**第二章 交换技术**

**1.3类MAC地址以及包长的最大最小值**

(1)单播:第一个字节的最低位为0,可作为目的地址和源地址

如：00-e0-fc-00-00-06

(2)组播第一个字节的最低位为1,仅能作为目的地址

如：01-e0-fc-00-00-06

(3)广播:48位全为1

如：ff-ff-ff-ff-ff-ff

**2.****CSMA/CD工作方式(3个关键术语)**

(1)工作原理:

①发送数据前先侦听信道是否空闲,若空闲,则立即发送数据。若信道忙碌，则等待一段时间至信道中的信息传输结束后再发送数据;

②如果两台或两台以上主机同时监听到信道空闲并发松数据，则发生冲突;

③若侦听到冲突,则立即停止发送数据,等待一段随机时间,再重新尝试。

简单总结为:先听在发,边发边听,冲突停发,随即延后重发.

(2)关键术语:

①载波侦听:发送节点在发送数据之前,必须侦听传输介质(信道)是否处于空闲状态.

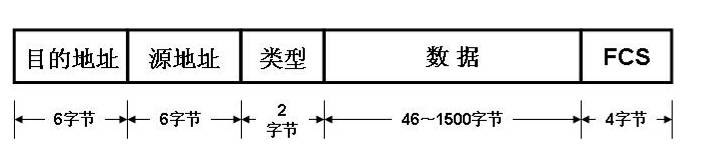
②多路访问:具有两种含义,既表示多个节点可以同时访问信道,也表示一个节点发送的数据可以被多个结点所接收.

③冲突检测:发送节点在发出数据的同时,还必须监听信道,判断是否发生冲突.

**3.****以太网帧格式和802.3格式的区别**

(1)帧格式

①EthernetII



各字段意义:

·目的地址:接受端的MAC地址,长度为6字节.

