基于意图的网络

弥合业务部门与 IT 部门之间的差异

简介

数字经济的演变是不可阻挡的潮流，网络在其中居于核心地位。全数字化正在以前所未有的速度改变企业、合作伙伴、员工和消费者之间的交互方式。通过基于 Web 的应用，人们只需点击一个按钮，即可定制、订购和交付产品及服务。业务数据现在可以即时获得、分析和交换。企业和消费者之间的地理界限正在趋于消失。其中，在推动数字经济发展的应用通信中，网络居于核心地位。

越来越多的传统企业和数据中心网络架构承受着快速适应这些动态需求的压力。应用正在向公共云、私有云和混合云环境迁移，并作为服务提供，从而模糊了企业网络和不受信任域之间原本定义明确的界限。受益于开源软件、容器、微服务和敏捷开发流程等大趋势，开发人员无需几个月乃至几年，而是只需短短几天就可以把应用从概念设计阶段推进到生产阶段。员工和客户希望能随时随地使用任何设备建立连接，以随时访问信息。随着物联网 (IoT) 的发展，传感器和自主管理型设备越来越多地实现了互联。与此同时，网络威胁正变得更加复杂，对所有组织的品牌声誉和财务方面构成危险。

传统的企业和数据中心网络架构及其各自的业务流程需要不断发展，以紧跟这些趋势。具体地说，新网络需要：

- 支持新的全数字化业务计划，而不是加以阻碍。具有灵活性，可迅速改变以适应不断快速变化的业务目标。
- 面对日益增长的规模和复杂性，更易于配置、操作和维护。当前的运营模式不可扩展或可持续。
- 在以下方面提供充分的可视性：网络的运作方式，以及如何保障支持所需的业务计划并实现合规性。识别任何差异并建议改正措施。
- 提前识别并消除安全威胁，防患于未然。多重云、物联网和移动的采用催生了新的威胁载体，网络需要针对它们不断加以防范。

目录

简介

目的：弥合业务部门与 IT 部门之间的差异

基于意图的企业网的构建块

- 转换
- 激活
- 保障

多域环境中基于意图的网络

基于意图的网络的优势

- 更高的业务灵活性
- 提高运营效率
- 网络与业务目标不断保持一致
- 更好的合规性和安全性
- 减少风险

转换到基于意图的网络

相关详细信息

这促使 IT 行业对更智能网络（通常称为“基于意图的网络”）的兴趣日益增长。

基于意图的网络 (IBN) 在如何规划、设计和操作网络方面提供了一个重要的范式转变。过去，工具无法声明意图并将其转换为实现预期结果所需的设备级配置。相反，网络设计师或操作员必须手动获得单个网络元素配置以支持所需的意图，例如，“我希望可以通过这些分支访问这些服务器；因此，我需要在网络中的每个设备上配置特定的 VLAN、子网和安全规则。”

基于意图的网络解决方案将常规做法（需要手动获得的单个网络元素配置的一致性）替换为由控制器引导的和基于策略的抽象，这更便于操作员表达意图（期望的结果），并随后验证网络正在执行他们所要求的操作。

与全数字化转换相关的规模、敏捷性和安全性需求要求按元素的网络配置替换为网络元素的自动化系统范围编程，这些元素具有一致的基于意图的策略。此外，在部署之前、期间和之后对数据进行情景分析，可以进行连续的验证，以帮助确保网络在任何时间点都提供所需的结果和保护。从多种不同来源不断收集遥测和其他形式的数据提供了丰富的信息环境，以优化系统并确保其安全。

基于意图的策略超出了客户端或应用的访问控制范围。它扩展到表达所需用户体验、应用优先级、需要应用于应用流的服务链网络功能，甚至是操作服务级别协议 (SLA) 规则，如“我只想在我的网络设备上部署黄金映像。”

“Gartner 认为基于意图的网络的最大好处是提高了网络的灵活性和可用性，并支持跨多个基础设施的统一意图和策略。”

