**命令行**

**交换机基本命令：**

**交换机命令行模式：enable,进入特权模式，configure termianl 进入全局配置模式；**

**全局配置模式中：interface fastEthernet 0/1 快速进入接口模式**

**配置交换机主机名：全局配置模式中：hostname +名字**

**查看交换机的配置：特权模式下：show running-config**

**显示IOS系统版本信息：特权模式下：show version**

**配置明文口令：全局配置模式下：enable password +密码,然后退出查看**

**特权模式下查看：show running-config**

**配置enable加密口令：全局配置模式下：enable secret +密码，然后退出查看**

**特权模式下查看：show running-config**

**配置Console口令：全局配置模式下：line console 0**

**Console接口模式下：password 密码**

**:login【生效】**

**保存交换机的配置：特权模式下：copy running-config startup-config**

**或者：write**

**恢复设备出长默认值：特权模式下：erase startup-config**

**重启生效：reload**

**取消自动退出配置界面：全局配置模式下：line consoe 0**

**console 0接口下：exet-timeout0 0**

**取消打断命令输入：全局配置模式下：line consoe 0**

**console 0接口下:logging synchronous**

**禁止用DNS查询：全局配置模式下：no ip domain-lookup**

**交换机配置命令**

**查看MAC地址表：特权模式下：show mac-address-table**

**查看邻居设备信息：特权模式下：show cdp neighbor**

**交换机指定工作模式的配置：接口模式下：duplex【full/half/auto】**

**指定接口额通信速率：接口模式下：speed【10/100/1000/auto】**

**查看接口的工作模式和通信速率：特权模式下：show interface fastEthernet 0/24**

**配置管理ip地址：全局配置模式下：interface vlan 1【进入虚拟vlan1口】**

**在vlan1接口模式下：ip address +ip**

**打开虚拟vlan1接口：no shutdown**

**交换机配置网关：全局配置模式下：ip default-gateway +网关**

**Telent【远程】**

**在交换机【路由器一样的操作】：--全局模式下配置：line vty 0 4 (允许5用户同时登陆)**

**设置密码：Password 密码【如果不想用密码直接 no login】**

**然后退出到全局配置模式下配置明文密码：enable password + 密码**

**在windows下操作：telnet +ip地址**

**ARP缓存的查询：在windows系统操作：arp -a**

**Ping命令使用及ICMP协议：ping -t/-l +目标ip 【-t表示ping通之后不会停止，-l是改变字节】**

**静态路由，浮动路由，默认路由**

**使用 ip route 命令达到指定ip 目的网络：**

**手动添加路由表：**

**全局模式下：ip route 目标网络ID 子掩网码 下一跳（向哪一条路走）**

**默认路由：ip route 0.0.0.0 0.0.0.0 +下一跳**

**如果想要用PC ping通跨网段的交换机，那么交换机上也必须配上网关**

**VLAN的配置：**

**将端口加入VLAN**

**在全局模式中进入将要被加入的端口：interface fastEthernet 0/1**

**:switchport access vlan 2**

**如果我想要将0/1端口从VLAN2中删除，那么我需要进入0/1端口：**

**：no switchport access vlan 2**

**同时将多个端口加入vlan中，需要进入组：全局模式下：interface range fastEthetnet 0/1-10**

**：switchport access vlan 2**

**如果想要将此组删除，那么我需要进入此组：interface range fastEthetnet 0/1-10**

**：no switchport access vlan 2**

**Show vlan brief**

**Show vlan id 2**

**VLAN Trunk的配置：**

**进入接口模式：interface fastEthernet 0/1**

**查看接口模式特权模式下：show interface fastEthernet 0/1 swtichport**

**:swtichport mode +模式**

**从VLAN中添加，删除VLAN**

**去除VLAN**

**接口模式下：switchport allowed vlan remove +数字**

**添加VLAN**

**接口模式下：switchport allowed vlan add +数字**

**配置以太网通道(不同vlan间通信只需要一条线)**

**配置接口为以太通道模式：**

**在全局配置模式中：interface