



专题：数据网与算力网络

互联网的设计理念与网络 5.0 技术

蒋林涛, 聂秀英, 张杰

(中国信息通信研究院, 北京 100191)

摘要: 互联网发展了 50 年, 其设计理念从未改变, 业务网完全采用 OTT 方式, IP 网至今还是“尽力而为”, 制约了互联网的发展。要不断满足社会发展的需要, 互联网设计理念需要变革, 可行的方向是由“以应用为中心”变为“以网络为中心”。网络 5.0 是第 5 代数据网, 与第 4 代数据网 (IP 网) 相比, 保留 IP 网的全部优点, 填补了 IP 网在网络性能和能力上的不足, 性能和能力上有质的进步。具体讨论了网络 5.0 在可扩展性、内生可信安全、确定性等多方面的关键技术。

关键词: 数据网; 网络 5.0; 互联网

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2021232

Internet design concepts and network 5.0 technologies

JIANG Lintao, NIE Xiuying, ZHANG Jie

China Academy of Information and Communications Technology, Beijing 100191, China

Abstract: The internet has been developed for more than 50 years, but its design concept has never changed. The business network is completely OTT, IP network is still “best effort”, which restricts the development of the internet. In order to continuously meet the needs of social development, the internet design idea needs to be changed, and the feasible direction is to be from “application-centered” to the “network-centered”. Network 5.0 is the fifth generation of data network, compared with the fourth generation of data network (IP network), it retains all the advantages of IP network, filling the absence of IP network in network performance and ability, with qualitative progress in performance and ability. The key technical issues on scalability, endogenous credible security, certainty and more aspects of network 5.0 were specifically discussed.

Key words: data network, network 5.0, internet

1 引言

互联网促进了社会的数字化和信息化, 在国计民生中起到越来越重要的作用。网络空间主权已经是国家主权的重要组成部分, 受到各国

政府的高度关注, 政府采取各种技术设施实现对网络空间主权的治理。为了满足业务发展的需要, 50 年来 IP 网技术补丁不断, 但设计理念和核心技术不变, 已经呈现出越来越“力不从心”的态势。

收稿日期: 2021-09-10; 修回日期: 2021-10-15

基金项目: 国家重点研发计划项目 (No.2018YFB1800100)

Foundation Item: The National Key Research and Development Program of China (No.2018YFB1800100)

2 互联网的发展

互联网由业务网和承载网组成,如图 1 所示。

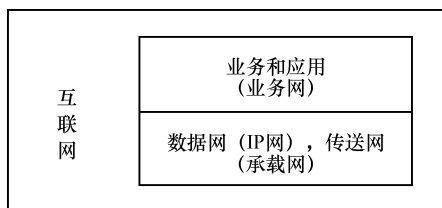


图 1 互联网的组成

业务网是互联网发展最活跃的部分, 50 年来其变化从来没有停止过, 它产生了无数种业务和应用, 是互联网发展的主动力。它的网络部分, 即 IP 网, 核心技术已经 50 年不变, 在技术高速发展的时代, 互联网要发展、要进步、要不断满足社会发展的需要, 是历史的必然。互联网如何发展, 目前这种依赖在网络技术上不断打补丁的办法, 越来越不能满足发展需要, 成为网络发展的瓶颈; 互联网要发展, 必须要有设计理念和核心技术上的突破。

目前的互联网是以应用为中心设计的。互联网的网络部分(即 IP 网)只是提供简单但扩展性好、连接能力强、能“尽力而为”的信息传输能力的网络。在互联网中, IP 网处于从属的地位。在传统互联网中应用可以完全不理会网络(端到端连接和信息传输的基本能力还是需要的)进行独立设计和独立运行(即 OTT (over the top) 模式), 甚至网络的某些能力缺陷也可由端侧解决(如用 TCP 来改进网络传输能力不足的问题)。互联网业务独立和灵活的发展能力, 极大地繁荣了互联网。但是, 以应用为中心的互联网设计理念存在严重隐患, 随着互联网应用范围的急剧扩大, 生活、社会、生产、制造等领域无所不包, 互联网的国家安全和网络主权已经到不能不考虑的时刻了。以应用为中心的互联网设计使得互联网没有边界, 这个问题以前是不考虑的, 甚至是作为一个优点被提出来的, 现在则要考虑了。互联网

