

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>

河南中医药大学信息管理与信息系统教研室
信息技术学院网络与信息系统科研工作室

2020.11

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

1.1域名系统概述

- 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

1.1域名系统概述

- 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。
 - 云计算时代下的业务发布需要经常变更。
 - 高负载下的CDN分发。
 - 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

1.1域名系统概述

- 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

1.1域名系统概述

□ 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 Website Speed Test
 Enter a URL, to test the load time of that page, analyze it and find bottlenecks.

URL: Test from: [START TEST](#)

[DOWNLOAD REPORT](#) [SHARE RESULT](#)

Summary Testing from New York City, New York, USA

Performance grade: **88** | Load time: **6.19 s**

Page size: **1.7 MB** | Requests: **33**

Performance insights

- 9 Leverage browser caching
- 100 Specify a cache validator
- 100 Specify a Vary: Accept-Encoding header

Response codes

| Category | Percentage | Count | Size | Category | Percentage | Count |
|---------------------|-----------------|--------------|----------------|---------------------|-----------------|-----------|
| Image | 97.0 % | 1,634 | 1.63 MB | Image | 77.4 % | 24 |
| Script | 2.4 % | 42 | 39 KB | Script | 16.3 % | 5 |
| network.51xueweb.cn | 6.1 % | 142 | 24 KB | network.51xueweb.cn | 26.3 % | 10 |
| Total | 100.00 % | 1,716 | 1.71 MB | Total | 100.00 % | 31 |

File requests

Sort by: Load order | Filter: | Legend: 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 | [DNS, Connect] | | | | | |
| network.51xueweb.cn/Templates/Network... | 6.0 kB | | [Wait] | | | | |
| network.51xueweb.cn/Templates/Network... | 33.4 kB | | [Wait] | | [Receive] | | |
| network.51xueweb.cn/Templates/Network... | 1.9 kB | | [Connect] | [Wait] | | | |
| network.51xueweb.cn/Templates/Network... | 1.7 kB | | [Connect] | [Wait] | | | |
| network.51xueweb.cn/Image/ | 20.9 kB | | [Wait] | | [Receive] | | |
| network.51xueweb.cn/Templates/Network... | 1.2 kB | | | | [Wait] | | |
| fileapi.portal.51xueweb.cn/Network/im... | 55.8 kB | | | | [DNS, Connect] | [Wait] | [Receive] |
| fileapi.portal.51xueweb.cn/Network/im... | 289.4 kB | | | | [DNS, Connect] | [Wait] | [Receive] |
| fileapi.portal.51xueweb.cn/Network/im... | 338.8 kB | | | | [DNS, Connect] | [Wait] | [Receive] |
| fileapi.portal.51xueweb.cn/Network/im... | 180.2 kB | | | | [DNS, Connect] | [Wait] | [Receive] |
| fileapi.portal.51xueweb.cn/Network/im... | 71.7 kB | | | | [DNS, Connect] | [Wait] | [Receive] |
| network.51xueweb.cn/Templates/Network... | 414 B | | | | | [Wait] | |

Server Response Codes

To make it easy for you to differentiate between the HTTP response codes in the waterfall chart, we color coded the text and background of each URL.

- 200: The server responded with a successful code
- 30x: The request was redirected to another target
- 4xx: A client error occurred, for example 404 page not found
- 5xx: A server error occurred, for example 500 internal server error
- ERR: Error Connection error, no response from the server

File requests

Sort by: | Filter: | Legend: 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 | [DNS, Connect] | | | | | |
| network.51xueweb.cn/Templates/Network... | 6.0 kB | | [Wait] | | | | |
| network.51xueweb.cn/Templates/Network... | 33.4 kB | | [Wait] | | [Receive] | | |
| network.51xueweb.cn/Templates/Network... | 1.9 kB | | [Connect] | [Wait] | | | |
| network.51xueweb.cn/Templates/Network... | 1.7 kB | | [Connect] | [Wait] | | | |
| network.51xueweb.cn/Image/ | 20.9 kB | | [Wait] | | [Receive] | | |
| network.51xueweb.cn/Templates/Network... | 1.2 kB | | | | [Wait] | | |
| fileapi.portal.51xueweb.cn/Network/im... | 55.8 kB | | | | [DNS, Connect] | [Wait] | [Receive] |
| fileapi.portal.51xueweb.cn/Network/im... | 289.4 kB | | | | [DNS, Connect] | [Wait] | [Receive] |
| fileapi.portal.51xueweb.cn/Network/im... | 338.8 kB | | | | [DNS, Connect] | [Wait] | [Receive] |
| fileapi.portal.51xueweb.cn/Network/im... | 180.2 kB | | | | [DNS, Connect] | [Wait] | [Receive] |
| fileapi.portal.51xueweb.cn/Network/im... | 71.7 kB | | | | [DNS, Connect] | [Wait] | [Receive] |
| network.51xueweb.cn/Templates/Network... | 414 B | | | | | [Wait] | |

Automate your Page Speed Testing [START FREE TRIAL](#)

pingdom

[TWITTER](#)
[FACEBOOK](#)
[GOOGLE+](#)

1. 域名系统DNS

1.1 域名系统概述

The screenshot shows a network monitoring tool interface with a table of requests and a detailed view on the right. The table lists various resources like style.css, jquery.js, and subnav_bg.png, along with their status, method, and response time. The detailed view on the right shows the DNS resolution process for the selected request.

| 状态 | 方法 | 文件 | 域名 | 类型 | 已传输 | 大小 | 0 毫秒 | 640 毫秒 | 1.28 秒 | 消息头 | Cookie | 参数 | 响应 | 耗时 |
|----|-----|-----|--|---------------------|-------|---------|----------|--------|--------|-----|--------|----|----|---------|
| ● | 200 | GET | / | network51.xueweb.cn | html | 3.49 KB | 16.17 KB | 24 ms | | | | | | 1546 ms |
| ○ | 200 | GET | style.css | network51.xueweb.cn | css | 已缓存 | 20.01 KB | | | | | | | 0 ms |
| ○ | 200 | GET | jquery.js | network51.xueweb.cn | js | 已缓存 | 78.42 KB | | | | | | | 0 ms |
| ○ | 200 | GET | setTab.js | network51.xueweb.cn | js | 已缓存 | 2.24 KB | | | | | | | 0 ms |
| ○ | 200 | GET | jquery.slide.js | network51.xueweb.cn | js | 已缓存 | 4.25 KB | | | | | | | 0 ms |
| ○ | 200 | GET | qswcmVisit.js | network51.xueweb.cn | js | 已缓存 | 1.12 KB | | | | | | | 0 ms |
| ○ | 200 | GET | qswcmSSO.js | network51.xueweb.cn | js | 已缓存 | 12.27 KB | | | | | | | 0 ms |
| ● | 200 | GET | UpdateVisitCount?callback=call1464800117090&visitInfo={"SiteID": "9... | url | plain | — | 0 KB | | | | | | | 1546 ms |
| ● | 200 | GET | GetUserInfo?callback=call1464800117093 | url | plain | — | 0 KB | | | | | | | 1546 ms |
| ● | 200 | GET | subnav_bg.png | network51.xueweb.cn | png | 0.98 KB | 0.98 KB | | 12 ms | | | | | 12 ms |

DNS 解析:

- 连接: 1546 ms
- 发送: 0 ms
- 等待: 0 ms
- 接收: 0 ms

网络 - BBC - Homepage

| 状态 | 方法 | 文件 | 域名 | 类型 | 已传输 | 大小 | 0 毫秒 | 20.48 秒 | 40.96 秒 | 消息头 | Cookie | 参数 | 响应 | 耗时 |
|-------|-----|------------------------|------------------------|------|----------|-----------|------------|---------|---------|-----|--------|----|----|----|
| ● 200 | GET | / | www.bbc.com | html | 33.27 KB | 199.76 KB | 1 - 456 ms | | | | | | | |
| ● 200 | GET | orb.min.css | static.bbci.co.uk | css | 4.73 KB | 26.01 KB | 1 - 400 ms | | | | | | | |
| ● 200 | GET | api.min.js | static.bbci.co.uk | js | 0.27 KB | 0.38 KB | 1 - 279 ms | | | | | | | |
| ● 200 | GET | id-cta.css | static.bbc.co.uk | css | 2.18 KB | 24.67 KB | 1 - 260 ms | | | | | | | |
| ● 200 | GET | main.min.css | mybbc.files.bbci.co.uk | css | 11.28 KB | 97.37 KB | 1 - 311 ms | | | | | | | |
| ● 200 | GET | wwhp.min.css | static.bbci.co.uk | css | 17.20 KB | 90.42 KB | 1 - 309 ms | | | | | | | |
| ● 200 | GET | modernizr.js | static.bbci.co.uk | js | 4.30 KB | 10.34 KB | 1 - 328 ms | | | | | | | |
| ● 200 | GET | bbc-blocks-light.png | static.bbci.co.uk | png | 0.71 KB | 0.71 KB | 1 - 536 ms | | | | | | | |
| ● 200 | GET | orb-search-light.png | static.bbci.co.uk | png | 0.26 KB | 0.26 KB | 1 - 549 ms | | | | | | | |
| ● 200 | GET | _89854240_89854236.jpg | ichef.bbci.co.uk | jpeg | 3.81 KB | 3.81 KB | 1 - 201 ms | | | | | | | |

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

| 状态 | 方法 | 文件 | 域名 | 类型 | 已传输 | 大小 | 0 毫秒 | 20.48 秒 | 40.96 秒 | 消息头 | Cookie | 参数 | 响应 | 耗时 |
|-------|-----|------------------------|------------------------|------|----------|-----------|------------|---------|---------|-----|--------|----|----|----|
| ● 200 | GET | / | www.bbc.com | html | 33.27 KB | 199.76 KB | 1 - 456 ms | | | | | | | |
| ● 200 | GET | orb.min.css | static.bbci.co.uk | css | 4.73 KB | 26.01 KB | 1 - 400 ms | | | | | | | |
| ● 200 | GET | api.min.js | static.bbci.co.uk | js | 0.27 KB | 0.38 KB | 1 - 279 ms | | | | | | | |
| ● 200 | GET | id-cta.css | static.bbc.co.uk | css | 2.18 KB | 24.67 KB | 1 - 260 ms | | | | | | | |
| ● 200 | GET | main.min.css | mybbc.files.bbci.co.uk | css | 11.28 KB | 97.37 KB | 1 - 311 ms | | | | | | | |
| ● 200 | GET | wwhp.min.css | static.bbci.co.uk | css | 17.20 KB | 90.42 KB | 1 - 309 ms | | | | | | | |
| ● 200 | GET | modernizr.js | static.bbci.co.uk | js | 4.30 KB | 10.34 KB | 1 - 328 ms | | | | | | | |
| ● 200 | GET | bbc-blocks-light.png | static.bbci.co.uk | png | 0.71 KB | 0.71 KB | 1 - 536 ms | | | | | | | |
| ● 200 | GET | orb-search-light.png | static.bbci.co.uk | png | 0.26 KB | 0.26 KB | 1 - 549 ms | | | | | | | |
| ● 200 | GET | _89854240_89854236.jpg | ichef.bbci.co.uk | jpeg | 3.81 KB | 3.81 KB | 1 - 201 ms | | | | | | | |

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

| 状态 | 方法 | 文件 | 域名 | 类型 | 已传输 | 大小 | 0 毫秒 | 20.48 秒 | 40.96 秒 | 消息头 | Cookie | 参数 | 响应 | 耗时 |
|-------|-----|----------------------|------------------------|------|----------|-----------|------------|---------|---------|-----|--------|----|----|----|
| ● 200 | GET | / | www.bbc.com | html | 33.27 KB | 199.76 KB | 1 - 456 ms | | | | | | | |
| ● 200 | GET | orb.min.css | static.bbci.co.uk | css | 4.73 KB | 26.01 KB | 1 - 400 ms | | | | | | | |
| ● 200 | GET | api.min.js | static.bbci.co.uk | js | 0.27 KB | 0.38 KB | 1 - 279 ms | | | | | | | |
| ● 200 | GET | id-cta.css | static.bbc.co.uk | css | 2.18 KB | 24.67 KB | 1 - 260 ms | | | | | | | |
| ● 200 | GET | main.min.css | mybbc.files.bbci.co.uk | css | 11.28 KB | 97.37 KB | 1 - 311 ms | | | | | | | |
| ● 200 | GET | wwhp.min.css | static.bbci.co.uk | css | 17.20 KB | 90.42 KB | 1 - 309 ms | | | | | | | |
| ● 200 | GET | modernizr.js | static.bbci.co.uk | js | 4.30 KB | 10.34 KB | 1 - 328 ms | | | | | | | |
| ● 200 | GET | bbc-blocks-light.png | static.bbci.co.uk | png | 0.71 KB | 0.71 KB | 1 - 536 ms | | | | | | | |
| ● 200 | GET | orb-search-light.png | static.bbci.co.uk | png | 0.26 KB | 0.26 KB | 1 - 549 ms | | | | | | | |

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

1.2因特网的域名结构

- 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称，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

1.2因特网的域名结构

- 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

1.2因特网的域名结构

- 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。
 - 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

1.2因特网的域名结构

□ 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

1.2因特网的域名结构

□ 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)



Help Us Improve Future Meetings

It takes just five minutes to take the ICANN60 survey. You'll rate your overall satisfaction, the sessions, networking opportunities, registration process, and venue. You can access the survey through the ICANN60 mobile app or the desktop version.

Get started

WE WANT YOUR FEEDBACK! COMPLETE OUR ICANN60 SURVEY.

ICANN 60
ANNUAL GENERAL
ABU DHABI
28 October–3 November 2017

News and Announcements

Wrap-Up Interview with Chérine Chalaby and Steve Crocker



ICANN's Brad White sits down with new Board Chair Chérine Chalaby and outgoing Board Chair Steve Crocker. They discuss the challenges that the ICANN Board faces going forward and the importance of transparency and accountability in building trust with the community. Watch the interview and learn more by clicking the link above.

Accepting Applications for ICANN Global Indigenous Ambassador Program

Application Deadline:
17 November 2017

The application round for the Global Indigenous Ambassador Program is now open. Two Indigenous Ambassadors will be selected from underrepresented indigenous communities to attend ICANN61. Applicants must be members

Quicklinks

Accountability Indicators

Board Activity

Data Privacy/Protection

Domain Name Registrants

Engagement Calendar

IANA Services

KSK Rollover

New gTLDs

Public Technical Identifiers (PTI)

Domain Names

[Overview](#)
Root Zone Management
[Overview](#)
Root Database
[Hint and Zone Files](#)
[Change Requests](#)
[Instructions & Guides](#)
[Root Servers](#)
[.INT Registry](#)
[.ARPA Registry](#)
[IDN Practices Repository](#)
[Root Key Signing Key \(DNSSEC\)](#)
[Reserved Domains](#)

Root Zone Database

The Root Zone Database represents the delegation details of top-level domains, including gTLDs such as .com, and country-code TLDs such as .uk. As the manager of the DNS root zone, we are responsible for coordinating these delegations in accordance with our [policies and procedures](#).

Much of this data is also available via the WHOIS protocol at whois.iana.org.

| DOMAIN | TYPE | TLD MANAGER |
|------------------------------|--------------|---|
| .aaa | generic | American Automobile Association, Inc. |
| .aarp | generic | AARP |
| .abarth | generic | Fiat Chrysler Automobiles N.V. |
| .abb | generic | ABB Ltd |
| .abbott | generic | Abbott Laboratories, Inc. |
| .abbvie | generic | AbbVie Inc. |
| .abc | generic | Disney Enterprises, Inc. |
| .able | generic | Able Inc. |
| .abogado | generic | Top Level Domain Holdings Limited |
| .abudhabi | generic | Abu Dhabi Systems and Information Centre |
| .ac | country-code | Network Information Center (AC Domain Registry) c/o Cable and Wireless (Ascension Island) |
| .academy | generic | Half Oaks, LLC |
| .accenture | generic | Accenture plc |
| .accountant | generic | dot Accountant Limited |
| .accountants | generic | Knob Town, LLC |
| .aco | generic | ACO Severin Ahlmann GmbH & Co. KG |
| .active | generic | Active Network, LLC |
| .actor | generic | United TLD Holdco Ltd. |
| .ad | country-code | Andorra Telecom |
| .adac | generic | Allgemeiner Deutscher Automobil-Club e.V. (ADAC) |
| .ads | generic | Charleston Road Registry Inc. |
| .adult | generic | ICM Registry AD LLC |
| .ae | country-code | Telecommunication Regulatory Authority (TRA) |
| .aeg | generic | Aktiebolaget Electrolux |
| .aero | sponsored | Societe Internationale de Telecommunications Aeronautique (SITA INC USA) |

| | | |
|--------------------------|--------------|--|
| .xfinity | generic | Comcast IP Holdings I, LLC |
| .xihuan | generic | QIHOO 360 TECHNOLOGY CO. LTD. |
| .xin | generic | Elegant Leader Limited |
| .测试 | test | Internet Assigned Numbers Authority |
| .कॉम | generic | VeriSign Sarl |
| .परीक्षा | test | Internet Assigned Numbers Authority |
| .セール | generic | Amazon Registry Services, Inc. |
| .佛山 | generic | Guangzhou YU Wei Information Technology Co., Ltd. |
| .இந்தியா | country-code | National Internet eXchange of India |
| .慈善 | generic | Excellent First Limited |
| .集团 | generic | Eagle Horizon Limited |
| .在线 | generic | TLD REGISTRY LIMITED |
| .한국 | country-code | KISA (Korea Internet & Security Agency) |
| .ଭାରତ | country-code | National Internet eXchange of India |
| .大众汽车 | generic | Volkswagen (China) Investment Co., Ltd. |
| .点看 | generic | VeriSign Sarl |
| .ଭାରତ | generic | VeriSign Sarl |
| .ভারত | country-code | National Internet eXchange of India |
| .八卦 | generic | Zodiac Gemini Ltd |
| .سازمان | generic | Suhb Electronic Establishment |
| .बिहार | country-code | Posts and Telecommunications Division |
| .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) |
| .香格里拉 | generic | Shangri-La International Hotel Management Limited |
| .网站 | generic | Global Website TLD Asia Limited |
| .移动 | generic | Afilias plc |
| .我爱你 | generic | Tycoon Treasure Limited |
| .MOCKBA | generic | Foundation for Assistance for Internet Technologies and Infrastructure Development (FAITID) |

| | | |
|--------------|--------------|--|
| .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. |
| .биз | 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. |
| .opr | 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 |

The 44th China Statistical Report on Internet Development

第44次中国互联网络发展状况统计报告

截至 2019 年 6 月，我国域名总数为 4800 万个。其中，“.CN”域名数量为 2185 万个，较 2018 年底增长 2.9%，占我国域名总数的 45.5%；“.COM”域名数量为 1456 万个，占我国域名总数的 30.3%；“.中国”域名数量为 171 万个，占我国域名总数的 3.6%；新通用顶级域名（New gTLD）数量为 806 万个，占我国域名总数的 16.8%。

表 2 分类域名数¹⁶

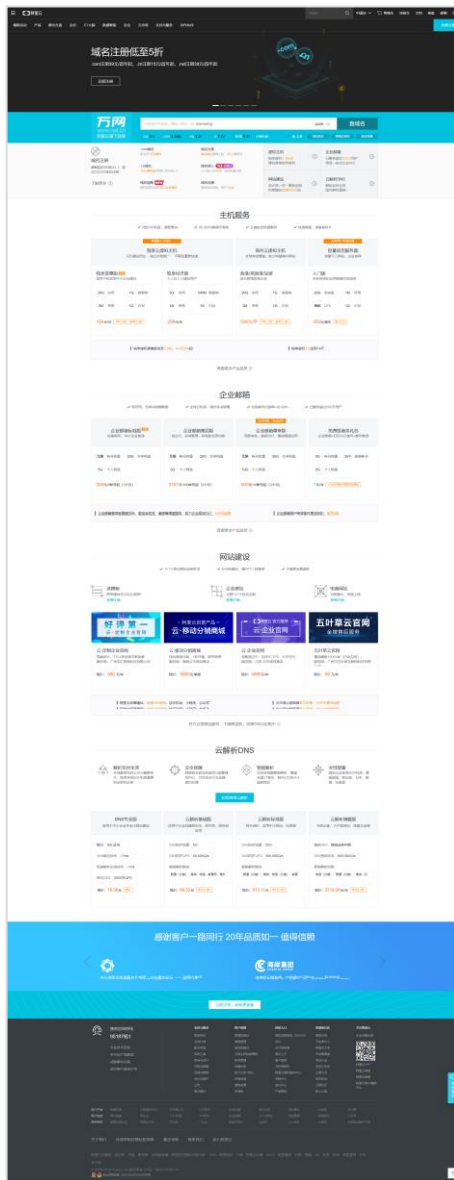
| | 数量 (个) | 占域名总数比例 |
|----------|------------|---------|
| .CN | 21,851,990 | 45.5% |
| .COM | 14,558,469 | 30.3% |
| .中国 | 1,705,861 | 3.6% |
| .NET | 1,126,268 | 2.3% |
| .BIZ | 357,174 | 0.7% |
| .ORG | 185,822 | 0.4% |
| .INFO | 62,506 | 0.1% |
| New gTLD | 8,057,424 | 16.8% |
| 其他 | 95,957 | 0.2% |
| 合计 | 48,001,471 | 100.0% |

表 3 分类“.CN”域名数

| | 数量 (个) | 占“.CN”域名总数比例 |
|---------|------------|--------------|
| .CN | 19,075,505 | 87.3% |
| .COM.CN | 2,228,998 | 10.2% |
| .NET.CN | 265,698 | 1.2% |
| .ORG.CN | 158,474 | 0.7% |
| .ADM.CN | 81,674 | 0.4% |
| .GOV.CN | 24,733 | 0.1% |
| .AC.CN | 10,543 | 0.0% |
| .EDU.CN | 6,264 | 0.0% |
| 其他 | 101 | 0.0% |
| 合计 | 21,851,990 | 100.0% |

如何申请一个域名?

