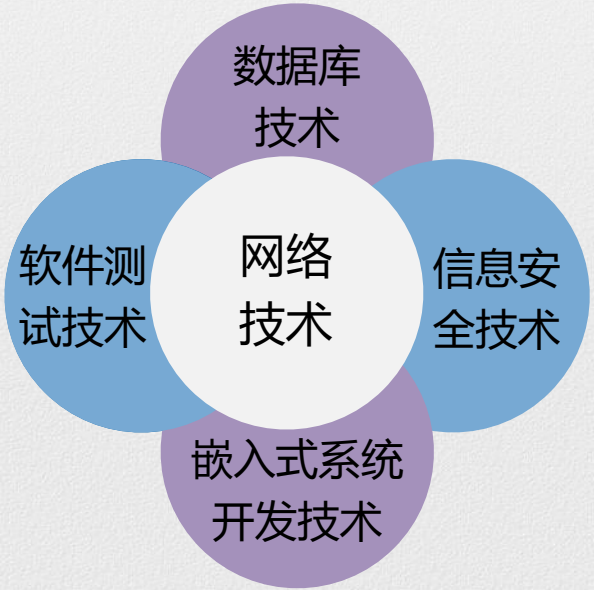
三级考试科目



三级网络技术考试人数众多，记忆、技巧性强，网上资源丰富，最适合无基础的同学选择的。

网络技术考试相关

考试时间

120分钟

时间绰绰有余，不用慌张

报名要求

不需要通过二级

报名者不受年龄、职业、学历等背景的限制，均可根据自己学习情况和实际能力选考相应的级别和科目。

无

题目来源

题库

刷题很有用

题目是从历年题库和新增题库中抽，有可能抽中原题

考试题型

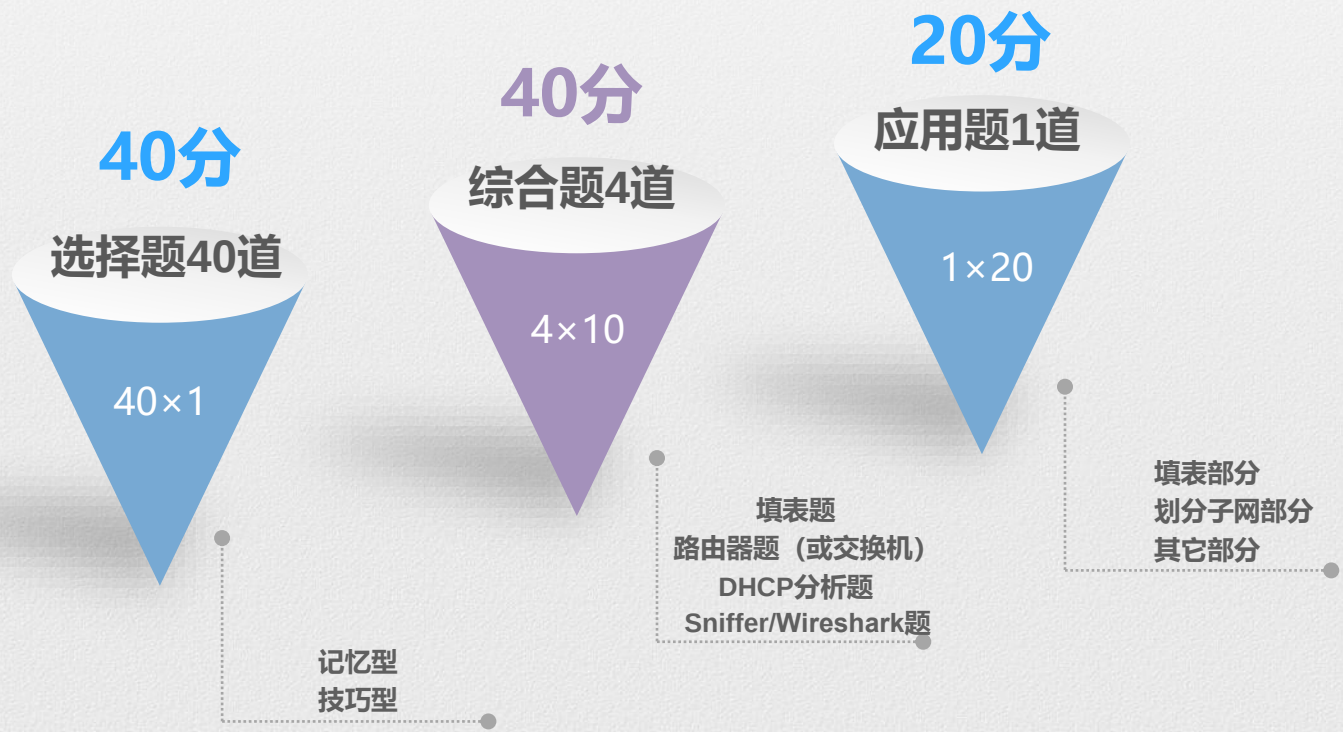
没有操作题！！

分为选择题、综合题、应用题。

综合题、应用题均是填空题

选填

考试题型


40分
选择题40道
40×1
记忆型
技巧型
40分
综合题4道
4×10
填表题
路由器题（或交换机）
DHCP分析题
Sniffer/Wireshark题
20分
应用题1道
1×20
填表部分
划分子网部分
其它部分

全国计算机等级考试三级网络技术考试大纲

1. 了解大型网络系统规划、管理方法。

2. 具备中小型网络系统规划、设计的基本能力。

3. 掌握中小型网络系统组建、设备配置调试的基本技术。

4. 掌握企事业单位中小型网络系统现场维护与管理基本技术。

5. 了解网络技术的发展。

考试内容

一、网络规划与设计

1. 网络需求分析。
2. 网络规划设计。
3. 网络设备及选型。
4. 网络综合布线方案设计。
5. 接入技术及案设计。
6. IP 地址规划与路由设计。
7. 网络系统安全设计。