由承载网和业务网组成, 传统互联网设计理念是: 以应用为中心, 业务和应用以 OTT 形态设计和运行, 甚至端到端的安全和加密也以 OTT 形态设计和运行的。所谓 OTT 形态即直接跨过 IP 网, 端到端直接工作, 在整个业务网运行过程中, IP 网是完全不知情的, 只是尽力而为地执行连接和传输。由于业务和应用的网站和终端是无边界的, 并且业务和应用是以 OTT 方式运行, 就整体而言, 互联网没有边界, 也无法设置边界。互联网的重要性日益增强, 网络空间的管理问题也变得日益重要。由于互联网的承载网(IP 网)是有边界的, “以网络为中心”可以使得网络空间主权“抓手”得到解决。由“以应用为中心”的互联网改变为“以网络为中心”的互联网, 是互联网设计理念和核心技术的突破。

目前互联网的业务网工作模式是 OTT 模式。OTT 模式除了使网络空间无边界外, 还使得互联网的业务网和承载网彻底解耦, 以致于有“服务质量”要求的业务难以提供, 网络轻载被认为是可行的方法, 但目前 ICT 已经是能源消费大户, 网络轻载不是长远之策, 由于已经有大量互联网业务存在, 这种模式将会继承和保留, 便于过渡和演进。今后互联网的业务网应该是非 OTT 模式, 在这种模式下, 业务网与数据网仍是解耦的, 业务网的设计开发自由度和灵活性与 OTT 模式相同, 增加的业务网和数据网接口, 便于业务网设计开发可以充分利用数据网的能力, 从而大大降低业务网开发的复杂度、提高业务应用的用户体验。

互联网的承载网由传送网和数据网组成。传送网解决点到点的通信问题, 是数据网网元间连接的基础, 传送网和互联网业务网没有直接接口。与互联网的业务网有直接关系的是数据网, 目前的数据网是 IP 网, IP 网存在的问题业界已经公认, 由于没有好的解决办法, 目前以不断打补丁的形式延续它的使用寿命。IP 网的核心技术, 由于商业、利益问题以及没有找到突破口而不能做出改



变。IP 网在数据网的分代中是第 4 代数据网（前 3 代数据网分别为频分复用数据网、时分复用数据网和面向连接的分组数据网），第 5 代数据网也就是网络 5.0，是在 IP 网的基础上继承和发展形成的。网络 5.0 的内生能力可以通过管理接口（南北向，API 形态）或控制信令（东西向，随路信令形态）向应用层提供（开放）能力或反馈响应信息。这些内生能力是：网络主导下的内生可信和安全能力、网络资源的内生感知和管控能力、网络内生的确定性（包括网络性能的确定性、路由确定性、时延确定性和用户体验确定性等）、广义可扩展性、泛在移动性和高速、大带宽能力等。

由于设计理念发生重大改变，网络从“尽力而为，诸事不管”到“以网络为中心”，网络技术发生重大改变是必然的。对于应用和业务，从原理上讲，已有的业务和应用可以不作改动正常使用，但是这些业务和应用无法用到网络 5.0 提供的能力，因此，业务和应用改动是必要的。好在目前业务和应用的改动已非难事，通过 App 或相关软件的升级即可实现。IPv6 的升级改造提供了一个极好的范例。

3 网络 5.0 的设计理念

网络 5.0 的设计理念是由互联网“以应用为中心”向互联网“以网络为中心”发展。具体为以下 3 个方面。

- 网络 5.0 设计理念保持互联网的可扩展性。互联网要保持强大的可扩展性，网络（数据网）可连接的用户数至少是目前互联网的 2~3 个数量级。这个设计理念主要来自继承。实际上目前互联网最大的特点是扩展性极好，它主要有三大特点：以自治域为核心的分散型网络结构，自治域相互独立，自治域的扩展不受限制也互不影响；采用不面向连接的分组数据网技术，无全局状态，无全局集中管理点；全网采用同

