

网络运维与网络安全 面试题手册

达内·网络运维与安全学院
2018 年 09 月

目 录

阶段 1-1、网络运维基础	4
1. 请简单描述 IPv4 地址的分类和范围？	4
2. 制作双绞线时，T568b、T568a 线序分别是什么？	4
3. 在华为交换机、路由器设备上，如何为接口配置 IP 地址？	4
4. 以华为设备为例，如何实现对路由器、交换机的远程管理？	4
5. 云服务器指的是什么，与普通服务器有何区别，有什么优势？	5
6. 在一台 CentOS7 服务器上搭建 Web 服务器，基本过程或思路是怎样的？	5
阶段 1-2、网络系统管理	6
1. Windows 主机上如何发布共享目录，如何访问共享目录？	6
2. 什么是 DNS，主要作用是什么？	6
3. RAID 阵列指的是什么，常见的阵列级别有哪些，各自的特点是什么？	6
4. Linux 目录结构是怎么样的，简述你所了解的 Linux 目录及用途？	7
5. Linux 系统中文档的访问权限是如何调控的？	7
6. 如果你有一台 CentOS7 或 RHEL7 服务器，如何为这台服务器配置 IP 地址参数？	8
阶段 2-1、网络通信原理	8
1. TCP 和 UDP 都可以实现客户端/服务端通信，这两个协议有何区别？	8
2. 网络通信中的 MAC 地址指的是什么，其作用和地址构成是怎样的？	8
3. ARP 是第几层的协议，其作用是什么？	9
4. 简单说一下交换机的工作原理？	9
5. 请列举你所知道的应用层协议有哪些，各自的作用及标准端口是什么？	9
6. OSI 模型由下往上依次包括哪几层？网络通信中各层的 PDU 单位分别是什么？	10
阶段 2-2、中小型企业网构建	10
1. 请简单介绍一下 VLAN 技术？	10
2. Trunk 链路 Access 链路的区别是什么？	10
3. 什么是 STP 协议？其作用和工作原理介绍一下？	10
4. 请描述一下路由器的工作原理？	11
5. DHCP 的作用是什么？什么情况下需要部署 DHCP 中继？	11
6. 一个大约 200 名员工的小型企，要实现新办公区的网络系统集成，说说你的规划？	11
阶段 2-3、大型企业网构建	12
1. VRRP 指的是什么，有什么作用？	12
2. 路由器应用中的 NAT 指的是什么，有哪几种类型？	12
3. 网络设备上的 ACL 技术指的是什么，有哪几种类型、各自的特点？	12
4. OSPF 指的是什么，在路由器上是怎么工作的？	13

5. IPv6 地址的总量是多少，如何表示？	13
6. OSPF 协议与 BGP 协议有哪些区别？	13
阶段 3-1、云网服务管理	14
1. 缓存 DNS 与权威 DNS 有什么区别？一般用户在上网时，DNS 解析过程是怎样的？	14
2. 动态网站与静态网站有什么区别，http 平台要支持 PHP 程序需要具备哪些条件？	14
3. 是否了解 Zabbix 监控系统，它是如何获取路由交换设备或 Linux 主机信息的？	15
4. 如何配置 httpd 服务器支持多个网站？	15
5. 在 CentOS7 或 RHEL7 服务器上，如何控制系统服务的开启、关闭及开机自动运行？	15
6. 如何为一台 CentOS7 或 RHEL7 服务器添加新的软件源？	16
阶段 3-2、数据库管理	16
1. 对于 MySQL 或 MariaDB 数据库服务器，如何为管理账号 root 设置密码？	16
2. 管理 MySQL 或 MariaDB 数据库服务器时，如何创建新库并授权用户？	16
3. 使用 SQL 指令在工资表 salary 中查询月薪资 yuexin 超过 10000 元的员工名单？	16
4. 在 MySQL 或 MariaDB 数据库服务器上，如何删除密码为空的 root 用户记录？	17
5. 如果忘记了 MySQL 或 MariaDB 数据库的管理密码，如何恢复？	17
6. 简述 MySQL 或 MariaDB 数据库的备份与恢复操作？	17
阶段 3-3、网络安全	18
1. ARP 欺骗、中间人攻击是基于哪种方式实现的？	18
2. 是否熟悉华为防火墙，其默认的安全区域有哪些？	18
3. DoS 攻击、DDoS 攻击分别指的是什么？	18
4. VPN 指的是什么，主要用在什么场合？	19
5. IDS 与 IPS 分别指的是什么，两者有什么区别？	19
6. 防火墙上的 QoS 管理指的是什么，有什么好处？	19

