the first time you visit the site on any computer. ✖ Dismiss

.বাংলা	country-code	Not assigned
.公益	generic	China Organizational Name Administration Center
.公司	generic	Computer Network Information Center of Chinese Academy of Sciences （China Internet Network Information Center）
.网站	generic	Global Website TLD Asia Limited
.移动	generic	Afilias Limited
.我爱你	generic	Tycoon Treasure Limited
.москва	generic	Foundation for Assistance for Internet Technologies and Infrastructure Development (FAITID)
.испытание	test	Internet Assigned Numbers Authority
.қаз	country-code	Association of IT Companies of Kazakhstan
.онлайн	generic	CORE Association
.сайт	generic	CORE Association
.联通	generic	China United Network Communications Corporation Limited
.срб	country-code	Serbian National Internet Domain Registry (RNIDS)
.бг	country-code	Not assigned
.бел	country-code	Reliable Software, Ltd.
.ভারত	generic	VeriSign Sarl
.时尚	generic	RISE VICTORY LIMITED
.微博	generic	Sina Corporation
.테스트	test	Internet Assigned Numbers Authority
.淡马锡	generic	Temasek Holdings (Private) Limited
.ファッション	generic	Amazon Registry Services, Inc.
.орг	generic	Public Interest Registry
.नेट	generic	VeriSign Sarl
.ストア	generic	Amazon Registry Services, Inc.
.삼성	generic	SAMSUNG SDS CO., LTD
.சிங்கப்பூர்	country-code	Singapore Network Information Centre (SGNIC) Pte Ltd
.商标	generic	HU YI GLOBAL INFORMATION RESOURCES(HOLDING) COMPANY.HONGKONG LIMITED

Delegation Record for .公司

(Generic top-level domain)

Sponsoring Organisation

Computer Network Information Center of Chinese Academy of Sciences （China Internet Network Information Center）
Floor 1, Building 1, Software Park, Chinese Academy of Sciences, 4 South 4th Street, Zhongguancun, Beijing
China

Administrative Contact

JIN Jian
Computer Network Information Center of Chinese Academy of Sciences （China Internet Network Information Center）
Floor 1, Building 1, Software Park, Chinese Academy of Sciences, 4 South 4th Street, Zhongguancun, Beijing
China
Email: ng@cnnic.cn
Voice: +86(0)10-58812624
Fax: +86(0)10-58812666

Technical Contact

HE Zheng
Computer Network Information Center of Chinese Academy of Sciences （China Internet Network Information Center）
Floor 1, Building 1, Software Park, Chinese Academy of Sciences, 4 South 4th Street, Zhongguancun, Beijing
China
Email: ngtech@cnnic.cn
Voice: +86(0)10-58813200
Fax: +86(0)10-58812666

Name Servers

Host Name	IP Address(es)
a.ngtld.cn	125.208.40.1 2001:dc7:ffc1:0:0:0:0:1
c.ngtld.cn	125.208.42.1 2001:dc7:ffc3:0:0:0:0:1
b.ngtld.cn	125.208.41.1 2001:dc7:ffc2:0:0:0:0:1
d.ngtld.cn	125.208.43.1
e.ngtld.cn	125.208.44.1

中国互联网络发展状况统计报告

（2016 年 1 月）

表 2　中国分类域名数[2]

	数量（个）	占域名总数比例
CN	16,363,594	52.8%
COM	10,997,941	35.5%
NET	1,415,001	4.6%
ORG	397,970	1.3%
中国	352,785	1.1%
BIZ	70,770	0.2%
INFO	26,107	0.1%
其他	1,396,346	4.5%
总和	31,020,514	100.0%

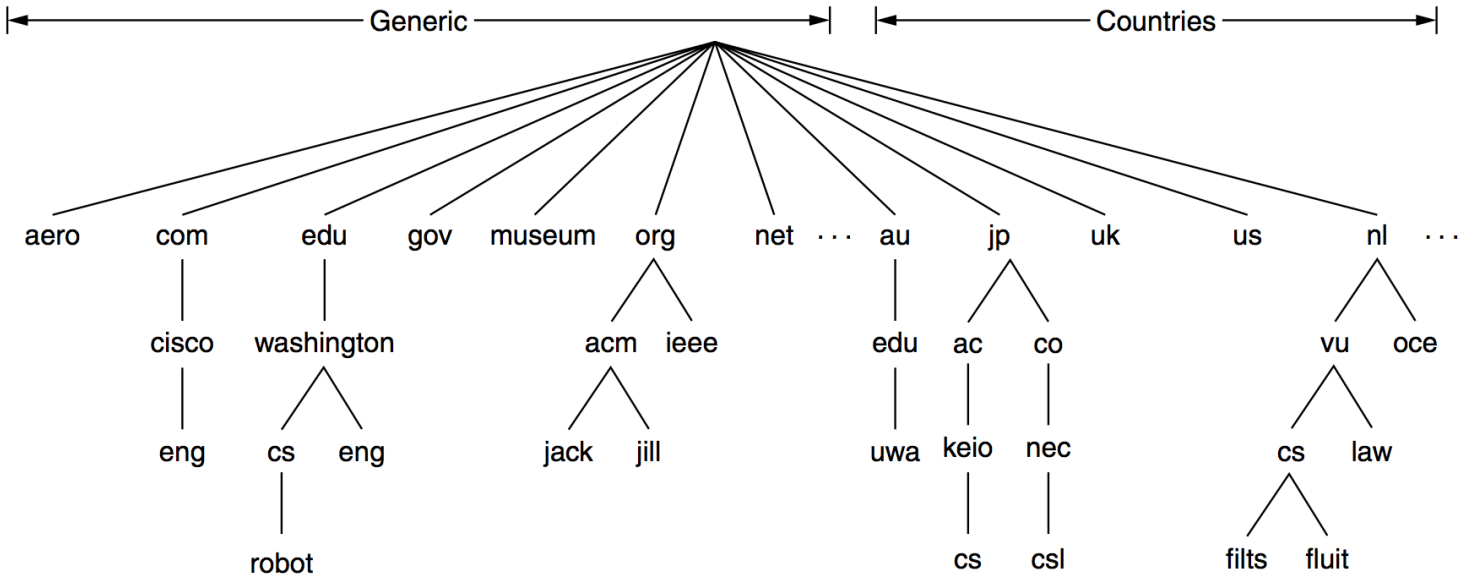
表 3　中国分类 CN 域名数

	数量（个）	占 CN 域名总数比例
.cn	11,729,750	71.7%
com.cn	2,405,969	14.7%
adm.cn	1,181,514	7.2%
net.cn	746,855	4.6%
ac.cn	124,821	0.8%
org.cn	110,779	0.7%
gov.cn	56,938	0.3%
edu.cn	6,894	0.0%
mil.cn	74	0.0%
合计	16,363,594	100.0%

截至 2015 年 12 月，中国“.CN”域名总数为 1636 万，年增长 47.6%，占中国域名总数比例为 52.8%，超过德国国家顶级域名".DE"，成为全球注册保有量第一的国家和地区顶级域名(ccTLD)；“.COM”域名数量为 1100 万，占比为 35.5%；“.中国”域名总数达到 35.3 万。

1.域名系统DNS

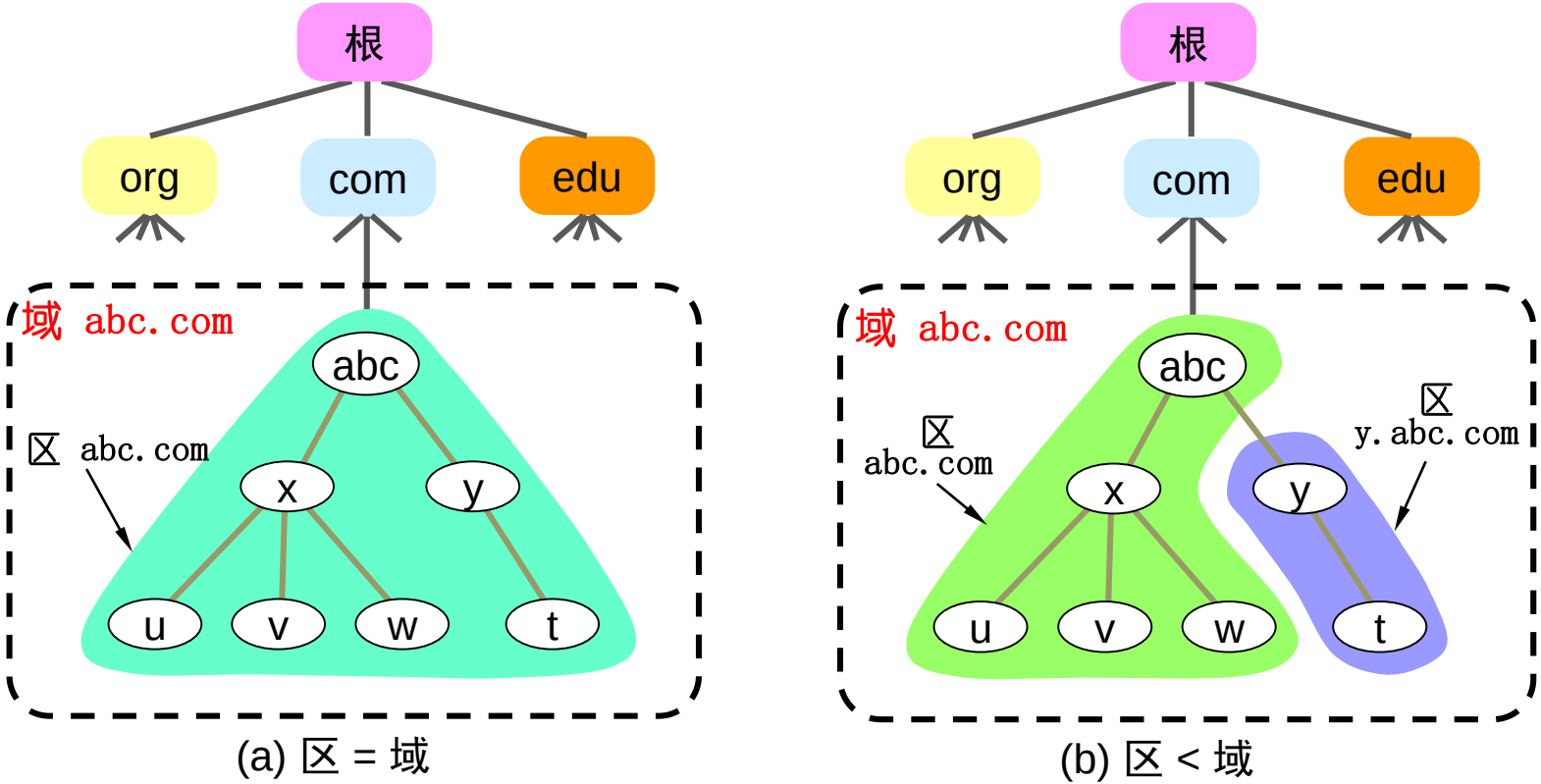
- 因特网的域名空间



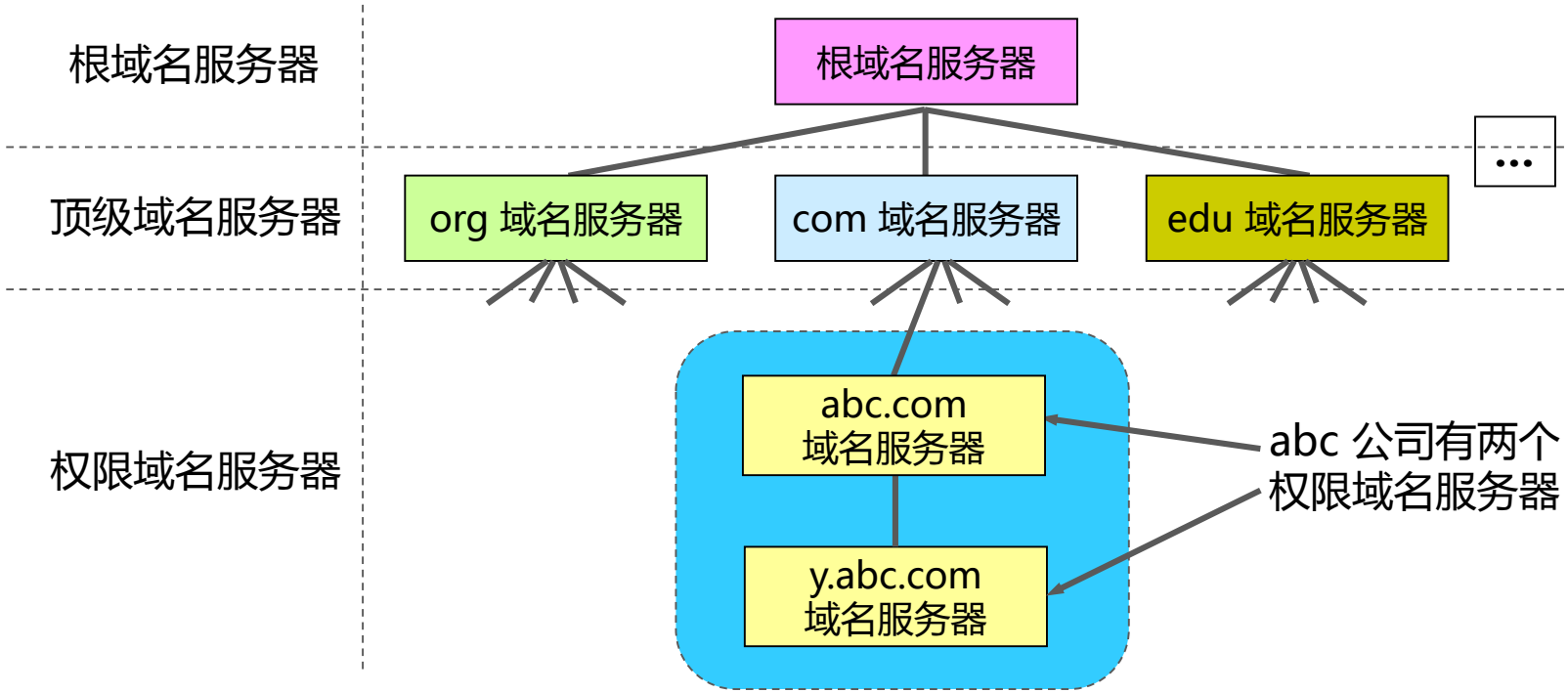
1.域名系统DNS

- 一个服务器所负责管辖的（或有权限的）范围叫做区(zone)。
- 各单位根据具体情况来划分自己管辖范围的区。但在一个区中的所有节点必须是能够连通的。
- 每一个区设置相应的权限域名服务器，用来保存该区中的所有主机的域名到IP地址的映射。
- DNS 服务器的管辖范围不是以“域”为单位，而是以“区”为单位。

1.域名系统DNS


根
org
com
edu
域 abc.com
区 abc.com
abc
x
y
u
v
w
t
(a) 区 = 域
根
org
com
edu
域 abc.com
区 abc.com
区 y.abc.com
abc
x
y
u
v
w
t
(b) 区 < 域

1.域名系统DNS


根域名服务器
顶级域名服务器
权限域名服务器
根域名服务器
org 域名服务器
com 域名服务器
edu 域名服务器
...
abc.com
域名服务器
y.abc.com
域名服务器
abc 公司有两个
权限域名服务器

1.域名系统DNS

根域名服务器
顶级域名服务器（TLD服务器）
权限域名服务器

本地域名服务器（Local Name Server）

1.域名系统DNS

- 根域名服务器
  - 根域名服务器是最重要的域名服务器。所有的根域名服务器都知道所有的顶级域名服务器的域名和IP地址。
  - 不管是哪一个本地域名服务器，若要对因特网上任何一个域名进行解析，只要自己无法解析，就首先求助于根域名服务器。
  - 在因特网上共有13个不同IP地址的根域名服务器，它们的名字是用一个英文字母命名，从a一直到m（前13个字母）。
  - 根域名服务器共有 13 套装置（不是13个机器）。

1.域名系统DNS

- 根域名服务器
  - 根域名服务器相应的域名分别是

    a.rootservers.net

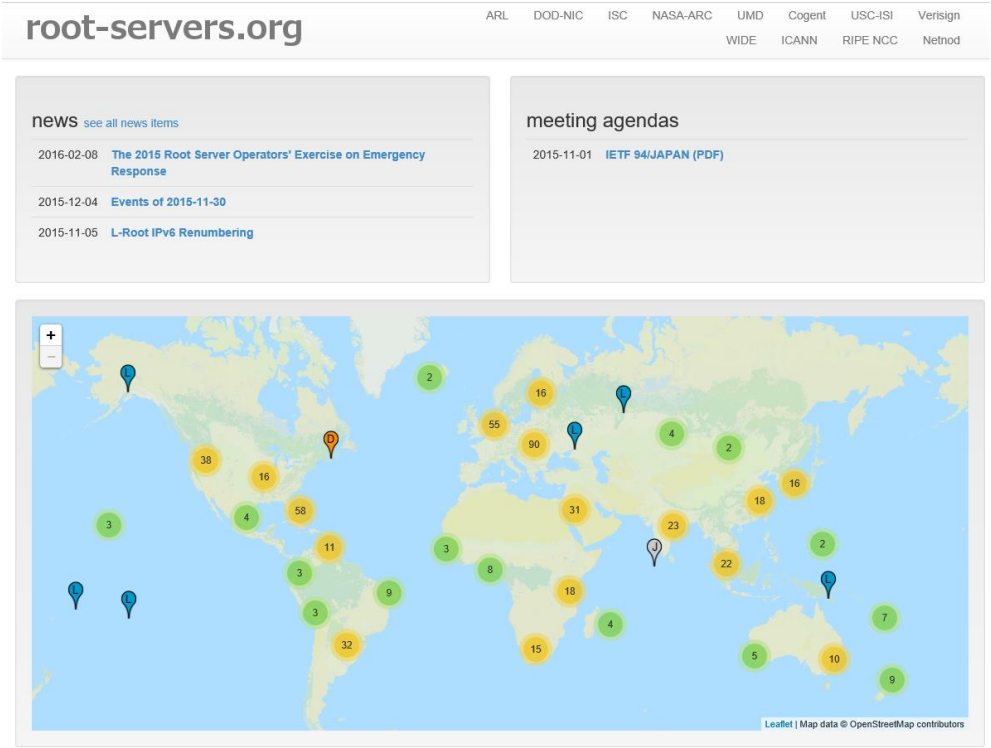
    b.rootservers.net

    …

    m.rootservers.net
  - 到2006年底全世界已经安装了一百多个根域名服务器机器，分布在世界各地。
  - 这样做的目的是为了方便用户，使世界上大部分 DNS 域名服务器都能就近找到一个根域名服务器。

1.域名系统DNS

- 根域名服务器位置分布：http://www.root-servers.org/



1.域名系统DNS

- 我国为什么没有根域服务器？
- 为什么根域服务器只有13套？还能够增加？

专家：中国急需自建根域名服务器

2014年1月22日，国家互联网应急中心发布消息称，1月21日15时20分，大量互联网用户无法正常访问域名以".com"、".net"等结尾的网站。事件发生后，国家互联网应急中心第一时间启动应急响应机制，协调组织部分技术支撑单位进行调查和应急处置，16时50分左右，用户访问基本恢复正常。经对已掌握的数据进行分析，初步判断此次事件是由于网络攻击导致我国境内互联网用户通过国际顶级域名服务解析时出现异常，攻击来源正在进一步调查中。

1月21日15时许，国内部分用户发现无法访问.com域名网站，国内多个门户网站无法正常访问。经过监测后发现，很多网站被解析到65.49.2.178这一个无法访问的美国IP地址。其还发现，国内三分之二DNS处于瘫痪状态。据域名服务商称，"断网"的原因与DNS故障有关，有业内专家分析称，攻击可能来自国内。

安全专家表示，由于根域名服务器全在美国以及日本和欧洲，我国对根域名几乎没有掌控权，如果根域名出现问题，将影响我国所有域名解析和网站访问，因此，需要建立一套完整的对DNS监控及灾备系统。

中国互联网的现状并不容乐观，漏洞来自于底层，而我国的操作系统、芯片、核心技术全是国外的产品。根服务器解析出问题，反映这样一个严峻又无奈的现实：互联网时代，世界的咽喉都在外国人手中，若有重大冲突，所有建立在互联网上的民航、铁路、金融、政府服务都可能崩溃。

专家还建议，当务之急，是针对目前根服务器掌控权握在他国手里的无奈，我国应立即建立起完善的对DNS监控及灾备系统，最好尽快建立自己的根域名服务器，以更好地确保我国网络安全。

此外，除了域名体系自身的安全问题，在互联网领域，外在的攻击也具备危害范围大、攻击手段多、防患应对难等特点。国家互联网应急中心数据显示，去年12月，境内感染网络病毒的终端数为222万余个，境内被篡改网站数量为6823个，被植入后门的网站数量为6171个。国家信息安全漏洞共享平台(CNVD)收集整理信息系统安全漏洞635个，其中，高危漏洞172个，可被利用来实施远程攻击的漏洞有566个。网络安全专家建议有关部门、行业协会与企业"三位一体"，合力构建完善网络安全保障系统，保护网络安全。(本刊编辑 x023)

1.域名系统DNS

- 顶级域名服务器（TLD服务器）
  - 顶级域名服务器负责管理在该顶级域名服务器注册的所有二级域名。
  - 当收到 DNS 查询请求时，就给出相应的回答（可能是最后的结果，也可能是下一步应当找的域名服务器的 IP 地址）。

1.域名系统DNS

- 权限域名服务器
  - 权限域名服务器负责一个区的域名服务器。
  - 当一个权限域名服务器还不能给出最后的查询回答时，就会告诉发出查询请求的 DNS 客户，下一步应当找哪一个权限域名服务器。

1.域名系统DNS

- 本地域名服务器
  - 本地域名服务器对域名系统非常重要。
  - 当一个主机发出 DNS 查询请求时，这个查询请求报文就发送给本地域名服务器。
  - 每一个因特网服务提供者 ISP，或一个大学，甚至一个大学里的系，都可以拥有一个本地域名服务器。
  - 这种域名服务器有时也称为默认域名服务器。
  - 本地域名服务器，就是日常在配置计算机IP地址时，配置的域名服务器。

