**一、问答题（每小题10分，共60分）**

**1****.TCP/IP 是分层体系结构的典范，但是数据在层与层之间交换时，由于频繁地封装和解封，产生了大量的额外开销，影响了网络的传输效率，那么为什么还要分层?**

1. 分层的原因是因为减少以后继续增加功能的成本；
2. 分层的好处是减少了耦合度，让功能的细化更加易于实现；
3. 分层导致的结果是层之间必须提供接口，让层可以互相认知（头部，协议类型）和标准化每个细化的具体格式（分组格式）。
4. 各层之间是独立的。
5. 灵活性好。
6. 结构上可分割开。
7. 易于实现和维护。
8. 能促进标准化工作。
9. **互联网采取"****尽最大努力的交付"，也就是说不能保证 100%的可靠，那么网络还可靠吗? 可靠性是如何保证的?低层的可靠能否保证高层的可靠?**

可靠，低层可靠能保证高层的可靠。因为目前网络常用的是TCP/IP四层分层结构，TCP是面向连接的，可靠的，尽最大努力交付的。

TCP协议里面有如下几种机制去保证可靠性：

一、字节编号机制

TCP的数据段里面的数据部分 ，每个字节都进行编号，就是为了更清楚的接收和发送。TCP数据是按序的，接收完之后按序组装好，才会交付给上层。

二、数据段的确认机制

TCP确认应答就是每一个数据段发送都会收到接收端返回的一个确认号，收到的确认号表示该号前面的数据全部接收。应答机制里有几个注意的点，TCP可以一次连续发送多个数据段、仅对连续接受的数据段进行确认、不连续序号的数据先缓存下来。

三、TCP的超时重传机制

超时重传机制是保证TCP在传输过程中数据丢失了一个回复措施。因此超时重传机制是保证可靠性很重要的机制。

1. **传统的IPV4 存在哪些致命问题?在IPV6中又是如何解决的?试举两个案例详细说明。**

答：

IPV4存在的问题：

1、地址空间不足。

2、骨干路由器路由表表项数量太大（路由器的路由表）。

3、很难进行自动配置和重新编址。

4、无法解决日益突出的安全问题和移动性需求。

案例（5选2）：

1. 更大的地址空间。IPv4中规定IP地址长度为32,即有2^32-1个地址；而IPv6中IP地址的长度为128,即有2^128-1个地址。
2. 更小的路由表。IPv6的地址分配一开始就遵循聚类(Aggregation)的原则,这使得路由器能在路由表中用一条记录(Entry)表示一片子网,大大减小了路由器中路由表的长度,提高了路由器转发数据包的速度。
3. 增强的组播(Multicast)支持以及对流的支持(Flow-control)。这使得网络上的多媒体应用有了长足发展的机会,为服务质量(QoS)控制提供了良好的网络平台。
4. 加入了对自动配置(Auto-configuration)的支持。这是对DHCP协议的改进和扩展,使得网络(尤其是局域网)的管理更加方便和快捷。
5. 更高的安全性。在使用IPv6网络中,用户可以对网络层的数据进行加密并对IP报文进行校验,这极大地增强了网络安全。
6. **（缓存）（Cache）技术广泛应用在计算机网络的各个层次中。请问缓存的基本功能是什么?哪些协议中使用了缓存技术，分别起到什么作用?**

基本功能：预读取、写入、临时存储。

HTTP协议

作用：

1. 减少了冗余的数据传输，节省了网费。

2. 减少了服务器的负担， 大大提高了网站的性能

3. 加快了客户端加载网页的速度

TCP协议

作用：

用来告诉TCP连接对端自己能够接收的最大数据长度

1. **"****三网融合"有几个含义?融合后的下一代互联网络将会发生哪些本质上的改变?**

两个：

1. 广义的上是指电信网、计算机网和[有线电视网](https://baike.baidu.com/item/%E6%9C%89%E7%BA%BF%E7%94%B5%E8%A7%86%E7%BD%91/3515951)三大网络的物理合一。
2. 指高层业务应用的融合，其表现为技术上趋向一致，网络层上可以实现互联互通，形成无缝覆盖，业务层上互相渗透和交叉，应用层上趋向使用统一的[IP协议](https://baike.baidu.com/item/IP%E5%8D%8F%E8%AE%AE/131947" \t "https://baike.baidu.com/item/%E4%B8%89%E7%BD%91%E8%9E%8D%E5%90%88/_blank)，为提供多样化、多媒体化、个性化服务的同一目标逐渐交汇在一起，通过不同的安全协议，最终形成一套网络中兼容多种业务的运维模式。

改变：

1.信息服务将由单一业务转向文字、话音、数据、图像、视频等多媒体综合业务。

2.有利于极大地减少基础建设投入，并简化网络管理，降低维护成本。

3.将使网络从各自独立的专业网络向综合性网络转变，网络性能得以提升，资源利用水平进一步提高。

4.三网融合是业务的整合，它不仅继承了原有的话音、数据和视频业务，而且通过网络的整合，衍生出了更加丰富的增值业务类型，如图文电视、VOIP、[视频邮件](https://baike.baidu.com/item/%E8%A7%86%E9%A2%91%E9%82%AE%E4%BB%B6" \t "https://baike.baidu.com/item/%E4%B8%89%E7%BD%91%E8%9E%8D%E5%90%88/_blank)和网络游戏等，极大地拓展了业务提供的范围。

5.三网融合打破了电信运营商和广电运营商在视频传输领域长期的恶性竞争状态，各大运营商将在一口锅里抢饭吃，看电视、上网、打电话资费可能打包下调。

**6.物联网是在互联网基础之上发展起来的，与互联网在基础设施上有一- 定程度的重合，但它不是互联网概念、技术和应用的简单扩展，那么物联网与互联网之间是怎样的关系?**（一）物联网联系的主体是物，而互联网连接的主体是人。从涵盖范围上来讲，物联网覆盖的范围要比互联网大得多

（二）物联网并不是单一的对物进行连接，物联网是连接了人之后，才延继而申到对“物”的连接；而互联网是可以直接对“人”进行连接的。

（三）从涵盖范围上来讲，物联网覆盖的范围要比互联网大得多。

（四）物联网的诞生重要是为了帮助人类更好地管理“物”，对物体等进行实时监控管理；而互联网的主要目标服务对象是人，用于互相交换信息。

（五）与互联网相比，物联网的实现相对要困难了许多；因为互联网服务过程是人直接参与的时候占了大部分。

（六）人可以对互联网中出现的问题，及时发现与解决；但是物联网却脱离了人的直接参与，物体出现的问题，也全部交由人工智能进行分析管理，而人工智能远远达不到人的头脑那么灵活，所以一些特殊性问题就难以得到及时的发现和解决。

（七）物联网比互联网更加的复杂，在未来，物联网的应用可能会远远超过互联网，比互联网的作用更大，更强。人类可以很轻松地对物体进行控制与管理。

**二、论述题(每小题20分，共40分)**  
**1.****在传统的网络中，路由器采取分组交换模式，各自管理着一个区域，通过相互协作交换路由信息来完成主机间的数据报传输。但路由器与互联网端系统上的网络应用无关，无法针对不同应用需求提供有区分的服务，且路由协议固化在控制器内部芯片中，用户对路由器的工作模式没有任何控制能力，研究人员也无法基于传统路由器平台测试新的技术。请你为下一代网络设计一种新的网络层路由解决方案，以满足开放、虚拟化、可编程、可重构、快速响应以及灵活部署等新的需求。**  
 基于软件定义网络（SDN）的路由解决方案通过实现控制平面与数据平面的分离，有效解决了传统网络中路由器无法灵活适配不同应用需求的问题，同时满足了开放性、虚拟化、可编程、快速响应和灵活部署等新兴网络需求。集中式控制器具备全局网络视图，可以动态优化路由策略并灵活调整数据传输路径，避免了传统分布式路由中存在的信息不一致和子最优路径问题。用户通过开放的北向接口可直接控制路由行为，定义个性化的网络策略，而数据平面则通过简单的转发设备负责规则执行，从而显著降低了硬件复杂度和成本。

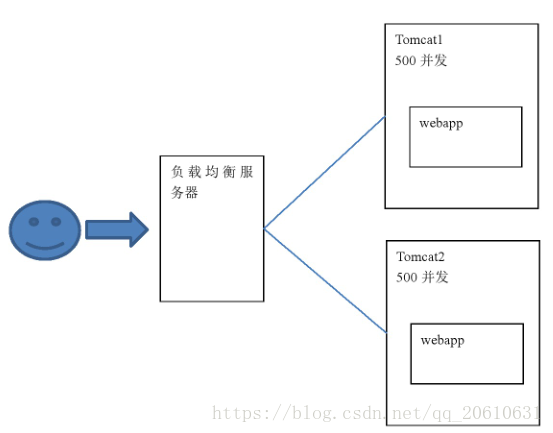
此外，该方案支持在物理网络上创建多个虚拟网络，满足多租户环境下资源隔离和灵活分配的要求。通过应用感知的动态路由技术，可以针对不同的业务需求（如带宽、时延、服务质量等）提供差异化的网络服务。系统还具有快速故障恢复能力，当网络发生变化时，控制器可以快速重新计算路径并下发新规则，从而确保业务的连续性。