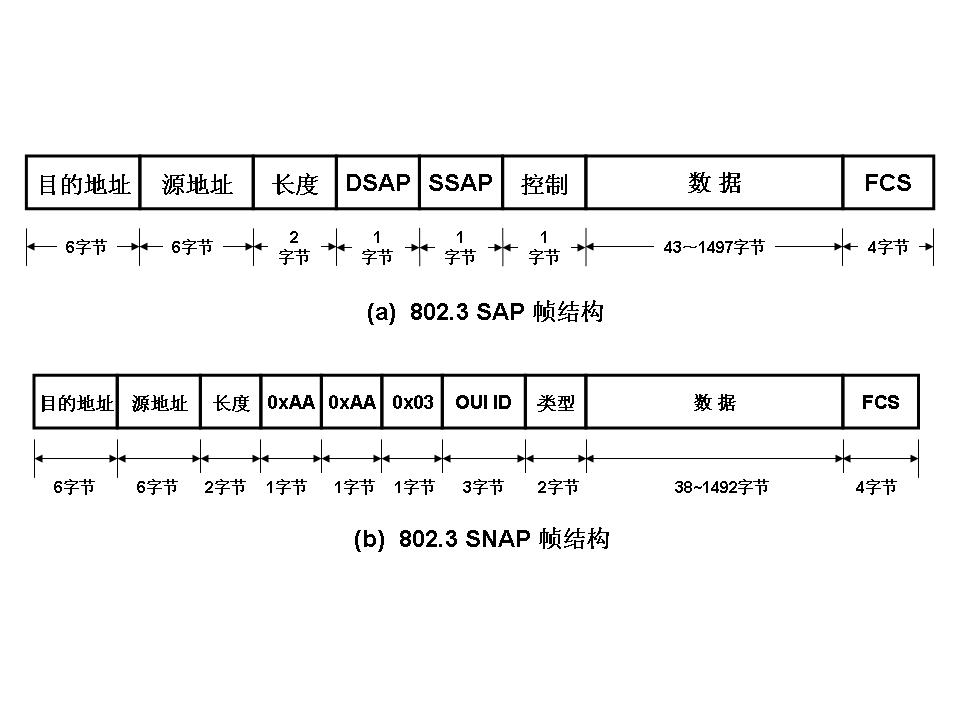
·源地址:发送端的MAC地址,长度为6字节

·类型:数据包的类型(即上层协议的类型),长度为2字节

·数据:被封装的数据包,长度为46字节-1500字节

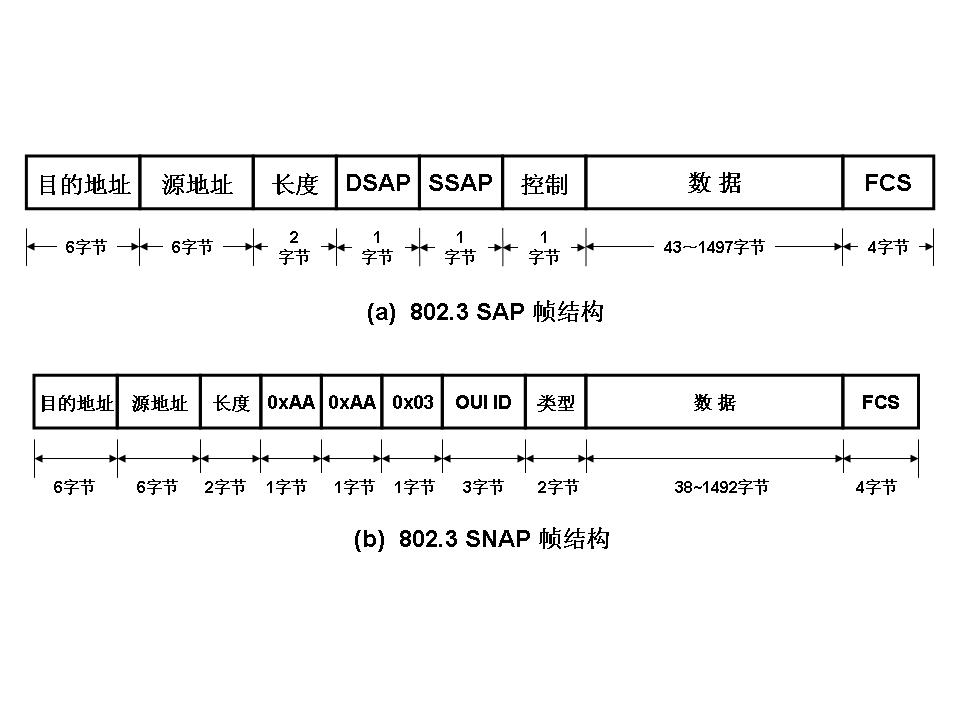
·校验码:错误检验,长度为4字节

②802.3 SAP帧结构



没有类型域(代之以长度域).在802.3 SAP帧中,新增的的802.2 LLC首部包括两个服务访问点:源服务访问点(SSAP)和目的服务访问点(DSAP).他们用于识别以太网帧所携带的上层数据类型.1字节的“控制”域,则用于指明该帧是信息帧、监控帧还是无编号帧.通常情况下,该字段被设置为0x03,指明是采用无连接服务的202.2无编号数据帧.

③802.3 SNAP帧结构



在802.3 SAP的基础上有添加了一个3字节的组织唯一标识符(OUI ID)域和一个2字节的类型域(同时将SAP的值置为AA),使其可以标识更多的上层协议类型

(2)区别

802.3 SNAP类型以太网帧格式和802.3 SAP类型以太网帧格式的主要区别在于:

①2字节的DSAP和SSAP字段内容被固定下来,其值为16进制数0XAA.

②1字节的“控制”字段内容被固定下来,其值为16进制数0x03.

③增加SNAP字段,由下面两项组成:

a.3字节的组织唯一标识符(OUI ID)字段,其值通常等于MAC地址的前3字节,即网络适配器厂商代码.

b.2字节的“类型”字段,用来标识以太网帧所携带的上层数据类型.

**4.冲突域和广播域的定义---------------------------------P46**

(1)冲突域:在[以太网](https://baike.baidu.com/item/%E4%BB%A5%E5%A4%AA%E7%BD%91)中，如果某个[CSMA/CD](https://baike.baidu.com/item/CSMA%2FCD)网络上的两台计算机在同时通信时会发生冲突，那么这个CSMA/CD网络就是一个冲突域.

(2)广播域:网络中的某一设备同时向网络中所有的其它设备发送数据，这个数据所能广播到的范围即为广播域.

**5.交换机的三项主要功能**

(1)MAC地址学习

(2)帧的转发和过滤

(3)消除第二层环路

**6.3种帧转发方式**

(1)直通转发

(2)存储转发

(3)无碎片直通转发

**7.交换机的访问方式**

(1)通过外带方式对交换机进行管理

(2)通过Telnet对交换机进行远程管理

(3)通过Web对交换机进行远程管理

(4)通过SNMP管理工作专对交换机进行远程管理

**8.交换机的三种工作模式以及子模式**

(1)用户模式:Switch>

(2)特权模式:Switch#

(3)配置模式:

①全局配置模式:Switch(config)#

②接口配置模式:Switch(config-if)#

③VLAN配置模式:Switch(config-vlan)#

④子接口配置模式:Switch(config-subif)#

⑤线路配置模式:Switch(config-line)#

⑥路由配置模式:Switch(config-router)#

⑦DHCP池配置模式:Switch(dhcp-config)#

**第三章 虚拟局域网(VLAN)**

**1.VLAN的主要功能和优点**

(1)具有的功能

①控制网络广播,提高网络性能;

②分隔网段,确保网络安全;

③简化网络管理,提高组网灵活性;

(2)优点

①由于实现了广播域隔离,VLAN可以将广播风暴控制在一个VLAN内部,划分VLAN后,随着广播域的缩小,网络中广播包消耗的贷款所占的比例大大降低,网络性能得到显著提高;

②不同的VLAN之间的数据传输是通过第三层(网络层)的路由来实现的,因此使用VLAN技术,结合数据链路层和网络层的交换设备可以搭建安全可靠的网络;

③由于VLAN是逻辑的而不是物理的,因此在规划网络时可以避免地理位置的限制.

