网络协议的演进和创新

Evolution and Innovation of Network Protocols

李星/LI Xing，包丛笑/BAO Congxiao
（清华大学，中国 北京 100084）
(Tsinghua University, Beijing 100084, China)

DOI：10.12142/ZTETJ.202406012
网络出版地址：http://kns.cnki.net/kcms/detail/34.1228.TN.20250109.0925.002.html
网络出版日期：2025-01-09
收稿日期：2024-10-15

摘要：总结了传输控制协议/互联网互联协议（TCP/IP）的分布式架构、无连接传输、尽力而为的服务模型、端对端通信模型和开放性5个基本特征，指出这些特征是TCP/IP优于其他网络协议的根本原因。针对新的网络需求，分析这些特征的异化。指出在当前快速变化的技术环境中，TCP/IP作为互联网的基石，其核心思想依然具有重要意义。要充分利用互联网协议第6版（IPv6）的机遇，努力创新以适应人工智能等新技术发展带来的挑战。

关键词：网络体系结构；网络协议；TCP/IP；IPv6

Abstract: The five basic characteristics of transmission control protocal (TCP)/Internet protocal (IP) are summarized, including distributed architecture, connectionless transmission, best-effort service model, end-to-end communication model, and openness. It points out that these characteristics are the fundamental reasons TCP/IP is better than network protocols. The alienation of these features for the new network requirements is analyzed. It also points out that in the current rapidly changing technological environment, TCP/IP, as the cornerstone of the Internet, its core idea is still of great significance. It is necessary to make full use of the opportunities of IPv6 and strive to innovate to meet the needs brought about by new technologies such as artificial intelligence.

Keywords: network architecture; network protocol; TCP/IP; IPv6

引用格式：李星, 包丛笑. 网络协议的演进和创新 [J]. 中兴通讯技术, 2024, 30(6): 74-83. DOI: 10.12142/ZTETJ.202406012
Citation：LI X, BAO C X. Evolution and innovation of network protocols [J]. ZTE technology journal, 2024, 30(6): 74-83. DOI: 10.12142/ZTETJ.202406012

1 TCP/IP的发明和网络技术演进

2024年是ARPANET诞生55周年，也是中国全功能接入互联网30周年。网络协议演进过程的回顾，对把握未来网络技术的发展方向具有重要的参考意义。

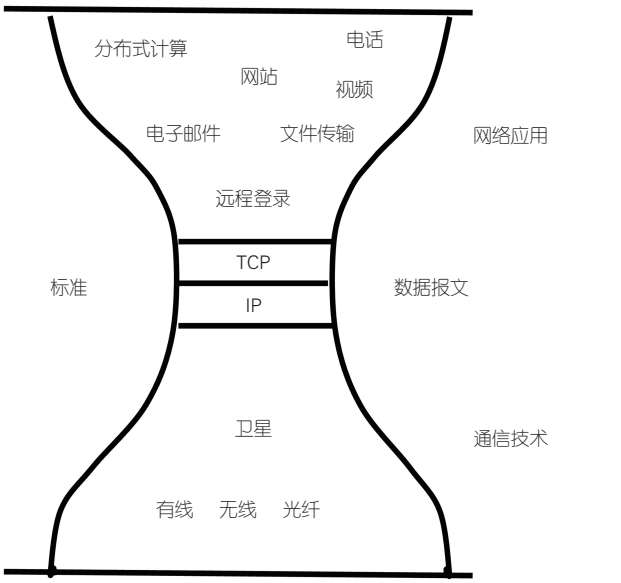
1.1 计划中的信息高速公路

人类于1852年发明了电报，1876年发明了电话，1946年发明了数字计算机（ENIAC），1957年发射了世界上第一颗人造地球卫星（Sputnik），1958年发明了集成电路。随着数字计算机、地球同步通信卫星和集成电路等技术的发展，模拟电话于20世纪70年代开始向数字电话演进。当时计划先从模拟电话网演进到综合数字网（ISDN），演进到窄带综合业务数字网（N-ISDN），并在“信息高速公路”概念的促进下，演进到宽带综合数字网（B-ISDN），最终成全球信息基础设施（GII）。虽然计划很完美，但传输控制协议/互联网协议（TCP/IP）的出现，改变了一切[1-2]。

1.2 ARPANET和TCP/IP

ARPANET是世界上第一个实现分组交换技术的计算机网络，ARPANET由美国国防部高级研究计划局（DARPA）于20世纪60年代末开始部署，旨在实现不同地理位置之间的计算机通信和资源共享，提供可靠的通信手段，促进科研合作，增强国家安全。在ARPANET的早期阶段，网络控制程序（NCP）是主要的通信协议。然而，随着网络规模的扩大和需求的增加，NCP的局限性逐渐显现出来。首先，NCP仅适用于特定类型的网络硬件，缺乏灵活性和可扩展性；其次，在处理复杂通信任务时表现不佳，难以满足日益增长的应用需求。为了突破这些局限性，研究人员开始探索新的网络协议。20世纪70年代初，人们提出了TCP/IP。TCP/IP采用分层架构，极大地提高了网络的可扩展性和兼容性。互联网体系结构的“细腰模型”如图1所示。

1983年1月1日，ARPANET正式从NCP过渡到TCP/IP，这一转变标志着互联网时代的真正开始[3]。



▲图1　互联网的“细腰模型”

1.3 TCP/IP 的基本特性

TCP/IP 协议族作为互联网的核心协议，具有多种特性。这些特性使得 TCP/IP 在全球范围内广泛应用并取得了巨大的成功[4–5]。

1）分布式架构

TCP/IP 采用了分布式设计理念。这意味着网络中的每个节点都具有相同的地位和功能，没有集中控制的核心节点。分布式架构的主要优势在于其高可靠性和灵活性。由于没有单一的控制中心，网络的故障点减少，即使某个节点出现问题，也不会影响整个网络的正常运行。

2）无连接传输

TCP/IP 中的 IP 采用了无连接传输的原理。无连接传输意味着每个数据包在网络中独立传输，不依赖于其他数据包或连接状态。这种设计使得网络能够处理大量并发数据流，提高了整体吞吐量和效率。

