**引用格式**:王宝生,赵锋. 网络发展趋势:从普适通用到场景专用的网络定制[J]. 信息对抗技术,2023, 2(4/5):113-122. [WANG Baosheng, ZHAO Feng. Computer networking trends: from generalizing to scenario specific customizing[J]. Information Countermeasure Technology, 2023, 2(4/5):113-122. (in Chinese)]

# 网络发展趋势:从普适通用到场景专用的网络定制

王宝生,赵 锋*

(国防科技大学计算机学院,湖南长沙 410073)

**摘 要** 传统的 IP 网络体制具有互联互通互操作等优点,得到了广泛的部署应用。然而,随着许多领域的用户对网络的可管可控性、安全性、服务质量、移动性、生存性、确定性、灵活性等诸方面要求的不断增长,传统的 IP 网络体制越来越难以满足需求。通过对领域网络差异化需求以及差异化特点的分析,结合新型网络、网络软件化等技术的发展积累,可以认为,基于领域网络特点进行网络定制将成为未来领域网络的重要发展趋势。论述了领域网络定制的必要性和可行性,首次提出了一个领域网络定制模型,即基于多维属性的领域网络定制模型,并从 3 个方面、6 个维度探讨了基于多维属性的领域网络机制化方法,可以为领域网络定制提供参考借鉴和技术支撑。

**关键词** 计算机网络;领域网络;定制模型;网络机制

**中图分类号** TP 393 **文章编号** 2097-163X(2023)04/05-0113-10

**文献标志码** A **DOI** 10.12399/j.issn.2097-163x.2023.04-05.007

# Computer networking trends: from generalizing to scenario specific customizing

WANG Baosheng, ZHAO Feng*

(College of Computer, National University of Defense Technology, Changsha 410073, China)

**Abstract** The traditional IP network has the advantages of interconnection and interoperability, so it has been widely deployed and applied in many fields. However, for domain specific networks, it is increasingly difficult to meet the increasing requirements for network controllability, security, quality of service, mobility, survivability, determinability, flexibility, and so on. Through the analysis of different requirements and characteristics of domain specific networks, and the consideration of the development and accumulation of new network architectures, network softwarization and other technologies, we believe that the network customization based on the characteristics of domain specific networks will become an important development trend in the future. This paper discussed the necessity and feasibility of domain specific network customization, proposed a domain specific network customization model (DSN-CM) based on multi-dimensional attributes of domain specific networks, and discussed the mechanism of domain specific networks based on multi-dimensional attributes from three quadrants and six dimensions, which can be used to conduct the customization for domain

**收稿日期**:2023-07-05 **修回日期**:2023-07-31

**通信作者**:赵锋,E-mail:fengzhao@nudt.edu.cn

**基金项目**:国家重点研发计划项目(2022YFB2901204)

specific networks.

**Keywords** computer network; domain specific network; customization model; network mechanism

## 0 引言

传统的IP网络体制具有互联互通互操作等优点,为国际互联网的蓬勃发展奠定了坚实的基础,在全球政治、经济、军事、科技、文化、教育等各领域的发展中发挥了举足轻重的作用。国际互联网的示范效应、IP网络体制的巨大成功以及IP网络产业链的丰富生态深刻影响了领域网络的发展建设理念。“拿来主义”一度深入人心,IP化一统天下。过去数十年,传统IP网络体制在许多领域得到广泛部署,发挥了重要作用。

然而,近些年来,传统IP网络体制在领域网络的实践表明,尽管其具备互联互通互操作的优点,却难以满足不同领域网络用户对网络可管可控性、安全性、服务质量、移动性、生存性、确定性、灵活性等诸方面的差异化需求,存在许多缺点和不足。未来领域网络采用什么样的体制、机制来满足用户需求是领域网络发展面临的重大挑战性问题。

通过对领域网络差异化需求以及差异化特点的分析,结合学术界和产业界以及国内外、军内外在新型网络体制研究方面的技术积累,可以认为,领域网络定制的序幕已经拉开,基于领域网络特点定制合适的网络机制以满足差异化需求已成为领域网络发展的重要趋势。

本文抽象了领域网络定制过程,提出了基于多维属性的领域网络定制模型,包括原始属性参数化、领域网络机制化、网络机制协议化、协议体系软件化、协议软件实例化、配置运维场景化6个过程。进一步地,针对最核心、最重要的领域网络机制化过程,从3个方面共6个维度探讨了基于多维属性的领域网络机制化方法。

## 1 领域网络发展趋势分析

领域网络,也称领域专用网络(domain specific network),是指在一个特定应用领域面向用户信息交换需求构建的网络。不同领域的网络用户对网络的安全性等诸方面能力需求不同,同时,不同领域的网络在管理特性、网络构成等方面有各自独有的特点。传统的IP网络体制在不同领域网络中的诸多应用问题表明,期望以一种网络体制在诸多网络领域都能满足用户需求几乎是不可能的。领域网络的特殊性,为面向领域网络特点解决网络问题提供了约束限定,使得一些难以在国际互联网中部署的技术和方案可以通过定制的方式应用到领域网络,从而提升领域网络满足用户需求的能力。另外,近20年来的新型网络体系结构及新型协议机制等研究成果为领域网络定制奠定了良好的技术基础,同时,网络全栈可编程、网络功能虚拟化、网络软件化等技术的发展也为领域网络加快部署新型定制网络体制提供了重要支撑。领域网络定制将成为领域网络发展的重要趋势。

