**CCIE RS5.0 T1+**

# Layer 2

## vtp

1)as12345 vtp

domain CCIE

password CCIErock?

sw1 sw2 mode是transparent

version 2

2)as34567 vtp

domain CCIE

password CCIErock?

sw3 mode server, sw4 mode client

version 2

【检查】

1)检查vtp

能看到vtp的version一致

sh vtp status

sh vtp password

【详解】

[sw1-sw4]以sw1为例

vtp version 2

vtp mode transparent #sw2为transparent，sw3为server，sw4为client

vtp domain CCIE

vtp password CCIErock? #先敲ctrl+v，再敲’?

## 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

【详解】

[sw1-sw4]以sw1为例

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

int range e0/0-3

switchport trunk encap dot

switchport mode trunk

int e0/1

sw acc vlan 14

int e0/2

sw acc vlan 15

int x #没有使用的接口

sw mode acc

sw acc vlan 999

shutdown

## stp

1)stp最多有3个instance

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

【详解】

[sw1-sw4]以sw1为例

spanning-tree mode mst

spanning-tree mst config

name cisco

instance 1 vlan 1, 15,23,35,57,67,999

instance 2 vlan 14,24,46

spanning-tree mst 1 priority 0 #sw2为4096

spanning-tree mst 2 priority 4096 #sw2为0

spanning-tree portfast default

spanning-tree portfast bpduguard default

mac address-table aging-time 7200

## 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

【详解】

[r18,r19]以r18为例

encap ppp

ppp chap hostname ACME\_R18

ppp chap password ccie

# Layer 3

## ospf

1. r1-r7建立ospf邻居关系
2. r1要求不要通告自己本地stub的link state信息给邻居，但是能够透传所有lsa
3. r1看到所有ospf路由，metric值都是65xxx

【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

【详解】

[r1-r7]

router ospf 12345

router-id 123.x.x.x

network 123.0.0.0 **0.255.255.255** area 0

[r1]

router ospf 12345

prefix-suppression

max-metric router-lsa

## eigrp

### as34567

1)r8到r11做负载均衡

[解法]vlan34 delay 100

【详解】

[r8-r11,sw3-sw4]

router eigrp 34567

router-id 123.x.x.x

network 123.0.0.0 **255.0.0.0**

no auto-summary

[sw3-sw4]

int vlan 34

delay 100

### as45678

1)不要求r15-r17支持64位metric

[解法]用命名形式配

2)eigrp路由器之间启用最强认证，使用秘钥ccie

3)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

【详解】

[r15-r17,sw5-sw6]

router eigrp cisco

address-family ipv4 autonomous-system 45678

network 123.0.0.0 **255.0.0.0**

topology base

no auto-summary

[r15-r17,sw5-sw6]启用最强认证

router eigrp cisco

address-family ipv4 unicast autonomous-system 45678

af-interface default

authentication mode hmac-sha-256 ccie

[r17]

rotuer eigrp cisco

address-family ipv4 unicast autonomous-system 45678

af-interface tunnel 0

no authentication mode

[r18-r19]

router eigrp 45678

network 123.18.18.18 #抄写错了？

no auto-summary

eigrp stub

## 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

5)r2 r3的预配取消了，需要自己配置

【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

【详解】

[r1]

router bgp 12345

no bgp default ipv4-unicast

bgp router-id 123.1.1.1

bgp log-neighbor-changes

neighbor iBGP peer-group

neighbor iBGP remote-as 12345

**#IBGP邻居关系做update-source lo 0, EBGP不做**

**neighbor iBGP update-source lo 0**

neighbor 123.2.2.2 peer-group iBGP

neighbor 123.3.3.3 peer-group iBGP

neighbor 123.6.6.6 peer-group iBGP

neighbor 123.7.7.7 peer-group iBGP

address-family ipv4

neighbor 123.2.2.2 activate

neighbor 123.3.3.3 activate

neighbor 123.6.6.6 activate

neighbor 123.7.7.7 activate

neighbor iBGP route-reflector-client

[r2,r3,r6,r7]以r2为例

routr bgp 12345

no bgp default ipv4-unicast

bgp router-id 123.x.x.x

bgp log-neighbor-changes

neighbor 123.1.1.1 remote-as 12345

neighbor 123.1.1.1 update-source lo 0

address-family ipv4

neighbor 123.1.1.1 activate

**#看拓扑图应该是在vrf口下建立EBGP邻居**

neighbor 102.123.1.1 remote-as 10002

**address-family ipv4 vrf [vrf\_id]**

neighbor 102.123.1.1 activate

### 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

【详解】

[r2,r3]以r2为例

ip vrf [vrf\_id]

rd [vrf\_number]:[vrf\_number]

