1.3章节思考题：管理员要经常在路由器上使用命

问题：管理员要经常在路由器上使用命令“display ip interface brief”查看接口状态，但该命令完整输入则较长，思考如何使用最简化且准确的方式输入这条命令？

解答：使用命令[Huawei]hotkey ctrl\_u " display ip interface brief "设置，以后按Ctrl加U键就等于输入了display ip interface brief

1.4章节思考题：Telnet是基于TCP协议还是UDP协议的

问题：Telnet是基于TCP协议还是UDP协议的应用？为什么？Telnet应用安全吗？为什么？

解答：Telnet是基于TCP协议的应用，默认使用的是TCP的23号端口，由于Telnet是用于internet的远程登录，要求用来承载的传输层是可靠的，面向连接的协议类型，而TCP协议是传输层的可靠的，面向连接的协议类型，UDP协议是面向无连接，尽最大努力交付的协议类型。Telnet是一种明文传送协议，数据在传输过程中没有使用任何加密技术，所以Telnet应用是不安全的。

1.5章节思考题：开启SSH客户端首次认证功能有什

问题：开启SSH客户端首次认证功能有什么缺陷？如果不开启此功能如何成功在客户端远程登录？

解答：开启SSH客户端首次认证功能时，不对SSH服务器的RSA公钥进行有效性检查。当客户端主机需要与服务器建立连接时，第三方攻击者冒充真正的服务器，与客户端进行数据交互，窃取客户端主机的安全信息，并利用这些信息去登录真正的服务器，获取服务器资源，或对服务器进行攻击。

如果不开启，可用拷贝粘贴方式将服务器上RSA公钥配置到客户端保存。

rsa peer-public-key 13.1.1.1

public-key-code begin

3047

0240

C31DBF37 400783C1 E2BB3075 8927DFB6 AAB9B2CE F0039875 F6450CDE A42AA5A8

E51AED28 122CF103 69AF53E1 3701183F 0F704B14 8EF19C0F 7A2272D0 01AB9CD7

0203

010001

public-key-code end

peer-public-key end

ssh client 13.1.1.1 assign rsa-key 13.1.1.1

1.6章节思考题：缺省情况下，FTP服务器端监听端

问题：缺省情况下，FTP服务器端监听端口号是21，能否在路由器上变更此端口号，有什么好处？

解答：如果FTP服务未使能，用户可以变更FTP服务器监听端口号。如果变更端口号前FTP服务已经启动，则不能变更成功。需执行undo ftp server命令关闭FTP服务，再进行端口号变更。但如果使用标准的监听端口号，可能会有攻击者不断访问此端口，导致带宽和服务器性能的下降，造成其他正常用户无法访问。所以可以重新配置FTP服务器的监听端口号，攻击者不知道FTP监听端口号的更改，有效防止了攻击者对FTP服务器的攻击。

2.1章节思考题：在实际操作中，通常使用自动协

问题：在实际操作中，通常使用自动协商模式还是手动配置模式？为什么？

解答：在实际操作中，通常使用手动配置模式。因为自动协商的结果可能和实际要求不符。

2.2章节思考题：在ARP代理开启的情况下，如果在

问题：在ARP代理开启的情况下，如果在PC-2上，ping 10.1.2.4（10.1.2.4主机不存在），icmp echo报文是在PC-2还是R1路由器丢掉的？为什么？

解答：R1的接口GE 0/0/1开启了ARP 代理后，收到PC-2的ARP广播请求报文后，R1根据ARP请求中的目标IP地址 10.1.2.3查看自身的路由表中是否有对应的目标网络，R1的GE 0/0/2接口就是10.1.2.0/24网络，所以，R1直接把自身的GE 0/0/1接口的MAC地址通过ARP响应返回给PC-2，PC-2接收到此ARP响应后使用该MAC作为目标硬件地址发送报文给R1。

R1的接口GE 0/0/1开启了ARP 代理后，收到PC-2的ARP广播请求报文后，R1根据ARP请求中的目标IP地址 10.1.2.3查看自身的路由表中是否有对应的目标网络，R1的GE 0/0/2接口就是10.1.2.0/24网络，所以，R1直接把自身的GE 0/0/1接口的MAC地址通过ARP响应返回给PC-2，PC-2接收到此ARP响应后使用该MAC作为目标硬件地址发送报文给R1。