综合来看，该解决方案不仅能提升网络资源的利用效率，还为研究人员提供了一个开放的测试平台，支持新协议和技术的快速部署与验证。它适用于数据中心、企业网络、运营商网络以及学术研究等多种场景，是下一代网络架构设计的重要方向。  
**2.某视频服务平台为用户提供清晰、流畅的视频资源。上线10年来，用户注册量已经达到数千万人，单日活跃用户超过千万。近来，越来越多的用户反映视频播放闪退、延迟、卡顿现象时有发生，严重损害了用户的体验感。作为企业CTO,请你分析可能的原因，并提出一种创新性的解决方案，画出示意图，并详细描述其工作原理。**

可能是同时浏览的人数过多，导致高并发事件。

解决方案：

在前端加上负载均衡服务器，当我们的服务器有1000个服务器请求的时候，因为tomcat 服务器一般只能是最多能够承担理论上只能是500，实际上也就是300-400个并发请求，所以1000个并发请求要平均分配给2个服务器，两个服务器之间session要共享；



IP协议

IPV4协议

头部各字段意义按顺序如下：

1. 版本号（4位）
2. 首部长度（4位）
3. 服务（8位）
4. 总长度（16位）
5. 标识（16位）
6. 标记（3位）
7. 分段偏移（13位）
8. 生存时间（8位）
9. 协议（8位）
10. 首部校验和（16位）
11. 源地址（32位）
12. 目的地址（32位）

IPV6协议

头部各字段意义按顺序如下：

1. 版本（4位）
2. 优先级（4位）：该字段定义当发生通信拥塞时的分组的优先级。
3. 流标号（24位）：该字段用来对特殊的数据流提供专门处理。
4. 有效载荷长度（16位：该字段定义整个IPv6数据报的字节长度，包括基本头部和有效载荷。其最大值为65，535字节。

（5）下一个头部（8位）：该字段定义了数据报中跟随在基本头部之后的头部。下一个头部可以是IP所使用的可选扩展头部，也可以是上层协议的头部。

（6）条数限制（8位）：该字段与IPv4中生存时间（TTL）字段一样是一种计数器，在丢弃数据报的每个点值依次减1直至减少为0。

（7）源地址（128位）：源主机IP地址，该字段在IPv4数据报从源主机到目的主机传输期间必须保持不变。

（8）目的地址（128位）

（9）扩展头部：该字段包含6个可选类型，包括逐跳选项、源路由选择、分段、鉴别、加密的安全有效载荷、目的端选项。

TCP

首部格式：

源端口（16位）、目的端口（16位）、序列号（32位 ）、确认序列号（32位）、数据偏移（4位）

标志位（6位）：URG（紧急比特）、ACK（确认比特）、PSH（复位比特）、SYN（连接比特）、FIN（关闭比特）

缓冲区（16位）、校验和（16位）、紧急指针（16位）

Mac（介质访问控制层）

它定义了数据帧怎样在介质上进行传输。在共享同一个带宽的链路中，对连接介质的访问是“先来先服务”的。物理寻址在此处被定义，逻辑拓扑（信号通过物理拓扑的路径）也在此处被定义。线路控制、出错通知（不纠正）、帧的传递顺序和可选择的流量控制也在这一子层实现。

互联网发展的三个阶段

第一阶段：从单个网络APPANET向互联网发展，TCP/IP协议的初步成型；

第二阶段：建成三级结构的Internet，分为主干网、地区网和校园网；

第三个阶段：形成多层次ISP结构的Internet，ISP首次出现。

WLAN

指应用[无线通信技术](https://baike.baidu.com/item/%E6%97%A0%E7%BA%BF%E9%80%9A%E4%BF%A1%E6%8A%80%E6%9C%AF/13873653" \t "https://baike.baidu.com/item/%E6%97%A0%E7%BA%BF%E5%B1%80%E5%9F%9F%E7%BD%91/_blank)将计算机设备互联起来，构成可以互相通信和实现资源共享的网络体系。它是相当便利的[数据传输系统](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E4%BC%A0%E8%BE%93%E7%B3%BB%E7%BB%9F/143597)，它利用[射频](https://baike.baidu.com/item/%E5%B0%84%E9%A2%91/775402)（Radio Frequency； RF）的技术，使用电磁波，取代旧式碍手碍脚的双绞铜线（Coaxial）所构成的局域网络，在空中进行通信连接，使得[无线局域网](https://baike.baidu.com/item/%E6%97%A0%E7%BA%BF%E5%B1%80%E5%9F%9F%E7%BD%91" \t "https://baike.baidu.com/item/%E6%97%A0%E7%BA%BF%E5%B1%80%E5%9F%9F%E7%BD%91/_blank)络能利用简单的存取架构让用户透过它，达到“信息随身化、便利走天下”的理想境界。

存储转发

存储转发（Store and Forward）是计算机网络领域使用得最为广泛的技术之一，以太网交换机的控制器先将输入端口到来的数据包缓存起来，先检查数据包是否正确，并过滤掉冲突包错误。确定包正确后，取出目的地址，通过查找表找到想要发送的输出端口地址，然后将该包发送出去。

CSMA/CD

先听后发，边听边发，冲突停止、延迟重发

**简答题**

**1.带宽、延迟等参数之间的关联（性能）**

**网络延迟（延时）** 是指数据从发送端到接收端所需要的时间。可以将其想象成信息在网络中的“旅行时间”。延迟通常以毫秒为单位进行测量。如果网络延迟高，信息就需要更长的时间才能从一个地方传输到另一个地方。这可能会导致在线游戏中的延迟、视频通话中的滞后以及网页加载速度变慢。

**带宽** 则是指网络能够传输的数据量，通常以每秒传输的比特数（比如兆比特每秒，Mbps）来表示。带宽决定了网络可以同时传输多少数据。高带宽意味着网络能够同时处理更多的数据，而低带宽可能会导致数据传输变慢或者出现阻塞。

**这两者对网络性能有着不同的影响：**

网络延迟影响：高延迟会导致数据传输的时间延长，从而使得实时交互受到影响。例如，在网络游戏中，高延迟可能导致你的操作与游戏中的实际响应之间存在时间差，从而影响游戏体验。在视频通话中，高延迟可能导致对方说话或移动时出现明显的延迟。

带宽影响：高带宽意味着能够同时传输更多的数据，这对于下载大文件、观看高清视频或同时连接多个设备至关重要。但是，带宽并不总是决定一切，因为即使有很高的带宽，如果网络延迟很高，数据传输仍然可能会感到迟缓。

综合来说，网络性能的好坏受到网络延迟和带宽的共同影响。理想情况下，我们希望网络具有低延迟和足够的带宽，以便实现快速的数据传输和实时交互。

**2.****互联网协议怎么设计的，每层是什么功能，为什么怎么做，有什么好处**

互联网协议是如何设计的？设计原则是什么？

互联网协议（如TCP/IP协议栈）的设计基于以下核心原则：

**分层原则：**将网络通信任务分解为若干功能独立的层次，每层完成特定功能并为上层提供服务，同时调用下层的功能。

**模块化设计：**每层功能独立，改动某一层不影响其他层，便于开发和维护。

简单性和高效性：设计遵循"只做所需的功能"，避免复杂的功能交叠和冗余。

**尽力而为传输（Best Effort）：**网络层提供不可靠但快速的数据包传输服务，可靠性交给更高层协议处理。

**可扩展性：**支持多种硬件和网络技术，允许协议在不同环境中运行，并适应未来发展。

各层次的功能是什么？为什么这样设计？

以下以TCP/IP协议栈为例，描述各层次功能及设计原因：

1）应用层功能：提供用户接口和应用服务，负责处理用户请求和返回结果。例如HTTP、FTP、SMTP等协议。设计原因：应用层直接面向用户，抽象化了底层的复杂通信过程，使开发者无需关心数据传输细节，只需专注于应用逻辑。

2）传输层功能：实现端到端通信，提供可靠（如TCP）或不可靠（如UDP）的传输服务。包括：数据分段和重组可靠性保障（重传、确认）流量控制和拥塞控制设计原因：不同应用对传输需求不同（可靠性、实时性等），传输层设计灵活的协议（TCP和UDP），满足多样化需求。

3）网络层功能：提供跨网络的数据包传输服务，核心功能包括路由和寻址（如IP协议）。设计原因：网络层负责连接异构网络，确保数据能够从源地址到达目标地址，而不考虑传输的可靠性，保持简单性和高效性。

4）数据链路层功能：

负责在同一链路（如局域网）上实现可靠的数据帧传输，包括错误检测和帧同步。设计原因：

链路层直接与硬件通信，设计旨在确保数据能在物理介质上传输时不受干扰和错误影响。

5）物理层功能：负责比特流的传输，定义硬件接口、电信号、光信号等物理特性。设计原因：物理层是整个通信的基础，为上层提供透明的比特流传输通道。

这种分层设计带来了哪些好处？

**1）模块化与灵活性：**各层独立工作，开发者可以专注于某一层的功能。例如，传输层协议可以更新，而不影响应用层协议的工作。

**2）简化开发与维护：**开发者无需关心全局，只需专注于本层逻辑，降低了开发复杂度和维护成本。

**3）支持多样化需求：**传输层提供可靠的TCP和快速的UDP，满足不同场景（如文件传输与实时通信）的需求。

应用层协议丰富多样（如HTTP、FTP、SMTP），适配不同的应用场景。

**4）互操作性：**分层设计促进了设备间的兼容性，不同厂商设备只需遵守相应层的协议标准即可实现互通。

**5）扩展性与通用性：**网络层屏蔽了底层硬件差异，支持异构网络互联。协议的扩展性（如从IPv4到IPv6）保证了系统能适应未来需求。

**6）效率与性能优化：**层次分工明确，各层只关注自身功能，减少了重复设计，提升了系统整体效率。

**总结：**互联网协议采用分层设计，通过明确的分工和灵活的模块化构造，满足了网络通信的多样化需求，同时简化了开发和维护过程。每层功能独立且专注，既确保了系统高效运行，又为未来的技术更新和扩展奠定了基础。

**3.****局域网，以太网（为什么局域网不用再以太网等）**

局域网的主要特点是什么？为什么局域网采用广播通信方式而广域网不采用呢？

答：局域网LAN是指在较小的地理范围内，将有限的通信设备互联起来的计算机通信网络

从功能的角度来看，局域网具有以下几个特点：（1） 共享传输信道，在局域网中，多个系统连接到一个共享的通信媒体上。（2） 地理范围有限，用户个数有限。通常局域网仅为一个单位服务，只在一个相对独立的局部范围内连网，如一座楼或集中的建筑群内，一般来说，局域网的覆盖范围越位10m~10km内或更大一些。

