Vlan 虚拟局域网

1. 控制广播，避免广播泛滥
2. 提高安全
3. 提高带宽的利用率
4. 降低了数据传递的延迟

Trunk 中继链路，可以在一条链路中传递多个vlan的数据

链路聚合 提高带宽 提高可靠

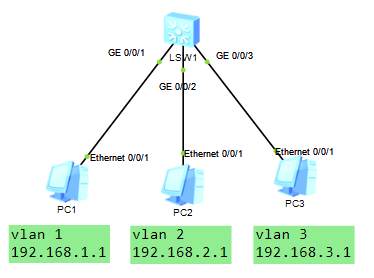
路由器

路由表的获取方式

1. 直连路由
2. 静态路由

三层交换机=二层交换+三层路由

实验一：使用三层交换机连接网络



1，创建vlan

[Huawei]vlan batch 2 3

[Huawei]in g0/0/2

[Huawei-GigabitEthernet0/0/2]port link-type access

[Huawei-GigabitEthernet0/0/2]port default vlan 2

[Huawei-GigabitEthernet0/0/2]in g0/0/3

[Huawei-GigabitEthernet0/0/3]port link-type access

[Huawei-GigabitEthernet0/0/3]port default vlan 3

2，三层交换机配置ip地址需要在虚拟接口（vlan接口）

[Huawei]in vlanif 1

[Huawei-Vlanif1]ip add 192.168.1.254 24

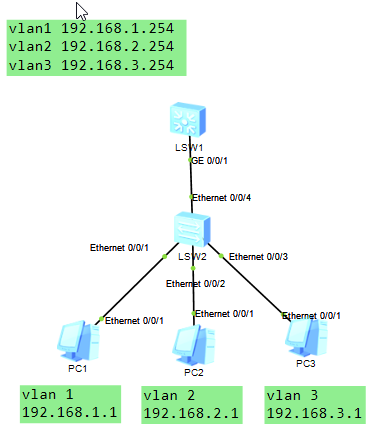
[Huawei-Vlanif1]in vlanif 2

[Huawei-Vlanif2]ip add 192.168.2.254 24

[Huawei-Vlanif2]in vlanif 3

[Huawei-Vlanif3]ip add 192.168.3.254 24

之后再依次将pc的ip与对应vlan的网关配置好，则可以实现全网互通

1. 改造网络拓扑，添加s3700交换机，更加合理的利用s5700三层交换机
2. 为了方便识别不同的交换机，首先修改主机名

然后将连接到sw2的pc加入到对应的vlan

S5700修改为 sw1 s3700修改 sw2

<sw2>system-view

[sw2]vlan batch 2 3

[sw2]in e0/0/2

[sw2-Ethernet0/0/2]port link-type access

[sw2-Ethernet0/0/2]port default vlan 2

[sw2-Ethernet0/0/2]in e0/0/3

[sw2-Ethernet0/0/3]port link-type access

[sw2-Ethernet0/0/3]port default vlan 3

再分别进入到2台交换机之间的接口配置trunk

[sw2]in e0/0/4

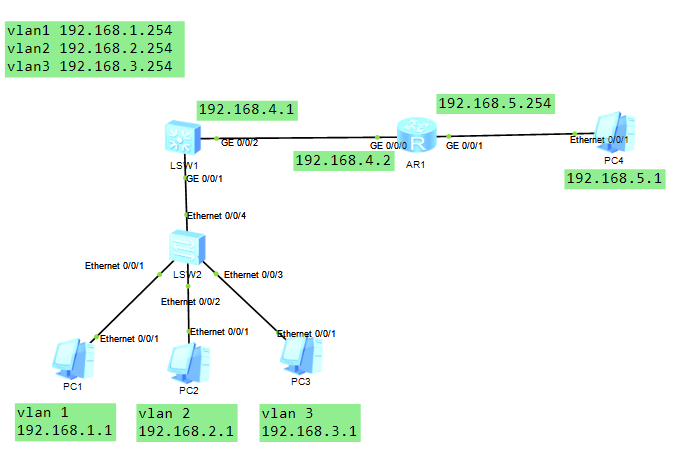
[sw2-Ethernet0/0/4]port link-type trunk

[sw2-Ethernet0/0/4]port trunk allow-pass vlan all

[sw1]in g0/0/1

[sw1-GigabitEthernet0/0/1]port link-type trunk

[sw1-GigabitEthernet0/0/1]port trunk allow-pass vlan all

1. 继续改造拓扑，按照规划配置ip地址

三层交换机接口配置ip思路

1. 确定需要配置的ip与接口
2. 创建一个vlan
3. 为此vlan的虚拟接口配置ip
4. 将要配置ip的交换机接口加入该vlan

[sw1]vlan 4

[sw1-vlan4]in vlanif 4

[sw1-Vlanif4]ip add 192.168.4.1 24

[sw1-Vlanif4]in g0/0/2