二、网络构建

1. 局域网组网技术。
(1)网线制作方法。
(2)交换机配置与使用方法。
(3)交换机端口的基本配置。
(4)交换机 VLAN 配置。
(5)交换机 STP 配置。
2. 路由器配置与使用。
(1)路由器基本操作与配置方法。
(2)路由器接口配置。
(3)路由器静态路由配置。
(4) RIP 动态路由配置。
(5) OSPF 动态路由配置。
3. 路由器高级功能。
(1)设置路由器为 DHCP 服务器。
(2)访问控制列表的配置。
(3)配置 GRE 协议。
(4)配置 IPSec 协议。
(5)配置 MPLS 协议。
4. 无线网络设备安装与调试。

三、网络环境与应用系统的安装调试

1. 网络环境配置。
2. WWW 服务器安装调试。
3. E – mail 服务器安装调试。
4. FTP 服务器安装调试。
5. DNS 服务器安装调试。

四、网络安全技术与网络管理

1. 网络安全。
(1)网络防病毒软件与防火墙的安装与使用。
(2)网站系统管理与维护。
(3)网络攻击防护与漏洞查找。
(4)网络数据备份与恢复设备的安装与使用。
(5)其他网络安全软件的安装与使用。
2. 网络管理。
(1)管理与维护网络用户账户。
(2)利用工具软件监控和管理网络系统。
(3)查找与排除网络设备故障。
(4)常用网络管理软件的安装与使用。

五、上机操作(选填)

在仿真网络环境下完成以下考核内容:

1. 交换机配置与使用。

2. 路由器基本操作与配置方法。

3. 网络环境与应用系统安装调试的基本方法。

4. 网络管理与安全设备、软件安装、调试的基本方法。

考试方法

上机考试,考试时长 120 分钟,满分 100 分。

1. 题型及分值

单项选择题 40 分、综合题 40 分、应用题 20 分。

2. 考试环境

中文版Windows。

三级网络技术选择题必背知识点

目录

BGP（边界网关协议）.....1
集线器.....2
OSPF协议.....3
攻击.....4
IPS（入侵防护系统）.....5
RPR（弹性分组环）.....6
路由器技术.....7
城域网.....8
接入技术.....10
蓝牙.....11
布线.....12
服务器技术.....14
DNS 服务器.....15
WWW 服务器.....16
FTP 服务器.....18
邮件（Winmail 邮件服务器）.....20
生成树协议.....22
IEEE.....23
VLAN 标识的描述.....25
DHCP服务器.....27

标题(不含括号里的内容)即为“试题搜索”的关键词

考频说明

10 以下	低频
10~20	中频
20~30	高频
30 以上	必考

每天点击一下公众号内的广告，就是对我的支持哟~

高频：约出现24 次

BGP（边界网关协议）

1. BGP 是边界网关协议，是外部而不是内部网关协议(是不同自治系统(AS)的路由器之间使用的协议)。
2. 一个 BGP 发言人使用 TCP（不是 UDP）与其他自治系统的 BGP 发言人交换路由信息。
3. BGP 协议交换路由信息的节点数是以自治系统数为单位的，BGP 交换路由信息的节点数不小于自治系统数。
4. BGP 采用路由向量协议，而RIP采用距离向量协议。
5. BGP 发言人通过 update 而不是 noticfication 分组通知相邻系统，使用 update 分组更新路由时，一个报文只能增加一条路由。
6. open 分组用来与相邻的另一个 BGP 发言人建立关系，两个 BGP 发言人需要周期性地（不是不定期）交换 keepalive 分组来确认双方的相邻关系。
7. BGP 路由选择协议执行中使用的四个分组为**打开(open)、更新(update)、保活(keepalive)**和**通知(notification)**分组。

路由协议	IGP（内部网关协议）	RIP（路由信息协议）——距离向量协议
		OSPF（开放最短路径优先协议）——分布式链路状态协议
		IS-IS（中间系统到中间系统）
		IGRP（内部网关路由协议）
	EGP（外部网关协议）	BGP（边界网关协议）——路由向量协议

查看BGP相关题目戳这里

高频 21 次

集线器

1. 工作在物理层，连接到一个集线器的所有结点共享/属于（不是独立）一个冲突域。
2. 每次只有一个结点能够发送数据，而其他的结点都处于接收数据的状态（多个节点可以同时接受数据帧）。连接到集线器的节点发送数据时，该节点将执行 CSMA/CD（不是 CA）介质访问控制方法。
3. 在网络链路中串接一个集线器可以监听该链路中的数据包。
4. 集线器不是基于 MAC 地址/网卡地址/IP 地址完成数据转发（基于 MAC 地址的是网桥或交换机等），而是信源结点利用一对发送线将数据通过集线器内部的总线广播出去。
5. 集线器使用双绞线连接工作站。
6. 使用 Sniffer 在网络设备的一个端口上能够捕捉到与之属于同一 VLAN 的不同端口的所有通信流量的设备是集线器。

查看集线器相关题目戳这

高频 21 次

OSPF 协议

1. OSPF 是内部网关协议的一种，采用最短路径算法，使用分布式链路状态协议。
2. 对于规模很大的网络，OSPF 通过划分区域来提高路由更新收敛速度。每个区域有一个 32 位的区域标识符，区域内路由器不超过 200 个。
3. 一个 OSPF 区域内每个路由器的链路状态数据库包含着本区域(不是全网)的拓扑结构信息，不知道其他区域的网络拓扑。
4. 链路状态“度量”主要指费用、距离、延时、带宽等，没有路径。
5. 当链路状态发生变化时用洪泛法向所有(不是相邻)路由器发送此信息。
6. 链路状态数据库中保存的是全网的拓扑结构图，而非一个完整的路由表，也不是只保存下一跳路由器的数据。
7. 为确保链路状态数据库一致，OSPF 每隔一段时间（不确定）刷新一次数据库中的链路状态

