**第一章：计算机网络及其参考模型**

LAN( Local Area Networks ) 局域网——是一组终端设备和由共同的组织管理的用户。

WAN( Wide Area Networks ) 广域网——连接分布于不同地理位置的LAN的网络。

为什么要使用数据包？

1.计算机可以轮流发包2.如果包丢失，只需重传少量的数据3.数据可从不同的路径到达。

OSI Open System Interconnection 开放系统互连

好处：

1.使得不同的网络软件或硬件相互通信

2.防止一层的改变影响另一层

3.网络组件的标准化使得得到多个厂商的支持

4.将网络通信分为小的部分，易于理解。

七层：

物理层：在设备间传送比特数据。物理层协议定义介质的规范。

数据链路层：为在局域网上主机到主机或广域网的设备间的发送建立和编制帧。（提供物理层提供可信的数据传输）

网络层：在两台路由发生的最终系统中提供连接和路径选择（为能通过在其他网络上的中间设备进行端到端的发送建立和编制包）

传输层：在源定义数据段并编号，传送数据，并在目的地重组数据

会话层：在用户间建立和管理会话。

表现层：为应用提供数据的表现形式。

应用层：为终端用户提供应用程序服务

物理层关键字：信号和媒介

数据链路层-KEY：帧，介质访问控制

网络层：路径选择，路由，寻址

传输层：可靠性，流控制，差错检验

会话层：对话和交谈

表现层：通用格式

应用层：浏览

TCP/IP

TCP：Transmission Control Protocol（传输层）

UDP:User Datagram Protocol

IP：Internet protocol （网际层）

四层：

网络接口层，网际层，传输层，应用层

Network access, Internet, Transport, Application

 应用层：

FTP - File Transfer Protocol 文件传输协议

HTTP - Hypertext Transfer Protocol  超文本传输协议

SMTP - Simple Mail Transfer protocol  简单邮件传输协议

DNS - Domain Name System 域名系统

TFTP - Trivial File Transfer Protocol 简单文件传输协议

网络拓扑：

总线，环形，星形，扩展星形，层次，网状

网络设备：

第一层设备：

hub集线器：重新生成信号并且传输，无过滤，无选择，单端口传到其他所有端口

repeater中继器：增强信号并且传输，无过滤，单端口传到另一端口

第二层设备：

NICs网卡：用来转换信号的发送接收器

switch交换机：是一种用于电信号转发的网络设备。它可以为接入交换机的任意两个网络节点提供独享的电信号通路。最常见的交换机是以太网交换机。

bridge网桥：过滤信息，让信息保持在局域网内。同时有一张mac表可以决定是否要转发到另外的网段。网桥就是通过MAC地址来实现多个LAN之间主机的连接的（但不管LAN内的事情），连接两个不同的局域网。

第三层设备：

router路由器：path selection and switching of packets to best route

**第二章：物理层**

 点对点网络环境：

一个设备通过link和另一个连接，在拨号网络里使用最多的连接方式。

coax同轴电缆：铜导线

接头：BNC（British Naval Connector  或Bayonet Neil Concelman)

STP（shielded twisted pair）：屏蔽双绞线

由4对细铜线组成，外有一层金属箔片或编织物

速度和吞吐量：10~100Mb

最大线缆长度：100m

接头：RJ-45

UTP：非屏蔽双绞线

同上；

几类双绞线：

1类（CAT 1)：用于电话通信

2类：可用于传输数据，最大为4Mb/s

LAN

3类：用于10BASET以太网，10Mb/S

4类：用于令牌环，16Mb/s

5类：用于快速以太网，100Mb/s

超五类：用于G比特以太网，1Gb/s

优点：

易于安装，单位介质便宜

不需要专门的管道

使用RJ接口，

不足：

比起其他网络介质，更容易受到电磁干扰

单根线长小于同轴电缆和光纤。

光纤：（Fiber-Optic）

单模光纤：

轴传播

比多模光纤快，能达到10Gb/s

直径小

使用发光二极管或激光（多数）

较多使用在WAN

多模光纤：

多使用在LAN

UTP：

交叉线和直通线

Rollover线（又称console cable）

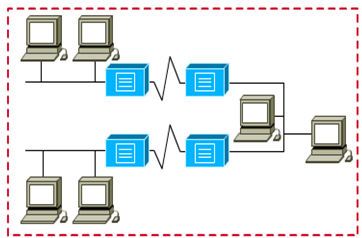
信号和传输问题

传输、衰减、反射、噪音、时间问题、

冲突：两个比特同时在一条网络上传输，就造成了冲突。

限制冲突域：网桥、交换机、路由器。

规则：五个网段，四个中继器。三个网段是有主机的网段，两个网段是连接网段。有一个大的冲突域。



 数字通信：

信号(signal)——数据的电气的或电磁的表现。

码元(code)——在使用时间域（或简称为时域）的波形表示数字信号时，代表不同离散数值的基本波形。

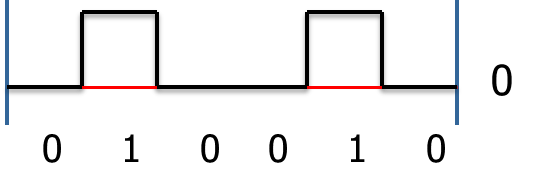
波特率（baud）和比特率（bit）

波特率（调制速率）：信号每秒钟变化的次数

比特率：每秒钟传送的二进制位数。

1单极性编码：

用0电平表示“0”，正电平表示“1”

