NETWORK day 03

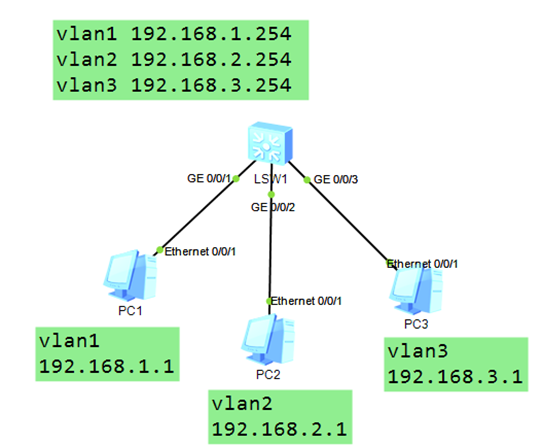
================================================

**三层交换机**

**同时具备交换机与路由器功能的强大网络设备**

**三层交换=二层交换+三层转发**

按图搭建拓扑，最上面的设备是s5700三层交换机



<Huawei>system-view //进入系统视图

[Huawei]undo info-center enable //关日志

[Huawei]vlan batch 2 3 //创建vlan2与3

[Huawei]display vlan //检查

[Huawei]interface GigabitEthernet 0/0/2 //进2口

[Huawei-GigabitEthernet0/0/2]port link-type access //配置接口类型为access

[Huawei-GigabitEthernet0/0/2]port default vlan 2 //把2口加入vlan2

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

[Huawei-GigabitEthernet0/0/3]port link-type access //配置接口类型为access

[Huawei-GigabitEthernet0/0/3]port default vlan 3 //把3口加入vlan3

[Huawei]interface Vlanif 1 //进入vlan1的接口

[Huawei-Vlanif1]ip address 192.168.1.254 24 //配置ip，该ip可以作为

vlan1的网关

[Huawei-Vlanif1]interface Vlanif 2 //进入vlan2的接口

[Huawei-Vlanif2]ip address 192.168.2.254 24 //配置ip，该ip可以作为

vlan2的网关

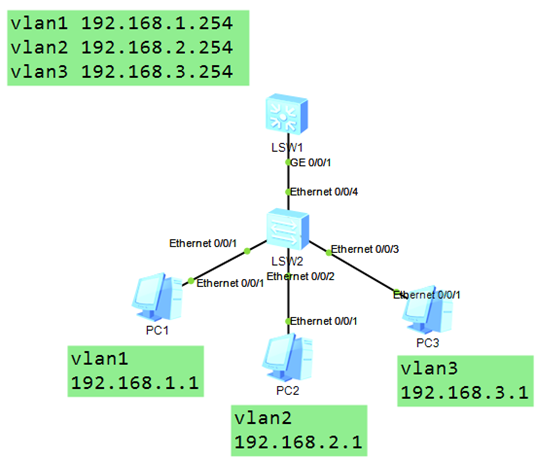
[Huawei-Vlanif2]interface Vlanif 3 //进入vlan3的接口