R1收到后，检测自己的ARP缓存表，发现没有10.1.2.4的映射条目。R1通过接口G0/0/2发送针对IP地址10.1.2.4的ARP广播请求。10.1.2.4主机不存在，所以R1不会收到ARP的应答报文，icmp echo报文封装失败，只能丢弃。

3.1章节思考题：在本实验中，如果将S2的接口E

问题：在本实验中，如果将S2的接口E 0/0/5配置为Access类型接口，并划入VLAN 30中，此时PC-1能否ping通PC-4？PC-1能否ping通PC-5？为什么？，

解答：S1通过接口E0/0/5连接SW2。E0/0/5接口在S1上属于vlan1，和PC-1连接的端口E0/0/1不在同一个VLAN，所以PC-1不会和S2连接的主机进行通信。PC-1不能ping通PC-4，也不能ping通PC-5。

3.2章节思考题：连接PC机的交换机接口也可以配置

问题：连接PC机的交换机接口也可以配置成Trunk接口吗？为什么？

解答：可以。当连接PC的交换机接口配置成TRUNK时，PC机发送的数据帧都不打VLAN标签。当交换机Trunk端口从PC机收到数据帧时，该帧不包含802.1Q的VLAN标签，将打上该Trunk端口的PVID。当交换机Trunk端口向PC机发送数据帧时，检测所发送数据的VLAN ID与端口的PVID，如果相同，则剥离VLAN标签后转发。

3.3章节思考题：在本实验中，如果将PC-5所连交换

问题：在本实验中，如果将PC-5所连交换机的接口E 0/0/4下的port hybrid pvid 30命令删除，PC-4所连的端口E 0/0/3下port hybrid pvid 10命令删除，其它端口配置则保持不变。此时在PC-5与PC-4间的连通性是否正常？报文经过S1和S2间端口时使用的VLAN Tag是哪个？为什么？

解答：PC-5与PC-4间的连通性正常。在交换机hybrid接口下删除port hybrid pvid vlan命令后，接口的PVID变为缺省vlan1。所以，PC-5与PC-4互访的报文经过S1和S2间端口时使用的VLAN Tag是vlan 1。

3.4章节思考题：VLAN间的通信可以利用单臂路由的

问题：VLAN间的通信可以利用单臂路由的方式实现，那么利用单臂路由实现数据转发会存在哪些潜在问题？该如何解决？

解答：利用单臂路由实现数据转发会存在两个问题：

1. 路由器和交换机是通过一条链路连接，容易成为网络单点故障，导致VLAN之间的通信就会中断；

2. 各个VLAN之间的通信都是由“单臂”链路承载，“单臂”链路可能会成为流量传输的瓶颈； 利用三层交换机实现VLAN间路由可以解决“单臂路由”存在的问题。

3.5章节思科题：试问三层交换机与路由器实现三

问题：试问三层交换机与路由器实现三层功能的方式是否相同？为什么？

解答：不相同。 因为三层交换机上面的物理接口都是2层接口。需要在三层交换机上配置VLANIF接口。VLANIF接口是基于网络层的接口，可以配置IP地址。借助于VLANIF接口，三层交换机就能实现路由转发功能。

4.1章节思考题：在什么场景下，选举根端口，指

问题：在什么场景下，选举根端口，指定端口时会比较到端口ID？

解答：当进行生成树BPDU比较时，根桥ID、开销值、发送者桥ID前三个参数依次比较没有办法分出优劣，这时就需要比较发送者的端口ID。

4.2章节思考题：交换机端口在发生状态转换时，

问题：交换机端口在发生状态转换时，都有哪些状态会经历一个Forward Delay？

解答：正常端口在发生状态转换时会在Listening、Learning两个状态时经历一个转发延迟。有特殊端口例如Portfast端口则会跳过此两个状态直接进入转发。

4.3章节思考题：S4交换机的E 0/0/2接口down之后，

问题：S4交换机的E 0/0/2接口down之后，E 0/0/3会成为新的根端口，如果此时S3交换机的指定端口E 0/0/3也down掉，S4交换机上会发生端口角色或状态的改变吗？如果边缘端口收到BPDU，此端口还是边缘端口吗？