查看OSPF相关题目戳这

必考 30 次

攻击

1. SYN Flooding 攻击：使用无效的 IP 地址，利用 TCP 连接的三次握手过程，使得受害主机处于开放会话的请求之中，直至连接超时。在此期间，受害主机将会连续接受这种会话请求,最终因耗尽资源而停止响应。
2. DDos 攻击：利用攻破的多个系统发送大量请求去集中攻击其他目标，受害设备因为无法处理而拒绝服务。
3. SQL 注入攻击：属于利用系统漏洞，基于网络的入侵防护系统和基于主机入侵防护系统都难以阻断。防火墙（基于网络的防护系统）无法阻断这种攻击。
4. Land 攻击：向某个设备发送数据包，并将数据包的源 IP 地址和目的地址都设置成攻击目标的地址。
5. 协议欺骗攻击：通过伪造某台主机的 IP 地址窃取特权的攻击。有以下几种：（1）IP 欺骗攻击。（2）ARP 欺骗攻击。（3）DNS 欺骗攻击。（4）源路由欺骗攻击。
6. DNS 欺骗攻击：攻击者采用某种欺骗手段，使用户查询服务器进行域名解析时获得一个错误的 IP 地址，从而可将用户引导到错误的 Internet 站点。
7. IP 欺骗攻击：通过伪造某台主机的 IP 地址骗取特权，进而进行攻击的技术。
8. Cookie 篡改攻击：通过对 Cookie 的篡改可以实现非法访问

目标站点，基于网络的入侵防护系统无法阻断。

9. Smurf 攻击：攻击者冒充受害主机的 IP 地址，向一个大的网络发送 echo request 的定向广播包，此网络的许多主机都做出回应，受害主机会收到大龄的 echo reply 消息。基于网络的入侵防护系统可以阻断 Smurf 攻击。
10. 基于网络的防护系统无法阻断 Cookie 篡改、DNS 欺骗、SQL 注入。
11. 基于网络的入侵防护系统和基于主机入侵防护系统都难以阻断的是跨站脚本攻击、SQL 注入攻击。

查看网络攻击相关题目戳这

中频 12 次

IPS（入侵防护系统）

1. 入侵防护系统(IPS)整合了防火墙技术和入侵检测技术，工作在 In-Line（内联）模式，具备嗅探功能。
2. IPS 主要分为基于主机的 IPS(HIPS)、基于网络的 IPS(NIPS)和应用 IPS(AIPS)。
3. HIPS 部署于受保护的主机系统中，可以监视内核的系统调用，阻挡攻击。
4. NIPS 布置于网络出口处，一般串联于防火墙与路由器之间（串接在被保护的链路中）。NIPS 对攻击的误报（不是漏报）会导致合法的通信被阻断。
5. AIPS 一般部署在受保护的应用服务器前端。

查看IPS相关题目戳这

高频 20 次

RPR（弹性分组环）

1. RPR 与 FDDI 一样使用双环结构。
2. RPR 环中每一个节点都执行 SRP 公平算法（不是 DPT、MPLS）。
3. 传统的 FDDI 环，当源结点向目的节点成功发送一个数据帧之后，这个数据帧由源结点从环中回收。但 RPR 环，这个数据帧由目的结点从环中回收。
4. RPR 环限制数据帧只在源节点和目的节点之间的光纤段上传输。
5. RPR 采用自愈环设计思路，能在 50ms（不是 30ms）时间内隔离故障结点和光纤段。
6. RPR 可以对不同的业务数据分配不同的优先级，是一种用于直接在光纤上高效传输 IP 分组的传输技术。
7. 两个 RPR 结点间的裸光纤最大长度可达 100 公里。
8. RPR 的外环（顺时针）和内环（逆时针）都可以用统计复用的方法传输分组和控制分组（不是频分复用）。

查看RPR相关题目戳这

中频 15 次

路由器技术

1. 路由器的包转发能力与端口数量、端口速率、包长度和包类型有关。（没有端口类型）
2. 高性能路由器一般采用采用可交换式的结构，传统的核心路由器采用共字背板的结构。
3. 丢包率是衡量路由器超负荷工作时的性能指标之一。（“路由表容量”不是）
4. 吞吐量是指路由器的包转发能力，包括端口吞吐量与整机吞吐量。背板能力决定路由器吞吐量。（不是吞吐量决定了路由器的背板能力）
5. 突发处理能力是以最小帧间隔发送数据包而不引起丢失的最大发送速率来衡量的，不单单是以最小帧间隔值来衡量的。
6. 语音视频业务对延时抖动要求较高。
7. 路由器的服务质量主要表现在队列管理机制、端口硬件队列管理和支持的 QoS协议类型上。(不是包转发效率)
8. 路由器通过路由表来决定包转发路径。
9. 路由器的队列管理机制是指路由器的队列调度算法和拥塞管理机制。

查看路由器技术相关题目戳这

高频 25 次

城域网

1. 宽带城域网保证服务质量 QoS 要求的技术有：资源预留(RSVP)、区分服务(DiffServ)与多协议标记交换(MPLS)。网络服务质量表现在延时、抖动、吞吐量与丢包率。
2. 宽带城域网以 TCP/IP 路由协议为基础。能够为用户提供带宽保证，实现流量工程。
3. 可以利用 NAT 技术解决 IP 地址资源不足的问题。
4. 利用传统的电信网络进行网络管理称为“带内”，而利用 IP 网络及协议进行网络管理的则称为“带外”。对汇聚层及其以上设备采取带外管理，而对汇聚层以下采用带内管理。
5. 宽带城域网带外网络管理是指利用网络管理协议 SNMP 建立网络管理系统。
6. 网络业务包括 Internet 接入业务、内容提供业务、视频与多媒体业务、数据专线业务、语音业务等。
7. 设计一个宽带城域网将涉及“三个平台一个出口”，即网络平台、业务平台、管理平台和城市宽带出口。
8. 核心交换层的基本功能：