阶段 1-1、网络运维基础

1. 请简单描述 IPv4 地址的分类和范围？

答案：

- A 类 1 - 127 网+主+主+主
- B 类 128 -191 网+网+主+主
- C 类 192 -223 网+网+网+主
- D 类 224 - 239 组播(多播)
- E 类 240 - 254 科研

2. 制作双绞线时，T568b、T568a 线序分别是什么？

答案：

T568b 线序：白橙、橙、白绿、蓝、白蓝、绿、白棕、棕

T568a 线序：白绿、绿、白橙、蓝、白蓝、橙、白棕 棕

3. 在华为交换机、路由器设备上，如何为接口配置 IP 地址？

答案：

交换机的 VLAN1 可以配置管理 IP，路由器的每一个接口都可以配置 IP 地址，基本思路如下：

```
<Huawei> system-view //进系统视图
[ar1] interface g0/0/1 //进接口 g0/0/1 配置
[ar1-GigabitEthernet0/0/1] ip address 192.168.1.254 24 //配 IP 地址 1
[ar1-GigabitEthernet0/0/1] undo shutdown //激活接口
```

4. 以华为设备为例，如何实现对路由器、交换机的远程管理？

答案：

基本配置过程：

- 1) 确认设备的 IP 地址（路由器接口、交换机 VLAN1）
- 2) 在设备上启用 AAA 认证（开启 AAA 模式、添加用户账号、允许 telnet 控制）
- 3) 从客户机 telnet 设备的 IP 地址，登录后执行管理

5. 云服务器指的是什么，与普通服务器有何区别，有什么优势？

答案：

云服务器指的通过互联网提供给个人或企业客户的虚拟服务器，在华为云、阿里云等服务商通常称之为 ECS（Elastic Compute Service，弹性计算服务）。

与普通服务器相比，从远程管理、操作系统管理、网络应用管理等方面来看，与普通服务器基本一样。云服务器还具有以下特点及优势：

- 客户不需要实体硬件，节省了硬件维护费用（主机、网络设备、机柜、机房等）
- 客户可以按需选配服务器、按需变更/升级配置、按需付费
- 服务器配置的变更/升级/系统恢复等方便、快速，几分钟就可以搞定

6. 在一台 CentOS7 服务器上搭建 Web 服务器，基本过程或思路是怎样的？

答案：

搭建 Web 服务器的基本过程：

- 1) 装软件包，比如 httpd（或者 nginx、tomcat 等）
- 2) 配置网站资源（部署网页）
- 3) 开启服务程序，比如 httpd（或者 nginx、tomcat 等）

其他相关操作：

- 1) 如果是互联网上的网站，最好申请一个简单易记的域名，更方便用户访问、有利于推广。
- 2) 国内的网站需要及时做好备案。

阶段 1-2、网络系统管理

1. Windows 主机上如何发布共享目录，如何访问共享目录？

答案：

发布共享目录的操作：

- 1) 环境设置，需要启用网络发现、启用文件和打印机共享，将防火墙关闭或允许 SMB 共享访问
- 2) 右击需要共享的目录，添加新共享，设置好共享名、调整好 NTFS 权限和共享权限

访问共享目录的操作：

Win+R 调出“运行”，输入共享资源地址，比如 \\服务器地址\共享名\，即可访问相应资源。

2. 什么是 DNS，主要作用是什么？

答案：

DNS 即 Domain Name System，域名系统。

主要作用：互联网中服务器数量众多，他们的 IP 地址对用户来说是不方便记住的，而 DNS 服务器可以为客户端提供“域名 <--> IP 地址”的地址解析服务，使用户体验更舒适。

3. RAID 阵列指的是什么，常见的阵列级别有哪些，各自的特点是什么？

答案：

RAID 即 Redundant Arrays of Independent Drives，廉价冗余磁盘阵列，指的是采用多块磁盘来组建具备更高 I/O 性能、硬件备份等特性逻辑磁盘的技术。