解答：当S3交换机的E0/0/3也down掉后，E0/0/4端口则会变为指定端口进入转发。所以对于S4来说没有产生影响，端口状态不会发生改变。边缘端口的作用是为了加速转发过程，所以当边缘端口收到BPDU后则会认为此端口已经不再是连接PC的端口进而改变自己的边缘特性变成普通交换机端口进行生成树选举来防止环路产生。

4.4章节思考题：当MSTP和RSTP混合使用的时候，如何

问题：当MSTP和RSTP混合使用的时候，如何选举根桥？

解答：MSTP协议可以把支持MSTP的交换机和不支持MSTP交换机划分成不同的区域，分别称作MST域和SST域。在MST域内部运行多实例化的生成树，在MST域的边缘运行RSTP兼容的内部生成树IST（Internal Spanning Tree）。对于RSTP来说可以将MSTP域内的设备看成一台RSTP设备来进行正常的根桥选举。

5.1章节思考题：GVRP能够应用在Hybrid类型的接口上

问题：GVRP能够应用在Hybrid类型的接口上吗？

解答：在配置GVRP时应该遵循此条原则：只能配置在Dot1Q链路上且两端都需要启用GVRP。

5.2章节思考题：Smart Link和Monitor Link的联合使用可

问题：Smart Link和Monitor Link的联合使用可以确保链路出现故障后及时的切换，如果所有链路都正常，是否所有数据都只能通过主链路转发？

解答：在同一个环网中，可能同时存在多个VLAN的数据流量，Smart Link可以实现流量的负载分担，即不同VLAN的流量沿不同Smart Link组所确定的路径进行转发。 通过把一个端口配置为多个Smart Link组的成员端口（每个Smart Link组的保护VLAN不同），且该端口在不同组中的转发状态不同，这样就能实现不同VLAN的数据流量的转发路径不同，从而达到负载分担的目的。所以可以通过设置使流量进行负载即不止一条链路转发数据。

5.3章节思考题：当接口数超出最大负载阈值时，

问题：当接口数超出最大负载阈值时，剩余接口是否转发流量？

解答：Eth-Trunk接口数超出时，多于接口会处于不转发流量的Unselect状态。

6.1章节思考题：在静态路由配置当中，可以采取

问题：在静态路由配置当中，可以采取指定下一跳IP地址的方式，也可以采取指定出接口的方式，这两种方式存在着什么区别？

解答：路由查找上的区别：指定下一跳的话，要多进行一次路由的递归查找，拿下一跳去进行递归，得到出接口。

2层地址解析时候的区别：指定下一跳的话使用最后一次递归的下一跳地址去解析下一跳2层地址。如果是指定出接口的路由，数据包匹配到后直接用目标地址去解析下一跳地址。

6.2章节思考题：在本实验的步骤3和4中，如果不在

问题：在本实验的步骤3和4中，如果不在R3上做和R1同样的对称配置，会产生什么样的现象？为什么？

完成负载均衡的配置之后，可以在R1上的S1/0/0和S1/0/1两个接口上启用抓包工具，且在主机PC-1上ping主机PC-2，观察R1的两个接口上的现象，为什么会产生这样的现象？

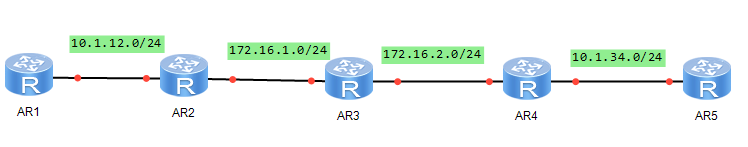
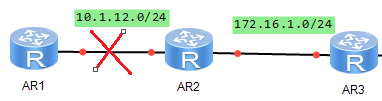
解答：R3上如果不配的话回程数据就不会负载均衡了。会看到数据走一路，因为思科设备默认基于流负载均衡，同样的数据只走一路，开启基于包负载均衡就可以看到效果。

7.2章节思考题：在本实验中，R1和R2上配置了认证

问题：在本实验中，R1和R2上配置了认证，R3没有配置认证，根据分析，R1和R2不会再接收R3发送的不包含认证信息的RIP更新，那R3是否会接收R1和R2发送过来的带有认证信息的RIP更新呢？为什么？

