



B站 UP : 澧劬閣 整理

第01章 计算机网络详解



讲师：韩立刚
51CTO学院金牌讲师
51CTO学院教学顾问
微软最有价值专家MVP
河北师大软件学院讲师
河北地质大学客座教授
计算机图书作者
QQ: 458717185

本章内容

- 1.1 计算机网络在当今社会的作用
- 1.2 认识网络
- 1.3 理解计算机通信使用的协议
- 1.4 TCP/IP协议
- 1.5 OSI参考模型
- 1.6 理解OSI参考模型
- 1.7 计算机网络性能指标
- 1.8 网络分类
- 1.9 企业局域网设计

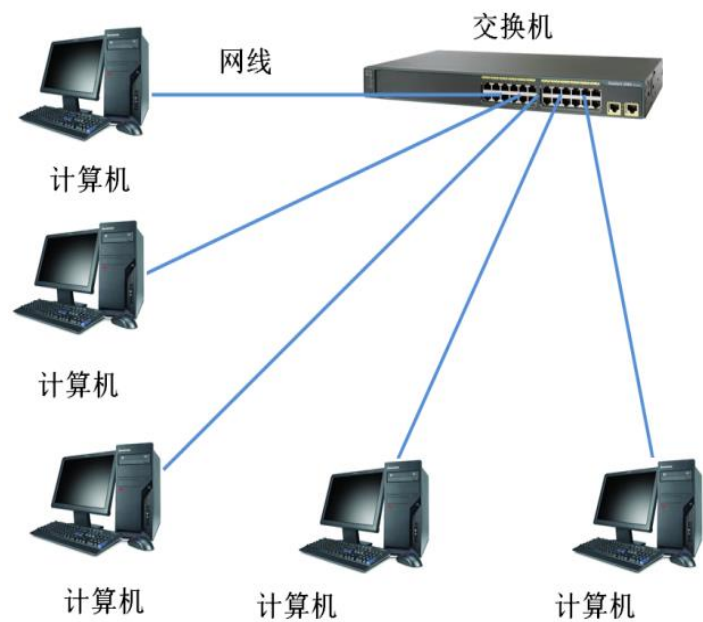
1.1 计算机网络在当今社会的作用

- 信息时代的重要特征21世纪的一些重要特征就是数字化、网络化和信息化，它是一个以网络为核心的信息时代。
- 网络是指“三网”，即电信网络、有线电视网络、和计算机网络。发展最快的并起到核心作用的是计算机网络。
- 计算机网络的概念计算机网络：指将地理位置不同的具有独立功能的多台计算机及其外部设备，通过通信线路连接起来，在网络操作系统、网络管理软件及网络通信协议的管理和协调下，实现资源共享和信息传递的计算机系统。

