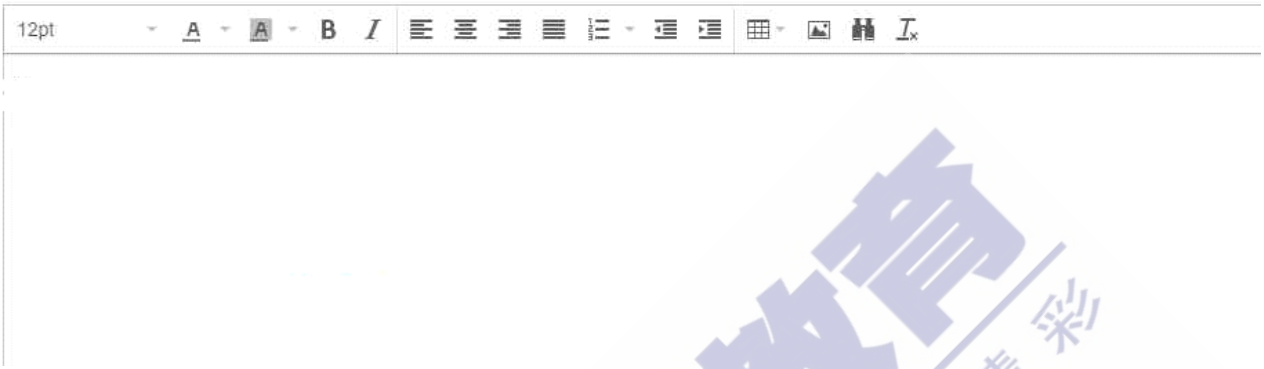
论述题（考场真题）

2021年10月21日 7:44

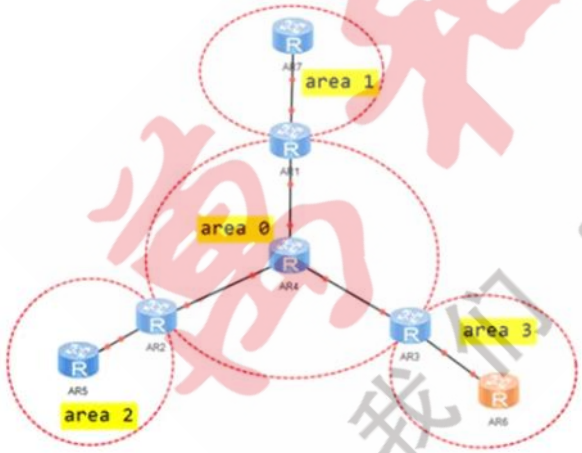
新LAB中TS、TAC、LAB都是可以确保拿A的，不需要多说了，
但是论述题满分20分（共两题，每题10分），需要单项≥15分，毕竟取代面试的模块，难度不小，需要好好准备；
据勇士鹏反馈，考场答题界面如下：



也就是说论述题可以附图，那么针对关键场景，可以尝试文字配合图片进行论述，毕竟之前面试画图也是必备技能。
目前整理的都是考场出现的考题，我尽量全面、措辞严谨的去分析了，有什么建议可以随时联系我。
一起拿下IE，加油！

OSPF论述题

第一题：OSPF园区网优化----------考场真题



上述为一个园区网内的OSPF网络的区域设计（只描述了部分区域与部分设备）

1、此时客户反映当网络变化之后部分业务出现中断时间过长，当接收到用户报修之后你该如何优化OSPF网络?

结合当前网络设计，从如下几个角度考虑加快OSPF收敛：

1、邻居关系建立层面

A、可以适当调整Hello/Dead时间，缩短邻居故障检测时间；

B、如果设备两两互联，可以将以太网接口的OSPF网络类型修改为P2P，不需要进行DR和BDR选举等待时间，缩短邻居关系建立时间；

C、接口下配置smart-discover功能，缩短邻居关系建立时间；

2、路由计算层面

A、智能计时器

在上述拓扑中可以通过智能定时器指定LSA产生、LSA接收的时间间隔为0，使得拓扑或者路由的变化可以通过LSA发布到网络

中，
或者立即被感知到，从而加快路由的收敛，智能计时器基本配置命令如下：
ospf 1
 lsa-originate-interval intelligent-timer 5000 0 100
上述命令的作用是：当网络稳定，拓扑或路由信息变化会立刻产生LSA并泛洪，而如果网络出现震荡则会对产生间隔进行一定的增加，
产生间隔最大值5s，智能计时器一定程度上既能保证快速收敛，又可以降低网络震荡的影响。
B、按优先级收敛
针对特定部分关键业务，配置按优先级收敛，保证关键业务更快完成路由收敛，相应配置命令如下：
[R2-ospf-1]prefix-priority ?
  critical Config the priority of routes as critical
  high   Config the priority of routes as high
  medium   Config the priority of routes as medium

3、快速收敛技术
A、借助BFD与OSPF联动进行快速故障检测
OSPF与BFD联动，通过BFD对链路故障的快速感应并通知OSPF协议，从而加快OSPF协议对于网络拓扑变化的响应，相应配置命令如下：
[R1]bfd
[R1-bfd]ospf 1
[R1-ospf-1]bfd all-interfaces enable
 [R1-ospf-1]bfd all-interfaces min-tx-interval 100 min-rx-interval 100
上述命令基于接口实现了OSPF与BFD的联动，并且通过将检测报文的收发间隔修改为100ms加速故障检测。
B、配置OSPF FRR 快速重路由加速收敛
OSPF FRR（Fast Reroute）利用LFA算法预先计算好备份链路，并与主链路一起加入转发表FIB。
当网络出现故障时，OSPF FRR可以在转发层面将流量快速切换到备份链路上，保证流量不中断，相应配置命令如下：
[R1]ospf 1
[R1-ospf-1]frr
[R2-ospf-1-frr]loop-free-alternate
C、其他高级技术
如果设备支持NSR不间断路由、GR等不间断转发能力，也可以开启对应特性从而保证业务不中断。

2、随着客户业务的发展，合作伙伴越来越多，此时用户的网络需要学到所有合作伙伴的业务路由，你该为客户推荐哪种方案进行解决，为什么采用这种方案?
解决方案：
由于用户需要学习到所有合作伙伴路由，建议在边界设备上配置静态路由，并通过引入静态路由的方式将合作伙伴路由引入进客户OSPF网络。
具体原因分析如下：
1、如果与合作伙伴之间进行OSPF协议交互，互联链路的报文交互会占用相应带宽资源；
2、如果与合作伙伴之间进行OSPF协议交互，客户与合作伙伴所在区域的拓扑信息能够相互传递，不够安全；
3、因为OSPF协议需要双方网络管理员都进行相应配置，管理成本较高；

引入静态路由方案后续可以进行如下优化：
A、路由汇总部署
引入合作伙伴静态路由之后，可以在ASBR上配置路由汇总，确保客户网络能够学习汇总路由，从而减少数据库和路由表规模，也可以避免明细路由震荡造成的路由信息频繁变化。建议部署完路由汇总之后考虑配置、自动生成Null0黑洞路由防止环路问题。

B、特殊区域部署

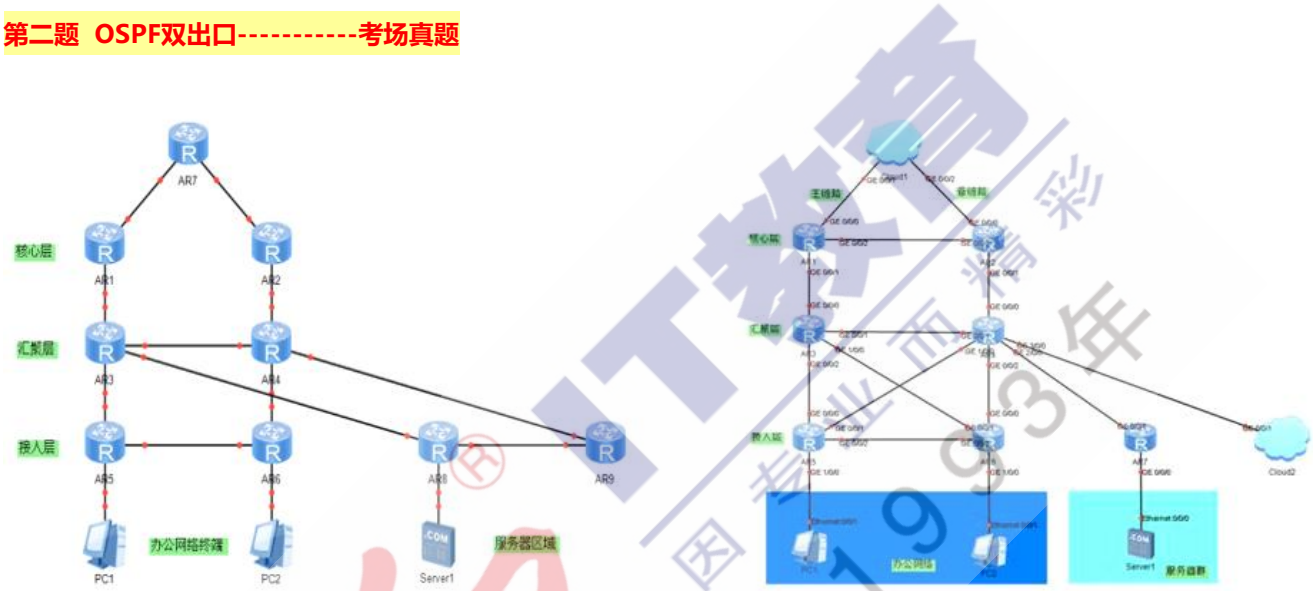
考虑上述园区网络设计已经部署多区域，可以将特定区域配置末节区域Totally Stub、Totally NSSA，减少该区域LSA、路由数量，

该区域设备可以通过ABR下发默认路由访问合作伙伴业务路由。

C、在边界路由器上将连接合作伙伴的接口配置静默接口，保证安全并节约带宽资源。

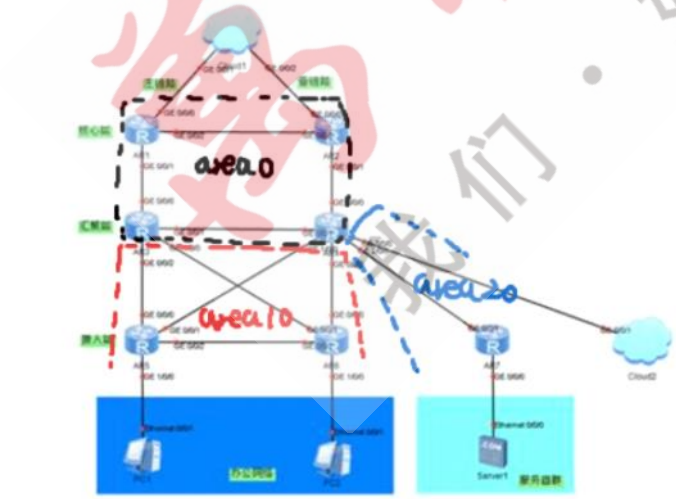
上述路由汇总和特殊区域部署的方式，一定程度上也可以实现快速收敛，因为相应特殊区域内的设备只存在默认路由，从而不需要针对域间明细进行重新计算。

第二题 OSPF双出口----------考场真题



1. 合理规划OSPF区域，使得办公网络发生变化时服务器区域（R7）路由表不会发生变化，写出两种方案，请详细描述该方案?