### 1.1 领域网络定制化必要性

#### 1.1.1 领域网络差异化需求

不同的领域网络运行环境和应用场景不同,因此,除了一些共性的互联互通互操作要求以及网络管理要求之外,不同的领域网络用户对网络能力往往有着不同的需求和期望,具体体现在以下10个方面:

1)在网络传输能力方面,有的领域网络需要具备大容量、高带宽的数据传输能力,而有的领域网络由于受链路特性的限制,只要求达到一定的交换容量和数据传输速率。

2)在安全防护能力方面,有的领域网络要求高安全性,包括机密性、完整性、访问控制、不可抵赖性等。在机密性方面,支持主机基于内容的信息实体加密或者基于整个网络的大规模加密,能承载绝密或机密等不同密级信息的分发传递,防止向网络和基础设施中未授权实体和进程暴露机密信息,抵御信息和流量分析攻击;在完整性方面,保证所交换信息不被篡改;在访问控制方面,要求设备进行单向或双向认证授权后才能连接和使用网络,并阻止非授权用户的访问,减少攻击面;在不可抵赖性方面,需要的时候能够提供信息源和接收者的证明。

3)在服务质量保障能力方面,有的领域网络要求可预留资源的虚拟专线保障能力,以及针对

不同级别用户、不同类型应用提供差异化的服务质量保障能力，支持基于优先级进行调度和抢占。

4）在确定性方面，有的领域网络需要具有强实时特征，要求端到端传输时延和抖动限制在一定范围，以保证多样化任务信息在规定时间内的收发传送，有效满足各种业务场景所需的网络带宽、时延、丢包率、服务等方面的约束，保证信息的时效性，有效支持各种关键业务的顺畅运行，实现信息价值最大化。

5）在移动性方面，有的领域网络要求支持用户终端和子网随遇接入，切换接入时可快速恢复原有连接和会话，支持非受阻的移动性和横向及纵向的无中断连通性。

6）在多宿主方面，有的领域网络要求支持多宿主、多手段接入，只要有一条链路可用，接入设备都可使用网络，并且在链路故障时，可以自动切换使用其他链路。

7）在运维管理能力方面，有的领域网络要求部署简易性，具备良好的自动化配置特性，自动配置相应的硬件或软件参数，网络无需用户手动配置或者只需很少配置就可以实现互联互通。有的领域网络要求具备自动故障管理能力，自动进行问题探测、故障隔离和诊断、问题追溯，执行自我修复操作，以解决网络问题或使网络恢复到期望状态。

8）在网络态势感知能力方面，有的领域网络对网络态势感知的全面性、准确性、实时性有较高要求。

9）在网络弹性方面，有的领域网络要求具备路由自动切换、多路冗余等特性，避免单点失效，保证在运行环境发生变化、级联失效、自然灾害、物理打击、网络攻击等原因导致网络结构发生改变时能提供必要服务，在修复时能快速提供所需服务。

10）在网络动态重构能力方面，有的领域网络要求网络是可扩展和自适应的，能动态支持新协议、新功能，避免网络固定僵化，以满足用户的动态需求。

上述 10 个维度的需求并不是孤立的，一个维度的网络指标会对另一个维度的网络指标产生影响。例如，为了提高安全性，网络可以引入链路加密、报文过滤等安全机制，但往往会加大网络传输延迟，降低网络传输能力。因此，很难期望一个网络同时满足安全防护能力、服务质量保障能力等多维度的高级指标要求。

### 1.1.2　领域网络差异化特性

不同的领域网络具有不同的特性，可以从管理特性和构成特性等维度进行刻画。

#### 1.1.2.1　管理特性维度

1）从开放程度来看，有的领域网络是开放的，不限定用户，可以接入国际互联网；有的领域网络是封闭的，特定用户才能接入，有相对固定的用户群体。

2）从网络规模来看，有的领域网络规模有限，而有的网络规模较为庞大。

3）从网络应用来看，有的领域网络应用相对明确稳定，而有的领域网络应用迭代变化快。

4）从管理权限来看，有的领域网络具有统一的管理权限，而有的领域网络由不同的利益相关方进行分域管理，各域自治。

#### 1.1.2.2　构成特性维度

1）从节点移动性来看，有的领域网络大部分节点是固定的，不移动；有的领域网络大部分节点是移动的。

2）从节点运动规律来看，有的领域网络节点高速有规律运动，而有的领域网络节点存在速度不确定、运动不规律等特征。

3）从节点能量来看，有的领域网络节点具备持续的能量输入；有的领域网络节点能量有限。

4）从链路速率来看，有的领域网络具有多个高速链路，链路速率可达 100 Gbps 以上，而有的领域网络大部分是低速链路，只达到 kbps 或者 Mbps 级别。

5）从链路延迟来看，有的领域网络节点间距离远，链路传输延迟大；有的领域网络节点距离近，传输延迟小。

6）从链路稳定性来看，有的领域网络的链路几乎不受环境影响；有的领域网络的链路受环境影响大，链路的带宽、误码率等随时发生变化。

### 1.1.3　传统 IP 网络体制问题

尽管传统 IP 网络体制具有互联互通互操作等优点，但其难以满足差异化的领域网络用户需求，存在诸多缺点和不足，具体有以下几方面。

1）在可管可控性方面，传统 IP 网络体制存在网络设备接口 IP 地址配置复杂，管理效率低等问题，许多配置得依靠手动进行，难以自动化，访

问控制规则在场景改变后(例如用户移动后)失效。

2) 在服务质量方面,传统 IP 网络体制采用“尽力而为”方式,路由转发时“只知 IP 地址、不知用户、不知应用”,难以实现全程服务质量保障和精细化服务质量控制;报文分组处理采用“人人平等”方法,出现拥塞时,无论报文是否重要都可能被丢弃、导致出现较大延迟,难以为重要用户和关键应用提供服务质量保证。

