

LAN(Local Area Networks) 局域网

WAN(Wide Area Networks) 广域网

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，数据链路层，网络层，传输层，会话层，表现层，应用层。

- ✧ 物理层关键字：信号和媒介。(Physical)
- ✧ 数据链路层：帧，介质访问控制 (MAC)。(Data Link)
- ✧ 网络层：路径选择，路由，寻址。(Network)
- ✧ 传输层：可靠性，流控制，差错检验。(Transport)
- ✧ 会话层：对话和交谈，建立连接。(Session)

✧ 表现层：通用格式，加密解密。(Presentation)

✧ 应用层：浏览。(Application)

TCP/IP

四层：

网络接入层，Internet 层，传输层，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，中继器

第二层设备：网卡，交换机，网桥

第三层设备：路由

同轴电缆：铜导线

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

STP：屏蔽双绞线 (Shielded Twisted-Pair)

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

数字通信：

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

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”

数据链路层：

处理差错通知，网络拓扑和流控制

局域网标准：

IEEE：802.3 介质访问控制（MAC）

IEEE：802.2 逻辑链路控制（LLC）

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

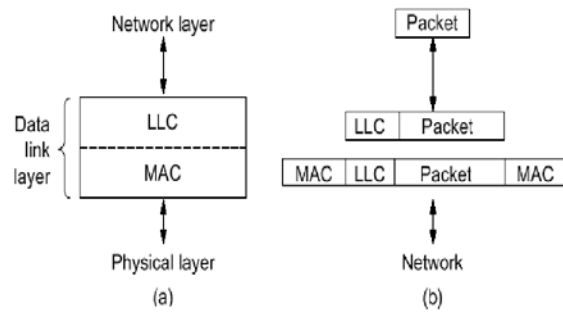
.

以太网帧格式：

前导码，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

LLC 既可以提供无连接服务也可以提供面向连接服务



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

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

确定的：令牌

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

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。

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）

802 Standards

IEEE	Title and Comments
802	Standards for Local and Metropolitan Area Networks
802.1	LAN and MAN Bridging and Management
802.2	Logical Link Control
802.3	CSMA/CD Access Method
802.3u	Fast Ethernet
802.3z	Gigabit Ethernet
802.4	Token Passing Bus Access Method
802.5	Token Ring Access Method
802.6	Distributed Queue Dual Bus Access Method (for WANs)
802.7	Broadband Local Area Networks
802.8	Fiber-Optic Local and Metropolitan Area Networks
802.9	Integrated Services
802.10	LAN/MAN Security
802.11	Wireless LANs
802.12	High-speed LANs
802.14	Cable TV Access Method

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

10BASE T :