一技术（同一种协议体系），相同的体系结构和相同的数据报结构，全网的端设备之间可以实现互联互通。

- 网络 5.0 设计保持业务网与承载网解耦，但增加资源关联和控制适配。业务网和数据网要做到既解耦，又有必要的接口，这是传统互联网所不具备的，但对今后发展的业务网是不可缺失的能力。业务网和承载网（数据网）主体是解耦的，但不能太彻底，业务网不能完全是 OTT 形态，以致有“服务质量”要求和对承载网由性能和能力支持要求的业务无法提供，或只能简单要求网络以轻载来保证“服务质量”。有的互联网业务网对网络能力是有要求的，特别是对网络资源、网络性能的确定性可以有直接的要求，以此提高业务网的质量和和应用服务范围。
- 传统互联网设计是网络（IP 网）能力缺位和业务网能力越位，设计者期望由业务网能力越位部分来弥补承载网（IP 网）的缺位部分，由此来维持信息系统的正常运行。但是 IP 网能力缺位，实际无法由业务网能力的越位来弥补。一个典型的例子是网络（IP 网）在资源能力缺位，通过业务网能力越位（调整 TCP 窗口）来弥补，实践表明仅在早期可行。网络（IP 网）在可信、安全能力上缺位问题就更大。

网络 5.0 的设计是网络能力和业务网能力都不缺位也不越位，各自把自己的事情做好。因此网络 5.0 的设计原则是继承和保留 IP 网的优点，补足 IP 网能力缺位的部分，改变数据网技术 50 年不变的窘境，使数据网技术取得本质上的进步。

4 网络 5.0 的关键技术

4.1 网络的可信安全

互联网的安全分为两大部分，一部分是网络安全，另一部分为信息安全，本文讨论的是网络

安全。网络安全又包括两部分，一部分是用户信息在通过网络时，网络能够保证用户信息的完整性，其中包括用户可溯源、信息不可截获、篡改，保证用户信息除网络的自然损伤（误码等）外，不能做任何改动；另一部分是，网络中的网元不受攻击，特别是网络中的重要网元（包括业务网的管理和控制面的重要网元）不受攻击，对 DDoS 具有抗攻击能力。

网络 5.0 可信安全的设计脉络是，以可信（信用）为基础，在可信环境的基础上，解决网络安全。网络 5.0 有经营主体的数据网部分（网络的核心和主体部分）是可信的，内设可信锚点，全网以可信锚点为核心建立全网设备间的可信关系。网络中运行的网元、设备、终端等均为网络可信设备。具体做法是，在网元、设备、终端中设可信标识载体，用网络的可信锚点来分配可信标识，并写入可信标识载体。设备或终端入网，需由可信锚点来验证可信标识，若通过即为网络可信设备，以此建立以网络为中心的可信体系。为了满足网络的可扩展性，可信体系为分散架构，分散自治构成可信自治域。不同的可信自治域间的可信关系由域间信用交互体系来完成，可以集中式、分布式或采用无中心的信用交互体系。在网络信任体系建立后，再实现网络安全。信任域内的网络安全分 3 个步骤。

- 网络可信区的建立，有经营主体的数据网部分（网络的核心和主体部分）是网络的可信区，即封闭区，封闭区是用户不可直达的区域，用户无法了解，也无法直接攻击。可信区中的管理面、控制面用户不可达，数据面用户数据可以穿越，无法落地。
- 网络可信区的边缘有可信边缘设备，可信边缘设备是建立在可信网元技术的基础上的，经论证的可信用户可以与可信设备连接，并在网络可信锚点主导下，建立安全连接，安全强度可分类、分级，从而可在