1.域名系统DNS

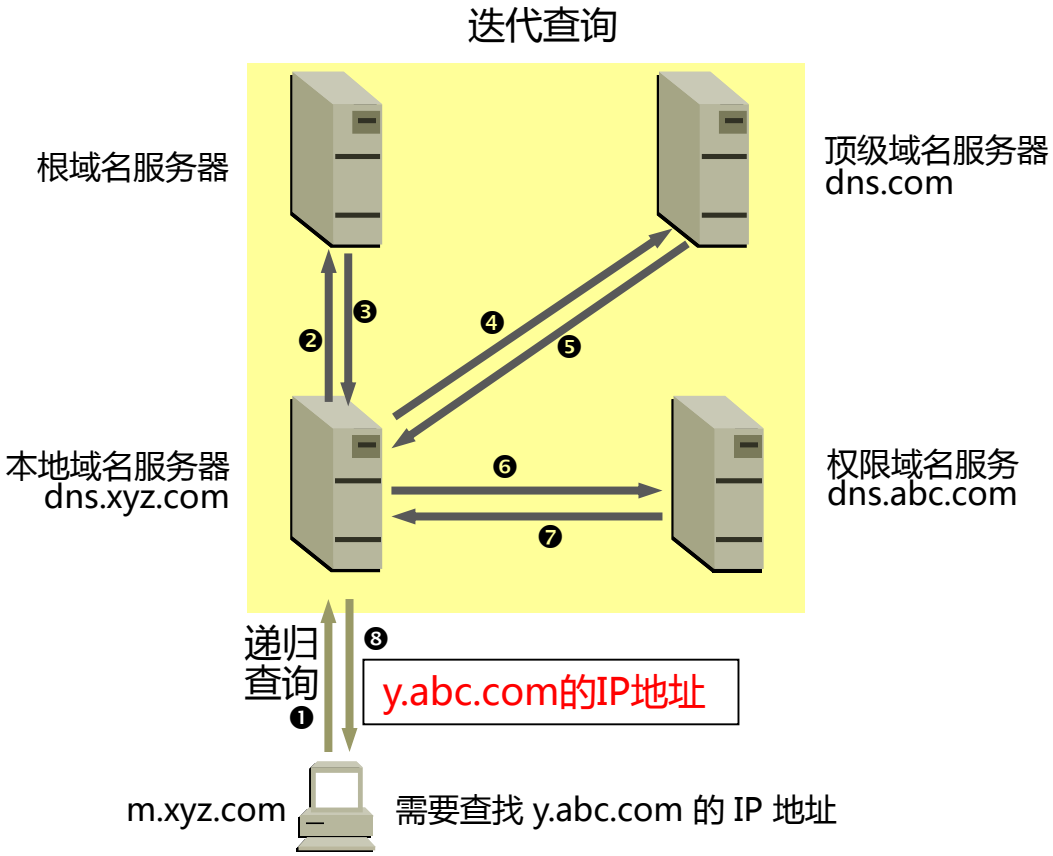
- 提高域名服务器的可靠性的方法
  - DNS 域名服务器都把数据复制到几个域名服务器来保存，其中的一个是主域名服务器，其他的是辅助域名服务器。
  - 当主域名服务器出故障时，辅助域名服务器可以保证 DNS 的查询工作不会中断。
  - 主域名服务器定期把数据复制到辅助域名服务器中，而更改数据只能在主域名服务器中进行。这样就保证了数据的一致性。

1.域名系统DNS

- 主机向本地域名服务器的查询一般都是采用递归查询。
  - 如果主机所询问的本地域名服务器不知道被查询域名的 IP 地址，那么本地域名服务器就以 DNS 客户的身份，向其他根域名服务器继续发出查询请求报文。
- 本地域名服务器向根域名服务器的查询通常是采用迭代查询。
  - 当根域名服务器收到本地域名服务器的迭代查询请求报文时，要么给出所要查询的 IP 地址，要么告诉本地域名服务器：“你下一步应当向哪一个域名服务器进行查询”。然后让本地域名服务器进行后续的查询。

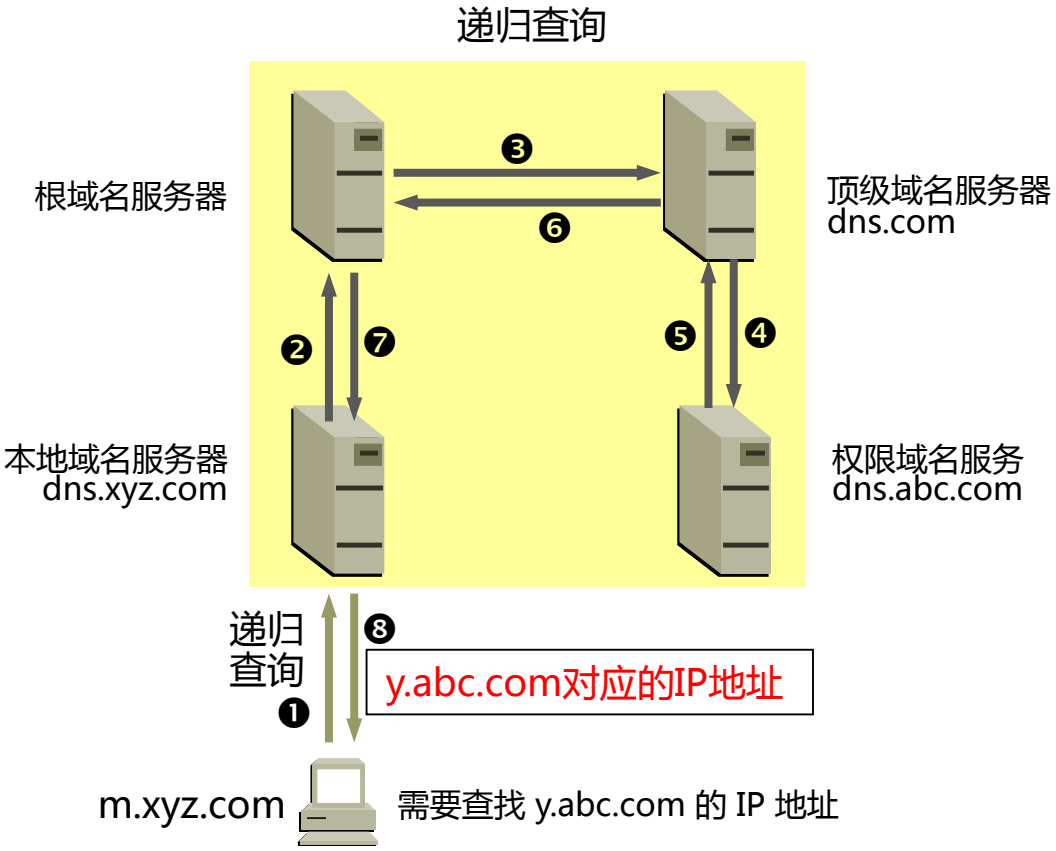
1.域名系统DNS

1.4域名的解析过程

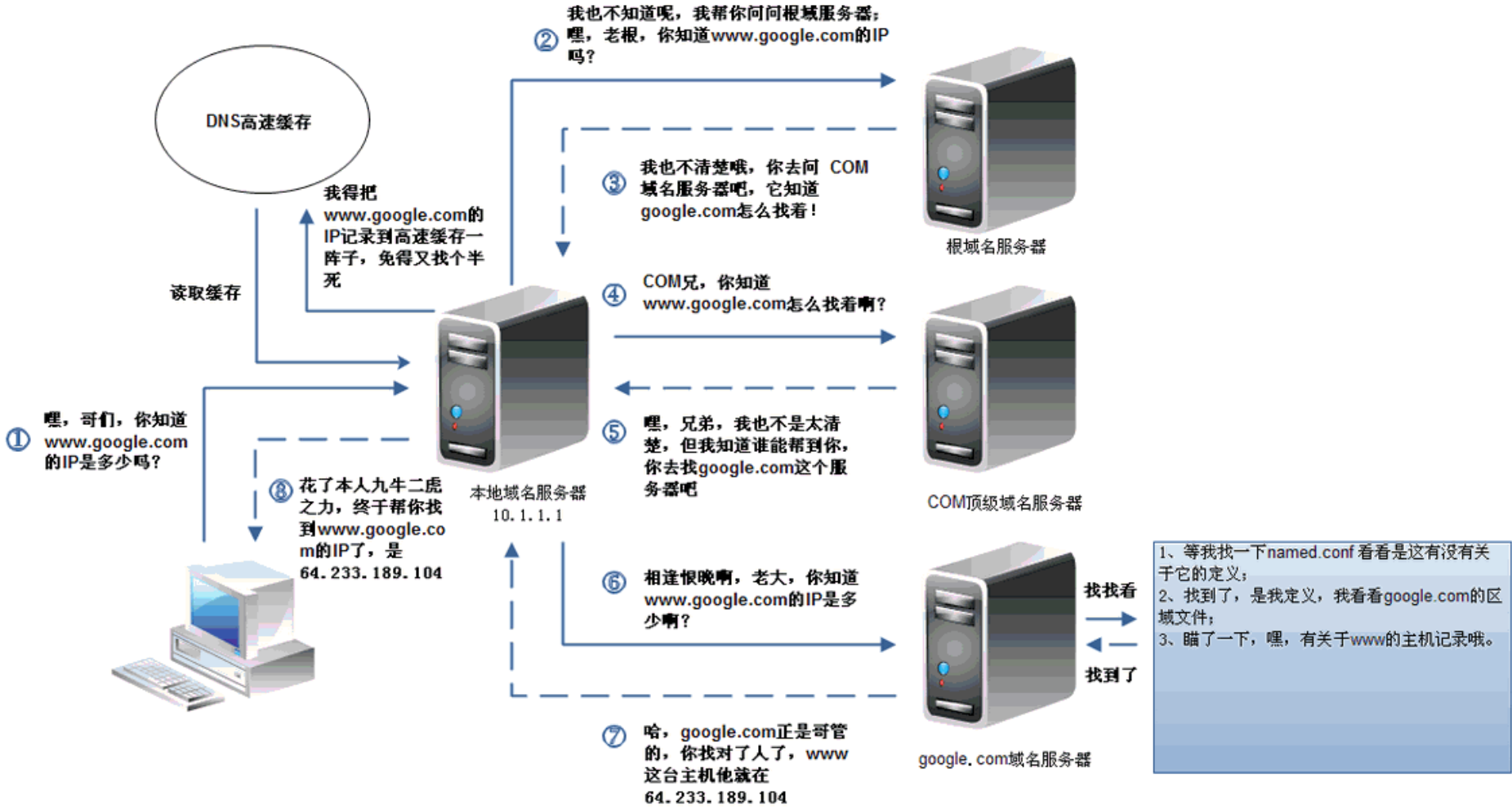


1.域名系统DNS

1.4域名的解析过程



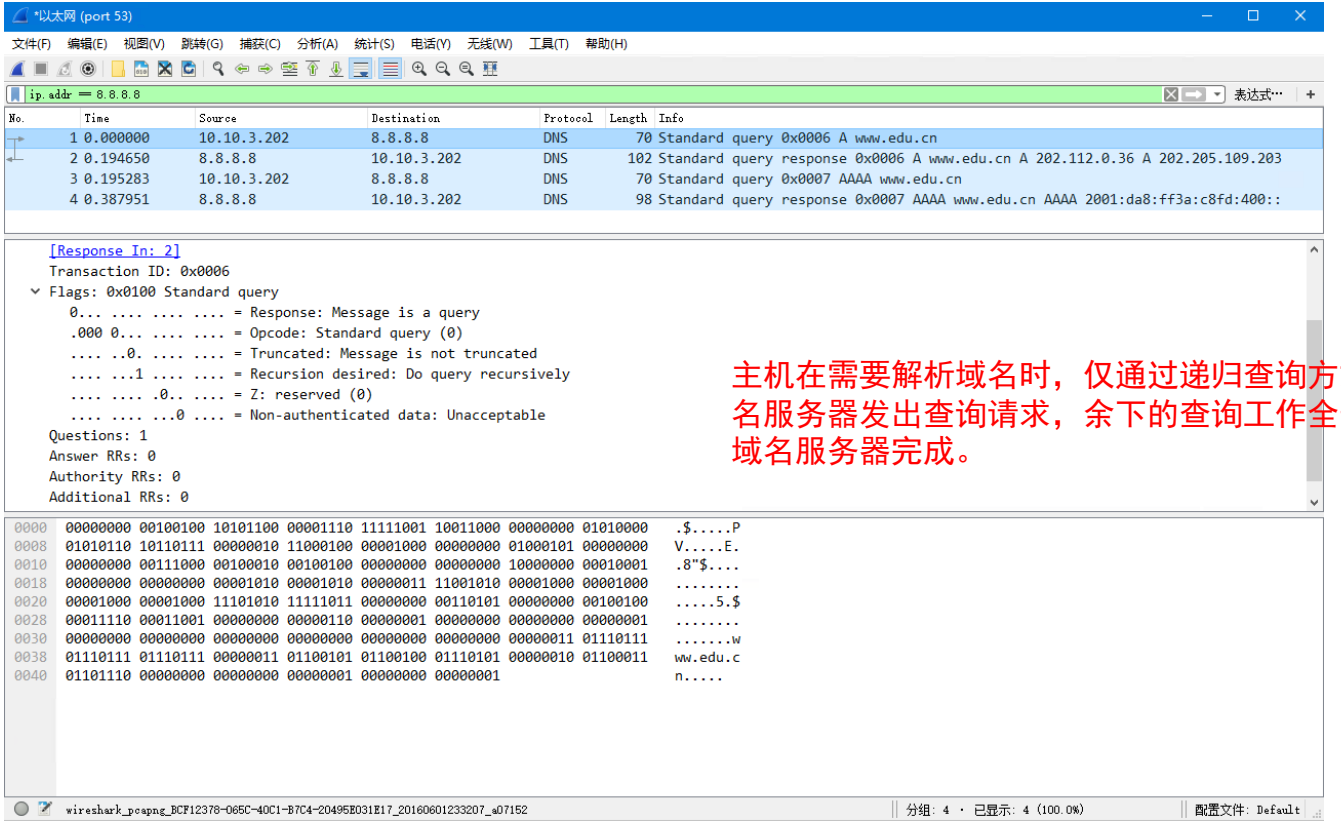
DNS域名解析过程



递归查询　　迭代查询

1.域名系统DNS

1.4域名的解析过程



主机在需要解析域名时，仅通过递归查询方式向本地域名服务器发出查询请求，余下的查询工作全部交由本地域名服务器完成。

1.域名系统DNS

- 每个域名服务器都维护一个高速缓存，存放最近用过的名字以及从何处获得名字映射信息的记录。
  - 高速缓存可大大减轻根域名服务器的负荷，使因特网上的 DNS 查询请求和回答报文的数量大为减少。
- 为保持高速缓存中的内容正确，域名服务器应为每项内容设置计时器，并处理超过合理时间的项（例如，每个项目只存放两天）。
  - 当权限域名服务器回答一个查询请求时，在响应中都指明绑定有效存在的时间值。增加此时间值可减少网络开销，而减少此时间值可提高域名转换的准确性。

1.域名系统DNS

- 不仅在本地域名服务器中需要高速缓存，在主机中也会保存域名解析的缓存。
- 主机在启动时从本地域名服务器下载名字和地址的全部数据库，维护存放自己最近使用的域名的高速缓存，并且只在从缓存中找不到名字时才使用域名服务器。
- 由于域名改动不是很频繁，因此高速缓存能够极大的提高域名查询的效率，提升网络访问的速度。

1.域名系统DNS

- 管理Windows操作系统中的域名高速缓存。
  - ipconfig /displaydns　　查看域名高速缓存记录
  - ipconfig /flushdns　　清除域名高速缓存记录

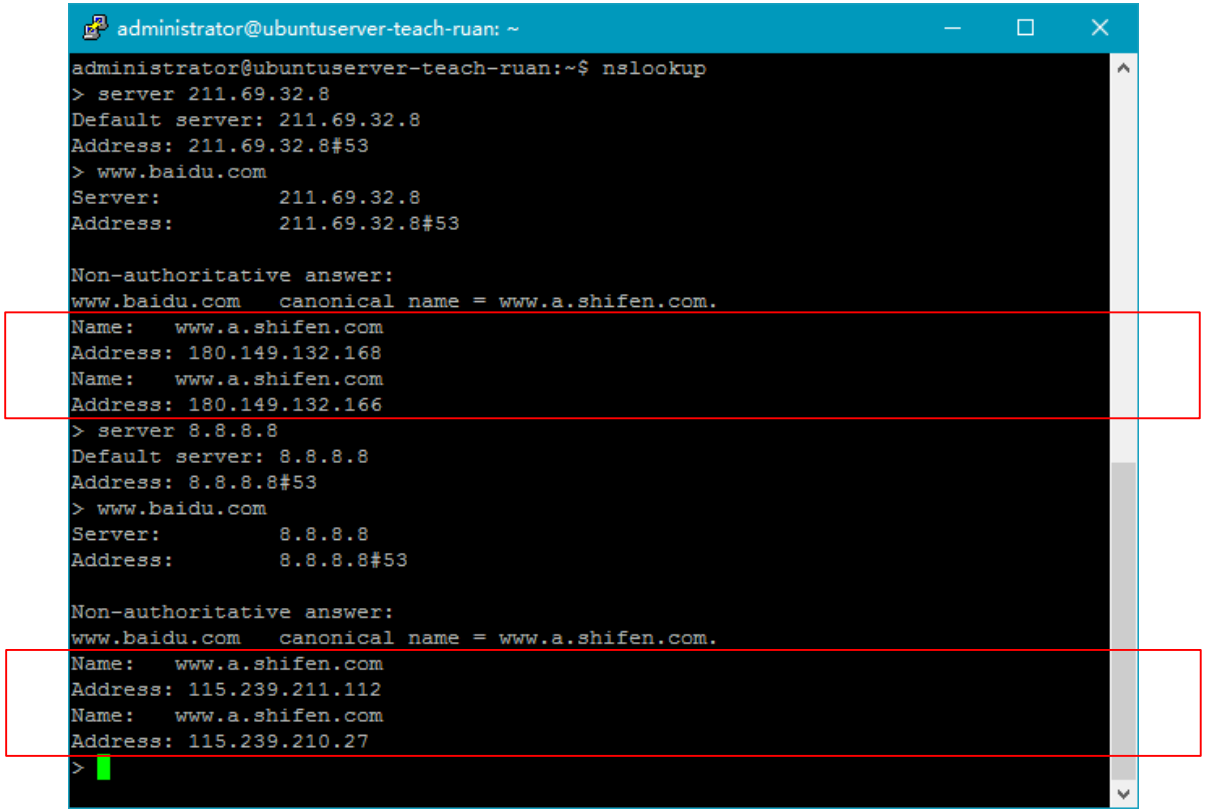
- 管理ubuntu操作系统中的域名高速缓存。
  - /etc/init.d/dns-clean start　　清除dns缓存记录

1.域名系统DNS

- 域名系统DNS在网络通信中的作用非常重要，确保DNS查询的可用性和正确性，是进行网络故障判断的常用手段。
- 域名解析的测试工具：
  - 操作系统内置工具：nslookup、dig
  - DNS测试软件：DNS Benchmark、Google namebench
  - 在线DNS测试服务：
    - http://tools.pingdom.com
    - http://ce.cloud.360.cn
    - http://tool.chinaz.com/dns
    - http://www.17ce.com/site/dns.html

1.域名系统DNS

1.6域名解析的测试



1

式

```
administrator@ubuntuserver-teach-ruan:~$ dig

; <<>> DiG 9.9.5-11ubuntu1.3-Ubuntu <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56571
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 23

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       14317   IN      NS      m.root-servers.net.
.                       14317   IN      NS      f.root-servers.net.
.                       14317   IN      NS      h.root-servers.net.
.                       14317   IN      NS      k.root-servers.net.
.                       14317   IN      NS      l.root-servers.net.
.                       14317   IN      NS      c.root-servers.net.
.                       14317   IN      NS      a.root-servers.net.
.                       14317   IN      NS      j.root-servers.net.
.                       14317   IN      NS      i.root-servers.net.
.                       14317   IN      NS      g.root-servers.net.
.                       14317   IN      NS      d.root-servers.net.
.                       14317   IN      NS      e.root-servers.net.
.                       14317   IN      NS      b.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net.     345431  IN      A       198.41.0.4
a.root-servers.net.     345431  IN      AAAA    2001:503:ba3e::2:30
b.root-servers.net.     345431  IN      A       192.228.79.201
c.root-servers.net.     345431  IN      A       192.33.4.12
d.root-servers.net.     345431  IN      A       199.7.91.13
d.root-servers.net.     345431  IN      AAAA    2001:500:2d::d
e.root-servers.net.     345431  IN      A       192.203.230.10
f.root-servers.net.     345431  IN      A       192.5.5.241
f.root-servers.net.     345431  IN      AAAA    2001:500:2f::f
g.root-servers.net.     345431  IN      A       192.112.36.4
h.root-servers.net.     345431  IN      A       128.63.2.53
h.root-servers.net.     345431  IN      AAAA    2001:500:1::803f:235
i.root-servers.net.     345431  IN      A       192.36.148.17
i.root-servers.net.     345431  IN      AAAA    2001:7fe::53
j.root-servers.net.     345431  IN      A       192.58.128.30
j.root-servers.net.     345431  IN      AAAA    2001:503:c27::2:30
k.root-servers.net.     345431  IN      A       193.0.14.129
k.root-servers.net.     345431  IN      AAAA    2001:7fd::1
l.root-servers.net.     345431  IN      A       199.7.83.42
l.root-servers.net.     345431  IN      AAAA    2001:500:3::42
m.root-servers.net.     345431  IN      A       202.12.27.33
m.root-servers.net.     345431  IN      AAAA    2001:dc3::35

;; Query time: 6 msec
;; SERVER: 211.69.32.8#53(211.69.32.8)
;; WHEN: Thu Jun 02 00:09:38 CST 2016
;; MSG SIZE  rcvd: 699

administrator@ubuntuserver-teach-ruan:~$
```

```
administrator@ubuntuserver-teach-ruan:~$ dig www.qq.com

; <<>> DiG 9.9.5-11ubuntu1.3-Ubuntu <<>> www.qq.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6546
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 11

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.qq.com.                    IN      A

;; ANSWER SECTION:
www.qq.com.             299     IN      A       115.25.209.39

;; AUTHORITY SECTION:
qq.com.                 31940   IN      NS      ns2.qq.com.
qq.com.                 31940   IN      NS      ns1.qq.com.
qq.com.                 31940   IN      NS      ns3.qq.com.
qq.com.                 31940   IN      NS      ns4.qq.com.

;; ADDITIONAL SECTION:
ns1.qq.com.             3539    IN      A       101.226.68.138
ns1.qq.com.             3539    IN      A       14.17.19.139
ns2.qq.com.             3539    IN      A       101.227.169.106
ns2.qq.com.             3539    IN      A       125.39.202.108
ns3.qq.com.             597     IN      A       182.140.177.149
ns3.qq.com.             597     IN      A       182.140.167.157
ns4.qq.com.             3539    IN      A       125.39.247.247
ns4.qq.com.             3539    IN      A       184.105.206.124
ns4.qq.com.             3539    IN      A       203.205.144.156
ns4.qq.com.             3539    IN      A       123.151.178.115

;; Query time: 222 msec
;; SERVER: 211.69.32.8#53(211.69.32.8)
;; WHEN: Thu Jun 02 00:11:10 CST 2016
;; MSG SIZE  rcvd: 287

administrator@ubuntuserver-teach-ruan:~$
```