- Gartner，2017 年

思科认为，一个完整的基于意图的网络（图 1）需要提供一些基本功能：

- **转换：**转换功能是关于意图的表征。它使网络操作员能够以声明性和灵活的方式表达意图，表示将最好地支持业务目标的预期网络行为是**什么**，而不是应**如何**配置网络元素以实现该结果。
- **激活：**然后需要将捕获的意图解释为可以在网络上应用的策略。激活功能使用全网自动化将这些策略安装到物理与虚拟网络基础设施中。
- **保障：**为了连续检查网络在任何时间点都遵守表达的意图，保障功能将保持连续的验证和确认循环。从遥测数据中提取的情景用于检查操作与意图的一致性。

图 1. 基于意图的网络功能

本文通过概述基于意图的网络的愿景及其架构带给网络策略师和建筑师的优势，并介绍思科对向基于意图的网络演进的观点。本文概述了基于意图的网络的主要功能构建块，并从数据中心和企业网络的角度提供了具体的示例。

Gartner，创新洞察：基于意图的网络系统，Andrew Lerner，Joe Skorupa，Sanjit Ganguli，2017 年 2 月 7 日

目的：弥合业务部门与 IT 部门之间的差异

今天，实施业务需求需要大量的人工解释和手动干预，以确保 IT 系统满足这些需求。在大多数情况下，该过程很长，资源非常密集，而且容易出错。在要服务的系统、设备、应用和服务越来越多的灵活全数字化业务环境中，这不符合环境的标准。

基于意图的网络以业务语言捕获业务意图，并将此意图转换为可在网络中应用和不断监视的 IT 策略。图 2 提供了意图（“什么”）和执行（“如何”）之间的区别示例。

图 2. 意图表达示例

基于意图的企业网的构建块

基于意图的网络提供了三个主要功能构建块（图 3）：捕获意图的功能、在整个网络基础设施中自动部署所表达意图的功能，以及确保预期意图正在实现的功能。

图 3. 基于意图的网络 (IBN) 的构建块

转换

转换涉及基于意图的模型中的几个功能。一个或多个操作员或一组操作员有能力描述他们所期望的意图。这可能采用易于使用的图形用户界面，这种抽象模型（如 YANG 或 JSON/XML）直观且与业务目标相关，甚至与预定义的语法或语言相关。应用开发人员可以作为连续集成/连续交付 (CI/CD) 过程的一部分定义该模型，将来甚至可以通过文本到语音转化表达来实现，操作者口头说出意图，基于意图的系统执行并提供口头或其他反馈。在对网络作业的这一接近业务的抽象的表达形式中，应当将基于意图的方法与传统的网络架构区分开来。

转换的另一个功能是将捕获的意图统一为公用的基于模型的策略 (MBP)，这通常需要借助于基于控制器的架构。由各种输入机制表示的意图（可能跨越多个网络域）转换为此类标准 MBP - 通过此基本步骤，可利用自动化，并允许应用复杂的一致性和完整性检查。

其中，从传统的网络部署迁移到 IBN 部署是一个重要挑战。在这种情况下，当前网络中已经存在有影响的策略，但网络操作员不一定具有所有当前部署策略的列表或完全可视性。因此，必须执行自动主机发现和策略发现，以确定操作中的策略，为操作员提供所有正在运行的策略的完全可视性以供审查，然后在 IBN 部署中自动激活所需的策略。

激活

激活功能确保派生的 MBP 在任何相关网络域中传播。IBN 中的物理或虚拟网络功能可以在不同的可操作区域（数据中心、广域网、分支机构、园区）中由相同或不同的运营团队管理。基于意图的网络中的协调功能允许将 MBP 传播到相关域中，这意味着策略也可以在范围内限制到网络的特定部分。

激活还可能使用其他功能进一步派生相应的设备配置。域的控制器可以将有关网络元素的信息、它们的功能和具有表达

MBP 的拓扑关联起来，以建立适当的设备配置。在使用基于标准的 API（如网络配置协议 [NETCONF] 或 YANG，或代表性状态传输 [REST]）编程网络元素之前，还可以应用对配置级别一致性的其他检查。

