计算机网络考研复习策略与知识点剖析

## 摘要

本文围绕考研计算机网络展开，系统梳理了计算机网络体系结构各层次知识点，包括 OSI 参考模型与 TCP/IP 模型、物理层基本概念及特性、数据链路层功能与机制、网络层主要功能及协议、传输层服务与协议、应用层主要协议，并对考研难点进行了分析，如物理层定理计算应用、数据链路层流量控制与可靠传输、网络层路由协议算法、传输层 TCP 协议相关内容等，为考生提供了全面的复习指导。

## 关键词

考研计算机网络；体系结构；知识点梳理；难点分析

## ABSTRACT

This paper focuses on the postgraduate entrance examination of computer networks. It systematically combs the knowledge points of each level of the computer network architecture, including the OSI reference model and TCP/IP model, basic concepts and characteristics of the physical layer, functions and mechanisms of the data link layer, main functions and protocols of the network layer, services and protocols of the transport layer, and main protocols of the application layer. It also analyzes the difficulties in the postgraduate entrance examination, such as the calculation and application of physical layer theorems, flow control and reliable transmission in the data link layer, routing protocols and algorithms in the network layer, and related contents of the TCP protocol in the transport layer. It provides comprehensive review guidance for candidates.

## Keywords

Postgraduate entrance examination of computer networks;Architecture;Knowledge points combing;Difficulty analysis

## 一、引言

计算机网络在考研中占据着重要的地位。随着信息技术的飞速发展，计算机网络的应用越来越广泛，其重要性也日益凸显。对于考研的学生来说，掌握计算机网络的知识点不仅是考试的要求，更是为今后的学习和工作打下坚实的基础。

本文旨在通过对计算机网络知识点的梳理和难点分析，为考生提供全面的复习指导。计算机网络涉及的内容广泛，包括计算机网络体系结构、物理层、数据链路层、网络层、传输层和应用层等。每个层次都有其特定的功能和协议，考生需要深入理解这些内容，才能在考试中取得好成绩。

在复习计算机网络时，考生需要注重理论与实践的结合。一方面，要掌握计算机网络的基本概念、原理和协议；另一方面，要通过实验和案例分析，加深对知识点的理解和应用。此外，考生还需要关注计算机网络的最新发展动态，了解新技术和新应用，为考试和未来的学习做好准备。

## 二、计算机网络体系结构

### （一）OSI 参考模型与 TCP/IP 模型

1. OSI 参考模型的层次结构、各层功能及特点。
   1. OSI 参考模型划分为 7 层结构，分别是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。
   2. 物理层：主要定义物理设备标准，如网线的接口类型、光纤的接口类型、各种传输介质的传输速率等。其主要作用是传输比特流，即由 1、0 转化为电流强弱来进行传输，到达目的地后再转化为 1、0。物理层的数据单位是比特。典型设备有光纤、同轴电缆、双绞线、中继器和集线器。
   3. 数据链路层：主要将从物理层接收的数据进行 MAC 地址（网卡的地址）的封装与解封装。常把这一层的数据叫做帧。在这一层工作的设备是交换机，数据通过交换机来传输。其功能包括在物理层提供的比特流的基础上，通过差错控制、流量控制方法，使有差错的物理线路变为无差错的数据链路，即提供可靠的通过物理介质传输数据的方法。
   4. 网络层：主要将从下层接收到的数据进行 IP 地址的封装与解封装。在这一层工作的设备是路由器，常把这一层的数据叫做数据包。其功能是在数据链路层提供的两个相邻端点之间的数据帧的传送功能上，进一步管理网络中的数据通信，控制数据链路层与传输层之间的信息转发，建立、维持和终止网络的连接，将数据设法从源端经过若干个中间节点传送到目的端，从而向传输层提供最基本的端到端的数据传输服务。
   5. 传输层：定义了一些传输数据的协议和端口号，如 TCP 和 UDP。主要是将从下层接收的数据进行分段和传输，到达目的地址后再进行重组。常常把这一层数据叫做段。其功能是向用户提供可靠的端到端的差错和流量控制，保证报文的正确传输，同时向高层屏蔽下层数据通信的细节，即向用户透明地传送报文。
   6. 会话层：通过传输层（端口号：传输端口与接收端口）建立数据传输的通路。主要在系统之间发起会话或者接受会话请求。
   7. 表示层：主要是进行对接收的数据进行解释、加密与解密、压缩与解压缩等，也就是把计算机能够识别的东西转换成人能够能识别的东西，如图片、声音等。
   8. 应用层：主要是一些终端的应用，比如说 FTP（各种文件下载），WEB（IE 浏览），QQ 之类的，可以把它理解成我们在电脑屏幕上可以看到的东西，是终端应用。
2. TCP/IP 模型的层次结构、各层功能及特点。
   1. TCP/IP 模型划分为 4 层结构，分别为应用层、传输层、互联网层和主机到网络层。
   2. 主机到网络层：这一层的功能是将数据从主机发送到网络上，相当于 OSI 模型中的物理层和数据链路层。
   3. 互联网层：是 TCP/IP 模型中的第二层。选择了分组交换技术作为解决方案，定义了标准的分组格式和接口参数，只要符合这样的标准，分组就可以在不同网络间实现漫游。
   4. 传输层：不仅可以提供不同服务等级、不同可靠性保证的传输服务，而且还可以协调发送端和接收端之间的传输速度差异。同 OSI 传输层。
   5. 应用层：由于并不是所有的网络服务都需要会话层和表示层的功能，所以这些功能逐渐被融合到 TCP/IP 模型中应用层的那些特定的网络服务中。是网络操作者的应用接口，为应用进程提供服务，对不同种类的应用程序使用不同协议，还能加密、解密、格式化数据，建立或解除与其他节点的联系，节省网络资源。
3. 对比 OSI 参考模型与 TCP/IP 模型的异同。
   1. 相同点：
      1. 两个协议都分层。
      2. OSI 参考模型的网络层与 TCP/IP 互联网层的功能几乎相同。
      3. 以传输层为界，上层都依赖传输层提供端到端的，与网络环境无关的传输服务。
   2. 不同点：
      1. TCP/IP 并未对网络接口层细分。
      2. OSI 分层模型在前，协议规范灾后。
      3. OSI 对服务和协议做了特别明显的区别，而 TCP/IP 并没有细分。