解答：也不会收，因为数据包里认证字段跟自己不匹配，所以路由器不收。单向的路由通常都是没有实际意义的而且(绝大多数应用都需要双向通信）。

7.3章节思考题：华为设备默认开启了RIPv2的自动汇

问题：华为设备默认开启了RIPv2的自动汇总，如果没有默认开启接口下的水平分割，即自动汇总生效的情况下，可能会导致出现环路以及不连续子网等问题。请设计一个相关场景，模拟在RIPv2开启了自动汇总且关闭了水平分割的情况下，导致路由环路或不连续子网问题的出现。  
  
解答：  
  
这样一个拓扑环境下，首先自动汇总开启的时候，R2和R4是主类网络边界，这样在R3上会看到从2个方向来的10.0.0.0/8的路由，这时候对于R3来说2条路由会进行基于流的负载均衡。这样从R3通过的数据是无法正常转发到各自的网段的，所以无法支持不连续的子网。  
如果图中设备R2和R3互联接口都关闭了水平分割：  
  
这时候R1和R2之间down掉，这样R2会失去10.1.12.0/24的路由。由于关闭了水平分割，会将从R2收来的路由10.0.0.0/8还给R2，R2还会将路由还给R3，这样直到最终达到16跳，在次时间之内R2和R3都会将去往10.开头的网段的数据包扔给对方，这就造成了环路。

7.4章节思考题：在此实验中，如果在R1上配置一条

问题：在此实验中，如果在R1上配置一条去往192.168.20.0网段的静态路由，再把RIP优先级修改为60，那么在R1的IP路由表中该网段路由来自RIP还是静态路由？为什么？

解答：R1会把静态路由加入IP路由表中，因为若同一条路由条目来自两个不同协议，且协议优先级一样，路由器会根据协议内部优先级来选择最优路由，内部优先级也就是协议优先级的初始值。

7.6章节思考题：在使用RIPv1的环境中，R2、R3和R

问题：在使用RIPv1的环境中，R2、R3和R4都配置了第二个IP地址，10.0.0.0/8的子网已经连续，如果R2是主网边界，为什么R3还能看到10.0.12.0/24的子网？如果R2不是主网边界，为什么在R3的路由表里能看到10.0.0.0/8的汇总路由？

解答：是主类网络边界，所以有10.0.0.0/8的路由，按接口主地址来。之所以能看到10.0.12.0/24是因为，rip1优先按收到路由的接口下网络号掩码来猜掩码，因为接口地址跟路由再同一个主类网络下，自动以接口下24位掩码作为收到路由的掩码，正好一样。

7.7章节思考题：水平分割可以防止环路，那为什

问题：水平分割可以防止环路，那为什么RIP协议还需要其它防环机制？水平分割的局限性在哪？

解答：因为，物理拓扑上的环路导致的路由环路，水平分割是防范不了的，这种环路，路由进出不是同一个接口。

7.8章节思考题：无论是配置metricin还是metricout都会

问题：无论是配置metricin还是metricout都会将所有RIP路由条目的度量值增加，如何在完成对财务部路由附加度量值配置的同时不影响其他RIP路由的Metric值？

解答：可以在这2个命令后面跟访问列表，来匹配路由，实现只给财务部路由附加度量值的需求。

7.9章节思考题：如果采用debug或者抓包的方式排错

问题：如果采用debug或者抓包的方式排错，与采用查看命令进行排错相比有什么优劣？

解答：debug信息相对命令行比较全，可以动态的看到数据包收发，以及协议或者feature的工作过程和方式，但是在业务繁忙的设备上可能过于消耗资源，甚至有可能导致设备瘫痪。抓包的话可以看到设备的工作方式以及所有具体的数据，是一种非常好的排错手段，但是很多现网环境不允许，导致无法抓包，而且抓包排错，对网络工程师技术要求比较高。查看命令行是最简单的排错方法，但是有很多不是由于命令导致的问题无法通过命令行找到。

7.10章节思考题：使用network命令方式通告路由，与

问题：使用network命令方式通告路由，与路由引入的方式通告路由有什么区别？

解答：network的作用不是通告路由，network匹配的是一个地址范围，落在范围的接口启用这个协议，而具体网络号掩码是协议自己根据接口参数找的。network范围包含的接口就会收发协议数据包。路由引入完全就是向路由协议注入路由的手段，不会影响任何接口工作方式。

