1 概览

1.1 Internet的发展史

TCP/IP

DNS

WWW

GII NII

NGI

FIND

VoIP

1.2 中国Internet的发展史

NCFC

FDDI

CNNIC

1.3 IPv6发展史

ITU

ISO

OSI

IEEE

IETF

IRTF

2 结构与模型

2.1 网络的构成

LAN

WiFi

RFC

UWB

ISP

ATM

网络的构成

端系统-收发, 链路-传输, 交换系统-转发

功能上分

主干网

接入网

协议上分

个域网

无线网

Bluetooth、ZigBee、UWB

局域网

有线网：Ethernet

无线网：WiFi

广域网 a

X.25、ATM

连接方式上分

广播型网络(共享媒体型)

点对点网路(交换型)

2.2 网络体系结构

SDU

PDU

PCI

SAP

O**SI**

PDU PCI SDU 三者关系

服务特点

面向连接: 可靠, 按顺序, 占用资源

非连接: 独自寻路, 可能顺序颠倒

ISO-OSI模型：7个层次

TCP/IP模型：4个层次

相互之间对应关系

3 物理层(通用)

3.1 通信基础

存储中 1k= 通信中 1k=

Nyquist定理 运用场景 公式

Shannon定理 运用场景 公式

3.3 数字调制与多路复用

FDM

TDM

CDM

WDM

CDMA

3.4 交换技术

电路交换

如传统电话网络

存储交换

报文交换, 如电报网络, 深空通信网a

分组交换

数据报交换网络, 如IP网络

无连接分组交换

虚电路网络, 如ATM网络

面向连接的分组交换

延时分析

4 数据链路层的点对点链路

4.1 数据链路层的基本概念与功能

MAC

ARQ

FEC

HEC

链路 分为两种

数据链路层 功能

向网络层提供良好服务接口

无确认无连接的服务(有线局域网)

有确认无连接的服务(无线局域网)

面向连接的服务(无线城域网a)

将物理层的比特流编辑成帧

差错控制与可靠性a

ARQ、FEC、HEC 各自的工作机理

流量控制

产生原因

解决方法

介质访问控制(局域网)

MAC与LLC子层

4.2 差错检测与纠正

CRC

FCS

检错码+确认重传

奇偶校验、改进的奇偶校验、CRC 、Checksum 各自的原理及算法

纠错码

Haming码 原理及算法

检dbit错, 需用最小距离d+1的编码

纠dbit错, 需用最小距离2d+1的编码

4.3 基本数据链路协议

停等协议

4.4 滑动窗口协议

带宽延迟乘积BD=单向延迟\*带宽, 链路利用最大值是2BD+1

回退N协议(出错全部重发协议

W\_T< W\_R=

选择重发协议

W\_T>1, W\_R>1

W\_R<

5 数据链路层的点对多点链路

5.1 传统LAN基本概念

LLC

局域网是小区域内数据通信互联的信息网

两个协议以及对应网络

OSI的数据链路层相当于IEEE802的MAC和LLC层, LLC在MAC之上

MAC子层

负责对共享介质访问进行控制、差错校验、不同的MAC子层a有相同的LLC子层, MAC子层针对不同类型局域网不同

LLC子层

对所有局域网都相同的a

定义了两个用户交换数据机制a

流量控制

提供服务

5.2 多路访问协议

CSMA

DCF

PCF

CD

CA

RTS

CTS

IFS

NAV

广播信道的分配问题

静态分配 例如TDM、FDM

动态分配

随机访问

有了就发, 有冲突再解决

适用于负载轻的网络

如Aloha, CSMA

控制访问

取得发送权再发, 避免冲突

适用于负载重的网络, 信道利用率很高

主要有轮询和预约两种方式

如802.11的PCF模式

Aloha协议

集中式

两个版本

纯Aloha

时隙Aloha

CSMA协议

讲前先听

非坚持式

1-坚持式

p-坚持式(时隙信道)

CSMA/CD

存在问题；不适用于

二进制指数退避算法

CSMA/CA

DCF PCF之间的关系

基本过程

扩展过程(绝大多数802.11都支持)

