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?

一．分层的原因是因为减少以后继续增加功能的成本；
二．分层的好处是减少了耦合度，让功能的细化更加易于实现；
三．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）。
四．各层之间是独立的。
五．灵活性好。
六．结构上可分割开。
七．易于实现和维护。
八．能促进标准化工作。

2. 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。

3. 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。

4. （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

5. "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，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。

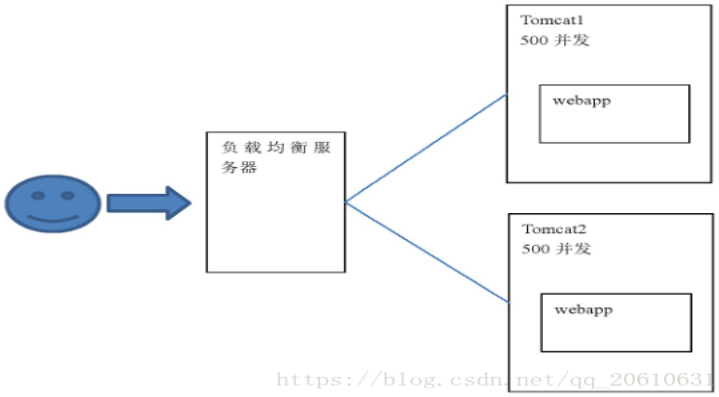
此外，该方案支持在物理网络上创建多个虚拟网络，满足多租户环境下资源隔离和灵活分配的要求。通过应用感知的动态路由技术，可以针对不同的业务需求（如带宽、时延、服务质量等）提供差异化的网络服务。系统还具有快速故障恢复能力，当网络发生变化时，控制器可以快速重新计算路径并下发新规则，从而确保业务的连续性。

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，它利用射频（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

1. **简述软件定义网络（SDN）的体系结构及其主要优点。**

   SDN 的体系结构主要包括控制平面、数据平面和应用平面。其主要优点包括灵活性高、易于管理、可编程性强，允许网络管理员通过集中控制来优化网络性能和安全。

2. **什么是网络功能虚拟化（NFV）？它与 SDN 有何关系？**

   NFV 是指将传统网络功能在虚拟环境中实现，如防火墙或路由器。NFV 与 SDN 相辅相成，NFV 提供网络功能的虚拟化，而 SDN 提供统一的网络控制，使网络管理更加灵活和高效。