**2.VLAN的定义方法**

(1)基于接口的VLAN(静态VLAN):根据以太网交换机的端口来划分VLAN.

(2)基于MAC地址的VLAN(动态VLAN):根据每个主机的MAC地址来划分VLAN.

(3)基于网络层的VLAN(动态VLAN):根据每个主机的网络层地址或协议类型(如果支持多协议)划分VLAN.

(4)基于IP组播的VLAN(动态VLAN):一个组播就是一个VLAN.

**3.IEEE 802.1q**

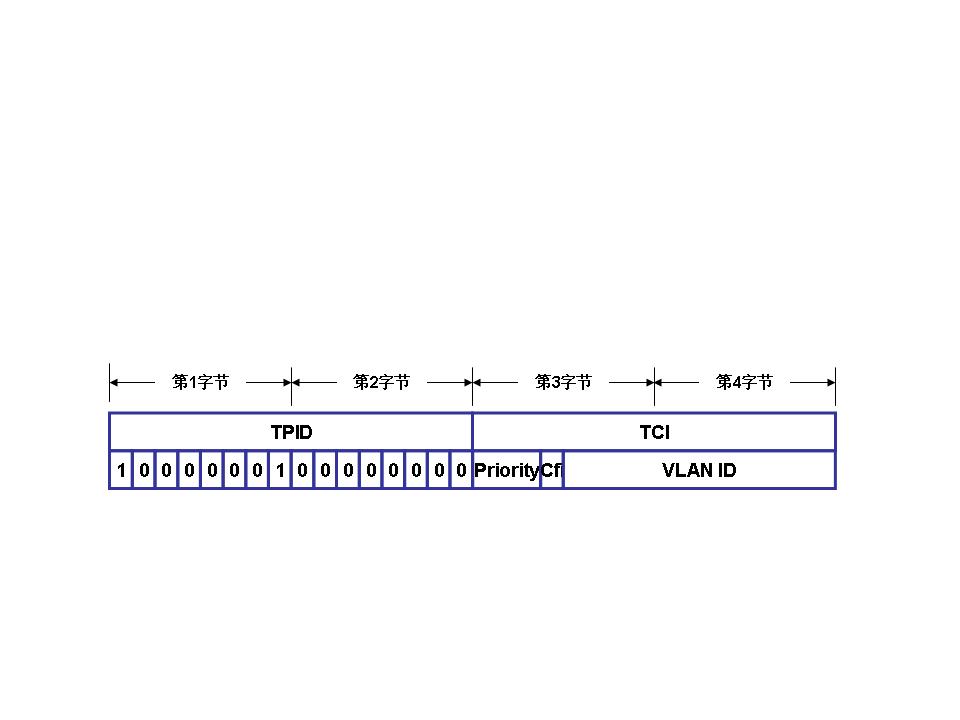
(1)802.1q帧格式



IEEE 802.1q使用4Byte的标记头来定义Tag(标记);

Tag头中包括2Byte的标签协议标识TPID(Tag Protocol Identifier)和2Byte的控制信息TCI(Tag Control Information)

(2)802.1q数据帧



标记协议标识(TPID):

固有值0x8100,表示该帧载有802.1q标记信息

标签控制信息(TCL):

Priority：3比特，表示优先级

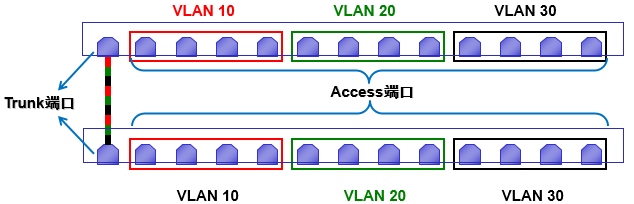
Canonical Format Indicator(CFI)：1比特，表示总线型以太网、FDDI、令牌环网

VlanID：12比特，表示VID，范围1－4094

(3)工作原理

交换机在从Trunk口转发数据前会在数据打上个Tag标签，在到达另一交换机后，再剥去此标签。

**4.Access接口和Trunk接口--------------------------------P79**



(1)Access接口(UnTagged接口),即接入接口

Access接口只能属于一个VLAN,它发送的帧不带有VLAN标签,一般用于连接计算机的端口,port VLAN.