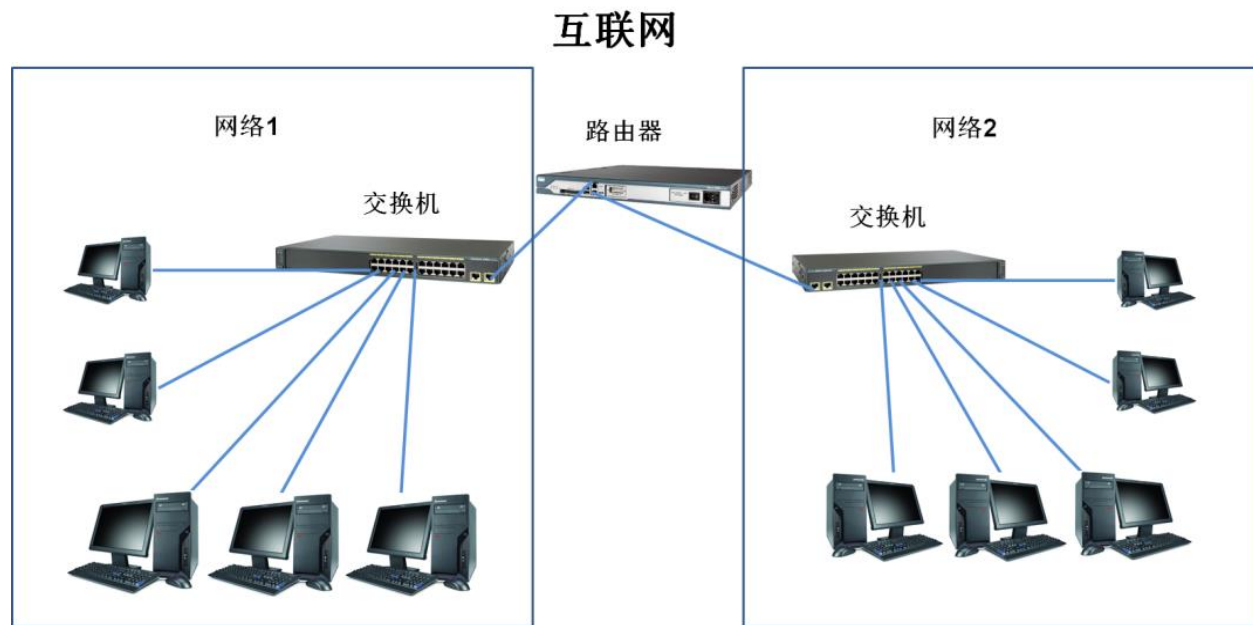
1.2认识网络

- 1.2.1网络和互联网络
- 1.2.2最大的互连网络-因特网
- 1.2.3企业组建的互联网络
- 1.2.4家庭通过ADSL访问Internet

1.2.1 网络和互连网络



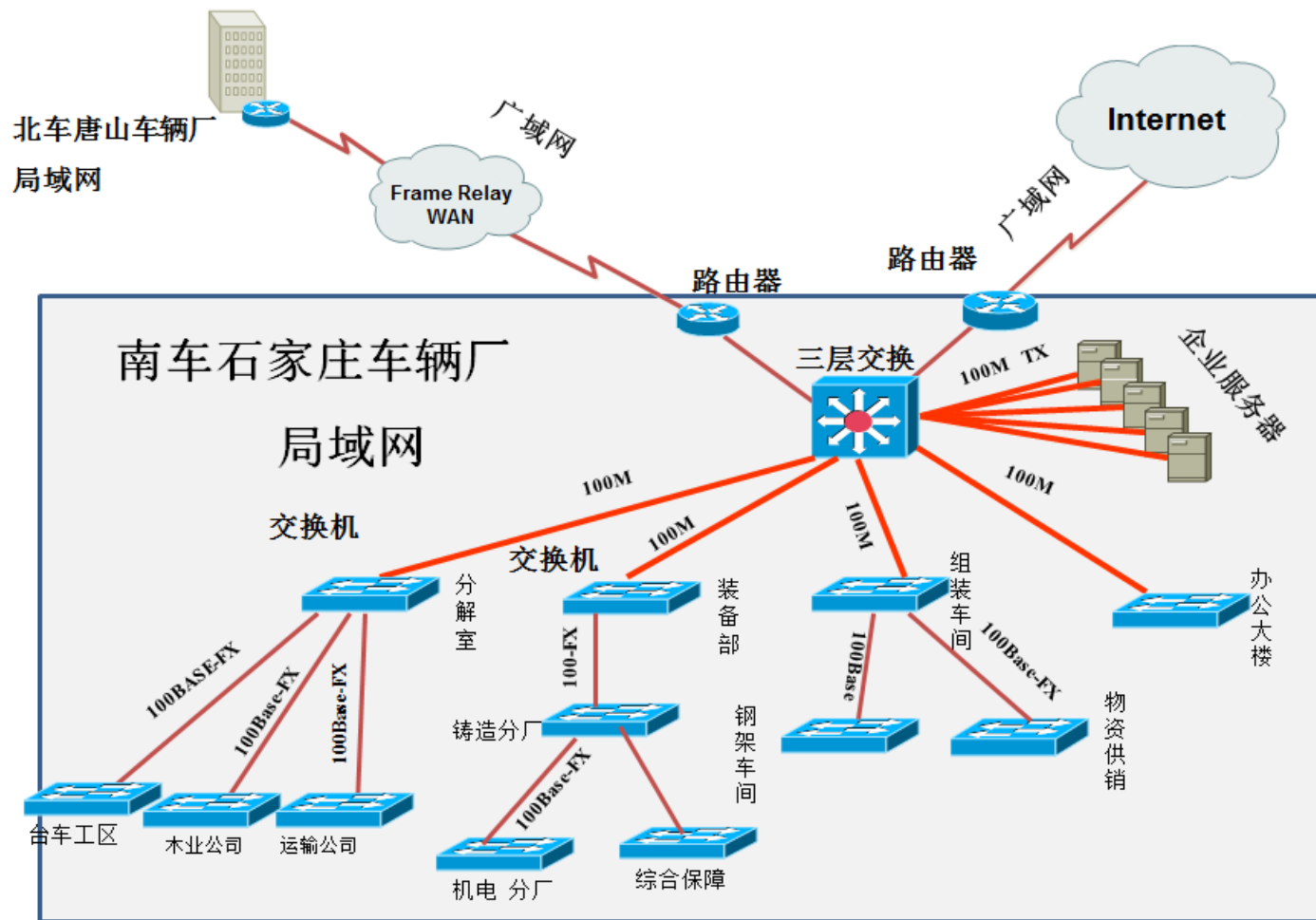
网络



互连网络

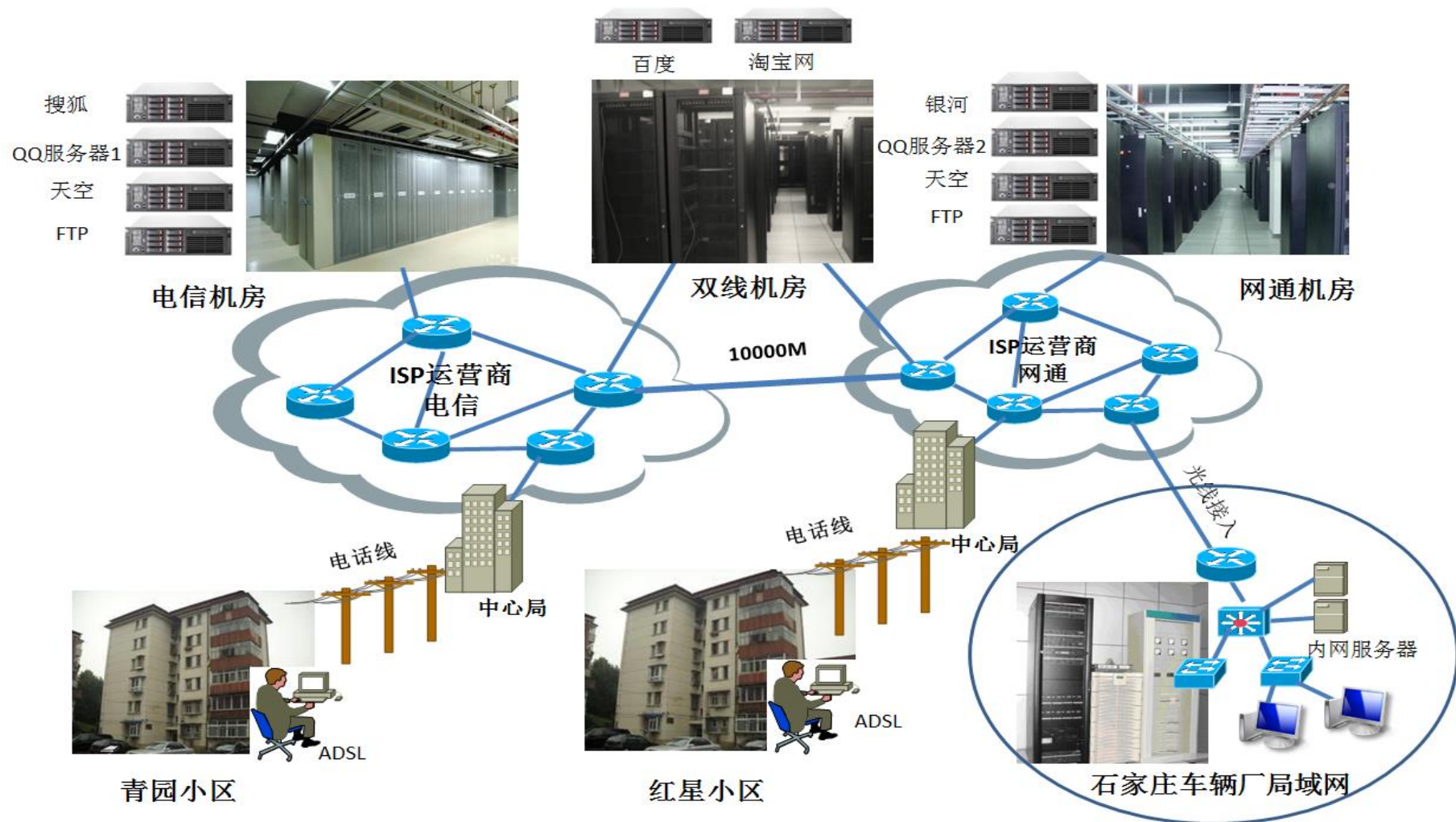
企业组建的网络

典型的企业网络应用环境



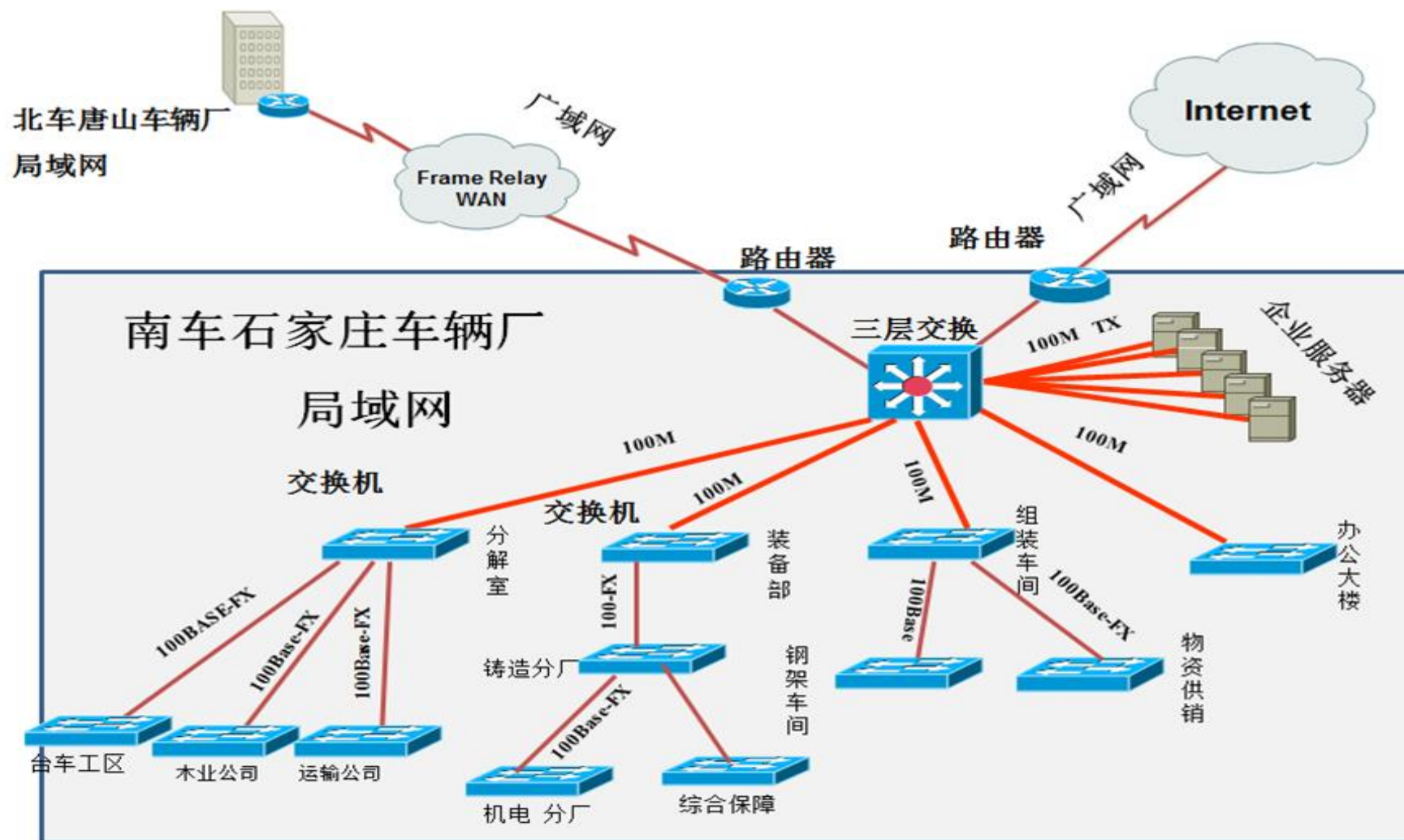
1.2.2最大的互联网-因特网

Internet示意图

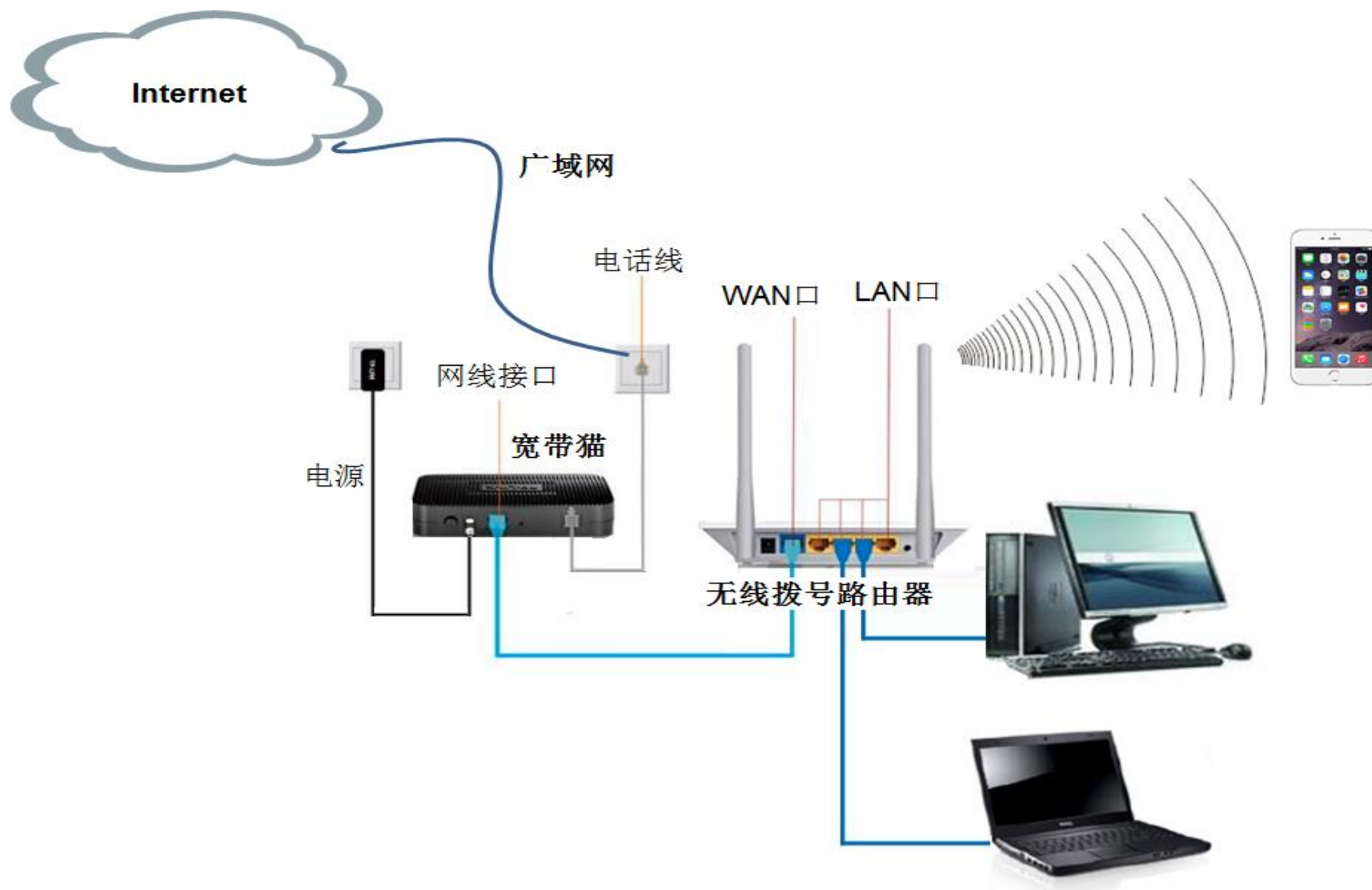


1.2.3 企业组建的互联网

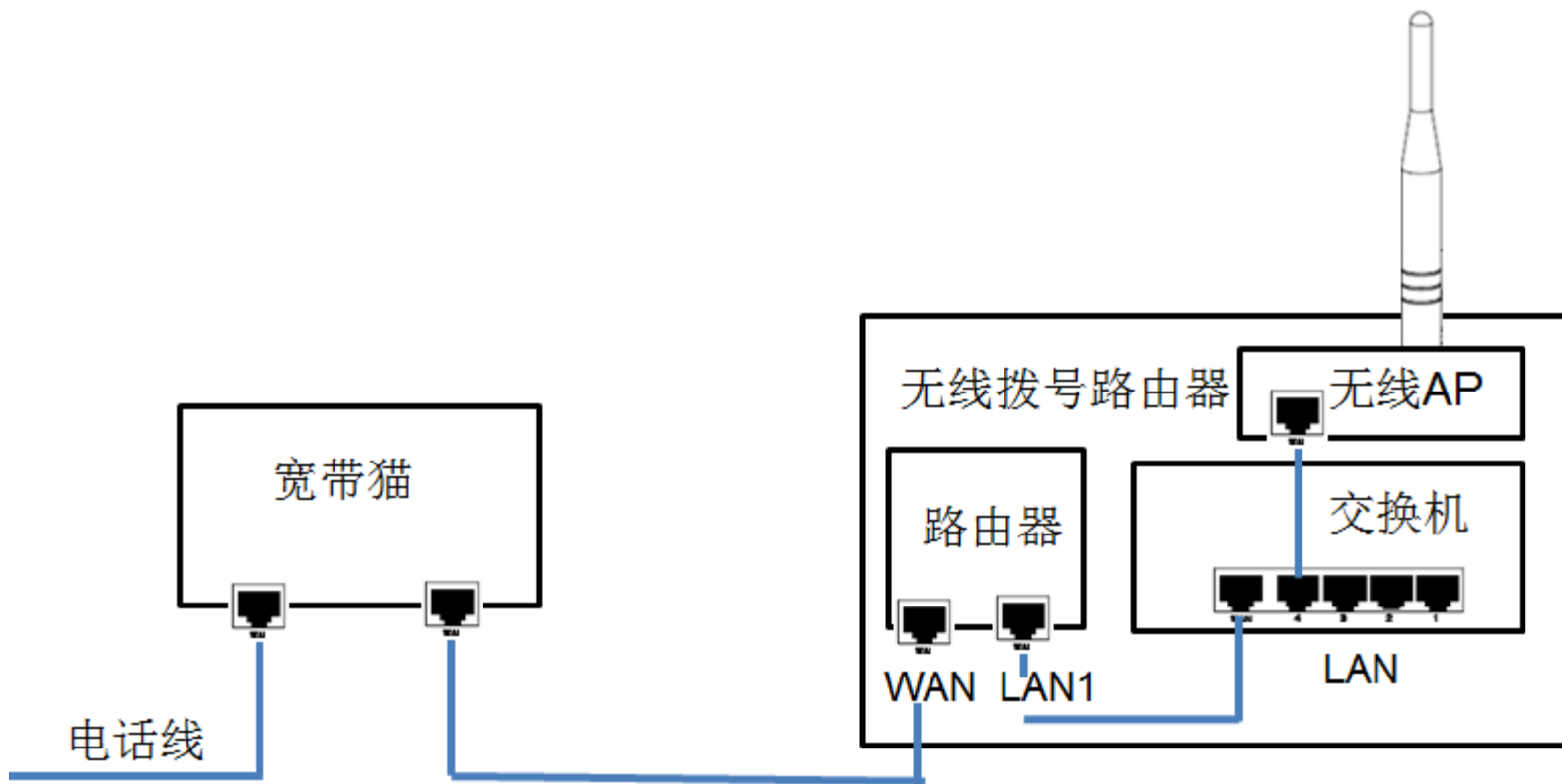
企业组建的互联网



1.2.4 通过无线路由器组件的家庭网络



家庭ADSL无线拨号路由器逻辑图



1.3 理解计算机通信使用的协议

- 1.3.1 生活中的协议
- 1.3.2 应用程序使用的协议
- 1.3.3 协议的标准化带来的好
- 1.3.4 以HTTP协议为例认识应用层协议
- 1.3.5 抓包分析HTTP协议报文格式

1.3.1 生活中的协议

- 协议中包括甲方和乙方。
- 签署协议的目的。
- 协议条款列出了双方关心的事项、甲方乙方的责任、需要做什么、什么时候做、各种意外如何处理。
- 协议最后还要有甲乙双方的签名，声明一式两份，意味着签协议的双方对协议中的条款达成一致，都要遵守协议中的约定。

租房协议

甲方（出租方）：_____ 身份证：_____

乙方（承租方）：_____ 身份证：_____

经双方协商一致，甲方将坐落于_____房屋出租给乙方使用。

一、租房从_____年____月____日起至_____年____月____日止。

二、月租金为_____元/月，押金_____元，以后每月____日交房租。

三、水_____吨，气_____立方，电_____度。

四、约定事项

- 1、乙方正式入住时，应及时的更换房门锁，若发生因门锁问题的意外与甲方无关。因用火不慎或使用不当引起的火灾、电、气灾害等非自然类的灾害所造成一切损失均由乙方负责。
- 2、乙方无权转租、转借、转卖该房屋，及屋内家具家电，不得擅自改动房屋结构，爱护屋内设施，如有人为原因造成破损丢失应维修完好，否则照价赔偿。并做好防火，防盗，防漏水，和阳台摆放、花盆的安全工作，若造成损失责任自负。
- 3、乙方必须按时缴纳房租，否则视为乙方违约，协议终止。
- 4、乙方应遵守居住区内各项规章制度，按时缴纳水、电、气、光纤、电话、物业管理等费用。乙方交押金给甲方，乙方退房时交清水、电、气、光纤和物业管理等费用，屋内设施家具、家电无损坏，下水管道、厕所无堵漏，甲方如数退还押金。
- 5、甲方保证该房屋无产权纠纷。如遇拆迁，乙方无条件搬出，已交租金甲方按未天数退还。

五、本协议一式两份，自双方签字之日起生效。

甲方签字（出租方）：_____

乙方签字（承租方）：_____

电话：_____

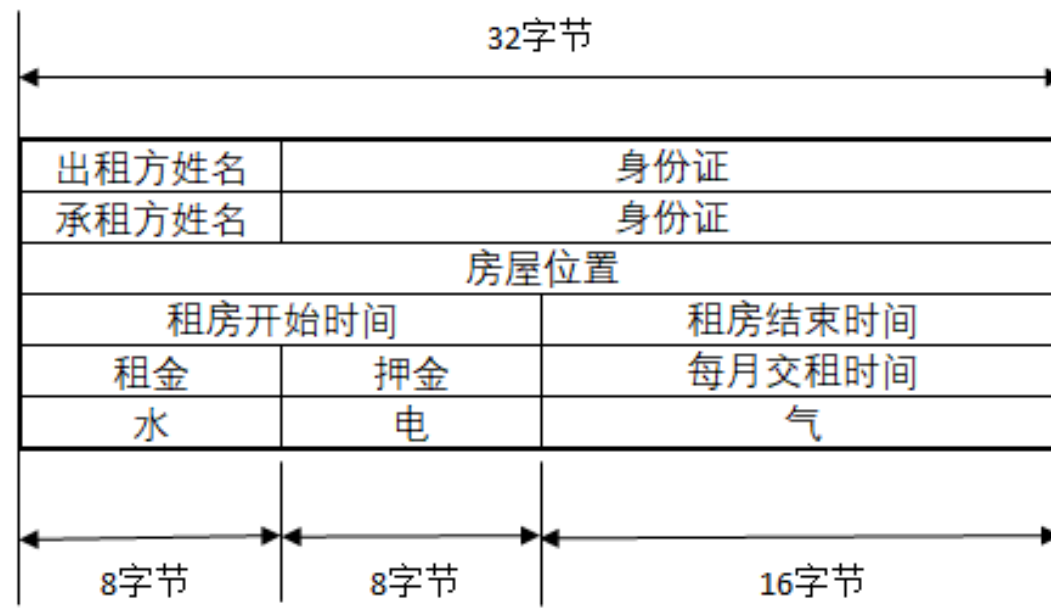
电话：_____

_____年____月____日

1.3.1 简化后的租房协议

- 租房协议简化和标准化后形成一张表格。
- 该表格规定了要填写的内容。
- 哪些协议中的条款，甲乙双方都知道，就不用在这里填写了。

- 这是计算机通信使用的IP协议。通信双方只需按着这个表格中的字段填写内容即可。
- 协议中的那些条款不必在通信过程中传输。



0	4	8	16	19	24	31
版 本	首部长度	区 分 服 务	总 长 度			
标 识			标 志	片 偏 移		
生 存 时 间	协 议		首 部 检 验 和			
源 IP 地 址						
目 标 IP 地 址						
可 选 字 段 (长 度 可 变)					填 充	

1.3.2 应用程序通信使用的协议

- 客户端程序能够向服务端程序发送哪些请求，也就是客户端能够向服务端发送哪些命令，这些命令发送的顺序，发送的请求报文有哪些字段，分别代表什么意思，都需要提前约定好。
- 服务端程序收到客户端发送来的请求，应该有哪些响应，什么情况发送什么响应，发送的响应报文有哪些字段，分别代表什么意思，也需要提前约定好。

服务端程序



Web服务

客户端发请求

服务端响应

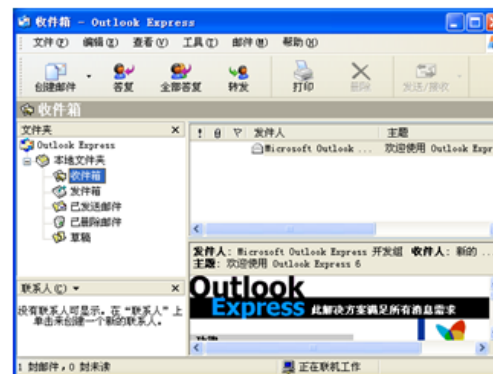
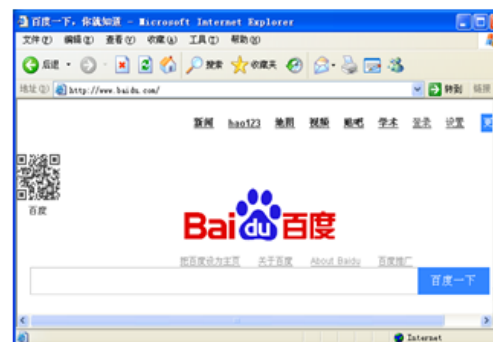