3. **简述 IPv6 地址的表示方法及其优点。**

   IPv6 地址采用 128 位表示，分为 8 个 16 进制数块，用冒号分隔。其优点包括更大的地址空间、简化的头部结构和更好的安全性，如 IPsec 支持。

4. **什么是网络质量-of-服务（QoS）？简述其主要实现机制。**

   QoS 确保特定类型流量的优先级，如视频流的流畅传输。主要实现机制包括流量整形、优先级排队和资源预留，以优化网络性能。

5. **简述无线局域网（WLAN）中的 CSMA/CA 协议及其工作原理。**

   CSMA/CA（载波感知多址访问/冲突避免）用于避免数据包碰撞。设备在发送数据前检查信道是否空闲，若空闲则发送，否则等待，以减少冲突。

6. **什么是网络缓存？简述其在计算机网络中的作用。**

   网络缓存存储频繁访问的数据，减少网络延迟和带宽消耗，提高网络性能，如同一网站的本地副本。

7. **简述 TCP 的滑动窗口机制及其在流量控制中的作用。**

   TCP 的滑动窗口机制通过允许发送一定数量的包后再等待确认，控制数据流量，防止接收方被淹没，管理网络拥塞。

8. **什么是网络拓扑结构？常见的拓扑结构有哪些，并简述其优缺点。**

   网络拓扑描述设备连接方式，常见类型有星型（易管理但依赖中心 hub）、环型（适合特定应用但单点故障）、总线型（简单但信号干扰）、网状型

（冗余高但复杂）。

9. **简述网络安全中的防火墙技术及其分类。**

   防火墙控制网络流量，分类包括包过滤防火墙（检查单个包）、应用代理防火墙（基于应用过滤）和状态检测防火墙（跟踪连接状态）。

10. **什么是网络虚拟化？简述其主要技术及其应用场景。**

    网络虚拟化将物理资源抽象为虚拟资源，技术包括 VLAN、VPN 和 SDN，

    应用于云 computing、数据中心和隔离网络环境。

11. **简述区块链技术在网络中的应用及其优势。**

    区块链用于安全数据交易和去中心化应用，优势包括不可篡改性、透明性和去中心化控制，增强网络交易的信任。

12. **什么是网络切片技术？简述其在 5G 网络中的应用。**

    网络切片创建多个虚拟网络，5G 中用于支持不同服务，如低延迟的自动驾驶和高带宽的流媒体。

论述题

1. **论述软件定义网络（SDN）在企业网络中的应用及其优势。**

   SDN 在企业网络中实现集中管理，简化配置和管理，提高灵活性和可编程性，适应业务变化，优化网络性能和安全。

2. **分析当前物联网面临的主要安全威胁，并提出相应的防护措施。**

   物联网面临数据泄露、设备劫持和 DDoS 攻击，防护措施包括数据加密、强认证、定期更新和网络隔离。

3. **论述云计算环境下的网络架构设计及其挑战。**

   云计算网络需高可用性、可扩展性和安全性，挑战包括多租户管理、性能一致性和虚拟网络复杂性，解决方案涉及 SDN、负载均衡和安全措施。

4. **分析 5G 技术对物联网发展的影响。**

   5G 提供高速度、低延迟和高连接密度，支持更多设备和实时应用，推动

智能城市、工业自动化和远程医疗发展。

5. **论述人工智能在网络安全中的应用及其挑战。**

   AI 用于异常检测和威胁预测，挑战包括模型复杂性、持续学习和潜在滥用，需平衡自动化与安全性。

6. **分析边缘计算对传统网络架构的影响，并探讨其未来发展方向。**

   边缘计算减少延迟，改变传统集中式架构，未来方向包括智能边缘设备、5G 集成和边缘数据处理安全。

计算机网络模拟试卷

一、问答题（每小题 10 分，共 60 分）

1. 为什么网络协议采用分层结构设计？请结合实际说明其优势和不足。
2. 简述 TCP 和 UDP 的主要区别，并说明它们各自适用的场景。
3. HTTP/3 是如何改进 HTTP/2 的？请简述其核心技术特点。
4. 什么是 DNS？在访问一个网站时，DNS 是如何工作的？
5. 什么是防火墙？其工作原理和主要类型有哪些？
6. 请简述网络中常见的拥塞控制方法，并说明拥塞控制对网络性能的影响。

二、论述题（每小题 20 分，共 40 分）

1. 随着云计算的普及，数据中心网络的高性能需求日益增加。请结合数据中心网络的特点，提出一种优化其性能的方法，并分析其优缺点。
2. 网络安全是当前互联网的热点问题之一，请简述 DDoS 攻击的基本原理，并提出一种基于分布式防护的解决方案。

答案及解析

一、问答题

1. **网络协议分层结构的优势和不足：**
   - **优势：**
     - 便于标准化：不同厂商设备可互通；
     - 易于维护和扩展：修改某一层无需影响其他层；
     - 简化复杂性：分解任务，便于实现。
   - **不足：**
     - 增加开销：分层通信需封装和解封；
     - 性能损失：部分信息需多次处理。
2. **TCP 和 UDP 的区别：**

- **TCP**：面向连接、可靠传输（确认机制、重传机制），适用于文件传输、邮件、网页等场景；
- **UDP**：无连接、快速传输，适用于实时应用（如视频流、在线游戏）。

3. **HTTP/3 的核心技术特点：**
   - 基于 **QUIC 协议**（UDP），减少握手延迟；
   - 集成 TLS 加密，提高安全性和性能；
   - 解决了 HTTP/2 的队头阻塞问题；
   - 多路复用连接，提升传输效率。
4. **DNS 的工作流程：**
   - 用户输入域名，浏览器查询本地缓存；
   - 若无缓存，向本地 DNS 服务器发送请求；
   - 本地 DNS 服务器递归查询其他服务器；
   - 获取结果后返回 IP 地址，浏览器发起连接。
5. **防火墙：**
   - **工作原理**：监控和过滤网络通信，根据规则允许或拒绝数据包。
   - **主要类型**：
     - 包过滤防火墙：检查 IP 地址和端口号；
     - 应用层防火墙：分析应用层协议；
     - 状态检测防火墙：跟踪会话状态，判断合法性。
6. **拥塞控制方法：**
   - **方法**：慢启动、拥塞避免、快速重传、快速恢复等；
   - **影响**：改善网络性能，减少丢包和延迟，但可能影响带宽利用率。

二、论述题

1. **数据中心网络优化方法：**
   - **方法**：采用 **SDN（软件定义网络）**；
   - **优点**：分离控制平面和数据平面，集中化管理，提高资源利用效率；
   - **缺点**：初期成本高，依赖控制器的可靠性。
2. **DDoS 攻击与防护方案：**
   - **原理**：利用僵尸网络，向目标服务器发送大量请求，耗尽其资源。
   - **分布式防护**：
     - 部署 CDN 和负载均衡，分散攻击流量；
     - 使用流量清洗中心，识别并过滤恶意流量；
     - 联动 ISP 和云服务商，建立大规模防护体系。

一、问答题（每小题 10 分，共 60 分）

1. 为什么 TCP 协议能够保证可靠传输？请简述其主要机制。
2. 对比 HTTP/1.1 与 HTTP/2，在性能优化方面有何差异？
3. 软件定义网络（SDN）如何实现路由优化？请结合实际应用场景说明。
4. IPv6 相较于 IPv4 在地址空间和安全性上有哪些改进？
5. 什么是 QoS（服务质量）？在网络中如何保证 QoS？
6. 请解释 CDN 的基本原理及其在高并发情况下的作用。

