

Eudemon防火墙的工作模式包括： （请选择3个答案）

1. 路由模式
2. 透明模式
3. 交换模式
4. 混合模式

Answer: A B D

1. 判断：Eudemon防火墙双机热备功能中会话表不是实时备份的。
2. True
3. False

Answer: B

解析：传统的VRRP机制主用防火墙生产的会话表不会备份到备用防火墙上，但双机热备份技术主防火墙会定时向从防火墙发送状态信息和需要备份的信息。

1. Eudemon防火墙中，下列哪些数据流定义为outbound方向？（请选择2个答案）
2. 数据流从Trust域到DMZ域
3. 数据流从Untrust域到DMZ域
4. 数据流从Local域到Trust域
5. 数据流从Untrust域到Local域

Answer: A C

解析： Trust---->Untrust：outbound；Trust---->DMZ：outbound；Trust---->Vzone：outbound；反之则为intbound；

Untrust---->DMZ：inbound；Untrust---->Vzone：outbound；DMZ---->Vzone：outbound。

1. 判断：防火墙的安全策略下发到接口上，而不是下发到区域间。
2. True
3. False

Answer: B

1. 对于支持多实例的Eudemon防火墙，系统默认存在几个区域？
2. 5 个
3. 4 个
4. 3 个
5. 2 个

Answer: A

解析：默认存在5个区域：Vzone、Untrust、Trust、DMZ、Local。

1. 对于Eudemon防火墙，Trust区域的优先级为
2. 10
3. 50
4. 75
5. 85

Answer: D

解析：默认5个区域的优先级为：Vzone——0、Untrust——5、DMZ——50、Trust——85，Local——100。

1. 判断：用户不可以根据需要更改防火墙系统默认的几个区域的优先级。
2. True
3. False

Answer:A

1. 判断：多通道协议是指某个应用在进行通讯或提供服务时需要建立两个或两个以上的会话（通道），其中有一个控制通道，其他的都为数据通道。
2. True
3. False

Answer: A

1. 防火墙技术从发展历史来看，可以分为以下几种类型？ （请选择3个答案）
2. 简单包过滤防火墙
3. 代理防火墙
4. 防DDos防火墙
5. 应用状态检测防火墙

Answer: A B D

1. 在各种防火墙的技术中，目前主流的防火墙采用的是
2. 应用状态检测
3. 简单包过滤
4. 路由访火墙
5. 防病毒

Answer: A

1. 判断：Eudemon防火墙工作在透明模式的特点是防火墙的接口配置IP地址，启用动态路由协议，像路由器一样工作。
2. True
3. False

Answer: B

解析： 路由模式——防火墙像一台路由器，在防火墙接口上需要配置IP地址，维护相关的路由信息；

透明模式——防火墙像交换机等二层设备一样布置在网络中，无需配IP地址，不改变网络逻辑拓扑。

混合模式——路由模式+透明模式，有些端口工作在三层（路由模式），有些端口工作在二层（交换模式）。

1. 判断：防火墙的工作模式包括：路由模式，透明模式和混合模式，系统默认是路由模式。
2. True
3. False

Answer: A

1. 判断：Eudemon防火墙工作在混合模式：就是接口上不配置IP地址，工作在二层，对过往数据进行检测处理。
2. True
3. False

Answer: B

解析： 路由模式——防火墙像一台路由器，在防火墙接口上需要配置IP地址，维护相关的路由信息；

透明模式——防火墙像交换机等二层设备一样布置在网络中，无需配IP地址，不改变网络逻辑拓扑。

混合模式——路由模式+透明模式，有些端口工作在三层（路由模式），有些端口工作在二层（交换模式）。

1. 判断：Eudemon防火墙工作在混合模式即存工作在路由模式的接口，又存工作在透明模式的接口，如果使用防火墙双机备份功能时，可以采用混合模式。
2. True
3. False

Answer: A

1. 判断：Eudemon只支持主备模式（Active-Standby）。
2. True
3. False

Answer：B

解析：主要支持两种组网方式：主备组网方式、负载分担组网方式、混合组网方式。

1. 判断：Eudemon防火墙支持两种方式的负载分担，逐包负载分担就和逐流负载分担。
2. True
3. False

Answer: A

1. 在Eudemon防火墙上，毎个虚拟防火墙包含多少缺省安全域？
2. 3
3. 4
4. 5
5. 6

Answer: C

1. 判断：Eudemon防火墙上，不同虚拟防火墙实例可以配置不同的安全策略。
2. True
3. False

Answer: A

1. 判断：Eudemon防火墙上，不同虚拟防火墙之间，默认情况下即使不指定安全策略也是允许相互访问的。
2. True
3. False

Answer: B

1. 下面QoS中Integrated Service与RSVP的说法，不正确的是？ （请选择2个答案）
2. Integrated Service其实也就是RSVP
3. Integrated Service采用RSVP作为它的信令机制
4. RSVP是一个多用途的协议，除了Integrated Service之外，RSVP还可用于其他领域
5. Integrated Service适合于在骨干网上大量应用

Answer: A D

解析：在IntServ服务模型中，负责传送QoS请求的信令是RSVP。

1. 判断：Eudemon防火墙黑名单老化的时间是可以设置的。
2. True
3. False

Answer: A

1. 判断：Eudemon防火墙生成黑名单条件为——防火墙配置地址扫描攻击防范功能或端口扫描攻击防范；防火墙开启黑名单功能；网络中存在攻击行为。
2. True
3. False

Answer: A

1. 判断：防火墙透明模式的优点是会改变现有网络的拓扑结构。
2. True
3. False

Answer: B

解析：透明模式最大的优点是无需修改任何已有的配置。

1. 判断：Smurf攻击采用UDP报文，Fraggle攻击采用ICMP报文。
2. True
3. False

Answer: B

解析： Smurf攻击方法是发ICMP应答请求，该请求包的目标地址设置为受害网络的广播地址。

Fraggle使用UDF应答消息而非ICMP。

1. 判断：IPv4的IP头中的flag字段中紧急指针一般在传输OOB数据时使用。
2. True
3. False

Answer: A

解析：此题答案应该是True，引自：<http://dwz.cn/3nUklf>。

1. TCP SYN Flood 网络攻击是利用TCP/IP栈只能允许有限个TCP连接来实施攻击的。TCP建立连接过程需要（ ）次握手。
2. 4
3. 3
4. 2
5. 1

Answer: B

1. 判断：Eudemon防火墙产品支持与IDS联动。
2. True
3. False

Answer: A

1. 判断：Eudemon防火墙产品支持实时流量统计分析、攻击报文统计。
2. True
3. False

Answer: A

1. 判断：华为Eudemon防火墙中除Local区域之外的其他区域都可以添加多个接口，每个接口也可以添加到多个区域中。
2. True
3. False

Answer: B

解析：接口只能加入到一个安全区域，该接口可以是物理接口，也可以是逻辑接口。

1. 判断：[Eudemon] firewall session aging-time icmp 15上述命令是说Eudemon防火墙建立了一条ICMP会话，如果15杪钟没有ICMP报文通过的话，该会话就会被老化掉。
2. True
3. False

Answer: A

1. 判断：ASPF是区别于OSPF的可以运行在华为Eudemon防火墙的一种链路状态路由协议。
2. True
3. False

Answer: B

解析：ASPF是一种改进的高级通信过滤技术。

1. 判断：华为Endemon防火墙在配置NAT时，最多支持255个地址池，每个地址池最多可配置255个公网地址。
2. True
3. False

Answer: B

解析：华为Endemon防火墙每个地址池最多可配置4096个公网地址。

1. 判断：华为Eudemon防火墙当同一域间存在多个nat outbound配置的时候，ACL组号越小的越先匹配。
2. True
3. False

Answer: B

1. 判断：防火墙系统对于小包的转发性能比对大包的转发性能要低。
2. True
3. False

Answer: A

解析：小包转发时对CPU/NE的开销更大，同样吞吐量下，小包的负荷比大包高，因此转发性能要低。

1. 判断：当外网用户访问已经使用NAT SERVER发布的内网服务器的公网地址时，华为Eudemon防火墙会将报文的目的地址转换为服务器的私网地址，但此时需要配置到该公网地址的路由。
2. True
3. False

Answer: A

1. 下面对华为Eudemon防火墙的支持的目的地址NAT描述不正确的是？
2. 通过防火墙目的地址NAT可以修改手机上网的WAP网关地址
3. 在使用目的NAT时，可以不定义精确的需要转换的数据流
4. 防火墙配置目的地址NAT时，只会进行报文的目的地址的转换
5. 防火墙配置目的地址NAT时，会进行报文的目的地址和源地址的转换

Answer: D

1. 华为Eudemon防火墙的支持的双向NAT描述不正确的是？
2. 通过防火墙双向NAT既要对源地址进行转换，又要对目的地址进行转换
3. 域内NAT和NAT Server一起使用其实是双向NAT的一个特殊应用场景
4. NAT Inbound和NAT Server一起使用主要用于简化配置NAT Server时的路由配置
5. 在处理双向NAT时，防火墙是先做NAT转换，然后再进行包过滤的检测

Answer: D

1. 判断：配置了No-PAT功能的NAT主要用于一对多的IP地址转换，转换时同时转换IP地址和端口。
2. True
3. False

Answer: B

解析：NAT——1对1的地址翻译；PAT——多个内网地址翻译到1个外网IP地址；NPAT——多个内网地址翻译到N个IP地址。

1. 判断：TCP-illeage-session攻击是用来对服务器发起TCP空连接请求，耗尽服务器的连接资源。
2. True
3. False

Answer: A

1. QoS针对各种不同的需求，提供不同的服务质量，以下属于QoS所提供的功能的有？ （请选择3个答案）
2. 支持为用户提供专用带宽
3. 可以减少报文的丢失率
4. 避免和管理网络拥塞
5. 可以设置报文的源地址

Answer: A B C

1. 网络中常见的攻击类型的描述不正确的是？
2. 网络攻击可分为拒绝服务型攻击、扫描窥探攻击和畸形报文攻击三大类
3. 拒绝服务攻击和其他类型的攻击不同之处在于：攻击者并不是去寻找进入内部网络的入口，而是阻止合法用户访问资源或路由器
4. 扫描窥探就能大致了解目标系统提供的服务一种类和潜在的安全漏洞
5. 畸形报文攻击是通过向目标系统发送有缺陷的IP报文，使得目标系统在处理这样的IP包时会出观崩溃
6. Ping of Death、Tear drop等是典型的拒绝服务型的攻击。

Answer: E

解析：Ping of Death和Tear drop属于畸形报文攻击。

1. DDOS和DoS都属于网络中常见的攻击类型，对此描述不正确的是？
2. SYN Flood、Fraggle都属于DoS攻击
3. DDoS（Distributed Denial of Service）攻击是一种DoS攻击，这种攻击是使用攻击者控制的几十台或几百台计算机攻击一台主机，使系统无法接受正常用户的请求，或者挂起不能正常的工作。
4. DoS ( Distributed Denial of Service )攻击是一种DDoS攻击，这种攻击是使用攻击者控制的几十台或几百台计算机攻击一台主机，使系统无法接受正常用户的请求，或者挂起不能正常的工作。
5. Smurf攻击是属于DoS攻击的一种。

Answer: C

1. 判断：Eudemon防火墙双机热备份时因为单点故障有导致网络中断的风险，为了防止一台设备出现意外故障而导致网络业务中断，采用两台防火墙形成的双机备份。
2. True
3. False

Answer: A

1. 判断：Eudemon防火墙会划分多个区域，为防火墙上多个区域提供双机备份功能时，需要在每一台防火墙上配置多个VRRP备份组。
2. True
3. False

Answer: A

1. Eudemon防火墙支持的最大的安全区域数目（不包含保留区域）是
2. 16
3. 14
4. 12
5. 11

Answer: D

解析：系统最多支持16个安全区域，包括5个保留区域在内。

1. 判断：Eudemon防火墙支持多台设备之间运行VRRP协议，但是只支持两台设备之间运行HRP协议。
2. True
3. False

Answer: A

解析：HRP用于在主用设备和备用设备之间备份关键配置命令和会话状态等关键信息。

1. 判断：Eudemon对要发送的VRRP报文不进行任何认证处理，收到VRRP报文的Eudemon也不进行任何认证，认为收到的都是真实的、合法的VRRP报文。
2. True
3. False