3) 在安全性方面,由于传统 IP 网络体制从学术研究发展而来,以用户相互信任为前提,“通”为第一原则,安全属于次要因素。虽经 40 多年修补,仍存在大量难以应对的安全问题。例如,身份信任模型先天不足带来各类欺骗攻击;尽力服务模型先天缺陷带来阻塞带宽攻击的威胁;复杂的人工分布式配置容易招致针对配置漏洞的攻击威胁;监视管理维护先天支持不足带来隐藏恶意行为的威胁。

4) 在移动性方面,IP 网络中大多数网络业务使用基于连接的协议 TCP 进行传输。业务会话或者应用的两个端点使用 IP 地址和端口号构成元组形成连接。节点在移动时,往往需要在不同接入点获取新的 IP 地址,而 IP 地址的任何改变都会断开连接,打断会话的持续性,影响应用体验。并且 IP 地址的改变可能会导致原有的网络访问控制等规则失效,级联引发安全等问题。

### 1.2 领域网络定制化可行性

#### 1.2.1 新型网络体制技术积累丰厚

为了解决传统 IP 网络体制的诸多问题,满足不同网络的共性或个性需求,国内外近 20 年来纷纷开展了新型网络体制的研究工作,从体系结构和协议机制上进行创新设计,取得了许多丰硕成果。从后向兼容性角度考虑,这些成果基本上可以分为两大类,即全新网络体制和兼容性网络体制。

代表性的全新网络体制主要包括以下 5 种:

1) 以内容或以信息为中心的网络体制。这类体制以命名数据网络(named data networking, NDN)[1]等为代表,认为网络的中心任务是信息传输或内容分发,因而网络体系结构应当以内容或信息为中心关注点来进行设计,网络体系结构的细腰应从以地址为中心的 IP 协议改为以数据或内容分发为中心的协议。

2) 以支持移动性为首要设计目标的网络体制。这类体制以移动为先(mobility first)[2]等为代表,认为未来互联网将包含大量移动设备,因此必须对网络节点的移动性提供很好的支持。

3) 以安全性为首要设计目标的网络体制。这类体制以 Ethane[3]等为代表,考虑从网络体系结构上对网络安全提供支持,以解决目前互联网面临的大量网络安全问题。

4) 面向服务的网络体制。这类体制以 NEBULA[4]等为代表,主要考虑在云计算的背景下改进现有互联网体系结构,以便更好地为用户提供云服务。

5) 面向精细控制的网络体制。这类体制以军用网络协议(military networking protocol, MNP)[5]为代表。MNP 由美国国防高级计划研究局(DARPA)牵头,其目标是为军用数据网络开发一种新的网络技术来提高安全性,提供动态的网络带宽分配和基于用户角色的流量处理。MNP 要求在网络中具有基于身份认证的系统,并且根据用户身份来为用户分配不同优先级和传输带宽。MNP 基于用户身份标识卡进行强制网络认证、严格网络流量控制与保证,通过网络控制器对网络进行预先规划和细粒度控制,从而建立一个相对独立的、安全可控的保障网络。

兼容性网络体制包括但不限于以下 2 种:

1) 容迟容断的网络(delay-tolerant networks, DTN)[6]体制。这类体制主要面向星际通信、救灾应急、传感器组网等特殊联网和应用环境,通过容忍传输延迟、容忍网络间断连通等网络操作来适应应用环境的特殊性,或满足网络节点休眠、无线电静默等特殊要求。为保持与现有互联网体系结构的兼容性,在 TCP/IP 协议栈传输层之上增加了一个“束”(bundle)层,以支持 DTN“传输—携带—转发”的通信模式。

2) 基于软件定义的网络体制。这类体制以软件定义网络[7]技术为基础,将网络的控制平面与数据平面分离,以开放可编程交换机构成数据平面,以集中式软件控制器构成控制平面。通过采集网络资源和状态信息构建全局统一的视图,并根据用户和应用需求动态编排网络资源,可有效提升园区网、数据中心网以及广域网的资源利用率和自动化运维能力。这类体制中比较有代表性的是 Google 的 B4 网络[8]。

尽管前述全新网络体制由于兼容性等原因,

难以在国际互联网中部署应用，但这些网络体制和新型协议为领域网络在体系结构设计、协议机制定制等方面提供了许多技术选择，为领域网络定制奠定了良好的技术积累。

1.2.2　网络软件化发展使能

随着协议无关报文处理[9]、网络功能虚拟化[10]、网络软件化[11]等技术的不断发展，网络逐渐从管控平面可编程延伸到数据平面可编程，走向全栈可编程。网络软硬件进一步开放解耦，网络软件在网络中将发挥越来越重要的作用。各种网络新功能或者新协议能以软件的方式承载、复用和动态在线部署，可有效减少专用设备的数量和压缩运维管理的开销，支撑实现领域网络定制，加快新型网络体制的推广应用。