[sw1-GigabitEthernet0/0/2]port link-type access

[sw1-GigabitEthernet0/0/2]port default vlan 4

路由器配置ip

[Huawei]in g0/0/0

[Huawei-GigabitEthernet0/0/0]ip add 192.168.4.2 24

[Huawei-GigabitEthernet0/0/0]in g0/0/1

[Huawei-GigabitEthernet0/0/1]ip add 192.168.5.254 24

<sw1>display ip interface brief 检查ip地址

动态路由 可以利用某种动态路由协议，在整个网络中自动传递路由信息

Ospf

宣告 向外告知自身所直连的网段

1. 配置动态路由

首先在三层交换机配置

[sw1]ospf 开启ospf功能，进入ospf协议视图

[sw1-ospf-1]area 0 进入区域0（首个使用ospf协议的网络都要在0号区域中）

[sw1-ospf-1-area-0.0.0.0]network 192.168.1.0 0.0.0.255 宣告直连网段

[sw1-ospf-1-area-0.0.0.0]network 192.168.2.0 0.0.0.255

[sw1-ospf-1-area-0.0.0.0]network 192.168.3.0 0.0.0.255

[sw1-ospf-1-area-0.0.0.0]network 192.168.4.0 0.0.0.255

然后在路由器配置

[Huawei]ospf

[Huawei-ospf-1]area 0

[Huawei-ospf-1-area-0.0.0.0]network 192.168.4.0 0.0.0.255

[Huawei-ospf-1-area-0.0.0.0]network 192.168.5.0 0.0.0.255

<Huawei>dis ip routing-table | in /24 查看路由表

-----------------------------------

使用路由器和交换机主要目的是让数据可以从一台主机传递到另外一台主机

传输层的主要功能是定义端口号，可以让只拥有一个ip地址的主机传递多个程序的数据

传输层定义了tcp以及udp

Tcp 可靠 效率低 面向连接

Syn 打算与对方建立连接

Ack 确认

Fin 打算与对方断开连接

三次握手

1，首先由客户端对服务器发出syn信号

2，服务器收到syn之后给客户机发送ack，与此同时也会给客户端发送syn信号

3，客户端收到来自服务器的syn之后会给服务器发送ack信号

四次断开

1. 由客户端向服务器发出fin信号
2. 服务器收到fin信号会给客户端发送ack
3. 待服务器检查自身也没有任何数据需要传递给客户端之后也会向客户端发送fin信号
4. 客户端收到服务器的fin信号，会再发送ack信号给服务器

常见的使用tcp的服务名与端口号

Udp 不可靠 效率高 无连接

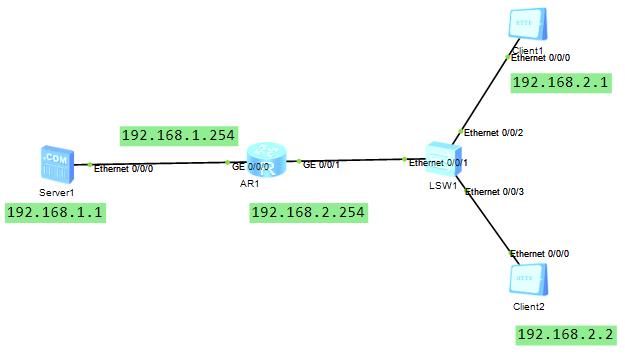
常见的使用udp的服务名与端口号

ACL 访问控制列表

基本acl 列表号 2000~2999 可以根据数据的源地址对数据进行限制

高级acl 列表号 3000~3999可以根据数据的源地址、目标地址、协议、端口号对数据进行限制

实验二：使用acl控制网络数据，禁止2.1访问1.1，但不影响其他数据

1，按拓扑配置ip与网关

2，在路由器中配置acl，并应用到接口

[Huawei]acl 2000 创建acl 列表号是2000

[Huawei-acl-basic-2000]rule deny source 192.168.2.1 0.0.0.0 定义规则，拒绝源地址是192.168.2.1的主机发送的数据