3）尽力而为的服务模型

TCP/IP 采用了尽力而为（Best–Effort）的服务模型。这种模型不保证数据包一定能够到达目的地，也不提供任何形式的质量保证或错误恢复机制。尽力而为地实现依赖于网络中各节点的自主决策和路由算法，每个数据包在传输过程中会根据当前网络状态选择最优路径。

4）端对端通信模型

TCP/IP 采用了端对端的通信模型。这意味着数据传输从源端到达目标端时，中间网络设备不对数据内容进行修改或处理。端对端通信模型在网络设计中具有重要意义：它简化了网络层的功能，使得应用层可以根据需要实现各种复杂功能。此外，端对端通信模型增强了数据传输的透明性和安全性，确保数据在传输过程中不会被篡改或泄露。

5）开放性

TCP/IP 协议族具有高度的开放性，这主要体现在其标准化流程上。互联网工程任务组（IETF）是负责 TCP/IP 标准化的主要机构。IETF 通过公开讨论和协作，确保所有相关方都能参与到标准制定的过程中。标准化流程通常包括以下几个步骤：提出草案、公开评审、修订并最终发布为 RFC（IETF 发布的一系列备忘录）文档。这种开放的标准化流程不仅促进了技术创新，还确保了协议的广泛接受和兼容性。开放性使得 TCP/IP 能够快速适应新技术和新需求，持续推动互联网的发展。

基于 TCP/IP 的互联网也是开放的，体现在地址的唯一性、域名的唯一性和协议标准和协议参数的唯一性上。边界网关协议（BGP）可以使各自管理独立的自治域实现互联互通。

1.4 协议之战

1）TCP/IP 与 X.25 之战

X.25 是一种早期的分组交换网络协议，由国际电信联盟（ITU）于 1976 年制定。它主要用于数据通信和远程终端连接，并在当时的公共数据网（PDN）中占据重要地位。X.25 采用面向连接的传输模式，提供可靠的错误检测和纠正机制，确保数据包能够准确到达目的地。X.25 虽然在早期占据重要地位，但其复杂性和灵活性不足使其逐渐被边缘化。TCP/IP 的成功证明了分布式、简洁、灵活和透明的协议设计在现代通信中的重要性[6]。

2）TCP/IP 与 ISDN 之战

ISDN 是一种在 20 世纪 80 年代和 90 年代业界推广的电信标准。它旨在提供高带宽的数字传输服务，能够同时处理语音、数据和视频等多种类型的通信需求。N–ISDN 协议采用了 2B+D 的结构：两个 B 信道用于传输数据，每个信道提供 64 kbit/s 的带宽；一个 D 信道用于控制信令，提供 16 kbit/s 或 64 kbit/s 的带宽。最终，TCP/IP 协议在与 ISDN 的竞争中胜出。主要原因包括：TCP/IP 的灵活性和可扩展性使其能够适应不断变化的互联网环境，而 ISDN 则显得相对僵硬。N–ISDN 一度成为互联网“最后一公里”的接入技术，称为“一线通”，但其成本和速率无法与后续的非对称数字用户线路（ADSL）和无源光纤网络（PON）技术竞争，而其话音强项又被网络电话（VoIP）完全替代[7]。

3）TCP/IP与ATM之战

异步传输模式（ATM）于20世纪80年代被业界提出，是一种高带宽、低延迟的网络技术，最初用于电信公司的语音和数据通信。ATM采用固定长度的53字节单元（称为信源）进行数据传输，这种设计使其能够提供高效的多媒体传输服务，包括实时语音、视频和数据。在20世纪90年代，ATM被认为是未来网络技术的重要组成部分，特别是在广域网（WAN）中的应用。最终，TCP/IP在与ATM的竞争中胜出，主要原因为：ATM与TCP/IP的分布式、无连接、尽力而为和端对端的特征完全是相反的，因此在大规模网络中面临可扩展性问题；虽然ATM提供了高质量服务，但其复杂性和成本在动态网络环境中无法实现。在1995年，ATM 155 Mbit/s的带宽比三次群T3（45 Mbit/s）或E3（34 Mbit/s）有优势，因此美国超高速网络服务（vBNS）使用了classic IP over ATM技术。在局域网中的ATM技术如 局域网仿真（LANE）和ATM支持多协议（MPOA）与IP over Ethernet的技术相比完全没有优势，但逐步衍生出了多协议标签交换（MPLS）[8]技术。

4）TCP/IP与私有协议之战

在互联网发展的早期阶段，TCP/IP还面临着多种私有协议的挑战。这些私有协议包括系统网络架构（SNA）、网络输入输出系统（NetBIOS）/ NetBIOS扩展用户界面（Net - BEUI）、数字设备公司网络（DECnet）、虚拟网络交换（VINES）、Xerox网络系统（XNS）、UNIX到UNIX复制（UUCP）、苹果交谈协议（AppleTalk）和互联网数据包交换（IPX）/序列分组交换协议（SPX）等。虽然它们在各自领域内占据重要地位，但最终都未能抵挡TCP/IP的崛起[9]。

（1）SNA

SNA是由IBM开发的网络架构，主要用于大型企业和政府机构的数据通信。它提供了强大的错误检测和纠正功能，适用于高可靠性需求的场景。SNA在网络层和更高层次上都采用面向连接的架构。

（2）NetBIOS/NetBEUI

NetBIOS是一种应用程序编程接口（API），该接口为开放系统互联（OSI）模型的会话层提供服务。它允许不同计算机上的应用程序通过LAN进行通信。NetBEUI是一种简单的轻量级网络协议，用于小型局域网。NetBIOS在会话层是面向连接的，但可以在网络层上运行无连接和面向连接的传输协议。

（3）DECnet

DECnet是由Digital Equipment Corporation开发的网络协议，主要用于虚拟地址扩展（VAX）和程序数据处理机（PDP）之间的通信。它提供了高效的数据传输和管理功能。DECnet IV在网络层采用面向连接的架构，在通信实体之间建立逻辑连接，以确保数据的可靠和有序传输。DECnet V（DECnet/OSI）在网络层支持面向连接和无连接通信。