Answer: A

解析：在一个安全的网络中，可以将认证方式设置为NO，路由器对要发送的VRRP报文不进行任何认证处理，而收到VRRP报文的路由器也不进行任何认证就认为是一个真实合法的VRRP报文，这种情况下，不需要设置认证字。

1. Eudemon防火墙中配置双机热备份的时候需要哪些协议支持： （请选择3个答案）
2. VRRP
3. RRPP
4. HRP
5. VGMP

Answer: A C D

解析：双机热备份技术依靠三种协议实现：VRRP/VGMP/HRP。

1. 判断：对于防火墙，报文的入接口和出接口属于同一区域时，会触发防火墙的安全规则。
2. True
3. False

Answer: B

1. 判断：使用备份中心后可以为防火墙上的任意接口提供备份接口，而且防火墙上的任一接口也可以作为其他接口（或逻辑连路）的备份接口。
2. True
3. False

Answer: B

1. 判断：地址转换所作的工作不仅仅是转换IP地址。
2. True
3. False

Answer: A

1. 判断：IP UNNUMBER是一项借用地址的技术，如果被借用接口有多个IP地址，只能借用主IP地址。
2. True
3. False

Answer: A

解析：IP UNNUMBER技术必须满足以下条件——

* 被借用方接口的地址本身不能为借用地址。
* 被借用方的地址可以借给多个接口。
* 如果被借用接口有多个ip地址，则只能借用主ip 地址。
* 如果被借用接口没有IP地址，则借用接口的IP地址为0.0.0.0。
* loopback 的地址可被其它接口借用，但本身不能借用其它接口的地址。
* 借给"它们地址的局域网接口必须满足2者之一：
* 相同主网不同子网，但掩码必须相同。
* 不同主网缺省掩码（即未被划分的主网

1. 防火墙的性能参数指标不包括： （请选择2个答案）
2. 内存大小
3. 最大连接数
4. 毎秒新建连接数
5. CPU处理能为

Answer: A D

解析：防火墙的四项性能指标——吞吐量、时延、新建连接速率、并发连接数。

1. 基于IP层的高级访问控制列表可以从以下哪些方面进行包过滤？ （请选择4个答案）
2. 源IP地址及其子网掩码
3. 目的IP地址及其子网掩码
4. 上层协议信息
5. 源目的的端口号
6. 数据包的长度
7. 源MAC地址

Answer: A B C D

解析：高级ACL根据数据包的源和目的IP地址及端口，IP承载的协议类型、协议特性等信息进行过滤。

1. 下面有关NAT叙述正确的是 （请选择3个答案）
2. NAT是英文“网络地址翻译“的缩写
3. 地址翻译又称地址转换，用来实现私有地址与公用网络地址之间的转换
4. 当内部网络的主机访问外部网络的时候，可能需要NAT
5. 地址转换不能缓解IP地址紧张的问题

Answer: A B C

1. Eudemon防火墙支持下面哪些NAT功能？ （请选择3个答案）
2. NAT多实例
3. NAT ALG
4. 域内NAT
5. NAT client

Answer: A B C

1. 判断：Eudemon防火墙NAT多实例功能会在设备上给不同的实例统一地维护NAT表，可以承担不同实例的地址转换服务。
2. True
3. False

Answer: B

解析：Eudemon防火墙NAT多实例功能会在设备上给不同的实例独立地维护NAT表，可以承担不同实例的地址转换服务。

1. 判断：Eudemon防火墙IPsec功能不支持NAT穿越。
2. True
3. False

Answer: B

解析：支持GRE、L2TP、VLAN等多种VPN方式组网；支持IPSec VPN、支持DES、AES、AES加密；支持IPSec穿越NAT。

1. 判断：Eudemon防火墙开启NAT的情况下，对系统性能影响大。
2. True
3. False

Answer: B

1. 假设对标记为AF21的报文设置的WRED丢弃策略为：下限设为35，上限设为40，丢弃概率是50%。那么，当AF21的报文到达时，WRED拥塞避免机制对该报文的处理结果描述错误的是 （请选择3个答案）
2. 如果当前队列的平均长度小于35，报文开始丢弃
3. 如果当前队列的平均长度大于下眼35，小于上限40，则该报文被丢弃的概率为50%
4. 如果当前队列的平均长度大于上限40，则该报文入队列
5. 如果当前队列的平均长度大于上限40，则该报文被丢弃

Answer: A B C

解析：当队列的长度大于高阀值时，丢弃所有的报文。

1. 判断：防火墙的黑名单仅对IP地址进行匹配，并且支持动态的刪除或添加。
2. True
3. False

Answer: A

解析：黑名单的特点：根据报文的源IP地址进行过滤，简单高效，可动态添加删除。

1. 判断：Land攻击的特点是数据包的源地址和目的地址相同，都是被攻击对象的IP地址或者是环回地址。各种受害者对Land攻击反应不同，许多UNIX主机将崩溃，NT主机会变得极其缓慢。
2. True
3. False

Answer: A

解析：Land攻击是把TCP SYN包的源目地址设为相同，将会向自己发送SYN-ACK消息。

1. 判断：IDS与防火墙联动，IDS与防火墙无需直接相连。
2. True
3. False

Answer: A

1. 判断：防火墙用于域间通信的报文安全过滤，对于防火墙不同端口之间，但属于一个域内的报文通信，防火墙也进行过滤。
2. True
3. False

Answer: B

解析：防火墙安全策略是基于域间的，不同的区域之间可以设置不同的安全策略，且本区域（相同区域）不同接口间的报文不过滤直接转发。

1. 在Eudemon防火墙上，关于IP和Mac地址绑定支持的防范描述错误的是 （请选择2个答案）
2. IP地址欺骗
3. Mac地址欺骗
4. Dos攻击
5. DDos攻击

Answer: C D

解析：IP和MAC绑定，可以防止仿冒IP地址攻击，ARP Flood攻击，DHCP Flood攻击等。

1. Eudemon防火墙支持的攻击防范有 （请选择3个答案）
2. SYN-Flood
3. 防止内部攻击
4. UDP/ICMP Flood攻击
5. Ping-Death

Answer: A C D

1. 现网业务出现故障时，现场在恢复业务前，需要采集的信息中最重要的防火墙信息是：
2. 攻击告警信息
3. 日志信息
4. 诊断信息
5. 网管信息

Answer: C

1. 防护ARP攻击的有效解决方案有 （请选择2个答案）
2. 同一个MAC地址可以同多个不同的IP地址进行关联
3. 交换设备（华为）开启ARP防护开关（识别ARP欺骗行为）
4. 进行网段隔离（在交换机上划分VLAN）
5. 启用IP包过滤

Answer: B C

1. 判断：Eudemon防火墙自身的端口映射功能和NAT的功能类似，都是为了修改数据包的端口信息。
2. True
3. False

Answer: B

解析：防火墙的端口映射并非要更改数据包的端口信息，而是解决端口和服务类型映射关系的一个功能。

1. Eudemon防火墙能够输出日志信息包括以下哪几种： （请选择4个答案）
2. 攻击防范日志
3. 黑名单日志
4. 地址绑定日志
5. NAT/ASPF日志
6. IDS日志

Answer: A B C D

解析：防火墙日志包括：NAT/ASPF日志、攻击防范日志、流量统计、黑名单、地址绑定。

1. 下面哪个不属于华为Eudemon防火墙的局限性的描述？（同72题重复）
2. 防火墙不能根据网络被恶意使用和攻击的情况动态调整自己的策略
3. 防火墙一般不提供对内部的保护
4. 防火墙无法防范数据驱动型的攻击
5. 防火墙不能防止Winnuke攻击

Answer: D

解析：winnuke攻击特征是攻击目标端口，被攻击的目标端口通常是139/138/113/53等。防火墙可以通过检测这些端口可以防范此类攻击。

1. 下面哪个不属于华为Eudemon防火墙的局限性的描述？（同71题重复）
2. 防火墙不能根据网络被恶意使用和攻击的情况动态调整自己的策略
3. 防火墙一般不提供对内部的保护
4. 防火墙无法防范数据驱动型的攻击
5. 防火墙不能防止Winnuke攻击

Answer: D

解析：winnuke攻击特征是攻击目标端口，被攻击的目标端口通常是139/138/113/53等。防火墙可以通过检测这些端口可以防范此类攻击。

1. [Eudemon-slb] vserver huawei vip 202.2.2.2 group group1对此命令的描述不正确的是：
2. 是在配置防火墙的负载均衡功能
3. 虚服务器的名字是huawei，IP地址是202.2.2.2
4. 虚服务器对应了 一个服务器组，组名为group1
5. group1可以稍后创建

Answer: D

1. 判断：华为的Eudemon防火墙支持把一个公有IP地址转换成无限个私有地址，突破了65535的端口限制。
2. True
3. False

Answer: A

1. 判断：Eudemon防火墙双机热备，可以工作在路由模式和混合模式两种模式下。
2. True
3. False

Answer: A

解析：防火墙双机热备份，可以工作在路由模式——防火墙业务端口和HRP备份通道接口均工作在路由模式；

混合模式——防火墙业务端口工作在透明模式下，而HRP备份通道接口工作在路由模式下。

1. 判断：配置TCP代理之后可以检测特定目的地址SYN报文的接收速率和TCP半开连接数，用来防止SYN-Flood的攻击。
2. True
3. False

Answer: A

解析：对于SYN-Flood攻击，可以采用TCP代理技术或者采用新建连接的限制或总连接数的限制来防范。

1. 判断：ip-spoofing攻击是为了获得访问权，入侵者生成一个带有伪造源地址的报文，在实际使用中ip spoofing攻击的用途不大，没有必要打开防范功能。
2. True
3. False

Answer: A

解析：当报文存在多出口路径的时候或者存在默认路由的时候，ip spoofing攻击防范效果很差，实际使用中ip spoofing攻击用途不大，没有必要打开。

1. Eudemon防火墙中关于Tear drop攻击的描述正确的是： （请选择4个答案）
2. Teardrop攻击是利用数据包分片进行的
3. Teardrop攻击是把分片偏移字段设置成错误的值进行攻击的
4. 某些系统中的TCP/IP在收到含有重叠偏移的伪造分段时将崩溃
5. Teardrop攻击应该属于畸形报文攻击
6. Teardrop攻击应该属于拒绝服务攻击

Answer: A B C D

解析：TCP Flag、IP分片攻击、Tear Drop、Ping of Death都属于畸形报文攻击。

1. 防火墙在配置双机热备时会关贮备状态的切换和状态信息的备份，对此描述不正确的是：（原题错误）
2. VGMP将同一台防火墙上的多个VRRP备份组都加入到一个VRRP管理组
3. VGMP通过统一控制各VRRP备份组状态的切换，来保证管理组内的所有VRRP备份组状态都是一致的
4. VGMP可以保证报文来回路径通过同一台防火墙，当主防火墙出现故障时，所有流量都将切换到备防火墙
5. HRBP用于在主用设备和备用设备之间备份关键配置命令和会话表状态关键信息

Answer: D

解析：HRP用于主用设备和备用设备之间备份关键配置命令和会话表状态关键信息。

1. 假设有四条流a、b、c、d分别为50M，端口总带宽为100M，发生了流量拥塞，进行拥塞管理，其中，流量a属于PQ队列调度；流量b、c、d属于WFQ队列调度，权重比为1:2:2，则下面对四种流量的调度结果描述错误的是： （请选择2个答案）
2. 流量a通过100M
3. 流量a通过50M
4. 流量b通过10M，流量c、d分别通过20M
5. 流量b通过25M，流量c、d分别通过12.5M

Answer: A D

解析：a采用PQ列队，流量为50M，剩余100-50=50M给b、c、d三个，根据权重，分别为10,20,20。

1. 判断：Eudemon的双机热备在和NAT一起实现时，主备设备需要使用相同的NAT地址池，此状态下不支持基于接口的NAT server
2. True
3. False

