网络功能：

资源共享

信息传递

提高可靠性 云盘

增加系统处理能力 web

分组交换

tcp/ip

web技术

iso

ieee

点到点 广域网

星形 易于实现 方便故障排查

网状 提高可靠性

osi七层模型 （理论框架）

tcp/ip五层模型 （实际应用）

10000Mbit

100000000bit

1k=1000

1M=1000k

物理层 数据链路层 网络层 传输层 会话层 表示层 应用层

http https dns ftp tftp smtp snmp

tcp udp

icmp igmp arp ip

物理层 数据链路层 网络层 传输层 应用层

比特流 数据帧 数据包 数据段

网卡 交换机 路由器 防火墙 计算机

100M cat5

100M cat5e 超五类

1000M cat6

10000M cat7

UTP 非屏蔽双绞线 STP 屏蔽双绞线

568A

568B

直通线

交叉线

全反线

准备win2008环境，密码Taren1

用户模式

Switch>

特权模式（一般用于查看配置信息）

Switch>enable

Switch#

全局配置模式（所做的配置对整个设备生效）

Switch#configure terminal

Switch(config)#

接口模式

Switch(config)#interface fastEthernet 0/1

Switch(config-if)#

exit 返回上一模式

end或快捷键 crtl+z 返回特权模式

思科设备命令行不区分大小写，与Linux命令行不同

命令输入错误卡住时同时按键盘ctrl+shift+6这三个键即可

远程控制终端软件：

SecureCRT

Xshell

no

Switch(config)# hostname s1 //配置主机名

s1# show running-config //查看当前的运行配置

Switch(config)#enable password 123 //配置密码为123，之后退出到用户模式再次进入特权模式测试密码

Switch#copy running-config startup-config //保存配置

Switch#write //保存配置，同上效果

Switch#erase startup-config //删除配置文件，恢复出厂设置

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] //此时系统询问是否确定删除，按回车即可

[OK]