[Huawei-Vlanif3]ip address 192.168.3.254 24 //配置ip，该ip可以作为

vlan3的网关

至此可以实现所有pc全网互通

**然后按下图添加s3700交换机，用来连接pc与三层交换机：**



在s3700交换机配置：

[Huawei]vlan batch 2 3 //首先创建vlan2与3

[Huawei]in e0/0/2

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

[Huawei-Ethernet0/0/2] port default vlan 2 //将e0/0/2口加入vlan2

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

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

[Huawei-Ethernet0/0/3] port default vlan 3 //将e0/0/3口加入vlan3

[Huawei-Ethernet0/0/3]in e0/0/4

[Huawei-Ethernet0/0/4]port link-type trunk //将4口配置为中继链路

[Huawei-Ethernet0/0/4]port trunk allow-pass vlan all //放行所有数据

再回到s5700配置：

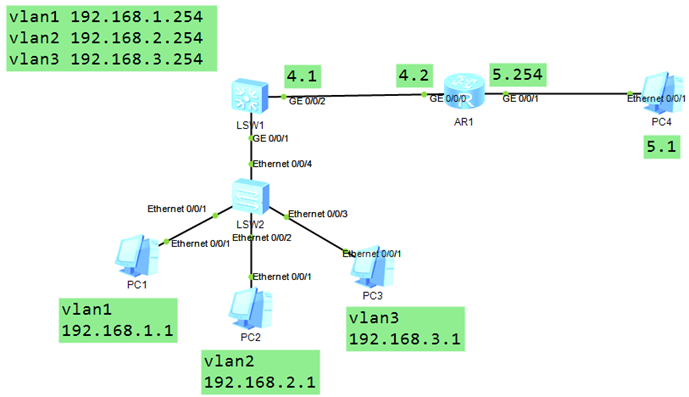
[Huawei-GigabitEthernet0/0/1]port link-type trunk //把g0/0/1口也配置为中继链路

[Huawei-GigabitEthernet0/0/1]port trunk allow-pass vlan all //放行所有vlan的数据

**三层交换机配置ip思路**

1. **创建一个vlan**
2. **进入该vlan的虚拟接口配置所需ip**
3. **将物理接口加入该vlan**

之后将拓扑延申，增加一台ar2220路由器，与pc一台，并按图配置好ip，pc的网关是192.168.5.254



s5700的 2接口要按照三层交换机接口配置ip的思路进行：

[Huawei]vlan 4 //创建vlan4

[Huawei-vlan4]in vlan 4 //进入vlan4接口

[Huawei-Vlanif4]ip add 192.168.4.1 24 //为vlan4配置ip

[Huawei-Vlanif4]in g0/0/2 //进入2接口

[Huawei-GigabitEthernet0/0/2]port link-type access //配置接口类型为access

[Huawei-GigabitEthernet0/0/2]port default vlan 4 //把2口加入vlan4

ar2220路由器的ip配置此处省略

如果需要路由器可以到达1.0网段，则需要添加

[Huawei]ip route-static 192.168.1.0 24 192.168.4.1

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

**S5700配置动态路由，配置之前可以先把静态路由删除**

[Huawei]undo ip route-static 192.168.5.0 255.255.255.0 192.168.4.2

[Huawei]ospf //进入ospf动态路由协议视图

[Huawei-ospf-1]area 0 //定义区域0，整个网络的第一个ospf区域

[Huawei-ospf-1-area-0.0.0.0]network 192.168.1.0 0.0.0.255 //依次宣告

自身所直连的网段

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

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

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

在路由器中配置动态路由：

[Huawei]undo ip route-static 192.168.1.0 255.255.255.0 192.168.4.1

[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]display ip routing-table | in /24 //查看路由表