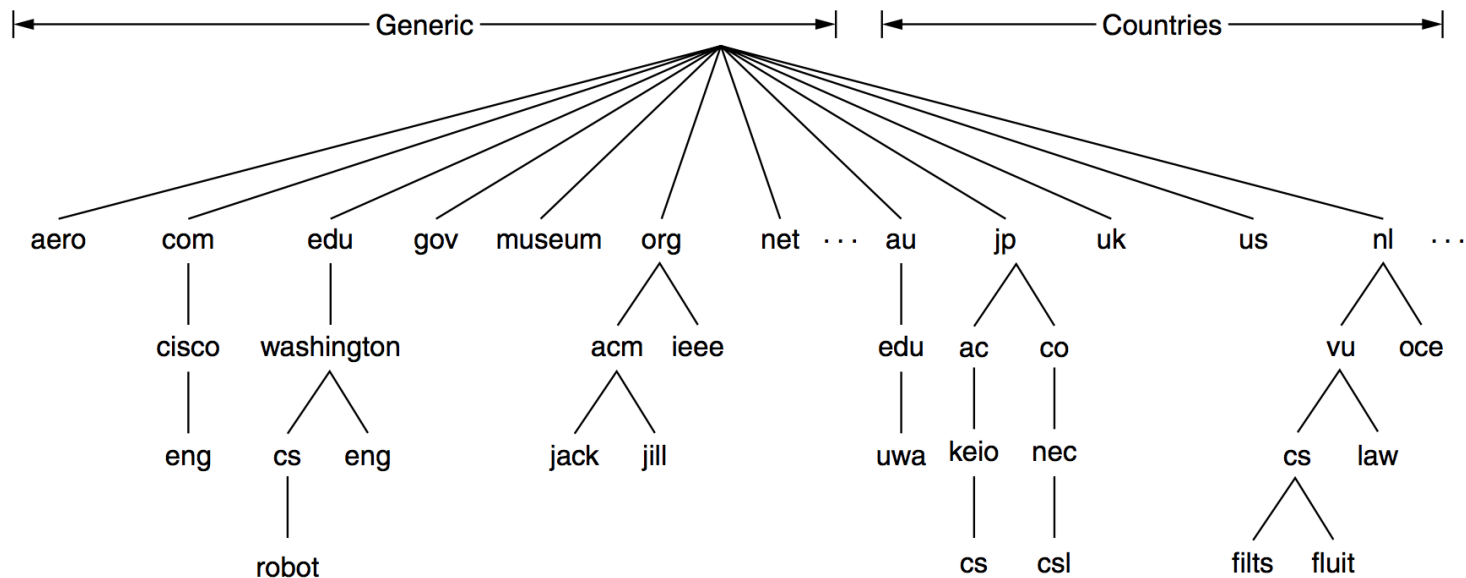
<https://wanwang.aliyun.com>



1. 域名系统DNS

1.2 因特网的域名结构

□ 因特网的域名空间



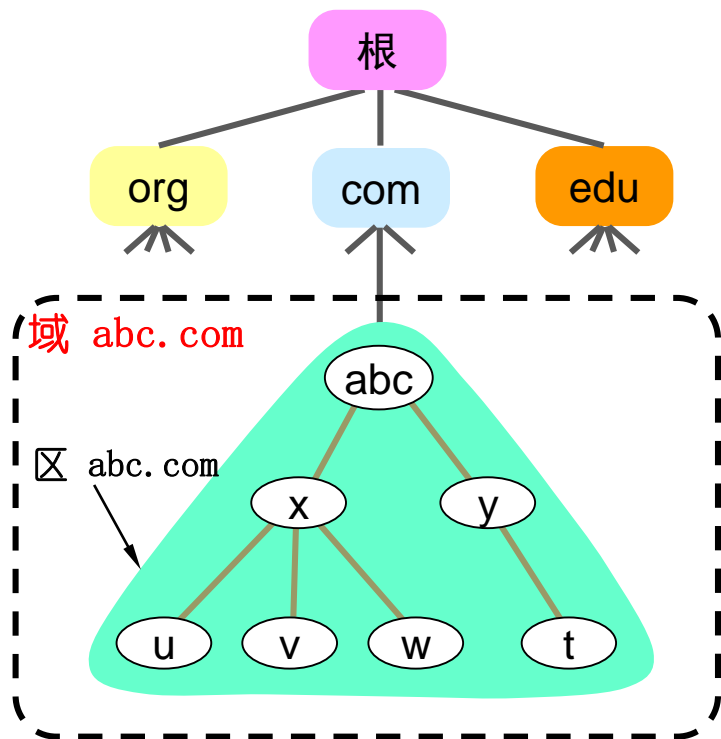
1.域名系统DNS

1.3域名服务器

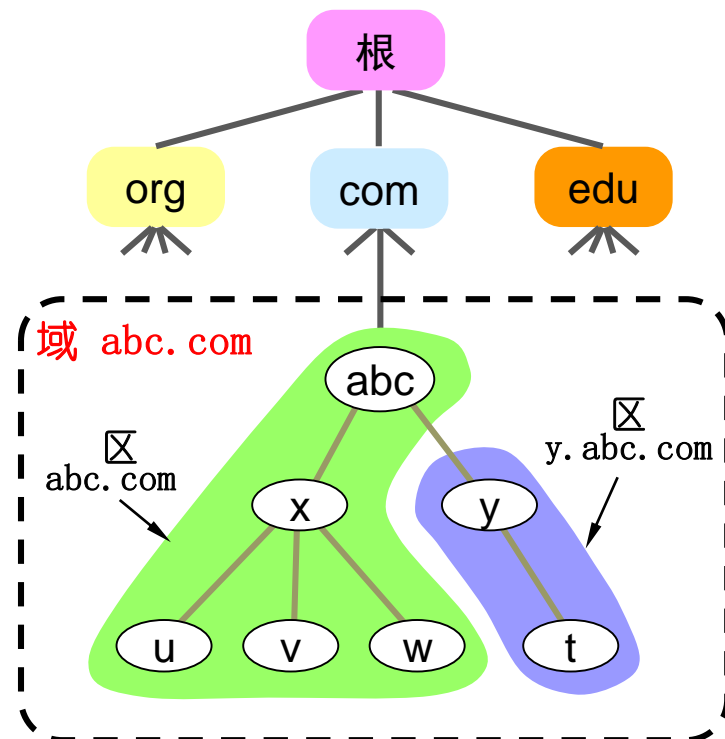
- 一个服务器所负责管辖的（或有权限的）范围叫做区(zone)。
 - 各单位根据具体情况来划分自己管辖范围的区。但在一个区中的所有节点必须是能够连通的。
 - 每一个区设置相应的权限域名服务器，用来保存该区中的所有主机的域名到IP地址的映射。
- DNS 服务器的管辖范围不是以“域”为单位，而是以“区”为单位。

1. 域名系统DNS

1.3 域名服务器



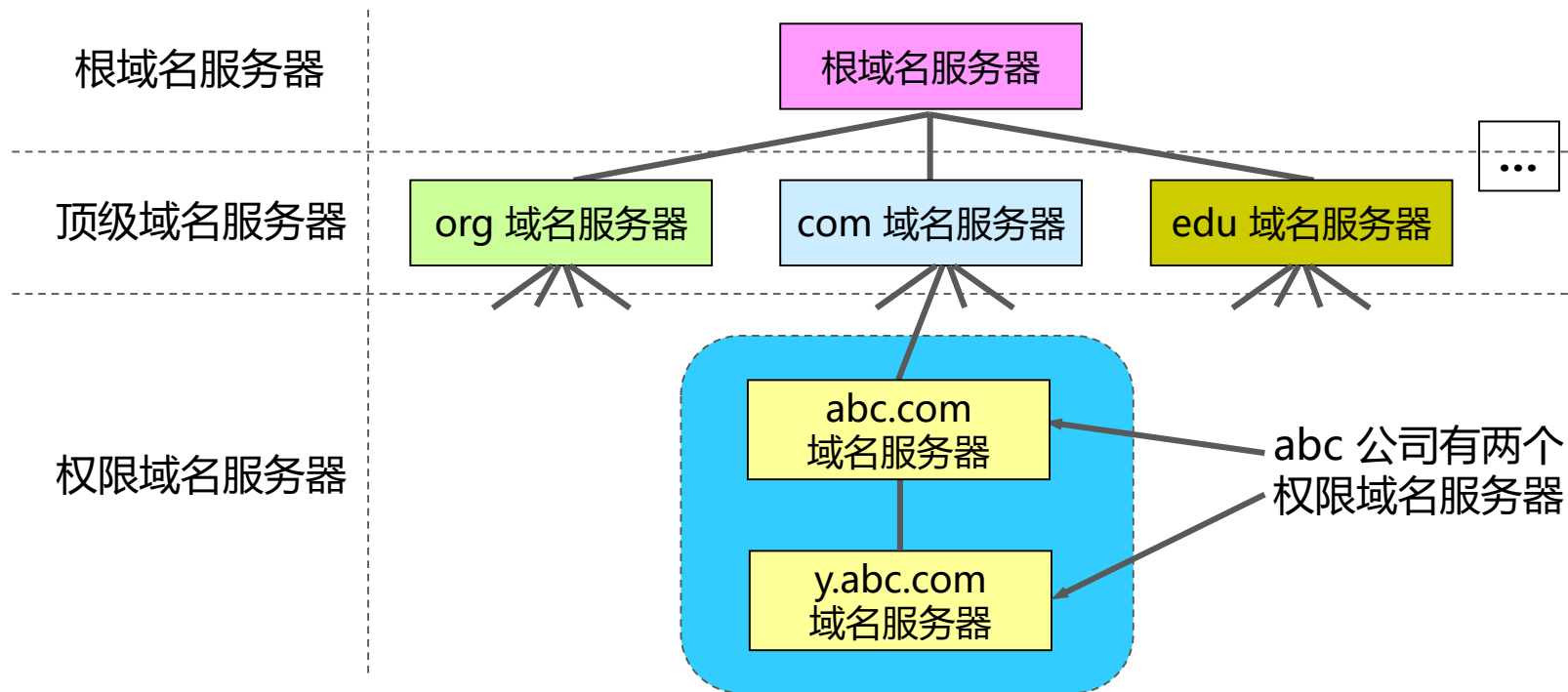
(a) ☒ = 域



(b) ☒ < 域

1.域名系统DNS

1.3域名服务器



1.域名系统DNS

1.3域名服务器

1

根域名服务器
顶级域名服务器 (TLD服务器)
权限域名服务器

2

本地域名服务器 (Local Name Server)

1.域名系统DNS

1.3域名服务器

□ 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

1.3域名服务器

□ 根域名服务器

- 根域名服务器相应的域名分别是

a.rootervers.net

b.rootervers.net

...

m.rootervers.net

- As of 2018-08-27, the root server system consists of 937 instances operated by the 12 independent root server operators.
- 这样做的目的是为了更方便用户，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。

News and publications [show all](#)

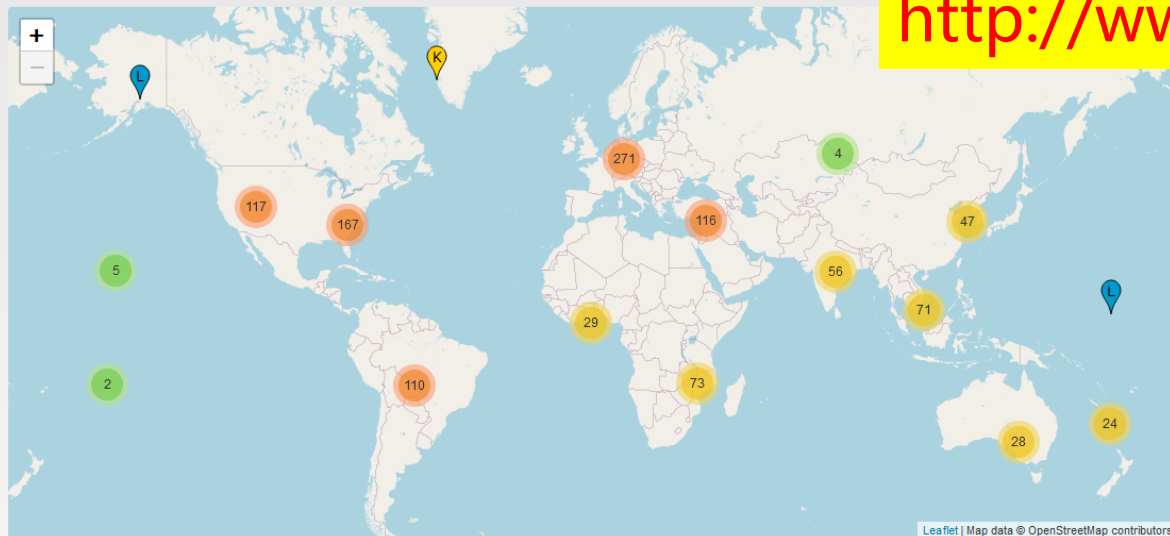
- 2019-08-14 [Threat Mitigation For the Root Server System \(Document\)](#)
- 2019-03-28 [Operational Statement on the final step in the KSK Rollover](#)
- 2019-03-14 [Operational Statement on the Integrity of the Root Server System](#)

Meeting agendas [show all](#)

- 2020-07-27 [IETF 108/Virtual \(PDF\)](#)
- 2020-03-23 [IETF 107/Virtual \(PDF\)](#)
- 2019-11-17 [IETF 106/Singapore \(PDF\)](#)

1.3 域名服务器

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



As of 11/24/2020 1:51 p.m., the root server system consists of 1341 instances operated by the 12 independent root server operators.

The 13 root name servers are operated by 12 independent organisations.

You can find more information about each of these organisations by visiting their homepage as found in the 'Operator' field below.

Technical questions about the Root Server System as a whole can be directed to the [Ask RSSAC](#) e-mail address.

1.域名系统DNS

1.3域名服务器

□ 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

1.3域名服务器

□ 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

1.3域名服务器

□ 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

1.3域名服务器

□ 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。

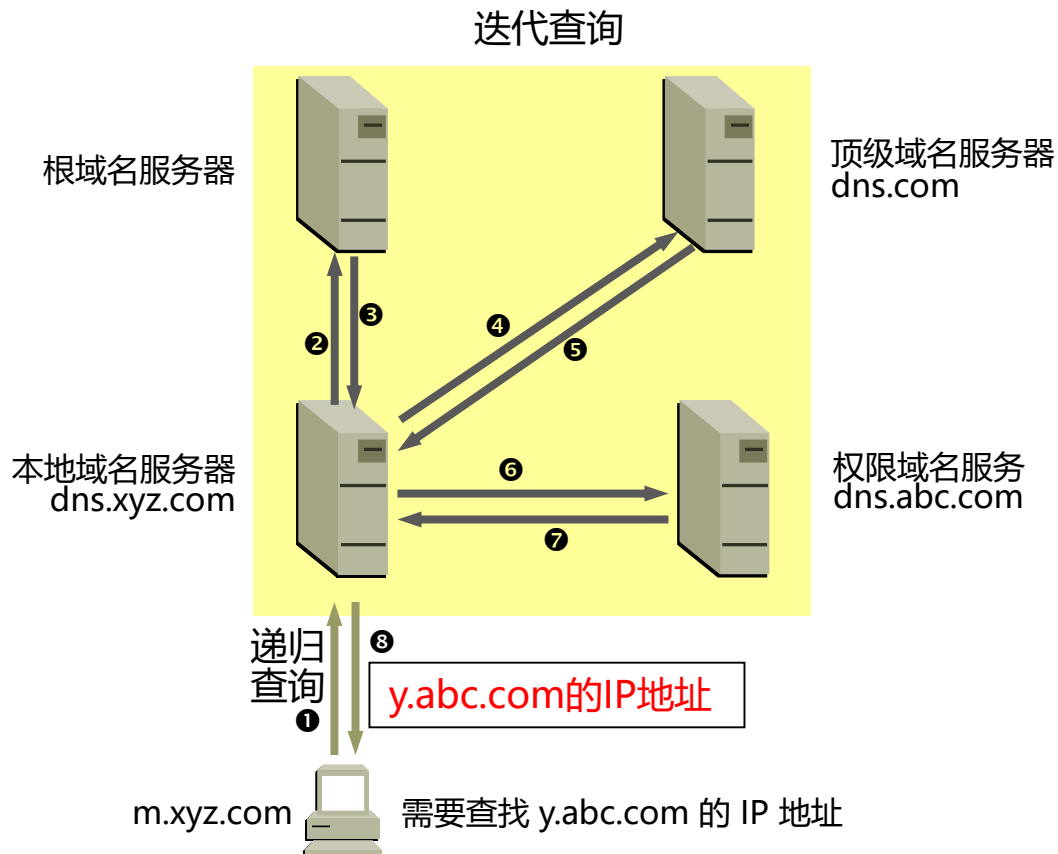
1.域名系统DNS

1.4域名的解析过程

- 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。

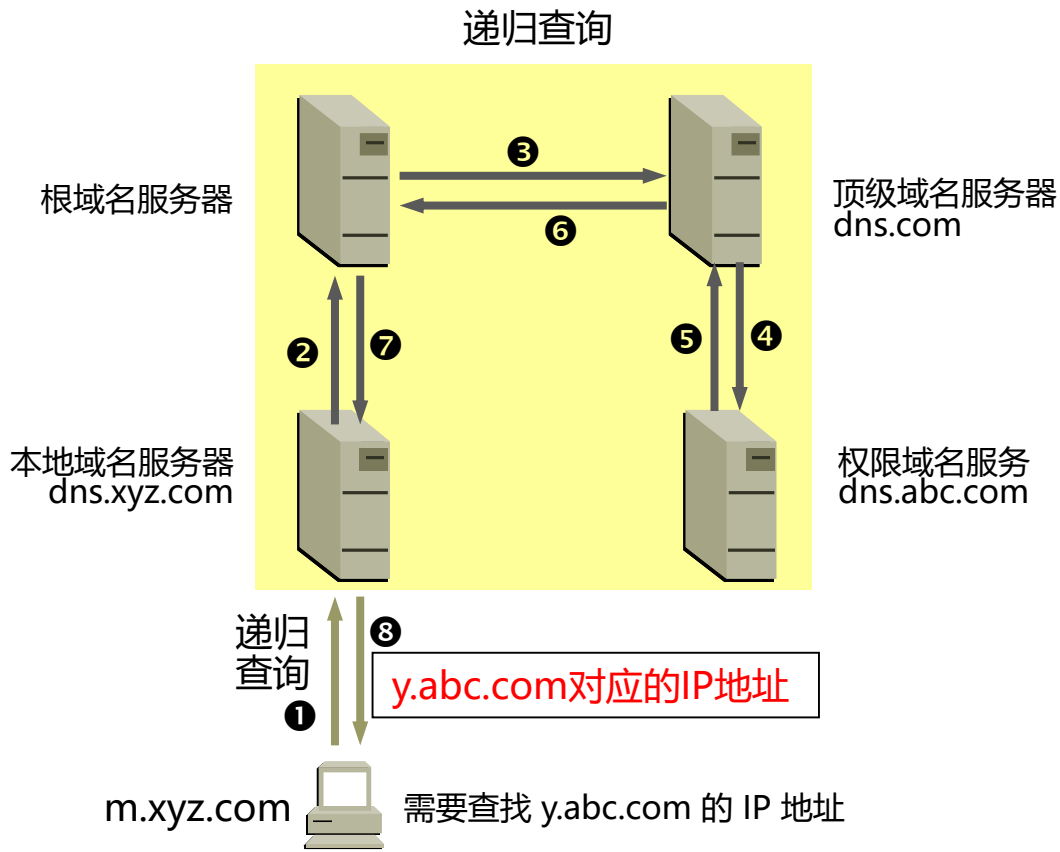
1.域名系统DNS

1.4域名的解析过程

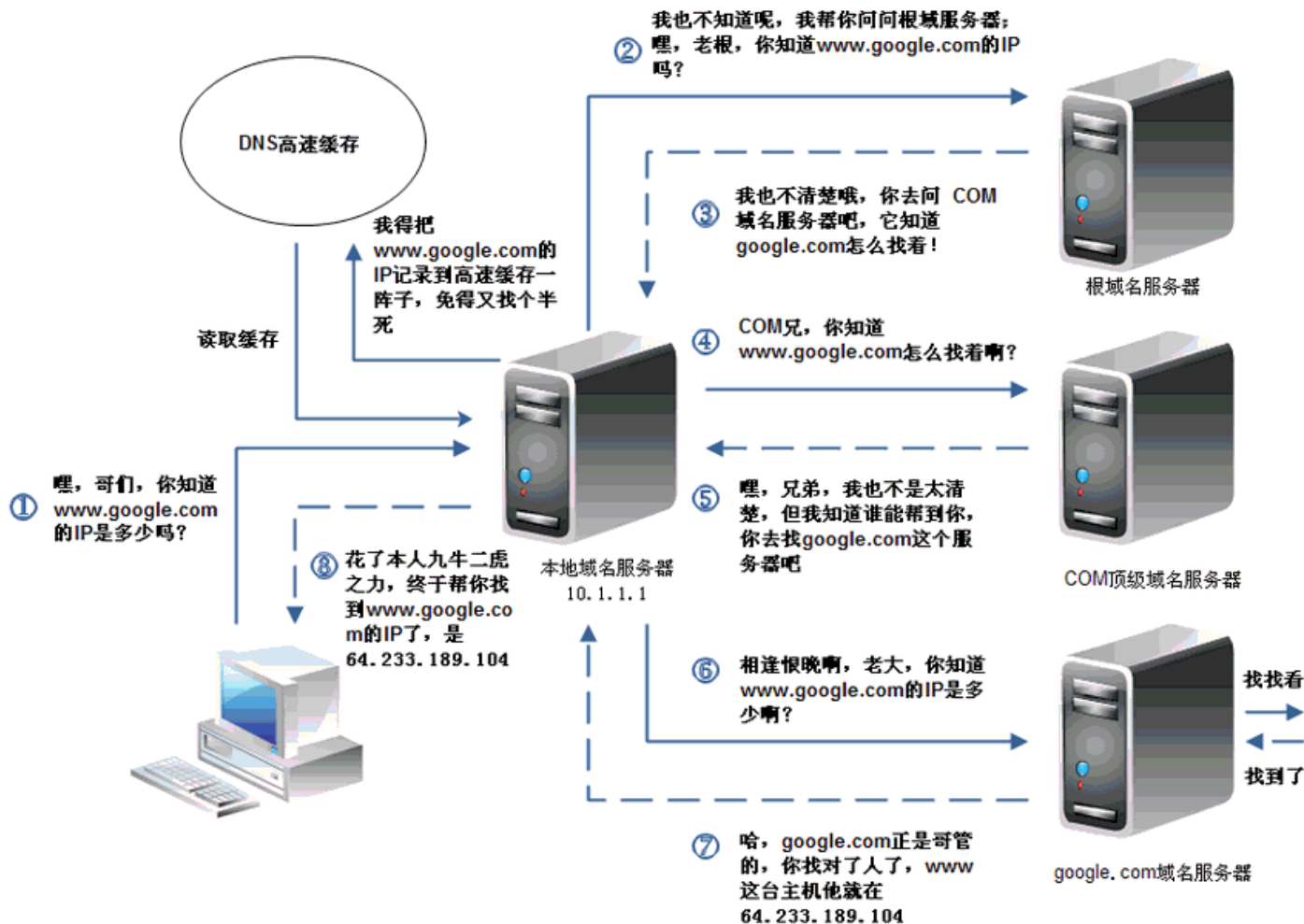


1.域名系统DNS

1.4域名的解析过程



DNS域名解析过程



- 1、等我找一下named.conf看看是这有没有关于它的定义；
- 2、找到了，是我定义，我看看google.com的区域文件；
- 3、瞄了一下，嘿，有关于www的主机记录哦。

递归查询

迭代查询

1.域名系统DNS

1.4域名的解析过程

The image shows a Wireshark capture of a DNS transaction on port 53. The packet list pane shows four packets:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-------------|-------------|----------|--------|--|
| 1 | 0.000000 | 10.10.3.202 | 8.8.8.8 | DNS | 70 | Standard query 0x0006 A www.edu.cn |
| 2 | 0.194650 | 8.8.8.8 | 10.10.3.202 | DNS | 102 | Standard query response 0x0006 A www.edu.cn A 202.112.0.36 A 202.205.109.203 |
| 3 | 0.195283 | 10.10.3.202 | 8.8.8.8 | DNS | 70 | Standard query 0x0007 AAAA www.edu.cn |
| 4 | 0.387951 | 8.8.8.8 | 10.10.3.202 | DNS | 98 | Standard query response 0x0007 AAAA www.edu.cn AAAA 2001:da8:ff3a:c8fd:400:: |

The packet details pane shows the response for transaction ID 0x0006:

```

[Response In: 2]
Transaction ID: 0x0006
Flags: 0x0100 Standard query
  0... .. = Response: Message is a query
  .000 0... .. = Opcode: Standard query (0)
  .... ..0. .... = Truncated: Message is not truncated
  .... ..1 .... = Recursion desired: Do query recursively
  .... ..0. .... = Z: reserved (0)
  .... ..0 .... = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
  
```

The packet bytes pane shows the raw DNS message structure in hexadecimal and ASCII:

```

0000  00000000 00100100 10101100 00001110 11111001 10011000 00000000 01010000  .$....P
0008  01010110 10110111 00000010 11000100 00001000 00000000 01000101 00000000  V.....E.
0010  00000000 00111000 00100010 00100100 00000000 00000000 10000000 00010001  .8"$....
0018  00000000 00000000 00001010 00001010 00000011 11001010 00001000 00001000  .....
0020  00001000 00001000 11101010 11111011 00000000 00110101 00000000 00100100  ....5.$
0028  00011110 00011001 00000000 00000110 00000001 00000000 00000000 00000001  .....
0030  00000000 00000000 00000000 00000000 00000000 00000000 00000011 01110111  .....w
0038  01110111 01110111 00000011 01100101 01100100 01110101 00000010 01100011  ww.edu.c
0040  01101110 00000000 00000000 00000001 00000000 00000001  n....
  
