# 问答题常见问题汇总

### 一 RAID 2.0 的优势

1. 快速重构 ：所有硬盘参与重构，对比传统raid ，raid2.0不是对一个硬盘重复擦写
2. 负载均衡：各个硬盘均衡分担负载，降低硬盘的故障率
3. 自愈性：无需配置热备盘，硬盘发生故障，自行重构解决故障

### 二 堆叠的优缺点

优点：

1. 简化运维管理：只需在一台设备上进行配置（多虚拟 一）
2. 跨设备链路聚合：无需部署stp 防环 ，端口利用率100%
3. 避免单点故障：一台故障，其余转发

缺点：

1. 局限性：不同厂家设备不能进行堆叠
2. 成本高：需要专门的堆叠线缆
3. 资源浪费：多引擎经过堆叠后，只能有一个引擎工作

### 三 堆叠对比级联

堆叠：1. 可共享背板单宽

1. 只需配置一台设备
2. 必须用专用的堆叠线缆进行连接
3. 统一管理
4. 不同厂家设备不能进行堆叠

级联：1.不可共享背板带宽

1. 每台设备都是独立的，都需要配置
2. 无法统一管理所有设备
3. 不同厂家设备都可以级联
4. 无需购买单独的线缆，双绞线即可

### 四 堆叠对比vrrp （实现冗余性）

堆叠：1. 无环路：无需部署stp 防环

1. 端口利用率高： 100%
2. 配置简单：只需配置一台设备

Vrrp：

1.跨厂商：运行vrrp的设备可以是不通厂商的

1. 成本低：无需多台设备
2. 配置难：配置的量大，技术难度也高

### 五 静态路由与默认路由的区别

静态路由：

优点： 配置简单，手工配置，可控性高

缺点： 无法动态相应拓扑变化，不适用于大型网络拓扑，易出错s

默认路由：一种特殊的静态路由

优点： 配置更简单，减少路由条目，不占用 路由cpu内存

缺点： 不可控性，不精确

### 六 ospf 与rip区别 相同点 ：都是动态路由协议

Ospf：链路状态协议

Cost值：100m/接口带宽 （不足1 取 1）

遇到网络拓扑变化再进行更新路由表（ hallo报文 点到点网络 10s NBMA 30s）

适用多规模网络

快速收敛

无自环

区域划分

路由分为Dr bdr

反掩码

等等

Rip：距离矢量协议 （rip v1与v2的区别）

Cost值：跳数 最大 15跳

周期性更新（广播）整张路由表 计时器：30s hallo 180s dead 120 s 删表

易产生环路 （如何防环）

用于小型网络

等等

包括 配置宣告 地址方式不同 等等，自行补充

### 七 ipsan 和 fc san

Ip san ：支持带宽大 ，用于音视频 等对带宽要求大的业务

直连以太网交换机

fc san ： 小块数据，吞吐能力强 用于数据库

连接fc 交换机

### 八 冗余

1. 设备冗余：

双机热备、集群/堆叠、双引擎、双电源、双交换网板（高端的交换芯片）

1. 链路冗余：

链路聚合/端口聚合/M-LAG(跨链路的端口聚合)、STP/RSTP/MSTP、smart-link(毫秒级切换)、环网协议ERPS/RRPP/RPR/SEP、主备链路（ standby接口）、三层路由多链路负载均衡、出口多链路负载均衡

1. 网关冗余：

堆叠、VRRP

### 九 无线

两种模式：隧道模式 和 直接转发 对比

隧道模式：ac集中发放

优点：安全性高 网络稳定性高

缺点：报文转发效率慢 ac 压力大

直接转发 ：不经过ac

优点：报文转发效率高 ac压力小

缺点：网络稳定性相对较差 ，不能集中控制

### 十 Ipsec 配置

分为 manual 手动 跟 isakmp

简述：共5步

1 基本配置：网络通

1. acl兴趣流
2. 创建安全提议（手动：ipsec proposal 自动：ike proposal）
3. 配置安全策略（手动：ipsec policy 自动：ike 对等体）
4. 出口应用

### 十一 Wlan 配置

简述：

Ap上线：

1. 配管理模板
2. 配置 ap组
3. 配 capwap 隧道
4. Ap上线认证
5. 检查上线

Ac下发业务

1. 创建安全模板
2. 创建ssid 模板
3. 创建vap 模板
4. 进入ap组 绑定

### 十二 胖瘦ap

胖 ap ：具备数据转发和管理功能。能独立工作 需要单独配置

适用于小型网络

瘦 ap ：无法单独工作 ac集中统一管理

适用于大型网络

### 十三 无线信号优化的两种方式

1. 调整无线ap的发射功率 2.优化或更改无线ap的信道

### 十四 二层攻击 和三层以上攻击

二层 ： Mac-flooding stp arp 攻击

预防：

1.限制端口学习mac 的 地址数量

1. 对 mac 进行静态绑定

三层以上：udp- flooding tcp -flooding syn -flooding （ddos攻击）

预防：

1. 部署流量清洗设备
2. 购买流量清洗服务
3. 限制最大连接数
4. 购买抗ddos设备

### 十五 预防 apt 攻击

技术角度 ：

部署沙箱 ，姿态感知等

联动 防火墙，ips ，ids ，交换机等设备对流量 进行分析和监控

管理角度 ：

1. 制定网络安全管理制度
2. 明确网络安全主题任务
3. 细化网络安全工作职责
4. 合理分配人员的权限

### 十六 apt 攻击者 为了隐藏身份和攻击痕迹

### 使用的方式有哪里

隐藏身份 ：使用代理 肉鸡 跳板

攻击痕迹 ：清除攻击日志，使用隐蔽信道

### 十七 其他的病毒攻击与预防

sql攻击

预防:

1. 部署数据库审计
2. Waf防火墙设备
3. 对用户的输入严格检查

Xss攻击

预防：

1. 部署waf 防火墙设备
2. 限制用户输入的特殊字符

木马攻击

预防：

1. 安装杀毒软件
2. 定期漏洞扫描
3. 部署防火墙 ips ids 等安全设备

暴力破解

预防：

1. 设置密码复杂度
2. 限制用户尝试输入次数
3. 定期修改密码

### 十八 策略路由 和 路由策略

策略路由：

作用于数据层面，用于流控 （acl）

根据策略对数据包进行转发控制 （traffic-policy）

重点：针对源ip 网段

路由策略：

作用于控制层面，用于路由选择 （presence ，浮动路由-静态/默认路由+bfd）

根据策略对路由控制 （route-policy filter-policy）

重点：针对于路由出口