8.1思考题：请列举链路状态协议与距离矢量路由

问题：请列举链路状态协议与距离矢量路由协议的相同点与不同点。

解答：

1. 有的距离矢量协议周期更新，链路状态协议使用触发更新

2. 距离矢量不知道整个拓扑，链路状态路由协议设备知道整个拓扑。

3. 距离矢量协议通常收敛较慢，链路状态路由协议通常收敛快（不是绝对）。

4. 距离矢量协议通常容易导致环路（但有防环手段各种），链路状态算法本身防环，不需要太担心（也不是绝对）。

5. 距离矢量路由协议通常配置简单，链路状态路由协议相对复杂些。

6. 距离矢量路由协议消耗系统资源小，链路状态路由协议消耗系统资源多。

7. 距离矢量路由协议需要更多带宽来传路由，链路状态相对需要更少一些。

8. 距离矢量路由协议是基于谣言的传播，也就是根据邻居的计算结果再进一步计算（有累加成分），链路状态路由协议自己知道整个拓扑，本地计算到达全网最优路径。

8.2章节思考题：在本实验中，如果现在公司总部

问题：在本实验中，如果现在公司总部配置的区域不是骨干区域0，而是其他非骨干区域，会有什么现象？

解答：这样做了之后会导致公司各个区域之间互相不能通信，因为跨区域路由只能由区域0的边界ABR进行类型3汇总得到。

8.3章节思考题：OSPF认证如果采用MD5验证模式，有

问题：OSPF认证如果采用MD5验证模式，有没办法可以获取到其密钥内容？

解答：没有办法，因为采用MD5验证方式后，OSPF传递的是一个128位的密文的摘要。这样比明文传送口令更加安全。

8.4章节思考题：在本实验中，通过配置被动接口

问题：在本实验中，通过配置被动接口可以禁止OSPF收发Hello报文，是否还有其他办法也能实现？

解答：接口网络类型改成NBMA也不会主动发送hello包，另外只能通过安全设备进行数据包过滤实现了。

8.5章节思考题：试问如果不同区域中的OSPF路由器

问题：试问如果不同区域中的OSPF路由器的Router-ID重叠又会导致什么问题的产生？

解答：首先，如果路由器ID重叠的设备在相邻区域，会导致相关ABR无法进行路由计算，因为在路由计算时，某些需要挂在这设备上的链路状态会因为ABR无法区分这2个节点。另外如果重叠的设备处于特殊位置，比如本身就是ABR，ASBR那也很容易导致类似的问题。理论上说，如果路由器ID重叠的设备如果不在相连的区域，可能可以没有问题。

8.6章节思考题：在本实验步骤二中，基础的OSPF网

8.6章节思考题

问题：在本实验步骤二中，基础的OSPF网络配置完毕后，为什么要同时重启下四台路由器上的OSPF进程？

解答：因为DR和BDR选举原则的不抢占，如果不是同时重启，可能会影响正常的选举结果，可能是优先级或者路由器id低的设备当选DR或BDR。

8.7章节思考题：OSPF的Dead计时器时长默认为什么要

问题：OSPF的Dead计时器时长默认为什么要保持是Hello计时器的4倍？一定要保持4倍关系吗？

解答：防止用户Hello时间调太大，邻居翻动，所以会自动保持，但是并不是说一定要4倍，邻居之间一样就可以。数值上通常要比Hello大，而且要留好余量，一般都会用2到3倍以上（因为网络可能会有延迟）。

8.8章节思考题：关于在路由引入时手工修改路由

问题：关于在路由引入时手工修改路由的Cost值，这么做还有其它的用处吗？

解答：在多点双向注入时还可以用来防止环路（通过cost值指定非常高，比内部所有路由的开销都高）。在引入RIP协议时，还可以通过设置16来作为一种路由过滤的手段。

8.9章节思考题：在本实验的步骤四中，OSPF中发布

问题：在本实验的步骤四中，OSPF中发布默认路由时使用到了命令default-route advertise always，如果末尾不加always参数，会出现什么情况？如何解决？

解答：如果不加，默认路由会无法发布。因为always参数代表如果本地路由表中没有默认路由的时候，OSPF也发布一条默认路由。解法方法是在本地手工配置一条静态默认路由。