①核心交换层将多个汇聚层连接起来，为汇聚层的网络提供高速分组转发，为整个城市提供一个高速、安全与具有 QoS 保障能力的数据传输环境。

②核心交换层实现与主干网络的互联，提供城市的宽带 IP

出口。

③核心交换层提供宽带城域网的用户访问 Internet 所需要的路由访问。

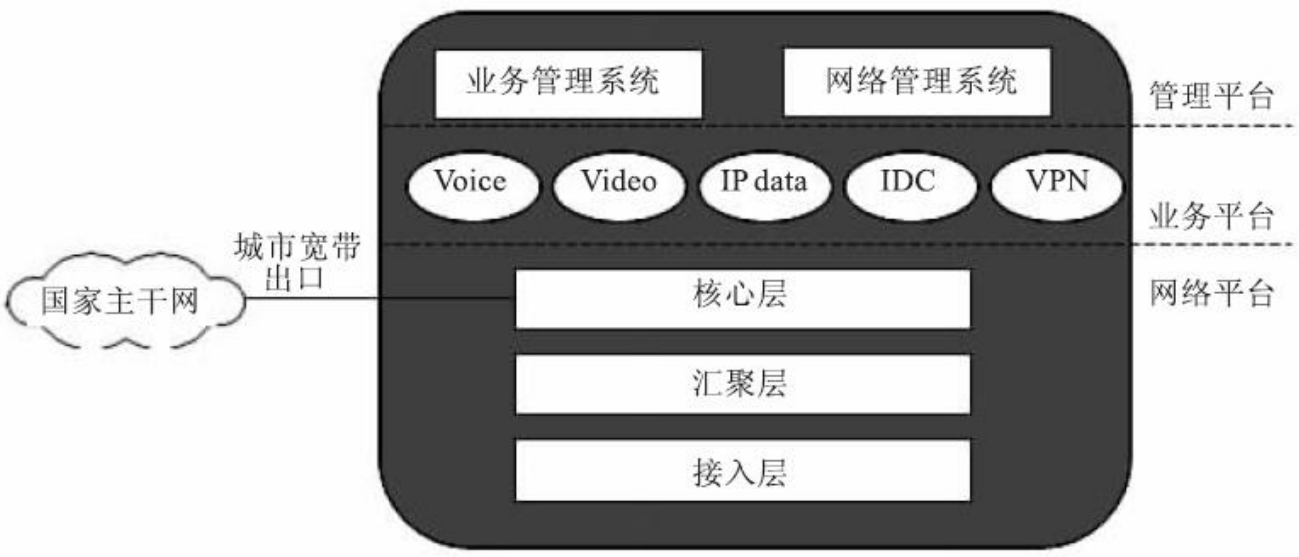
9. 汇聚层的基本功能是：

①汇接接入层的用户流量，进行数据分组传输的汇聚、转发与交换。

②根据接入层的用户流量，进行本地路由、过滤、流量均衡、QoS 优先级管理，以及安全控制、IP 地址转换、流量整行等处理。

③根据处理结果把用户流量转发到核心交换层或在本地进行路由处理。

查看城域网相关题目戳这



宽带城域网的总体结构

高频 26 次

接入技术

1. 光纤传输系统的中继距离可达 100km 以上。
2. Cable Modom（电缆调制解调器）利用频分复用(FDM)的方法将信道分为上行信道和下行信道，把用户计算机与有线电视同轴电缆连接起来。Cable Modem 的传输速率可以达到 10～36Mbps。
3. ASDL 使用一对铜双绞线，具有非对称技术特性。
4. 宽带接入技术主要有：数字用户线 xDSL 技术、光纤同轴电缆混合网 HFC 技术、光纤接入技术、无线接入技术与局域网接入技术。（没有 SDH）
5. 无线接入技术主要有：WLAN、WiMAX、WiFi、WMAN 和 Ad hoc 等。
6. APON、DWDM、EPON 是光纤接入技术。
7. “三网融合”中的三网是指计算机网络、电信通信网和广播电视网。
8. HFC 接入方式采用共享式的传输方式 HFC 网上的用户越多，每个用户实际可用的带宽就越窄。（非独享）
9. 按 IEEE 802.16 标准建立的无线网络，基站之间采用全双工、宽带通信方式工作。
10. 将传输速率提高到 54Mbps 的是 802.11a 和 802.11g，802.11b 将传输速度提高到 11Mbps。

11. 远距离无线宽带接入网采用 802.16 标准。IEEE 802.15 标准专门从事 WPAN(无线个人局域网)标准化工作，是适用于短程无线通信的标准。

查看接入技术相关题目戳这

低频 9 次

蓝牙

1. 工作频段在 2.402GHz~2.480GHz 的ISM 频段。
2. 同步信道速率 64kbps。
3. 跳频速率为 1600 次/秒，频点数是 79 个频点/MHz。
4. 非对称的异步信道速率为 723.2kbps/57.6kbps，对称的异步信道速率为 433.9kbps（全双工）。
5. 发射功率为 0dBm(1mW)时，覆盖 1～10 米，20dBm(100mW)时覆盖 100 米。
6. 信道间隔为 1MHz。
7. 标称数据速率是 1Mbps。
8. 话音编码方式为 CVSD 或对数 PCM。