另外，随着深度学习和强化学习等人工智能技术的不断发展，可利用人工智能技术对网络流量大数据、网络运行状态时序数据等进行训练学习、判断决策[12]。网络的自动化、智能化技术不断发展，可极大降低网络运维管理人员在分析海量事件和问题警报等方面的困难和负担，提升网络态势感知的实时性、准确性和全面性，以及网络管理控制决策的准确性，提升网络的易用性、好用性，有效降低新型网络体制的管理使用门槛，加快领域定制网络的应用部署。

## 2　基于多维属性的领域网络定制模型

领域网络定制过程本质上是以领域网络设计开发人员为主导，和领域网络用户、建设部署人员、运维管理人员协同沟通，确定最优或者较优网络解决方案的过程。本文将该过程进行建模，首次提出了一个领域网络定制模型，即基于多维属性的领域网络定制模型 DSN-CM（domain specific network customizing model），该模型是目前业界第一个领域网络定制模型。

基于多维属性的领域网络定制模型 DSN-CM 主要由 6 个过程组成：原始属性参数化、领域网络机制化、网络机制协议化、协议体系软件化、协议软件实例化、配置运维场景化，如图 1 所示。

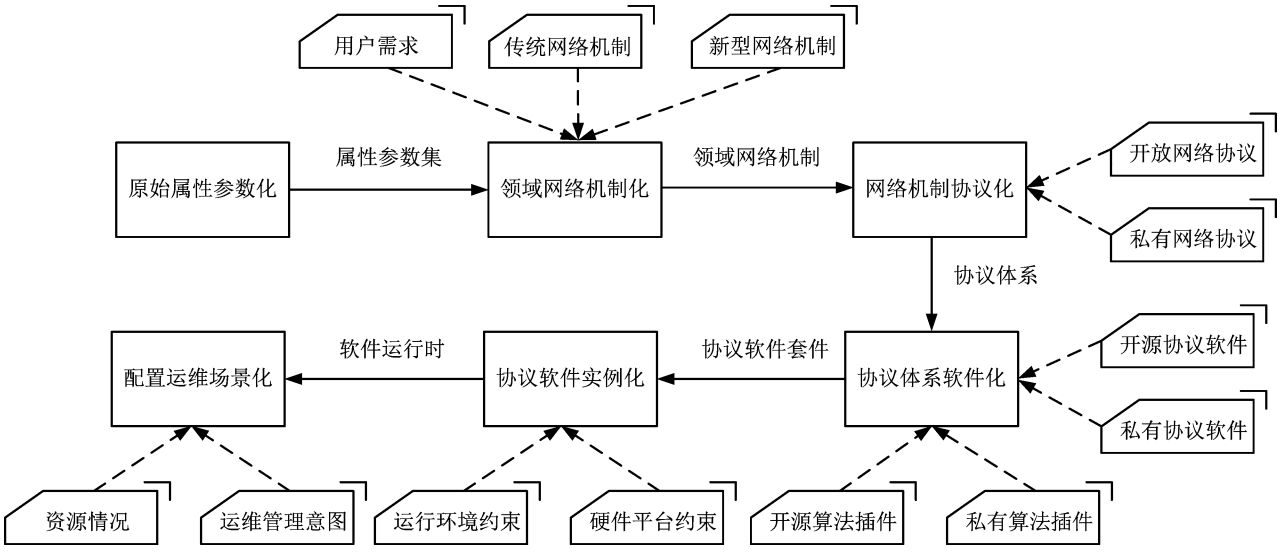


**图 1　领域网络定制模型 DSN-CM**

**Fig. 1　The domain spacific network customizing model DSN-CM**

### 2.1　原始属性参数化

原始属性参数化是抽取领域网络中对领域网络机制化有影响的基本参数并确定其值域的过程。领域网络原始属性是指领域网络不管运行哪一种协议体系都具有的基本属性，即这些属性用于刻画领域网络的基本特征，独立于网络运行的协议。对于全栈可编程网络，可理解为网络尚未加载运行网络协议或协议软件时所具有的属性。

领域网络的原始属性可从网络整体以及组成领域网络的节点、链路等方面建模抽取。当前，DSN-CM 模型包括网络移动性（可用移动节点数目占整个网络节点数的比例进行度量，对于传统固网，网络移动性为 0；对于移动自组织网络，网络移动性为 1；对于有部分节点移动的网络，网络移动性介于 0 和 1 之间）、网络规模、网络可否集中管控、链路带宽、链路延迟、链路丢包率、节点转发延迟等原始属性。不同类型的原

始属性值域可根据需要使用布尔类型、区间范围、概率分布函数或者概率密度函数等进行描述。

### 2.2 领域网络机制化

网络机制化是研究确定网络构造和工作原理的过程。领域网络机制化主要是依据网络原始属性参数化过程产生的属性参数集，结合领域网络用户需求，在一系列传统网络机制和新型网络机制中评估选择比较适合的网络机制，并在已有网络机制不能满足用户需求时，设计开发新的网络机制。

领域网络机制化需要先从顶层着手确定领域网络的基本设计原则，然后在基本设计原则的指导下，以典型网络业务或者潜在网络业务流程为牵引，确定网络的工作原理和基本工作过程，从路由寻址、安全控制、服务质量等多个方面研究确定相应的网络机制。