网络可信锚点的主导下，实现业务网设备、终端等相互间的安全连接。建立基于可信的网络安全体系，在数据网上实现。

- 网络可信区为封闭区，封闭区是用户不可直达的，用户无法直接攻击可信区内的网元设备，业务网设备、终端等相互间的安全连接保证了用户信息传输的安全，也保证了用户设备、终端被控，造成数据会聚。从而保证不能构成 DDoS 攻击流，在很大程度上保证核心网元设备的安全。由于网络边缘设备是用户可直达的，这是用户可攻击的设备，由于接入用户是可信用户，攻击是便于溯源的，由于终端和接入边缘设备是建立安全连接的，用户信息的完整性是可以保证的，所有很难形成聚集类攻击，加上接入边缘设备是按可信设备来设计的，这样的网络安全性是可以得到保证的。

4.2 网络的确定性

传统互联网的设计者由于没有想到互联网能发展到如此规模，也没有想到互联网在信息社会的作用如此巨大。传统互联网是没有确定性的设计的。确定性是一个网络极为重要的特性，是网络可规划、可适配、可管控和可绿色发展的基础，是能够满足用户体验的技术基础。随着互联网的发展从生活走向生产、走向社会的方方面面，确定性越来越重要。确定性的涉及面非常广，目前大部分研究集中在时间的确定性上，其实时间确定性是确定性问题上的一项，而且实际上是比较好解决的。在数据网中确定性有：时间的确定性（包括时延的确定性和时延抖动的确定性）、路径的确定性、网络资源的确定性、网络性能的确定性、网络用户体验的确定性等。本文只讨论时间的确定性、路径的确定性和资源的确定性。

时间确定性分为时延的确定性和时延抖动的确定性。发包到收包之间的时间差为时延，对于时延的确定性通常用最大时延来定义，在现有的



网络中,这个指标是很重要的,特别是对实时业务,如视频播放业务、电话业务、游戏、实时交易等,它们对最大时延是敏感的,业务能否开展有明确且具体的指标。时延抖动是在相同路径下,不同数据包间到达的时延差。由于讨论时间确定性的文章很多,这里不再赘述,唯一需要提及的是在大网环境下的时间确定性和在小网环境下的时间确定性技术差距太大,在小网环境下可用的技术,在大网往往不能用。网络 5.0 是研究大网技术的,它的连接数是目前互联网的 2~3 个数量级,所以时间确定性要分级、分类来讨论,采用的技术路线也会是多样的。

路径(由)的确定性在需要资源保证的业务和应用中永远是重要的。互联网在这方面也作了很大的努力,这些工作都是在 IP 网上进行的。最早是 RSVP,这是建立在软连接基础上的路由确定性技术,通过定时维护路由节点中的状态,保持软连接及该连接所需的资源,由于其过于繁杂、可扩展性太差而没有被使用。其次是 MPLS,在一个不面向连接的 IP 网中,建立面向连接的隧道,面向连接一定存在 N 平方问题,其扩展性必然成问题,因此 MPLS 只能是局部技术,不可能成为大网的确定性路由技术。目前热门的是分段路由(segment routing, SR)技术,其要解决的问题也是确定性路由问题,SR 技术比 MPLS 技术好一些,它是建立在不面向连接的网络基础之上的,技术思路非常简单,在数据包的报头中,将沿途要经过的网络节点地址全数列出,但它有着非常严重的缺点。由于要知道沿途的全部节点的具体地址,必须要有一个能够了解网络全部细节的设备,目前一般这个设备是 SDN 控制器。SDN 控制器的管理范围是 SR 技术的可达范围,所以只能是一种局部技术,不能用于全局。合理的解决办法是网络内生的确定性路由。

资源的确定性与业务分类有相关性,网络传输资源可以分为 4 种类别:第一类是资源完全保

证类(类似 ATM 中的 CBR 类),这类业务的资源是完全保证的,不用的资源是闲置的,他人不能使用;第二类是部分资源保证类,它主要依据标记,作标记部分网络资源是确保的,不作标记的部分信息所需的网络资源是不确保的,网络资源充足即传,反之这部分信息就被丢弃(类似 ATM 中的 ABR 类);第三类是可变速率类,这是针对实时业务的,一般来说实时业务是连续和稳态的,尽管速率可变,一段时间的平均数码率是稳定的,只要保证平均数码率是确定的,即可保证业务的良好用户体验,当然会引入适度的时延(类似 ATM 中的 VBR 类),音视频业务是合适的;第四类是提供“尽力而为”传输能力的业务,突发性很强、无法预测的数据类业务对时延不太敏感,可以使用这一类业务的传输能力(类似 ATM 中的 BEF 类)。业务分类,不同业务可以获得它所需要的网络传输资源,有效地提高网络的传输效率,最大限度满足用户对网络传输资源确定性的要求。

