速记 50 个高频知识点

1. R 进制表示及互转

（1）进制间互转一般是无符号的数。

（2）三位二进制的数可以转换成一位八进制的数，四位二进制的数可以转换成一位十六进制数。

（3）十六进制数中的 10-15 用英文的 A、B、C、D、E、F（或 a—f）表示。

2. 冯·诺依曼体系结构

（1）运算器和控制器由于逻辑关系和电路结构上联系紧密，所以统称中央处理器。

（2）运算器包含：算术逻辑单元 ALU、累加寄存器 AC、数据缓冲寄存器、状态条件寄存器、多路转换器。

（3）控制器包含：程序计数器 PC、指令寄存器 IR、指令译码器 ID、地址寄存器 AR、时序部件。

3. 主存容量计算

（1）主存使用随机存储方式存取，需要对每个存储单元进行编址。

（2）所谓编址即用一个 16 进制数来表示一个存储单元。

（3）存储单元就类似于仓库，每个仓库有一个编号（这就是编址），一个仓库能容纳箱子的数量（就是存储单元的容量）。

（4）按字节编址，表示存储单元容量是以字节为单位，一个字节有 8 个 bit。按字编址，表示存储单元容量是以字为单位，而字是字节的倍数（看题目中如何描述）。

（5）各个存储单元合起来就是主存的总容量。

4. 文件管理

（1）在 Windows 下，使用反斜杆\，在 Linux 下，使用斜杆/。

（2）在 Windows 下

绝对路径:

例如: E 盘的根目录下存在 document1 文件夹，用户在该文件夹下已创建了 document2 文件夹，而当前文件夹为，document1。若用户将 test.docx 文件存放 document2 文件夹中，则该文件的绝对路径为 E:\document1\document2。

相对路径:

对于上述示例，相对路径则为 document2\，因为用户在 document1 目录下，document2 是 document1 的子目录。

（3）在 Linux 下

绝对路径:

路径的写法，由根目录/写起，例如：/usr/share/doc 这个目录。

相对路径：

路径的写法，不是由/写起，例如由/usr/share/doc 要到/usr/share/man 底下时，可以写成：../man，其中..表示上级目录。

5. 设备管理

（1）所谓设备管理，是对硬件设备进行管理，包括输入输出设备的分配、启动、完成和回收。

（2）最常考的是程序中断方式和 DMA 方式。

（3）中断方式：能实现一定的 CPU 并行，提高 CPU 效率。（鼠标、键盘）

（4）中断相关概念：

中断向量：形成中断服务程序的入口地址。

保护现场：帮助 CPU 处理完中断后，返回原来被打断的地址继续执行。

中断响应时间：从发出中断请求到开始进入中断处理程序的时间。

（5）DMA 方式：数据传输过程没有 CPU 的参与，由专门的 DMA 控制器（DMAC）接口直接与存储器进行高速传输。

6. 项目管理基础

（1）时间最长的路径即为关键路径，该时间即是工期。

（2）其他路径的时间会小于工期。

（3）在不影响工期的情况下，其他路径上的点可以稍作休息，晚几天再开始也没关系，这段时间是松弛时间，但是松弛时间加上该路径的总时间不能大于关键路径。

（4）路径上的点由正常开始时间，加上松弛时间即是最晚开始时间。

7. 复用技术

（1）E1 载波的速率是 2.048Mbps，一共 32 个子信道（速率 64kbps），其中 2 个控制信道的位置是 CH0 与 CH16。

（2）T1 载波的速率是 1.544Mbps，一共 24 个子信道。

8. 数字调制技术

（1）熟悉常见的调制技术波形图 ASK、FSK、PSK

（2）知道常见调制技术所拥有的码元种类数及比特数，如 ASK、FSK、PSK、2DPSK 的码元种类数是 2，比特数是 1。4DPSK、QPSK 的码元种类数是 4，比特数是 2。

9. 数字编码与编码效率

（1）PCM 脉冲编码调制技术：有采样、量化和编码 3 个过程。

（2）采样定理：取最高频率的 2 倍。

（3）曼彻斯特编码：电压从高到低表示 1，反之则表示 0。当然定义也可以相反。

（4）差分曼彻斯特编码：比特前沿是否电平跳变，遇 0 翻转，遇 1 不变。

（5）曼码和差分曼码的编码效率是 50%，4B/5B 和 8B/10B 编码效率是 80%。

（6）曼码应用于传统 10M 以太网，4B/5B 应用于 100Base-FX、FDDI，8B/10B 应用于 1000Base-X，MLT-3 应用于 100Base-TX。