5.4 WLAN的MAC协议(802.11)

5.5 网桥

STP

功能

局域网的互联设备, 在数据链路层工作

转发数据帧, 必要时转换帧格式(不能存储)

可以隔离碰撞域, 不能隔离广播域

丢弃出错帧

6 网络层

6.1 网络层向传输层提供的服务

6.2 数据报与虚电路

VC

VCI

LCN

OSI网络层提供两种服务

数据报, 无连接

特点

有转发表来确定分组转发

寻路独立, 可合理利用网络资源

可能先发后到

网络风暴->生存时间限制

虚电路, 面向连接

发出连接请求, 建立连接, 通信, 拆除连接

每个分组只需携带链路范围有效的VCI, 能标识自己的VC即可

特点

建立连接时就已分配资源, 带宽独占, 延时预设定, 质量有保证

一条虚电路可对应多条逻辑信道

由逻辑信道级联形成, 会占用节点缓存器的一个储存空间

有效防止拥塞

6.3 路由算法

DV

LS

DVR

RIP

OSPF

IGRP

SPF

IGP

EGP

AS

算法有两类, 非自适应和自适应

非自适应

静态路由, 路由表固定

简便可靠易行

适用于拓扑结构稳定或变化不大的网络以及用户主机

自适应

动态路由, 根据路由协议定时刷新路由表

算法复杂, 会增加网络负担, 但能根据网络状态动态调整路由表

适用于路由器

自适应路由算法有两类, 距离矢量算法和链路状态算法

距离矢量算法(DV, 对应RIP协议)

Bellman Ford算法!

问题

解决方法

水平分割法

链路状态算法(LS, 对应OSPF协议)

Dijkstra算法!

问题

解决方法

降低子网复杂度来减少子网路由器数量

DV和LS区别和特点

DV

节点向相邻节点告诉它所知道的所有节点路由信息

节点根据相邻节点路由更新自己的路由表

分布式计算

可扩展性差

LS

节点向所有节点告诉它相邻节点的状态信息

每个节点都有全局拓扑结构

根据拓扑结构集中计算路由表

可扩展性好

6.4 流量控制与拥塞控制

RED

流量控制

拥塞控制

全局问题, 主机和路由器等设备均会波及

网络负载不均衡, 路由器收发速度不匹配

对无连接的网络很难在网络层控制住, 因此需要网络层传输层一起控制

现象

原因

后果

控制原理

开环控制(基于良好设计, 进行业务量整形)

整流限速

漏桶算法(直接限速)

令牌桶算法(允许一定突发流量)

闭环控制(基于反馈概念, 进行监测与调整)

由主机或路由器发送询问分组获取拥塞情况

分组头保留位或域用于通知拥塞信息

检测到拥塞, 就告诉源端或者直接广播所有主机

虚电路拥塞控制

建立连接时便预留资源

如果拥塞, 则拒绝建立新的虚电路

建立虚电路会绕开拥塞区域

数据报拥塞控制

随机早期检测(RED)

抑制分组

源抑制

逐跳抑制

6.5 网络互连

L1

L2

L3

L4到L7

安全网关-防火墙

7 网络层(Internet的IP协议)

7.2 IP地址

IANA

ISP

DHCP

IPv4共32位

特殊IP

广播

测试

IP配置方法

手动配置

拨号上网(PPP协议)

DHCP

客户/服务器模型, UDP协议封装

IP地址分配机制

自动分配(永久分配)

动态分配(一段时间有效)

手动分配(管理员分配, DHCP只负责报告地址)

分配过程

客户端广播DHCPDiscover消息

消息包含源IP全0, 目的IP全1, 用MAC地址标识客户端

服务器们回应DHCPOffer消息

消息包含分配的IP地址, 租用期限等参数

客户端广播DHCPRequest消息

消息包含选择的服务器以及其分配的IP

被选定的服务器回应DHCPACK消息

消息包含配置的参数

客户端对接收到的DHCPACK检查

然后就可以使用了

释放过程

客户端向服务器发送DHCPRelease消息

消息包含客户端MAC地址

然后就可以释放IP了

DHCP可以中继

7.3 地址解析协议(IETF)