结合上述拓扑，建议部署OSPF多区域网络，OSPF区域规划如下：



注意：考场如果支持插入图片，最好通过画图适当的进行补充

首先将核心路由器和汇聚路由器之间所有链路部署在区域0骨干区域，

然后将办公网络接入路由器和汇聚路由器之间链路部署在区域10；服务器网络接入路由器和汇聚路由器之间链路部署在区域20。

为了实现办公网络路由发生变化而服务器所在网络不受影响可以通过如下方案实现：

方案一、路由汇总

注意考场拓扑，如果R3和R4都为ABR
AR3和AR4作为ABR配置路由汇总，将区域10的路由进行汇总，ABR只会将汇总路由通告进服务器所有区域
办公网络明细路由发生变化，服务器所在区域路由表不会变化。
如果R4连接R7，则R4作为ABR
AR4作为ABR配置路由汇总，将区域10的路由进行汇总，ABR只会将汇总路由通告进服务器所有区域
办公网络明细路由发生变化，服务器所在区域路由表不会变化。
建议手工配置或者自动生成指向Null0黑洞路由，防止路由汇总导致环路问题
方案二、特殊区域
将服务器所有区域配置为Totally stub区域，考虑到后续可能会引入直连路由建议配置为Totally NSSA区域。
该方式所有域间明细路由、外部路由都不会进入NSSA区域，ABR会下发默认路由指导本区域设备访问域间和域外。
由于域间明细路由、外部路由都无法进入NSSA区域，本区域设备无法感知其他路由变化。

上述解决方案主要就区域划分进行了分析，而利用OSPF多进程实现办公网络和服务器网络的隔离，在OSPF进程之间进行相应的路由引入，
可以通过路由过滤和路由汇总进行相应的路由控制，如果后续对业务隔离及安全性要求较高，也可以考虑多进程方案。

2. 客户提出需求，R1和R2上使用静态路由（默认路由）访问外网，当网络正常时，所有流量经过R1出去，R2作为备份链路，请写出方案?

当前拓扑需要在R1和R2通过OSPF下发默认路由，缺省情况下OSPF下发的默认路由会以LSA-5形式在除特殊区域以外的整个自治系统泛洪。
此时可以通过如下方案影响外部路由选路：
方案一：修改外部路由类型
由于外部路由对应的LSA-5存在两种度量值类型：Type-1和Type-2，其中Type-1类型外部路由进行路由计算时会优于Type-2类型外部路由。
考虑到缺省情况下外部路由的度量值类型为Type-2，为了实现流量优选R1访问外部，可以在R1配置下发默认路由命令的同时修改度量值类型为Type-1类型，具体配置命令如下：

```
ospf 1
 default-route-advertise type 1
```

方案二：修改路由开销值
A、外部开销值修改
由于默认情况OSPF下发默认路由会以类型-2的LSA-5形式传递，类型-2的LSA-5进行选路比较时候首先比较外部开销值，在R2配置如下命令修改外部开销值影响选路，将外部开销值改大：

```
[R2]ospf  1
[R2-ospf-1]default-route-advertise cost 1000
```

B、内部开销值修改
假设R1和R2都通过相应命令下发默认路由，类型-2的LSA-5进行选路比较时候首先比较外部开销值，而外部开销默认为1，然后继续比较内部开销值（去往ASBR）
建议修改接入路由器AR6和汇聚路由器AR4、汇聚路由器AR4和核心路由器AR2之间互联链路的开销值，配置如下：
以AR4为例

```
interface GigabitEthernetX/X/X
 ospf cost 100
```

上述方案成功部署之后，可以满足所有业务流量通过R1访问外部，但是考虑到当前网络拓扑中R2设备自身会通过本地配置的默认路由访问外部网络，为保证所有流量包括R2设备访问外部的流量都将R1作为出口，建议进行如下配置：
首先，R1配置默认路由指向ISP并通过OSPF下发默认路由，由于R2也配置了上述命令以实现备份，所以缺省情况下R2不会使用R1下发LSA-5进行路由计算，需要在R2配置命令允许计算R1下发默认路由，具体配置如下：

```
 ospf 1
```

default-route-advertise permit-calculate-other

其次，由于静态路由协议优先级为60，要优于OSPF外部路由优先级150，所以R2需要修改之前配置指向ISP默认路由优先级，建议修改为151，

具体配置如下：

ip route-static 0.0.0.0 0.0.0.0 X.X.X.X（ISP下一跳地址） preference 151

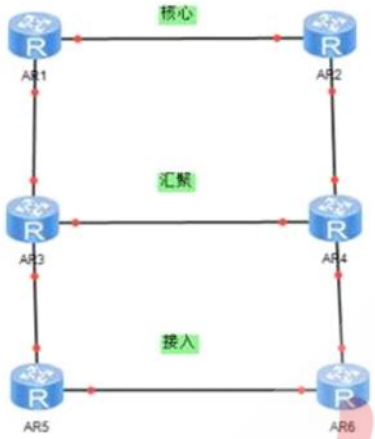
修改之后R2会优选R1通过OSPF下发默认路由，整个OSPF自治系统全部选择R1作为出口访问ISP。

注意：如果考场描述通过静态路由访问特定业务网段而不是默认路由访问Internet（ISP）

当前拓扑需要在R1和R2通过OSPF引入静态路由，默认情况下外部路由会以LSA-5形式在除了特殊区域以外的自治系统内泛洪。

也就是将上面方案描述里面的“下发默认路由” 修改成 “引入静态路由”，其他不变

第三题：日字形组网（六台设备组网）---不太确定是否为真题，需要重点关注



1. 汇聚和接入之间运行ospf并且是以太网链路，如何加快收敛，请举例？

考虑到以太网默认情况OSPF网络类型为广播型，

在邻居关系层面可以通过如下方式实现快速收敛：

A、上述拓扑设备之间两两互联，可以将以太网接口OSPF网络类型修改为P2P，不需要DR和BDR选举等待时间，缩短邻居关系建立时间

B、可以适当调整Hello\Dead时间，缩短邻居关系故障检测时间

在路由计算层面可以通过如下方式实现快速收敛：

A、智能计时器

在上述拓扑中可以通过智能定时器指定LSA产生、LSA接收的时间间隔为0，使得拓扑或者路由的变化可以通过LSA发布到网络中，或者立即被感知到，

从而加快路由的收敛，智能计时器基本配置命令如下：

ospf 1

lsa-originate-interval intelligent-timer 5000 0 100

当网络稳定，拓扑变化、路由变化会立刻产生LSA并泛洪，如果网络出现震荡则会对产生间隔进行惩罚，产生间隔最大值5s，其他智能计时器则不再赘述

B、按优先级收敛

针对特定部分关键业务，配置按优先级收敛，保证关键业务更快完成路由收敛，相应配置命令如下：

[R2-ospf-1]prefix-priority ?

critical Config the priority of routes as critical

high Config the priority of routes as high

medium Config the priority of routes as medium

针对故障切换的场景可以通过如下方式实现快速收敛：

A、借助BFD与OSPF联动进行快速故障检测

OSPF与BFD联动，BFD对链路故障的快速感应通知OSPF协议，从而加快OSPF协议对于网络拓扑变化的响应，相应配置命令如下：

[R1]bfd

[R1-bfd]ospf 1

[R1-ospf-1]bfd all-interfaces enable

[R1-ospf-1]bfd all-interfaces min-tx-interval 100 min-rx-interval 100

B、配置OSPF FRR 快速重路由加速收敛

OSPF FRR（Fast Reroute）利用LFA算法预先计算好备份链路，并与主链路一起加入转发表FIB。

当网络出现故障时，OSPF FRR可以在转发层面将流量快速切换到备份链路上，保证流量不中断，相应配置命令如下：

[R1]ospf 1

[R1-ospf-1]frr

[R2-ospf-1-frr]loop-free-alternate

2. R5和R6下游通过二层交换机接入了部分PC，这些PC持续收到无用的OSPF协议报文，请提供解决方案?

解决方案：

A、静默接口

通过配置静默接口关闭特定接口收发OSPF报文能力，该接口对应直连路由仍然可以被其他路由器学习到，相应配置命令如下：

ospf 1

silent-interface *interface-type interface-number*

B、引入直连

根据题意描述可以判断已经将相应接口宣告进OSPF，建议先将相应接口直连路由引入进OSPF，后续择期删除之前宣告命令。

3. 如果运行ospf，核心和汇聚之间的ospf的区域0，汇聚和接入之间的是ospf的区域1，汇聚路由器之间的链路应该放在哪个区域？请分析。

为了保证网络可靠，需要将汇聚路由器之间链路宣告进区域0。

分析：

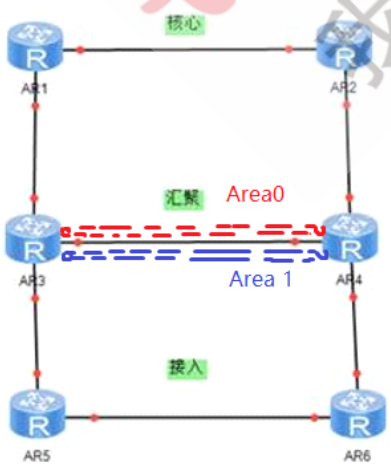
假设将汇聚路由器之间链路宣告进区域1，而核心路由器之间单一链路如果故障，则会导致骨干区域被分割。

汇聚路由器作为ABR无法使用区域1非骨干区域传递LSA-3进行路由计算。

而将汇聚路由器之间链路宣告进区域0，一定程度上可以让区域网络更可靠。

上述方案如果R3和R4之间链路带宽相对较高的话可以采用子接口的方式实现链路复用，创建两个逻辑子接口配置两个不同网段，

将不同网段分别宣告进区域0和区域1，从而流量互访的最优路径



4、该网络中，正常能实现接入左右相互分流，现在发现，接入层所有接入设备的流量都从左侧上行，请列出可能的原因（2

个)