Answer: A

1. 判断：Eudemon防火墙双机热备采用VRRP协议用于在主用设备和备用设备之间备份关键命令和会话表状态等关键信息。
2. True
3. False

Answer: B

解析： HRP协议主要用于主用设备和备用设备之间备份关键配置命令和会话表状态信息。

1. 判断：如果将防火墙的接口加入到某个区域，则该接口就属于该区域。
2. True
3. False

Answer: B

解析：接口添加进区域表达的意思是该接口所连接的网络属于该区域，但接口本身是属于Local区域的。

1. 关于Eudemon防火墙安全策略，以下说法不正确的是 （请选择2个答案）
2. Local 区域默认可以访问其它区域
3. Trust区域默认可以访问DMZ区域
4. Untrust区域默认不能访问Trust区域
5. 防火墙的区域默认都不能互访

Answer: A B

1. 关于Eudemon的区域优先级，以下说法正确的有 （请选择3个答案）
2. Local区域的优先级为100
3. Trust区域的优先级为85
4. Untrust区域的优先级为50
5. DMZ区域的优先级为50

Answer: A B D

解析：Untrust区域的优先级为5。

1. 判断：状态检测是一种高级通信过滤，它检查传输层协议信息并且监控基于连接的应用层协议状态，对于所有连接，每一个连接状态信息都将被ASPF维护并用于动态地决定数据包是否被允许通过防火墙或丢弃。
2. True
3. False

Answer: B

解析：ASPF不但对报文的网络层的信息进行检测，还能对丰富的应用层协议进行深度检测。

1. 关于防火墙技术，下面哪些选项是正确的描述？ （请选择3个答案）
2. 应用网关主要检测通过此网关的所有数据包中的应用层的数据价
3. 电路级网关主要检验数据包中所含的会话信息，只在会话层进行验证
4. 包过滤用于在两个不同安全级别的网络之间控制流入和流出网络的数据
5. Web代理支持内网用户通过Eudemon访问内网的web服务器资源，为用户提供基于HTTP方式的web应用服务

Answer: A B C

1. 防火墙性能指标主要体现在哪几个方面？ （请选择3个答案）
2. 小包/大包吞吐量
3. 每秒新建和并发连接数
4. 非对称加密性能
5. 处理延时

Answer: A B D

1. 在Eudemon防火墙上，下面描述Anti-DdoS主要使用的技术中，错误的有哪些？ （请选择2个答案）
2. TCP代理技术
3. 源认证及控制技术
4. 目标认证及控制技术
5. 指纹识别技术（特征检测技术）
6. 会话异常检测技术
7. 带宽限制技术

Answer: C F

解析：Anti-DdoS主要使用的技术包含：TCP代理技术、源认证及控测技术、标准协议栈识别技术、指纹识别技术(特征检测技术)、会话异常检测技术、流量控制技术。

1. 关于DDoS攻击的类型描述错误的是： （请选择2个答案）
2. 特殊报文攻击
3. 扫描类攻击
4. 物理层攻击
5. 传输层攻击

Answer: A B

解析：DDoS属于拒绝服务供给。

1. 以下哪些是DDoS攻击？ （请选择4个答案）
2. syn flood
3. syn/ack flood
4. udp flood
5. middle man attack
6. dns-flood

Answer: A B C E

1. 解析：middle man attack属于间接的入侵攻击。
2. Eudemon防火墙中ASPF的描述正确的是： （请选择2个答案）
3. ASPF支持对应用层协议进行深度检测
4. ASPF能够对MSN，QQ，ICQ等即时通讯软件发送的应用层信息检测
5. ASPF 识别完应用数据之后，直接生成会话表项，就可以依据表项转发报文了
6. 在使用NAPT功能时，Eudemon防火墙设备会为数据流建立Server-map表，表中只有转换后的IP的映射关系，不会存在转换前的内网IP

Answer: A B

解析：Server-map本质上是一个三元组表项，包含：源IP地址、源端口、协议号。

1. Eudemon防火墙中关于长连接的描述正确的是 （请选择3个答案）
2. 当—条会话在长时间没有被任何报文匹配，则该条会话所对应的连接可能己经关闭，会话也会被老化掉
3. 用户通过FTP下载大文件，需要间嗝很长时间才会在控制通道继续发送控制报文，此时就需要开启长连接功能
4. 在长连接功能中，可以通过ACL来指定流量，为这些特殊流量设定超长的老化时间
5. 目前Eudemon防火墙仅支持对TCP和UDP协议配置长连接

Answer: A B C

1. [Eudemon]nat server global 202.1.1.20 inside 192.168.1.10

[Eudemon]firewall zone trust

[Eudemon-zone-trust]nat outbound 3000 address-group 1

关于Eudemon防火墙上述配置中描述正确的是： （请选择3个答案）（同95题重复）

1. 内网服务器的私有IP地址为192.168.1.10
2. 内网客户端访问NAT SERVER的公网地址的时候，必须使用202.1.1.20
3. 内网客户端访问服务器时的数据包的源地址会被转换
4. 内网客户端访问服务器时的数据包的目的地址会被转换

Answer: A C D

1. [Eudemon]nat server global 202 1.1.20 inside 192 168.1.10

[Eudemon]firewall zone trust

[Eudemon-zone-trust]nat outbound 3000 address-group 1

关于Eudemon防火墙上述配置中描述正确的是： （请选择3个答案）（同94题重复）

1. 内网服务器的私有IP地址为192.168.1.10
2. 内网客户端访问NAT SERVER的公网地址的时候，必须使用202.1.1.20
3. 内网客户端访问服务器时的数据包的源地址会被转换
4. 内网客户端访问服务器时的数据包的目的地址会被转换

Answer: A C D

1. 华为Eudemon防火墙做了以下操作：

[sysname]display interzone trust untrust interzone trust untrust detect ftp#

说法不正确的是

1. 这是在查看防火墙域间配置信息
2. 域间配置了信任与非信任区域检测防止FTP报文攻击的功能
3. 防火墙配置了针对FTP协议数据包的ALG功能
4. 防火墙配置了针对FTP协议数据包的ASPF的功能

Answer: B

1. 对于TCP Flag攻击的描述错误的是：
2. 是利用TCP报文的6个标志位：URG、ACK、PSH、RST、SYN、FIN进行攻击
3. 6个标志全部为1，也就是圣诞树攻击
4. 6个标志全部为0，可以用来检测目的主机使用的操作系统
5. SYN和RST位同时为1的话不属于TCP Flag攻击

Answer: D

1. 判断：ICMP重定向报文攻击可能跨越网段向另外一个网络的主机发送虚假的重定向报文，以改变主机的路由表，干扰主机正常的IP报文发送。
2. True
3. False

Answer: A

1. 防火墙NAT应用场景中，业务存在分片报文，需要打开（ ）功能。
2. 分片透传
3. 分片缓存
4. 分片重组
5. 分片转发

Answer: B

1. 假设有双桶双速流量监管，C桶的令牌数量TC，P桶的令牌数量TP，当一个长度为B的报文进入时，下面对该报文处理描述正确的是 （请选择2个答案）

如果TP-B>0，且TC-B>0，报文被标记为green

如果TP-B>0，且TC-B<0，报文被标记为red

如果TP-B<0，且TC-B<0，报文被标记为red

如果TP-B>0，且TC-B<0，报文被标记为green

Answer: A C

1. 对于Eudemon防火墙上的会话表和Server-map表描述错误的是：
2. 会话表中记录的信息很多，一般是根据五元组来判断：一个报文是否和一条会话表项匹配
3. 来回路径不一致的组网通常是在网络中存在多个通信通道的情况下出现，此时防火墙收不到首包的问题就无法解决
4. 防火墙在转发FTP、RSTP等多通道协议的数据会生成Server-map表项
5. Server-map表是为了解决使用NAT或ASPF功能的情况下，可能存在外网用户通过随机端口主动访问内网服务器的情况

Answer: B

解析：如果在一次通信过程中，部分报文由一个设备转发，另外一部分报文由另一设备转发的情况，也有可能出现来回路径不一致。

1. 关于Eudemon防火墙包过滤与状态检测机制、会话表的关系描述正确的是： （请选择3个答案）
2. “状态检测”机制以流量为单位来对报文进行检测和转发
3. Eudemon防火墙缺省开启了状态检测机制
4. 开启状态检测机制后的包过滤机制可以总结为“对首包按照包过滤规则进行检查，如果检查通过，则建立会话表项，后续报文直接格局会话表进行转发”
5. 一个报文在没有响应的会话表项的情况下，只要通过包括包过滤在内的各种安全机制的检查，就可以生成会话表项，而不管其是否是首包

Answer: A B C

1. 在业务报文来回路径不一致组网下，防火墙需要关闭
2. 状态检测功能
3. 攻击防范功能
4. NAT功能
5. 状态备份功能

Answer: A

解析：当来回路径不一致的情况下，为了使业务能够正常通过，唯一的解决方法是关闭设备的状态检测机制。

1. 某条数据流出现故障，在防火墙上最直观查看和定位的方法是查看
2. 防火墙告警
3. 查看黑名单
4. 防火墙系统全局统计
5. 会话表

Answer: D

1. 使用Tracert定位问题时，如果Tracert报文经过防火墙，为了能够正常显示Tracert结果，需要在防火墙上关闭哪种攻击防范？
2. Land
3. icmp-unreachable
4. tracert
5. smurf

Answer: C

1. 负载分担组网中，两台Eudemon防火墙的业务口都需要配置
2. hrp track master
3. hrp track slave
4. hrp interface
5. hrp enable

Answer: A

1. Eudemon防火墙关于VGMP管理组抢占延时，缺省抢占时间是：
2. 120S
3. 60S
4. 30s
5. 1s

Answer: C

解析：缺省情况下，抢占功能已经配置了，抢占延时时间是30s。

1. 在Eudemon防火墙上查看会话的详细信息时，标识“hitted”的含义是什么？
2. 对于TCP类型会话来说，表示是否完成TCP三次握手，对于其他协议来说，表示正向访问是否有后续报文通过
3. 只对TCP类型的会话有意义，表示该TCP连接是否已经关闭，当正向访问发送了一个带FIN标识的报文，或者任意方向上发送了一个带FIN标识的报文，则会置上此标识
4. 应用于多通道协议，与ASPF功能相关，标识会话是否是由控制通道协商出来的子通道会话（即数据通道）
5. 应用于多通道协议，与ASPF功能相关，标识该会话是否是由数据通道协商出来的控制通道

Answer: A

解析：对于TCP类型会话来说，表示是否完成TCP三次握手；对于其它协议来说，表示正向访问是否有后续报文通过。

1. 在Eudemon防火墙上，查看防火墙会话老化时间的命令是
2. display firewall statistic system
3. display firewall session aging-time
4. display firewall session table verbose
5. display firewall session table detail

Answer: B

1. 判断：通常只使用平均修复时间MTTR (Mean Time to Repair)这一指标来评价产品或系统的可靠性。
2. True
3. False

Answer: B

解析：通常使用平均修复时间MTTR和MTBF这两个指标来衡量产品或系统的可靠性。

1. 判断：BFD只是一种通用的快速检测技术，自身可以实现快速倒换的功能，没有必要和其他快速例换技术一起才能起到作用。
2. True
3. False

Answer: B

解析：BFD只是一种通用的快速检测技术，自身并不能实现快速倒换的功能，因此要和其他快速倒换技术一起才能起到作用。

1. 判断：早期的BFD草案中定义了版本号0，当前VRP5.7版本支持的BFD版本号为1，与使用版本号0的BFD是完全兼容的。
2. True
3. False

Answer: B

1. 判断：BFD提供两种检测模式：异步模式和查询模式。
2. True
3. False

Answer: A

1. 判断：CV报文在LSP的源端LSR以每秒1个的速率产生，由LSP的宿端LSR接收。这一速率是可以调整的。
2. True
3. False

Answer: B

解析：CV报文在LSP的源端LSR以每秒一个的速率产生，由LSP的宿端LSR接收，且不可调整。

1. 判断：BFD发送的检测报文只有控制报文。
2. True
3. False

Answer: B

解析：BFD发送的检测报文是UDP报文，定义两种类型的报文:控制报文和回声报文(ECHO)。

1. 判断：BFD会话建立完成之后，用户也可以改变BFD的相关配置参数，例如最小发送间隔、最小接收间隔、检测模式等，不影响会话的当前状态。
2. True
3. False