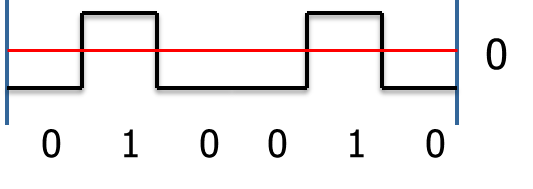


极化编码：

不归零制码（NRZ：Non-Return to Zero）

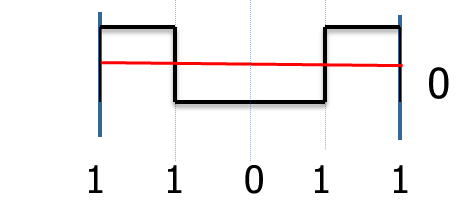
1.不归零电平编码（: Non-Return to Zero）

用负电平表示“0”，正电平表示“1”（或相反



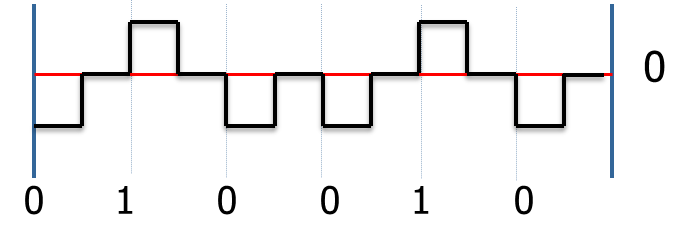
2.不归零反相编码

信号电平的一次翻转代表比特1，无电平变化代表0



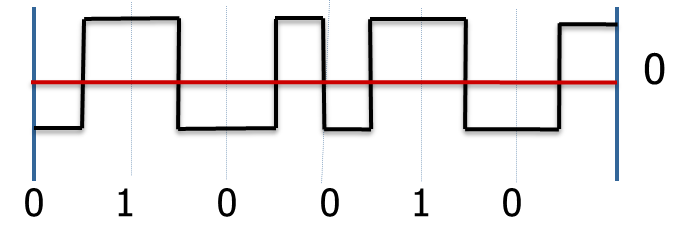
归零制码（RZ：Return to Zero）

1.用负电平表示“0”，正电平表示“1”（或相反），比特中位跳变到零电平，从而提供同步



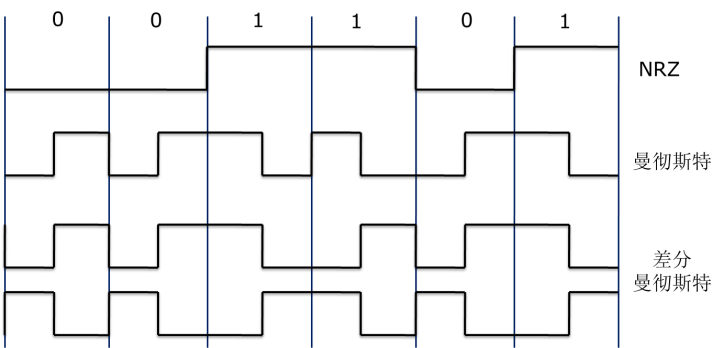
2.曼彻斯特码（Manchester）

每一位中间都有一个跳变，从低跳到高表示“0”，从高跳到低表示“1”



3.差分曼彻斯特码（Differential Manchester）

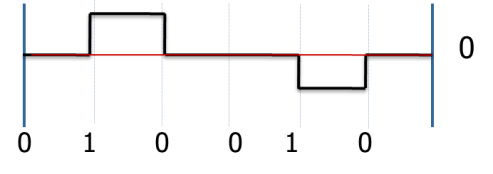
每一位中间都有一个跳变，每位开始时有跳变表示“0”，无跳变表示“1”。位中间跳变表示时钟，位前跳变表示数据



双极性编码：

双极性传号交替反转码（AMI）

与RZ相同，采用三个电平：正、负与零。与RZ不同的是，零电平表示“0”，正负电平的跃迁表示“1”



多路复用：由于一条传输线路的能力远远超过传输一个用户信号所需的能力，为了提高线路利用率，经常**让多个信号共用一条物理线路**

时分复用TDM（Time Division Multiplexing）

频分复用FDM (Frequency..)、

波分复用WDM (Wavelength…)、

码分复用CDM (Code…)。

单工(simplex transmission)

半双工(half-duplex transmission)

全双工(duplex transmission)