range fastEthernet 0/1-3 【若不是连续0/1,f0/3】,将1-3接口捆绑一在一起**

**：channel-group 1 mode on【1表示以太网的序号，可以为别的数字】**

**重新配置trunk 链路**

**进入以太网通道：interface fastEthernet port-channel 1**

**配置trunk链路:Switchport mode trunk**

**单独一个接口也可以加入组：**

**进入需要加入的接口：interface fastEthernet0/5**

**：channel-group 1 mode on**

**从以太网通道中删除某一个端口，进入将要被删除的接口**

**：interface fastEthernet0/7**

**：on channel-group 1 mode on**

**DHCP服务配置 【自动获取IP配置】**

**DHCP：动态主机配置协议：**

**定义IP地址池：全局配置模式：ip dhcp pool +名字**

**动态分配IP地址段：network 加某网段**

**设定网关地址： default-router +网关**

**为客户段配置DNS地址：dns-server+DNS(例如：8.8.8.8)**

**预留静态IP地址：ip dhcp excluded-address + IP地址【比如我想留下一段IP 那么：192.168.1.2 192.168.1.9】**

**预留静态IP 地址，是为其他服务工作的设备准备的，为了就是在池中预留下的，比如打印机，：**

**三层交换的配置命令：**

**启动路由功能**

**全局模式下：ip routing 【启用路由功能】**

**配置虚拟接口的ip:**

**全局模式下：interface vlan 1 【进入vlan】**

**：ip address ip地址**

**：no shutdown 【打开】**

**配置路由接口：no switchport【在三层交换机上，使用接口进行配置IP的时候进行】**

**在三层交换机上配置trunk链路，并接口封装为802.1q**

**全局配置模式中：interface fastEthernet0/24**

**:switchport trunk encapsulation dot1q**

**:switchport mode trunk**

**RIP的配置：【动态路由设置】**

**全局模式下：router rip**

**:version 2 【启用版本2】**

**：no auto-sunnary 【关闭自动汇总】**

**：net 主网络ID【进行网段的喊话】**

**OSPF动态路由协议【内部网关协议】设置**

**启用路由功能：ip routing**

**全局配置模式下：router ospf + 名字**

**：network + 网段 + 反子网掩码 area 0**

**HSRP热备份路由协议**

**配置HSRP：**

**配置为HSRP的成员：【当只有一台交换机的时候，可以在物理接口上，当有两台交换机，不管有没有划分vlan ,在vlan 接口模式配置比较方便，主要在vlan 接口模式中配置】**

**Standby + 数字【任意】 ip + 地址**

**配置成为HSRP配置速端口**

**接口模式下：优先级：**

**Standby + 数字【任意】 priority +数字【范围0-255，默认100】【数字越大，优先级越高】**

**查看HSRP摘要信息【特权模式】：show standby brief**

**配置HSRP的占先权**

**优先级高的路由器重新获得转发权，恢复成为活跃路由器**

**HSRP占先权配置：【物理接口模式下】**

**:Standby + 数字【任意】 + preempt**

**PVST+ 的配置命令【每个VLAN中生成树】：主要是为了负载分但，负载均衡**

**启用生成树命令：**

**全局模式下：spanning-treev vlan +2【比如vlan2】**

**指定根网桥：spanning-treev vlan 2 priority +数字【必须是4096的倍数】**

**指定主根，次根：spanning-treev vlan 2 root primary/secondary**

**查看生成树的配置：特权模式下：show spanning-tree**

**查看某个VLAN的生成树详细信息：**

**特权模式下：show spanning-tree vlan**

**配置速端口**

**接口模式下：spanning-tree portfast 【物理端口，为了就是不浪费时间运行生成树法则】**

**访问控制列表配置：**

**标准访问控制列表  
 创建ACL：**

**全局模式下：**

**access -list + 1【序号1-99】 permit/deny +host +源ip + host目标地址**

**应用示例：**

**access -list 1 deny 192.168.1.1 0.0.0.0 【禁止这个IP的主机通过】 可以写成：access -list 1 deny host 192.168.1.1**

**access -list 1 permit 192.168.1.1 0.0.0.255 (反掩码可以写成any：access -list + 1 permit any )【允许这个网段通过】【读取的顺序就是设置的顺序，所以应该先设置禁止的在设置允许通过的】**