9.1章节思考题：如果主路由器出现故障，比如断

问题：如果主路由器出现故障，比如断电停机了，备份路由器是通过什么机制检测到的？

解答：通过hello包来检测，自己根据优先级算出来的抢占时间内收不到master的hello包，就会抢占master。

9.2章节思考题：在步骤四中，如果将R2配置成为虚

问题：在步骤四中，如果将R2配置成为虚拟组2的虚拟IP拥有者，试问此时R2能否抢占成为Master？

解答：可以的会立刻成为master，只要是虚拟IP的拥有者一定会变master

9.3章节思考题：在本实验中，可以通过配置监视

问题：在本实验中，可以通过配置监视上行接口来提高VRRP的可靠性，但是监视上行接口仍然等同于监视直连链路，如果非直连链路出现故障，VRRP协议能否感知？

解答：是不能感知的，但是可以通过NQA来监控到目标连通性，并且使用vrrp去监视NQA的状态进行切换来实现。

10.2章节思考题：在本实验的OSPF网络中，如果AC

问题：

解答：不能，因为ACL只能过滤路由条目或数据包，而OSPF在区域内是传递的链路状态信息，链路状态信息无法过滤。

10.3章节思考题：如果将前缀列表中已配置好的语

问题：如果将前缀列表中已配置好的语句顺序打乱会对实验结果产生影响吗？

解答： 会的，前缀列表3个条目匹配范围有冲突，范围小的必须放上面也就是序列号要小，不然会被范围大的行为覆盖导致不生效。

11.1章节思考题：假设在某一直连链路上，一端接

问题：假设在某一直连链路上，一端接口的链路层协议为PPP，另一端为HDLC，此时能否正常通信？

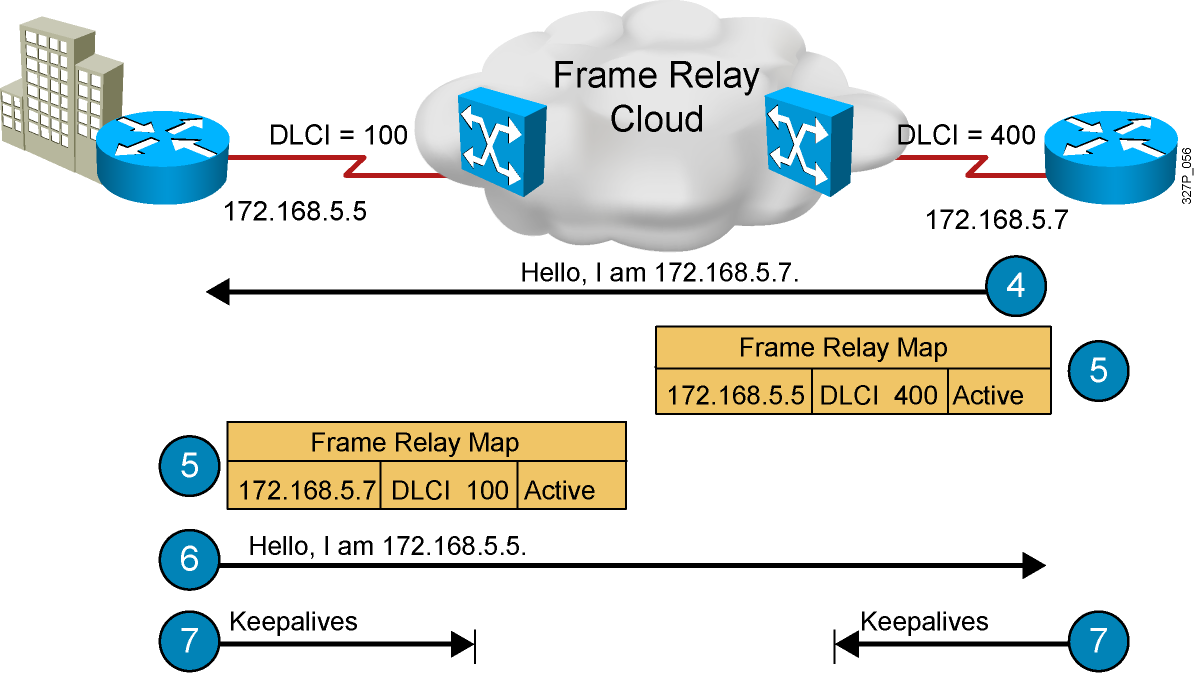
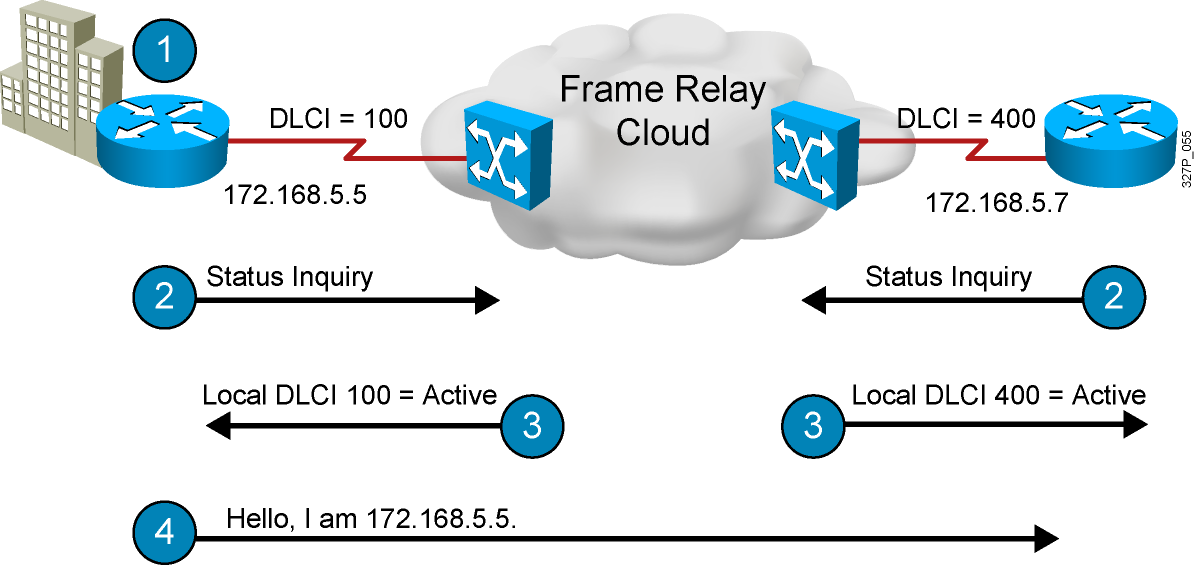
解答：不能。数据链路层封装不通，在设备接口收到数据帧时，由于对帧的封装协议不同，设备会丢掉数据报文。