**第三章：数据链路层：**

两层：Media Access Control (MAC) ：定义了物理线路上怎样传输帧。解决了物理地址问题，定义网络拓扑和流水线。

Logical Link Control (LLC)：逻辑上标志不同的协议类型并且封装起来。

处理差错通知，网络拓扑和流控制

Frame：封装形式成为协议数据单元（PDU: Protocol data unit）

局域网标准：

MAC：定义了怎样在物理线缆上传输帧

       处理物理寻址

       定义网络拓扑

       定义线缆规章

LLC：标示不同的协议类型，并封装他们

      ····

以太网帧格式：

前同步码，目的MAC地址，源MAC地址，长度，数据，帧校验序列

注意：目的地址在前，

前同步码的作用是通知接收站帧的到来

目的地址可以是单播、多播、广播，源地址基本是单播

LLC既可以提供无连接服务也可以提供面向连接服务

LLC的封装：

第二层通过LLC和高层通信

第二层使用帧组织数据

第二层使用MAC地址寻找目的计算机

MAC地址：48bits（12H）

前6位16进制数标示制造商，供货商

剩下的由供货商管理

第二层广播地址为：FFFF.FFFF.FFFF.FFFF（48位均为1）

广播在下面两种情况下发生：1不知道目的MAC地址

                          2目的地为全体工作站

以太网：逻辑拓扑-总线型

令牌环：环形

FDDI：环形

ＭＡＣ：用来确定在共享介质环境中哪个计算机允许传输数据的协议

分为两类：

确定的：令牌环和FDDI

不确定（先来先服务）：以太网/IEEE 802.3

以太网/IEEE 802.3：CSMA/CD 载波侦听多址访问/冲突检测（ Carrier Sense Multiple Access with Collision Detection ）

CSMA：先侦听线路，如果发现空闲，则发送数据，（过一段时间）否则继续等待

（三种CSMA：1-persist CSMA, non-persist CSMA, p-persist CSMA）

CD：在传输过程中，仍然侦听线路，如果冲突检测到，则先广播拥塞信号

      后退算法决定哪个设备再次接入介质。

LLC流控制：

假设：单工传输，发送方无休止工作、接收方无休止工作、通信线路（信道）不损坏或丢失信息帧

滑动窗口协议、流水线技术

以太网是一种无连接的网络结构，是一种尽力而为传送系统（best-effort delivery system)

以太网特别适合在本地通信介质上高速传输零星，不定时大流量数据的应用场合

工作方式：1. 广播网；2. 发送碰撞后广播一个间信号，回退一段时间再重新发送。

10BASE-T：10 基站式 双绞线

无线协议

802.11b：wifi

连接过程：scanning（active passtive）主动去找一个无线网加入/被动等待无线网来请求加入。

CSMA/CA：

Carrier Sense Multiple Access with Collision Avoidance载波侦听多址访问/冲突避免

发送站点在发送数据前，以控制短帧刺激接收站点发送应答短帧，使接收站点周围的站点监听到该帧，从而在一定时间内避免数据发送

DSSS：Direct Sequence Spread Spectrum直接序列扩展, 802.11的关键技术。可以达到11Mbps

二层设备：

网卡：

逻辑链路控制-和上层协议通信

      提供唯一的MAC地址

      成帧

      使用内置在收发器创建信号和接口与介质

网桥：

      划分冲突域

      保存并转发设备

交换机：

有些支持直通交换

       提高以太网带宽-点对点，分段，虚电路

二层设备还是在同一个广播域中。

**第四章：网络层：**

网络层的作用：

1、在网络中传输数据

2、采用分级寻址模式

3、将网络分段，并且控制流量

4、减少拥塞

5、与其他网段交流

三层设备：路由

IP地址和子网：

IP地址：32Bits   网络号+主机号

Class A:0+7bits网络号+24bits主机号

Class B:10+14bits网络号+16bits主机号

Class c:110+21bits网络号+8bits主机号

0–127 Class A 地址

128-191 Class B 地址

192–223 Class C 地址

224–239 Class D – 组播

240–255 Class E - 研究

保留地址：

1.广播地址：该网段的主机号全为1

2.网段号：所有主机号位为0

子网：

提供灵活的寻址，通常由网管分配，能够减少广播域

可借位数为主机号位数-2

子网划分：

先确定是哪类网

在确定要多少子网根据子网数切割host ID

然后计算子网掩码

三层设备：

路由：

路径选择

每个路由接口都必须有网络地址

IP地址的分配：

1.静态分配

2.动态分配：

 RARP ：  逆向地址解析协议     Reverse Address Resolution Protocol

 BOOTP：自举协议 BOOTstrap Protocol

 DHCP：动态主机配置协议 Dynamic Host Configuration Protocol

RARP：客户端机发送RARP请求给服务器，服务器回一个RARP响应

BOOTP：客户机发送UDP广播请求IP地址，服务器返回UDP广播，包含请求的ip地址

DHCP：1.发现阶段：DHCP客户机以广播方式发送DHCP discover发现信息来寻找DHCP服务器（UDP广播）。

2.服务器提供 IP 租用地址。（UDP）单播。

3.客户端接受 IP 租约。（广播）--告诉DHCP服务器接受了哪台服务器的租约

4.租约确认。--服务器确认租期

ARP协议：（地址解析协议 Address Resolution Protocol）

运行在第三层为IP第二层为以太的基础之上

Ip->MAC

先查本地的ARP表，如果不存在目的IP的MAC地址，则广播（二层），目的主机收到广播报文之后，发现与自己的IP相匹配，就会发一个响应，其中包含自己的MAC地址，源主机收到响应报文之后，把目的主机MAC加入ARP表，然后再发送数据。(ARP请求->检察-> ARP相应->缓存->目标地址->网络会话