从网络的体系结构和传输检测提醒来看，局域网也有自己的特点：（1）低层协议简单（2） 不单独设立网络层，局域网的体系结构仅相当于相当与OSI/RM的最低两层（3）采用两种媒体访问控制技术，由于采用共享广播信道，而信道又可用不同的传输媒体，所以局域网面对的问题是多源，多目的的连连管理，由此引发出多中媒体访问控制技术在局域网中各站通常共享通信媒体，采用广播通信方式是天然合适的，广域网通常采站点间直接构成格状网。

什么是局域网（LAN）？

局域网（Local Area Network，LAN） 是在有限范围内（如家庭、公司、学校等）连接计算机和其他设备的网络，通常通过有线或无线技术连接。局域网的特点是通信速度较快，设备间距离较近，一般覆盖一个建筑物或一个小区域。

局域网通常用于共享资源（如文件、打印机等）、连接互联网，以及支持内部通信。

什么是以太网（Ethernet）？

以太网 是最常用的局域网技术，它定义了数据在局域网中的传输方式，包括物理硬件和数据链路层协议。最初，以太网是通过同轴电缆传输数据，后来发展为通过双绞线和光纤传输，支持10Mbps到100Gbps等不同速度。

以太网通过帧格式传输数据，并使用CSMA/CD（载波侦听多路访问/冲突检测）协议来管理传输冲突。现代以太网技术，如千兆以太网和10G以太网，在速度和带宽上有了显著提高。

局域网为什么不再仅仅依赖传统的以太网技术，或当前的局域网技术有哪些新的发展和趋势？

**以太网在局域网中的广泛应用：**传统上，局域网使用有线以太网技术（如10/100/1000以太网）作为主要的物理连接手段，提供较高的带宽（通常为1Gbps或更高）。不过，随着技术的发展，局域网的需求变得更加多样化，传统的以太网已经不再满足所有场景的需求。

**无线局域网（WLAN）技术的兴起：**随着无线通信技术的进步，尤其是Wi-Fi技术的广泛应用，现代局域网越来越多地采用无线局域网（WLAN）来代替传统的有线以太网。无线局域网不仅提供灵活的接入方式，还支持移动设备（如智能手机、平板电脑）接入网络，已成为家庭和企业中不可或缺的部分。

**更高带宽和低延迟的需求：**随着应用需求（如高清视频、虚拟现实、云计算等）的增加，局域网需要更高的带宽和更低的延迟。传统以太网虽能提供1Gbps或更高的速度，但对于超高带宽和低延迟的应用（如8K视频、数据中心通信等）来说，可能需要10Gbps甚至更高速度的以太网（如10G、40G、100G以太网）来满足需求。

**软件定义网络（SDN）和虚拟化的引入：**随着SDN和网络功能虚拟化（NFV）的发展，局域网的网络管理逐渐从传统的硬件控制模式转向软件定义的灵活控制模式。SDN可以让网络管理员动态地调整网络配置和优化流量管理，提高了局域网的可扩展性和灵活性。

**智能交换机和路由技术的进步：**现代局域网越来越多地采用智能交换机、路由器和其他网络设备，这些设备可以实现更高效的流量管理、更好的带宽分配、网络故障检测和优化等功能。例如，交换机可以根据实时流量进行负载均衡，提高整个局域网的吞吐量和性能。

**总结：**传统的以太网技术在局域网中得到了广泛应用，但随着无线网络技术的发展、带宽需求的增加以及软件定义网络和虚拟化技术的引入，局域网的技术架构正在不断演进，既有有线以太网，也有无线局域网（Wi-Fi）以及更加智能、灵活的网络管理手段。现代局域网不仅仅依赖于传统的以太网，还结合了多种新兴技术来满足更高效、更高带宽、更灵活的网络需求。

**4.****以前路由无QoS，现在有了QoS路由，区分服务模型，SDN干什么的，解决什么问题**

在传统路由中，QoS功能未得到支持，而现在的路由实现了QoS。请阐述QoS路由与传统路由的区别，并简要介绍SDN（软件定义网络）如何通过区分服务模型解决网络中的哪些问题？

答案：

1. **传统路由与QoS路由的区别**：

**传统路由**：传统路由一般没有内建的QoS功能，数据包的处理依赖于路由算法和路由表，网络的流量控制较为简单，可能无法满足高需求服务（如视频流或实时通信）对带宽和延迟的严格要求。

**QoS路由**：QoS（服务质量）路由允许网络根据流量类型、优先级、带宽要求和延迟限制等特征，为不同的数据流提供不同级别的服务。QoS确保关键应用（如语音、视频等）优先获得网络资源，提高网络服务的可靠性和性能。

1. **区分服务模型**：

**区分服务（Differentiated Services, DiffServ）模型**：是一种基于IP头中的DS字段对流量进行分类和标记的模型。通过将不同的数据流分配到不同的服务类别，路由器可以根据这些类别优先处理某些数据流。这种模型减少了传统的基于连接的状态维护，提高了网络性能。

**其他服务模型**：如IntServ（Integrated Services）模型则是一个端到端的服务质量保障机制，依赖于每个路由器保持状态信息，但相对较为复杂，且不适用于大规模网络。

1. **SDN的作用与解决的问题**：

**SDN（软件定义网络）**：SDN是通过集中式控制器管理整个网络的架构，在网络控制层和数据层之间提供解耦，允许管理员通过软件进行动态配置、管理和优化网络流量。

**SDN解决的问题**：

**灵活的网络管理**：通过集中控制，SDN能够实时调整流量路由，动态调整QoS策略，以应对不同的网络负载和需求变化。

**简化网络配置和维护**：传统网络设备需要手动配置，SDN通过集中管理提供统一的控制接口，使得网络配置更简便和一致。

**高效的资源分配**：SDN可以智能地根据流量类型和优先级进行资源调度，确保实时应用和重要任务的优先级和网络质量，优化带宽利用率，减少网络拥塞。

**支持虚拟化与多租户**：在数据中心和云计算环境中，SDN能够为多个租户提供隔离的网络资源，并实现虚拟化网络管理。

总结：QoS路由通过对不同数据流进行优先级划分和资源保障，解决了网络中不同应用的质量保障问题，而SDN通过软件化的控制，提供了更加灵活和高效的网络管理，解决了传统网络中配置复杂、响应慢、难以适应动态变化等问题。

**5.域名服务（1）什么样的服务（2）解决什么样的问题**

（1）DNS是什么样的服务？

**域名系统（DNS，Domain Name System）** 是一种分布式的网络服务，用于将易于记忆的域名（如：www.example.com）转换为计算机能够识别和处理的IP地址（如：192.0.2.1）。

DNS服务提供了一个层次化的命名系统，使得用户能够通过域名访问互联网上的资源，而不需要记住每个资源的IP地址。

DNS工作原理类似于电话簿，用户输入域名，DNS服务器查询并返回相应的IP地址。

（2）DNS解决了哪些网络中的问题？

**人类可读性问题**：域名服务使得用户可以使用易于记忆的域名来访问网站，而不是直接使用数字型的IP地址。比如用户记住"www.baidu.com"比记住其IP地址更方便。

**IP地址管理问题**：通过DNS，用户和应用程序可以通过域名访问大量可能变化的服务器，而不需要直接管理这些服务器的IP地址。DNS使得服务器迁移、负载均衡等操作对用户透明。

**分布式查询和容错性**：DNS系统是分布式的，多个DNS服务器提供冗余，确保网络服务的可靠性和容错性。如果某个DNS服务器无法响应，其他服务器可以继续提供服务。

**高效的资源定位**：通过DNS的缓存机制和分级查询（递归查询、迭代查询），DNS能够快速地定位和返回正确的资源，降低了查询延迟和负担。

**支持多种服务记录**：除了基础的A记录（IP地址）外，DNS还可以支持各种服务记录（如MX记录用于邮件服务、CNAME记录用于别名服务等），使得不同网络服务可以统一管理和定位。

总结：DNS作为一个基础性的网络服务系统，不仅解决了人类可读性和IP地址管理的问题，还通过分布式架构提高了网络的可靠性和效率，同时支持多种服务记录以便更好地满足网络资源的分配和定位需求。

**6.IPv6有什么用，解决什么样的问题，IPv4怎么到IPv6的**

什么是IPv6，它的主要作用和特点是什么？

IPv6（Internet Protocol version 6） 是下一代互联网协议，设计用于取代现有的IPv4协议。IPv6采用128位地址空间，可以提供比IPv4（32位地址）多得多的地址数量。