ARP

RARP

VLAN

IP地址与MAC地址的区别

位数

固化&变化

个性化

数据在链路中的IP和MAC地址变化

ARP过程(IETF)

若在同一个网络内(同一个广播域)

step 1 2 3 4

若不在同一个网络内(不同广播域, 同一个网段)

代理ARP

使用缺省路由

两种方案主机发出的目的MAC地址均为路由器

RARP(IETF)

用于查找自己IP, 针对无法自己得知IP的小型设备

7.4 IP协议

MTU

Maximum Transmission Unit

最大传输单元

帧格式

4bit 4bit 1B 2B 2B 3bit 13bit 1B 1B 2B 4B 4B 0<=40B nB

Vers Len ToS TL ID Flag FO TTL Ptc Cks SI DI Opt+Pad Data

IP分段

7.5 IP路由和转发

IGP

EGP

BGP

IP寻址

一个IP标识一个主机或者路由器的一个接口

一个主机若连接两个网络时会有两个IP, 叫多接口主机

一个路由器至少连接两个网络, 原则上至少两个IP, 一个出口对应一个

分组转发

根据目的IP地址检查路由表进行转发

路由表至少有目的网络以及下一跳的对应

路由表可以非自适应手动配置也可以自适应通过协议自动进行动态维护

分为显式路由和缺省路由, 缺省路由可以缩短路由表表项

路由表和转发表不尽相同

路由表有网络号和下一跳等

转发表有网络号, 接口, MAC地址等

转发表由路由表生成

但是一般两者不做区分

路由选择

通过路由协议建立路由表的过程

路由转发

路由器等设备接受分组

根据分组目的地址查询路由表

按照指定端口转发

路由协议

自治系统AS

同一个实体控制下且具有相同路由选择策略的IP网和路由器的集合

也称为路由选择域

协议分两类, IGP和EGP

IGP

RIP协议, 基于DV算法

上层使用UDP协议(快速)

适合变化不大的网络, 变化仅告诉相邻节点

收敛慢

OSPF协议, 基于LS算法

直接走IP协议(简单)

适用于规模大的网络, 允许将广播域划分成小区

允许到同一位置路由相同开销

EGP

BGP协议, 基于DV算法!

上层使用TCP协议(稳定)

适合规模庞大需要边界路由代表的网络

周期性检测发送keepalives数据保证TCP连接

可发送update数据更新消息

可扩展到大规模网络连接全球

7.6 ICMP协议(IETF)

ICMP

IP是尽力服务, 如果出错就通过ICMP来发送错误报告

是网络层协议, 但是也需要IP封装

无连接

定义了两类报文

差错报文

信息报文

网络诊断工具

ping

traceroute

7.7 IGMP协议(IETF)

IGMP

用于IP组播

一对多或多对多的传输方式, 与单播相对

用D类地址作组播地址

分成两类, 永久组地址和临时组地址

组播路由协议

基于源的组播协议, 以发送端为多播树的根, 包含所有组成员

DVMRP, MOSPF

基于共享树的组播协议, 对每个组使用同一棵树

CBT

混合型协议

PIM系列的PIM/DM, PIM/SM

IGMP嗅探可以让二层交换机识别在组内的主机, 不会局域网全广播, 而是只给组员

7.8 IPv4的可扩展性

CIDR

VLSM

NAT

8 传输层(OSI的机制和Internet的应用)