（4）VINES

VINES是由Banyan Systems开发的网络协议，主要用于企业级局域网通信。它提供了高效的路由和服务定位功能。在网络层采用面向连接的架构。

（5）XNS

XNS是由施乐公司开发的网络协议，主要用于局域网通信。它提供了高效的数据传输和管理功能。XNS中的网络层协议是无连接的。

（6）AppleTalk

AppleTalk是由苹果公司开发的网络协议，主要用于Macintosh计算机之间的通信。它提供了高效的数据传输和管理功能。AppleTalk中的网络层协议是无连接的。

（7）IPX

IPX是一种网络协议，最初由Novell开发，用于其Net - Ware操作系统。它主要用于在计算机网络中传输数据包，特别是在LAN和WAN环境中。IPX中的网络层协议是无连接的。

总之，基于面向连接架构的私有网络协议与TCP/IP比较，灵活性、简单性差一些。虽然私有网络协议也有无连接的，但这些协议基本上是基于局域网的，不具备可扩展性。同时，所有私有网络协议都不具有开放性，因此在与TCP/IP的对决中失败是必然的。

5）TCP/IP与OSI之战

OSI模型是由国际标准化组织（ISO）在20世纪80年代提出的网络通信标准。OSI模型将网络通信过程分为7层，每一层具有不同的功能。这种分层设计使得各层之间独立运行，便于模块化开发和维护。OSI模型在当时被认为是网络通信标准的未来方向，具有系统性和科学性的特点。但是，OSI模型在网络层提供了面向连接的协议（如X.25）和无连接网络协议（CLNP），这两种协议分别满足不同的通信需求。OSI模型在传输层只有面向连接的TP4协议，提供可靠的数据传输服务。与之相比，TCP/IP的网络层协议IP采用无连接传输方式，数据包独立传输，不需要建立连接。TCP/IP的传输层包括TCP和用户数据报协议（UDP）。TCP提供面向连接的可靠传输，而UDP则提供无连接的不可靠传输服务。这种选择使得TCP/IP既简单适用于各种链路层协议（IP over Everything），又能够灵活地应对各种应用的需求（Everything over IP）[10]。

2 TCP/IP 网络的异化

TCP/IP 的“分布式”“无连接”“尽力而为”“端对端”和“开放性”的技术特征带来的最大优势是“可扩展性”，而 TCP/IP 的“安全性”和“服务质量”是相对的弱项。研究人员希望从体系结构上改进 TCP/IP，以使弱项变强，但却有意识或无意识地把 TCP/IP 的技术特征异化。

2.1 去“分布式”的异化

1）软件定义网络（SDN）

SDN 的主要目标是通过将网络控制与数据转发分离来简化网络管理，提高灵活性。其技术特点为：控制平面与数据平面分离，集中化管理，通过虚拟化技术支持网元的可编程性。由于 SDN 是中心式而不是分布式的架构，其所面临的问题为：控制器有单点故障风险，总体复杂性增加，兼容性差。SDN 可以在特定场景下（如数据中心、企业内部网络等）提供更高的灵活性和管理效率，而不可能在多个独立管理域的情况下被大规模使用[11]。

（1）域名系统（DNS）和域名系统安全扩展（DNSSEC）

DNS 是一个分布式数据库系统，用于将人类可读的域名（如 www.example.com）转换为计算机可理解的 IP 地址。这使得互联网上的资源更容易被访问和管理。尽管 DNS 是一个分布式系统，但其“根”服务器和顶级域名服务器在某种程度上具有中心化的特征。这可能导致单点故障、性能瓶颈和安全风险。DNSSEC 是一套用于增强 DNS 安全性的协议扩展，通过数字签名来确保 DNS 查询响应的真实性和完整性。DNSSEC 通过引入信任链和密钥管理机制，增强了对中心化服务器（如根服务器和顶级域名服务器）的依赖性。这在某种程度上加强了 DNS 系统的中心化趋势。因此，DNS 的运行确实存在着解析链断裂的问题，这给网络的可生存性带来风险。目前各种解决方案的本质是试图使域名系统重新具有“分布式”的特性[12]。

（2）路由安全和资源公钥基础设施

互联网上运行 BGP 的路由系统是典型的分布式系统，但是这一系统面临着路由劫持等安全风险。近年来互联网引入了资源公钥基础设施（rPKI）。rPKI 是一种基于密码学的安全框架，它可以通过验证 IP 地址和自治系统号码（ASN）的所有权来防止 BGP 路由劫持等问题。rPKI 系统由 5 个信任锚点构成，每个信任锚点由一个区域互联网注册管理机构（RIR）管理。这些 RIR 包括亚太网络信息中心（APNIC）、北美互联网号码分配机构（ARIN）、非洲网络信息中心（AFRINIC）、拉丁美洲网络信息中心（LACNIC）和欧洲网络协调中心（RIPE NCC）。虽然 rPKI 系统有 5 个信任锚点，但 rPKI 的运行确实存在着丢锚的问题，给网络的可生存性带来风险[13]。

2.2 去“无连接”的异化

1）OpenFlow

OpenFlow 是一种 SDN 技术，它通过将控制平面与数据平面分离，使网络设备的转发行为由中心化的控制器动态管理。OpenFlow 可以被认为是一种面向连接的技术，因为中心控制器根据 OpenFlow 五元组（源 IP 地址、目的 IP 地址、源端口号、目的端口号和协议类型）甚至更多的特征来决定数据包的转发路径。OpenFlow 交换机维护一个或多个流表，每个流表包含一组流条目。每个流条目包括匹配域、优先级、计数器、操作集合和超时值。OpenFlow 具有的特点为：灵活性、可编程性、网元的可管理性和控制接口的开放性，但是没有了无连接的特性。这使得 Openflow 的问题，例如可扩展性差、复杂度高、兼容性差等突显出来。OpenFlow 可以在特定场景下（如数据中心、企业内部网络等）提供更高的灵活性和管理效率，但却不能在多个独立管理域的情况下大规模使用[14]。