邮件服务

客户端发请求

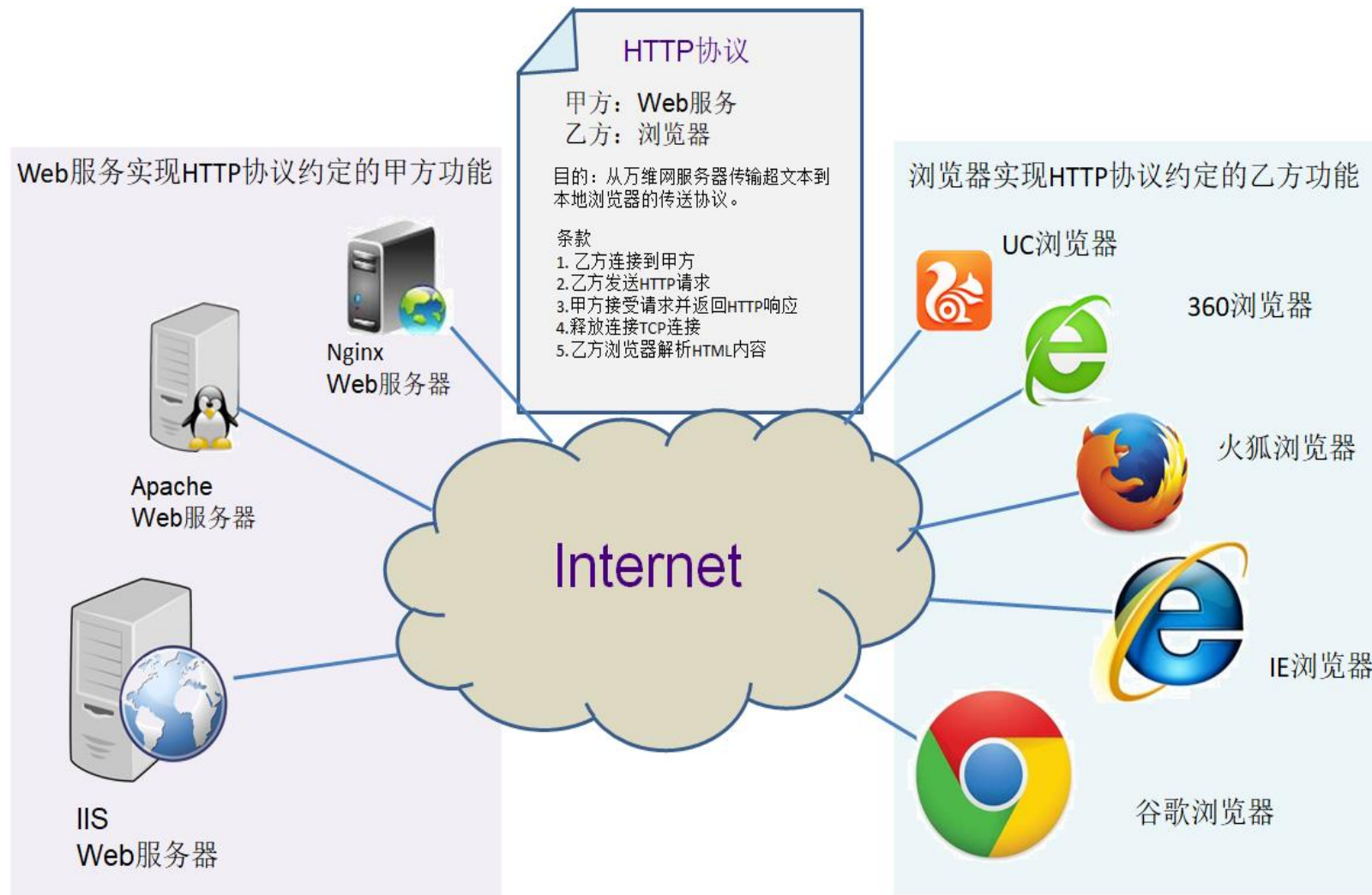
服务端响应

客户端程序



1.3.3 协议的标准化带来的好处

■互联网中有很多常见的应用，很多家公司开发服务端程序，也有很多家公司开发客户端程序。为了使不同厂家开发的服务端程序和客户端程序能够通信，必须将这些应用程序通信协议的协议进行标准化。



TCP/IP协议组中知名的应用层协议

- 超级文本传输协议--HTTP，用于访问Web服务。
- 安全的超级文本传输协议--HTTPS，能够将HTTP协议通信进行加密访问。
- 简单邮件传输协议--SMTP，用于发送电子邮件。
- 邮局协议版本3 --POP3，用于接收电子邮件。
- 域名解析协议--DNS，用于域名解析。
- 文件传输协议--FTP，用于在Internet上传和下载文件。
- 简单文件传输协议--TFTP，在客户机与服务器之间进行简单文件传输的协议。
- 远程登录--telnet协议，用于远程配置网络设备和Linux系统。
- 动态主机配置协议--DHCP，用于计算机自动请求IP地址。

1.3.4 以HTTP协议为例认识应用层协议

- HTTP协议的甲方乙方分别是 Web服务器和浏览器
- 该协议就是规定浏览器访问网站方法和规则。
- 定义了客户端能够向服务器发送哪些请求。
- 服务器能够向客户端发送哪些响应。
- 定义了请求报文格式。
- 定义了响应报文格式。

方法名称是区分大小写的。当某个请求所针对的资源不支持对应的请求方法的时候，服务器应当返回状态码 405 (Method Not Allowed)；当服务器不认识或者不支持对应的请求方法的时候，应当返回状态码 501 (Not Implemented)。

HTTP 协议

甲方： Web 服务

乙方： 浏览器

HTTP 协议是 Hyper Text Transfer Protocol (超文本传输协议) 的缩写，是从万维网 (WWW: World Wide Web) 服务器传输超文本到本地浏览器的一种传送协议。HTTP 是一个基于 TCP/IP 通信协议来传递数据 (HTML 文件, 图片文件, 查询结果等) 的应用层协议。

HTTP 协议工作在客户端-服务端架构之上。浏览器作为 HTTP 客户端通过 URL 向 HTTP 服务端即 WEB 服务器发送所有请求。Web 服务器根据接收到的请求, 向客户端发送响应信息。

协议条款:

一、HTTP 请求、响应的步骤

1. 客户端连接到 Web 服务器

一个 HTTP 客户端, 通常是浏览器, 与 Web 服务器的 HTTP 端口 (默认使用 TCP 协议的 80 端口) 建立一个 TCP 套接字连接。

2. 发送 HTTP 请求

通过 TCP 套接字, 客户端向 Web 服务器发送一个文本的请求报文, 请求报文由请求行、请求头部、空行和请求数据 4 部分组成。

3. 服务器接受请求并返回 HTTP 响应

Web 服务器解析请求, 定位请求资源。服务器将资源副本写到 TCP 套接字, 由客户端读取。一个响应由状态行、响应头部、空行和响应数据 4 部分组成。

4. 释放 TCP 连接

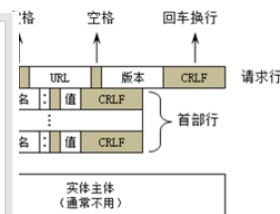
若 connection 模式为 close, 则服务器主动关闭 TCP 连接, 客户端被动关闭连接, 释放 TCP 连接; 若 connection 模式为 keepalive, 则该连接会保持一段时间, 在该时间内可以继续接收请求。

5. 客户端浏览器解析 HTML 内容

客户端浏览器首先解析状态行, 查看表明请求是否成功的状态代码。然后解析每一个响应头, 响应头告知以下为若干字节的 HTML 文档和文档的字符集。客户端浏览器读取响应数据 HTML, 根据 HTML 的语法对其进行格式化, 并在浏览器窗口中显示。

二、请求报文格式

由于 HTTP 是面向文本的, 因此在报文中的每一个字段都是一些 ASCII 码串, 因而各个字段的长度都是不确定的。HTTP 请求报文由三个部分组成, 如下图所示。



还是响应报文。在请求报文中的开始行叫做请求行, 而在响应报文中叫做状态行。在开始行的三个字段之间都以空格分隔, 'r' 分别代表“回车”和“换行”。

服务器或报文主体的一些信息。首部可以有好多行, 但也可只有一行。首部行中都有首部字段名和它的值, 每一行在结束的地方以“换行”。整个首部行结束时, 还有一空行将首部行和后面

都不使用这个字段, 而在响应报文中也可能没有这个字段。

发送以下八种方法 (有时也叫“动作”) 来表明对 URL 指

新标识的资源。在浏览器的地址栏中输入网址的方式访问网页。GET 方法向服务器请求网页。

的资源后附加新的数据。要求被请求服务器接受附在请求后交表单。比如向服务器提交信息、发帖、登录。

URL 所标识的资源的响应消息报头。

一个资源, 并用 URL 作为其标识。

删除 URL 所标识的资源。

回送收到的请求信息, 主要用于测试或诊断。

服务器。

服务器的性能, 或者查询与资源相关的选项和需求。

计算机通信使用的协议包含三要素

■计算机通信使用的协议包含三要素：语法、语义和同步。

■语法

- 定义协议中每种报文的格式：有哪些字段，字段是定长还是变长，如果是变长，字段分割符是什么，都要在协议中定义。一个协议有可能需要定义多种报文格式，比如ICMP协议，定义了ICMP请求报文格式、ICMP响应报文格式、ICMP差错报告报文格式。

■语义

- 客户端能够向服务器发送那些请求（方法或命令），服务器有哪些响应（状态代码），每种状态代码代表什么意思。

■同步

- 客户端访和服务服务器命令交互顺序，比如POP3协议，需要先验证用户身份才能收邮件。

1.3.5 抓包分析HTTP协议报文格式

■ 请求报文中的GET方法

显示筛选器

HTTP请求包

HTTP响应包
200是状态代码

HTTP请求方法

HTTP请求报文
中的各个字段

The image shows a Wireshark packet capture window titled '*WLAN'. The packet list on the left shows several HTTP packets. Packet 323 is selected, which is an HTTP GET request. The packet details pane on the right shows the structure of the packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The Hypertext Transfer Protocol section is expanded, showing the GET method and various headers like Referer, User-Agent, Accept, Accept-Language, and Accept-Encoding. The packet bytes pane at the bottom shows the raw data of the packet, with the first few bytes highlighted in blue.

No.	Time	Source	Destination	Protocol	Length
234	2.801988	192.168.2.163	47.93.94.253	HTTP	1002e HTTP/1.1
323	2.936178	192.168.2.163	203.107.41.32	HTTP	656tion?sysNum=a8d9
330	3.016862	47.93.94.253	192.168.2.163	HTTP	60/html)
349	3.079701	203.107.41.32	192.168.2.163	HTTP	1391ication/json)
354	3.095035	192.168.2.163	203.107.41.32	HTTP	555fflineMsgSize.ac

Frame 323: 656 bytes on wire (5248 bits), 656 bytes captured (5088 bits) on interface 0
Ethernet II, Src: IntelCor_f9:d2:51 (00:db:df:f9:d2:51), Dst: B:e9:96:a4:61)
Internet Protocol Version 4, Src: 192.168.2.163, Dst: 203.107.41.32
Transmission Control Protocol, Src Port: 57552, Dst Port: 80, Seq: 3055888, Win: 0, Len: 0
Hypertext Transfer Protocol
GET /chat/user/load.action?sysNum=a8d9379eaf884b4f81a4834897k=callback1546085419
Referer: http://home.51cto.com/index\r\n\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36\r\n\r\nAccept: */*\r\n\r\nAccept-Language: zh-Hans-CN,zh-Hans;q=0.8,en-US;q=0.5,en;q=0.3\r\n\r\nAccept-Encoding: gzip, deflate\r\n\r\n

0030 ff ff 3e e0 00 00 47 45 54 20 2f 63 68 61 74 2f -->...G
0040 75 73 65 72 2f 6c 6f 61 64 2e 61 63 74 69 6f 6e user/lo
0050 3f 73 79 73 4e 75 6d 3d 61 38 64 39 33 37 39 65 ?sysNum:
0060 61 66 38 38 34 62 34 66 38 31 61 34 38 33 34 38 af884b4

Text item (text), 117 bytes | Packets: 1155 0 (0.0%) | Profile: Classic

1.3.5 抓包分析HTTP协议报文格式

■ 请求报文中的 POST方法

显示筛选器

HTTP登录数据包

HTTP协议
POST方法

登录账户

登录密码

The image shows a Wireshark packet capture analysis of an HTTP POST request. The packet list at the top shows four packets, with packet 635 selected. The packet details pane shows the structure of the selected packet, which is an HTTP POST request to /index. The request includes a Referer, Cache-Control, Content-Type, User-Agent, and Accept-Language header. The body of the request is an HTML Form URL Encoded string containing form items for csrf, LoginForm[username], LoginForm[password], LoginForm[rememberMe], show_qr, and login-button. The packet bytes pane at the bottom shows the raw data of the selected packet, with the form data highlighted in blue.