11.2章节思考题:当PPP链路Up后，在PPP链路一端加上

问题：当PPP链路Up后，在PPP链路一端加上认证配置而另一端不加，为什么一定要重启端口后认证才能生效使双方不能正常通信？

解答：PPP认证的协商在发生在PPP会话建立阶段，当PPP会话成功建立后PPP链路将一直保持通信，不再更改协商的参数直至关闭这条链路的连接。只有关闭连接后重新建立会话时才重新协商参数，认证方式的更改才能生效。

11.3章节思考题：帧中继中动态映射的过程是怎么

问题：帧中继中动态映射的过程是怎么样的？它和ARP机制的区别在哪里？解答：第一问解答：帧中继动态映射是采用inverse ARP来实现的。 用于帧中继网络中IP地址和虚电路号的映射关系的动态维护。IARP用于在帧中继网络中自动建立路由器IP地址与帧中继DLCL的映射关系。如图：  
A首先发送单播消息请求其对应目的硬件地址的IP地址是多少，同时在该广播消息中还附带自己的IP地址。  
B接受到该广播包后，修改该请求数据包，从帧中继帧头中提取硬件地址放入请求包的源硬件地址域中，即可形成A的地址映射。然后形成单播响应，响应包中包含B的IP地址以及A的IP地址和硬件地址。  
A收到响应，修改响应数据包，从帧头中取出硬件地址放入响应数据包的源硬件地址域中，然后将其添加到地址映射表中。之后设备A和B就可以正常进行数据传送了。

