简单题目

1: 交换机是如何转发数据包的 ？

答： 交换机通过学习数据帧中的源 MAC 地址生成交换机的 MAC 地址表，交换机查看数据帧的目标 MAC 地址，根据 MAC 地址表转发数据，如果交换机在表中没有找到匹配项，则向除接受到这个数据帧的端口以外的所有端口广播这个数据帧。

2、windows 查看本机网卡 mac 地址的命令是什么？

答： 在光标闪烁处输入： ipconfig /all ，注意： ipconfig 和 /中间有 1 个空格， all 后面没有标点。然后，回车。

3、TCP 与 UDP 协议的主要区别？

答： TCP--- 传输控制协议 ,提供的是面向连接、 可靠的字节流服务。 当客户和服务器彼此交换数据前， 必须先在双方之间建立一个 TCP 连接，之后才能传输数据。 TCP 提供超

时重发，丢弃重复数据，检验数据，流量控制等功能，保证数据能从一端传到另一端。

UDP--- 用户数据报协议，是一个简单的面向数据报的运输层协议。 UDP 不提供可靠性，它只是把应用程序传给 IP 层的数据报发送出去，但是并不能保证它们能到达目的地。由于 UDP 在传输数据报前不用在客户和服务器之间建立一个连接，且没有超时重发等机制，故而传输速度很快。

4、linux 配置 2 块网卡的 IP 地址，第一块为 192.168.10.1 ，第二块为 192.168.10.2 ，如何配置命令？

答： Ifconfig eth0 192.168.10.1; ifconfig eth1 192.168.10.2 如果要永久保存 ,可用: Netconfig 以及 netconfig -d eth1 来配置 IP, 配完后 service network restart

5、写出 1433、 110、 161 端口对应的协议以及具体用途

答：1433 用于 sqlserver ； 110 ：sun 公司的 rpc 服务端口； 161 ：snmp，远程设备信息获取。

6、请解释 Vtp 协议和作用？

答： Vtp ： VLAN 中继协议， VTP，VLAN TRUNKING PROTOCOL，是 CISCO 专用协议，大多数交换机都支持该协议。 VTP 负责在 VTP 域内同步 VLAN 信息，这样就不必在每个交换上配置相同的 VLAN 信息。 VTP 还提供一种映射方案，以便通信流能跨越混合介质的骨干。 VTP 最重要的作用是，将进行变动时可能会出现在的配置不一致性降至最低。
不过， VTP 也有一些缺点，这些缺点通常都与生成树协议有关.

7、 限制内部一部分电脑浏览网页 其余电脑不受限制 用什么方法？具体语句是什么？

答： access-list 101 deny tcp [网络号] [反掩码] any eq http Access-list 101 permit ip any any

8、ARP 和 RARP 各用在什么场合？

答： ARP 和 RARP 都是工作在网络层，具体场合如下：
ARP 即地址解析协议， 是根据 IP 地址获取物理地址的一个 TCP/IP 协议。 主机发送信息时将包含目标 IP 地址的 ARP 请求广播到网络上的所有主机，并接收返回消息，以此确

定目标的物理地址；收到返回消息后将该 IP 地址和物理地址存入本机 ARP 缓存中并保留一定时间，下次请求时直接查询 ARP 缓存以节约资源。地址解析协议是建立在网络中各个主机互相信任的基础上的，网络上的主机可以自主发送 ARP 应答消息，其他主机收到应答报文时不会检测该报文的真实性就会将其记入本机 ARP 缓存；由此攻击者就可以向某一主机发送伪 ARP 应答报文，使其发送的信息无法到达预期的主机或到达错误的主机， 这就构成了一个 ARP 欺骗。ARP 命令可用于查询本机 ARP 缓存中 IP 地址和 MAC 地址的对应关系、添加或删除静态对应关系等。

RARP反向地址转换协议，允许局域网的物理机器从网关服务器的 ARP 表或者缓存上请求其 IP 地址。网络管理员在局域网网关路由器里创建一个表以映射物理地址 （MAC）和与其对应的 IP 地址。当设置一台新的机器时，其 RARP 客户机程序需要向路由器上的 RARP 服务器请求相应的 IP 地址。假设在路由表中已经设置了一个记录， RARP 服务器将会返回 IP 地址给机器，此机器就会存储起来以便日后使用。 RARP 可以使用于以太网、光纤分布式数据接口及令牌环。