2）MPLS

MPLS 是一种高效的网络传输机制，它结合了第二层和第三层的功能。在数据包前面加上固定长度的标签进行路由和转发决策。MPLS 通过引入标签和标签交换路径（LSP），实现了一种类似于虚电路的面向连接机制。这使得 MPLS 在提供高效转发、流量工程和服务质量（QoS）保证方面具有显著优势。虽然 MPLS 在某些方面仍然保留了无连接网络的特性（如 IP 地址的路由决策），但其核心机制是基于面向连接的原则设计的。因此，我们可以认为 MPLS 是一种面向连接的技术。MPLS 一般在单个自治域内部署，无法扩展到整个互联网[15]。

3）分段路由（SR）和基于 IPv6 转发平面的 SR

SR 是一种源路由技术，它允许数据包沿着预定义的路径在网络中传输。SRv6 是将 SR 应用于 IPv6 网络的具体实现。SRv6 使用分段 ID（SID）来表示网络中的节点或路径段。每个 SID 可以表示一个 IPv6 地址或其他类型的标识符。SRv6 允许在源节点上对数据包进行路径编程，即在发送数据包时指定其完整的传输路径。这使得网络可以根据业务需求和策略动态调整数据流的路径。SRv6 在极端情况下，可以类比为面向连接的模式。SRv6 的特点为：当每一跳都被明确定义时，数据包的传输路径是确定的，从而可以更精细地控制流量分布，优化网络资源利用率；由于路径是预先定义的，SRv6 也可以降低数据包在网络中被随意转发的风险，

增强安全性。一般认为SRv6可以根据分段的多少，在面向连接和无连接之间寻找平衡，以达到预设的目标[16]。

2.3 去“尽力而为”的异化

为了确保网络QoS，避免在“尽力而为”模式下可能出现的性能问题，研究人员开发了若干技术[17]。

1）集成服务

集成服务（IntServ）的典型实现为资源预留协议（RSVP），用于预留网络资源，确保特定数据流获得所需的带宽、延迟和抖动。RSVP能够为每个数据流提供精确的QoS保证，支持动态资源预留和释放，适应网络变化。但是RSVP可扩展性差，在大规模网络中，管理大量数据流的资源预留非常复杂，且资源消耗大，需要在每个节点上维护大量状态信息，这增加了网络设备的负担。

2）区别服务（DiffServ）

DiffServ通过在数据包头部添加流类标记DSCP字段来标识不同的服务类别，比InterServ有更好的可扩展性。DiffServ简化了网络中的QoS管理，但是难以为单个数据流提供精确的QoS保证。同时，DiffServ需要在整个网络中统一配置和管理QoS策略，否则可能出现不一致性。

2.4 去“端对端”的异化

传统的TCP/IP是端对端的。动态地址分配、地址转换设备（NAT）和内容分发网络（CDN）的引入，使互联网不再支持端对端的特性[18]。

1）地址转换设备

由于IPv4的地址耗尽问题，地址转换设备（NAT）技术广泛应用于客户机联网。NAT将内部私有IP地址映射到外部公共IP地址，以便在公共网络中进行通信。为了区分多个内部主机的流量，NAT设备会使用不同的端口号进行映射。NAT的特点是：缓解IPv4地址短缺问题，能够在对上游网络运营商的情况下有效地进行流量调度，简化了网络管理。NAT破坏了端对端连接，带来了连接穿透问题，并因为协议兼容性增加了溯源的难度。

2）CDN

CDN通过在全球范围内部署大量的服务器节点，将内容缓存到距离用户最近的节点上，以减少延迟，提高访问速度。CDN根据网络状况、服务器负载和用户位置等因素动态分配流量，确保资源利用率最大化；通过缓存静态内容（如图片、视频、层叠样式表文件等）和部分动态内容，减少源站的负载并加快响应速度；通过DNS解析技术将用户请求重定向到最佳的服务器节点，实现智能路由和流量优化；提供多层次的安全防护，包括分布式拒绝服务（DDoS）攻击防御、安全套接层（SSL）/传输层安全性协议（TLS）加密、Web应用防火墙（WAF）等，确保内容传输的安全性。但是CDN使用分布式服务器节点，用户请求被重定向到最佳的节点上，源站的IP地址并不唯一。这打破了传统TCP/IP模型中端对端通信的直接性，使得数据传输路径变得更加复杂，难以进行端到端的追踪和监控。CDN也存在缓存一致性问题。在动态内容频繁更新的场景下，确保所有节点上的缓存内容一致性对CDN来说是一个挑战。

2.5 去“开放性”的异化

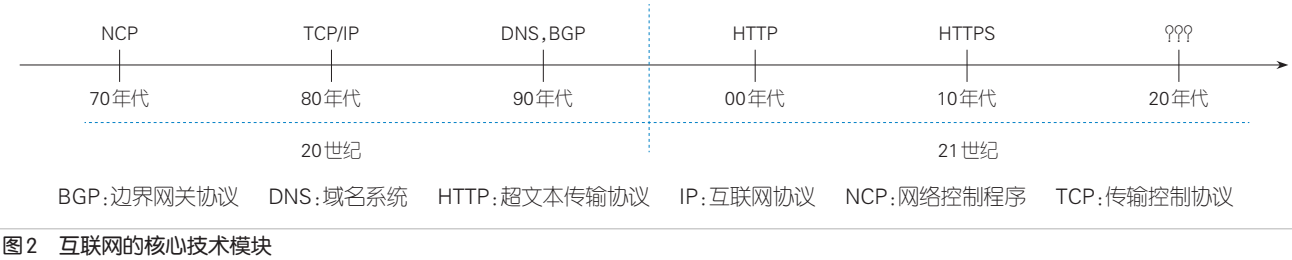
总体来说，目前互联网标准的制定过程依然延续着IETF的工作流程，保持了TCP/IP标准的开放性。但基于某些原因，若干设备厂商和运营商也在推行不经过IETF流程的私有协议。在专网和“围墙花园”的场景下，网内确实可以采用未经IETF标准化的私有协议，也不需要全球的地址唯一性和域名唯一性，但这确实是一种对于“开放性”的异化，从长远的视角看会对全球互联网的互联互通带来危害[19]。