**router-target** [vrf\_number]:[vrf\_number]

int e1/0

no shutdown

int e1/0.[vrf\_number]

ip address 10.201.[vrf\_number].1 255.255.255.252

ip vrf forwarding [vrf\_id]

encap dot [vrf\_number]

router bgp 12345

neighbor 10.201.[vrf\_number].2 remote-as 65112

address-family ipv4 vrf [vrf\_id]

neighbor 10.201.[vrf\_number].2 activate

[r20]

int e1/0

no shutdown

int e1/0.[vrf\_number]

ip address 10.201.[vrf\_number].2 255.255.255.252

ip vrf forwarding [vrf\_id]

encap dot [vrf\_number]

int e1/1

no shutdown

int e1/1.[vrf\_number]

ip address 10.201.[vrf\_numbe]r.6 255.255.255.252

ip vrf forwarding [vrf\_id]

encap dot vrf\_number

router bgp 65112

no bgp default ipv4-unicast

bgp router-id 123.20.20.20

neighbor 10.201.[vrf\_number].1 remote-as 12345

neighbor 10.201.[vrf\_number].5 remote-as 12345

address-family ipv4

neighbor 10.201.[vrf\_number].1 activate

neighbor 10.201.[vrf\_number].5 activate

neighbor 10.201.[vrf\_number].1 default-originate #except 99

neighbor 10.201.[vrf\_number].1 default-originate #except 99

network 123.20.20.20 mask 255.255.255.255

network 10.20.1.0 mask 255.255.255.0

network 10.20.2.0 mask 255.255.255.0

aggregate-address 10.0.0.0 mask 255.0.0.0 summary-only

aggregate-address 123.0.0.0 mask 255.0.0.0 summary-only

### 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

【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

【详解】

[r8-r11]以r8为例

router bgp 34567

no bgp default ipv4-unicast

bgp router-id 123.8.8.8

neighbor 123.9.9.9 remote-as 34567

neighbor 123.10.10.10 remote-as 34567

neighbor 123.11.11.11 remote-as 34567

neighbor 123.9.9.9 update-source lo 0

neighbor 123.10.10.10 update-source lo 0

neighbor 123.11.11.11 update-source lo 0

address-family ipv4

neighbor 123.9.9.9 activate

neighbor 123.10.10.10 activate

neighbor 123.11.11.11 activate

neighbor 123.9.9.9 next-hop-self

neighbor 123.10.10.10 next-hop-self

neighbor 123.11.11.11 next-hop-self

neighbor 101.34.1.1 remote-as 10001

address-family ipv4

neighbor 101.34.1.1 activate

[r9-r11]以r9为例

router bgp 34567

bgp default local-preference 500 #r11为400

router eigrp 34567

redistribute bgp 34567 metric 10000 100 255 1 1500 route-map b2e

**route-map b2e permit 10**

**match ip address prefix default**

ip prefix-list default permit 0.0.0.0/0

### 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)r16-r19面向as20003的接口都被划进vrf，并且只能从as20003收到默认路由

6)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

【详解】

[r15-r19]以r15为例

router bgp 45678 #r18,r19的as号为65222

no bgp default ipv4-unicast

bgp router-id 123.x.x.x

neighbor 103.45.1.1 remote-as 10003

address-family ipv4

neighbor 103.45.1.1 activate

[r15]

router bgp 45678

redistribute eigrp 45678

**aggregate-address 123.20.1.0 mask 255.255.255.0 summary-only**

router eigrp cisco

address-family ipv4 autonomous-system 45678

topology base

redistribute bgp 45678 metric 10000 100 255 1 1500

[r16-r19]