## 三、物理层

### （一）基本概念

1. 数据、信号、码元、信源、信道、信宿的定义。
   1. 数据：是指传送信息的实体。
   2. 信号：是指数据的电气或电磁表现，是数据在传输过程中的存在形式。
   3. 码元：码元是指用一个固定时长的信号波形（数字脉冲），代表离散数值的基本波形，是数字通信中数字信号的计量单位。例如，在使用二进制编码时，只有两种不同的码元状态，一种代表 0 状态，另一种代表 1 状态。
   4. 信源：是产生和发送数据的源头。
   5. 信道：是信号的传输媒介，向某一个方向传送信息的介质。
   6. 信宿：接收数据的终点。
2. 速率、波特、带宽的概念及转换关系。
   1. 速率也叫数据率，是数据的传输速率，表示单位时间内传输的数据量。可以用码元传输速率和信息传输速率表示。
   2. 码元传输速率，又称码元速率、波形速率等，它表示单位时间内数字通信系统所传输的码元个数（也可称为脉冲个数或信号变化的次数），单位是波特。
   3. 信息传输速率，又称信息速率、比特率等，它表示单位时间内数字通信系统传输的二进制码元个数（即比特数），单位是比特/秒（b/s）。若一个码元携带 n bit 的信息量，则 M Baud 的码元传输速率所对应的信息传输速率为 M×n bit/s。
   4. 带宽原是指信号具有的频带宽度，单位是赫兹（Hz）。在实际网络中，带宽表示单位时间内从网络中的某一点到另一点所能通过的“最高数据率”。
3. 奈奎斯特定理和香农定理的应用。
   1. 奈奎斯特定理指出在理想低通（没有噪声、带宽有限）的信道中，极限码元传输率为 2W Baud，其中 W 是理想低通信道的带宽，单位为 Hz。若用 V 表示每个码元离散电平的数目，则极限数据率为理想低通信道下的极限数据传输率 = 2Wlog₂V（单位：b/s）。
   2. 香农定理给出了带宽受限且有高斯自噪声干扰的信道的极限数据传输速率。信道的极限数据传输速率 = Wlog₂(1 + S/N)（单位：b/s），式中，W 为信道的带宽，S 为信道所传输信号的平均功率，N 为信道内部的高斯噪声功率。S/N 为信噪比，即信号的平均功率和噪声的平均功率之比，信噪比 = 10log₁₀(S/N)（单位：dB）。
   3. 在实际应用中，若题目多是求数据极限传输速率，看条件选择使用奈奎斯特定理或香农定理。若两种都可以用，则分别计算，取较小的极限传输速率。
4. 编码与调制的方式及特点。
   1. 数字数据编码为数字信号：
      1. 非归零码，高 1 低 0，编码容易实现，但没有检错功能，且无法判断一个码元的开始和结束，以至于收发双方难以保持同步。
      2. 曼彻斯特编码，将一个码元分成两个相等的间隔，前一个间隔为低电平后一个间隔为高电平表示码元 1；码元 0 则正好相反。也可以采用相反的规定。该编码的特点是在每一个码元的中间出现电平跳变，位中间的跳变既作时钟信号（可用于同步），又作数据信号，但它所占的频带宽度是原始的基带宽度的两倍。
      3. 差分曼彻斯特编码，同 1 异 0，常用于局域网传输，其规则是：若码元为 1，则前半个码元的电平与上一个码元的后半个码元的电平相同，若为 0，则相反。该编码的特点是，在每个码元的中间，都有一次电平的跳转，可以实现自同步，且抗干扰性强于曼彻斯特编码。
      4. 4B/5B 编码，比特流中插入额外的比特以打破一连串的 0 或 1，就是用 5 个比特来编码 4 个比特的数据，之后再传给接收方，编码效率为 80%。只采用 16 种对应 16 种不同的 4 位码，其他的 16 种作为控制码（帧的开始和结束，线路的状态信息等）或保留。
   2. 数字数据调制为模拟信号：
      1. 幅移键控（ASK），通过改变载波信号的振幅来表示数字信号 1 和 0，而载波的频率和相位都不改变。比较容易实现，但抗干扰能力差。
      2. 频移键控（FSK），通过改变载波信号的频率来表示数字信号 1 和 0，而载波的振幅和相位都不改变。容易实现，抗干扰能力强，目前应用较为广泛。
      3. 相移键控（PSK），通过改变载波信号的相位来表示数字信号 1 和 0，而载波的振幅和频率都不改变。它又分为绝对调相和相对调相。
      4. 正交振幅调制（QAM），在频率相同的前提下，将 ASK 与 PSK 结合起来，形成叠加信号。
   3. 模拟数据编码为数字信号：常用于对音频信号进行编码的脉码调制（PCM），主要包括采样、量化和编码三个步骤。其中采样频率 fₘₛ必须大于或等于最大频率 f 的两倍（采样定理又称为奈奎斯特定理）。
   4. 模拟数据调制为模拟信号：为了实现传输的有效性，可能需要较高的频率。这种调制方式还可以使用频分复用（FDM）技术，充分利用带宽资源。
5. 电路交换、报文交换、分组交换的区别。
   1. 电路交换：在进行数据传输前，两个结点之间必须先建立一条专用（双方独占）的物理通信路径。优点是通信时延小、有序传输、没有冲突、适用范围广、实时性强、控制简单；缺点是建立连接时间长、线路独占，使用效率低、灵活性差、难以规格化（只能保证顺序传输，不能保证无差错传输）。
   2. 报文交换：数据交换的单位是报文，报文携带有目标地址、源地址等信息。报文交换在交换结点采用的是存储转发的传输方式。优点是无需建立连接、动态分配线路、提高线路可靠性、提高线路利用率、提供多目标服务；缺点是引起转发时延、要求网络结点需要有较大的缓存空间。
   3. 分组交换：同报文交换一样，分组交换也采用了存储转发方式，但解决了报文交换中大报文传输的问题。分组交换限制了每次传送的数据块大小的上限。优点是无建立时延、线路利用率高、简化了存储管理（相对于报文交换）加速传输、减少了出错几率和重发数据量（因为分组较短）；缺点是存在传输时延、需要传输额外的信息量、当分组交换采用数据报服务时，可能出现失序、丢失或重复分组。
6. 数据报与虚电路的特点。
   1. 数据报特点（无连接不可靠）：发送分组前不需要建立连接、不同的分组可以走不同的路径，也可以按不同的顺序到达目的结点。网络尽最大努力交付，传输不保证可靠性，所以可能丢失、发送的分组中要包括发送端和接收端的完整地址，以便可以独立传输、分组在交换结点存储转发时，需要排队等候处理，这会带来一定的时延、收发双方不独占某一链路，资源利用率较高。
   2. 虚电路特点（有连接可靠）：在分组发送之前，发送方和接收方建立一条逻辑上相连的虚电路、虚电路通信链路的建立和拆除需要时间开销、虚电路提供了可靠的通信功能，能保证每个分组正确且有序到达、即当网络中的某个结点或某条链路出故障而彻底失效时，则所有经过该结点或该链路的虚电路将遭到破坏。分组首部并不包含目的地址，而是包含虚电路标识符，相对数据报方式开销小、两个端系统之间也可以有多条虚电路为不同的进程服务。
7. 传输介质的分类及特点。
   1. 传输介质分为导向性传输介质和非导向性传输介质。
   2. 导向性传输介质：
      1. 双绞线：由两根采用一定规则并排绞合的、相互绝缘的铜导线组成。绞合可以减少对相邻导线的电磁干扰。加上金属屏蔽层的为屏蔽双绞线（STP），无屏蔽层为非屏蔽双绞线（UTP）。价格便宜，是最常用的传输介质之一，在局域网和传统电话网中普遍使用。通信距离一般为几公里到数十公里。距离太远时，对于模拟传输，要用放大器放大衰减的信号；对于数字传输，要用中继器将失真的信号整形。
      2. 同轴电缆：由导体铜质芯线、绝缘层、网状编织屏蔽层和塑料外层组成。按特性阻抗数值的不同，通常将同轴电缆分为 50Ω 同轴电缆和 75Ω 同轴电缆。50Ω 同轴电缆主要用于传送基带数字信号，在局域网中得到广泛应用；75Ω 同轴电缆主要用于传送宽带信号，主要用于有线电视系统。抗干扰特性比双绞线好，价格比双绞线贵。
      3. 光纤：光纤中传递的是光脉冲。光纤通信就是利用光导纤维（简称光纤）传递光脉冲来进行通信。有光脉冲表示 1，无光脉冲表示 0。光纤主要由纤芯（实心的）和包层构成，当光线从高折射率的介质射向低折射率的介质时，若入射角足够大，就会出现全反射，光也就沿着光纤传输下去。光纤的特点有传输损耗小，中继距离长，对远距离传输特别经济；抗雷电和电磁干扰性能好；无串音干扰，保密性好，也不易被窃听或截取数据；体积小，重量轻。
   3. 非导向性传输介质：包括无线电波，微波，红外线和激光等。
8. 接口特性的四个方面。
   1. 机械特性：定义物理连接的特性，规定物理连接时所采用的规格、接口形状、引线数目、引脚数量和排列情况。
   2. 电气特性：规定传输二进制位时，线路上信号的电压范围、阻抗匹配、传输速率和距离限制等。
   3. 功能特性：指明某条线上出现的某一电平表示何种意义，接口部件的信号线的用途。
   4. 规程特性：定义各条物理线路的工作规程和时序关系。
9. 常见接口标准。
   1. 无明确提及的常见接口标准写作素材，暂无法详细阐述。
10. 物理层设备（中继器、集线器）的作用。
    1. 中继器：是连接网络线路的一种装置，常用于两个网络节点之间物理信号的双向转发工作。主要完成物理层的功能，负责在两个节点的物理层上按位传递信息，完成信号的复制、调整和放大功能，以此来延长网络的长度。中继器是模拟设备，用于连接两根电缆段。中继器不理解帧、分组和头的概念，他们只理解电压值。
    2. 集线器：是中继器的一种形式，区别在于集线器能够提供多端口服务，也称为多口中继器。集线器在 OSI/RM 中的物理层。集线器的主要功能是对接收到的信号进行再放大，扩大网络的传输距离，同时把所有的节点集中在以它为中心的节点上。集线器实质上是一个中继器，采用广播方式发送数据，当它要向某节点发送数据时，不是直接把数据发送到目的节点，而是把数据包发送到与集线器相连的所有节点。