Erase of nvram: complete

Switch#reload //重启设备

switch(config)#no ip domain-lookup //禁止dns查询，不会因为错误的命令卡住

Switch(config)#line console 0

Switch(config-line)#logging synchronous //实现输入同步，不被系统信息干扰

Switch(config)#line console 0

Switch(config-line)#exec-timeout 10 0 //修改10分钟后锁屏，设置0 0 是永不超时

资源共享

信息传递

增加可靠

提高系统处理能力

osi 7层

tcp/ip 5层

点对点 广域网

星形 好实现 方便故障排查 易于扩扩展

网状 提高可靠

wan 广域网 lan 局域网

物理层 数据链路层 网络层 传输层 应用层

rj-45

双绞线

568A

568B

cat5

cat5e 100M

cat6

cat7

ip 32位 十进制 跨网络的数据传递 192.168.0.1

mac 48位 十六进制 同局域网范围内的数据传递

全球唯一

前24位 厂商标示

后24位 产品的唯一编号

fe54：00:00:00:0b

单播 1对1

组播 1对多

广播 1对所有

MAC 物理地址 硬件地址

8 bit 比特 = 1 byte 字节

100Mb 12+MB

mtu 最大传输单元

交换机查看MAC地址表

Tarena-sw1#show mac-address-table

windows中查看网络信息，比如mac地址使用 ipconfig /all

学习 源MAC地址

广播

转发

更新 300秒

vlan数量 默认 允许创建 4096个 0～4095

1000

vlan1是默认存在的

Switch(config)#vlan 2 //在全局配置模式下创建VLAN2

Switch(config)#no vlan 2 //删除VLAN2

Switch(config)# interface f0/1 //进入f0/1接口

Switch(config-if)# switchport access vlan 2 //将接口加入vlan2

Switch(config-if)# no switchport access vlan 2 //取消加入vlan2

将多个接口添加到某个VLAN中：

Switch(config)# interface range f0/1–10 //进入组接口模式

Switch# show vlan brief //查看vlan摘要信息

提前熟悉路由器基本操作

使用2911路由器可以测试以下配置：

模式的切换（注意，路由器接口是千兆的 gigabitethernet 0/1），配密码，改主机名，保存，重启，清空配置等。。。

思考：

如何使同vlan设备互通

trunk 中继链路，可以实现不通vlan的数据在一条链路中传递

Switch(config-if)#switchport mode trunk //配置接口为trunk模式

access 接入链路 可以承载1个vlan

trunk 中继链路 可以承载多个vlan

以太通道，提高带宽，增加可靠性

Switch(config)# interface range fastEthernet 0/1 – 2 //同时进入1口与2口

Switch(config-if-range)#channel-group 1 mode on //捆绑为以太通道

Switch(config-if)#shutdown //关闭接口

Switch(config-if)#no shutdown //开启接口

Switch# show etherchannel summary //查看以太通道汇总信息

MAC 48位 6字节 前24位厂商标示 后24位产品唯一编号

MTU 最大传输单元 1500

学习 广播 转发 更新 超300秒，链路down

vlan 广播控制 增加安全 提高带宽利用 降低数据延迟

trunk 打标记

以太通道 增加带宽，提高可靠

192.168.1.1/24

网络位 主机位

255.255.255.0

网络ID

192.168.1.0

广播地址

192.168.1.255

192.168.1.2/24

A 1～127

255.0.0.0

B 128～191

255.255.0.0

C 192～223

255.255.255.0

192.168.1.1/16

192.168.10.1/16

172.16.0.1

172.16.0.0

172.16.10.1

172.16.0.0

Router(config)#interface gigabitEthernet 0/0 //进入千兆接口

Router(config-if)#ip address 192.168.1.254 255.255.255.0 //配置ip地址

Router(config-if)#no shutdown //开启接口

Router#show ip route //查看路由表

C 直连路由，接口配置好ip，并开启后自动生成

S 静态路由 ip route

S\* 默认路由 ip route 0.0.0.0 0.0.0.0 下一跳

动态路由

只允许配置对外方向，否则容易出现路由环路

路由器1配置的静态路由

Router(config)#ip route 192.168.3.0 255.255.255.0 192.168.2.2

路由器2配置的静态路由

