H3C 常用命令

1. 查看交换机整体配置

   Display current-configuration

2. 进入系统配置模式命令 system-view
3. 新建 VLAN 命令：vlan 10
4. 查看已有的 vlan：display vlan
5. 把端口加入到 VLAN 里面：vlan 10

   port Ethernet0/4/2;

   Interface Ethernet0/4/2

   port access vlan 10

   把端口从 VLAN 里面删除：interface Ethernet0/4/3

   undo port access vlan

6. 设备命名：sysname SW1
7. 端口绑定：interface Ethernet0/4/7

   user-bind ip-address 1.1.1.1 mac-address 2222-3333-5555

   在此端口下，只能用网卡地址是 2222-3333-5555 的电脑，而且此电脑只能用 1.1.1.1 这个 IP，换了电脑或者电脑换了 IP 都是不行的

8. 一个 vlan 就是一个网段，不同网段之间要相互访问必须用到三层设备
9. 端口类型：acess　trunk

   Interface Ethernet 0/4/1;port link-type access 交换机默认的端口类型

   Interface ethernet0/4/1;port link-type trunk;port trunk permit vlan all;允许所有 vlan 通过，只能接交换机

   interface Ethernet0/4/5

   port link-mode bridge

   port link-type trunk

   port trunk permit vlan all

10. dhcp 功能配置：　(如果要取消就 undo dhcp enable)

    dhcp enable

    dhcp server ip-pool 123

network 192.168.1.0 mask 255.255.255.0

gateway-list 192.168.1.1

dns-list 202.101.226.68 202.101.224.69

dhcp server forbidden-ip 192.168.1.1 192.168.1.100----屏蔽不被分配出去的 IP 地址

10. 给端口配置 IP 地址：

interface Vlan-interface1

ip address 192.168.1.1 255.255.255.0 此地址可以用作 web 登陆地址

local-user admin----------此用户可用作 web 登陆

password simple 12345

service-type telnet

user-interface vty 0 4

authentication-mode scheme

11. 配置远程管理用户：

telnet server enable---------根据设备而定，有的设备开了，有的设备没开

local-user admin

password simple 12345

service-type telnet

user-interface vty 0 4

authentication-mode scheme

12. 保存命令：save
13. 清楚配置命令：reset saved-configuration 在尖括号下就可运行此命令
14. 中括号是配置模式，尖括号是查看模式
15. 退出命令：quit
16. 路由：ip route-static 0.0.0.0 0.0.0.0 192.168.1.1
17. 静态 IP 上网功能：

Interface Ethernet 0/0

Ip address 218.87.66.98 255.255.255.192----------外网接口接口设置地址

Nat outbound 2000----------外网接口 NAT 转换

Interface Ethernet 0/1

Ip address 192.168.1.1 255.255.255.0----------内网接口设置内网网关

Ip route-static 0.0.0.0 0.0.0.0 218.87.66.1-外网接口设置内网网关

Acl number 2000

Rule 0 permit source 192.168.1.0 0.0.0.255

18. 拨号上网：

dialer-rule 1 ip permit

interface dialer 1

dialer user 1

dialer-group 1

dialer bundle 1

nat outbound 2000

ip address ppp-negotiate

ppp pap local-user 07998888888 password cipher 123456

ppp chap user 07998888888

ppp chap password 123456

interface ethernet 0/0----------在外网口应用

pppoe-client dial-bundle-number 1

Interface Ethernet 0/1

Ip address 192.168.1.1 255.255.255.0----------在内网口输入网关地址

Acl number 2000

Rule 0 permit source 192.168.1.0 0.0.0.255

Ip route-static 0.0.0.0 0.0.0.0 dialer 1

19. 保存配置文件：tftp 192.168.1.11 get star

20. 上传配置文件：tftp 192.168.1.11 put star.