查看蓝牙相关题目戳这

必考 34 次

布线

1. 双绞线可以避免电磁干扰。
2. 嵌入式插座用来连接双绞线。（不是连接楼层配线架）
3. 多介质插座用来连接**铜缆**和**光纤**（写其他的错），满足用户“光纤到桌面”的需求。
4. 建筑群子系统可以是多种布线方式的任意组合（“一般用双绞线连接”错）。
5. STP比UTP 成本高、复杂，但抗干扰能力强、辐射小。
6. 作为水平布线系统电缆时，UTP 电缆长度通常应该在 90 米以内。
7. 管理子系统设置在楼层配线间内，提供与其他子系统连接的手段。
8. 对于高速率终端可采用光纤直接到桌面的方案。
9. 适配器是用于连接不同信号的数模转换或数据速率转换装置。
10. 在建筑群布线子系统所采用的铺设方式中，能够对线缆保护**最有利**的方式是地下管道布线（管道内布线），**较好**的是巷道布线，**最不利**的是直埋布线。
11. ISO/IEC 18011 不是综合布线系统的标准。
12. 综合布线采用在管理子系统中更改、增加、交换、扩展线缆的方式来改变线缆路由。

13. 干线线缆铺设经常采用点对点结合和分支结合两种方式。

查看布线相关题目戳这

四种布线方式	
巷道布线法	利用建筑物之间的地下巷道铺设电缆，不仅造价低而且还可以利用原有的安全设施给线缆提供保护。由于地下巷道存在热水管道，因此可能会把电缆烫伤。
架空布线法	利用原有的电线杆布线，这种布线方法成本较低，但是保密性、安全性和灵活性较差。
直埋布线法	该方法除了穿过基础墙部分电缆外，电缆的其余部分都没有管道保护，容易受到破坏。
管道内布线法 （地下管道布线）	由管道和入孔组成的地下系统，用来对网络内的各建筑物进行互联。由于管道是由耐腐蚀材料做成的，所以这种方法对电缆提供了最好的机械保护，使电缆受到维修的机会减到最小程度。

中频 11 次

服务器技术

1. 热插拔功能允许用户在不切断电源的情况下更换**硬盘、板卡、电源**等（不能更换主板、主背板）。
2. 集群技术中，如果一台主机出现故障，不会影响正常服务，但会影响系统性能。
3. 磁盘性能表现在储存容量和 I/O 速度。
4. 服务器总体性能取决于 CPU 数量、CPU 主频、系统内存、网络速度(只写 CPU 数量错)。
5. RAID 技术可以提磁盘存储容量但是不能提高容错能力。
6. 采用 RISC 结构处理器的服务器通常使用 UNIX 系统(不是 Windows、Android)。
7. 分布式内存访问（NUMA）技术将对称多处理器（SMP）和集群（Cluster）技术结合起来。
8. 对称多处理技术可以在多 CPU 结构的服务器中均衡负载。
9. 通常用平均无故障时间（MTBF）来度量系统的**可靠性**，用平均维修时间（MTBR）来度量系统的**可维护性**，**系统的可用性**定义为：可用性=MTBF/(MTBF+MTBR)，**路由器的可用性**可用 MTBF 描述。

查看服务器技术相关题目戳这

中频 19 次

DNS 服务器

适合题型样式:下列关于 Windows 2003 系统 DNS 服务器的描述中,正确的是

1. 动态更新允许客户机在发生更改时动态更新其资源记录。
2. DNS 服务器中的根服务器被**自动**加入到系统中，不需管理员手工配置。
3. 主机记录的生存时间（TTL）指该记录被客户端查询到，放在**缓存**中的持续时间。
4. DNS 服务器配置的主要参数（1）正向查找域（2）反向查找域（3）资源记录（4）转发器
5. 转发器是网络上的 DNS 服务器（不是路由器），用于外域名的 DNS 查询（用于将外部域名的 DNS 查询转发给该 DNS 服务器）。
6. 反向查找区域用于将 IP 地址解析为域名，在反向查找区域中可以**手工**增加主机的指针记录。
7. 正向查找区域用于将域名解析为 IP 地址，正向查找区域**自动**增加主机的指针记录。
8. DNS 服务器的 IP 地址不是由 DHCP 服务器动态分配的，其 IP 地址应该是静态设置的固定地址。
9. DNS 服务器中常用的资源记录包括：主机地址资源记录；邮件交换器资源记录；别名资源记录（没有 FTP 服务器记录）。别名资源记录用于将别名映射到标准 DNS 域名。

10. 缺省情况下,Windows 2003 系统中**未安装** DNS 服务。
11. DNS 服务器按层次分为 **3 类**服务器：根 DNS 服务器、顶级域(TLD)服务器、权威 DNS 服务器。
12. 命令：ipconfig 显示当前 TCP/IP 网络配置；netstat 显示本机与远程计算机的基于 TCP/IP 的 NeTBIOS 的统计及连接信息；pathping 将报文发送到所经过地所有路由器，并根据每一跳返回的报文进行统计；route 显示或修改本地 IP 路由表条目；使用 nslookup 命令可以测试正向和反向查找区域；使用 ping 命令可以测试正向查找区域。

查看DNS服务器相关题目戳这

高频 20 次

WWW 服务器

适合题型样式:下列关于 Windows 2003 系统下 WWW 服务器配置的描述中，正确的是

1. Web 站点可以配置**静态**和**动态** IP 地址。
2. 建立 Web 站点时必须为该站点指定一个**主目录**（不一定在本地计算机/服务器），也可以是**虚拟的子目录**。
3. 设置 Web 站点时，不是设置网站的默认文档后才能被访问。设置了默认页面，访问时才会直接(自动)打开 default.html 等设置的默认页面。如果没有设置默认内容文档，访问站点时需要提供首页内容的文件名。
4. 访问 Web 站点时可以使用站点的域名或站点的 IP 地址。

5. 性能选项包括影响带宽使用的属性、客户端 Web 连接的数量(不包括超时时间)。网站性能选项中，**带宽限制选项**限制该网站的可使用带宽；**网站连接选项**可设置客户端 Web 连接数量。
6. 主目录选项卡中，可配置主目录的读取和写入等权限，可设置用于存放网页的文件路径。
7. 目录安全选项卡可以选择配置身份验证和访问控制、IP 地址和域名限制、安全通信三种方法。（不可配置主目录的访问权限）
8. 网站选项包括网站的标识、设置站点的连接限制、网站连接的超时时间以及启用日志记录并配置站点的日志记录格式。