2.文件传送协议

- 文件传送协议 FTP (File Transfer Protocol) 是因特网上使用得最广泛的文件传送协议。
- FTP 提供交互式的访问，允许客户指明文件的类型与格式，并允许文件具有存取权限。
- FTP 屏蔽了各计算机系统的细节，因而适合于在异构网络中任意计算机之间传送文件。
- FTP是有RFC 959定义的，且很早就成为了因特网的正式标准。

2.文件传送协议

- 网络环境中的一项基本应用就是将文件从一台计算机中复制到另一台可能相距很远的计算机中。
- 初看起来，在两个主机之间传送文件是很简单的事情。
- 其实这往往非常困难。原因是众多的计算机厂商研制出的文件系统多达数百种，且差别很大。

2.文件传送协议

- 网络环境下复制文件的复杂性：
  - 计算机存储数据的格式不同。
  - 文件的目录结构和文件命名的规定不同。
  - 对于相同的文件存取功能，操作系统使用的命令不同。
  - 访问控制方法不同。

2.文件传送协议

- 文件传送协议FTP只提供文件传送的一些基本的服务，使用TCP可靠的运输服务。
- FTP的主要功能是减少或消除在不同操作系统下处理文件的不兼容性。
- FTP使用客户/服务器方式。
  - 一个FTP服务器进程可同时为多个客户进程提供服务。
  - FTP 的服务器进程由两大部分组成：一个主进程，负责接受新的请求；另外有若干个从属进程，负责处理单个请求。

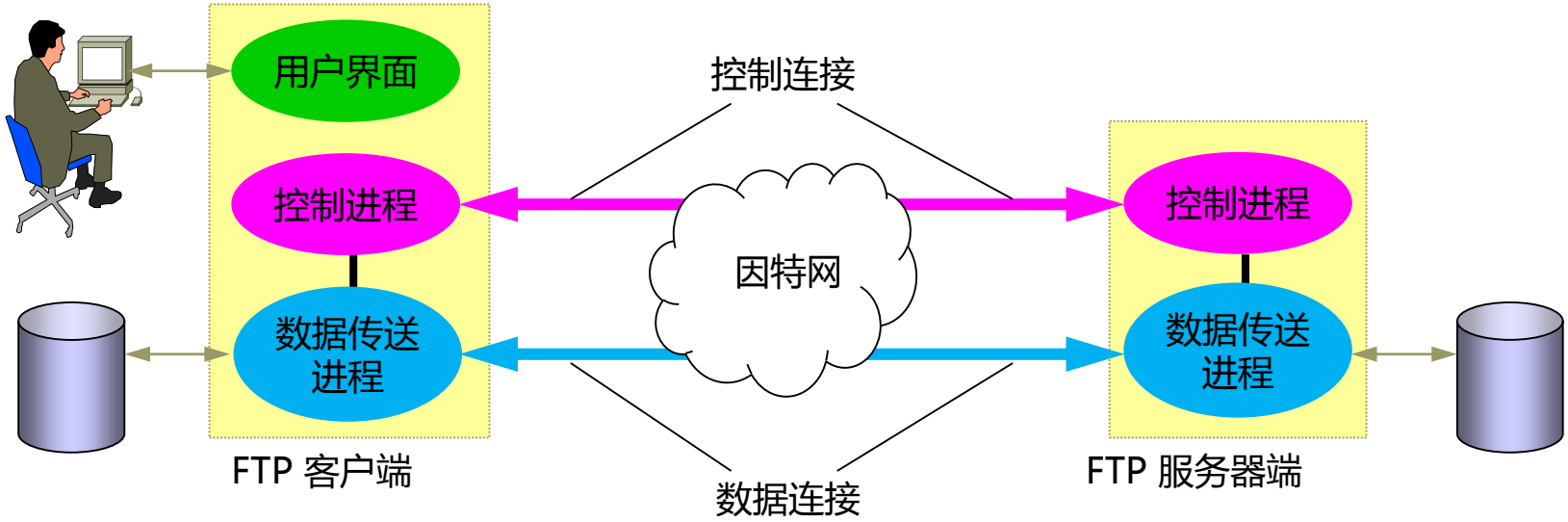
2.文件传送协议

- FTP的主进程工作步骤如下：
  - 打开熟知端口（端口号为21），使客户进程能够连接上。
  - 等待客户进程发出连接请求。
  - 启动从属进程来处理客户进程发来的请求。从属进程对客户进程的请求处理完毕后即终止，但从属进程在运行期间根据需要还可能创建其他一些子进程。
  - 回到等待状态，继续接受其他客户进程发来的请求。主进程与从属进程的处理是并发地进行。

2.文件传送协议

- FTP在通信中保持两个连接：
  - 控制连接在整个会话期间一直保持打开，FTP客户发出的传送请求通过控制连接发送给服务器端的控制进程，但控制连接不用来传送文件。
  - 实际用于传输文件的是“数据连接”。服务器端的控制进程在接收到FTP客户发送来的文件传输请求后就创建“数据传送进程”和“数据连接”，用来连接客户端和服务器端的数据传送进程。
  - 数据传送进程实际完成文件的传送，在传送完毕后关闭“数据传送连接”并结束运行。

2.文件传送协议



2.文件传送协议

- FTP在通信中使用两个端口号：
  - 当客户进程向服务器进程发出建立连接请求时，要寻找连接服务器进程的熟知端口(21)，同时还要告诉服务器进程自己的另一个端口号码，用于建立数据传送连接。
  - 接着，服务器进程用自己传送数据的熟知端口(20)与客户进程所提供的端口号码建立数据传送连接。
  - 由于FTP使用了两个不同的端口号，所以数据连接与控制连接不会发生混乱。
- 使用两个端口号的优势：
  - 使协议更加简单和更容易实现。
  - 在传输文件时还可以利用控制连接。

*以太网

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

ip.addr == 10.10.3.49

No.	Time	Source	Destination	Protocol	Length	Info
2140	31.761873	10.10.3.202	10.10.3.49	FTP	64	Request: AUTH TLS
2141	31.762090	10.10.3.49	10.10.3.202	FTP	121	Response: 534 Local policy on server does not allow TLS secure connections.
2142	31.762287	10.10.3.202	10.10.3.49	FTP	64	Request: AUTH SSL
2143	31.762469	10.10.3.49	10.10.3.202	FTP	121	Response: 534 Local policy on server does not allow TLS secure connections.
2144	31.762744	10.10.3.202	10.10.3.49	FTP	70	Request: USER tiliatech
2145	31.762951	10.10.3.49	10.10.3.202	FTP	77	Response: 331 Password required
2146	31.763123	10.10.3.202	10.10.3.49	FTP	72	Request: PASS qishi#09319
2147	31.763619	10.10.3.49	10.10.3.202	FTP	123	Response: 230-Directory has 10,576,245,096,448 bytes of disk space available.
2148	31.763695	10.10.3.49	10.10.3.202	FTP	75	Response: 230 User logged in.
2149	31.763733	10.10.3.202	10.10.3.49	TCP	54	59058 → 21 [ACK] Seq=55 Ack=275 Win=65280 Len=0
2150	31.763757	10.10.3.202	10.10.3.49	FTP	68	Request: OPTS UTF8 ON
2151	31.763970	10.10.3.49	10.10.3.202	FTP	112	Response: 200 OPTS UTF8 command successful - UTF8 encoding now ON.
2152	31.773323	10.10.3.202	10.10.3.49	FTP	79	Request: CWD /\344\270\264\346\227\266\346\225\260\346\215\256\344\272\244\346\215\242
2153	31.773690	10.10.3.49	10.10.3.202	FTP	83	Response: 250 CWD command successful.
2154	31.774233	10.10.3.202	10.10.3.49	FTP	62	Request: TYPE I
2155	31.774469	10.10.3.49	10.10.3.202	FTP	74	Response: 200 Type set to I.
2156	31.775567	10.10.3.202	10.10.3.49	FTP	80	Request: PORT 10,10,3,202,230,179
2157	31.775975	10.10.3.49	10.10.3.202	TCP	66	20 → 59059 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2158	31.776212	10.10.3.202	10.10.3.49	TCP	66	59059 → 20 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1
2159	31.776268	10.10.3.49	10.10.3.202	FTP	84	Response: 200 PORT command successful.
2160	31.776378	10.10.3.49	10.10.3.202	TCP	60	20 → 59059 [ACK] Seq=1 Ack=1 Win=65536 Len=0
2161	31.776418	10.10.3.202	10.10.3.49	FTP	101	Request: STOR FileZilla_3.18.0_win64-setup_bundled.exe
2162	31.776833	10.10.3.49	10.10.3.202	FTP	108	Response: 125 Data connection already open; Transfer starting.
2163	31.778293	10.10.3.202	10.10.3.49	FTP-DATA	14654	FTP Data: 14600 bytes
2164	31.778650	10.10.3.49	10.10.3.202	TCP	60	20 → 59059 [ACK] Seq=1 Ack=13141 Win=65536 Len=0
2165	31.778716	10.10.3.202	10.10.3.49	FTP-DATA	19034	FTP Data: 18980 bytes
2166	31.778815	10.10.3.49	10.10.3.202	TCP	60	20 → 59059 [ACK] Seq=1 Ack=14601 Win=65536 Len=0
2167	31.778847	10.10.3.202	10.10.3.49	FTP-DATA	2974	FTP Data: 2920 bytes
2168	31.779031	10.10.3.49	10.10.3.202	TCP	60	20 → 59059 [ACK] Seq=1 Ack=26281 Win=65536 Len=0
2169	31.779076	10.10.3.202	10.10.3.49	FTP-DATA	17574	FTP Data: 17520 bytes
2170	31.779349	10.10.3.49	10.10.3.202	TCP	60	20 → 59059 [ACK] Seq=1 Ack=36501 Win=65536 Len=0

```
Frame 2148: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0
    Interface id: 0 (\Device\NPF_{BCF12378-065C-40C1-B7C4-20495E031E17})
    Encapsulation type: Ethernet (1)
    Arrival Time: Jun  6, 2016 16:07:16.611161000 ��ú����ñ⁶��
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1465200436.611161000 seconds
    [Time delta from previous captured frame: 0.000076000 seconds]
```

```
0000  00000000 01010000 01010110 10110111 00000010 11000100 00000000 01010000   .PV....P
0008  01010110 10101111 11111010 11010110 00001000 00000000 01000101 00000000   V.....E.
0010  00000000 00111101 00111111 11101101 01000000 00000000 10000000 00000110   .=?.@...
0018  10011111 10111111 00001010 00001010 00000011 00110001 00001010 00001010   .....1..
0020  00000011 11001010 00000000 00010101 11100110 10110010 00100100 11100100   ......$.
```

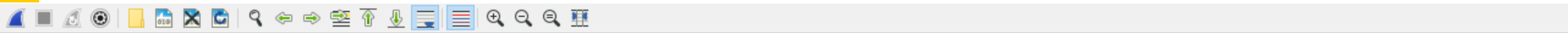
wireshark_pcapng_BCF12378-065C-40C1-B7C4-20495E031E17_20160606160644_a07920

分组: 2981 · 已显示: 624 (20.9%) · 已丢弃: 0 (0.0%)

配置文件: Default

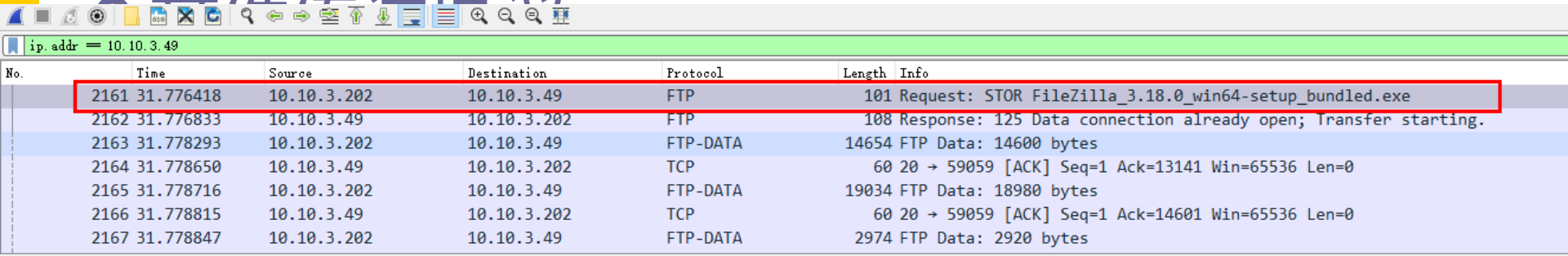
2.文件传送协议

2.2FTP的基本工作原理



ip.addr == 10.10.3.49

No.	Time	Source	Destination	Protocol	Length	Info
2161	31.776418	10.10.3.202	10.10.3.49	FTP	101	Request: STOR FileZilla_3.18.0_win64-setup_bundled.exe
2162	31.776833	10.10.3.49	10.10.3.202	FTP	108	Response: 125 Data connection already open; Transfer starting.
2163	31.778293	10.10.3.202	10.10.3.49	FTP-DATA	14654	FTP Data: 14600 bytes
2164	31.778650	10.10.3.49	10.10.3.202	TCP	60	20 → 59059 [ACK] Seq=1 Ack=13141 Win=65536 Len=0
2165	31.778716	10.10.3.202	10.10.3.49	FTP-DATA	19034	FTP Data: 18980 bytes
2166	31.778815	10.10.3.49	10.10.3.202	TCP	60	20 → 59059 [ACK] Seq=1 Ack=14601 Win=65536 Len=0
2167	31.778847	10.10.3.202	10.10.3.49	FTP-DATA	2974	FTP Data: 2920 bytes
2168	31.779031	10.10.3.49	10.10.3.202	TCP	60	20 → 59059 [ACK] Seq=1 Ack=26281 Win=65536 Len=0
2169	31.779076	10.10.3.202	10.10.3.49	FTP-DATA	17574	FTP Data: 17520 bytes
2170	31.779349	10.10.3.49	10.10.3.202	TCP	60	20 → 59059 [ACK] Seq=1 Ack=36501 Win=65536 Len=0
2171	31.779385	10.10.3.202	10.10.3.49	FTP-DATA	16114	FTP Data: 16060 bytes
2172	31.779443	10.10.3.49	10.10.3.202	TCP	60	20 → 59059 [ACK] Seq=1 Ack=51101 Win=65536 Len=0
2173	31.779475	10.10.3.202	10.10.3.49	FTP-DATA	20494	FTP Data: 20440 bytes



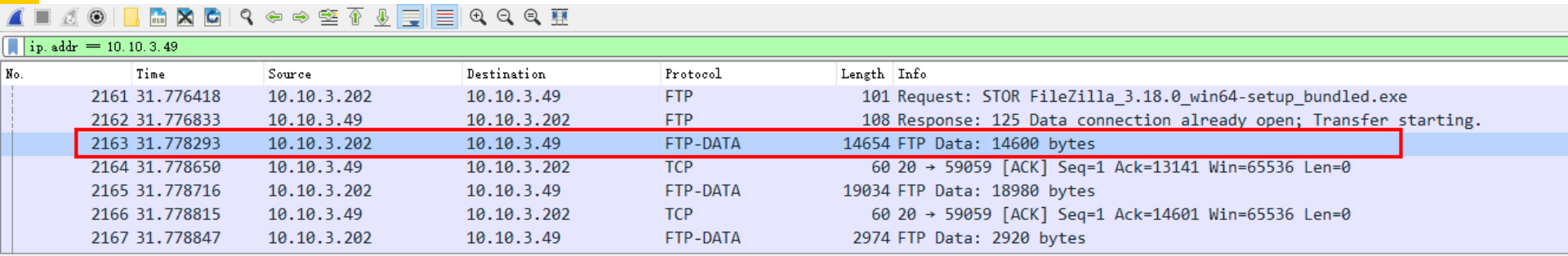
ip.addr == 10.10.3.49

No.	Time	Source	Destination	Protocol	Length	Info
2161	31.776418	10.10.3.202	10.10.3.49	FTP	101	Request: STOR FileZilla_3.18.0_win64-setup_bundled.exe
2162	31.776833	10.10.3.49	10.10.3.202	FTP	108	Response: 125 Data connection already open; Transfer starting.
2163	31.778293	10.10.3.202	10.10.3.49	FTP-DATA	14654	FTP Data: 14600 bytes
2164	31.778650	10.10.3.49	10.10.3.202	TCP	60	20 → 59059 [ACK] Seq=1 Ack=13141 Win=65536 Len=0
2165	31.778716	10.10.3.202	10.10.3.49	FTP-DATA	19034	FTP Data: 18980 bytes
2166	31.778815	10.10.3.49	10.10.3.202	TCP	60	20 → 59059 [ACK] Seq=1 Ack=14601 Win=65536 Len=0
2167	31.778847	10.10.3.202	10.10.3.49	FTP-DATA	2974	FTP Data: 2920 bytes

```
> Frame 2161: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interface 0
> Ethernet II, Src: Vmware_b7:02:c4 (00:50:56:b7:02:c4), Dst: Vmware_af:fa:d6 (00:50:56:af:fa:d6)
> Internet Protocol Version 4, Src: 10.10.3.202, Dst: 10.10.3.49
v Transmission Control Protocol, Src Port: 59058 (59058), Dst Port: 21 (21), Seq: 128, Ack: 412, Len: 47
    Source Port: 59058
    Destination Port: 21
    [Stream index: 8]
    [TCP Segment Len: 47]
    Sequence number: 128    (relative sequence number)
    [Next sequence number: 175    (relative sequence number)]
    Acknowledgment number: 412    (relative ack number)
    Header Length: 20 bytes
  > Flags: 0x018 (PSH, ACK)
    Window size value: 255
    [Calculated window size: 65280]
    [Window size scaling factor: 256]
  > Checksum: 0x1b58 [validation disabled]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
v File Transfer Protocol (FTP)
  v STOR FileZilla_3.18.0_win64-setup_bundled.exe\r\n
      Request command: STOR
      Request arg: FileZilla_3.18.0_win64-setup_bundled.exe
```

2.文件传送协议

2.2FTP的基本工作原理



ip.addr == 10.10.3.49

No.	Time	Source	Destination	Protocol	Length	Info
2161	31.776418	10.10.3.202	10.10.3.49	FTP	101	Request: STOR FileZilla_3.18.0_win64-setup_bundled.exe
2162	31.776833	10.10.3.49	10.10.3.202	FTP	108	Response: 125 Data connection already open; Transfer starting.
2163	31.778293	10.10.3.202	10.10.3.49	FTP-DATA	14654	FTP Data: 14600 bytes
2164	31.778650	10.10.3.49	10.10.3.202	TCP	60	20 → 59059 [ACK] Seq=1 Ack=13141 Win=65536 Len=0
2165	31.778716	10.10.3.202	10.10.3.49	FTP-DATA	19034	FTP Data: 18980 bytes
2166	31.778815	10.10.3.49	10.10.3.202	TCP	60	20 → 59059 [ACK] Seq=1 Ack=14601 Win=65536 Len=0
2167	31.778847	10.10.3.202	10.10.3.49	FTP-DATA	2974	FTP Data: 2920 bytes

```
> Frame 2163: 14654 bytes on wire (117232 bits), 14654 bytes captured (117232 bits) on interface 0
> Ethernet II, Src: Vmware_b7:02:c4 (00:50:56:b7:02:c4), Dst: Vmware_af:fa:d6 (00:50:56:af:fa:d6)
> Internet Protocol Version 4, Src: 10.10.3.202, Dst: 10.10.3.49
v Transmission Control Protocol, Src Port: 59059 (59059), Dst Port: 20 (20), Seq: 1, Ack: 1, Len: 14600
    Source Port: 59059
    Destination Port: 20
    [Stream index: 9]
    [TCP Segment Len: 14600]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 14601    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Header Length: 20 bytes
  > Flags: 0x010 (ACK)
    Window size value: 32768
    [Calculated window size: 4194304]
    [Window size scaling factor: 128]
  > Checksum: 0x1b15 [validation disabled]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
FTP Data (14600 bytes data)
```