21. 查看是否有三层口功能： dis ip interface brief

22. 三层交换机配置 VLAN 接口： Interface vlan interface 100

23. 配置文件相关命令

[H3C]display current-configuration ;显示当前生效的配置

[H3C]display saved-configuration ； 显示 flash 中配置文件，即下次上电启动时所用的配置文件

<H3C>reset saved-configuration ； 檫除旧的配置文件

<H3C>reboot ； 交换机重启

<H3C>display version ； 显示系统版本信息

24. 基本配置

[H3C]super password ； 修改特权用户密码

[H3C]sysname ； 交换机命名

[H3C]interface ethernet 0/1 ； 进入接口视图

[H3C]interface vlan x ； 进入接口视图

[H3C-Vlan-interfacex]ip address 10.65.1.1 255.255.0.0 ； 配置 VLAN 的 IP 地址

[H3C]ip route-static 0.0.0.0 0.0.0.0 10.65.1.2 ； 静态路由＝网关

25. telnet 配置

[H3C]user-interface vty 0 4 ； 进入虚拟终端

[S3026-ui-vty0-4]authentication-mode password ； 设置口令模式

[S3026-ui-vty0-4]set authentication-mode password simple 222 ； 设置口令

[S3026-ui-vty0-4]user privilege level 3 ； 用户级别

26. 端口配置

[H3C-Ethernet0/1]duplex {half|full|auto} ； 配置端口工作状态

[H3C-Ethernet0/1]speed {10|100|auto} ； 配置端口工作速率

[H3C-Ethernet0/1]flow-control ； 配置端口流控

[H3C-Ethernet0/1]mdi {across|auto|normal} ； 配置端口平接扭接

[H3C-Ethernet0/1]port link-type {trunk|access|hybrid} ； 设置端口工作模式

[H3C-Ethernet0/1]undo shutdown ； 激活端口

[H3C-Ethernet0/2]quit ； 退出系统视图

27. 链路聚合配置

[DeviceA] link-aggregation group 1 mode manual ； 创建手工聚合组 1

[DeviceA] interface ethernet 1/0/1 ； 将以太网端口 Ethernet1/0/1 加入聚合组 1

[DeviceA-Ethernet1/0/1] port link-aggregation group 1

[DeviceA-Ethernet1/0/1] interface ethernet 1/0/2 ；将以太网端口 Ethernet1/0/1 加入聚合组 1

[DeviceA-Ethernet1/0/2] port link-aggregation group 1

[DeviceA] link-aggregation group 1 service-type tunnel # 在手工聚合组的基础上创建 Tunnel 业务环回组。

[DeviceA] interface ethernet 1/0/1 # 将以太网端口 Ethernet1/0/1 加入业务环回组。

[DeviceA-Ethernet1/0/1] undo stp

[DeviceA-Ethernet1/0/1] port link-aggregation group 1

28. 端口镜像

[H3C]monitor-port <interface_type interface_num> ；指定镜像端口

[H3C]port mirror <interface_type interface_num> ；指定被镜像端口

[H3C]port mirror int_list observing-port int_type int_num ；指定镜像和被镜像

29. VLAN 配置

[H3C]vlan 3 ；创建 VLAN

[H3C-vlan3]port ethernet 0/1 to ethernet 0/4 ；在 VLAN 中增加端口

配置基于 access 的 VLAN

[H3C-Ethernet0/2]port access vlan 3 ；当前端口加入到 VLAN

注意：缺省情况下，端口的链路类型为 Access 类型，所有 Access 端口均属于且只属于 VLAN1

配置基于 trunk 的 VLAN

[H3C-Ethernet0/2]port link-type trunk ； 设置当前端口为 trunk

[H3C-Ethernet0/2]port trunk permit vlan {ID|All} ； 设 trunk 允许的 VLAN

注意：所有端口缺省情况下都是允许 VLAN1 的报文通过的

[H3C-Ethernet0/2]port trunk pvid vlan 3 ；设置 trunk 端口的 PVID

配置基于 Hybrid 端口的 VLAN

[H3C-Ethernet0/2]port link-type hybrid ;配置端口的链路类型为 Hybrid 类型

[H3C-Ethernet0/2]port hybrid vlan vlan-id-list { tagged | untagged } ;允许指定的 VLAN 通过当前 Hybrid 端口