3 互联网的核心技术模块

以10年为一个周期，过去50年来最具代表性的互联网核心技术模块如图2所示。

3.1 NCP

20世纪70年代业界的核心技术是网络控制程序（NCP）



▲图2 互联网的核心技术模块

协议。NCP是ARPANET在20世纪70年代的核心技术组件，是世界上第一个规模部署的分组网络，为主机间通信管理、数据传输和流量控制提供了基本功能。值得一提的是NCP协议是一个面向连接的协议。尽管NCP最终被TCP/IP取代，但它在互联网早期的发展中扮演了关键角色，为现代网络协议的设计和实现积累了宝贵经验[3]。

3.2 TCP/IP

20世纪80年代业界的核心技术是TCP/IP。TCP/IP是一组通信协议，用于在互联网上的数据传输。这些协议由DARPA资助开发，最初用于ARPANET的改进和扩展，之后IETF接手了其标准化方面的工作。TCP/IP协议是现代互联网的基础，提供了可靠、灵活和高效的通信能力。TCP/IP协议栈在20世纪80年代的推广和标准化为互联网奠定了基础，其分层架构、可靠传输机制和灵活的路由算法使得全球范围内的计算机网络能够高效地进行通信和数据交换[3]。

TCP/IP中的IP是网络层协议，TCP是传输层协议。

1）IP

IP实现了TCP/IP的“分布式”“无连接”和“尽力而为”的技术特征。目前仍然广泛使用的是版本4（IPv4），但其面临着地址耗尽的问题。IPv6是下一代的网络层协议。全球互联网目前仍然处于从IPv4到IPv6的过渡阶段。

2）TCP等

TCP等传输层协议实现了TCP/IP的“端对端”技术特征。在早期的互联网设计中，TCP和IP是紧密结合在一起的。然而，随着需求的增加和应用场景的多样化，两者的分离成为必要。这主要有两个原因：一是，不同的应用对传输层协议有不同的需求，例如，TCP提供可靠的数据传输，而UDP则提供无连接、尽力而为的服务，适合于实时性要求高但可以容忍一定丢包率的应用；二是，分离后的IP层能够更好地处理路由和网络层的问题，这使得整个网络架构更加灵活和模块化。这种分离不仅简化了协议设计，还为后续的扩展和优化提供了便利。

TCP的拥塞控制算法是TCP成功的关键因素之一，包括慢启动、指数增长和后退机制。通过这些机制，TCP能够有效地避免网络拥塞，提高整体性能。在慢启动阶段，发送端逐步增加发送窗口大小，直至检测到丢包；在指数增长阶段，迅速扩大传输速率，以充分利用可用带宽；后退机制在检测到拥塞时减少发送窗口，从而缓解网络负担。这些算法共同作用，确保了数据传输的高效性和稳定性，为互联网的顺利运行提供了坚实的基础。

从广义上来讲，任何在网络层之上的协议都可以被视为传输层协议，具体由IPv4报头中的“协议”或IPv6的“下一个报头”来定义。这意味着可以有256种广义传输层协议，包括但不限于TCP和UDP。但是，互联网严格意义上的传输层协议只有TCP和UDP取得了广泛的应用，其他协议如数据报拥塞控制协议（DCCP）、流控制传输协议（SCTP）等并未获得同样的成功，原因主要在于这些协议在设计和实现上存的局限性。此外，TCP和UDP已经形成了庞大的生态系统和标准化体系，新协议难以替代它们。

运行在TCP之上的TLS取得了巨大的成功。TLS通过加密数据传输和身份验证，有效地防止了数据窃听、篡改和伪造等威胁。运行在TLS之上最典型的应用层协议是超文本传输协议（HTTPS），它广泛应用在电子商务、金融交易和社交媒体等领域，确保了数据传输的安全性和隐私保护。

在UDP基础上运行的快速UDP互联网连接（QUIC）协议集成了端对端的数据一致性、安全性和流控，是传输层协议的重大进展。QUIC通过减少握手时间和改进拥塞控制算法，显著提高了数据传输的效率和可靠性。其多路复用机制还能够在单个连接上并行传输多个流，从而优化资源利用，降低延迟。

未来，传输层协议的发展可能包括以下几个方向：进一步优化拥塞控制算法，以适应更加复杂和动态的网络环境；增强安全性和隐私保护措施，以应对日益严峻的网络威胁；探索基于人工智能和机器学习的自适应传输策略，以提高数据传输的智能化水平。

3.3 BGP和DNS

20世纪90年代业界的核心技术是BGP和DNS。

1）BGP

BGP是一种在自治系统之间交换路由信息的互联网协议。作为外部网关协议（EGP）的一部分被引入，BGP具有优越的可扩展性，最终取代了EGP。1994年，BGP版本4（BGP–4）在RFC 1654中正式发布，这是目前广泛使用的版本。BGP–4引入了多个重要特性：支持路径向量协议，拥有自治域号码（ASN）和路径属性，支持策略控制、循环检测，具备扩展性。BGP–4的引入极大地提升了互联网的稳定性和扩展性。它允许不同自治系统之间进行高效的路由交换，并通过策略控制机制提供了灵活的管理手段。随着IPv6的普及和MPLS等技术的引入，BGP也不断演化以适应新的需求[20]。

2）DNS

DNS是互联网中用于将人类可读的域名转换为计算机可理解的IP地址的关键协议。从20世纪末到21世纪初，DNS

逐渐成熟并广泛应用于互联网中。DNS技术特征为：拥有分布式数据库，支持层次结构、多种记录类型，具备缓存机制，支持动态更新。20世纪90年代逐步成熟的DNS协议在互联网发展中扮演了至关重要的角色，其技术特征和里程碑事件不仅推动了域名解析技术的进步，也为后续的网络扩展和创新奠定坚实的基础。通过不断的改进和优化，DNS协议继续在全球互联网中发挥着关键作用[12]。