2.文件传送协议

- NFS允许应用进程打开一个远地文件，并能在该文件的某一个特定的位置上开始读写数据。
- NFS可使用户只复制一个大文件中的一个很小的片段，而不需要复制整个大文件。
- 对于上述例子，计算机 A 的 NFS 客户软件，把要添加的数据和在文件后面写数据的请求一起发送到远地的计算机 B 的 NFS 服务器。NFS 服务器更新文件后返回应答信息。
- 在网络上传送的只是少量的修改数据。

2.文件传送协议

- TFTP是一个很小且易于实现的文件传送协议。
- TFTP使用客户服务器方式和使用 UDP 数据报，因此TFTP需要有自己的差错改正措施。
- TFTP只支持文件传输而不支持交互。
- TFTP没有一个庞大的命令集，没有列目录的功能，也不能对用户进行身份鉴别。

2.文件传送协议

- TFTP的主要特点是：
  - 每次传送的数据PDU中有512字节的数据，但最后一次可不足512字节。
  - 数据PDU也称为文件块（block），每个块按序编号，从1开始。
  - 支持ASCII码或二进制传送。
  - 可对文件进行读或写。
  - 使用很简单的首部。

2.文件传送协议

- TFTP的工作很像停止等待协议：
  - 发送完一个文件块后就等待对方的确认，确认时应指明所确认的块编号。
  - 发完数据后在规定时间内收不到确认就要重发数据PDU。
  - 发送确认PDU的一方若在规定时间内收不到下一个文件块，也要重发确认PDU。这样就可保证文件的传送不致因某一个数据报的丢失而告失败。

2.文件传送协议

- TFTP的工作很像停止等待协议：
  - 在一开始工作时。TFTP 客户进程发送一个读请求 PDU 或写请求 PDU 给 TFTP 服务器进程，其熟知端口号码为 69。
  - TFTP 服务器进程要选择一个新的端口和 TFTP 客户进程进行通信。
  - 若文件长度恰好为 512 字节的整数倍，则在文件传送完毕后，还必须在最后发送一个只含首部而无数据的数据 PDU。
  - 若文件长度不是 512 字节的整数倍，则最后传送数据 PDU 的数据字段一定不满512字节，这正好可作为文件结束的标志。

2.文件传送协议

- TFTP是FTP的简化版本，在确切地知道想要得到的文件名及准确位置情况下，才可有选择地使用TFTP。
- TFTP是一个非常易用的、快捷的程序。
  - TFTP不提供目录浏览的功能，只能完成文件的发送和接收操作。
  - TFTP发送比FTP更小的数据块，同时没有FTP所需要的传送确认，因而是不可靠的。

2.文件传送协议

- 在用途上：
  - FTP是完整、面向会话、常规用途文件传输协议。
  - TFTP用作特殊目的文件传输协议。
- 在交互性上：
  - FTP允许交互通信。
  - TFTP仅允许单向传输文件。
- 在认证上：
  - FTP提供身份验证。
  - TFTP不支持身份验证。
- 在运输层上：
  - FTP使用已知TCP端口号21作为控制连接，TCP端口号20作为数据连接。
  - TFTP使用UDP端口号69作为文件传输活动。

3.远程终端协议TELNET

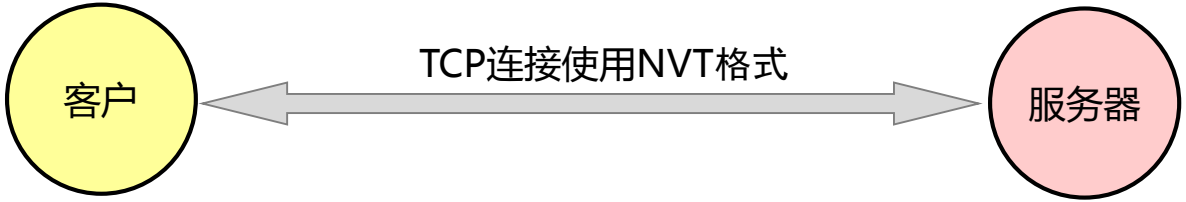
- TELNET是一个简单的远程终端协议，也是因特网的正式标准【RFC 854】。
- 用户用TELNET就可在其所在地通过TCP连接注册（即登录）到远地的另一个主机上（使用主机名或 IP 地址）。
- TELNET能将用户的击键传到远地主机，同时也能将远地主机的输出通过TCP连接返回到用户屏幕。这种服务是透明的，因为用户感觉到好像键盘和显示器是直接连在远地主机上。

3.远程终端协议TELNET

- TELNET使用客户/服务器方式。在本地系统运行TELNET客户进程，而在远地主机则运行TELNET服务器进程。
- 和FTP的情况相似，服务器中的主进程等待新的请求，并产生从属进程来处理每一个连接。

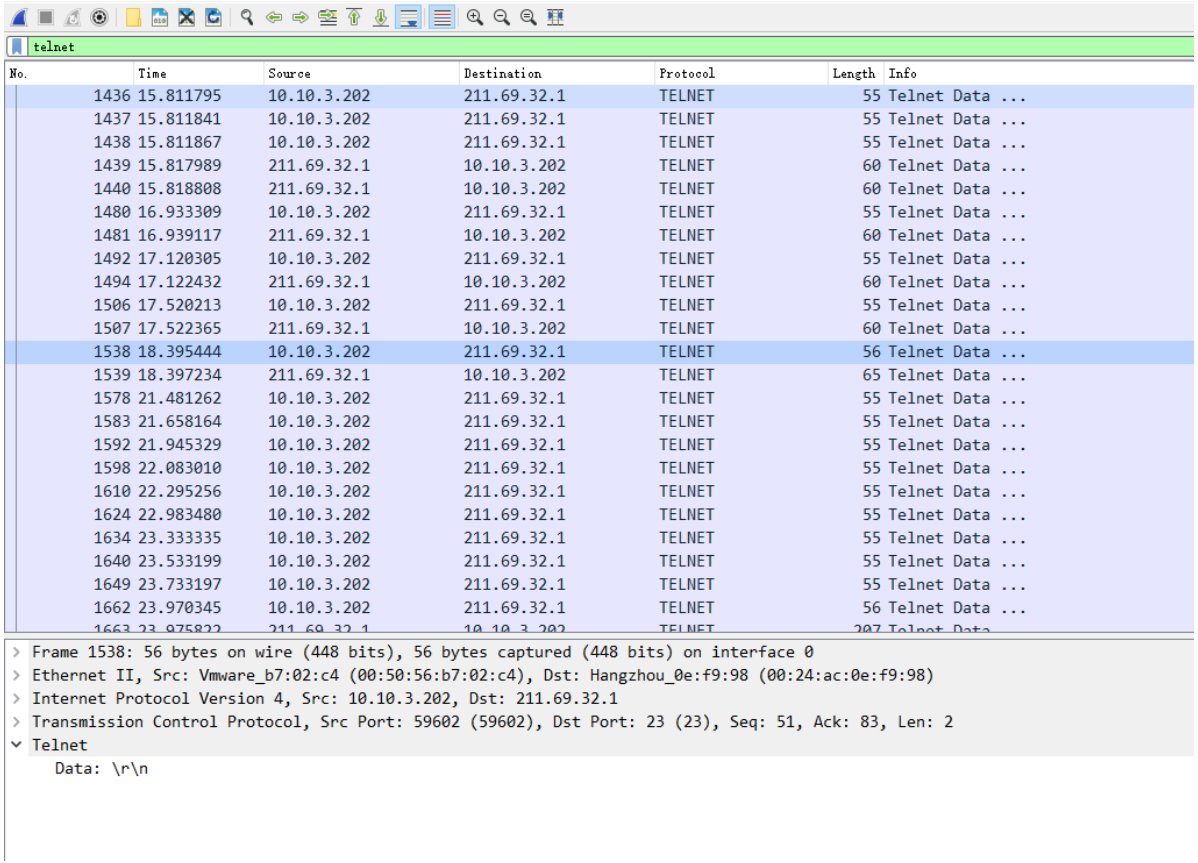
3.远程终端协议TELNET

- TELNET使用网络虚拟终端NVT格式。
  - 客户软件把用户的击键和命令转换成NVT格式，并送交服务器。
  - 服务器软件把收到的数据和命令，从NVT格式转换成远地系统所需的格式。
  - 向用户返回数据时，服务器把远地系统的格式转换为NVT格式，本地客户再从NVT格式转换到本地系统所需的格式。



3.远程终端协议TELNET

3.2TELNET的基本工作原理



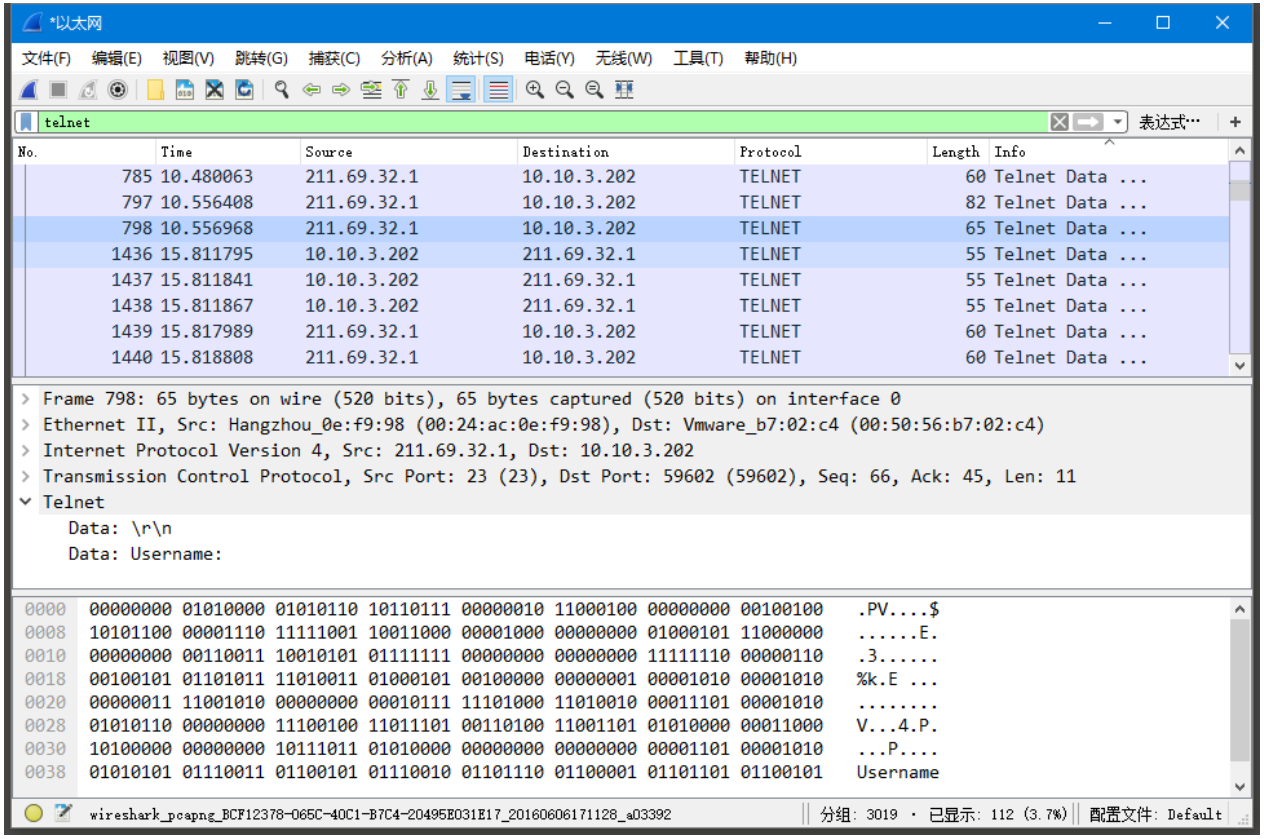
telnet

No.	Time	Source	Destination	Protocol	Length	Info
1436	15.811795	10.10.3.202	211.69.32.1	TELNET	55	Telnet Data ...
1437	15.811841	10.10.3.202	211.69.32.1	TELNET	55	Telnet Data ...
1438	15.811867	10.10.3.202	211.69.32.1	TELNET	55	Telnet Data ...
1439	15.817989	211.69.32.1	10.10.3.202	TELNET	60	Telnet Data ...
1440	15.818808	211.69.32.1	10.10.3.202	TELNET	60	Telnet Data ...
1480	16.933309	10.10.3.202	211.69.32.1	TELNET	55	Telnet Data ...
1481	16.939117	211.69.32.1	10.10.3.202	TELNET	60	Telnet Data ...
1492	17.120305	10.10.3.202	211.69.32.1	TELNET	55	Telnet Data ...
1494	17.122432	211.69.32.1	10.10.3.202	TELNET	60	Telnet Data ...
1506	17.520213	10.10.3.202	211.69.32.1	TELNET	55	Telnet Data ...
1507	17.522365	211.69.32.1	10.10.3.202	TELNET	60	Telnet Data ...
1538	18.395444	10.10.3.202	211.69.32.1	TELNET	56	Telnet Data ...
1539	18.397234	211.69.32.1	10.10.3.202	TELNET	65	Telnet Data ...
1578	21.481262	10.10.3.202	211.69.32.1	TELNET	55	Telnet Data ...
1583	21.658164	10.10.3.202	211.69.32.1	TELNET	55	Telnet Data ...
1592	21.945329	10.10.3.202	211.69.32.1	TELNET	55	Telnet Data ...
1598	22.083010	10.10.3.202	211.69.32.1	TELNET	55	Telnet Data ...
1610	22.295256	10.10.3.202	211.69.32.1	TELNET	55	Telnet Data ...
1624	22.983480	10.10.3.202	211.69.32.1	TELNET	55	Telnet Data ...
1634	23.333335	10.10.3.202	211.69.32.1	TELNET	55	Telnet Data ...
1640	23.533199	10.10.3.202	211.69.32.1	TELNET	55	Telnet Data ...
1649	23.733197	10.10.3.202	211.69.32.1	TELNET	55	Telnet Data ...
1662	23.970345	10.10.3.202	211.69.32.1	TELNET	56	Telnet Data ...
1663	23.975822	211.69.32.1	10.10.3.202	TELNET	207	Telnet Data

> Frame 1538: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
> Ethernet II, Src: Vmware_b7:02:c4 (00:50:56:b7:02:c4), Dst: Hangzhou_0e:f9:98 (00:24:ac:0e:f9:98)
> Internet Protocol Version 4, Src: 10.10.3.202, Dst: 211.69.32.1
> Transmission Control Protocol, Src Port: 59602 (59602), Dst Port: 23 (23), Seq: 51, Ack: 83, Len: 2
v Telnet
    Data: \r\n

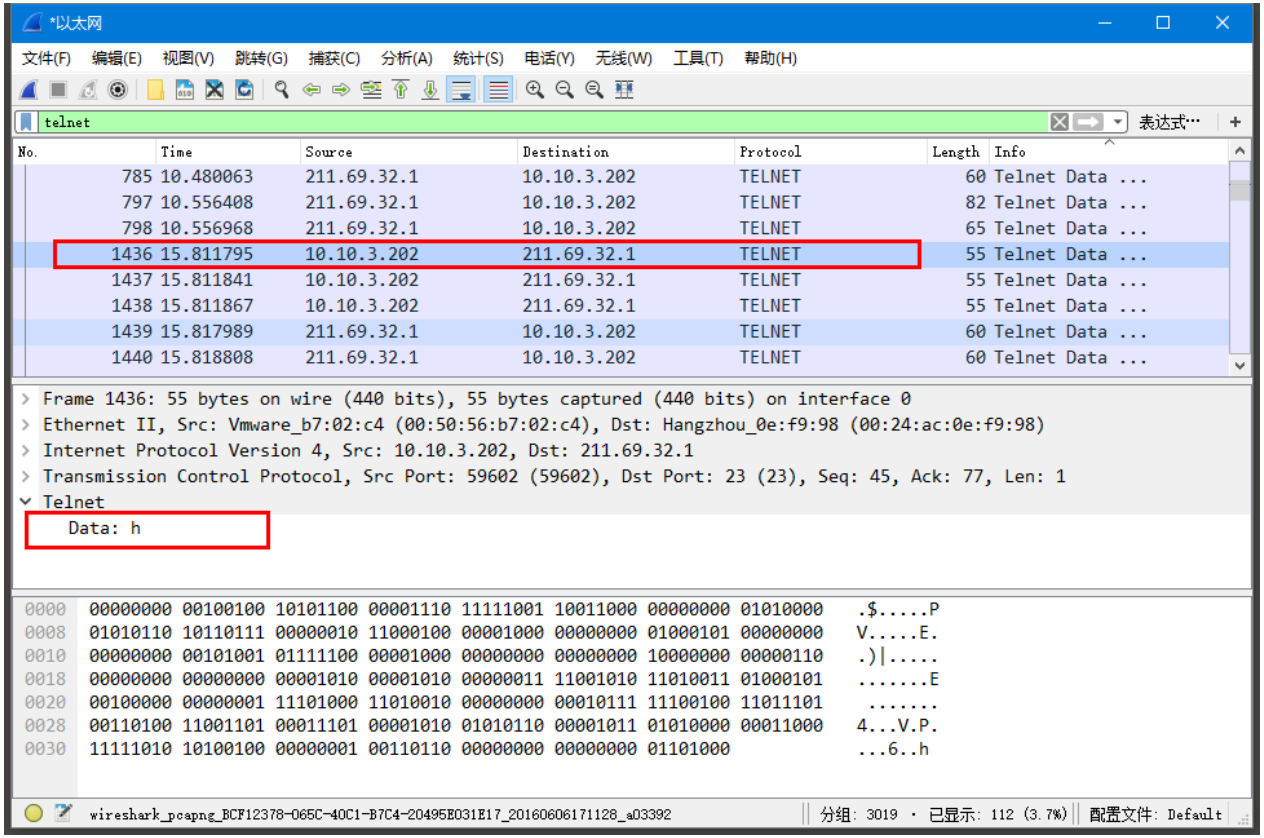
3.远程终端协议TELNET

3.2TELNET的基本工作原理



3.远程终端协议TELNET

3.2TELNET的基本工作原理



3.远

工作原理

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

telnet

No.	Time	Source	Destination	Protocol	Length	Info
2189	34.512085	211.69.32.1	10.10.3.202	TELNET	70	Telnet Data ...
2228	35.046339	10.10.3.202	211.69.32.1	TELNET	55	Telnet Data ...
2229	35.048143	211.69.32.1	10.10.3.202	TELNET	106	Telnet Data ...
2230	35.048861	211.69.32.1	10.10.3.202	TELNET	1054	Telnet Data ...
2232	35.049684	211.69.32.1	10.10.3.202	TELNET	284	Telnet Data ...
2233	35.050467	211.69.32.1	10.10.3.202	TELNET	68	Telnet Data ...
2448	38.506900	10.10.3.202	211.69.32.1	TELNET	55	Telnet Data ...
2449	38.508527	211.69.32.1	10.10.3.202	TELNET	60	Telnet Data ...
2459	38.583770	10.10.3.202	211.69.32.1	TELNET	55	Telnet Data ...