No.	Time	Source	Destination	Protocol	Length	Info
517	10.664566	192.168.2.163	111.7.73.24	HTTP	1225	POST /qexquery HTTP/1.1
537	12.229952	192.168.2.163	111.7.73.24	HTTP	1393	POST /qexquery HTTP/1.1
635	28.209736	192.168.2.163	47.93.94.253	HTTP	263	POST /index HTTP/1.1 (application/x-www-form-urlencoded)
890	29.296969	192.168.2.163	111.7.73.24	HTTP	1393	POST /qexquery HTTP/1.1

Frame 635: 263 bytes on wire (2104 bits), 263 bytes captured (2104 bits) on interface 0

Ethernet II, Src: IntelCor_f9:d2:51 (00:db:df:f9:d2:51), Dst: PhicommS_96:a4:61 (d8:c8:e9:96:a4:61)

Internet Protocol Version 4, Src: 192.168.2.163, Dst: 47.93.94.253

Transmission Control Protocol, Src Port: 57554, Dst Port: 80, Seq: 10087, Ack: 7497, Len: 209

[4 Reassembled TCP Segments (3614 bytes): #632(1444), #633(1444), #634(517), #635(209)]

Hypertext Transfer Protocol

POST /index HTTP/1.1\r\n

Referer: http://home.51cto.com/index\r\n

Cache-Control: max-age=0\r\n

Content-Type: application/x-www-form-urlencoded\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3399.104 Safari/537.36\r\n

Accept-Language: zh-Hans-CN,zh-Hans;q=0.8,en-US;q=0.5,en;q=0.3\r\n

HTML Form URL Encoded: application/x-www-form-urlencoded

Form item: "_csrf" = "cVNLL1JCWXA/K39LDSVsHSM1Mm0rCyMyOyQgHT81aCU7H39/PQc9Fw=="

Form item: "LoginForm[username]" = "onesthan"

Form item: "LoginForm[password]" = "1234567890"

Form item: "LoginForm[rememberMe]" = "0"

Form item: "show_qr" = "0"

Form item: "login-button" = "登录"

00dd0 34 35 36 37 38 39 30 26 4c 6f 67 69 6e 46 6f 72 4567890& LoginFor

0de0 6d 25 35 42 72 65 6d 65 6d 62 65 72 4d 65 25 35 m%5Breme mberMe%5

Frame (263 bytes) Reassembled TCP (3614 bytes)

Text item (text), 28 bytes

Packets: 1155 · Displayed: 4 (0.3%) · Dropped: 0 (0.0%) Profile: Classic

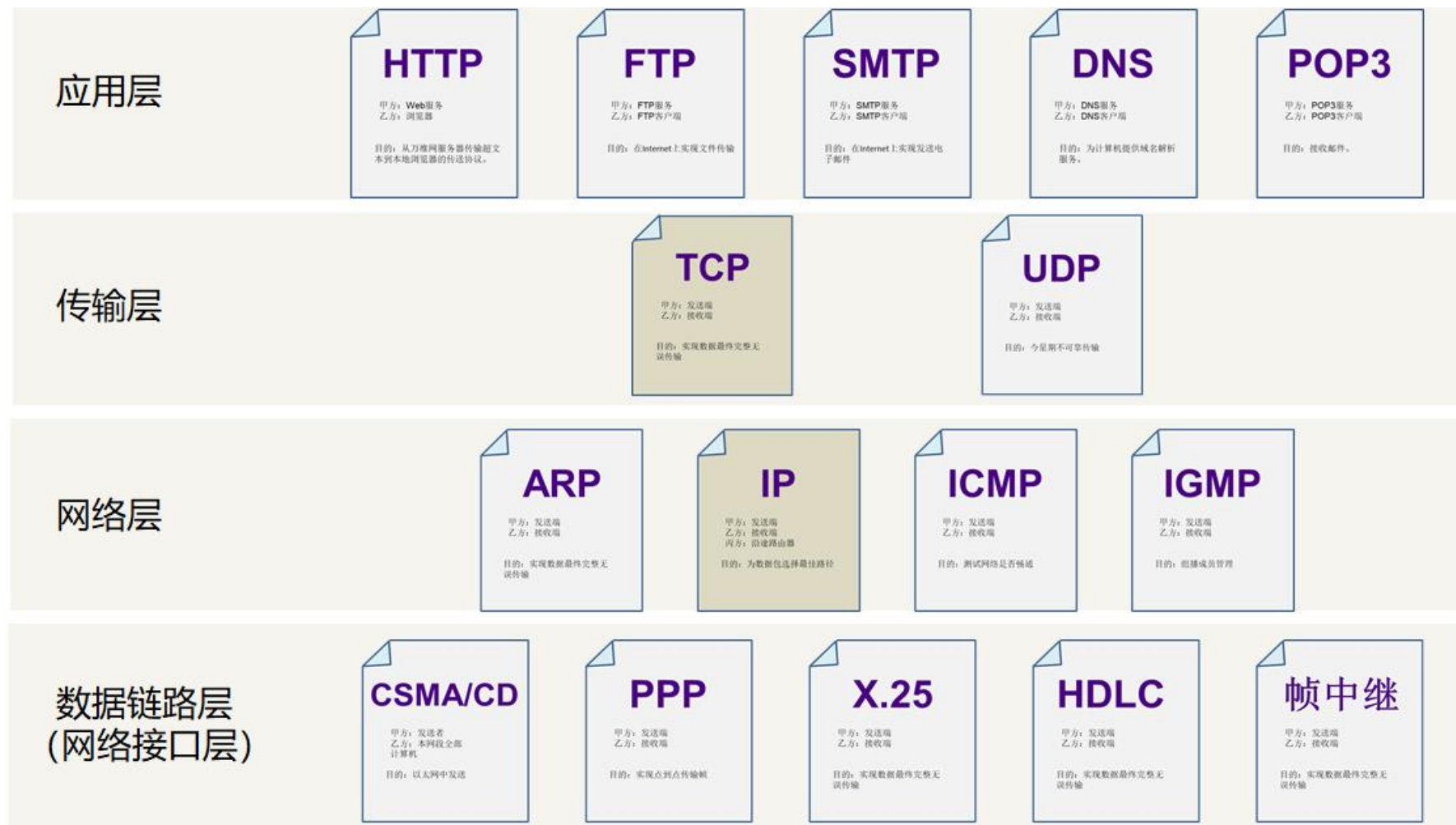
1.4 TCP/IP协议

- 1.4.1 TCP/IP协议分层
- 1.4.2 封装和解封
- 1.4.3 将计算机通信分层的好处
- 1.4.4 TCP/IP协议的体系结构

1.4.1 TCP/IP协议分层

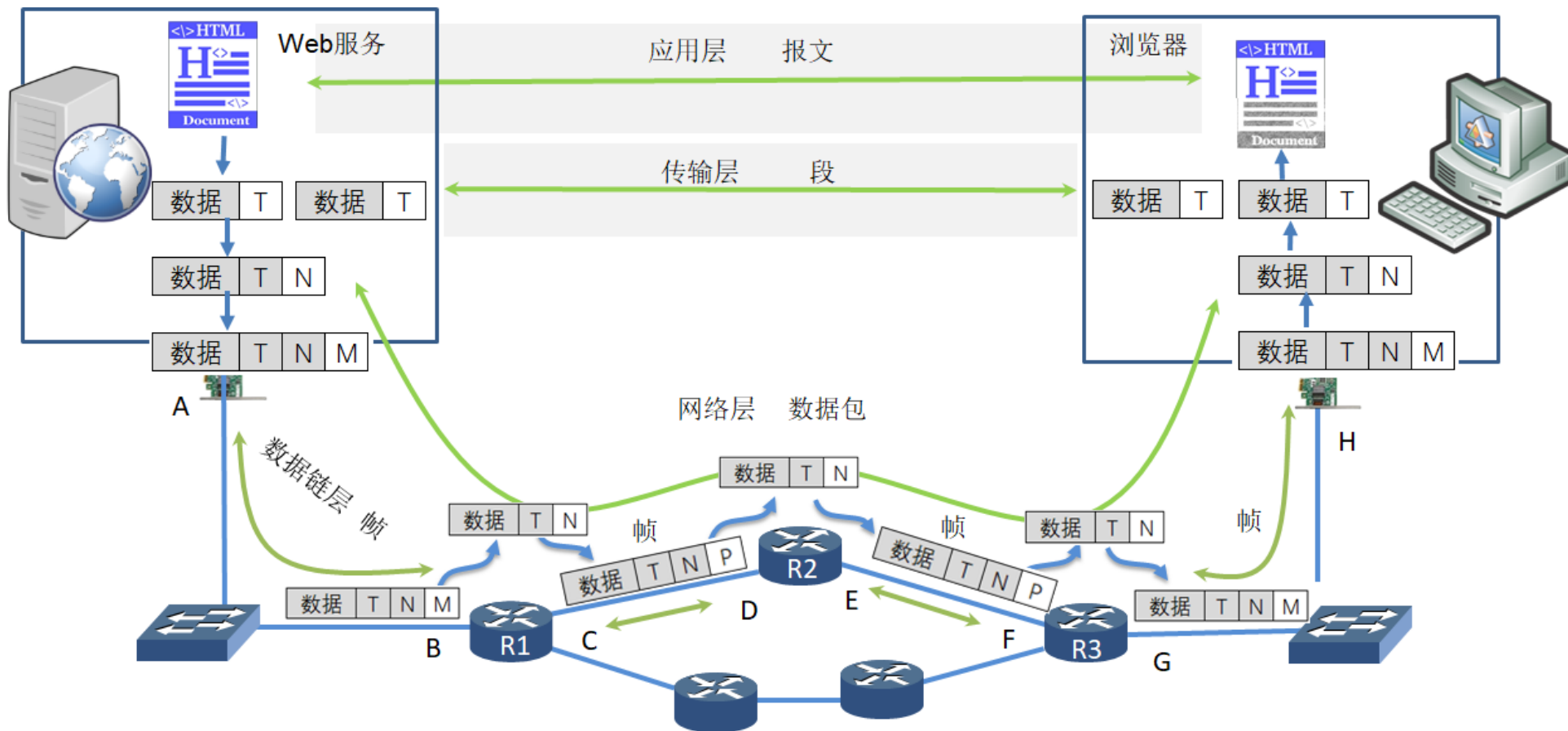
■TCP/IP协议是互联网通信的工业标准，其实它是一组协议，TCP和IP协议是这一组协议的代表。

■这些协议按功能分为应用层协议、传输层协议、网络层协议、数据链路层协议。



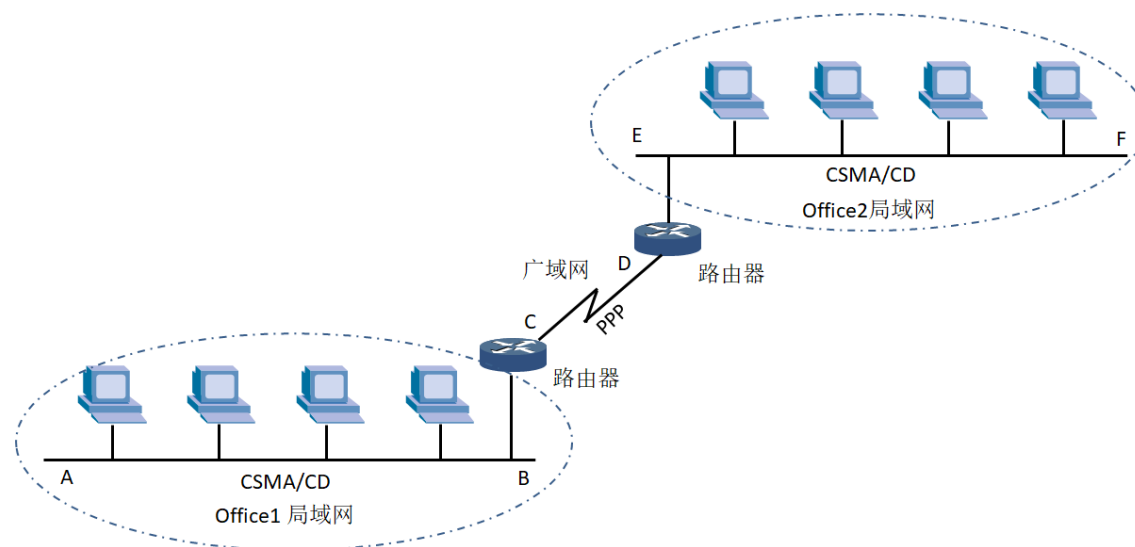
1.4.2 封装和解封

- 发送端加上传输层首部、网络层首部、数据链路层首部的过程叫做封装。
- 接收端收到后，去掉数据链路层首部、去掉网络层首部、去掉传输层首部的过程叫做解封。
- 每经过一个链路，数据包都要重新封装成帧。



1.4.3 将计算机通信分层设计的好处

- 各层之间相互独立。
- 灵活性好。
- 结构上可以分开。
- 易于实现和维护。
- 能促进标准化工作。



TCP/IPv4协议组

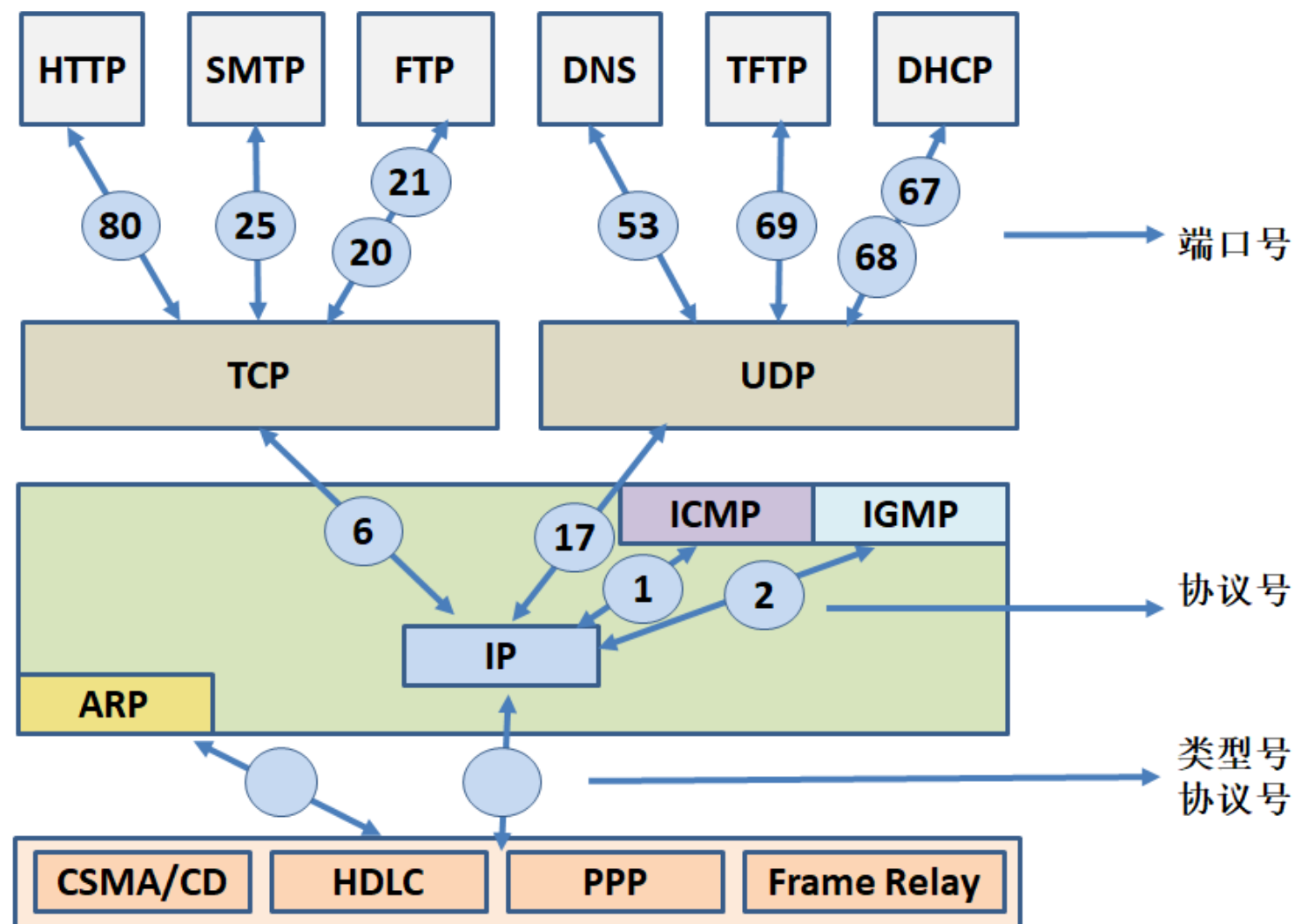
HTTP	FTP	SMTP	POP3	Telnet	DHCP	DNS	TFTP
TCP				UDP			
IPv4						ICMP	IGMP
ARP							
CSMA/CD		X.25	HDLC	Frame Relay		PPP	

TCP/IPv6协议组

HTTP	FTP	SMTP	POP3	Telnet	DHCP	DNS	TFTP
TCP				UDP			
IPv6						ND	MLD
						ICMPv6	
CSMA/CD		X.25	HDLC	Frame Relay		PPP	