3.4 HTTP

21世纪初业界的核心技术是支持万维网（WWW）的超文本传输协议（HTTP）。HTTP是互联网中用于数据通信的基础协议。HTTP技术特征为：具有请求-响应模型、无状态性、头部信息、缓存控制，支持多种方法、持久连接等。21世纪初是HTTP协议快速发展和普及的时期。其技术特征和里程碑事件不仅推动了Web技术的进步，也为后续的网络扩展和创新奠定了坚实的基础。通过不断的改进和优化，HTTP协议继续在全球互联网中发挥着关键作用，支持各种复杂的Web应用和服务[21]。

3.5 HTTPS

21世纪00年代，业界核心的技术是HTTPS。HTTPS和TLS是互联网中用于保障数据传输安全性的关键技术。21世纪10年代是HTTPS/TLS协议快速发展和普及的时期，技术特征和里程碑事件显著推动了其在全球范围内的应用和扩展。HTTPS/TLS技术特征为：加密传输，需要身份验证，数据具有完整性，使用密钥交换，支持多版本、扩展机制等。值得一提的是：2013年的斯诺登事件、2015年由电子前沿基金会（EFF）和Mozilla等组织推动的HTTPS Everywhere运动，使HTTPS得到了广泛的部署。HTTPS/TLS协议在全球互联网中发挥着关键作用，保障数据传输的安全性和隐私性[21]。

4 互联网技术部署速率和创新

从互联网具体技术模块的角度看，可以观察到一个非常有趣的现象，有些创新型的技术虽然非常重要，但是其部署过程非常缓慢，例如：IPv6、DNSSEC、rPKI等；也有些黑马类的技术，其普及过程极其迅速，例如：NAT、HTTPS等。

4.1 部署速率比较分析

1）DNS安全扩展

DNSSEC是一项用于增强DNS安全性的技术，其主要目标是通过数字签名和加密来保护DNS查询和响应，防止DNS欺骗和缓存中毒等。DNSSEC规范于1997年发布，1998—1999年进行了改进和重新设计，2006年再次修订。2010年，根区域启用了DNSSEC签名，这标志着DNSSEC开始在全球范围内逐步部署和推广。但是，目前DNSSEC的部署和使用情况仍然相当有限。究其原因在于：DNSSEC复杂性大，存在兼容性问题，缺乏部署动力，并存在实施风险等[12]。

2）rPKI

rPKI的主要目标是提高互联网路由安全性，防止BGP劫持等攻击。2010年IETF定义了rPKI的基本框架和操作规范，2015年区域互联网注册管理机构（RIR）和互联网服务提供商（ISP）开始逐步部署rPKI，并推动其在全球范围内的采用。但直至今日，rPKI的部署和使用情况仍然相当有限。究其原因在于：rPKI复杂性大，存在兼容性问题，缺乏部署动力，实施存在风险等[13]。

3）NAT

NAT主要目的是解决IPv4地址短缺问题，提高网络安全性。1994年IETF定义了NAT的基本框架以及地址转换和端口映射操作规范，至此NAT就迅速得到普及。NAT快速普及的原因为：NAT简单易实现，安全性强，兼容性好，能够对部署者立即产生正面效果[22]。

4）HTTPS

HTTPS是一种在HTTP协议基础上加入SSL/TLS安全层的通信协议，其主要目的是提高数据传输的安全性，防止数据在网络传输过程中被窃取或篡改。1994年Netscape Communications公司开发了SSL协议。1995年Netscape发布了SSL 2.0和3.0版本，并开始在其浏览器中支持这些协议。1999年IETF标准化了SSL 3.0，并将其发展为TLS 1.0协议。2018年IETF发布了TLS 1.3版本，大幅度改进了安全性和性能，减少了连接延迟并移除了一些不安全的加密算法。HTTPS技术在全球范围内得到了快速部署和广泛应用，主要原因为：人们对于安全需求有所增加，主流浏览器支持HTTPS；搜索引擎优化促进HTTPS推广；HTTPS技术快速成熟。特别是免费证书颁发机构如Let's Encrypt的出现，使得获取和管理SSL/TLS证书更加便捷和低成本。此外，政策和法规的推动以及技术生态系统支持也是重要原因[21]。

综上所述，部署缓慢的技术有如下特点：

- 涉及范围广，需要从设备到软件再到基础设施的全面升级。
- 复杂性高，配置和管理复杂，需要人们具备专业知识和经验。
- 成本高，硬件和软件升级涉及高额成本。

• 现有系统依赖，许多应用和服务仍然基于旧协议设计，迁移需要时间和资源。

部署迅速的技术有如下特点：

• 涉及范围小，通常只需在局部进行配置或升级。

• 复杂性低，配置和管理相对简单，无须大规模基础设施升级。

• 成本低，硬件和软件升级成本较低，甚至不需要额外投资。

• 用户需求驱动，能够迅速满足用户或市场的需求，提供明显的短期效益。

4.2 IPv6过渡技术分析

IPv6技术也是典型的部署缓慢的技术，主要原因包括：需要对现有基础设施投资；无法和IPv4互联互通；IPv4仍有一个活跃的二级市场，供企业或用户满足需求；企业和用户缺乏强烈的动机去主动转向IPv6[22]。

1） 以双栈技术为主的传统IPv6过渡技术

传统的IPv6过渡技术的思路是“尽量使用双栈，必要时使用隧道”。然而，双栈方法虽然在技术上可行，但无法解决上述部署成本高、无法与IPv4互联互通等一系列重大问题。

2） 以翻译技术为主的新一代IPv6过渡技术

新一代的IPv6过渡技术（如RFC6145、RFC6052、RFC6146、RFC7599等）提出了“尽量使用翻译，必要时使用双重翻译或隧道，外特性为双栈”的思路。通过翻译技术，IPv6单栈服务器和IPv6单栈客户机可以与现有的IPv4互联网互联互通。这样一来，部署翻译器的网络可以率先过渡到IPv6单栈，同时保证与IPv4互联互通。翻译技术的优点为：