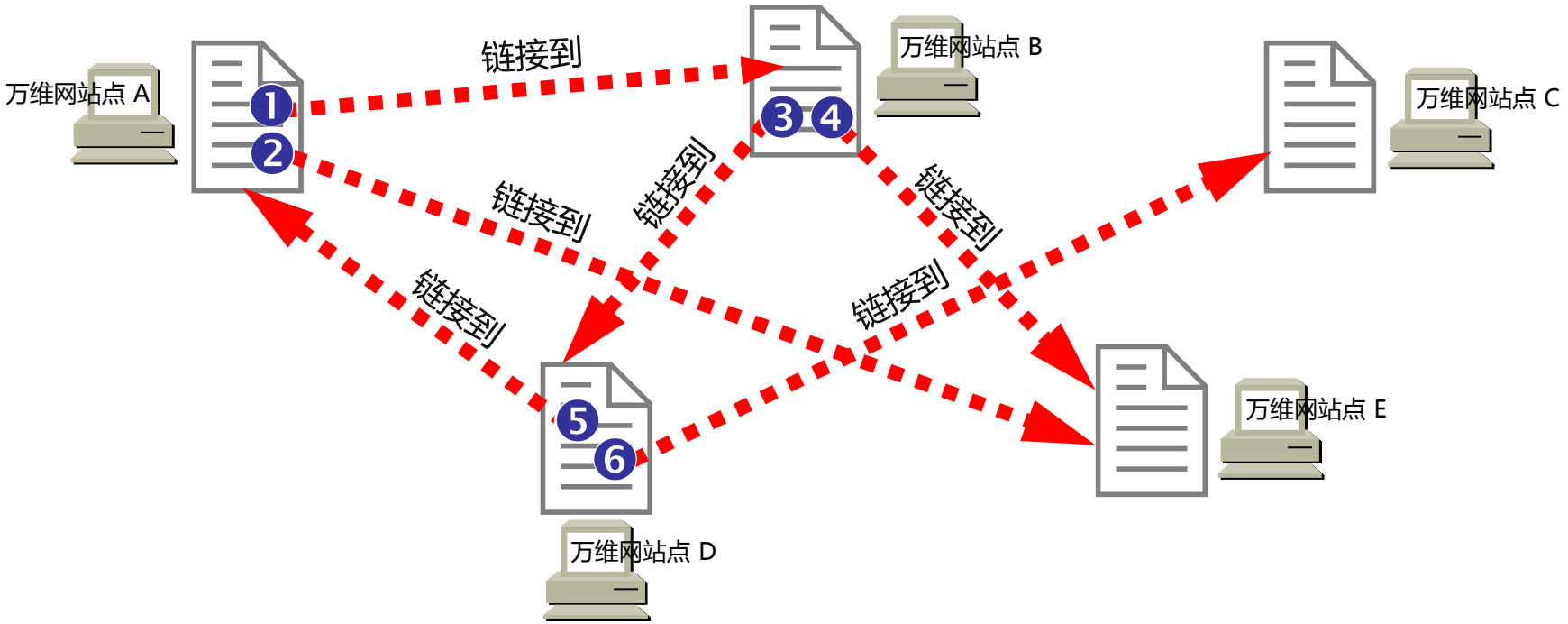
```
> Frame 2230: 1054 bytes on wire (8432 bits), 1054 bytes captured (8432 bits) on interface 0
> Ethernet II, Src: Hangzhou_0e:f9:98 (00:24:ac:0e:f9:98), Dst: Vmware_b7:02:c4 (00:50:56:b7:02:c4)
> Internet Protocol Version 4, Src: 211.69.32.1, Dst: 10.10.3.202
> Transmission Control Protocol, Src Port: 23 (23), Dst Port: 59602 (59602), Seq: 18223, Ack: 82, Len: 1000
v Telnet
    Data: TNQA                0%        0/  8cc2a5      TNQAC                     \r\n
    Data: TTNQ                0%        0/    45bb      TTNQAS                    \r\n
    Data: TARP                0%        0/       0      TARPING                   \r\n
    Data: TTVP                0%        0/       0      TTVPLS                    \r\n
    Data: L2                  0%        0/  975d38      L2                        \r\n
    Data: VRRP                0%        0/ 17e4f84      VRRP                      \r\n
    Data: L2_P                0%        0/ 27ac3a0      L2_PR                     \r\n
    Data: ARP                 0%        0/       0      ARP                       \r\n
    Data: NTPT                0%        0/   fd3c7      NTPT task                 \r\n
    Data: SIMC                0%        0/       0      SIMC                      \r\n
    Data: RMON                0%        0/  176c6e      RMONRemote monitoring     \r\n
    Data: IFLP                0%        0/  15348c      IFLP                      \r\n
    Data: bcmD
```

```
0000  00000000 01010000 01010110 10110111 00000010 11000100 00000000 00100100   .PV....$
0008  10101100 00001110 11111001 10011000 00001000 00000000 01000101 11000000   ......E.
0010  00000100 00010000 10011111 01101111 00000000 00000000 11111110 00000110   ...o....
0018  00010111 10011110 11010011 01000101 00100000 00000001 00001010 00001010   ...E ...
0020  00000011 11001010 00000000 00010111 11101000 11010010 00011101 00001010   ........
0028  10011100 11101101 11100100 11011101 00110100 11110010 01010000 00011000   ....4.P.
0030  10100000 00000000 11001110 11001100 00000000 00000000 01010100 01001110   ......TN
0038  01010001 01000001 00100000 00100000 00100000 00100000 00100000 00100000   QA
0040  00100000 00100000 00100000 00100000 00100000 00100000 00100000 00100000
0048  00100000 00100000 00100000 00100000 00110000 00100101 00100000 00100000       0%
```

4.万维网WWW

- 万维网WWW(World Wide Web)不是某种特殊的计算机网络。
- 万维网是一个大规模的、联机式的信息储藏所。
- 万维网用链接的方法能非常方便地从因特网上的一个站点访问另一个站点，从而主动地按需获取丰富的信息。
- 这种访问方式称为“链接”。

4.万维网WWW


万维网站点 A
链接到
万维网站点 B
万维网站点 C
链接到
链接到
链接到
链接到
链接到
万维网站点 E
万维网站点 D
1
2
3
4
5
6

4.万维网WWW

- 万维网是分布式超媒体(hypermedia)系统，它是超文本(hypertext)系统的扩充。
- 一个超文本由多个信息源链接成。利用一个链接可使用户找到另一个文档。这些文档可以位于世界上任何一个接在因特网上的超文本系统中。超文本是万维网的基础。
- 超媒体与超文本的区别是文档内容不同。超文本文档仅包含文本信息，而超媒体文档还包含其他表示方式的信息，如图形、图像、声音、动画，甚至活动视频图像。

4.万维网WWW

- 万维网以客户/服务器方式工作。
- 浏览器就是在用户计算机上的万维网客户程序。万维网文档所驻留的计算机则运行服务器程序，因此这个计算机也称为万维网服务器（Web Server）。
- 客户程序向服务器程序发出请求，服务器程序向客户程序送回客户所要的万维网文档。
- 在一个客户程序主窗口上显示出的万维网文档称为页面(page)。

4.万维网WWW

- 万维网必须解决的问题：
  - 怎样标志分布在整个因特网上的万维网文档？
    - 使用统一资源定位符 URL (Uniform Resource Locator)来标志万维网上的各种文档。
    - 使每一个文档在整个
  - 用何协议实现万维网上各种超链的链接？
    - 在万维网客户程序与万维网服务器程序之间进行交互所使用的协议，是超文本传送协议 HTTP (HyperText Transfer Protocol)。
    - HTTP 是一个应用层协议，它使用 TCP 连接进行可靠的传送。因特网的范围内具有唯一的标识符 URL。

4.万维网WWW

- 万维网必须解决的问题：
  - 怎样使各种万维网文档都能在因特网上的各种计算机上显示出来，同时使用户清楚地知道在什么地方存在着超链？
    - 超文本标记语言 HTML (HyperText Markup Language)使得万维网页面的设计者可以很方便地用一个超链从本页面的某处链接到因特网上的任何一个万维网页面，并且能够在自己的计算机屏幕上将这些页面显示出来。
  - 怎样使用户能够很方便地找到所需的信息？
    - 为了在万维网上方便地查找信息，用户可使用各种的搜索工具（即搜索引擎）。

4.万维网WWW

- URL的格式：
  - 统一资源定位符URL是对可以从因特网上得到的资源的位置和访问方法的一种简洁的表示。
  - URL给资源的位置提供一种抽象的识别方法，并用这种方法给资源定位。
  - 只要能够对资源定位，系统就可以对资源进行各种操作，如存取、更新、替换和查找其属性。
  - URL相当于一个文件名在网络范围的扩展。因此URL是与因特网相连的机器上的任何可访问对象的一个指针。

4.万维网WWW

- URL的一般形式：
  - 由以冒号隔开的两大部分组成，并且在URL中的字符对大写或小写没有要求。
  - URL的一般形式是：

<协议>://<主机>:<端口>/<路径>

ftp —— 文件传送协议FTP

http —— 超文本传送协议HTTP

News —— USENET新闻

4.万维网WWW

- URL的一般形式：
  - 由以冒号隔开的两大部分组成，并且在URL中的字符对大写或小写没有要求。
  - URL的一般形式是：

<协议>://<主机>:<端口>/<路径>

<主机>是存放资源的主机在因特网中的域名

4.万维网WWW

- URL的一般形式：
  - 由以冒号隔开的两大部分组成，并且在URL中的字符对大写或小写没有要求。
  - URL的一般形式是：

<协议>://<主机>:<端口>/<路径>

使用默认值时可以省略

浏览器可以自动补齐

4.万维网WWW

- 使用HTTP的URL：
  - 使用 HTTP 的 URL 的一般形式：

http://<主机>:<端口>/<路径>

表示使用HTTP协议

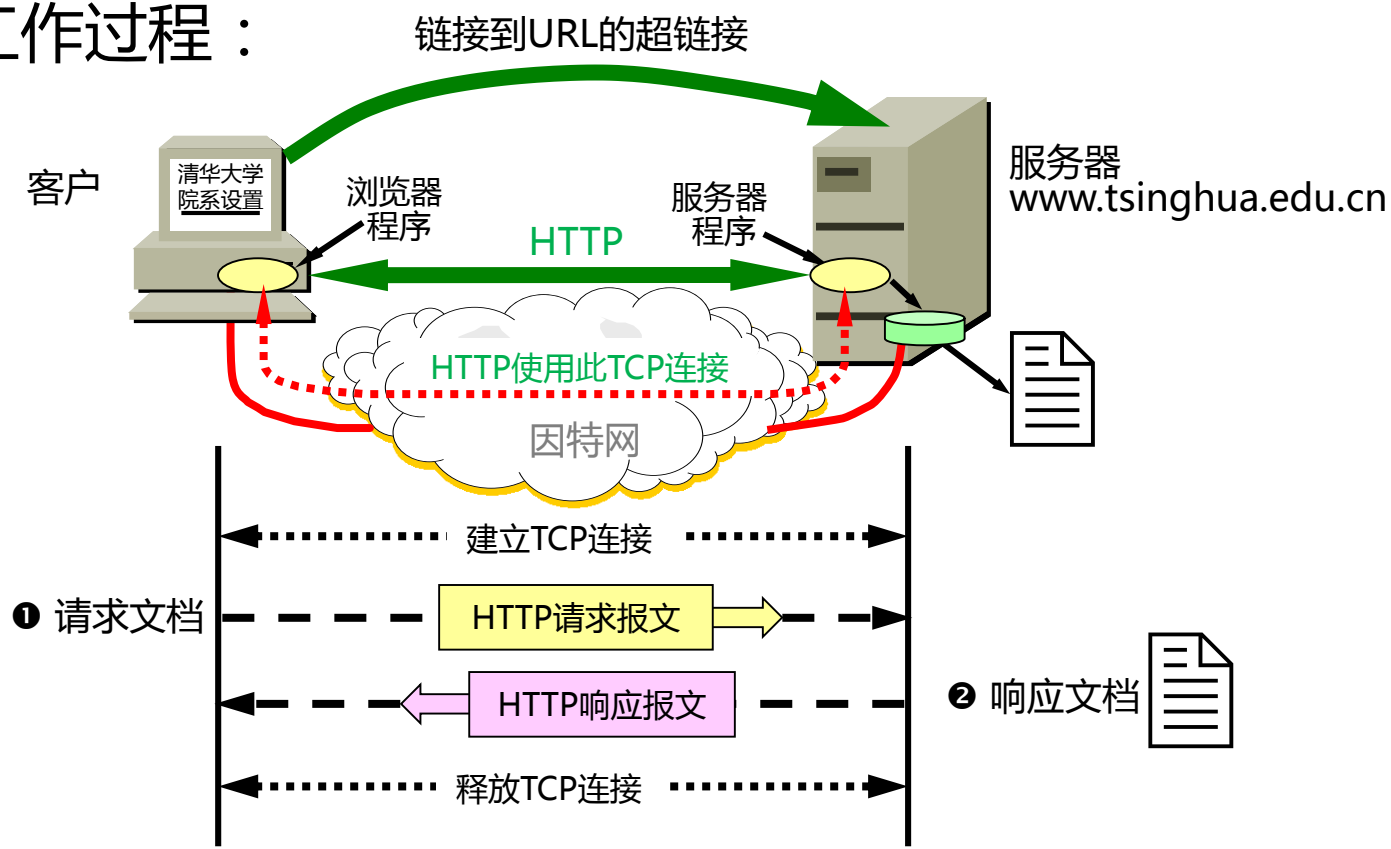
http://www.csdn.net/
http://list.jd.com/list.html?cat=737,13297,13298
http://www.hactcm.edu.cn/info/1014/11646.htm

4.万维网WWW

- HTTP的操作过程：
  - 为了使超文本的链接能够高效率地完成，需要用HTTP协议来传送一切必须的信息。
  - 从层次的角度看，HTTP是面向事务的(transaction-oriented)应用层协议，它是万维网上能够可靠地交换文件（包括文本、声音、图像等各种多媒体文件）的重要基础。

4.万维网WWW

- 万维网的工作过程：



4.万维网WWW

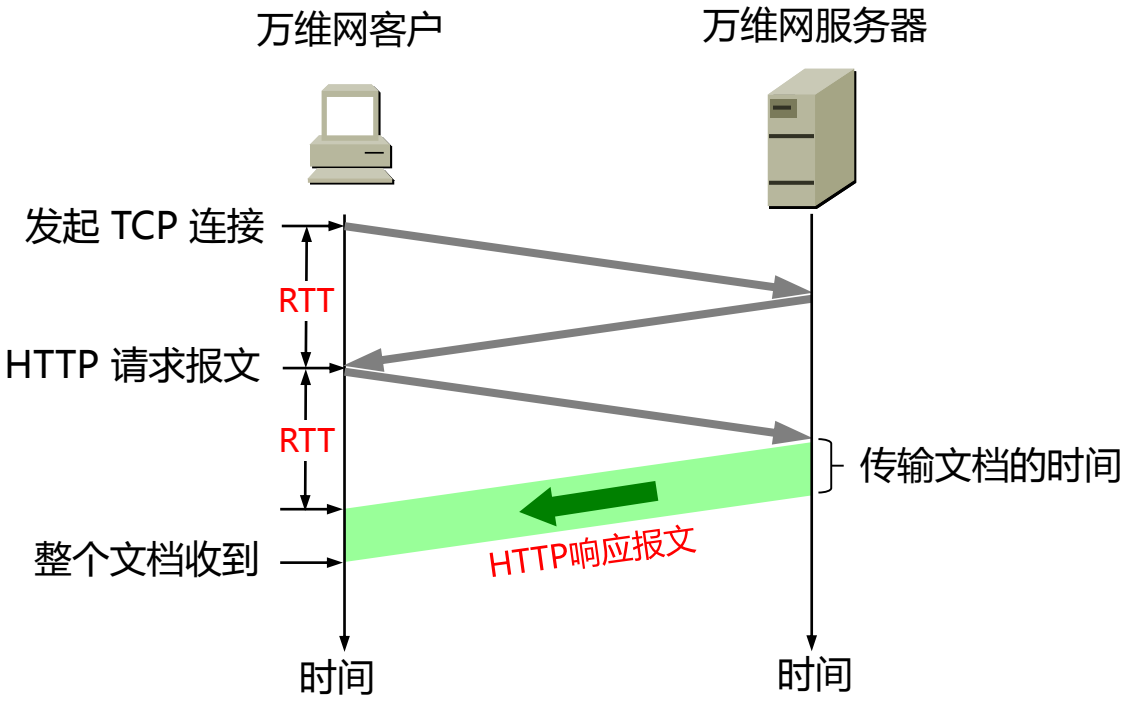
- HTTP的操作过程：（用户点击鼠标后所发生的事件）
  - 浏览器分析超链指向页面的URL。
  - 浏览器向DNS请求解析www.tsinghua.edu.cn的IP地址。
  - 域名系统DNS解析出清华大学服务器的IP地址。
  - 浏览器与服务器建立TCP连接
  - 浏览器发出取文件命令：GET /chn/yxsz/index.htm。
  - 服务器给出响应，把文件index.htm发给浏览器。
  - TCP连接释放。
  - 浏览器显示“清华大学院系设置”文件中的所有文本。

4.万维网WWW

- HTTP的主要特点：
  - HTTP是面向事务的客户服务器协议。
  - HTTP 1.0协议是无状态的(stateless)。
  - HTTP协议本身也是无连接的，虽然它使用了面向连接的TCP向上提供的服务。

4.万维网WWW

- 请求一个万维网文档所需的时间：



4.万维网WWW

- 持续连接(persistent connection)：
  - HTTP/1.1协议使用持续连接。
  - 万维网服务器在发送响应后仍然在一段时间内保持这条连接，使同一个客户（浏览器）和该服务器可以继续在这条连接上传送后续的HTTP 请求报文和响应报文。
  - 这并不局限于传送同一个页面上链接的文档，而是只要这些文档都在同一个服务器上就行。
  - 目前浏览器的默认设置就是使用HTTP/1.1。

4.万维网WWW

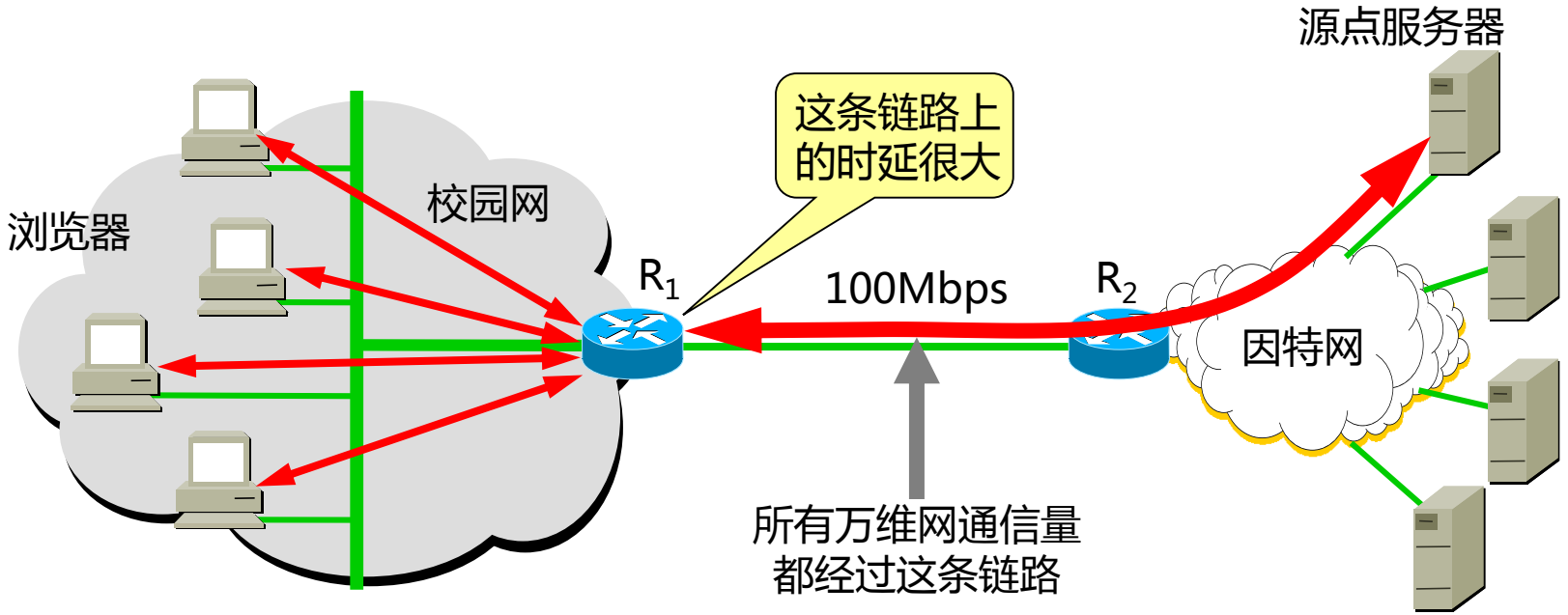
- 持续连接(persistent connection)：
  - 持续连接的两种工作方式为：非流水线方式、流水线方式。
    - 非流水线方式：客户在收到前一个响应后才能发出下一个请求。这比非持续连接的两倍RTT的开销节省了建立TCP连接所需的一个RTT时间。但服务器在发送完一个对象后，其TCP连接就处于空闲状态，浪费了服务器资源。
    - 流水线方式：客户在收到HTTP的响应报文之前就能够接着发送新的请求报文。一个接一个的请求报文到达服务器后，服务器就可连续发回响应报文。使用流水线方式时，客户访问所有的对象只需花费一个RTT时间，使TCP连接中的空闲时间减少，提高了下载文档效率。

4.万维网WWW

- 代理服务器(proxy server) ：
  - 代理服务器(proxy server)又称为万维网高速缓存(Web cache)，它代表浏览器发出HTTP请求。
  - 万维网高速缓存把最近的一些请求和响应暂存在本地磁盘中。
  - 当与暂时存放的请求相同的新请求到达时，万维网高速缓存就把暂存的响应发送出去，而不需要按 URL 的地址再去因特网访问该资源。

