# Layer 2

## vtp

1)as12345 vtp

domain CCIE

password CCIErock$

sw1是server，sw2是client

version 2

2)as34567 vtp

domain CCIE

password CCIErock$

mode transparent

version 2

[检查]

1)检查vtp

能看到vtp的version一致

sh vtp status

sh vtp password

## vlan & trunk

1)as12345

vlan 14,15,23,24,35,46,57,67,999

e2/0-3 trunk(看拓扑图)

无用的接口划入vlan999且关闭

2)as34567

vlan 34,38,310,49,411,999

e2/0-3 trunk(看拓扑图)

无用的接口划入vlan999且关闭

[检查]

1)ping通直连设备，可以先配ospf和eigrp，如果其邻居正常，则2层没有问题

2)查看无用的接口是否划入vlan999

sh ip int br

sh int status

3)查看trunk是否起来

sh int trunk

## stp

1)stp只有3个端口状态

2)

sw1奇数vlan为根桥，偶数vlan为备份根桥

sw2偶数vlan为根桥，奇数vlan为备份根桥

所有access的接口无延迟进入转发状态

所有access的接口收到bpdu就要shutdown，no shutdown可以恢复

3)mac地址表的老化时间为2h

[检查]

1)查看stp

能看到protocol为rstp

sh spanning-tree

2)查看stp配置

能看到mode,portfast,vlan priority

sh run | se spanning-tree

3)查看mac地址老化时间

sh mac address-table aging-time

## ppp

1)r18,r19和as20003的连接用ppp封装

2)运营商使用chap方式认证

用户名为：ACME\_R18、ACME\_R19，密码为：ccie

[检查]

1)r18,r19接口shutdown在no shutdown可以up并认证

# Layer 3

## ospf

[检查]

1)看到所有as12345邻居关系

sh ip ospf neighbor

2)看到ospf路由表

sh ip route ospf

至少2台设备上看路由表，确认r1-r7的ospf路由都有r1-r7

## eigrp

1. as34567跑eigrp

1)r8到r11做负载均衡

[解法]vlan34 delay 100

2. as45678跑eigrp

1)r15-r17支持64位metric

[解法]用命名形式配

2)r18-r19不收eigrp查询

[解法]r18-r19配eigrp stub

[检查]

1.

1)查eigrp邻居，确认邻居都有，r8-r11和sw3-sw4

sh ip eigrp neighbor

2)至少在2台设备上查看eigrp路由表，确认eigrp路由都有

sh ip route eigrp

3)在r8和r9上查看路由表信息，确认负载均衡

2.

1)在r15-r17上查看eigrp邻居关系，能看到r16-r17和sw5-sw6

sh ip eigrp neighbor

## bgp

1. as12345配bgp

1)r2,r3,r6,r7跑bgp，r4-r5不跑bgp

2)r1成为路由反射器

3)r2,r3,r6,r7用peer group配，名字为iBGP

4)PE和和as10001、as10002、as20001、as20002建立bgp邻居

[解法]注意as20001只在GREEN/BLUE/INET下宣告，as20002只在BLUE/RED/INET下宣告

[检查]

1)在r1上查看bgp邻居关系，有r2,r3,r6,r7

sh ip bgp summary

2)在r1上查看bgp配置，确认配置了路由反射器

sh run | begin r b

或者 sh run | se bgp

2. as65112

1)r2,r3配5个vrf口朝向r20，GREEN/BLUE/RED/YELLOW/INET

2)r2,r3分别在5个vrf口下与r20建立bgp邻居

3)r20在ipv4口下与r2,r3建立bgp邻居

4)宣告10网段和123网段

5)抑制10网段和123网段的细路由

[检查]

1)r20上查看邻居关系，能看到r2和r3的vrf口的邻居

sh ip bgp summary

2)r20上查看汇总路由和细路由宣告结果

能看到10网段和123网段的下一跳为0.0.0.0

sh ip bgp

3)r20上看默认路由配置

能看到除了INET(99)以外的vrf口都做了default originate

sh run | b r b

3. as34567配bgp

1)全路径

2)所有IBGP下一跳可达

3)r9和r11从as30000只收默认路由，重分发进eigrp

r9是默认出口，r11是备份出口

4)PE和和as10001、as10002、as20001、as20002建立bgp邻居

[检查]

