

如今，基于意图的网络 (IBN) 正越来越多地用于实施基于策略的自动化、服务保障和安全措施。但是，只有在能够与相关应用、系统和流程交换情报时，IBN 的全部潜力才能得以发挥。通过将基于意图的网络转化为开放性平台，可确保 IT 持续有效地满足动态业务和 IT 目标的需求。

基于意图的网络需要开放性平台的原因

2018 年 6 月

作者: **Brandon Butler**, 网络基础设施高级研究分析师

全数字化时代的网络战略

网络对新技术的推动作用已达到前所未有的程度。在连接到云的过程中，网络发挥着核心作用，它推动了移动革命的兴起，并把我们将引向物联网世界。IDC 把这些结构性转变认作第三平台技术，虽然它们提高了效率、带来了新商机、保障了高安全性，但第三平台技术也给网络带来了巨大压力。要充分利用第三平台技术，组织的网络必须实现自动化管理。

然而，IT 部门经常需要将不同的系统作为孤岛加以控制。这就需要以手动方式对网络进行临时的管理。今天，IT 更多地扮演着“人力中间设备”的角色，而非致力于推动令人心潮澎湃的新技术。效率低下的操作会导致安全漏洞，并降低

最终用户和应用的服务级别。“人力中间设备”需要在多个

开放性平台能够简化 IT 和非 IT 系统的自动化管理，要想实现网络的全部价值，这样的开放性平台不可或缺。

系统之间相互关联并交换信息，这通常最终会导致忽视部分至关重要的趋势和活动。为应对这些问题，近年来，网络行业不断进行有力的创新。能够以计算机速度交换情报及相关信息的网络平台现已问世。网络平台显著地提高了效率，使得 IT 能够专注于交付服务和改善用户体验。通过集成安全系统消除漏洞，网络还能成为强大的安全平台。要推动平台运行，支持新应用，并提供

更高级别的网络可编程性，就需要实现更高的自动化水平。基于控制器的网络自动化能推动 IT 作用的提升，并帮助 IT 应对全数字化业务的压力。这种自动化得益于软件定义网络 (SDN)，从更大程度上讲，是得益于基于意图的网络的全方位愿景。

概述

关键主题

IT 需要在管理复杂环境的同时，确保业务需求得到满足，这让他们倍感压力。

重点

基于意图的网络将自动化、可视性和保障水平提升到新的维度。

要点

通过创建开放性网络平台，IBN 将成为整个组织 IT 和非 IT 应用与系统的创新引擎和集成点。

IDC 在 2017 年第四季度对 1000 多家企业进行的一项调查便证实了这一点：参与调查的组织中有超过三分之二表示，希望在下一年内可在其企业园区环境中部署部分软件定义网络（SDN）元素。这项调查显示，受访者使用 SDN 的首要原因是为了提高网络灵活性及支持虚拟化应用（占受访者比例的 55% 以上）；第二大原因是为了实现网络的可编程性与提高 IT 操作效率的目标（占受访者比例的一半）。这些统计信息清楚表明了组织渴望提高自动化水平，并希望从这种自动化中受益。

通过在整个企业内实现应用和流程策略的集中协调，IT 便可利用网络情报来为业务提供支持与保护。但是，要让业务和 IT 应用取得预期结果并充分利用网络情报，必须依赖开放性网络平台。开放性平台可使用已发布的应用编程接口（API）与相邻网络和 IT 服务进行集成并交换情报，并与其他 IT 资源、安全工具，以及业务部门应用和第三方基础设施进行集成。开放性网络平台必须能够从这些来源中获得信息，并自动提供所需的网络资源。

