# 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

## 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

## 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

## 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

# Layer 3

## ospf

as12345配ospf

## eigrp

### as34567

1)r8到r11做负载均衡

### as45678

1)r15-r17支持64位metric

2)r18-r19不收eigrp查询

## bgp

### as12345

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

### 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

### as34567

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

### as45678

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

## ipv6 ospfv3 & bgp

### 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

### 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

## bgp policy

### 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

# 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

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

5)配PE的mpls，使traceroute看不到P

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

## dmvpn & encryption

1. 配DMVPN

1)r17是hub，r18,r19是spoke

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

3)r17-r19能够起来

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

## multicast

1. as45678跑组播，源在sw5的vlan5里面

2. r15的loopback是RP，用标准RP选举机制

3. r18和r19的以太网口加入232.1.1.1，sw5可以ping通

4. sw5中剩下的接口划入vlan5

# 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!”

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

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

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

5. netflow

r15 ping r19

top talkers 1/10 on r17

in next 10 seconds sort-by bytes

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