```

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

1.5域名的高速缓存

- 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

1.5域名的高速缓存

- 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

1.5域名的高速缓存

- 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

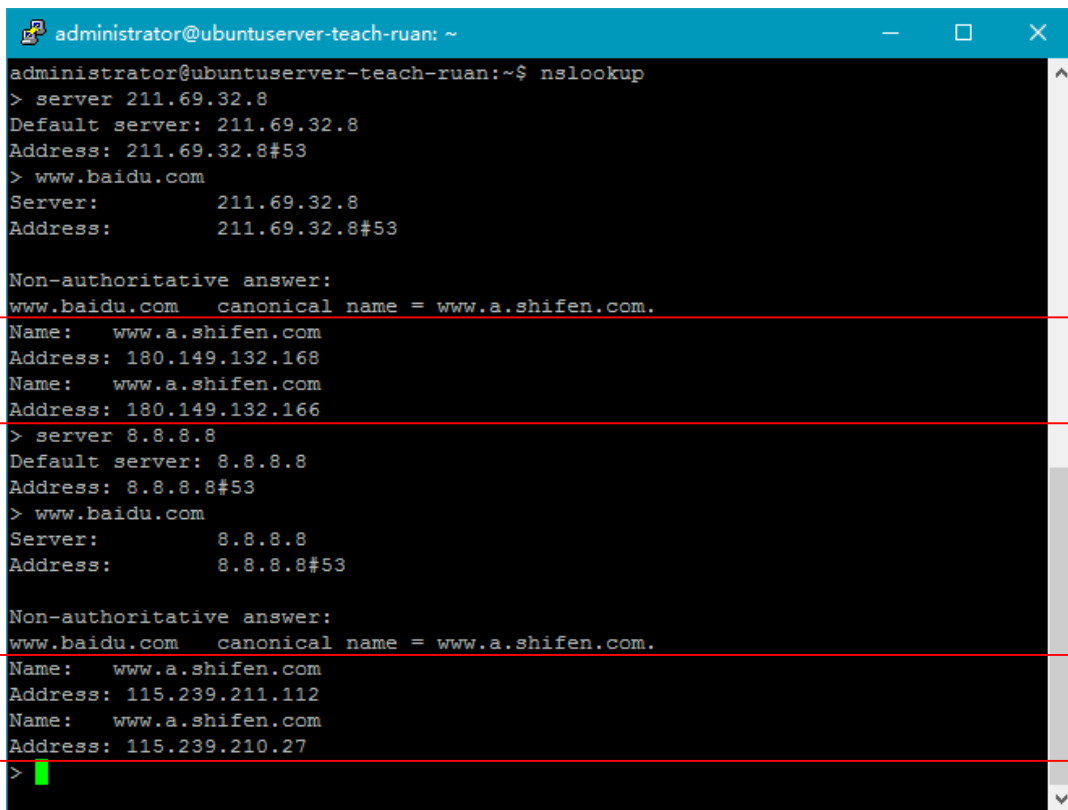
1.域名系统DNS

1.6域名解析的测试

- 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



```
administrator@ubuntuserver-teach-ruan: ~
administrator@ubuntuserver-teach-ruan:~$ nslookup
> server 211.69.32.8
Default server: 211.69.32.8
Address: 211.69.32.8#53
> www.baidu.com
Server:          211.69.32.8
Address:         211.69.32.8#53

Non-authoritative answer:
www.baidu.com  canonical name = www.a.shifen.com.
Name:   www.a.shifen.com
Address: 180.149.132.168
Name:   www.a.shifen.com
Address: 180.149.132.166
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> www.baidu.com
Server:          8.8.8.8
Address:         8.8.8.8#53

Non-authoritative answer:
www.baidu.com  canonical name = www.a.shifen.com.
Name:   www.a.shifen.com
Address: 115.239.211.112
Name:   www.a.shifen.com
Address: 115.239.210.27
>
```

1

```

administrator@ubuntu-server-teach-ruan: ~
administrator@ubuntu-server-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@ubuntu-server-teach-ruan:~$

```

式

4

```

administrator@ubuntu-server-teach-ruan: ~
administrator@ubuntu-server-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@ubuntu-server-teach-ruan:~$

```

2. 文件传送协议

2.1 FTP概述

- 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

2.1 FTP概述

- 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

2.2FTP的基本工作原理

- 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

2.2FTP的基本工作原理

- 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

2.2FTP的基本工作原理

- 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。

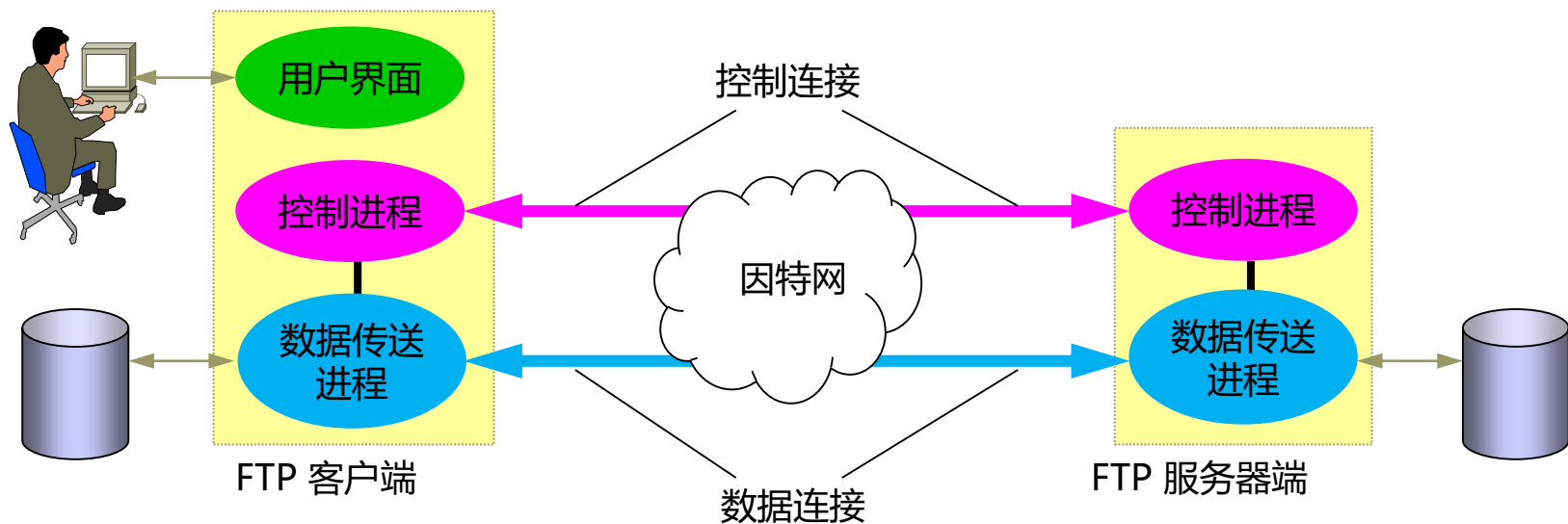
2.文件传送协议

2.2FTP的基本工作原理

- 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

2.2 FTP的基本工作原理



2.文件传送协议

2.2FTP的基本工作原理

- 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。

| 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, CHR] 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
 [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 11110101 11010110 00001000 00000000 01000101 00000000 V.....E
0010  00000000 00111101 00111111 11010101 01000000 00000000 10000000 00000110 .=?.@...
0018  10011111 10111111 00001010 00001010 00000011 00110001 00001010 00001010 .....1..
0020  00000011 11001010 00000000 00010101 11100110 10110010 00100100 11000100 .....$.
  
```

2.文件传送协议

2.2FTP的基本工作原理

The image shows a Wireshark network traffic capture window. The top bar indicates the selected IP address is 10.10.3.49. Below the toolbar, a table displays the captured packets, highlighting FTP-related traffic. The table columns are No., Time, Source, Destination, Protocol, Length, and Info.

| 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
- ▼ 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]

- ▼ File Transfer Protocol (FTP)

- ▼ 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

2.2 FTP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
- ▼ 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

2.3简单文件传送协议TFTP

- ❑ 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

2.3简单文件传送协议TFTP

□ 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

2.3简单文件传送协议TFTP

□ 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

2.3简单文件传送协议TFTP

□ 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

2.4FTP与TFTP的对比

- 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

2.4FTP与TFTP的对比

□ 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：

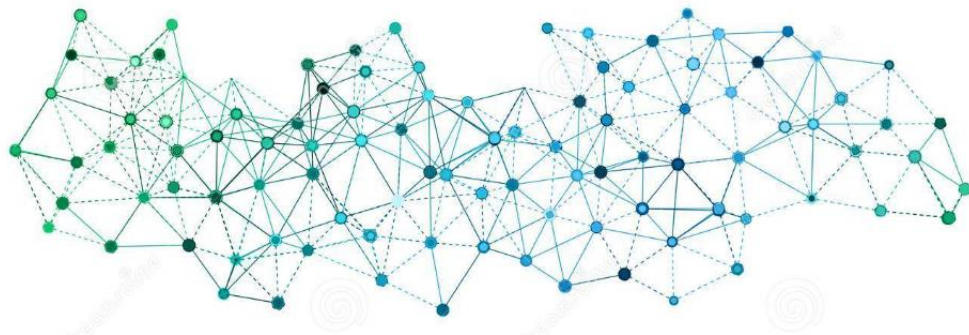
- FTP允许交互通信。
- TFTP仅允许单向传输文件。

□ 在认证上：

- FTP提供身份验证。
- TFTP不支持身份验证。

□ 在运输层上：

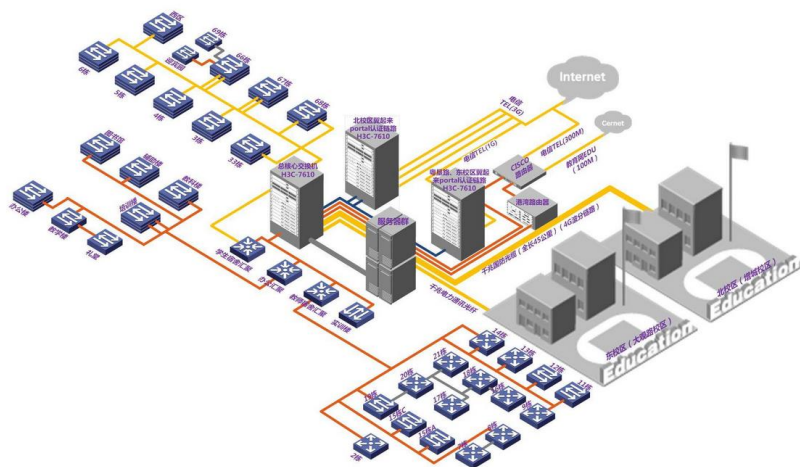
- FTP使用已知TCP端口号21作为控制连接，TCP端口号20作为数据连接。
- TFTP使用UDP端口号69作为文件传输活动。



3. 远程终端协议TELNET

3.1 客观问题

- 随着网络规模的扩大，网络应用的丰富，园区网部署的网络设备（例如路由器、交换机、无线设备等）越来越多，对设备的可靠运行要求也越来越高。
- 如何进行设备管理与维护？



3.远程终端协议TELNET

3.1客观问题

远程
管理



集中
控制

3.远程终端协议TELNET

3.2 TELNET的基本概念

- TELNET是简单的远程终端协议。
- TELNET是因特网正式标准。
 - 该标准定义文档为【RFC 854】【RFC 5198】。
 - <https://www.rfc-editor.org/info/rfc854>。
- TELNET协议是TCP/IP协议族的一员，是Internet远程登录服务的标准协议。
 - 用TELNET可通过TCP连接登录到远程主机上。
 - 用TELNET访问远程主机使用主机名或 IP 地址。
 - 远程主机使用TCP 23端口进行通信。

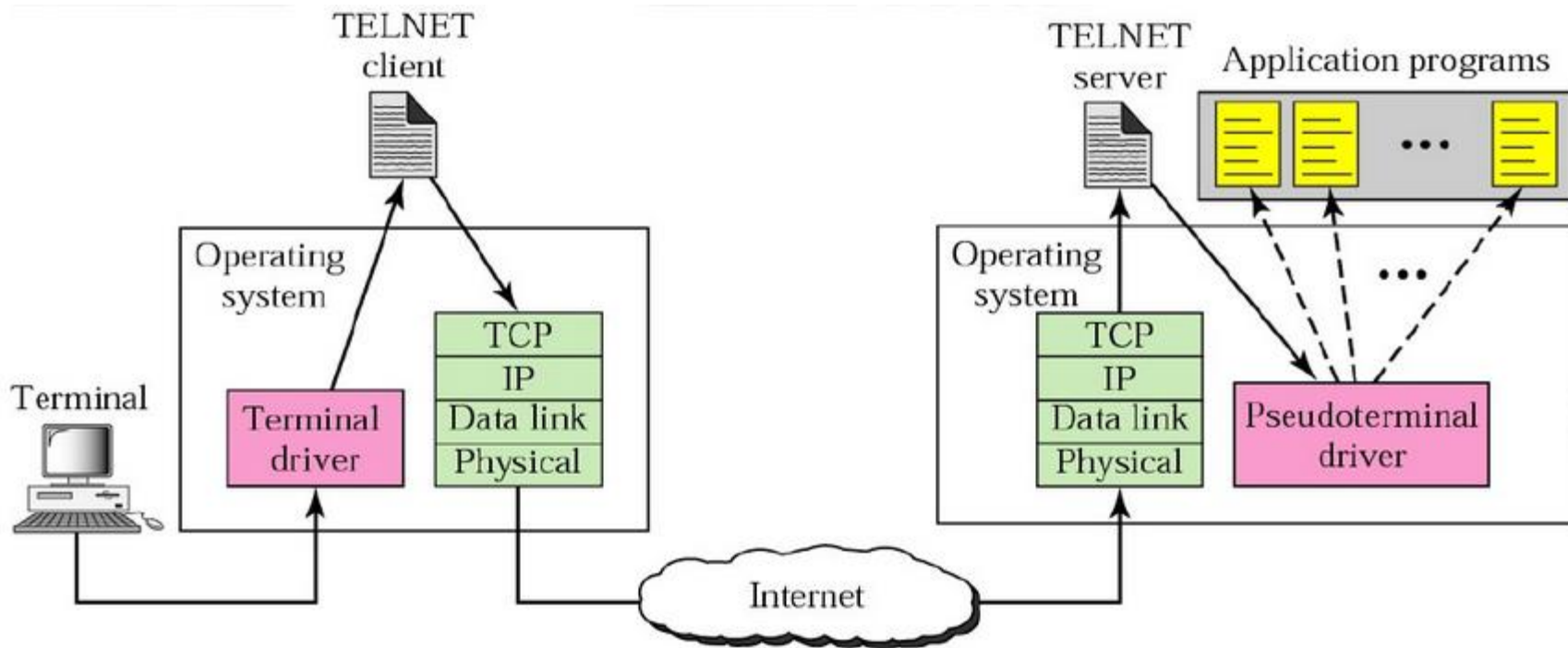
3.远程终端协议TELNET

3.3 TELNET的实现方式

- TELNET使用 客户/服务器 方式。
- TELNET实现需要三个组成部分。
 - TELNET客户端软件：
 - 安装在本地主机，处理用户输入/输出。
 - TELNET服务端软件：
 - 安装在远程受控设备。
 - TELNET协议接口程序：
 - 存在TELNET客户端和服务端软件中，实现 TELNET 协议，并维护协议状态。

3. 远程终端协议 TELNET

3.3 TELNET的实现方式



3. 远程终端协议TELNET

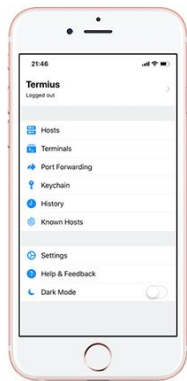
3.3 TELNET的实现方式

□ TELNET客户端软件要做两件事：

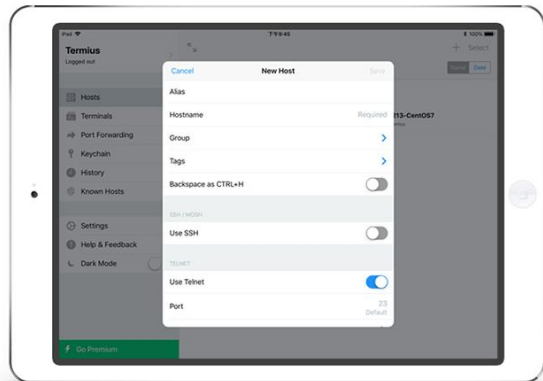
- 读取用户在键盘上键入的字符，通过TCP连接发送到远程服务器上。
- 读取从TCP连接上收到的字符，显示在用户的终端上。



JuiceSSH
For Android



Termius
For iPhone



Termius
For iPad



Xshell
For Windows



演示：使用TELNET远程控制和报文分析



1 本地Shell

Xshell 5 (Build 1339)

Copyright (c) 2002-2017 NetSarang Computer, Inc. All rights reserved.

Type 'help' to learn how to use Xshell prompt.

[c:\-] \$

会话

所有会话

| 名称 | 主机 | 端口 | 协议 | 用户名 | 说明 |
|-------------------------------------|---------------|----|--------|------------|----|
| 211.69.35.213-CentOS 7 | 211.69.35.213 | 22 | SSH | root | |
| 211.69.35.213-CentOS 7-Teach | 211.69.35.213 | 22 | SSH | root | |
| 211.69.35.214-Ubuntu Server 17.10.1 | 211.69.35.214 | 22 | SSH | adminis... | |
| DEMO SSH | 211.69.35.177 | 22 | SSH | | |
| DEMO TELNET | 211.69.35.177 | 23 | TELNET | | |

启动时显示此对话框(S)

连接(C) 关闭

DEMO TELNET 属性

类别(C):

- 连接
- 用户身份验证
 - 登录提示符
 - 登录脚本
- SSH
 - 安全性
 - 隧道
 - STP
 - TELNET
 - RLOGIN
 - SERIAL
 - 代理
 - 保持活动状态
- 终端
 - 键盘
 - VT 模式
 - 高级
- 外观
 - 窗口
- 高级
 - 跟踪
 - 日志记录
- 文件传输
 - X/MODEM
 - ZMODEM

连接

常规

名称(N): DEMO TELNET

协议(P): TELNET

主机(H): 211.69.35.177

端口号(O): 23

说明(D):

重新连接

连接异常关闭时自动重新连接(A)

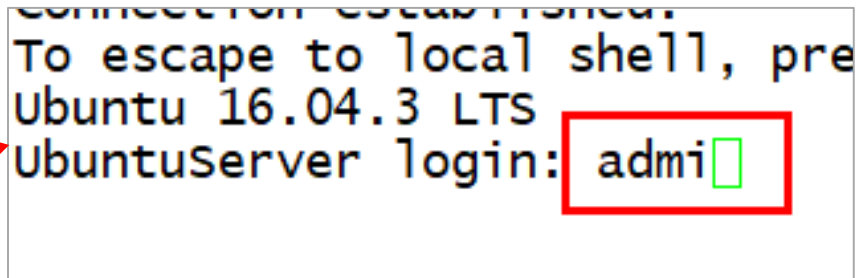
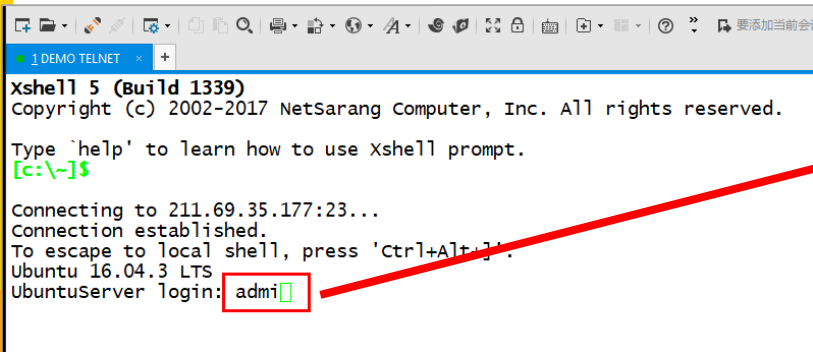
间隔(V): 0 秒 限制(L): 0 分钟

TCP选项

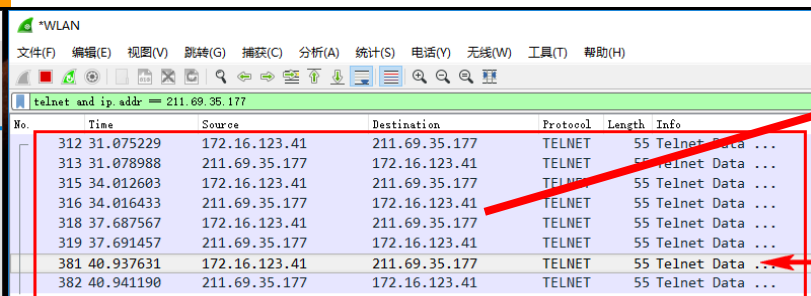
使用Nagle算法(L)

确定 取消

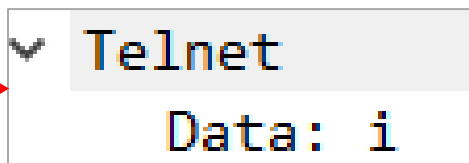
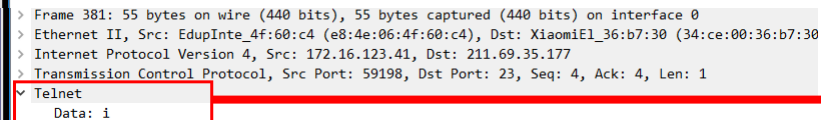
Telnet操作



抓包结果



| | |
|---------------|---------------|
| 172.16.123.41 | 211.69.35.177 |
| 211.69.35.177 | 172.16.123.41 |
| 172.16.123.41 | 211.69.35.177 |
| 211.69.35.177 | 172.16.123.41 |
| 172.16.123.41 | 211.69.35.177 |
| 211.69.35.177 | 172.16.123.41 |
| 172.16.123.41 | 211.69.35.177 |
| 211.69.35.177 | 172.16.123.41 |



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 and ip.addr == 211.69.35.177

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|---------------|---------------|----------|--------|-----------------|
| 312 | 31.075229 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 | Telnet Data ... |
| 313 | 31.078988 | 211.69.35.177 | 172.16.123.41 | TELNET | 55 | Telnet Data ... |
| 315 | 34.012603 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 | Telnet Data ... |
| 316 | 34.016433 | 211.69.35.177 | 172.16.123.41 | TELNET | 55 | Telnet Data ... |
| 318 | 37.687567 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 | Telnet Data ... |
| 319 | 37.691457 | 211.69.35.177 | 172.16.123.41 | TELNET | 55 | Telnet Data ... |
| 381 | 40.937631 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 | Telnet Data ... |
| 382 | 40.941190 | 211.69.35.177 | 172.16.123.41 | TELNET | 55 | Telnet Data ... |

> Frame 381: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface
> Ethernet II, Src: EdupInte_4f:60:c4 (e8:4e:06:4f:60:c4), Dst: XiaomiE1_36:b7:30 (
> Internet Protocol Version 4, Src: 172.16.123.41, Dst: 211.69.35.177
> Transmission Control Protocol, Src Port: 59198, Dst Port: 23, Seq: 4, Ack: 4, Len

▼ Telnet

Data: i


```
Connecting to 211.69.35.177:23...
Connection established.
To escape to local shell, press 'Ctrl+Alt+]'.
Ubuntu 16.04.3 LTS
UbuntuServer login: administrator
Password:
Last login: Thu Jun 21 23:26:18 CST 2018 from 10.10.0.1 on pts/1
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-87-generic x86_64)
```

| | | | | | |
|-----|-----------|---------------|---------------|--------|---------------------|
| 165 | 5.575288 | 211.69.35.177 | 172.16.123.41 | TELNET | 64 Telnet Data ... |
| 250 | 8.362583 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 Telnet Data ... |
| 252 | 8.787578 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 Telnet Data ... |
| 279 | 9.350046 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 Telnet Data ... |
| 328 | 11.487617 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 Telnet Data ... |
| 331 | 12.237094 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 Telnet Data ... |
| 333 | 12.712563 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 Telnet Data ... |
| 357 | 13.637572 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 Telnet Data ... |
| 359 | 16.124757 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 Telnet Data ... |
| 361 | 16.127401 | 211.69.35.177 | 172.16.123.41 | TELNET | 56 Telnet Data ... |
| 363 | 16.180029 | 211.69.35.177 | 172.16.123.41 | TELNET | 120 Telnet Data ... |

正在捕获 WLAN

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 and ip.addr == 211.69.35.177

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|---------------|---------------|----------|--------|-----------------|
| 138 | 4.812019 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 | Telnet Data ... |
| 139 | 4.816820 | 211.69.35.177 | 172.16.123.41 | TELNET | 55 | Telnet Data ... |
| 160 | 5.524435 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 | Telnet Data ... |
| 161 | 5.528119 | 211.69.35.177 | 172.16.123.41 | TELNET | 56 | Telnet Data ... |
| 165 | 5.575288 | 211.69.35.177 | 172.16.123.41 | TELNET | 64 | Telnet Data ... |
| 250 | 8.362583 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 | Telnet Data ... |
| 252 | 8.787578 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 | Telnet Data ... |
| 279 | 9.350046 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 | Telnet Data ... |
| 328 | 11.487617 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 | Telnet Data ... |
| 331 | 12.237094 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 | Telnet Data ... |
| 333 | 12.712563 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 | Telnet Data ... |
| 357 | 13.637572 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 | Telnet Data ... |
| 359 | 16.124757 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 | Telnet Data ... |
| 361 | 16.127401 | 211.69.35.177 | 172.16.123.41 | TELNET | 56 | Telnet Data ... |
| 363 | 16.180029 | 211.69.35.177 | 172.16.123.41 | TELNET | 120 | Telnet Data ... |
| 365 | 16.255872 | 211.69.35.177 | 172.16.123.41 | TELNET | 338 | Telnet Data ... |
| 367 | 16.375132 | 211.69.35.177 | 172.16.123.41 | TELNET | 118 | Telnet Data ... |

此处8条连续的本地主机发往远程服务器的通信。
说明：密码7位，最后一条是回车确认。

> Frame 250: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
 > Ethernet II, Src: EdupInte_4f:60:c4 (e8:4e:06:4f:60:c4), Dst: XiaomiE1_36:b7:30 (34:ce:00:36:b7:30)
 > Internet Protocol Version 4, Src: 172.16.123.41, Dst: 211.69.35.177
 > Transmission Control Protocol, Src Port: 59207, Dst Port: 23, Seq: 15, Ack: 26, Len: 1

▼ Telnet
 Data: a 密码的第一个字母是：a

```

0000 34 ce 00 36 b7 30 e8 4e 06 4f 60 c4 08 00 45 00 4 -·6·0·N ·0`···E·
0010 00 29 5d 5d 40 00 80 06 7f 41 ac 10 7b 29 d3 45 ·)]]@····A·{·}·E
0020 23 b1 e7 47 00 17 dc 17 b5 59 19 e0 35 ba 50 18 #··G·····Y··5·P·
0030 01 00 67 30 00 00 61 ··g0··a
  
```

WLAN: <live capture in progress> 分组: 428 · 已显示: 41 (9.6%) Profile: Default

The image displays two windows. The left window is a terminal titled 'Xshell 5 (Build 1339)' showing a Telnet session to 211.69.35.177:23. The session is successful, with the user 'administrator' logging in. The terminal output includes the system version 'Ubuntu 16.04.3 LTS' and system updates information. The right window is a network analysis tool showing a list of Telnet connections. A red box highlights a sequence of 8 consecutive local-to-remote connections. Below the list, a detailed view of a frame shows the captured data as 'a', with a note indicating that 'a' is the first character of the password.

正在捕获 WLAN

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|---------------|---------------|----------|--------|-----------------|
| 138 | 4.812019 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 | Telnet Data ... |
| 139 | 4.816820 | 211.69.35.177 | 172.16.123.41 | TELNET | 55 | Telnet Data ... |
| 160 | 5.524435 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 | Telnet Data ... |
| 161 | 5.528119 | 211.69.35.177 | 172.16.123.41 | TELNET | 56 | Telnet Data ... |
| 165 | 5.575288 | 211.69.35.177 | 172.16.123.41 | TELNET | 64 | Telnet Data ... |
| 250 | 8.362583 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 | Telnet Data ... |
| 252 | 8.787578 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 | Telnet Data ... |
| 279 | 9.350046 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 | Telnet Data ... |
| 328 | 11.487617 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 | Telnet Data ... |
| 331 | 12.237094 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 | Telnet Data ... |
| 333 | 12.712563 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 | Telnet Data ... |
| 357 | 13.637572 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 | Telnet Data ... |
| 359 | 16.124757 | 172.16.123.41 | 211.69.35.177 | TELNET | 55 | Telnet Data ... |
| 361 | 16.127401 | 211.69.35.177 | 172.16.123.41 | TELNET | 56 | Telnet Data ... |
| 363 | 16.180029 | 211.69.35.177 | 172.16.123.41 | TELNET | 120 | Telnet Data ... |
| 365 | 16.255872 | 211.69.35.177 | 172.16.123.41 | TELNET | 338 | Telnet Data ... |
| 367 | 16.375132 | 211.69.35.177 | 172.16.123.41 | TELNET | 118 | Telnet Data ... |

Frame 250: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
 > Ethernet II, Src: EduPInte_4f:60:c4 (e8:4e:06:4f:60:c4), Dst: XiaomiE1_36:b7:30 (34:ce:00:36:b7:30)
 > Internet Protocol Version 4, Src: 172.16.123.41, Dst: 211.69.35.177
 > Transmission Control Protocol, Src Port: 59207, Dst Port: 23, Seq: 15, Ack: 26, Len: 1

Telnet
 Data: a 密码的第一个字母是: a