### 2.3 网络机制协议化

网络机制协议化是研究确定领域网络采用的协议集合（协议体系）的过程。网络机制协议化主要是依据所选择的网络机制，在一系列开放网络协议（如 IETF 组织的 RFC 标准、ISO/IEC 国际标准等）以及私有网络协议中，评估选择比较适合的网络协议，按需进行针对性修改定制，并在某些网络机制没有对应协议时，设计开发相应的领域网络新协议。

在路由寻址方面，若采用传统的面向网络接口的命名与路由，则可在已标准化的域内路由协议 RIP、OSPF、IS-IS 中选择评估，在网络规模较大需要分区域管理时，再纳入边界网关协议 BGP；若采用新型的身份路由机制，则需要基于 IS-IS 进行定制修改或者设计新协议。在安全控制方面，若采用传统的 PKI 机制，则可采用 EAP、TLS 等协议；若采用新型的身份密码 IBE 机制，则可参考借鉴 EAP、TLS 等协议，修改定制或者设计新的认证协议、传输层安全等协议。在服务质量保障方面，可选择传统 MPLS 协议或者针对性设计新的协议来构建隧道或者虚拟专线。

网络机制协议化最终是要建立领域网络正常运行所必须的网络基础协议集合（从上层网络业务可扩展的角度考虑，上层网络业务对应的网络应用层协议，并不纳入网络基础协议集合），即网络基础协议体系。

### 2.4 协议体系软件化

协议体系软件化是研究确定领域网络使用的协议软件集合的过程。协议体系软件化主要是依据领域网络基础协议体系，针对每一个网络协议，在开源协议软件以及私有网络协议软件中，评估选择比较适合的相应协议软件，按需进行裁剪定制，去除不必要的繁杂功能或者增加新功能，并在某些网络协议没有对应的协议软件时，设计开发相应的新协议软件。例如，针对路由寻址，开源的路由套件 FRR 已实现标准的 RIP、OSPF、BGP、IS-IS 等路由协议，可按需裁剪使用。

在协议体系软件化过程中，尽量将网络算法（例如拥塞控制算法、散列算法、加解密算法等）插件化，即解耦协议软件和相关算法，增加软件灵活性，以便在需求或者环境变化时切换为更合适的网络算法。例如，在传输控制协议 TCP 的实现中，Reno、CUBIC 等基于丢包的拥塞控制算法，以及 Vegas、TCP-LP 等以时延为拥塞信号的算法都可以基于动态内核模块的方式进行插件化。

协议体系软件化最终是要针对领域网络中的路由、交换、终端、网管等不同类型的网络节点建立相应的基础协议软件集合。

### 2.5 协议软件实例化

协议软件实例化是开展协议软件代码承载、映射、调度、加载运行的过程。协议体系软件化主要是根据协议软件执行代码以及运行环境约束、结合领域网络管理控制需求与转发交换硬件平台约束，确定协议软件执行代码承载形式（容器或者其他形式），研究建立协议软件执行代码和领域网络节点或节点部件的映射关系，并根据映射关系调度加载协议软件执行代码到相应的网络节点或节点部件上运行。

协议软件实例化是建设网络后开通运行网络以提供网络服务的重要环节，需要针对领域网络中的每一个网络节点，加载运行其对应的基础协议软件集合。依据基础协议软件的特点，可采取随节点操作系统启动或者远程动态加载启动等方式。对于可编程的数据面可能需要加载对应的执行代码，例如，对于 P4 交换芯片，可能需要动态加载 P4 执行码，对于网络处理器，需要加载相应的微码，等等。如果基础协议软件以容器

镜像方式提供，可能需要动态加载运行 1 个或者多个容器。

### 2.6　配置运维场景化

配置运维场景化是结合领域网络具体应用场景设置网络算法和网络参数的过程。配置运维场景化围绕运维管理意图，基于各节点运行的协议软件，结合领域网络的带宽、节点的计算存储资源等情况，优选网络算法、设置合适的协议参数，满足领域网络各项能力要求，尽可能优化网络综合能力水平。

配置运维场景化是达成网络管理人员运维管理意图和网络用户使用意图的重要环节，网络管理人员可根据临时或者规划任务需要，改变用户或者网络业务的优先属性，动态建立或者撤销虚拟专线或者改变专线带宽，针对重要的视频会议等业务动态分配相应的网络资源。网络管理人员也可结合网络环境变化或者流量变化，在 AI 智能辅助下，动态调整网络参数等配置。

## 3　基于多维属性的领域网络机制化方法

网络机制化是领域网络的顶层设计过程，也是领域网络定制化最核心最重要的环节。因此，本文提出基于多维属性的领域网络机制化方法，从 3 个方面共 6 个维度来探讨评估相应的网络机制。

### 3.1　路由寻址

从计算机网络的发展历史来看，报文分组机制是其设计最成功的机制，也是最基础的机制。目前已有的各种新型网络机制的设计也都基于报文分组机制。因此，未来很长一段时间，领域网络仍然是以报文分组为主要信息载体的网络。领域网络信息传输的过程本质上仍然是将报文分组从源向目的转发的过程。报文分组中的源和目的语义（即代表什么实体）是路由寻址机制定制的核心要素。路由信息的生成与维护是路由寻址机制定制的关键要素。