注意：缺省情况下，所有 Hybrid 端口只允许 VLAN1 通过

[H3C-Ethernet0/2]port hybrid pvid vlan vlan-id ;设置 Hybrid 端口的缺省 VLAN

注意：缺省情况下，Hybrid 端口的缺省 VLAN 为 VLAN1

VLAN 描述

[H3C]description string ；指定 VLAN 描述字符

[H3C]description ；删除 VLAN 描述字符

[H3C]display vlan [vlan_id] ； 查看 VLAN 设置

私有 VLAN 配置

[SwitchA-vlanx]isolate-user-vlan enable ； 设置主 vlan

[SwitchA]Isolate-user-vlan <x> secondary <list> ； 设置主 vlan 包括的子 vlan

[H3C-Ethernet0/2]port hybrid pvid vlan <id> ； 设置 vlan 的 pvid

[H3C-Ethernet0/2]port hybrid pvid ； 删除 vlan 的 pvid

[H3C-Ethernet0/2]port hybrid vlan vlan_id_list untagged ； 设置无标识的 vlan

如果包的 vlan id 与 PVId 一致，则去掉 vlan 信息. 默认 PVID=1。

所以设置 PVID 为所属 vlan id, 设置可以互通的 vlan 为 untagged.

30. STP 配置

[H3C]stp {enable|disable} ； 设置生成树,默认关闭

[H3C]stp mode rstp ； 设置生成树模式为 rstp

[H3C]stp priority 4096 ；设置交换机的优先级

[H3C]stp root {primary|secondary} ； 设置为根或根的备份

[H3C-Ethernet0/1]stp cost 200 ；设置交换机端口的花费

MSTP 配置：

配置 MST 域名为 info，MSTP 修订级别为 1，VLAN 映射关系为 VLAN2～VLAN10 映射到生成树实例 1 上，VLAN20～VLAN30 映射生成树实例 2 上。

<Sysname> system-view

[Sysname] stp region-configuration

[Sysname-mst-region] region-name info

[Sysname-mst-region] instance 1 vlan 2 to 10

[Sysname-mst-region] instance 2 vlan 20 to 30

[Sysname-mst-region] revision-level 1

[Sysname-mst-region] active region-configuration

31. MAC 地址表的操作

在系统视图下添加 MAC 地址表项

[H3C]mac-address { static | dynamic | blackhole } mac-address interface interface-type interface-number vlan vlan-id ；添加 MAC 地址表项

在添加 MAC 地址表项时，命令中 interface 参数指定的端口必须属于 vlan 参数指定的 VLAN，否则将添加失败。

如果 vlan 参数指定的 VLAN 是动态 VLAN，在添加静态 MAC 地址之后，会自动变为静态 VLAN。

在以太网端口视图下添加 MAC 地址表项

[H3C-Ethernet0/2]mac-address { static | dynamic | blackhole } mac-address vlan vlan-id

在添加 MAC 地址表项时，当前的端口必须属于命令中 vlan 参数指定的 VLAN，否则将添加失败；

如果 vlan 参数指定的 VLAN 是动态 VLAN，在添加静态 MAC 地址之后，会自动变为静态 VLAN。

[H3C]mac-address timer { aging age | no-aging } ；设置 MAC 地址表项的老化时间

注意：缺省情况下，MAC 地址表项的老化时间为 300 秒，使用参数 no-aging 时表示不对 MAC 地址表项进行老化。

MAC 地址老化时间的配置对所有端口都生效，但地址老化功能只对动态的（学习到的或者用户配置可老化的）MAC 地址表项起作用。

[H3C-Ethernet0/2]mac-address max-mac-count count ；设置端口最多可以学习到的 MAC 地址数量

注意：缺省情况下，没有配置对端口学习 MAC 地址数量的限制。反之，如果端口启动了 MAC 地址认证和端口安全功能，则不能配置该端口的最大 MAC 地址学习个数。