   网站的**连接超时选项**是指 HTTP 连接的保持时间。

   网站的**带宽选项**能限制该网站可使用的网络带宽。
9. 作为网络标识的有 IP 地址、非 TCP 端口号、主机头、网站描述。(没有主目录)
10. 在 Windows2003 中添加操作系统组件 IIS 就可实现 Web 服务，建立 Web 站点前必须安装。
11. Web 站点可以动态获取 IP 地址。在一台服务器上可构建**多个**网站。
12. 缺省情况下 Windows2003 系统没有安装 DNS 服务。

查看WWW服务器相关题目戳这

高频 25 次

FTP 服务器

适合题型样式:以下关于 Serv_U FTP 服务器配置的描述中，正确的是

1. 初始状态下没有设置管理员密码，可以直接进入 Serv-U 管理程序。
2. FTP 服务器缺省端口号为 21，但是有时因为某种原因则不能使用 21 号端口，但可以选择其他合适的端口号。
3. FTP 服务器可以使用动态 IP 地址，使用动态 IP 地址时，服务器 IP 地址应配置**为空**，为空代表全部 IP 地址，服务器有多个 IP 地址时，IP 地址为空比较方便（不需分别添加，空不是 0.0.0.0）。
4. 服务器可构建多个由 IP 地址和端口号识别的虚拟服务器，每个虚拟服务器（域）**由 IP 地址和端口号唯一识别**，而不是只依靠 IP 地址。
5. 向服务器中添加“anonymous”，系统自动判定为匿名用户。而不是创建新域时**自动**添加一个“anonymous”匿名。
6. 服务器最大用户数是指服务器允许同时在线的最大用户数量。
7. 用户上传下载选项要求 FTP 客户端在下载信息的同时也要上传文件。（不是配置用户的上传和下载的速率）
8. 服务器选项不提供“IP 访问选项”。用户常规选项中不包含“用户主目录”。
9. 配置域存储位置时，小的域应选择 INI 文件存储而大的域应

选择注册表存储。

10. 配置服务器域名时，可以使用域名或其它描述。（不是必须使用该服务器的域名，不必是合格的域名）
11. 需要拥有**管理员**操作权限的用户，才能在 Serv-U FTP 服务器中注册用户。（用户**不可**在服务器中自行注册新用户）
12. FTP 服务器的域创建完成后需要添加用户，才能被客户端访问。用户包括**匿名用户**和**命名用户**。添加匿名用户时用户名必须为"anonymous"，如果添加的是匿名用户，系统将不会要求输入密码。
13. Serv-U 中可以限制用户名上传信息占用存储空间的选项是用户配额选项。
14. 服务器可构建多个由 IP 地址和端口号识别的虚拟服务器。
15. Serv-U FTP 服务器最大上传或下载速度是指整个服务器占用的带宽。
16. 选择拦截“FTP BOUNCE”和 FXP 后，则不允许在两个 FTP 服务器间传输文件
17. 对用户数大于 500 的域，将域存放在注册表中可提供更高的性能。
18. 访问 FTP 服务器除了可以使用专用的客户端外，如 cuteFTP，还可以使用浏览器。
19. 检查匿名用户密码选项是指使用匿名用户登录时需用电子邮件地址作为登录密码。