**扩大地址空间：**提供几乎无限的IP地址数量，支持更多设备接入互联网。

**提高路由效率：**通过更简洁的路由表设计和自动配置功能减少网络复杂性。

**增强网络安全：**内置了IPsec（Internet Protocol Security）协议，提供端到端的加密和认证支持。

**支持移动性和多播：**更高效地支持移动设备以及多播通信。

IPv6解决了IPv4存在的哪些问题？

**地址耗尽问题：**IPv4提供约43亿个地址，由于互联网用户和设备的爆炸式增长（如IoT设备），IPv4地址已经几乎耗尽。IPv6的128位地址空间可提供约3.4×1038个地址，完全消除了地址不足的问题。

**网络复杂性问题：**IPv4依赖NAT（网络地址转换）来缓解地址短缺，但NAT增加了网络配置和管理的复杂性。IPv6支持无状态地址自动配置（SLAAC），简化了网络配置。

**质量和服务问题：**IPv6中头部格式更简洁，提升了路由效率；同时，IPv6为实时应用提供了流量标记和优先级管理功能，支持更高质量的服务（QoS）。

**安全性问题：**IPv6协议内置IPsec，可以提供更强的网络安全性，而IPv4的安全特性需要额外配置。

IPv4到IPv6的过渡过程是如何设计和实现的？

IPv4和IPv6的地址格式和协议栈不同，二者不兼容，不能直接互通。因此需要采用过渡技术来实现平滑过渡。

主要过渡机制：

**双栈机制（Dual Stack）：**设备和网络同时运行IPv4和IPv6协议栈，能够处理IPv4和IPv6流量。这种方法适合过渡期，但需要更高的设备性能和内存支持。

**隧道技术（Tunneling）**：通过将IPv6数据封装在IPv4报文中，从而在IPv4网络上传输IPv6流量。常见的隧道技术包括6to4隧道和ISATAP（Intra-Site Automatic Tunnel Addressing Protocol）。

**地址翻译（NAT64/DNS64）：**在IPv4和IPv6网络之间进行地址转换，使得IPv6设备能够与IPv4设备通信。

**分阶段过渡：**由于现有网络和设备大量使用IPv4，向IPv6过渡通常是分阶段进行的，包括骨干网的IPv6改造、终端设备支持IPv6、部署过渡机制等。

**总结：**IPv6通过提供更大的地址空间和改进的协议特性，解决了IPv4地址耗尽、网络复杂性、服务质量和安全性等问题。向IPv6的过渡是互联网发展的重要阶段，通过双栈、隧道和地址翻译等技术，确保IPv4和IPv6的共存和互通，逐步实现向完全IPv6网络的迁移。

**7.****为什么设计TCP可靠，UDP不可靠，UDP怎么不可靠的，IP为什么不类似TCP**

为什么设计TCP为可靠传输，而UDP为不可靠传输？

**TCP的设计目标：**TCP用于需要数据完整性和可靠传输的场景，如文件传输、电子邮件、网页浏览等。它通过一系列机制（如握手、确认、重传、流量控制、拥塞控制等）确保数据按顺序、无丢失、无重复地到达接收端。

**UDP的设计目标：**UDP则面向实时性要求更高、对数据可靠性要求不高的场景，如视频流、在线游戏、语音通信等。它追求的是简单、高效和低延迟，不对数据包进行确认和重传，降低了协议的复杂性和开销。

**区别设计的原因：**网络应用需求多样化：有些应用需要可靠性，有些则更看重速度和实时性。设计不同的协议以满足不同需求，使得网络协议栈更灵活。

**网络层次分工：**可靠性要求较高的功能由传输层协议（如TCP）实现，而对速度要求更高的功能则由UDP提供。

UDP具体是如何表现为不可靠的？

**无连接性：**UDP在通信前不建立连接，也不保持连接状态。数据包直接发送给目标，无需握手或建立会话。

**无数据确认机制：**UDP不提供确认数据是否到达的机制，发送方不会知道数据包是否成功传递到接收方，也不会进行重传。

**无顺序保证：**UDP数据包可能乱序到达目标主机，协议本身不负责重新排序。

**无流量控制：**UDP不调节数据流速率，不管网络是否拥堵，都会直接发送数据包。

**无内置校验和重传：**UDP头部仅提供简单的校验和检测，但不负责纠错，丢失的数据包不会重传。

为什么IP协议不设计为类似TCP的可靠协议？

**分层架构的设计原则：**网络协议栈采用分层设计，每层负责特定的功能，避免冗余。IP协议作为网络层协议，其主要功能是提供地址寻址和数据包转发，而不涉及传输层的可靠性保障。可靠性由更高层（如TCP）来实现。

**性能与效率的考虑：**IP协议的目标是快速转发数据包，过多的可靠性机制会显著增加处理开销和延迟。

**适应多样化需求：**网络层提供简单的、不可靠的数据传输服务（"best-effort delivery"），为传输层提供灵活性。需要可靠性的应用可以选择TCP，不需要的应用可以直接使用UDP。

**全球互联的需求：**IP作为通用的网络层协议，必须支持多种传输场景和设备，保持简洁性以适应不同的硬件和网络条件。复杂的可靠性设计会降低协议的通用性和适配性。

**总结：**TCP被设计为可靠协议以满足数据完整性需求，而UDP追求简单和高效，适用于实时性强的应用场景。IP作为网络层协议，定位于提供简单、高效、无连接的数据传递服务，不涉及传输层的可靠性功能。分层设计原则和需求多样化促成了TCP、UDP和IP协议在功能和可靠性上的差异化设计。

**8.****网络怎么设计，从上向下，网络可不可靠，解决了没有**

网络设计是如何从上到下进行的？

**分层设计的基本思想：**网络系统的设计遵循分层模型的原则（如OSI七层模型和TCP/IP模型），将复杂的通信任务划分为多个层次，每层负责特定功能，彼此独立又相互协作。

应用层（顶层）：提供用户直接交互的功能，如网页浏览（HTTP）、电子邮件（SMTP）、文件传输（FTP）等。

传输层：负责端到端的可靠传输或无连接服务，如TCP提供可靠传输，UDP提供高效传输。

网络层：实现跨网络的数据包传输，主要功能是路由和寻址，协议如IP。

数据链路层：负责点到点的通信，提供帧的封装和错误检测。

物理层（底层）：负责比特流的传输，定义硬件接口和信号传输。

**从上到下的设计过程：**

需求分析：确定用户需求和应用场景，例如实时通信、文件传输、流媒体播放等。

功能定义：从应用层开始定义应用程序需要的服务，并逐步分解到下层，如可靠性需求交由传输层处理。

协议设计：每层根据功能需求设计相应的协议，如应用层协议（HTTP）、传输层协议（TCP/UDP）。

实现与测试：最终在物理层和硬件上实现协议栈，并通过模拟或真实环境进行测试。

网络是否可靠？如何定义网络的可靠性？

网络的可靠性定义：网络可靠性是指数据能够按时、完整、无误地从发送方传输到接收方的能力。

涉及的指标包括：数据丢失率、错误率、延迟、抖动等。

**网络的可靠性取决于多个因素：**物理层可靠性：硬件的稳定性、信号质量。链路层可靠性：帧的错误检测与重传机制。传输层可靠性：TCP等协议提供的确认和重传机制。网络层的努力：尽力而为的传递，不保证可靠性。

**网络是否可靠：**网络本身并不保证完全可靠性（如IP网络采用“尽力而为”模式），但通过传输层（如TCP）和应用层的协同，可以提高数据传输的可靠性。

网络中的可靠性问题是否已经解决？

**已解决的部分：**传输可靠性：通过TCP的重传、确认和拥塞控制机制，解决了数据丢失、乱序、重复等问题。物理和链路层改进：现代网络硬件和链路协议（如光纤通信、5G技术）大幅提升了物理传输的可靠性。路由容错性：动态路由协议（如OSPF、BGP）可以快速响应网络故障，提供路由冗余。

**未完全解决的部分：**实时性与可靠性的平衡：在某些场景（如实时语音或视频通信）中，丢失一些数据可能比重传更优，但如何平衡可靠性和实时性仍是挑战。

网络拥塞问题：虽然有拥塞控制算法（如TCP的慢启动、拥塞避免），但在高流量情况下仍可能出现性能下降。安全性与可靠性：网络攻击（如DDoS、MITM）可能破坏可靠性，安全性问题始终是网络可靠性的重要威胁。