4.3 网络资源感知、管理和控制

网络内生的资源感知和管控涉及 3 个方面的问题。其一是网络资源,主要是节点传输资源和能力的感知,网络资源感知(本文主要谈的是资源供给方的感知)是后随网络资源管控的基础,网络资源不能准确地感知是无法实现对网络资源的管控的。由于要对全网所有节点的全部资源实现完整的感知,且要实时和精准,其难度是很大的。对目前的实现能力而言,对于单一节点内资源感知是不困难的,大部分网络节点均有这个能力。但是要对全网所有节点的全部资源实现完整的感知较为困难。首先是全网资源感知的方式,是分散式、分布式还是集中式。因为要实时和精准的资源感知,集中式显然是不行的,全网节点到集中资源感知节点的通信量不可估量(与采样密度有关);分布式同样也不行,原因和集中式相同,全网节点到分布式资源感知节点的通信量同样不可估量(与采样密度有关);要实时和精准的

资源感知只能采用分散式架构,即节点“各自为政”,资源分散感知。可知网络资源的全程感知是一个极为困难的问题,需要分散式、分布式和集中式协同配合使用,需要极为巧妙的设计才有可能得到解决,当然也仅可能是一个次优解。

资源管理一般包括两个方面的问题,一个是配置管理,即根据实际需求来配置合适的资源,以求获得资源的良好效益比;另一个是性能管理,了解已配置的网络资源可获得的性能,这将与用户体验有直接的关联)。由于网络的资源感知是一个极其困难的事,需要分散式、分布式和集中式协同配合使用才有可能完成。对管理而言,由于网络规模过大,集中式显然不行,集中设备无论能力多强,都无法实现,如果采样过多、过密,网络也承受不了。分布式实际上是集中式的一种变态,集中式存在的问题它都有,因此也不可用。可用的是分散自治、集中互通的模型,从技术上可以实现,并具有很好的可扩展性。网络的资源管理是通过管理面,由网管来实现。对于所有网络,管理面都是内生的,网络资源管理都是网络的内生技术。

网络资源的可控制是真正的目的。无论是网络资源感知,还是网络资源的管理,其真正的目的是期望网络能够根据用户的要求提供资源。要使用户获得所需要的资源,网络又无须用轻载的方式,以提供过渡的资源来保证,这需要通过网络资源控制实现。从网络资源的角度来看,有网络资源的供给方和网络资源使用方两个方面,两者以某种形态匹配,网络资源消耗和用户体验将会是最佳的。对于面向连接的网络,无论是基于 TDM 技术,还是基于分组技术,都可以做到这一点。只要在建立连接的过程中将所需资源协商好,并在通信的全程保持资源的供给,通信完成网络资源收回,这是一个简单、有效和完美的过程。但是只能用于面向连接的工作方式,它的致命缺点是存在 N 平方问题,网络的可扩展性太差,对

