**作业1：**

子网划分：

子网的主机数量：Lan7>Lan2>Lan1>Lan4>Lan3>Lan6>Lan5

Lan7有60台主机，所以主机位需要6位：

IP范围：192.168.1.1/26 - 192.168.1.62/26

网络地址：192.168.1.0

广播地址：192.168.1.63

Lan2有50台主机，所以主机位需要6位：

IP范围：192.168.1.65/26 - 192.168.1.126/26

网络地址：192.168.1.64

广播地址：192.168.1.127

Lan2有45台主机，所以主机位需要6位：

IP范围：192.168.1.129/26 - 192.168.1.190/26

网络地址：192.168.1.128

广播地址：192.168.1.191

Lan4有30台主机，所以主机位需要5位：

IP范围：192.168.1.193/27 - 192.168.1.222/27

网络地址：192.168.1.192

广播地址：192.168.1.223

Lan3有台14主机，所以主机位需要4位：

IP范围：192.168.1.225/28 - 192.168.1.238/28

网络地址：192.168.1.224

广播地址：192.168.1.239

Lan2有5台主机，所以主机位需要3位：

IP范围：192.168.1.241/29 - 192.168.1.246/29

网络地址：192.168.1.240

广播地址：192.168.1.247

Lan2有5台主机，所以主机位需要3位：

IP范围：192.168.1.249/26 - 192.168.1.254/29

网络地址：192.168.1.248

广播地址：192.168.1.255

**作业2：**

**一、网络可靠传输**

核心思想：

网络可靠传输旨在确保数据在不可靠的网络环境中能够完整、准确地到达目标端。其核心思想包括以下几点：

1. 确认机制（Acknowledgment）：发送方在发送数据后，等待接收方的确认。如果在一定时间内未收到确认，发送方将重传数据。

2. 序列号（Sequence Number）：每个数据包都包含一个唯一的序列号，接收方通过序列号来重组数据和检测丢失的数据包。

3. 校验机制：发送方对数据进行校验和计算，接收方接收到数据后再计算一次校验和，若不匹配则请求重传。

方法：

1. 超时重传（Timeout and Retransmission）：如果发送方在指定的时间内没有收到确认，则假设数据丢失并重传。

2. 快速重传：如果发送方收到3个冗余ACK就会出发快速重传，重传报文段。

3. 校验和（Checksum）：报文段中所有16位的和进行反码运算，并且求和时的任何溢出都会被回卷。

方法与协议：

在实际网络中，常用的可靠传输协议包括TCP（Transmission Control Protocol）。TCP实现了上述的所有机制，实现了所有方法，所以确保了数据可靠传输。然而在UDP协议中只是实现了报文段头部带上校验和，其他机制都没有实现，这也导致了UDP提供的服务是不可靠的此外。但这也带来了TCP所不具备的优点比如延迟低、开销小等等。TCP协议设计中还包括流量控制和拥塞控制，这将在后续部分详细讨论。

**二、流量控制**

核心思想：

流量控制旨在防止发送方发送数据的速度超过接收方处理能力，从而避免数据丢失或溢出。其核心思想包括：

1. 窗口机制（Window Mechanism）：接收方通过TCP报文段头部的接收窗口字段来告知发送方其接收能力。发送方根据窗口大小控制发送数据的数量。

2. 流量调整：根据网络和接收方的状态动态调整发送速率。

方法与协议：

在TCP协议中，流量控制主要通过滑动窗口协议实现。具体包括：

1. 接受窗口大小调整：接收方把缓冲区剩余的空间记录下来并当作接收窗口大小的值，然后在TCP头部的窗口字段中指示其接收能力，发送方根据该字段调整发送速率。

**三、拥塞控制**

核心思想：

拥塞控制旨在防止网络过载，确保所有用户都能公平地使用网络资源。其核心思想包括：

1. 拥塞检测（Congestion Detection）：通过丢包率、延迟等指标检测网络拥塞情况。

2. 拥塞避免（Congestion Avoidance）：在检测到潜在拥塞时，主动降低发送速率，防止拥塞进一步恶化。

3. 流量控制与调整（Traffic Control and Adjustment）：根据网络状态动态调整数据发送速率。

方法与协议：

TCP中的拥塞控制算法主要包括：

1. 慢启动（Slow Start）：初始阶段指数增长发送速率，快速探测网络容量。

2. 拥塞避免（Congestion Avoidance）：在慢启动阶段结束后，线性增加发送速率，避免拥塞。

3. 快速恢复（Fast Retransmit and Fast Recovery）：在检测到轻微拥塞（如三个重复的ACK）时，迅速重传丢失数据并部分恢复发送速率。