通过查找MAC地址表,交换机对发往不同VLAN的数据不转发.

(2)Trunk接口(TagAware接口),即干道接口

可以允许多个VLAN通过,它发出的帧一般是带有VLAN标签的,一般用于交换机之间连接的端口,TAG VLAN.

在交换机之间或交换机与路由器之间，互相连接的端口上配置中继模式，使得属于不同VLAN的数据帧都可以通过这条中继链路进行传输。

**5.VLAN和Trunk的配置------------------------------------P80**

**6.VLAN间的通信-----------------------------------------P88**

(1)利用单臂路由实现VLAN间的通信

单臂路由:在路由器的物理接口上创建多个子接口,不同的子接口用于转发不同VLAN标签的数据帧,从而实现不同VLAN之间的通信.

①在路由器上为每个VLAN划分一个子接口

②每个子接口配置IP地址,作为相应VLAN的网关

③利用路由器的路由功能,实现不同子接口数据的转发

(2)利用三层交换机实现VLAN间的通信

①三层交换机内含交换机模块和路由器模块

②使用ASIC硬件处理路由，可以实现高速路由

③路由与交换模块内部汇聚连接，可以确保带宽

默认三层交换机的路由功能是开启的

默认交换机上的接口都是工作在2层的,只能识别2层数据帧(MAC地址)

可以将2层接口配置为3层接口,从而让接口可以识别3层数据包(IP地址)

SVI端口:交换机虚拟接口(Switch Virtual Interface)

三层设备交换机上配置SVI接口地址

各VLAN中主机将三层交换机上相应VLAN的SVI接口地址作为本VLAN网关

数据到达三层交换机后利用路由功能转发到其他VLAN

**第四章 局域网中的冗余链路**

**1.冗余拓扑带来的问题----------------------------------P104**

(1)冗余拓扑的目的

①减少网络因单点故障引起的停机损耗

②增加网络可靠性

(2)冗余拓扑带来的问题

①广播风暴

2层环路导致广播在网络中不停地转发（广播风暴）。会瞬间耗尽交换机所有处理能力，使交换机无法转发其它数据。

②多帧复制

2层环路会导致目标节点收到多个相同的数据帧。从而既浪费节点的处理能力又浪费网络带宽。

③MAC地址抖动

交换机上的 MAC地址表不稳定，导致交换机在MAC地址表学习上浪费更多资源

**2.生成树协议------------------------------------------P107**

STP协议的主要思想是当网络中存在备份链路时，只允许主链路激活，如果主链路失效，备份链路才会被打开。STP协议的本质就是利用图论中的生成树算法，对网络的物理结构不加改变，而在逻辑上切断环路，封闭某个网桥，提取连通图，形成一个生成树，以解决环路所造成的严重后果。

(1)工作原理

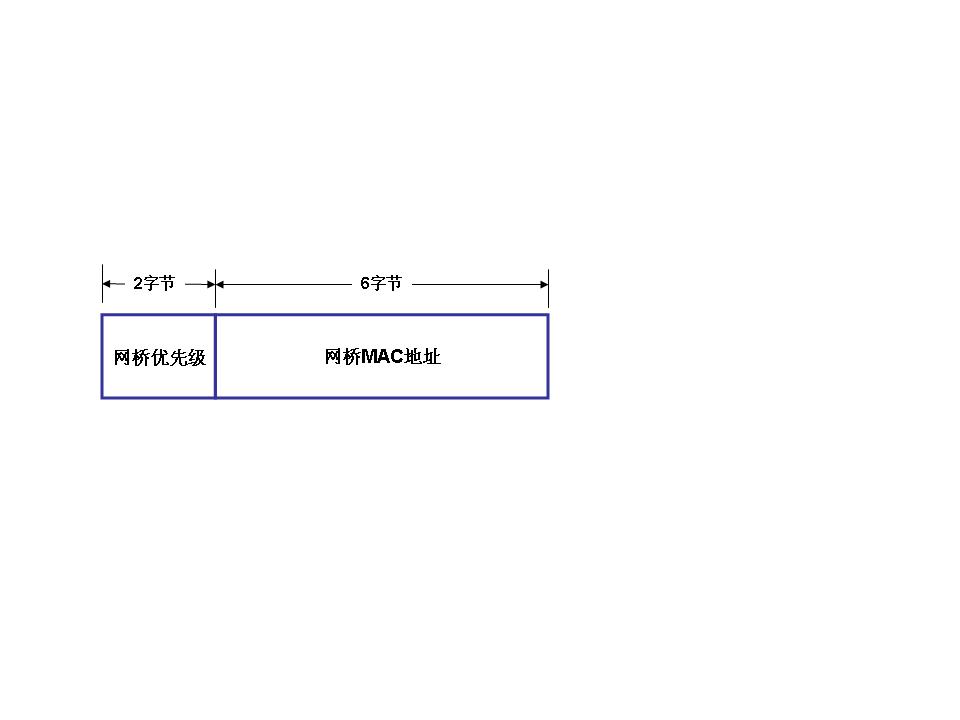
STP协议会阻塞冗余端口,使网络中的节点在通信时, 只有一条链路生效(没有冗余).