#### 3.1.1　面向接口 VS 面向节点

在传统互联网的网络层命名与路由机制中，IP 地址本质上指定的不是一台计算机，而是计算机的一个网络接口。传统的互联网路由的本质是将报文从一台机器的一个网络接口送到另一台机器的一个网络接口，是一种位置路由。面向网络接口的命名与路由具有路由扩展性好、便于问题排查等优点，但存在不能有效支持移动性和安全性、不能有效支持多宿主、管理配置复杂等缺点。

在新型的面向网络节点的命名与路由机制[13-14]中，网络节点可被赋予一个全局唯一的、独立于拓扑的身份标签。网络节点之间可基于邻居关系建立扁平路由。面向网络节点的命名与路由是一种身份路由，节点移动过程中身份保持不变，可以比较好地保持会话的持续性、已有安全规则的有效性。路由节点不必再配置接口 IP 地址，可以有效避免面向网络接口的命名与路由机制的缺点，但存在网络规模大时路由开销较大等不足之处。

因此，在决策领域网络的命名与路由机制时，可根据领域网络的移动性、网络规模等属性特点，选择相应的命名与路由机制，或者在网络的不同区域应用不同的命名与路由机制，有效发挥不同的命名与路由机制的优点。考虑当前的计算、存储、网络带宽等能力现状，对于移动节点比例大的网络或者有限规模的网络，例如百万节点规模级别以下的网络或网络区域，建议采用面向网络节点的命名与路由机制。

#### 3.1.2　分布路由 VS 集中路由

传统的网络主要采用分布路由机制，各个路由节点之间通过交换链路状态或者距离矢量、路径矢量等信息，计算形成各自的路由表项。分布路由机制具有抗毁性好等优点，但在流量工程支持等方面存在不足之处。

伴随着软件定义网络等技术的发展，一些网络场景使用集中路由机制[15-16]，通过网络控制器获取网络链路状态，构建网络拓扑视图，集中计算路由表项，自动分发到相应的网络节点。集中路由机制具有网络全局视图，便于网络运维管理人员实施高层路由策略，具有较好支持流量工程等优点，但在抗毁性等方面还存在不足。

因此，在决策领域网络的路由机制时，可根据领域网络的移动性等属性特点，结合网络抗毁性等需求，选择相应的路由机制。对于既要求抗毁性高，也要求灵活性好的网络，建议采用集中控制与分布协同相结合的路由方式[17]，区分路由表项优先级，优先选择集中控制分发的路由，没有集中路由时，再回退到分布路由，以有效发挥不同路由机制的优点。

### 3.2 安全控制

#### 3.2.1 公钥设施 VS 身份密码

领域网络的接入认证、不可抵赖性、机密性、完整性机制都离不开密码系统的支持。

传统的密码系统依赖公钥基础设施 PKI，基于证书来实现签名认证和加解密等操作。基于 PKI 的安全机制面临比较复杂的证书管理问题，同时，第三方在线验证过程中的证书交互可能导致敏感信息泄漏和证书中间人攻击等问题。

新兴的基于身份的密码系统 IBS 为新型安全机制的设计提供了支撑[18-19]。RFC 5408 定义了基于身份加密的体系结构[20]，ISO/IEC 14888-3 标准定义了 IBS-1 签名认证方案。IBS 采用身份作为公钥，可以消除复杂的证书管理、敏感信息泄漏和证书中间人攻击等问题。但在 IBS 中，网络实体需要向值得信赖的密钥生成中心提供其公钥以生成私钥，信息的机密性保障有一定的约束限制。

因此，在研究决策领域网络的身份认证、机密性、完整性等机制时，可根据安全性要求以及领域网络的管理属性选择不同的密码系统，或者组合不同的密码系统。例如，对于可集中统一管控的网络，在网络基础设施安全防护方面建议基于 IBS 系统来实现，在内容安全方面可提供 PKI 支持，满足特定用户对特定信息机密性保障的需求。

#### 3.2.2 网络可见 VS 网络隐藏

传统的 IP 网络中，路由设备接口和终端设备接口的 IP 地址都来自同样的数值空间，最长前缀匹配路由方式并不区分报文是送往路由设备还是终端设备。因此，网络设施对终端用户可见。网络设施可见具有方便网络管理、便于故障排查等优点，但存在网络攻击面大、恶意用户可以直接对网络基础设施进行攻击等问题。

网络设施隐藏机制，即核心和边缘分离机制，通过分离终端命名空间和网络设备命名空间、在入口节点通过报文再封装或者访问控制列表等方式[21-22]，将网络基础设施透明化，阻止终端设备对网络基础设施中网络设备的非授权访问，保护路由等设备免遭终端上的恶意软件或者恶意终端的攻击。网络设施隐藏机制提升了网络的安全性，但一定程度上影响了网络管理的便捷性。

是否进行网络设施隐藏，采取什么样的网络设施隐藏机制，一方面依赖于网络设施安全性和管理便捷性之间的平衡选择，另一方面也和路由转发机制的设计相关。对于网络设施安全性要求高的网络，可采用报文再封装的网络设施隐藏机制。

### 3.3 服务质量

#### 3.3.1 应用自决 VS 多维统筹

传统 IP 报文中定义了优先级字段，但网络应用各自指派优先级，导致网络中间节点难以对不同网络节点的不同网络应用做出真正有效的调度决策，服务质量保障所需的核心要素优先级字段相当于虚设。同时，由于传统 IP 网络中缺少使用人员实体、网络应用实体等信息，因此难以提供面向不同使用人员、不同网络应用的服务质量保障功能。