10. 差错控制—奇偶校验

（1）检错码的构造：检错码＝信息字段＋校验字段。

（2）信息字段和校验字段中，1 的个数是奇数个就是奇校验，1 的个数是偶数个就是偶校验。

（3）奇偶校验是检错码，只检错不纠错。

11. 差错控制—海明校验

（1）$m+k+1<=2^k$，m 表示数据位的位数，k 表示校验位的位数，题目中会给出 m 值，让求 k 值。

（2）每个数据位由确定位置关系的校验位来校验。

（3）校验位是放在 2 的幂次方位上，也就是第（1）（2）（4）（8）（16）……位上。

（4）例如第 3 位是数据位，第三位（3）用 2 进制表示就是 0011，第三位的数据是由第 1，2 位的校验位来校验的。

（5）海明码是纠错码，不仅可以检错，还可以纠错。

12. 差错控制—CRC 循环冗余校验

（1）要计算 CRC 校验码，需根据 CRC 生成多项式进行，题目中会给出。例如：原始报文为 11001010101，其生成多项式为 X^4+X^3+X+1。

（2）通过生成多项式的最高次幂获得新的数据，例如示例中是 4，在原始报文后面补 4 个 0 获得新的数据。

（3）通过生成多项式获得对应除数，如示例中是 11011。

（4）最后用新数据对 11011 进行模二除法运算，得到的余数替换新数据后的 4 个 0，即得到 CRC 校验码。

（5）CRC 校验码是检错码，只用于检错不纠错。

（6）以太网中使用的校验就是 CRC 循环冗余校验。

13. OSI 模型和 TCP/IP 模型

（1）对等层协议要一致，下层是上层的服务提供者。

层次	名称	主要功能	主要设备及协议
7	应用层	实现具体的应用功能	POP3、FTP、HTTP、Telnet、SMTP DHCP、TFTP、SNMP、DNS
6	表示层	数据的格式与表达、加密、压缩	
5	会话层	建立、管理和终止会话	
4	传输层	端到端的连接	TCP、UDP
3	网络层	分组传输和路由选择	三层交换机、路由器 ARP、RARP、IP、ICMP、IGMP
2	数据链路层	传送以帧为单位的信息	网桥、交换机（多端口网桥）、网卡 PPTP、L2TP、HDLC、PPP
1	物理层	二进制传输	中继器、集线器（多端口中继器）

14. CSMA/CD 协议

（1）载波侦听算法有：

非坚持型监听算法：链路利用率低，发生冲突的概率也低

1-坚持型监听算法：链路利用率高，发生冲突的概率也高

P-坚持型监听算法：链路利用率高，发生冲突的概率低

（2）求最短帧长需要牢记公式：发送时延>=2 倍传播时延

（3）再次发生冲突的概率：第 n 次冲突后，再次发生冲突的概率为：$1/2^n$（n<10）

（4）CSMA/CD 协议标准：IEEE802.3

15. 以太网的帧格式

（1）以太网中，帧的最小长度是 64 字节，最大长度是 1518 字节。

（2）以太网中，帧的数据部分占 46—1500 字节。

（3）以太网中，数据帧的 MTU 值是 1500 字节，MTU 即最大传输单元。

16. 移动通信 5G

5G 增强型移动宽带（eMBB）

5G 大带宽技术

大规模多输入多输出天线阵列 Massive MIMO 技术

F-OFDM

高阶 QAM 调制技术

Polar 和 LDPC 编码技术

17. 交换式以太网

（1）交换机在工作过程中，会维护一张端口——MAC 地址映射表。

（2）交换机通过接收到的数据帧的源 MAC 地址进行学习。

（3）交换机通过接收到的数据帧的目的 MAC 地址进行转发。

（4）交换机 MAC 地址表的老化时间是 300 秒。

18. VLAN 虚拟局域网技术

（1）VLAN 的作用：有效控制广播域范围（隔离广播），增强局域网安全性（业务安全），灵活构建虚拟工作组（规划、布线灵活性）。

（2）划分 VLAN 的方式：基于端口的静态划分和基于 MAC 地址、协议、子网、策略的动态划分。

（3）VLAN 值的范围是 1-4094，0 和 4095 保留。

（4）VLAN 的接口类型有 access、trunk（常考的 2 种）和 hybrid。Access 口仅允许一种 vlan 通过，trunk 口允许多种 vlan 通过。