## 四、数据链路层

### （一）功能概述

1. 差错控制的方法及检错编码（CRC 重点掌握）。
   1. 数据在传输过程中可能会出现差错，数据链路层需要采用差错控制的方法来确保数据的准确性。差错控制主要包括检错编码和纠错编码。检错编码只能发现错误，不能纠正错误；纠错编码不仅能发现错误，还能纠正错误。
   2. 奇偶校验码是一种简单的检错编码方法。它分为奇校验和偶校验。奇校验是指原始码流加上校验位后，1的个数为奇数；偶校验是指原始码流加上校验位后，1的个数为偶数。奇偶校验码只能检查出奇数个比特错误，检错能力为 50%。例如，传输字符‘S’的 ASCII 码 1100101，使用奇校验码，在数据前添加 1 位冗余位 1，表明 1 的个数为奇数。如果接收到的数据中 1 的个数是偶数个，此时就能检测出数据错误；如果接收到的数据中 1 的个数为奇数个，那么就会判断接收的数据是正确的，无法检查出偶数个错误。
   3. CRC（循环冗余码）是一种常用的检错编码方法。发送端要传输的数据除以生成多项式，得到的余数就是 FCS（帧检验序列），也就是冗余码。最终发送的数据是要传输的数据加上冗余码。接收端将接收到的数据除以同样的生成多项式，如果余数为 0，说明传输过程中没有错误；如果余数不为 0，说明数据帧错误，且不知道哪里出现错误，丢弃该数据帧，重新发送。例如，要发送的数据是 1101011011，采用 CRC 校验，生成多项式是 10011。首先在发送的数据后补 4 个 0，然后进行模 2 除法。计算得出余数为 1110，那么最终发送的数据就是 11010110111110。接收端接收数据并校验，将数据与生成多项式相除，如果余数为 0 说明该数据帧没有差错；余数不为 0，说明数据帧错误，丢弃。
2. 流量控制与可靠传输机制（停止 - 等待协议、后退 N 帧协议、选择重传协议）。
   1. 较高的发送速度和较低的接收能力不匹配会造成传输出错，因此流量控制是数据链路层的一项重要工作。数据链路层的流量控制是点对点的，传输层的流量控制是端到端的。数据链路层流量控制手段是接收方收不下就不回复确认；传输层的流量控制手段是接收端给发送端一个窗口公告，告诉发送方窗口大小和缓冲区大小。
   2. 可靠传输是指发送端发啥，接收端收啥。数据链路层的可靠传输通常使用确认和超时重传两种机制来完成。确认是一种无数据的控制帧，接收方可以让发送方知道哪些内容被正确接收。超时重传是指发送方在发送某个数据帧后开启一个计时器，在一定时间内如果没有得到确认帧，就重新发送该数据帧。
   3. 停止 - 等待协议：每发送完一个帧就停止发送，等待对方的确认，在收到确认后再发送下一个帧。如果出现数据帧丢失或检测到数据帧出错，发送端会启动超时计时器，超时后重传数据帧，并保留副本。如果 ACK 丢失，发送端超时未收到确认帧会重传，接收端丢弃重复的帧并重传确认帧。如果 ACK 迟到，发送端收到重复的确认帧就丢弃。该协议简单但信道利用率低。
   4. 后退 N 帧协议（GBN）：发送方可以连续发送帧，发送窗口大小大于 1，接收窗口大小为 1。对 n 号帧的确认采用累积确认的方式，标明接收方已经收到 n 号帧和它之前的全部帧。如果出现超时，发送方重传所有已发送但未被确认的帧。接收方如果正确收到 n 号帧且按序，就为 n 帧发送一个 ACK，并将该帧中的数据部分交付给上层，其余情况都丢弃帧，并为最近按序接收的帧重新发送 ACK。
   5. 选择重传协议（SR）：为了解决 GBN 需要批量重传的问题，可以只传送出错的帧。设置单个确认，加大接收窗口，设置接收缓存，缓存乱序到达的帧。发送方从上层收到数据后，检查下一个可用于该帧的序号，如果序号位于发送窗口内，则发送数据帧；收到 ACK 后，如果该序号在窗口内，则将那个被确认的帧标记为已接收，如果窗口的下界被确认，则窗口向前移动，若有未发送帧且在窗口内，则发送这些帧。每个帧都有自己的定时器，超时事件发生后只重传一个帧。接收方将确认一个正确接收的帧而不管其是否按序，失序的帧将被缓存，并返回给发送方一个该帧的确认帧，直到所有序号更小的帧皆被收到为止，这时才可以将一批帧按序交付给上层，然后向前移动滑动窗口。
3. 介质访问控制（信道划分、随机访问、轮询访问）。
   1. 介质访问控制要完成的主要任务是，为使用介质的每个结点隔离来自同一信道上其他结点所传送的信号，以协调活动结点的传输。常见的介质访问控制方法有信道划分介质访问控制、随机访问介质访问控制和轮询访问介质访问控制。前者是静态划分信道的方法，后两者是动态分配信道的方法。
   2. 信道划分介质访问控制基本原理是将使用介质的每个设备与来自同一通信信道上的其他设备的通信隔离开来，把时域和频域资源合理地分配给网络上的设备。多路复用技术是实现信道划分介质访问控制的途径，把多个信号组合在一条物理信道上进行传输，使多个计算机或终端设备共享信道资源，提高了信道的利用率。信道划分介质访问控制分为以下 4 种：
      1. 频分多路复用（FDM）：将多路基带信号调制到不同频率载波上，再叠加形成一个复合信号的多路复用技术。用户在分配到一定的频带后，在通信过程中自始至终都占用这个频带。频分复用的所有用户在同样的时间占用不同的频率带宽资源。优点是充分利用传输介质带宽，系统效率较高；由于技术比较成熟，实现也较容易。
      2. 时分多路复用（TDM）：将时间划分为一段段等长的时分复用帧（TDM 帧），其中每一个时分复用的用户在每一个 TDM 帧中占用固定序号的时隙，所有用户轮流占用信道。类似于“并发”。改进的统计时分复用（STDM），每一个 STDM 帧中的时隙数小于连接在集中器上的用户数，各用户有了数据就随时发往集中器的输入缓存，然后集中器按顺序依次扫描输入缓存，把缓存中的输入数据放入 STDM 帧中，一个 STDM 帧满了就发出。STDM 帧不是固定分配时隙，而是按需动态分配时隙。