9、简述一下 stp 的定义和 STP 计算的过程。

Stp 生成树协议。

一个良好的网络应该要考虑到链路的冗余，比如二层的交换机做冗余， 来防范单点故障带来的问题。但是二层做冗余的话会带来一些问题：

1.广播风暴，因为二层对未知数据帧的处理是进行广播，而且二层的封装结构又不像三层那样有 TTL 的机制来防护。所以一旦广播风暴产生，其他的交换机就会跟着广播，造成链路的堵塞瘫痪。

2.MAC 地址的重复。因为二层的工作原理，会造成交换机对一个 MAC 的多次重复的去学习，造成不必要的资源浪费，直到设备瘫痪

3.MAC 地址表的不稳定，因为要重复去学习一些地址。造成转发效率缓慢。

二层环路带来的后果是严重的 ， stp 协议就是在冗余的环境下，逻辑上去 DOWN 掉一个借口，打破环路的产生，同时做到冗余。当环境变化时，会自动跳转 down 的接口。

计算过程如下：

1.选择根网桥 2.选择根端口 3.选择指定端口 4.指定阻塞端口

B1. 什么是静态路由，其特点是什么？什么是动态路由，其特点是什么？（ 10 分）

答：静态路由是由系统管理员设计与构建的路由表规定的路由。适用于网关数量有限的场合，且网络拓朴结构不经常变化的网络。 其缺点是不能动态地适用网络状况的变化， 当网络状况变化后必须由网络管理员修改路由表。

动态路由是由路由选择协议而动态构建的， 路由协议之间通过交换各自所拥有的路由信息实时更新路由表的内容。动态路由可以自动学习网络的拓朴结构，并更新路由表。其缺点是路由广播更新信息将占据大量的网络带宽。

B2. OSPF 有什么优点 ?为什么 OSPF 比 RIP 收敛快？（10 分）

答：优点： **1**、收敛速度快； **2**、支持无类别的路由表查询、 **VLSM** 和超网技术； **3**、支持等代价的多路负载均衡； **4**、路由更新传递效率高（区域、组播更新、 **DR/BDR** ）； **5**、根据链路的带宽进行最优选路 采用了区域、组播更新、增量更新、 **30** 分钟重发 **LSA**

B3. 什么是 TCP/IP，在 TCP/IP 标准中共有几种协议来进行数据通讯？（ 10 分）

答：**TCP/IP** 是 **INTERNET** 的基础协议，也是一种电脑数据打包和寻址的标准方法。在数据传送中，可以形象地理解为有两个信封， **TCP** 和 **IP** 就像是信封，要传递的信息被划分成若干段，每一段塞入一个 **TCP** 信封，并在该信封面上记录有分段号的信息，再将 **TCP** 信封塞入 **IP** 大信封，发送上网。在接受端，一个 **TCP** 软件包收集信封，抽出数据，按发送前的顺序还原，并加以校验，若发现差错，**TCP** 将会要求重发。因此， **TCP/IP** 在 **INTERNET** 中几乎可以无差错地传送数据。在任何一个物理网络中,各站点都有一个机器可识别的地址 ,该地址叫做物理地址 .

B5. TCP/IP 的分层模型，请简述。（ 10 分）

答： **1**、应用层：应用层是我们经常接触使用的部分，比如常用的 **http** 协议、 **ftp** 协议（文件传输协议）、 **snmp**（网络管理协议）、 **telnet** （远程登录协议 ）、 **smtp**（简单邮件传输协议）、 **dns**（域名解析），这次主要是面向用户的交互的。这里的应用层集成了 **osi** 分层模型中 的应用、会话、表示层三层的功能。

2、传输层：传输层的作用就是将应用层的数据进行传输转运。比如我们常说的 **tcp**（可靠的传输控制协议）、 **udp**（用户数据报协议）。传输单位为报文段。

3、网络层：网络层用来处理网络中流动的数据包，数据包为最小的传递单位，比如我们常用的 **ip** 协议、 **icmp** 协议、 **arp** 协议（通过分析 **ip** 地址得出物理 **mac** 地址）。