[H3C-Ethernet0/2]port-mac start-mac-address ；配置以太网端口 MAC 地址的起始值

在缺省情况下，E126/E126A 交换机的以太网端口是没有配置 MAC 地址的，因此当交换机在发送二层协议报文（例如 STP）时，由于无法取用发送端口的 MAC 地址，

将使用该协议预置的 MAC 地址作为源地址填充到报文中进行发送。在实际组网中，由

于多台设备都使用相同的源 MAC 地址发送二层协议报文，会造成在某台设备的不同端口学习到相同 MAC 地址的情况，可能会对 MAC 地址表的维护产生影响。

[H3C]display mac-address ； 显示地址表信息

[H3C]display mac-address aging-time ； 显示地址表动态表项的老化时间

[H3C]display port-mac ； 显示用户配置的以太网端口 MAC 地址的起始值

32. GVRP 配置

[SwitchA] gvrp # 开启全局 GVRP

[SwitchA-Ethernet1/0/1] gvrp # 在以太网端口 Ethernet1/0/1 上开启 GVRP

[SwitchE-Ethernet1/0/1] gvrp registration { fixed | forbidden | normal } # 配置 GVRP 端口注册模式 缺省为 normal

[SwitchA] display garp statistics [interface interface-list] ； 显示 GARP 统计信息

[SwitchA] display garp timer [interface interface-list] ； 显示 GARP 定时器的值

[SwitchA] display gvrp statistics [interface interface-list] ； 显示 GVRP 统计信息

[SwitchA] display gvrp status ； 显示 GVRP 的全局状态信息

[SwitchA] display gvrp statusreset garp statistics [interface interface-list] ； 清除 GARP 统计信息

33. DLDP 配置

[SwitchA] interface gigabitethernet 1/1/1 # 配置端口工作在强制全双工模式，速率为 1000Mbits/s。

[SwitchA-GigabitEthernet1/1/1] duplex full

[SwitchA-GigabitEthernet1/1/1] speed 1000

[SwitchA] dldp enable # 全局开启 DLDP。

[SwitchA] dldp interval 15 # 设置发送 DLDP 报文的时间间隔为 15 秒。

[SwitchA] dldp work-mode { enhance | normal } # 配置 DLDP 协议的工作模式为加强模式。 缺省为 normal

[SwitchA] dldp unidirectional-shutdown { auto | manual } # 配置 DLDP 单向链路操作模式为自动模式。 缺省为 auto