默认网关：连接这个网段的路由接口的ＩＰ

Proxy ARP：（代理ARP）：ARP协议的一种变换形式。在这种形式下，中间设备（比如路由器）代表目的端发送一个ARP应答给发送请求的主机。（即没有缺省网关可以工作，主机不会意识到中间有一个路由器。效率比较低）

ARP只针对同一网段，要访问其他网段需要通过Proxy ARP或者缺省网关

网络层服务：

环交换：强调实际上必须有一条通路

包交换：数据报文的封装形式，也可以是无连接

面向连接的服务：在未发送任何数据之前建立从源到目的的连接

无连接服务：并无达成协议（IP）

无连接和包交换不同（有不同的路径，可以不按次序到达），面向连接和环交换不同

路由和可路由协议：

可路由协议通过网络传输数据（IP IPX）

路由选择协议允许路由器适当的将数据从一个特定的区域定向到另一个特定的区域。

 路由协议决定可路由协议如何被发送（路由）。

非可路由协议：NetBEUI（网络BIOS扩充用户接口）【微软的对等协议】

静态路由和动态路由：RIP, IGRP, EIGRP, OSPF

静态路由：隐藏内部网段，测试特定的网络连接，便于维护路由表

动态路由：IGP（Interior Gateway Protocols ）内部网关协议

              RIP, IGRP, EIGRP, OSPF

          EGP（Exterior Gateway Protocols）外部网关协议

DVP（Distance-Vector Protocols ）距离矢量协议：

RIP, IGRP

LSP（Link State Protocols）链路状态协议：

OSPF

RIP：（Route Information Protocol）路由选择信息协议：

跳数位唯一的度量标准;

最大跳数位15；

每30秒更新一次；

不选择最快路径；

产生很多网络拥塞；

IGRP（Interior Gateway Route Protocol）内部网关路由选择协议和

EIGRP（Enhanced Gateway Route Protocol）增强····

以延迟，带宽，负载，可靠性位度量标准

最大跳数：255

每90秒更新

OSPF(Open Shortest Path First)开放最短路径优先

以代价，速度，可靠性，安全性为衡量。

以事件出发更新。

CIDR ：Classless InterDomain Routing ，无类别域间路由选择

VLSM（ Variable-Length Subnet Masks）变长子网掩码：

Classful routing 有类路由-一个网络只能有一个子网掩码

优点：更有效的使用IP地址

      使用路由汇总的能力更强

支持无类路由的协议：

OSPF，EIGRP，RIP v2，静态路由

只有未使用的子网才能在被划分

先划分需要主机数最多的，然后接着按次序划分。

别忘了每个路由上两个ip地址。

路由聚合：

减少路由表条目的数量

隔离拓扑的变化

**传输层：**

作用：

将上层应用的数据分段

建立端到端的操作

将段从一台主机发送到其他主机

流控制和可靠性

服务质量

提供端到端的控制，通过滑动窗口机制提供流控制，通过序号和确认机制来保证可靠性。

TCP 面向连接的协议保证可靠性

TCP(Transmission Control Protocol）传输控制协议

面向连接

可靠

将数据分为段

在目的站点重组数据

数据重传

UDP（User Datagram Protocol）用户数据报协议：

无连接

不可靠

分段没有软件的检查

没有认证，流控制

TCP：

不支持单播或组播(while socket 不支持组播和广播)

端对端

代码位：URG（紧急） ACK,RST(重置），SYN（序列），FIN（拆除连接）

建立连接（三次握手）

停止等待协议：

每个报文发送后都会保留一份副本

每个报文都有ID

重新发送时间必须大于平均传输时间的两倍

停止等待协议是一个简单协议，效率很低。

可信通信

ARQ：Automatic repeat reQuest。就是说重新发送的请求是自动发送的，接受者不需要请求重新发送错误的信息。

TCP信道是全双工信道

滑动窗口：-流控制机制；要求源设备在向目的设备发送一定数量数据之后接受一个确认。

拆除连接：

四次握手

最后等待两个MSL是为了确保客户端最后的ACK可以到达B，这样连接上所有的报文就保证都已经没有了。

 UDP：

用于：对丢包可以忍受，但对速率敏感的场合。

用UDP传输的协议：RIP，DNS，SNMP，TFTP，DHCP

NAT & PAT

NAT（Network Address Translator）网络地址转换：

将内部（本地）网络地址转换为注册的网络地址，即全局网络地址

是把保留地址空间转化为注册地址空间的有效方法

PAT（Port  Address Translator) 端口地址转换

应用层：

1.会话层：

 一些应用：NFS（network file system)：

           SQL：(Structured Query Language)

           RPC, x Windown System, apple talk session protocol

2.表示层：

 三个功能：数据格式化，数据压缩，数据加密

Graphic Interchange Format (GIF)

Joint Photographic Experts Group (JPEG).