当通信链路出现故障时,将处于“阻塞状态”的端口重新打开,从而保证网络正常通信.

(2)基本概念

①根交换机(Root Bridge): 交换网络中所有交换机共同选举一台最低网桥ID的交换机为根交换机

②网桥ID(Brideg ID)=网桥优先级(Priority)+网桥MAC地址(BridgeAddr)

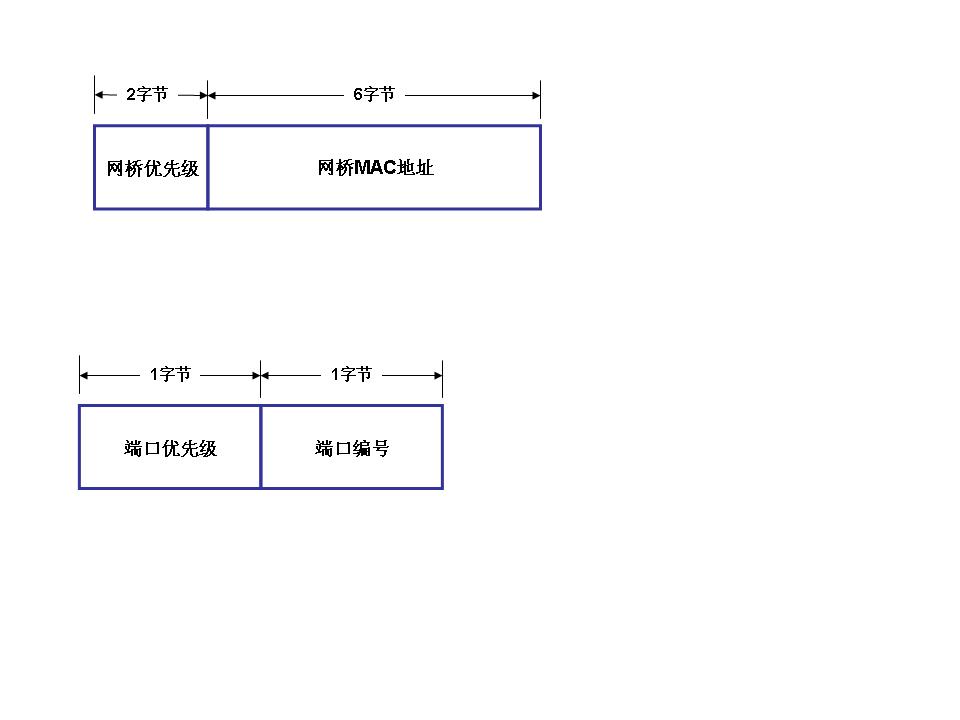


网桥优先级取值范围:0-65535,默认值为:32768(0x8000)

首先判断网桥优先级,优先级值最小的网桥将成为根网桥

如果网桥优先级相同,则比较网桥MAC地址,具有最低MAC地址的交换机或网桥将成为根网桥.

③端口ID(Prot ID)=端口优先级+端口编号



端口优先级是从0-255的数字,默认为128(0x80)

端口优先级越小,则优先级越高.

如果端口优先级相同,则编号值越小,优先级越高

④根路径开销(Root Path Cost):某交换机到根桥所经过的路径开销(与链路带宽有关)的总和

⑤根端口(Root ID):各个交换机通往根桥的根路径开销最低的端口,若有多个端口具有相同的根路径开销,则发送网桥ID最小的为根端口,如果网桥ID也相同,则发送端口ID最小的端口为根端口

⑥每个LAN中都有一个交换机被称为指定交换机(Designated Bridge),它是该LAN中与根桥连接而且路径开销最低的交换机

⑦指定端口(Designated Port):如果指定桥中有两个以上的端口连在这个LAN上,则具有最高优先级的端口被选举为指定端口.根桥上的端口都可以称为指定端口,交换机上除根端口之外的端口都可以称为指定端口.

⑧根端口和指定端口进入转发(Forwarding)状态,其他的冗余端口则处于阻塞(Discarding)状态.

