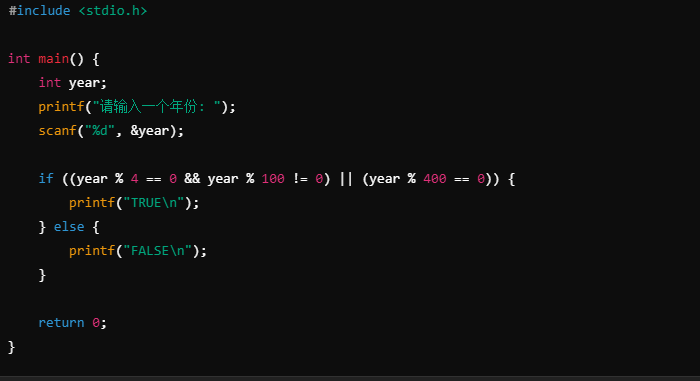
## 2024年真题解析

1. 编程题
2. 判别闰年



### 逻辑说明：

* **普通闰年**：能被 4 整除但不能被 100 整除。
* **世纪闰年**：能被 400 整除。
* 其他情况都不是闰年。

手写代码易错点：scanf函数中的取址符号&容易漏写。

1. 循环读入学生成绩，如果输入-1则停止输入，最后输出总成绩和平均成绩



3.分析下列程序异常及可能的输出

1. 分析udp相关的程序和可能输出，并判断该报文是否可以在[以太网](https://zhida.zhihu.com/search?content_id=241626467&content_type=Article&match_order=1&q=%E4%BB%A5%E5%A4%AA%E7%BD%91&zhida_source=entity" \t "https://zhuanlan.zhihu.com/p/_blank)中一次性传输

## ****程序分析****

### ****1. 代码解析****

该代码定义了一个 udp 结构体，并使用一个 udph 变量进行初始化。代码的主要作用是：

**定义 UDP 头部结构：**

struct udp {

short source\_port;

short desport\_port;

short len;

short check;

};

* 1. source\_port: 源端口（2 字节）
  2. desport\_port: 目的端口（2 字节）
  3. len: UDP 长度字段（2 字节）
  4. check: 校验和（2 字节）
  5. 结构体总大小应为 8 字节，但可能会因**结构体对齐**而增加（视编译器而定）。

**初始化 UDP 头部**

struct udp udph = {

0x100, // 源端口

0x200, // 目的端口

0x8000, // 长度字段

0x0 // 校验和

};

这里 len 赋值 0x8000（即 32768），表示该 UDP 报文长度为 32768 字节（包括 UDP 头部 + 数据）。

**输出** len **字段的值**

printf("len is %d", udph.len);

udph.len 的值是 0x8000（即 32768）。

**打印 UDP 结构体的内存数据**

char \*pt = (char \*)&udph;

for(int i = 0; i < sizeof(udph); i++) {

printf("%.02X ", 0xff & \*pt++);

}

该 for 循环按**字节**遍历 udph 结构体，并以十六进制格式打印其内容。

### ****2. 可能的程序输出****

#### ****(1)**** len ****的打印****

len is 32768

#### ****(2) UDP 头部的十六进制数据****

假设 **小端存储**（Little Endian，如 x86 架构），则：

* 0x100（源端口）存储为 00 01
* 0x200（目的端口）存储为 00 02
* 0x8000（长度字段）存储为 00 80
* 0x0（校验和）存储为 00 00

因此，输出的十六进制数据为：

00 01 00 02 00 80 00 00

如果是 **大端存储**（Big Endian），则：

01 00 02 00 80 00 00 00

具体输出取决于 CPU 的字节序。

## ****3. UDP 报文是否能在以太网中一次性传输？****

### ****以太网帧限制****

在 **以太网（Ethernet）** 传输中：

* **最小帧长**：64 字节
* **最大帧长**（MTU, Maximum Transmission Unit）：通常是 **1500 字节**（不包括以太网帧头）。
* **UDP 头部大小**：固定 **8 字节**。
* **UDP 负载最大值**：
  + IPv4 下，最大 **65507 字节**（65535 - 20（IP 头）- 8（UDP 头））。
  + IPv6 下，最大 **65527 字节**。

### ****判断是否可一次性传输****

#### ****UDP 报文的总长度****

代码中的 len 赋值 0x8000，即 **32768 字节**，远超 **1500 字节的以太网 MTU**。

#### ****传输情况****

* 以太网 **无法一次性传输 32768 字节的数据**，因为它远超 MTU（1500 字节）。
* **必须进行 IP 分片**：
  + **IPv4** 可以将数据分片，每个片最大 **1500 字节**，然后由接收端重新组装。
  + **IPv6** 不支持中间路由器分片，发送端必须自己分片或使用 **Path MTU Discovery（PMTUD）**。

