基础

**IP地址**

V4: 32位 42亿(2的32次方)

V6: 128位 (2的128次方)

169.254.xxx.xxx 无效的临时地址 (此地址不能用)

127. 回环

**Mac地址**

物理地址 硬件地址

48位/6字节 看到的是十六进制 前面是厂商

一个数据帧最大运输大小1500字节

Ifconfig ---> mtu 后的为 1500

网络位: 所在的网段

主机位: 网段下的第几个主机

192.168.1.0: 网络id

单播 1对1

组播 1对多

广播 1对所有

E口是百兆 交换机 接口起始序号: 0/0/1

G口是千兆 路由器 接口起始序号: 0/0/0

### 交换机

作用: 交换机是组建网络的基本设备,能够实现不同设备数据共享

其实华为的交换机也具备三层交换机的功能,只是性能比较差,把他仍在核心地带不合适,所以作为普通交换机来用

Mac地址表

交换机工作原理

学习--学习源mac地址,记录对应的接口号

交换机连交换机,还是这个过程(若接口下有多个mac地址,都记录)

广播--向除了数据来源之外的所有接口发送信息

转发--1对1进行数据传递

更新--超过300秒无任何数据通讯,mac地址记录将被删除

接口设备更换,或者接口down掉

<Huawei>display mac-address //查看mac地址表

### 转发决策

交换机的转发决策有三种操作：丢弃、转发和扩散。

丢弃：当本端口下的主机访问已知本端口下的主机时丢弃。

转发：当某端口下的主机访问已知某端口下的主机时转发。

扩散：当某端口下的[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA" \t "/home/student/文档\\x/_blank)访问未知端口下的主机时要扩散。

每个操作都要记录下发包端的MAC地址，以备其它主机路由器: 实体接口配ip

三层交换机: 虚拟接口(vlan)配ip

原理: 数据包vlan标签转换

的访问。

**Vlan ---> virtual LAN**

**-- 虚拟局域网**

**4096 4094可用**

他不是用物理方式划分广播域, 而是软件层次,相当于物理隔离

**相同广播域:** 能够接受到同一组广播的区域

一个vlan就是一个广播域

通常交换机能创建有4096个vlan,有的是1000多个,控制在1000左右即可

vlan标记 默认vlan1

交换机默认不给数据包打标记

若数据包没有打vlan记号, 接口收到数据后会认为数据是跟自己是一个vlan进行数据转发

例如: 两个交换机相连, 左交换机口: vlan1, 右交换机口: vlan2 那vlan1就能ping同对面的vlan2,不能ping同对面的vlan1,这样会错乱,所以trunk来解决

作用: ①控制广播

②增加安全(如: 不能访问财务部数据)

③提高带宽利用率

④降低数据延迟

**接口组**

将一批接口加入组中, 对组的操作=对组成员的操作

**Trunk中继链路**

让接口可以承载多个vlan, 给数据打上vlan标记

让链路具备识别能力

需恢复接口配置, 接口配置过,就不能配其他的配置了

一般只有交换机连接交换机才需要trunk 或连接的是建有多台虚拟机的服务器,虚拟机配的不同网段的地址

**聚合链路**

建出一个虚拟接口,将做聚合链路的接口加入到虚拟接口

一个虚拟接口可容纳63组聚合

--虚拟接口名: interface eth-trunk

--配置:

需恢复接口配置!!!!!

在虚拟接口里配置trunk什么的,跟在普通接口里配置一样

区别: eth-trunk group组

虚拟接口可以将接口捆绑，但组不是

######################################################

**路由器**

交换机: 控制广播域 不能通信

路由器: 控制广播域 , 同时还能通信 或 连接不同网段

指路, 且是通往目标最畅通的路

作用: 传递不同网段的数据,实现不同网段互通

网关: 让主机能从一个网段跑到另一个网段的地址

跨网段ping的时候,可能第一个包可能是超时的, 这正常,之后就不会超时了

**路由表**

路由的核心, 能不能转发, 在于此表

看24位的,

#destination: 目标地址

#nexthop: 下一跳

#32位的为自身连接的

#direct: 直连路由,由设备接口配置好的ip,并且接口是开启状态,这样才会生成

**1.直连路由:**

由设备接口配置好的ip,并且接口是开启状态,这样才会生成

**2.静态路由**

手动配置 下一跳 告诉路由器方向

**3.动态路由**

基于某种路由协议(动态路由协议,**ospf**是其中一种)

减少管理任务(不为配置吓一跳而头疼)

都开启动态路由, 路由表 会趋向于同步

**动态路由协议:** **OSPF: (开放式最短路径优先)**

**原理: 数据包vlan标签转换**

**--宣告:** 最关键的动作

--区域划分: 每个ospf路由器只维护所在区域的完整链路状态信息

--区域ID:

--(默认区域)区域0: 第一个区域, 第一个区域必须为0 不能从1开始

适合大型网络协议

网络特别大时, 可以做区域划分

配置:

开启ospf 序号 协议 --> 定义区域 --> 对外宣告(**网段**, **反掩码**)

弹出loadingdone为交流结束

1. **默认路由(特殊的静态路由)**

实质: 是把静态路由的”目标ip”变为 0.0.0.0 (全部网段)

(ip route-static **0.0.0.0 0**  192.168.2.2)

若路由器接到自己不知道的目标网段,就交给就往2.2扔

其实就是静态路由, 就是比较特殊

所以可以匹配任意网段

**Nat (网络地址转换)**

作用: 将内部与外部地址进行转换,实现内外互通

节省公网ip

1. **静态nat**
2. **Easy IP**

######################################################

**三层交换机**

本质还是交换机,数据链路层 接口无法直接配置ip

路由器: 实体接口配ip

三层交换机: 虚拟接口(vlan)配ip

原理: 数据包vlan标签转换

当数据到达三层交换机后, 看目的ip, 再看目的ip段在哪个vlan, 此vlan对应哪个接口, 将数据转发给此接口,数据的vlan会变成目标ip段的vlan

给vlan配ip 可对vlan下的网段做标识, 以便知道该往哪转发数据

起始接口: g0/0/1

虚拟接口名: interface vlanif 序号

Vlan ----> interface vlanif

进入vlanif接口中, 就相当与进入虚拟接口

把实际接口加入vlan, 给vlanif配ip,

三层交换机 连接 交换机 配置trunk

######################################################

Tcp:传输控制协议

可靠,面向链接

Udp:用户数据报协议

不可靠,无连接的服务

######################################################

**ACL 访问控制列表 反掩码 进/出**

基本acl 2000-2999 源ip

高级acl 3000-3999 源ip 目标ip 端口 协议

定义规则 放入接口：　进 / 出

**匹配即停止**

基本acl:

] rule permit|deny source 192.168.2.1 0 //允许 源192.168.2.1

# permit／deny: => 允许／拒绝

# source => 源

# 0 => 0.0.0.0(**反掩码)** 就匹配这个主机ip (针对一个ip)

# 0.0.0.255 => 匹配到: 192.168.2.x 即为匹配 (匹配一个网段)

[进入接口] traffic-filter inbound acl 2000　　　　//将规则放入接口