新型的多维统筹的服务质量保障机制在网络中新引入人员实体、网络应用实体等实体类型，由网络运维管理人员基于人员实体、网络应用实体的属性信息，按照管理意图统一映射网络优先级，并分发映射表到相应的网络入口节点[23-25]。入口节点即可根据网络报文中的人员身份属性以及网络应用属性等信息设置报文优先级。入口节点和后续节点可按相应的优先级进行区分处理，从而在全网范围，实现不同级别用户、不同类别应用的精细服务保障能力。

对于可集中统一管理的网络，若其统一纳管使用人员和网络应用等实体，则可以基于多维统筹的服务质量保障机制满足不同用户、不同业务的服务质量保障需求。否则，可采用折中方式：人员未纳管时，可退回到使用 IP 地址或者设备身份替代；网络应用未纳管时，可使用端口号替代。在此基础上统一映射优先级，提供一定的差异化服务质量保障能力。

#### 3.3.2 尽力而为 VS 确定转发

传统的 IP 报文转发本质上采用尽力而为方式。尽力而为方式具有实现简单、统计利用率高等优点，但会导致拥塞崩溃、数据分组时延等问题，难以满足时延敏感等类型的网络业务要求。

为了“准时、准确”地控制端到端的时延，业界面向局域网发展了时间敏感网络（time sensitive network，TSN）等技术[26]。国际互联网工程任务组（internet engineering task force，IETF）的 DetNet（deterministic network）工作组专注于网络层及更高层次的广域确定性网络技术，提出了确定性网络操作、管理和维护整体架构，支持多

跳路由的时间同步、管理、控制操作。

对于可集中统一管理的网络，在时延敏感型业务相对确定的情况下，可预留出合适的网络、计算、存储资源，应用确定转发机制。其他的资源可用于支撑其他转发方式，保障其余业务。

## 4　模型应用

以某领域网络为例，简要说明基于多维属性的领域网络定制模型 DSN-CM 的应用方法。面向最终的部署应用目标，该领域网络节点规模在百万量级以下，以散布全国各地的固定节点为主，部分节点具有移动性。因此，在定制流程中，首先，进行原始属性参数化，将网络规模值域范围设置为 100 万以下，网络移动性设置为 10%以下，网络可否集中管控设置为 1，相应设置其他原始属性参数值。接着，进行领域网络机制化，基于该网络规模和移动性等特征、以及集中管控特点，在路由寻址方面，采用面向网络节点的命名、集中控制与分布协同相结合的路由机制；在安全控制方面，基于身份的密码系统 IBS 设计网络接入认证、不可抵赖性、机密性、完整性相关机制，采用网络隐藏机制以降低攻击面；在服务质量方面，采用多维统筹的服务质量保障机制。随后，确定领域网络机制之后，开展网络机制协议化，针对这些新型机制设计对应的身份路由等协议，结合互联网协议，构建形成该领域网络的基础协议体系。接下来，进行协议体系软件化，针对这些新协议涉及的不同种类的网络节点，设计相应的身份路由等协议软件，结合开源路由协议套件 FRR 的部分协议软件，建立基础协议软件集合。建立网络之后，进行协议软件实例化，启动各网络节点，根据节点角色，加载运行身份路由等相应的基础协议软件。最后，进行配置运维场景化，根据任务需求动态改变网络参数（如身份路由的邻居发现间隔），调配虚拟专线带宽等网络资源，满足用户要求。

## 5　结束语

期望一种网络体制在诸多网络领域都能满足用户需求是不现实的。领域网络的特殊性，为面向领域网络特点解决网络问题提供了约束限定。同时，新型网络技术的发展也为领域网络发展提供了重要支撑，领域网络定制将成为领域网络发展的重要趋势。本文提出了基于多维属性的领域网络定制模型，针对最核心最重要的网络机制化过程，从 3 个方面共 6 个维度探讨基于多维属性的领域网络机制化方法，可以为领域网络机制定制提供参考借鉴和技术支撑。

当前，领域网络定制研究工作还处于初步阶段，领域网络定制模型中的每一个过程都有待于进一步深入研究。

## 参 考 文 献


[1] ZHANG L, AFANASYEV A, BURKE J, et al. Named data networking[J]. ACM SIGCOMM Computer Communication Review, 2014, 44(3): 66-73.

[2] DIPANKAR R, NAGARAJA K, et al. Mobilityfirst: a robust and trustworthy mobility-centric architecture for the future internet[J]. ACM SIGMOBILE Mobile Computing and Communications Review, 2012, 16(3): 2-13.

[3] CASADO M, MICHAEL J F, PETTIT J, et al. Ethane: taking control of the enterprise[J]. ACM SIGCOMM Computer Communication Review, 2007, 37(4): 1-12.

[4] TOM A, KEN B, ROBERT B, et al. A brief overview of the NEBULA future internet architecture[J]. ACM SIGCOMM Computer Communication Review, 2014, 44(3): 81-86.

[5] JOYCE K. Raytheon BBN technologies awarded $16 Million in DoD funding to develop a secure, attributed military network system [EB/OL]. (2011-07-13) [2023-06-10]. https://raytheon.mediaroom.com/index.php?item=1870.

[6] JONES, LI L, SCHMIDTKE J, et al. Practical routing in delay-tolerant networks[J]. IEEE Transactions on Mobile Computing, 2007, 6(8): 943-959.