常见 RAID 级别及特性如下：

- RAID0：条带模式，至少 2 块磁盘，通过并发读写提高效率
- RAID1：镜像模式，至少 2 块磁盘，通过镜像备份提高磁盘设备的可靠性
- RAID10：条带+镜像模式，相当于 RAID1+RAID0，至少 4 块磁盘，读写效率及可靠性都更高

- RAID5：高性价比模式，至少 3 块磁盘，其中 1 块磁盘容量用来存放恢复校验数据
- RAID6：相当于扩展版的 RAID5，至少 4 块磁盘，其中 2 块磁盘容量用来存放恢复校验数据

4. Linux 目录结构是怎么样的，简述你所了解的 Linux 目录及用途？

答案：

Linux 系统没有 C:、D: 盘这些，所有的文档资源都组织在以 “/” 根开始的目录结构中。
常见的几个目录及用途如下：

- /：整个 Linux 文件系统的根目录
- /boot：存放系统内核、启动菜单配置等文件
- /home：存放普通用户的默认家目录（同名子目录）
- /root：管理员的家目录
- /bin、/sbin：存放系统命令、可执行的程序
- /dev：存放各种设备文件
- /etc：存放各种系统配置、系统服务配置文件
- /proc：存放内存运行数据的映射文件

5. Linux 系统中文档的访问权限是如何调控的？

答案：

Linux 文档的访问主要由归属关系、权限类别共同决定 —— 系统将来访者分为拥有人（u）、拥有组（g）、其他人（o）三个归属，权限区分为读取（r）、写入（w）、可执行（x）三个类别。

需要修改文档的归属关系时，使用 chown 命令，比如：

```
# chown -R 属主:属组 文档...  
# chown -R 属主 文档...  
# chown -R :属组 文档...
```

需要修改文档的权限标记时，使用 chmod 命令，比如：

```
# chmod -R ugoa+--rwx 文档
```

6. 如果你有一台 CentOS7 或 RHEL7 服务器 如何为这台服务器配置 IP 地址参数？

答案：

可以使用 nmcli 工具来配置网络连接的各项参数，比如：

```
# nmcli connection modify "连接名" ipv4.method manual ipv4.address "IP 地址/掩码长度"
ipv4.gateway "默认网关地址" ipv4.dns DNS 服务器地址 connection.autoconnect yes
# nmcli connection up "连接名"
```

如果原来没有为网卡设置任何连接，还需要先添加好网络连接，比如：

```
# nmcli connection add con-name "连接名" ifname "接口名" type ethernet
```

阶段 2-1、网络通信原理

1. TCP 和 UDP 都可以实现客户端/服务端通信，这两个协议有何区别？

答案：

TCP 协议面向连接、可靠性高、适合传输大量数据；但是需要三次握手、数据补发等过程，耗时长、通信延迟大。

UDP 协议面向非连接、可靠性低、适合传输少量数据；但是连接速度快、耗时短、延迟小。

2. 网络通信中的 MAC 地址指的是什么，其作用和地址构成是怎样的？

答案：

MAC 即 Media Access Control (介质访问控制)，主要用来标记网络接口卡的物理地址。

MAC 地址由 6 个字节组成，长度为 48 位；其中前 3 个字节是全球范围内的网络设备厂商代码，后 3 个字节为接口卡的地址。

3. ARP 是第几层的协议，其作用是什么？

答案：

ARP 即 Address Resolution Protocol (地址解析协议)，算是 OSI 参考模型第 2 层 (数据链路层) 的协议；其作用是根据 IP 地址获取物理地址，实现数据帧的快速封装。

4. 简单说一下交换机的工作原理？

答案：

交换机根据数据发送方和接收方的物理地址在不同端口间转发数据，主要依据为 MAC 地址表。

生成 MAC 地址表：当交换机在一个端口收到数据帧时，会将数据帧中的源 MAC 地址与入端口进行对应关联，形成 MAC 地址表条目。

查找 MAC 地址表：交换机将数据帧中的目标 MAC 地址与 MAC 地址表条目进行比对。如果能找到对应条目，则通过对应端口转发出去；如果没有找到对应条目，则进行广播 (即向来源端口以外的其他端口发送出去)。