**总结：**网络设计采用从上到下的分层思想，各层独立实现其功能，传输层和应用层通过协作提升整体可靠性。虽然网络可靠性在协议设计和硬件层面取得了巨大进步，但在实时性、拥塞处理和安全性等方面仍存在挑战，需要持续优化。

**9.****怎么把应用层，网络层，TCP/IP三层，横向，**

如何理解应用层、网络层和TCP/IP三层在网络通信中的作用？

**应用层：**功能：为用户提供直接的网络服务，如网页浏览（HTTP）、文件传输（FTP）、电子邮件（SMTP）、即时通信（WebSocket）等。特点：专注于用户交互和数据的具体表现形式，通常与应用程序直接关联。

**网络层：**功能：实现数据在不同网络间的传输，主要负责路由选择和寻址（如IP协议）。

特点：以“尽力而为”的方式提供数据包传输，不保证可靠性，但确保数据包能在不同网络之间正确转发。

**TCP/IP协议：**传输层（TCP/UDP）：提供端到端的传输服务。TCP提供可靠传输（连接建立、确认、重传），UDP提供快速、无状态传输。

**互联网层（IP）：**负责数据包的寻址和路由，是TCP/IP协议栈的核心组件。

特点：TCP/IP协议栈是网络通信的整体实现框架，包含从应用层到物理层的完整功能。

从横向视角，三者如何协同工作实现数据传输？

从横向视角，可以将应用层、网络层和TCP/IP协议栈视为分工明确、协同运作的体系：

**应用层的角色：**用户发送请求或数据（如访问网站、发送文件），应用层协议将用户数据封装为应用层报文。例如，HTTP会将网页请求封装为一个HTTP报文，并交给下层协议处理。

传输层（TCP/UDP）的角色：

**TCP模式：**对接收到的应用层数据，分段（Segmentation）后封装为TCP报文段，并附加端口号等信息。负责数据传输的可靠性保障（如确认、重传、流量控制）。

**UDP模式：**直接将应用层数据封装为UDP报文段，附加端口号等信息，快速传输但不做确认。

**网络层的角色：**将传输层的报文段进一步封装为IP数据包，附加源IP地址、目标IP地址等信息。负责路由选择，确保数据包能通过多跳路径到达目标设备。

数据链路层和物理层的支持：将IP数据包封装为帧，通过链路层协议（如以太网协议）在物理链路上传输。

**接收端的解封装过程：**数据包到达目标设备后，依次进行解封装：链路层->网络层->传输层->应用层，最终由应用程序接收用户所需的数据。

这种分层模式对网络系统设计有哪些优势？

**模块化设计：**各层独立开发，便于维护和升级。例如，应用层协议的更新不会影响网络层和传输层。

**灵活性与兼容性：**不同的应用层协议可以共用传输层和网络层。例如，HTTP和SMTP都可以运行在TCP之上。

**便于理解和教学：**分层模型将复杂的网络通信过程拆解为简单的功能模块，方便学习和研究。

**支持多样化需求：**应用层满足不同应用场景需求（如可靠性、实时性）；传输层（TCP/UDP）提供灵活选择；网络层确保数据跨网络传递。

**标准化和互操作性：**分层设计允许不同厂商的设备和协议栈兼容运行，促进了互联网的全球化发展。

**总结：**应用层、网络层和TCP/IP协议栈通过分工协作，构建了一个高效、灵活、模块化的网络通信体系。横向理解三者的协同工作过程，可以更清晰地认识从用户请求到数据传输的完整流程，以及这种分层模式对网络系统设计的深远意义。

**计算题**

传输层，网络层，TCP/IP

时延计算问题：

（1）发送时延：发送时延=数据帧长度（bit）/发送速率（bit/s）

（2）传播时延：传播时延=信道长度（m）/电磁波在信道上的传播速率（m/s）

（3）处理时延题目中会给出。

（4）排队时延和处理时延一般题目都会忽略不计。

（5）总时延=发送时延+传播时延+处理时延+排队时延

（6）时延带宽积=传播时延\*带宽

（7）往返时间RTT：发送时间=数据长度/发送速率；有效数据率=数据长度/(发送时间+RTT)

（8）利用率：D。表示网络空闲时的时延，D表示网络当前的时延，网络当前的利用率为U，则：D=D。/(1-U)

（9）带宽时延积=带宽×(距离/传播速率）(也指传播信道上比特数目最大的数值）

**论述题**

**P2P物联网，****云物一大致**

**课后题，为什么**

**一、简答题(每小题5分，共25分)**

**1.移动IP技术实现的基本方法是什么?**

**2.传输网中可能引起报文丢失的原因有哪些?**

**3.应用层多播与网络层多播有什么区别?**

**4.什么是SDN?有哪些核心技术?SDN解决了哪些问题?又存在哪些问题?**

**5.在互联网中，DNS仅仅就是实现了将域名解析为对应的地址吗?说明理由**

**1.多播有什么好处?有哪些因素影响了多播在互联网中的部署?**

**2.C/S模型与P2P模型主要差别在哪里?**

**3.运输层最大报文段长度MSS设置的太大或太小有什么影响?**

**4.TCP拥塞控制的实现与IP路由协议的实现有没有关系?说明理由**

**5.什么是SDN?如果在互联网中全面实现有什么问题吗?**

### ****1. 移动IP技术实现的基本方法是什么?****

移动IP（Mobile IP）技术是一种在终端设备改变网络位置时，仍能维持通信会话的协议，基本实现方法包括以下步骤：

* **地址注册：** 移动节点（MN）向其归属代理（Home Agent，HA）注册当前地址（转交地址，Care-of Address，CoA）。
* **数据隧道：** 数据包通过隧道技术由HA转发到移动节点当前的位置。
* **数据转发：** 在接收到数据包后，转交地址负责将数据包传递给移动节点。
* **路由优化（可选）：** 消除三角路由问题，使通信效率更高。

### ****2. 传输网中可能引起报文丢失的原因有哪些?****

* **拥塞：** 网络设备如路由器或交换机缓存满，导致丢弃新到的报文。
* **链路错误：** 数据传输过程中由于线路干扰等原因导致比特错误。
* **设备故障：** 网络设备如路由器、交换机硬件或软件故障。
* **协议超时：** 超过协议规定的等待时间未收到确认（如TCP）。
* **QoS策略：** 优先级较低的流量被丢弃以保障高优先级流量。

### ****3. 应用层多播与网络层多播有什么区别?****

* **实现层次：**
  + **应用层多播：** 在应用层实现，节点通过逻辑层级组建多播树，完全由应用端处理。
  + **网络层多播：** 在IP层实现，利用网络层的多播组地址（如IPv4中的组播地址224.0.0.0/4）直接将数据传递到组播组。
* **适用范围：**
  + **应用层多播：** 无需对网络设备进行更改，适合在现有互联网中部署，但效率较低。
  + **网络层多播：** 需要网络设备支持（如IGMP、PIM协议），效率高，但部署成本高。
* **复杂性：**
  + **应用层多播：** 简单实现，但会引入额外的延迟和开销。
  + **网络层多播：** 高效但实现复杂，需要广泛支持的协议。

### ****4. 什么是SDN?有哪些核心技术?SDN解决了哪些问题?又存在哪些问题?****

#### ****SDN定义：****

软件定义网络是一种通过控制面与数据面的分离，实现网络集中控制和灵活配置的新型网络架构。

#### ****核心技术：****

* **控制面和数据面的分离：** 使用OpenFlow等协议进行通信。
* **集中控制：** 使用集中式控制器（如ONOS）管理网络。
* **可编程性：** 网络设备的行为由软件定义。

#### ****解决的问题：****

* **灵活性：** 可根据需求快速配置网络。
* **集中化管理：** 提高网络监控和优化的能力。
* **资源优化：** 高效利用网络资源。
* **网络虚拟化：** 支持多个虚拟网络在同一物理网络中共存。

#### ****存在的问题：****

* **单点故障：** 控制器故障可能影响整个网络。
* **扩展性：** 在大型网络中的性能和效率可能会下降。
* **安全性：** 控制器成为潜在的攻击目标。

### ****5. 在互联网中，DNS仅仅就是实现了将域名解析为对应的地址吗?说明理由****

DNS（域名系统）不仅仅是将域名解析为IP地址的工具，其功能包括但不限于：

* **域名解析：** 将域名解析为IP地址，支持正向解析和反向解析。
* **负载均衡：** 通过解析同一域名为不同的IP地址，实现负载均衡。
* **邮件路由：** 通过MX记录指定邮件服务器。
* **服务发现：** 使用SRV记录定位网络服务。
* **安全性：** DNSSEC（DNS安全扩展）保护数据完整性。

DNS在互联网中扮演着重要角色，不仅解决了易记忆性和网络寻址之间的矛盾，还提供了一些增强型功能，支持现代互联网服务的运行。

### ****1. 多播的好处及影响部署的因素****

#### ****好处：****

* **高效性：** 多播通过一次性传输数据到多个接收者，减少网络带宽消耗。
* **可扩展性：** 支持大规模的数据分发，如视频流和股票交易。
* **实时性：** 减少了冗余传输，降低延迟，适合实时应用。

#### ****影响部署的因素：****

* **网络设备支持：** 多播需要设备支持多播协议（如IGMP、PIM），现有网络设备可能不具备该功能。
* **安全性：** 多播组的加入/退出缺乏有效的访问控制机制，易受攻击。
* **复杂性：** 多播路由和管理复杂，尤其在跨域情况下。
* **经济因素：** 网络运营商可能缺乏部署多播的动力，因为收益不明确。

### ****2. C/S模型与P2P模型主要差别****

* **架构：**
  + **C/S模型（Client/Server）：** 客户端发起请求，服务器响应。服务器为中心，提供资源。
  + **P2P模型（Peer-to-Peer）：** 每个节点既是客户端又是服务器，节点之间共享资源。
* **资源分布：**
  + **C/S：** 集中式资源管理，服务器压力大。
  + **P2P：** 分布式资源管理，节点共享负载。
* **扩展性：**
  + **C/S：** 受服务器硬件和带宽限制，扩展性较差。
  + **P2P：** 高度可扩展，新增节点可增加系统容量。
* **容错性：**
  + **C/S：** 服务器宕机会导致服务中断。
  + **P2P：** 单点失效影响较小，系统更健壮。

### ****3. 运输层最大报文段长度（MSS）设置太大或太小的影响****

* **MSS设置太大：**
  + 容易导致IP分片：分片后可能增加网络负担，且某些分片丢失会影响整个报文的重组。
  + 适配性差：在MTU较小的网络中可能无法传输。
* **MSS设置太小：**
  + 增加了报文数量：引发更多的包头开销，降低传输效率。
  + 处理开销增大：需要更多的传输控制操作，如确认报文。