可以从控制层面和转发层面两个角度分析可能性，考虑到控制层面配置路由过滤、修改开销值，转发层面接入路由器配置策略路由等情况，

上述情况通常为人为修改配置造成，如果排除人为修改配置的可以，则考虑其他相关的主要原因分析如下：

原因一、OSPF邻居关系层面存在故障

接入路由器R2和汇聚路由器R4、汇聚路由器R4和核心路由器R6出现OSPF邻居关系的故障，可以从分层角度分析故障可能。

依次从物理链路层面到网络层OSPF邻居关系故障，自下而上排查故障原因。

原因二、R4配置stub-router后重启恢复

假设R4出现故障并且从故障恢复，考虑各协议联系为了防止流量丢失可能在R4配置了如下命令：

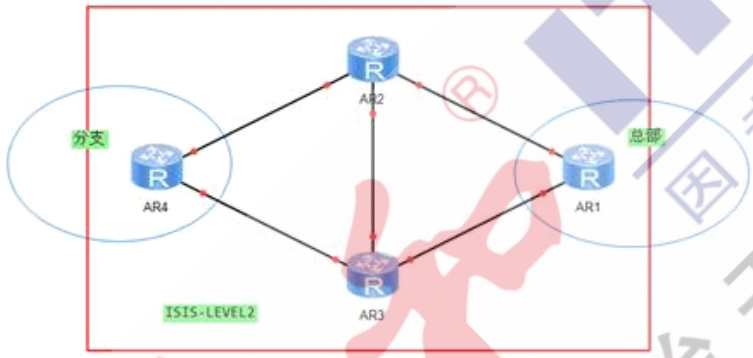
ospf 1

stub-router on-startup

在该设备重启完成之后会等待诸如BGP等协议收敛完成，在计时器到期之前会发布最大开销值，也会出现流量只通过左侧链路上行。

IS-IS论述题

第一题：isisi割接-----考场真题



如图为某企业骨干网，R1、R2、R3、R4部署了IS-IS，根据ISIS生成的路由条目，实现总部和各分支之间的流量互通。

现在您需要进行设备割接，将R3由低性能设备替换成高性能设备，同时您需要尽可能保证业务不中断，请给出三种业务不中断的方案。

解决方案：

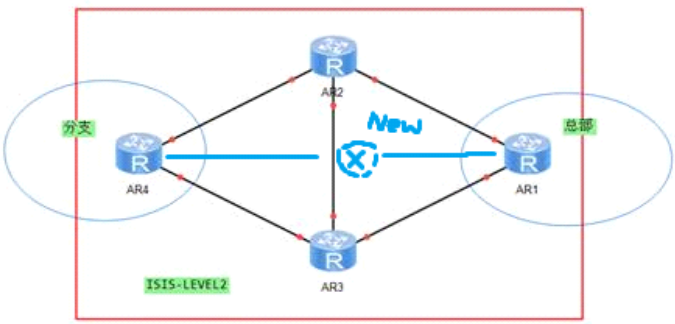
根据上述拓扑对现网概况进行充分调研，确保割接前期的需求分析、风险预案、割接方案等得到充分论证，然后根据割接方案择期进行割接。

目前在所有链路开销值一致情况下，总部和分支之间互访流量应该会采用负载分担方式流经R2和R3；

考虑该割接场景需要对R3设备进行替换，可以采用直接替换或者逐步融入方式进行上述割接的实现，

为了防止业务中断，建议采用逐步融入的方式进行设备替换。

首先将新设备接入目前网络当中，然后正确配置接口IP以及IS-IS相关配置，拓扑如下：



目前路由器IS-IS配置完成之后，所有路由器仍然参与到转发，可以采用如下方案实现割接路径切换：
方案一：设置R3的过载标识位Overload状态
设置R3的Overload-bit过载位之后，R3产生IS-IS LSP报文中的Overload-bit会置位，其它设备如R1和R4在进行SPF计算时不会使用R3做转发
（除R3直连路由以外），从而暂时将R3从当前网络中隔离，业务流量不会再经过R3转发，设置过载位相应配置命令如下：

```
isis 1
 set-overload
```

方案二：修改与R3直连链路IS-IS开销值或者下一跳权重
假设默认情况下所有链路开销值为默认值10，针对上述拓扑可以将R4连接R3、R1连接R3、R2连接R3链路两端接口开销值修改为100，
修改完链路开销在R1、R4计算路由不会再经过R3，修改链路开销命令如下：

```
interface GigabitEthernet0/0/0
 isis enable 1
 isis cost 100
```

由于修改开销值涉及设备较多，可以直接在该等价负载分担场景下通过配置下一跳权重影响选路，相应命令如下：
R1和R4的IS-IS进行下配置

```
 isis 1
 nexthop X.X.X.X weight 1
```

注：X.X.X.X为R2或者新路由器直连R1、R4接口地址，即R1或者R4路由下一跳地址

方案三：通过策略路由影响数据转发从而实现切换
上述方案一和方案二都是影响控制层面路由表，而借助基于接口策略路由可以在路由表不调整的情况下直接影响数据转发。
在R1和R4连接各自网络接口下配置策略路由，进行数据转发重定向，将流量引流至R2或者新增路由器，相应配置命令如下：

```
traffic classifier C
 if-match acl 2000
```

注：此处ACL 2000 可以根据业务网段自行定义

```
 traffic behavior C
 redirect ip-nexthop X.X.X.X
```

注：X.X.X.X为R2或者新路由器直连R1、R4接口地址，即R1或者R4路由下一跳地址

```
traffic policy C
 classifier C behavior C
interface GigabitEthernet0/0/2
 traffic-policy C inbound
```

通过上述方案，从控制层面或者转发层面将流量引导至R2或者新增路由器，后续测试业务正常之后将R3移除即可。

BGP论述题

第一题：BGP邻居故障及选路--------考场真题

1、AR2-AR4的EBGP邻居关系有问题，如何排查，通过哪些命令实现？（5分）
根据当前拓扑规划，按照分层排查思路进行故障排查，步骤如下：

一、检查物理层是否存在故障
通过**display interface brief**观察接口状态是否为up，**display interface Gx/x/x**观察特定接口是否收到错误包，排查物理层故障。
如果存在物理层故障可以考虑更换模块、线缆来解决。

二、检查数据链路层是否存在故障
此时R2和R4通过以太网链路直接相连，并没有经过交换机，所以初步排除以太网数据链路层故障，
而如果R2和R4通过广域网链路相连，可以通过**display interface brief**检查协议是否up，排查广域网数据链路层存在故障。
如果数据链路层广域网协议不匹配则修改为一致即可。

三、检查网络层连通性
通过**display ip interface brief**命令观察R2和R4的直连接口配置是否正确，如果配置正确则可以通过ping测试直连链路连通性。
假设R2和R4之间通过环回口建立EBGP对等体，需要保证环回口可达，利用ping测试检查环回口连通性。
请使用命令**ping –a source-ip-address –s packetsize host**来检测两端的互通性，指定源地址可以同时检测两端路由是否可达，
指定ping的字节可以检查大包在链路上传输是否正常，排除MTU影响。
如果无法ping通相应地址，则可以进行如下检查：
控制层面检查路由表，通常情况下在AS之间通过静态路由实现环回口可达，通过**display ip routing-table protocol static**检查静态路由配置是否正确。
转发层面排除存在基于特定源、目地址的流量过滤行为，可以通过**display traffic-filter/traffic-policy applied-record**检查是否存在流量过滤，假设存在流量过滤，通过**display acl all**检查ACL规则是否配置正确，修改添加相应规则放行流量即可。

四、检查BGP邻居关系故障
由于BGP基于TCP建立对等体关系，可以通过命令**display tcp status**检查TCP状态验证TCP会话建立情况、是否开放相应端口，
也可以判断BGP对等体配置是否正确。
通过**display bgp peer**观察目前邻居关系停留状态，根据停留状态分析故障原因如下：
邻居关系停留在idle状态，在该场景中则可能由于：更新源地址配置错误、AS号配置错误、router-id冲突、EBGP多跳未配置等原因造成；
邻居关系停留在connect状态，在该场景中则可能由于：存在认证错误、基于TCP 179端口的流量过滤；
邻居关系停留在Active状态，在该场景中则可能由于：使用环回口建立EBGP对等体但是没有修改更新源；

部分错误可以通过**display bgp error**进行排查定位。
通过命令**display current-configuration configuration bgp**查看BGP配置，针对BGP的配置错误修改相应配置，针对TCP流量过滤修改ACL相应规则即可。

2、AS100上做操作，在网络没有问题的时候，如何控制让AS200访问10.1.1.1 选择AR1-AR3的路径，请写出2种方案（5分）有问题?
根据BGP选路原则，可以通过诸如协议优选值Preferred-value、本地优先级Local-Preference、AS-Path属性、Origin起源属性、MED等属性调整选路。
考虑当前网络工程师只能在AS100进行相应操作，推荐使用MED属性、AS-Path属性调整流量入站选路。
由于需要控制流量通过AR1-AR3之间路径转发，则将AR2和AR4之间链路作为备份链路，配置方案如下：
一、修改MED属性方案
在AR2出向进行路由MED属性调整，具体命令如下：

```
ip ip-prefix  10 permit  10.1.1.1 32                    //通过前缀列表匹配特定路由，ACL也可以实现
route-policy MED permit node 10                         //通过路由策略修改特定路由MED属性
 if-match ip-prefix 10
 apply cost 1000
route-policy MED permit node 20                         //其他路由正常放行
bgp 100
peer X.X.X.X route-policy MED export                 //出向调用路由策略
```

验证：利用ping -r -a 10.1.1.1 X.X.X.X 验证流量回包路径是否满足方案。

二、修改AS-Path属性方案
在AR2出向进行路由AS-Path属性调整，具体命令如下：

```
ip ip-prefix  10 permit  10.1.1.1 32                    //通过前缀列表匹配特定路由，ACL也可以实现
route-policy AS permit node 10                          //通过路由策略修改特定路由AS-Path属性
 if-match ip-prefix 10
 apply as-path 100 additive
route-policy AS permit node 20                          //其他路由正常放行
bgp 100
peer X.X.X.X route-policy AS export                     //出向调用路由策略
```

验证：利用ping -r -a 10.1.1.1 X.X.X.X 验证流量回包路径是否满足方案。
上述两种方案可以完成流量入站访问10.1.1.1选路优选AR1和AR3之间链路，而修改路由Origin起源属性也可以满足要求，此次不再赘述。

第二题：RR选型----------考场真题

路由反射器选型：
1、公司采购两台路由器作为RR，路由器有很多指标：NAT、QoS能力等，该路由器不兼任ASBR、P角色，请你写出觉得最重要的两个指标，为什么?