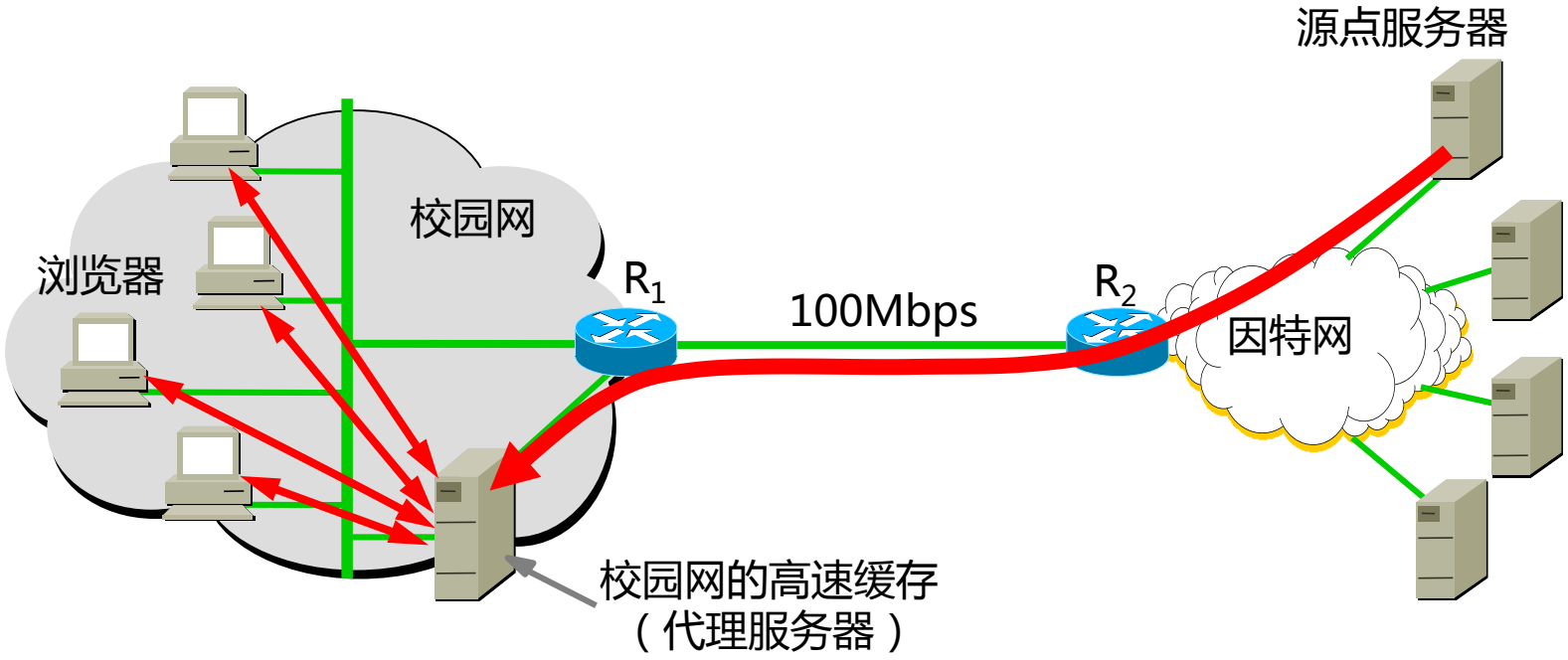
4.万维网WWW

- 代理服务器(proxy server) ：



4.万维网WWW

- 代理服务器(proxy server) ：

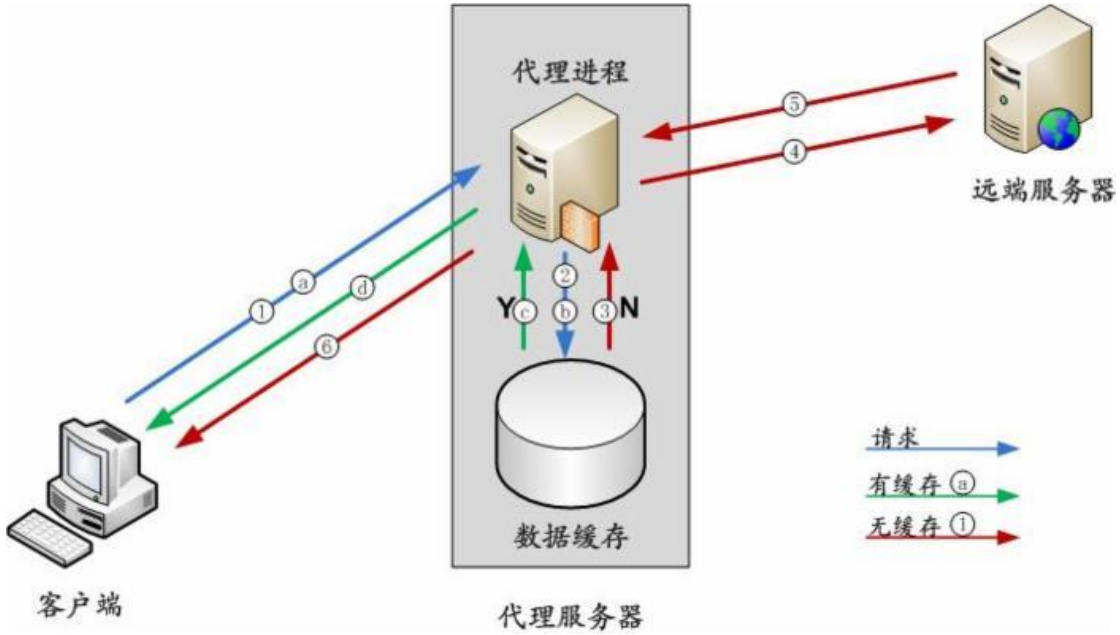


4.万维网WWW

- 代理服务器(proxy server) ：
  - 浏览器访问因特网的服务器时，要先与校园网的高速缓存建立TCP连接，并向高速缓存发出HTTP请求报文
  - 若高速缓存已经存放了所请求的对象，则将此对象放入HTTP响应报文中返回给浏览器。
  - 否则，高速缓存就代表发出请求的用户浏览器，与因特网上的源点服务器建立TCP连接，并发送HTTP请求报文。
  - 源点服务器将所请求的对象放在HTTP响应报文中返回给校园网的高速缓存。
  - 高速缓存收到此对象后，先复制在其本地存储器中（为今后使用），然后再将该对象放在HTTP响应报文中，通过已建立的TCP连接，返回给请求该对象的浏览器。

4.万维网WWW

- 代理服务器(proxy server) ：



4.万维网WWW

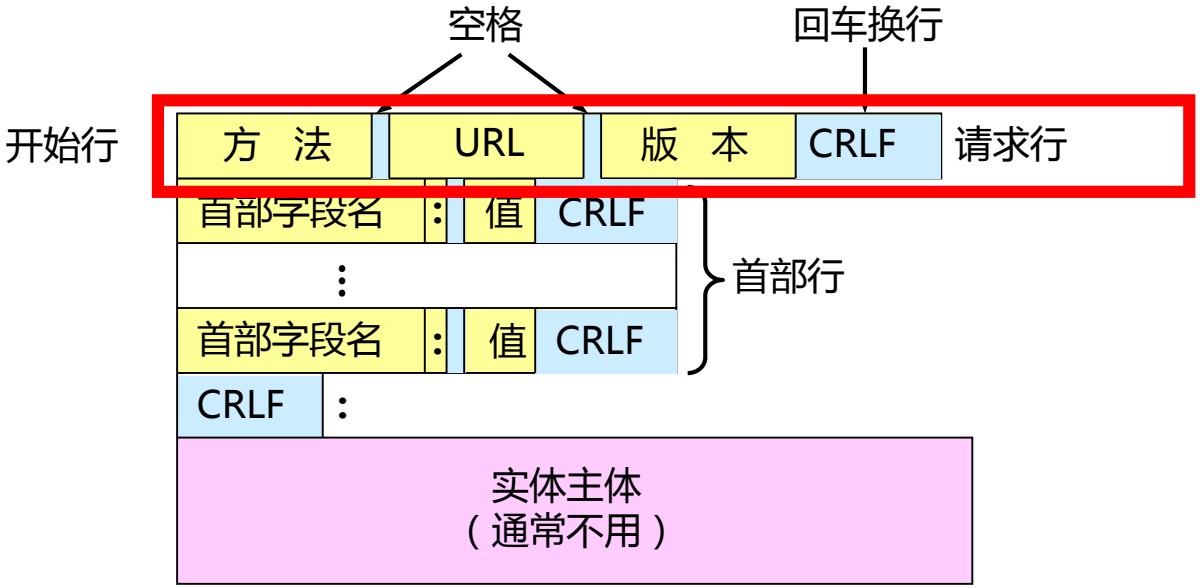
- 现场演示：
  - 使用CCProxy建立代理服务器。
  - 使用Putty建立代理服务器。
  - 演示浏览器中代理服务器的配置方法。

4.万维网WWW

- HTTP有两类报文：请求报文、响应报文。
  - 请求报文：从客户向服务器发送请求报文。
  - 响应报文：从服务器到客户的回答。
  - 由于HTTP是面向正文的(text-oriented)，因此在报文中的每一个字段都是一些ASCII码串，因而每个字段的长度都是不确定的。

4.万维网WWW

- HTTP请求报文的结构。
  - 报文由三个部分组成，即开始行、首部行和实体主体。
  - 在请求报文中，开始行就是请求行。



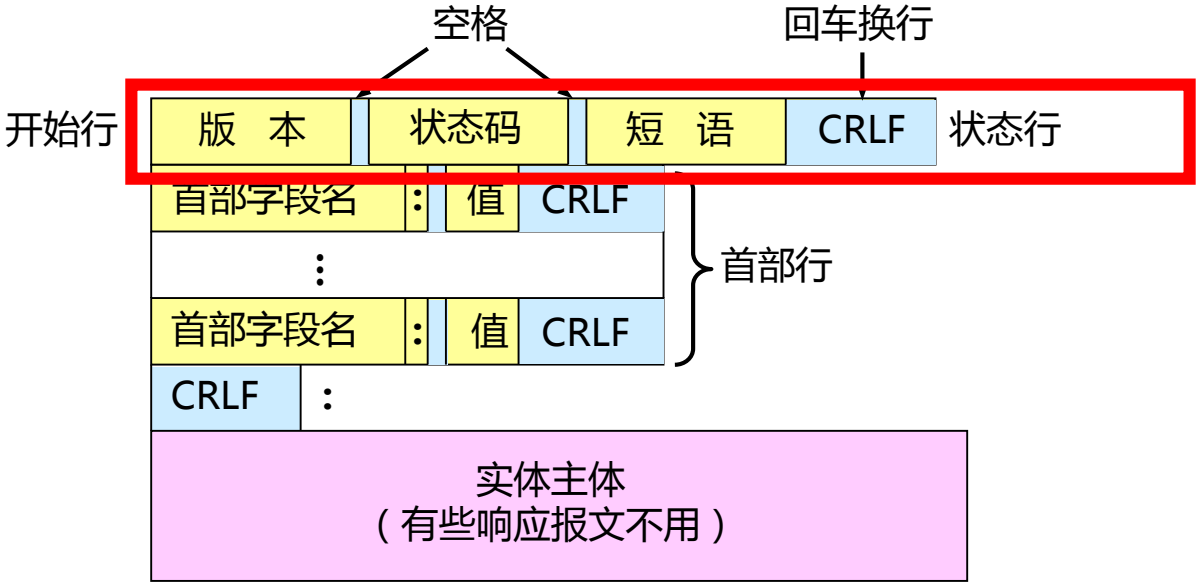
4.万维网WWW

- HTTP请求报文的结构。
  - “方法”就是对所请求的对象进行的操作，方法实际上就是命令。
  - 请求报文的类型是由它所采用的方法决定的。
    - OPTION　请求一些选项的信息
    - GET　请求读取由URL所标志的信息，并返回实体主体
    - HEAD　请求读取由URL所标志的信息的首部
    - POST　向指定资源提交数据进行处理请求，数据被包含在请求体中
    - PUT　从客户端向服务器传送的数据取代指定的文档的内容。
    - DELETE　删除指明的URL所标志的资源
    - TRACE　回显服务器收到的请求，主要用于测试或诊断。
    - CONNECT　HTTP/1.1预留给能够将连接改为管道方式的代理服务器。

https://www.w3.org/Protocols/rfc2616/rfc2616-sec9.html

4.万维网WWW

- HTTP响应报文的结构。
  - 响应报文的开始行是状态行。
  - 状态行包括三项内容，即 HTTP 的版本，状态码，以及解释状态码的简单短语。



4.万维网WWW

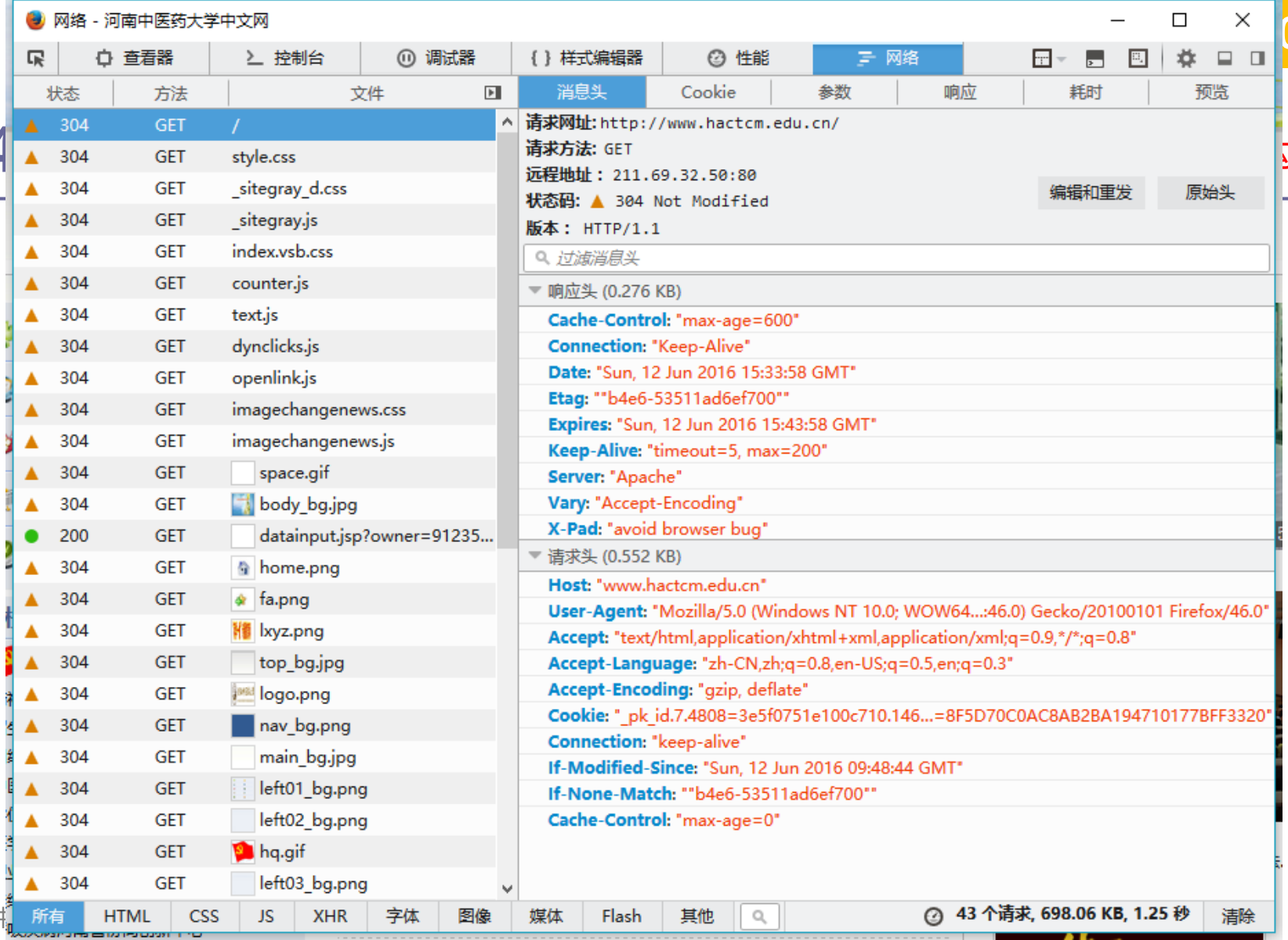
- HTTP响应报文的结构。
  - 状态码都是三位数字 。
    - 1xx　　表示通知信息的，如请求收到了或正在进行处理。
    - 2xx　　表示成功，如接受或知道了。
    - 3xx　　表示重定向，表示要完成请求还必须采取进一步的行动。
    - 4xx　　表示客户的差错，如请求中有错误的语法或不能完成。
    - 5xx　　表示服务器的差错，如服务器失效无法完成请求。

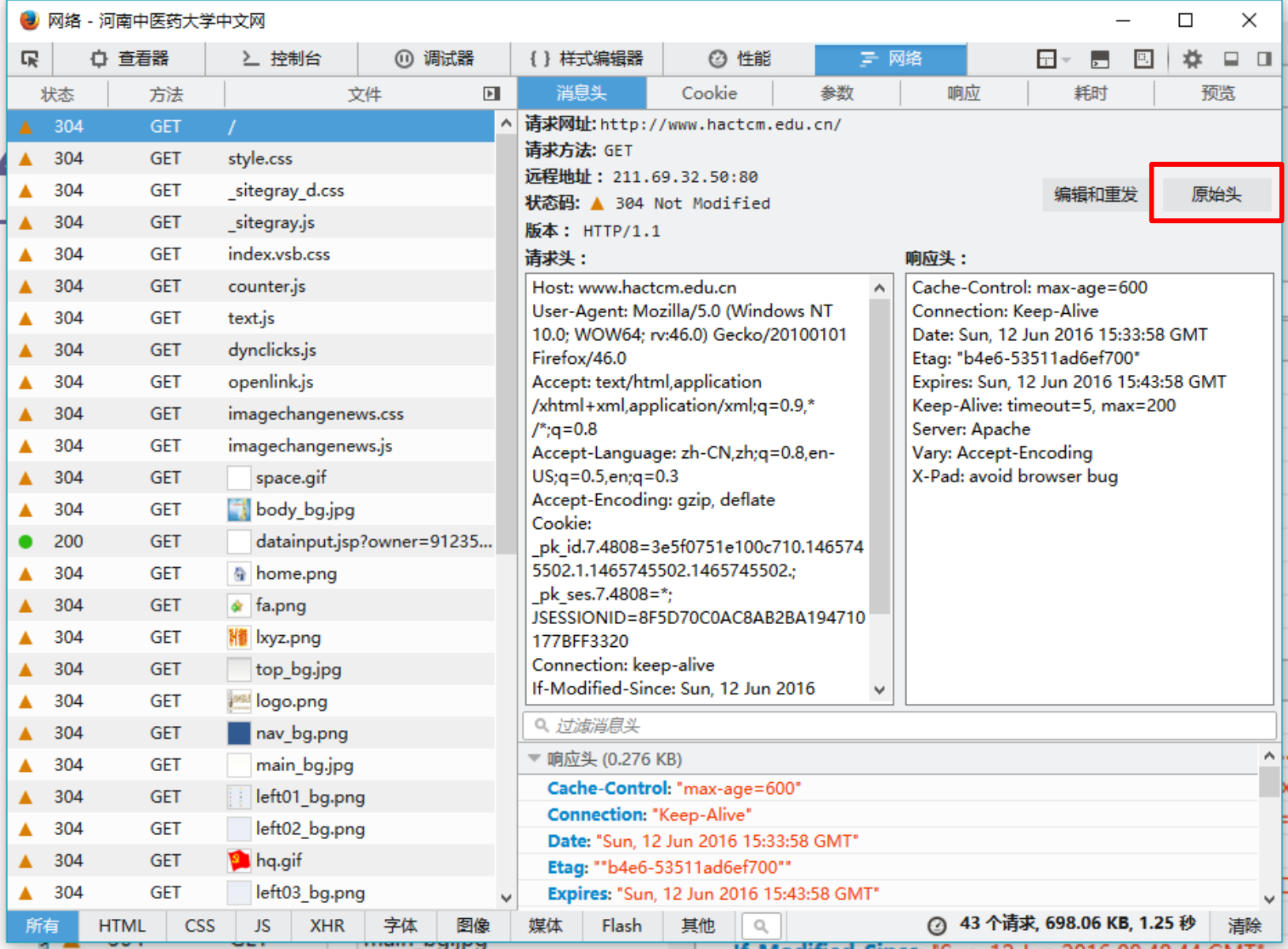
https://www.w3.org/Protocols/rfc2616/rfc2616-sec6.html#sec6.1.1