（5）trunk 使用的封装协议是 IEEE 802.1q。

19. STP 生成树协议

（1）生成树协议将一个物理成环的网络，通过逻辑的阻塞一个或多个端口，形成一个逻辑上的树状网络结构。

（2）网桥 ID 用来选择根网桥，网桥 ID 由网桥优先级和 mac 地址组成，网桥 ID 小的就是根网桥。

（3）网桥优先级的范围是 0-65535，默认值是 32768，修改网桥优先级要是 4096 的倍数。

（4）根网桥选完之后，再选根端口和指定端口。根端口是在非根网桥上，而不是在根网桥上。根端口是用来接收根网桥信息的端口，指定端口是用来发送根网桥信息的端口。

（5）生成树协议的标准是 IEEE802.1d。

20. 无线局域网

（1）无线局域网有多个标准。一般考查其各个标准下所对应的运行频段与速率。

IEEE 802.11b 和 802.11g 运行在 2.4GHz 的频段，802.11a 运行在 5GHz 的频段，802.11n 运行在 2.4GHz 和 5GHz 频段。注意一下 2.4GHz 频段信道划分。

802.11n 的速率一般最大为 300Mbps，利用 MIMO 和 OFDM 技术的结合，理论上可以达到 600Mbps。IEEE 802.11ac（WIFI5）标准目前应用最广，工作于 5GHz。IEEE 802.11ax（WIFI6）工作于 2.4GHz 和 5GHz。

（2）无线局域网使用的是 CSMA/CA 协议，而不是 CSMA/CD 协议。

（3）无线局域网中的加密算法有 WEP、WPA 和 WPA2，安全性依次增加。

（4）WLAN 的组网：① FIT：AP+AC+路由器 ② FAT：AP+路由器

21. 云 AP

通过云管理平台，可以实现任意地点对设备进行集中的管理和维护，大大降低网络部署运维成本。

适用范围：中小型企业。

优势 (对比 AC+FIT AP 架构)

即插即用，自动开局，减少网络部署成本。

统一运维：所有云管理网元统一在云管理平台上进行监控和管理。

工具化：通常情况下，云解决方案会在云端提供各类工具，有效降低各类开支。

22. 各种新技术相关概念及功能

名称	关键词
大数据	大量数据、数据分析
云计算	强计算能力、多台计算机
物联网	物联网、传感器
区块链	分布式账本数据库
SDN	软件定义网络、通过分离以实现更灵活的网络

23. 接入网技术-光纤接入网

（1）与有源光网络的区别：无源光网络（PON）主要特征是 ODN 全部采用无源光器件组成，避免了有源设备的电磁干扰和雷电影响，减少了线路和外部设备的故障率，提高了系统可靠性。

（2）PON（无源光网络）由光线路终端（OLT）、光分配网络（ODN）、光网络单元（ONU）组成。

（3）PON 采用点到多点模式，下行采用广播、上行采用 TDMA 时分多址方式。

（4）PON 可以灵活地组成树型、星型、总线型等拓扑结构（典型结构为树型）。

（5）根据 ONU 的位置、不同应用类型和投资情况，分为 FTTH（光纤到户）、FTTC（光纤到路边）、FTTB（光纤到大楼）、FTTZ（光纤到小区）。

24. IPV4 协议—分类的 IP 地址

（1）A 类地址第一字节的范围是 1-126，B 类地址第一字节的范围是 128-191，C 类地址第一字节的范围是 192-223，D 类组播地址第一字节的范围是 224-239。其中组播地址比较常考。