由于该路由器不兼任ASBR、P等设备角色，判断RR路由反射器部署在骨干承载网络中，该场景中最重要的指标分析如下：
一、可靠性指标
虽然通过采购两台路由器并部署备份RR的方式一定程度上可以提供相应的冗余能力，但是路由反射器作为骨干网络控制层面的核心设备，我们仍然需要关注该设备的可靠性指标，需要保证RR路由器能够提供如下可靠性保证：
（1）设备可靠性
作为部署在骨干网络中的关键路由器，为了保证系统可用性、业务连续性，需要保证关键部件的冗余备份。RR路由反射器需要进行大量的路由计算，而路由协议报文处理、路由计算等工作通常是由主控板完成的，因此必须保证主控板的冗余；其次交换

网板作为路由器数据交换的核心组件也需要保证冗余；最后设备的电源、风扇等关键组件也需要保证冗余，上述路由器关键组件的冗余可以避免硬件层面单点故障，另外可以部署NSR不间断路由、NSF不间断转发等技术，可以进一步提升设备级可靠性。

（2）网络可靠性

RR路由反射器承载控制层面的各种路由协议的交互，可以通过BFD技术进行快速故障检测，部署FRR快速重路由技术实现相应协议的快速收敛，需要保证RR支持上述高可靠技术来保证网络可靠性。

二、业务承载能力指标

作为骨干网络的核心设备，RR路由反射器无论在底层IGP、还是上层BGP都需要具备强大的路由承载能力，需要支持较大规格的路由表。另外考虑到骨干网络业务承载的复杂性，RR路由反射器需要支持各种IGP协议、MPLS/SR/SRv6、IPv4/IPv6双栈、L2VPN/L3VPN、单播/组播等能力，因此需要RR路由反射器具备更高的业务承载能力。

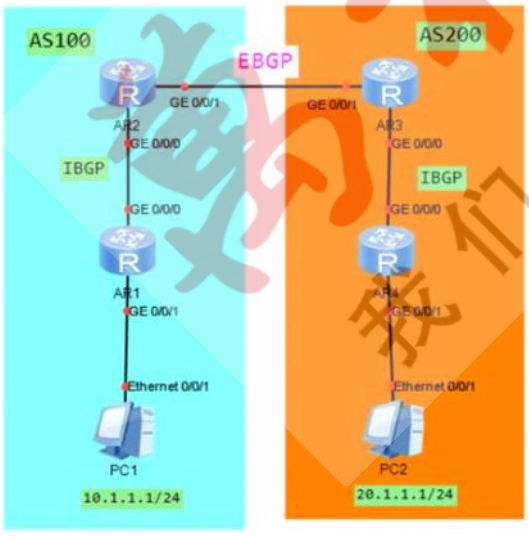
此处我们仅针对骨干网络的RR路由反射器关键指标进行介绍，而数据中心、SD-WAN场景中可能还需要关注RR路由反射器的EVPN能力，同时考虑开放接口以实现SDN控制器纳管。

2、RR上存在接口板卡，对于接口板规格需求是否有要求，跟ASBR、P设备相比，你认为RR的接口板卡性能较高还是较低，为什么?

考虑到接口板卡规格涉及到转发性能、接口数量、接口速率、接口类型等，结合上述场景该RR路由器工作在骨干网络但是不再承担诸如ASBR设备、P设备角色，因此RR路由反射器更多的是控制层面通过BGP协议完成路由计算的工作，考虑到IBGP对等体需要通过TCP会话维系对等体关系、交互协议报文，也就意味着路由反射器控制层面需要维系大量的会话、交互大量协议报文，因此接口卡的接口速率和转发性能仍然需要满足较高规格。考虑Underlay物理拓扑层面，RR只需要在满足可靠性的情况下与部分P设备、PE设备或者ASBR设备存在物理连接，因此接口密集程度和接口类型的丰富程度要求相对较低。

综上，我们可以选择转发性能、接口速率较高但是接口数量相对较低、接口类型相对单一的单板。

第三题：BGP业务及安全----------不确定是否真题，重点关注



1.如图所示，所有的设备只运行了BGP协议，R1、R4分别network相应的业务网段，此时PC1无法正常访问PC2，请问如何排查问题?

PC1无法访问PC2，可以在PC上利用ping和tracert命令验证、定位是否发生故障。

可以分段故障排查思路定位故障发生范围、节点，排查PC与网关之间故障，保证PC和网关之间可以通信。

而PC和网关之间故障通常存在物理层、数据链路层、网络层等故障，排查思路：

一、检查物理层是否存在故障

通过**display interface brief**观察接口状态是否为up，**display interface Gx/x/x**观察特定接口是否收到错误包，排查物理层

故障。
如果存在物理层故障可以考虑更换模块、线缆来解决。
二、检查数据链路层是否存在故障
通过在网关设备上display arp或者在PC设备arp -a 检查是否存在相应ARP记录，排查是否存在以太网数据链路层故障。
修改相应配置确保PC和网关在同一广播域。
三、检查网络层连通性
通过**display ip interface brief**命令观察网关直连接口配置是否正确，PC可以通过ipconfig观察地址与网关配置是否正确，如果配置正确则可以通过ping测试直连链路连通性。

如果排除PC和网关之间的故障之后可以通过如下方式快速定位路由器之间BGP协议故障。
一、控制层面故障
通过display bgp routing-table判断相应设备是否存在业务网段BGP路由，
如果自身路由没有通告进BGP则需要通过display current-configuration configuration bgp检查network配置是否正确；
如果自身路由正确通告进BGP但是无法学习到邻居设备的BGP路由，则考虑BGP邻居关系是否存在故障，考虑到该拓扑只运行BGP没有运行相应IGP，推荐使用物理接口建立IBGP、EBGP对等体，可以通过display ip interface brief检查接口地址配置，是否正确，排除直连接口连通性故障。
而BGP邻居关系故障原因分析如下：
1、部分路由器的Router ID冲突导致邻居关系停留在Idle状态
2、部分路由器对等体AS号配置错误导致邻居关系停留在Idle状态
3、部分路由器对端配置了**peer ignore**命令，禁止建立对等体导致邻居关系停留在Idle状态
4、配置BGP认证但是认证密码不一致邻居关系停留在Connect状态
5、存在基于TCP 179端口流量过滤导致邻居关系停留在Connect状态
由于该拓扑没有使用环回口建立对等体（不存在底层IGP实现环回口可达），后续建议优化为环回口建立IBGP对等体，注意需要配置
peer x.x.x.x connect-interface Loopback 修改更新源地址。而如果EBGP使用环回口建立对等体则需要配置ebgp-max-hop多跳。

如果排除BGP邻居关系故障，再次通过display bgp routing-table判断相应设备是否存在业务网段BGP路由。
如果仍然不存在对应业务网段路由，则可能原因如下：
1、部分路由下一跳不可达，因为默认情况收到EBGP对等体的路由传递给IBGP对等体下一跳不变，需要额外配置next-hop-local
2、存在响应路由过滤策略，过滤了对应路由，则需要修改命令放行对应路由

二、数据层面故障
解决上述路由表问题之后如果仍然存在PC流量访问故障，则考虑存在数据转发层面流量过滤策略。
可以通过**display traffic-filter/traffic-policy applied-record**检查是否存在流量过滤，假设存在流量过滤，
通过**display acl all**检查ACL规则是否配置正确，修改添加相应规则放行流量即可。

2.如何提升BGP安全性和可靠性，请写出方案
一、BGP安全性
1、BGP认证
可以通过配置BGP MD5 Password认证或者BGP keychain，如果认证不通过无法建立TCP会话保证BGP安全性。
BGP MD5认证具体配置命令如下：
执行命令**bgp** as号 //进入BGP视图
执行命令**peer** ip-address **password cipher** *cipher-password* XXXXXX //配置MD5认证密码
BGP Keychain认证具体配置命令如下：
执行命令**bgp** as号 //进入BGP视图

执行命令**peer** ip-address **keychain** *keychain-name*　//配置Keychain认证
注意该配置需要提前创建keychain。
2、BGP GTSM通用TTL安全机制
可以通过配置BGP GTSM实现BGP安全，配置GTSM功能缺省动作为丢弃时，可以根据网络拓扑选择合适的TTL有效范围，不符合TTL值范围的报文会被设备直接丢弃，这样就避免了网络攻击者模拟的“合法”BGP报文攻击设备，浪费CPU资源。
执行命令**bgp** as号　//进入BGP视图
执行命令**peer** ip-address　**valid-ttl-hops** [*hops*]　//配置BGP GTSM功能

二、BGP可靠性
1、利用相应技术实现快速故障感知
A、配置BGP与BFD联动
BGP协议引入了BGP与BFD联动功能。BFD可以通过UDP报文实现毫秒级检测，可以在快速通报BGP对等体间链路的故障，因此能够提高BGP路由的收敛速度，保障链路快速切换，减少流量损失，配置命令如下：
执行命令**bfd**　//开启BFD能力
执行命令**bgp**　as号　//进入BGP视图
执行命令**peer**　ip-address　**bfd enable**　//开启对等体之间BGP能力
执行命令**peer**　ip-address **bfd** { *min-tx-interval* | *min-rx-interval* | *multiplier* }　//修改BFD报文收发间隔和检测倍数

B、配置BGP tracking
使能了BGP Tracking功能的BGP对等体之间的链路发生故障时，BGP Tracking将快速感知到达邻居的路由不可达，并由路由管理模块通知到BGP对等体关系，从而实现快速收敛，配置命令如下：
执行命令**bgp**　as号　//进入BGP视图
peer　ip-address　**tracking**　//开启本地tracking命令

2、BGP GR平滑重启
BGP GR平滑重启技术保证了在设备重启或者主备倒换过程中转发层面能够继续指导数据的转发，同时控制层面邻居关系的重建以及路由计算等动作，不会影响转发层面的功能，从而避免了路由震荡引发的业务中断，提高了整网的可靠性。
执行命令**bgp**　as号　//进入BGP视图
执行命令**graceful-restart**　//使能BGP协议的GR能力。

3、BGP与IGP联动
A、BGP与OSPF联动场景
假设底层IGP采用OSPF协议，存在主备路径，主路径设备故障恢复之后，用于OSPF收敛较快会先于BGP完成收敛，后续数据报文切换到主路径，但是主路径路由器BGP没有收敛完成，导致数据报文丢包。
配置特定命令实现OSPF收敛等待BGP收敛完成，OSPF通过stub-router实现，当路由器故障恢复之后，首先将自身设置stub-router状态，
将自身LSA中链路开销值修改为最大值，不影响直连链路路由学习，流量绕过该设备，等到计时器到期之后才会取消最大开销值，
将流量切换到主路径，具体配置命令如下：
ospf 1　//进入OSPF协议视图
 stub-router on-startup 600　//配置stub-router