二、论述题（每小题 20 分，共 40 分）

1. 传统网络中，网络资源分配效率较低，导致服务质量无法保证。试结合网络虚拟化技术，设计一个提高资源分配效率的方案。
2. 物联网设备逐渐普及，但其安全问题引发了广泛关注。请结合实际，提出一种解决方案，并分析其优缺点。

一、问答题

1. **TCP 的可靠传输机制：**
   - **字节编号**：确保数据按序到达；
   - **确认应答**：发送数据需接收方确认；
   - **超时重传**：未确认数据包超时后重发；
   - **滑动窗口**：提高传输效率，控制流量；
   - **拥塞控制**：如慢启动、拥塞避免。
2. **HTTP/1.1 vs HTTP/2：**
   - HTTP/2 使用 **多路复用**，一个连接传输多个请求，减少延迟；
   - 支持 **头部压缩**，减小数据量；
   - **服务器推送**，主动传输资源；
   - HTTP/2 基于二进制帧，传输更高效。
3. **SDN 路由优化：**
   - SDN 分离控制平面和数据平面；
   - 控制器具有全局网络视图，优化路由策略；
   - 动态调整数据传输路径，满足不同业务需求；
   - **案例**：在数据中心中，SDN 控制器可动态分配流量，避免拥堵。
4. **IPv6 改进：**
   - **地址空间**：IPv6 提供 128 位地址，解决 IPv4 地址枯竭问题；
   - **安全性**：内置 IPsec 协议，支持加密和认证；
   - **其他改进**：支持自动配置、减少路由表项。
5. **QoS：**
   - **定义**：确保网络服务的带宽、延迟、抖动和丢包率满足需求；
   - **方法**：流量优先级划分、带宽预留、排队调度算法（如 WFQ）。
6. **CDN 原理：**
   - 在多个节点分布缓存内容；
   - 用户请求由距离最近的节点响应；
   - 减少主服务器负载，提高访问速度。

1. 网络虚拟化技术提升资源分配效率的方案

方案设计：基于网络虚拟化的资源分配优化

网络虚拟化通过逻辑层面的网络分割，将物理网络资源抽象为多个虚拟网络实例，为不同的用户或业务提供隔离、按需分配的网络资源。以下是具体方案：

1. **虚拟网络切片**：将物理网络切分为多个独立的虚拟网络，每个虚拟网络根据特定的业务需求（如带宽、时延）进行定制化配置。
2. **集中式资源管理**：结合软件定义网络（SDN），使用集中式控制器进行资源监控和动态分配。
3. **动态带宽分配**：根据流量负载和业务优先级动态调整带宽，避免资源浪费或竞争。
4. **负载均衡**：通过虚拟网络设备（如虚拟交换机、虚拟路由器）均衡流量，防止某些链路过载。

优点

- **资源利用率高**：虚拟化使物理资源按需分配，减少空闲和冗余。
- **灵活性和可扩展性**：支持快速部署新业务或应用。
- **隔离性强**：确保多租户环境中业务间互不干扰，提高安全性。

缺点

- **初期成本较高**：虚拟化平台的搭建需要投入额外资源。
- **复杂性增加**：虚拟网络管理和维护需要专业技能。
- **延迟问题**：多层抽象可能增加传输延迟，需要优化架构设计。

---

2. 物联网设备安全问题的解决方案

方案设计：基于边缘计算和区块链的安全架构

1. **设备认证与访问控制**：
    - 在设备接入时，使用公钥基础设施（PKI）进行认证；
    - 基于角色的访问控制（RBAC）限制设备权限。
2. **边缘计算保护**：
    - 部署边缘计算节点，在靠近物联网设备的地方进行数据预处理和存储；
    - 边缘节点负责过滤恶意流量，减轻中心服务器的负担。
3. **区块链技术保障数据完整性**：

    - 利用区块链的去中心化特点，确保物联网设备间数据传输的完整性和不可篡改；
    - 为设备生成唯一的区块链身份标识，追踪设备行为。
4. **定期更新与补丁管理：**
    - 自动化推送更新，修复已知漏洞；
    - 强制执行设备厂商的安全合规标准。

优点

- **增强安全性**：边缘计算降低了攻击面，区块链确保数据可信。
- **分布式管理**：减少单点故障的风险，提升系统可靠性。
- **可扩展性**：适应未来大规模物联网设备的接入需求。

缺点

- **成本增加**：区块链和边缘计算的部署成本较高。
- **计算开销大**：区块链验证可能带来延迟，尤其在低功耗设备中。
- **依赖生态建设**：需要物联网设备厂商、服务商共同合作推进。

通过这些措施，网络资源分配和物联网设备的安全性问题可得到有效改善，同时为未来更广泛的网络应用场景奠定基础。