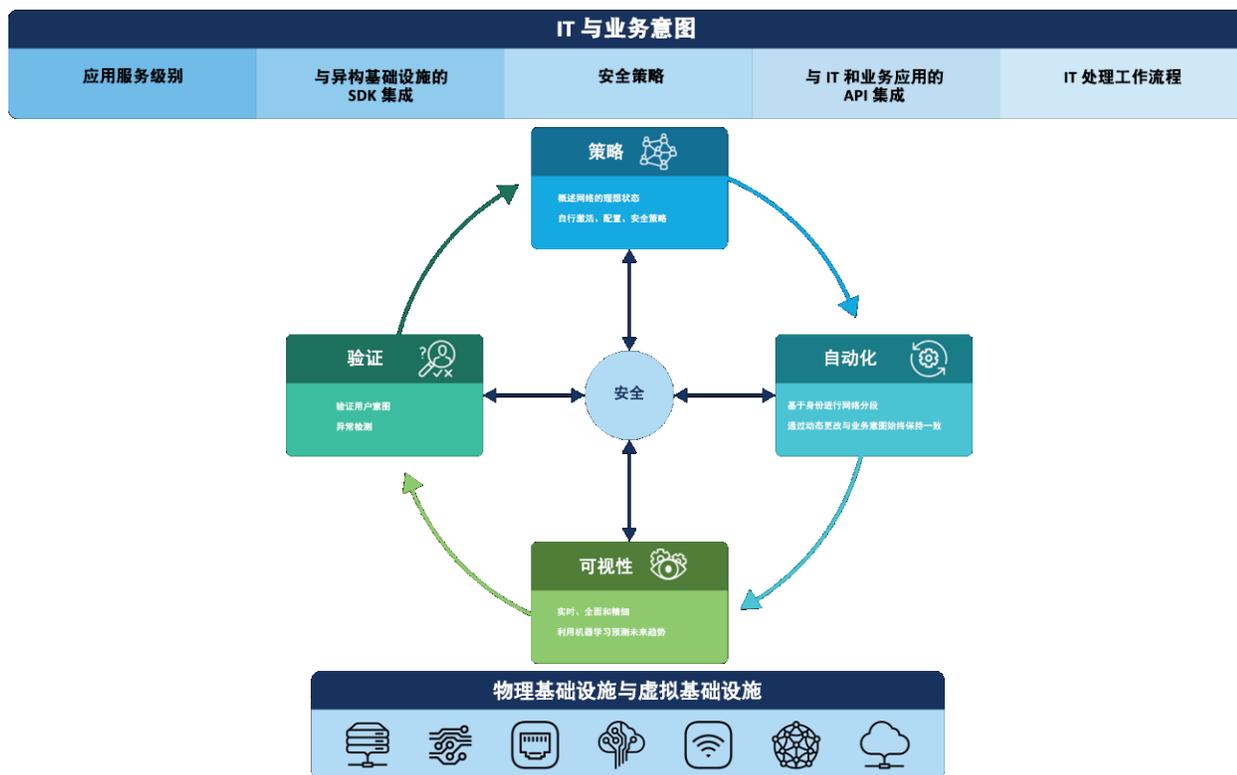
基于意图的网络的定义

基于意图的网络（IBN）是一种行业模型，它以创建面向结果的网络系统为基础，可以通过自动调整来满足以传输或感知方式获得的动态业务和 IT 意图。所谓“意图”，可以是指应用服务级别、安全性和合规性策略、IT 操作流程，以及需要网络支持的任何其他意图（见图 1）。基于意图的网络构建于 SDN 的自动化功能之上，依靠策略驱动的全网自动化交互，以及先进的可视性、分析和保障工具来实施、保护并动态维持所需的网络状态，以满足不断变化的业务和 IT 意图。

只有在能够与相关应用、系统和流程交换情报时，基于意图的网络的全部潜力才能得以发挥。

近年来，IBN 的愿景已开始初显成果，并从特定的单点产品（例如，与用户和设备自行激活相关的产品）向网络范围延伸。IBN 现已发展成为用于管理企业网络完整生命周期的全网自动化系统。下一步，IBN 需要发展为开放性平台，与其他 IT 和业务应用与流程集成到一起。开放性 IBN 平台可确保动态、持续地满足企业对网络的需求。

图 1：基于意图的网络模型



来源：2018 年 IDC

基于意图的网络需要开放性平台的原因

如果没有开放性平台，能够实现基于意图的网络吗？根据定义，IBN 系统会配置资源来确保满足业务需求。但是，要实现这一点，IBN 必须能够从业务和 IT 应用接收数据。IBN 系统必须功能全面，能够与网络工程师所处域之外的应用实现集成。如果没有开放性平台，IBN 系统将无法充分发挥全部潜力。