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。

网络层：

在网络中传输数据

采用分级寻址模式

将网络分段，并且控制流量

减少拥塞

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

子网：

提供灵活的寻址，通常由网管分配，能够减少广播域

Network	Subnet	Host
---------	--------	------

可借位数为主机号位数-2

子网划分：

先确定是那类网

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

BOOTP：自举协议

DHCP：动态主机配置协议

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）

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。

默认网关：连接这个网段的路由接口的 I P

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。

网络层服务：

面向连接的服务：

无连接服务：IP

有不同的路径，可以不按次序到达

路由和被路由协议：

被路由协议通过网络传输数据

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。

非被路由协议：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。

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。

别忘了两个路由上的 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：

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

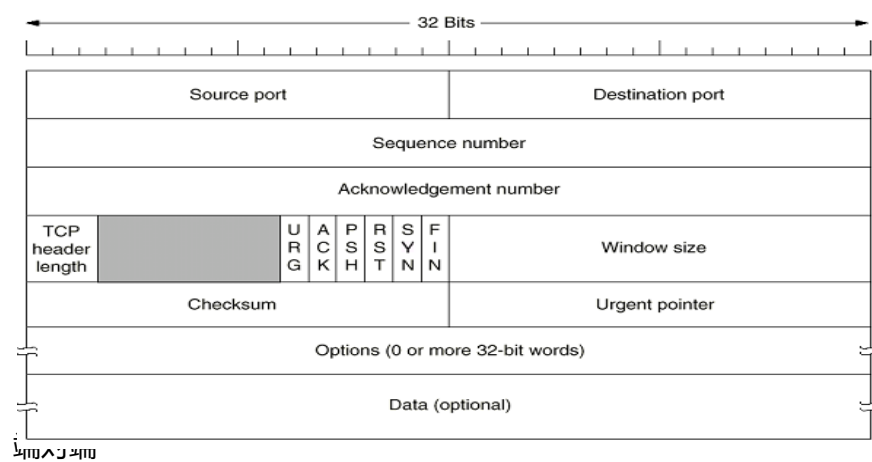
不可靠

分段没有软件的检查

没有认证，流控制

TCP：

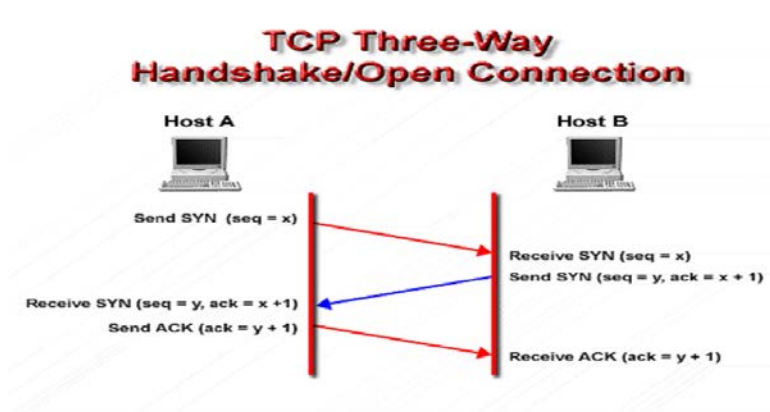
不支持单播或组播



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）：

书 P291



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

书 P295

UDP：

用于：对丢包可以忍受，但对速率敏感场合。

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

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 Window 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 :

FTP and TFTP (无连接服务 , 使用 UDP)

Telnet

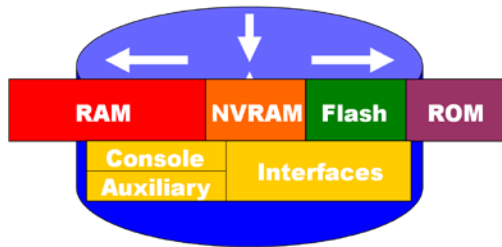
SMTP

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

Domain Name Server (DNS)

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)

启动过程：

1.加电自检--从 ROM 诊断所有硬件

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：

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：

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：书 P448

3.路由中毒：将跳数设置为最大跳数加 1 来实现。

4.毒性反转：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：书 P450

6.触发更新：

链路状态协议：

链路状态通告

拓扑数据库

最短路径优先

路由选择表

具体过程：书 P434

三个要考虑的问题：处理器的开销，内存的需求，带宽的消耗。

路由协议：

RIP：

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

毗邻数据库， -> 拓扑数据库， ----SPF----> 路由表

使用度量

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

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。

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 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

Network Mask		
Hello Interval	Options	Router Priority
Dead Interval		
Designated Router		
Backup Designated Router		
Neighbor Router ID		
Neighbor Router ID		
(additional Neighbor Router ID fields can be added to the end of the header, if necessary)		