      3. 波分多路复用（WDM）：即光的频分多路复用，在一根光纤中传输多种不同波长（频率）的光信号，由于波长不同，各路光信号互不干扰，最后再用波长分解复用器将各路波长分解出来。
      4. 码分多路复用（CDM）：采用不同的编码来区分各路原始信号的一种复用方式。1 个比特分为多个码片/芯片，每一个站点被指定一个唯一的 m 位码片序列。发送 1 时站点发送芯片序列，发送 0 时发送芯片序列反码。多个站点同时发送数据时，要求各个站点芯片序列相互正交。各路数据在信道中线性相加，到达站点后，进行数据分离，通过与源站规格化内积来确定发送的数据。码分多路复用技术具有频谱利用率高、抗干扰能力强、保密性强、语音质量好等优点，还可以减少投资和降低运行成本，主要用于无线通信系统，特别是移动通信系统。
   3. 随机访问介质访问控制：所有用户可随机发送信息，发送信息时占全部带宽。包括 ALOHA 协议和 CSMA 协议等。
      1. ALOHA 协议：
         1. 纯 ALOHA 协议：不监听信道，不按时间槽发送，随机重发，想发就发。如果发生冲突，接收方不予确认，发送方在一定时间内收不到就判断发生冲突，超时后等一随机时间再重传。
         2. 时隙 ALOHA 协议：把时间分成若干个相同的时间片（槽），所有用户在时间片开始时刻同步接入网络信道，若发生冲突，则必须等到下一个时间片开始时刻再发送。
      2. CSMA 协议：
         1. 1 - 坚持 CSMA：发送帧之前，监听信道。信道空闲则发送完整帧；信道忙则继续监听，直到信道空闲立即发送。
         2. 非坚持 CSMA：发送帧之前，监听信道。信道空闲则发送完整帧；信道忙则随机等待一段时间后再监听。
         3. p - 坚持 CSMA：发送帧之前，监听信道。信道空闲则以概率 p 发送帧，以概率 1 - p 延迟一段时间后再监听；信道忙则继续监听，直到信道空闲。
      3. CSMA - CD 协议：载波监听多路访问/冲突检测协议。在发送数据的同时检测冲突，一旦检测到冲突就立即停止发送，并发送干扰信号，等待随机时间后再重新尝试发送。
      4. CSMA - CA 协议：载波监听多路访问/冲突避免协议。在发送数据之前先进行信道预约，避免冲突的发生。
   4. 轮询访问介质访问控制：包括轮询协议和令牌传递协议。
      1. 轮询协议：主站依次询问各站是否有数据要发送，被询问的站如有数据则发送，主站接收数据后再询问下一站。
      2. 令牌传递协议：网络中的一个特殊的控制帧（令牌）在各站之间依次传递，拥有令牌的站才能发送数据。
4. 局域网的基本概念与体系结构。
   1. 局域网是在一个局部的地理范围内（如一个学校、工厂和机关内），将各种计算机、外部设备和数据库等互相联接起来组成的计算机通信网。它的典型拓扑结构有总线型和星型（逻辑总线型）。
   2. 局域网的体系结构包括物理层和数据链路层。数据链路层又分为逻辑链路控制（LLC）子层和介质访问控制（MAC）子层。LLC 子层负责与网络层的接口，提供可靠的通信服务；MAC 子层负责介质访问控制，决定广播信道中信道分配的协议。
5. 以太网与 IEEE802.3、IEEE802.11 的特点。
   1. 以太网是一种基于总线型拓扑结构的局域网技术，采用 CSMA/CD 介质访问控制方法。IEEE802.3 是以太网的标准，规定了以太网的物理层和数据链路层的技术规范。以太网的特点包括：
      1. 简单、易于实现和成本低。
      2. 采用广播通信方式，所有节点共享通信介质。
      3. 支持高速数据传输，速率从 10Mbps 到 100Gbps 不等。
      4. 具有良好的兼容性和扩展性。
   2. IEEE802.11 是无线局域网的标准，采用 CSMA/CA 介质访问控制方法。无线局域网的特点包括：
      1. 灵活性高，不受有线网络的限制，可以在任何有无线信号覆盖的地方接入网络。
      2. 安装方便，不需要铺设电缆。
      3. 支持移动性，用户可以在不同的位置移动而保持网络连接。
      4. 数据传输速率相对较低，受环境因素影响较大。
6. 令牌环网的基本原理。
   1. 令牌环网是一种基于环形拓扑结构的局域网技术，采用令牌传递介质访问控制方法。在令牌环网中，一个特殊的控制帧（令牌）在各站之间依次传递，拥有令牌的站才能发送数据。数据在环上单向传输，每个站都可以接收数据，并将数据转发给下一个站。当数据帧绕环一周回到发送站时，发送站将其从环上删除。如果站没有数据要发送，就将令牌传递给下一个站。
7. 数据链路层设备（网桥、局域网交换机）的工作原理。
   1. 网桥是一种在数据链路层实现局域网互连的设备。它根据 MAC 地址转发帧，将两个或多个局域网连接起来，形成一个更大的局域网。网桥的工作原理是：当一个帧到达网桥时，网桥检查帧的目的 MAC 地址，如果目的地址在本网桥所连接的局域网内，则将帧转发到相应的端口；如果目的地址不在本网桥所连接的局域网内，则将帧转发到其他端口。网桥可以过滤通信量，提高网络性能，同时也可以隔离冲突域，减少网络中的冲突。
   2. 局域网交换机是一种多端口的网桥，它可以在多个端口之间同时转发帧。局域网交换机的工作原理与网桥类似，也是根据 MAC 地址转发帧。不同的是，局域网交换机可以在每个端口上实现全双工通信，提高了网络的带宽和性能。同时，局域网交换机还可以通过虚拟局域网（VLAN）技术，将一个物理局域网划分成多个逻辑局域网，提高网络的安全性和管理性。