开放性平台能够简化 IT 和非 IT 系统的自动化管理，要想实现网络的全部价值，这样的开放性平台不可或缺。

要实现意图并为意图提供端到端保障（从客户端和设备到任何位置的任何服务），必须跨所有域（园区、分支机构、广域网、云、数据中心、安全）统一应用策略并提供保障。IBN 需要开放接口来实现策略的跨域传达与协调，并为跨域实施策略提供保障。

另外，IBN 系统也需要开放性平台才能集成到操作工作流程。开放性的 IBN 平台会在整个系统范围自动监控事件或威胁，并自动激活意图策略。如果网络是一个开放性平台，那么 IT 将能够跨多个应用、系统和异构网络设备对可视性、管理、分析、安全性和故障排除进行集中处理，从而提供更好的 IT 和用户体验。

这对安全性而言尤为重要。网络与安全操作之间的交互日益增多，但这些群组往往仍然属于“孤岛”。IBN 系统具有获取并自动执行安全策略的独特能力。但是，要实现这一点，IBN 必须是一个开放性平台，从而确保与安全工具进行集成。开放性的 IBN 平台将成为一个功能强大的分布式安全策略执行器、威胁检测器和缓冲器。IBN 会在网络和安全操作之间架设一座桥梁，从而确保对业务的监控和保护。

开放性网络平台建立在基于意图的网络之上，会根据业务需求不断调整网络，从而弥合业务与 IT 之间的差距。业务和 IT 应用将由此能够充分利用网络功能。为实现所有这些目标，开放性网络平台应提供跨多个组件的集成点，包括：

- **基于意图的应用编程接口 (API)**，让 IT 内部及来自业务线和安全团队的应用和系统能够把需求传达给 IBN。诸如应用策略、合规性设置、必要资源调配、软件映像管理，以及保障已妥善实施自动化等数据，均可通过 API 实施。IT 系统（例如，Active Directory）和业务应用（例如，SAP 或 Oracle）能够通过北向 API 自动传输取得最佳性能所需的网络资源。
- **多供应商软件开发工具包 (SDK)**，让组织或系统集成商合作伙伴能够在开放性网络平台和异构基础设施之间实现自定义集成，从而将第三方网络设备映射到数据模型。通过实施 SDK，能够为思科、Dell-EMC、Hewlett Packard Enterprise 等供应商的基础设施提供 1 级操作支持（例如，发现、资产、拓扑、可用性及运行状况评分）。利用 SDK 还能跨异构网络设备进行自定义集成，从而将这些设备整合到基于意图的网络之中。
- **流程集成 API** 能够与 IT 服务管理 (ITSM)（如 ServiceNow）、IP 地址管理 (IPAM)（如 InfoBlox）及 IT 报告服务（如 Tableau）进行集成，实现跨网络和 IT 操作的自动化工作流程。通过利用其他域集成 API，能够跨技术域（例如，园区、分支机构、局域网、SD-WAN 广域网和数据中心）实现意图和策略交换。与高级威胁检测系统集成后，IBN 可确保在整个组织中一致地实施安全策略。

通过 API 和 SDK 网络扩展性，IT 能够更好地满足业务和 IT 应用的需求，简化操作，并确保对投资的保护。

开放性网络平台的优势

开放性网络平台能够推动构建面向结果的网络。这种网络平台接受来自应用和设备的策略规范、能够利用集中式自动化功能，还能验证系统是否满足业务需求。这些功能不仅仅是用于核心网络基础设施，还能应用于其他硬件设备、安全工具和业务部门应用。通过 API 和 SDK 集成能够实现持续的一致性，这意味着所进行的集成不是仅仅在单一时间点实现的连接，而是建成了一条双向通道来为 IBN 系统提供关键诊断、遥测和运行状况监控功能。反之，IBN 平台能够协调必要资源来确保整个系统安全平稳地运行。这就可以通过简化跨网络系统、IT 应用、业务部门流程和第三方应用（之前单独管理）的工作流程来改善 IT 服务交付。

诸如物理或虚拟防火墙、基于身份的身份认证系统、深度数据包检测、入侵防御等安全服务可以向开放性 IBN 系统馈送数据。反之，IBN 能够动态地配置网络来监控威胁并作出回应（即使流量是加密的）。IBN 系统还会自动确保网络服务始终配置正确，以实现法规框架的合规性。它可以随着环境的变化对网络进行更改，以确保满足合规性要求。