(3)STP的工作过程

①选举一个根网桥(Root Bridge)

依据网桥ID选举根网桥,ID值最小者当选

②在每个非根网桥上选举一个根端口(Root Port)

选举依据:

根路径成本最小

发送网桥ID最小

发送端口ID最小

③在每个网段上选举一个指定端口(Designated Port),用于向根交换机发送和接受流量

选举依据:

根路径成本最小

所在交换机的网桥ID最小

端口ID最小

④阻塞非根端口,非指定端口,形成逻辑上无环路的拓扑结构

(4)STP的选举结果

①网络中选举出一个交换机为根交换机

②每个非根交换机都有一个根端口

③每个LAN都有指定交换机,每个指定交换机都有指定端口

④根端口和指定端口进入转发状态

⑤其他冗余端口处于阻塞状态

**3.快速生成树协议--------------------------------------P115**

(1)新增加的端口角色

①替代端口(Alternate Port)AP:为根端口到根网桥的连接提供了替代路径

②备份端口(Backup Port)BP:提供了到达同段网络的备份路径

(2)RSTP端口角色

①根端口(Root Port):根端口处于非根交换机上,根端口是本地交换机距离根交换机最近的端口.非根交换机通过根端口接受BPDU

②指定端口(Designated Port):RSTP的指定端口也和STP中的一样,指定端口是以太网段用于转发数据的端口

③替代端口(Alternate Port):替代端口是RSTP中新引入的端口角色,作为根端口的备份端口.替代端口可以接收BPDU报文但是不转发数据.

④备份端口(Backup Port):RSTP中的备份端口作为指定端口的备份端口,可以接收BPDU报文但是不转发数据.

(3)RSTP端口状态小结

①Forwarding端口：最优路径；

②Discarding端口：备份链路，备份端口：用于指定端口到生成树叶子节点的路径的备份，仅在到共享LAN网段有2个或2个以上连接，或2个端口通过点到点链路连接为环路时存在；

③Discarding状态端口充当两种角色（Alternate Port，Backup Port），从Alternate Port，Backup Port中选择到达Root的次优路径；

④当网络拓扑结构发生变化以后立刻转发  
 （收敛时间小于1秒）

(4)改进

①为根端口和指定端口设置了快速切换用的替换端口（Alternate Port）和备份端口（Backup Port）两种角色，当根端口/指定端口失效的情况下，替换端口/备份端口就会无时延的进入转发状态.

②在只连接了两个交换端口的点对点链路中，指定端口只需与下游交换机进行一次握手就可以无时延地进入转发状态；如果是连接了三台以上交换机的共享链路则需要等待两倍Forward Delay的时间；

③将直接与终端相连而不是与其他网桥相连的端口定义为边缘端口(Edge Port)。边缘端口可以直接进入转发状态，不需要任何延时。由于网桥无法知道端口是否直接与终端相连，因此需要人工配置。

**4.端口聚合--------------------------------------------P128**

端口聚合(又称为链路聚合),将交换机上的多个端口在物理上连接起来,在逻辑上捆绑在一起,形成一个拥有较大宽带的逻辑端口,形成一条干路,可以实现负载分担,并提供冗余链路.

(1)聚合端口Aggregate Port(AP):把多个物理接口捆绑在一起而形成的一个逻辑接口

聚合标砖:IEEEE 802.3ad

聚合优点:

扩展链路带宽

实现成员端口上的流量平衡

自动链路冗余备份

(2)端口聚合的流量平衡

流量平衡:把流量平均地分配到AP的成员链路中去

流量平衡的方式:

根据源MAC地址

根据目的MAC地址

根据源IP地址

根据目的IP地址

根据源、目标MAC地址

根据源、目标IP地址

(3)注意事项

AP成员端口的速率必须一致

AP成员端口必须属于同一个VLAN

AP成员端口使用的传输介质应相同

默认情况下创建的Aggregate Port 是二层AP

二层端口只能加入二层AP，三层端口只能加入三层AP

AP不能设置端口安全功能

当把端口加入一个不存在的AP时，AP会被自动创建

一个端口加入AP，端口的属性将被AP的属性所取代

一个端口从AP中删除，则端口的属性将恢复为其加入AP前的属性

当一个端口加入AP后，不能在该端口上进行任何配置，直到该端口退出AP

**第五章 IP协议及子网规划**

**关于IP地址的计算题**

**第六章 路由技术**

**1.静态路由、默认路由与浮动路由-------------------------P168**

(1)静态路由:指由网络管理员手工配置的路由信息.

配置如:Router(config)#ip route 目的IP网段 目的IP掩码 下一跳IP地址

(2)默认路由:指路由表中未直接列出目标网络的路由选择项,它用于在不明确的情况下指示数据帧下一跳的方向.

配置如:Router(config)#ip route 0.0.0.0 0.0.0.0 下一跳IP地址©©©

(3)浮动路由:指当首选路由发生失败的时候,启动的备份路由.

配置如: Router(config)#ip route 目的IP网段 目的IP掩码 下一跳IP地址 管理距离

**2.动态路由协议的分类----------------------------------P176**

(1)动态路由协议按运行的区域范围划分如下:

①Interior gateway protocol(IGP):内部网关协议,用来在同一个自治系统内部交换路由信息.