B、BGP与IS-IS联动场景
假设底层IGP采用IS-IS协议，存在主备路径，主路径设备故障恢复之后，用于IS-IS收敛较快会先于BGP完成收敛，后续数据报文切换到主路径，
但是主路径路由器BGP没有收敛完成，导致数据报文丢包。
配置特定命令实现IS-IS收敛等待BGP收敛完成，IS-IS通过过载位实现，当路由器故障恢复之后，将自身产生LSP的OL

overload-bit置位，其他路由器不会适应OL位置位LSP计算路由（直连链路路由除外）；流量绕过该设备，等到计时器到期之后才会取消最大开销值，将流量切换到主路径，具体配置命令如下：

isis 1

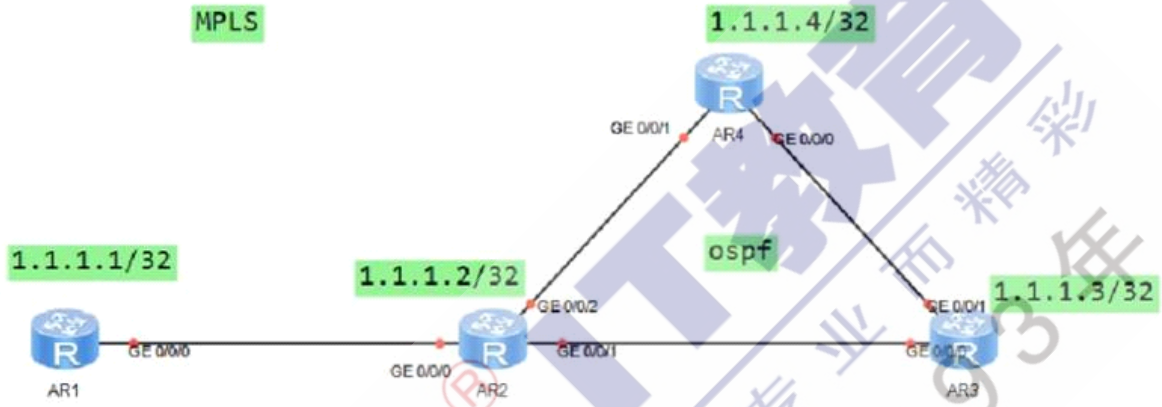
set-overload on-startup wait-for-bgp //配置OL过载位等待BGP收敛完成

4、部署备份RR

部署路由反射器简化IBGP对等体关系，用于RR作为整个AS内关键节点，需要考虑可靠性，可以通过增加备份RR实现。而配置备份RR需要注意为了避免路由重复、环路问题，通常需要将RR和备份RR的cluster-id配置一致。

MPLS及MPLS VPN

第一题：MPLS隧道建立失败----------考场真题



1、如图所示，在4台路由器使用OSPF互联互通的情况下，建立MPLS企业网LSP隧道，但发现 LSP隧道建立失败，那么影响MPLS公网LSP的因素有哪些？（至少写出4点）

结合上述拓扑，分析影响公网LSP隧道建立的因素如下：

A、底层IGP存在故障导致特定路由（传输地址）无法学习到，而通常情况下LDP会话建立使用传输地址，需要通过IGP实现可达，

可以通过display ip routing-table protocol ospf检查IGP路由表；

B、MPLS LSR-ID配置错误，导致LDP会话无法建立，默认情况下设备基于链路发现机制会使用LSR-ID的地址作为传输地址，可以通过display mpls ldp peer检查传输地址配置、display mpls ldp session检查会话是否建立；

C、某些设备系统视图或者接口视图缺少MPLS/MPLS LDP配置，可以通过display mpls interface 或者display mpls ldp interface进行检查；

D、某些设备标签通告方式配置不一致也会影响LDP会话，DU下游主动和DOD下游按需不同的通告方式无法建立LDP会话，可以通过display mpls ldp session检查会话是否建立、display mpls ldp interface检查接口配置；

E、某些设备环回口地址没有配置为/32主机地址，华为设备默认情况下仅会为IGP的/32主机路由分配并通告标签；

F、底层IGP如果配置多区域的OSPF，在ABR执行汇总也会导致LSP无法建立，可以通过跨域扩展longest-match解决；

G、存在LSP-trigger等命令匹配前缀列表不为特定路由分配标签。

2.MPLS VPN网络中，tracert命令为何不适用（中间会回显***）？

Tracert作为基于ICMP的常用故障检测工具，其工作原理具体过程如下：

首先tracert源端节点会构造UDP报文，目标端口号≥33434，目标地址为访问测试地址，通过不断将TTL加1的方式检测经过路径；

中间节点会向着源地址返回ICMP TTL超时消息，目标节点最终会返回ICMP端口不可达的消息；

考虑到MPLS VPN网络转发层面的特殊性，私网的数据报文会在公网MPLS域中进行转发，所以tracert不适用的原因分析如下：

原因1：MPLS对TTL的处理模式

管道PIPE模式
管道模式仅在入口节点和出口节点将IP报文的TTL进行减1操作，而不会复制到MPLS报文 TTL当中，MPLS报文转发过程中独立处理TTL值，
所以可能导致Tracert无法正常工作；
统一Uniform模式
统一模式会在入口设备将IP报文的TTL值复制进MPLS TTL当中，后续MPLS报文 TTL在出口设备会复制回IP报文的TTL当中；
由于缺省情况下对VPN报文不使能TTL复制功能，如果希望将MPLS VPN网络中完整路径进行追踪可以配置为统一模式，
执行命令**mpls**
执行命令 **ttl propagate vpn**

原因2：中间节点P设备可能无法回应的ICMP响应消息
缺省情况下，中间节点收到的MPLS报文只包含一层标签时，LSR使用IP路由返回ICMP响应报文，由于没有IP路由出现超时情况；
中间节点收到的MPLS报文包含多层标签时，LSR使用LSP返回ICMP响应报文；
针对中间节点收到MPLS报文只包含一层标签情况，可以通过配置命令使用LSP返回ICMP响应报文
执行命令**mpls**
执行命令**undo ttl expiration pop**

3.MPLS网络如何检测故障?

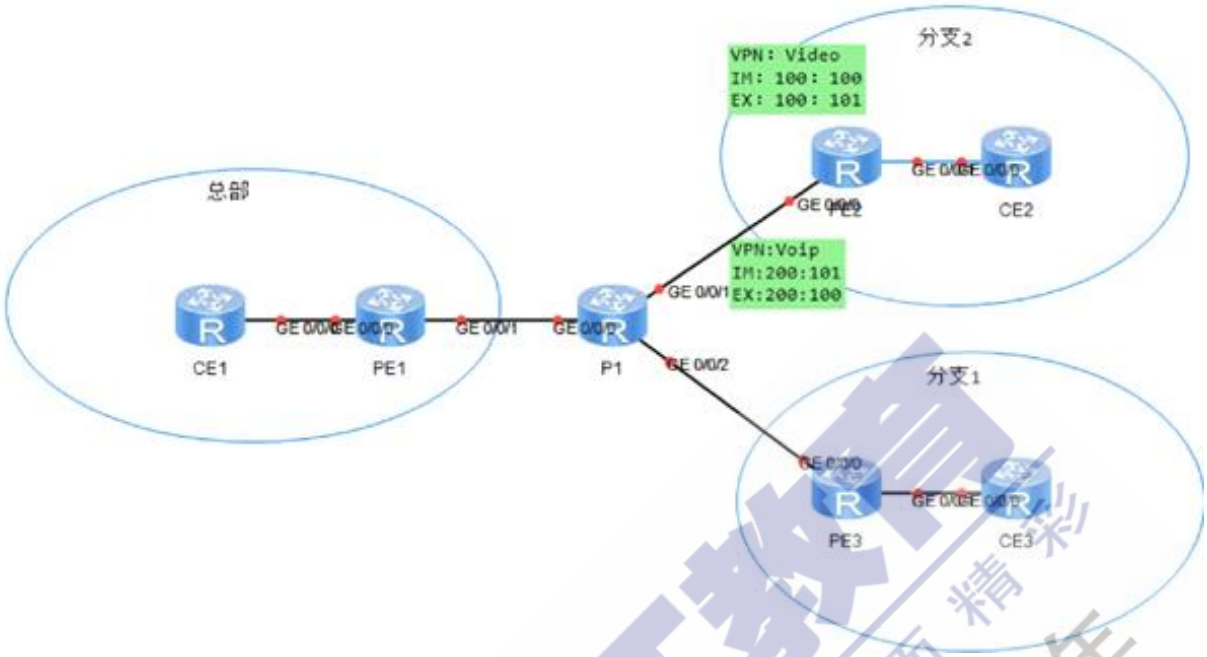
可以利用MPLS ping和MPLS tracert进行MPLS LSP连通性检测，具体工作原理分析如下：
上述两个工具可以利用MPLS回显请求（Echo Request）报文和MPLS回显应答（Echo Reply）报文检测LSP的可用性，两种消息都以UDP报文格式发送，其中Echo Request的UDP端口号为3503。

一、MPLS PING具体过程：
具体MPLS Ping命令 ping lsp ip X.X.X.X 32， MPLS echo Request会携带FEC的信息，从而实现对LSP的检测
1、Ingress入节点查找该LSP是否存在，如果不存在，返回错误信息，停止Ping。如果存在，则构造MPLS Echo Request报文，IP头中的目的地址为127.0.0.1，IP头中的TTL值为1，同时将FEC地址填入报文中的traget FEC中。然后查找相应的LSP，压入相应标签，将报文发送给Transit节点。
2、Transit节点对MPLS Echo Request报文进行普通MPLS转发，如果中间节点MPLS转发失败，则中间节点返回带有错误码的MPLS Echo Reply报文。
3、当MPLS转发路径没有故障，则MPLS Echo Request报文到达LSP的Egress出节点，将报文解封装之后检查目的FEC中包含的目标FEC地址是否为自己的接口地址，
以此来确认是否该FEC的真正出口后，返回正确的MPLS Echo Reply报文，完成整个MPLS Ping过程。

二、MPLS Tracert具体过程：
1、Ingress入节点检查LSP是否存在。如果不存在，返回错误信息，停止Tracert，如果存在，则继续构造MPLS Echo Request报文，IP头中的目的地址为127.0.0.1，同时将目标FEC地址填入报文中的目的FEC中，然后查找相应的LSP，压入LSP的标签并且将MPLS TTL设置为1，将报文发送给Transit，注意此MPLS Echo Request报文中包含下游映射TLV（携带下游信息，比如下一跳地址、出标签等）。
2、Tranist节点收到上游发送来的报文后，将MPLS Echo Request中MPLS TTL减1为0后发现TTL超时，然后继续检查是否存在对应FEC的LSP，分析下游映射TLV中的下一跳地址、出标签是否正确，如果两项检查都正确，返回正确的MPLS Echo Reply报文。如果检查有不正确，则返回错误的MPLS Echo Reply报文。
返回MPLS Echo Reply报文必须携带Tranist节点本身的包含下一跳和出标签的下游映射TLV。
3、Ingress入节点收到正确的MPLS Echo Reply报文后再次发送MPLS Echo Request报文，此时将LSP标签的MPLS TTL设置为2，下游映射TLV中携带为Tranist的下游信息。然后transit节点收到该报文后进行普通MPLS转发。
4、重复上述步骤直到Egress节点收到MPLS Echo Request报文，Egress节点同时检查目的FEC中包含的目的IP是否为自己的

接口地址，如果为自身接口地址则返回不带下游信息的MPLS Echo Reply报文，至此整个MPLS Tracert过程结束。

第二题：MPLS设计--------考场真题



1.(5分)