## 五、网络层

### （一）主要功能

1. 路由与转发的实现方式。
   1. 路由器在网络层中起着关键作用，负责路由与转发数据报。路由器根据不同的路由算法生成转发表，通过转发表实现数据报的转发。路由与转发分为“路由”和“转发”两步。路由选择确定数据报走哪一条路径，即路由器根据不同的算法生成动态的路由表。分组转发则是路由器根据转发表将用户的 IP 数据从合适的端口报转发出去。
   2. 路由选择协议分为静态路由和动态路由。静态路由由管理员手动配置路由信息，不适合大型和复杂的网络环境。动态路由由路由器根据路由算法动态生成路由信息，适应不断变化的网络，随时获取最优的寻路效果。动态路由算法有距离 - 向量路由算法和链路状态路由算法。
   3. 在距离 - 向量路由算法中，每个结点仅与它的直接邻居交谈，为邻居提供从自己到网络中所有其他结点的最低费用估计。在链路状态路由算法中，每个结点通过广播的方式与所有其他结点交谈，告诉它们与自己直接相连的链路的费用。相较之下，距离 - 向量路由算法有可能遇到路由环路等问题，而链路状态算法收敛更快，在一定程度上比距离 - 向量路由算法更不易产生路由循环。但链路状态算法要求比距离 - 向量路由算法有更强的 CPU 能力和更多的内存空间。
2. 距离 - 向量路由算法、链路状态路由算法。
   1. 距离 - 向量路由算法：所有的结点都定期地将它们整个路由选择表传递给所有与之直接相邻的结点。路由选择表包含每条路径的目的地和路径的代价（如 RIP 算法将其定义为“跳数”，每经过一个路由器跳数加 1）。所有节点都必须参与距离 - 向量交换，以保证路由的有效性和一致性。当被通告一条新的路由，该路由在本节点的路由表中不存在时，本地节点加入；当收到的更新信息中有一条到某个目的地的路由比当前使用的路由更好时，本地节点更新其路由表；当从一个邻居接收到一个路由表项，其中的距离字段值加 1 后比本节点路由表中对应的值更大时，本地节点不改变其路由表。
   2. 链路状态路由算法：了解网络整体连接状态的基础上生成路由控制表。每个路由器掌握的信息是一致的，所有路由器上的信息都是正确的，且不会发生路由循环问题。但需要处理的信息多，需要高速 CPU 和大量的内存。
3. IP 协议（IPv4 地址与 NAT、子网划分、子网掩码、CIDR、IPv6 的主要特点及地址分配方式）。
   1. IPv4 协议：数据报由头部和数据组成。头部长度可由 20 - 60 个字节组成，包含版本、首部长度、区分服务、总长度、标识、标志、片位移、生存时间 TTL、协议、首部校验和、源地址、目的地址等字段。IPv4 地址是由 4 个字节组成的 32 位二进制数，通常用点分十进制表示。为了让 IP 划分出更多的网络和主机，引入了子网掩码的概念，它能划分出一个 IP 地址中的网络部分和主机部分。子网掩码用 1 和 0 的分布决定了 IP 地址的网络标识和主机标识，1 表示网络部分，0 表示主机部分。CIDR（无类域间路由）表示法是一种用于标识和分配 IP 地址的方法，它取代了传统的基于类别（Classful）的 IP 地址分配方式，格式是 IP 地址/前缀长度。
   2. NAT（网络地址转换）：用于解决 IPv4 地址耗尽问题。它可以将私有 IP 地址转换为公有 IP 地址，实现多个私有 IP 地址共享一个公有 IP 地址上网。
   3. 子网划分：通过将一个网络划分为多个子网，提高 IP 地址的利用率。子网划分可以根据需要灵活调整网络规模。
   4. 子网掩码：用于确定 IP 地址的网络部分和主机部分。
   5. CIDR：允许更灵活、有效地分配 IP 地址，避免了传统 A、B、C 类地址划分的限制。
   6. IPv6 的主要特点：IPv6 地址是由 128 位二进制数组成，解决了 IPv4 地址耗尽的问题。IPv6 取消了首部长度字段，因为 IPv6 的首部长度是固定 40 个字节。IPv6 有流量等级字段，代替了 IPv4 中的 Type of Service 字段，有助于处理实时数据以及任何需要特别处理的数据。IPv6 还有流标签字段，用来标识同一个流里面的报文。IPv6 的下一报头字段用来指明报头后接的报文头部的类型，是 IPv6 各种功能的核心实现方法。
   7. IPv6 地址分配方式：IPv6 地址分配可以通过自动配置、DHCPv6 等方式进行。
4. ARP 协议、DHCP 协议与 ICMP 协议。
   1. ARP 协议（地址解析协议）：ARP 解析是自动进行的，ARP 是网络层协议。它用于将 IP 地址解析为 MAC 地址。当一个设备要向另一个设备发送数据时，如果只知道对方的 IP 地址，就需要通过 ARP 协议查询对方的 MAC 地址。
   2. DHCP 协议（动态主机分配协议）：是应用层协议，使用客户/服务器方式，客户端和服务端通过广播方式进行交互，基于 UDP。DHCP 提供即插即用联网机制，主机可以从服务器动态获取 IP 地址、子网掩码、默认网关、DNS 服务器名，允许地址重用，支持移动用户加入网络，支持在用地址续租。
   3. ICMP 协议（网际控制报文协议）：支持主机或路由器的差错（或异常）报告和网络探询。ICMP 报文的结构包括差错报告报文和询问报文。ICMP 的应用有 ping 命令，只使用了 ICMP 询问报文中的回送和回答报文。