1.4.4 TCP/IP协议体系结构

- 体系结构就是包括哪些协议以及他们之间的关系。
- 如果底层协议能够支持多种上层协议的封装，在底层协议必然要有一个字段用来指明封装的是哪种上层协议。否则接收端就不知道提交给上层的那个协议。



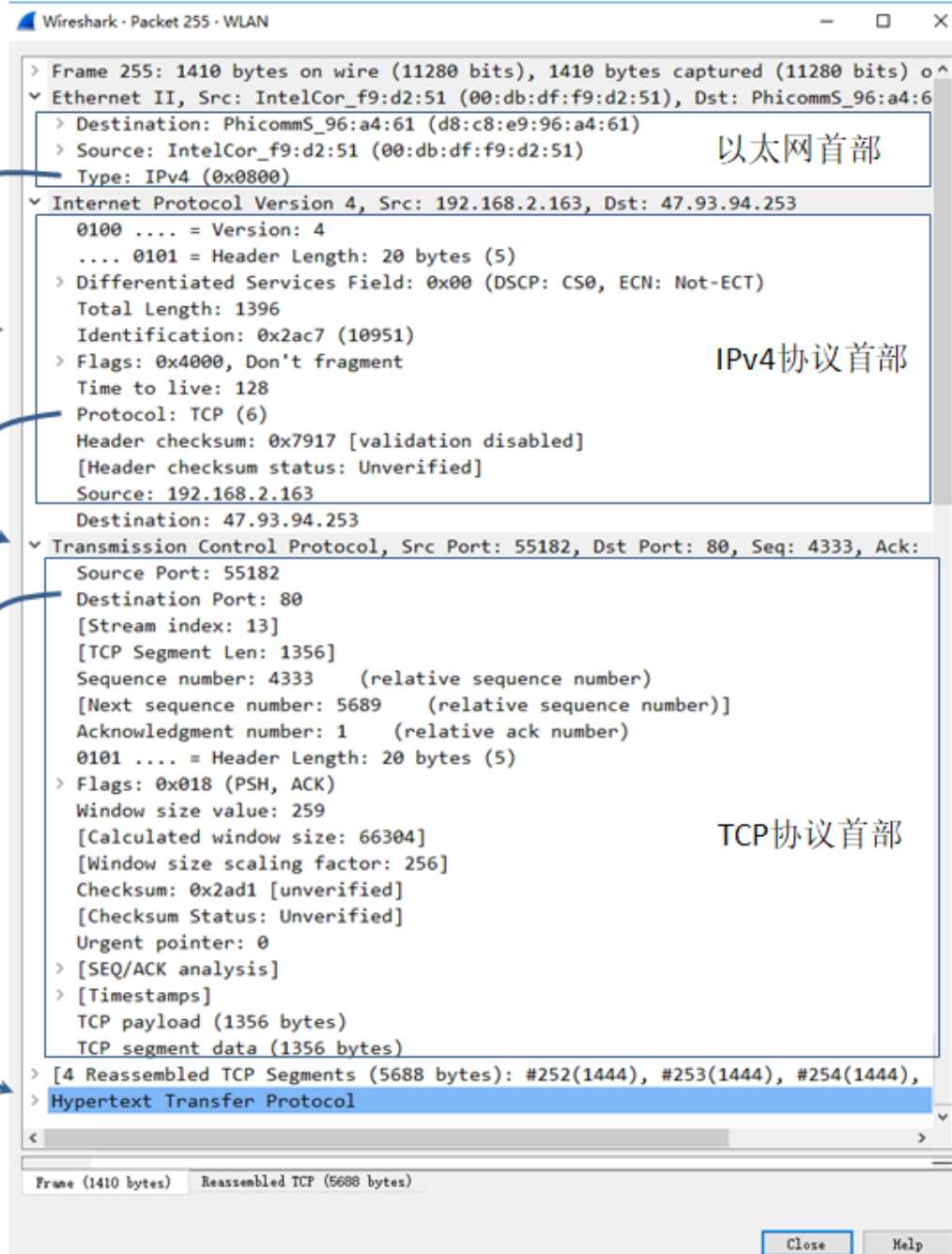
TCP/IP协议体系结构

■抓包分析TCP/IP协议体系结构。

以太网数据链路层
首部的Type字段标
明网络层是什么协议

IP协议首部的
Protocol字段标明
传输层是什么协议

TCP首部的Protocol
字段标明应用层是
什么协议



1.5 OSI参考模型

- 1.5.1 OSI参考模型和TCP/IP协议
- 1.5.2 OSI参考模型每层功能

1.5.1 OSI参考模型和TCP/IP协议

- OSI参考模型定义计算机通信每层的功能，不是协议。
- TCP/IP协议是具体的协议，实现了OSI参考模型规定的功能。

OSI参考模型	TCP/IP分层	TCP/IP协议组						本书按5层讲解
应用层 表示层 会话层	应用层	HTTP	FTP	SMTP	DNS	TFTP	DHCP	应用层
传输层	传输层	TCP		UDP				传输层
网络层	网络层	ARP	IP	ICMP		IGMP		网络层
数据链路层 物理层	网络接口层	CSMA/CD	HDCL	PPP	Frame Relay			数据链路层 物理层

1.5.2 OSI参考模型每层功能

- **应用层**，根据互联网中需要通信的应用程序的功能，定义客户端和服务端程序通信的规范，应用层向表示层发出请求。
- **表示层**，定义数据格式、是否加密或压缩。例如，**FTP**允许你选择以二进制或**ASCII**格式传输。如果选择二进制，那么发送方和接收方不改变文件的内容。如果选择**ASCII**格式，发送方将把文本从发送方的字符集转换成标准的**ASCII**后发送数据。在接收方将标准的**ASCII**转换成接收方计算机的字符集。
- **会话层**，它定义了如何开始、控制和结束一个会话，包括对多个双向消息的控制和管理，以便在只完成连续消息的一部分时可以通知应用，从而使表示层看到的数据是连续的。
- **传输层**，常规数据递送，面向连接或无连接。面向连接实现可靠传输，比如**TCP**协议，面向无连接，提供不可靠传输，比如**UDP**协议。
- **网络层**，根据网络地址为数据包选择选择转发路径。网络层为传输层提供服务，只是尽力转发数据包，不保证不丢包，也不保证按顺序到达接收端。
- **数据链路层**，数据链路层常简称链路层，两台主机之间的数据传输，总是在一段一段的链路上传送的，这就需要专门的链路层的协议。
- **物理层**，在物理层上所传输的数据单位是比特。发送方发送**1**（或**0**）时，接收方应该收到**1**（或**0**），而不是**0**（或**1**）。因此物理层要考虑用多大电压代表“**1**”或“**0**”，以及接收方如何识别出发送方所代表的比特。物理层还要确定连接电缆的的插头应当有多少根引脚以及各条引脚应如何连接。

1.6 理解OSI参考模型

- 1.6.1 IT人员工作在OSI参考模型的哪一层
- 1.6.2 理解表示层
- 1.6.3 抓包查看数据包内容
- 1.6.4 学以致用—传输层连接
- 1.6.5 网络设备和OSI七层模型
- 1.6.6 用分层的思想考虑问题
- 1.6.7 OSI参考模型与排错

1.6.1 IT人员工作在OSI参考模型的哪一层

- 程序员开发网络应用程序，他们负责解决应用程序之间如何通信，通信是否需要加密和压缩，避免出现乱码。从这个角度说程序员的工作是OSI参考模型的应用层、表示层和会话层
- 网络工程师，调试路由器和交换机，路由器属于网络层设备，交换机属于数据链路层设备，从这个角度说网络工程师工作是OSI参考模型的网络层和数据链路层。
- 通信工程师，专门研究如何在链路上如何更快的速率通信，其工作可以认为是OSI参考模型的物理层。



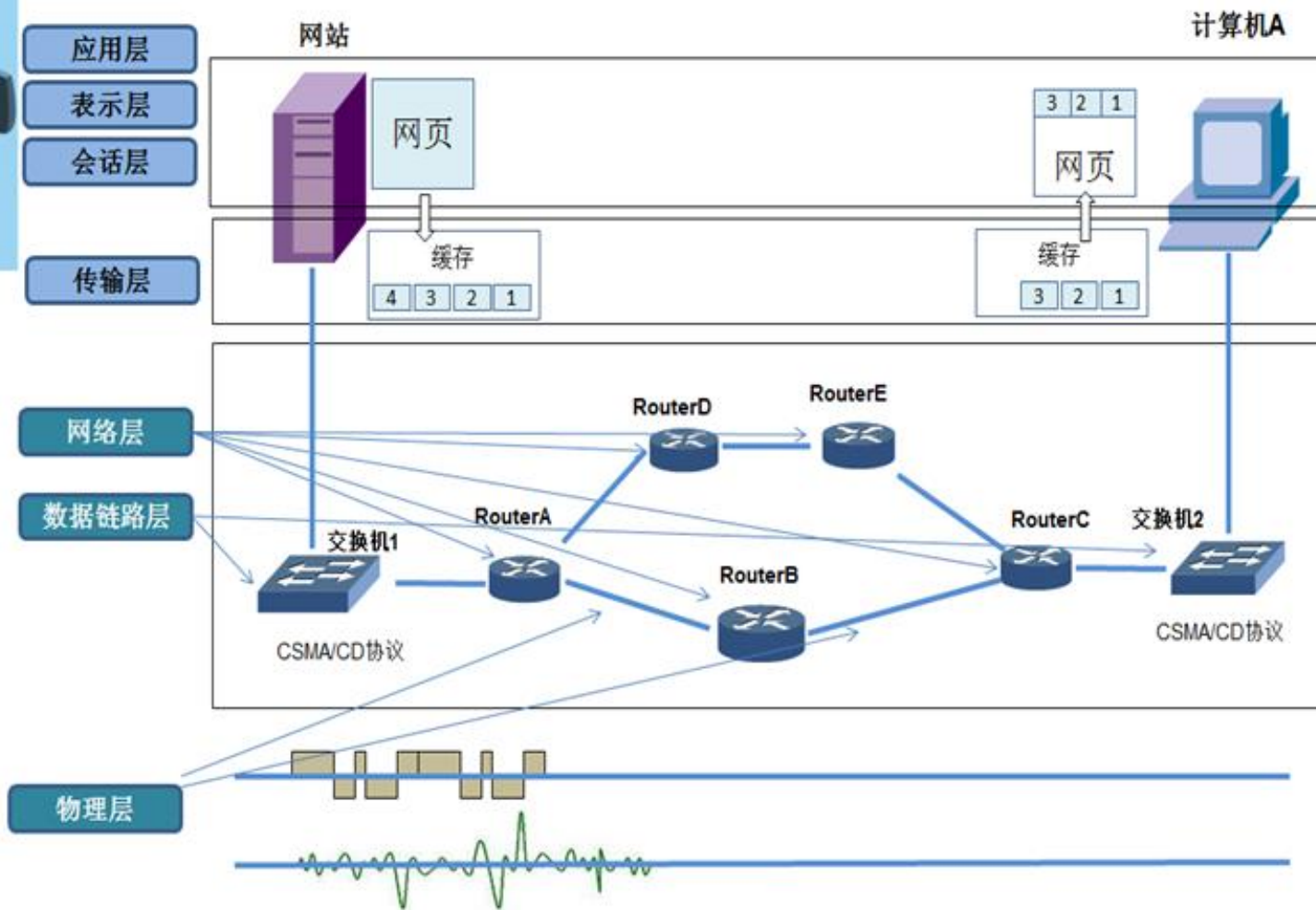
程序员



网络工程师



通信工程师



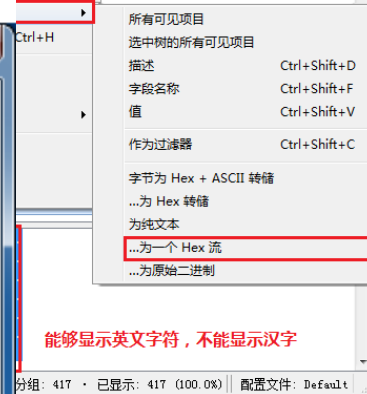
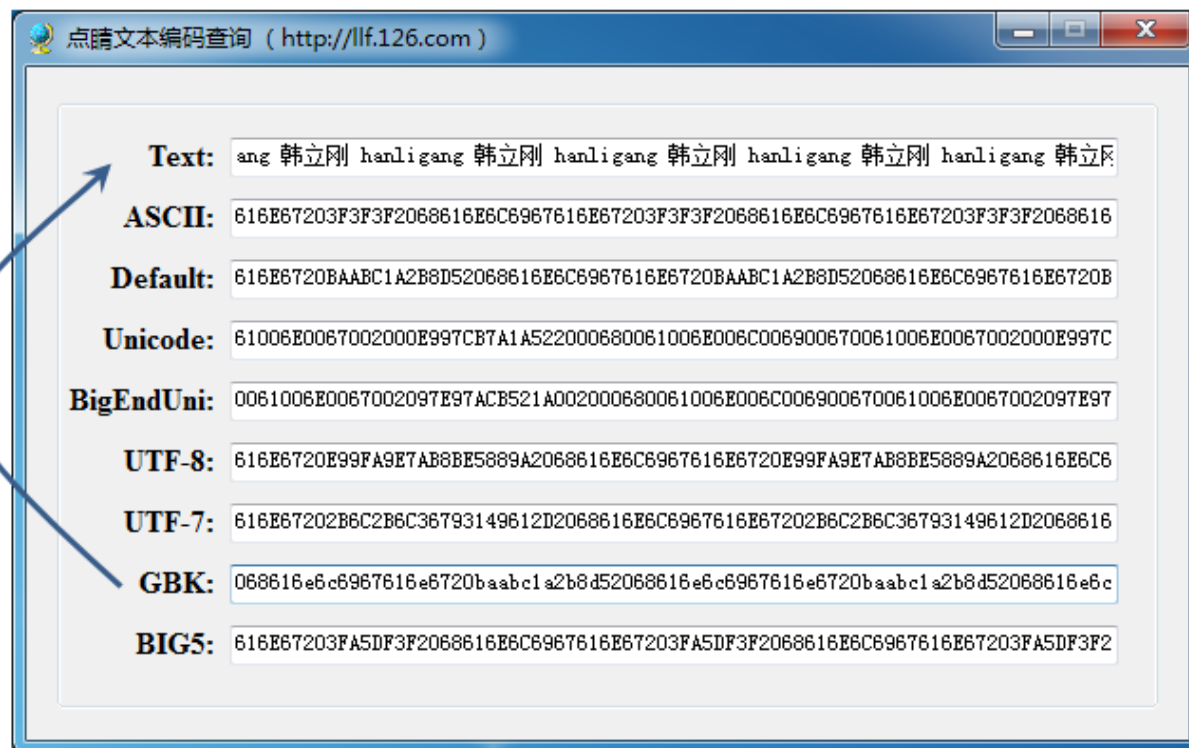
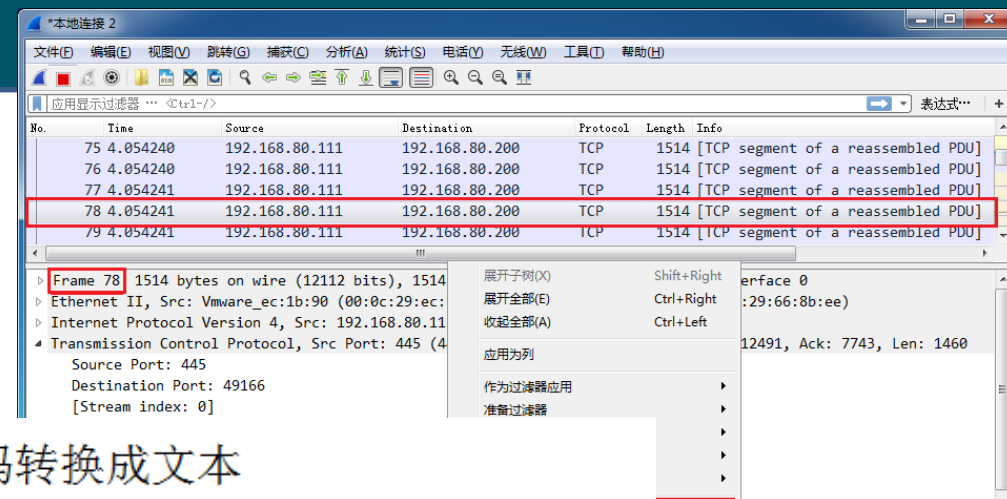
1.6.2 理解表示层