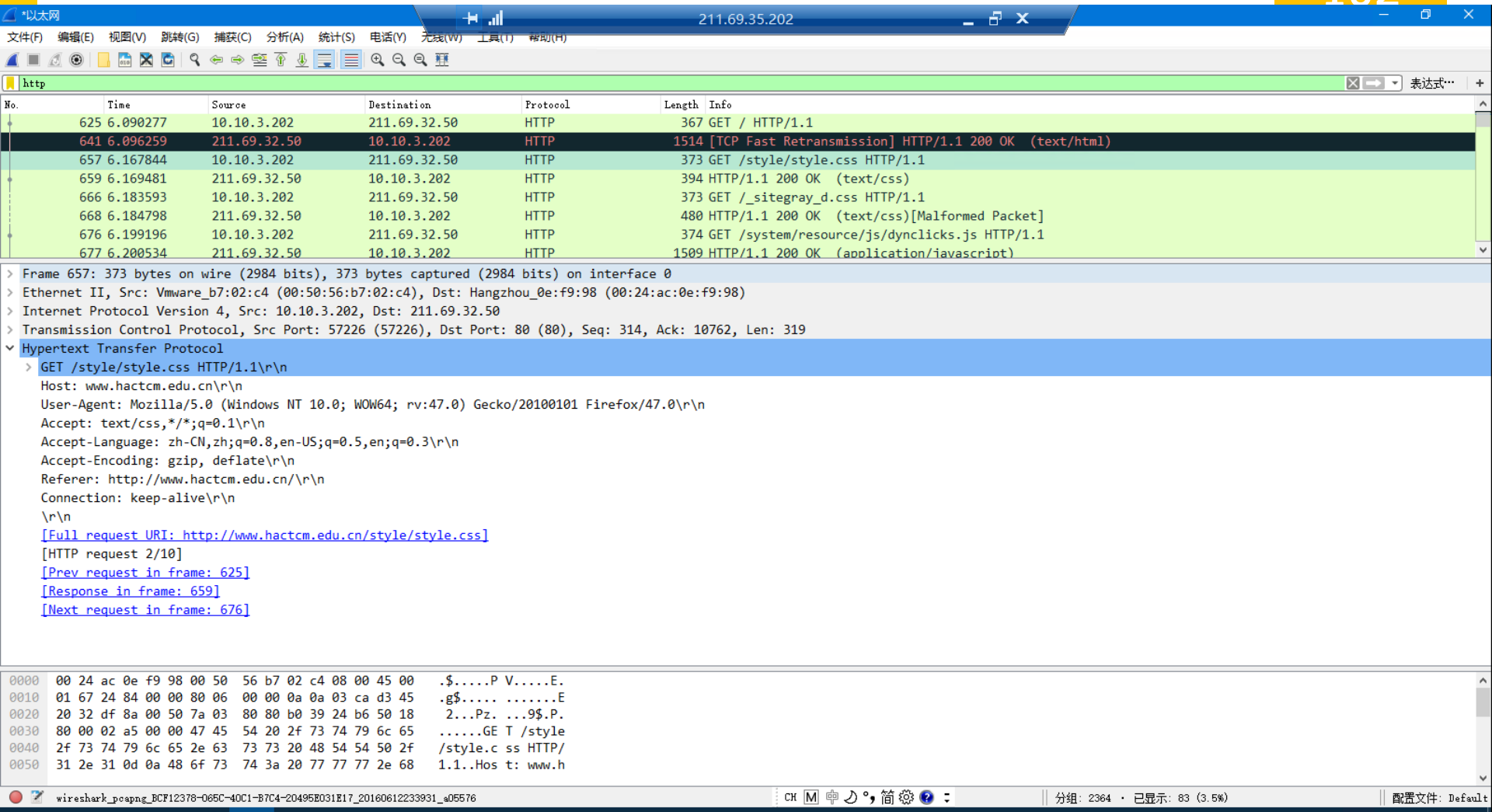
4.万维网WWW

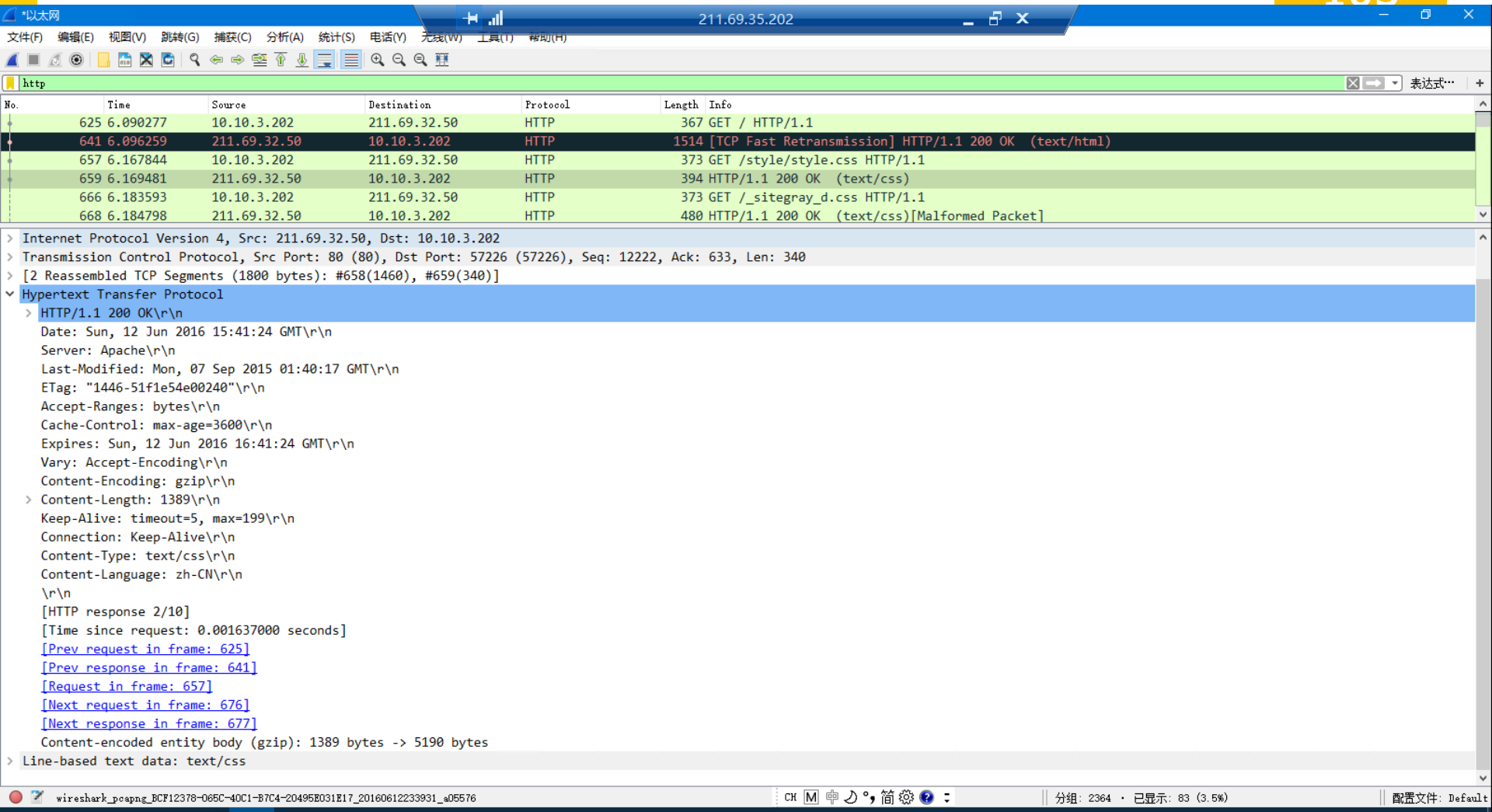
4.5HTTP的报文结构

```
Status-Code    =
      "100"  ; Section 10.1.1: Continue
    | "101"  ; Section 10.1.2: Switching Protocols
    | "200"  ; Section 10.2.1: OK
    | "201"  ; Section 10.2.2: Created
    | "202"  ; Section 10.2.3: Accepted
    | "203"  ; Section 10.2.4: Non-Authoritative Information
    | "204"  ; Section 10.2.5: No Content
    | "205"  ; Section 10.2.6: Reset Content
    | "206"  ; Section 10.2.7: Partial Content
    | "300"  ; Section 10.3.1: Multiple Choices
    | "301"  ; Section 10.3.2: Moved Permanently
    | "302"  ; Section 10.3.3: Found
    | "303"  ; Section 10.3.4: See Other
    | "304"  ; Section 10.3.5: Not Modified
    | "305"  ; Section 10.3.6: Use Proxy
    | "307"  ; Section 10.3.8: Temporary Redirect
    | "400"  ; Section 10.4.1: Bad Request
    | "401"  ; Section 10.4.2: Unauthorized
    | "402"  ; Section 10.4.3: Payment Required
    | "403"  ; Section 10.4.4: Forbidden
    | "404"  ; Section 10.4.5: Not Found
    | "405"  ; Section 10.4.6: Method Not Allowed
    | "406"  ; Section 10.4.7: Not Acceptable

    | "407"  ; Section 10.4.8: Proxy Authentication Required
    | "408"  ; Section 10.4.9: Request Time-out
    | "409"  ; Section 10.4.10: Conflict
    | "410"  ; Section 10.4.11: Gone
    | "411"  ; Section 10.4.12: Length Required
    | "412"  ; Section 10.4.13: Precondition Failed
    | "413"  ; Section 10.4.14: Request Entity Too Large
    | "414"  ; Section 10.4.15: Request-URI Too Large
    | "415"  ; Section 10.4.16: Unsupported Media Type
    | "416"  ; Section 10.4.17: Requested range not satisfiable
    | "417"  ; Section 10.4.18: Expectation Failed
    | "500"  ; Section 10.5.1: Internal Server Error
    | "501"  ; Section 10.5.2: Not Implemented
    | "502"  ; Section 10.5.3: Bad Gateway
    | "503"  ; Section 10.5.4: Service Unavailable
    | "504"  ; Section 10.5.5: Gateway Time-out
    | "505"  ; Section 10.5.6: HTTP Version not supported
    | extension-code

extension-code = 3DIGIT
Reason-Phrase  = *<TEXT, excluding CR, LF>
```


网络 - 河南中医药大学中文网
查看器
控制台
调试器
样式编辑器
性能
网络
状态
方法
文件
消息头
Cookie
参数
响应
耗时
预览
304 GET /
304 GET style.css
304 GET _sitegray_d.css
304 GET _sitegray.js
304 GET index.vsb.css
304 GET counter.js
304 GET text.js
304 GET dynclicks.js
304 GET openlink.js
304 GET imagechangenews.css
304 GET imagechangenews.js
304 GET space.gif
304 GET body_bg.jpg
200 GET datainput.jsp?owner=91235...
304 GET home.png
304 GET fa.png
304 GET lxyz.png
304 GET top_bg.jpg
304 GET logo.png
304 GET nav_bg.png
304 GET main_bg.jpg
304 GET left01_bg.png
304 GET left02_bg.png
304 GET hq.gif
304 GET left03_bg.png
请求网址: http://www.hactcm.edu.cn/
请求方法: GET
远程地址： 211.69.32.50:80
状态码: 304 Not Modified
编辑和重发
原始头
版本： HTTP/1.1
过滤消息头
响应头 (0.276 KB)
Cache-Control: "max-age=600"
Connection: "Keep-Alive"
Date: "Sun, 12 Jun 2016 15:33:58 GMT"
Etag: ""b4e6-53511ad6ef700""
Expires: "Sun, 12 Jun 2016 15:43:58 GMT"
Keep-Alive: "timeout=5, max=200"
Server: "Apache"
Vary: "Accept-Encoding"
X-Pad: "avoid browser bug"
请求头 (0.552 KB)
Host: "www.hactcm.edu.cn"
User-Agent: "Mozilla/5.0 (Windows NT 10.0; WOW64...:46.0) Gecko/20100101 Firefox/46.0"
Accept: "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8"
Accept-Language: "zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3"
Accept-Encoding: "gzip, deflate"
Cookie: "_pk_id.7.4808=3e5f0751e100c710.146...=8F5D70C0AC8AB2BA194710177BFF3320"
Connection: "keep-alive"
If-Modified-Since: "Sun, 12 Jun 2016 09:48:44 GMT"
If-None-Match: ""b4e6-53511ad6ef700""
Cache-Control: "max-age=0"
所有
HTML
CSS
JS
XHR
字体
图像
媒体
Flash
其他
43 个请求, 698.06 KB, 1.25 秒
清除


网络 - 河南中医药大学中文网
查看器
控制台
调试器
样式编辑器
性能
网络
状态
方法
文件
消息头
Cookie
参数
响应
耗时
预览
304 GET /
304 GET style.css
304 GET _sitegray_d.css
304 GET _sitegray.js
304 GET index.vsb.css
304 GET counter.js
304 GET text.js
304 GET dynclicks.js
304 GET openlink.js
304 GET imagechangenews.css
304 GET imagechangenews.js
304 GET space.gif
304 GET body_bg.jpg
200 GET datainput.jsp?owner=91235...
304 GET home.png
304 GET fa.png
304 GET lxyz.png
304 GET top_bg.jpg
304 GET logo.png
304 GET nav_bg.png
304 GET main_bg.jpg
304 GET left01_bg.png
304 GET left02_bg.png
304 GET hq.gif
304 GET left03_bg.png
请求网址: http://www.hactcm.edu.cn/
请求方法: GET
远程地址： 211.69.32.50:80
状态码: 304 Not Modified
版本： HTTP/1.1
编辑和重发
原始头
请求头：
Host: www.hactcm.edu.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: _pk_id.7.4808=3e5f0751e100c710.1465745502.1.1465745502.1465745502.; _pk_ses.7.4808=*; JSESSIONID=8F5D70C0AC8AB2BA194710177BFF3320
Connection: keep-alive
If-Modified-Since: Sun, 12 Jun 2016
响应头：
Cache-Control: max-age=600
Connection: Keep-Alive
Date: Sun, 12 Jun 2016 15:33:58 GMT
Etag: "b4e6-53511ad6ef700"
Expires: Sun, 12 Jun 2016 15:43:58 GMT
Keep-Alive: timeout=5, max=200
Server: Apache
Vary: Accept-Encoding
X-Pad: avoid browser bug
过滤消息头
响应头 (0.276 KB)
Cache-Control: "max-age=600"
Connection: "Keep-Alive"
Date: "Sun, 12 Jun 2016 15:33:58 GMT"
Etag: ""b4e6-53511ad6ef700""
Expires: "Sun, 12 Jun 2016 15:43:58 GMT"
所有
HTML
CSS
JS
XHR
字体
图像
媒体
Flash
其他
43 个请求, 698.06 KB, 1.25 秒
清除


*以太网
211.69.35.202
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
http
表达式…
No. Time Source Destination Protocol Length Info
625 6.090277 10.10.3.202 211.69.32.50 HTTP 367 GET / HTTP/1.1
641 6.096259 211.69.32.50 10.10.3.202 HTTP 1514 [TCP Fast Retransmission] HTTP/1.1 200 OK (text/html)
657 6.167844 10.10.3.202 211.69.32.50 HTTP 373 GET /style/style.css HTTP/1.1
659 6.169481 211.69.32.50 10.10.3.202 HTTP 394 HTTP/1.1 200 OK (text/css)
666 6.183593 10.10.3.202 211.69.32.50 HTTP 373 GET /_sitegray_d.css HTTP/1.1
668 6.184798 211.69.32.50 10.10.3.202 HTTP 480 HTTP/1.1 200 OK (text/css)[Malformed Packet]
676 6.199196 10.10.3.202 211.69.32.50 HTTP 374 GET /system/resource/js/dynclicks.js HTTP/1.1
677 6.200534 211.69.32.50 10.10.3.202 HTTP 1509 HTTP/1.1 200 OK (application/javascript)
Frame 657: 373 bytes on wire (2984 bits), 373 bytes captured (2984 bits) on interface 0
Ethernet II, Src: Vmware_b7:02:c4 (00:50:56:b7:02:c4), Dst: Hangzhou_0e:f9:98 (00:24:ac:0e:f9:98)
Internet Protocol Version 4, Src: 10.10.3.202, Dst: 211.69.32.50
Transmission Control Protocol, Src Port: 57226 (57226), Dst Port: 80 (80), Seq: 314, Ack: 10762, Len: 319
Hypertext Transfer Protocol
GET /style/style.css HTTP/1.1\r\n
Host: www.hactcm.edu.cn\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0\r\n
Accept: text/css,*/*;q=0.1\r\n
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3\r\n
Accept-Encoding: gzip, deflate\r\n
Referer: http://www.hactcm.edu.cn/\r\n
Connection: keep-alive\r\n
\r\n
[Full request URI: http://www.hactcm.edu.cn/style/style.css]
[HTTP request 2/10]
[Prev request in frame: 625]
[Response in frame: 659]
[Next request in frame: 676]
0000 00 24 ac 0e f9 98 00 50 56 b7 02 c4 08 00 45 00 .$.....P V.....E.
0010 01 67 24 84 00 00 80 06 00 00 0a 0a 03 ca d3 45 .g$..... ....E
0020 20 32 df 8a 00 50 7a 03 80 80 b0 39 24 b6 50 18 2...Pz. ...9$.P.
0030 80 00 02 a5 00 00 47 45 54 20 2f 73 74 79 6c 65 ......GE T /style
0040 2f 73 74 79 6c 65 2e 63 73 73 20 48 54 54 50 2f /style.c ss HTTP/
0050 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 68 1.1..Hos t: www.h
wireshark_pcapng_BCF12378-065C-40C1-B7C4-20495E031E17_20160612233931_a05576
分组: 2364 · 已显示: 83 (3.5%)
配置文件: Default
23:40
2016/6/12

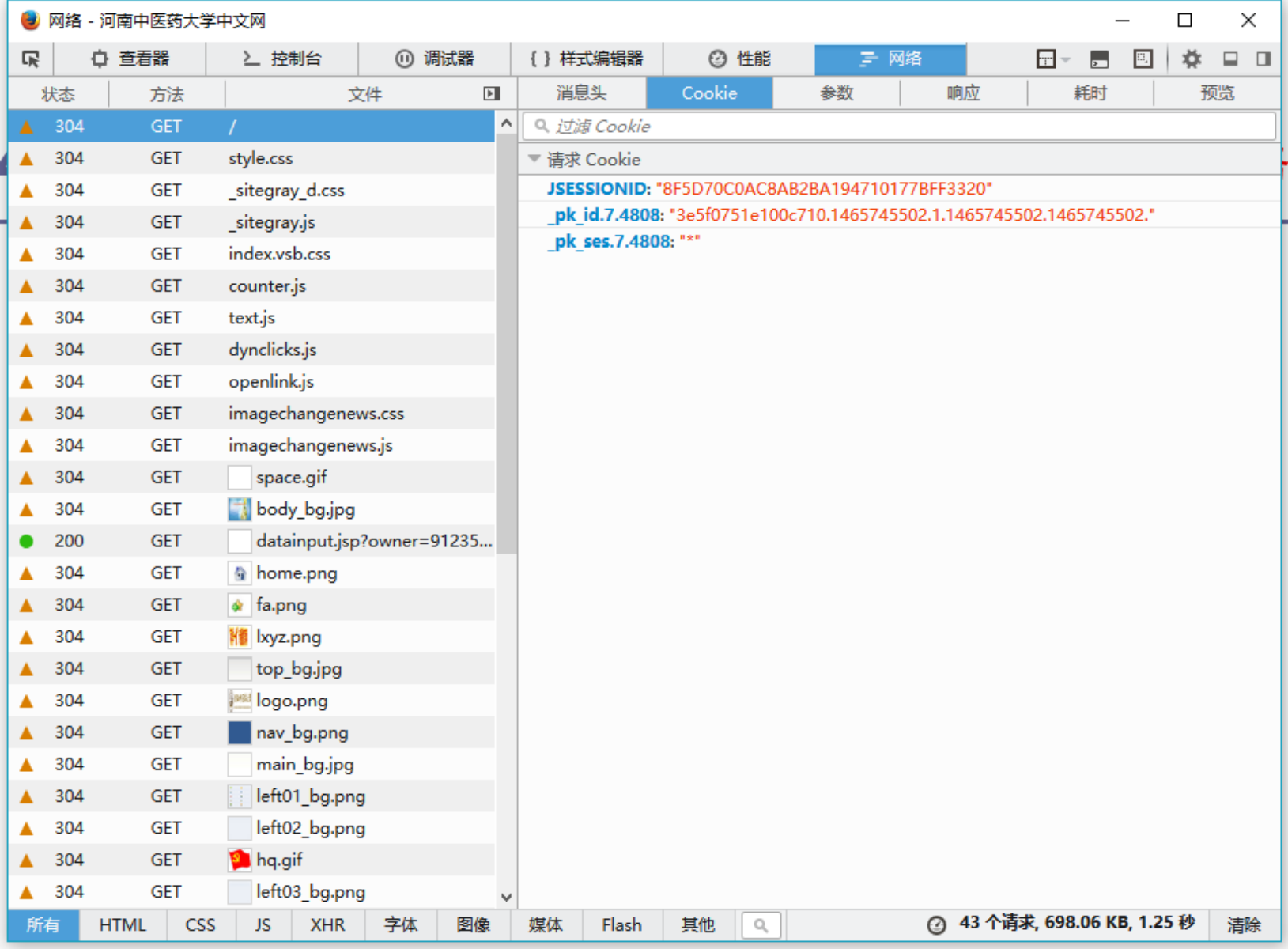

*以太网
211.69.35.202
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
http
表达式…
No. Time Source Destination Protocol Length Info
625 6.090277 10.10.3.202 211.69.32.50 HTTP 367 GET / HTTP/1.1
641 6.096259 211.69.32.50 10.10.3.202 HTTP 1514 [TCP Fast Retransmission] HTTP/1.1 200 OK (text/html)
657 6.167844 10.10.3.202 211.69.32.50 HTTP 373 GET /style/style.css HTTP/1.1
659 6.169481 211.69.32.50 10.10.3.202 HTTP 394 HTTP/1.1 200 OK (text/css)
666 6.183593 10.10.3.202 211.69.32.50 HTTP 373 GET /_sitegray_d.css HTTP/1.1
668 6.184798 211.69.32.50 10.10.3.202 HTTP 480 HTTP/1.1 200 OK (text/css)[Malformed Packet]
Internet Protocol Version 4, Src: 211.69.32.50, Dst: 10.10.3.202
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 57226 (57226), Seq: 12222, Ack: 633, Len: 340
[2 Reassembled TCP Segments (1800 bytes): #658(1460), #659(340)]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Sun, 12 Jun 2016 15:41:24 GMT\r\n
Server: Apache\r\n
Last-Modified: Mon, 07 Sep 2015 01:40:17 GMT\r\n
ETag: "1446-51f1e54e00240"\r\n
Accept-Ranges: bytes\r\n
Cache-Control: max-age=3600\r\n
Expires: Sun, 12 Jun 2016 16:41:24 GMT\r\n
Vary: Accept-Encoding\r\n
Content-Encoding: gzip\r\n
Content-Length: 1389\r\n
Keep-Alive: timeout=5, max=199\r\n
Connection: Keep-Alive\r\n
Content-Type: text/css\r\n
Content-Language: zh-CN\r\n
\r\n
[HTTP response 2/10]
[Time since request: 0.001637000 seconds]
[Prev request in frame: 625]
[Prev response in frame: 641]
[Request in frame: 657]
[Next request in frame: 676]
[Next response in frame: 677]
Content-encoded entity body (gzip): 1389 bytes -> 5190 bytes
Line-based text data: text/css
wireshark_pcapng_BCF12378-065C-40C1-B7C4-20495E031E17_20160612233931_a05576
分组: 2364 · 已显示: 83 (3.5%)
配置文件: Default
23:41
2016/6/12

4.万维网WWW

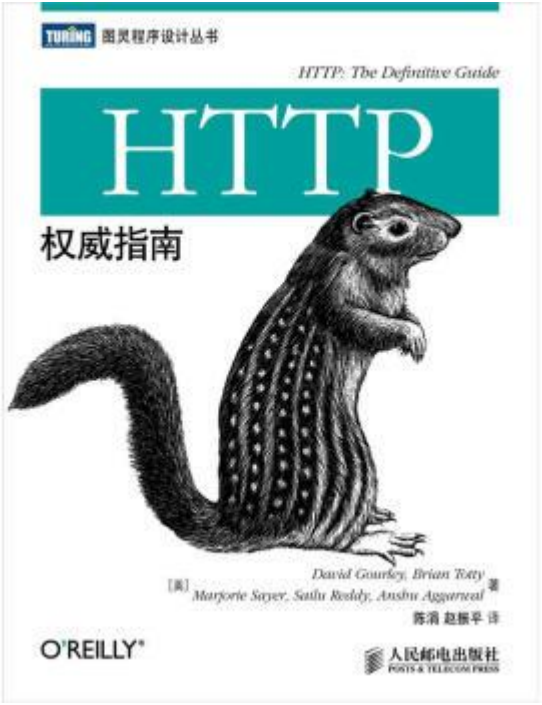
现场演示：Fiddler进行HTTP分析

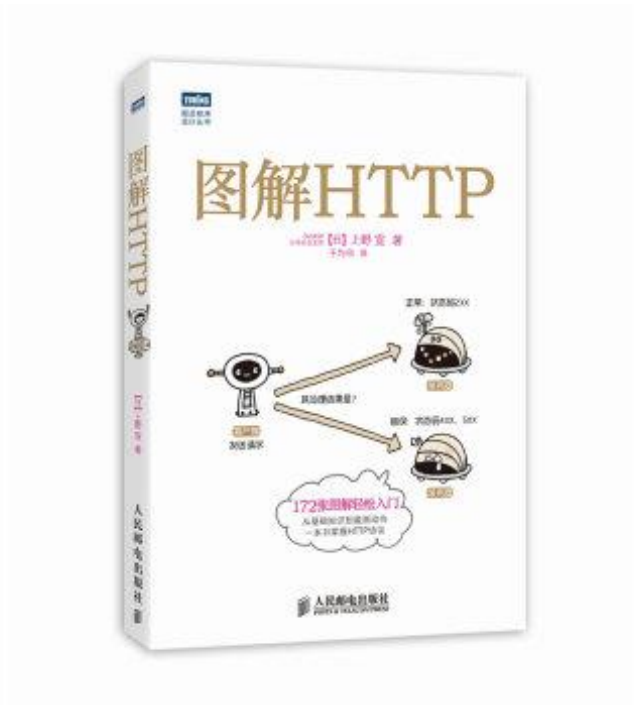
4.万维网WWW

- 万维网站点使用Cookie来跟踪用户。
- Cookie表示在HTTP服务器和客户之间传递的状态信息。
- 使用Cookie的网站服务器为用户产生一个唯一的识别码。利用此识别码，网站就能够跟踪该用户在该网站的活动。