保障

保障是基于意图的网络的关键功能。它使用数据的情景分析来提供验证，即已按预期应用意图，并不断验证所期望的结果是否已实际实现。基于意图的网络的保障能力涵盖了三个主要方面，图 4 也强调了这几个方面：

- **在部署之前、期间和之后不断验证 IBN 系统行为：**检查系统行为是否在任何时间点都与表达的意图一致。此功能需要对网络元素状态和事件进行持续观察。基于意图的遥测数据具体衡量表达意图的表现，不断地收集该数据并报告给 IBN 保障功能。保障算法，包括从正规数学模型到基于遥测和机器学习的方法，保障网络状态和行为在域和跨域级别上都与期望的意图一致。
- **基于分析（事件的相关性以及利用机器学习和人工智能 [ML/AI]）获得洞察力以进行验证、理解和预测：**除了验证当前网络状态及其与表达的意图相一致，保障功能还可以针对基于意图的网络行为获得更复杂的洞察力和可视性。例如，保障功能可以在应用更改之前预测任何不符合所表达意图之处，了解或预测趋势，标识异常，预测和验证系统级网络性能。
- **利用封闭式循环来实现纠正操作和优化：**通过利用激活构建块以实现系统范围调整，可以通过编程方式补救异常、违反和简单的缺少 SLA（表达意图）情况。因此，基于意图的网络使相应机制能够自动纠正任何违反基于意图的策略之处，或者允许自动进行连续优化，以保障网络在任何时间点实现表达的意图。请注意，根据策略的不同，操作可以自动执行，也可以作为建议提供给操作员，在这种情况下，操作员决定执行。

图 4. 保障的三个主要方面

在下面的表 1 中列出了传统网络与基于意图的网络之间的主要架构、构建块和结果差异。

表 1. 比较传统网络与基于意图的网络

服务内容	传统网络	基于意图的网络
架构	• 逐个设备管理 • 单向配置 • 不可编程设备 • 不稳定网络安全	• 全网系统管理 • 闭环自动化配置和保障 • 可编程物理与虚拟基础设施 • 系统地集成在整个架构中的安全功能 • 以 API 为中心，基于模型 • 开放式硬件和软件堆栈
转换	• 临时操作符解释和临时转换	• 支持，通过意图捕获和转换系统功能进行转换
意图验证	• 不支持	• 支持，完整性和一致性检查
策略支持	• 有限，通过设备命令表达	• 基于模型的基于意图的策略
激活	• 有限，通过设备命令表达	• 自动化，通过控制器网络级激活
遥感勘测	• 有限支持	• 广泛支持
保障	• 手动，逐个设备	• 自动化，支持通过 AI/ML 或形式方法进行完整分析
反馈环路	• 基于操作员临时的手动监控	• 实现操作员或系统激活自动化
成果	• 有限、尽力而为的业务一致性 • 规模管理复杂且成本高昂	• 持续的业务一致性 • 简化、高效的规模管理