Router(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.1

静态路由如果配置错误要及时删除

Router(config)#no ip route 192.168.1.0 255.255.255.0 192.168.2.1

配置思路：

1，检查路由表 （show ip route），找到无法到达的网段

2，使用静态路由，添加网段

三层交换机=二层转发+三层路由

在三层交换机启用路由功能

Switch(config)# ip routing

配置虚接口的IP

Switch(config)# interface vlan 1

Switch(config-if)# ip address 192.168.1.254 255.255.255.0

Switch(config-if)# no shutdown

在三层交换机上配置Trunk前要先指定接口封装为802.1q

Switch(config)#interface fastEthernet 0/24

Switch(config-if)#switchport trunk encapsulation dot1q

Switch(config-if)#switchport mode trunk

排错思路：

1，检查ip地址与网关

2，检查接口是否加入相应的vlan

3，网关设备（三层交换）的vlan虚接口ip是否配置正确并开启

4，交换机与交换机之间的链路是否配置为trunk

5，三层交换的路由功能是否开启

show ip interface brief //查看接口摘要信息，是否配置ip，是否开启

三层交换机配置默认路由前往外网：

Switch(config)#ip route 0.0.0.0 0.0.0.0 192.168.4.2

宣告 向动态路由邻居通告自身所连接的网段

准备使用动态路由前将路由器的静态路由删除

三层交换机的默认路由保留

首先在三层交换机配置：

Switch(config)# router ospf 1 //启动OSPF路由进程

指定OSPF协议运行的接口和所在的区域

Switch(config-router)# network 192.168.1.0 0.0.0.255 area 0

Switch(config-router)# network 192.168.2.0 0.0.0.255 area 0

Switch(config-router)# network 192.168.3.0 0.0.0.255 area 0

Switch(config-router)# network 192.168.4.0 0.0.0.255 area 0

然后在路由器中配置

Route(config)# router ospf 1 //启动OSPF路由进程

指定OSPF协议运行的接口和所在的区域

Route(config-router)# network 192.168.4.0 0.0.0.255 area 0

排错，分别检查三个方面：

vlan

ip

路由

传输层实现了端到端的数据传递

0～65535 端口总数

1～1023 常用端口

SYN 想与对方建立连接

ACK 确认

FIN 想与对方断开连接

TCP 可靠 ，面向连接，效率低

UDP 不可靠，无连接，效率高

访问控制列表（ACL）

读取第三层、第四层 头部信息

根据预先定义好的规则对数据进行过滤

对已经建设好的网络，可以通过ACL管理，使网络环境更加健康

标准ACL

基于源IP地址过滤数据包

标准访问控制列表的访问控制列表号是1～99

扩展ACL

基于源IP地址、目的IP地址、指定协议、端口来过滤数据包

扩展访问控制列表的访问控制列表号是100～199

192.168.2.1

255.255.255.0

0.0.0.255

0.0.0.0

0严格匹配

1不匹配

1题 禁止192.168.2.1与192.168.1.1通信，不影响其他数据

Router(config)#access-list 1 deny 192.168.2.1 0.0.0.0 //拒绝192.168.2.1通过

Router(config)#access-list 1 permit any //允许其他所有人通过

Router(config)# in g0/1

Router(config-if)# ip access-group 1 in //在接口应用acl

2题 只允许192.168.2.1与192.168.1.1通信

Router(config)#access-list 2 permit 192.168.2.1 0.0.0.0 //允许192.168.2.1通过

Router(config)# in g0/1

Router(config-if)# ip access-group 2 in //在接口应用acl

使用扩展acl限制192.168.2.1访问192.168.1.1的ftp服务

Router(config)#access-list 100 deny tcp 192.168.2.1 0.0.0.0 192.168.1.1 0.0.0.0 eq 21

Router(config)# in g0/1

Router(config-if)# ip access-group 100 in //在接口应用acl

使用扩展acl限制192.168.2.2访问192.168.1.1的www服务

Router(config)#access-list 100 deny tcp 192.168.2.2 0.0.0.0 192.168.1.1 0.0.0.0 eq 80

