telnet登录交换机（极大概率不考）

2019年12月30日　　16:04

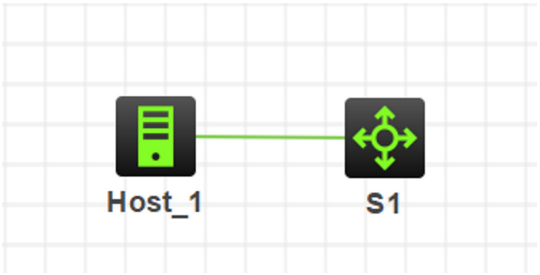
1. ## 先配置交换机：

   <H3C> system
   [H3C] interface vlan-interface 1
   [H3C-vlan-interface1] ip address 192.168.0.2 255.255.255.0
   [H3C]telnet server enable
   [H3C] user-interface vty 0 4
   [H3C-ui-vty0-4] authentication-mode password
   [H3C-ui-vty0-4] set authentication password simple 123456
   [H3C-line vty0-4]user-role level-15
   在HCL上要放host，不要放PC，PC无法实现telnet登录

2. ## 配置电脑网络里的VirtualBox Host-only的ip地址，与交换机在同一网段默认网关不用配

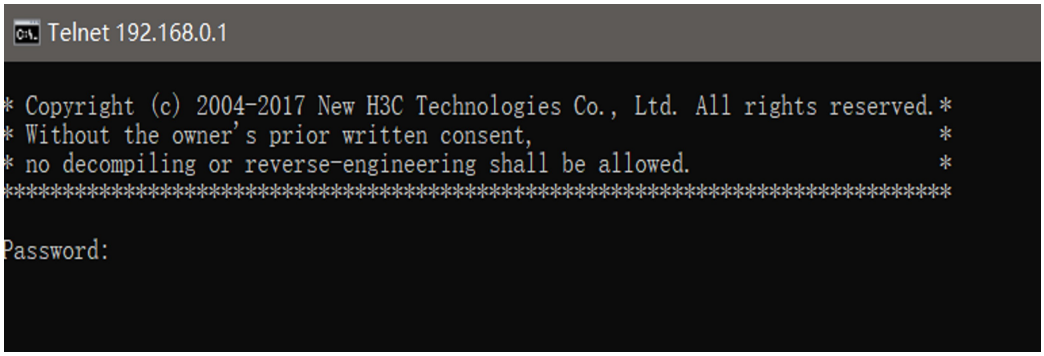
   

   HCL拓扑图

3. ## 在windows下安装telnet，打开“启动或关闭windows功能”，可在电脑左下搜索框搜索

   打开cmd
   首先ping 192.168.0.2，看是否ping通
   若ping通
   输入命令telnet 192.168.0.2
   输入密码即可登录



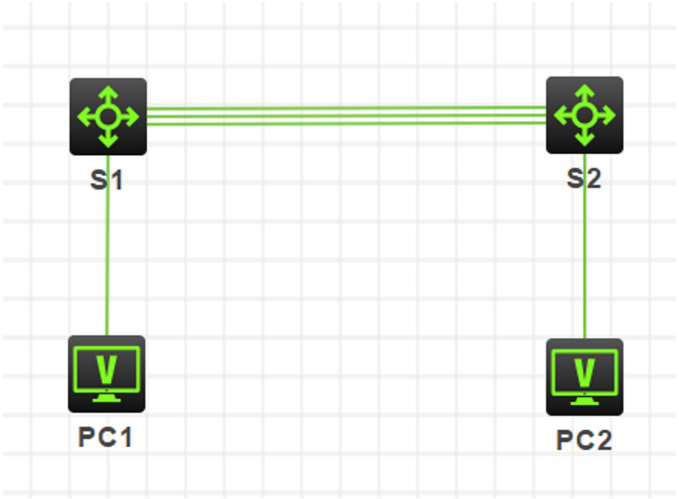
标题栏显示的ip地址就是交换机的地址（我配的是192.168.0.1

telnet登录路由器我懒得写了，我觉得应该不会考这个吧

交换机-端口聚合（不考）

2019年12月30日　21:19

拓扑图



1. 配置交换机

例：将以太网端口Ethernet1/0/1 加入聚合端口22。

[H3C] interface bridge-aggregation 22

（此处理论值为1-1024，但是我用1的时候出现迷之错误）

[H3C] interface Ethernet1/0/1

[H3C-Ethernet1/0/1]port link-aggregation group 22

重复操作，之到将两个交换机的三个端口都加入聚合端口

注：两台交换机聚合端口号要一致，如果要配置聚合端口，要先把端口加进去在配置聚合属性。（trunk，permit vlan）,这样在聚合内的端口都会被设置相应的属性