（2）私网地址的范围：

A 类私网地址网络号：10

B 类私网地址网络号：172.16—172.31

C 类私网地址网络号：192.168.0—192.168.255

（3）主机地址、环回地址（127 开头）和自动专用地址（169.254 开头）可以作源地址和目的地址。

0.0.0.0 可以作源地址，不可以作目的地址。

广播/组播地址可以作目的地址，不可以作源地址。

25. IPV4 协议—IP 数据报

（1）IP 数据报首部长度最小为 20 字节，其在首部长度字段中数值为 5。

（2）常考字段如下：

标识符：一个唯一的标识数字，用来标识一个数据包或者一组分片的数据包。

片偏移：如果数据包被分片，可以通过片偏移把这些分片的数据包组装起来。

标志：一个数据包是否是一组分片数据包的一部分。

TTL：表明 IP 数据报的生命，每经过一台路由器，TTL-1，到 0 的时候丢弃。

26. ARP 协议

（1）ARP 协议是通过 IP 地址来获取对应的 mac 地址。

（2）查询方通过广播请求，询问 IP 地址对应的 mac 地址。被查询方通过单播来告知查询方自己的 mac 地址。

（3）注意题目中问的是 ARP 帧中的目的 MAC 还是 ARP 报文内的目的 MAC。

（4）掌握 arp 相关命令，arp –a 查看 arp 缓存，arp –d 清除 arp 缓存，arp –s 静态添加 ARP 条目。

27. ICMP 协议

（1）ICMP 的作用是向源主机发送传输错误警告。

（2）ICMP 被 IP 封装。

（3）ICMP 下的两个应用是 ping 和 tracert（traceroute），ping 利用到了 ICMP 中的回送和响应请求报文，tracert 利用了 ICMP 中的时间超过报文和目标不可达报文。

28. IPv6 协议

（1）IPv6 是为解决 IPv4 中地址不够用的问题，IPv6 地址有 128 位。

（2）IPv6 地址以 16 位为一组，共 8 组，用 16 进制表示。来自任何 16 进制数字组的一个或多个前导零被删除；通常对全部或全部前导零进行此操作。例如，组 0042 被转换为 42。零的连续部分用双冒号（::）替换。双冒号只能在地址中使用一次。

（3）IPv6 地址类型

地址类型	地址前缀	IPv6 前缀标识
链路本地地址	1111111010	FE80::/10
站点本地地址	1111111011	FEC0::/10
全球单播地址	全球路由选择前缀（48bit），前 3 位固定为 001	

（4）过渡技术有：双协议栈、隧道技术、网络地址转换技术。

29. 传输层协议—UDP 与 TCP

（1）UDP 是无连接不可靠的协议，TCP 是面向连接的可靠的传输层协议。

（2）UDP 首部 8B，开销小，而 TCP 头部最小长度是 20B。

（3）TCP 头部中常见字段含义：

序号：用这个数字表示一个 TCP 片段。

确认号：给对方一个确认回应，同时这个数字是通信中希望从另一个设备得到的下一个数据包的序号。

URG：紧急位

ACK：确认号位

RST：重建连接或者拒绝一个无效连接

SYN：请求建立连接的标志

FIN：请求关闭一个连接

窗口：指的接收窗口，表示缓冲区的大小

紧急指针：如果 URG 位置 1，这个域将被检查作为额外的指令，告诉 CPU 从哪里读数据。

（4）三次握手数据包的特征：第一和第二个报文会出现 SYN 的标志。

（5）理解 TCP 实现流量控制和拥塞控制的方法。

（6）知道常见应用协议的端口号（在后面的应用层知识点中会提及）。

30. 域名系统 DNS 协议

（1）DNS 使用 UDP 53 号端口。

（2）**客户机域名解析顺序如下：**首先查看本地 DNS 缓存是否有相关的历史记录，如果没有的话，再查看本地 HOSTS 文件有没有相对应的记录，如果还是没有，则向本地 TCP/IP 配置中的“首选的 DNS 服务器”的 DNS 服务器查询，如果“首选 DNS 服务器”也没有对应的记录，则会向“备用 DNS 服务器”查询。其查询顺序主要分为三步：“本地 DNS 缓存”“本地 HOSTS 文件”“DNS 服务器”。

DNS 服务器域名解析顺序：首先查看本身 DNS 服务器的区域记录，其次再查 DNS 服务器缓存；如果还没有得到结果，则继续进行下一步查询。如果 DNS 服务器配置了转发器，则会向设置的转发 DNS 服务器发出域名解析请求，如果没有配置转发器，则会向根 DNS 服务器发出域名解析请求，再由根 DNS 服务器逐级向下转发相关查询命令。