#### ****总结****

该 **UDP 报文不能在以太网中一次性传输**，必须进行 **IP 分片** 或使用 **更大的 MTU（如 Jumbo Frame）** 才能发送。

1. [DNS劫持](https://zhida.zhihu.com/search?content_id=241626467&content_type=Article&match_order=1&q=DNS%E5%8A%AB%E6%8C%81&zhida_source=entity" \t "https://zhuanlan.zhihu.com/p/_blank)的工作原理和应对措施

## ****DNS 劫持的工作原理和应对措施****

### ****一、DNS 劫持的工作原理****

DNS（Domain Name System，域名系统）用于将域名解析为 IP 地址。当 DNS 被劫持时，攻击者可以篡改 DNS 解析结果，将用户引导至恶意网站，以实施**钓鱼攻击、信息窃取、流量劫持**等恶意行为。

DNS 劫持主要通过以下方式实现：

**本地劫持（Local Hijacking）**

**方法**：恶意软件或病毒感染用户计算机，修改本地的 hosts 文件或 DNS 服务器地址，使 DNS 请求被篡改。

**影响**：用户访问合法网站时，被重定向到仿冒网站，可能会泄露账号密码等敏感信息。

**路由器劫持（Router Hijacking）**

**方法**：攻击者利用默认密码、漏洞或远程管理功能，侵入家庭或企业路由器，修改其 DNS 服务器地址。

**影响**：连接到该路由器的所有设备都会受到 DNS 劫持影响。

**ISP 劫持（Internet Service Provider Hijacking）**

**方法**：某些 ISP（互联网服务提供商）为了广告收益或其他目的，拦截并修改 DNS 查询结果，将用户重定向到广告页面或自家搜索引擎。

**影响**：用户可能被强制看到广告，甚至访问受限网站时会被重定向。

**中间人攻击（MITM, Man-In-The-Middle）**

**方法**：攻击者在网络传输过程中拦截 DNS 请求，并返回伪造的 DNS 响应。

**影响**：用户被重定向到恶意网站，可能导致数据泄露或金融诈骗。df

**DNS 服务器劫持（DNS Server Hijacking）**

**方法**：攻击者侵入合法的 DNS 服务器，篡改域名解析记录，将合法网站的 IP 地址替换为恶意服务器的地址。

**影响**：影响面广，全球用户可能被引导至恶意网站。

### ****二、应对措施****

为防止 DNS 劫持，可以采取以下措施：

#### ****1. 个人用户防护****

✅ **使用安全的 DNS 服务器**

✅ **检查本地 DNS 配置**

确保 DNS 服务器地址未被篡改。

✅ **修改路由器默认密码**

登录路由器管理页面（通常是 192.168.1.1），修改默认管理员密码，防止黑客篡改 DNS 设置。

✅ **避免访问 HTTP 网站**

**优先使用 HTTPS**，如果网站未启用 HTTPS，则需警惕可能的劫持攻击。

✅ **定期检查** hosts **文件**

#### ****2. 企业级防护****

✅ **部署企业级 DNS 解决方案**

✅ **防火墙与入侵检测**

✅ **定期监测 DNS 解析记录**

✅ **使用 VPN 或专有网络**

通过加密隧道防止 ISP 或中间人攻击劫持 DNS 查询。

### ****三、总结****

| **DNS 劫持方式** | **攻击原理** | **影响** | **应对措施** |
| --- | --- | --- | --- |
| **本地劫持** | 恶意软件篡改 hosts 文件或 DNS 配置 | 访问被重定向到钓鱼网站 | 及时查杀病毒，检查 hosts，修改 DNS 设置 |
| **路由器劫持** | 黑客篡改路由器 DNS 设置 | 所有连接设备均被劫持 | 修改默认密码，关闭远程管理 |
| **ISP 劫持** | 运营商修改 DNS 响应 | 广告注入，流量重定向 | 使用安全 DNS 服务器（Google DNS、Cloudflare） |
| **中间人攻击** | 拦截 DNS 请求并伪造响应 | 伪造网站，窃取敏感信息 | 启用 DoH/DoT，加密 DNS 请求 |
| **DNS 服务器劫持** | 攻击者篡改权威 DNS 服务器记录 | 影响全球用户 | 使用 DNSSEC，定期检查解析记录 |