3.应用层：

HTTP：因特网的基本协议 port 80

 FTP（port 21&20） and TFTP（无连接服务，使用UDP）

 Telnet

 SMTP

 SNMP（Simple Network Management Protocol ）简单网络管理协议

 Domain Name Server (DNS)多级DNS

**路由与路由器：**

路由组件：

RAM：存储路由表，ARP 缓存，快速交换缓存，包缓冲，包等待队列

NVRAM：非易失 RAM

         存储备份或开始配置文件

FLASH：存储Cisco IOS

        允许不更换芯片升级软件

        可以存储多个版本的IOS

ROM：POST（Power On Self Test）加电自检

       自举程序（加载ISO）

       操作系统（备份）

Interfaces：工作接口和辅助接口

具体数据转发接口。

Console口：见识口，把机器上的监视信号给Router

启动过程：

1. 加电自检--从ROM诊断所有硬件（POST: Perform a pOwer-up Self Test）

2.查找ISO

 FLASH——》TFTP——》ROM

3.操作系统镜像被加载

4.加载配置文件（NVRAM）并执行

5.如果没有找到配置文件，操作系统进入setup Mode

路由：

路由工作：Path determination & switching

Switching: 把报文从一个网段转发到另一个网段

路径选择：选择最优路径传输报文。

静态路由：

当一个网段只能有一条路径被访问到，静态路由就足够了，这样的分割叫做stub 网络。

管理距离：

提供路由可靠性的一个可选参数。0-255

管理值越小越可靠。

静态路由：1

EIGRP：90

IGRP：100

OSPF：110

RIP：120

默认路由：当目的地址不在路由表中时，将报文发给默认路由。

Router(config)# ip route 0.0.0.0 0.0.0.0 [next-hop-ip-address| exit-interface]

动态路由：

收敛时间

距离矢量协议：DVP Distance Vector Protocol

定期的将路由选择表的拷贝从一个路由发往另一个路由。

问题：路由环

解决方法：

1.定义最大跳数。

2.水平分割：如果F断开，E通知了A，那么不接受A告诉E说F可以到达。

这样会产生问题，如果真的存在一条通路可以到达，这条通路就不可能打开了。

3.路由中毒：如果F断开，E通知A，E到网段需要大于n的跳数。那么A就认为E无法到达网段

4.毒性反转：A回复E，A不可以到达网段F。(一旦从一个接口学习到了一个路由，那么这个路由作为不可达路由从同一个接口回送。)