4、数据链路层：数据链路层一般用来处理连接硬件的部分，包括控制网卡、硬件相关的设备驱动等。
传输单位数据帧。

5、物理层：

物理层一般为负责数据传输的硬件，比如我们了解的双绞线电缆、无线、光纤等。比特流光电等信号发送接收数据。

B6. 请简述 OSPF的防环措施 ?(10 分）

答：**1**）**SFP** 算法无环 （**2**）更新信息中携始发者信息，并且为一手信息 （**3**）多区域时要求非骨干区域，必须连接骨干区域，才能互通路由，防止了始发者信息的丧失，避免了环路。

B7. 请简述 OSPF 邻接形成过程 ?（10 分）

答： 互发 **HELLO** 包，形成双向通信

根据接口网络类型选 **DR/BDR**

发第一个 **DBD**，选主从

进行 **DBD** 同步

交互 **LSR**、**LSU**、**LSack** 进行 **LSA** 同步

同步结束后进入 **FULL**

B10. OSPF 虚链路在什么情况下用到 ?为什么要用虚链路 ?（10 分）

答： 在实际企业网络中，由于各种原因会存在主干区域不连续或者某一个区域与主干区域不相连的情况。在这两种情况下网络管理人员只能通过设置虚拟链路 **virtual-link** 来解决 **.**

B12：简述 STP 的作用及工作原理？（ 10 分）

STP（**Spanning Tree Protocol**）是生成树协议的英文缩写。该协议可应用于在网络中建立树形拓扑，消除网络中的环路，并且可以通过一定的方法实现路径冗余，但不是一定可以实现路径冗余。生成树协议适合所有厂商的网络设备， 在配置上和体现功能强度上有所差别， 但是在原理和应用效果是一致的。

生成树协议最主要的应用是为了避免局域网中的单点故障、网络回环，解决成环以太网网络的“ 广播风暴 ”问题，从某种意义上说是一种网络保护技术， 可以消除由于失误或者意外带来的循环连接。 **STP** 也提供了为网络提供备份连接的可能，可与 **SDH** 保护配合构成以太环网的双重保护。新型以太单板支持符合 **IEEE 802.1d** 标准的生成树协议 **STP** 及 **IEEE 802.1w** 规定的快速生成树协议 **RSTP**，收敛速度可达到 **1s**。

但是，由于协议机制本身的局限， **STP** 保护速度慢（即使是 **1s** 的收敛速度也无法满足电信级的要求） ，如果在城域网内部运用 **STP** 技术，用户网络的动荡会引起运营商网络的动荡。目前在 **MSTP** 组成环网中，由于 **SDH** 保护倒换时间比 **STP** 协议收敛时间快的多，系统采用依然是 **SDH MS-SPRING** 或 **SNCP**，一般倒换时间在 **50ms** 以内。但测试时部分以太网业务的倒换时间为 **0** 或小于几个毫秒，原因是内部具有较大缓存。 **SDH** 保护倒换动作对 **MAC** 层是不可见的。这两个层次的保护可以协调工作，设置一定的“拖延时间”（ **hold-off**），一般不会出现多次倒换问题。

B14：简述有类与无类路由选择协议的区别

IP 路由协议可以被分为两大类，一类是有类的，另一类是无类的。

1、有类的路由不会识别子网的信息 **,**如宣告 **10.0.1.0/24 172.16.1.0/22 192.168.1.64/28** 路由表中只会识别 **A** 类 **10.0.0.0/8,B** 类 **172.16.0.0/16 C** 类 **192.168.1.0/24**；

2、无类的路由协议不会根据 **A B C** 类来识别 **,**根据子网掩码的长度来区分网段 **,**所以说无类的路由协议都可以不支持路由自动汇总；

3、有类的路由协议只会传送网络前缀（网络地址），但是不会包含子网掩码。当它传送更新时，它首先检查直接连接的网络是否和发送更新的网络属于同一个大一点的子网， 如果是的， 那么它会继续检查它们的子网掩码是否相等，如果不等，那么更新信息会被丢弃而不会被广播；

4、无类路由协议传输网络前缀（网络地址）的同时也会传输子网掩码，所以它支持 **VLSM** 。

从管理距离上看，无类的路由协议一般在子网中使用，所以距离较小。

中等难度题目

10、三层交换和路由器的不同

答：虽说三层交换机和路由器都可以工作在三层， 但本质上还是有所区别。

一 在设计的功能上不同

现在有很多的多功能路由器，又能实现三层的路由功能，包括 NAT 地址转换。有提供了二层的端口，有的还配置了无线功能。再有就是还具备防火墙的功能。 但是你不能它单独的划分为交换机或者是防火