### ****4. TCP拥塞控制与IP路由协议的关系****

#### ****是否有关系：****

TCP拥塞控制和IP路由协议的实现**没有直接关系**，但两者在网络性能优化中存在间接关联。

#### ****理由：****

* **实现层次不同：**
  + **TCP拥塞控制：** 位于运输层，负责调整发送速率以避免网络拥塞。
  + **IP路由协议：** 位于网络层，负责选择最优路径传输数据。
* **间接影响：**
  + 路由协议可以通过调整路由路径改变拥塞状况。
  + TCP拥塞控制通过动态调整流量减少对路由的压力。
* **相互独立：** TCP不直接依赖于特定路由协议，但路由性能会影响拥塞控制的效果。

### ****5. 什么是SDN？如果在互联网中全面实现有什么问题？****

#### ****SDN定义：****

SDN（软件定义网络）通过控制面和数据面的分离，实现网络设备行为的可编程化和集中化管理（参考前述回答）。

#### ****全面实现SDN在互联网中的问题：****

* **复杂的兼容性问题：** 现有传统网络设备和协议需要更新，涉及巨大成本。
* **规模化挑战：** 大规模互联网环境中，集中式控制器可能面临扩展性和性能瓶颈。
* **单点故障：** 控制器成为关键节点，其故障可能影响整个网络。
* **安全性风险：** 控制器是攻击的主要目标，可能导致整个网络的安全性下降。
* **标准化问题：** SDN生态尚未完全成熟，不同厂商的设备和技术难以互操作。

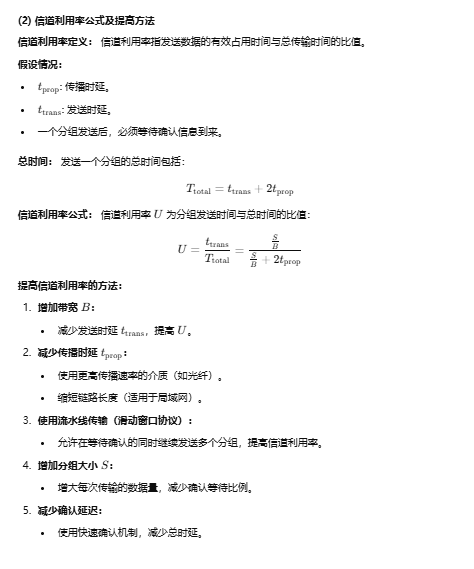
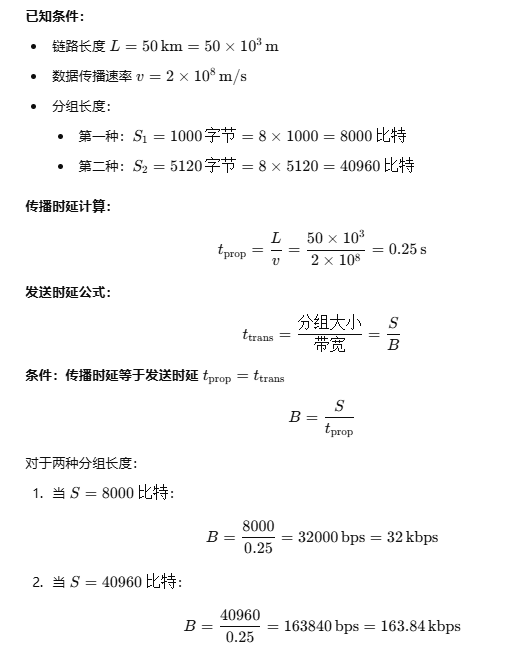
尽管SDN提供了灵活性和高效性，但在全球互联网中全面实现仍需要克服技术、经济和管理上的诸多挑战。

**计算题**

1.有一个点对点链路，长度为50km。若数据在此链路上的传播速率为2x10^8m/s

(1)试问链路带宽应为多少才能使传播时延和发送1000字节的分组的发送时延一样大?如果发送的是5120字节长的分组，结果又如何?

(2)如果发送一个分组就停止，直到接收方确认信息到来后才继续发送下一分组，忽略确认信息的发送时延，给出信道的利用率的计算公式，分析提高信道利用率可能采用的方法。



**提高信道利用率的方法：**

1. **增加带宽 B**
2. **减少传播时延**
3. **使用流水线传输（滑动窗口协议）**
4. **增加分组大小 S**

**2、主机A基于TCP向主机B连续发送3个TCP报文段,第一个报文段的序号为100.第2个报文段的序号为121，第3个报文段的号为180。**

**（1）第1、2个报文段中有多少数据?**

在TCP中，序号表示数据的起始位置。第一个报文段的序号是100，表示数据从第100字节开始；第二个报文段的序号是121，表示从第121字节开始。因此，第一个报文段的数据长度是121 - 100 = 21字节，第二个报文段的数据长度是180 - 121 = 59字节。

所以，第一个报文段有21字节数据，第二个报文段有59字节数据。

**（2）假设第2个报文段丢失而其他两个报文段到达主机B，在主机B发往主机A的确认报文中，确认号应是多少?**

TCP的确认号表示期望接收的下一个字节的序号。由于第2个报文段（序号121）丢失，主机B收到了第1个报文段（序号100到120），但没有收到第2个报文段，所以确认号应是121，表示期望接收从第121字节开始的数据。

因此，确认号应是121。

**（3）如果在UDP中加入确认与重传机制用于实现可靠传输，则发送上述同样数量的数据，是否也是分为3个UDP报文发送?说明你的理由。**

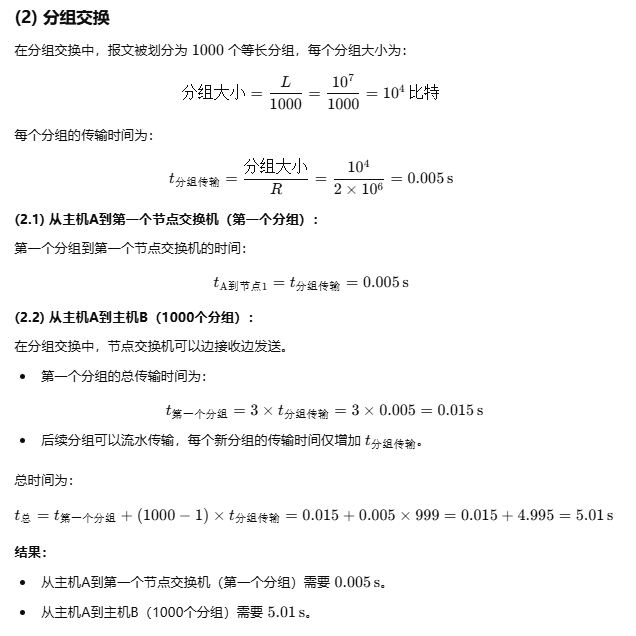
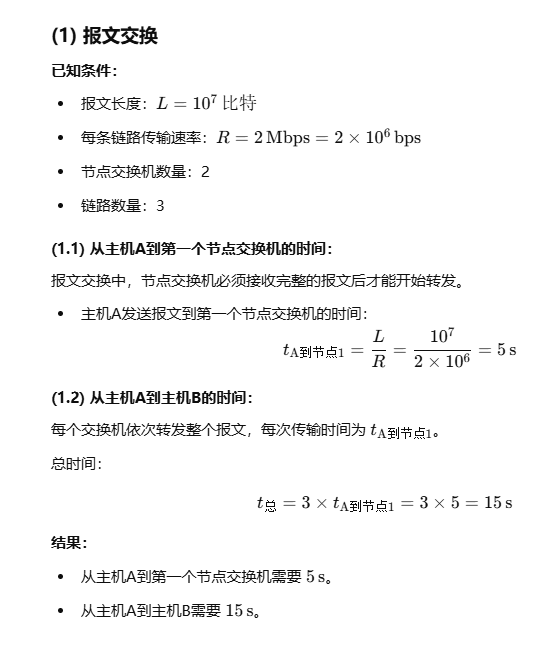
在UDP中加入确认与重传机制来实现可靠传输时，可能并不一定分为3个UDP报文发送。UDP是无连接的，每个报文都是独立的，具体是否分为3个报文发送取决于实现的策略。可能选择将数据分成3个报文，每个报文携带数据和序列号，类似于TCP的分段，或者根据需要调整分片大小。因此，虽然可能分为3个报文，但具体实现方式可能因设计不同而有所差异。

**1.主机A向主机B发送一个长度为10^7比特的报文，中间要经过两个节点交换机即一个经过三段链路。设每条链路的传输速率为2Mbits。忽略所有的传播、处理和排队时延。**

**(1)如果采用报文交换，即整个报文不分段，每台节点交换机收到整个的报文后再转发。问从主机A把报文传送到第一个结点交换机需要多长时间?从主机A把报文传送到主机B需要多长时间?**

**(2)如果采用分组交换，报文被划分为1000个等长的分组(这里忽略分组首部对本题计算的影响)，并连续发送。节点交换机能够边接收边发送。问从主机A把第一个分组传送到第一个结点交换机需要多长时间?从主机A把1000个分组传送到主机B需要多长时间?**

