注意：一定要把题本完完整整的看一遍，平时练习到位，时间一定够，别慌！！！

TAC不提了

TAC有点傻，不知道TAC拓扑跟TS在一张拓扑，还傻傻的问了考官TAC拓扑怎么打开。

TS我按照题目顺序做的，遇到点小问题如下：

1.做MUX-VLAN这题注意，ISIS区域，我看现场三台都是47.0004区域，我以为是对的，等做完后检查题本发现是49.0004。

2.做MPLS VPN跨域的时候注意，我在现场的题本写了一条R5配置正确。

3.做VRRP的时候看清楚给的输出结果，我碰到的是master抢占延时不一致。

LAB：

LAB2我按照题目顺序做的，由于做题顺序不同，某些现象可能暂时出不来，建议按照平时练的顺序做。

注意：考场的地址有变动，接口有变动，问题不大。

我产生的问题：eth-trunk源目ip或mac看清楚，我反正是配错了，后面检查出来的。

论述两题：

园区网出口

第一问：

解答：根据题述，默认情况下访问internet优先走ISP1链路，ISP2链路作为备份，可以使用如下两种方案实现：

1.浮动静态路由（控制层面）

由于默认情况下静态路由的优先级为60，可以通过调整静态路由优先级实现主备冗余的作用，具体配置命令如下：

Ip route-static 0.0.0.0 0.0.0.0 x.x.x.x(ISP1接口地址) preference 50

Ip route-static 0.0.0.0 0.0.0.0 x.x.x.x(ISP2接口地址)

上述命令通过调整指向ISP1的默认路由优先级，指向ISP1的默认路由优于指向ISP2的默认路由，使得访问internet优先走ISP1链路，ISP2链路作为备份，当ISP1链路故障时，切换至备份路径，使用ISP2链路转发。

2.策略路由（转发层面）

可以部署策略路由借助MQC的配置方式，直接影响数据转发，在内网接口入向调用使得访问internet直接使用ISP1链路转发。具体配置步骤如下：

默认路由使用负载分担的方式配置：

Ip route-static 0.0.0.0 0.0.0.0 x.x.x.x(ISP1接口地址)

Ip route-static 0.0.0.0 0.0.0.0 x.x.x.x(ISP2接口地址)

Acl 2000 //创建ACL匹配业务网段：

Rule permit source x.x.x.x x.x.x.x

Traffic classifier hcie //通过流分类匹配ACL

If-match acl 2000

Traffic behavior hcie //通过流行为指定下一跳为ISP1接口地址

Redirect ip-nexthop x.x.x.x(ISP1接口地址)

Traffic policy hcie //通过流策略关联流分类和流行为

Classfier hcie behavior hcie

Interface GigabitEthernet X/X/X //进入内网接口入向调用流策略

Traffic-policy hcie inbound

第二问：

考虑到上述控制层面和转发层面的部署方案仍然存在缺陷，当R1设备控制板故障时，无法处理相应报文，但是其接口状态仍然正常，静态路由无法感知，无法切换至备份路径，导致流量丢失。针对该故障，可以部署如下方案：

方案一：静态路由联动NQA测试例

可以配置NQA测试例，使用NQA ICMP测试例检测丢包情况，当检测报文丢包率到达设置值时，联动默认路由失效，从而实现路径切换，具体配置命令如下：

Nqa test-instance admin icmp //创建NQA测试例，并进入测试例视图

Test-type icmp //配置测试例类型为icmp

Destination-address ipv4 x.x.x.x(ISP1接口地址) //配置目的地址为ISP1接口地址

Fail-percent 30 //指定NQA测试失败的百分比

start now //立即执行测试例

Ip route-static 0.0.0.0 0.0.0.0 x.x.x.x(ISP1接口地址) preference 50 track nqa admin icmp

Ip route-static 0.0.0.0 0.0.0.0 x.x.x.x(ISP2接口地址)

上述命令可以实现：当探测失败比例到达30%时，测试失败，联动指向ISP1的默认路由失效，从而切换至备份路径，使用ISP2链路转发。

方案二：静态路由联动BFD会话

考虑到运营商不方便管理，可以采用BFD单臂回声的方式检测链路连通性，使得未开启BFD功能的设备收到BFD检测报文时直接将其环回，利用该特性检测链路连通性。配置命令如下：

Bfd //全局开启BFD功能

Bfd toisp1 bind peer-ip x.x.x.x(ISP1接口地址) interface GigabitEthernet X/X/X(连接ISP1的接口) one-arm-echo //创建BFD单臂回声会话

Discriminator local 1 //配置单臂回声功能的BFD会话的标识符

Commit //提交配置

Ip route-static 0.0.0.0 0.0.0.0 x.x.x.x(ISP1接口地址) preference 50 track bfd session-name toisp1

Ip route-static 0.0.0.0 0.0.0.0 x.x.x.x(ISP2接口地址)