[SwitchA] display dldp 1 # 查看 DLDP 状态。

当光纤交叉连接时，可能有两个或三个端口处于 Disable 状态，剩余端口处于 Inactive 状态。

当光纤一端连接正确，一端未连接时：

如果 DLDP 的工作模式为 normal，则有收光的一端处于 Advertisement 状态，没有收光的一端处于 Inactive 状态。

如果 DLDP 的工作模式为 enhance，则有收光的一端处于 Disable 状态，没有收光的一端处于 Inactive 状态。

dldp reset 命令在全局下可以重置所有端口的 DLDP 状态，在接口下可以充值该端口的 DLDP 状态

34. 端口隔离配置

通过端口隔离特性，用户可以将需要进行控制的端口加入到一个隔离组中，实现隔离组中的端口之间二层、三层数据的隔离，既增强了网络的安全性，也为用户

提供了灵活的组网方案。

[Sysname] interface ethernet1/0/2 # 将以太网端口 Ethernet1/0/2 加入隔离组。

[Sysname-Ethernet1/0/2] port isolate

[Sysname]display isolate port # 显示隔离组中的端口信息

配置隔离组后，只有隔离组内各个端口之间的报文不能互通，隔离组内端口与隔离组外端口以及隔离组外端口之间的通信不会受到影响。

端口隔离特性与以太网端口所属的 VLAN 无关。

当汇聚组中的某个端口加入或离开隔离组后，本设备中同一汇聚组内的其它端口，均会自动加入或离开该隔离组。

对于既处于某个聚合组又处于某个隔离组的一组端口，其中的一个端口离开聚合组时不会影响其他端口，即其他端口仍将处于原聚合组和原隔离组中。

如果某个聚合组中的端口同时属于某个隔离组，当在系统视图下直接删除该聚合组后，该聚合组中的端口仍将处于该隔离组中。

当隔离组中的某个端口加入聚合组时，该聚合组中的所有端口，将会自动加入隔离组中

35. 端口安全配置

[Switch] port-security enable # 启动端口安全功能

[Switch] interface Ethernet 1/0/1 # 进入以太网 Ethernet1/0/1 端口视图

[Switch-Ethernet1/0/1] port-security max-mac-count 80 # 设置端口允许接入的最大 MAC 地址数为 80

[Switch-Ethernet1/0/1] port-security port-mode autolearn # 配置端口的安全模式为

autolearn

[Switch-Ethernet1/0/1] mac-address security 0001-0002-0003 vlan 1 # 将Host 的MAC地址0001-0002-0003 作为 Security MAC 添加到 VLAN 1 中

[Switch-Ethernet1/0/1] port-security intrusion-mode disableport-temporarily # 设置 Intrusion Protection 特性被触发后，暂时关闭该端口

[Switch]port-security timer disableport 30 # 关闭时间为 30 秒。

36. 端口绑定配置

通过端口绑定特性,网络管理员可以将用户的MAC地址和IP地址绑定到指定的端口上。进行绑定操作后，交换机只对从该端口收到的指定 MAC 地址和 IP 地
址的用户发出的报文进行转发，提高了系统的安全性，增强了对网络安全的监控。

[SwitchA-Ethernet1/0/1] am user-bind mac-addr 0001-0002-0003 ip-addr 10.12.1.1 # 将 Host 1 的 MAC 地址和 IP 地址绑定到 Ethernet1/0/1 端口。

有的交换机上绑定的配置不一样

[SwitchA] interface ethernet 1/0/2

[SwitchA-Ethernet1/0/2] user-bind ip-address 192.168.0.3 mac-address 0001-0203-0405