```

0000 34 ce 00 36 b7 30 e8 4e 06 4f 60 c4 08 00 45 00 4..6.0.N.0...E.
0010 00 29 5d 5d 40 00 80 06 7f 41 ac 10 7b 29 d3 45  -]]@...-A-{}-E
0020 23 b1 e7 47 00 17 dc 17 b5 59 19 e0 35 ba 50 18  #-G....Y..S.P.
0030 01 00 67 30 00 00 61                               -g0..a
  
```

此处8条连续的本地主机发往远程服务器的通信。
 说明：密码7位，最后一条是回车确认。

注：信息管理与信息系统本科专业在教学中提出【全演示】要求，目前所有专业课上已基本全实现。

具体要求是：

教学中的所有实验和案例，都要求在现场进行演示和讲解，不截图讲操作，不用视频说流程。

所有操作都会在现场逐步完成，坚持用演示性讲解引导教学全过程。

3.远程终端协议TELNET

3.4 TELNET的使用方法

- TELNET将用户的**击键**传到远程受控设备，同时将远程受控设备的输出返回到用户屏幕。
- TELNET服务是透明的，使用TELNET进行远程控制就仿佛自己的键盘和显示器是直接连在远地主机上。

3.远程终端协议TELNET

3.5 TELNET的特点




跨平台
支持



传送
击键



明文
传输



低成本
实现



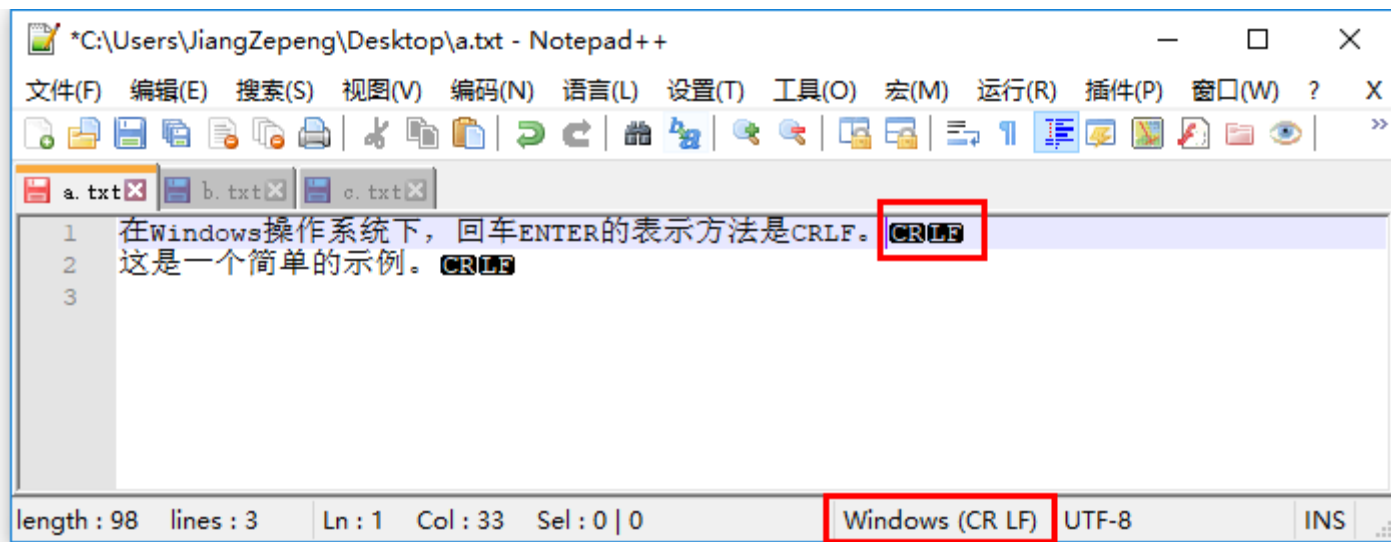
讨论：为什么TELNET不用加密的方式通信？



工程应用以最优为原则

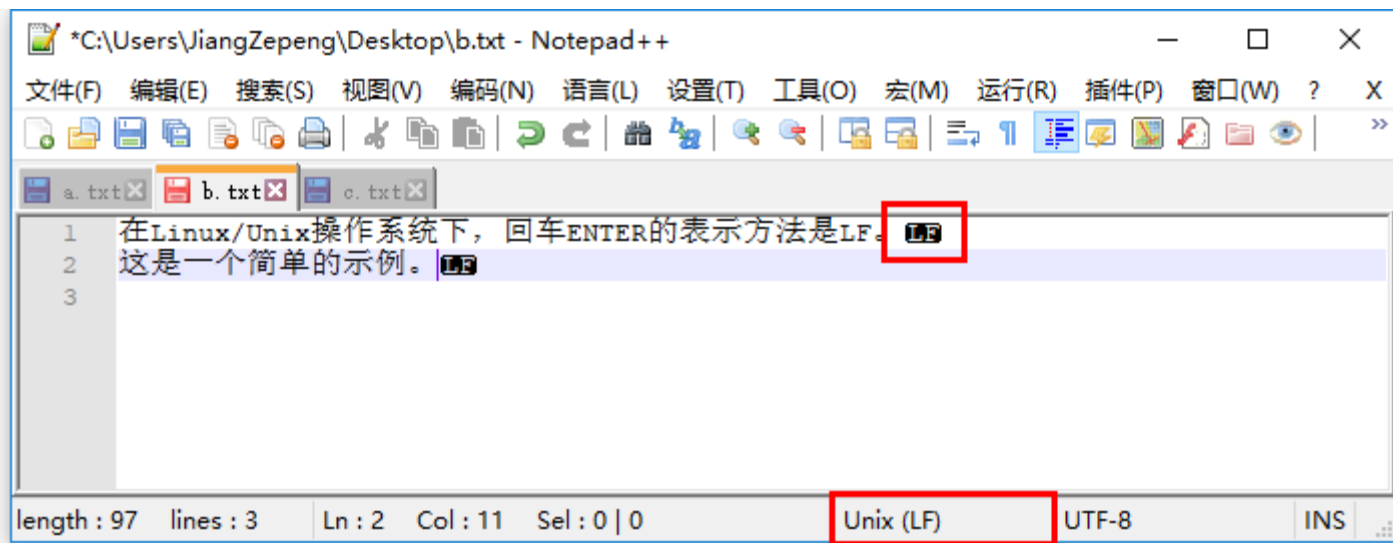
3.远程终端协议TELNET

3.6 NVT



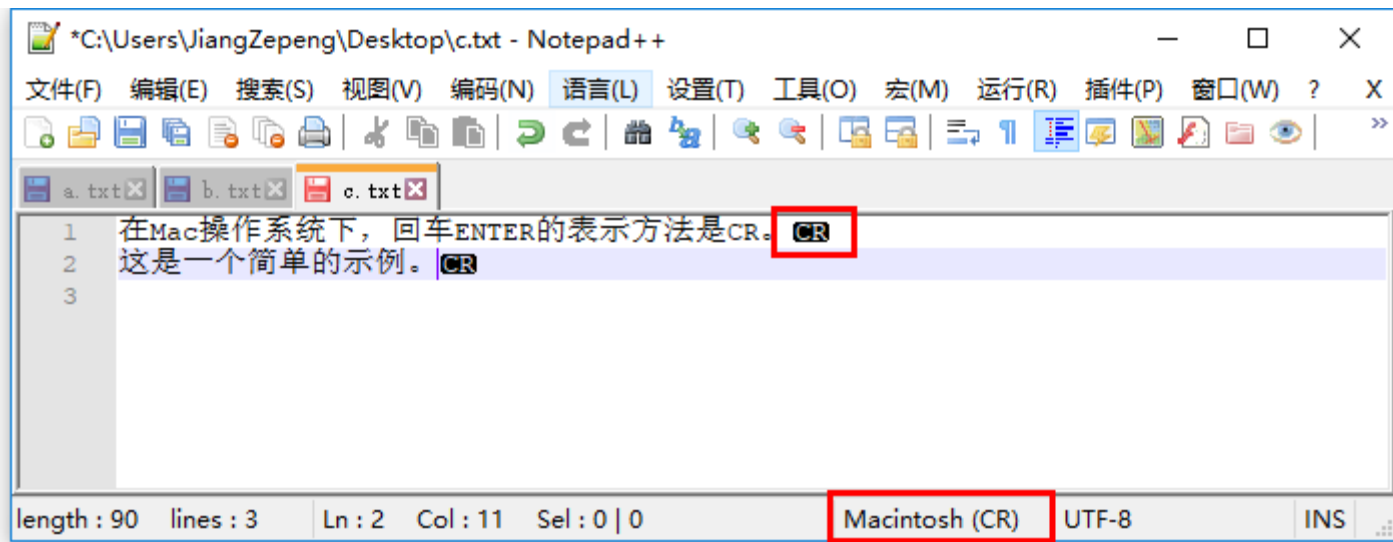
3.远程终端协议TELNET

3.6 NVT



3.远程终端协议TELNET

3.6 NVT





讨论：

本地主机是Windows操作系统，
远程受控设备是Linux操作系统，
通过TELNET进行远程管理时进行回车操作，
远程受控主机能够识别么？



3.远程终端协议TELNET

3.6 NVT

- 为了使多个操作系统间的Telnet交互操作成为可能，就必须详细了解异构计算机和操作系统。
 - 比如，一些操作系统需要每行文本用ASCII回车控制符（CR）结束，另一些系统则需要使用ASCII换行符（LF），还有一些系统需要用两个字符的序列回车-换行（CR-LF）；
 - 比如，大多数操作系统为用户提供了一个中断程序运行的快捷键，但这个快捷键在各个系统中有可能不同（一些系统使用CTRL+C，而另一些系统使用ESCAPE）。如果不考虑系统间的异构性，那么在本地发出的字符或命令，传送到远地并被远地系统解释后很可能会不准确或者出现错误。

3.远程终端协议TELNET

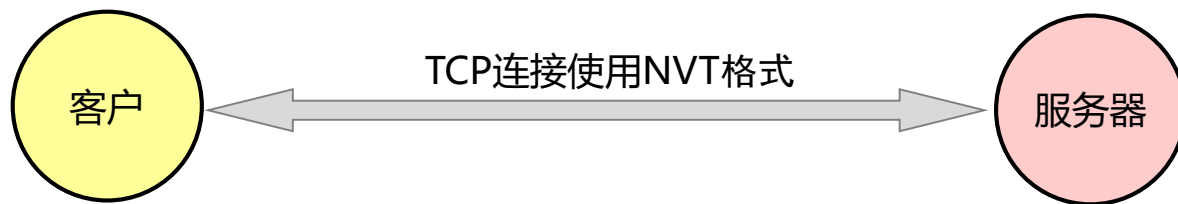
3.6 NVT

- 为了适应异构环境，TELNET协议定义了数据和命令在Internet上的传输方式，此定义被称作**网络虚拟终端NVT (Net Virtual Terminal)**。
- 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

3.6 NVT

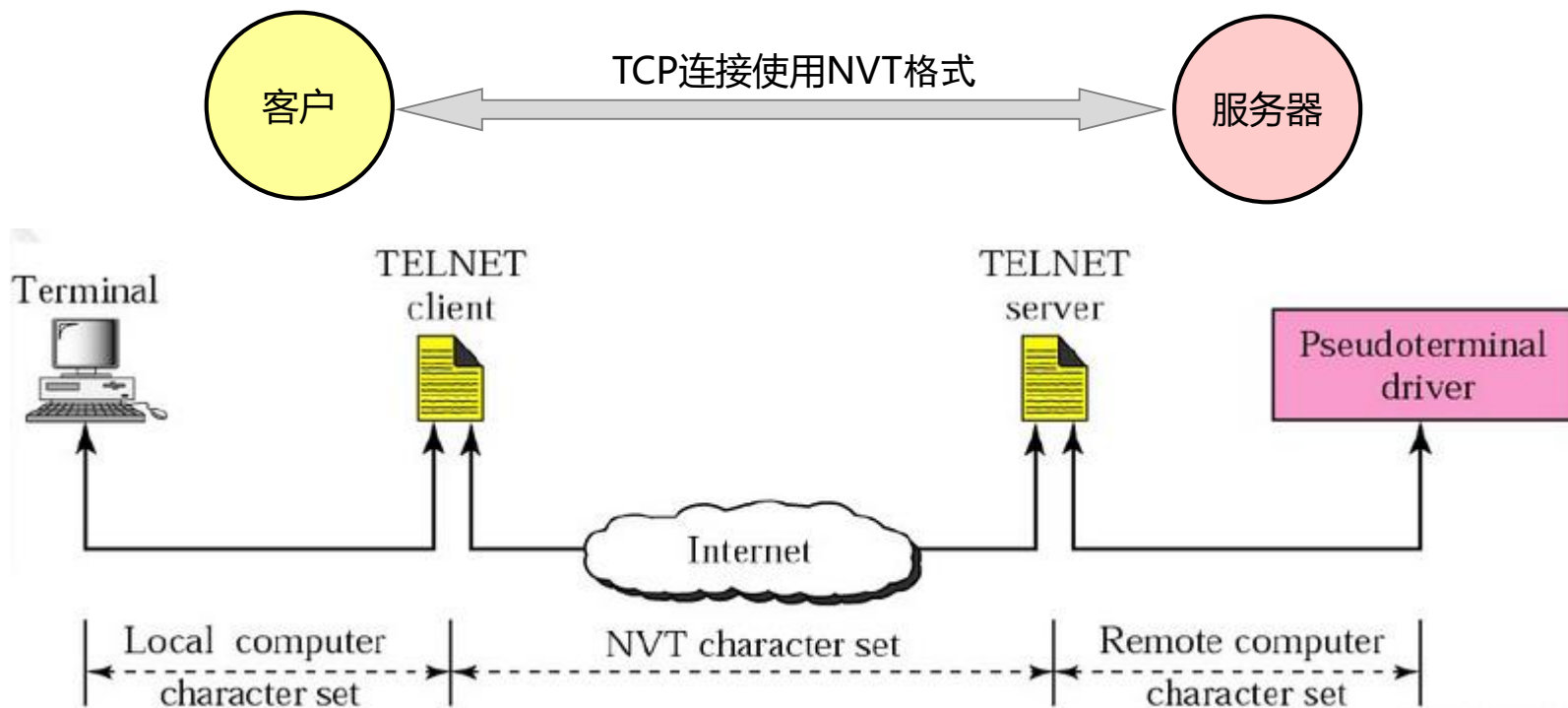
- TELNET使用网络虚拟终端NVT格式。



3. 远程终端协议TELNET

3.6 NVT

- TELNET使用网络虚拟终端NVT格式。





讨论：还有其他远程管理方式么？

3.远程终端协议TELNET

3.7扩展：远程管理的更多实现方式



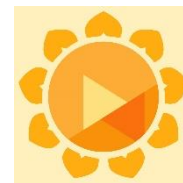
RDP
Windows



VNC
Linux、UNIX、Windows、Mac



SSH
Linux、UNIX、Mac



Agent
Linux、UNIX、Windows、Mac

3.远程终端协议TELNET

3.8还有两个问题

□ 操作协商：

- 基本的NVT设备所具有特性十分有限，只能接收和显示7位的ASCII码，为此TELNET协议定义了一组协议用于扩展基本NVT的功能，使NVT达到用户终端所具有的功能。
- TELNET协议规定在扩展NVT功能时采用协商的机制，只有通信双方通过协商后达成一致的的特性才能使用。
- 有哪些扩展？如何进行协商？

□ TELNET报文结构：

- 发送与接收报文的结构如何？各字段的含义与取值？

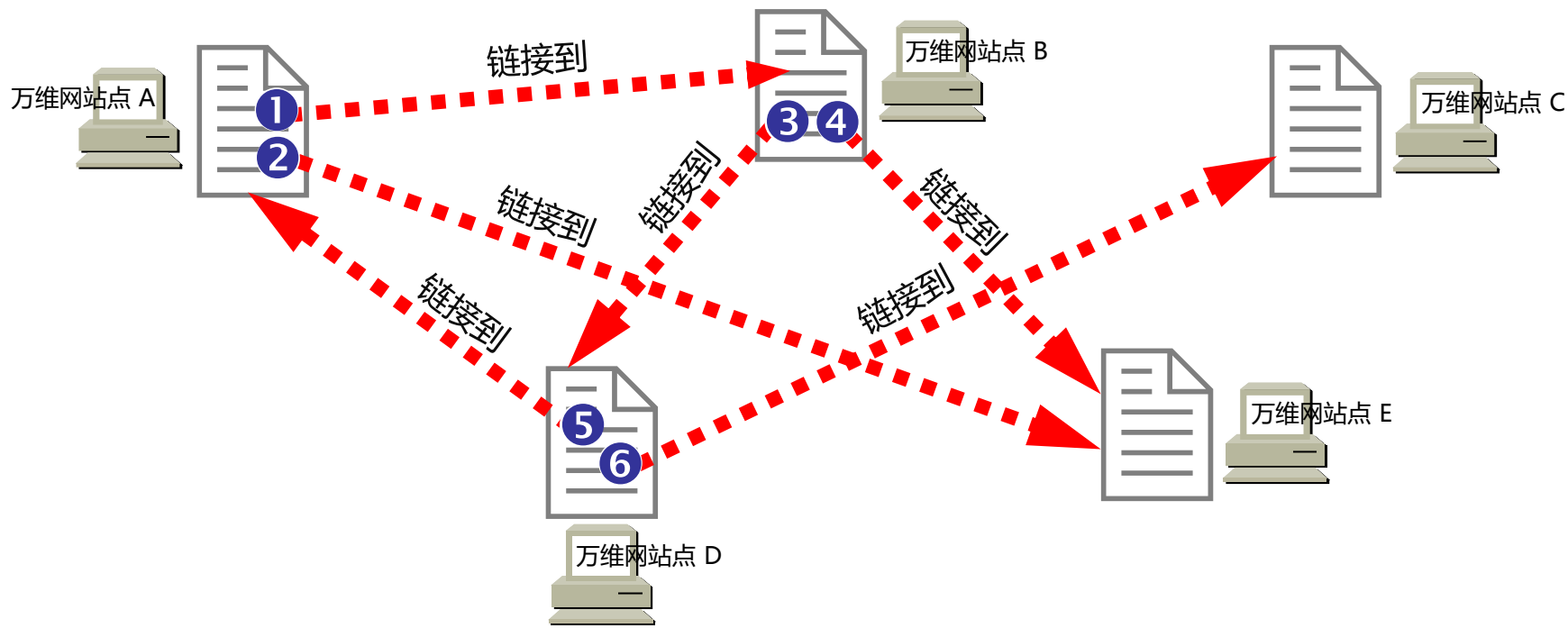
4.万维网WWW

4.1万维网概述

- 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

4.1万维网概述



4.万维网WWW

4.1万维网概述

- 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
 - 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

4.1万维网概述

- 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

4.1万维网概述

□ 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连接？
 - 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

4.1万维网概述

□ 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

4.2统一资源定位符URL

□ 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。
- 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