1)任意3台设备上查看bgp邻居

要能看到其他3台设备和EBGP邻居(例如as10001)

sh ip bgp summary

2)检查路由表，确认路由都优先r9

sh ip bgp

3)r8,r10,r11查看默认路由，确认是eigrp路由，r9的默认路由是bgp路由

r8,r10,r11能看到via eigrp 34567，r9是via bgp 34567

sh ip route 0.0.0.0

4)r11上查看EBGP路由表，能看到next-hop as30000的路由

sh ip bgp

4. as45678配bgp

1)as45678配bgp没有IBGP

2)r15双向重分发

3)r15在bgp上汇总路由为123.20.1.0/24，抑制细路由

4)r16-r19默认走eigrp，bgp作为备份

5)PE和和as10003、as20003建立bgp邻居

[检查]

1)在r16-r19上查看EBGP邻居关系和默认路由

能看到r16-r19的bgp邻居关系，默认路由是从eigrp学到的

sh ip bgp vpnv4 unicast all summary

sh ip route 0.0.0.0

2)在r15上查看双向重分发的配置

sh run | se eigrp

sh run | se bgp

## ipv6 ospfv3 & bgp

1. as34567中sw3-sw4和r10-r11跑ipv6 ospfv3

1)ospfv3进程号为1

2)r10,r11做bgp和eigrp的双向重分发

3)相应接口以及loopback需要划入相应的area(看图)

4)r10,r11在ipv6上配bgp和eigrp的双向重分发

[检查]

1)r10和r11上查看ospfv3的路由表

sh ipv6 route ospf

2)r12的e0/0能ping通r14的e0/0

2. r12,r13,r14配ipv6 bgp

1)r12,r13,r14和as20001、as20002建立bgp邻居

2)r13调整选路，优先as20002

[检查]r12的e0/0能ping通r14的e0/0

## bgp policy

1. as12345和as34567配bgp策略

1)as12345和as34567的PE只通告A类的123.0.0.0/8路由进ISP的INET的EBGP邻居

2)r13优先走as20002，as20001作为备份

[解法]已经在bgp里做了，调整neighbor的weight

[检查]

1)r2,r3,r6,r7,r8-r11上查看EBGP邻居、INET方向BGP策略配置

2)r13上查看路由选路

能看到去as20002的路由的weight值为1000

sh ip bgp

# VPN

## mpls

1. as12345配vpn

1)as12345配vpn邻居

2)r1作为路由反射器

3)r1,r4,r5配成P，r2,r3,r6,r7配成PE

[解法]在bgp的vpnv4上激活邻居关系

[检查]

a)sh run | se vpnv4看到r1的vpnv4配置为route-reflector-client

b)sh bgp vpnv4 unicast all summary

在r1上查看bgp邻居，能看到r2,r3,r6,r7

在r2,r3,r6,r7上能看到r1

在r2,r3还能看到和r20的邻居关系

4)配mpls，用ldp作为标签分发协议，用loopback0作为ldp的id

[解法]在所有接口上配mpls ldp

[检查]sh mpls ldp neighbor

5)配PE的mpls，使traceroute看不到P

[解法]no mpls ip aggregate-ttl

6)r20出来后要选择r3，从r12-r14traceroute1.2.3.4要7跳

[检查]用r12/r13/r14 traceroute 1.2.3.4，看不到P，一共7跳

## dmvpn & encryption

1. 配DMVPN

1)r17是hub，r18,r19是spoke

[解法]

1)r17是nhs，nhrp配multicast dynamic

2)在r18和r19上配nhs为r17的serial口ip 203.45.17.2

3)r17-r18是以命名形式配的eigrp，需要在eigrp进程下关闭水平分割

2)r17,r18,r19使用tunnel口，其配置如下：

bandwitdth 1000

delay 10000ms

nhrp auth key 45678key

nhrp holdtime 5min

nhrp network-id 45678

mtu 1400

tcp mss 1360

disable icmp redirect

[解法]配nhrp map，做tunnel和ip的映射

3)r17-r19能够起来

[检查]检查eigrp邻居，需要把tunnel口宣告进eigrp

4)spoke之间可以直接建立隧道

2. 配ipsec

1)phase1:

isakmp police 10

auth preshare-key CCIE

encrypting aes

group 2

2)phase2:

esp-aes

transport mode

transform-set name CCIEXFORM

ipsec profile name DMVPNPROFILE

[检查]