5. 请列举你所知道的应用层协议有哪些，各自的作用及标准端口是什么？

答案：

- FTP，文件传输协议 (为客户端提供文件上传/下载)，TCP 21 端口 (控制连接)、TCP 20 端口 (数据连接)
- SSH，安全命令行协议 (提供远程管理设备的安全通道)，TCP 22 端口
- TELNET，远程网络终端协议 (提供远程管理设备的接口)，TCP 23 端口
- DNS，域名解析协议 (实现 “域名<-->IP 地址” 查询)，UDP 53 端口 (查询)、TCP 53 端口 (数据同步)
- HTTP，超文本传输协议 (提供网页资源传输接口)，TCP 80 端口
- HTTPS，安全的超文本传输协议 (提供网页资源的加密传输接口)，TCP 443 端口
- SMTP，简单邮件传输协议 (用来发送和传递邮件)，TCP 25 端口
- POP3，邮局协议 (为客户端提供收取邮件接口)，TCP 110 端口
- IMAP，Internet 邮件访问协议 (为客户端提供在线管理邮件接口)，TCP 143 端口

6. OSI 模型由下往上依次包括哪几层？网络通信中各层的 PDU 单位分别是什么？

答案：

OSI 参考模型：物理层->数据链路层->网络层->传输层->会话层->表示层->应用层。

各层 PDU 单位：物理层（位）、数据链路层（帧）、网络层（包）、传输层（段）。

阶段 2-2、中小型企业网构建

1. 请简单介绍一下 VLAN 技术？

答案：

VLAN，即 Virtual LAN（虚拟局域网），指在物理网络中根据业务需求划分的逻辑网络，不同 VLAN 之间等同于物理隔离，也可以按需要连通。

VLAN 本质上是一种 2 层技术，通过交换机的逻辑管理来实现广播域的隔离，从而可以减小数据广播风暴对交换网络的影响，降低了网络管理难度，同时可以实现网络规模的灵活扩展。

2. Trunk 链路与 Access 链路的区别是什么？

答案：

Trunk 链路同一时刻可以支持多个 VLAN 的数据转发，数据携带 VLAN 标签（native vlan 除外）。

Access 链路同一时刻只能传输一个 VLAN 的数据，发送和接收的数据，都没有标签。

3. 什么是 STP 协议？其作用和工作原理介绍一下？

答案：

当二层网络存在冗余链路的情况下，用来防止二层转发环路的发生。

默认情况下，交换机启动 STP 功能。加电开机后，通过与相连的交换机互相发送和比较 BPD

U，从而确保网路中去往任何设备，仅存在一条最短的、无环、二层数据转发路径。

具体过程如下：

- 1) 首先确定交换机的角色：根交换机和非根交换机
- 2) 其次确定端口的角色：根端口、指定端口和非指定端口
- 3) 最后确定端口的状态：down、listening、learning、forwarding、blocking

4. 请描述一下路由器的工作原理？

答案：

路由器是基于三层转发的设备，转发依据是记录了到达不同目标地址的网络路线的“路由表”。

当路由器收到一个数据包以后，会检查 IP 数据包头中的目标 IP 地址，并检索“路由表”条目以决定从哪一个接口转发此数据包。如果有匹配成功的路由条目，则按照对应的接口转发出去；如果匹配失败，则将数据包丢弃。

5. DHCP 的作用是什么？什么情况下需要部署 DHCP 中继？

答案：

DHCP 即 Dynamic Host Configuration Protocol (动态主机配置协议)，主要用来为客户机自动配置 IP 地址相关的网络参数，包括 IP 地址、子网掩码、默认网关、DNS 服务器等。

DHCP 通信为广播的方式，因此当需要 DHCP 服务器为不同广播域（路由或 VLAN 网段）的客户机分配地址时，就得在网关路由器上开启 DHCP 中继服务，这样才能使 DHCP 通信包跨广播域。。