墙吧。只能说是个多功能的路由器。　防火墙二层交换只是他的附加功能。三层交换也一样，主要功能还是解决局域网内数据频繁的通信，三层功能也有，但不见得和路由器差很多。

二　应用的环境不同

三层交换的路由功能比较简单，　因为更多的把他应用到局域网内部的通信上，主要功能还是数据的交换

路由器的主要功能就是选路寻址，　更适合于不同网络之间，　比如局域网和广域网之间，或者是不同的协议之间。

三　实现方式不同

路由器能够实现三层的路由（或转发）　　是基于软件的实现方式，当收到一个数据包要转发的时候，　要经过查看路由表，　最长匹配原则等一系列复杂的过程最终实现数据包的转发，相比三层交换效率略低。

而三层交换是基于硬件的方式实现三层的功能，　　他成功转发一个数据包后，就会记录相应的　IP 和 MAC 的对应关系，当数据再次转发是根据之前的记录的表项直接转发。　这个过程成为“一次路由，多次交换”。

总之，三层交换和路由器的最大区别是路由器可以基于端口做　　NAT，而三层交换机不能。　路由器直接接入光纤可以直接上网，　而三层交换机不能。主要是三层交换机的每一个接口都有专有的　　MAC 地址和特定的 ASIC 集成电路。

11、无端口木马与反弹端口木马有什么不同　？

答：反弹木马：由木马服务端主动连接客户端，　因此在互联网上可以访问到局域网里通过　NAT 代理 (透明代理) 上网的电脑，并且可以穿过防火墙　(包括：包过滤型及代理型防火墙　)。 防火墙对于连入的连接往往会进行非常严格的过滤，但是对于连出的连接却疏于防范。　于是，与一般的木马相反，　反弹端口型木马的服务端 (被控制端) 主动连接客户端　(控制端)，为了隐蔽起见，客户端的监听端口一般开在　80(提供 HTTP 服务的端口)，这样，即使用户使用端口扫描软件检查自己的端口，发现的也是类似　TCP UserIP:1026 ControllerIP:80 ESTABLISHED　的情况，稍微疏忽一点，你就会以为是自己在浏览网页　　(防火墙也会这么认为的　)。

无端口木马：

将 DLL 木马，注入到其它　EXE 文件中，使其成为木马的合法载体。（一般黑客会选择　Explorer.exe 、Svchost.exe 等系统关键性服务程序，这样用户就很难终止木马的运行）。而所谓的无端口，　实际上是重复利用了机器已经打开的端口　（如 80、135，　139 等常用端口）来传送数据，这样就避免了开新端口，也能骗过防火墙。并且这样的端口复用是在保证端口默认服务正常工作的条件下进行复用，这是它区别于端口劫持的地方。

12、 MPLS VPN配置流程。

答：　1.配置 PE-P-PE之间的 IGP 以保证它们的联通性，配置　IGP 的目的 C 仅仅是为了保证在建立　iBGP 时邻居的可达性

2.启用 PE-P-PE相连接口的　LDP 以及 MPLS 功能（需要注意的是　MPLS功能需要 CEF的支持，默认已经开启）

```
PE(config)#int s0/0
PE(config-if)#mpls ip
PE(config-if)#mpls mtu 1508          # 更改接口 MTU 值。需要在 PE 与 P 互联的所
```

有接口上配置。

3.在 PE上定义并配置 VRF参数

PE(config)#ip vrf vrf_name

用于标示用户 VPN实例，每个 vrf_name 必须保证唯一。在理解 vrf 时我们 可以把它看做每个 vrf 是由一台虚拟的路由器来单独维护一张 vrf 路由表。注意区分 vrf_name 的大小写。

PE(config-vrf)#rd ASN:nn/IP-address:nn

用来区分不同 VRF中相同地址段，也就是解决地址空间 CCIE培训重叠的问题。通常建议配置基于 VRF的 RD，而不是基于 VPN的 RD。

PE(config-vrf)#router-target [both/export/import] [ASN:nn/IP-address:nn]

它是 BGP的一个扩展团体属性，格式同 RD。用来表示该 VRF路由表接收和发送路由的意愿（ import 表示接收意愿； export 表示发送意愿。如果某个 VRF同时存在两条 CCIE培训以上 import 或 export 则它们之间是“或”的关系。