## 六、传输层

### （一）服务与协议

1. 传输层提供的服务（无连接服务与面向连接的服务）。
   1. 传输层作为计算机网络体系结构中的关键层次，为应用层提供了两种主要的服务类型：无连接服务和面向连接的服务。
   2. 无连接服务：在无连接服务中，两个通信实体之间无需事先建立连接，就可以直接进行数据传输。数据的发送方将数据分组发送到网络中，每个分组独立地在网络中传输，可能会经过不同的路径到达接收方。这种服务类似于邮政系统中的平信投递，发信人不需要与收信人建立连接，信件可以通过不同的邮路到达目的地。无连接服务的优点是简单、高效，适用于对实时性要求较高、数据量较小的应用场景，如实时视频会议、在线游戏等。然而，由于没有建立连接，无连接服务不能保证数据的可靠传输，数据可能会丢失、重复或乱序到达。
   3. 面向连接的服务：面向连接的服务在通信双方进行数据传输之前，必须先建立连接。这个连接就像一条虚拟的管道，确保数据按照顺序、可靠地从发送方传输到接收方。建立连接的过程通常包括三次握手，即发送方发送一个连接请求报文，接收方收到请求后回复一个确认报文，发送方再发送一个确认报文，以确认连接建立成功。在连接建立后，数据可以双向传输，并且传输过程中会进行差错检测和流量控制等操作，以保证数据的正确性和可靠性。面向连接的服务适用于对数据可靠性要求较高的应用场景，如文件传输、电子邮件等。
2. UDP 协议（数据包结构头部各字段、校验和计算方式）。
   1. UDP（User Datagram Protocol）即用户数据报协议，是一种无连接的传输层协议。UDP 数据包由头部和数据部分组成，头部结构相对简单，只有 8 个字节。
   2. UDP 头部各字段含义如下：
      1. 源端口：占 2 字节，是发送方的端口号。在需要对方回信时选用，不需要时可用全 0。
      2. 目的端口：占 2 字节，是接收方的端口号。在终点交付报文时必须要使用到。
      3. 长度：占 2 字节，表示 UDP 数据报的总长度，包括头部和数据部分。最小值是 8（仅首部）。
      4. 校验和：占 2 字节，用于检测数据传输过程中是否出现错误。有错就丢弃。
   3. UDP 校验和计算方式：UDP 计算校验和的方法和 IP 数据报首部校验和的方法相似。UDP 的校验和是把首部和数据部分一起都检验，需要加上 UDP 伪首部。伪首部指源地址、目的地址、UDP 数据长度、协议类型（0x11），协议类型就一个字节，但需要补一个字节的 0x0，构成 12 个字节。伪首部+UDP 首部+数据一起计算校验和。具体计算方法是：按每 16 位求和得出一个 32 位的数；如果这个 32 位的数，高 16 位不为 0，则高 16 位加低 16 位再得到一个 32 位的数；重复上一步直到高 16 位为 0，将低 16 位取反，得到校验和。
3. TCP 协议（连接管理、序号机制、可靠传输、滑动窗口、累积确认、流量控制与拥塞控制）。
   1. 连接管理：TCP 是面向连接的传输层协议，连接的建立和终止需要通过特定的过程来完成。连接建立通过三次握手，即客户端发送一个 SYN 报文请求连接，服务器收到后回复一个 SYN 和 ACK 报文，客户端再发送一个 ACK 报文确认连接建立成功。连接终止需要四次挥手，数据传输结束后，客户端发送 FIN 报文表示关闭连接，服务器收到后回复 ACK 报文，进入关闭等待状态，然后服务器发送 FIN 报文，客户端回复 ACK 报文，进入等待时间状态，最后连接完全关闭。
   2. 序号机制：TCP 为每个发送的字节都分配一个序号，用于保证数据的顺序传输。在连接建立时，双方会交换初始序列号，后续的数据传输中，序号随着发送的字节数不断增加。接收方根据序号可以确定数据的顺序，并且可以判断是否有数据丢失或重复。
   3. 可靠传输：TCP 通过确认和超时重传机制实现可靠传输。发送方在发送数据后启动一个计时器，等待接收方的确认。如果在计时器超时前没有收到确认，发送方会重传数据。接收方收到数据后会发送确认报文，告知发送方数据已经正确接收。此外，TCP 还通过校验和、序号等机制来保证数据的正确性。
   4. 滑动窗口：TCP 滑动窗口技术通过动态改变窗口大小来调节两台主机间数据传输。发送方和接收方都有一个滑动窗口，窗口大小表示可以发送或接收的数据量。发送方在发送数据的过程中，根据接收方的确认和窗口大小来调整发送窗口的位置。当接收方处理数据的速度较慢时，会减小接收窗口的大小，发送方相应地减小发送窗口，以避免数据的拥塞。滑动窗口机制可以提高数据传输的效率，避免不必要的等待和重传。
   5. 累积确认：TCP 采用累积确认的方式，即接收方对按序到达的多个数据报文只发送一个确认报文，确认号表示接收方期望收到的下一个序号。这种方式可以减少确认报文的数量，提高传输效率。例如，接收方收到序号为 1、2、3 的报文，只会发送一个确认号为 4 的确认报文，表示已经收到了序号为 1、2、3 的报文，期望收到序号为 4 的报文。
   6. 流量控制：TCP 通过滑动窗口机制实现流量控制，确保发送方不会发送过多的数据导致接收方无法处理。接收方在确认报文中会告知发送方自己的接收窗口大小，发送方根据这个大小来调整发送窗口，从而控制数据的发送速度。例如，如果接收方的接收窗口变小，发送方会相应地减小发送窗口，降低发送速度。
   7. 拥塞控制：TCP 采用拥塞控制机制来避免网络拥塞。拥塞控制的方法包括慢启动、拥塞避免、快重传和快恢复等。在连接建立初期，发送方采用慢启动策略，逐渐增加发送窗口的大小。当网络出现拥塞时，发送方会减小发送窗口，降低发送速度，以缓解拥塞。快重传和快恢复则用于快速恢复数据传输，减少因丢包而导致的传输延迟。

