

# 中国刑事警察学院硕士研究生招生考试

## 《公安技术（二）》考试大纲

（2023 年 8 月）

公安技术（二）（科目代码：805）包含刑事科学技术总论与计算机网络两部分考核内容。试卷满分为 150 分，考试时间为 180 分钟。考查内容包括刑事科学技术总论与计算机网络两部分，其中刑事科学技术总论占 30 分，计算机网络占 120 分。考试方式为闭卷、笔试。本考试大纲分别对两部分的考核内容予以说明。

### 《刑事科学技术总论》考试大纲

#### I. 考查目标

要求考生能够掌握刑事科学技术的相关专业素质和基本能力。具体包括：

1. 了解并掌握刑事科学技术的基本概念、研究对象、研究内容、发展简史、基本原理和技术分析方法；理解掌握物证的系统属性与关联分析、物证特征的层次结构分类以及物证量化检验鉴定的相关方法。

2. 全面了解刑事科学技术所包含的电子物证技术的具体研究对象的自身特点；具体掌握各类研究对象的具体概念、检验鉴定程序、检验鉴定技术方法以及检验鉴定过程中应注意的问题。

#### II. 试卷结构

刑事科学技术总论共计 30 分，其中名词解释 10 分，简答题 20 分。

#### III. 考查内容

## 第一部分 刑事科学技术概述

### 一、刑事科学技术概论

1. 刑事科学技术的概念
2. 刑事科学技术的研究内容
3. 刑事科学技术的技术体系
4. 刑事科学技术的任务和作用

### 二、刑事科学技术的基本原理

1. 物质交换原理
2. 种属识别原理
3. 同一认定原理

### 三、刑事科学技术的技术分析方法

1. 形态学方法
2. 物理方法
3. 化学方法
4. 医学与生物学检验方法
5. 仪器分析方法

## 第二部分 犯罪现场勘查与物证鉴定

### 一、犯罪现场勘查

1. 犯罪现场勘查的概念
2. 犯罪现场勘查的程序

### 二、物证鉴定

1. 物证的概念、分类和保管
2. 物证在刑事案件侦破中的作用
3. 鉴定的概念和种类
4. 鉴定的程序

### 第三部分 物证关联分析与量化检验鉴定

#### 一、物证的系统属性

1. 案件系统与现场物证系统的要素
2. 物证系统的层次与结构功能

#### 二、物证的关联分析

1. 物证关联分析的依据
2. 物证系统关联分析的意义、步骤和融贯方法

#### 三、物证量化检验鉴定数学原理与量化方法

1. 物证量化检验鉴定的数学基础
2. 物证特征的层次结构分类
3. 客观概率与主观概率的概念及特点
4. 物证特征质量与数量价值定律的内涵

### IV. 参考书目

1. 单大国. 刑事科学技术（第二版） [M]. 高等教育出版社，2021

### 《计算机网络》考试大纲

#### I. 考查目标

要求考生能够具备计算机网络的相关专业素质和基本能力。具体包括：

1. 全面掌握计算机网络理论的相关知识及其内涵。
2. 正确理解计算机网络理论的重要概念、特征及其内容。
3. 准确把握计算机网络理论的基本原理和体系。
4. 灵活运用计算机网络的相关理论，准确分析、判断公安工作中的实际问题。