- 如果客户端和服务端程序交换数据，使用的字符集不一样，会出现乱码，这类故障就属于OSI参考模型的表示层故障。



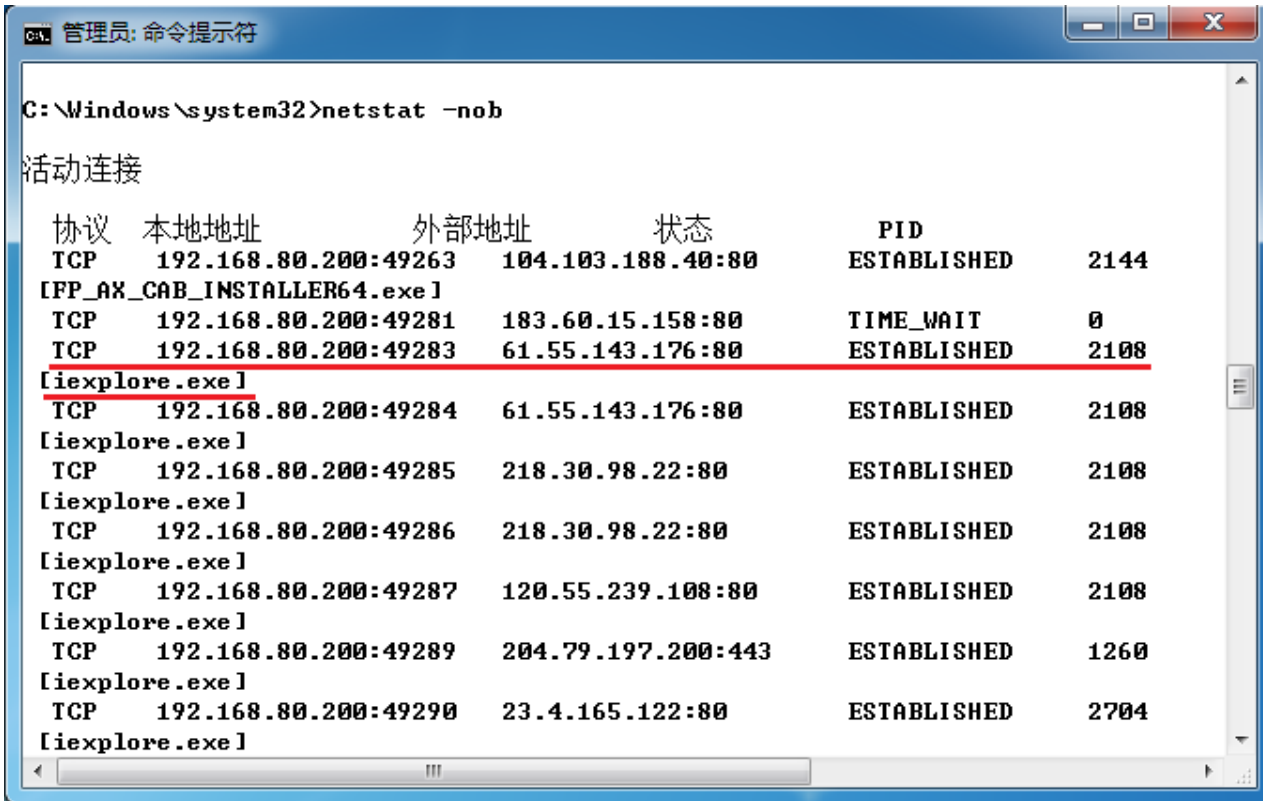
1.6.3 抓包查看数据包内容

■从Windows共享文件夹中拷贝字符集文件，其编码使用字符集是GBK字符集，将捕获的数据包的数据部分复制，拷贝到点睛文本编码查询，可以看到传输的数据，**GBK**字符集支持英文字符和汉字。



1.6.4 学以致用—传输层连接

- 传输层的TCP协议是可靠传输，通信的之前客户端需要服务器建立连接，通信结束释放连接。
- 使用netstat -nob可以查看计算机建立的TCP连接。
- 可以看到建立TCP连接的进程。
- 如果怀疑中了木马，可以根据建立的可以连接找到可以进程。进而查杀木马。



```
管理员: 命令提示符

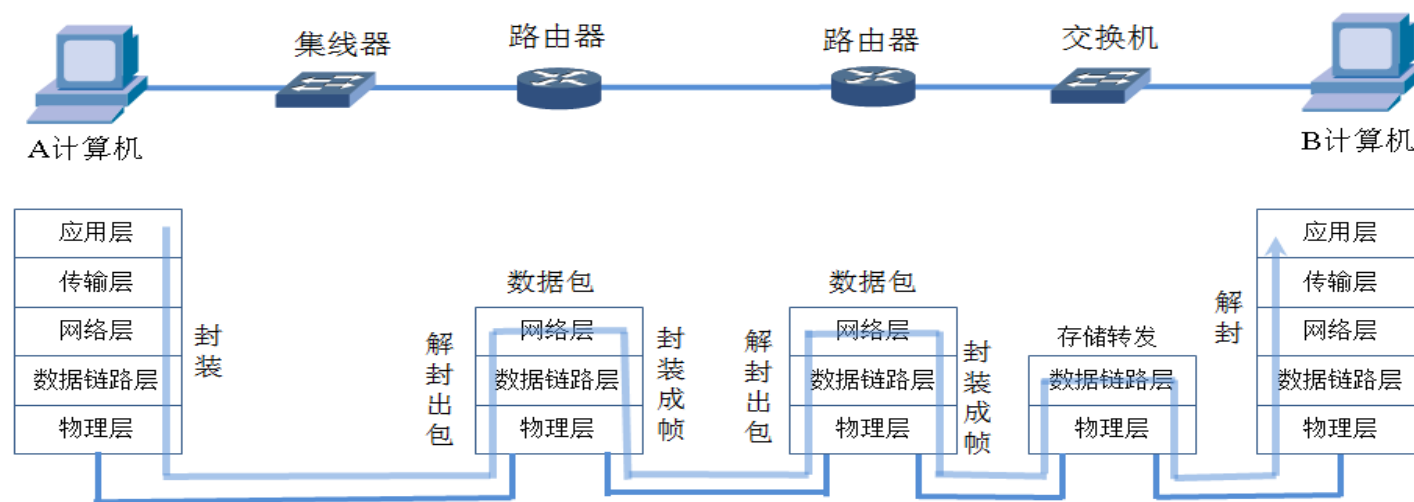
C:\Windows\system32>netstat -nob

活动连接

 协议 本地地址           外部地址           状态           PID
TCP    192.168.80.200:49263  104.103.188.40:80  ESTABLISHED    2144
[FP_AX_CAB_INSTALLER64.exe]
TCP    192.168.80.200:49281  183.60.15.158:80   TIME_WAIT      0
TCP    192.168.80.200:49283  61.55.143.176:80   ESTABLISHED    2108
[iexplore.exe]
TCP    192.168.80.200:49284  61.55.143.176:80   ESTABLISHED    2108
[iexplore.exe]
TCP    192.168.80.200:49285  218.30.98.22:80    ESTABLISHED    2108
[iexplore.exe]
TCP    192.168.80.200:49286  218.30.98.22:80    ESTABLISHED    2108
[iexplore.exe]
TCP    192.168.80.200:49287  120.55.239.108:80  ESTABLISHED    2108
[iexplore.exe]
TCP    192.168.80.200:49289  204.79.197.200:443 ESTABLISHED    1260
[iexplore.exe]
TCP    192.168.80.200:49290  23.4.165.122:80    ESTABLISHED    2704
[iexplore.exe]
```

1.6.5 网络设备和OSI七层模型

- 计算机工作在应用层、传输层和网络层，计算机的网卡工作在数据链路层和物理层。
- 集线器这种设备工作在物理层。
- 路由器接口工作在物理层和数据链路层，路由器根据IP首部转发数据包，所以说路由器工作在网络层。
- 交换机根据MAC地址转发帧，MAC地址属于数据链路层地址，所以交换机工作在数据链路层。当然交换机的接口也有物理层功能。

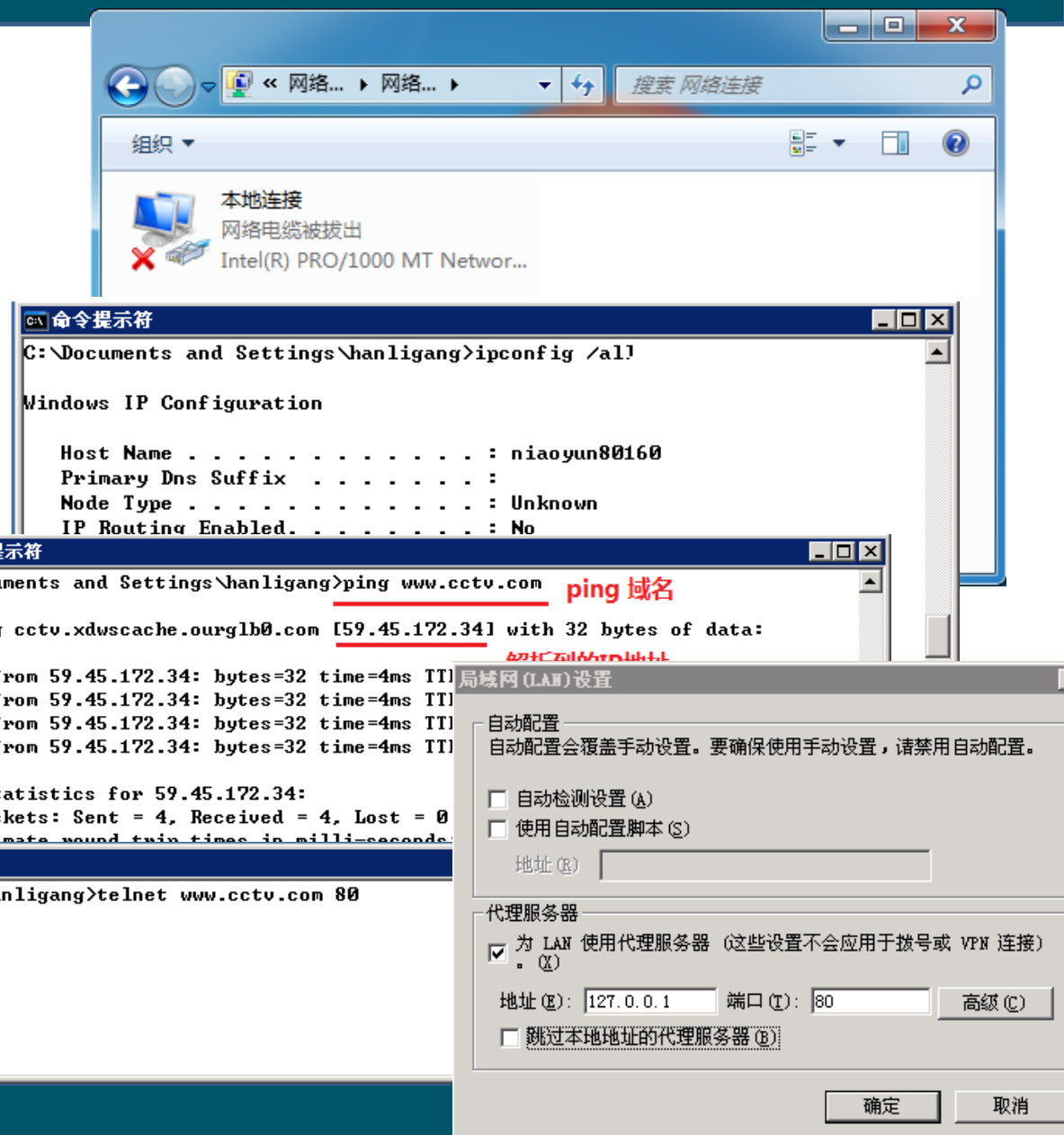


1.6.6 用分层的思想考虑问题

- 计算机通信按功能分层的好处就是当某一层有变换不会波及其他层。
- 比如单位的网络IP地址重新规划，不会影响企业内外的服务的访问。
- 要实现这个分层，就不要再在应用层包含网络层的信息，比如开发的客户端程序连接服务器就不要写服务器的IP地址，而是写服务器的名称。如果将服务器的IP地址写进应用程序，就没有采纳OSI参考模型的分层思想。网络一旦调整，就需要修改客户端程序。这就是网络层变换引起应用层变化了。

1.6.7 OSI参考模型与排错

- OSI参考模型中底层为其上层提供服务，因此排除网络故障也应该从底层到高层依次排查。
- 先检查物理层，也就是网线是否接好。
- 再检查数据链路层，比如MAC地址是否冲突，计算机是否接入了正确的VLAN。
- 再检查网络层，输入Ipconfig /all查看IP地址、子网掩码、网关、DNS是否设置正确。
- 再ping Internet上的网站域名，测试域名解析是否正常。
- 测试时应用层，telnet 服务对应的端口，看看是否能够成功。
- 检查应用层，看看客户端软件的配置是否正确。

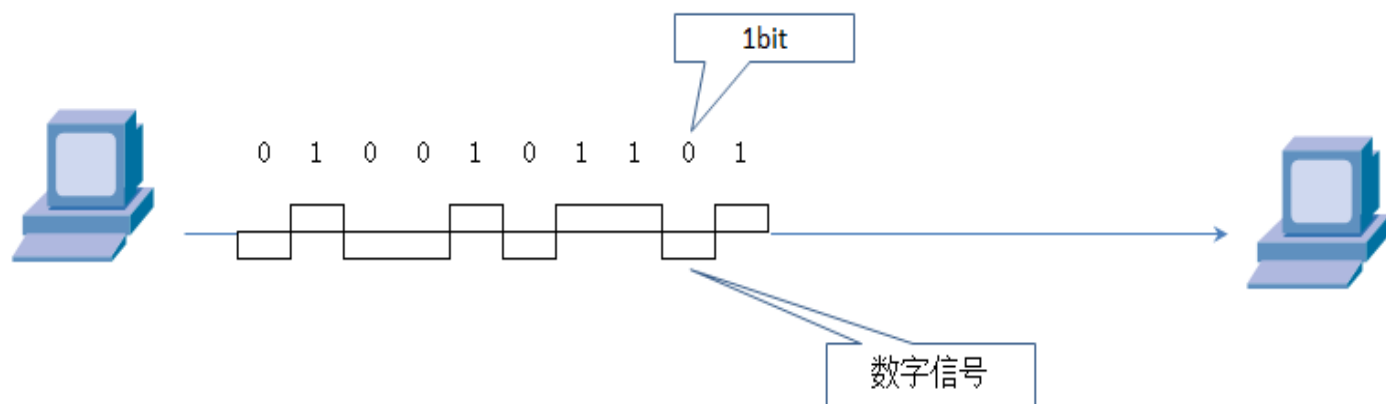


1.7 计算机网络的性能指标

- 1.7.1 速率
- 1.7.2 带宽
- 1.7.3 吞吐量
- 1.7.4 时延
- 1.7.5 时延带宽积
- 1.7.6 往返时间
- 1.7.7 利用率