4.2统一资源定位符URL

□ 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

4.2统一资源定位符URL

□ 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

4.2统一资源定位符URL

□ 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

4.2统一资源定位符URL

□ 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

4.3超文本传送协议HTTP

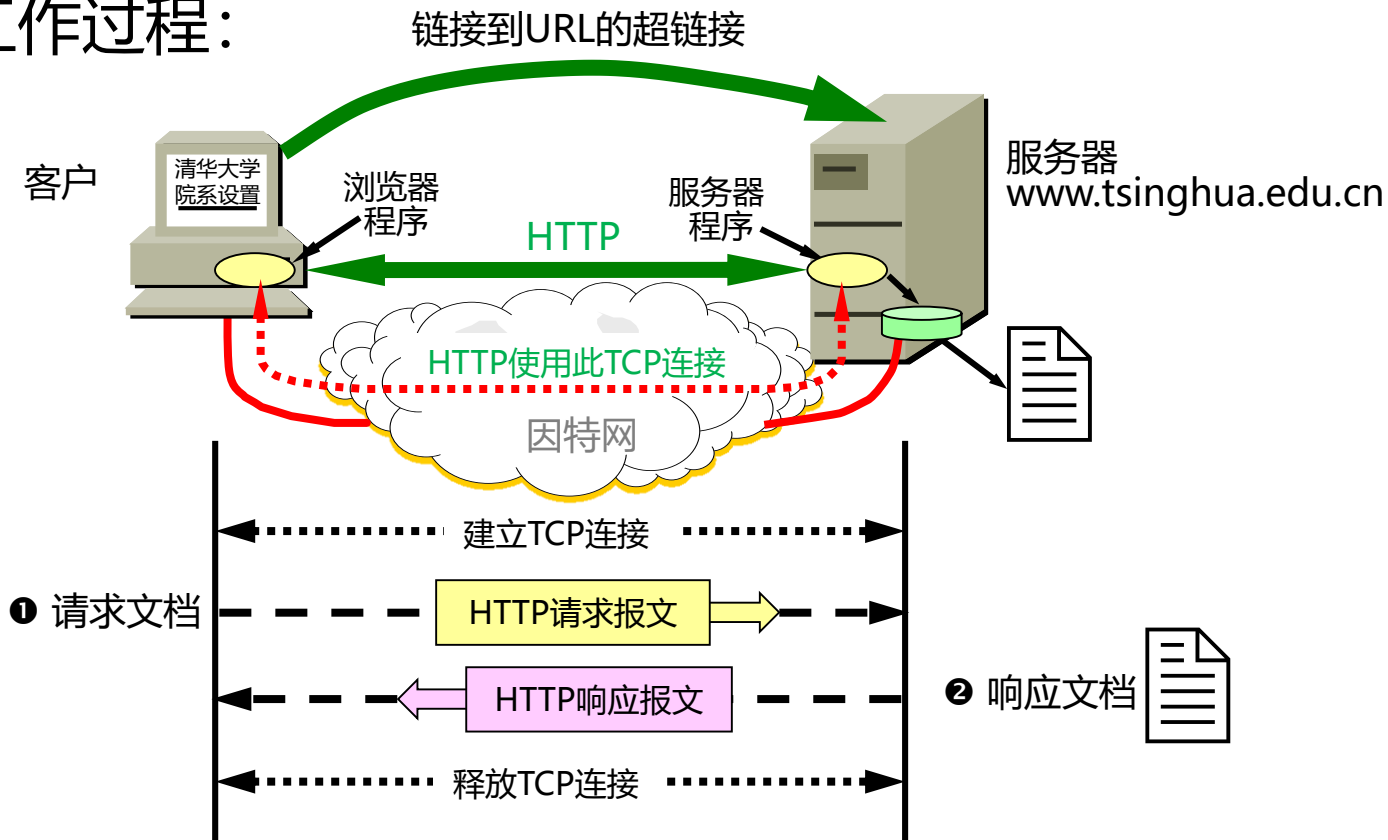
□ HTTP的操作过程:

- 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

4.3超文本传送协议HTTP

□ 万维网的工作过程:



4.万维网WWW

4.3超文本传送协议HTTP

- 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/yxsj/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

4.3超文本传送协议HTTP

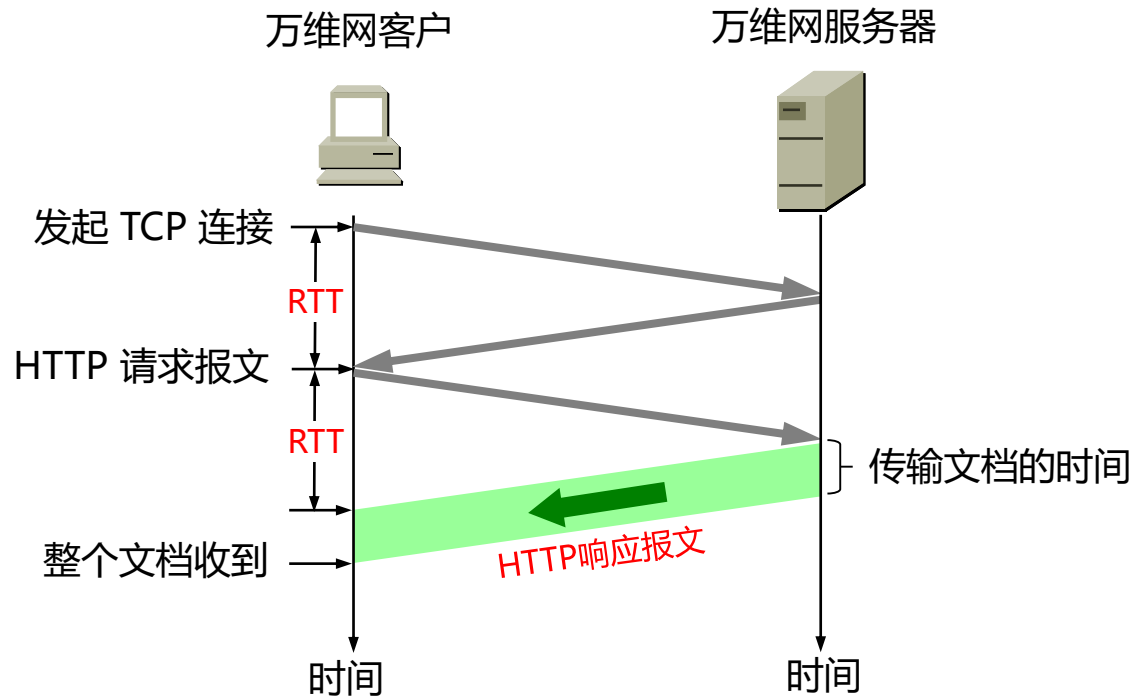
□ HTTP的主要特点:

- 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

4.3超文本传送协议HTTP

- 请求一个万维网文档所需的时间:



4.万维网WWW

4.3超文本传送协议HTTP

- 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

4.3超文本传送协议HTTP

- 持续连接(persistent connection):
 - 持续连接的两种工作方式为:
 - **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

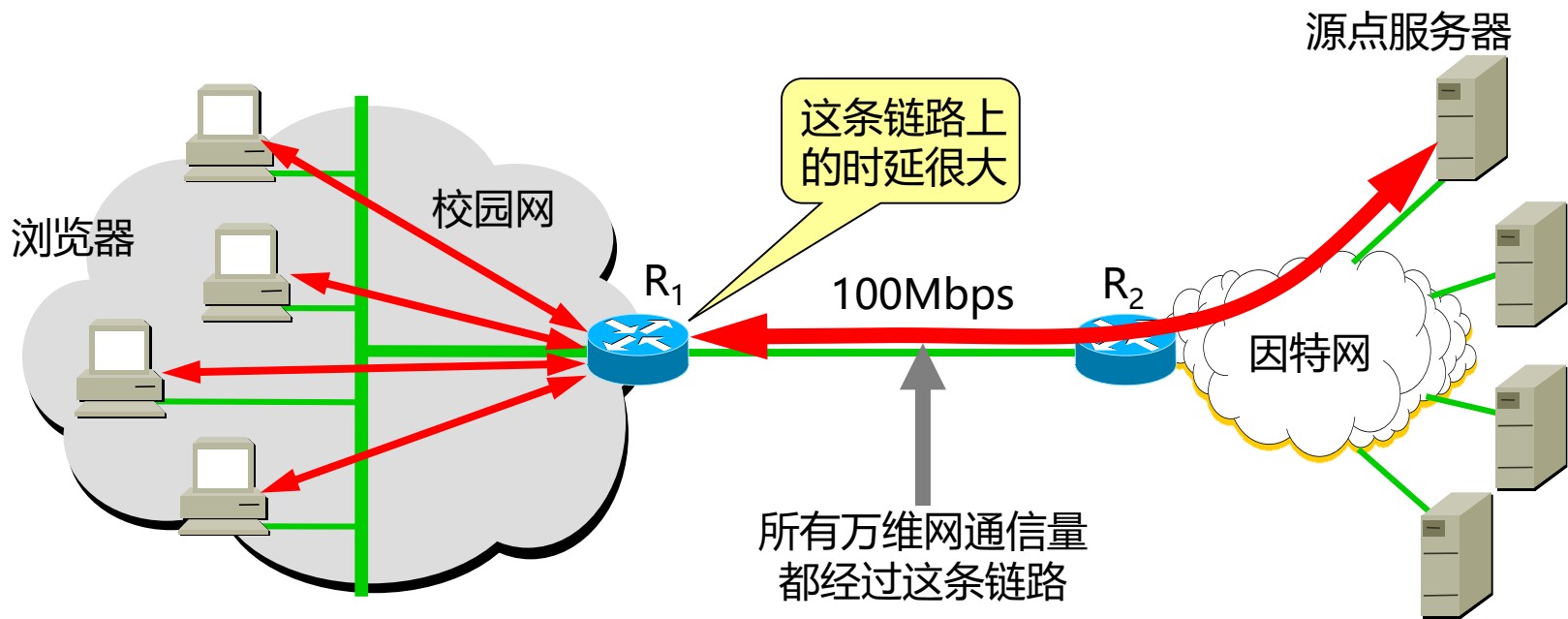
4.4代理服务器

- 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

4.4代理服务器

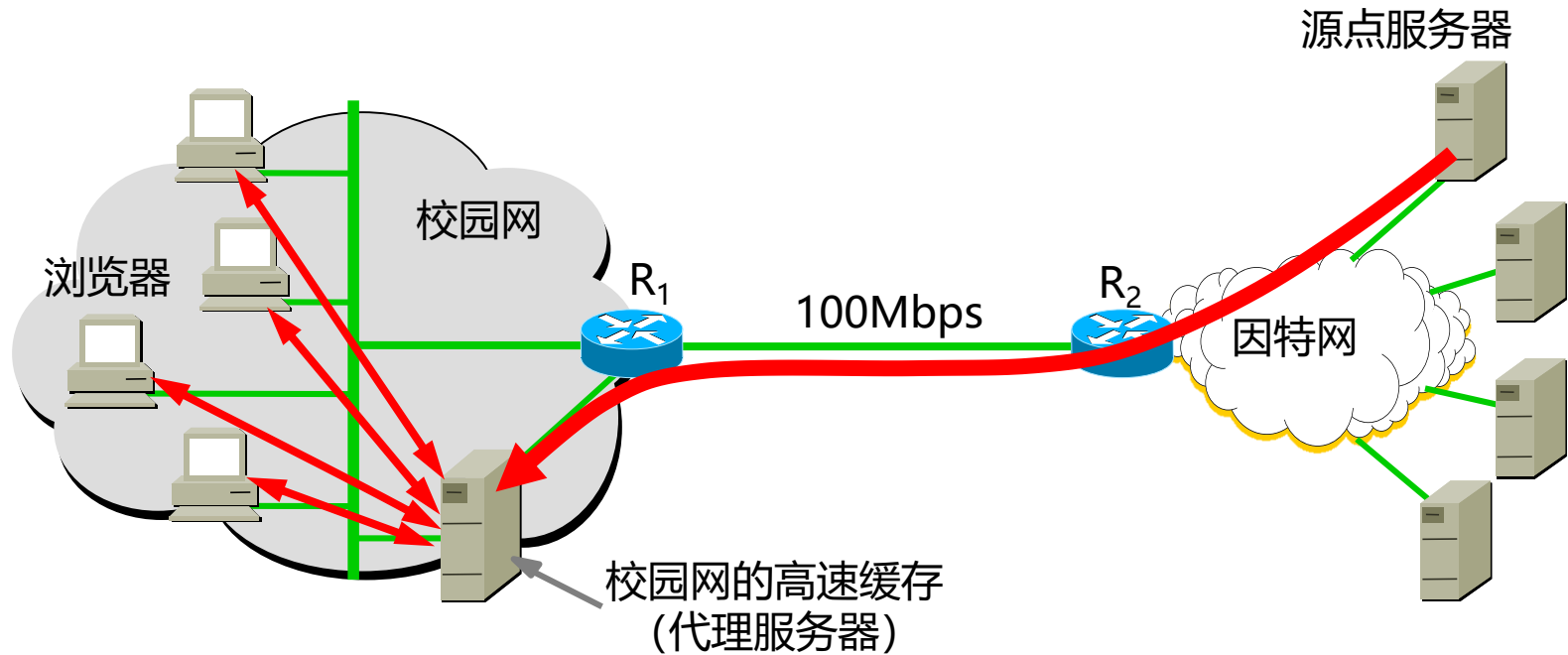
□ 代理服务器(proxy server) :



4.万维网WWW

4.4代理服务器

- 代理服务器(proxy server) :



4.万维网WWW

4.4代理服务器

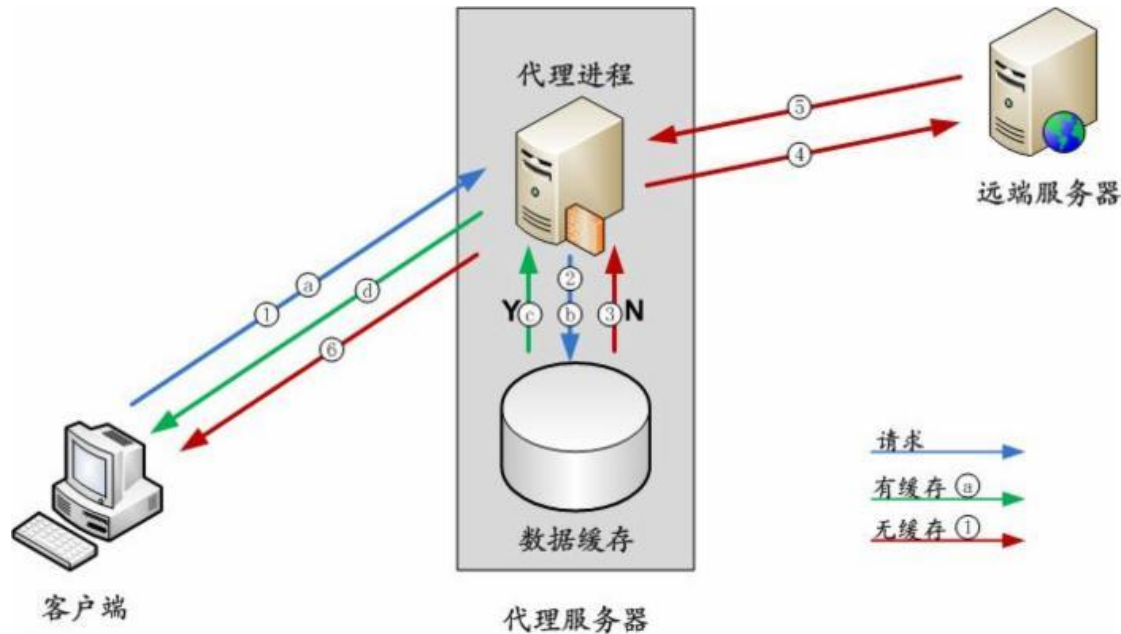
□ 代理服务器(proxy server) :

- 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

4.4代理服务器

□ 代理服务器(proxy server) :



4.万维网WWW

4.4代理服务器

□ 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

4.5HTTP的报文结构

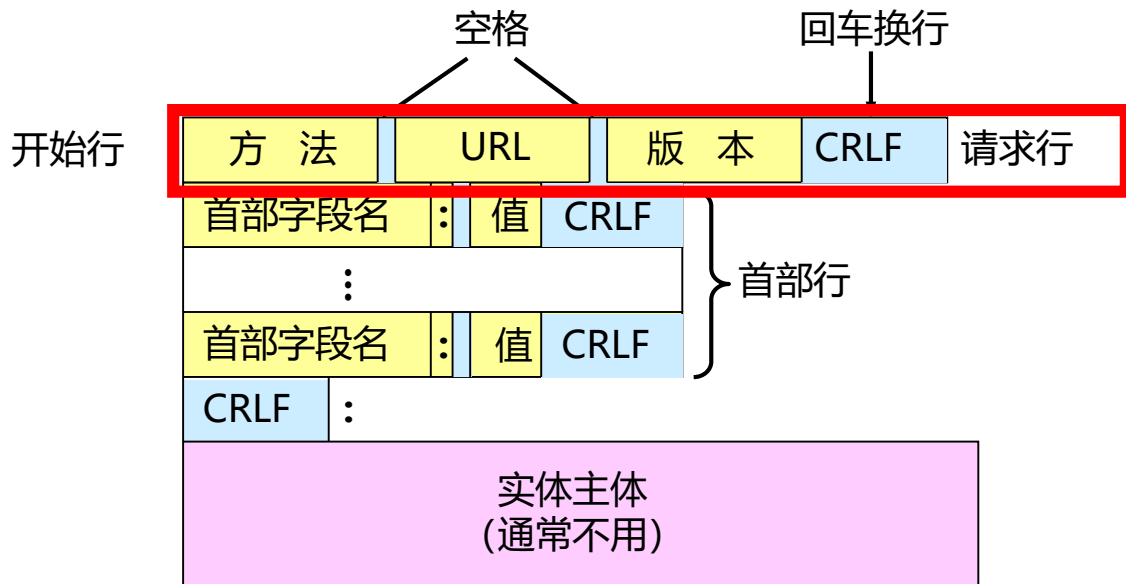
- HTTP有两类报文：请求报文、响应报文。
 - 请求报文：从客户向服务器发送请求报文。
 - 响应报文：从服务器到客户的回答。
 - 由于HTTP是面向正文的(text-oriented)，因此在报文中的每一个字段都是一些ASCII码串，因而每个字段的长度都是不确定的。

4.万维网WWW

4.5HTTP的报文结构

□ 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

4.5HTTP的报文结构

□ 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。

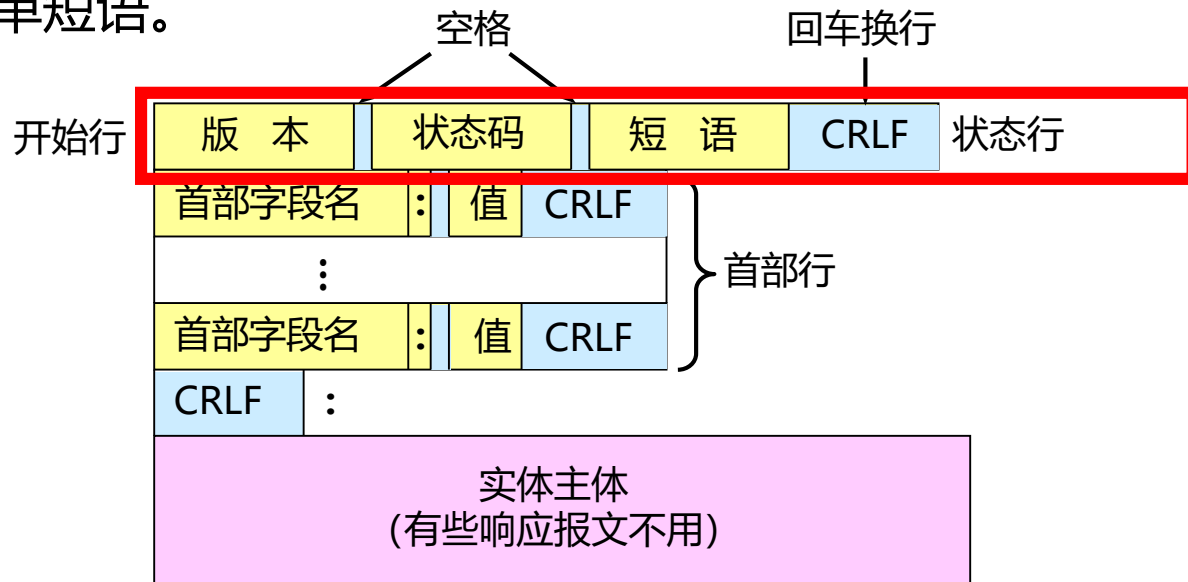
□ <https://www.w3.org/Protocols/rfc2616/rfc2616-sec9.html>

4.万维网WWW

4.5HTTP的报文结构

□ 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

4.5HTTP的报文结构

□ 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>

4.5 HTTP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>

| 状态 | 方法 | 文件 | 消息头 | Cookie | 参数 | 响应 | 耗时 | 预览 |
|-------|-----|------------------------------|--|--------|----|----|----|----|
| ▲ 304 | GET | / | 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 | | | | | |
| ▲ 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

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

| 状态 | 方法 | 文件 |
|-------|-----|------------------------------|
| ▲ 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 |

请求地址: 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

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
```