**将ACL应用于接口：【物理接口】**

**接口模式下：ip access-group 1 in/out【应用于出口还是进口】**

**取消在前面加 no**

**查看访问控制列表：特权模式下：show access-list**

**扩展ACL的配置**

**创建ACL：**

**全局模式下：access-list 100 【序号，99-199之间】deny tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq www**

**permit ip any any【只允许来自192.168.1.1通过查看**

**号100-199】 + permit/deny + 协议 +host地址 + host目标地址 + eq +端口号**

**删除ACL：在全局模式下：no access-list 10**

**将ACL应用于接口：【物理接口】**

**接口模式下：ip access-group 1 in/out【应用于出口还是进口】**

**在接口上取消ACL应用：no ip address-group 1 in**

**应用示例：**

**全局模式下：**

**1. access-list 105 permit tcp 192.168.1.1 0.0.0.255 host 192.168.2.1 eq 80【80是www的端口号】 只允许192.168.1.0这个网段访问192.168.2.1的www**

**access-list 105 deny ip any any【其他任何都不行】**

**2.access-list 105 deny tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq www**

**access-list 105 permit ip any any**

**标准命名ACL**

**创建ACL：**

**全局模式下：ip access-list standby + 名字**

**应用示例：**

**Ip access-list standby + 名字**

**Perimit host 192.168.1.1**

**deny any**

**只允许来自192.168.1.1通过查看**

**查看ACL配置信息**

**特权模式：show access-list**

**更改ACL内的条件：**

**全局配置模式：Ip access-list ciso**

**15 permit host 192.168.2.1【添加 15 允许来自主机192.168.2.1通过】**

**【删除组中单一ACL：no 20 (删除序列号就行)】**

**将ACL应用于接口:ip access-group + 名字**

**将ACL在接口上取消：ip access-group + 名字**

**扩展命名ACL的配置**

**创建ACL：**

**全局模式下：ip access-list extended + 名字**

**应用示例：**

**Ip access-list standby + 名字**

**deny tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq www**

**permit ip any any 只允许来自192.168.1.1通过查看**

**查看ACL配置信息**

**特权模式：show access-list**

**更改ACL内的条件：**

**全局配置模式：Ip access-list standby + 名字**

**15 permit host 192.168.2.1 host 192.168.2.2【添加 15 允许来自主机192.168.2.1通过】**

**【删除组中单一ACL：no 20 (删除序列号就行)】**

**将ACL应用于接口:ip access-group + 名字**

**将ACL在接口上取消：ip access-group + 名字**

**NAT静态，动态转换**

**静态NAT的配置：**

**全局配置模式下: ip inside source static + 源私有地址【需要被转化的私有ip】 +公有地址 【没有被物理接口使用的】**

**在端口上应用 ：interface fastEthernet0/1**

**: ip nat outside**

**: interface fastEthernet0/0**

**: ip nat in side**

**配置默认路由：ip route 0.0.0.0 0.0.0.0 + 下一跳**

**动态NAT的配置：**

**定义将要被转换的地址列表：**

**全局模式下：**

**access-list 1 permit 192.168.1.0 0.0.0.255**

**定义动态转换为的地址池**

**全局模式下：**

**Ip nat pool + DNS【起的名字】 + 61.159.62.131 61.159.62.134【一段的公有IP】+反子网掩码**

**将列表1转换为DNS**

**全局模式下：ip nat inside source list 1 pool NDS**

**在端口上应用 ：interface fastEthernet0/1**

**: ip nat outside**

**: interface fastEthernet0/0**

**: ip nat in side**

**配置默认路由：ip route 0.0.0.0 0.0.0.0 + 下一跳**

**PAT 的配置**

**定义内部访问列表：**

**全局模式下：access-list 1 permit 192.168.10.0 0.0.0.255**

**定义合法的IP地址，直接使用外部接口地址，所以不再定义地址池，设置复用动态的IP 地址转换：**

**全局模式下：ip nat inside source list 1 interface fastEthernet 0/1 【外部接口】 overload**

**在端口上应用 ：interface fastEthernet0/1**

**: ip nat outside**

**: interface fastEthernet0/0**

**: ip nat in side**

**查看NAT转换条目：特权模式下：show ip nat translations**

**清楚NAT转换条目：clear ip nat translation【静态NAT条目不会被清楚】**

**跟踪NAT【只要有关于NAT的操作就会显示】： debug ip nat**

**取消跟踪NAT【只要有关于NAT的操作就会显示】：undebug ip nat**