**(3)就一般情况而言，比较用整个报文来传送和用划分多个分组来传送的优缺点。**



(3) 报文交换与分组交换的优缺点比较

**报文交换：**优点：

简单：无需对报文进行分割或重组。

整体传输：报文在接收端完整到达，不需要额外的排序或重组操作。

缺点：高时延：必须等到整个报文到达交换机后才能继续传输，导致总时延较大。

占用资源：报文过长时，可能占用较多的缓存资源。

**分组交换：**优点：

低时延：交换机可以边接收边转发分组，传输过程流水化。

高效利用：链路可以同时传输多个流的分组，充分利用网络资源。

灵活性：分组可以独立转发和路由，适合复杂网络环境。

缺点：复杂性：需要在发送端对报文分割，在接收端重组。

数据丢失风险：分组丢失可能需要重传，增加复杂性。

**三、问答题(每小题10分，共30分)**

**1.TCP是一个可靠的传输层协议，为了实现可靠传输，TCP大量采用了计时器的机制，以便及时发现异常情况而采取措施。请问TCP有哪几类计时器，分别可以解决哪类问题?为了提高传输效率，这此计时器的等待时间应如何设置?**

**2.从技术实现角度看，局域网与广域网有何不同?以太网是一种典型的局域网技术为什么可以应用于广域网?**

**3.分别从控制层面和数据层面分析路由器的报文处理过程?**

### ****1. TCP的计时器类型及作用****

TCP使用多种计时器来确保可靠传输，主要包括以下几类：

#### ****(1) 重传计时器 (Retransmission Timer)****

* **作用**：用于检测数据包或确认包的丢失，并在超时后重传数据。
* **设置**：
  + 等待时间（超时重传时间，RTO）应动态调整。
  + 通过RTT（往返时延）的采样和估计，结合抖动情况计算RTO值。
  + 通常根据公式： RTO=SRTT+4×RTTVAR其中，SRTT 是平滑的 RTT 值，RTTVAR 是 RTT 的变化量。

#### ****(2) 保活计时器 (Keepalive Timer)****

* **作用**：用于检测对端是否存活。当连接长时间没有数据传输时，发送保活探测包。
* **设置**：
  + 保活时间间隔通常较长（如几分钟至数小时）。
  + 需要在空闲连接上保持适当的探测频率，避免网络资源浪费。

#### ****(3) 推迟确认计时器 (Delayed ACK Timer)****

* **作用**：在一定时间内延迟发送 ACK，期望更多数据到达后发送一个累计确认，以减少ACK包的数量。
* **设置**：
  + 通常设置为 40~200 毫秒。
  + 时间过长会降低响应速度；时间过短则会导致过多的小包传输。

#### ****(4) 持续计时器 (Persistence Timer)****

* **作用**：防止“死锁”问题。如果发送窗口为 0，发送端定期探测接收端的窗口是否重新打开。
* **设置**：
  + 初始间隔较短，后续探测间隔逐渐指数增长。
  + 需保证探测不占用过多带宽，同时尽快发现窗口恢复。

#### ****(5) 时间等待计时器 (TIME-WAIT Timer)****

* **作用**：确保连接的最后一个 ACK 被对方成功接收，同时防止旧数据包干扰新连接。
* **设置**：
  + 持续时间一般为 2×最大报文寿命 (MSL)。
  + MSL 通常设置为 30~120 秒。

### ****2. 局域网与广域网的技术实现差异****

#### ****(1) 局域网 (LAN) 的技术特点：****

1. **范围**：覆盖范围小（如家庭、办公室）。
2. **拓扑结构**：常用星型、总线型、环型等简单拓扑。
3. **数据速率**：一般较高（如 100 Mbps 到数 Gbps）。
4. **通信协议**：以太网（IEEE 802.3）是主流技术，使用 CSMA/CD（载波监听多路访问/冲突检测）。
5. **资源共享**：主要用于共享本地资源（如打印机、文件）。

#### ****(2) 广域网 (WAN) 的技术特点：****

1. **范围**：覆盖范围广（如城市间、国家间）。
2. **拓扑结构**：复杂，通常采用分层的网状结构。
3. **数据速率**：一般较低（如数 Mbps 至数百 Mbps），但现代技术提高了速率。
4. **通信协议**：常用 PPP、MPLS 等协议，传输技术包括光纤、卫星、无线等。
5. **资源共享**：主要用于长距离通信与数据交换。

#### ****(3) 为什么以太网可以应用于广域网？****

1. **扩展性**：现代以太网（如千兆以太网和万兆以太网）支持长距离传输和高带宽。
2. **多协议支持**：以太网可以与广域网协议（如 MPLS 和 SD-WAN）结合使用。
3. **简单性与经济性**：以太网技术成熟、成本低、部署方便。
4. **虚拟化技术**：基于以太网的 VLAN 和 VXLAN 支持分割广域网流量，增强灵活性。

### ****3. 路由器的报文处理过程分析****

路由器主要分为控制层面和数据层面两部分，各自的处理过程如下：

#### ****(1) 控制层面 (Control Plane)****

控制层面负责路由器的逻辑决策和路由管理，包括以下过程：

1. **路由发现**：通过路由协议（如 OSPF、BGP）与其他路由器交换路由信息。
2. **路由计算**：基于拓扑信息生成路由表，决定到达每个目标地址的最佳路径。
3. **路由更新**：定期更新或在拓扑变化时重新计算路由。
4. **策略控制**：应用网络管理员配置的访问控制列表（ACL）、流量策略等。

#### ****(2) 数据层面 (Data Plane)****

数据层面负责具体的报文转发操作，包括以下步骤：

1. **报文接收**：
   * 路由器接收来自输入接口的报文。
   * 检查报头的合法性（如校验和）。
2. **查找路由表**：
   * 根据报文的目标 IP 地址，在路由表中查找匹配项。
   * 如果未找到匹配项，则丢弃报文并可能发送 ICMP 错误信息。
3. **更新报头**：
   * 减少 TTL 字段值。
   * 重新计算校验和。
4. **转发报文**：
   * 根据路由表的结果，将报文发送到对应的输出接口。
   * 在必要时，进行封装转换（如 PPP、MPLS）。

### ****总结****

* **TCP计时器**通过不同的超时机制保证可靠性，其参数需动态调整以平衡可靠性与效率。
* **局域网与广域网**在范围、速率、协议等方面不同，以太网因其高扩展性和经济性被应用于广域网。
* **路由器报文处理**通过控制层面的路由管理与数据层面的高效转发协同完成。

**1.****一个应用进程使用UDP通信,到了IP层将数据报再划分为4个数据报片发送出去结果前两个数据报片丢失，后两个到达目的站。过了一段时间应用程序重传上述 UDP报文，而卫层仍然划分为4个数据报片来传送。结果这次前两个到达目的站而后两个丢失。试问:在目的站能否将这两次传输的4个数据报片组装成完整的数据报?(假定目的站第一次收到的后两个数据报片仍然保存在目的站缓存中)**

**2.我们在互联网上传送数据通常是从某个源点传送到某个终点,而并非传送过去又传**

**送回来，为什么往返时间RTT是个很重要的性能指标呢?**

**3.如果在局域网中使用TCP/IP协议族进行站点之间通信，是不是就可以放弃原来的局域网协议?说明理由。**

### ****1. UDP 数据报片组装问题****

UDP本身是无连接的、尽力而为的协议，而 IP 数据报的分片是由 IP 层完成的。分片在目的站重组时有以下特点：

#### ****分析：****

* **分片重组要求：**
  + 每个分片都有一个 **标识字段 (Identification)**，用于标识属于同一个数据报的所有分片。
  + 如果任何一个分片丢失，则整个数据报无法重组，分片将被丢弃。
* **第一次传输：**
  + 前两个数据报片丢失，后两个数据报片到达并缓存在目的站。
  + 重组失败，因为数据报片不完整。
* **第二次传输：**
  + 前两个数据报片到达，后两个数据报片丢失。
  + 重组仍然失败，因为再次分片的标识字段与第一次传输的数据报片不同（UDP 每次发送数据报都会分配新的标识字段）。

#### ****结论：****

目的站无法将两次传输的 4 个数据报片组装成完整的数据报，因为 IP 分片的标识字段不同，目的站无法将它们视为属于同一数据报。

### ****2. 为什么往返时间 (RTT) 是重要的性能指标？****

#### ****RTT 的定义：****

RTT（Round-Trip Time）是指从发送端发送一个数据包到接收端并收到确认的总时间。

#### ****RTT 的重要性：****

1. **TCP 协议依赖 RTT：**
   * TCP 使用 RTT 估算超时时间 (RTO)，以便在丢包时触发重传。
   * RTT 的变化直接影响 TCP 拥塞控制机制（如慢启动、拥塞避免）。
2. **网络性能衡量：**
   * RTT 是衡量网络时延的关键指标，能够反映网络中路由器排队、链路时延等因素的综合影响。
   * RTT 对实时应用（如视频通话、在线游戏）尤为重要，影响用户体验。
3. **优化网络协议：**
   * 应用层协议（如 HTTP/2、QUIC）利用 RTT 优化数据传输流程。
   * 在高 RTT 的网络中，协议需要通过减少握手次数等方式提高效率。
4. **诊断网络问题：**
   * RTT 增大可能意味着网络拥塞、链路质量下降等问题，是故障排查的重要依据。