（3）**递归查询：**当服务器收到一个查询请求，在本地没有记录的时候，此服务器继续会向其他服务器发出查询请求，而后再返回对应的结果给查询请求方。

迭代查询：当服务器收到一个查询请求，不能直接返回结果，而是让查询方找另外一台服务器进行查询。

（4）掌握常见的资源记录，如主机（A）记录，指针（PTR）记录，别名（CNAME）记录、MX 记录。

31. 动态主机配置协议 DHCP

（1）DHCP 服务器使用 UDP 67 号端口，客户端使用 UDP 68 号端口。

（2）使用 DHCP 协议时，如果客户端能正常获取 IP 地址等参数。说明 DHCP discover、DHCP offer、

DHCP request、DHCP ack 这 4 个报文成功交互。

（3）由客户端发送的 DHCP discover 和 DHCP request 报文是广播报文。而服务器端发送的 DHCP offer 和 DHCP ack 报文可以是单播报文也可以是广播报文，如果题目中问到是使用单播还是广播，建议选择广播。

（4）Windows 服务器配置 DHCP 时，默认租约是 8 天，华为路由器的默认租约是 1 天。

（5）使用 DHCP 中继，可以实现由一台 DHCP 服务器为多个子网进行地址的动态分配。中继可以转发 DHCP 报文。

（6）客户机在收到 DHCP ack 报文之前，始终使用 0.0.0.0 地址。

32. ospf 邻居建立不起来的原因

1.routerid 一致，因为 routerid 是唯一的

2.areaid 不一致

3.认证方式不一致

4.认证密码不一致

5.掩码不一致

6.hello、deadtime 不一致

7.接口链路故障，接口没有启用 ospf，导致收不到对端发送的报文

8.网络类型不一致 network-type

9.区域类型不一致

特殊区域 非特殊区域

10.静默端口

33. 文件传输服务 FTP 协议

（1）FTP 在主动模式下，控制连接使用 21 号端口，数据连接使用 20 号端口。

（2）FTP 在被动模式下，控制连接使用 21 号端口，数据连接使用 1024-65535 中的任一端口。

（3）上下午考试中，没有特殊说明是数据连接端口而只是说 FTP 端口的话，选择 21 号端口。

34. 认证技术

对比项	802.1X 认证	MAC 认证	Portal 认证
适合场景	新建网络、用户集中、信息安全要求严格的场景	打印机、传真机等哑终端接入认证的场景	用户分散、用户流动性大的场景
客户端需求	需要	不需要	不需要

优点	安全性高	无需安装客户端	部署灵活
缺点	部署不灵活	需登记 MAC 地址，管理复杂	安全性不高

35. Windows 的基本管理

（1）需要熟悉掌握常见命令，如 ipconfig、ping、tracert、netstat、route print、nslookup。

（2）ipconfig 可以显示当前 TCP/IP 网络配置的内容，注意后续的参数。

（3）ping 可以测试网络连通性，注意后续的参数。

（4）tracert 可以显示路由路径。

（5）netstat 可以显示传输控制协议 TCP（传入和传出），路由表，许多网络接口的网络连接和网络协议统计，注意后续的参数。

（6）route print 显示路由表，和 netstat –r 等价。

（7）nslookup 用于查询域名系统（DNS）以获取域名或 IP 地址映射或任何其他特定 DNS 记录。

36. 常见的广域网协议

（1）HDLC 和 PPP 协议均是数据链路层协议。

（2）HDLC 是一种应用很广的面向比特的高级数据链路控制协议。

（3）HDLC 使用 0111 1110 作为帧的边界，会使用到零比特填充法。

（4）PPP 协议是在 HDLC 上发展出来的，是面向字符的协议。

（5）PPP 协议的框架中包含了 LCP 报文和 NCP 报文。LCP 报文建立、配置、验证和测试数据链路连接，NCP 报文建立和配置不同的网络层协议。

（6）PPP 协议框架中有可选的认证协议：PAP 和 CHAP，其中 CHAP 的安全性高，使用到 3 次握手机制，不传递明文密码信息。

37. RAID 技术

（1）RAID0，磁盘利用率 100%，没有冗余，可靠性最差。

（2）RAID1，磁盘利用率 50%，数据通过镜像，完全放在两个不同的磁盘上，可靠性高。

（3）RAID3，磁盘利用率（n-1）/n，有特定的校验磁盘，使用奇偶校验，校验数据单独放在校验盘上。可靠性较高。

（4）RAID5，磁盘利用率（n-1）/n，没有特定校验盘，校验数据分散存放在各个磁盘上。可靠性较高。

（5）RAID6，磁盘利用率（n-2）/n，上述技术解决了一个磁盘出现故障，依旧可以恢复出数据的问题，但是当 2 个磁盘出现故障时，就无法恢复，所以用到了 RAID6 技术。每个磁盘有 2 个校验数据，校验数据分散存放在各个磁盘上。