企业使用MPLS VPN组网。现有两种业务：

视讯业务 “video"只需要分支2和总部通讯，语音” voip"业务需要分支之间和总部都能通讯。

分支2的RT如图部署，请使用图中规划的RT，设计PE1和PE3上的RT。

一、视讯业务“Video”的RT规划与VPN实例配置

因为视讯业务 “Video"只需要分支2和总部通讯，根据分支2的RT设置，部署总部VPN实例，具体配置命令如下：

```
ip vpn-instance  Video
ipv4-family
 route-distinguisher AA:NN
 vpn-target 100:100 export-extcommunity
 vpn-target 100:101 import-extcommunity
```

可以实现分支2和总部VPNv4路由相互学习，并且将路由加入对应VRF

二、语音业务“VOIP”的RT规划与VPN实例配置

此时规划语音业务互访的时候需要考虑两种场景：

场景一：出于安全的考虑分支之间VOIP流量互访必须经由总部

可以考虑利用hub-spoke模型的VPN实现上述需求，具体配置命令如下：

A、分支1的RT和VPN实例具体配置命令如下：

```
ip vpn-instance  VOIP
ipv4-family
 route-distinguisher AA:NN
 vpn-target 200:100 export-extcommunity
 vpn-target 200:101 import-extcommunity
```

B、总部的RT和VPN实例考虑Hub-spoke模型需要创建两个VPN实例，具体配置命令如下：

```
ip vpn-instance  VOIP-IN
ipv4-family
 route-distinguisher AA:NN
 vpn-target 200:100 import-extcommunity
```

ip vpn-instance VOIP-OUT
ipv4-family
route-distinguisher AA:NN
vpn-target 200:101 export-extcommunity

场景二：分支之间VOIP业务流量互访不需要经由总部
考虑延迟、抖动等因素分支之间的VOIP业务不需要经过总部，可以考虑利用全互联Full-mesh模型的VPN实现上述需求，具体配置命令如下：
A、分支1的RT和VPN实例具体配置命令如下：
ip vpn-instance VOIP
ipv4-family
route-distinguisher AA:NN
vpn-target 200:100 200:101 export-extcommunity
vpn-target 200:100 200:101 import-extcommunity

B、总部的RT和VPN实例考虑全互联模型只需要维护一个实例即可，具体配置命令如下：
ip vpn-instance VOIP
ipv4-family
route-distinguisher AA:NN
vpn-target 200:100 import-extcommunity
vpn-target 200:101 export-extcommunity

2.（5分）
如若严格正确按照上述规划RT之后，分支1用户反应Voip业务可以和总部通讯，但是无法和分支2通讯，请分析可能的故障原因
根据故障情况分析故障可能原因，从控制层面和转发层面两个角度分析故障可能：
1、路由控制层面
A、IBGP对等体关系
首先排查是否存在VPNv4对等体无法建立故障，如果采用IBGP全互联，则通过display bgp vpnv4 all peer检查邻居关系，判断分支2和分支1之间对等体关系是否建立；
由于采用IBGP建立对等体，IBGP推荐使用环回口建立对等体，是否存在底层IGP故障导致环回口不可达，无法建立对等体关系。
B、RR配置是否正确
如果采用RR路由反射器，则需要通过display current-configuration configuration bgp命令检查路由反射器客户端是否正确配置，因为如果RR路由发生器只是指定了总部PE作为VPNv4路由客户端，也会导致分支之间非客户端路由无法正确传递；
C、VPN实例中存在特定路由过滤
可能因为特定路由过滤导致VPNv4路由无法加入相应VRF当中，则需要放行对应路由；
ip vpn-instance A
ipv4-family
import route-policy Test
D、Hub-Spoke模型的特殊配置
考虑上述场景可能采用Hub-Spoke模型，如果总部PE和CE之间运行EBGP，则需要额外考虑允许as号重复 allow-as-loop。

E、PE和CE之间引入路由执行过滤
分支1需要将私网路由进行相应双向引入，可能由于路由过滤导致分支2的路由没有引入进私网IGP，可以在分支2的CE设备检查路由表display ip routing-table验证路由引入；

2、MPLS LSP层面

由于MPLS-VPN需要建立MPLS LSP隧道保证私网流量可达，所以底层MPLS LSP出现故障也会导致路由无效，

考虑分支1和总部能够正常通信，排查LDP会话出现故障可能，在分支1的PE上通过display mpls lsp检查是否存在去往分支2的PE的LSP隧道。

3、数据转发层面

考虑到VOIP等语音流量通常基于UDP进行承载的，所以特定路由器如果过滤UDP流量也会导致VOIP也去无法正常通信。

首先可以利用ping测试业务地址连通性，然后利用display acl all检查是否存在基于VOIP（UDP）流量过滤，如果存在放行即可。

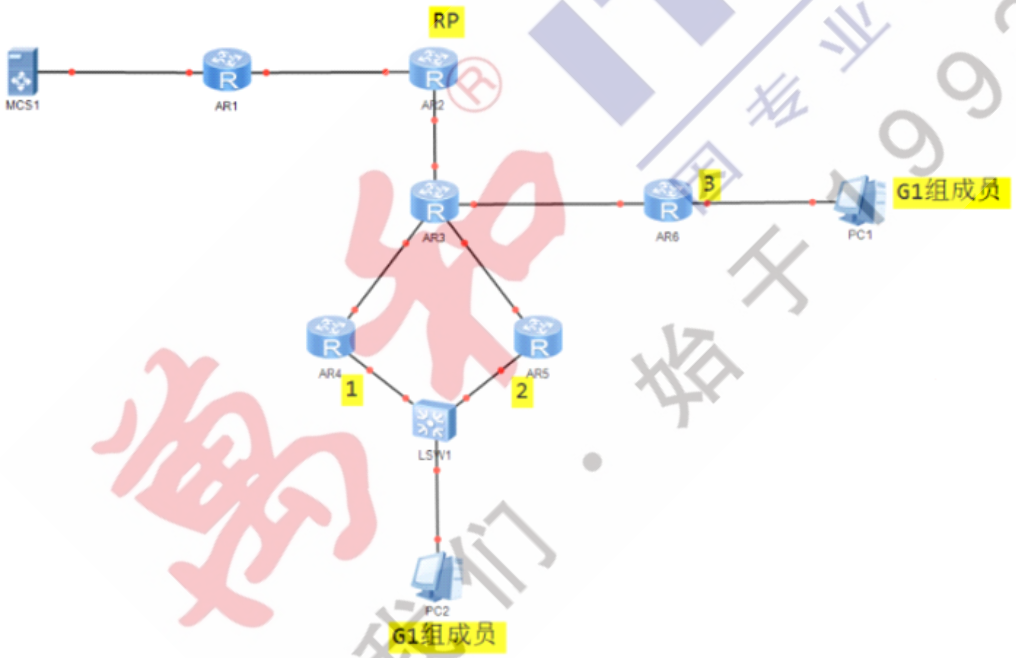
变种：

如若严格正确按照上述规划RT之后，分支和总部Video业务正常，分支1用户反应Voip业务可以和总部通讯，但是无法和分支2通讯，请分析可能的故障原因

与上述场景分析一致。

组播

第一题：组播的协议及RP可靠性----------考场真题



某组播网络示意图如图，其中MCS1是组播地址（G1）的组播源，PC1和PC2是组G1的接收者。

1、上述组播网络中，端口1、2、3需要运行哪些协议，为什么需要运行这些协议？（仅填必配的组播协议）详细写出具体原因（5分）

结合上述拓扑，考虑到存在RP场景，因此运行组播路由协议为PIM-SM协议，并且组播模型为ASM任意源模型。

（1）启用IGMP

端口1、2、3都连接组成员，所以需要考虑最后一台路由如何维系组成员关系，需要配置IGMP协议，具体分析原因如下：

A、运行IGMPv1版本1的情况

由于IGMPv1版本1无法自行选举查询器，所以需要借助PIM协议协助选举查询器，保证IGMPv1可以正常工作。

B、运行IGMPv2版本2的情况

由于IGMPv2版本2可以自行选举查询器，接口IP地址小的一方会被选举为查询器，只需要运行IGMPv2版本2即可。

（2）启用PIM SM

上文已经介绍过IGMP版本1必须借助PIM协助选举查询器的情况，此处不再赘述

考虑网络扩展性，由于端口1和端口2连接共享网络，后续可能出现新增路由器的情况，此时这两个接口则必须启用PIM SM功能，保证组播流量可以正常转发，另外PIM断言机制可以防止组播流量重复。
考虑网络可管理性，由于PIM SM网络中，组成员端DR会向着RP发送（*，G）Join报文构建RPT共享树，端口1和端口2可以开启PIM SM通过相应命令控制DR选举，命令如下：

```
[R6]interface  GigabitEthernet 0/0/1
[R6-GigabitEthernet0/0/1]
[R6-GigabitEthernet0/0/1]pim hello-option  dr-priority  ?
  INTEGER<0-4294967295>  Value of DR priority
```

2、在大型组播网络中，RP如何保障可靠性，降低RP的负担（详细过程）（5分）
在大型PIM SM的组播网络中，汇聚点RP为组播网络中一台重要的PIM路由器，因此需要保证可靠性。
考虑网络规模较大，静态RP的部署需要在网络中的所有PIM路由器上都配置相同的RP地址但是由于静态RP配置量较大，且无法感知拓扑变化，所以不适用于大型网络拓扑，此处考虑通过BSR机制动态选举RP保证可靠性并且降低RP负担。
我们从如下几个方案或角度来分析：
（1）配置多台C-RP并且指定服务组地址范围
假设上述拓扑场景将部分路由器配置为C-RP，同时配置多台C-BSR，保证C-BSR和C-RP都不会出现单点故障问题。
可以继续通过配置不同C-RP服务与不同组播组地址范围，实现不同组播地址选择不同的RP，降低单一RP的负担，配置方式如下：
假设R2服务组地址范围为239.1.1.0/24

```
acl 2000
 rule 5 permit source 239.1.1.0  0.0.0.255
pim
 c-rp LoopBack0 group-policy 2000
```

假设R3服务组地址范围为239.1.2.0/24

```
acl 2000
 rule 5 permit source 239.1.0.0  0.0.255.255
pim
 c-rp LoopBack0 group-policy 2000
```

所有组地址为239.1.1.0/24的业务会选择R2作为RP；所有组地址为239.1.2.0/24的业务会选择R3作为RP，提升可靠性同时降低RP负担

（2）保证开启组成员端DR触发切换。
华为设备默认情况下组成员端DR收到第一个组播数据包后立即进行SPT切换，切换之后组播流量可以通过最优路径经由SPT源树从组播源转发至组成员；
此时允许流量不经过RPT共享树，降低RP的组播流量转发负担，需要保证切换功能正常开启，不能配置永不切换。具体配置命令如下：

```
[R2-pim]spt-switch-threshold  ?
  INTEGER<1-4194304>  Value of data speed in kbps
  infinity            Never switch
```