②Exterior gateway protocol(EGP):外部网关协议,用来在不同的自治系统间交换路由信息.

(2)IGP内根据路由选择协议的算法不同划分如下:

①距离矢量(distance vector):根据距离矢量算法,确定网络中节点的方向与距离.包括RIP路由协议及IGRP(cisco私有协议)路由协议.

②链路状态(link-state):根据链路状态算法,计算生成网络的拓扑.包括OSPF路由协议与IS-IS路由协议.

③混合算法(hybird):根据距离矢量和链路状态的某些方面进行集成.包括EIGRP路由协议(cisco私有协议).

**第七章 RIP路由协议**

**1.防止路由环路的方法----------------------------------P189**

(1)路由毒化

使用毒化路由传播关于路由失效的坏消息.

(2)引入最大跳数

解决数据在网络上无休止的循环,导致的跳数趋于无穷大.

默认最大跳数为15跳,每经过一个设备,跳数加1.因此,数据包在网络上的循环次数是有限的.

16跳为不可达.缺点是限制了网络的规模

(3)水平分割

解决路由器收到自己发出的路由信息,且路由信息是不正确的,从而导致路由表不正确产生的环路.

路由器记住每一条路由信息的来源，并且不在收到这条信息的端口上再次发送它 ，从而解决了上述问题

(4)触发更新

解决更新周期过长,在周期内无法收敛的现象.

得知网络拓扑结构发生改变，不等待发送周期，立刻通告更新的路由表.

触发更新不受更新计时器限制，可以快速的将失败的路由同步到邻居。从而加快收敛速度避免环路.

(5)毒性逆转

解决失败的网络连接因为水平分割而不能同步到其他路由器,导致数据在网路上环路的情况.

当路由器学习到一条毒化路由（度量值为16）时，对这条路由忽略水平分割的规则，并通告毒化的路由

(6)抑制计时器

解决网络中部稳定的网络连接导致无法收敛,从而出现环路的情况.

在抑制时间内，失效的路由不接受任何更新信息，除非这条信息是从原始通告这条路由的路由器来的

时间一般是180s

减少了路由的浮动，增加了网络的稳定性

**2.RIP版本1和版本2的区别------------------------------P193**

(1)RIPv1是有类路由协议，RIPv2是无类路由协议

(2)RIPv1不能支持VLSM，RIPv2可以支持VLSM

(3)RIPv1没有认证的功能，RIPv2可以支持认证，并且有明文和MD5两种认证

(4)RIPv1没有手工汇总的功能，RIPv2可以在关闭自动汇总的前提下，进行手工汇总

(5)RIPv1是广播更新，RIPv2是组播更新，地址：224.0.0.9

(6)RIPv1对路由没有标记的功能，RIPv2可以对路由打标记（tag），用于过滤和做策略

(7)RIPv1发送的updata最多可以携带25条路由条目，RIPv2在有认证的情况下最多只能携带24条路由

(8)RIPv1发送的updata包里面没有next-hop属性，RIPv2有next-hop属性，可以用与路由更新的重定向。

**3.RIP协议的配置---------------------------------------P195**

**第八章 OSPF路由协议**

**1.OSPF分组--------------------------------------------P224**



**2.多区域OSPF的一些概念---------------------------------PPT**

(1)残域:其他区域产生的lsa,只有第三类lsa能进来,其他的4类,5类都会被ABR过滤掉.该区域的路由器也不能引入外部路由.

(2)完全末节:其他区域的lsa都进不来,包括第三类的,该区域的ABR会产生一个缺省的3类lsa,区域内其他路由器通过这条lsa,计算出默认路由.

(3)次残域:这个区域可以引入外部路由.3类lsa可以进来,但是4类和5类lsa仍然被过滤,引入的外部路由会以7类lsa的形式存在,ABR也会产生一个缺省的7类lsa,其他路由器通过这条lsa计算出默认路由.

(4)完全次残域:连3类lsa都过滤掉,即其他区域产生的lsa将无法进入该区域.但是ABR会产生一个缺省的3类lsa,其他路由器通过这条lsa计算出默认路由.

**第九章 点对点协议PPP**

**1.PAP和CHAP的认证过程和区别---------------------------P239**

(1)PAP的认证过程

PAP(Password Authentication Protocol)密码验证协议,通过两次握手机制,为建立远程节点的验证提供了简单的方法.



PAP认证过程经过两个阶段,习惯上被称为两次握手:

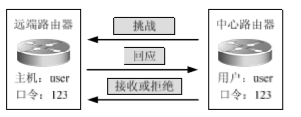
第一阶段为被验证方(远端路由器)发送用户名和口令到验证方;

第二阶段为验证方(中心路由器)对接收的用户名和口令进行验证,并根据结构接收或拒绝链路连接的认证请求.