## 七、应用层

### （一）主要协议

1. DNS 系统域名解析过程。
   1. 当用户在浏览器中输入一个域名时，首先会在本地浏览器缓存中查找是否有该域名对应的 IP 地址记录。如果没有找到，接着会在操作系统的缓存以及 hosts 文件中查找。如果仍然没有找到，就会向本地 DNS 服务器发起 DNS 域名解析请求。
   2. 本地 DNS 服务器如果有请求域名对应的 IP 地址，则直接返回告诉主机；如果没有，就向根域名服务器发送请求。根域名服务器不直接用于域名解析，而是告诉本地 DNS 服务器去找对应的顶级域名服务器。
   3. 本地 DNS 服务器接着去找对应的顶级域名服务器请求，顶级域名服务器会告诉本地 DNS 服务器去找对应的权威 DNS 服务器。
   4. 本地 DNS 于是再转向问权威 DNS 服务器，权威 DNS 服务器查询后将对应的 IP 地址告诉本地 DNS，本地 DNS 再将 IP 地址返回给主机。
   5. 为了避免下次对这个域名发起 DNS 解析时重复上述过程，主机和本地 DNS 都会对刚刚的域名解析结果进行缓存，下次再解析时，如果有缓存就可以直接从缓存中获取解析结果。
2. FTP 协议的工作原理。
   1. FTP 架构采用客户机/服务器架构，用户通过各种 FTP 客户端程序借助 FTP 协议连接 FTP 服务器进行文件上传或下载。
   2. FTP 通讯端口包括控制链路的 TCP 端口 21 和数据链路的 TCP 端口 20。控制链路用于传送命令和服务器反馈指令，数据链路用于传送数据。
   3. FTP 连接有主动模式和被动模式两种。在主动模式下，客户端把自己的高位端口和服务器端口 21 建立控制链路，当需要传送数据时，客户端会发消息给服务器端，告诉自己的位置和打开的高位端口，等候服务器的 20 端口和客户端打开的端口进行连接，从而进行数据的传输。在被动模式下，当客户端发送数据请求后，服务器会发信息给客户端，告诉客户端服务器在本地打开了一个高位端口，客户端去连接该端口，连接成功后，数据链路就建立了。
3. HTTP 协议（一次网页访问的工作过程）。
   1. 在浏览器输入 URL 后，首先进行 DNS 域名解析，找到与域名相对应的 IP 地址。如果有缓存，可以直接拿取数据，如果没有缓存，就需要进行请求。
   2. 解析出 IP 地址后，进行三次握手建立 TCP 连接。TCP 协议在传输层进行可靠的传输，将报文加上 TCP 首部封装。
   3. 在网络层，加上 IP 首部进行封装，经过网络层传输到服务器。
   4. 服务器解析请求报文，知道请求的是一个 HTML 页面后，按照 HTTP 协议的要求构建响应报文，经过网络层、传输层传输回客户端。
   5. 客户端拿到 HTTP 响应报文，渲染呈现出 HTML 页面。
4. 电子邮件系统及相关协议。
   1. 电子邮件系统中，SMTP、POP 和 IMAP 这三种协议起着至关重要的作用。SMTP 负责邮件的发送，将邮件从发件人传输到邮件服务器，并在服务器之间转发。POP 负责邮件的接收，允许用户从邮件服务器下载邮件到本地设备进行离线阅读，下载后通常会从服务器删除此邮件。IMAP 也负责邮件的接收，它提供了更灵活的邮件管理功能，用户可以在多个设备上同步邮件状态，并且邮件始终保存在服务器上，方便随时访问和管理。
   2. SMTP 协议即简单邮件传输协议，主要负责将邮件从发件人的邮件客户端传送到收件人的邮件服务器。它使用 TCP/IP 协议簇，建立在 FTP 文件传输服务之上，通过“推送”的方式传递信息，确保邮件能够可靠且有效地在不同系统之间传输。其工作流程包括建立连接、握手与域名确认、身份验证（如有需要）、指定发件人、指定收件人、发送邮件内容和连接释放等步骤。
   3. POP 协议即邮局协议，主要用于接收邮件。常用的是 POP3 版本，它使用 TCP 的 110 端口，采用 C/S 工作模式，默认使用 TCP/IP 协议进行传输，属于应用层协议。用户可以通过电子邮件客户端设置 POP3 服务器的地址等参数，连接服务器后下载邮件。
   4. IMAP 协议与 POP3 不同，它提供了一种更为灵活的方式来访问远程服务器上的邮件。用户可以实时查看邮件服务器上的邮件，并且可以在多个设备间同步邮件状态，邮件保留在服务器上，方便随时访问和管理。

