# 网络的功能

信息传递,资源共享,提高可靠性,增加系统处理性能

60年代 分组交换 提高传输效率

70~80年代 tcp/ip 统一标准

90年代 web

wan 广域网 几十~几千千米

lan 局域网 1千米以内 办公室, 教室, 机房,宿舍

cisco 思科

华为

路由器 交换机

## 拓扑结构:

点对点 广域网

星形 局域网 易于实现,易于扩展,易于故障排查

网状 局域网 增加可靠,提供容错

## iso 国际标准化组织

osi 七层参考模型,理论框架

tcp/ip 五层 实际应用

1000Mbit

1000=1k

1000k=1M

1000000000

传输层 数据段

网络层 数据包

数据链路层 数据帧

物理层 比特流

## 视图

用户视图 保存

系统视图

接口视图

协议视图

ctrl+z 等于 return

[Huawei]sysname SW1 //修改主机名

[Huawei]display version //查看软硬件版本

[Huawei]display current-configuration //查看正在运行的配置,按空格翻页

aaa模式,负责授权认证审计,可以在此模式创建账户和密码

ctrl + ] 彻底退出系统

<Huawei>save //保存设置

<Huawei>reboot //重启设备

<Huawei>reset saved-configuration //重置配置文件(恢复出厂)

<Huawei>reboot //重启设备

ip

mac 硬件地址 物理地址 ,全球唯一不重复 48bit

0123456789ABCDEF

## 关闭各种信息提示(控制台超时后失效)

undo terminal debugging

undo terminal monitor

undo terminal logging

undo terminal trapping

## 设置控制台永不超时

sys

user-interface console 0

idle-timeout 0

网络的功能

信息传递 资源共享 提高可靠 增加系统处理性能

60年代 分组交换

70~80 tcp/ip

90年代 web技术

拓扑结构

点对点 wan

星形 lan

网状 lan

osi七层参考模型

tcp/ip五层参考模型

应用层

传输层 防火墙

网络层 路由器

数据链路层 交换机

物理层 网卡

用户视图

系统视图

接口视图

协议视图

交换机工作原理

学习,广播,转发,更新

广播泛滥

广播域

## **vlan**

虚拟局域网

virtual

控制广播

增加安全

提高带宽的利用率

降低数据传递的延迟

50~60ms 100ms

20ms

1s=1000ms

vlan 最大数量4096个

vlan1 默认vlan,无需创建,不能删除

1, 创建vlan

进入系统视图

vlan 2 //创建vlan2

undo vlan 2 //删除vlan 2

2, 将接口加入相关vlan

in e0/0/3 //进入接口3

port link-type access //接口类型更改为接入,表示即将为某一个vlan传输数据

port default vlan 2 //修改接口服务的vlan

display vlan 查看vlan列表验证之前的操作

vlan batch 10 20 30

undo vlan batch 10 20 30

[Huawei]vlan batch 2 3 //创建VLAN2、3

[Huawei]port-group 1 //建组,组号是1

[Huawei-port-group-1]group-member Ethernet0/0/3 Ethernet0/0/4 //组中加入3口和4口

[Huawei-port-group-1]port link-type access //在组1中所敲的命令,等于对该组中所有接口敲

[Huawei-port-group-1]port default vlan 2

网段

vlan1

192.168.1.1

192.168.1.2

vlan2

192.168.2.1

192.168.2.2

vlan3

192.168.3.1

192.168.3.2

access 接入链路 承载1个vlan

trunk 中继链路 承载多个vlan 打vlan标记

in e0/0/7

port default vlan 1 //恢复默认vlan

port link-type trunk //修改为中继链路

port trunk allow-pass vlan all //允许通过所有vlan

链路聚合,增加可靠,增加带宽

进入系统视图

clear configuration interface ethernet0/0/7 //清空所有配置,恢复默认,此时接口会自动关闭

[Huawei]interface ethernet0/0/7

undo shutdown //打开接口

[Huawei]interface Eth-trunk 1 //进入(创建)链路聚合接口1

[Huawei- Eth-trunk1]trunkport e 0/0/7 0/0/8 //捆绑7口和8口,此步骤如果接口不是默认状态,会提示报错,要求恢复默认.