2. 配置PC

配置两个PC的IP地址和掩码，不用配置网关

注：两个IP地址需处于同一网段

3. 设置端口的链路类型

[H3C-Ethernet1/0/1] port link-type { access | trunk | hybrid }

恢复为缺省值命令：

[H3C-Ethernet1/0/1] undo port link-type

设置当前Trunk端口，允许某些VLAN的帧通过：

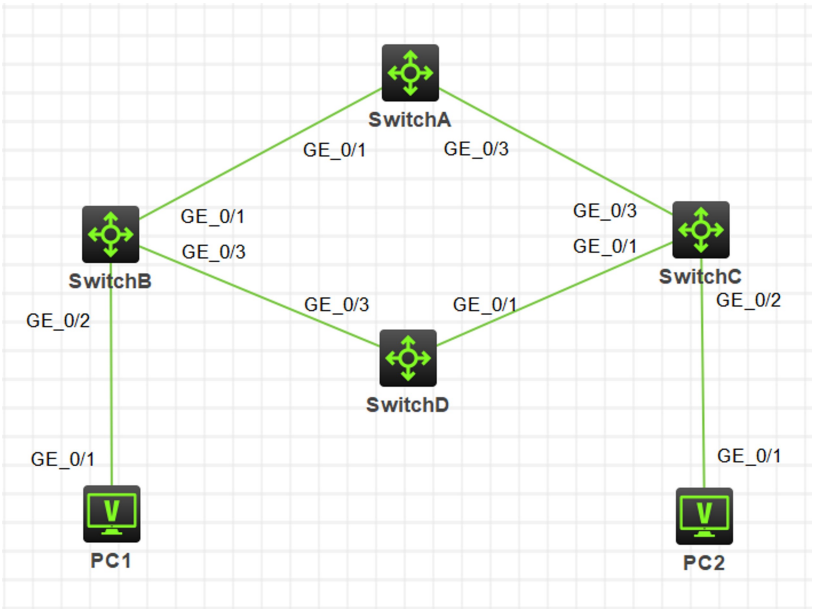
[H3C-Ethernet1/0/1] port trunk permit vlan 2 6 to 10 25