（6）RAID10 和 RAID01：RAID10 是 RAID1 和 RAID0 的结合，先镜像再条带化。RAID01 是 RAID0

和 RAID1 的结合，先条带化再进行镜像。可靠性方面是 RAID10 更好。

38. 网络存储

（1）直接连接存储（DAS）是直接连接到访问它的计算机的数字存储，例如我们的个人电脑、普通的一台服务器都可以认为是 DAS。

（2）网络附加存储（NAS）是连接到计算机网络的文件级计算机数据存储服务器。如果想利用以太网访问文件级数据就可以使用 NAS。

（3）存储区域网络（FC-SAN）是一个计算机网络，其提供了访问合并，块级数据存储。如果想利用光纤通道访问块级数据就可以使用 SAN。

（4）IP-SAN：更加经济的以太网存储区域网络。

39. 计算机病毒

（1）常见病毒前缀有 trojan（木马病毒）、Hack（黑客病毒）、worm（蠕虫病毒）、macro（宏病毒）、script（脚本病毒）、win32（系统病毒）

病毒类型	特征	危害
宏病毒	针对 Office 的一种病毒，由 Office 的宏语言编写	只感染 Office 文档，其中以 Word 文档为主
脚本病毒	通过 IE 浏览器激活	用户浏览网页时会感染，清除较容易
蠕虫	有些采用电子邮件附件的方式发出，有些利用操作系统漏洞进行攻击	破坏文件、造成数据丢失，使系统无法正常运行，是目前危害性最大的病毒
木马	通常是病毒携带的一个附属程序	夺取计算机控制权

40. 加密技术

（1）对称加密是在加密和解密数据使用同一把密钥，而非对称加密使用不同的密钥。

（2）常见的对称加密算法有 DES、3DES、IDEA、AES，同时这些也属于分组加密。

（3）常见的非对称加密算法有 RSA（常考）、ECC、DSA 等。

（4）DES 的密钥长度为 56 位，3DES 的密钥长度为 112 位，IDEA 的密钥长度为 128 位，AES 的密钥长度有 128、192、256 位三种。