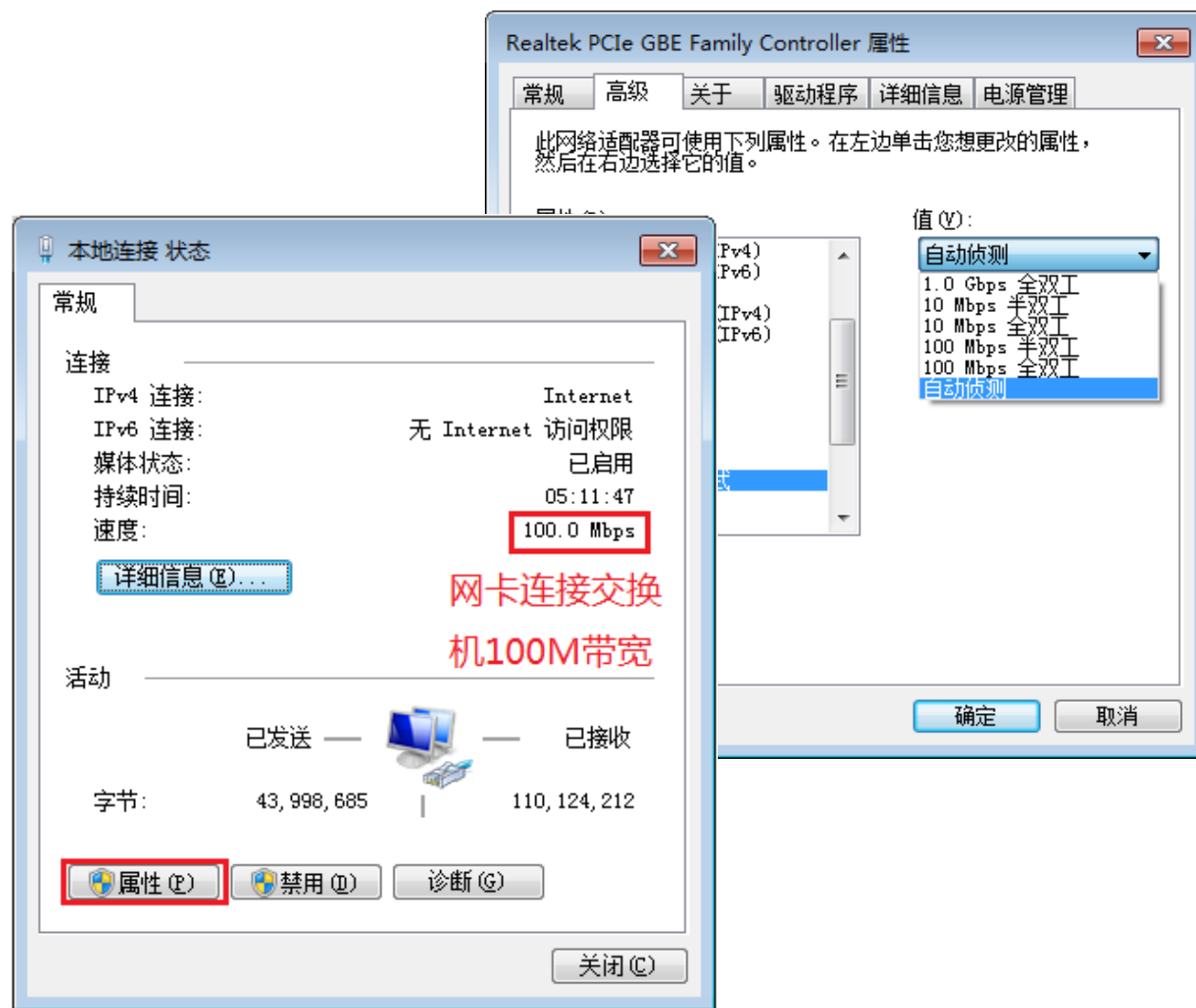
1.7.1 速率

- 网络技术中的速率指的是每秒钟传输的比特数量，称为数据率（data rate）或比特率（bit rate），速率的单位为b/s（比特每秒）或bit/s，有时也写为bps，即bit per second。当速率较高时，就可以用kb/s（k=103=千）、Mb/s（M=106=兆）、Gb/s（G=109=吉）或Tb/s（T=1012=太）。现在人们习惯于用更简洁但不严格的说法来描述速率，比如10M网速，而省略了单位中的b/s。
- Windows操作系统中，速率以字节为单位。大写的B代表字节，是byte的缩写，8比特=1字节。
- 速率是指的一个发端一个接收端平均每秒中发送多少bit。



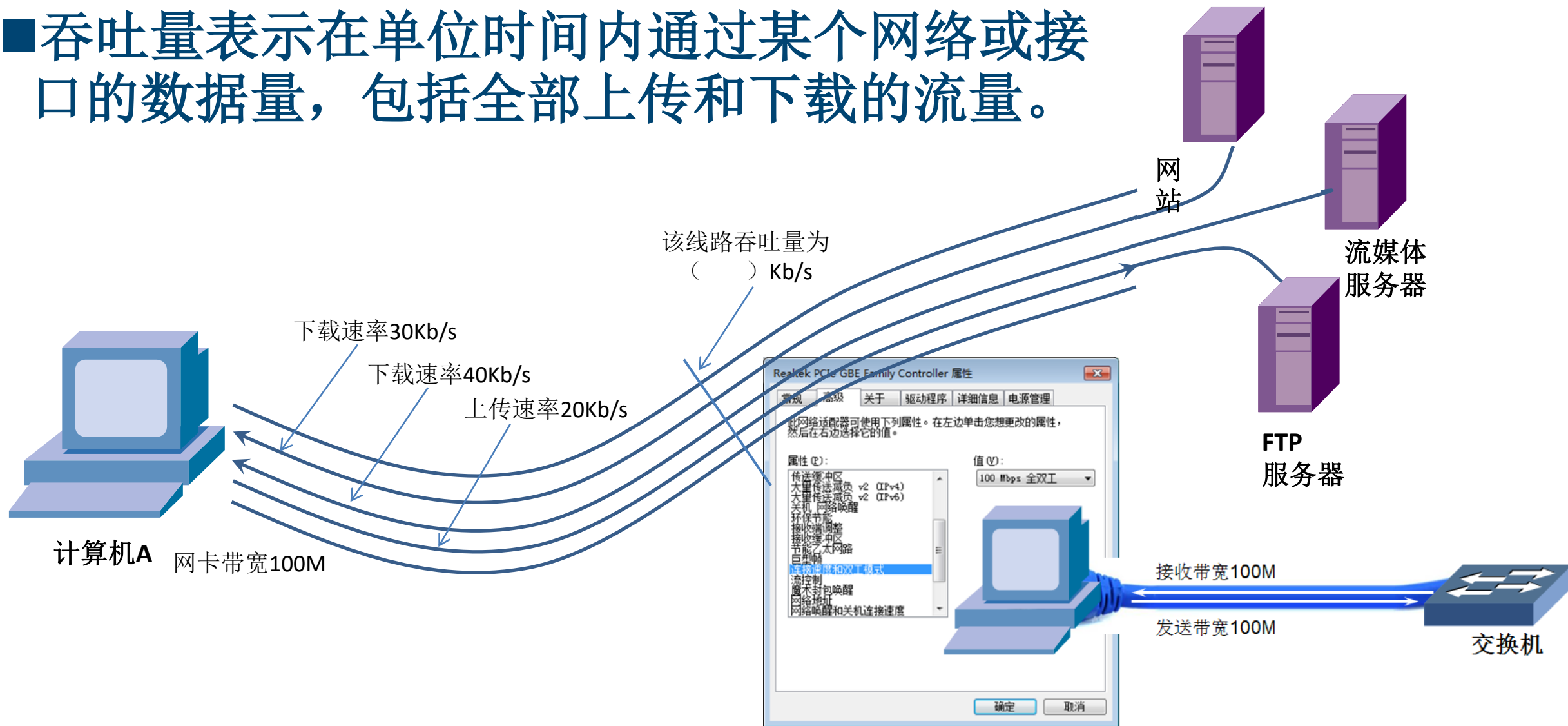
1.7.2 带宽

- 在计算机网络中，带宽用来表示网络通信线路传输数据的能力，即最高速率。
- 可以设置电脑网卡的带宽。



1.7.3 吞吐量

■ 吞吐量表示在单位时间内通过某个网络或接口的数据量，包括全部上传和下载的流量。



1.7.4 时延

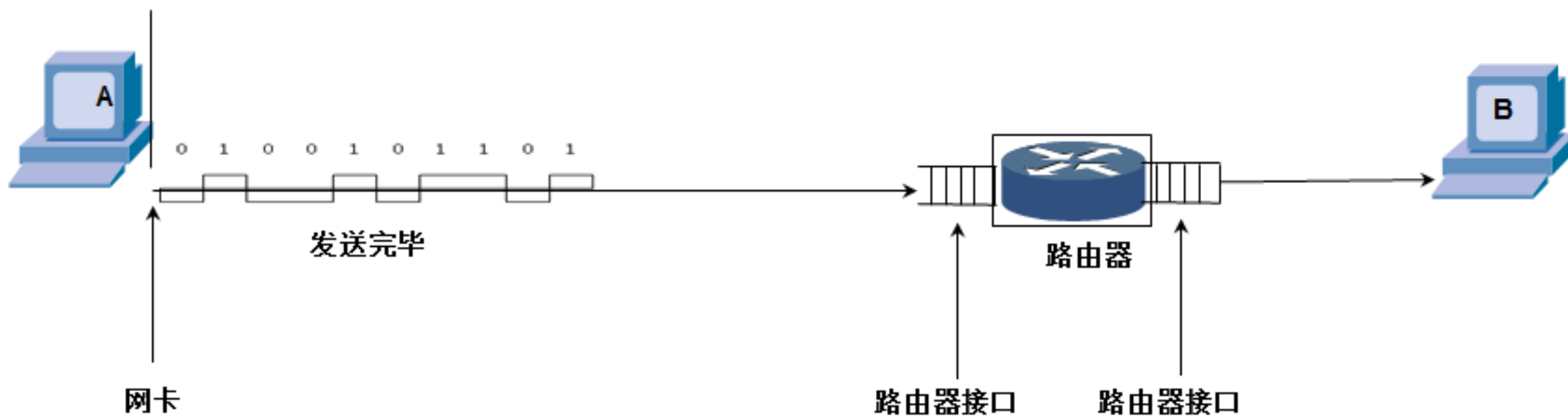
■时延（**delay**或**latency**）是指数据（一个数据包或bit）从网络的一端传送到另一端所需要的时间。时延是一个很重要的性能指标，有时也称为延迟或迟延。



(1) 发送时延

- 发送时延 (transmission delay) 是主机或路由器发送数据帧所需时间，也就是从发送数据帧的第一个比特开始，到该帧最后一个比特发送完毕所需要的时间。下图表示数据流发送完毕。

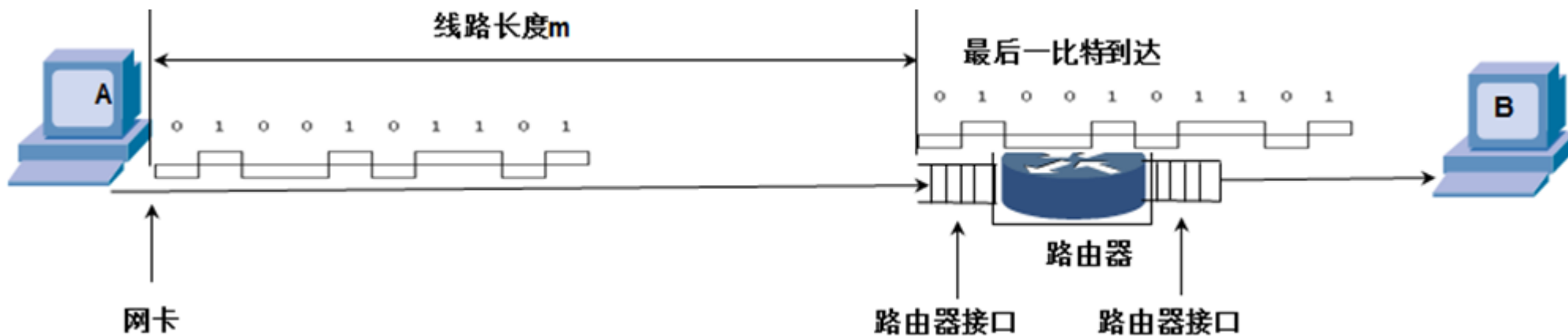
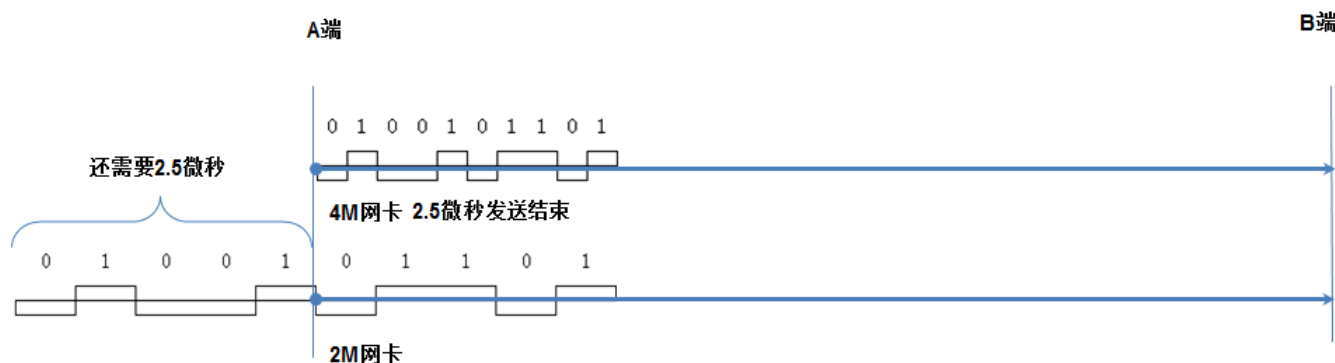
$$\text{发送时延} = \frac{\text{数据帧长度 (b)}}{\text{发送速率 (b/s)}}$$