5.抑制定时器：（优化水平分割）E通知A之后，在一段时间（大于消息传递一圈的时间）内不接受A告诉E说F可以到达。

6.触发更新：

链路状态协议：Link State Protocol，LSP

优点：不会产生环路。

工作：1. 交换LSA报文 2. 构建对网络的整体认知 3. 形成生成树； 4. 把树填给路由，行程路由表。

链路状态通告：LSA，Link State Advertisements

拓扑数据库

最短路径优先 SPF

路由选择表

性能瓶颈：处理器的开销，内存的需求，带宽的消耗。

 更新问题：链路状态路由必须确保所有路由器都能得到整体的LSA报文

**路由协议：**

RIP：

Interior Gateway Protocol, IGP 内部网关协议

距离矢量协议；

每30秒更新

最大跳数为15；

最多6路负载均衡，默认为4路

V1

不发送子网掩码

255.255.255.255作为广播地址

不支持认证

不支持变长子网掩码

V2

等待时间（即定时器时间默认为180s）

使用水平分割（距离定时器）防止路由环

认为16跳即为无限长

支持变长子网掩码（无类路由）

提供认证

以224.0.0.9作为广播地址

OSPF（单区域）

链路状态协议内部网关协议

毗邻数据库（neighbourship database），->拓扑数据库（topological database），使用SPF算法---->路由表

特点：

使用度量：带宽

适合于大型的网络

**以后可以将网络划分为多个区域**

**支持变长子网掩码**

**快速收敛**

**支持多路等价**

优点：robust健壮

Scalable 可扩展

DR（Designated Router ）：指定路由器：

在同一个区域中，被选举出来代表所有路由的路由。

为了减少在同一个网段中几个邻居互相交换信息的数量。

Backup Designated Router (BDR) ：备份指定路由器。

Area：由32位进行标识

area 0 或 area 0.0.0.0

area border router 区域边界路由器

单区域中，Area号为0

多区域中，所有的其他区域都要求接到Area0，所以Area0称为骨干

OSPF收敛五个步骤：

1.建立邻接关系

2.选举DR和BDR

3.发现路由

4.选择合适的路由路径

5.维护路由信息

OSPF 7个状态

停止，初始，双向（Two-Way) ,准启动（EX-Start)，交换，加载，全毗邻。

OSPF网络类型：

多路接入（以太网），点对点，非广播多路接入（虚电路-帧中继）

 OSPF Cost = Metric

Cost = 100000000/bandwidth

OSPF广播地址： 224.0.0.5

Hello分组：地址224.0.0.5

           默认每10秒发送一次，在多路接入和点对点网络中。

           在NBMA网络和帧中继中，每30秒一次

选举DR和BDR：优先级和Router ID

默认优先级为1，范围可以是0-255，数字越大，优先级越高

Router ID:高的内环地址--->高的接口地址--》

使用Hello分组侦听新的路由或Down掉的路由。

链路拓扑改变时，路由器通过224.0.0.6通知DR或BDR

DR或BDR通过224.0.0.5通知该区域内的路由。

书P57

EIGRP：

最大跳数为224

度量有32位长，IGRP有24位

快速收敛

有效利用带宽

支持VLSM和CIDR（无类别域间路由选择）

多网络层的支持

独立于被路由协议

路由发现：使用小的Hello报文

RTP，DUAl，PDM

 OSPF报文

Function Name

Hello Hello

Database Description DBD

Link-State Request LSR

Link-State Update LSU

Link-State Acknowledgement LSAck

**局域网间交换和VLAN**

交换：

两个基本功能：

建立和维护交换表，帧交换

和网桥的区别：

高速，通过微分段实现VLAN

交换机使用硬件实现交换，网桥使用软件实现

交换机增加21微秒的延迟

使用贯穿式（switch 一收到目的MAC地址就转发）

存储转发式

交换机作用

创建维护交换表，快速把帧进行传输。

每次交换机存一个MAC地址，都会有一个时间戳（Time-Stamped）

每次帧的到达，时间戳都会更新。

如果时间戳到期，将会从交换表中删除。

交换的好处：

有效，允许建立虚电路，更加灵活的管理网络，减少冲突域，能与802.3兼容

对称和不对称交换（内存缓冲）

缓冲区：1.每个端口都有缓冲内存，也就是平分真个内存

        2.共享内存

交换方式：

直通转发Cut-through 收到报文后，读，从某个字节开始转发。

快速直通转发：把目的地址收完后开始转发。（若信号不好，则需要校验多）

无碎片直通转发：数据部分收到64个字节后开始转发。

存储转发式 Store-and-forward. 收到报文后，存储、分析，没有错误后转发。路由器都是存储转发

生成树协议： Spanning-Tree Protocol

 解决桥接环路问题，可能导致广播环或者某些MAC地址表不停翻转。

冗余拓扑产生环。

减少冗余路径而不导致网络延时

通过计算稳定的生成树拓扑来防止网络环路

发送BPDU（网桥协议数据单元）来决定生成树拓扑

BPDU：STP需要网络设备互相交换消息来检测桥接环境，交换机发送的用于构建无环路拓扑的消息。

决定顺序：

最低的根网桥（BID)