6. 一个大约 200 名员工的小型企业，要实现新办公区的网络系统集成，说说你的规划？

答案：

具体方案应该取决于办公区域的结构及部门需要，需求决定设计。

简单来看应该包括这么几个部分：

- 1) 互联网接入，选择光纤宽带接入+路由器 NAT 共享。

- 2) 办公局域网, 200 人的规模可以考虑按部门划分 VLAN, 实现网段隔离。
- 3) 无线覆盖, 区域面积宽的话可以部署无线 AC/AP; 否则也可以采取小型无线路由桥接覆盖。
- 4) 大概需要接入层 24 口交换机 10~12 个、网管交换机 2~4 个, 路由器 1~2 个, 具体拓扑得根据部门/房间定。

阶段 2-3、大型企业网构建

1. VRRP 指的是什么, 有什么作用?

答案:

VRRP 即 Virtual Router Redundancy Protocol (虚拟路由冗余协议), 主要用来实现路由备份, 可以在同一组多个路由器之间确定一个虚拟路由器 IP 地址, 增强网关的稳定性。

2. 路由器应用中的 NAT 指的是什么, 有哪几种类型?

答案:

NAT 即 Network Address Translation (网络地址转换), 用来实现内网私有 IP 地址与外网公有 IP 地址的转换, 从而实现内网与外网的互通。可以实现局域网主机共享网关的公网 IP 地址接入互联网, 也可以面向互联网发布本来位于局域网内的企业服务器; 在此过程中隐藏了内部网络的结构, 增强了企业网络的安全性。

NAT 类型包括: 静态 NAT、动态 NAT (包括 PNAT)。

3. 网络设备上的 ACL 技术指的是什么, 有哪几种类型、各自的特点?

答案:

ACL 即 Access Control List (访问控制列表), 主要用来匹配并过滤特征流量。

常见类型包括基本 ACL、扩展 ACL。基本 ACL 只能匹配 IP 头部中的源 IP 地址; 扩展 ACL 可以同时匹配 IP 头部中的源 IP 地址和目标 IP 地址, 以及传输层协议的内容, 控制流量更加精确。

4. OSPF 指的是什么，在路由器上是怎么工作的？

答案：

OSPF 即 Open Shortest Path First (开放式最短路径优先协议)，是一种动态建立路由表条目的路由协议，用在公司网络内部快速形成一个最短、无环、三层转发路径。

路由器上启用 OSPF 路由协议以后，其工作过程主要包括三个环节：

- 1) 首先建立 OSPF 邻接表
- 2) 其次同步 OSPF 数据库
- 3) 最后计算 OSPF 路由表

5. IPv6 地址的总量是多少，如何表示？

答案：

IPv6 即第六代 IP 协议，IPv6 地址使用 128 个二进制位表示，所以总量为 2 的 128 次方。表示 IPv6 地址时，采取冒号分隔的 16 进制数形式。

6. OSPF 协议与 BGP 协议有哪些区别？

答案：

OSPF 与 BGP 都是动态路由协议，都是用来快速学习路由表条目。

两者的主要区别体现在以下几个方面：

- OSPF 为内部网关协议；BGP 为外部网关协议。
- OSPF 基于链路状态计算路由；BGP 本身不计算路由，而是把其他协议生成的路由条目拿来用。
- OSPF 适用于单一自治系统 (内部网)；BGP 适用于多个自治系统，比如联通网、电信网之间。
- OSPF 基于 IP 协议组播，协议号是 89；BGP 基于 TCP 封装，端口号 179。
- OSPF 工作在 OSI 模型的第 3 层；BGP 工作在 OSI 模型的第 7 层。

阶段 3-1、云网服务管理

1. 缓存 DNS 与权威 DNS 有什么区别？一般用户在上网时，DNS 解析过程是怎样的？

答案：

权威/官方 DNS：至少管理一个 DNS 区域，需要 IANA 等官方机构授权；比如根域 DNS、一级域 DNS、二级域 DNS 服务器等等。

缓存 DNS：无需管理任何 DNS 区域，但是能够替客户机查询，通过缓存、复用查询结果来提高客户机体验的响应速度；比如 ISP 服务商、企业局域网。

用户上网时的 DNS 解析过程，按照优先顺序如下：

- 1) 首先检查本机的 DNS 缓存（内存中的记录）
- 2) 然后检查本机的 hosts 文件
- 3) 然后向网络配置中指明的首选 DNS 服务器（企业或 ISP 的缓存 DNS）提交查询
- 4) 由首选 DNS 发起递归查询（问另一个缓存 DNS）或迭代（问根、一级、二级、.....DNS）查询，最终返回解析结果