41. 数字签名

（1）数字签名是基于公钥体系（非对称加密体系）的。

（2）数字签名的功能有：验证发送方身份、不可抵赖、完整性鉴别。

（3）发送方用自己的私钥对报文进行签名，接收方接收到报文后，用发送方的公钥验证签名。

（4）是基于公钥体系的，所以需要知道数字签名里面使用的算法就是非对称加密中的算法。

42. 数字证书

（1）数字证书的作用是证明公钥的合法性，证书中包含有公钥信息。

（2）数字证书由 CA 签证中心签发，可用 CA 的公钥核实证书的真伪。

43. 报文摘要

（1）报文摘要算法：可用于实现报文鉴别，即对报文完整性进行鉴别。

（2）常见的报文摘要算法如下：

MD5：产生 128 位的输出。

SHA-1（安全散列算法）：产生 160 位的输出。

（3）报文摘要算法不是加密算法。

44. 网络攻击

（1）被动攻击：不影响源站与目的站之间的通信过程，如窃听。

（2）重放攻击：指攻击者发送一个目的主机已接收过的包，来达到欺骗系统的目的，可使用时间戳来预防。

（3）DOS 攻击：向目标主机发送大量非正常报文，使目标主机无法提供正常的服务。

（4）DDOS 攻击：DOS 攻击的升级版本，攻击力度更大，隐藏性更好。

（5）SQL 注入攻击：涉及注入 SQL 命令，可使用 WAF 设备、IPS 防御。

（6）XSS 攻击：涉及上传恶意的 HTML 代码，可使用 WAF 设备、IPS 防御。

45. 网络安全协议

（1）SSL 协议，常和 HTTP 协议结合，形成 HTTPS 协议，默认端口号为 TCP 443，可用来实现 WEB 传输的安全性。

（2）TLS，安全的传输层协议，是 SSL 协议的升级版本。SET 协议是安全的电子交易协议。

（3）安全的电子邮件协议是 PGP，默认使用的摘要算法为 MD5。

46. 防火墙

（1）防火墙最基本的功能就是隔离网络，通过将网络划分成不同的区域，制定出不同区域之间的访问控制策略来控制不同信任程度区域间传送的数据流。

（2）防火墙不是用来防病毒的。

（3）常考的包过滤防火墙是基于“五元组”来对数据包进行过滤，“五元组”即源 IP 地址、目的 IP 地址、协议号、源端口、目的端口。

（4）防火墙一般分为 3 个区域，可信任区域（内网区域）、DMZ 区域、非信任区域（外网区域）。其中在 DMZ 区域放置可供外网访问的服务器设备。

（5）防火墙模式：路由模式、透明模式和混合模式。路由模式可以理解为是带有防火墙功能的路由器。透明模式是在保证原有网络部署不变的情况下，将防火墙设备接到路由器和交换机中间，这种部署方式不需要配置接口 IP。

47. VPN 技术

（1）PPTP VPN、L2TP VPN 工作在第二层数据链路层，IPsec VPN、GRE VPN 工作在第三层网络层、SSL VPN 工作在应用层。

（2）认证头 AH：提供完整性和数据源认证功能，不提供机密性保护。

（3）封装安全的有效载荷 ESP：提供完整性和数据源认证功能及机密性保护。

（4）IPsec VPN 的两种模式：

传输模式：不改变原有的 IP 包头，通常用于主机与主机之间。

隧道模式：增加新的 IP 头，通常用于私网与私网之间通过公网进行通信。

48. 入侵检测系统

（1）IDS 设备（入侵检测系统）依照一定的安全策略，对网络、系统的运行状况进行监视，尽可能发现各种攻击企图、攻击行为或者攻击结果，以保证网络系统资源的机密性、完整性和可用性。一般会与防火墙一起联动使用。

（2）IDS 设备一般旁挂在交换机的镜像端口下，该镜像端口可以获得所需要监测的流量数据。

（3）IPS 入侵防御系统，可看成是 IDS 和防火墙的结合，更加主动，IPS 设备一般以串连的方式，放置在要被保护的网络（一般是内网区域）的前面。

49. 网络故障

（1）网络故障排除常用命令

Display：可用于查看网络设备的配置情况，以实现对故障的定位

Ping：用户检测网络上不同设备之间的连通性

Tracert：用于路由跟踪，以确定故障位置

（2）专用故障排除工具

电缆测试器：可用于检测电缆的物理连通性

时域反射仪 TDR：能够快速定位到电缆中的断路等问题

光时域反射仪 OTDR：可在一端精确测量光纤的断裂处、衰减等问题

50. 路由器设备的配置

（1）路由信息协议 RIP，以跳数作为度量值，最大跳数 15 跳。以 30s 为周期向邻居路由器发送自己的路由表来维持和更新路由表，为避免路由环路要使用到水平分割、毒性逆转、触发更新等技术。

（2）链路状态路由协议 OSPF，以开销作为度量值，通常使用带宽来计算开销，当拓扑发生变化时发送更新，使用 SPF 算法保证路由无环路。

（3）VRRP 虚拟路由冗余协议需要掌握其原理、其活动路由器选举规则、以及虚拟网关 IP 和优先级及跟踪上联接口的相关配置。

（4）ACL 的配置需要重点掌握，在下午考题中常考，需要了解基本访问控制列表和高级访问 控制列表的区别及命令的写法。

（5）NAT 的概念及配置了解即可。在 NAT 技术中，静态 NAT 和基于端口的 PAT 常考。

（6）Windows 服务器配置类的大题中近几年考察 DHCP 的几率下降，但关于路由器配置 DHCP 是个常考点，需要重点关注。

（7）IPsec VPN 是一个难点，它的原理与配置需要有基本印象。

（8）需要了解策略路由技术，明白其作用，结合题目说明能准确完成配置书写。

（9）IPv6 相关内容在近年考试中出现频率有所提高，也需要重点关注。

制作于 23 年 12 月 适用于第 5 版教材