[H3C-Ethernet1/0/1] port trunk permit vlan all

交换机-STP（不考）

2019年12月31日　　9:36

拓扑图

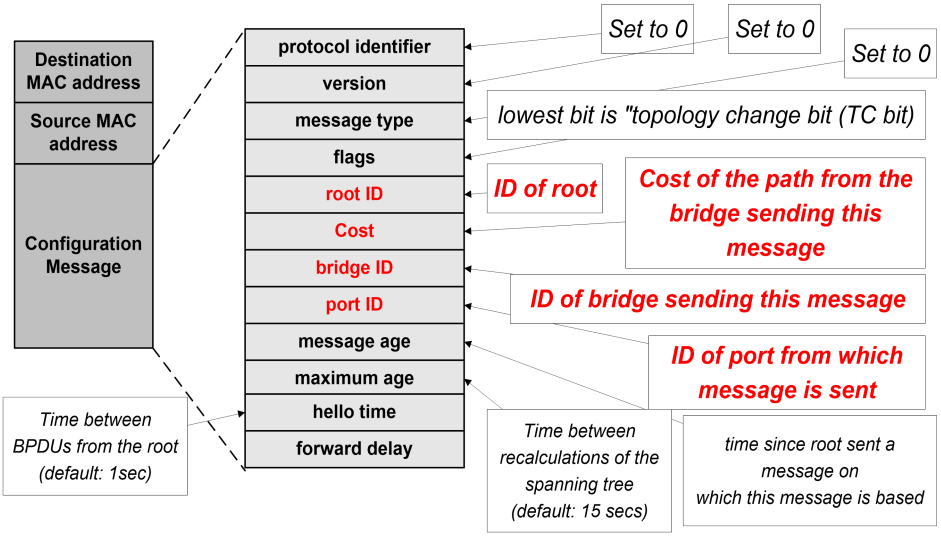


知识点回顾

根交换机比较方法：Bridge ID + priority 最小的就是根交换机

根端口比较方法：Port ID + cost 最小的就是根端口

生成树路径生成比较顺序：下图中靠上的优先，即优先比较root ID



1. 启动stp协议

在四台交换机上分别执行：

[SwtichX] stp enable

[SwtichX] display stp （显示本机Bridge ID，priority，和Root ID）

2. 设置优先级以改变更根交换机

在任意一台交换机上输入

[SwitchX] stp priority 4096

[SwtichX] display stp （查看Root ID是否为本机）

3. 查看一台交换机上哪个端口为根端口

[SwitchX] display stp interface G 1/0/1

[SwitchX] display stp interface G 1/0/3

```
----[CIST][Port2(GigabitEthernet1/0/1)][FORWARDING]----
Port protocol          : Enabled
Port role              : Root Port (Boundary)
Port ID                : 128.2
Port cost(Legacy)      : Config=auto, Active=20
Desg.bridge/port       : 32768.acd8-a0d9-0200, 128.2
```

```
----[CIST][Port4(GigabitEthernet1/0/3)][DISCARDING]----
Port protocol          : Enabled
Port role              : Alternate Port (Boundary)
Port ID                : 128.4
Port cost(Legacy)      : Config=auto, Active=20
Desg.bridge/port       : 32768.acd8-a2fa-0300, 128.4
```

Port role 后面为此端口角色，

Port ID后面的128为priority， 2才是ID

4. 改变端口cost以改变根端口

首先进入一个端口下，输入

[SwtichX-GigabitEthernet1/0/X] stp cost 2

（此处与上机不同，上机写的是20，因为上机默认的cost为200，模拟器为20）

[SwitchX] display stp interface G 1/0/X

（再次查看端口，看结果是否符合预期）

交换机-vlan配置

2019年12月31日 13:48

1. 创建vlan，并加入端口

每个交换机默认都有一个vlan1， 所有的端口都在vlan1下面

[Switch]vlan 2（创建vlan 2）

[Switch-vlan2]port G 1/0/1（将端口1/0/1加入vlan2）

2. 给vlan配置IP地址

系统视图下，进入vlan-interface，这与上一步是不一样的

[Swtich] interface Vlan-interface 2（进入vlan2的视图）

[Switch-Vlan-interface2]ip address *IP地址* 24

或

[Switch-Vlan-interface2]ip address *IP地址* 255.255.255.0 （两种写法等价）

3. 查看vlan

[Switch]display vlan（查看有几个vlan）

[Switch]display vlan 1（详细查看vlan 1下面的内容）

注意事项

一台交换机上的不同vlan之间路由不用配置路由表，交换机自动生成

不同交换机上的vlan需要配置**静态路由**

不要忘记与端口/vlan相连的PC机的**默认网关**，地址就是端口/vlan的ip地址

只有vlan才能配IP地址, 端口本身无法配置ip地址

没配默认网关也能ping通第一跳，一定要查看PC配置检查

重点-路由器-路由配置（Static、RIP、OSPF）

2019年12月31日 15:56

1. 静态路由配置

在路由器系统视图下

[Router] ip route-static *目的IP地址 掩码 下一跳IP地址*

缺省路由配置

[Router] ip route--static 0.0.0.0 0 *下一跳IP地址*

缺省路由的作用是，如果在路由表里没有匹配到目的IP地址，就会按缺省路由指定的下一条地址跳转。

2. RIP配置

rip命令用来**启动RIP**，并进入RIP视图。

undo rip命令用来关闭RIP。

[Router]rip [process-id] (process-id)也可以不写，默认是1

[Router]undo rip [process-id]

在路由器所连接的一个**网段**启动/关闭RIP

[Router] [undo] network *network-address*

network-address: 路由器相应接口的IP地址（**在路由器自己身上的IP地址**）

在路由器所连接的所有网段启动/关闭RIP

[Router] [undo] network 0.0.0.0

注：

缺省情况下，路由器不启动RIP。

RIP 的大部分特性都需要在RIP 视图下配置，接口视图下也有部分RIP 相关属性的配置。

RIP只在指定网段上的接口运行；因此，RIP 启动后**必须指定其工作网段。**

3. OSPF配置

1. 配置路由器ID

[Router] [undo] router id 1.1.1.1

注：

通常的做法是将路由器的ID配置为与该路由器某个接口的IP地址，这样便可以保证它的唯一性。

这步操作很容易忘记

2. 启动OSPF

[Router] [undo] ospf

注：

缺省情况下，路由器不启动OSPF。

OSPF的大部分特性都需要在OSPF视图下配置，接口视图下也有部分OSPF相关属性的配

置。

3. 配置接口所在区域

创建/删除区域

[Router-ospf] [undo] area area-id

例如：[Router-ospf] area 0

[Router-ospf-area0]