方案三：策略路由联动NQA

静态路由仍然采用负载分担的方式配置，配置命令如下：

Ip route-static 0.0.0.0 0.0.0.0 x.x.x.x(ISP1接口地址)

Ip route-static 0.0.0.0 0.0.0.0 x.x.x.x(ISP2接口地址)

配置策略路由借助MQC的配置方式联动NQA测试例，使用NQA ICMP测试例检测丢包情况，当检测报文丢包率到达设置值时，联动策略路由失效，配置命令如下：

Nqa test-instance admin icmp //创建NQA测试例，并进入测试例视图

Test-type icmp //配置测试例类型为icmp

Destination-address ipv4 x.x.x.x(ISP1接口地址) //配置目的地址为ISP1接口地址

Fail-percent 30 //指定NQA测试失败的百分比

start now //立即执行测试例

Acl 2000 //创建ACL匹配业务网段：

Rule permit source x.x.x.x x.x.x.x

Traffic classifier hcie //通过流分类匹配ACL

If-match acl 2000

Traffic behavior hcie //通过流行为指定下一跳为ISP1接口地址并联动NQA测试例

Redirect ip-nexthop x.x.x.x(ISP1接口地址) track nqa admin icmp

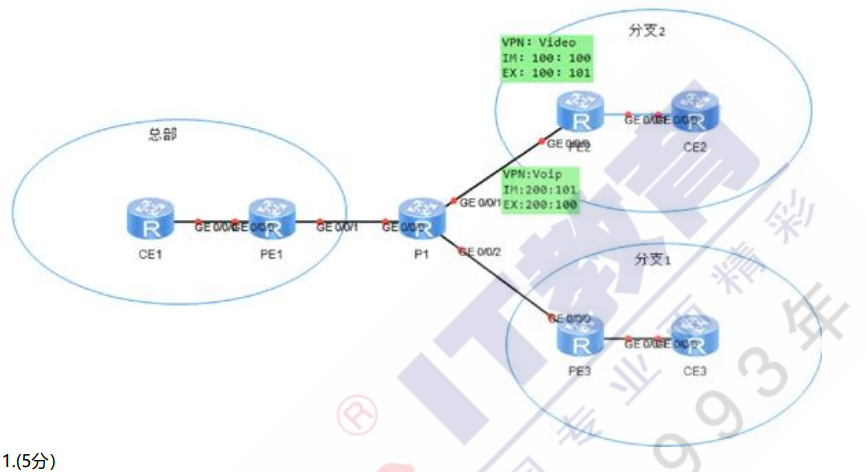
Traffic policy hcie //通过流策略关联流分类和流行为

Classfier hcie behavior hcie

Interface GigabitEthernet X/X/X //进入内网接口入向调用流策略

Traffic-policy hcie inbound

RT值规划



第一问：视频video业务，分支1和分支2都能访问总部，但是分支之间不能互访。

语音voip业务，分支和总部可以互访，分支之间也可以互访。

解答：

1.视频业务

根据题意可知，分支可以和总部互访但是分支之间无法互访，RT值规划如下：

PE1：

VPN：video IM：100:101 EX：100:100

PE3：

VPN：video IM：100:100 EX：100:101

2.语音业务

考虑安全的情况下分支之间的互访需要经过总部，通过Hub-spoke模型设计RT值如下：

PE1：

VPN：voip-im IM：200:100

VPN：voip-ex EX：200:101

PE3：

VPN：voip IM：200:101 EX：200:100

如果分支之间的互访无需经过总部，通过full-mesh全互联的方式设计RT值如下：

PE1：

VPN：voip IM：200:100 200:101 EX：200:101 200:100

PE3：

VPN：voip IM：200:100 EX：200:101

第二问：视频业务正常，但是语音业务分支1无法访问分支2

1. PE2和CE2之间的邻居关系故障：

A．注意子接口是否绑定VPN实例

B．运行的路由协议是否基于VPN实例

C．如果PE2和CE2之间的voip业务使用ospf建立邻居，需要注意DN-bit防环，确保CE2的OSPF进程下配置了vpn-instance-capability禁止环路检测。

2.full-mesh特殊场景：

A．PE2和PE3的MPBGP对等体故障。

B．PE2-P1-PE3路径的MPLS LSP隧道出现故障。

C．如果分支1和分支2的用户BGP AS号相同，需要考虑allow-as-loop允许AS号重复。

3.路由过滤：

A．VPN实例中过滤了相应业务网段的路由。

B．PE2或PE3将VPNv4路由引入进私网时错误过滤了对方分支的路由。

4.流量过滤：

A．考虑到语音业务通常由UDP承载，分支1和分支2设备可能存在过滤UDP流量行为。

B．分支1的CE3接口入向存在基于源IP地址为分支2的用户地址的流量过滤。

C．分支2的CE2接口入向存在基于源IP地址为分支1的用户地址的流量过滤。

可以通过display acl all命令查看ACL规则，如果配置错误，可以通过修改或添加规则放行相应的流量。