#### ****总结：****

尽管大部分数据传输是单向的，但 RTT 能全面反映网络性能，直接影响数据传输的效率和可靠性。

### ****3. 是否可以放弃局域网协议使用 TCP/IP？****

#### ****局域网协议与 TCP/IP 的关系：****

1. **局域网协议（如以太网）：**
   * 工作在链路层，负责数据帧的封装、寻址和局域网内的传输。
   * 提供 MAC 地址，用于局域网中设备之间的通信。
2. **TCP/IP 协议：**
   * 工作在网络层和传输层，负责跨网络的路由选择（IP 协议）和端到端的数据传输（TCP/UDP 协议）。
   * 依赖底层链路层协议（如以太网）完成数据链路的传输。

#### ****是否可以放弃局域网协议？****

不可以直接放弃。原因包括：

1. **层次依赖：**
   * TCP/IP 协议栈需要底层链路层协议支持，才能在局域网中发送数据。
   * 以太网等局域网协议负责为 IP 数据报提供物理和数据链路层传输。
2. **地址映射：**
   * 局域网中使用 ARP（地址解析协议）将 IP 地址映射到 MAC 地址，而 MAC 地址由局域网协议提供。
3. **局域网优化：**
   * 局域网协议为局域网环境进行了特定优化（如冲突检测、广播等）。
   * 放弃局域网协议会导致性能下降。

#### ****总结：****

在局域网中使用 TCP/IP 协议族进行通信，仍然需要局域网协议的支持。TCP/IP 协议栈与局域网协议协同工作才能完成数据的可靠传输。

**四、综合题(第1小题15 分，第2小题10分，共25 分)**

**1.物联网是如何定义的?你是如何理解物联网与互联网之间的发展与继承关系的?**

**2.人工智能技术，特别是深度学习技术可用于网络拥塞控制吗?谈谈你的想法。**

### ****1. 物联网的定义与其与互联网的关系****

#### ****物联网的定义：****

物联网（IoT, Internet of Things）是指通过各种信息传感设备（如传感器、RFID、GPS、摄像头等）将物理世界中的对象（设备、机器、人等）与互联网连接，进行信息交换与通信，以实现智能化识别、定位、跟踪、监控和管理的网络系统。

#### ****物联网与互联网的发展与继承关系：****

**(1) 继承性：**

* **技术基础：**
  + 物联网建立在互联网的基础上，利用互联网的传输协议（如 TCP/IP）和通信技术（如 Wi-Fi、5G）。
  + 互联网提供了基础的连接能力，而物联网扩展了连接对象的范围。
* **逻辑架构：**
  + 两者都采用分层架构。互联网的核心是网络层和传输层，物联网则进一步细化了感知层（采集数据）和应用层（数据处理与智能决策）。

**(2) 发展差异：**

* **连接范围：**
  + 互联网主要连接人与信息，连接的终端设备是电脑、手机等。
  + 物联网拓展到物理世界，连接设备、物体、环境等。
* **数据驱动：**
  + 互联网的核心是信息共享与传播，数据传输是主要任务。
  + 物联网更注重数据采集、分析与智能决策，推动边缘计算与云计算的发展。

**(3) 互补性：**

* 物联网与互联网并非独立存在，而是相辅相成。物联网通过感知与设备管理拓展了互联网的能力，推动了智能城市、工业4.0等创新应用。

### ****2. 深度学习技术在网络拥塞控制中的应用****

#### ****深度学习在网络拥塞控制中的潜力：****

深度学习（DL）技术，特别是强化学习（RL），在解决复杂的动态问题中表现出色，适合应用于网络拥塞控制。以下是可能的应用思路：

**(1) 拥塞预测：**

* **传统方法的局限性：**
  + 传统 TCP 拥塞控制机制依赖于固定的规则（如慢启动、拥塞避免）和简单的网络指标（如丢包率）。
  + 这些规则对网络环境变化（如链路速率突变、流量激增）的适应性差。
* **深度学习的优势：**
  + 通过卷积神经网络（CNN）和循环神经网络（RNN），可以从网络流量历史数据中提取复杂的时间序列特征。
  + 实现对网络拥塞的实时预测，提前调整流量控制策略。

**(2) 动态调整：**

* **强化学习（RL）：**
  + RL 算法可以通过奖励机制学习最优的流量控制策略，动态调整发送速率或路由选择。
  + 在网络环境发生变化时，RL 模型可以自适应调整，避免拥塞。
* **示例：**
  + 使用深度 Q 网络（DQN）或 Proximal Policy Optimization（PPO）算法，实时优化发送窗口大小和数据传输路径。

**(3) 流量分类与优先级分配：**

* 通过深度学习模型对网络流量进行分类（如视频流、文件传输、实时通信），实现基于优先级的带宽分配。

#### ****可能的挑战与局限：****

1. **实时性问题：**
   * 深度学习模型的计算复杂度较高，在高吞吐量的网络中可能导致延迟。
   * 边缘计算或 FPGA 加速可部分缓解这一问题。
2. **泛化能力：**
   * 深度学习模型需要大量的训练数据，模型可能对未见过的网络场景表现不佳。
   * 引入联邦学习等技术可能提高模型的适应性。
3. **安全性问题：**
   * 深度学习模型易受对抗样本攻击，可能导致错误的拥塞决策。
4. **部署复杂性：**
   * 在大规模分布式网络中部署深度学习系统需协调多个节点，增加了系统复杂度。

#### ****总结：****

深度学习技术在网络拥塞控制中的应用具有广阔前景，可以通过智能预测、动态调整和流量优化显著提升网络性能。然而，在实际部署中仍需解决实时性、泛化能力和安全性等问题。

**1.如何认识发展下一代互联网的必要性?有人说下一代互联网就是IPv6，谈谈你的看法。**

**2.移动互联网、物联网与互联网有何区别与联系?**

### ****1. 发展下一代互联网的必要性与 IPv6 的作用****

#### ****发展下一代互联网的必要性：****

1. **地址空间的限制：**
   * 当前互联网（基于 IPv4）的地址空间（约 43 亿个地址）已基本耗尽，无法满足全球设备快速增长的需求。
   * 随着物联网设备的爆炸式增长，下一代互联网需要提供更大的地址空间。
2. **更高效的路由：**
   * IPv4 的路由表复杂度较高，下一代互联网需要更简洁、高效的路由机制，降低路由器的计算和存储开销。
3. **更强的安全性：**
   * 现有互联网面临大量的安全问题（如 DDoS 攻击、IP 欺骗）。
   * 下一代互联网需要内置安全机制（如数据加密、身份认证），减少攻击面。
4. **服务质量（QoS）：**
   * 传统互联网无法有效支持高质量的视频会议、AR/VR 等新兴应用。
   * 下一代互联网需优化服务质量，支持实时性要求高的应用。
5. **移动性支持：**
   * 当前互联网对移动设备的支持有限，而移动互联网和物联网对无缝切换、移动性支持的需求更高。

#### ****IPv6 与下一代互联网的关系：****

有人认为下一代互联网就是 IPv6，这种观点部分正确，但并不全面。

**(1) IPv6 的特点与作用：**

* **地址空间：**
  + IPv6 提供 128 位地址（2^128 个），几乎无穷的地址空间，能满足未来数十年的需求。
* **内置特性：**
  + 支持组播、自动配置、IPsec 等功能，优化了路由和安全性。
* **移动性支持：**
  + IPv6 为移动设备提供更好的支持，能实现更高效的地址切换。

**(2) 下一代互联网不仅仅是 IPv6：**

* IPv6 是下一代互联网的基础，但不是全部。
* 下一代互联网还包括：
  + **网络架构的优化：** 更高效的传输协议、边缘计算等技术。
  + **智能化网络：** 引入 AI 技术实现网络的智能管理与优化。
  + **服务模式创新：** 支持智能城市、工业互联网等新场景。

#### ****总结：****

IPv6 是下一代互联网的重要组成部分，为扩展地址空间和提高网络性能提供了基础。但下一代互联网是一个更综合的概念，还需要在安全性、移动性、服务质量等方面进行全面提升。

### ****2. 移动互联网、物联网与互联网的区别与联系****

#### ****区别：****

| **特点** | **互联网** | **移动互联网** | **物联网** |
| --- | --- | --- | --- |
| **核心目标** | 信息共享与传播 | 提供随时随地的信息访问 | 实现物理对象的互联与智能化管理 |
| **连接对象** | 计算机和服务器 | 智能手机、平板等移动设备 | 传感器、设备、机器等物理对象 |
| **通信方式** | 基于固定终端的通信 | 基于无线网络和移动终端的通信 | 设备间直接通信或通过网关通信 |
| **协议和技术** | TCP/IP、HTTP | 4G/5G、移动应用协议 | MQTT、CoAP、LoRa 等 |
| **主要应用场景** | Web、电子商务、云计算 | 移动社交、移动办公、移动娱乐 | 智能家居、工业互联网、智能交通 |

#### ****联系：****

1. **技术继承：**
   * 移动互联网和物联网都是互联网的延伸，基于 TCP/IP 协议栈进行通信。
   * 都依赖互联网的基础设施，如云计算、路由器等。
2. **数据驱动：**
   * 三者都以数据为核心，互联网侧重信息共享，移动互联网强调数据的移动性，而物联网注重数据的采集与智能分析。
3. **互相补充：**
   * 移动互联网通过智能手机为用户提供数据入口，而物联网通过传感器和设备实现数据采集，共同推动智能化应用。
4. **融合发展：**
   * 物联网和移动互联网在应用层面高度融合，如智能家居设备可通过手机控制，工业物联网设备可通过移动终端监控。

#### ****总结：****

互联网是基础，移动互联网实现了终端的移动化，而物联网扩展到物理世界中的设备和环境。三者相辅相成，共同推动了信息化和智能化社会的发展。