2. 动态网站与静态网站有什么区别，http 平台要支持 PHP 程序需要具备哪些条件？

答案：

静态网站：浏览器通过 URL 访问到的网页内容固定不变，对应服务端静态提供的资源文件，主要包括.txt 文本、.html 网页、.jpg|.png 图片、.zip|.tar.gz 压缩文件等等。

动态网站：浏览器通过 URL 访问到的网页内容动态变化，对应服务端的网页程序动态生成的资源文件，主要包括 .php、.jsp、.asp、.wsgi 等不同网页语言编写的程序。

支持 PHP 程序：安装 httpd、php、php-mysql 软件包

3. 是否了解 Zabbix 监控系统，它是如何获取路由交换设备或 Linux 主机信息的？

答案：

Zabbix 是一套集中展示网络设备、主机信息的开源监控平台，通过 C/S 模式采集数据，通过 B/S 模式在 WEB 端展示和配置。

由 zabbix server 通过 SNMP, zabbix agent, ping, 端口监视等方法获取被监控设备信息。

zabbix agent 需要安装在被监控的目标服务器上，主要完成硬盘、内存、CPU 等硬件信息的收集。

而对于路由器、交换机等网络设备，则通过 SNMP 协议向 zabbix server 提供监控信息。

4. 如何配置 httpd 服务器支持多个网站？

答案：

在同一套 Web 服务器上提供多个网站的技术称为虚拟主机，标配的 httpd 并不支持虚拟主机。

若需要 httpd 支持多个 Web 网站，需要添加如下配置（每一个站点添加一段）：

```
<VirtualHost *:80>
    ServerName 此虚拟站点的 DNS 名称
    DocumentRoot 此虚拟站点的网页根目录
</VirtualHost>
```

5. 在 CentOS7 或 RHEL7 服务器上，如何控制系统服务的开启、关闭及开机自动运行？

答案：

控制系统服务的开启、关闭：

```
# systemctl start 服务名 XX... //启动 XX 服务
# systemctl stop 服务名 XX... //停止 XX 服务
# systemctl status 服务名 XX... //查看 XX 服务的状态
# systemctl restart 服务名 XX... //重启 XX 服务
```

设置系统服务开机是否自动运行：

```
# systemctl status 服务名 XX... //查看 XX 服务的状态
# systemctl restart 服务名 XX... //重启 XX 服务
```


6. 如何为一台 CentOS7 或 RHEL7 服务器添加新的软件源？

答案：

```
# vim /etc/yum.conf
...
gpgcheck = 0                                //禁止软件签名检查
# yum-config-manager --add-repo 软件源的 URL 网址    //添加新配置
# yum repolist                                //确认仓库列表
```

阶段 3-2、数据库管理

1. 对于 MySQL 或 MariaDB 数据库服务器，如何为管理账号 root 设置密码？

答案：

可以使用 mysqladmin 工具，修改密码参考如下操作：

```
# mysqladmin -uroot -p 旧密码 password '旧密码'
```

2. 管理 MySQL 或 MariaDB 数据库服务器时，如何创建新库并授权用户？

答案：

以管理账号 root 连接数据库，建库、授权操作分别使用 CREATE、GRANT，例如：

```
MariaDB [(none)]> CREATE DATABASE 数据库名;
MariaDB [(none)]> GRANT all ON 数据库名.表名 TO 用户名@客户机地址 IDENTIFIED BY '密码';
```

3. 使用 SQL 指令在工资表 salary 中查询月薪资 yuexin 超过 10000 元的员工名单？

答案：


```
MariaDB [(none)]> SELECT * FROM salary WHERE yuexin > 10000;
```

4. 在 MySQL 或 MariaDB 数据库服务器上 ,如何删除密码为空的 root 用户记录 ?

答案 :

```
MariaDB [(none)]> DELETE FROM mysql.user WHERE User='root' AND Password='';
```

5. 如果忘记了 MySQL 或 MariaDB 数据库的管理密码 , 如何恢复 ?