Answer: A

1. 判断：自从2004年7月推出BFD标准的第一个草案起，一直到2005年7月，IETF开始BFD协议的讨论修订，从draft base-00发展到draft base-03，在这期间只经历了一次版本的变化，从版本0直接升级到版本2。
2. True
3. False

Answer: B

1. 判断：当本地BFD状态为“init”后，再接受到状态为“down”的报文不会自动切换回dwon。
2. True
3. False

Answer: B

1. 判断：VRRP的接口IP地址和虚拟IP地址可以相同。
2. True
3. False

Answer: A

解析：虚拟IP地址可以直接指定,也可以借用该VRRP组所包含的路由器上某接口地址。

1. 在设置WRED丢弃策略时，对标记为AF21的流量下限设为35，上限设为40；标记为AF22的流量下限设为30，上限设为40,；标记AF23的流量下限设为25，上限设为40，另外，在达到上限时的丢弃概率是10%，那么，在发生拥塞之前，哪个优先级的数据包优先得到保证？
2. AF21
3. AF22
4. AF23
5. 都一样

Answer: A

1. 判断：减少MTTR，都可以提高设备的可用性。
2. True
3. False

Answer: A

解析：MTTR：平均修复时间。

1. 判断：当虚拟路由器回应ARP请求时，使用主路由器的真实MAC地址。
2. True
3. False

Answer: B

解析：虚拟MAC地址——虚拟路由器根据虚拟路由器ID生成的MAC地址。 当虚拟路由器回应ARP请求时，使用虚拟MAC地址，而不是接口的真实MAC地址。

1. 判断：VRRP不能提供基于状态的备份功能。
2. True
3. False

Answer: A

解析：VRRP均为相对独立，且单独工作，无法保证同意防火墙上各接口的VRRP状态一致性。

1. 判断：VRRP协议的优点之一是当VRRP主路由器感知到故障后立即切换至VRRP备用路由器，保证业务短时间内恢复。
2. True
3. False

Answer: A

1. 判断：静态LACP通过LACPDU与对端交互信息。
2. True
3. False

Answer: A

解析：LACP协议通过LACPDU（Link Aggregation Control Protocol Data Unit，链路汇聚控制协议数据单元）与对端交互信息。

1. 判断：如果一个BGP Speaker在OPEN报文中有GR能力字段，但其中没有任何<AFI,SAFI>，说明这个BGP Speaker没有备份转发表，所以只能作为GR Restarter,
2. True
3. False

Answer: B

解析：此情况下，只能作为GR Helper 帮助邻居完成GR过程。

1. 判断：BGP GR的helper本身必须具备了GR能力，才能协助GR Restarter完成GR。
2. True
3. False

Answer: B

解析： a：教材指出GR helper为GR Restarter的邻居，至少能够识别GR信令就可以协助GR Restarter完成GR；

b：百度百科给出的解释为——能协助重启的GR Restarter保持路由关系的稳定，它也必须具备GR能力。

1. 判断：RPR （弹性分组数据环）是一种高效可靠的环网技术。
2. True
3. False

Answer: A

1. 判断：SDH/SONET（数字同步系列）是目前广泛应用在传输网络里面的一种环网技术，支持单环、多还，但是不具备高可靠性。
2. True
3. False

Answer: B

解析：SDH/SONET（数字同步系列）是目前广泛应用在传输网络里面的一种环网技术，支持单环、多还，具备高可靠性，故障自愈机制。

1. 判断：RPR环的数据操作包括：数据上环、数据过环、数据下环、数据剥离。
2. True
3. False

Answer: A

1. 判断：系统发生故障时进行主备倒换是提供系统可用性的一种重要方法，因为主备倒换不会导致数据丢失。
2. True
3. False

Answer: B

解析：主备倒换会导致数据丢失，大部分丢失的数据可通过HSB提供的数据平滑过程恢复。

1. 判断：MTTR（Mean Time to Repair）, 平均修复时间的计算公式为：MTTR=故障检测时间+单板更换时间+系统初始化时间+链路恢复时间+路由覆盖时间+转发恢复时间。上述各项的值越小，平均修复时间的MRRT也就越大，设备的可用性也就越高。
2. True
3. False

Answer: B

1. 判断：HSB（Hot Standby）是提供热备份的一个关键技术，它将系统的静态和动态配置信息备份。
2. True
3. False

Answer: A

解析：HSB的功能是将系统的静态和动态配置信息从AMB备份到SMB。

1. 判断：GR（Graceful Restart）可以实现所有协议重启时数据转发不中断的效果。
2. True
3. False

Answer: B

解析：目前具备GR能力的路由协议主要有IS-IS、OSPF、BGP。

1. 判断：快速检测技术用来尽可能快的检测与相邻设备间的通信故障，以便系统及时采取措施保证业务不中断。
2. True
3. False

Answer: A

解析：快速检测技术为改善网络性能，相邻系统之间快速检测通信故障，更快地建立起备用通道恢复通信。

1. 判断：BFD (双向转发检测）技术属于快速检测技术，但它较为复杂，需要特殊厂商设备支持。
2. True
3. False

Answer: B

解析：BFD（双向转发检测）是一套用来实现快速检测的国际标准协议，提供一种轻负荷、持续时间短的检测。可以在任何类型通道上进行故障检测。

1. 判断：FRR技术提供一套快速倒换机制，FRR结合BFD使用可以完成IP和MPLS网络的快速故障检测和倒换功能，将缺陷恢复时间缩小至50ms内。
2. True
3. False

Answer: A

1. 判断：MPLS OAM技术为MPLS网络提供了一套缺陷检测的工具及缺陷纠正机制，通过MPLS OAM及保护倒换构件可以定成CR-LSP转发平面的检测功能，并在缺陷发生后的50ms内完成保护例换，从而将缺陷所产生的影响减小到最低。
2. True
3. False

Answer: A

1. 判断：动态协议（如OSPF、BGP）GR的过程中并不需要保持邻居关系。
2. True
3. False

Answer: B

1. 假设出端口流量发生拥塞，报文A与报文B被缓存在各自的队列中，报文B属于PQ队列，报文A属于WFQ队列，那么，哪一种报文先被调度出去？
2. 报文A优先
3. 报文B优先
4. 同时出去
5. 都被丢弃

Answer: B

解析：PQ为绝对优先级队列调度，WFQ为加权公平队列调度。

1. 下向哪个不属于环网技术
2. Eth-Trunk
3. Token Ring
4. SDH/SONET
5. RPR

Answer: A

1. 下面哪个不是RPR环的技术特点
2. 物理层多样性
3. 关键节点带宽分配
4. 拓扑自动发现机制，支持即插即用
5. 流量等级保证QoS，支持带宽预留的业务

Answer: B

解析：RPR环技术特点——物理层多样性、带宽高利用率、快速保护机制、公平的节点带宽分配、拓扑自动发现机制，支持即插即用、有效支持组播和广播、流量等级保证QoS，支持带宽预留业务。

1. 判断：RRPP收敛性能比MSTP要快得多。
2. True
3. False

Answer: A

解析：RRPP是H3C独有的二层快速环网协议，相比STP收敛速度要快。

1. 下面哪个关于RPR环的槪念描述是错误的
2. 节点（Station）：RPR环网上的设备，它负责接收和转发数据。
3. 链路（Link）：连接相邻节点之间的一段传输通道，相邻节点之间由方向相反的两条链路连接。
4. 0环（ringlet0）：RPR双环中，数据帧发送方向为逆时计的称为0环，也称”外环”。
5. 1环（ringlet1）：RPR双环中，数据帧发送方向为逆时计的称为1环，也称”内环”。

Answer: C

解析：0环在RPR双环中，数据帧发送方向为顺时针的称为0环，也称“外环”。

1. 下面哪个不属于NSF技术对系统的要求
2. 硬件要求：系统双主控板冗余配置，分布式结构，数据转发和控制分离
3. 软件需求：正常运行时能备份设备信息：主备倒换时接口板不需要重启，接口保持UP，接口板转发不撤销
4. 协议要求：可扩展支持GR功能的相关网络协议
5. 电源要求：必须具备1+1以上级别的备份电源

Answer: D

1. 下面哪个技术不属于专用故障检测技术
2. BFD
3. APS
4. RPR OAM
5. MPLS OAM

Answer: A

解析：BFD属于通用故障检测技术，可检测各个层面的故障。

1. 下面哪个不是组成NSF的技术
2. 冗余备份技术
3. Eth-Trunk技术
4. HSB技
5. GR技术

Answer: B

解析：Eth-Trunk技术属于以太网技术。

1. 判断：NSF（None Stop Forwarding，不间断转发），是一项重要的高可靠性技术，它可以保还路由器控制层面出现故障时，数据转发仍然正常执行，从而保护网络上关键业务不受影响，同时对于支持NSF的协议不需要具有GR能力。
2. True
3. False

Answer: B

解析：协议要求提出各相关网络协议（OSPF、IS-IS、BGP、RSVP）做扩展以具备GR能力。

1. 判断：NSF（None Stop Forwarding，不间断转发），是一项重要的高可靠性技术，它可以保还路由器控制层面出现故障时，数据转发仍然正常执行，从而保护网络上关键业务不受影响。
2. True
3. False

Answer:A

1. 判断：对于NSF来说需要支持的协议如ISIS、OSPF、BGP具有GR能力。
2. True
3. False

Answer: A

解析：协议要求提出各相关网络协议（OSPF、IS-IS、BGP、RSVP）做扩展以具备GR能力。

1. 判断：动态协议（如OSPF、BGP）GR的过程中邻居关系会得到保持。
2. True
3. False

Answer: A

解析：支持GR能力的协议，能够在主备倒换的时候通知邻居，请求邻居保持与自己的邻接关系。

1. 判断：因为BFD是快速检测技术，在邻居设备主备倒换后BFD会快速检测到故障并且通告给相关协议，导致协议退出GR，即便如此BFD和GR两种技术也能同时使用。

True

False

Answer: A

解析：BFD采用转发/控制分离，控制平面的变化不影响BFD检测，如：控制平面为ISIS，当ISIS重启/GR时，BFD可以继续监测链路状态。

1. 以BFD网络故障检测的模式划分，下面哪一项是正确的？
2. 异步模式和查询模式
3. 查询模式和回声功能
4. 回声模式和对等模式
5. 对等体模式和异步模式

Answer: A

解析：以网络故障检测的模式划分，有三种模式——异步模式：周期性发送探测报文；查询模式：发一系列报文请求确认；回声模式：将对端发送过来的报文不做任何改动反射回去。

1. —个VRRP虚拟路由器配置VRID是3，虚拟IP地址是100.1.1.10，那么虚拟MAC地址是多少？
2. 00-00-5E-00-01-64
3. 00-00-5E-00-01-03
4. 01-00-5E-00-01-64
5. 01-00-5E-00-01-03

Answer: B

解析：虚拟MAC地址是虚拟路由器根据虚拟路由器ID生成的地址。 一个虚拟路由器拥有一个虚拟MAC地址，格式为：00-00-5E-00-01-{VRID}。 当虚拟路由器回应ARP请求时，使用虚拟MAC地址，而不是接口的真实MAC地址。

1. VRRP的报文的组播目的地址是
2. 224.0.0.18
3. 224.0.0.20
4. 224.0.1.18
5. 224 0.1.20

Answer: A

解析：VRRP报文封装在IP报文中，发送到分配给VRRP的IPv4组播地址。在IP报文头中，源地址为发送报文的主接口地址（不是虚拟地址或辅助地址），目的地址是224.0.0.18，TTL是255，协议号是112