必考 30 次

邮件（Winmail 邮件服务器）

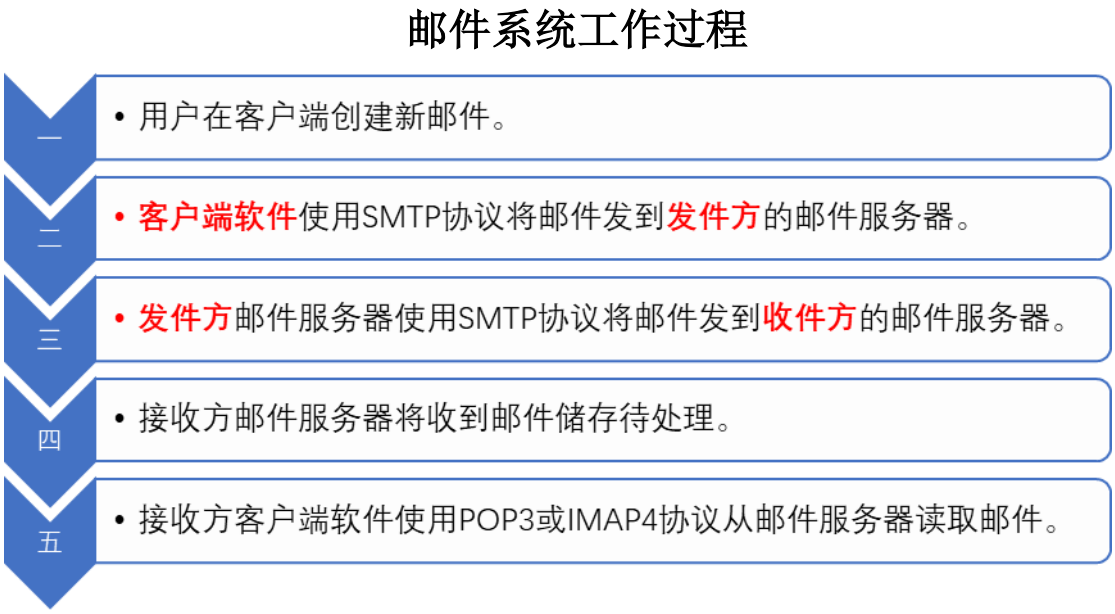
适合题型样式：下列关于 Winmail 邮件服务器的描述中，正确的是

1. Winmail 邮件服务器支持基于 Web 方式的访问和管理，因此在安装邮件服务器软件之前要安装 IIS。
2. Winmail 邮件服务器允许用户自行注册新邮箱，需输入邮箱名、密码等信息，而域名是服务器固定的，并不能自行设置。但 Winmail 用户不可以使用 Outlook 自行注册新邮箱。
3. 在 Winmail 快速设置向导（不是系统设置）中创建新用户时，输入新建用户的信息，包括用户名、域名及用户密码（不是系统邮箱的密码、管理员密码），可选择是否允许客户通过 Winmail 注册新邮箱。
4. 建立邮件路由时，需在 DNS 服务器中建立该**邮件服务器主机记录**和**邮件交换器记录**（缺一不可）。
5. 发送邮件时通常采用 **SMTP 协议**，接收/读取邮件时通常采用 **POP3** 或者 **IMAP 协议**。Winmail 用户使用浏览器查看邮件会使用到 **HTTP 协议**。CMIP 不属于电子邮件系统协议。
6. 邮件交换器记录的配置只能在服务器上，不能通过浏览器配置。
7. 管理工具包括系统设置、域名设置、用户和组设置、系统状态和系统日志等项目。（不包含邮件管理）
8. 在域名设置中（不是系统设置），可以增加新的域，用于构

建**虚拟邮件服务器**、删除已有的域。域名设置是可设置 Winmail 邮件服务器是否允许自行注册新用户的选项。

9. 系统设置包括 SMTP 设置、邮件过滤、更改管理员密码等。（没有域名设置）。
10. 使用 Outlook 等客户端软件只能访问 Winmail 邮件服务器，**不能管理** Winmail 邮件服务器。

查看邮件相关题目截这



中频 15 次

生成树协议

适合题型样式:下列对生成树协议 STP 的描述中，正确的是

1. IEEE 制定的最早的 STP 标准是 EEE802.1D。IEEE 802.1d 是当前流行的 STP(生成树协议)标准。透明网桥标准 STP 定义在 IEEE 802.1d 标准中。
2. 在交换机之间传递网桥协议数据单元 BPDU,其数据包有两种类型:一种是包含配置信息的配置 BPDU(不超过/小于 35 个字节)，另一种是包含拓扑变化信息的拓扑变化通知 BPDU(不超过/小于 4 个字节)。
3. STP 在交换机之间传递 BPDU 数据包，默认每 2 秒定时发送一次。在网络发生故障或拓扑结构产生变化时也发送新的 BPDU。
4. 阻塞的端口仍然是一个激活端口，但它只能接收 BPDU。
5. 生成树协议是一个二层链路管理协议。
6. STP 运行在交换机和网桥设备上（不是运行在路由器上），它通过计算建立一个稳定的树状结构网络。
7. Bridge ID 用 8 个字节表示，由 2 个字节的优先级值和 6 个字节的交换机 MAC 地址组成。优先级值的增值量是 4096。优先级的取值范围是 0-61440，一般默认值为 32768。
8. Bridge ID 值最小的成为根网桥或根交换机。

查看生成树协议相关题目戳这

必考 31 次

IEEE

适合题型样式:下列关于 IEEE XXX 协议的描述中，正确的是

1. IEEE 802.11 的三个物理层定义包括了两个扩频技术（FHSS、DSSS）和一个红外传播规范。
2. 802.11 无线传输频道定义在 2.4GHz ISM 频段，定义的传输速率是 1Mbps 和 2Mbps。
3. IEEE802.11 在 MAC 子层引入了一个 RTS/CTS 选项。
4. 802.11 定义了两种类型的设备：无线结点和无线接入点。
5. 无线接入点 AP 的作用是提供无线和有线网络之间的桥接，而非无线结点。
6. IEEE 802.11 的运作模式分为点对点模式和基本模式。
7. 点对点模式是指无线网卡和无线网卡之间的通信方式。它最多可以允许 256 台 PC 连接。
8. 基本模式是指无线网络规模扩充或无线和有线网络并存时的通信方式。接入点负责频段管理及漫游等指挥工作，一个接入点最多可连接 1024 台 PC。
9. 802.11b 最大容量 33 Mbps，将传输速率提高到 11Mbps，802.11a 和802.11g 将传输速率提高到54Mbps。
10. IEEE 802.11b 标准使用的是开放的 2.4GHZ 频段，无须申请就可以直接使用。
11. IEEE 802.1d 是当前最流行的 STP（生成树协议）标准。

12. 802.11 标准的重点在于解决局域网范围的移动结点通信问题，802.16 标准的重点是解决建筑物之间的数据通信问题，802.16a 增加了非视距和对无线网格网结构的支持，用于固定结点接入。
13. IEEE802.11 运行在 2.4GHz ISM 频段，最大传输速率是 1~2Mbps；
14. IEEE802.11b 运行在 2.4GHz ISM 频段，最大传输速率是 11Mbps，最大容量是 33Mbps；
15. IEEE802.11a 运行在 5GHz UNII 频段，最大传输速率是 54Mbps，最大容量是 432Mbps；
16. IEEE802.11g 运行在 2.4GHz ISM 频段，最大传输速率是 54Mbps,实际吞吐量是 28~31Mbps,最大容量是 162Mbps。

查看IEEE相关题目戳这

IEEE 802.16 系列主要标准的基本情况及比较

协议标准	使用频段	信道条件	固定/移动	信道带宽/MHz	传输速度/Mbit/s	额定小区半径/km
IEEE 802.16	10～66GHz	视距	固定	25/28	32～134	<5
IEEE 802.16a	<11GHz	非视距	固定	1.25/20	75	5～10
IEEE 802.16d-2004	10～66GHz <11GHz	视距＋非视距	固定	1.25/20	75	5～15
IEEE 802.16e-2005	<6GHz	非视距	固定 移动＋漫游	1.25/20	30	若干