在区域中指定/取消网段

[Router-ospf-area0] [undo] network *ip-addr mask*

ip-addr：路由器接口IP

mask: 反子网掩码

例如： [Router-ospf-area0] network *192.168.1.1 0.0.0.255*

注：与RIP一样，启动OSPF后也要**设置生效网段**，而且OSPF要**多写一个反掩码**

4. 路由引入

引入/取消其它协议的路由

[Router-ospf] [undo] import-route protocol

protocol: Direct, Static, RIP, BGP, IS-IS

关键是什么时候要引入，要引入什么?

通常来说，使用路由协议会覆盖掉其他的路由协议，比如说使用了OSPF，路由表内相关的static和direct就都失效了，所以要进行路由引入

考试的时候，**多余的路由引入会扣分**

边缘路由器不要做路由引入

一般来说，核心路由器的RIP和OSPF要引入所有的协议（RIP，OSPF， direct，static）中的2-3个，根据实际情况选择，不要进行无意义的引入。

路由器-验证配置

2019年12月31日 18:56

1. ppp配置

[Router-Serial0] link-protocol ppp

（由于路由器默认是开启ppp的，所以这条不用写）

PAP验证

验证方:

[Router-Serial0] ppp authentication-mode pap

[Router] local-user *username* class network

[Router-luser] service-type ppp

[Router-luser] password simple *password*

被验证方:

[Router-Serial0] ppp pap local-user *username* password simple *password*

CHAP验证

验证方:

[RA-Serial0] ppp authentication-mode chap

[RA-Serial0] ppp chap user *user -a*

[RA] local-user *user-b* class network

[RA-luser] service-type ppp

[RA-luser] password simple *password*

被验证方:

[RB-Serial0] ppp chap user *user -b*

[RA] local-user *user–a* class network

[RA-luser] service-type ppp

[RA-luser] password simple *password*

在路由器里，养成每个接口配置完成后随手shutdown undo shutdown的好习惯

2. HDLC配置

[Router-Serial0] link-protocol hdlc

路由器-防火墙配置

2019年12月31日 19:07

1. 创建ACL

[Router] acl advanced/basic *acl-number* [match-order { config | auto }]

config：匹配规则时按用户的配置顺序。 //缺省值

auto：匹配规则时按“深度优先”的顺序。

例：[Router] acl advanced 3001 match-order auto

2. 配置ACL

PPT上这部分说的太复杂了，直接看例子就行了

创建完acl直接进入了acl视图

[Router-acl-adv-3001]rule deny ip source *源ip地址 反掩码* destination *目的ip地址 反掩码*

（反掩码写0就是完整匹配）

第七章PPT17页有很详细的举例，建议看一看

3. 启动防火墙

[Router] firewall enable

HCL虚拟机使用操作系统版本默认开启防火墙，**无需手动启动**

4. 在接口上应用ACL

在接口上应用ACL的命令为：

[Router-Serial0] packet-filter *acl-number* { inbound | outbound }

inbound：入方向

outbound：出方向

注：在一个接口的一个方向上，可以配置多个ACL，匹配时从acl-number 大的ACL开始

5. 查看配置好的ACL

[任意视图] display acl { all | *acl-number* }

路由器-NAT配置（不考）

2019年12月31日 19:52

1. 定义地址池

[Router] nat address-group *1*

[Router-nat-address-group-1] address *202.38.1.2 202.38.1.3*

2. 定义地址池与ACL的关联

[Router-Serial0] nat outbound *3001* address-group *1*

关联前先按防火墙配置里写的把ACL配置好

3. 建立内部服务器

建议直接看第七章PPT42页内容

设置内部FTP 服务器

[Router-Serial0] nat server protocol tcp global 202.38.160.101 21 inside 10.110.10.1

设置内部WWW服务器1

[Router-Serial0] nat server protocol tcp global 202.38.160.102 www inside 10.110.10.2 http

设置内部WWW服务器2

[Router-Serial0] nat server protocol tcp global 202.38.160.102 8080 inside 10.110.10.2 http

设置内部SMTP 服务器

[Router-Serial0] nat server protocol tcp global 202.38.160.102 smtp inside 10.110.10.4 smtp

4. 配置信息显示

查看地址转换的配置信息：

[任意视图] display nat all

查看地址转换表：

[任意视图] display nat static