（3）配置Anycast-RP
上文介绍的C-RP方案中，每个组播组都只能映射到一个RP，当网络流量较大、负担较重，可能导致RP压力过大；而RP失效后路由收敛较慢。
可以通过可以应用基于PIM协议的Anycast RP，可实现组播源端DR就近注册和组成员端DR就近加入，可以缓解单个RP的负担，也实现了RP备份。
假设网络中在R2和R3上都创建环回口，配置相同的地址10.10.10.10作为anycast RP，通过底层IGP保证环回口地址可达，相应anycast RP配置如下：

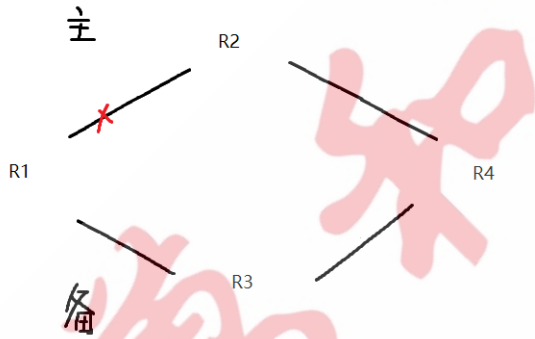
以R2为例
[R2] **pim**
[R2-pim] **c-bsr loopback 0**
[R2-pim] **c-rp loopback 0**
[R2-pim] **anycast-rp 10.10.1.1**
[R2-pim-anycast-rp-10.10.1.1] **local-address 2.2.2.2**　　R2本端地址
[R2-pim-anycast-rp-10.10.1.1] **peer 3.3.3.3**　　R3对端地址

Feature及项目

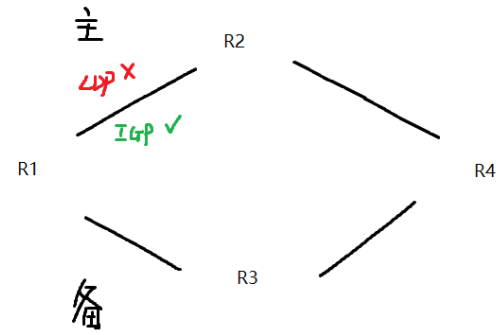
第一题：三条命令----------考场真题

ospf ldp-sync
vrrp vrid preempt-mode timer delay
stub-router on-startup
请论述上述三条命令的作用，各自的应用场景，这三条命令的共同点；

1、针对命令 ospf ldp-sync的作用及场景介绍如下：
该命令主要针对IGP与LDP联动的场景，解决因为OSPF协议与LDP协议收敛不一致导致的流量丢失问题，提升网络可靠性。
该命令通过引入相应的计时器来保证OSPF协议和LDP协议的收敛同步，具体计时器原理及场景介绍如下：
（1）hold-down timer计时器
该计时器主要通过抑制OSPF的邻居关系建立，等待LDP收敛完成，实现两种协议的同步收敛，具体场景如图所示：



当主链路故障恢复之后，OSPF协议可能会先完成收敛，而LDP收敛过程需要等待邻居发现、会话建立、标签分配及通告等阶段，
这会导致OSPF最优路径切换至主路径，但是主路径的LSP却无法建立，在MPLS-VPN等场景下公网LSP无法建立会导致流量丢失。
开启OSPF和LDP同步之后，主链路故障恢复之后会抑制OSPF邻居关系建立同时启动hold-down timer计时器，等待主链路LDP
收敛完成之后同步OSPF邻居关系建立，从而避免流量回切时流量丢失的情况。
（2）hold-max-cost计时器
该计时器主要是防止主链路OSPF协议正常，但是LDP协议故障，导致流量丢失的情况，具体场景如图所示：



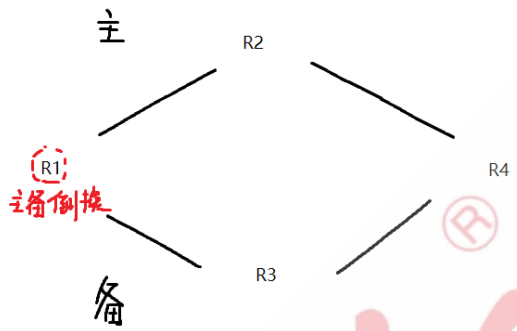
当主链路OSPF正常但是LDP出现故障之后，LDP缺省情况下只会使用最优下游分配并通告的标签，此时由于主链路的LDP故障导致LSP无法正确建立，而此时由于主链路OSPF协议正常，流量也不会切换到备份路径，所以导致流量丢失。

开启OSPF和LDP同步之后，主链路LDP故障之后会联动OSPF发布最大开销值，同时启动hold-max-cost计时器，此时由于主链路的OSPF路由已经不是最优路由，流量会切换到备份路径并使用备份路径的LSP进行转发，避免了流量丢失。

(3)delay timer

该计时器主要防止设备启用GR特性后设备发生主备倒换，OSPF等协议在LDP收敛之前完成GR，导致路径切换、流量丢失的情况，

具体场景如图所示：

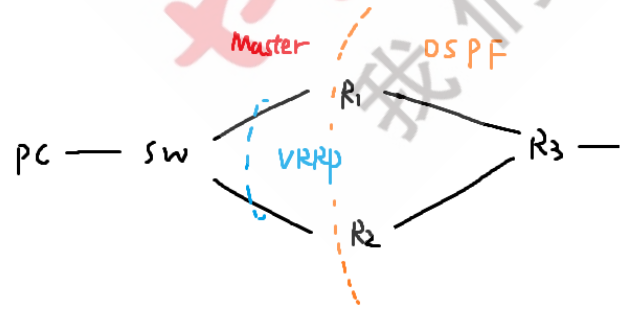


假设R1启用GR特性发生主备倒换，此时控制层面重启但是转发层面仍然可以经由主链路进行转发，后续OSPF GR完成但是LDP并未收敛完成，则OSPF可能会发布最大开销值将流量错误的切换到备份路径，出现少量流量丢失的情况。

开启OSPF和LDP同步之后，Delay Timer可以抑制OSPF协议GR的过程，等待LDP收敛完成之后再完成GR，保证控制层面OSPF和LDP的同步收敛。

2、针对命令vrrp vrid preempt-mode timer delay的作用及场景介绍如下：

上述命令通过配置VRRP Master设备的抢占延时来提升网络的稳定性，防止主备设备频繁切换导致的流量丢失问题，同时上述命令也考虑了同时部署VRRP和OSPF等协议的场景，如图所示：

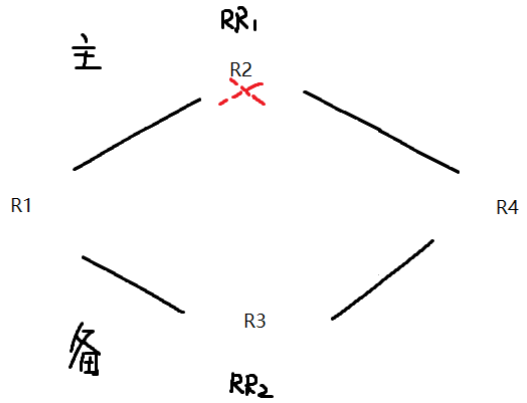


假设R1故障重启，由于R1的优先级较高所以缺省会进行抢占成为Master设备，由于R1还运行了OSPF协议进行路由学习，R1重启完成之后DR选举、数据库同步、路由计算等过程导致OSPF收敛较慢，此时PC访问外部的流量经过R1之后出现丢失的情况。

而部署VRRP抢占延时之后，可以指定VRRP的抢占延时，从而实现VRRP等待上层各协议收敛之后再进行抢占，避免流量丢失的情况。

3、针对stub-router on-startup命令的作用及场景介绍如下：

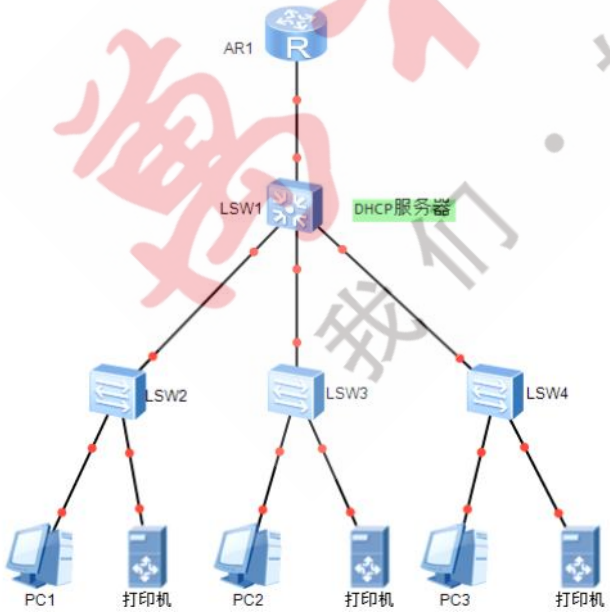
Stub-router的命令可以设置路由器成为Stub-router，通过发布最大开销值（65535）的方式实现流量不经过对应的路由器转发，可以暂时将设备从网络中独立出来，以完成一些升级迁移的计划，而此处Stub-router on-startup也可以用于OSPF与BGP的联动的场景，如图所示：



上述场景中R2作为主链路的节点发生故障重启，重启完成之后OSPF收敛较快，但是BGP收敛较慢，则R1访问R4的流量通过下一跳
迭代查表之后切换到主路径，而由于R2的BGP收敛未完成导致出现路由黑洞，造成流量丢失。
配置OSPF stub-router on-startup命令之后，当R2重启之后OSPF会启动相应计时器并发布最大开销值，在计时器到期之前会等待BGP等协议收敛，从而保证BGP收敛完成之后流量统一切换回主路径，避免流量丢失的情况。

上述三条命令的共同点分析如下：
通过上述作用和场景的分析，我们发现三条命令都考虑到了网络部署时各协议的相互影响，无论是链路主备切换、设备主备倒换，还是设备升级或者故障重启等场景，都可以实现诸如OSPF与LDP、OSPF与VRRP、OSPF与BGP等协议的同步收敛，通过引入相应的计时器来实现OSPF或者VRRP等协议等待其他协议收敛完成，保证各协议的一致性。在网络拓扑中存在主备冗余的场景中，上述配置命令也可以配合使用，尽量避免流量丢失，从而提升整个网络的可靠性及稳定性。

园区网安全----------考场真题



考题一：
（1）园区网规划如图，网络中存在部分终端无法访问网关，并且存在大量ARP表项翻动。网络中还存在部分终端IP地址为169.254.X.X。请分析可能原因，定位并排除故障。（5分）