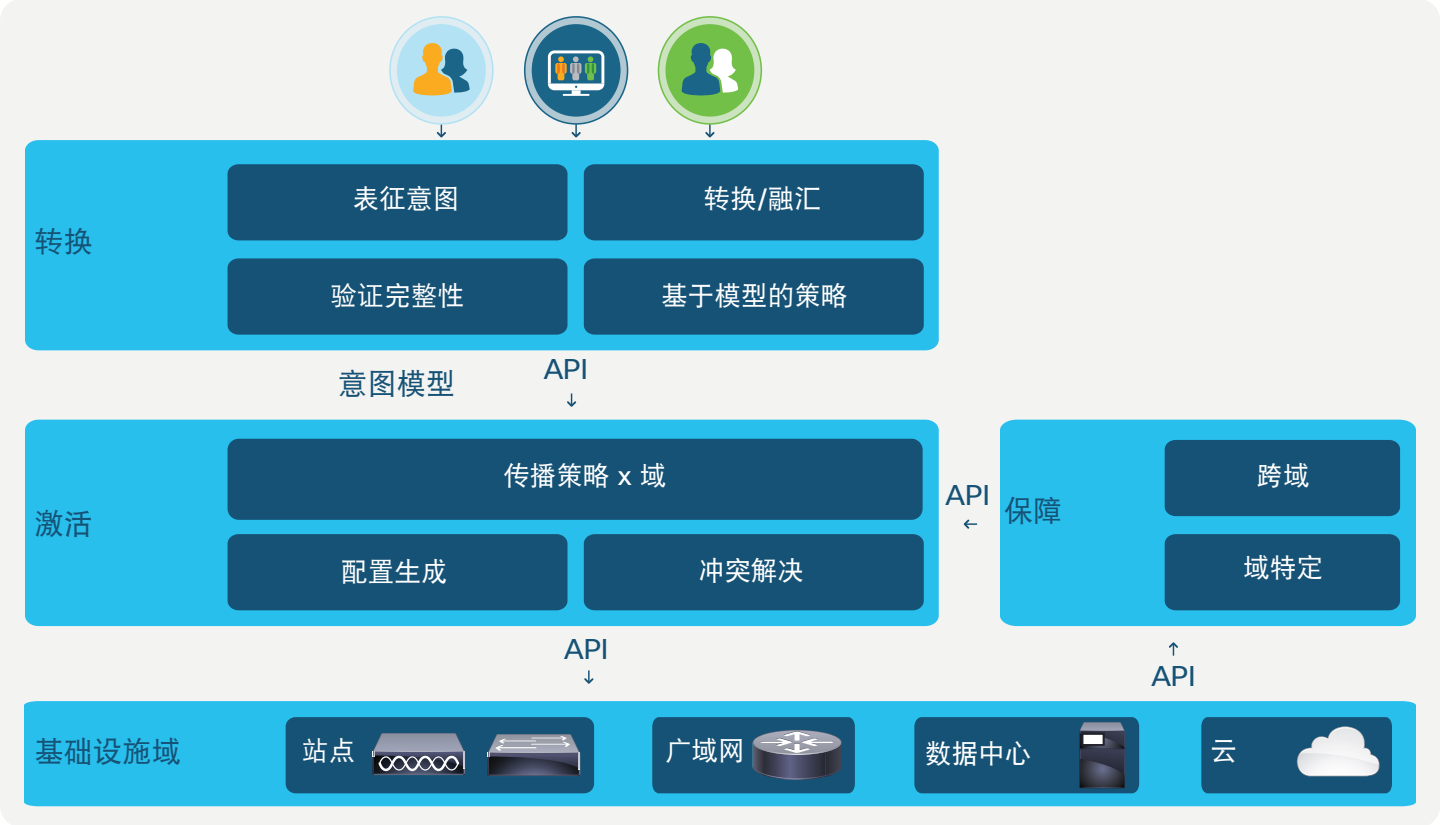
多域环境中基于意图的网络

企业的网络基础设施可以在不同域中进行管理，将操作职责拆分到园区和分支站点、WAN、数据中心和云。在数据中心或云中托管的应用以及客户端也可能有自己的操作过程，因而被视为域。在基于意图的网络中，预期由一个控制器管理一个或多个域，该控制器提供基础设施的整体视图，并保持一致状态（配置、软件映像等）。

基于意图的系统将网络基础设施的这一安排纳入到域中。跨域应用转换和协调功能，允许在园区和分支站点、WAN、数据中心和云中对全网络的基于意图的策略进行表征。协调功能将捕获的策略传播到相关域，也可以通过设计限制某些策略的范围。特定于域的控制器自动将基于模型的策略转换为特定于设备的配置，并将它们实例化到网络基础设施中。IBN 保障功能可应用于特定域，以确保遵守基于意图的明确策略。此外，保障功能跨域运行，以检查网络范围和端到端（从应用到应用，无论应用的托管位置）是否符合表达的意图。