编辑和重发 原始头

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"

| 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..Host: www.h
```

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

| 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_20180612233931_a05576

CH M 简 23:41 2016/6/12

分组: 2364 · 已显示: 83 (3.5%) 配置文件: Default

4.万维网WWW

4.5HTTP的报文结构

Telerik Fiddler

OVERVIEW SOLUTIONS DOCS & SUPPORT PRICING SIGN IN

Q

DOWNLOAD NOW

Fiddler Everywhere: The Web Debugging Proxy Tool Loved by Users Just Got Better

Capture all HTTP(S) traffic between your computer and the Internet with Fiddler HTTP(S) proxy. Inspect traffic, set breakpoints, and fiddle with requests & responses.

Download Now

Looking for Fiddler Classic? [Download it here](#)

现场演示：Fiddler进行HTTP分析

4.万维网WWW

4.6在服务器上存放用户的信息

- 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。

| 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 | | | | | | |

过滤 Cookie

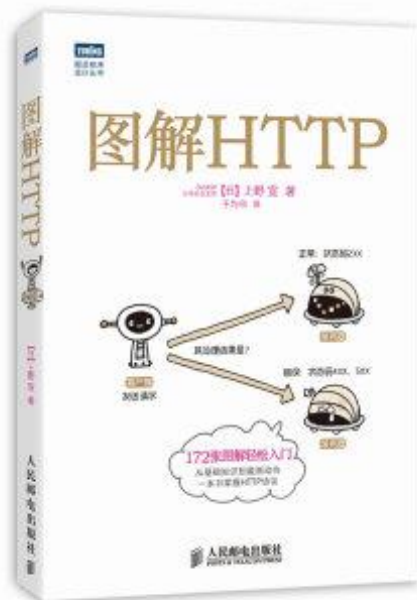
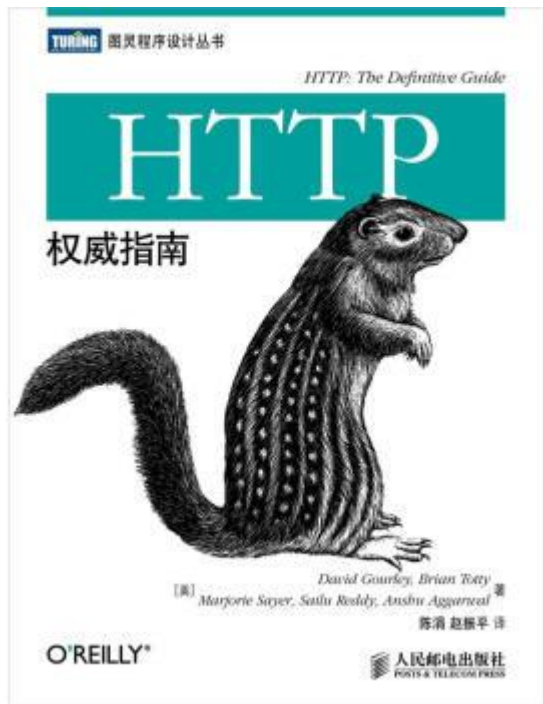
请求 Cookie

JSESSIONID: "8F5D70C0AC8AB2BA194710177BFF3320"

_pk_id.7.4808: "3e5f0751e100c710.1465745502.1.1465745502.1465745502."

_pk_ses.7.4808: ""

4.万维网WWW



5.电子邮件

5.1电子邮件概述

- 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

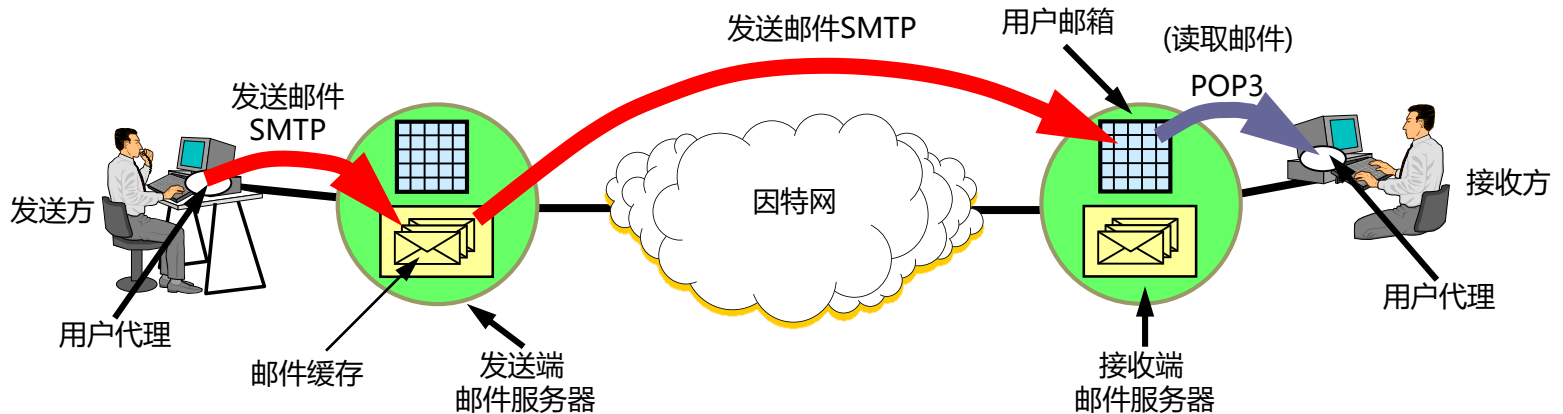
5.1电子邮件概述

□ 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

5.1电子邮件概述



5.电子邮件

5.1电子邮件概述

□ 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

5.1电子邮件概述

□ 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

5.1电子邮件概述

- 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

5.1电子邮件概述

□ 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

5.1电子邮件概述

□ 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

5.2简单邮件传送协议SMTP

- 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

5.2简单邮件传送协议SMTP

□ 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

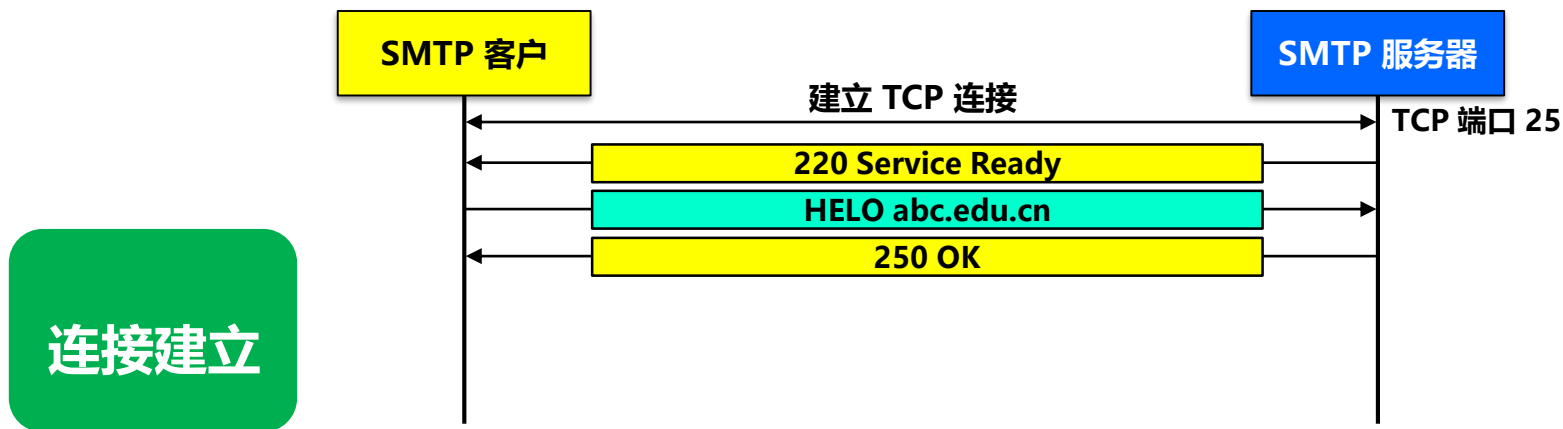
■ 连接释放

- 邮件发送完毕后，SMTP应释放TCP连接。

5.电子邮件

5.2简单邮件传送协议SMTP

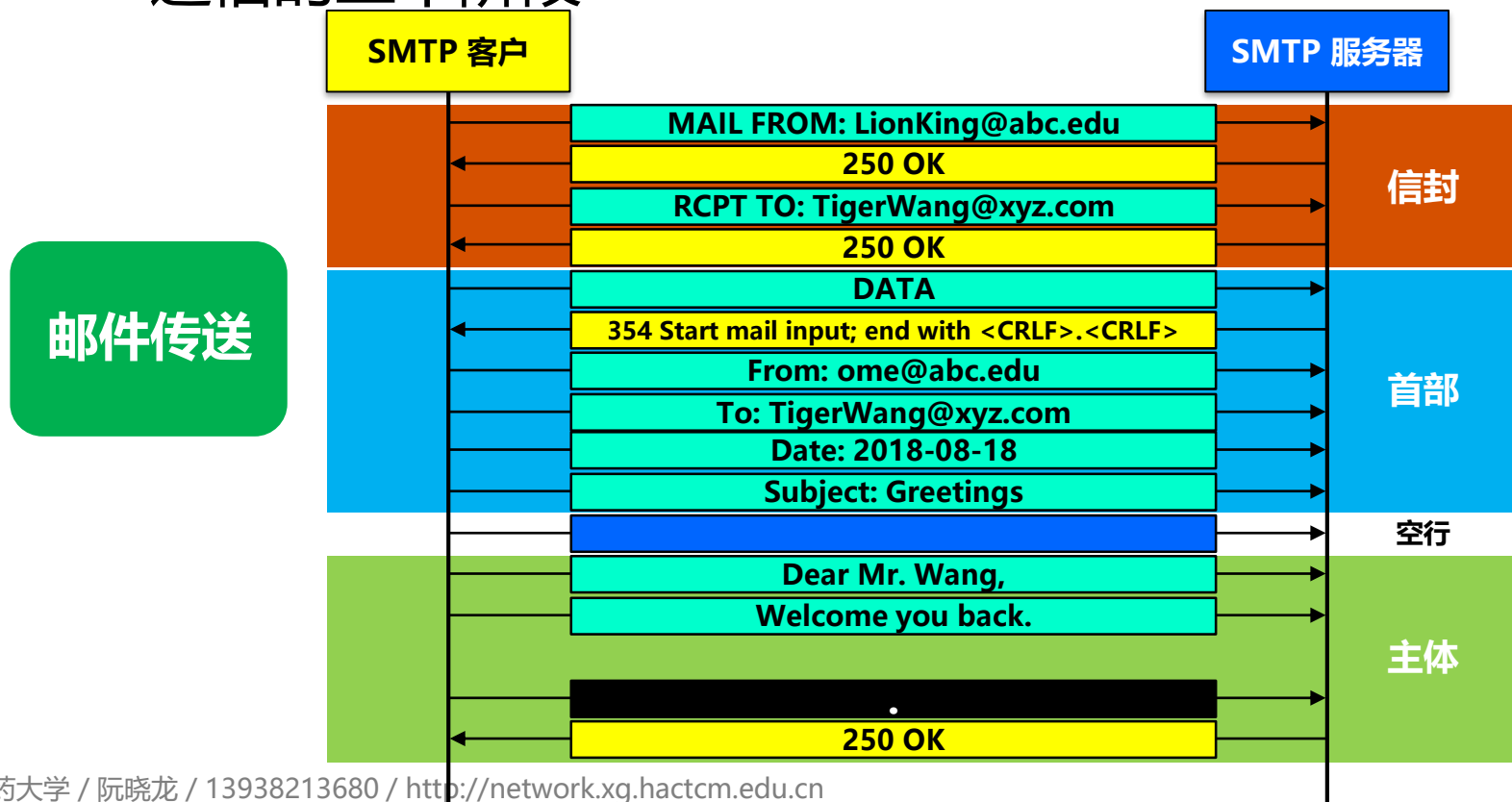
□ SMTP通信的三个阶段:



5.电子邮件

5.2简单邮件传送协议SMTP

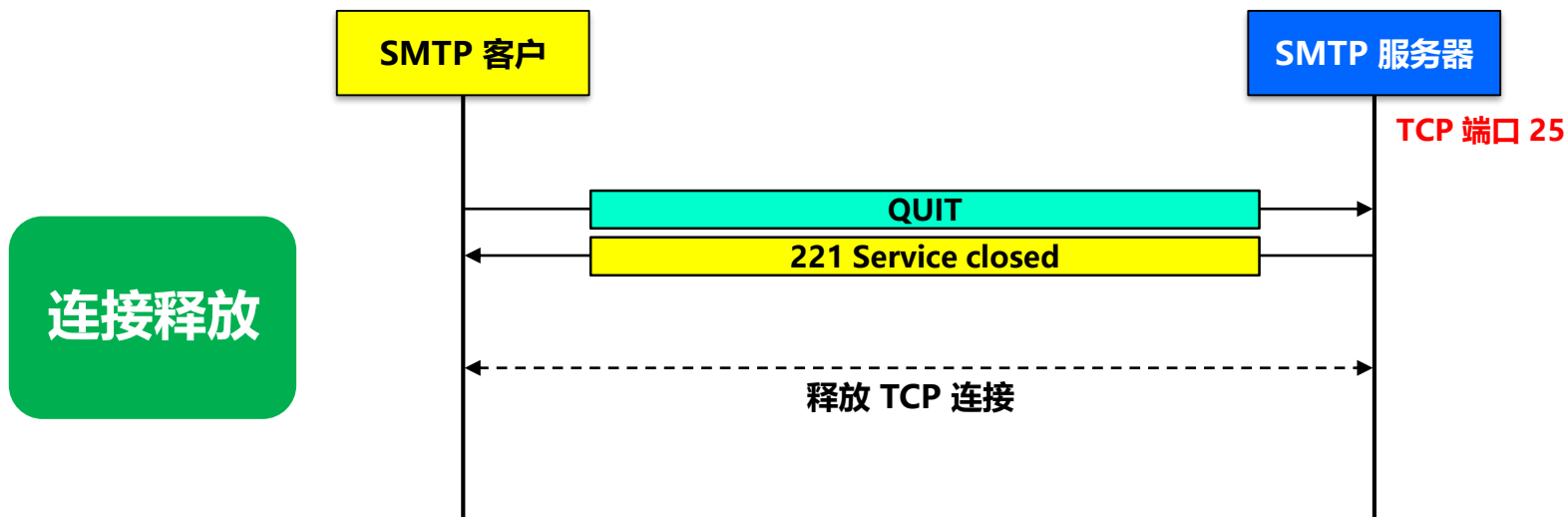
□ SMTP通信的三个阶段：



5.电子邮件

5.2简单邮件传送协议SMTP

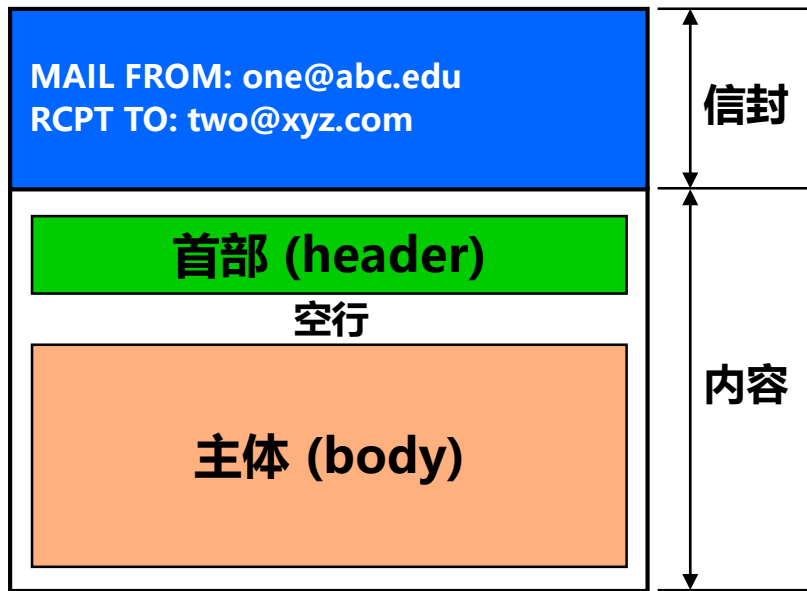
□ SMTP通信的三个阶段：



5.电子邮件

5.3电子邮件的信息格式

- 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
 - 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。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

5.3电子邮件的信息格式

□ 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

5.4邮件读取协议POP3和IMAP

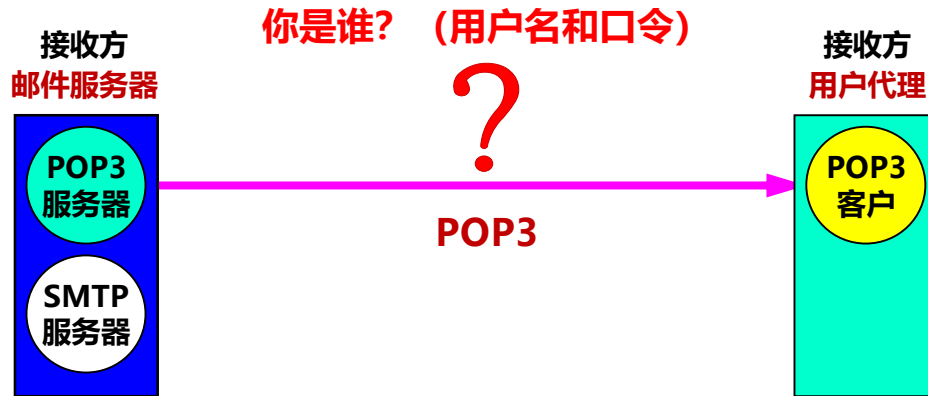
□ POP3:

- 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

5.4邮件读取协议POP3和IMAP

□ POP3:



- POP3 支持用户鉴别。
- POP3 服务器删除被用户读取了的邮件。

5.电子邮件

5.4邮件读取协议POP3和IMAP

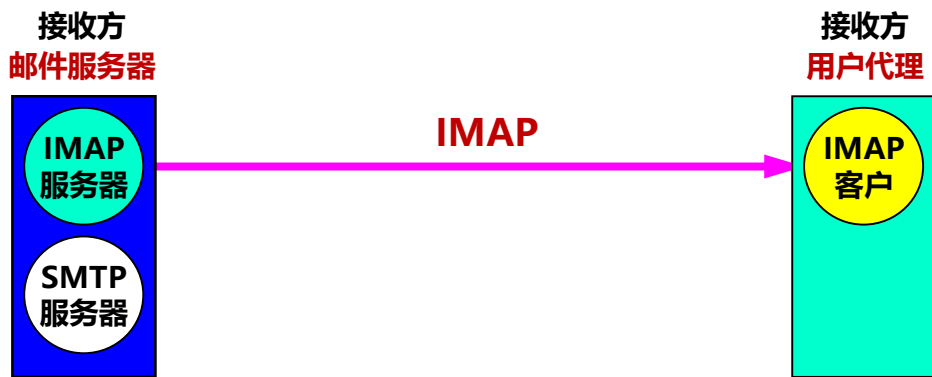
□ IMAP:

- 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

5.4邮件读取协议POP3和IMAP

□ IMAP:



- IMAP 使用客户-服务器方式。
- IMAP 基于TCP实现客户与服务器的通信。
- IMAP是一个联机协议。

5.电子邮件

5.4邮件读取协议POP3和IMAP

□ IMAP:

■ IMAP的优势是:

- 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,邮件一直是存放在IMAP服务器上,要想查阅邮件,必须先联网。
- 用户需要经常与IMAP服务器建立连接。

5.电子邮件

5.4邮件读取协议POP3和IMAP

IMAP 与 POP3 比较

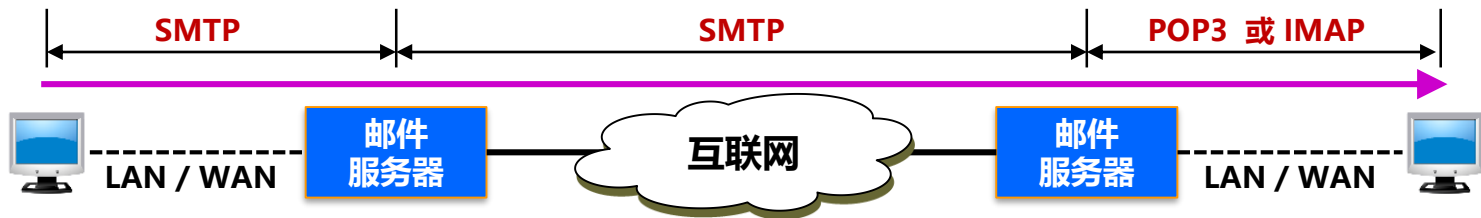
| 操作位置 | 操作内容 | IMAP | POP3 |
|-------|----------------|------------|--------|
| 收件箱 | 阅读、标记、移动、删除邮件等 | 客户端与邮箱更新同步 | 仅在客户端内 |
| 发件箱 | 保存到已发送 | 客户端与邮箱更新同步 | 仅在客户端内 |
| 创建文件夹 | 新建自定义的文件夹 | 客户端与邮箱更新同步 | 仅在客户端内 |
| 草稿 | 保存草稿 | 客户端与邮箱更新同步 | 仅在客户端内 |
| 垃圾文件夹 | 接收并移入垃圾文件夹的邮件 | 支持 | 不支持 |
| 广告邮件 | 接收并移入广告邮件夹的邮 | 支持 | 不支持 |

5.电子邮件

5.4邮件读取协议POP3和IMAP

□ POP、IMAP和SMTP:

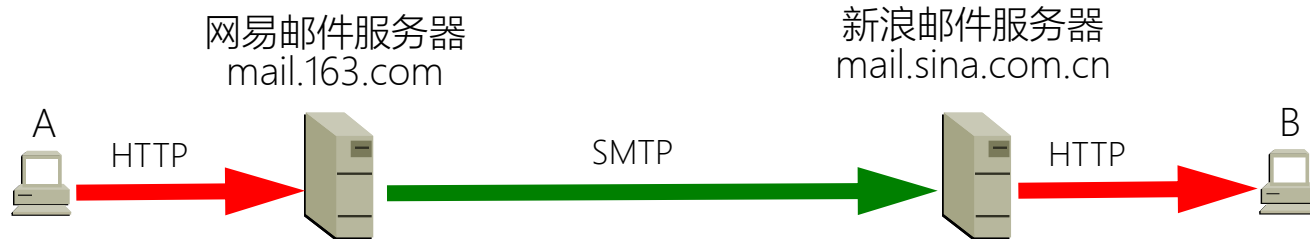
- 不要将邮件读取协议POP或IMAP与邮件传送协议SMTP弄混。
- 发信人的用户代理向源邮件服务器发送邮件，以及源邮件服务器向目的邮件服务器发送邮件，都是使用SMTP协议。
- POP协议或IMAP协议则是用户从目的邮件服务器上读取邮件所使用的协议。



5.电子邮件

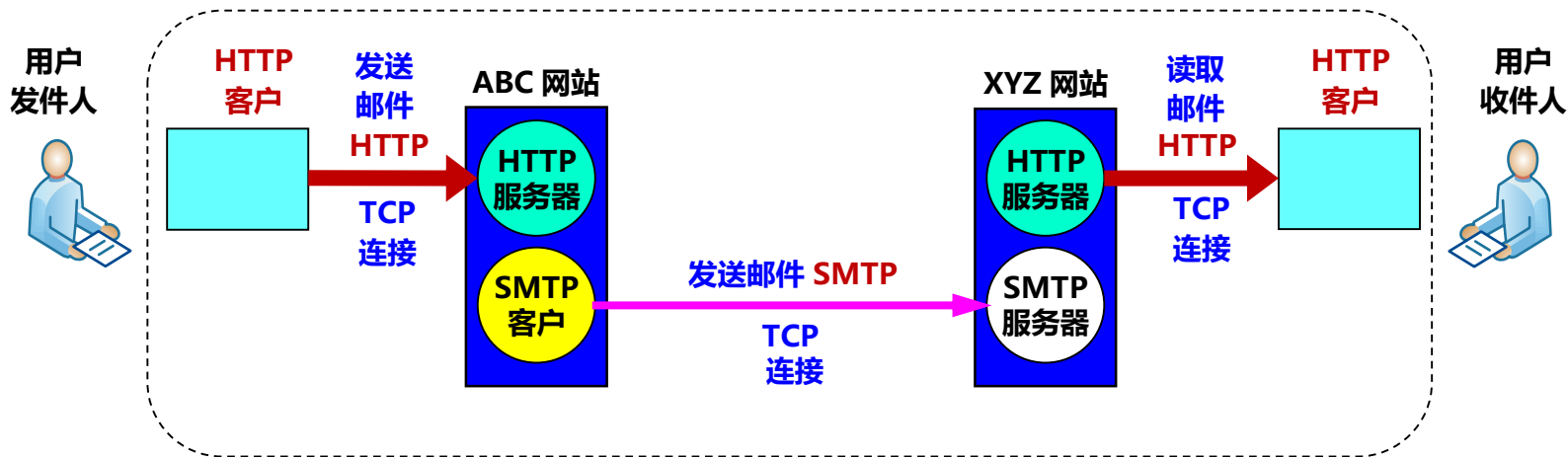
5.5基于万维网的电子邮件

- 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

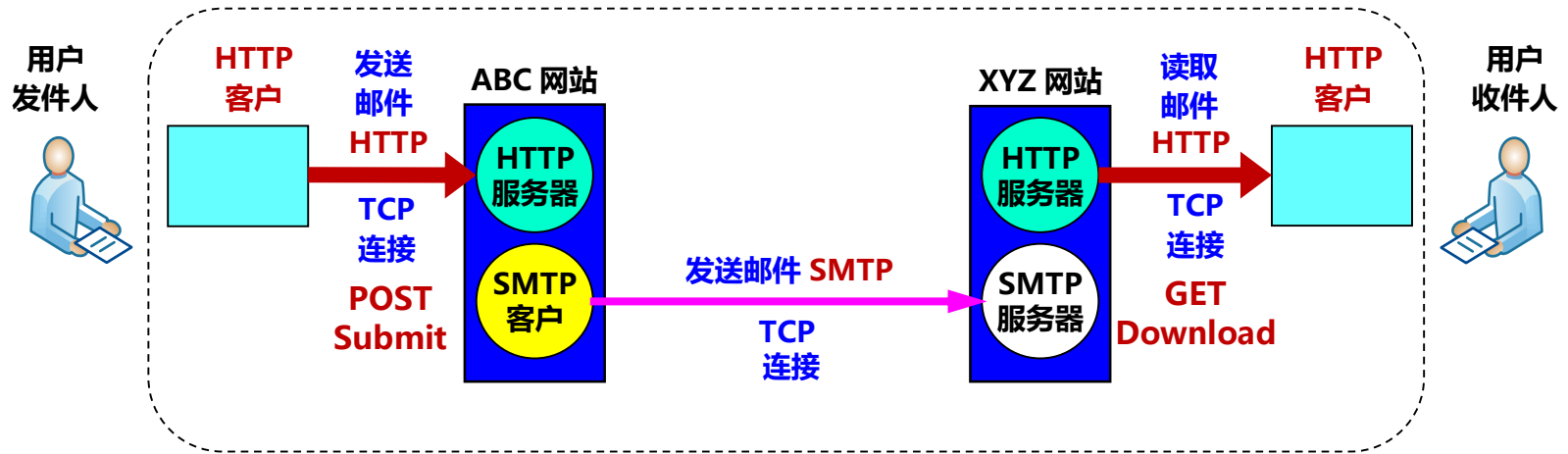
5.5基于万维网的电子邮件



- 发送、接收电子邮件时使用 HTTP 协议。
- 两个邮件服务器之间传送邮件时使用 SMTP。

5.电子邮件

5.5基于万维网的电子邮件



- 发送、接收电子邮件时使用 HTTP 协议。
- 两个邮件服务器之间传送邮件时使用 SMTP。

5.电子邮件

5.6通用因特网邮件扩充MIME

□ 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

5.6通用因特网邮件扩充MIME

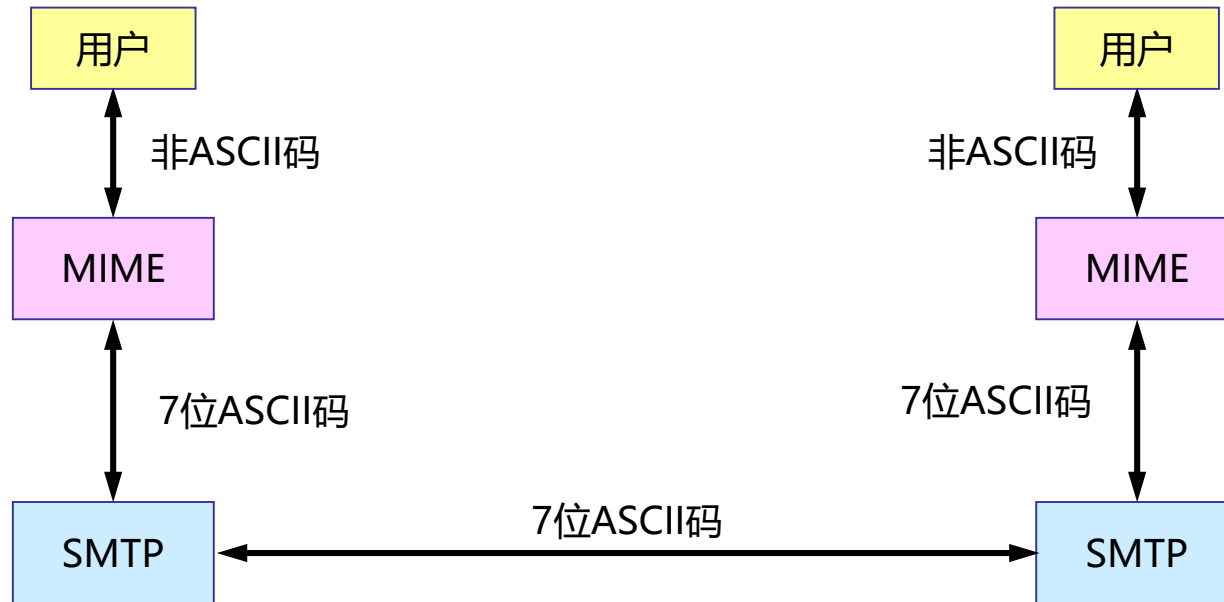
□ 什么是MIME:

- 通用互联网邮件扩充 MIME 并没有改动 SMTP 或取代它。
- MIME 的意图是继续使用目前的 [RFC 822] 格式, 但增加了邮件主体的结构, 并定义了传送非 ASCII 码的编码规则。

5.电子邮件

5.6通用因特网邮件扩充MIME

□ MIME和SMTP的关系:



5.电子邮件

5.6通用因特网邮件扩充MIME

- 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

5.6通用因特网邮件扩充MIME

- 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

5.6通用因特网邮件扩充MIME

- 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

5.6通用因特网邮件扩充MIME

内容传送编码(Content-Transfer-Encoding)

| 编码方法 | 说明 |
|------------------|---|
| 7bit | 7 位 ASCII 编码，每行不能超过 1000 个字符（包括回车和换行）。缺省编码方法。 |
| 8bit | 8 位非 ASCII 编码，每行不能超过 1000 个字节（包括回车和换行）。 |
| Binary | 8 位非 ASCII 编码，任意长度的字节串。 |
| Base64 | 将任意长度的字节串转换为用 7 位 ASCII 编码表示的字符串。可用于二进制和非文本数据的编码。 |
| Quoted-printable | 将任意长度的字节串转换为 ASCII 编码表示的字符串。可用于二进制和非文本数据的编码。 |

5.电子邮件

5.6通用因特网邮件扩充MIME

□ 内容类型：

- MIME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。
- MIME允许发件人和收件人自己定义专用的内容类型。
 - 但为避免可能出现名字冲突，标准要求为专用的内容类型选择的名字要以字符串 X-开始。

5.电子邮件

5.6通用因特网邮件扩充MIME

MIME Content-Type 说明中的类型及子类型

| 内容类型 | 子类型举例 | 说明 |
|------------------|--------------------------------------|-------------|
| text (文本) | plain, html, xml, css | 不同格式的文本 |
| image (图像) | gif, jpeg, tiff | 不同格式的静止图像 |
| audio (音频) | basic, mpeg, mp4 | 可听见的声音 |
| video (视频) | mpeg, mp4, quicktime | 不同格式的视频 |
| model (模型) | vrml | 3D模型 |
| application (应用) | octet-stream, pdf, javascript, zip | 不同应用程序产生的数据 |
| message (报文) | http, rfc822 | 封装的报文 |
| multipart (多部分) | mixed, alternative, parallel, digest | 多种类型的组合 |