0.0.0.0 代表的含义是针对某台主机，如果要限制的是一个网段那可以用反掩码0.0.0.255

[Huawei]in g0/0/1 进入离2.1最近的路由器的接口

[Huawei-GigabitEthernet0/0/1]traffic-filter inbound acl 2000 激活（应用）刚刚创建的acl

最后测试 2.1 不可以ping 通 1.1 ，而2.2可以ping通1.1

实验三：在上图中，使用acl控制网络数据，允许2.1访问1.1，但拒绝其他客户机访问1.1

[Huawei]undo acl 2000 删除之前的acl

[Huawei]acl 2001 从新创建acl 2001

[Huawei-acl-basic-2001]rule permit source 192.168.2.1 0.0.0.0 放行192.168.2.1

[Huawei-acl-basic-2001]rule deny source any 拒绝所有主机

注意：acl在过滤数据时会按照编写acl的先后顺序，上述acl不能颠倒顺序写

[Huawei-acl-basic-2001]quit

[Huawei]in g0/0/1

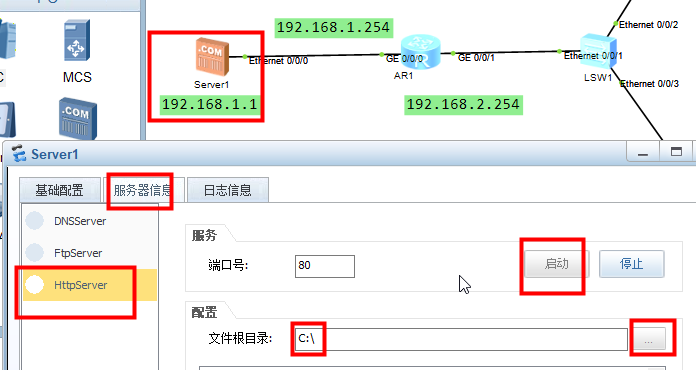
[Huawei-GigabitEthernet0/0/1]undo traffic-filter inbound

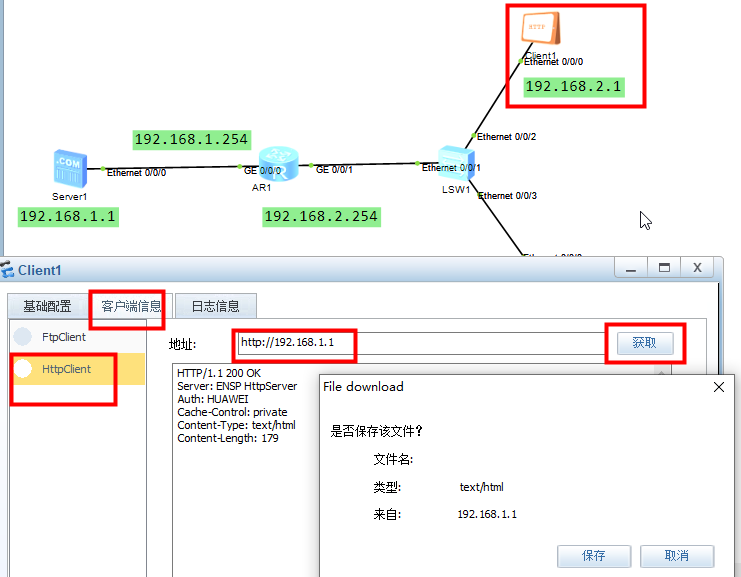
[Huawei-GigabitEthernet0/0/1]traffic-filter inbound acl 2001

实验四：使用高级acl过滤数据，禁止2.1访问1.1的网站服务，不影响其他业务

[Huawei]undo acl 2000 删除之前的acl

[Huawei]undo acl 2001 删除之前的acl

按下图在服务器开启web服务

然后在客户端连接服务器的web服务，看到下载文件，则说明访问网站成功

[Huawei]acl 3000 创建acl3000

[Huawei-acl-adv-3000]rule deny tcp source 192.168.2.1 0.0.0.0 destination 192.168.1.1 0.0.0.0 destination-port eq 80 拒绝2.1访问1.1的80端口(web服务)，其中eq表示等于

[Huawei-acl-adv-3000]in g0/0/1 进入离2.1最近的接口

[Huawei-GigabitEthernet0/0/1]undo traffic-filter inbound 删除老acl

[Huawei-GigabitEthernet0/0/1]traffic-filter inbound acl 3000 放上新acl

配置完毕后，使用2.1已结无法访问1.1的网站，但是可以ping通