port link-type trunk //将链路聚合接口修改为中继链路

port trunk allow-pass vlan all //放行所有vlan

网络层 路由器 ip

数据链路层 交换机 mac

不同部门=不同vlan=不同网段=不同广播域

2的n次方-2

A 1~127 1677万+

255.0.0.0

B 128~191 65534

255.255.0.0

C 192~223 254

255.255.255.0

192.168.0.1~192.168.0.254

每个网段第一个地址是网络id,最后一个地址是广播地址

192.168.0.1

172.16.0.0 172.16.255.255

172.16.0.1~172.16.255.254

icmp 英特网控制报文协议 可以查询网络状态并反馈相应数据

undo ip add 进入接口,删除ip

在接口中使用 display this 查看配置的ip地址

## 路由表

直连路由 路由器接口配置ip,并开启之后自动产生

静态路由 由管理员手工配置,小规模网络适用

R1

ip route-static 192.168.3.0 24 192.168.2.2

ip route-static 192.168.4.0 24 192.168.2.2

R2

undo ip route-static 192.168.1.0 24 192.168.2.3

ip route-static 192.168.1.0 24 192.168.2.1

display ip routing-table | include /24 查看路由表包含/24的行

交换机 二层

vlan

控制广播,增加安全,带宽利用率提高,降低数据传递的延迟

路由器 实现不同网段的链接 ,在物理接口配置ip

## 三层交换机=二层交换+三层路由 ,在虚拟接口配置ip

使用三层交换机搭建网络:

1,三层交换机创建vlan 2 3

vlan batch 2 3

2,将接口加入对应vlan

in g0/0/2

port link-type access

port default vlan 2

dis vlan

3,进入vlan接口(虚拟接口)配置ip地址,此ip将作为

终端设备的网关

in vlan 1

ip add 192.168.1.254 24

dis cur

添加S3700交换机, 达到更合理利用三层交换机的目的

1,在S3700创建vlan2 3

2,在S3700将pc所链接的接口加入相应vlan

3,将2台交换机之间的链路配置为中继链路

port link-type trunk

port trunk allow-pass vlan all

排错

1,查ip,网关

2,所属vlan

3,测试与网关的链接

网段 , vlan

为三层交换机接口配置ip的思路:

1,S5700创建vlan4

2,进入vlan4虚拟接口配置ip

in vlan 4

ip add 192.168.4.1 24

3,将g0/0/2口加入vlan4

动态路由 是由某种动态路由协议实现全网互通的目的,适用于大型网络

rip,isis,eigrp,bgp,ospf

宣告

三层交换机配置:

ospf //开启动态路由ospf

area 0 //进入第一个区域,一般超大型网络才需要多个区域,中小规模只使用第一个也就是0区域即可

network 192.168.1.0 0.0.0.255 //宣告设备自身所链接的网段

network 192.168.2.0 0.0.0.255

network 192.168.3.0 0.0.0.255

network 192.168.4.0 0.0.0.255

路由器:

ospf

area 0

network 192.168.4.0 0.0.0.255

network 192.168.5.0 0.0.0.255

display ip routing-table | include /24 查看最终结果

直连路由 配置ip,并开启接口自动生成

静态路由 手工配置 192.168.1.0 24 192.168.1.X

动态路由

默认路由 是特殊的静态路由,能够匹配任意网段,当路由表中无法查询到目标网段时使用,通常用在内部设备访问公网时使用.

三层交换机

ip route-static 0.0.0.0 0 192.168.4.2 //可以匹配任意网络

路由器

ip route-static 0.0.0.0 0 192.168.5.1

传输层 端口号 端到端

网络层 路由器 ip 点到点

数据链路层 交换机 vlan trunk mac

http 80 tcp

https 443

mysql 3306 tcp

## tcp 传输控制协议

可靠性高,效率低,面向链接

syn 打算与对方建立链接

ack 确认

fin 打算与对方断开链接

三次握手 syn-->ack,syn-->ack

四次断开 fin-->ack--> fin-->ack

## udp 用户数据报协议

可靠性低,效率高,无链接

## acl 访问控制列表,对匹配的数据进行限制.

基本acl 2000~2999 可以对源ip限制

高级acl 3000~3999 可以对源ip,目标ip,协议,端口限制

acl练习1:

[Huawei]interface GigabitEthernet 0/0/0

[Huawei-GigabitEthernet0/0/0] ip address 192.168.1.254 24

[Huawei]acl 2000 //创建acl,列表号是2000,表示即将使用基本acl

[Huawei-acl-basic-2000]rule deny source 192.168.2.1 0 //创建规则,拒绝源ip是192.168.2.1的数据通过

[Huawei]interface GigabitEthernet 0/0/1

[Huawei-GigabitEthernet0/0/1]ip address 192.168.2.254 24

[Huawei-GigabitEthernet0/0/1]traffic-filter inbound acl 2000

//进入g0/0/1接口后,放置acl 2000,用来过滤即将进入路由器的数据.

acl练习2:

acl 2000 //重新进入列表2000

display this //查看

undo rule 5 //删除之前的条目,根据序号删除

rule permit source 192.168.2.1 0 //创建新条目,允许2.1通过

rule deny //拒绝所有人通过

在同接口的同方向,只能放一条acl

## nat 网络地址转换

1,节约公网ip地址

2,增加安全

A 1~127

B 128~191

C 192~223

### 内部私有地址

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

ipv4版本地址总数42亿+

ipv6

192.168.0.1 200.0.0.1 200.0.0.2 192.168.0.1

192.168.0.2

192.168.0.3

服务器搭建服务 nat 静态转换 1对1

仅仅访问外部网络 nat easy ip 多对1

acl

配置静态nat,实现1对1的内外通讯

[Huawei]interface G 0/0/1 //进入路由器外网接口

[Huawei-GigabitEthernet0/0/1] ip address 100.0.0.1 8

[Huawei-GigabitEthernet0/0/1]nat static global 100.0.0.2 inside 192.168.2.1 //开启静态nat转换, 使内部主机2.1出门时将源ip转换为100.0.0.2

思考:

1,外部设备如何找到内部设备?

2,2.2也想出门如何做到?

[Huawei-GigabitEthernet0/0/1]nat static global 100.0.0.3 inside 192.168.2.2 //开启静态nat转换, 使内部主机2.2出门时将源ip转换为100.0.0.3

配错的转换列表要及时删除

undo nat static global 100.0.0.3 inside 192.168.2.2

使用easy ip达到节约公网ip的目的

[Huawei]acl 2000

[Huawei-acl-basic-2000]rule permit source any //使用acl定义任何内部地址

或者

[Huawei-acl-basic-2000]rule permit source 192.168.2.0 0.0.0.255 //仅允许192.168.2.0网段的主机

[Huawei-acl-basic-2000]rule deny

[Huawei]interface g0/0/1

[Huawei-GigabitEthernet0/0/1]nat outbound 2000 //可以利用g0/0/1的ip访问外网,acl列表2000中定义了谁能通过就允许谁可以访问外网