## 八、计算机网络考研难点分析

### （一）知识点难点

1. 物理层的奈奎斯特定理和香农定理的计算及应用。
   1. 奈奎斯特定理和香农定理是计算机网络物理层的重要理论。奈奎斯特定理指出在理想低通（没有噪声、带宽有限）的信道中，极限码元传输率为 2W Baud，其中 W 是理想低通信道的带宽，单位为 Hz。若用 V 表示每个码元离散电平的数目，则极限数据率为理想低通信道下的极限数据传输率 = 2Wlog₂V（单位：b/s）。香农定理给出了带宽受限且有高斯自噪声干扰的信道的极限数据传输速率。信道的极限数据传输速率 = Wlog₂(1 + S/N)（单位：b/s），式中，W 为信道的带宽，S 为信道所传输信号的平均功率，N 为信道内部的高斯噪声功率。S/N 为信噪比，即信号的平均功率和噪声的平均功率之比，信噪比 = 10log₁₀(S/N)（单位：dB）。
   2. 在实际应用中，若题目多是求数据极限传输速率，看条件选择使用奈奎斯特定理或香农定理。若两种都可以用，则分别计算，取较小的极限传输速率。例如，在已知信道带宽和信号电平数的情况下，可以使用奈奎斯特定理计算无噪声信道的极限数据传输率；而在已知信道带宽和信噪比的情况下，可以使用香农定理计算有噪声信道的极限数据传输率。
2. 数据链路层的流量控制与可靠传输机制、CSMA/CD 原理及相关计算。
   1. 数据链路层的流量控制是点对点的，主要通过接收方的反馈来控制发送方的数据发送速率，以避免接收方缓冲区溢出。可靠传输机制则通过确认和超时重传等方式保证数据的正确传输。停止 - 等待协议、后退 N 帧协议和选择重传协议是三种常见的可靠传输机制。
   2. CSMA/CD（载波监听多路访问/冲突检测）原理是在发送数据的同时检测冲突，一旦检测到冲突就立即停止发送，并发送干扰信号，等待随机时间后再重新尝试发送。相关计算包括最小数据帧长度的计算，根据网络带宽、信号传输速度和最大网络结点间距离的关系，Lmin / R = 2dmax / V，其中 Lmin 为最小数据帧长度，R 为信道带宽，V 为信号传输速度，dmax 为最大网络结点间距离。
3. 网络层的路由协议和路由算法。
   1. 网络层的主要功能是路由与转发，路由协议和路由算法是实现这一功能的关键。距离 - 向量路由算法和链路状态路由算法是两种常见的路由算法。距离 - 向量路由算法中，每个结点仅与它的直接邻居交谈，为邻居提供从自己到网络中所有其他结点的最低费用估计。链路状态路由算法中，每个结点通过广播的方式与所有其他结点交谈，告诉它们与自己直接相连的链路的费用。
   2. 比较两种算法，距离 - 向量路由算法有可能遇到路由环路等问题，而链路状态算法收敛更快，在一定程度上比距离 - 向量路由算法更不易产生路由循环。但链路状态算法要求比距离 - 向量路由算法有更强的 CPU 能力和更多的内存空间。
4. 传输层的 TCP 协议的连接管理、可靠传输、流量控制与拥塞控制。
   1. TCP 协议是面向连接的传输层协议，连接管理通过三次握手建立连接，四次挥手释放连接。可靠传输通过确认和超时重传机制实现，发送方在发送数据后启动一个计时器，等待接收方的确认。如果在计时器超时前没有收到确认，发送方会重传数据。
   2. 流量控制通过滑动窗口机制实现，确保发送方不会发送过多的数据导致接收方无法处理。拥塞控制采用慢开始、拥塞避免、快重传和快恢复等算法，避免网络拥塞。滑动窗口机制通过动态改变窗口大小来调节两台主机间数据传输，发送方和接收方都有一个滑动窗口，窗口大小表示可以发送或接收的数据量。累积确认是 TCP 采用的一种确认方式，即接收方对按序到达的多个数据报文只发送一个确认报文，确认号表示接收方期望收到的下一个序号。

## 九、结论

计算机网络考研知识点繁多且复杂，考生需系统地梳理各个层次的知识点，重点掌握难点内容，通过多做真题和练习题来加深理解和提高解题能力。

在复习过程中，考生要明确计算机网络体系结构中各层的功能和特点，如 OSI 参考模型和 TCP/IP 模型的分层结构、各层的主要任务及相互之间的异同点。对于物理层，要掌握数据、信号、码元等基本概念，理解奈奎斯特定理和香农定理的应用，熟悉编码与调制的方式及特点，了解不同的交换方式和传输介质。数据链路层是考研的重点之一，考生需掌握差错控制的方法，包括检错编码和纠错编码，尤其是 CRC 校验的原理和应用；掌握流量控制与可靠传输机制，如停止 - 等待协议、后退 N 帧协议和选择重传协议；理解介质访问控制的方法，包括信道划分、随机访问和轮询访问；熟悉局域网的基本概念与体系结构，以及以太网、IEEE802.11 和令牌环网的特点；了解数据链路层设备的工作原理。

网络层的路由与转发是关键内容，考生要掌握距离 - 向量路由算法和链路状态路由算法，理解 IP 协议的相关内容，包括 IPv4 地址与 NAT、子网划分、子网掩码、CIDR 和 IPv6 的主要特点及地址分配方式；熟悉 ARP 协议、DHCP 协议与 ICMP 协议的作用。传输层的 TCP 和 UDP 协议也是考研的重点，考生要掌握 TCP 协议的连接管理、序号机制、可靠传输、滑动窗口、累积确认、流量控制与拥塞控制等内容，了解 UDP 协议的数据包结构头部各字段和校验和计算方式。应用层的主要协议，如 DNS 系统域名解析过程、FTP 协议的工作原理、HTTP 协议和电子邮件系统及相关协议，也是考生需要掌握的内容。

总之，计算机网络考研需要考生全面系统地掌握各个层次的知识点，注重理论与实践的结合，多做真题和练习题，关注计算机网络的最新发展动态，为考试和未来的学习做好充分准备。