## II. 试卷结构

计算机网络部分共计 120 分，其中：名词解释 10 分，填空题 10 分，判断题 10 分，简答题 60 分，论述题 30 分。

## III. 考查内容

### 第一部分 计算机网络概述

#### 一、计算机网络与因特网概述

1. 网络的概念
2. 协议的概念
3. 网络的分类

#### 二、计算机网络的发展过程

1. 计算机网络的产生
2. 电路交换和分组交换
3. 因特网的发展

#### 三、计算机网络的体系结构

1. 计算机网络体系结构的形成
2. 协议与划分层次
3. 计算机网络的原理体系结构
4. OSI 与 TCP/IP 体系结构的比较

### 第二部分 物理层

#### 一、物理层的基本概念

1. 物理层的作用
2. 串行传输和并行传输

#### 二、数据通信的基础知识

1. 数据通信系统的模型

2. 有关信道的几个基本概念

三、物理层下面的传输媒体

1. 导引型传输媒体

2. 非导引型传输媒体

四、模拟传输与数字传输

1. 调制解调器

2. 数字传输系统

五、信道复用技术

六、网络接入技术

### 第三部分 数据链路层

一、使用点对点信道的数据链路层

二、点对点协议 PPP

三、使用广播信道的数据链路层

四、扩展的以太网

五、高速以太网

### 第四部分 网络层

一、网络层提供的服务

二、网际协议 IP

1. 虚拟互联网络

2. 分类的 IP 地址

3. IP 地址与硬件地址

4. 地址解析协议 ARP

5. IP 数据报的格式

6. IP 层转发分组的流程

三、划分子网和构造超网

1. 子网划分方法

2. 子网掩码

3. 设计子网

四、网际控制报文协议 ICMP

五、路由选择协议

1. 路由选择协议的作用

2. 路由选择算法的分类

3. 分层路由选择协议

4. 路由信息协议 RIP

5. 开放最短路径优先协议 OSPF

6. 路由器的结构

六、组播协议

1. 组播的概念

2. 组播的路由选择

七、虚拟专用网 VPN 和网络地址转换 NAT

1. 虚拟专用网 VPN

2. 网络地址转换 NAT

八、IPV6 协议

1. IPV6 的概念

2. IPV6 首部

3. IPV6 编址

4. 从 IPV4 向 IPV6 过渡

## 第五部分 运输层

一、运输层协议概述

1. 进程之间的通信

2. 运输层的两个主要协议

3. 运输层的端口

二、用户数据报协议 UDP

1. UDP 概述

2. UDP 的首部格式

三、传输控制协议 TCP 概述

四、可靠传输的工作原理

五、TCP 报文段的首部格式

六、TCP 可靠传输的实现

七、TCP 的流量控制

八、TCP 的拥塞控制

九、TCP 的运输连接管理

## 第六部分 应用层

一、域名系统 DNS

1. 域名系统概述

2. 互联网的域名结构

3. 域名服务器

二、文件传输协议 FTP

1. FTP 协议概述

2. FTP 协议的基本工作原理

3. 简单文件传输协议 TFTP

三、万维网 WWW

1. 万维网概述

2. 统一资源定位符 URL

3. 超文本传输协议 HTTP

- 4. 万维网的文档
- 5. 万维网的信息检索系统

#### 四、电子邮件

- 1. 电子邮件概述
- 2. 简单邮件传送协议 SMTP
- 3. 电子邮件的信息格式
- 4. 邮件读取协议 POP3 和 IMAP
- 5. 基于万维网的电子邮件
- 6. 通用互联网邮件扩充 MIME

#### 五、动态主机配置协议 DHCP

#### 六、简单网络管理协议 SNMP

### 第七部分 网络安全

#### 一、网络安全问题概述

- 1. 计算机网络面临的安全性威胁
- 2. 安全的计算机网络
- 3. 数据加密模型

#### 二、两类密码体制

- 1. 对称密钥密码体制
- 2. 公钥密码体制

#### 三、数字签名

#### 四、鉴别

- 1. 报文鉴别
- 2. 实体鉴别

#### 五、密钥分配

- 1. 对称密钥的分配



2. 公钥的分配

## 六、互联网使用的安全协议

1. 网络层安全协议

2. 运输层安全协议

3. 应用层安全协议

## 七、系统安全：防火墙和入侵检测

1. 防火墙

2. 入侵检测系统

## IV.参考书目

1. 谢希仁. 计算机网络（第八版）[M]. 电子工业出版社，2021

## V.参考试题举例（非完整试题，仅为样式与分值说明）

### 刑事科学技术总论

#### 一、名词解释（每题 2 分，共 10 分）

1. 刑事科学技术

#### 二、简答题（每题 10 分，共 20 分）

1. 刑事科学技术的作用

### 计算机网络

#### 一、名词解释（共 10 分）

1. 计算机蠕虫

#### 二、填空题（共 10 分）

1. 在 IP 数据报首部中有三个字段负责分片和重装机制，分别是\_\_\_\_\_、\_\_\_\_\_和\_\_\_\_\_。

#### 三、判断题（共 10 分）

1. ARP 请求分组是单播发送的，ARP 响应分组是广播发送的。

四、简答题（共 60 分）

1. 一台路由器具有表 1 所示的 RIP 路由表，如果该路由器从路由器 C 接收到表 2 所示的 RIP 报文，请写出更新之后的路由表。

| 目的网络 | 距离 | 下一跳 |
|------|----|-----|
| N1   | 4  | B   |
| N2   | 2  | C   |
| N3   | 1  | F   |
| N4   | 5  | G   |