第二问解答：与ARP的区别：  
[ARP](http://baike.baidu.com/view/32698.htm)用于已知本端IP地址和硬件地址以及对端IP地址的情况下，求解对端的MAC地址，其工作原理简示如下：  
A首先发送广播消息请求其对应目的IP地址的硬件地址是多少？同时在该广播消息中还附带自己的IP地址和硬件地址。  
B接受到该广播包后，取出A的IP地址和硬件地址，将其添加到地址映射表中。同时返回单播响应，响应包中包含B的IP地址和硬件地址。  
A收到响应，取出B的IP地址和硬件地址，将其添加到地址映射表中。  
之后设备A和B就可以正常进行数据传送了。  
Inverse ARP用于帧中继网络中IP地址和虚电路号的映射关系的动态维护。其工作原理简示如下：  
A首先发送单播消息请求其对应目的硬件地址的IP地址是多少，同时在该广播消息中还附带自己的IP地址。  
B接受到该广播包后，修改该请求数据包，从帧中继帧头中提取硬件地址放入请求包的源硬件地址域中，即可形成A的地址映射。然后形成单播响应，响应包中包含B的IP地址以及A的IP地址和硬件地址。  
A收到响应，修改响应数据包，从帧头中取出硬件地址放入响应数据包的源硬件地址域中，然后将其添加到地址映射表中。之后设备A和B就可以正常进行数据传送了

11.4章节思考题：在上文中将R1的DR优先级设置成了

问题：在上文中将R1的DR优先级设置成了100，为什么要这么做？

解答：将R1的OSPF链路优先级设置为100，保证R1在s1/0/0链路上称为DR。因为OSPF在链路上默认的优先级为1，DR选举中，优先级越大越优，R1称为DR。

12.1章节思考题： DHCP Server 从地址池分配IP的顺序

问题： DHCP Server 从地址池分配IP的顺序如何，是按顺序还是随机的？DHCP Server如何防范地址冲突的问题？

解答：DHCP服务器按照顺序的分配地址，可以通过IP + MAC地址的绑定来分配可将特定的IP分配给某台电脑防止地址冲突。

12.2章节思考题：请问DHCP服务器在分配地址的时候

问题：请问DHCP服务器在分配地址的时候是从该网段中最小的地址进行分配还是最大的地址进行分配，这样有什么好处？

解答：DHCP服务器按照顺序依次从大向小分配地址，尽量避免了静态地址与DHCP自动分配地址配置的重复。

12.3章节思考题：在R1充当DHCP中继代理时，客户的

问题：在R1充当DHCP中继代理时，客户的DHCP请求包经DHCP中继R1到达DHCP服务器R3后，如果R3上定义有不同网段的多个IP地址池，R3是如何知道该从哪个地址池分配地址给PC-1和PC-2 ？

解答：根据中继代理连接客户PC端的接口，DHCP服务器选择与其接口相同网段的地址池来进行分配。

13.1章节思考题：如果路由器的某一接口下配置了

问题：如果路由器的某一接口下配置了多个IPv6地址，互相之间是否会产生影响？

解答：不会产生影响

13.2章节思考题：RIPng支持认证吗？为什么？

问题：RIPng支持认证吗？为什么？

解答：RIPng自身不提供认证功能，而是通过使用IPv6提供的安全机制来保证自身报文的合法性。

13.3章节思考题：在本实验中，OSPFv3协议修改了全

问题：在本实验中，OSPFv3协议修改了全球单播地址，邻居关系未受影响，请问各网络间的通信是否正常？从此处能够得到什么启示？

解答：可以正常通信，OSPFv3协议基于链路运行，与具体的IPv6地址、前缀分离开，即使同一链路上的不同节点具有不同网段的IPv6地址时，协议也可以正常运行。

14.3章节思考题：GRE是一种三层的隧道协议，可以

问题：GRE是一种三层的隧道协议，可以形成逻辑的点到点直连隧道，支持组播数据的传输，但是它的安全性能较差，不能实现隧道中所传输数据的加密，那GRE应采用何种方式实现组播数据跨互联网的加密传输？

解答：虽然GRE协议安全性能不高，但是它能支持组播和非ip协议的传输，而IPSec VPN技术能够实现加密和数据完整性校验，但不支持组播和非IP协议。所以，实际项目部署中，大多是将GRE技术和IPSec VPN技术结合使用，称为”GRE over IPSec”。

14.4章节思考题：什么情况下需要使用到NAT的双向

问题：什么情况下需要使用到NAT的双向转换？

解答：当两个私有网络的IP地址相同（发生重叠），并又想能够实现互相访问是，就可以通过中间的设备部署双向的nat转换了