IEEE 802.11a、IEEE 802.11b、IEEE 802.11g 3 种协议的特性比较

协议种类	Wi-Fi 联盟认证	实际吞吐量	最大数据传输率	最大容量	室内距离	与 IEEE 802.11b 的后向兼容性	与其他设备之间的干扰
IEEE 802.11b	是	5～7Mbit/s	11Mbit/s	33Mbit/s（3 信道×11）	100m	是 在 2.4GHz ISM 频段上运行	是 如无线电话，微波炉，蓝牙
IEEE 802.11a	是	28～31Mbit/s	54Mbit/s	432Mbit/s（8 信道×54）	与 IEEE 802.11b 和 IEEE 802.11g 比，在 30m 内速度更快	否 在 5GHz 的频段上运动	否
IEEE 802.11g	否	28～31Mbit/s（纯 IEEE 802.11g 环境） 10～12Mbit/s（与 IEEE 802.11b 客户端混合）	54Mbit/s	162Mbit/s（3 信道×54）	与 IEEE 802.11b 相比，在 30m 内速度更快	是 在 2.4GHz ISM 频段上运行 （注意：总吞吐量在 IEEE 802.11b 和 IEEE 802.11g 混合网中会降低）	是 如无线电话，蓝牙，微波炉

中频 15 次

VLAN 标识的描述

适合题型样式：下列对 VLAN 标识的描述中，正确的是

1. VLAN 工作在 OSI 参考模型的第二层(数据链路层)，而不是网络层。VLAN 之间通信必须通过路由器。
2. VLAN 以交换式网络为基础。
3. 建立不给定名字的 VLAN，系统自动按缺省的 VLAN 名(VLANOOxxx)建立，“xxx”是 VLAN ID。
4. IEEE802.1Q 标准规定，用于标识 VLAN 的 VLAN ID 用 12bit（位、比特）表示。

5. 每个 VLAN 都是一个独立的逻辑网络、单一的广播域。
6. 按每个连接到交换机设备的 MAC 地址定义 VLAN 成员是种动态 VLAN。
7. VLAN 的划分不受用户所在的物理位置和物理网段的限制，也不受实际交换机区段的限制。
8. VLAN ID 标准范围是 1~1005,扩展范围是 1025~4096。
9. 在 VLAN ID 标准范围内，可用于 Ethemet 的 VLAN ID 为 2~1000。
10. VLAN 使用一个 VLAN 名(VLAN name)和 VLAN 号(VLAN ID)来标识的。VLAN 名用 1~32 个字符表示，它可以是字母和数字。
11. ID 为 1 的 VLAN 是系统默认 VLAN，通常用于设备管理，用户只能使用这个 VLAN，但不能执行删除操作，即**无法执行"no vlan 1"命令**。2~1000 用于 Ethenet VLANs，可以建立、使用和删除这些 VLAN。1002~1005 是预留给 FDDI 和 Token Ring VLANs 使用的，1025~4094 是扩展的 VLAN ID，其他为保留 ID 号。

查看VLAN相关题目戳这

中频 22 次

DHCP 服务器

（1）作用域

1. 作用城是用于网络的可能 IP 地址的完整**连续**范围（**并不负责 IP 地址分配**），定义了作用域并应用排除范围之后，**必须激活**才可为客户机分配地址，剩余的地址在作用域内形成可用的“**地址池**”。
2. 服务器**可为多个网段分配 IP 地址**，多个网段 IP 地址，则需要配置**多个作用域**、地址池。
3. 在 DHCP 服务器中新建作用域时，在租约期限中不可调整的时间单位是**周**。
4. 作用域配置信息有作用域 IP 地址范围、作用域名称、保留、排除。（无 DHCP 服务器地址）
5. **新建作用域**时，必须输入的信息是**起始 IP 地址和结束 IP 地址**。

（2）排除

6. 排除是 DHCP 服务器不分配的 IP 地址。
7. 排除范围是作用域内从 DHCP 服务中排除的**有限** IP 地址序列。添加排除的 IP 地址范围，只需输入起始 IP 地址和结束 IP 地址，如果想排除一个单独的 IP 地址，**只需要输入起始 IP 地址**（结束 IP 地址省略）。**添加排除**时**不需要**获取客户机的 **MAC 地址**信息。（添加保留时需要）

（3）租约

8. 租约是客户机可使用指派的 IP 地址期间 DHCP 服务器指定的时间长度（不能控制用户上网时间）。租约期限决定租约何时期满以及客户端需要向服务器对它进行更新的频率。

（4）保留

9. 使用保留创建通过 DHCP 服务器的永久地址租约指派，客户端**可以释放**该租约。保留地址可以使用作用域地址范围中的**任何** IP 地址（包括被排出的 IP 地址序列）。保留确保了子网上指定的硬件设备始终可使用**相同的 IP 地址**。

10. 新建保留：新建（添加）保留时需输入保留名称、IP 地址、**MAC 地址**、描述和支持类型等项目。（无子网掩码）

（6）租约

11. 续约：默认的地址租约期限为 8 天，租约到期前客户端需要续订，续订是由客户端软件**自动**完成。地址租约期限的最小可调整单位是**分钟**。

12. 客户机与 DHCF 服务器在同一网段时，采用 DHCP 消息收到的子网所处的网段分配 IP 地址。**不在同一网段**时，选择转发“DHCP 发现”消息的**中继**所在的子网网段（需修改该消息中的相关字段）。收到非中继转发的“DHCP 发现”消息时，会选择收到“DHCP 发现”消息的子网所处的网段分配 IP 地址（不是任选）。

完

更多三级知识，请关注

微信搜一搜

恒风远博

名副其实举世无双

UID: 24517269

支付宝 ALIPAY

向我捐赠

微信支付

版本V1.8 2021.8.28