(表 1)

| 目的网络 | 距离 | 下一跳 |
|------|----|-----|
| N1   | 2  | B   |
| N2   | 4  | C   |
| N3   | 3  | F   |
| N4   | 7  | G   |

(表 2)

五、论述题（共 30 分）

1. 网络拓扑结构如图 1 所示，交换机上连接了三台主机，其中主机 1 连接在 1 号端口，主机 2 连接在 2 号端口，主机 3 连接在 3 号端口。图中给出了每台主机的 IP 地址和 MAC 地址。假设交换机刚接通电源，MAC 地址转换表中没有转换记录。请论述交换机的地址学习机制。

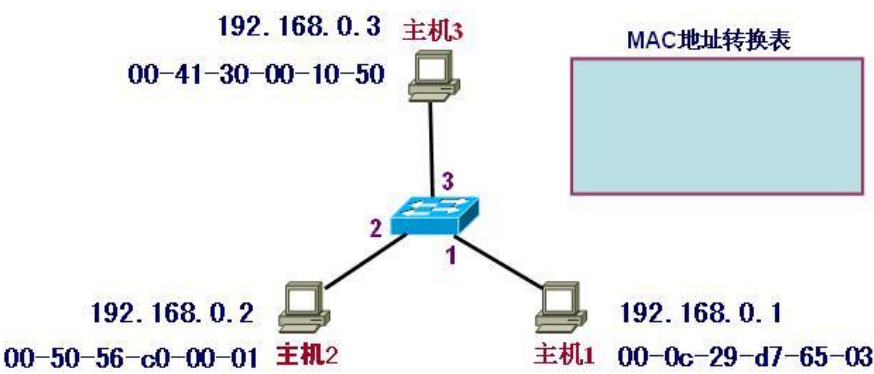


图 1

## VI. 参 考 答 案

### 刑事科学技术总论

#### 一、名词解释

##### 1. 刑事科学技术

答：刑事科学技术是以诉讼中可能成为物证的各种物质、物品、痕迹、影像为研究对象，以提供侦查线索与破案证据、查明案件事实为目的，研究应用自然科学技术手段与方法，解决犯罪现场勘查取证与分析重建、物证信息检索与分析以及相关物证专门性问题的一门学科。

#### 二、简答题

##### 1. 刑事科学技术的作用

答：刑事科学技术的作用主要有：

- （1）分析案件性质，确定是否立案；
- （2）分析作案手段、作案过程；
- （3）分析作案人的特点；
- （4）提供侦查方向；
- （5）有助于审查证人证言及犯罪嫌疑人的口供；
- （6）认定作案人、作案工具。

### 计算机网络

#### 一、名词解释

1. 一种通过网络的通信功能将自身从一个结点发送到另一个结点并自动启动运行的程序。

#### 二、填空题

1. （标识） （标志） （分片偏移）。

### 三、判断题

1. 错。

### 四、简答题

| 1. 目的网络 | 距离 | 下一跳 |
|---------|----|-----|
| N1      | 3  | C   |
| N2      | 5  | C   |
| N3      | 1  | F   |
| N4      | 5  | G   |

### 五、论述题

1. 当交换机刚接通电源时，MAC 地址表中没有转换记录。下面通过三个实例分析交换机的地址学习机制。

①主机 1 给主机 3 发送一个报文，交换机收到该报文后，在 MAC 地址转换表中添加一条记录：00-0c-29-d7-65-03 <-> 端口 1，由于 MAC 地址表中没有主机 3 的地址信息，交换机在 2、3 端口转发这个报文。

②主机 2 给主机 3 发出一个报文，交换机收到该报文后，先在 MAC 地址转换表中添加一条记录：00-50-56-c0-00-01 <->端口 2，然后在 1、3 端口转发这个报文。

③主机 3 给主机 1 发出一个报文，交换机收到该报文后，先在 MAC 地址转换表中添加一条记录：00-41-30-00-10-50 <-> 端口 3，然后根据 MAC 地址转换表中的记录在 1 号端口转发报文。

至此交换机的 MAC 地址转换表已经形成，在 MAC 地址表的形成过程中，由于地址信息不全，交换机可能会以广播的方式转发报文，这时交换机的工作性质类似集线器。当交换机的 MAC 地址转换表形成之后，交换机只在特定的端口转发报文。