• 涉及范围小，通常只需在局部进行配置或升级。

• 复杂性低，配置和管理相对简单，无须大规模基础设施升级。

• 成本低，硬件和软件升级成本较低，甚至不需要额外投资。

• 用户需求驱动，能够迅速满足用户或市场的需求，提供明显的短期效益。

• 快速部署，通过翻译器，IPv6单栈设备可以迅速与现有的IPv4网络互联互通，加快了IPv6的普及速度。

• 安全性强，由于“木桶效应”，双栈系统的总体安全性是IPv4或IPv6中安全性差的那一个，IPv6单栈系统可以充分利用IPv6增强的安全性。

5 新的挑战

虽然当今互联网基本上保持了TCP/IP的“分布式”“无连接”“尽力而为”“端对端”和“开放性”的技术特征，但“去分布式”“去无连接”“去尽力而为”和“去端对端”的异化也带来了新的挑战[14]。

5.1 网络韧性

在当今全球化和数字化的世界中，网络基础设施的韧性至关重要。网络韧性指的是系统在面对干扰、故障或攻击时仍能保持正常运行的能力。然而，地缘政治和自然灾害对网络韧性提出了严峻的挑战。

地缘政治紧张局势可能导致网络攻击、信息封锁和互联网服务中断。例如，国家之间的网络战争可能通过DDoS、恶意软件等手段破坏对方的关键基础设施。不同国家和地区的互联网管理政策和法规差异，可能导致跨境数据传输受阻，影响全球网络的连通性和韧性。某些国家可能实施严格的网络封锁或内容过滤政策，削弱了网络的整体韧性。地缘政治因素也可能影响关键资源的分配和使用，如海底光纤电缆的铺设和维护。这些基础设施的中断或破坏将直接影响网络的韧性。

台风、飓风、暴雨等自然灾害可能导致电力中断、设备损坏和通信线路故障，影响网络的正常运行。地震、海啸等地质活动可能破坏关键的通信基础设施，导致大规模的网络中断。长期的气候变化可能增加极端天气事件的频率和强度，进一步考验网络基础设施的韧性。

为了应对上述挑战，恢复和加强分布式网络结构是关键。分布式网络结构具有更高的冗余性、灵活性和弹性，能够在局部故障或攻击发生时保持整体网络的正常运行。一般来讲，韧性网络具有以下特征：

1）多重路径

分布式网络通过多条路径传输数据，确保即使某些路径受阻或中断，数据仍能通过其他路径传递到目的地。这种设计可以有效应对自然灾害和地缘政治因素导致的局部网络故障。

2）去中心化

分布式网络没有单一的控制中心，数据存储和处理分散在多个节点上。这种结构减少了单点故障的风险，提高了系统的整体韧性。

3）动态调整

分布式网络能够根据实时情况动态调整数据传输路径和负载分配，确保在面对突发事件时能够迅速响应并恢复正常运行。

4）本地化服务

通过增加本地化的数据中心和服务节点，减少对远程资源的依赖，提高网络在局部灾害或冲突发生时的自愈能力。

5） 跨国合作

国际社会需要加强合作，共同制定和实施全球性的网络安全和韧性标准，确保关键基础设施的互联互通和稳定运行。

5.2 人工智能

近年来，以ChatGPT为代表的生成式人工智能对互联网和TCP/IP体系结构提出了新的挑战[23-24]。

1）高性能网络的挑战

AI模型通常需要处理大量数据，尤其是在训练阶段。高带宽可以确保数据快速传输，从而提升训练效率。低延时对于实时应用（如对话式AI）至关重要；高延时会影响用户体验和系统响应速度；网络抖动会导致数据传输的不稳定，影响模型训练和推理的一致性；高丢包率会导致数据传输的不完整，影响模型的准确性和性能。以英伟达为代表的图形处理器（GPU）集群为例，NVLink被用于Nvidia GPU之间的通信，因为它提供了远超传统高速串行计算机扩展总线标准（PCIe）接口的带宽和更低的延时，对于需要大规模并行计算的AI任务（如深度学习训练）至关重要。Fiber Channel主要用于数据中心内部的存储网络，因为它提供了极低延时和高带宽，确保数据传输的高效性和稳定性，对于需要快速访问大量数据的AI应用尤为重要。TCP/IP被广泛用于数据中心之间的通信，主要原因在于其标准化和广泛支持。它可以在不同硬件和软件平台上运行，适合大规模分布式系统。目前的技术在近期无法使TCP/IP一统天下。

2）分裂化的挑战

随着国际关系的复杂化，以及各国对数据主权、隐私保护以及网络安全的重视程度的提高，互联网的分裂问题日益严重。具体到人工智能的服务领域，许多公司开始根据源IP地址决定是否提供服务，这种做法在未来可能会产生深远的影响。例如，从2024年7月9日起，OpenAI严格限制其API服务的IP地址范围。这意味着只有特定国家或地区的用户才能访问和使用OpenAI提供的人工智能服务。从长远看，这可能会导致这些地区在技术创新方面有所落后，全球范围内的研究和开发合作将变得更加困难，最终影响技术进步的速度和质量。

3）集中化的挑战

人工智能，特别是大型基础模型（如语言模型、图像识别模型等）的训练，需要大量的计算资源（如GPU）和能源。这些资源的成本非常高昂，只有少数超大公司才能负担得起，从而导致了人工智能领域的中心化趋势。其长远影响在于：大公司对于技术的垄断阻碍创新；超大公司控制了大量用户数据，可能导致数据隐私问题加剧；中心化的系统更容易成为黑客攻击的目标，一旦被攻破，后果将非常严重等；中心化趋势可能进一步加大数字鸿沟，使得资源和技术更集中在发达国家和地区。