结合园区网拓扑以及故障现象进行综合分析，初步判断网络中存在ARP攻击或者DHCP攻击的情况，现就可能原因、排障思路

和排障方案分析如下：

一、ARP欺骗攻击导致表项翻动

ARP欺骗攻击主要针对网关设备的ARP表项和终端的ARP表项两个层面来分析并定位故障。

1、网关设备的ARP表项翻动

由于网络中部分终端无法访问网关，在网关设备上通过display arp all观察ARP表项，发现ARP表项翻动的情况，可以判断存在ARP欺骗攻击伪造并修改ARP应答消息中相应字段，导致网关设备频繁更新表项。针对上述故障，我们可以在网关设备上将故障终端的ARP信息配置为静态ARP表项，如果对应终端故障暂时消失，我们可以进一步部署相应技术保证网关设备的ARP安全，解决方案如下：

（1）ARP表项固化

使能ARP表项固化功能后，可以实现网关设备初次学习到ARP表项之后，不再允许用户更新此ARP表项，或者通过发送单播ARP请求报文的方式对更新ARP条目的报文进行合法性确认。

（2）ARP表项严格学习

使能ARP表项严格学习之后，只有网关设备主动发送的ARP请求报文之后收到的应答报文才能触发本设备学习ARP，其他设备主动向本设备发送的ARP应答报文不能触发本设备学习ARP。

2、终端的ARP表项翻动

如果终端设备学习到网关设备的ARP信息为错误信息，也会导致终端设备无法访问网关，可以在终端设备上通过arp -a观察ARP记录，判断终端学习到的网关IP地址和MAC地址信息是否正确，如果错误则说存在针对网关设备的ARP欺骗攻击。

针对网关ARP欺骗攻击的解决方案如下：

（1）ARP防网关冲突

开启ARP防网关冲突之后，网关设备将生成ARP防攻击表项，并在后续一段时间内丢弃伪造的ARP报文，从而防止与网关地址冲突的ARP报文在VLAN内广播，避免终端学习到错误的ARP信息。

（2）网关设备发送免费ARP

使能网关设备周期发送免费ARP（VRRP场景默认开启），网关设备周期发送免费ARP刷新终端设备的ARP记录，避免终端学习到错误的ARP信息。

除了上述故障的排除方案，考虑到网络中存在DHCP服务器，在接入交换机部署DHCP Snooping的情况下也可以通过DAI动态ARP检测来避免ARP欺骗攻击。

二、ARP泛洪攻击导致无法通信

排查完ARP欺骗攻击并且进行相应的加固方案之后，需要进一步考虑ARP泛洪攻击导致上述故障的可能，可以在网关设备上通过display cpu-defend statistics packet-type arp-request / arp-reply all命令观察是否存在大量ARP报文丢弃，如果存在则可能出现ARP泛洪攻击。针对ARP泛洪攻击的解决方案如下：

（1）ARP报文限速

通过ARP报文限速功能，可以防止网关设备因处理大量ARP报文，导致CPU负担较高而无法相应正常的报文。

（2）ARP表项限制

ARP表项存在规格限制，如果ARP表项的泛洪攻击可能导致表项空间耗尽，导致合法用户表项无法正常学习，可以通过限制相应接口ARP表项条目数避免上述攻击。

另外针对ARP欺骗攻击和泛洪攻击进行相应的终端安全加固是必要的，比如为终端设备安装相应的杀毒软件和防火墙，也可以较大程度的降低ARP攻击的风险。

三、DHCP攻击导致客户端无法学习到IP地址

考虑到ARP的欺骗攻击和泛洪攻击会导致客户端与网关通信正常，如果通过上述解决方案排除ARP攻击的故障之后，网络中仍然存在终端无法获取到IP地址的情况，则考虑存在DHCP攻击的情况。我们可以从几个层面考虑DHCP攻击导致终端无法获取到地址的情况，并给出相应的排障方案，分析如下：

（1）非法DHCP服务器

如果网络中存在非法的DHCP服务器，但是被没有配置与客户端在同网段的地址段，会导致客户端无法正确获取到IP地址。此时可以通过dhcp snooping的信任功能，指定合法服务器接口为信息接口解决上述问题。

（2）DHCP报文泛洪攻击

针对报文的泛洪攻击，我们可以通过display cpu-defend statistics packet-type dhcp-client观察是否存在大量DHCP请求报文被丢弃，从而判断是否收到的DHCP报文泛洪攻击，针对泛洪攻击可以通过DHCP Snooping报文限速功能进行防范。

（3）DHCP地址池拒绝服务攻击

客户端不断伪造DHCP请求报文中客户端MAC地址，然后将地址池资源耗尽也会导致客户端无法获取到IP地址，可以在DHCP服务器上通过display ip pool观察地址池空闲地址数量，如果没有空闲地址则判断存在上述攻击，可以通过使能dhcp snooping对报文的CHADDR字段进行检查功能防范上述攻击。

（2）此园区网需要防止非法有线接入，请提供可行性方案。（5分）

考虑到上述园区网的拓扑设计和业务类型，针对该园区网络的非法接入，主要从以下几个角度进行防范：

（1）MAC地址安全及端口安全

接入交换机从MAC地址表层面，针对部分固定MAC地址的攻击可以通过配置黑洞MAC地址条目来实现安全防护，另外配置端口安全然后通过sticky方式形成MAC地址条目，限制接口学习到的MAC地址条目数及保护行为，可以一定程度上防止非法客户端的接入。

（2）DAI动态ARP检测

针对非法客户端接入后可能造成的ARP欺骗攻击，在开启了DHCP Snooping功能之后可以形成（MAC、IP、接口、VLAN）的绑定表项，开启DAI动态ARP检测之后，借助形成的DHCP Snooping绑定表项完成对ARP消息的合法性检测，从而防止ARP中间人等欺骗攻击。

（3）IPSG IP源防护

针对非法客户端接入后造成的IP地址欺骗攻击，也可以在开启DHCP Snooping功能之后利用DHCP Snooping绑定表项进行IP报文的合法性检测，防止非法客户端静态修改IP地址，进行IP欺骗攻击等行为。针对部分手工分配IP地址的打印机或者客户端可以手工创建静态用户绑定表项，从而通过IPSG的检测。

（4）边缘端口配合保护机制

非法客户端接入后如果伪造STP报文诸如TC BPDU也会导致整个交换网络因为拓扑变更而产生震荡，此时通过边缘端口的部署可以解决上述问题，边缘端口可以加速接口的收敛，同时不会因为端口状态迁移触发拓扑变更，配置BPDU防护等技术可以防范针对STP的恶意攻击。

（5）NAC

上述攻击防范一定程度上可以避免非法接入者带来的攻击，但是无法彻底阻断非法接入，可以通过在接入交换机上部署NAC网络接入控制来拒绝非法接入，从而实现企业网络安全。

该园区网络场景我们主要通过802.1X认证进行终端接入控制，终端设备安装802.1x客户端软件后，用户接入网络后接入交换机发起认证申请，接入交换机和用户终端交互信息后，把用户信息发送到认证服务器（如Radius服务器）进行认证，认证成功后接入机才会将相应接口作为授权接口。

针对打印机等无法安全802.1x客户端的设备，采用MAC地址认证，接入交换机将把打印机的MAC地址作为用户名和密码上送到认证服务器进行认证；认证成功之后相应的打印机设备可以访问网络；

考题二：

（1）该网络存在一些攻击，导致终端设备获取不到地址信息，请分析故障原因及如何解决？

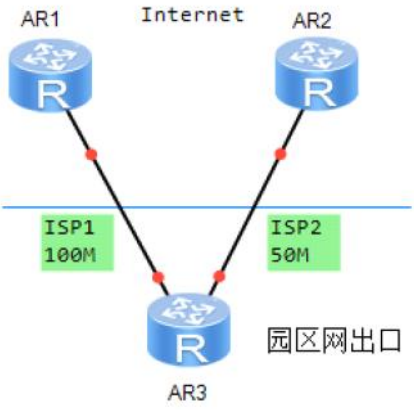
（2）为了保障网络的安全、可靠，使用何种技术来增加网络的安全性，请给出合理的方案并解释说明？

考题三：

（1）办公网络组网中，汇聚交换机和接入交换机你会部署哪些配置（6）

（2）为了该办公网络的安全，你会部署哪些安全防范（4）

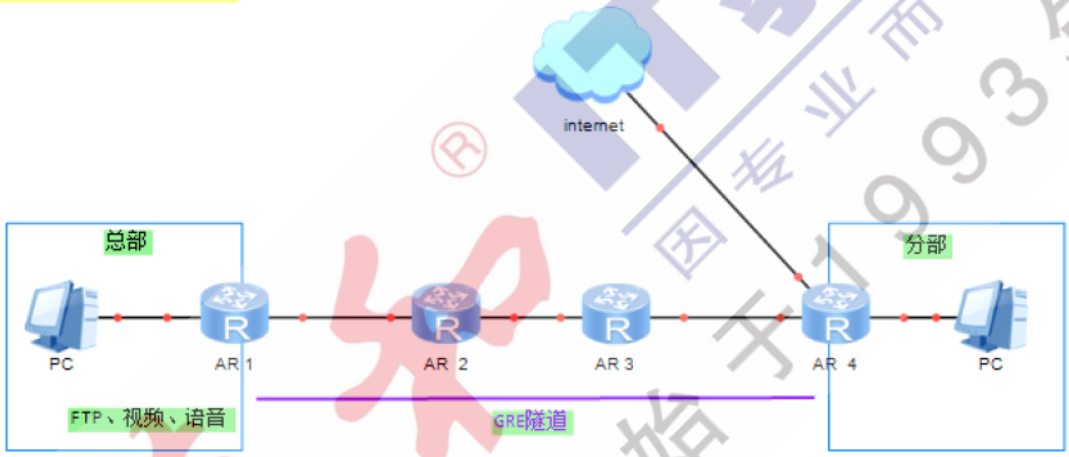
双出口------考场真题



1.公司向运营商租用两条宽带，ISP1为100M，ISP2为50M，默认情况下园区网用户访问Internet优先走ISP1链路，请提供解决方案（5分）

2.现在R1设备控制板发生了宕机，如何去实现园区网用户访问Internet走ISP2链路（再不运行动态路由协议的情况下），请您至少提供两点解决方案。（5分）

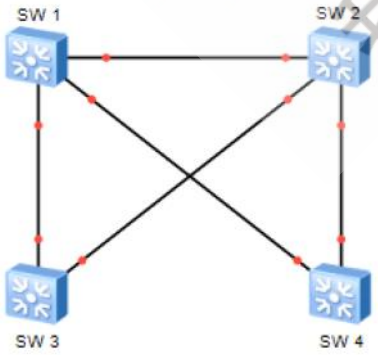
QoS---------考场真题



（1）总部和分部之间视频出现花屏、语音图像不同步的现象是有哪些原因导致的（2）

（2）现在为了保证总部和分部的通信质量，在之间部署QOS，问在哪台设备桑部署（只需要写出设备名即可）（1）如何部署QOS，需要知名详细的配置参数信息（3）

园区网规划-----据说考试真题，不太确定，重点关注



1.园区网络中，网关部署在汇聚层有什么优点（5）

2.园区网络中，网关部署在接入层有什么优点（5）