1. VRRP报文的IP协议号是
2. 112
3. 114
4. 116
5. 118

Answer: A

解析：VRRP报文封装在IP报文中，发送到分配给VRRP的IPv4组播地址。在IP报文头中，源地址为发送报文的主接口地址（不是虚拟地址或辅助地址），目的地址是224.0.0.18，TTL是255，协议号是112

1. 关于VRRPv3的认证方式描述不正确的是
2. null
3. 简单字符认证
4. MD5认证
5. VRRPv3不支持认证

Answer: D

解析：定义了三种认证方式：无认证（no authentication）、简单字符认证（simple clear text passwords）和 MD5认证 （MD5）。

1. 关于VRRP的负载分担描述正确的是 （请选择2个答案）
2. 在路由器的一个接口上可以创建多个虚拟路由器，使得该路由器可以在一个虚拟路由器中作为Master路由器，同时在其他的虚拟路由器中作为Backup路由器。
3. 负载分担方式是指多台路由器同时承担业务，因此负载分担方式需要两个或者两个以上的虚拟路由器
4. 负载分担方式是指建立两个或更多备份组，多台路由器同时承载业务
5. 在配置优先级时，三个虚拟路由器的VRRP master可以在不同路由器上

Answer: C D

解析：一台路由器的一个接口上可以创建多个VRRP备份组。该路由器既可以作为一个VRRP备份组的master路由器，又可以作为其他的VRRP备份组的backup。

负载分担方式是指多台路由器同时承担业务，因此负载分担方式需要建立两个或更多的备份组实现负载分担。

1. 关于管理VRRP描述正确的是：
2. —个管理VRRP备份组只能绑定一个业务VRRP备份组
3. —个管理VRRP备份组可以作为业务VRRP和其他管理VRRP进行绑定
4. 一个业务VRRP可以绑定到多个管理VRRP
5. 管理VRRP绑定多个业务VRRP后，通过只在管理VRRP上运行VRRP协议报文来决定其下而的所有业务VRRP的状态，这样极大降低VRRP协议报文数量，提高了协议报文处理效率

Answer: D

解析：一个业务VRRP备份组只能绑定到一个管理VRRP备份组，但一个管理VRRP组可以绑定多个业务VRRP备份组。

1. 假设有四条流量a、b、c、d分别为100M，端口总带宽为200M，发生了流量拥塞，进行拥塞管理，流量a、b、c、d同属于WFQ队列凋度，权重比为1:2:3:4，则四条流量大小约为
2. 流a、b、c、d分别通过20M、40M、60M、80M
3. 流a、b、c、d分别通过100M、100M、0M、0M
4. 流a、b、c、d分别通过80M、60M、40M、20M
5. 由于拥塞导致流量全部丢弃

Answer: A

1. 以下哪个标准是关于RPR的标准
2. IEEE802.3ad
3. IEEE802.3ac
4. IEEE802 1d
5. IEEE802.17

Answer: D

解析：IEEE 802.17：弹性分组环（RPR）工作组。（引自百度百科）。

1. RPR在对于过环的流里进行转发处理时，可以使用以下哪个队列转发模式
2. 存储转发模式
3. Fragment-Free模式
4. 剥离模式
5. 碎片转发

Answer: A

解析：对于过环，只需二层执行快速转发即可。

1. 根据RPR业务的分组ADM式交换方式，RPR MAC具有以下队列 （请选择2个答案）
2. 上环缓存队列
3. 过环缓存队列
4. 下环缓存队列
5. 保护倒换缓存队列

Answer: A B

解析：请参考华为RPR技术白皮书队列技术有关资料。

1. OSPF是通过哪一类LSA实现GR的功能的？
2. Type-5 LSA
3. Type-7 LSA
4. Type-9 LSA
5. Type-10 LSA

Answer: C

解析：IETF标准OSFP为了对GR实现机制，对OSPF协议进行了扩展，增加第九类LSA，用以在GR Restarter重启时，通知周边邻居进入GR Helper流程。

1. RPR在对于过环的流量进行转发处理时，关于转发模式说法正确的有 （请选择3个答案）
2. 存储转发模式并不一定需要支持
3. 可以使用存储转发模式和直通模式
4. 存储转发模式实现起来简单通用，而直通模式则能够进一步提高效率
5. 即便是采用直通模式的时候，仍然有可能用到存储转发模式

Answer: B C D

解析：RPR在对于过环的流量进行转发处理时，有两种队列转发模式：存储转发模式和直通模式。存储转发模式实现起来简单通用，而直通模式则能够进一步提高效率。存储转发模式是基础，必须要要求支持。即便是采用直通模式的时候，仍然有可能用到存储转发模式，例如直通队列被临时阻塞，就需要转入存储转发模式。（引自华为RPR技术白皮书）

1. 与SDH相比，RPR技术有如下优点 （请选择3个答案〉
2. 公平的节点带宽分配
3. 快速保护机制
4. 有效支持组播和广播
5. 带宽高利用率

Answer: A C D

1. RPR的故障自愈能为很强，可以采用的保护方式有： （请选择3个答案）
2. 绕回（Wrap）方式
3. 抄近（Steering）方式
4. 先绕回（Wrap）再抄近（Steering）方式
5. 先抄近（Steering）再绕回（Wrap）方式

Answer: A B C

1. GR（Graceful Restart）成功的前提包括以下哪几个 （请选择2个答案）
2. 使用BFD及时发现网络故障
3. GR helper发送状态给GR Rstarter
4. 转发和控制分离
5. GR Time时间内网络拓扑和接口状态不发生变化

Answer: C D

1. RPR支持以下哪些分配带宽的算法 （请选择3个答案）
2. 绝对公平方式
3. 带宽独占方式
4. 加权公平方式
5. 关键位置保护方式

Answer: A B C

1. 在最新的草案中BFD控制报文封装在UDP报文中传送，多跳BFD控制报文的目的端口号是多少？
2. 2784
3. 3784
4. 4784
5. 5784

Answer: C

解析：在多跳检测中，封装BFD控制报文的UDP报文的目的端口号是3784，源端口号取值范围是49152~65535。

1. VRP版本支持的BFD版本号是多少？
2. Version 1
3. Version 2
4. Version 3
5. Version 4

Answer: A

解析：当前VRP5.7版本支持的BFD版本号为1。

1. 当两端BFD检测时间间隔分别为30ms和40ms时，下面描述正确的是
2. bfd会话可以建立，协商后取40ms
3. bfd会话可以建立，协商后取30ms
4. bfd会话可以建立，各自按照自己的时间间隔发送
5. bfd会话无法建立

Answer: A

解析：BFD控制报文发送时间间隔是本端Desired Min TX Interval与对端Required RX Interval两者的最大值，本端BFD检测时间等于对端BFD报文中的Detect Mult乘以协商好后的对端报文的发送时间间隔。

1. 关于smart link链路发生链路切换时的刷新机制描述错误的是
2. 自动通过流量刷新MAC及ARP
3. Smart Link设备从新的链路上发送Flush报文
4. 不能自动通过流量刷新MAC及ARP
5. 当原主用链路故障恢复时，将维持在阻塞状态，不进行抢占，从而保持流量稳定

Answer: C

解析：当主链路恢复后，如果该Smart Link组配置允许角色抢占，备链路将自动阻塞并切换到待命状态，而主链路将切换到转发状态。当Smart Link发生链路切换时，网络中各设备上的MAC地址转发表项和ARP/ND表项可能已经不是最新状态，为了保证报文的正确发送，需要提供一种MAC地址转发表项和ARP/ND表项的更新机制。（个人感觉D描述也错了）

1. 关于monitor link的描述错误的是
2. Monitor Link组也叫监控链路组，由上行端口和下行端口共同组成
3. 一个组包含一个上行端口和若干个下行端口
4. 下行端口的状态随上行端口的变化而变化
5. Monitor Link组也叫监控链路组，由上行端口组成

Answer: D

解析：Monitor Link组也叫监控链路组，每个组由上行端口和下行端口共同组成。参考：http://www.h3c.com.cn/Products\_\_\_Technology/Technology/LAN/

1. 当传递VRRP心跳报文的中间链路故障时关于VRRP和VRRP的状态切换描述正确的是
2. VRRP两端同时变为master状态，VRRP心跳报文通过TCP传输
3. VRRP两端同时变为master状态，VRRP心跳报文通过UDP传输
4. VRRP两端同时变为slave状态，VRRP心跳报文通过TCP传输
5. VRRP两端同时变为slave状态，VRRP心跳报文通过UDP传输

Answer: B

1. 关于VRRP的描述错误的是
2. VRRP组中的路由器根据优先级选举出Master
3. Master路由器通过发送免费ARP报文，将自己的虛拟MAC地址通知给与它连接的设备或者主机
4. 如果Master路由器出现故障，虚拟路由器中的Backup路由器将根据优先級重新选举新的Master
5. 因为优先级的范围为1-255，所以当Backup设备收到的VRRP通告报文中的优先级值为0时，Backup将丢弃该报文，不做任何处理

Answer: D

解析：优先级的取值范围为0到255 （数值越大表明优先级越高），缺省值是100，但是可配置的范围是1到254。0为系统保留为特殊用途来使用。255则保留给IP地址拥有者。（参考华三官网资料）

1. 关于高可用性网络的特点描述正确的 （请选择2个答案）
2. 不能频频出现故障
3. 出现故障后能很快恢复
4. 不会出现故障
5. 一旦出现故障只能通过人工干预恢复业务

Answer: A B

1. 下列关于BFD回声报文的描述错误的是 （请选择2个答案）
2. BFD协议未定义回声报文的格式
3. BFD协议严格定义了回声报文的格式
4. 协议规定回声报文采用的UDP端口号为3785
5. 协议规定回声报文采用的TCP端口号为3785

Answer: B D

解析：回声功能启动后，会话的一端周期性地发送BFD Echo报文，BFD Echo报文采用UDP封装，目的端口号为3785，目的IP地址为发送接口的地址，源IP地址由配置产生。

BFD协议并未定义回声报文的格式，但是对于回声报文，其格式只是与本地相关，远端只需把此报文在反向通道上返回。

1. 下列关于BFD控制报文的描述错误的是 （请选择2个答案）
2. BFD控制报文封装在UDP报文中传送，包括一个必选部分和一个可选的验证部分
3. 目前VRP5.7提供BFD验证功能
4. 协议规定控制报文采用的UDP端口号为3784
5. 协议规定控制报文采用的TCP端口号为3785

Answer: B D

解析：BFD控制报文包括强制部分和可选认证部分。协议定义了控制报文所使用的UDP目的端口号为3784。

1. 以下关于QoS中的Diff-Serv服务模型说法错误的是
2. 它需要信令，即应用程序在发出报文前，不需要通知路由器，网络不需要为每个流维护状态
3. 它可以以用不同的方法来指定报文的QoS，如IF包的优先级位（IP Prcedence），报文的源地址和目的地址等
4. 它一般用来为一些重要的应用提供端到端的QoS保证
5. 它可以通过CAR或队列等技术实现

Answer: A

解析：Differentiated Service可以满足不同的QoS需求，它不需要信令，即应用程序在发出报文前，不需要通知路由器。可以用不同的方法来制定报文的QoS，如IP包的优先级、报文的源地址和目的地址等。它通过CAR或队列技术来实现。

1. 下来关于BFD在查询模式的描述错误的是 （请选择2个答案）
2. 本端按一定的发送周期发送BFD控制报文，需要在远端检测本端系统发送的BFD控制报文
3. 检测本端发送的BFD控制报文是在本端系统进行的
4. 如果某个系统在检测时间内没有收到对端发来的BFD控制报文，就宣布会话为Down
5. 每个系统都有一个独立的方法用来确认它连接到其他系统，这样一旦一个BFD会话建立起来以后，系统停止发送BFD控制报文

Answer: A C

解析：本端发送本端接收，远端不对报文进行处理，而只是将此此报文在反向通道上返回。如果在检测时间内没有收到返回的报文就宣布会话为Down，如果收到对端的回应报文，协议再次保持沉默。