4）可信性的挑战

大语言模型在处理自然语言任务时，有时会生成看似合理但实际上并不准确或可信的回答。这种现象被称为“幻觉”。与此同时，互联网用户还面临来自黑客攻击和劫持的威胁，这使得区分大语言模型生成的幻觉和恶意行为变得更加复杂。其长远影响在于：如果用户无法区分大语言模型生成的幻觉和恶意行为，则可能会对人工智能服务失去信任，影响其广泛应用；企业提供的人工智能服务如果频繁出现幻觉或被黑客攻击，可能会导致品牌声誉受损；黑客攻击和劫持可能导致用户数据泄露，造成严重的隐私问题，大语言模型生成的幻觉可能误导用户做出错误决策，甚至引发安全事件。因此，需要通过网络对联网实体（不管是真实的人类，物联网设备和“机器人”）通过真实的网络地址建立更强的认证和信任机制。

6 结束语

在本文中，我们回顾了TCP/IP的历史演进、TCP/IP的核心思想以及各技术模块的发展过程，通过深入分析，我们得出以下结论：

在当前快速变化的技术环境中，TCP/IP作为互联网的基石，其核心思想依然具有重要意义。未来的发展应当坚持“守正创新”的原则：一方面，保持TCP/IP“分布式”“无连接”“尽力而为”“端对端”和“开放性”的基本技术特征；另一方面，大胆创新，适应人工智能等新技术带来的需求。通过这种方式，我们可以在确保网络基础设施稳定性的同时，推动技术进步和创新。

随着IPv4地址资源的枯竭和互联网应用需求的不断增长，IPv6作为下一代互联网协议，为技术创新提供了坚实的基础。IPv6不仅解决了地址空间不足的问题，还能够为移动互联网、物联网和人工智能提供不受限制的创新空间。

参考文献

[1] “863”计划通信技术主题总体技术研究组. BIP-ISDN概念研究报告[R]. 1995

[2] LEINER B, CERF V, CLARK ,et al. A brief history of the Internet

[EB/OL]. (2022-02-22) [2024-10-13]. https://www.internethalloffame.org/brief-history-internet
[3] 李星, 包丛笑. 五十年互联网技术创新发展的回顾与思考 [J]. 汕头大学学报(人文社会科学版), 2019, 35 (12): 5-12
[4] RUSSELL A L. OSI: the Internet that wasn't [EB/OL]. (2013-07-29) [2024-10-04]. https://spectrum. ieee. org/osi-the-internet-that-wasnt
[5] CLARK D. Designing an Internet- information policy [M]. Cambridge: The MIT Press, 2018
[6] U. 布莱克. 计算机网络 - 协议、标准与接口 [M]. 北京: 人民邮电出版社, 1990
[7] MigiTing. ISDN与Internet [M]. 北京: 机械工业出版社, 1997
[8] 邢秦中. ATM通信网 [M]. 北京:人民邮电出版社, 1998
[9] SCHHATT, STAN. Linking LANs - a micro manager's guide [M]. PA: TAB BOOKS, 1991
[10] 和永明, 陈地虎. OSI协议和计算机网 [M]. 北京:电子工业出版社, 1994
[11] HALEPLIDIS E, PENTIKOUSIS K, DENAZIS S, et al. Software-defined networking (SDN): layers and architecture terminology [S]: RFC7426. 2015
[12] IETF. Domain name system [EB/OL]. [2024-10-10]. https://www.ietf.org/technologies/dns/
[13] MANDERSON T, VEGODA L, KENT S. Resource public key infrastructure (RPKI) objects Issued by IANA RFC6491 [EB/OL]. [2024-10-06]. https://datatracker.ietf.org/doc/rfc6491/
[14] 晃通, 宫永直树, 岩田淳. 图解OpenFlow [M]. 北京: 人民邮电出版社, 2016
[15] BUSI L, ALLAN D. Operations, administration, and maintenance framework for MPLS-based transport networks RFC6371 [EB/OL].[2024-10-03]. https://datatracker.ietf.org/doc/rfc6371/
[16] FILSFILS C, LEDDY J, VOYER D, et al. Segment routing over IPv6 (SRv6) network programming RFC8986 [EB/OL].[2024-10-03]. https://datatracker.ietf.org/doc/rfc8986/
[17] BERNET Y, FORD P, YAVATKAR Y, et al. A framework for integrated services operation over diffserv networks RFC2998 [EB/OL].[2024-10-03]. https://datatracker.ietf.org/doc/rfc6371/
[18] CARPENTER B. Internet Transparency RFC2775 [EB/OL]. [2024-10-03]. https://datatracker.ietf.org/doc/rfc2775/
[19] IETF. Internet standards process [EB/OL]. [2024-10-03]. https://www.ietf.org/process/process/
[20] REKHTER Y, LI T. A border gateway protocol 4 (BGP-4) RFC1771 [EB/OL]. [2024-10-05]. https://datatracker.ietf.org/doc/rfc1771/
[21] FIELDING R, NOTTINGHAM M, RESCHKE J. HTTP semantics RFC9110 [EB/OL]. [2024-10-05]. https://datatracker.ietf.org/doc/rfc9110/
[22] 李星, 包丛笑. 新一代IPv6过渡技术——IPv6单栈和IPv4即服务 [M]. 北京: 科学出版社, 2024
[23] WILLIAM J, DARK VINTON G, KLEINWACHTER C W. Internet fragmentation: an overview [EB/OL]. [2024-10-10]. https://www3. weforum. org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf 2016
[24] ISOC. Artificial intelligence – Internet society [EB/OL]. [2024-10-10]. https://www.internetsociety.org/issues/past-categories/ai/

作 者 简 介

李星，清华大学教授、CERNET网络中心副主任；主要研究领域为计算机网络体系结构、通信技术等；作为负责人完成多项国家级项目，获中国科技进步一等奖、中国科技发明二等奖、通信学会科学技术奖一等奖等，入选国际互联网名人堂，获互联网波斯塔尔奖；作为联合作者撰写11个IETF RFC，发表学术论文300余篇，获国家发明专利40余项。

包丛笑，清华大学副教授；主要研究领域为计算机网络体系结构、IPv6过渡技术和网络测量；作为技术骨干完成多项国家级项目，获中国通信学会科学技术奖一等奖；作为联合作者撰写9个IETF RFC，发表学术论文30余篇，获国家发明专利40余项。