(2) 传播时延

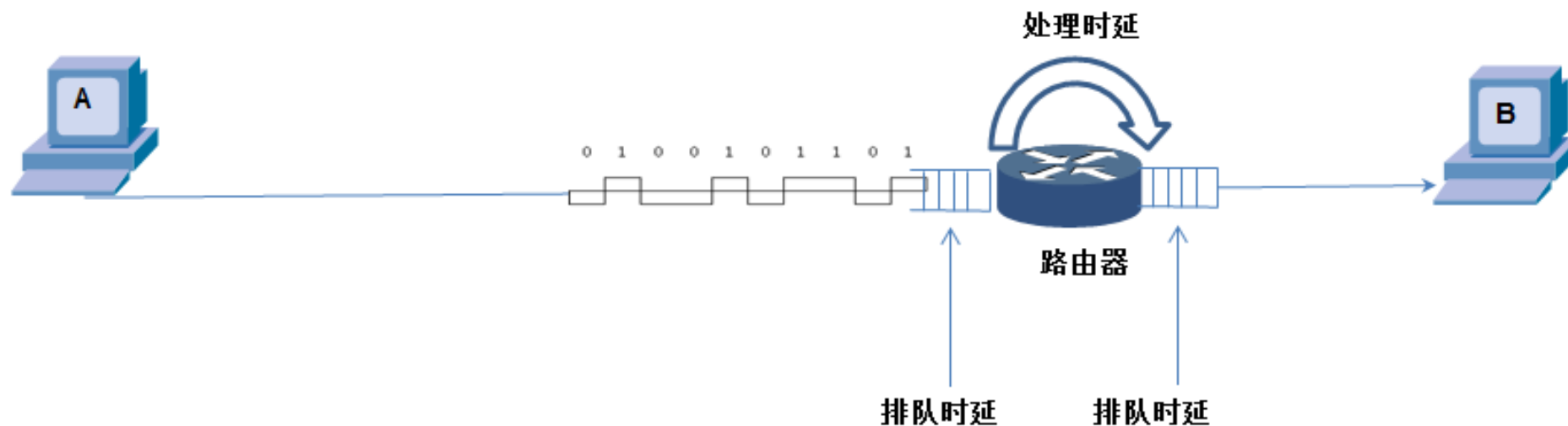
- 传播时延 (propagation delay) 是电磁波在信道中传播一定的距离需要花费的时间。如下图所示，从最后一比特发送完毕到最后一比特到达路由器接口需要的时间就是传播时延。

$$\text{传播时延} = \frac{\text{信道长度 (m)}}{\text{电磁波在信道上的传播速率 (m/s)}}$$



(3) 排队时延

- 分组在经过网络传输时，要经过许多的路由器。但分组在进入路由器后要先在输入队列中排队等待处理。

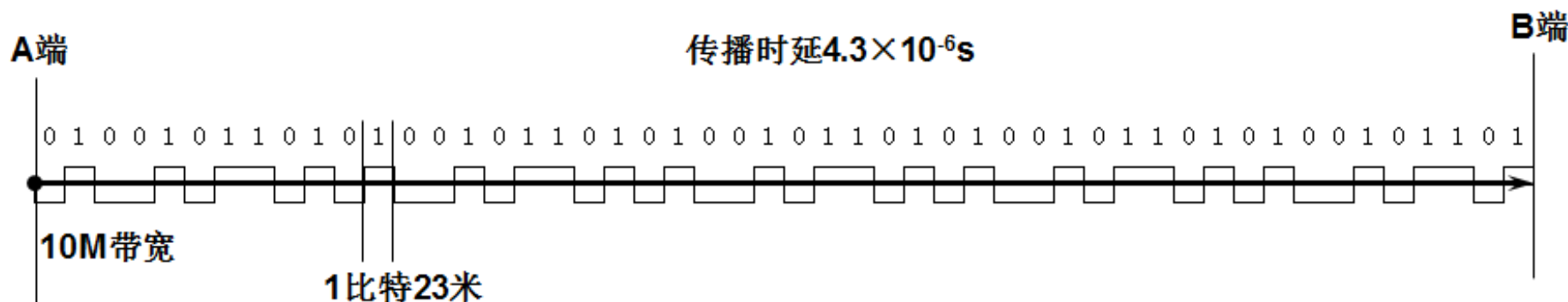


(4) 处理时延

- 路由器或主机在收到数据包时，要花费一定时间进行处理，例如分析数据包的首部、进行首部差错检验，查找路由表为数据包选定转发出口，这就产生了处理时延。
- 数据在网络中经历的总时延就是以上四种时延的总和。
- $\text{总时延} = \text{发送时延} + \text{传播时延} + \text{处理时延} + \text{排队时延}$

1.7.5 时延带宽积

- 把链路上的传播时延和带宽相乘，就会得到时延带宽积。这对我们以后计算以太网的最短帧非常有帮助。
- 时延带宽积=传播时延×带宽



1.7.6 往返时间

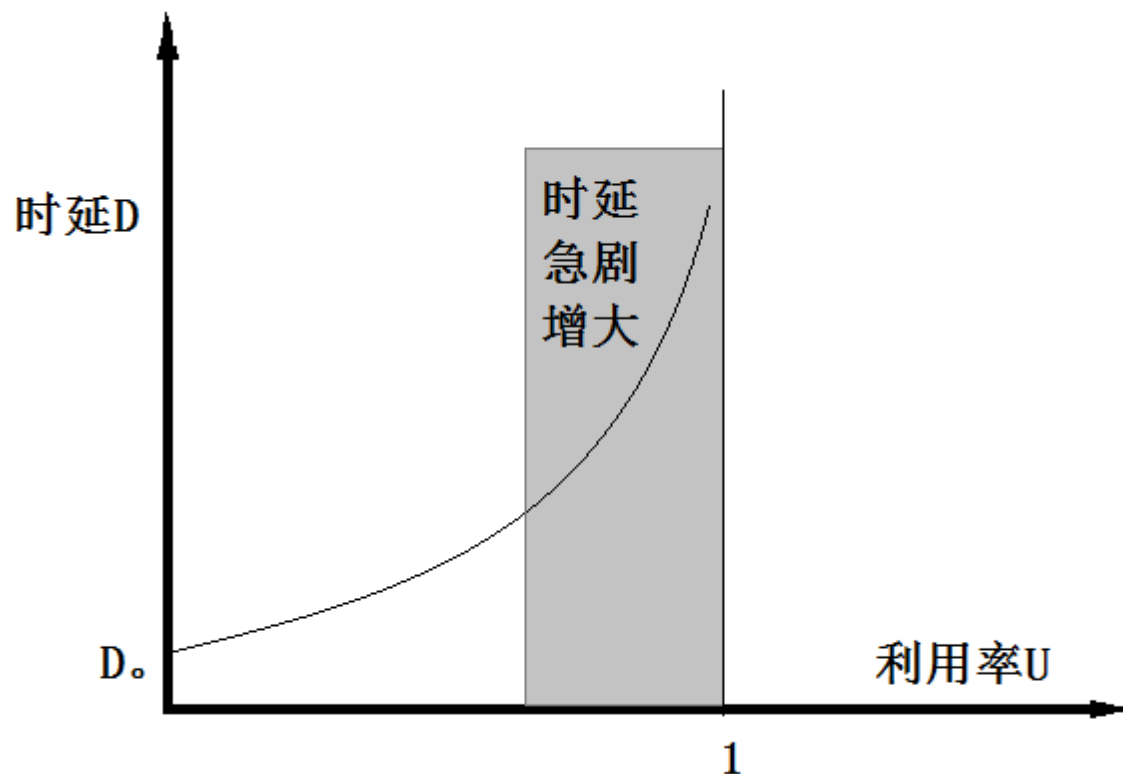
- 在计算机网络中，往返时间RTT（Round-Trip Time）也是一个重要的性能指标，它表示从发送端发送数据开始，到发送端接收到来自接收端的确认（发送端收到后立即发送确认），总共经历的时间。
- 往返时间带宽积，可以用来计算当发送端连续发送数据时，接收端如发现有错误，立即向发送端发送通知使发送端停止，发送端这段时间发送的比特量。

```
C:\Windows\system32\cmd.exe
C:\Users\han>ping 10.7.10.1                ping 网关
正在 Ping 10.7.10.1 具有 32 字节的数据:
来自 10.7.10.1 的回复: 字节=32 时间=1ms TTL=64
来自 10.7.10.1 的回复: 字节=32 时间=1ms TTL=64
来自 10.7.10.1 的回复: 字节=32 时间=1ms TTL=64
来自 10.7.10.1 的回复: 字节=32 时间<1ms TTL=64
10.7.10.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 1ms, 平均 = 0ms
C:\Users\han>ping www.cctv.com            ping 国内网站
正在 Ping cctv.xdwscache.ourglb0.com [211.142.22.114] 具有 32 字节的数据:
来自 211.142.22.114 的回复: 字节=32 时间=12ms TTL=55
来自 211.142.22.114 的回复: 字节=32 时间=12ms TTL=55
来自 211.142.22.114 的回复: 字节=32 时间=15ms TTL=55
来自 211.142.22.114 的回复: 字节=32 时间=13ms TTL=55
211.142.22.114 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 12ms, 最长 = 15ms, 平均 = 13ms
C:\Users\han>ping www.microsoft.com      ping 美国网站
正在 Ping e10088.ca2.s.tl88.net [96.7.101.129] 具有 32 字节的数据:
来自 96.7.101.129 的回复: 字节=32 时间=41ms TTL=50
来自 96.7.101.129 的回复: 字节=32 时间=41ms TTL=50
来自 96.7.101.129 的回复: 字节=32 时间=40ms TTL=50
来自 96.7.101.129 的回复: 字节=32 时间=40ms TTL=50
96.7.101.129 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 40ms, 最长 = 41ms, 平均 = 40ms
C:\Users\han>
```

1.7.7 利用率

- 利用率是指网络有百分之几的时间是被利用的（有数据通过），没有数据通过的网络利用率为零。网络利用率越高，数据分组在路由器和交换机处理时就需要排队等待，因此时延也就越大。下面的公式表示网络利用率和延迟之间的关系。

$$D = \frac{D_0}{1 - U}$$



1.8 网络分类

- 1.8.1 按网络的范围进行分类
- 1.8.2 按网络的使用者进行分类

1.8.1 按网络的范围进行分类

- **局域网（Local Area Network, LAN）** 是在一个局部的地理范围内（如一个学校、工厂和机关内），一般是方圆几千米以内，将各种计算机、外部设备和数据库等互相连接起来组成的计算机通信网。
- **广域网（Wide Area Network, WAN）** 通常跨接很大的物理范围，所覆盖的范围从几十公里到几千公里，能连接多个城市或国家，或横跨几个洲并能提供远距离通信，形成国际性的远程网络。
- **城域网（Metropolitan Area Network, MAN）** 的作用范围一般是一个城市，可跨越几个街区甚至整个城市，其作用距离约为5~50km。城域网可以为一个或几个单位所拥有，但也可以是一种公用设施，用来将多个局域网进行互连。目前很多城域网采用的是以太网技术，因此有时也将其并入局域网的范围进行讨论。
- **个人区域网（Personal Area Network, PAN）** 就是在个人工作的地方把属于个人使用的电子设备（如便携式电脑等）用无线技术连接起来的网络，因此也常称为无线个人区域网（Wireless PAN, WPAN），比如无线路由器组建的家庭网络，就是一个PAN，其范围大约在几十米左右。

1.8.2 按网络的使用者进行分类

- 公用网（**public network**）是指电信公司（国有或私有）出资建造的大型网络。“公用”的意思就是所有愿意按电信公司的规定交纳费用的人都可以使用这种网络。因此公用网也可称为公众网，因特网就是全球最大的公用网络。
- 专用网（**private network**）是某个部门为本单位的特殊业务工作需要而建造的网络。这种网络不向本单位以外的人提供服务。例如，军队、铁路、电力等系统均有本系统的专用网。
- 公用网和专用网都可以传送多种业务。如传送的是计算机数据，则分别是公用计算机网络和专用计算机网络。

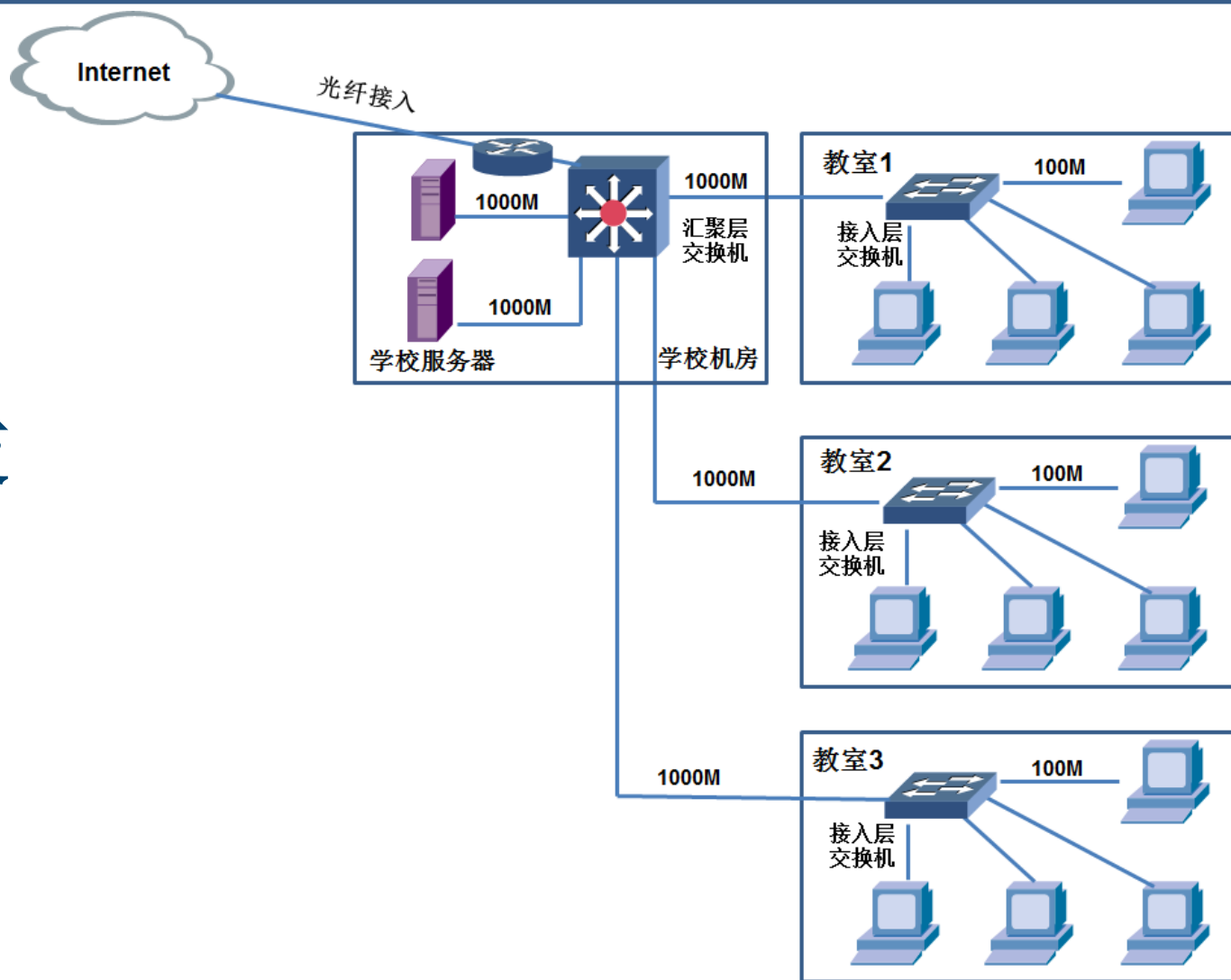
1.9 企业局域网设计

■1.9.1 二层结构的局域网

■1.9.2 三层结构的局域网

1.9.1 二层结构的局域网

- 接入层连接计算机
- 汇聚层连接接入层交



1.9.3 三层结构的局域网

- 接入层
- 汇聚层
- 核心层