这些算法协同工作，确保TCP协议既能高效利用网络资源，又能在出现拥塞时迅速调整，保证整体网络性能。

通过对网络可靠传输、流量控制与拥塞控制的核心思想和方法的总结和分析，可以看出，这些技术相辅相成，共同保证了现代计算机网络的稳定和高效运行。TCP协议通过一系列精心设计的机制，实现了数据的可靠传输、有效的流量控制和拥塞管理，确保了在复杂的网络环境中数据通信的稳定性和高效性。

**作业三：**

一、问题定义

在电子邮件收发的问题中，问题定义即为需要建立一个高效、可靠和安全的电子邮件通信系统。具体问题包括：

1. 电子邮件的发送与接收。

2. 电子邮件的存储与检索。

3. 保证邮件通信的安全性和隐私性。

4. 提供用户友好的界面和操作体验。

二、需求分析

需求分析包括功能需求和性能需求：

1. 功能需求：

- 用户身份验证与授权。

- 邮件的发送、接收、存储与删除功能。

- 附件的处理和病毒扫描。

- 群发邮件和邮件过滤功能。

2. 性能需求：

- 高可靠性和可用性。

- 高效的邮件传输和处理速度。

- 可扩展性以支持大量用户和邮件量。

三、可行性分析

可行性分析涉及技术、经济和时间等方面的评估：

1. 技术可行性：

- 现有的网络协议和邮件服务器软件（如SMTP、IMAP、POP3）。

- 服务器硬件和存储设备的性能是否满足需求。

- 安全技术（如SSL/TLS加密）是否能提供足够的保护。

2. 经济可行性：

- 预算是否足以覆盖硬件采购、软件许可和运维成本。

- 人力资源是否充足，技术人员是否具备相应技能。

3. 时间可行性：

- 项目开发和部署周期是否在预期时间内完成。

- 是否有足够的时间进行测试和优化。

四、技术方案

技术方案设计需要详细规划每一层的功能和实现：

1. 物理层：

- 选择合适的网络硬件，如交换机、路由器和服务器。

- 规划网络拓扑结构，确保高带宽和低延迟。

2. 数据链路层：

- 配置局域网（LAN）和广域网（WAN），确保数据可靠传输。

- 实现链路层协议，如以太网协议，保证数据帧的传输。

3. 网络层：

- 使用IP地址规划和路由协议（如BGP、OSPF）实现数据包路由。

- 设计防火墙策略，保护网络安全。

4. 传输层：

- 使用TCP协议确保邮件数据传输的可靠性和完整性。

- 配置UDP协议用于某些实时应用。

5. 会话层：

- 管理用户会话，维护连接状态。

- 实现SSL/TLS协议，确保会话安全。

6. 表示层：

- 处理数据加密、解密和压缩，保证数据传输的有效性和安全性。

7. 应用层：

- 部署邮件服务器软件（如Postfix、Dovecot）和Webmail服务（如Roundcube）。

- 实现用户认证、授权和邮件存储。

六、总结个人感悟

通过网络分层模型，可以清晰地理解和管理网络系统的各个部分，使得设计和实现变得更加有条理和系统化。经过一学期的学习我认识到了分层的好处：

1.各层次之间是独立的。某一层并不需要知道它的下一层是如何实现的，而仅仅需要知道该层通过层间的接口所提供的服务。这样，整个问题的复杂程度就下降了。也就是说上一层的工作如何进行并不影响下一层的工作，这样我们在进行每一层的工作设计时只要保证接口不变可以随意调整层内的工作方式。

2.灵活性好。当任何一层发生变化时，只要层间接口关系保持不变，则在这层以上或以下层均不受影响。当某一层出现技术革新或者某一层在工作中出现问题时不会连累到其它层的工作，排除问题时也只需要考虑这一层单独的问题即可。

3.结构上可分割开。各层都可以采用最合适的技术来实现。技术的发展往往不对称的，层次化的划分有效避免了木桶效应，不会因为某一方面技术的不完善而影响整体的工作效率。

4.易于实现和维护。这种结构使得实现和调试一个庞大又复杂的系统变得易于处理，因为整个的系统已经被分解为若干个相对独立的子系统。进行调试和维护时，可以对每一层进行单独的调试，避免了出现找不到、解决错问题的情况。

5.能促进标准化工作。因为每一层的功能及其所提供的服务都已有了精确的说明。标准化的好处就是可以随意替换其中的某一层，对于使用和科研来说十分方便。