最终用户对开放性网络平台提供的机会非常满意。一家总部位于美国的医疗服务提供商拥有约 15,000 名用户、1,000 台交换机和 60,000 个以太网端口。这个医疗服务提供商的

高水平的网络自动化不仅仅给 IT 带来优势，还对把握新商机大有裨益。

网络经理在企业网络范围内实现了多项功能的自动化。这位网络经理表示：“虽然要管理的 IT 规模庞大，但无需手动配置交换机端口就能实现让用户自动访问适当资源，这给我们带来了巨大优势。”这个多层面的环境包含来自思科、CheckPoint 和 F5 的系统。该经理指出，通过打造开放性网络来与业务应用、异构基础设施及企业范围内的各种系统实现集成，之前需人工完成的任务获得了更多种自动化的方法，这极大提高了 IT 效率。该经理还表示：“如果我们能用一个集中的平台来管理所有这些组件，那么我们实现全方位监控、管理配置并减少因使用单独管理平台而浪费的时间就有了完美解决方案。”

开放性 IBN 使用案例

统一通信 (UC) 应用的网络需求非常强劲且难以预测。通过开放性的 IBN，UC 应用可通过 API 自动传达所需的网络资源，从而确保为 VOIP 通话提供高质量的服务。

通过开放式集成，UC 系统实现了与 Active Directory 协作的对接来对会议参加者进行身份验证，并通过调用 API 来确保整个通话期间带宽充足。用户可以在通话时提供实时反馈，开放性网络平台会采集这些信息并自动进行更改，从而优化通话质量。通话结束后，开放性网络平台会自动对发起通话的部门执行回收操作。

如果没有开放性网络平台，所有这些流程都需要 IT 人工干预。而在开放性网络平台上，它们是通过智能的 IBN 完成的。在企业中，可以针对企业资源规划 (ERP) 流程、计费、客户拓展、后勤保障、人力资源和许多其他服务创建类似的自动化工作流程。

引入高水平的网络自动化对 IT 以外的领域也大有裨益。依靠人工流程来完成新应用、新设备或新用户的自行激活会减缓探索新商机的进程。开放性网络能够精简流程，从而更好地为新技术提供支持。想象一下，营销部门发现的一个基于云的应用很有吸引力，利用它能寻找新的潜在客户。开放性网络平台可自动启用基于身份的访问策略，从而只寻求部分高管访问该应用。新应用和后端企业数据库之间的 API 集成可以使用 IBN 进行配置和管理。监控工具可集成到系统中，用来跟踪应用和企业之间的所有通信，从而确保适当的安全检查始终落实到位。凭借开放性网络平台，IT 成为了实现此款新应用的推动因素，而绝不是阻碍因素。

在物联网 (IoT) 部署等大型环境中，这种对应用、设备和流程基于网络的自动化管理特别有用。管理这些设备的生命周期（从自行激活到优化网络连接，再到确保安全策略时效性）需要采用自动化网络平台来支持各种基础设施、分析工具和连接方法。此过程可直接集成到一个开放性的 IBN 平台之内。当设备上线时，网络可以自动识别它们，然后系统会安装适当的配置并运行验证检查，以确保它们符合要求。在设备运行过程中，开放性 IBN 平台能够监控诊断信息并自动配置网络设置来促进将数据从设备传输到中央位置，而且所有连接均实现加密。如果采用人工方式，每一道流程设置和执行起来都可能需要繁重工作。然而，采用开放性的 IBN 平台则可实现物联网工作流程的完全自动化。

开放性的网络平台面向未来，能够支持新的应用和基础设施，并把它们整合到 IBN 工作流程之中。

作为开放性平台，网络也具备满足未来需求的特点。为企业内各种应用和服务开发的 API 和 SDK 可以随时更改。新的应用、基础设施和设备进入网络后，可以将它们所需的网络资源传达给开放性的 IBN 系统。开放性网络已成为网络管理平台面向未来的一种方式，它能够确保网络管理平台不仅能够满足当今的业务需求，还能满足未来增长的网络需求。