PAP认证可以在一方进行,即由一方认证另一方的身份,也可以进行双向身份认证.这是将要求通信的双方都要通过对方的认证,否则,无法建立两者之间的链路.

(2)CHAP的认证过程

CHAP(Challenge Hand Authentication Protocol)挑战握手验证协议,使用三次握手机制来启动一条链路和周期性的验证远程节点.



CHAP的认证过程包含三个阶段,通常被称为三次握手:

第一阶段:当被验证方(远端路由器)向验证方(中心路由器)发送用户名做请求连接后,验证方向被验证方发送一串随机字符(“挑战”阶段);

第二阶段:被验证方利用MD5算法对口令和接收到的随机字符串进行加密产生密文,并将密文发送给被验证方(“回应”阶段);

第三阶段:验证方利用同样的方式对随机字符串和用户数据库中的记录进行加密,并将产生的密文与接收的密文进行比较,然后根据比较结果接收或拒绝连接请求.

(3)PAP与CHAP的区别

PAP是简单二次握手身份验证协议,用户名和密码明文传送,安全性低.

CHAP是一种挑战响应式协议,三次握手身份验证,口令信息加密传送,安全性高；同时，CHAP的身份认证可以随时进行，包括在双方正常通信的过程中。因此，非法用户即使截获并成功破译了一次密码，此密码也将在一段时间内失效。

**第十章 园区网安全**

**1.端口安全--------------------------------------------P255**

(1)基本功能

①限制交换机端口的最大连接数

②端口的安全地址绑定

**2.端口安全的配置--------------------------------------P256**

**3.访问控制列表的基础知识------------------------------P259**

访问控制列表(Access Control List,ACL)是一个有序的语句集,它通过对比报文中字段值与访问控制列表参数,来允许或拒绝报文通过某个接口.

(1)访问控制列表的作用

①安全控制

②流量过滤

③数据流量标识

(2)ACL语句组成

①条件:用来匹配数据包中字段值

②操作:条件匹配时,可以采取允许和拒绝两个操作

(3)ACL种类

①标准ACL:只能过滤IP数据包头中的源IP地址

②扩展ACL:可以过滤源IP地址、目的IP地址、协议(TCP/IP)、协议信息(端口号、标志代码)等

③MAC ACL:可以过滤源MAC、目标MAC等

④专家ACL:可以过滤源IP、源MAC、源端口、目标IP、目标MAC、目标端口、时间等

⑤时间ACL:可以根据时间段进行扩展ACL过滤

(4)ACL编号范围



**4.ACL的配置**

**第十一章 网络地址转换(NAT)**

**1.NAT术语---------------------------------------------P280**

(1)内部本地IP地址

分配给内部网络主机的IP地址,可能是非法的未向相关机关注册的IP地址,也可能是合法的私有地址.

(2)内部全局IP地址

合法的全局可路由地址,在外部网络代表着一个或多个内部本地地址.

(3)外部本地IP地址

外部网络的主机在内部网络中表现的IP地址,该地址是内部可路由地址,往往是一个公网地址.

(4)外部全局IP地址

外部网络分配给外部主机的IP地址,可能是一个私网地址.

**2.NAT/NAPT的概念---------------------------------P279/P288**

(1)网络地址转换NAT(Network Address Translation),它是一种把内部私有网络地址翻译成合法公网IP地址的技术

(2)网络地址端口转换NAPT(Network Address Port Translation)，是动态NAT的一种实现形式,NAPT利用不同的端口号将多个内部IP地址转换为一个外部IP地址.

(3)NAT和NAPT的区别

NAPT不仅转换IP包中的IP地址,还对IP包中TCP和UDP的Port进行转换.这使得多台私有网主机利用1个NAT公共IP就可以同时和公共网进行通信.

**第十三章 网络规划与设计**

**网络层次化以及各层次的作用----------------------------P317**

(1)接入层(Access Layer)

①功能

接入层为用户提供对网络的访问接口,是整个网络的可见部分,也是用户与该网的连接场所.

②特点

建立独特的冲突域

建立工作组与汇聚层的连接

部署用户的安全接入控制决策

(2)汇聚层(Distribution Layer)

①功能

用于把大量接入层的路径进行汇聚和集中,并连接至核心层,同时在接入层和核心层之间提供协议转换和带宽管理

②特点

广播域的划分

不同网段之间的互相访问

用户访问网络的权限控制

(3)核心层(Core Layer)

①功能

核心层为网络提供了骨干组件或高速交换组件.在纯粹的分层设计中,核心层只完成数据交换的特殊任务

②特点

提高可靠性

提供冗余链路

提供故障隔离

迅速适应升级

提供较少的延时和良好的可管理性