1. 下列关于BFD 回声功能的描述正确的是 （请选择3个答案）
2. 本地发送一系列BFD回声报文，远端系统通过它的转发通道将它们环回回来
3. 如果本地系统连续几个回声报文都没有接收到，会话就被宣布为Down
4. 回声功能可以和上述两种检测模式一起使用
5. 不可以使用回声功能来代替BFD控制报文的检测的任务

Answer: A B C

解析：本地发送一系列BFD回声报文，远端系统通过它的转发通道将它们环回回来。如果本地系统连续几个回声报文都没有接收到，会话就被宣布为Down。回声功能可以和上述两种检测模式一起使用，可以使用回声功能来代替BFD控制报文的检测的任务，这样可以降低控制报文的发送周期（异步模式下）或者完全取消BFD控制报文（查询模式下）。（参考华为BFD技术白皮书）

1. 下列关于VRRP的描述正确的是 （请选择3个答案）
2. VRRP是一种冗余备份协议，为具有组播或广播能为的局域网 （如以太网）设计，保证局域网内主机的下一跳路由器设备出现故障时，可以及时地由另一台路由器来代替，从而保持网络通信的连续性和可靠性
3. 在使用VRRP协议时，需要在路由器上配置虚拟路由器号和虚拟IP地址，直接使用主用路由器的真实MAC，这样在这个网络中就加入了—个虚拟路由器
4. 网络上的主机与虚拟路由器通信，不需要了解这个网络上物理路由器的所有信息
5. —个虚拟路由器由一个主路由器和若干个备份路由器组成，主路由器实现真正的转发功能，当主路由器出现故障时，一个备份路由器将成为新的祝路由器，接替它的工作

Answer: A C D

解析：解析：虚拟MAC地址——虚拟路由器根据虚拟路由器ID生成的MAC地址。 当虚拟路由器回应ARP请求时，使用虚拟MAC地址，而不是接口的真实MAC地址。

1. 下列关于VRRP的描述正确的是 （请选择3个答案）
2. VRRP根据优先级来确定虚拟路由器中每台路由器的地位
3. 如果Backup路由器工作在非抢占方式下，则只要Master路由器没有出现故障，Backup路由器即使随后被配置了更高的优先级也不会成为Master路由器
4. 如果已经存在Master，Backup也会进行抢占。
5. 当两台优先级相同的路由器同时竞争Master时，比较接口IP地址大小，接口地址大者当选为Master。

Answer: A B D

解析：一旦备份组中的某台路由器成为主路由器，只要它没有出现故障，其它路由器即使随后被配置更高的优先级，也不会成为主路由器，除非被设置为抢占方式。

1. 关于VRRP master设备的描述正确的是 （请选择3个答案）
2. 定期发送VRRP报文
3. 以虚拟MAC地址响应对虚拟IP地址的ARP请求
4. 转发目的MAC地址为虚拟MAC地址的IP报文
5. 即使该路由器已经为Master，也会被优先级高的Backup路由器抢占

Answer: A B C

解析：一旦备份组中的某台路由器成为主路由器，只要它没有出现故障，其它路由器即使随后被配置更高的优先级，也不会成为主路由器，除非被设置为抢占方式。

1. 关于VRRP slave设备的描述正确的是 （请选择3个答案）
2. 接收Master发送的VRRP报文，判断：Master的状态是否正常
3. 当收到优先级为0的VRRP报文时，Salve直接升级为Master
4. 丢弃目的MAC地址为虚拟MAC地址的IP报文
5. 响应目的IP地址为虚拟IP地址的IP报文

Answer: A B C

解析：VRRP中定义了三种状态模型：初始状态（Initialize）、活动状态（Master）、备份状态（Backup）。其中，只有活动状态可以为到虚拟IP地址的转发请求服务。

1. 关于VRRP快速切换的描述错误的是 （请选择2个答案）
2. 使用VRRP监视BFD session或者EFM功能，在BFD session或者是EFM会话状态改变后通知VRRP模块，实现VRRP快速切换
3. —个VRRP备份组不能同时监视Peer BFD、Link BFD和Normal BFD
4. VRRP备份组监视普通BFD时，当BFD状态变化时，通过修改备份组优先级改变主备状态，被监视的BFD会话状态恢复时，路由器在备份组中的优先级将恢原来的值
5. 同时配置监视多个BFD的情况下，各个配置相互关联，可能会有影响

Answer: B D

解析： 使用VRRP监视BFD session功能，在BFD session状态改变后通知VRRP模块。VRRP模块根据配置降低或增加优先级，实现VRRP快速切换。

如果不配置peer或link参数，则执行命令vrrp vrid track bfd-session表示配置VRRP监视普通BFD。

如果配置了peer或link参数，则执行命令vrrp vrid track bfd-session表示配置VRRP监视Peer BFD或Link BFD。

1. 关于管理VRRP的描述正确的是 （请选择3个答案）
2. 管理VRRP备份组可绑定其他的业务备份组，并根据绑定关系，决定相关业务备份组的状态
3. 一个管理VRRP备份组可绑定多个业务备份组，它不能作为业务备份组与其他管理备份组进行绑定
4. 成员VRRP备份组与管理VRRP备份组绑定之后，成员VRRP状态机就丧失了独立性，即会删除协议定时器，不再收发协议报文，通过直接拷贝管理备份组的状态来实现自己的状态机
5. 普通VRRP备份组被加入管理VRRP备份组后，需要自己发送VRRP协议报文来决定自己的状态

Answer: A B C

1. 关于smart-link组的描述错误的是 （请选择2个答案）
2. 一个组内只能包含一个端口
3. 正常情况下，只有一个端口出于转发（active）状态，另一个端口被阻塞，处于待命（standby）状态
4. 当转发状态的端口链路故障（可能是物理上的故障、OAM的连接故障或者单通等）时，Smart Link组会自动将该端口阻塞，并将原阻塞的待命端口切换到转发状态
5. 当主端口故障恢复后备用端口会重新进入阻塞状态，流量切回主链路

Answer: A D

解析：Smart Link组也称为灵活链路组，一个Smart Link组包含两个成员端口，其中一个被指定为主端口（Master Port），另一个被指定为副端口（Slave Port），不同的Smart Link组可以包含同一个端口。正常情况下，只有一个端口（主端口或副端口）处于转发（ACTIVE）状态，另一个端口被阻塞（BLOCK），处于待命（STANDBY）状态。当处于转发状态的端口发生链路故障（链路故障目前主要是指端口状态转为DOWN、以太网OAM链路故障等）时，Smart Link组会自动将该端口阻塞，并将原阻塞的处于待命状态的端口切换到转发状态。

如果Smart Link组配置为角色抢占模式，当主用链路故障恢复后，主端口将抢占为转发状态，副端口则进入待命状态。只有当主用链路故障时，副端口才会从待命状态切换到转发状态。

如果Smart Link组配置为非角色抢占模式，当主用链路故障恢复后，副端口将继续处于转发状态，主端口继续处于待命状态，这样可以保持流量的稳定。（参考H3C官网资料——Smart Link & Monitor Link技术白皮书）

1. Smart Link发生链路切换时，可以刷新的MAC利ARP的机制有哪几种？ （请选择2个答案）
2. 手工通过流量刷新MAC及ARP
3. Smart Link设备从新的链路上发送Flush报文
4. 等持MAC地址老化
5. 等待ARP表项

Answer: A B

解析：MAC地址和ARP表项刷新目前主要有以下两种：通过FLUSH报文通知设备更新表项，通过流量刷新MAC及ARP。

1. 关于链路聚合的基本槪念下面描述正确的是 （请选择3个答案）
2. 链路聚合是将一组物理接口捆绑在一起作为一个逻辑接口来增加带宽及可靠性的方法
3. 链路聚合遵循IEEE802.3ad协议
4. 将若干条物理链路捆绑在一起所形成的逻辑链路称为链路聚合组（LAG）或者Trunk
5. 链路聚合只存在活动接口

Answer: A B C

1. 关于链路聚合的分类下面描述错误的是 （请选择2个答案）
2. 根据是否启用链路聚合控制协议分为手工负载分担模式链路聚合和LACP协议链路聚合两种
3. 动态LACP模式下所有活动接口都参与数据的转发，分担负载流量，因此成为负载分担模式
4. 静态LACP模式下，Eth-Trunk的建立，成员接口的加入，都是由手工配置完成的，但与手工负载分担模式链路聚合不同的是，该模式下LACP协议报文参与活动接口的选择
5. 动态LACP模式下，Eth-Trunk的建立，成员接口的加入，活动接口的选择需要手工配置

Answer: B D

解析：动态 LACP 模式下，Eth-Trunk 接口的建立，成员接口的加入，活动接口的选择完全由LACP 协议通过协商完成。

1. 关于LACP协议的描述正确的是 （请选择2个答案）
2. 基于IEEE802.3au标准
3. 通过LACPDU （Link Aggregation Control Protocol Data Unit）：与对端交互信息
4. 两端设备根据系统LACP优先级和系统ID确定主动端
5. 两端设备根据被动端接口LACP优先级和接口ID确定活动接口

Answer: B C

解析：基于 IEEE802.3ad 标准的LACP（Link Aggregation Control Protocol，链路汇聚控制协议）是一种实现链路动态汇聚与解汇聚的协议。两端设备根据接口LACP 优先级确定活动接口。

1. 下面哪些操作可以加快OSPF的快速收敛 （请选择3个答案）
2. 配置动态BFD for OSPF
3. 调整OSPF计算间隔
4. 调整hello时间间隔
5. 配置LSDB中External LSA的最大数量

Answer: A B C

1. BGP GR Restarter进行主备倒换时，邻居检测到因为TCP连接中断，下面哪些操作是正确的？ （请选择2个答案）
2. 保留协商过程中GR Restarter通告的各个地址族的路由表，并对这些表项作老化（Stale )标记，启动一个State定时器
3. 启动Restart Time定时器
4. 如果在Restart Time定时器超时后，GR Restarter仍然没有和自己重建BGP连接，保留所有与GR Restarter相关的路由和转发表项
5. 保持邻居关系不中断

Answer: A B

1. MPLS OAM使用的报文分是哪三类 （请选择3个答案）
2. 故障检测
3. 连通性检测
4. 前向缺陷通告FDI
5. 后叫缺陷通过BDI

Answer: B C D

解析：MPLS OAM使用的报文分为三类：连通性检测——包含FFD、CV；前向缺项通告FDI；后向缺陷通告BDI。

1. 关于可靠性组网原则描述正确的是 （请选择2个答案）
2. 分层组网：将网络分为核心层，汇聚层，边缘层
3. 同层内不要进行互联，互联会增加网络的复杂性
4. 下层双归或多归到上层多个设备的单点上或是多点上
5. 整体根据业务流量情况全面调整

Answer: A C

1. RPR环中有A、B、C, D四个节点，RPR链路带宽为2.5Gbps，流量通过0环传送， A、B、C都试图往环上发送1000M的流垦。分忻在执行完公平算法以后，A/B/C节点占用的带宽是多少？采用什么算法法实现？ （请选择2个答案）
2. A-833M B-833M C-833M
3. A-1000M B-750M C-750M
4. 绝对公平算法
5. 关键节点保护算法

Answer: A C

解析：RPR环公平算法平均享用带宽。

1. RPR节点的MAC数据通道与各自子环数据传送直接挂钩，包括以下方面的功能： （请选择2个答案）
2. 流量整形（shaping），使其能够有序地进入共享的环介质
3. 要选择在内环还是外环传输数据帧
4. 不用选择数据帧就可以从环上剔除
5. 在源节点时，数据帧要开路（staging）；在过环节点时，数据帧要排队（queuing）

Answer: A D

解析：MAC数据通道与各自资环数据传送直接挂钩，包括四个方面：

* 流量整形（Shaping），使其能够有序地进入共享环介质；
* 在源节点时，数据帧要开路（Staging）：在过环节点时，数据帧要排队（Queuing）；
* 要选择数据帧递送到本地客户端或控制子层；
* 要选择数据帧从环上剔除。（参考http://dwz.cn/3oAsAl）