4.将 VRF与相应的接口进行关联（ PE与 CE相连接的接口）

PE(config)#int s0/0

PE(config-if)#ip vrf forwarding vrf_name

PE(config-if)#ip add x.x.x.x y.y.y.y # 接口和 VRF关联后会删除这个接口的 IP地址，需要重新配置接口的 IP 地址

5.配置 PE到 PE的 iBGP连接（MP-BGP）

……

6.配置 PE与 CE间的 vrf 路由（注意这里与传统路由的区别）

……

B4. MPLS L3 VPN，如果我想让两个不同的 VPN作单向互访，怎样做 ?（10 分）

B8. IBGP 为什么采用全互联 ?不采用全互联怎么部署 ?（10 分）

B9. 路由反射器的反射原则 ?（10 分）

B11. 说说 BGP路由协议与 IGP 路由协议的区别 ?（10 分）

答：一台路由器只能创建一个 **BGP** 实力，而 **IGP** 则叫灵活。比如 **OSPF**，有多少个活动的接口，即可创建多少个实例。

协议设计重点的区别：

与 **OSPF**、**RIP** 等 **IGP** 不同，其着眼点不在于发现和计算路由，而在于控制路由的传播和选择最好的路由。

AS 号的区别

在 **BGP** 中，**AS** 号用于标识路由器属于那个组织，决定两个对等体建立邻居关系是 **IBGP** 还是 **EBGP**。在 **IGP** 中，比如 **OSPF**，只是一个进程标识，本地有意义；**EIGRP** 中 **AS** 的作用也用于标识路由器属于哪个 **AS**，属于不同 **AS** 的路由器不能建立邻居关系。

转发表的区别：

BGP 没有给出每个 **AS** 域内的拓扑结构，因此 **BGP** 只能看到 **AS** 树，而 **IGP** 只能看到 **AS** 域内拓扑结构。

与 **OSPF**，**RIP** 等 **IGP** 协议相比，**BGP** 的拓扑图要更抽象和粗略一些。因为 **IGP** 协议构造的是 **AS** 内部的路由器的拓扑图。

IGP 把路由器抽象成若干端点，把路由器之间的链路抽象成边，根据链路的状态等参数和一定的度量标准，每条边配以一定的权值，生成拓扑图。根据此拓扑图选择代价（两点间经过的边的权值和）最小的路由。这里有一个假设，即路由器（端点）转发数据包是没有代价的。而在 **BGP** 中，拓扑图的端点是一个 **AS** 区域，边是 **AS** 之间的链路。此时，数据包经过一个端点（**AS** 自治区域）时的代价就不能假设为 **0** 了，此代价要由 **IGP** 来负责计算。

这体现了 **BGP** 和 **IGP** 是分层的关系。即 **IGP** 负责在 **AS** 内部选择花费最小的路由，**BGP** 负责选择 **AS** 间花费最小的路由。

B13 ：有一台交换机上的所有用户都获取不了 IP 地址 ,但手工配置后这台交换机上的同一 vlan 间的用户之间能够相互 ping 通,但 ping 不通外网 ,请说出排障思路 .

B15： OSPF 协议中， DR 一定是网段中优先级最高的路由器 ?并说明判断根据。

B16：客户某 H3C 路由器上（ AR28 系列，版本： VRP3.4）存在如下配置：

```
interface serial 1/0
  undo shutdown
  ip address 10.1.1.10 255.255.255.252

  interface Ethernet 0/0
```