答案 :

基本恢复思路 :

- 1) 首先停止数据库系统服务
- 2) 然后绕过授权直接开启 mysqld_safe 程序 (比如 mysqld_safe --skip-grant-tables)
- 3) 然后使用 mysql 连接数据库 , 通过 grant 重新为用户 root 授权 , 刷新授权表
- 4) 最后关闭 mysqld_safe 进程 , 正常启动数据库系统服务

6. 简述 MySQL 或 MariaDB 数据库的备份与恢复操作 ?

答案 :

备份操作使用 mysqldump 命令 , 例如 :

```
# mysqldump -u 用户名 -p 数据库名 > 备份.sql
```

恢复操作使用 mysql 命令 , 例如 :

```
# mysql -u root 数据库名 < 备份.sql
```

阶段 3-3、网络安全

1. ARP 欺骗、中间人攻击是基于哪种方式实现的？

答案：

这两种方式都是针对 ARP 地址解析协议实施的，主要见于企业局域网环境。

交换网络中主机之间的通信依赖于 ARP 缓存表，其中记录了网络内不同 IP 地址的 MAC 地址以及交换机接口，而 ARP 缓存表的更新比较被动（来源于通信发起方主机），非常容易受到攻击者干扰。

如果攻击者针对受害主机发送大量的虚假“IP->MAC”记录，就可能导致受害主机的网络通信异常，构成 ARP 欺骗攻击。

如果攻击者针对通信双方同时进行 ARP 欺骗，可以进一步诱使通信双方把信息都转发给攻击者主机，从而构成 ARP 中间人攻击，这种攻击方式可能导致敏感信息泄露。

2. 是否熟悉华为防火墙，其默认的安全区域有哪些？

答案：

- Untrust(非受信任区域)：安全级别为 5，通常用于定义互联网流量。
- DMZ (非军事化区域)：安全级别 50，通常用于定义服务器所在区域。
- Trust(受信任区域)：安全级别 85，通常用于定义内网所在区域。
- Local(本地区域)：安全级别 100，该区域主要定义，设备自身发启的流量，或者是抵达设备自身流量。比如 Telnet、SNMP、NTP、IPsecVPN 等流量。

3. DoS 攻击、DDoS 攻击分别指的是什么？

答案：

DoS 即 Deny of Service (拒绝服务)，指的是通过任何一种方式，最终导致目标系统失去响应，从而无法为正常用户提供服务或资源的攻击。DDoS 即 Distribute DoS (分布式拒绝服务)，指的是从分散在互联网各地的大量主机同时发起针对同一个目标的 DoS 攻击。

DoS 攻击中比较常见的是洪水方式，如 SYN Flood。

SYN Flood 攻击利用 TCP 协议三次握手的原理，发送大量伪造源 IP 地址的 SYN，服务器每收到一个 SYN 就要为这个连接信息分配核心内存并放入半连接队列，然后向源地址返回 SYN + ACK，并等待源端返回 ACK。由于源地址是伪造的，所以源端永远都不会返回 ACK。如果短时间内接收到的 SYN 太多，半连接队列就会溢出，操作系统就会丢弃一些连接信息。这样正常的客户发送的 SYN 请求连接也会被服务器丢弃。

4. VPN 指的是什么，主要用在什么场合？

答案：

VPN 即 Virtual Private Network (虚拟专用网)，指的是在两个网络实体之间建立的一种长距离、受保护的专用连接。这两个实体可以通过点到点的链路直接相连，也可以跨越不安全的 Internet 相连。

VPN 主要应用于以下场合：

- 跨国企业、跨城市企业的分公司之间的企业内部网络互连
- 移动办公/出差员工与企业总部内部网络的互连
- 基于安全目的需要经过专用/加密通道访问某些特定网站

5. IDS 与 IPS 分别指的是什么，两者有什么区别？

答案：

入侵检测系统 (Intrusion Detection System , IDS) 对入侵行为发现 (告警) 但不进行相应的处理。

入侵防护系统 (Intrusion Prevention System , IPS) 对入侵行为发现并进行相应的防御处理。

6. 防火墙上的 QoS 管理指的是什么，有什么好处？

答案：

QoS 即 Quality of Service (服务质量)，指的是在防火墙对网络中的流量按照一定的规则进行分类，并对这些流量进行带宽的预留和保证的技术。通过 QoS 管理措施，可以确保特征流量在网络中高效率、低延迟的转发，对垃圾流量进行及时处理。