1. 相对于流量监管，流量整形引入了列队，用于缓存超过限制的流量，关于流量整形下面描述不正确的是
2. 相对于流量监管，流量整形具有更好的抗突发能力
3. 流量整形可以使报文以比较均匀的速度向外发送
4. 由于引入队列，当发生拥塞时，报文的时延相对增加
5. 语音业务采用流量整形，而不是流里监管

Answer: D

解析：网络中，当从高速链路向低速链路传输数据时，带宽会在低速链路接口处出现瓶颈，导致数据丢失严重，特别是会影响到低延时要求的数据如语音等。流量监管 TP（Traffic Policing）的典型应用就是为了避免这种瓶颈的出现，通过监督进入网络的某一流量的规格，把它限制在一个合理的范围之内，保护网络资源和运营商的利益。

1. NSF对于系统的要求描述错误的是 （选择2个答案）
2. 硬件要求：系统双主控冗余配罝，分布式结构，数据转发和控制分离
3. 系统软件要求：主板正常运行的过程中，会把配置信息、接口状态信息备份到备用板；主备倒换的时候，接口板不需要重启，接口保持Up，接口板转发表不撤销
4. 协议要求：要求各相关网络协议具备GR（Graceful Restart，优雅重启）能力，但是LDP不能支持GR
5. 对邻居设备没要求

Answer: C D

1. 普通的BGP/MPLS IPV4 VPN中，IGP采用OSPF，标签协议釆用LDP和私网邻居采用静态路由，如果要达到PE设备具备NSF功能，需要哪些协议使能GR？ （请选择3个答案）
2. OSPF
3. LDP
4. BGP
5. 静态路由

Answer: A B C

1. 当前VRP5平台支持GR的动态协议有哪些？ （请选择3个答案）
2. RSVP
3. OSPF
4. BGP
5. STP

Answer: A B C

解析：目前具备GR能力的路由协议主要有IS-IS、OSPF、BGP、RSVP。

1. 下面关于BFD的描述正确的是 （请选择3个答案）
2. 能够对mpls网络进行检测
3. 对相邻转发引擎之间的路径提供轻负荷、短持续时间的检测
4. 采用单一机制对所有类型的介质、协议层进行检测，实现全网统一的检测机制
5. 是一种单向检测机制

Answer: A B C

解析：双向转发BFD是一套全网统一的检测机制，用于快速检测、监控网络中链路或者IP路由的转发联通状况。

1. 下面关于BFD会话的建立方式的描述正确的是 （请选择3个答案）
2. BFD会话的建立只有通过动态建立BFD会话
3. 静态配置BFD会话是指通过命令手工配置BFD会话参数，包括了配置本地标识符和远端标识符等，然后手工下发BFD会话建立请求
4. 动态建立BFD会话时，动态分配本地标标识符
5. 系统通过划分标识符区域的方式来区分静态BFD会话和动态BFD会话

Answer: B C D

解析：BFD会话的建立也可通过动态方式，如BFD for OSPF。

1. 判断：传统IP网络的尽为服务不可能识别和区分出网络中的各种通信类别，不能满足应用的需求。QoS技术的出现便致力于解决这一问题。
2. True
3. False

Answer: A

1. 判断：拥塞管理是指网络在发生拥塞时，如何进行管理和控制，处理方法是使用队列调度技术。
2. True
3. False

Answer: A

1. 判断：传统的丢包策略采用尾部丢弃（Tail-Drop）的方法，这种丢弃方法会导致TCP全局同步现象。
2. True
3. False

Answer: A

1. IETF DiffServ工作组目前定义了几种PHB？
2. 4
3. 3
4. 2
5. 1

Answer: A

解析：IETF DiffServ工作组目前定义了四种PHB：Default PHB、Class-Selector PHB、Expedited forwarding PHB、Assured Forwarding PHB。

1. 简单流分类可以对报文的哪些信息进行标记或重标记？
2. IP D3CP、IP Precedence、802.1p、EXP信息
3. IP Source、Destination Address、EXP信息
4. MAC Address信息
5. 报文中的任何信息

Answer: A

解析：简单流分类是指采用简单的规则，如IP DSCP值，MPLS报文的EXP域值，VLan报文头中的802.1P值。（原题目缺少简单流分类）

1. 对于标签，可以根据报文的什么信息来进行简单流分类？
2. DSCP信息
3. IP Precedence信息
4. MPLS EXP信息
5. 802.1 P信息

Answer: C

1. 拥塞避免通常采用的QoS技术是
2. GTS
3. LR
4. Car
5. WRED

Answer: D

解析：拥塞避免通常可使用RED或WRED来避免全局同步现象。

1. Best-Effort Service模型是通过什么队列技术来实现的？
2. FIFO
3. WFQ
4. PQ
5. LQ

Answer: A

解析：传统尽力传送（Best Effort）方式，采用先入先出（FIFO）的策略进行处理。

1. 端口队列调度中那一种队列没有公平性、不同的流之间不能相隔离？
2. CQ+WFQ
3. PQ+WFQ
4. FIFO
5. WRR

Answer: C

解析：传统尽力传送（Best Effort）方式，采用先入先出（FIFO）的策略进行处理。

1. 可以对RTP和TCP报文头进行压缩的链路效率机制是
2. IPHC
3. LFI
4. PPP
5. HDLC

Answer: A

解析：VRP提供了两种链路效率机制：IP报文头压缩协议（IP Header Compression，IPHC）和链路分片与交叉（Link Fragmentation and lnterleaving，LFI），其中IPHC协议可以对 RTP和TCP报文头进行压缩。

1. QoS （即服务质量），通常包括哪几个方面？ （请选择3个答案）
2. 传输的带宽
3. 传输的时延和抖动
4. 数据的丢包率
5. 增加网络的带宽

Answer: A B C

1. 判断：抖动是由于属于同一个流的数据包的端到端时延不相等造成的。
2. True
3. False

Answer: A

1. 下面关于时延和抖动描述正确的是 （请选择2个答案）
2. 端到端时延等于处理时延与队列时延之和
3. 抖动是因为每个包的端到端时延不相等造成的
4. 抖动的大小跟时延的大小相关，时延小则抖动的范围也小，时延大则可能的抖动范围也大
5. 抖动的大小跟时延不相关

Answer: B C

解析：端到端的时延由传输时延、处理时延和队列时延组成。

1. QoS服务模型包括 （请选择3个答案）
2. Best-Effort Service模型
3. lntegrated Service模型
4. Differentiated Service模型
5. FIFO Service模型

Answer: A B C

解析：传统尽力传送（Best Effort）方式，采用先入先出（FIFO）的策略进行处理，不属于QoS服务。

1. 以下解决方案可以提高网络QoS的有？ （请选择3个答案）
2. 提高链路带宽
3. 合理使用队列调度和拥塞避免机制
4. 使用链路有效性机制提高链路的效率
5. 将不同的业务安排在不同时段来提供服务

Answer: A B C

1. 按照分类规则参考信息的不同，流量分类可以分为 （请选择2个答案）
2. 简单流分类
3. 复杂流分类
4. 按需流分类
5. 业务流分类

Answer: A B

1. 对于IPv4报文，我们可以根据报文的什么信息来进行简单流分类？ （请选择2个答案）
2. DSCP信息
3. IP Precedence信息
4. Traffic Class信息
5. 802.1P信息

Answer: A B

解析：简单流分类是指采用简单的规则，如IP报文头就采用DSCP或者IP-PRE值。

1. 流量整形通常采用的技术有 （请选择2个答案）
2. GTS
3. LR
4. AR
5. RED

Answer: A B

解析：通过流量整形采用的技术有：Generic Trafficd Shaping（GTS）、Line Rate（LR）。

1. 网络管理者可以使用约定访问速度CAR（Committed Access Rate）来对流量进行控制监管，常用的Car流量监管实现方法有 （请选择3个答案）
2. 单桶单速
3. 双桶单速
4. 双桶双速
5. 单桶双速

Answer: A B C

1. 关于GTS、LR与CAR二者的区别，以下描述正确的是 （请选择3个答案）
2. 在进行报文流量控制时，CAR对超过流量限制的报文进行丢弃
3. 在进行报文流量控制时，GTS将超过流量限制的报文缓存在GTS队列中
4. 在进行报文流屋控制时，LR对超过流量限制的报文进行丢弃
5. 在进行报文流量控制时，LR对超过流量限制的报文不但能进行丢弃，还能是报文进行QoS队列进行处理

Answer: A B D

解析：LR能够限制在物理接口上通过的所有报文，CAR和GTS在IP层实现，对不经过IP层处理的报文不起作用，LR与GTS比较，LR不但能够对超过流量限制的报文进行缓存，还能使报文进入了QoS队列机制进行处理。

1. 常见的队列调度技术有 （请选择4个答案）
2. FIFO
3. LR
4. WRR
5. CIR
6. CQ
7. WFQ

Answer: A C E F

解析：LR属于流量整形。

1. 拥塞发生时，通常会影响到QoS的有哪些指标？ （请选择3个答案）
2. 传输时延
3. 传输抖动
4. 传输带宽
5. 传输距离

Answer: A B C

1. 判断：端到端时延等于路径上所有处理时延与队列时延之和。
2. True
3. False

Answer: B

解析：端到端的时延由传输时延、处理时延和队列时延组成。

1. 传统的拥塞避免机制（Tail-Drop）尾丢弃的缺点包括 （请选择3个答案）
2. TCP全局同步
3. 高抖动和高延迟
4. 高费用
5. 无差别的丢弃，没有区分各种不同优先级的报文

Answer: A B D

1. 在下面描述拥塞避免机制中的丢弃策略中，错误的有 （请选择2个答案）
2. FIFO
3. RED
4. WRED
5. WFQ

Answer: A D

解析：FIFO、WFQ属于队列调度技术。

1. 为避免TCP全局同步现象，可使用的拥塞避免机制有 （请选择2个答案）
2. RED
3. WRED
4. Tail-Drop
5. WFQ

Answer: A B

解析：常用的拥塞避免技术中能避免全剧同步的有RED/WRED。

1. 常用于提升链路效率机制有 （请选择2个答案）
2. IPHC
3. LFI
4. PPP
5. 没有正确答案

Answer: A B

解析：VRP提供了两种链路效率机制：IP报文头压缩协议（IP Header Compression，IPHC）和链路分片与交叉（Link Fragmentation and lnterleaving，LFI）。

1. 判断：网络中采用QoS，提高了某类业务的服务质量的同时肯定会损害其它业务的服务质量。
2. True
3. False

Answer: A

1. 判断：在Best-Effort、Integrated Service、Differentiated Service三种服务模型中，只有Integrated Service与Differentiated Service这两种能提供多服务的QoS保障，实际网络建设中网络边缘应该使用Integrated Service方式，网络核心使用Differentiated Service方式。
2. True
3. False

Answer: B

解析：Best-Effort也属于QOS常见三种模型之一。在提供IP网络的QoS时，为了适应不同规模的网络，一般在骨干网需要采用DiffServ体系结构。

1. 以下关于QoS中的DSCP说法正确的是？ （请选择3个答案）
2. 用TOS字段的前6个比特（高6位比特）来标识不同的业务类型，称为DSCP
3. 可以使用DSCP将流量分成32类
4. 每个DSCP值对应一个BA（Behavior Aggregate），然后可以对每一个BA指定一种PHB
5. 可以使用某些QoS机制来实现这个PHB

Answer: A C D

解析：若使用DSCP，即ToS域的前6位，则最多可分成2^6=64类。

1. 以下说法可以准确描述EF PHB的是
2. 用最小的报文丢失确保端到端的服务
3. 为不同优先级的流量提供差异化的服务
4. WRED
5. 尽为而为地传送报文