端口过滤配置

[SwitchA] interface ethernet1/0/1 # 配置端口 Ethernet1/0/1 的端口过滤功能。

[SwitchA-Ethernet1/0/1] ip check source ip-address mac-address

[SwitchA] dhcp-snooping # 开启 DHCP Snooping 功能。

[SwitchA] interface ethernet1/0/2 # 设置与 DHCP 服务器相连的端口 Ethernet1/0/2 为信任端口。

[SwitchA-Ethernet1/0/2] dhcp-snooping trust

在端口 Ethernet1/0/1 上启用 IP 过滤功能，防止客户端使用伪造的不同源 IP 地址对服务器进行攻击

37. BFD 配置

Switch A、Switch B、Switch C 相互可达，在 Switch A 上配置静态路由可以到达 Switch C，并使能 BFD 检测功能。

在 Switch A 上配置静态路由，并使能 BFD 检测功能，通过 BFD echo 报文方式实现 BFD 功能。

<SwitchA> system-view

[SwitchA] bfd echo-source-ip 123.1.1.1

[SwitchA] interface vlan-interface 10

[SwitchA-vlan-interface10] bfd min-echo-receive-interval 300

[SwitchA-vlan-interface10] bfd detect-multiplier 7

[SwitchA-vlan-interface10] quit

[SwitchA] ip route-static 120.1.1.1 24 10.1.1.100 bfd echo-packet

在 Switch A 上打开 BFD 功能调试信息开关。

<SwitchA> debugging bfd event

< SwitchA> debugging bfd scm

< SwitchA> terminal debugging

在 Switch A 上可以打开 BFD 功能调试信息开关，断开 Hub 和 Switch B 之间的链路，验证配置结果。验证结果显示，

Switch A 能够快速感知 Switch A 与 Switch B 之间链路的变化。

38. QinQ 配置

Provider A、Provider B 之间通过 Trunk 端口连接，Provider A 属于运营商网络的 VLAN1000，Provider B 属于运营商网络的 VLAN2000。

Provider A 和 Provider B 之间，运营商采用其他厂商的设备，TPID 值为 0x8200。

希望配置完成后达到下列要求：

Customer A 的 VLAN10 的报文可以和 Customer B 的 VLAN10 的报文经过运营商网络的 VLAN1000 转发后互通；Customer A 的 VLAN20 的报文可以

和 Customer C 的 VLAN20 的报文经过运营商网络的 VLAN2000 转发后互通。

[ProviderA] interface ethernet 1/0/1 # 配置端口为 Hybrid 端口，且允许 VLAN10，VLAN20，VLAN1000 和 VLAN2000 的报文通过，并且在发送时去掉外层 Tag。

[ProviderA-Ethernet1/0/1] port link-type hybrid

[ProviderA-Ethernet1/0/1] port hybrid vlan 10 20 1000 2000 untagged

[ProviderA-Ethernet1/0/1] qinq vid 1000 # 将来自 VLAN10 的报文封装 VLAN ID 为 1000 的外层 Tag。

[ProviderA-Ethernet1/0/1-vid-1000] raw-vlan-id inbound 10

[ProviderA-Ethernet1/0/1-vid-1000] quit

[ProviderA-Ethernet1/0/1] qinq vid 2000 # 将来自 VLAN20 的报文封装 VLAN ID 为 2000

的外层 Tag。

[ProviderA-Ethernet1/0/1-vid-2000] raw-vlan-id inbound 20

[ProviderA] interface ethernet 1/0/2 # 配置端口的缺省 VLAN 为 VLAN1000。

[ProviderA-Ethernet1/0/2] port access vlan 1000

[ProviderA-Ethernet1/0/2] qinq enable # 配置端口的基本 QinQ 功能，将来自 VLAN10 的报文封装 VLAN ID 为 1000 的外层 Tag。

[ProviderA] interface ethernet 1/0/3 # 配置端口为 Trunk 端口，且允许 VLAN1000 和 VLAN2000 的报文通过。

[ProviderA-Ethernet1/0/3] port link-type trunk

[ProviderA-Ethernet1/0/3] port trunk permit vlan 1000 2000

[ProviderA-Ethernet1/0/3] qinq ethernet-type 8200 # 为与公共网络中的设备进行互通，配置端口添加外层 Tag 时采用的 TPID 值为 0x8200。

[ProviderB] interface ethernet 1/0/1 # 配置端口为 Trunk 端口，且允许 VLAN1000 和 VLAN2000 的报文通过。

[ProviderB-Ethernet1/0/1] port link-type trunk

[ProviderB-Ethernet1/0/1] port trunk permit vlan 1000 2000

[ProviderB-Ethernet1/0/1] qinq ethernet-type 8200 # 为与公共网络中的设备进行互通，配置端口添加外层 Tag 时采用的 TPID 值为 0x8200。

[ProviderB-Ethernet1/0/1] quit

[ProviderB] interface ethernet 1/0/2 # 配置端口的缺省 VLAN 为 VLAN2000。

[ProviderB-Ethernet1/0/2] port access vlan 2000

[ProviderB-Ethernet1/0/2] qinq enable # 配置端口的基本 QinQ 功能，将来自 VLAN20 的报文封装 VLAN ID 为 2000 的外层 Tag。