开放性网络平台也会在 IT 的控制下跨多个域实现扩展。数据中心、企业园区、广域网和云之间的集成将日益增长。通过在这些域实施一致的策略、自动化及分析，能够提高可视性和保障水平。开放性 IBN 能够确保不论应用或流程在什么地方运行，网络都能不断满足业务需求。

关于思科

为了满足 IT 对动态且高效的基础设施日益增长的需求，思科启动了重要激励措施，在业界率先跨多个技术域交付基于意图的网络系统。这包括在数据中心、私有云、园区、广域网和分支机构中提供基于意图的开放性网络模型。

对于数据中心和私有云，基于意图的网络首先通过使用思科 Tetration 了解应用需求来捕获业务意图。接下来，利用以应用为中心的基础设施来定义、策划和管理 IT 策略。网络保障引擎通过高级分析功能提供持续保障，从而使网络运行保持理想状态。IT 团队能够在开放且可编程的环境中使用自己的工具。思科还通过技术合作伙伴提供广泛的解决方案，且这些合作伙伴形成了广泛的集成解决方案生态系统。

此外，思科还在整个园区、分支机构和广域网中提供了一个开放且可扩展的基于意图的网络平台，称为思科全数字化网络架构 (DNA)。DNA 中心是 DNA 的核心，它起着控制中心作用，能够提供基于意图的企业级封闭式网络的所有要素，包括基于策略的自动化、市场细分以及高级可视性、分析和保障。

随着基于意图的 API、流程和域集成 API 以及多供应商的 SDK 的推出，IT 团队和开发人员现在可以在 DNA 中心本地自动化、保障和分析功能的基础上构建集成并进行创新。IT 团队现在可以自行使用这些开放接口，也可以利用思科的合作伙伴生态系统来对网络进行定制，从而满足自己特定的 IT 和业务目标。DNA 中心提供多种跨域集成，包括数据中心内的思科 ACI、Stealthwatch 安全和 Meraki 网络。

结论

组织需要提高敏捷性并获得对环境动态的更深入可视性。如今，对通过自动化流程来取代网络系统中人工临时管理流程的呼声越来越高。此外，组织需要确保系统以安全的方式进行管理，从而提供绝佳的应用和最终用户体验。这正是基于意图的网络的行业愿景要承诺实现的目标。

只有凭借开放性平台方法，IT 团队才能发挥基于意图的网络的全部价值，从而实现与其他 IT、业务应用、系统及流程的集成。这使得 IBN 原则能够在整个企业范围内实现业务需求与 IT 执行的对接，并确保整个企业获得可靠且安全的网络性能。

通过使用基于意图的集成 API、SDK 和定制集成，组织可以简化 IT 运营，确保环境安全性，并集中管理不同的系统。这让 IT 能够摆脱“人力中间设备”角色，利用自动化平台来确保网络满足组织当今和未来发展的需求。



关于分析师:
Brandon Butler, 企业网络高级研究分析师

Brandon 负责探究以太网交换、路由、无线局域网和邻近新兴市场（如 SDN 和 SD-WAN）的市场和技术趋势，并开展预测和竞争分析。在加入 IDC 之前，Brandon 有十多年的技术和业务记者从业经验。他在 Network World 工作了六年，担任新兴网络技术领域（包括软件定义网络 [SDN] 和软件定义广域网 [SD-WAN]）高级编辑。

 **IDC Custom Solutions**

本出版物由 IDC Custom Solutions 编写。除非注明具体的供应商发起人，本文展示的观点、分析和研究结果均源自 IDC 独立进行和发布的更为详细的调查和分析。IDC 定制解决方案以多种形式提供 IDC 内容，供众多公司发行。许可分发 IDC 内容并不表示对被许可人或其观点的认可。

IDC 信息和数据的外部出版 — 凡是在广告、新闻发布稿或促销资料中使用任何 IDC 信息，都必须事先获得相应 IDC 副总裁或国家区域经理的书面同意。此类申请均应附上所提议文件的草案。IDC 保留以任何理由拒绝批准外部使用的权利。

版权所有 2018 IDC。未经书面许可，严禁复制。

IDC Corporate USA

5 Speen Street
Framingham,
MA 01701, USA
电话 508.872.8200
传真 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com