undo shutdown

ip address 20.1.1.10 255.255.255.252

interface Ethernet 0/1

undo shutdown

ip address 30.1.1.10 255.255.255.252

#

ip route-static 10.19.32.0 255.255.255.0 10.1.1.9 preference 60

ip route-static 20.19.32.0 255.255.255.0 Ethernet 0/0 preference 60

ip route-static 10.1.0.0 255.255.0.0 30.1.1.9 preference 60

#

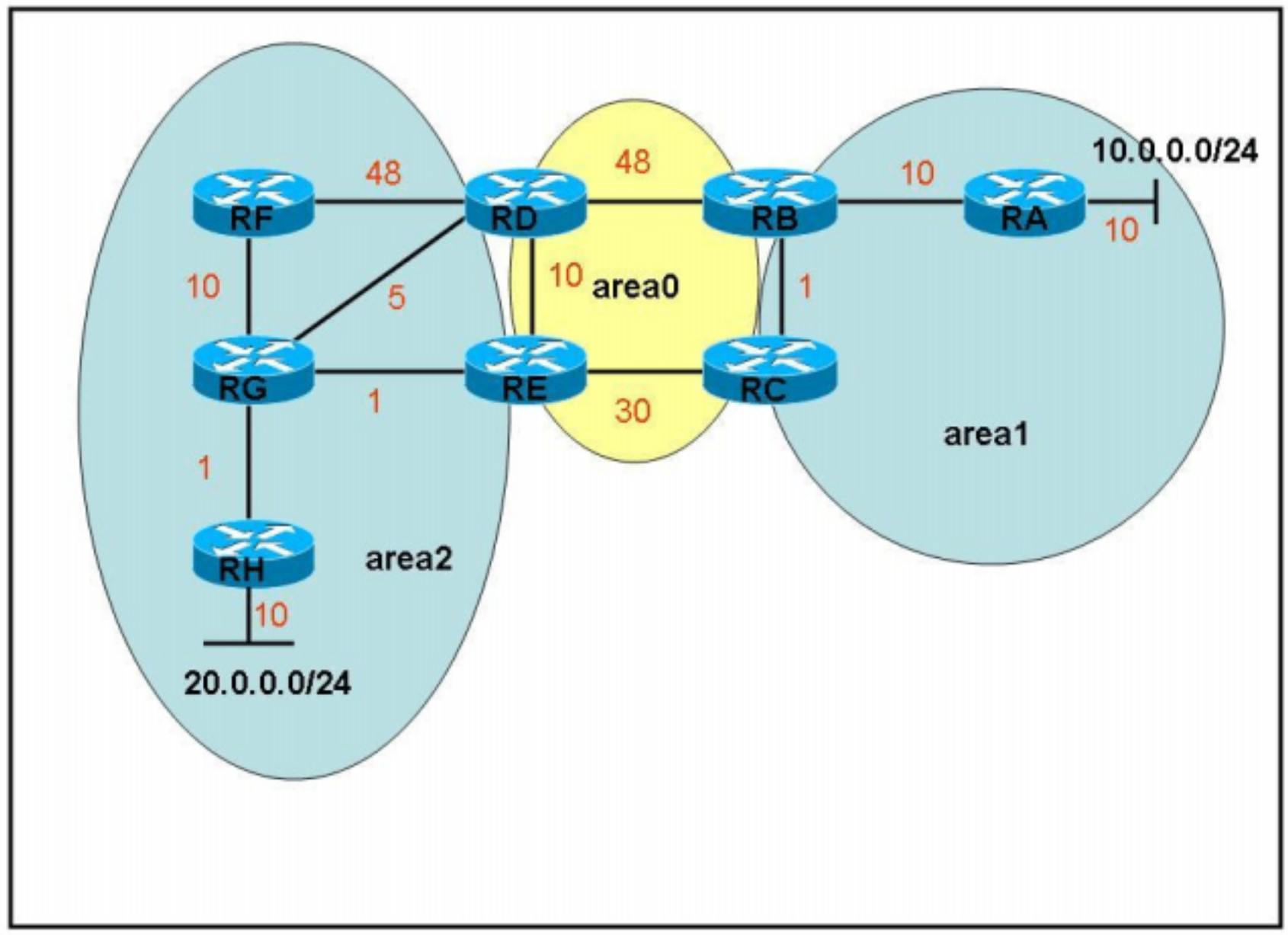
请问：

a) 当网络正常时（题中的 3 个接口都是 UP 的），执行命令 display ip route ，上述三条静态路由在路由表中是否都生效？

b) 当网络正常时（题中的 3 个接口都是 UP 的），上述三条静态路由中，有一条无法完成正常转发，请指出，并改正。

c) 客户发现当接口 serial 1/0 down 掉后，发现第一条静态路由在路由表中仍旧是生效的，为什么？应该如何改正？

B17：某机关网络拓扑如下图所示，所有路由器运行 Ospf 路由协议，区域分为 Area0、Area1、Area2 共三个区域，红色字体为各个路由器相连链路的 Cost 值。请问当网络 10.0.0.0/24 访问网络 20.0.0.0/24 的时候路径是如何选择的？并解释原因。


RF
RD
RB
RA
RG
RE
RC
RH
48
48
10
10
10
10
5
1
1
1
30
10
area0
area1
area2
10.0.0.0/24
20.0.0.0/24