ip prefix-list default permit 0.0.0.0/0

router bgp 45678 #r18,r19为65222

address-family ipv4 vrf xxx

neigh x.x.x.x remote-as 20003

neigh x.x.x.x activate

neigh x.x.x.x prefix-list default in

#network 0.0.0.0 backdoor

#backdoor不需要做了，因为bgp的默认路由和eigrp的默认路由已经不在同一张路由表中

## 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

5)sw3是BDR，sw4是DR

6)不允许使用以下命令：

ipv6 router ospf

ipv6 ospf 1 area

【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

【详解】

[sw3,sw4,r10,r11]以sw3为例

ipv6 unicast-routing

router ospfv3

router-id 123.x.x.x

int lo 0

ospfv3 1 ipv6 area 0

int vlan 34

ospfv3 1 ipv6 area 0

int vlan 310

ospfv3 1 ipv6 area 10

[sw3-sw4]以sw3为例

**int vl 34**

**ipv6 ospf priority 254 #sw4为255，若先做sw3，需要clear ipv6 ospf process**

[r10-r11]

router bgp 34567

address-family ipv6

**redistribute ospf 1 match internal external**

**ipv6 router ospf 1**

**redistribute bgp 34567**

[r10,r11]以r10为例

router bgp 34567

neighbor **[as20001 ipv6 address]** remote-as 20001

address-family ipv6

neighbor **[as20001 ipv6 address]** activate

### r12,r13,r14配ipv6 bgp

1)r12,r13,r14和as20001、as20002建立bgp邻居

【检查】r12的e0/0能ping通r14的e0/0

**【注意】战报：r12、r14的ipv4和ipv6的lo 0 都要宣告出去**

【详解】

[r12-r14]以r12为例

router bgp 65222

neighbor [as20001 ipv6 address] remote-as 20001

address-family ipv6

neighbor [as20001 ipv6 address] activate

**network [lo 0 ipv6 address]/128**

**network [e0/0 ipv6 address]/64 #去掉最后的一位**

## 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

【解法】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

【详解】

[r2,r3,r6,r7,r8-r11]以r2为例

**ip prefix-list 123 permit 123.0.0.0/8 le 32**

**router bgp 12345**

**address-family ipv4 vrf INET #r8-r11在ipv4下做，没有vrf口**

**neighbor 101.123.1.1 prefix 123 out**

[r13]

router bgp 65222

**neighbor 202.65.1.1 weight 1000**

# 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

【详解】

[r1]

router bgp 12345

address-family vpnv4

neighbor 123.2.2.2 activate

neighbor 123.3.3.3 activate

neighbor 123.6.6.6 activate

neighbor 123.7.7.7 activate

neighbor iBGP route-reflector-client

[r2,r3,r6,r7]

router bgp 12345

address-family vpnv4

neighbor 123.1.1.1 activate

**no mpls ip aggregate-ttl**

[r1-r7]以r1为例

**mpls ldp router-id lo 0 force**

int e0/1

**mpls ip**

int e0/2

mpls ip

[r20]

**ip prefix list a permit 1.2.3.4/32**

**route-map abc permit 10**

**match ip address prefix a**

**set weight 100**

**rotue-map abc permit 20**

**router bgp 65112**

**address-family ipv4**

**neighbor 10.201.99.5 route-map abc in**

## dmvpn & encryption

### 配DMVPN

1)r17是hub，r18,r19是spoke

【解法】配nhrp server和client，若r17为命名形式eigrp，需在eigrp下关闭水平分割

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

**【疑问】来自战报：r17不能关闭水平分割？是T1还是T1+？**

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)利用vrf接口的连通性配置全局的dmvpn

4)r17-r19能够起eigrp邻居

【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

【详解】

1.