一个像互联网要求的数据网这样的大网,面向连接的工作方式局部可以、全局无用。网络要有强的可扩展性,必须采用不面向连接的工作方式,不面向连接不是不连接,而是用户之间通信不需要事先建立连接,用户在线即存在连接,随时可以通信,用户间通信无须建立连接,也无须为连接保持各种状态。理论上讲,采用不面向连接的网络,可扩展性是无限的,IP 网的成功也证明了这一点。采用不面向连接的网络可扩展性极好,又为连接无须保留任何状态,进一步提升了网络的可扩展性。但是确定性资源控制极难,IP 网至今还是一个“尽力而为”提供传输能力的网络。信息技术的日益发展,“尽力而为”提供传输能力的网络已经越来越不能满足需要,致命的问题是效率低、能耗高、非绿色而且无法保证用户所需的确定性。目前的难题是,要在采用不面向连接工作方式的网络上,实现确定性资源的供给,实在是一件困难的事情。这就是网络 5.0 面临的问题,仅凭管理面是难以实现的,必须结合控制面才能实现。提到控制面目前是有误区的,经常可以看到“数据面和控制面分离”,特别是 SDN 技术盛行后,这种现象就更明显了。其实,目前的 IP 网,控制面的主要任务,一个是邻居发现和动态路由,一个探测网络性能和能力的随路信令(如 ping)等,SDN 控制器将邻居发现和动态路由接管过去,传统 IP 网的网络节点(路由器)路由是通过控制面的信息交换由各节点独立自主生成路由转发表;在 SDN 环境下,节点路由生成的功能被 SDN 的控制器接管,SDN 控制器在它管辖的范围内,计算并生成路由和所管辖节点的全部路由转发表,以配置的方式下发到相应节点,特别要注意的是,网络路由的生成已经从控制面转移到管理面去实现了。SDN 控制器虽然叫“控制器”,但实际地位是完成管理面网管的部分功能——配置管理功能。共路信令可以分离(IP 网中基本不用),随路信令的控制面是无法和数据转发面分离



的。前文已经提到,控制面、管理面和数据面是从逻辑意义上来定义的,与实际上所在的物理设备没有必然关系,3个平面可以在同一个物理设备中,也可以是分离的,但数据面和控制面分离实际上是很难的,只有以共路信令为其唯一控制信令时分离可以实现,如果还有随路信令存在,则无法分离。很遗憾的是,对通信资源的控制,随路信令将会大量存在。所以,在网络总体设计时,控制、数据分离是一种误导。

5 结束语

互联网促进了社会的数字化和信息化,在国计民生中起着越来越大的作用,但互联网所存在的问题也日益显现,已经不是简单地打补丁就能解决的。到目前为止,互联网的三大设计思想是无法颠覆的:以自治域为核心的分散型网络结构,自治域相互独立;采用不面向连接的分组数据网技术,无全局状态,无全局集中管理点;全网采用同一技术(同一种协议体系),相同的体系结构和相同的数据报结构,全网的端设备之间可以实现互联互通。但是,由“以应用为核心”的互联网转向“以网络为中心”的互联网,将是互联网的发展方向。

参考文献:

- [1] 蒋林涛. 数据网的现状及发展方向[J]. 电信科学, 2019, 35(8): 2-15.
JIANG L T. Current situation and development trend of data network[J]. Telecommunications Science, 2019, 35(8): 2-15.
- [2] 蒋林涛. 从云网融合到 ICT 基础设施[J]. 信息通信技术, 2019, 13(2): 4-6.

JIANG L T. From cloud-network convergence to ICT infrastructure[J]. Information and Communications Technologies, 2019, 13(2): 4-6.

- [3] 江伟玉, 刘冰洋, 王闯. 内生安全网络架构[J]. 电信科学, 2019, 35(9): 20-28.

JIANG W Y, LIU B Y, WANG C. Network architecture with intrinsic security[J]. Telecommunications Science, 2019, 35(9): 20-28.

- [4] 强鹏, 刘冰洋, 于德雷, 等. 大规模确定性网络转发技术[J]. 电信科学, 2019, 35(9): 12-19.

QIANG L, LIU B Y, YU D L, et al. Large-scale deterministic network forwarding technology[J]. Telecommunications Science, 2019, 35(9): 12-19.

[作者简介]



蒋林涛 (1946-), 男, 中国信息通信研究院科学技术委员会主任, 长期从事多媒体、数据通信、互联网等方面的研究和开发工作。



聂秀英 (1965-), 女, 中国信息通信研究院教授级高级工程师, 主要研究方向为数据通信、多媒体通信、互联网等领域研究和标准制定。



张杰 (1971-), 女, 中国信息通信研究院高级工程师, 主要研究方向为未来网络、网络 5.0 等。