8.1 传输层服务

TSAP

NSAP

目的

实现用户对数据传输控制

实现运行在不同主机上进程之间通信

屏蔽下层网络异质性

8.2 传输层寻址

传输层为上层提供复用机制, 因此进程间建立连接时, 需要指明传输层TSAP地址

TSAP获取方法

周知端口 20 21 25 53 80 110

进程服务器

名字服务器

NSAP和TSAP标识了一个主机的进程, 是ISO定义的概念

在Internet中, NSAP对应IP地址, TSAP对应端口号

{IP地址, 端口号, 协议类型}标识主机上的服务用户进程

{源IP地址, 源端口号, 目的IP地址, 目的端口号, 协议类型}传输服务数据流

8.3 建立连接

CR

DR

面向连接的服务提供了流量控制和拥塞控制

8.4 Internet的传输层协议

UDP

TCP

SCTP

MPTCP

QUIC

MSS

RTT

RWND

CWND

SWND

SSTHRESH

两个常用的Internet的传输层协议

UDP TPDU为数据报

特点

TCP TPDU为数据段

特点

IP地址标识Internet的主机, 数据中的IP地址由程序或系统指定

MAC地址标识链路上接口设备, 数据中的MAC地址由系统指定

数据在网络中传输时, 端口和IP不变, 但是MAC会变化

部分知名端口号 20 21 25 53 80 110

20/TCP FTP主动数据

21/TCP FTP命令

25/TCP SMTP

53/UDP DNS

80/TCP WWW

110/TCP POP3

UDP

简单高效

客户服务器模式应用, 如DNS

话音, 视频等实时多媒体应用

理解 UDP帧格式

帧格式

2B 2B 2B 2B nB

SP DP Len Cks Data

SP源端口号

DP目的端口号

Len整个UDP帧长度

Cks整个UDP数据帧的16位校验和

计算时需要添加一个虚的伪IP头标进行

伪头标

4B 4B 1B 1B 2B

SI DI Res Ptc Len

TCP

字节流传输

数据字节编号, 但是起始编号随机

滑动窗口机制, 发送数据量以窗口大小为单位, 并非应用层消息

面向连接

建立连接, 三次握手

断开连接, 对称释放

与连接相关的定时器

流量控制与拥塞控制

流量控制

傻瓜窗口症状

发送方

why

解决方法

Nagle算法 控制发送

Clark算法 控制接受

与流量控制相关的定时器

拥塞控制

分组在路由器排队延迟和丢包概率增大

主机大量重传分组

网络有效吞吐量下降

正反馈数据越来越多, 恶性循环

通过发送端数据超时判断是否拥塞

Reno算法

慢启动, 拥塞避免, 快速重传算法, 快速恢复算法

图示

描述已自动生成

与可靠性保证相关的定时器

超时间隔Timeout设置方法(太长等待时间长, 太短重复不必要数据)

Jacobson

性能测试, 动态调整

对每条链接, TCP保存变量RTT

RTT\_{n}=

D\_{n}=

Timeout\_{n}=

5个定时器及其功能

两个算法

快速恢复算法(Reno算法)

丢包后的拥塞控制

快速重传算法

可靠性重传

掌握 TCP帧格式

帧格式

2B 2B 4B 4B 4bit 6bit 6bit 2B 2B 2B 0<=40B nB

SP DP Seq Ack Len Res Ctrl WS Cks UP Opt+Pad Data

SP 源端口号

DP 目的端口号

Seq 将要发送的数据段的字节编号

Ack 期待收到的数据段的字节编号

Len 整个TCP帧头长度, 单位是4字节, 范围5到15, 即20到60B

Res 全是0, 用于填充

Ctrl 控制指示, URG紧急, ACK确认, PSH提交, RST重连, SYN同步, FIN断开

WS 窗口大小, 用于流量控制和拥塞控制

Cks 整个TCP数据帧的16位校验和

计算时需要添加一个虚的伪IP头标进行

4B 4B 1B 1B 2B

SI DI Res Ptc Len

SI 发送者IP地址

DI 接收者IP地址

Res 全是0, 用于填充

Ptc 协议号, 06是TCP

Len 整个TCP帧长度

若结果为全0, 则校验和置为全1! 其他按照正常校验和处理即可

UP

紧急指针, 指向紧急数据的最后一个字节, 仅在URG为1有效

Opt+Pad

可选项, 如果有则必须填充到4字节的整数倍

用于提供排错, 测量, 安全等措施

增加功能, 但是增加了路由器开销, 不过这部分很少用

Data

数据段

理解 Socket编程的具体流程

8.5 Berkeley Socket

Socket原语

SOCKET(建立套接字)

创建新通信端点的连接

BIND(套接字绑定端口)

本地地址关联到套接字上

LISTEN(主动变被动服务器, 开始侦听端口有无连接请求)

宣布愿意接受连接, 给出等待连接的队列大小

ACCEPT(接受侦听的连接请求, 给它新的套接字, 原来的套接字还在侦听)

阻塞调用方, 直到有人企图连接

CONNECT(发送连接请求)