5.电子邮件

5.6通用因特网邮件扩充MIME

<< 返回 删除会话 举报 移动到 ▾ 整理 ▾

☆ 您在京东有1张优惠券到账，请注意查收 标记智能标签 ▾

 京东JD.com 回复 转发 ...
 收件人： ruanxiaolong 2016年06月13日 13:45 收起

发件人： 京东JD.com <customer_service@jd.com>
 收件人： ruanxiaolong <ruanxiaolong@163.com>




 6.18 购物狂欢节 6.01-6.20 我的京东 VIP 京东会员 ✉ 退订投诉

尊敬的 八百里伏牛山 您好：

昨日您的京东账号中有 **1** 张优惠券到账，请注意查收！用京东优惠券购物，享受既划算又放心的购物乐趣！
 您可以点击 [我的京东 -- 优惠券](#) 查看详情。
 优惠券使用说明请参考：<https://help.jd.com/user/issue/169-266.html>
 为了保证您正常使用优惠券，请尽快到 [账户设置 - 账户安全](#) > 完善您绑定的手机和您的支付密码！

 **优惠券**

| 类别 | 面值 | 所需消费金额 | 有效期至 | 使用限制 |
|----|-------------|--------|------------|------|
| 东券 | 20.0 | ¥200.0 | 2016-06-14 | 全品类 |

5. 电子

Received: from mail406.jd.com (unknown [36.110.177.37])
by edm4 (Coremail) with SMTP id icCowECZPkk7SF5XW394Ag--.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=Nnz87X1MKPqfkDfp3JFfXvRjznkAj3RegEHmCPHo1Y4=;
b=F8JNcwm/pJr4g6dNUHbfihQBmVeMNPi5I/1mBOxVTIRyaitnL05ZTwxLME12RpEB
qJKht++FLG0hBkVPKsCCUo9eL70afivkMoyeODQiNm9vP4yM9ASNuoXBtK8z7Du2Tjc
1xx3JXZh12ZwnhkfAdQkfcHvgfhvHfCNiRCrY03U=

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?5oKo5Zyo5Lqs5Lic5pyJMeW8o0S8m0aDoA==?=
=?UTF-8?B?5Yi45Yiw6LSm77yM6K+35r0o5oSP5p+15pS2?=>

MIME-Version: 1.0

Content-Type: text/html; charset=utf-8

Content-Transfer-Encoding: quoted-printable

X-CM-TRANSID: icCowECZPkk7SF5XW394Ag--.39586S2

Authentication-Results: edm4; spf=pass smtp.mail=customer_service@jd.c
om; dkim=pass header.i=@jd.com

X-Coremail-Antispam: 1Uf129KBjvJXoW7KF1kJF48XFwftFykCFyUWrg_yoW8Jwlkpr
Z5Ww48Wr4jya1S9r4UWw1Igr4UJanaga1Yq34xtFwFxrWUJF92yrW7KF93ua4fXwnrZan7
X3WFq3sYgwn0k3DanT9S1TB71UUUU4JqntZGkaVYY2UrUUUUjbIjqfuFe4nvWSU5nxnvy2
9KBjdUYxBIdaVfxhVjvjdTur1kJVWrZrnYChsFpT7I43ZEXa7xR_LvtUUUUU==

<!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=

6.动态主机配置协议DHCP

- 在协议软件中，给协议参数赋值的动作叫做**协议配置**。
- 一个协议软件在使用之前必须是已正确配置的。
- 具体的配置信息有哪些，取决于协议栈。
- 连接到互联网的计算机的协议软件需要配置的参数包括：
 - IP 地址
 - 子网掩码
 - 默认路由器的 IP 地址
 - 域名服务器的 IP 地址

6.动态主机配置协议DHCP

6.1 DHCP

- 互联网广泛使用的动态主机配置协议 DHCP (Dynamic Host Configuration Protocol) 提供了即插即用连网 (plug-and-play networking) 的机制。
 - 这种机制允许一台计算机加入新的网络和获取 IP 地址, 而不用手工配置。
 - DHCP给运行服务器软件、且位置固定的计算机指派一个永久地址, 给运行客户端软件的计算机分配一个临时地址。

6.动态主机配置协议DHCP

6.2 DHCP的工作方式

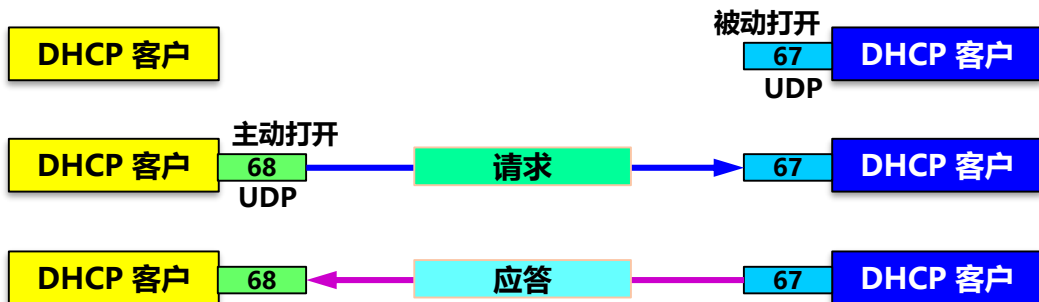
□ DHCP 使用客户 - 服务器方式

- 需要 IP 地址的主机在启动时
 - 向 DHCP 服务器广播发送发现报文 (DHCPDISCOVER) , 这时该主机就成为 DHCP 客户。
 - 本地网络上所有主机都能收到此广播报文, 但只有 DHCP 服务器才回答此广播报文。
- DHCP 服务器先在其数据库中查找该计算机的配置信息
 - 若找到, 则返回找到的信息。
 - 若找不到, 则从服务器的 IP 地址池 (address pool) 中取一个地址分配给该计算机。
 - DHCP服务器的回答报文叫做提供报文 (DHCPOFFER) 。

6.动态主机配置协议DHCP

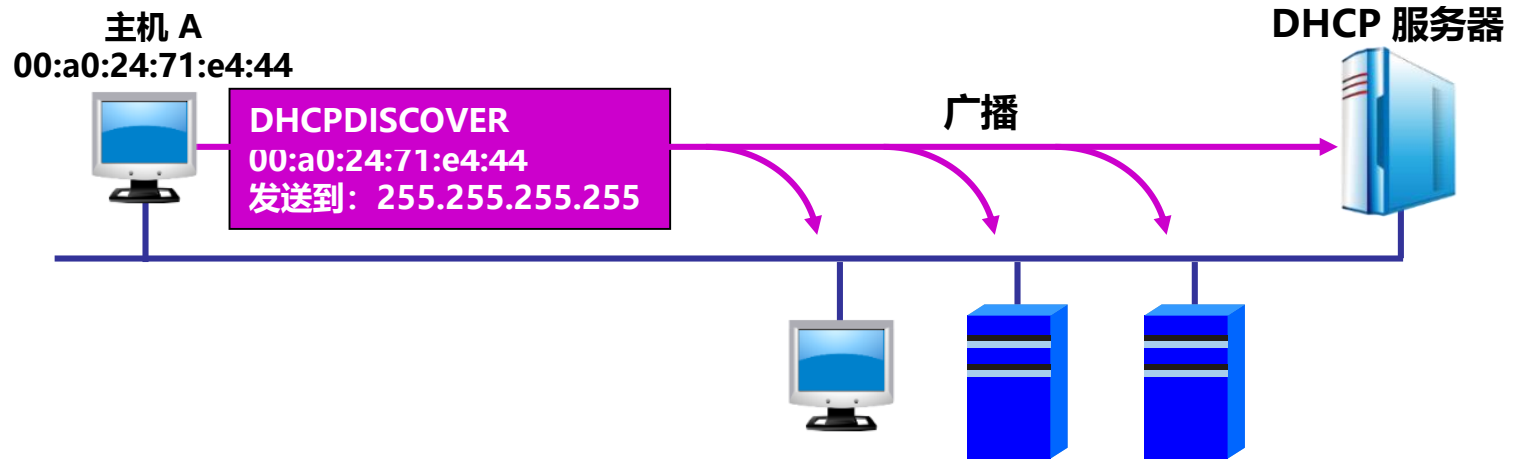
6.2 DHCP的工作方式

- DHCP 使用客户 - 服务器方式
 - DHCP 基于 UDP 工作
 - DHCP 服务器运行在 67 号端口
 - DHCP客户运行在 68 号端口



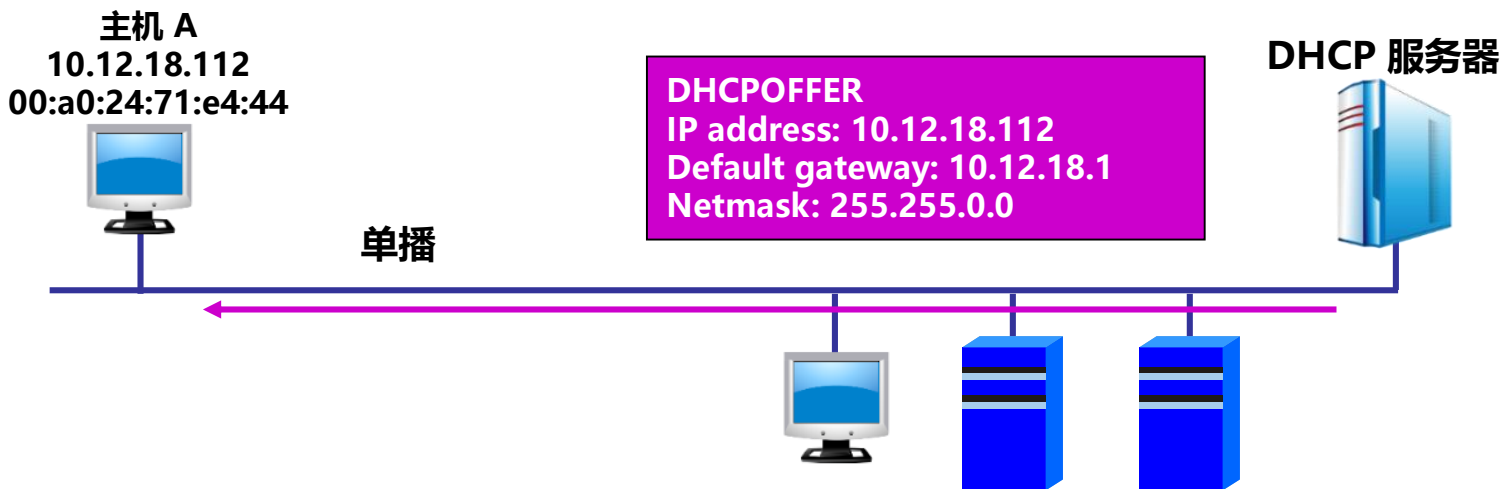
6.动态主机配置协议DHCP

6.2 DHCP的工作方式



6.动态主机配置协议DHCP

6.2 DHCP的工作方式



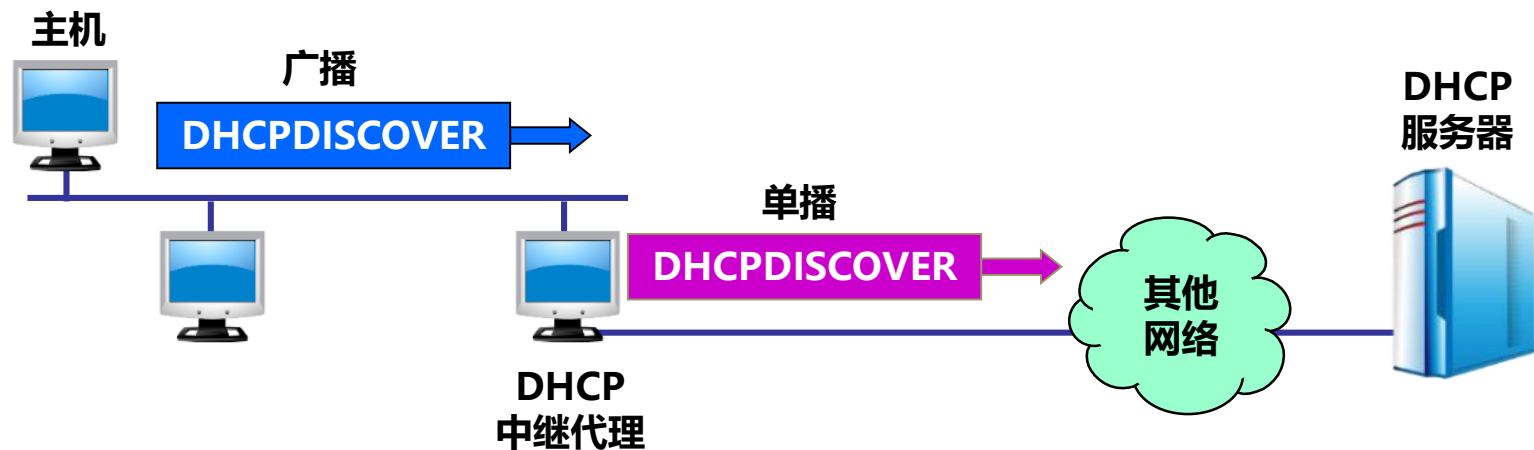
6.动态主机配置协议DHCP

6.3 DHCP中继代理(relay agent)

- 并不是每个网络上都有DHCP服务器，这样会使DHCP服务器的数量太多。
- 现在是每一个网络至少有一个 DHCP 中继代理，它配置了 DHCP 服务器的 IP 地址信息。
- 当 DHCP 中继代理收到主机发送的发现报文后，就以单播方式向 DHCP 服务器转发此报文，并等待其回答。
- 收到 DHCP 服务器回答的提供报文后，DHCP 中继代理再将此提供报文发回给主机。

6.动态主机配置协议DHCP

6.3 DHCP中继代理(relay agent)



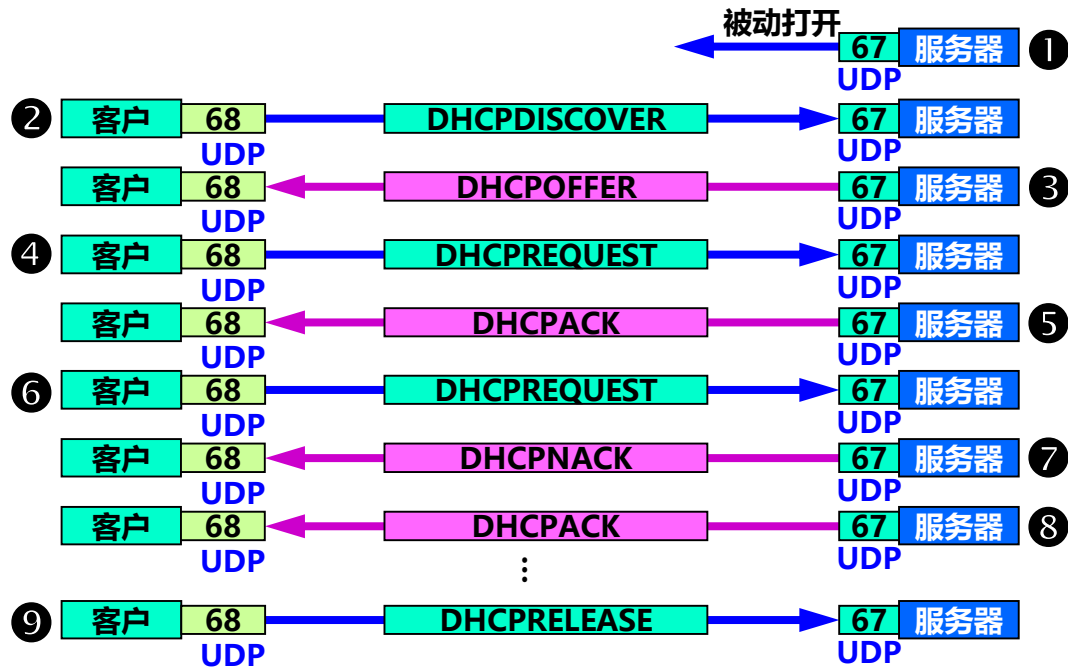
6.动态主机配置协议DHCP

6.4 租用期(Lease Period)

- DHCP 服务器分配给 DHCP 客户的 IP 地址的临时的，因此 DHCP 客户只能在一段有限的时间内使用这个分配到的 IP 地址。
- DHCP 协议称这段时间为**租用期**。
 - 租用期的数值应由 DHCP 服务器自己决定。
 - DHCP 客户也可在自己发送的报文中（例如，发现报文）提出对租用期的要求。

6.动态主机配置协议DHCP

6.5 DHCP协议的工作过程



7.简单网络管理协议SNMP

7.1 网络管理

□ 网络管理简称为网管。

- 网络管理包括对硬件、软件和人力的使用、综合与协调，以便对网络资源进行监视、测试、配置、分析、评价和控制，这样就能以合理的价格满足网络的一些需求，如实时运行性能，服务质量等。
- 网络管理并不是指对网络进行行政上的管理，通常分为五大功能。
 - **故障管理**：故障检测、隔离和纠正。
 - **配置管理**：初始化网络、并配置网络。
 - **计费管理**：记录网络资源的使用。
 - **性能管理**：估价系统资源的运行状况及通信效率等。
 - **网络安全管理**：对授权机制、访问控制、加密和加密关键字的管理。

7.简单网络管理协议SNMP

7.1 网络管理

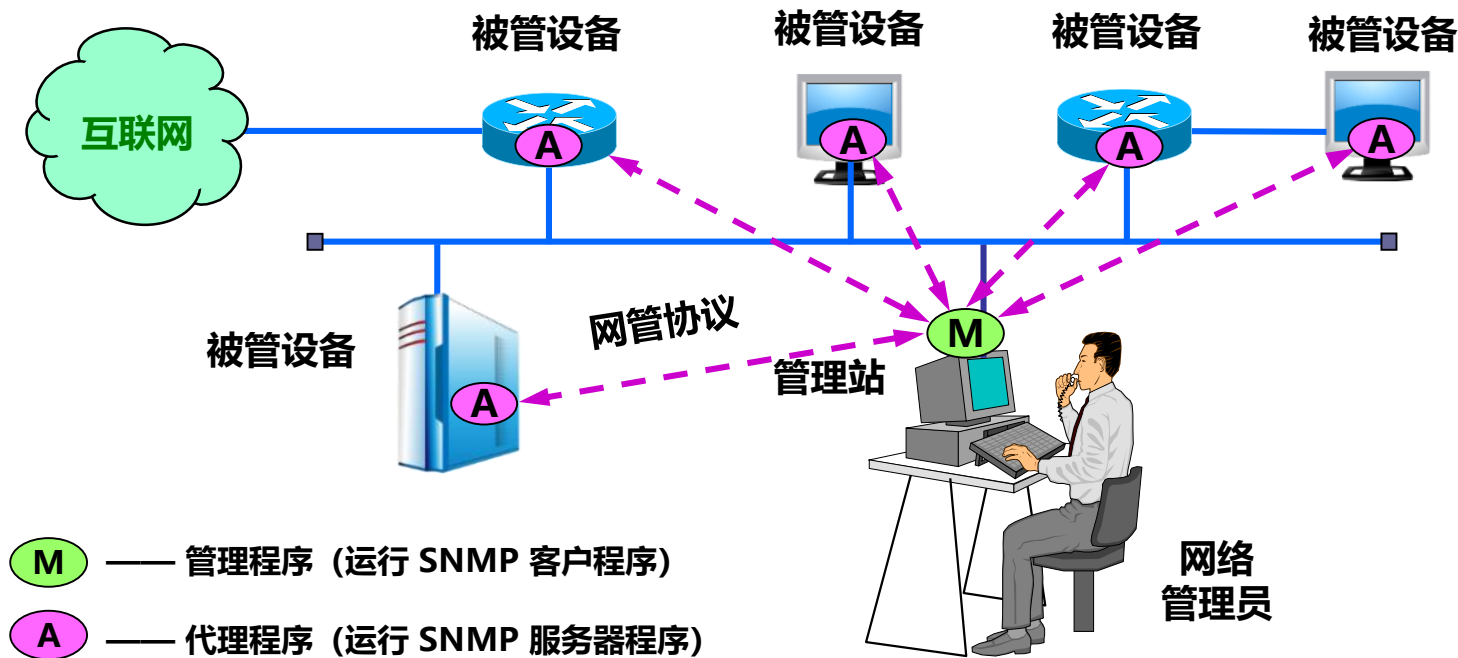
□ 网络管理的基本原理

- 若要管理某个对象，就必然会给该对象添加一些软件或硬件，但这种“添加”必须对原有对象的影响尽量小些。

7.简单网络管理协议SNMP

7.1 网络管理

网络管理的一般模型



7.简单网络管理协议SNMP

7.1 网络管理

□ 网络管理模型中的主要构件：

■ 管理站：

- 管理站也常称为**网络运行中心** NOC (Network Operations Center), 是网络管理系统的核心。
- 管理程序在运行时就成为**管理进程**。
- 管理站 (硬件) 或管理程序 (软件) 都可称为**管理者**(manager)。Manager 不是指人, 而是指机器或软件。
- **网络管理员** (administrator) 指的是负责网络管理的人员。
- 大型网络往往实行多级管理, 因而有多个管理者, 而一个管理者一般只管理本地网络的设备。

7.简单网络管理协议SNMP

7.1 网络管理

□ 网络管理模型中的主要构件：

■ 被管对象：

- 网络的每一个被管设备中可能有多个被管对象。
- 被管设备有时可称为网络元素或网元。
- 在被管设备中也会有一些不能被管的对象。

■ 代理 (agent)

- 在每一个被管设备中都要运行一个程序以便和管理站中的管理程序进行通信。这些运行着的程序叫做网络管理代理程序，或简称为代理。
- 代理程序在管理程序的命令和控制下在被管设备上采取本地的行动。

7.简单网络管理协议SNMP

7.1 网络管理

- 网络管理模型中的主要构件：
 - 网络管理协议：
 - 网络管理协议简称为网管协议。
 - 网络管理协议是管理程序和代理程序之间进行通信的规则。
 - 网络管理员利用网络管理协议，通过管理站对网络中的被管设备进行
管理。
 - 需要注意的是，网管协议本身不管理网络。

7.简单网络管理协议SNMP

7.2 SNMP

- 简单网络管理协议SNMP (Simple Network Management Protocol)
 - 管理程序和代理程序按客户-服务器方式工作。
 - 管理程序运行 SNMP 客户程序，向某个代理程序发出请求（或命令），代理程序运行 SNMP 服务器程序，返回响应（或执行某个动作）。
 - 在网管系统中，往往是一个（或少数几个）客户程序与很多的服务程序进行交互。

7.简单网络管理协议SNMP

7.2 SNMP

- SNMP 最重要的指导思想就是要尽可能简单。
- SNMP 的基本功能包括：
 - 监视网络性能
 - 检测分析网络差错
 - 配置网络设备

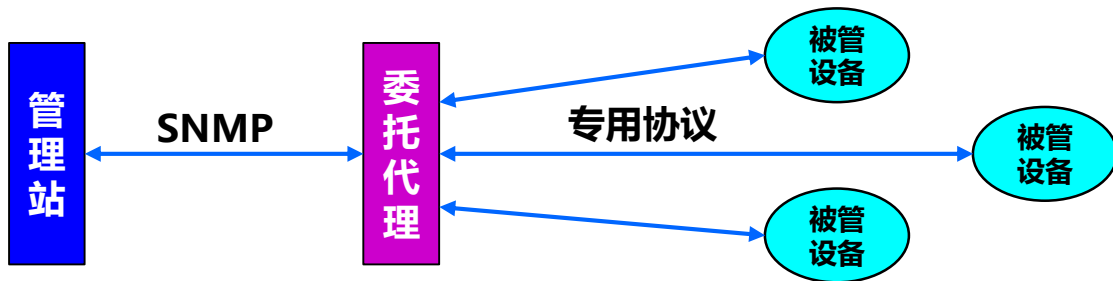
- 在网络正常工作时，SNMP 可实现统计、配置、和测试等功能。
- 当网络出故障时，可实现各种差错检测和恢复功能。
- 虽然 SNMP 是在 TCP/IP 基础上的网络管理协议，但也可扩展到其他类型的网络设备上。

7.简单网络管理协议SNMP

7.2 SNMP

□ SNMP 的管理站和委托代理

- 整个系统必须有一个管理站。
- 若网络元素使用的不是 SNMP 而是另一种网络管理协议，SNMP 协议就无法控制该网络元素，此时可使用委托代理 (proxy agent)。
- 委托代理能提供协议转换和过滤操作等功能，对被管对象进行管理。



7.简单网络管理协议SNMP

7.2 SNMP

- SNMP 的网络管理由三个部分组成：
 - SNMP 本身
 - 管理信息结构 SMI (Structure of Management Information)
 - 管理信息库 MIB (Management Information Base)。

- 简单网络管理协议 SNMP
 - SNMP 定义了管理站和代理之间所交换的分组格式。
 - 所交换的分组包含各代理中的对象（变量）名及其状态（值）。
 - SNMP 负责读取和改变这些数值。

7.简单网络管理协议SNMP

7.2 SNMP

□ 管理信息结构 SMI

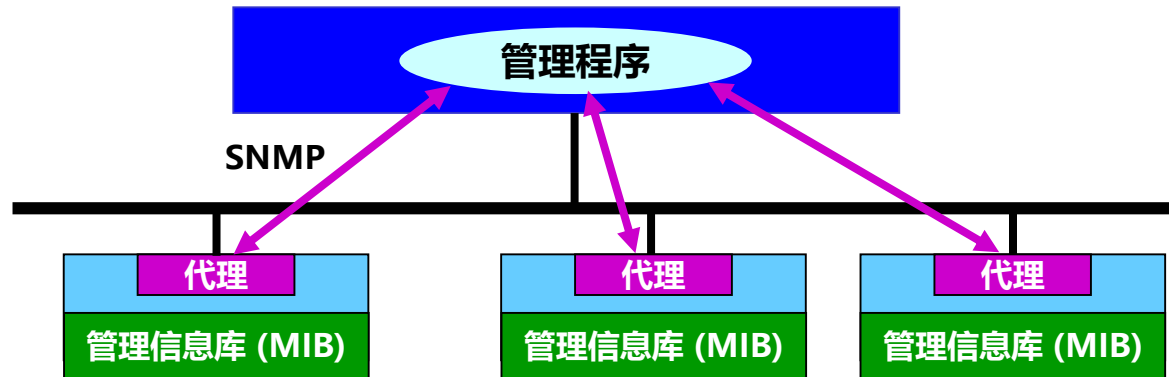
- SMI 定义了命名对象和定义对象类型（包括范围和长度）的通用规则，以及把对象和对象的值进行编码的规则。
- 这样做是为了确保网络管理数据的语法和语义的无二义性。但从 SMI 的名称并不能看出它的功能。