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

传输层，定义了端口号

**传输层协议**

tcp 传输控制协议 可靠 效率低 面向连接

标志位：

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：syn---ack,syn---ack

四次断开：fin---ack---fin---ack

使用了TCP的服务名称以及端口号



udp 用户数据报协议 不可靠 效率高 无连接

使用了UDP的服务名称以及端口号



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

**ACL 访问控制列表**

基本acl 列表号2000~2999 对数据的源ip地址过滤

高级acl 列表号3000~3999 对数据的源ip、目标ip、协议、端口过滤

**反掩码使用规则：**

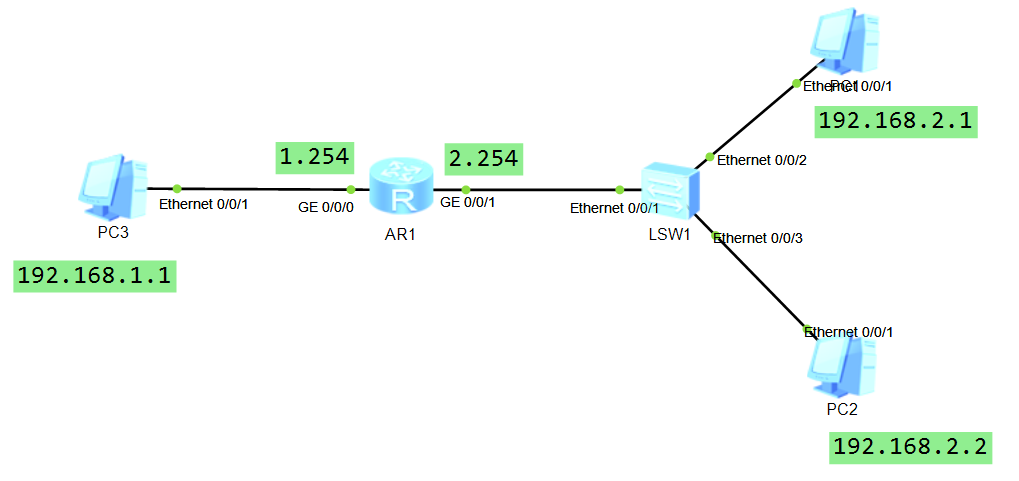
0 检查 1 不检查 这里的1只的是二进制写法，十进制可以用255标识

比如这样写 192.168.0.1 0.0.0.255 那么192.168.0.100来了就会执行acl规则，因为0.0.0.255是只要检查192.168.0.1的前三位，192.168.0.100的前三位与之一致，如果是192.168.1.100来了就不执行。

如果这样写 192.168.0.1 0.0.255.255 就是检查前两位， 那么 192.168.1.100来了就执行

如果这样写 192.168.0.1 0.0.0.0 就是检查前整个ip，那么只有192.168.0.1来了才执行

首先按照以下拓扑组建网络：



路由器配置ip：

[Huawei]in g/0/0 //进入0口

[Huawei-GigabitEthernet0/0/0]ip add 192.168.1.254 24 //配置ip

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

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

之后所有的pc都要按图配置ip

1.0网段的网关是1.254 2.0网段的网关是2.254

**禁止主机PC2(2.1)与PC1(1.1)通信，而允许所有其他的流量**

[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 //创建规则

拒绝源地址是192.168.2.1的数据通过

[Huawei-acl-basic-2000]undo rule 5 //如果规则写错，可以根据规则号码

删除

[Huawei-acl-basic-2000]in g0/0/1 //进入1口

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

数据是入方向，并应用之前创建的acl2000

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

[Huawei-GigabitEthernet0/0/1]display acl 2000 //查看acl 2000的内容

**相同接口相同方向同时只能应用一个acl列表**

**允许主机pc2(2.1)与pc1(1.1)互通，而禁止其他设备访问pc1**

[Huawei-GigabitEthernet0/0/1]acl 2001 //创建新acl，列表号是2001

[Huawei-acl-basic-2001]rule permit source 192.168.2.1 0 //创建规则，允许2.1通

过

[Huawei-acl-basic-2001]rule deny source any //拒绝所有设备通过

[Huawei-acl-basic-2001]in g0/0/1 //进入应用acl的接口

[Huawei-GigabitEthernet0/0/1]undo traffic-filter inbound //在接口取消之前

的acl2000

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

**练习：**

1，传输层有哪些协议，各有什么特点？

2，描述TCP三次握手以及四次断开的基本过程

3，SMTP、DNS、SSH、TFTP、NTP分别是什么协议，使用了什么端口，在传输层使用什么协议？

4，网络设备中的ACL技术常见类型有哪些，各有什么区别？

**参考答案：**

1，传输层有哪些协议，各有什么特点？

TCP 传输控制协议

可靠的、面向连接的协议 传输效率低

UDP 用户数据报协议

不可靠的、无连接的服务 传输效率高

2，描述TCP三次握手以及四次断开的基本过程

三次握手

1，用户发送syn给服务器

2，服务器发送ack与syn给用户

3，用户发送ack给服务器

四次断开

1，用户发送fin给服务器

2，服务器发送ack给用户

3，服务器发送fin给用户

4，用户发送ack给服务器

3，SMTP、DNS、SSH、TFTP、NTP分别是什么协议，使用了什么端口，在传输层使用什么协议？

参考答案

SMTP 简单邮件传输协议 端口号25 tcp

DNS 域名系统 端口号53 tcp/udp

ssh 远程登录 端口号22 tcp

TFTP 简单文件传输协议 端口号69 udp

NTP 网络时间协议 端口号123 udp

4，网络设备中的ACL技术常见类型有哪些，各有什么区别？

参考答案

基本ACL

基于源IP地址过滤数据包

基本访问控制列表的列表号是2000~2999

高级ACL

基于源IP地址、目的IP地址、指定协议、端口来过滤数据包

高级访问控制列表的列表号是3000~3999