Router(config)#access-list 100 permit ip any any //放行其他所有数据

A

B

C

IPV4 32位 42亿

100.0.0.1 20M 3万

200.0.0.1

NAT 网络地址转换，可以将内部私有ip转换为外部公有ip

私有ip地址范围

A 10.0.0.0～10.255.255.255

B 172.16.0.0～172.31.255.255

C 192.168.0.0～192.168.255.255

IPV6 128位

2，配置静态nat转换

Router(config)#ip nat inside source static 192.168.1.1 100.0.0.2

Router(config)#ip nat inside source static 192.168.1.2 100.0.0.3

Router(config)#interface g0/1

Router(config-if)#ip nat outside

Router(config)#interface g0/0

Router(config-if)#ip nat inside

静态 一对一 服务器发布服务时才使用

PAT 一对多 端口多路复用，通常只用来访问外网

使用PAT技术，让内网所有主机利用外网接口的公网地址出门

首先使用acl定义内部ip地址

Router(config)#access-list 1 permit any

使用pat复用外网接口地址

Router(config)#ip nat inside source list 1 interface g0/1 overload

传输层

TCP 面向连接

三次握手

SYN----ACK，SYN----ACK

四次断开

FIN----ACK----FIN----ACK

HTTP 80

DNS 53

SSH 22

FTP 21

SMTP 25

HTTPS 443

UDP 不可靠 无连接 效率高

DNS 53

TFTP 69

NTP 123

ACL 访问控制列表

标准 针对源ip限制 1～99

扩展 源ip ，目标ip，协议，端口 100～199

NAT 网络地址转换，私有ip转换为公有ip

A 10.0.0.0～10.255.255.255

B 172.16.0.0～172.31.255.255

C 192.168.0.0～192.168.255.255

静态 一对一

PAT 一对多

STP 生成树协议，通过临时断开某接口避免广播风暴，当其他链路断开后，此接口会自动恢复，起到备份链路的效果

决定断开接口的是主根网桥与次根网桥

通过修改优先级可以实现主根与次根的配置

优先级默认 32768，越小越优先，如果要修改，必须为4096的倍数

1，在Switch1中配置

Switch(config)#spanning-tree vlan 1 priority 24576

Switch#show spanning-tree //查看所有vlan的生成树信息

Switch#show spanning-tree vlan 1 //查看vlan1的生成树信息

阻塞接口 BLK

转发接口 FWD

Switch(config)#spanning-tree vlan 1 root primary //将当前设备配置为主根

Switch(config)#spanning-tree vlan 1 root secondary //将当前设备配置为次根

vlan1 vlan2

MS1 vlan1的主根 vlan2的次根

MS2 vlan1的次根 vlan2的主根

HSRP 热备份路由选择协议

主要功能：网关备份

三层交换机物理接口配置ip首先转换为路由器接口

no switchport 再开启路由功能 ip routing

in vlan 1 //进入vlan1 配置ip

路由器

outer(config)#router ospf 1

Router(config-router)#network 192.168.4.0 0.0.0.255 area 0

Router(config-router)#network 192.168.3.0 0.0.0.255 area 0

Router(config-router)#network 192.168.2.0 0.0.0.255 area 0

MS1

Switch(config)#ip routing

Switch(config)#router ospf 1

Switch(config-router)#network 192.168.1.0 0.0.0.255 area 0

Switch(config-router)#network 192.168.2.0 0.0.0.255 area 0

MS2

Switch(config)#ip routing

Switch(config)#router ospf 1

Switch(config-router)#network 192.168.1.0 0.0.0.255 area 0

Switch(config-router)#network 192.168.3.0 0.0.0.255 area 0

三层交换机开启HSRP功能：

Switch(config)#interface vlan 1

Switch(config-if)#standby 1 ip 192.168.1.254

Switch(config-if)#standby 1 priority 105

Switch(config-if)#standby 1 preempt

综合拓扑：

1，为每台2960交换机分别添加10、20、30、40这四个vlan

2，将每台2960交换机的f0/5口分别加入vlan10、20、30、40

注意：最后一台要加5口与6口到vlan40中

SW1#conf t

SW1(config)#in f0/5

SW1(config-if)#switchport access vlan 10 //第一台加vlan10

3，为三层交换机分别添加10、20、30、40这四个vlan

4，将所有交换机与交换机之间的链路配置为trunk

Switch(config)#interface range fastEthernet 0/1-5

Switch(config-if)#switchport trunk encapsulation dot1q

Switch(config-if)#switchport mode trunk

5，通过配置生成树协议，实现负载均衡

MS1 vlan10、20 主根 vlan30、40 次根

MS2 vlan10、20 次根 vlan30、40 主根

第一台三层交换机配置：

Switch(config)#spanning-tree vlan 10 root primary //将当前设备配置为vlan10的主根

Switch(config)#spanning-tree vlan 20 root primary //将当前设备配置为vlan20的主根

Switch(config)#spanning-tree vlan 30 root secondary //将当前设备配置为vlan30的次根

Switch(config)#spanning-tree vlan 40 root secondary //将当前设备配置为vlan40的次根

第二台三层交换机配置：

Switch(config)#spanning-tree vlan 40 root primary //将当前设备配置为vlan40的主根

Switch(config)#spanning-tree vlan 30 root primary //将当前设备配置为vlan30的主根

Switch(config)#spanning-tree vlan 20 root secondary //将当前设备配置为vlan20的次根

Switch(config)#spanning-tree vlan 10 root secondary //将当前设备配置为vlan10的次根