网络 - 河南中医药大学中文网
查看器
控制台
调试器
样式编辑器
性能
网络
状态
方法
文件
消息头
Cookie
参数
响应
耗时
预览
过滤 Cookie
请求 Cookie
JSESSIONID: "8F5D70C0AC8AB2BA194710177BFF3320"
_pk_id.7.4808: "3e5f0751e100c710.1465745502.1.1465745502.1465745502."
_pk_ses.7.4808: "*"
304 GET /
304 GET style.css
304 GET _sitegray_d.css
304 GET _sitegray.js
304 GET index.vsb.css
304 GET counter.js
304 GET text.js
304 GET dynclicks.js
304 GET openlink.js
304 GET imagechangenews.css
304 GET imagechangenews.js
304 GET space.gif
304 GET body_bg.jpg
200 GET datainput.jsp?owner=91235...
304 GET home.png
304 GET fa.png
304 GET lxyz.png
304 GET top_bg.jpg
304 GET logo.png
304 GET nav_bg.png
304 GET main_bg.jpg
304 GET left01_bg.png
304 GET left02_bg.png
304 GET hq.gif
304 GET left03_bg.png
所有
HTML
CSS
JS
XHR
字体
图像
媒体
Flash
其他
43 个请求, 698.06 KB, 1.25 秒
清除

4.万维网WWW


TURING 图灵程序设计丛书
HTTP: The Definitive Guide
HTTP
权威指南
David Gourley, Brian Totty
Marjorie Sayer, Sailu Reddy, Anshu Aggarwal
陈清 赵振平 译
O'REILLY
人民邮电出版社


图解HTTP
人民邮电出版社

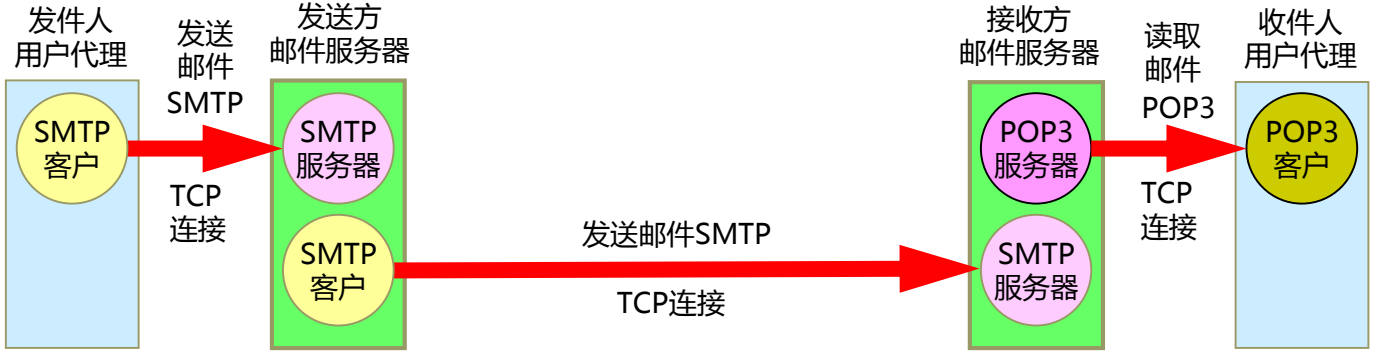
5.电子邮件

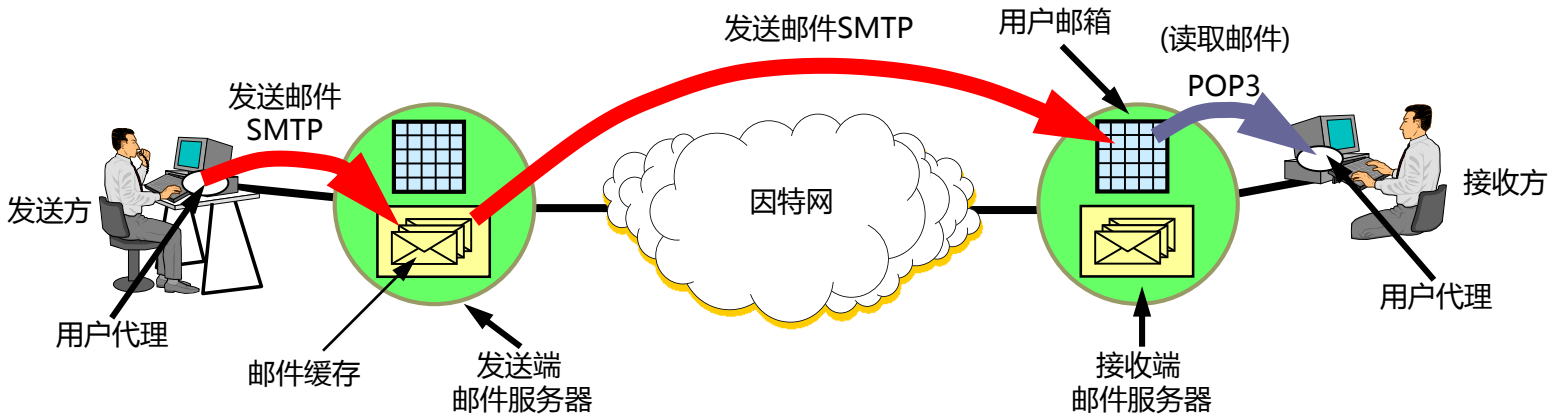
- 电子邮件(e-mail)是因特网上使用得最多的和最受用户欢迎的一种应用。
- 电子邮件把邮件发送到收件人使用的邮件服务器，并放在其中的收件人邮箱中，收件人可随时上网到自己使用的邮件服务器进行读取。
- 电子邮件不仅使用方便，而且还具有传递迅速和费用低廉的优点。
- 现在电子邮件不仅可传送文字信息，而且还可附上声音和图像。

5.电子邮件

- 电子邮件的一些标准：
  - 发送邮件的协议：SMTP
  - 读取邮件的协议：POP3 和 IMAP
  - MIME：在其邮件首部中说明了邮件的数据类型(如文本、声音、图像、视像等)，使用 MIME 可在邮件中同时传送多种类型的数据。

5.电子邮件


发件人
用户代理
发送
邮件
SMTP
发送方
邮件服务器
SMTP
客户
TCP
连接
SMTP
服务器
SMTP
客户
发送邮件SMTP
TCP连接
接收方
邮件服务器
POP3
服务器
SMTP
服务器
读取
邮件
POP3
TCP
连接
收件人
用户代理
POP3
客户


发送邮件SMTP
用户邮箱
(读取邮件)
POP3
发送邮件
SMTP
因特网
发送方
接收方
用户代理
邮件缓存
发送端
邮件服务器
接收端
邮件服务器
用户代理

5.电子邮件

- 用户代理UA(User Agent)：
  - 用户代理 UA 就是用户与电子邮件系统的接口，是电子邮件客户端软件。
  - 用户代理的功能：撰写、显示、处理和通信。
  - 邮件服务器的功能是发送和接收邮件，同时还要向发信人报告邮件传送的情况（已交付、被拒绝、丢失等）。
  - 邮件服务器按照客户服务器方式工作。邮件服务器需要使用发送和读取两个不同的协议。

5.电子邮件

- 邮件服务器：
  - 一个邮件服务器既可以作为客户，也可以作为服务器。
  - 例如，当邮件服务器 A 向另一个邮件服务器 B 发送邮件时，邮件服务器 A 就作为 SMTP 客户，而 B 是 SMTP 服务器。
  - 当邮件服务器 A 从另一个邮件服务器 B 接收邮件时，邮件服务器 A 就作为 SMTP 服务器，而 B 是 SMTP 客户。

5.电子邮件

- 发送和接收电子邮件的几个重要步骤：
  - 发件人调用PC机中的用户代理撰写和编辑要发送的邮件。
  - 发件人的用户代理把邮件用SMTP协议发给发送方邮件服务器，
  - SMTP服务器把邮件临时存放在邮件缓存队列中，等待发送。
  - 发送方邮件服务器的SMTP客户与接收方邮件服务器的SMTP服务器建立TCP连接，然后就把邮件缓存队列中的邮件依次发送出去。
  - 运行在接收方邮件服务器中的SMTP服务器进 程收到邮件后，把邮件放入收件人的用户邮箱中，等待收件人进行读取。
  - 收件人在打算收信时，就运行PC机中的用户代理，使用POP3（或IMAP）协议读取发送给自己的邮件。

5.电子邮件

- 电子邮件的组成：
  - 电子邮件由信封(envelope)和内容(content)两部分组成。
  - 电子邮件的传输程序根据邮件信封上的信息来传送邮件。用户在从自己的邮箱中读取邮件时才能见到邮件的内容。
  - 在邮件的信封上，最重要的就是收件人的地址。

5.电子邮件

- 电子邮件地址的格式：
  - TCP/IP 体系的电子邮件系统规定电子邮件地址的格式如下：

收件人邮箱名@邮箱所在主机的域名

  - 符号“@”读作“at”，表示“在”的意思。

5.电子邮件

- SMTP所规定的就是在两个相互通信的SMTP进程之间应如何交换信息。
- 由于SMTP使用客户服务器方式，因此负责发送邮件的SMTP进程就是SMTP客户，而负责接收邮件的SMTP进程就是SMTP服务器。
- SMTP规定了14条命令和21种应答信息。每条命令用4个字母组成，而每一种应答信息一般只有一行信息，由一个3位数字的代码开始，后面附上（也可不附上）很简单的文字说明。

5.电子邮件

- SMTP通信的三个阶段：
  - 连接建立：连接是在发送主机的SMTP客户和接收主机的SMTP服务器之间建立的。SMTP不使用中间的邮件服务器。
  - 邮件传送。
  - 连接释放：邮件发送完毕后，SMTP应释放TCP连接。

5.电子邮件

- 一个电子邮件分为信封和内容两大部分。
- RFC 822只规定了邮件内容中的首部(header)格式，而对邮件的主体(body)部分则让用户自由撰写。
- 用户写好首部后，邮件系统将自动地将信封所需的信息提取出来并写在信封上。所以用户不需要填写电子邮件信封上的信息。
- 邮件内容首部包括一些关键字，后面加上冒号。最重要的关键字是：To和Subject。

5.电子邮件

- 邮件内容的首部：
  - To：后面填入一个或多个收件人的电子邮件地址。用户只需打开地址簿，点击收件人名字，收件人的电子邮件地址就会自动地填入到合适的位置上。
  - Subject：是邮件的主题。它反映了邮件的主要内容，便于用户查找邮件。
  - Cc：表示应给某某人发送一个邮件副本。
  - From和Date：表示发信人的电子邮件地址和发信日期。
  - Reply-To：是对方回信所用的地址。

5.电子邮件

- POP3：
  - 邮局协议POP是一个非常简单、但功能有限的邮件读取协议，现在使用的是它的第三个版本POP3。
  - POP也使用客户服务器的工作方式。
  - 在接收邮件的用户PC机中必须运行POP客户程序，而在用户所连接的ISP的邮件服务器中则运行POP服务器程序。

5.电子邮件

- IMAP：
  - IMAP也是按客户服务器方式工作，现在较新的是版本4，即IMAP4。
  - 用户在自己的PC机上就可以操纵ISP的邮件服务器的邮箱，就像在本地操纵一样。
  - IMAP是一个联机协议。当用户PC机上的IMAP客户程序打开IMAP服务器的邮箱时，用户就可看到邮件的首部。若用户需要打开某个邮件，则该邮件才传到用户的计算机上。

5.电子邮件

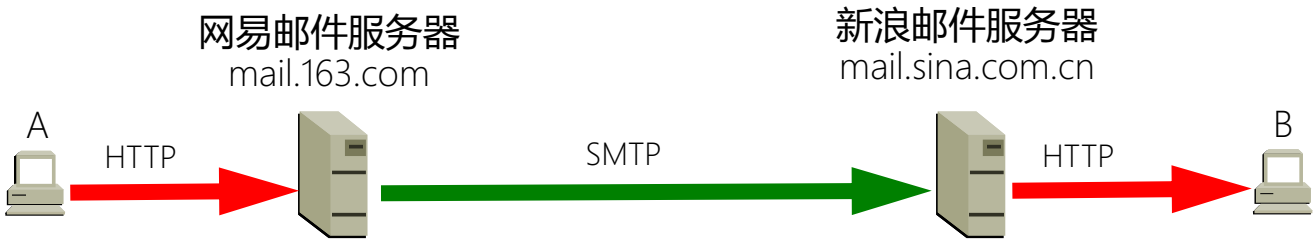
- IMAP：
  - IMAP最大的好处就是用户可以在不同的地方使用不同的计算机随时上网阅读和处理自己的邮件。
  - IMAP还允许收件人只读取邮件中的某一个部分。为了节省时间，可以先下载邮件的正文部分，待以后有时间再读取或下载这个很长的附件。
  - IMAP的缺点是如果用户没有将邮件复制到自己的PC机上，则邮件一直是存放在IMAP服务器上。因此用户需要经常与IMAP服务器建立连接。

5.电子邮件

- POP、IMAP和SMTP：
  - 不要将邮件读取协议POP或IMAP与邮件传送协议SMTP弄混。
  - 发信人的用户代理向源邮件服务器发送邮件，以及源邮件服务器向目的邮件服务器发送邮件，都是使用SMTP协议。
  - POP协议或IMAP协议则是用户从目的邮件服务器上读取邮件所使用的协议。

5.电子邮件

- 电子邮件从A发送到网易邮件服务器是使用HTTP协议。
- 两个邮件服务器之间的传送使用SMTP。
- 邮件从新浪邮件服务器传送到B是使用HTTP协议。

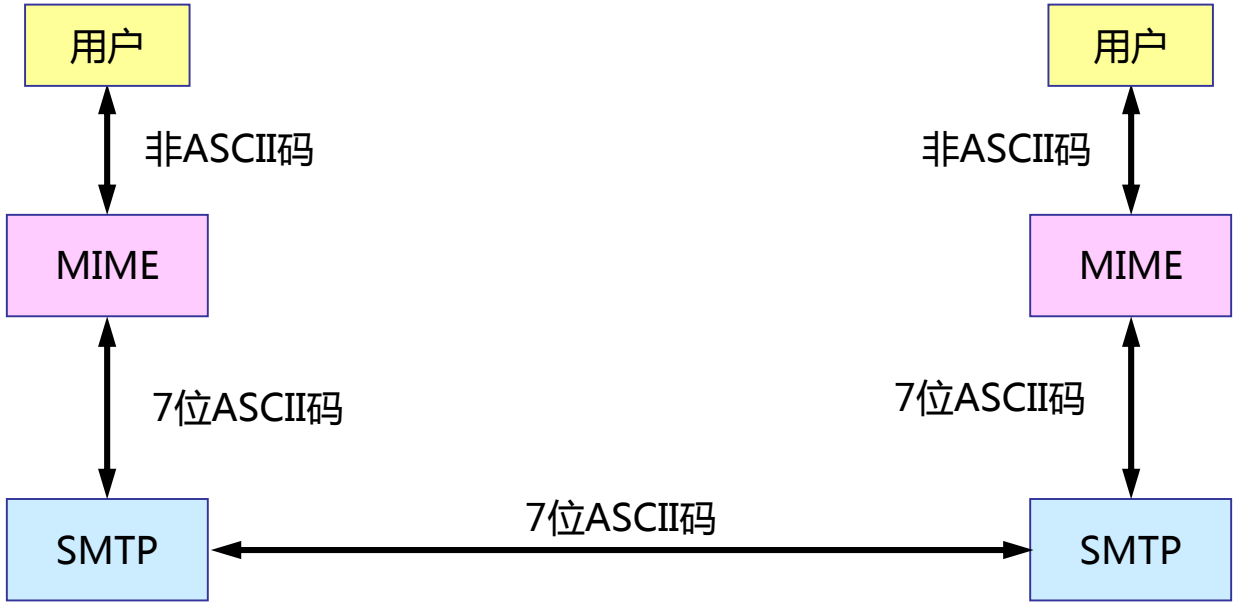


5.电子邮件

- SMTP有以下缺点：
  - SMTP不能传送可执行文件或其他的二进制对象。
  - SMTP限于传送7位的ASCII码。许多其他非英语国家的文字（如中文、俄文，甚至带重音符号的法文或德文）就无法传送。
  - SMTP服务器会拒绝超过一定长度的邮件。
  - 某些SMTP的实现并没有完全按照[RFC 821]的 SMTP 标准。

5.电子邮件

- MIME和SMTP的关系：



5.电子邮件

- MIME主要包括三个部分 ：
  - 5个新的邮件首部字段，它们可包含在[RFC 822]首部中。这些字段提供了有关邮件主体的信息。
  - 定义了许多邮件内容的格式，对多媒体电子邮件的表示方法进行了标准化。
  - 定义了传送编码，可对任何内容格式进行转换，而不会被邮件系统改变。

5.电子邮件

- MIME增加5个新的邮件首部：
  - MIME-Version：标志MIME的版本。现在的版本号是1.0。若无此行，则为英文文本。
  - Content-Description：这是可读字符串，说明此邮件是什么。和邮件的主题差不多。
  - Content-Id：邮件的唯一标识符。
  - Content-Transfer-Encoding：在传送时邮件的主体是如何编码的。
  - Content-Type：说明邮件的性质。

5.电子邮件

- 内容传送编码（Content-Transfer-Encoding）：
  - 最简单的编码就是7位ASCII码，而每行不能超过1000个字符。MIME对这种由ASCII码构成的邮件主体不进行任何转换。
  - 另一种编码称为quoted-printable，这种编码方法适用于当所传送的数据中只有少量的非ASCII码。
  - 对于任意的二进制文件，可用base64编码。

5.电子邮件

- 内容类型：
  - MIME着标准规定Content-Type说明必须含有两个标识符，即内容类型(type)和子类型(subtype)，中间用“/”分开。
  - MIME 标准定义了7个基本内容类型和15种子类型。

5.电子邮件

5.6通用因特网邮件扩充MIME

5.电子

扩充MIME

```
Received: from mail406.jd.com (unknown [36.110.177.37])
        by edm4 (Coremail) with SMTP id icCowECZPkx7SF5XW394Ag--.39586S2;
        Mon, 13 Jun 2016 13:45:31 +0800 (CST)
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple; t=1465796730;
        s=leo; d=jd.com; i=leo@jd.com;
        h=Date:From:To:Message-ID:Subject:MIME-Version:Content-Type:Content-Transfer-Encoding;
        bh=Nnz87X1MKPqfkDfp3JFfXvRjznkAj3RegEHmCPHolY4=;
        b=F8JNcwm/pJr4g6dNUHbfihQBmVeMNPi5I/1mBOxVTIRyaitnLO5ZTwxLME12RpEB
        qJKht++FLG0hBkVPKsCCUo9eL7OafivkMoye0DQiNm9vP4yM9ASNuoXBtK8z7Du2Tjc
        lxx3JXZh12ZwnhkfAdQkfcHvgfhvHfCNiRCrY03U=
Date: Mon, 13 Jun 2016 13:45:30 +0800 (CST)
From: =?utf-8?B?5Lqs5LicSkQuY29t?= <customer_service@jd.com>
To: ruanxiaolong@163.com
Message-ID: <752153985.21007141465796730970.JavaMail.admin@host-10-187-18-98>
Subject: =?UTF-8?B?5oKo5Zyo5Lqs5Lic5pyJMeW8oOS8mOaDoA==?=
 =?UTF-8?B?5Yi45Yiw6LSm77yM6K+35rOo5oSP5p+l5pS2?=
MIME-Version: 1.0
Content-Type: text/html;charset=utf-8
Content-Transfer-Encoding: quoted-printable
X-CM-TRANSID:icCowECZPkx7SF5XW394Ag--.39586S2
Authentication-Results: edm4; spf=pass smtp.mail=customer_service@jd.c
        om; dkim=pass header.i=@jd.com
X-Coremail-Antispam: 1Uf129KBjvJXoW7KF1kJF48XFWftFykCFyUWrg_yoW8Jw1kpr
        Z5Ww48Wr4jya1S9r4UWw1Igr4UJanaga1Yq34xtFWfXrWUJF92yrW7KF93ua4fXwnrZan7
        X3WFq3sYgwn0k3DanT9S1TB71UUUU4JqnTZGkaVYY2UrUUUUjbIjqfuFe4nvWSU5nxnvy2
        9KBjDUYxBIdaVFxhVjvjDtur1kJVWrZrnYChsFpT7I43ZEXa7xR_LvttUUUUU==

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.=
w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns=3D"http://www.w3.org/1999/xhtml">
 <head>=20
  <meta http-equiv=3D"Content-Type" content=3D"text/html; charset=3Dutf-8">=
=20
  <title>=E6=82=A8=E5=9C=A8=E4=BA=AC=E4=B8=9C=E6=9C=891=E5=BC=A0=E4=BC=98=
=E6=83=A0=E5=88=B8=E5=88=B0=E8=B4=A6=EF=BC=8C=E8=AF=B7=E6=B3=A8=E6=84=8F=E6=
=9F=A5=E6=94=B6</title>
 </head>=20
 <body><!-- webmail_open_begin --><table style=3D'display:none;' width=3D'1=
' height=3D'1'><tr><td> <img width=3D'1' height=3D'1' src=3D'http://dc2.jd.=
com/auto.php?service=3Dtransfer&type=3Dpms&from=3Ddmp&kid=3D155&klid=3D8814=
```

Thanks