应用层协议原理

写出能够运行在不同端系统和通过网络彼此通信的程序。

网络应用程序体系结构

- C/S结构
  - 有一个总是打开的主机,具有固定的IP(服务器)
  - 主机不能响应所有客户的请求，需要为大量主机配置数据中心
- P2P体系结构
  - 自扩展性
  - 互联的双方是对等的

应用层协议

应用	应用层协议	支撑的运输层协议
电子邮件	SMTP	TCP
远程终端访问	Telnet	TCP
Web	HTTP	TCP
文件传输	FTP	TCP
流式多媒体	HTTP	TCP
因特网电话	SIP,RTP或专用的	UDP或TCP

应用层协议定义了运行在不同端系统上的应用程序进程如何相互传递报文。特别是应用程序定义了:

- 交换的报文类型
- 各种报文类型的语法
- 字段的语义
- 一个进程何时以及如何发送报文，对报文进行响应的规则

超文本传输协议(HyperText Transfer Protocol,HTTP)

HTTP由两个程序实现，一个客户端程序，一个服务端程序。客户程序和服务器程序运行在不同的端系统中，通过交换报文进行会话。HTTP定义了这些报文的结构以及客户和服务器进行报文交换的方式。

HTTP服务器不保存关于客户的任何信息，所以它是一种无状态协议。

- 非持续连接
  - 每个请求/响应对是由单独的TCP连接发送
- 持续连接
  - 所有请求/响应对由相同的TCP连接发送

正确理解持续连接与HTTP的无状态

持续连接会保持连接一段时间，超时后会断开TCP连接，所以持续连接的目的是提高连接的利用率以响应同一个客户端的持续请求。

HTTP的无状态是针对请求/响应对来说的，HTTP要求遵循该规范的应用程序不会记住请求/响应状态，就好比某一次请求要用到之前请求的某个状态的时候，服务器找不到该状态，只会重传.

这与持续连接是两码事.

文件传输协议(File Transfer Protocol,FTP)

FTP使用两个TCP连接来传输文件，一个是控制连接，一个是数据连接.

- 控制连接
  - 用于在两主机之间传输控制信息
  - 控制连接保持在整个用户会话期间
- 数据连接
  - 用于实际发送一个文件
  - 会话期间，每一次发送文件都要重新建立连接　　FTP服务器必须在整个会话期间保留用户的状态。比如用户当前所在的目录，维护远程文件目录树等.

简单邮件传输协议(Simple Mail Transfer Protocol,SMTP)

电子邮件

电子邮件系统由用户代理，邮件服务器，简单邮件传输协议三部分组成。

邮件的发送从发送方的用户代理开始， 传输到发送方的邮件服务器，再传输到接收方的邮件服务器，然后从接收方的邮件服务器分发到接收方的邮箱中。接收用户可以从他的邮件服务器中读取该邮件。

如果接收方的邮件服务器故障，那么发送方邮件服务器会将该邮件滞留，过一段时间再尝试重新发送，一般是30分钟一次，如果几天后都没有成功，则通知发送方发送失败，并且删除该邮件。

SMTP

SMTP的传输层使用TCP连接，在发送方服务器和接收方服务器之间建立传输层连接之后，会进行一系列应用层握手。

握手过程由双方互相问好，发送方服务器向接收方陈述发送方邮箱和接收方邮箱，然后通过一个MALL FROM指令开始发送邮件，以一个句点表示结束指令。

QUIT表示发送完毕。接收方服务器收到QUIT后断开连接.

HTTP与SMTP的比较

- 二者都是持续连接
- HTTP是一个拉协议，而SMTP是一个推协议
- HTTP对报文的字符没有限制，SMTP要求发送的报文是7比特ASCII字符（可见字符）
- HTTP把每个对象封装到自己的报文中，而SMTP则把所有报文对象放在一个报文之中

域名系统(Domain Name System,DNS)

提供主机名到IP地址转换的服务.这就是域名系统.

DNS是拥有分层的DNS服务器实现的分布式数据库，一个使得主机能够查询分布式数据库的应用层协议。

DNS服务器通常是运行BIND软件的UNIX机器。DNS由UDP提供传输层支持，使用53号端口.