Answer: A

解析：EF PHB代表DiffServ网络中最高的服务质量。

1. 在Diff-Serv网络中，用DSCP最多可以定义的有意义的取值数目是
2. 3
3. 6
4. 8
5. 64

Answer: D

解析：若使用DSCP，即ToS域的前6位，则最多可分成2^6=64类。

1. 在网络层，以下不可以用来对IP报文进行分类的有
2. 报文长度
3. VLAN ID
4. 源IP地址和目的IP地址
5. TOS字段

Answer: B

解析：源MAC地址、目的MAC地址、VLAN等都属于二层报文信息。

1. 判断：带宽决定数据传输的速率，传输的最大带宽是由传输路径上的最小链路带宽决定的。
2. True
3. False

Answer: A

解析：木桶原理。

1. 判断：对于同一个流的数据包，IP头部的大部分字段是不同的，所以不能对这些字段进行压缩。
2. True
3. False

Answer: B

1. 下列IP Precedence的取值中，代表Immediate的业务流量的是
2. 0
3. 2
4. 5
5. 6

Answer: B

1. 以下关于华为产品QoS缺省PHB说法错误的是
2. 对应的DSCP值是000000
3. 对应的队列机制是FIFO
4. 对应的队列机制是WFQ
5. 对应的丢弃策略是WRED

Answer: C

1. 判断：对于带有AF DSCP标记的数据，应该给它们一定数量的保证带宽，如果存在没有使用的带宽，它们不能占用这些额外的带宽。
2. True
3. False

Answer: B

1. 判断：拥塞管理的中心内容是制定调度策略决定数据包处理的先后顺序。
2. True
3. False

Answer: A

1. 判断：QoS中，RTPQ就是在WFQ或CBQ队列机制上增加一个RTP优先队列。
2. True
3. False

Answer: A

解析：RTPQ就是在WFQ或CBQ中增加一个低时延队列，保证VOIP报文的及时处理。

1. 判断：在部署QoS时候，可以使用PBR来进行流量分类和标记，可以依据ACL定义的规则（源 IP地址、目的IP地址、协议类型、端口号等）和数据包的长度范围进行分类，然后修改数据包的DSCP或IP Precedence字段进行标记
2. True
3. False

Answer: A

1. 判断：物理接口总速率限制（简称LR）可以在一个物理接口上，限制接口发送报文（包括紧急报文）的总速率。
2. True
3. False

Answer: A

1. 判断：Round Robin调度方式按每个队列定义的字节数轮询发送，每个队列占用的带宽比率等于本队列定义的字节数与所有队列字节数之和的比值。
2. True
3. False

Answer: A

1. 判断：PQ的分类机制支持使用标准或扩展的IP访问列表。
2. True
3. False

Answer: A

解析：PQ可以使用ACL对报文进行分类，报文丢弃策略只采用Tail Drop机制。队列长度设置为0，表示该队列无穷大。

1. 判断：丢包仅发生在报文的发送端。
2. True
3. False

Answer: B

1. 判断：CBQ流量策略可以无限嵌套。
2. True
3. False

Answer: B

1. 判断：复杂流分类是指根据五元组（源/目的地址、源/目的端口号、协议类型）等信息对报文进行分类，通常应用在网络的核心位置。
2. True
3. False

Answer: B

解析：通过在Diff-Serv域边界路由器上对流量进行复杂流分类。

1. 判断：Diff-Serv域的核心路由器通常进行简单流分类。
2. True
3. False

Answer: A

1. 判断：IP报文中有专门的字段进行QoS的标记，在IPv4中为TOS，TOS字段用前6bit来标记DSCP。
2. True
3. False

Answer: A

解析：在IP报文中有专门的字段进行QoS的标记，在IPV4中为TOS，IPv6中为TrafficClass。TOS字段用前6bit来标记DSCP，如果只用前3 bit 就为IP优先级。DSCP和IP优先级都是标记的标准。

1. 判断：流量分类是按照一定的规则识别符合某类特征的报文，特征不同的报文可以享受到不同的服务，按照分类规则参考信息的不同，流量分类可以分为简单流分类和复杂流分类。
2. True
3. False

Answer: A

1. 判断：CAR（Committed Access Rate）是利用令牌桶技术来进行流量整形的。
2. True
3. False

Answer: B

解析：CAR是利用令牌桶来进行流量控制的。

1. 判断：流量整形通常使用队列来完成。
2. True
3. False

Answer: B

解析：流量整形通常使用缓冲区或队列和令牌桶来完成。常用的技术有GTS、LR。

1. 判断：IntServ模型，在应用程序发送报文前，需要向网络申请预留资源。
2. True
3. False

Answer: A

解析：IntServ集成服务模型是一个综合服务模型，可以满足多种QoS需求，在发送报文前，需要向网络申请特定的服务，这个请求是通过信令来完成的。

1. 下面关于时延与抖动的关系描述正确的是
2. 抖动的大小跟时延的大小直接相关
3. 抖动是由于属于不同流的数据包的端到端时延不相等造成的
4. 时延大则抖动范围也小，时延小则可能的抖动范围也大
5. 抖动的大小跟时延不相关

Answer: A

1. 判断：所谓拥塞，是指由于供给资源的相对不足而造成服务速率下降（引入了额外的延迟）的一种现象，拥塞避免的技术包括：RED和WRED
2. True
3. False

Answer: A

1. 下面对“报文标记”描述不正确的是
2. 可以对报文的QoS信息字段进行标记
3. 可以对IP报文的DSCP、IP Precedence信息进行标记
4. 可以对Vlan报文的802.1P信息进行标记
5. 可以对报文的MAC进行标记

Answer: D

1. 若使用DSCP ( ToS域的的前6位），则最多可将报文分成几类？
2. 8
3. 16
4. 32
5. 64

Answer: D

解析：使用前6位标记，则2^6=64

1. 根据IP Precedence、MPLS EXP或802.1P信息，可以将报文分为几种业务类型？
2. 2
3. 4
4. 6
5. 8

Answer: D

解析：如果使用前3位，则2^3=8

1. 为了给不同的用户或业务提供不同的服务，可以根据报文的信息（如报文优先级、源IP、目的IP、端口号等）来精细划分用户或业务。为实现划分功能我们通常采用的QoS技术是
2. 流量监管
3. 复杂流分类
4. 拥塞避免
5. 拥塞管理

Answer: B

1. CAR不仅可以对流量进行限制，还可以对报文颜色进行标记。以单桶单速的流量监管为例，当令牌充足时，报文颜色将被标记为
2. red
3. green
4. yellow
5. blue

Answer: B

1. 双桶双速流量监管，当CIR配置为1M，PIR配置为2M时，标记为green的流量能通过的最大平均速率为
2. 1M
3. 2M
4. 4M
5. 8M

Answer: A

1. 以下队列调度技术中，那种队列调度技术的公平性较好？
2. WFQ
3. PQ
4. FIFO
5. RR

Answer: A

1. 可以根据报文中的哪些信息来进行复杂流分类？ （请选择3个答案）
2. 报文的包长度
3. 源、目的地址信息
4. 协议类型
5. 源、目的MAC地址信息

Answer: B C D

解析：复杂流量分类可以采用五元组分类。

1. 判断：PHB（Per-Hop Behavior）是DS节点作用于数据流的行为，每个DS节点必须支持缺省PHB。
2. True
3. False

Answer: A

解析：如果发现未定义到PHB的映射，则DS节点将选择采用缺省PHB进行转发处理，每个DS节点必须支持该缺省PHB。

1. 下面对流量监管的功能描述正确是 （请选择2个答案）
2. 对报文不能进行着色处理
3. 对报文进行着色处理
4. 对超过流量限制的报文进行缓存
5. 对超过流量限制的报文不能进行缓存

Answer: B C

1. 以下关于QoS中丢包的说法正确的有？ （请选择3个答案）
2. 路由器在收到数据包的时候因为CPU繁忙，没办法处理数据包，导致丢包
3. 在把数据包调度到队列的时候因为队列满而导致丢包
4. 数据包在链路上传输的时候因为链路故障、冲突等原因异致丢包
5. 丢包一般是因为延时造成的，在队列满的时候，一般采用尾丢弃丢包

Answer: A B C

解析：在很多时候，丢包一般是因为队列满造成的，在队列满的时候，一般采用尾丢弃来进行丢包。

1. QoS中，Integrated Service提供的不同于Best-Effort的服务类型是？ （请选择2个答案〉
2. 先进先出
3. 保证服务
4. 负载控制服务
5. 类似ISDN的服务

Answer: B C

解析：IntServ可以提供以下两种服务：保证服务，提供保证的带宽和时延限制来满足应用程序的要求；负载控制服务，保证即使在网络过载情况下，能对报文提供近似于网络未过载类似的服务。

1. 为什么说可以通过提高链路带宽容量来提高网络的QoS？ （请选择3个答案）
2. 链路带宽的增加可以支持更高的流量
3. 链路带宽的增加意味着更小的延迟和抖动
4. 链路带宽的增加减小了拥塞发生的几率，从而减少了丢包的数量
5. 链路带宽的增加可以增加控制协议的可用带宽

Answer: A B C

1. 以下关于QoS中Integrated Service服务模型的说法正确的是？ （请选择3个答案）
2. 传送QoS请求的信令是RSVP，它通知路由器应用程序的QoS需求
3. 它可以提供保证的带宽和时延限制来满足应用程序的要求
4. 它可以提供负载控制服务（Controlled-Load service），保证即使在网络过载（overload）的情况下，能对报文提供近似于网络未过载类似的服务，即在网络拥塞的情况下，保证某些应用程序的报文的低时延和高通过
5. 在这种模型下，网络将为每个流（由源和目的两端的IP地址、端口号）维护一个状态，并基于这个状态执行报文的分类、流量监管（policing）、排队及调度，来满足对应用程序的承诺

Answer: A B C

解析：D. 在这种模型下，网络将为每个流（由两端的IP地址、端口号）维护一个状态，并基于这个状态执行报文的分类、流量监管（policing）、排队及调度，来满足对应用程序的承诺。

1. QoS中，Differentiated Service与Integrated Service的主要区别是？ （请选择2个答案）
2. Differentiated Service里，去往不同目的地的分组获得的服务是不同的
3. Differentiated Service里，来自不同信源的分组获得的服务是不同的
4. 在Differentiated Service无须为每个流维护状态信息
5. Differentiated Service适合于在大型骨干网络上应用

Answer: C D

1. 判断：通常QoS中的Diff-Serv时，边界路由器通过报文的源地址和目的地址等对报文进行分类，对不同的报文设置不同的IP优先级，而其他路由器只需要用IP优先级来进行报文的分类。
2. True
3. False

Answer: A

1. 为了达到EF PHB的要求，定义的QoS机制不包括
2. 采用PQ队列调度机制保证EF包能够得到最快的调度，从而使EF包能够获得最小的延迟、抖动性能
3. 需要定义一种流量监管策略，给EF流量规定一定的带宽，在规定带宽范围内的流量可以获得低延迟的服务
4. 超过规定带宽的流量会被丢弃
5. 采用RTQ队列调度机制保证EF包能够得到最快的调度

Answer: D

1. 在Drtf-Serv网络中，定义EF类的业务类型的主要目的是
2. 为有低时延、低丢失、低抖动和确保带宽的优先业务提供业务保证
3. 为报文转发提供通道
4. 为特定流量确保带宽
5. 保证报文转发时尽可能低的时延

Answer: A

1. 判断：QoS技术中的简单流分类是指采用简单的规则，比如IP报文中的DSCP值、MPLS报文中的EXP值、Vlan报文头中的802.1p值对报文进行简单的分类。
2. True
3. False

Answer: A

解析：简单流分类是指采用简单的规则，如IP DSCP值，MPLS报文的EXP域值，VLan报文头中的802.1P值。

1. 判断：FIFO可以为不同的业务分配权重，对时延和抖动控制较好。
2. True
3. False

Answer: B

解析：FIFO为先入先出，无权重，对时延和抖动控制较差。

1. 判断：流量整形会对超过流量限制的报文进行缓存，在令牌桶的控制下载均匀地发送这些缓存的报文。
2. True
3. False

Answer: A

1. 判断：双桶单速流量监管是以CIR速率向令牌桶注入令牌，同时向CBS令牌桶和EBS令牌桶填充令牌。
2. True
3. False

Answer: B

解析：两个令牌桶以相同CIR速率注入令牌，CBS令牌桶满后，再向EBS注入令牌。