主动尝试建立连接

SEND(发)

从连接上发送数据

RECV(收)

从连接上接收数据

CLOSE(关闭套接字)

释放连接

TCP

服务器 客户

UDP

服务器 客户

9 应用层(通用)

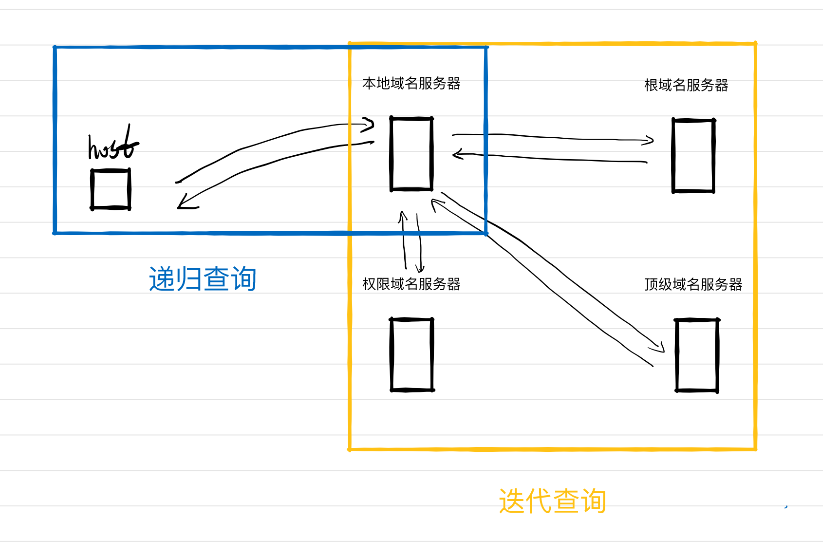
理解 DNS的结构与工作过程

9.2 域名系统DNS(53/UDP)

树形结构, 逐层查找

应用流程

step 1 2 3 4



工作类型

递归查询

迭代查询

理解 FTP的工作过程

9.3 文件服务FTP(21/TCP)

表格

中度可信度描述已自动生成

了解 HTTP的工作过程

9.4 万维网HTTP(80/TCP)

URL

用户输入URL或者点击超链接对应的URL

主机分析URL, 通过DNS服务器找到IP地址

主机与IP对应的80端口建立TCP连接

主机请求服务器获得某页面(请求消息)

服务器响应回复页面(响应消息)

TCP连接释放

浏览器显示页面

了解 SMTP和POP3的工作过程

9.5 电子邮件SMTP和POP3(25/TCP 110/TCP)

SMTP工作类型(发)

发信人调用用户代理编写邮件

用户代理用SMTP把邮件发送到预设的发送邮件服务器

发送邮件服务器把邮件放入缓存等待发送

发送邮件服务器SMTP向接收邮件服务器建立TCP连接

SMTP开始向远程的SMTP发邮件

发送完毕, SMTP将TCP连接释放

接收邮件服务器把邮件放入收信人邮箱

POP3工作类型(收)

收信人打算收信时, 用POP3取回服务器里的邮件到本地

10 网络安全概要

了解 网络安全的典型协议名称

了解 网络上常见的攻击以及分类

10.4 典型的网络安全威胁

主动攻击, 更改或伪造数据

伪装

重放

篡改

拒绝服务

被动攻击, 偷听或监视传输

报文分析

流量分析

攻击分类

口令破解

连接盗用

服务拒绝

网络窃听

数据篡改

地址欺骗

社会工程

恶意扫描

基础设施破坏

数据驱动攻击

理解 公私钥密码

数字签名

一个发送者 A 想要传些资料给大家，用自己的私钥对资料加密，即签名。这样一来，所有收到资料的人都可以用发送者的公钥进行验证，便可确认资料是由 A 发出来的了。（因为只有Ａ使用私钥签名得到的信息，才能用这个公钥来解）

非对称算法，过程如下：

首先 接收方 生成一对密钥，即私钥和公钥；

然后，接收方 将公钥发送给 发送方；

发送方用收到的公钥对数据加密，再发送给接收方；

接收方收到数据后，使用自己的私钥解密。