到跟网桥最低的路径成本

最低的发送网桥ID

最低的端口ID

每个网桥都分配一个唯一的标识（BID），有2字节优先级+6字节MAC地址所构成。

默认优先级为32768

如果相同则小的MAC地址的网桥被选中

BID中含有网桥优先级，网桥优先级是一个可自定义的值，可通过设置来影响根桥选举过程。

路径代价：

STP五种状态：

阻塞（Blocking）：不转发数据；接受BPDU

侦听（Listening）：···       ；侦听数据帧

学习（Learning）：···        ；学习地址

转发（Forwarding）：转发    ；学习地址

禁止（Disable）：   不转发   ；不接受BPDU

BPDU帧格式：

收敛步骤：

1.根交换机选择

2.选举根端口（非根交换机的其他交换机）

3.选取指定端口

VLAN（虚拟局域网）

IEEE 802.1q

逻辑的网络设备或用户分组（逻辑上的子网）

网络设备以功能，部门，应用等划分，而不依赖于物理的区域分段（不受物理拓扑限制）

每个VLAN产生一个广播域

广播仅能在同一个VLAN下传播

 VLAN的是实现完全通过软件，为实际网络提供分域功能。

 使用路由连接两个VLAN

骨干网络（trunk）：用来完成VLAN与VLAN之间的传输，必须是百兆以上的port

 为什么要有trunk：因为不然有几个VLAN就需要几条线，浪费端口。

但使用trunk会使VLAN1、VLAN2、VLAN3的数据混淆。所以需要：

 帧过滤和帧标记

帧过滤：交换表

帧标记：在骨干上传的时候加上标记位，当从骨干上卸下来时，去掉标记位。

两个标准：IEEE802.1Q规定标记帧写法，简单。

ISL(Inter-Switch Link)【cisco】头加26bytes，尾部加4bytes（CRC）

Name      Encapsulation Label      Media

802.1Q    No   Yes  Ethernet

ISL  Yes  No   Ethernet

VLAN的实现：

静态（VLAN之间没有路由器，数据不能交互）：手工配置，

动态；告诉机器那些MAC属于哪些VLAN，发帧后动态查找。

静态：容易查错，但修改费力。

动态：修改方便，灵活性好。未授权机器介入后有集中相应。

端口为中心的VLAN：

路由分配用户

VLANs 便于管理，可以使用router划分流量

提供更高的安全性

包不会泄露到其他域中

接入链路和中继链路（Access Links &Trunking Links）

接入链路：接入链路是在交换机上只属于一个VLAN的链路，任何接入的设备并不知情有VLAN的存在

Trunking VLANS：

支持多个VLANs

主要用来连接交换机和交换机

支持在快速以太网和G比特以太网

点对点，支持多个VLANs

节省端口

不需要属于某个特定的VLAN

可以配置位能传输所有VLANs或者有限个VLANs

Trunk可能有一个本地VLAN

**广域网：（WAN）**

在前三层上都有操作，主要是前两层。

设备：CPE：Customer Premises Equipment 客户端设备

CO：Central Office 中心局；

注意：1Kbit/s=1000bit/s 不是1024

本地环local loop：CPE到CO

服务端设备：DCE（data circuit-terminating equipment）数据通信设备 ISP

用户端设备：DTE（data terminal equipment）数据终端设备

交换虚电路：（Switched Virtual Circuits）SVC

3阶段：建立，数据传输，拆除

电话和ATM使用的是SVC

永久虚电路：（Permanent Virtual Circuits）PVC

X.25和帧中继使用的是PVC

设备：

CSU (channel service unit) 信道服务单元

DSU（data service unit）数据服务单元

要连接到租用的线路，用户必须：

连接到提供者的回路

有一个合适并且可用的路由器端口

有CSU/DSU, modem, ISDN Terminal Adapter（信道服务/数据单元，调制解调器、ISDN终端适配器）

路由器的作用：

连接网络，WAN的串行口

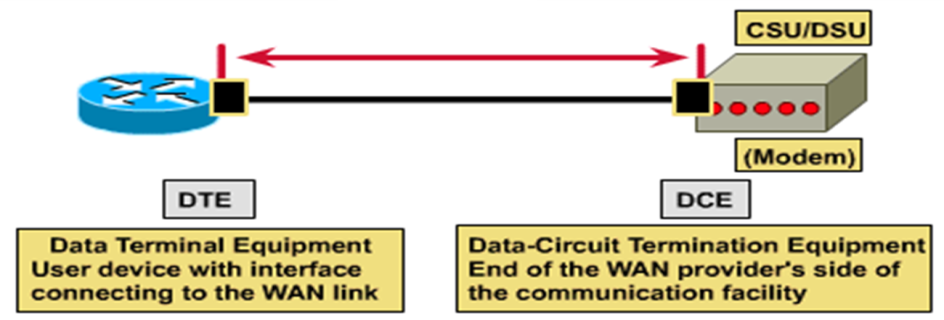
路由可以作为：内部路由，骨干路由，区域边界路由，自治系统边界路由

Modem就是CSU/DSU

WANs标准：

物理层，to provide electrical, mechanical, operational, and functional connections for WAN services

定义了DTE和DCE间的接口



协议：EIA/TIA-232

EIA/TIA-449

数据链路层：

描述了数据怎样在单一的链路上在系统之间传送

封装：

帧中继：没有差错检验

点对点

**PPP：**

由IETF开发，用来代替SLIP（只支持IP，不支持认证，压缩，差错检验，动态分配IP地址）

有一位代表网络层协议

能在连接建立时检查链路质量

提供PAP（Password Authentication Protocol）和CHAP（Challenge Handshake Authentication Protocol）认证

HDLC：

Cisco的默认串行线封装

没有窗口或者流控制

有属性类型位

两台路由使用Cisco的IOS（如果不是Cisco设备，则应使用同步PPP）

PPP提供了：

在同步或异步串行线上广泛使用的封装协议

网络层的多链路技术

动态IP地址的分配

认证：PAP ，CHAP

压缩

差错检验

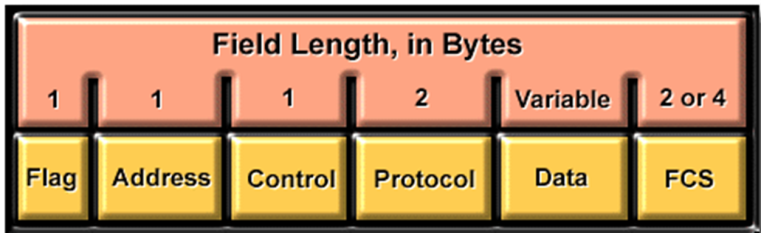
PPP组件：

使用HDLC（ISO）（高级数据链路控制）作为3层的报文的封装

使用LCP（Link control protocol）链路控制协议：建立链路，配置连接选项，检测链路质量

使用NCP（Network Control Protocol）网络控制协议：选择和配置3层协议

帧格式：



PPP会话的建立与终止：

1.链路的建立和配置协商  LCP

2.链路的质量检测

3.网络协议的配置协商 NCP

4.链路终止

PAP（Password Authentication Protocol）：密码验证协议

双向握手

远程节点不停的在链路上反复发送用户名/密码，直到验证通过或者连接终止

不健壮的身份认证协议，使用明文发送密码

连接建立后只有一次认证

CHAP（Challenge Handshake Authentication Protocol）质询握手验证协议：

3次握手：质询；回应；接受或拒绝

书P298，第一段

Hash 函数

ISDN（Integrated Services Digital Networks）:综合业务数字网：在已有的电话线上传输语音或数字信号

Link Access Procedure, Balanced (LAPB):

Cisco/IETF:

High-Level Data Link Control (HDLC):

HDLC: 高线数据链路High-Level Data Link Control

PPP: 点到点协议（适用于串线形）Point-to-Point Protocol

ISDN 综合业务数字网Integrated Services Digital Networks

集合多个信道为用户提供专享的贷款，可以同时传输声音、video and data。最初由三个信道组成，D信道用来控制指令（16k bandwidth）

2个B信道，用来传输数据（64k bandwidth）

后来把更多的B信道和D信道集成起来

BRI原始3信道，144k Basic Rate Interface基本速率接口

PRI 更多B信道和D信道 Primary Rate Interface主要速率借口

SPID:配置ISDN号。Service Profile Identifier

最常见的广域网点对点封装是PPP和HDLC

ADSL：非对称（指上行和下行带宽不对称）数字用户线 Asymmetric Digital Subscribe Line

xDSL是用数字技术对现有的模拟电话用户线进行改造（利用频分复用），使它能够承载宽带业务。

电话线也是双绞线UTP

SONET：同步光纤网

SONET标准的四个光接口层：

光子层

断层

线路层

路径层

HFC：光纤同轴混合网。部署在有线电视网上

**网络安全**

通信的四种威胁：

截获、中断、篡改、伪造

被动攻击：截获信息。不干扰信息流。

主动攻击：更改信息、拒绝用户使用。

更改报文流

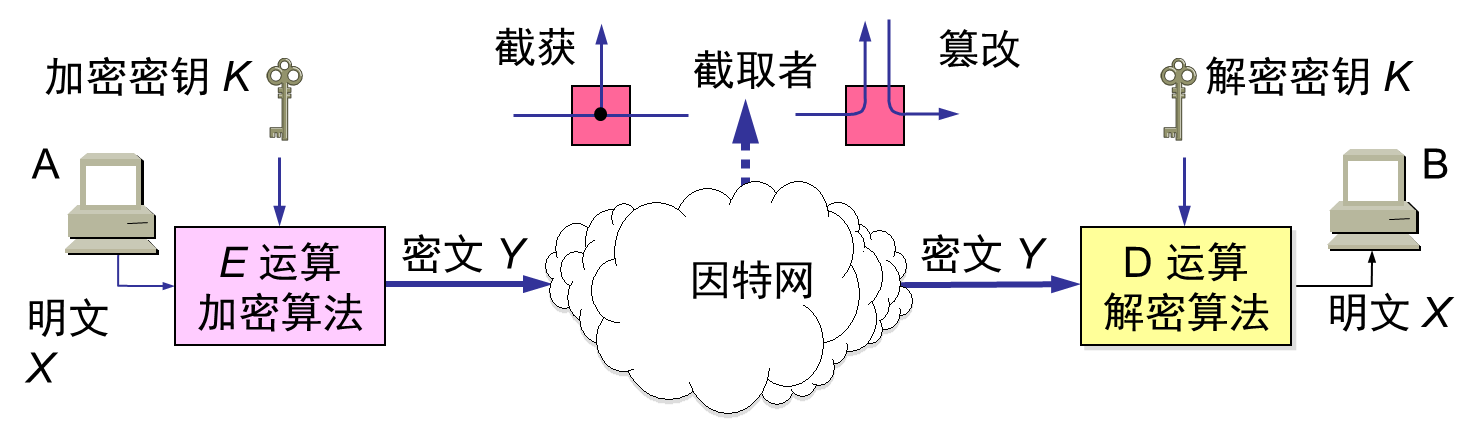
拒绝报文服务

伪造连接初始化

网络安全的内容：

保密性、安全协议的控制、访问控制

一般的数据加密模型



对称密钥：加密密钥与解密密钥(密钥都，算法公开)相同（常规/传统密钥密码体制），e.g:DES

公钥密码：加密密钥(密钥公开，加密算法公开)与解密密钥(密钥保密，解密算法公开)不同，是一种“由已知加密密钥推导出解密密钥在计算上是不可行的”密码体制。e.g:RSA

数字签名必须保证：报文鉴别（识别发送方）、报完完整性（不可抵赖曾发送）、不可否认（不可伪造）数字签名采用公钥算法更容易实现

防火墙：网络级（分组过滤、授权服务器）、应用级

ACL(访问控制列表）Access Control Lists

一些告诉路由哪些包该拒绝哪些包能通过的序列集。

可以根据源地址，目的地址，链路协议来决定。

如果包没有在ACL找到相应的条目，则会被丢弃。

隐式的deny any

通配符掩码：

32比特的数字字符串，4个8位组。0表示“检查相应的位”，1表示不检查。

通配子网：

和子网掩码相反

通配any：

Permit 0.0.0.0 255.255.255.255或permit any

通配host：

Permit 192.168.100.3 0.0.0.0或 permit host 192.168.100.3

标准ACL：没有目的参数，所以将ACL表放在靠近需要保护的目的地的路由

扩展ACL：可根据多种属性过滤分组（如协议类型、源地址/端口、目标地址/端口等），放在离将被拒绝的数据流的信源尽可能近的地方

ftp:21

telnet:23

smtp:25

dns:53

tftpz:69