[r17]

int tunnel 0

ip address **10.18.19.1** 255.255.255.0

tunnel mode gre multipoint

tunnel source s2/0

tunnel key 45678

int vrf xxx

ip nhrp network-id 45678

ip nhrp auth 45678key

ip nhrp map multicast dynamic

ip nhrp holdtime 300

ip nhrp redirect

no ip redirects

bandwidth 1000

delay 1000

ip mtu 1400

ip **tcp adjust-mss** 1360

no ip split-horizon eigrp 45678

**router eigrp cisco**

**topology base**

**af-interface tunnel 0**

**no split-horizon**

[r18,r19]以r18为例

int tunnel 0

ip address **10.18.19.18** 255.255.255.0

tunnel mode gre multipoint

tunnel source s1/0

tunnel key 45678

int vrf xxx

ip nhrp network-id 45678

ip nhrp auth 45678key

**ip nhrp map multicast 203.45.17.2**

**ip nhrp map 10.18.19.1 203.45.17.2**

**ip nhrp nhs 10.18.19.1**

ip nhrp shortcut

ip nhrp holdtime 300

no ip redirects

bandwidth 1000

delay 1000

ip mtu 1400

ip **tcp adjust-mss** 1360

**[r18-r19]在eigrp下宣告tunnel口，以r18为例，check下r17是否需要宣告tunnel口**

**router eigrp c45678**

**address-family ipv4**

**network 203.45.18.2 255.255.255.0**

### 配encryption 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

【详解】

[r17-r19]phase1

#phase1: isakmp

crypto isakmp policy 10

**encrypt aes**

auth pre-share

group 2

crypto isakmp **key** CCIE **address 0.0.0.0**

#phase2: ipsec

**crypto ipsec transform-set CCIEXFORM**

**mode transport**

**crypto ipsec profile DMVPNPROFILE**

**set transform-set CCIEXFORM**

**int tunnel 0**

**tunnel protection ipsec profile DMVPNPROFILE**

## 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

【详解】

[r15-r19,**sw5,sw6**]以r15为例

**ip multicast-routing**

int e0/1

ip pim sparse-mode

int e0/2

ip pim sparse-mode

[r15]

**int lo 0**

**ip pim sparse-mode**

**ip pim rp-candidate lo 0**

**ip pim bsr-candidate lo 0**

[r18,r19]

int tunnel 0

ip pim sparse-mode

**int e0/0**

**ip pim sparse-mode**

**ip igmp join-group 232.1.1.1**

[sw5]

int x #

sw acc vlan 5

# 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. t1的netflow取消，变为下面这题：

给出r17的show命令结果

r17#sh int | grep 'is up'

Ethernet0/1 is up, line protocol is up

Ethernet0/2 is up, line protocol is up

Ethernet0/3 is up, line protocol is up

Loopback0 is up, line protocol is up

Tunnel0 is up, line protocol is up

Tunnel1 is up, line protocol is up

#r17sh int | grep 'is up' | wc -l

6

【详解】

r17(config) # shell processing full

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

5)ntp需要开启认证

【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

【详解】

1.

[r20]

banner login #Caution!No unauthorized access!#

2.

[sw3]

int range e0/0-3

switchport port-security

switchport port-security mac-address sticky

switchport port-security maximum 1

switchport port-security violation shutdown

3.

[r20]

**username test privilege 1 password test**

**ip ssh logging events**

**ip ssh max session 5? #需要在机器上确认下？**

**crypto key generate rsa**

**768**

**line vty 0 4**

**login local**

**transport input ssh**

**access-class 1 in**

**access-list 1 permit 123.10.2.0 0.0.0.255**

4.

[r20]

**access-list 2 permit 10.1.0.0 0.0.255.255**

**access-list 2 permit 10.2.0.0 0.0.255.255**

**ip nat inside source list 2 int lo 0 overload**

**int e1/0.99**

**ip nat outside**

**int e1/0.vrf\_number #except 99**

**ip nat inside**

**int e1/1.99**

**ip nat outside**

**int e1/1.vrf\_number #except 99**

**ip nat inside**

5.

[r15]

**ip cef**

**int tunnel 0**

**ip flow egress**

**ip flow-top-talker**

**sort-by bytes**

**cache-timeout 10000**

**top 10**

**show ip flow top-talkers**

6.

[sw3]

ntp master

ntp source lo 0

ntp authenticate

ntp authentication-key 1 md5 cisco

ntp trust-key 1

[r10,r12]

ntp server 2001:123::3:3:3 key 1

ntp source lo 0

ntp authenticate

ntp authentication-key 1 md5 cisco

ntp trust-key 1