图 5 展示了 IBN 的转换、激活和保障构建块的附加功能细节，以及它们如何与不同的基础设施域相关。该图还突出显示了反馈环路，它将保障功能获得的洞察力发送回激活功能，来进行网络的持续优化。

图 5. 基于意图的网络模型和功能详细信息



基于意图的网络的优势

基于意图的网络方法可以为业务和 IT 主管带来一些好处。其中包括改进的业务灵活性和操作效率、更好的合规性和安全性、持续 IT 和业务协调以及降低风险。

更高的业务灵活性

开放 API 支持的 IBN 的抽象性和完全自动化性质确保了网络能够响应数字经济中预期的动态。新应用可以在最合适的地方（企业数据中心、虚拟私有云 (VPC)，甚至是作为服务使用）快速加入网络。基于意图的系统抽象地捕获新应用意图的能力简化了向此类应用提供连接性和安全性的过程。复杂的完整性检查、与应用相关的网络策略的自动配置以及持续的保障使基础设施团队能够自信地支持快速的应用开发。

提高运营效率

IBN 提供的功能保障了运营效率，甚至降低了运营支出 (OpEx)。预计能够大大减少网络操作员用于网络设计、实施、测试和故障排除的时间。基于意图的网络完全是模型驱动的：操作员可以直观地表达意图，并易于转换成基于模型的策略。在模型中捕获意图后，可以应用复杂的一致性和完整性检查，以确保新的意图与先前表达的意图一致，或者不同操作组表达的意图一致。将基于模型的策略转换为标准的网络元素配置可以完全自动化，从而提高网络的一致性。因此，IBN 极大地简化了传统过程，即为架构中每个网络元素的策略手动派生命令行界面 (CLI) 配置，每当新的应用或设备类型加入时都重复此手动过程，并确保任何配置更改不会破坏或违反先前的策略。

基于意图的模型中的抽象和自动化级别也支持全数字化网络架构中预期的规模增长。例如，意图和策略通常表示为组级别。对应用、设备和用户进行分组以及表达与关联组相关的意图支持简化的操作模型。随着新员工加入公司或应用层级扩展，可以在现有组中创建新端点，从而利用以前表达的意图和策略。此外，IBN 的标准化和自动化特性本质上支持比传统的手动、非自动化过程更高的规模。

通过其闭环设计，基于意图的网络也大大减少（或者在许多情况下消除）了在当今网络中发生的复杂的故障排除情况。保障过程验证网络配置与意图的一致性，因此可以在潜在问题发生之前发现问题，或者可以快速高效地找出问题的根本原因。

对常见问题的标准更改甚至可以自动化，同时保持与 IT 服务管理 (ITSM) 系统的集成，可能会进一步显著降低运营支出。IBN 可以推动由操作员策划的知识库（例如，当今表现为帮助台工具或配置管理数据库）转变为系统或机器学习的知识库，作为实现闭环自动化的途径，该知识库涵盖越来越多的“预先批准”更改。

网络与业务目标不断保持一致

基于意图的网络系统允许以抽象的、业务性的术语表达网络的期望行为：**什么**，而不是**如何**。此功能有助于确保网络始终与业务运营完全一致。以前，将业务目标转换为设备配置是由高技能工程师执行的过程。例如，业务目标

“应用 X 对业务至关重要”需要深入了解每个网络元素以过滤应用 X 流量，并在网络中的每个相关跃点上配置各自的服务质量 (QoS) 策略。在 IBN 中，同样表达的意图被转化为策略，并且网络元素的配置完全自动化。IBN 内置的反馈机制会检查衍生策略是否始终得到遵守，并且如果网络不再符合所表达的意图，则可以帮助自动调整网络配置。