除了进行主机名到IP地址的转换外，DNS还提供了一些重要的服务:

- 主机别名
  - 主机别名比规范的主机名更容易记忆
- 邮件服务器别名
  - 邮件服务器名也比规范的邮件服务器名更好记忆
- 负载分配

- DNS也用于在冗余的服务器之间进行负载分配，采用的方法通常是轮询法
- 不采用集中式分布的原因:
  - 单点故障：DNS崩溃，整个因特网都完蛋
  - 通信容量：单个DNS不得不处理所有的DNS查询
  - 远距离的集中式数据库：单个DNS服务器不可能"邻近"所有查询客户
  - 维护：单个DNS服务器将不得不为所有的因特网主机保留记录

DNS工作机理概述

DNS采用分布式，层次数据库,逐层向下分为:

- 根DNS服务器：提供安全性和可靠性
- 顶级域服务器：负责顶级域名的查询，如com,org,gov,edu,net等
- 权威DNS服务器：将主机名字映射为IP地址，这些服务器由专门的组织机构提供和维护

DNS记录

资源记录(Resource Record,RR)提供了主机名到IP地址的映射。每个DNS回答报文中包含了一条或多条资源记录.
资源记录的格式如下:

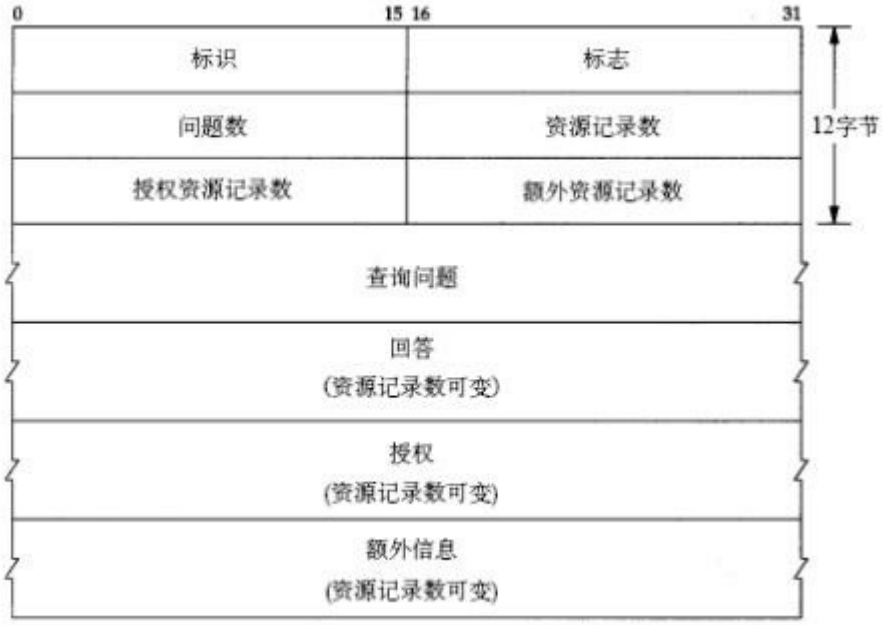
(Name,Value,Type,TTL)

Name和Value取决于Type,TTL是该记录的生存时间，它决定了资源记录应当从缓存中删除的时间。
Type类型:

- A记录
  - Name-Value对应主机名-IP
- NS记录
  - Name-Value对应域-权威服务器
  - 这种记录表示，要查询这个域(Name)，要从这个权威服务器(Value)中查询
- CNAME记录
  - Name-Value对应别名-规范主机名
- MX记录
  - Name-Value对应邮件服务器别名-规范主机名

DNS报文

DNS报文格式如下图:



* 前12字节是首部区域 * 标识字段是一个16 bits的数，用于标识该查询 * 标志字段有若干1bit标志，如查询报文(0)/回答(1) * 剩下四个是有关数量的字段 * 问题区域包含着正在进行的查询信息 * 名字字段：表明正在被查询的主机名字 * 类型字段：指出有关该名字的正被询问的问题类型 * 回答区域包含了对最初请求的名字的资源记录 * 回答报文的回答区域中可以包含多条资源记录，因此一个主机名能够有多个IP地址 * 权威区域包含了其他权威服务器的记录 * 附加区域包含了其他有帮助的记录 * 例如，一条MX请求的回答报文中在该区域附加了一个A类型的记录，包含该规范主机名的IP地址

Author:寒江雪

Date:2017.10.18