选举 DR 和 BDR：优先级和 Router ID

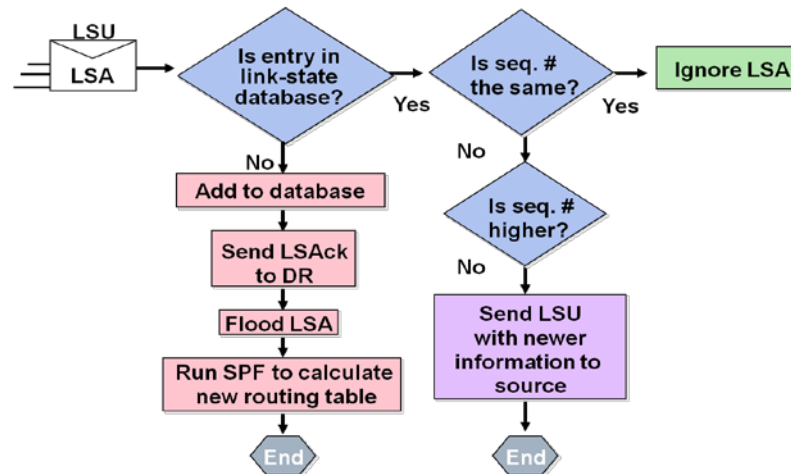
默认优先级为 1，范围可以是 0-255，数字越大，优先级越高

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

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

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，也就是平分整个内存

2.共享内存

交换方式：贯穿式，存储转发式

生成树协议：

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

路径代价：

STP 五种状态：

阻塞 (Blocking)：不转发数据；接受 BPDU

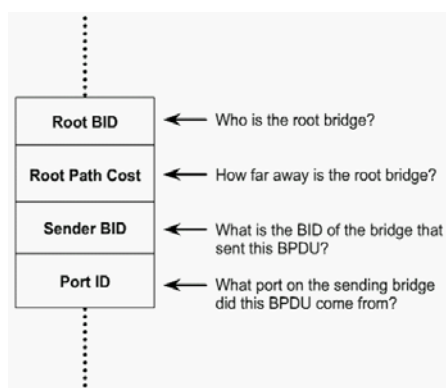
侦听 (Listening)：；侦听数据帧

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

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

产生单一的广播域

广播仅能在同一个 VLAN 下传播

骨干网络 (trunk)

使用路由连接两个 VLAN

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

ISL(Inter-Switch Link) 【cisco】

Name	Encapsulation	Label	Media
------	---------------	-------	-------

802.1Q	No	Yes	Ethernet
--------	----	-----	----------

ISL	Yes	No	Ethernet
-----	-----	----	----------

VLAN 的实现：

静态和动态；

端口为中心的 VLAN：

路由分配用户

VLANs 便于管理

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：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

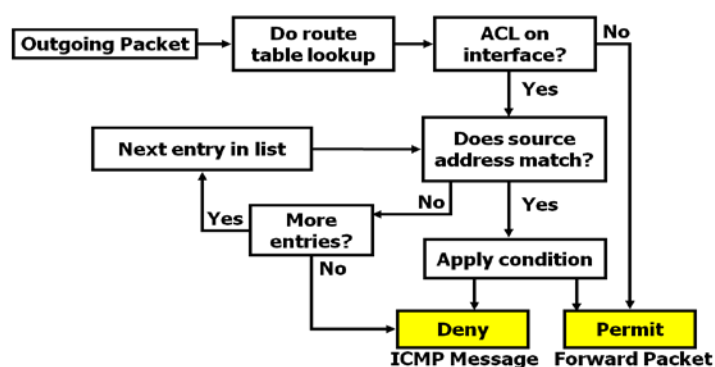
ACL(访问控制列表) Access Control Lists

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

ftp:21

telnet:23

smtp:25

dns:53

tftpz:69

广域网 : (WAN)

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

DCE (data circuit-terminating equipment) 数据通信设备 ISP

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

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：

WANs 标准：

物理层，to provide electrical, mechanical, operational, and functional connections

for WAN services

DCE 和 DTE

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

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):

最常见的广域网点对点封装是 PPP 和 HDLC

PPP：

由 IETF 开发

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 ISO

PPP

SLIP:

只支持 IP , 不支持认证 , 压缩 , 差错检验 , 动态分配 IP 地址

PPP :

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

书 P294

使用 HDLC (ISO) (高级数据链路控制) 作为 3 层的报文的封装

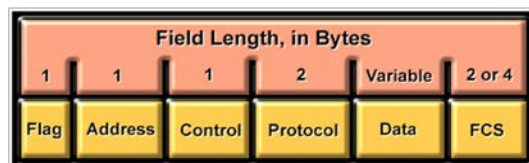
使用 LCP (Link control protocol) 链路控制协议：

建立连接，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

过程：书 P297

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