## stp 生成树协议

广播风暴,提供链路备份的功能

## vrrp 虚拟路由冗余协议

网关备份,自动切换

SW1

in vlan 1

ip add 192.168.1.252 24

vlan 2

in vlan 2

ip add 192.168.2.2 24

in g0/0/2

port link-type access

port default vlan 2

ospf

area 0

network 192.168.1.0 0.0.0.255

network 192.168.2.0 0.0.0.255

SW2

in vlan 1

ip add 192.168.1.253 24

vlan 3

in vlan 3

ip add 192.168.3.2 24

in g0/0/2

port link-type access

port default vlan 3

ospf

area 0

network 192.168.1.0 0.0.0.255

network 192.168.3.0 0.0.0.255

路由器

ospf

area 0

network 192.168.2.0 0.0.0.255

network 192.168.3.0 0.0.0.255

network 192.168.4.0 0.0.0.255

display ip routing-table | include /24

排错

在两台三层交换机配置vrrp

in vlan 1

vrrp vrid 1 virtual-ip 192.168.1.254

display vrrp brief

主路由器 master

备份路由器 backup

通过多vlan的配置实现vrrp负载均衡

所有交换机创建vlan 10 20

vlan batch 10 20

S5700

port-group 1

group-member g0/0/1 to g0/0/3

port link-type trunk

port trunk allow-pass vlan all

S3700

port-group 1

group-member e0/0/1 e0/0/2

port link-type trunk

port trunk allow-pass vlan all

两台S5700配置vrrp

in vlan 10

vrrp vrid 10 virtual-ip 192.168.10.254

in vlan 20

vrrp vrid 20 virtual-ip 192.168.20.254

进入第1台5700

in vlan 10

vrrp vrid 10 priority 105

进入第2台5700

in vlan 20

vrrp vrid 20 priority 105

display vrrp brief //最后检查结果,第1台5700是vlan10的主,vlan20的备份, 第2台5700是vlan20的主,vlan10的备则正确

## 企业大型网络架构实验

1,所有交换机创建vlan 10 20

2,所有交换机之间的链路设置trunk

3,SW1配置虚拟接口ip

vlan 10 192.168.10.252

vlan 20 192.168.20.252

SW2配置虚拟接口ip

vlan 10 192.168.10.253

vlan 20 192.168.20.253

4,配置vrrp

SW1 vlan 10 主路由器 105

vlan 20 备份路由器

SW2 vlan 20 主路由器 105

vlan 10 备份路由器

===========================================

组建大型企业网络:

1,所有交换机创建vlan 10 20 30 40

vlan batch 10 20 30 40

display vlan

2,所有交换机之间的链路设置trunk

S5700

port-group 1

group-member g0/0/4 g0/0/5

port link-type trunk

port trunk allow-pass vlan all

S3700

port-group 1

group-member e0/0/1 e0/0/2

port link-type trunk

port trunk allow-pass vlan all

3,修改设备名称 SW1~SW6

4,配置SW1与SW2的虚拟接口地址

SW1

in vlan 30

ip add 192.168.30.252 24

in vlan 40

ip add 192.168.40.252 24

SW2

in vlan 30

ip add 192.168.30.253 24

in vlan 40

ip add 192.168.40.253 24

5,配置vrrp

SW1

vlan 10 主路由器 :

in vlan 10

vrrp vrid 10 virtual-ip 192.168.10.254

vrrp vrid 10 priority 105

vlan 20 备份路由器 :

in vlan 20

vrrp vrid 20 virtual-ip 192.168.20.254

vlan 30 主路由器 :

in vlan 30

vrrp vrid 30 virtual-ip 192.168.30.254

vrrp vrid 30 priority 105

vlan 40 备份路由器 :

in vlan 40

vrrp vrid 40 virtual-ip 192.168.40.254

SW2

vlan 10 备份路由器 :

in vlan 10

vrrp vrid 10 virtual-ip 192.168.10.254

vlan 20 主路由器 :

in vlan 20

vrrp vrid 20 virtual-ip 192.168.20.254

vrrp vrid 20 priority 105

vlan 30 备份路由器 :

in vlan 30

vrrp vrid 30 virtual-ip 192.168.30.254

vlan 40 主路由器 :

in vlan 40

vrrp vrid 40 virtual-ip 192.168.40.254

vrrp vrid 40 priority 105

display vrrp brief 查看结果

为pc配置对应vlan的网关(192.168.X.254),测试是否全网互通

6,添加路由器并配置ip与三层交换机互联

7,在三层交换机与路由器开启ospf实现全网互通

10.0.0.0~10.255.255.255

172.16.0.0~172.31.255.255

192.168.0.0~192.168.255.255

8,路由器连接外网的接口配置ip地址,

另外外网的交换机在vlan1配置ip地

址100.0.0.10

9,两台路由器配置 nat

1, acl 放行所有人

acl 2000

rule permit source any

2, 在接口开启nat

in g0/0/2

nat outbound 2000

10,两台路由器配置默认路由

ip route-static 0.0.0.0 0 100.0.0.10

在ospf中宣告默认路由

[Huawei]ospf

[Huawei-ospf-1]default-route-advertise