1)r18的e0/0能ping通r19的e0/0

2)在r18上sh ip nhrp，有spoke to spoke tunnel的动态映射

3)在r17-r19上查看tunnel口的配置

## multicast

1. as45678跑组播，源在sw5的vlan5里面

[解法]

1)ip multicast-routing

2)跑组播的接口配ip pim sparse-mode

2. r15的loopback是RP，用标准RP选举机制

[解法]

1)r15的lo 0配ip pim sparse-mode

2)rp-candidate和bsr-candidate

3. r18和r19的以太网口加入232.1.1.1，sw5可以ping通

[解法]ip igmp join-group 232.1.1.1

4. sw5中剩下的接口划入vlan5

[解法]只是划入vlan5，不要shutdown

[检查]

1)r15上查rp的状态：sh ip pim rp mapping

2)r15 ping通232.1.1.1

# Other: Security and Advanced Networks

1. r20上，用户在ssh或console连上设备时看到信息：“Caution!No unauthorized access!”

[解法]banner login ##

2. sw3上e0/0-3不允许任何非法设备接入

每个接口上只允许1个mac地址

mac地址被自动绑定到端口上

如果收到任何非法数据帧，接口进入error-disable状态

[解法]

1)不允许非法接入：switchport port-security

2)每个接口上只允许1个mac地址：maximum 1

3)mac绑定：mac-address sticky

4)非法接入disable：violation shutdown

3. r20上配ssh

username: test

password: test

privilege: 1

next session: 5

不要启用aaa

只有123.10.2.0/24用户可以访问

用标准访问列表，只能ssh连设备

任何ssh都要产生日志

[解法]

1)username/password/privilege：username test privilege 1 password test

2)next session 5: ip ssh max.. 5?

3)任何ssh都要产生日志：ip ssh logging events

3)ssh加密：crypto key generate rsa, 768

4)只有123.10.2.0/24用户可以ssh访问：line vty配置

ssh访问：transport input ssh

访问控制列表：access-list 1 permit 123.10.2.0 0.0.0.255

[检查]sw3上测ssh

sw3# ssh -l test 123.20.20.20

1)能看到“Caution!No unauthorized access!”

2)r20上有ssh log

4. r20 nat INET

1) 10.1.0.0/16 和 10.2.0.0/16通过公网访问internet(AS 34567)

2) 用r20的loopback 0地址作为源地址，允许多个并发的连接，用标准访问列表

3) 要求r12-r14以及r18-r19:

trace 1.2.3.4 source e0/0时被r20翻译

trace 1.2.3.4 source loopback 0 时不被r20翻译

[解法]

1)建立访问控制列表：

access-list 2 permit 10.1.0.0 0.0.255.255

access-list 2 permit 10.2.0.0 0.0.255.255

2)做nat：lo 0作为源地址，允许多个并发连接，用访问控制列表

ip nat inside source list 2 int lo 0 overload

3)r20 nat到INET：

int ex/x.99

ip nat outside

int x/x.vrf\_number

ip nat inside

[检查]

1)用as65112以及r18和r19的10网段ping通1.2.3.4

2)在r20上查看nat的配置

5. netflow

r15 ping r19

top talkers 1/10 on r17

in next 10 seconds sort-by bytes

[检查]

1)用r15 ping r19，在r17上看流量

r17# sh ip flow top-talkers

能看到SrcIPaddress为r15，DstIPaddress为r19

6. ntp

1) r10 r12 同sw3同步时间

2) r10 r12应该和sw3同步时钟，用loopback 0作为连接地址

r10 r12用xxxx:xxxx...(ipv6地址和sw3同步)

3) sw3不能从r10 r12学到时钟信息

4) 用ntp v4

[解法]

1)sw3为同步源：ntp master

2)lo 0作为连接地址：ntp source lo 0

3)用ipv6地址同步：ntp server [sw3 ipv6 address]

[检查]

1)r10和r12上看ntp状态

#r10 sh ntp status

2)在sw3,r10,r12上查看ntp配置，确认使用loopback0做源