- SMI 并不定义一个实体应管理的对象数目，也不定义被管对象名以及对象名及其值之间的关联。

7.简单网络管理协议SNMP

7.2 SNMP

管理信息库 MIB

- MIB 在被管理的实体中创建了命名对象，并规定了其类型。
- 管理程序使用 MIB 中的信息，对网络进行管理。



7.简单网络管理协议SNMP

7.3 SMI

□ SMI 的功能:

- 被管对象应怎样命名
- 用来存储被管对象的数据类型有哪些种
- 在网络上传送的管理数据应如何编码

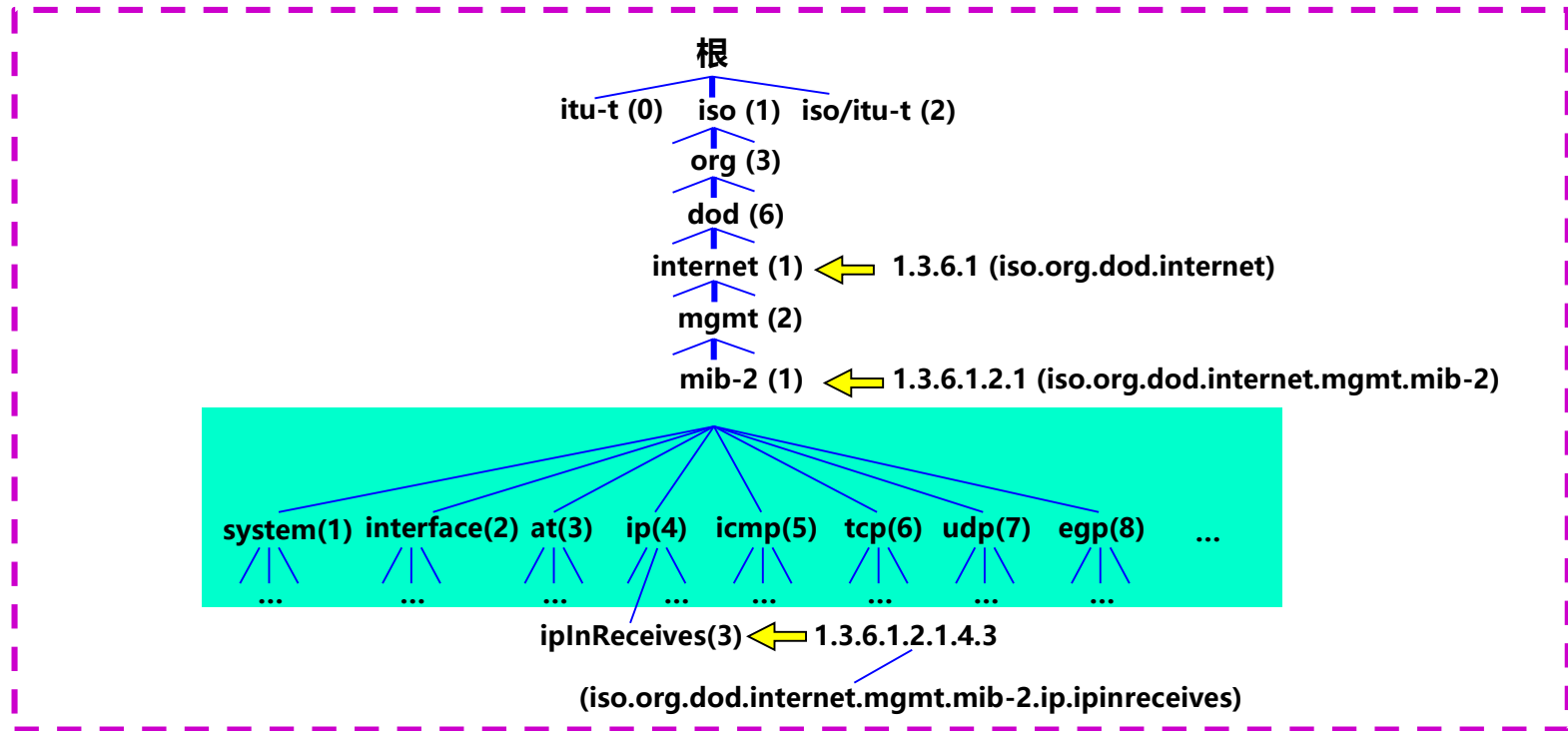
□ SMI 标准指明:

- 所有的 MIB 变量必须使用抽象语法记法 1 (ASN.1) 来定义。
- SMI 既是 ASN.1 的子集, 又是 ASN.1 的超集。
- ASN.1 记法很严格, 它使得数据的含义不存在任何可能的二义性。

7.简单网络管理协议SNMP

7.3 SMI

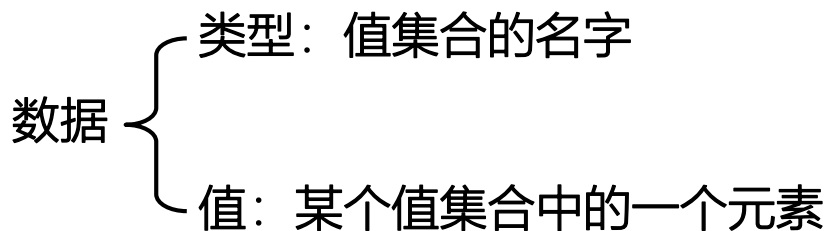
SMI 规定所有被管对象必须在命名树上



7.简单网络管理协议SNMP

7.3 SMI

- SMI 把数据类型分为两大类：
 - 简单类型
 - 结构化类型



7.简单网络管理协议SNMP

7.3 SMI

ASN.1 部分数据类型

| 分类 | 数据类型名称 | 含义 |
|-------|-------------------|----------------|
| 简单类型 | INTEGER | 任意长度整数 |
| | BIT STRING | 0 位或多位组成的二进制串 |
| | OCTET STRING | 0 位或多位组成的字节串 |
| | NULL | 空值 |
| | OBJECT IDENTIFIER | 定义的数据类型 |
| 结构化类型 | SEQUENCE | 由多个数据类型按序组成的值 |
| | SEQUENCE OF | 由同一数据类型按序组成的值 |
| | CHOICE | 可以从多个数据类型中选择一个 |
| | ANY | 任何数据类型 |

7.简单网络管理协议SNMP

7.3 SMI

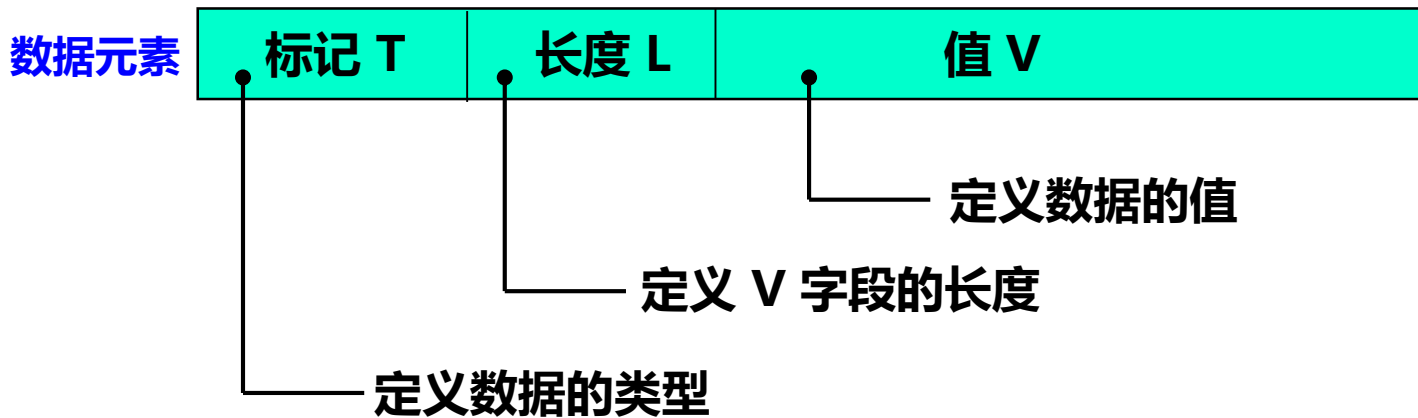
□ 基本编码规则 BER

- ISO 在制订 ASN.1 语言的同时也为它定义了一种标准的编码方案, 即基本编码规则 BER (Basic Encoding Rule)。
- BER 指明了每种数据类型中每个数据的值的表示。
- 发送端用 BER 编码, 可将用 ASN.1 所表述的报文转换成唯一的比特序列。
- 接收端用 BER 进行解码, 得到该比特序列所表示的 ASN.1 报文。

7.简单网络管理协议SNMP

7.3 SMI

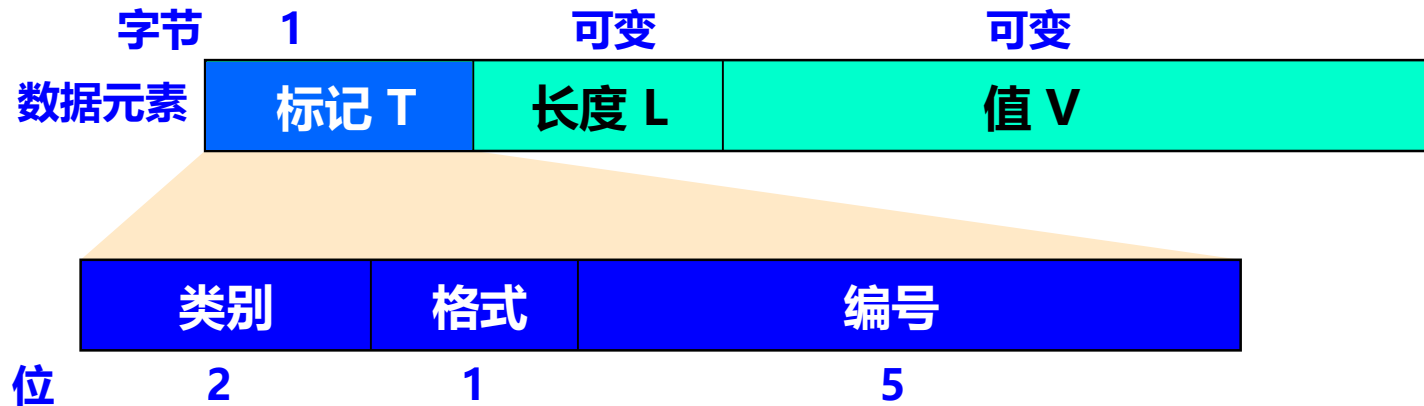
□ 用 TLV 方法进行编码



7.简单网络管理协议SNMP

7.3 SMI

□ TLV 中的 T 字段定义数据的类型



7.简单网络管理协议SNMP

7.3 SMI

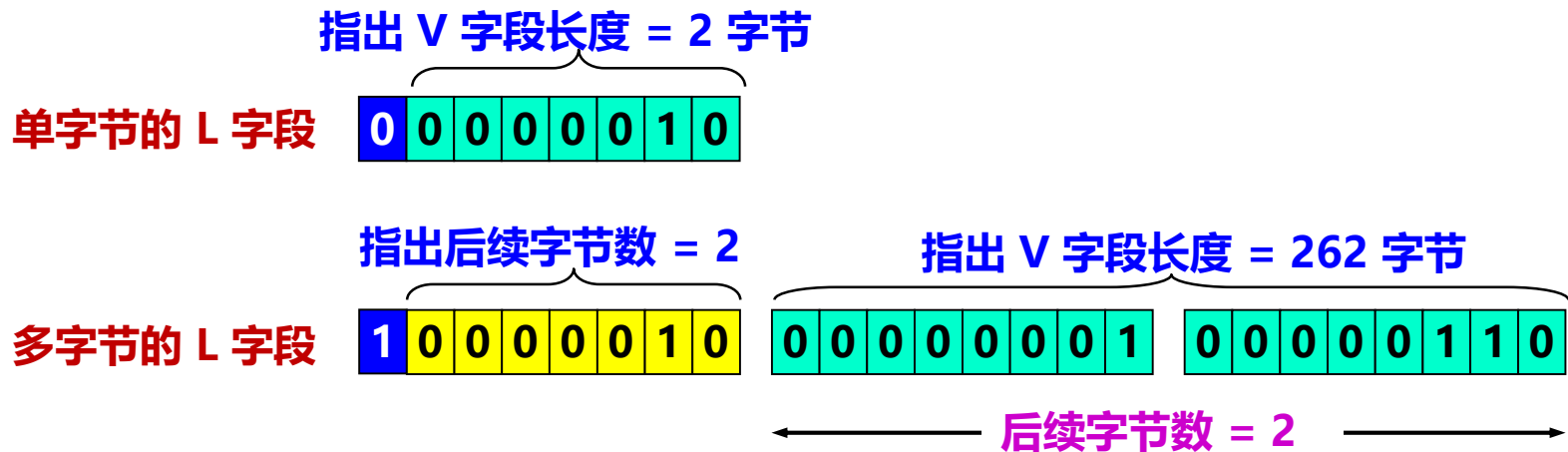
□ TLV 中的 T 字段定义数据的类型

| 数据类型 | 类别 | 格式 | 编号 | T字段 (二进制) | T字段 (十六进制) |
|-----------------------|----|----|-------|-----------|------------|
| INTEGER | 00 | 0 | 00010 | 00000010 | 02 |
| OCTET STRING | 00 | 0 | 00100 | 00000100 | 04 |
| OBJECT IDENTIFIER | 00 | 0 | 00110 | 00000110 | 06 |
| NULL | 00 | 0 | 00101 | 00000101 | 05 |
| Sequence, sequence of | 00 | 1 | 10000 | 00110000 | 30 |
| IPAddress | 01 | 0 | 00000 | 01000000 | 40 |
| Counter | 01 | 0 | 00001 | 01000001 | 41 |
| Gauge | 01 | 0 | 00010 | 01000010 | 42 |
| TimeTicks | 01 | 0 | 00011 | 01000011 | 43 |
| Opaque | 01 | 0 | 00100 | 01000100 | 44 |

7.简单网络管理协议SNMP

7.3 SMI

□ TLV 中的 L 字段定义 V 字段的长度



7.简单网络管理协议SNMP

7.3 SMI

□ TLV 中的 V 字段定义数据的值

| 类 型 | 大 小 | 说 明 |
|-------------------|------|--------------------------------------|
| INTEGER | 4 字节 | 在 -2^{31} 到 $2^{31} - 1$ 之间的整数 |
| Integer32 | 4 字节 | 和 INTEGER 相同 |
| Unsigned32 | 4 字节 | 在 0 到 $2^{32} - 1$ 之间的无符号数 |
| OCTET STRING | 可变 | 不超过 65535 字节长的字节串 |
| OBJECT IDENTIFIER | 可变 | 对象标识符 |
| IPAddress | 4 字节 | 由 4 个整数组成的IP地址 |
| Counter32 | 4 字节 | 可从 0 增加到 2^{32} 的整数；当它到达最大值时就返回到 0 |
| TimeTicks | 4 字节 | 记录时间的计数值，以 1/100 秒为单位 |
| BITS | — | 比特串 |
| Opaque | 可变 | 不解释的串 |

7.简单网络管理协议SNMP

7.3 SMI

□ TLV 举例:

- INTEGER 15, 其 T 字段是02, INTEGER 类型要用 4 字节编码

| T | L | V |
|----|----|-------------|
| 02 | 04 | 00 00 00 0F |

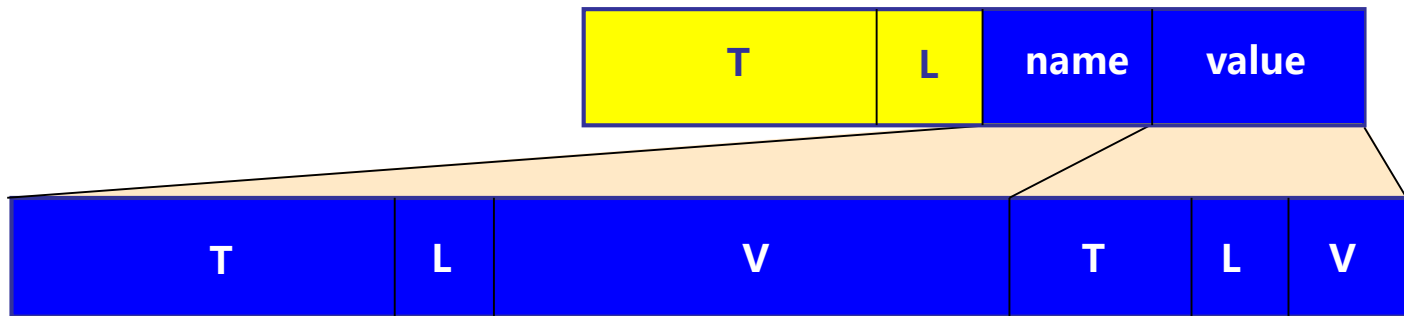
- IPAddress 192.1.2.3, 其 T 字段是 40, V 字段需要 4 字节表示

| T | L | V |
|----|----|-------------|
| 40 | 04 | C0 01 02 03 |

7.简单网络管理协议SNMP

7.3 SMI

- TLV 中的 V 字段可嵌套其他数据元素的 TLV 字段



7.简单网络管理协议SNMP

7.4 MIB

- ❑ 被管对象必须维持可供管理程序读写的若干控制和状态信息。这些信息总称为管理信息库 MIB (Management Information Base) 。
- ❑ 管理程序使用 MIB 中这些信息的值对网络进行管理（如读取或重新设置这些值）。
- ❑ 只有在 MIB 中的对象才是 SNMP 所能够管理的。

7.简单网络管理协议SNMP

7.4 MIB

节点 mib-2 所包含的信息类别举例

| 类别 | 标号 | 所包含的信息 |
|---------------------|-----|-------------------|
| system | (1) | 主机或路由器的操作系统 |
| interfaces | (2) | 各种网络接口 |
| address translation | (3) | 地址转换 (例如, ARP 映射) |
| ip | (4) | IP 软件 |
| icmp | (5) | ICMP 软件 |
| tcp | (6) | TCP 软件 |
| udp | (7) | UDP 软件 |
| egp | (8) | EGP 软件 |

7.简单网络管理协议SNMP

7.4 MIB

MIB 变量的例子

| MIB 变量 | 所属类别 | 意义 |
|-----------------|------------|-----------------|
| sysUpTime | system | 距上次重启的时间 |
| ifNumber | interfaces | 网络接口数 |
| ifMtu | interfaces | 特定接口的最大传送单元 MTU |
| ipDefaultTTL | ip | IP 在生存时间字段中使用的值 |
| ipInReceives | ip | 接收到的数据报数目 |
| ipForwDatagrams | ip | 转发的数据报数目 |
| ipOutNoRoutes | ip | 路由选择失败的数目 |
| ipReasmOKs | ip | 重装的数据报数目 |
| ipFragOKs | ip | 分片的数据报数目 |
| ipRoutingTable | ip | IP 路由表 |
| icmpInEchos | icmp | 收到的 ICMP 回送请求数目 |
| tcpRtoMin | tcp | TCP 允许的最小重传时间 |
| tcpMaxConn | tcp | 允许的最大 TCP 连接数目 |
| tcpInSegs | tcp | 已收到的 TCP 报文段数目 |
| udpInDatagrams | udp | 已收到的 UDP 数据报数目 |

7.简单网络管理协议SNMP

7.5 SNMP 协议数据单元与报文

- SNMP 的操作只有两种基本的管理功能。
 - “读”操作，用 get 报文来检测各被管对象的状况
 - “写”操作，用 set 报文来改变各被管对象的状况
- SNMP 的这些功能通过**探测**操作来实现。
 - 探测操作：SNMP 管理进程定时向被管理设备周期性地发送探测信息。
 - 探测的好处：
 - 可使系统相对简单。
 - 能限制通过网络所产生的管理信息的通信量。
 - 探测的缺点：
 - 不够灵活，而且所能管理的设备数目不能太多。
 - 开销也较大。

7.简单网络管理协议SNMP

7.5 SNMP 协议数据单元与报文

□ SNMP 陷阱(SNMP trap)

- SNMP 不是完全的探询协议，它允许不经过询问就能发送某些信息。这种信息称为陷阱，表示它能够捕捉“事件”。
- 当被管对象的代理检测到有事件发生时，就检查其门限值。代理只向管理进程报告达到某些门限值的事件（即过滤）。
- 过滤的好处是：
 - 仅在严重事件发生时才发送陷阱
 - 陷阱信息很简单且所需字节数很少

7.简单网络管理协议SNMP

7.5 SNMP 协议数据单元与报文

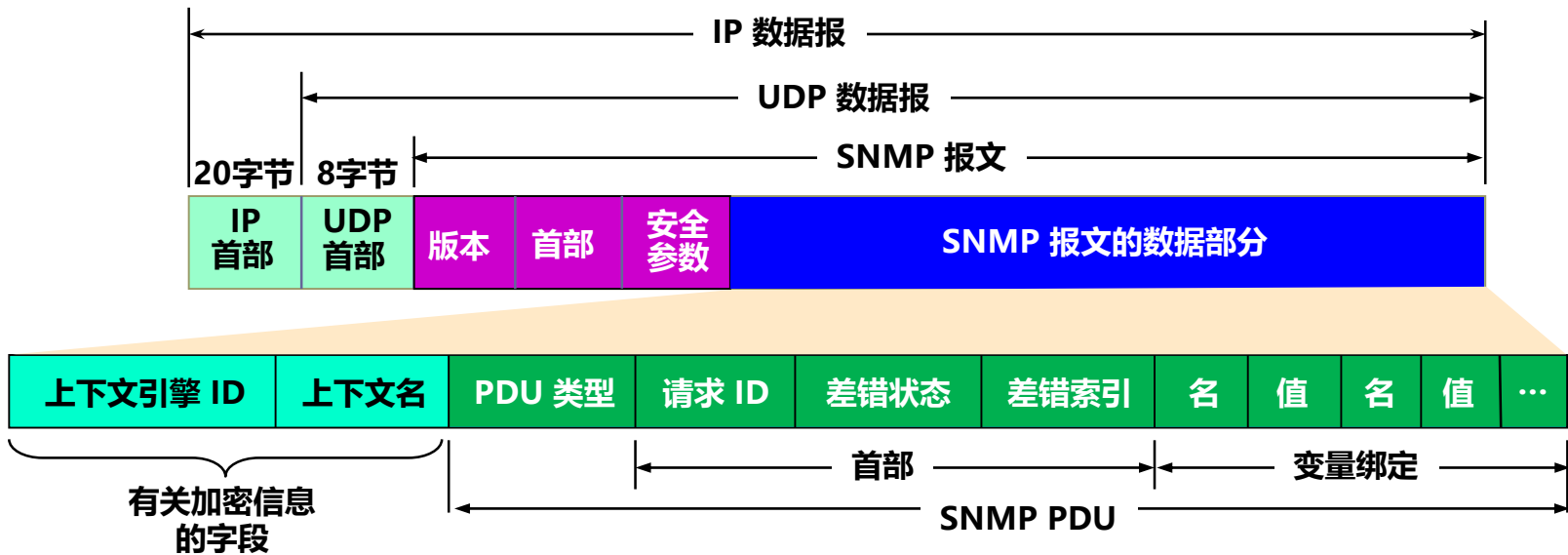
- SNMP 是有效的网络管理协议
 - 使用探询（至少是周期性地）以维持对网络资源的实时监视。
 - 同时也采用陷阱机制报告特殊事件，使得 SNMP 成为一种有效的网络管理协议。

- SNMP 使用无连接的 UDP
 - SNMP 使用无连接的 UDP，不保证可靠交付。
 - 在运行代理程序的服务器端用熟知端口 161 来接收 get 或 set 报文和发送响应报文（与熟知端口通信的客户端使用临时端口）。
 - 运行管理程序的客户端使用熟知端口 162 来接收来自各代理的 trap 报文。

7.简单网络管理协议SNMP

7.5 SNMP 协议数据单元与报文

SNMP 的报文格式



7.简单网络管理协议SNMP

7.5 SNMP 协议数据单元与报文

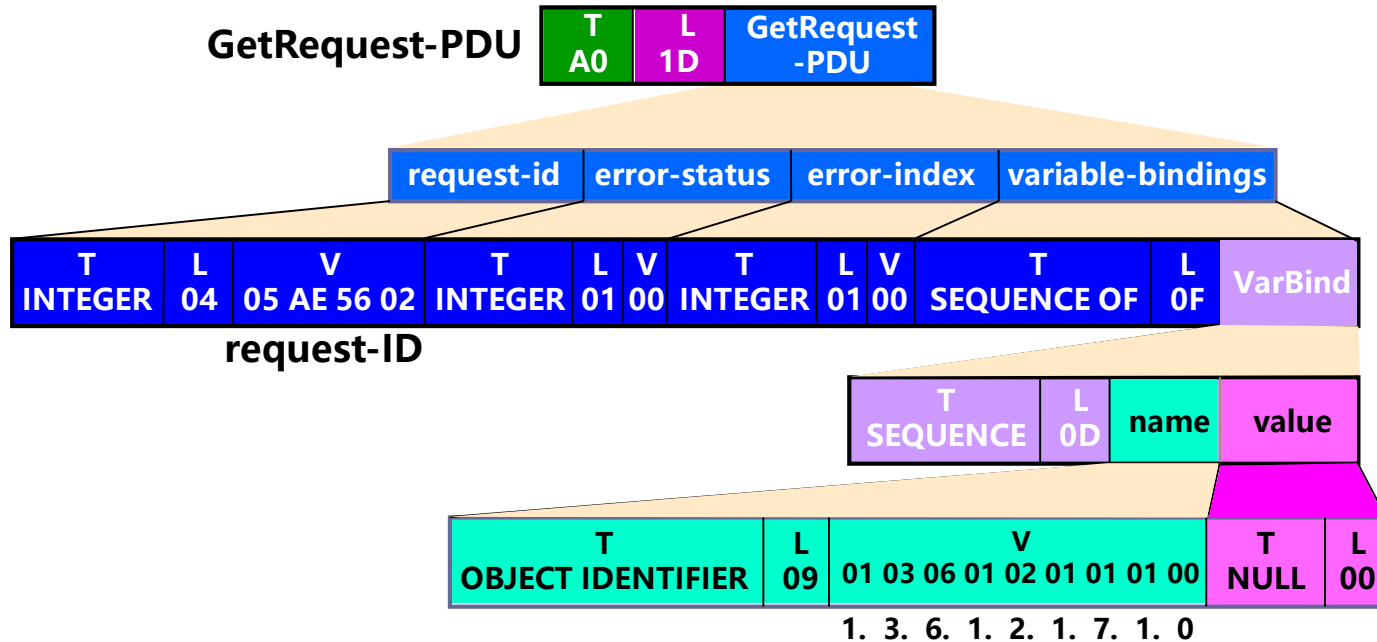
SNMPv1 定义的协议数据单元 (PDU) 类型

| PDU 编号 (T字段) | PDU 名称 | 用途 |
|--------------|----------------|-----------------------------|
| 0 (A0) | GetRequest | 用来查询一个或一组变量的值 |
| 1 (A1) | GetNextRequest | 允许在 MIB 树上读取下一个变量, 此操作可反复进行 |
| 2 (A2) | Reponse | 代理向管理者或管理者向管理者发送响应 |
| 3 (A3) | SetRequest | 对一个或多个变量值进行设置 |
| 5 (A5) | GetBulkRequest | 管理者从代理读取大数据块的值 |
| 6 (A6) | InformRequest | 管理者从另一管理者读取代理的变量 |
| 7 (A7) | SNMPv2Trap | 代理向管理者报告异常事件 |
| 8 (A8) | Report | 管理者之间报告某些差错 |

7.简单网络管理协议SNMP

7.5 SNMP 协议数据单元与报文

Get-request 报文 ASN.1 编码



Thanks