[7] JARRAYA Y, MONTREA QC, MADI T, et al. A survey and a layered taxonomy of software-defined networking[J]. IEEE Communications Surveys & Tutorials, 2014, 16(8): 1955-1980.

[8] JAIN S, KUMAR A, MANDAL S, et al. B4: experience with a globally-deployed software defined WAN [J]. Computer Communication Review, 2013, 43(4): 3-14.

[9] BOSSHART P, DALY D, IZZARD M, et al. Programming protocol-independent packet processors[J]. ACM SIGCOMM Computer Communication Review, 2013, 44(3): 87-95.

[10] LONG Q, ASSI C, SHABAN K, et al. Delay-aware scheduling and resource optimization with network function virtualization [J]. IEEE Transactions on Communications, 2016, 64(9): 3746-3758.

[11] 王飞跃，杨柳青，胡晓娅，等. 平行网络与网络软件化：一种新颖的网络架构[J]. 中国科学：信息科学，

2017，47：811-831.
WANG Feiyue，YANG Liuqing，HU Xiaoya，et al. Parallel networks and network softwarization：a novel network architecture[J]. SCIENTIA SINICA Infortionis，2017，47：811-831.(in Chinese)

[12] FADLULLAH Z M，TANG F，MAO B，et al. State-of-the-art deep learning：evolving machine intelligence toward tomorrow's intelligent network traffic control systems[J]. IEEE Communications Surveys & Tutorials，2017，19(4)：2432-2455.

[13] ZHAO F，LIU Y P，WANG B S. DROUND：direct routing on unique network-layer identifier[C]//Proceedings of the 6th International Conference on Ubiquitous and Future Networks. [S. l.：s. n.]，2014：328-333.

[14] 国防科技大学. 一种适用于园区网的扁平单播路由方法：201611085243. 5[P]. 2016-11-30.
National University of Defense Technology. A flat routing method for campus networks：201611085243. 5 [P]. 2016-11-30.(in Chinese)

[15] 国防科技大学. 一种软件定义的跨域多路径路由规划方法：201810674497. 3 [P]. 2020-07-17.
National University of Defense Technology. A software defined method for cross domain multipath routing planning：201810674497. 3 [P]. 2020-07-17.(in Chinese)

[16] 国防科技大学. 一种基于软件定义的集中组播控制方法：201810674357. 6 [P]. 2020-05-15.
National University of Defense Technology. A software defined method for centralized multicast control：201810674357. 6[P]. 2020-05-15.(in Chinese)

[17] 高先明，王宝生，邓文平. SDRS：集中与分布控制相结合的弹性多路径路由机制[J]. 计算机学报，2018，41(9)：1976-1989.
GAO Xianming，WANG Baosheng，DENG Wenping. SDRS：elastic multi-path routing mechanism with integration of centralization control and distribution control[J]. Chinese Journal of Computers，2018，41(9)：1976-1989.(in Chinese)

[18] 国防科技大学. 一种报文来源真实性和内容完整性的验证方法：201811624216. X [P]. 2019-04-05.
National University of Defense Technology. A verification method for authentication and integrity of packets：201811624216. X [P]. 2019-04-05.(in Chinese)

[19] 国防科技大学. 一种基于报文认证码的软件白名单控制方法：201811627029. 7 [P]. 2019-04-02.
National University of Defense Technology. A software whitelist control method based on message authentication code：201811627029. 7 [P]. 2019-04-02.(in Chinese)

[20] APPENZELLER G，MARTIN L，SCHERTLER M. Identity-based encryption architecture and supporting data structures[EB/OL]. [2023-06-10]https://www.rfc-editor.org/rfc/rfc5408.

[21] LI K，WANG S，XU S Z，et al. Evaluating the benefit of the core-edge separation on intradomain traffic engineering under uncertain traffic demand[J]. Journal of Network and Computer Applications，2014，40(1)：216-226.

[22] 国防科技大学. 一种基于 LISP 的终端快速移动切换方法：201611083308. 2 [P]. 2019-11-12.
National University of Defense Technology. A fast switching method for mobile hosts based on LISP：201611083308. 2 [P]. 2019-11-12.(in Chinese)

[23] 国防科技大学. 一种用户和业务属性融合的 64 个等级服务质量保障方法：201810731694. 4 [P]. 2020-08-28.
National University of Defense Technology. A 64 level service quality assurance method by integrating attributes of users and applications：201810731694. 4 [P]. 2020-08-28.(in Chinese)

[24] 国防科技大学. 一种多优先级的跨域资源预约集成服务保障方法：201810674502. 0 [P]. 2018-06-27.
National University of Defense Technology. A integration service guarantee method for multiple priority cross domain resource reservation：201810674502. 0 [P]. 2018-06-27.(in Chinese)

[25] ZHAO F，ZHAO B K，YUAN Y L. ABN：attribute based networking for enterprise networks[C]//Proceedings of the 17th IEEE International Conference on Communication Technology. [S. l.：s. n.]，2017：405-411.

[26] NORMAN F. Introduction to time-sensitive networking[J]. IEEE Communications Standards Magazine，2022，6(4)：8-13.

## 作 者 简 介

**王宝生**
男，1970 年生，博士，研究员，博士研究生导师，新世纪优秀人才，研究方向为计算机网络与信息安全
E-mail：wangbaosheng@126. com

**赵 锋**
男，1980 年生，博士，副研究员，研究方向为计算机网络与信息安全
E-mail：fengzhao@nudt. edu. cn

**责任编辑** 董 莉