更好的合规性和安全性

虽然有时会被忽视，但改进的保护和快速威胁遏制实际上是基于意图的网络可以实现的主要优点之一。IBN 中的每个构建块都有助于显著提高网络的整体安全性和合规性。与安全性和合规策略相关的意图持续保持一致应该成为 IBN 的核心目标。为实现此目标，将安全性作为每个 IBN 功能区域的组成部分，并提供闭环策略实施和威胁遏制。安全操作团队可以独立于其他操作组来表示安全策略。架构中的完整性验证功能会检查策略是否互相抵消。此外，正在进行的遥测和保障功能提供了最新的网络状态图，这对于安全性和合规性报告至关重要。先进的分段技术可防止终端、用户和应用之间横向感染的传播，以保护核心资产的可用性。

减少风险

随 IBN 引入的抽象、自动化和保障承诺降低在用户、设备和应用之间提供通信服务的整体操作风险。在基于意图的系统中，最大程度减少手动、易出错的基于 CLI 的进程。例如，请考虑网络中流量过滤器的情况。通常，在整个网络中配置访问控制列表 (ACL) 以过滤流量，以实现安全或流量控制目的（QoS，路径确定）。许多 ACL 随着时间的推移而增长，并且做出任何修改都有可能会造成安全漏洞，或者可能会抵消以前所期望的策略。IBN 中基于意图的策略的可预测和一致的表达，应用一致性和完整性检查（例如使用形式化数学方法）的能力，以及标准化转换和部署到网络元素配置中都可以提高网络的一致性 - 甚至面对多个操作员组和不同的技术。

此外，基于意图的网络通过预测对全系统网络状态的影响来显著降低网络故障的风险。例如，考虑主站点正常运行的情况，但仅在灾难恢复情况下访问的辅助站点不适用。IBN 系统将能够识别这种潜在的错误配置并将其标记给操作员（或自动纠正）以避免潜在的网络故障。

“我们认为，全面的 IBNS 实现可以将网络基础设施交付给业务主管的时间减少 50% 到 90%，同时将停机的次数和持续时间减少至少 50%。”

- Gartner，2017 年

Gartner，创新洞察：基于意图的网络系统，Andrew Lerner，Joe Skorupa，Sanjit Ganguli，2017 年 2 月 7 日

转换到基于意图的网络

对于许多组织而言，向完全基于意图的网络的进化将是一个旅程，需要结合现有和新技术以及过程变化。当在所有网络域（包括数据中心、园区、分支和 WAN）中部署 IBN 时，其全部潜力最终得到认可。

整个行业中的许多举措都在努力实现意图承诺，而许多有助于建立基于意图的模式的功能构建块今天都可以使用，而且已经提供了大量的好处。许多基础元素（包括软件定义的网络、虚拟化和分析）已经成熟到可以在今天进行部署的地步，这是更长期的基于意图的策略的一部分。通过自动发现组织的当前网络上运行的主机和策略，然后为操作员提供相应功能以审查运行策略并确定应在其 IBN 中激活哪些策略，还可以大大简化并加速向 IBN 的转换。

思科正在帮助 IT 领导者在我们的数据中心和企业网络的开放平台以及第三方技术的生态系统的基础上，着手实现端到端的基于意图的网络。

在数据中心中，Cisco® 以应用为中心的基础设施 (Cisco ACI™) 解决方案提供了基于策略的自动化网络结构，涵盖基于意图的框架转换和激活阶段，而思科网络保障引擎在数据中心网络中提供保障。

在企业网络方面，思科全数字化网络架构 (Cisco DNA™) 为企业园区、分支和 WAN 环境提供类似的服务，为有线和无线、软件定义的访问和软件定义的广域网域提供转换、激活和保障功能。此外，思科的身份服务引擎提供基于身份的策略和丰富的上下文信息。

将网络提升到基于意图的模型的旅程正在进行之中！

相关详细信息

了解有关基于意图的网络的更多信息：https://www.cisco.com/c/en/us/solutions/enterprise-networks/intent-based-networking.html

C11-740210-00 01/18